Le théorème de Mordell pour les courbes elliptiques

Simone Melchiorre Chiarello et Maxime Chaminadour

juin 2014

Table des matières

1 Introduction

L'étude des points à coordonnées rationnelles sur une courbe algébrique est liée à la recherche de solutions entières aux équations diophantiennes, ces solutions entières étant *a fortiori* des solutions rationnelles. On entend dans un premier temps par *courbe algébrique* le lieu des zéros dans le plan d'un polynôme à deux variables. À de telles courbes, on peut associer un entier positif, le *genre*, dont la définition précise ne sera pas discutée ici, mais que l'on peut exprimer comme $g = ((d-1)(d-2))/2$ où d est le degré de la courbe (ici on a exprimé le genre dit *arithmétique*).

Lorsqu'une courbe "lisse" est de genre 0 (donc de degré 1 ou 2, il s'agit d'une droite ou d'une conique), il suffit d'avoir un point rationnel pour pouvoir paramétrer tous les autres points rationnels. Il y en a alors une infinité. Pour les courbes "lisses" de genre plus grand que 2 (donc de degré plus grand que 4), le théorème de Faltings précise qu'il y a toujours un nombre fini de points rationnels. Le présent texte porte sur les courbes de genre 1 (de degré 3), les courbes elliptiques. Celles ci sont munies d'une loi de groupe abélien naturelle, qui facilite leur étude. Nous allons ici démontrer un résultat central de l'étude des points rationnels sur les courbes elliptique, le théorème de Mordell, datant de 1922, qui stipule que le groupe des points rationnels sur une courbe elliptique est de type fini.

2 Notions générales

2.1 Première définition et énoncé du théorème de Mordell

Nous allons ici énoncer la définition que nous utiliserons des courbes elliptiques. Celle ci sera justifiée dans la partie suivante.

Définition 1. *Un courbe elliptique E définie sur un corps K est le lieu des zéros d'une équation de la forme*

$$E : Y^2 = X^3 + aX + b,\ a, b \in K,\ 4a^3 + 27b^2 \neq 0$$

Il sera utile dans la suite de considérer la courbe dans l'espace projectif $\mathbb{P}^2(K)$, on utilisera alors l'équation homogène

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

On notera $E(K)$ l'ensemble des zéros de cette équation dans $\mathbb{P}^2(K)$, et on distingue le point $O = [0 : 1 : 0] \in E(K)$.

La condition $4a^3 + 27b^2 \neq 0$ assure que la courbe ne contient pas de points singuliers.

Les courbes elliptiques seront les objets principaux que l'on étudiera dans la suite de cet exposé, avec une attention particulière pour les courbes définies sur $\mathbb{Q}$. On verra que les courbes elliptiques ont beaucoup de propriétés algébriques et sont pour ça très étudiées. L'un des faits les plus importants est que si E est une courbe elliptique définie sur un corps K, alors $E(K)$ est munie d'une structure de groupe abélien. Le but de tout le travail sera de démontrer le *théorème de Mordell*, qui stipule que ce groupe est de type fini, dans le cas $K = \mathbb{Q}$. On démontrera d'abord la version faible du théorème :

Théorème 1. *Si E est une courbe elliptique définie sur le corps des nombres rationnels $\mathbb{Q}$, le groupe quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini.*

Après, par une procédure de *descente* qui permet de remonter d'un quotient A/mA au groupe A (avec A un groupe abélien et m un entier positif), on montrera la version forte

Théorème 2. *Si E est une courbe elliptique définie sur le corps des nombres rationnels $\mathbb{Q}$, le groupe des points rationnels $E(\mathbb{Q})$ est de type fini.*

Il y a beaucoup de problèmes ouverts dans le domaine des courbes elliptiques, dont le plus important est peut-être la conjecture de Birch et de Swinnerton-Dyer, qui exprime le rang du groupe des points rationnels d'une courbe elliptique en fonction des propriétés d'une fonction analytique particulière : la fonction L de Hasse-Weil. On ne traitera pas de cela dans cet exposé.

La preuve du théorème de Mordell n'utilise que la définition que l'on vient de donner. La lecture de ce qui suit n'est pas nécessaire à la lecture de la preuve, mais la preuve que la condition $4a^3 + 27b^2 \neq 0$ est équivalente à la lissité de la courbe est effectuée ci-dessous (proposition 3).

2.2 Définitions et propriétés supplémentaires

Dans cette section on introduira les courbes elliptiques en partant des courbe algébriques, et on montrera les propriétés fondamentales de ces objets. Ces notions permettent d'avoir une idée géométrique d'une courbe (et par exemple, la définition de la loi de groupe est donnée en termes géométriques). Comme les résultats de cette première section ne seront pas fondamentaux pour le sujet principal (le théorème de Mordell) et aussi à cause de la difficulté de certains théorèmes, certaines preuves sont omises. Avec K on dénotera toujours un corps algébriquement clos, mais dans la suite il sera suffisant de considérer le corps $K = \mathbb{C}$ des nombres complexes.

Définition 2. *Soit n un entier positif et $A = K[x_1, \ldots, x_n]$ l'anneau des polynômes en n variables. Soit $I \subseteq A$ un idéal. La* variété *de I est l'ensemble*

$$V(I) = \{z \in K^n \mid p(z) = 0,\ \textit{pour tout } p \in I\}$$

De façon duale, on définit l'*idéal* d'un ensemble $Z \subseteq K^n$ comme

$$\mathcal{I}(Z) = \{p \in A \mid p(z) = 0 \text{ pour tout } z \in Z\}$$

Dans ces définitions, on dit que $V(I)$ est une *variété affine*, car c'est un sous-ensemble de l'espace affine K^n, et on dit que cette variété est *plongée* dans K^n. Il est clair que $V(A) = \emptyset$ et $V(0) = K^n$. Il est aussi évident que $I_1 \subseteq I_2$ implique $V(I_1) \supseteq V(I_2)$. Une variété V est dite *irréductible* si écrire $V = V_1 \cup V_2$ où les V_i sont des sous-variétés (c'est-à-dire des sous-ensembles qui sont aussi des variétés plongées dans le même espace) implique $V_1 = V$ ou $V_2 = V$. Il est facile de montrer que si V est une variété irréductible, son idéal $\mathcal{I}(V)$ est un idéal premier, et que la réciproque est vraie aussi (cela dépend lourdement du fait que K est algébriquement clos). Comme A est noethérien, chaque chaîne décroissante de sous-variétés $V_1 \supseteq V_2 \supseteq \ldots$ a une longueur finie. Le maximum de ces longueurs avec tous les V_i irréductibles est appelé la *dimension* de la variété (si la chaîne a n variétés, sa longueur est $n-1$, et la variété vide n'est pas considérée irréductible). Il n'est pas tout à fait trivial que cette dimension soit finie : cela découle d'un fait général sur les K-algèbres de type fini.

Théorème 3. *Soit $\mathfrak{p} \subseteq A$ un idéal premier, et $V(\mathfrak{p})$ sa variété. Alors la dimension de $V(\mathfrak{p})$ est finie et égale au degré de transcendance sur K du corps des fractions de $A/\mathfrak{p}$.*

On ajoute ici un autre théorème, qui sera très utile pour notre traitement des courbes.

Théorème 4. *Soit $V \subseteq \mathbb{C}^n$ une variété affine de dimension k. Alors, dans la topologie euclidienne, il existe un sous-ensemble ouvert et dense $D \subseteq V$ qui est une variété topologique, dont la dimension (topologique) est $2k$. De plus, le complémentaire $W = V \backslash D$ est une variété affine de dimension strictement plus petite que k.*

2.2.1 Les courbes affines

Définition 3. *Une* courbe affine *est une variété affine irréductible de dimension 1.*

En particulier, les seules sous-variétés d'une courbe affine sont elle-même et les points. Grâce au théorème ci-dessus, on peut imaginer une courbe affine comme une courbe dans le sens classique, mais sans restrictions sur l'injectivité (elle peut s'intersecter) ni sur la régularité (elle peut avoir des pointes).

On se restreint maintenant au cas $n = 2$, c'est-à-dire que l'on regarde les courbes dans le plan K^2. On a alors le théorème suivant, qui est une conséquence des théorèmes fondamentaux de la théorie de la dimension et du Nullstellensatz de Hilbert.

Théorème 5. *Soit $C \subseteq K^2$ une courbe. Alors il existe un polynôme $p \in K[x, y]$ tel que $C = V((p))$. Si on impose la contrainte que p soit réduit (c'est-à-dire sans facteurs carrés), alors p est unique à multiplication par polynômes sans racines près.*

On a donc justifié une nouvelle définition *ad hoc* des courbes affines, que l'on utilisera toujours, sauf mention du contraire.

Définition 4. *Une* courbe affine $C \subseteq K^2$ *est le lieu des zéros d'un polynôme $f \in K[x, y]$ irréductible. Les points $P \in C$ tels que $\nabla f(P) = 0$ sont appelés* points singuliers *de la courbe. Si un point n'est pas singulier, on le dit* régulier *ou bien* lisse. *Une courbe n'ayant pas de points singuliers est appelée* courbe lisse.

2.2.2 Les courbes elliptiques

Si $d = \deg f$, on dit qu'une courbe C définie par le polynôme f (de degré minimal parmi les polynômes la définissant) est de *degré d*. Une courbe lisse de degré 3 et un point à l'infini O est une *courbe elliptique*. Si maintenant le concept de "point à l'infini" n'est pas clair, il sera défini rigoureusement dans le cadre des courbes projectives.

Si $C \subseteq K^2$ est une courbe affine, on peut considérer le polynôme la définissant $f \in K[x,y]$. Ses coefficients seront contenus dans un sous-corps $F \subseteq K$. Dans ce cas là, on dit que la courbe C est *définie* sur F, et on appelle *points F-rationnels* les points de C avec coordonnées dans F. On notera $C(F)$ l'ensemble des points F-rationnels, et on exige dans ce cas là que $O \in C(F)$.

Les courbes elliptiques affines ne sont pas très indiquées pour être munies d'une structure de groupe. En fait, si on continuait à utiliser les objets affines, on se rendrait compte qu'il manque un élément identité à la structure de groupe et que cet élément peut être naturellement identifié avec le "point à l'infini" de la courbe elliptique. Pour rendre rigoureux ce concept, il faut introduire les variétés projectives, qui seront le sujet de la prochaine partie.

2.2.3 Les variétés projectives

Il y a plusieurs définitions de l'espace projectif et des variétés projectives. On utilisera ici la plus concrète, qui permettra d'effectuer des calculs.

Définition 5. *Soit K un corps et n un entier. L'*espace projectif *de dimension n sur K est le quotient de $K^{n+1} \setminus \{0\}$ par l'action de K par multiplication scalaire. On note cet espace $\mathbb{P}^n(K)$. Une* transformation projective *est le quotient par cette action d'un isomorphisme linéaire de K^2.*

Si $K = \mathbb{R}$ ou bien $\mathbb{C}$, cet espace est aussi un espace topologique muni de la topologie quotient. On note un élément de $\mathbb{P}^n(K)$ comme $[x_0 : \ldots : x_n]$, où $(x_0, \ldots, x_n)$ est un représentant de $K^{n+1} \setminus \{0\}$; on a donc que si $\lambda \in K \setminus \{0\}$, les représentants sont égaux $[x_0 : \ldots : x_n] = [\lambda x_0 : \ldots : \lambda x_n]$. Les ensembles $U_i = \{x_i \neq 0\}$ sont alors en bijection avec K^n, grâce à l'application $[x_0 : \ldots : x_n] \mapsto (x_0/x_i, \ldots, x_n/x_i)$ où on n'a pas écrit x_i/x_i. On appelle ces U_i les *cartes affines* de $\mathbb{P}^n(K)$.

Définition 6. *Soit $I \subseteq K[x_0, \ldots, x_n]$ un idéal homogène (c'est-à-dire engendré par des polynômes homogènes). L'ensemble*

$$Z(I) = \{P \in \mathbb{P}^n(K) \mid F(P) = 0 \text{ pour tout } F \in I \text{ homogène}\}$$

est appelé variété *de I.*

On note que comme chaque F dans la définition est homogène, l'ensemble $Z(I)$ est bien défini. Les variétés de ce type sont appelées *variétés projectives*.

Les mêmes considérations faites au début de la section précédente peuvent être répétées pour le cas projectif, en plaçant le mot "homogène" chaque fois que l'on fait mention d'un polynôme.

Pour chaque polynôme homogène $F \in K[x_0, \ldots, x_n]$ et pour chaque $0 \leq i \leq n$, on peut obtenir un polynôme $f \in K[y_1, \ldots, y_n]$ en plaçant $x_i = 1$ et en renumérotant les variables. Réciproquement, si $f \in K[y_1, \ldots, y_n]$ est un polynôme, on pose $y_j = x_j/x_i$ et on multiplie par $x_i^{\deg f}$ pour obtenir un polynôme homogène $F \in K[x_0, \ldots x_n]$. On note alors $f = D_i F$ et $F = H_i f$. On a toujours $f = D_i H_i f$ et si $x_i \nmid F$ on a aussi $F = H_i D_i F$. Avec ces procédures on a la proposition suivante, dont la démonstration est triviale.

Proposition 1. *Si $f \in K[y_1, \ldots, y_n]$ définit une variété affine V, alors $F = H_i f$ définit une variété projective $\overline{V}$, appelé* fermeture projective *de V, telle que $V = U_i \cap \overline{V}$. Réciproquement, si $Z \subseteq \mathbb{P}^n(K)$ est une variété projective qui ne contient pas l'hyperplan $\{x_i = 0\}$, alors il existe $V \subseteq U_i$ variété affine (on utilise l'identification donnée par la carte affine) telle que $Z = \overline{V}$. Si Z est définie par le polynôme homogène F, alors V est définie par le polynôme $f = D_i F$.*

Cette proposition nous permet de définir la *dimension* d'une variété projective Z comme la dimension de n'importe quelle variété affine dont la fermeture projective est Z. Une *courbe projective* est alors une variété projective irréductible de dimension 1.

On a aussi l'équivalent projectif du théorème de caractérisation des courbes affines dans le plan.

Théorème 6. *Soit $C \subseteq \mathbb{P}^2(K)$ une courbe projective. Alors il existe un polynôme homogène $F \in K[x_0, x_1, x_2]$ tel que $C = Z((F))$. Si on impose la contrainte que F soit réduit (c'est-à-dire sans facteurs carrés), alors F est unique à multiplication par polynômes sans racines près.*

On répète donc la définition donnée dans le cas affine, que l'on utilisera en général.

Définition 7. *Une* courbe projective $C \subseteq \mathbb{P}^2(K)$ *est le lieu des zéros d'un polynôme $F \in K[x_0, x_1, x_2]$ irréductible et homogène. Le* degré *de la courbe est le degré du polynôme la définissant de degré minimal. Les points $P \in C$ tels que $\nabla F(P) = 0$ sont appelés* points singuliers *de la courbe. Si un point n'est pas singulier, on le dit* régulier *ou bien* lisse. *Une courbe n'ayant pas de points singuliers est appelée* courbe lisse.

On définit alors une *courbe elliptique* comme une courbe $C \subseteq \mathbb{P}^2(K)$ de degré 3, sur laquelle on choisit un point $O \in C$. Si en plus C est défini sur le sous-corps K', on demande que $O \in C(K')$.

Si on prend une carte affine $U_i \subseteq \mathbb{P}^2(K)$ telle que $\text{card}(C \cap \{x_i = 0\}) = 1$ et si on regarde la courbe C sur U_i, on ne voit pas le point $O \in C \cap \{x_i = 0\}$, qui devient donc un "point à l'infini" ; ce point est le seul point qui n'est pas dans la carte U_i. En effet on peut imaginer la droite $\{x_i = 0\}$ comme le lieu des limites pour y_j tendant vers l'infini des directions radiales $(\alpha y_j, \beta y_j)$ avec α et β dans K non nuls. On peut alors atteindre le point O en parcourant la courbe "jusqu'à l'infini". Bien sûr ces discours ne sont pas rigoureux, mais ils peuvent aider à visualiser les idées. La seule chose qui se passe est que le polynôme n'est plus homogène, et que le point à l'infini est le point qu'il faut ajouter pour obtenir la fermeture projective de la courbe elliptique.

À partir de maintenant, quand on parlera de courbe elliptique, cela s'entendra une courbe projective avec une spécification d'un point $O \in C$, ou bien une courbe affine avec le point O comme point à l'infini.

On énonce sans preuve un théorème qui sera très utile pour l'étude des courbes elliptiques.

Théorème 7. (Bézout) *Soient C et D deux courbes projectives de $\mathbb{P}^2(\mathbb{C})$, de degré respectivement e et f. Alors C et D s'intersectent en ef points, s'ils sont comptés avec leur multiplicité.*

2.2.4 Les équations de Weierstrass

Soit $C \subseteq \mathbb{P}^2(K)$ une courbe elliptique munie du point $O = [0 : 1 : 0]$; quitte à effectuer une transformation projective, on peut toujours se ramener au cas $O = [0 : 1 : 0]$. On suppose à partir de maintenant que $\text{char}(K) \neq 2,\ 3$.

On ne considérera qu'un type particulier de courbes elliptiques : celles qui peuvent être écrites (avec $O = [0 : 1 : 0]$) comme lieu des zéros d'une équation de la forme

$$Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3$$

c'est-à-dire qu'on n'a pas un terme de la forme X^2Y ni XY^2. Si telle équation existe, on l'appelle *équation de Weierstrass* de C. Cette restriction n'est pas très lourde : on a en fait la proposition suivante, qui suit du théorème de Riemann-Roch et que l'on ne montrera pas ici.

Proposition 2. *Quitte à modifier les coordonnées par des transformation rationnelles (c'est-à-dire des quotients de polynômes), toute courbe elliptique admet une équation de Weierstrass.*

Donc on pourrait bien utiliser la nouvelle définition ci-dessous de courbe elliptique, qui est équivalente à celles qui précèdent.

Définition 8. *Soit K un corps algébriquement clos. Une* courbe elliptique $C \subseteq \mathbb{P}^2(\mathbb{K})$ *est le lieu des zéros d'une équation de la forme*

$$Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3$$

munie du point $O = [0 : 1 : 0]$ et $a_i \in K$. Si les a_i sont dans un sous-corps $K' \subseteq K$, on dit que la courbe elliptique est définie *sur K'.*

À partir de maintenant, toute courbe elliptique sera donnée par ses équation de Weierstrass et si on regarde la carte affine U_1, c'est-à-dire que l'on amène le point O à l'infini, on obtient l'équation définissante de la courbe elliptique affine

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

Ces deux équations sont appelées *équations de Weierstrass* de C. Si on fait la substitution $y \mapsto \frac{1}{2}(y - a_1x - a_2)$ on obtient la nouvelle équation

$$y^2 = 4x^3 + b_1x^2 + 2b_2x + b_3$$

pour certains coefficients b_i qui sont des polynômes dans les a_i. On définit alors les quantités

$$\alpha = a_1^2a_5 + 4a_3a_5 - a_1a_2a_4 + a_3a_2^2 - a_4^2$$

$$\Delta = -b_1^2\alpha - 8b_2^3 - 27b_3^2 + 9b_1b_2b_3$$

et on appelle Δ le *discriminant* de la courbe elliptique. On précise que le discriminant dépend de l'équation choisie : en changeant les variables, le discriminant change aussi. Comme conséquence de la prochaine proposition, on verra pourtant que la nullité du discriminant est invariante par transformations projectives (c'est-à-dire, par changement de variables). On est quand même intéressé par une expression particulière du discriminant, que l'on utilisera presque toujours sauf dans la preuve de la prochaine proposition. Si on substitue $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$, on obtient un forme simplifiée de l'équation de Weierstrass de C

$$y^2 = x^3 + Ax + B \tag{1}$$

où A et B sont des polynômes dans les a_i.

Si on considère l'équation de Weierstrass ci-dessus, on voit par le calcul que le discriminant de C devient

$$\Delta = -16(4A^3 + 27B^2)$$

ce qui est l'expression qui nous intéresse. On a alors la proposition suivante :

Proposition 3. *Soit C une courbe de degré 3. Alors C est lisse (et c'est donc une courbe elliptique) si et seulement si $\Delta \neq 0$. Si $\Delta = 0$, il n'y a qu'un seul point singulier.*

Preuve. Le point à l'infini n'est jamais singulier : en prenant le polynôme homogène

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_2YZ^2 - X^3 - a_3X^2Z - a_4XZ^2 - a_5Z^3$$

et en considérant $O = [0 : 1 : 0]$ on voit que $\frac{\partial F}{\partial Z}(O) = 1 \neq 0$ car $\mathrm{char}(K) \neq 2$. Alors $\nabla F(O) \neq 0$ et O n'est pas singulier.

On fait la substitution $y \mapsto \frac{1}{2}(y - a_1x - a_2)$ pour simplifier les calculs. L'équation de Weierstrass devient donc de la forme

$$y^2 = 4x^3 + b_1x^2 + 2b_2x + b_3$$

En prenant le gradient, on voit que les points singuliers sont exactement les points $(x_0, 0)$ avec x_0 racine double du polynôme $4x^3 + b_1x^2 + 2b_2x + b_3$. Le discriminant de ce polynôme est 16Δ et un polynôme a une racine double si et seulement si son discriminant est zéro.

Comme un polynôme de degré 3 ne peut avoir qu'une seule racine double, on en déduit aussi qu'il y a au plus un point singulier. □

3 La loi de groupe sur les courbes elliptiques

3.1 Définition de la loi de groupe

Soit $E : F(X,Y,Z) = 0$ un courbe définie par le polynôme F homogène de degré 3, sur laquelle on a choisi un point O non singulier. Nous allons voir que l'ensemble $E(K)^{(0)}$ des points non singuliers de E dans $\mathbb{P}^2(K)$ est muni d'une loi de groupe d'élément neutre O.

Définition 9. *Soient $A, B \in E(K)$ des points non singuliers de E. Si A et B sont distincts, on pose $A \circ B = C$ où C est le troisième point d'intersection de la droite passant par A et B avec E. Si $A = B$, on pose $A \circ B = C$ où C est l'autre point d'intersection de la tangente à E en A avec E. On pose alors $A + B = O \circ (A \circ B)$.*

Proposition 4. *$(E(K)^{(0)}, +)$ est un groupe abélien d'élément neutre O. En particulier, si E est une courbe elliptique, $E(K) = E(K)^{(0)}$, et alors $(E(K), +)$ est un groupe abélien d'élément neutre O.*

Il découle facilement de la définition par la méthode des sécantes et des tangentes que la loi proposée est commutative et est d'élément neutre O. La partie délicate est l'associativité, dont nous allons donner un schéma de preuve à partir du théorème de Bézout. Pour une démonstration complète utilisant des outils élémentaires, voir [2].

Soient $A, B, C \in E(K)$. On pose :

$$\begin{aligned} A \circ B = D, A + B = G, \\ B \circ C = U, B + C = V \\ A \circ V = W, G \circ C = F \\ l(X,Y,Z) \text{ équation de la droite passant par } A, B, D \\ m(X,Y,Z) \text{ équation de la droite passant par } G, C, F \\ n(X,Y,Z) \text{ équation de la droite passant par } O, U, V \\ r(X,Y,Z) \text{ équation de la droite passant par } A, W, V \\ s(X,Y,Z) \text{ équation de la droite passant par } B, C, U \\ t(X,Y,Z) \text{ équation de la droite passant par } D, G, O \end{aligned} \tag{2}$$

Montrer l'associativité revient à montrer que F et W sont le même point qui est l'intersection de r et m.

Lemme 1. *Soit $A_1, ..., A_8 \in \mathbb{P}^2(K)$ 8 points du plan tels que 4 ne soient pas alignés et 7 ne soient pas sur une même conique. Alors il existe un point A_9 tel que toute courbe de degré 3 passant par $A_1, ..., A_8$ passe aussi par A_9.*

Preuve. Un polynôme homogène de degré 3 $F(X,Y,Z)$ est déterminé par 10 coefficients. Si F s'annule en $A_1, ..., A_8$, on peut montrer que la condition sur $A_1, ..., A_8$ est équivalente à dire que les conditions qu'imposent $A_1, ..., A_8$ sur les coefficients de F sont linéairement indépendantes. Si on fixe F_1 et F_2 homogène de degré 3 qui s'annulent en $A_1, ..., A_8$, alors nécessairement F est de la forme $F = \lambda F_1 + \mu F_2$. Par le théorème de Bézout, F_1 et F_2 s'annulent sur 9 points en communs, et alors F s'annule aussi sur ces 9 points. □

Si maintenant on pose $F_1(X,Y,Z) = l(X,Y,Z)m(X,Y,Z)n(X,Y,Z)$ et $F_2(X,Y,Z) = r(X,Y,Z)s(X,Y,Z)t(X,Y,Z)$, alors notre courbe définie par $F(X,Y,Z) = 0$ passe par 8 points d'intersection de F_1 et F_2, qui sont A, B, C, D, G, V, U, O, elle doit donc passer par le neuvième qui est l'intersection de $m = 0$ et $r = 0$, et alors $F = W$.

3.2 Étude de la torsion

On considère maintenant que notre courbe est sous équation de Weierstrass. Soit

$$E : Y^2 = X^3 + aX + b,\ a, b \in \mathbb{Q}$$

une courbe elliptique définie sur $\mathbb{Q}$ telle que $4a^3 + 27b^2 \neq 0$. De façon homogène, on écrit

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

Le point $[0 : 1 : 0]$ est toujours sur la courbe. On le distingue donc, on le note O est on considère à présent la loi de groupe d'élément neutre O.

Le résultat principal sur la torsion est le suivant :

Théorème 8. *Le sous groupe de torsion du groupe $E(\mathbb{Q})$ des points rationnels de E est fini.*

Ce résultat est nécessaire à la démonstration qui suit du théorème de Mordell. Sa démonstration fournit de plus une condition sur les points de torsion facilitant le calcul du sous groupe de torsion. L'outil principal utilisé sera la réduction de la courbe modulo un nombre premier.

3.3 Preuve du théorème

Si c est le *ppcm* des dénominateurs de a et b, en multipliant par c^6 on obtient

$$c^6Y^2Z = c^6X^3 + ac^6XZ^2 + bc^6Z^3$$

En posant $Y' = c^3Y$, $X' = c^2X$ et $Z' = Z$, on a

$$Y'^2Z' = X'^3 + ac^4X'Z'^2 + ac^6Z'^3$$

où ac^4 et bc^6 sont entiers, et $4(ac^4)^3+27(bc^6)^2 = c^{12}(4a^3+27b^2) \neq 0$. On peut donc supposer sans perte de généralité que $a, b \in \mathbb{Z}$.

Soit $p \in \mathbb{Z}$ un nombre premier. En notant $\overline{a} = a \pmod p$, on définit la courbe réduite

$$\overline{E} : Y^2Z = X^3 + \overline{a}XZ^2 + \overline{b}Z^3$$

sur $\mathbb{F}_p$. Celle ci peut contenir des points singuliers ; or la loi de groupe n'est pas définie en les points singuliers. On note donc $\overline{E}(\mathbb{F}_p)^{(0)}$ le groupe des points non singuliers de $\overline{E}(\mathbb{F}_p)$.

On définit la réduction d'un point de $A \in E(\mathbb{Q})$ dans $\overline{E}(\mathbb{F}_p)$, que l'on notera $\overline{A}$, comme suit : le point à l'infini $O = [0 : 1 : 0]$ est envoyé sur le point à l'infini de la courbe réduite ; les autres points de la courbe ont une troisième coordonnée non nulle, et on pose

$$[\frac{u}{v} : \frac{u'}{v'} : 1] \mapsto [\overline{\frac{u}{v}k} : \overline{\frac{u'}{v'}k} : \overline{k}]$$

où u/v et u'/v' sont sous forme réduite, et où $k = ppcm(v, v')$. On note alors $E(\mathbb{Q})^{(0)}$ les points de $E(\mathbb{Q})$ qui se réduisent sur des points non singuliers.

Proposition 5. *$E(\mathbb{Q})^{(0)}$ est un groupe et la réduction $E(\mathbb{Q})^{(0)} \to \overline{E}(\mathbb{F}_p)^{(0)}$ est un morphisme.*

Preuve. Si $A, B \in E(\mathbb{Q})^{(0)}$, $C \in E(\mathbb{Q})$ sont tels que $A+B-C = O$, alors $A, B, -C$ sont sur une même droite d'équation $\alpha Z = \beta X + \gamma Y$, $\alpha, \beta, \gamma \in \mathbb{Z}$. Leur réductions sont alors sur la droite d'équation $\overline{\alpha}Z = \overline{\beta}X+\overline{\gamma}Y$. Or $\overline{A}, \overline{B} \in \overline{E}(\mathbb{F}_p)^{(0)}$ qui est un groupe, donc $\overline{C} \in \overline{E}(\mathbb{F}_p)^{(0)}$ et alors $C \in E(\mathbb{Q})^{(0)}$. □

Les points non nuls dans le noyau de cette réduction sont ceux dont la troisième coordonnée s'annule modulo p, c'est dire les points $[x : y : 1]$ tels que $v_p(x) < 0$ ou $v_p(y) < 0$, où v_p est la valuation p-adique sur $\mathbb{Q}$. On a

$$v_p(y^2) = 2v_p(y) = v_p(x^3 + ax + b) = 3v_p(x)$$

car $a, b \in \mathbb{Z}$.

Définition 10. *Soit $n(x : y : 1) \geq 1$ l'unique entier tel que $v_p(y) = -3n(x : y : 1)$ et $v_p(x) = -2n(x : y : 1)$. On l'appelle le niveau de $[x : y : 1]$. Pour $v_p(x), v_p(y) \geq 0$ par définition le niveau de $[x : y : 1]$ est 0. Le niveau de O est $+\infty$.*

Pour les entiers $N \geq 1$, on pose $X_N = p^{2N}X$, $Y_N = p^{3N}Y$ et $Z_N = Z$. On obtient la courbe

$$E_N : Y_N^2 Z_N = X_N^3 + p^4 a X_N Z_N^2 + p^6 b Z_N^3$$

qui se réduit en

$$\overline{E_N} : Y_N^2 Z_N = X_N^3$$

qui a un point singulier en $[0 : 0 : 1]$. On a

$$v_p(p^{2N}x) = 2N + v_p(x) \text{ et } v_p(p^{3N}y) = 3N + v_p(y)$$

ce qui montre la proposition suivante.

Proposition 6. *Si $n(x : y : 1) < N$, alors $[x : y : 1] \in E(\mathbb{Q})$ se réduit en le point singulier $[0 : 0 : 1] \in \overline{E_N}(\mathbb{F}_p)$; si $n(x : y : 1) > N$, alors $[x : y : 1] \in E(\mathbb{Q})$ se réduit en le point nul $[0 : 1 : 0] \in \overline{E_N}(\mathbb{F}_p)$.*

Pour $N \geq 1$ on pose

$$E(\mathbb{Q})^{(N)} = \{A \in E(\mathbb{Q}),\, n(A) \geq N\}$$

Lemme 2. *Les $E(\mathbb{Q})^{(N)}$ sont des groupes.*

$$E(\mathbb{Q}) \supset E(\mathbb{Q})^{(0)} \supset E(\mathbb{Q})^{(1)} \supset ... \supset E(\mathbb{Q})^{(N)} \supset ..$$

Pour $N \geq 1$, $E(\mathbb{Q})^{(N)}/E(\mathbb{Q})^{(N+1)} \simeq \mathbb{F}_p$ et $E(\mathbb{Q})^{(0)}/E(\mathbb{Q})^{(1)}$ est isomorphe à un sous groupe de $\overline{E}(\mathbb{F}_p)$.

Preuve. On montre que ce sont des groupes de la même façon que l'on a montré que $E(\mathbb{Q})^{(0)}$ est un groupe, mais cette fois si en considérant la réduction $E(\mathbb{Q})^{(N)} \to \overline{E_N}(\mathbb{F}_p)^{(0)}$.

On note que pour $N \geq 0$, $E(\mathbb{Q})^{(N+1)}$ est le noyau de la réduction $E(\mathbb{Q})^{(N)} \to \overline{E_N}(\mathbb{F}_p)^{(0)}$. Or $\overline{E_N}(\mathbb{F}_p)^{(0)}$ (le groupe des points non singuliers de $\overline{E_N}(\mathbb{F}_p)$) est isomorphe à $\mathbb{F}_p$. En effet, $\overline{E_N}(\mathbb{F}_p)^{(0)} = \overline{E_N}(\mathbb{F}_p) \setminus \{[0 : 0 : 1]\}$, toute droite ne passant pas par $[0 : 0 : 1]$ s'écrit sous la forme $Z_N = lX_N + mY_N$, elle rencontre la courbe lorsque

$$X_N^3 - Y_N^2(lX_N + mY_N) = 0$$

si on note $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ les solutions de cette équation dans $\mathbb{F}_p$, on a

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} + \frac{x_3}{y_3} = 0 \text{ et } [x_1 : y_1 : 1] + [x_2 : y_2 : 1] + [x_3 : y_3 : 1] = o \text{ dans } \overline{E_N}(\mathbb{F}_p)$$

ce qui définit bien un isomorphisme $\overline{E_N}(\mathbb{F}_p)^{(0)} \to \mathbb{F}_p$. □

Proposition 7. *Soit $[x : y : 1] \in E(\mathbb{Q})$ d'ordre fini premier à p. Alors $v_p(x), v_p(y) \geq 0$.*

Preuve. Sinon, $[x : y : 1] \in E(\mathbb{Q})^{(n(x:y:1))} \setminus E(\mathbb{Q})^{(n(x:y:1)+1)}$ donc est envoyé sur un point non nul de $E(\mathbb{Q})^{(n(x:y:1))}/E(\mathbb{Q})^{(n(x:y:1)+1)}$ qui lui est d'ordre p. □

Nous allons maintenant relaxer l'hypothèse que l'ordre du point est premier à p. On pose

$$\begin{array}{rccc} & E(\mathbb{Q}) & \longrightarrow & \mathbb{Q} \\ u: & O & \longmapsto & 0 \\ & [x:y:1] & \longmapsto & \frac{x}{y} \end{array}$$

Pour $A \in E(\mathbb{Q}) \setminus \{O\}$ on a $v_p(u(A)) = n(A)$.

Lemme 3. *Soit $A, B \in E(\mathbb{Q})^{(1)}$. Alors :*

$$v_p(u(A+B) - u(A) - u(B)) \geq 5 \min(v_p(u(A)), v_p(u(B)))$$

Preuve. Si $A = O$ ou $B = O$, le résultat est évident. Si $A + B = O$, on a $u(A) + u(B) = 0$ et le résultat suit en considérant que $v_p(0) = +\infty$. On suppose donc que $A, B, A + B \neq O$. On suppose de plus sans perte de généralité que $v_p(u(A)) \leq v_p(u(B))$.

On pose $N = n(A) = v_p(u(A))$. Comme $A, B, A + B$ ne se réduisent pas sur $[0:0:1] \in \overline{E_N}(\mathbb{F}_p)$, ils sont sur une droite d'équation $Z_N = lX_N + mY_N$ où $v_p(l), v_p(m) \geq 0$ (sinon la droite réduite passe par $[0:0:1]$). Celle ci rencontre $E_N(\mathbb{Q})$ lorsque

$$\begin{aligned} 0 &= -Y_N^2(lX_N + mY_N) + X_N^3 + p^{4N} a X_N (lX_N + mY_N)^2 + p^{6N} b (lX_N + mY_N)^3 \\ &= c_3 X_N^3 + c_2 X_N^2 Y_N + c_1 X_N Y_N^2 + c_0 Y_N^3 \end{aligned}$$

où $c_3 = 1 + p^{4N} a l^2 + p^{6N} b l^3$ et $c_2 = 2p^{4N} lma + 3p^{6N} l^2 mb$, donc $v_p(c_3) = 0$ et $v_p(c_2) \geq 4N$.

Pour $T_N = X_N / Y_N$, les racines de $c_3 T_N^3 + c_2 T_N^2 + c_1 T_N + c_0$ sont celles qui correspondent aux points $A, B, -(A+B)$, c'est à dire $p^{-N} u(A), p^{-N} u(B), -p^{-N} u(A+B)$. Leur somme est $-c_2/c_3$, donc

$$\begin{aligned} v_p(u(A+B) - u(A) - u(B)) &= v_p(p^N \tfrac{c_2}{c_3}) \\ &\geq 5N \end{aligned}$$

d'où le résultat. □

Proposition 8. *Pour $s \in \mathbb{Z}$ et $A \in E(\mathbb{Q})^{(1)}$, on a $v_p(u(sA)) = v_p(s) + v_p(u(A))$.*

Preuve. Par récurrence sur le lemme, on a $v_p(u(sA) - su(A)) \geq 5 v_p(u(A))$. En effet,

$$v_p(u((s+1)A) - u(sA) - u(A)) \quad \geq 5 \min(v_p(u(sA)), v_p(u(A)))$$

$$\begin{aligned} v_p(u(sA)) &= v_p(u(sA) - su(A) + su(A)) \\ &\geq \min(v_p(u(sA) - su(A)), v_p(su(A))) \end{aligned}$$

Cela permet de montrer le résultat lorsque $p \nmid s$ ou $p = s$, car si on suppose que $v_p(u(sA)) \neq v_p(su(A))$, on a

$$v_p(u(sA) - su(A)) = \min(v_p(u(sA)), v_p(su(A))) \geq 5 v_p(A)$$

or

$$\min(v_p(u(sA)), v_p(su(A))) \leq v_p(su(A)) \leq v_p(u(A)) + 1 < 5 v_p(u(A))$$

car $v_p(u(A)) = n(A) \geq 1$, donc on a contradiction.

On montre alors le résultat pour $s \in \mathbb{Z}$ quelconque par récurrence sur $v_p(s)$, et en constatant que $u(-A) = -u(A)$. □

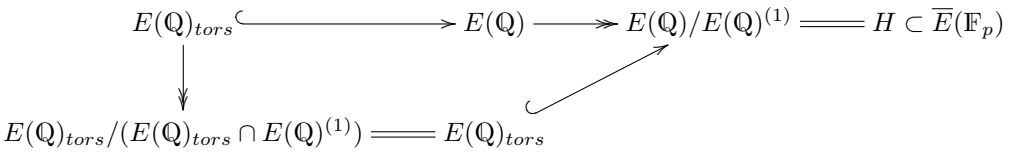
Proposition 9. *$E(\mathbb{Q})^{(1)}$ est sans torsion. Soit $A = [x:y:1] \in E(\mathbb{Q})$ de torsion. Alors $v_p(x), v_p(y) \geq 0$.*

Preuve. En effet, pour $A \in E(\mathbb{Q})^{(1)}$, $v_p(u(sA))$ prend une infinité de valeure lorsque s parcourt $\mathbb{Z}$, donc A ne peut pas être de torsion.

Soit $A = [x:y:1] \in E(\mathbb{Q})$ de torsion. Alors $A \notin E(\mathbb{Q})^{(1)}$, c'est à dire que $n(A) = 0$, donc par définition $v_p(x), v_p(y) \geq 0$. □

Proposition 10. *Si $p \neq 2$ et $p \nmid 4a^3 + 27b^2$, alors le sous groupe de torsion de $E(\mathbb{Q})$ est isomorphe à un sous groupe de $\overline{E}(\mathbb{F}_p)$.*

Preuve. Dans ce cas, aucun point de $\overline{E}(\mathbb{F}_p)$ n'est singulier et alors $E(\mathbb{Q}) = E(\mathbb{Q})^{(0)}$, donc il y a un sous groupe H de $\overline{E}(\mathbb{F}_p)$ tel que $H \simeq E(\mathbb{Q})/E(\mathbb{Q})^{(1)}$. On a alors



□

Théorème 9. *Le groupe $E(\mathbb{Q})_{tors}$ des points d'ordre fini de $E(\mathbb{Q})$ est fini. Si $[x : y : 1] \in E(\mathbb{Q})_{tors}$, alors $x, y \in \mathbb{Z}$, et $y = 0$ ou $y^2 \mid 4a^3 + 27b^2$.*

Preuve. $E(\mathbb{Q})_{tors}$ est fini comme sous groupe du groupe fini $\overline{E}(\mathbb{F}_p)$ par la proposition 10.

Si $[x : y : 1] \in E(\mathbb{Q})_{tors}$, par la proposition 9, pour tout premier p, $v_p(x), v_p(y) \geq 0$, c'est à dire que $x, y \in \mathbb{Z}$.

Soit $[x : y : 1] \in E(\mathbb{Q})_{tors}$. En dérivant l'équation de Weierstrass par rapport à X, on obtient :

$$2Y\frac{dY}{dX} = 3X^2 + a$$

On voit alors que si $2[x : y : 1] = O$, c'est à dire que la tangente en $[x : y : 1]$ est verticale, alors $y = 0$. Sinon, on pose $2[x : y : 1] = [u : v : 1]$ où $[u : v : 1]$ est aussi de torsion, donc $u, v \in \mathbb{Z}$. La droite passant par $[x : y : 1]$ et $[u : v : 1]$ n'est pas verticale (sa pente est l'opposée de celle de la tangente), donc elle s'écrit sous la forme $Y = lX + mZ$, où $l = -\frac{dY}{dX}(x, y) = -\frac{3x^2+A}{2y}$. Elle intersecte la courbe lorsque

$$X^3 + aX + b - (lX + m)^2$$

et donc on a

$$u + 2x = l^2 = (\frac{3x^2 + a}{2y})^2 = \frac{(3x^2 + a)^2}{4y^2}$$

donc $y^2 \mid (3x^2 + a)^2$.

Or, considérant que $(X^3 + aX + b)^2 = X^6 + 2aX^4 + a^2X^2 + 2bX^3 + 2abX + b^2$:

$$\begin{aligned}(3X^2 + 4a)(3X^2 + a)^2 &\equiv 27X^6 + 54aX^4 + 27a^2X^2 + 4a^3 && (\text{mod } X^3 + aX + b)\\ &\equiv -27(2bX^3 + 2abX + b^2) + 4a^3 && (\text{mod } X^3 + aX + b)\\ &\equiv 4a^3 + 27b^2 && (\text{mod } X^3 + aX + b)\end{aligned}$$

□

3.4 Exemple

On considère la courbe E définie par $E : Y^2Z = X^3 - 5XZ^2 + Z^3$. On suppose que $[x : y : 1] \in E(\mathbb{Q})$ est un point de torsion. Alors par ce qui précède, $y = 0$ ou $y^2 \mid -500 + 27 = -463$. On a $y \neq 0$ car il n'y a pas de solutions entières à $x^3 - 5x + 1 = 0$. On a aussi que 463 est un nombre premier, alors nécessairement $y^2 = 1$ et alors la seule solution entière est $x = 0$. Le point $[0 : 1 : 1]$ est bien de torsion, il est en effet de 2-torsion puisque la tangente à la courbe y est verticale. D'où $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}$.

4 Le théorème de Mordell faible

Soit E une courbe elliptique définie sur $\mathbb{Q}$ avec point à l'infini O, et soit $E(\mathbb{Q})$ l'ensemble de ses points rationnels. On montrera dans cette section le théorème suivant, dit *théorème de Mordell faible*, par rapport à la version finale du théorème homonyme qui sera discutée plus tard.

Théorème 10. *Le groupe $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini.*

Ce théorème est en effet presque le théorème de Mordell fort, qui découle du théorème faible grâce à un argument de "descente" qui n'utilise que de la théorie élémentaire des groupes. Avant de démontrer le théorème faible, on précise que l'on ne connaît pas d'algorithme pour calculer effectivement le groupe $E(\mathbb{Q})/2E(\mathbb{Q})$, et que ceci c'est la seule vraie raison pour laquelle le groupe des points rationnels $E(\mathbb{Q})$ n'est pas facilement déterminé. En fait, il sera clair pendant la preuve de la procédure de descente qu'à partir du groupe quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ on peut "remonter" à $E(\mathbb{Q})$ de façon algorithmique.

Pour simplifier la preuve, on fera à partir de maintenant la supposition suivante.

$$\textit{Il existe un point rationnel de } E(\mathbb{Q}) \textit{ d'ordre } 2 \tag{3}$$

On précise que le théorème est vrai même sans cette hypothèse (qui peut bien sûr ne pas être vérifiée), mais la démonstration est plus compliquée.

Preuve. Avec la supposition (3), on peut modifier par translation l'équation de Weierstrass de notre courbe afin que E soit définie par l'équation

$$Y^2 = X(X^2 + aX + b)$$

avec a et b nombres rationnels, et le point $(0,0)$ d'ordre 2. Comme E est une courbe elliptique, on doit avoir aussi $a^2 - 4b \neq 0$ et $b \neq 0$ pour ne pas avoir de points singuliers.

On écrit un point de E avec ses coordonnées $A = (x, y)$. On écrit aussi $A_1 = A + (0,0)$ c'est-à-dire, en utilisant les formules d'addition des courbes elliptiques,

$$(x_1, y_1) = (\frac{b}{x}, -\frac{by}{x^2})$$

Si on définit les deux quantités

$$\lambda = \frac{y^2}{x^2} = \frac{x^2 + ax + b}{x}$$

$$\mu = y + y_1$$

on voit qu'elles satisfont la relation algébrique

$$\mu^2 = \lambda(\lambda^2 - 2a\lambda + (a^2 - 4b))$$

et par les relations $\lambda^{-1/2}\mu = x - b/x$ et $\lambda = x + (b/x) + a$, on obtient aussi les formules inverses

$$x = \frac{1}{2}(\lambda + \lambda^{-1/2}\mu - a)$$

$$y = \lambda^{1/2}x$$

Grâce aux relations algébriques trouvées, si on définit une nouvelle courbe elliptique par

$$F : Y^2 = X(X^2 - 2aX + (a^2 - 4b)) \tag{4}$$

on voit que la fonction $(x,y) \mapsto (\lambda,\mu)$ se prolonge à un morphisme $\phi : E \to F$ en envoyant le point à l'infini de E sur le point à l'infini de F. Soit $A_1 = (x_1, y_1)$ et $A_2 = (x_2, y_2) \in E$ et $A_1 \neq \pm A_2$. Alors $A_1 + A_2 \neq O$ et ses coordonnées sont

$$x(A_1 + A_2) = (\frac{y_2 - y_1}{x_2 - x_1})^2 - a - x_1 - x_2$$

$$y(A_1 + A_2) = -(\frac{y_2 - y_1}{x_2 - x_1})x(A_1 + A_2) - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

Avec des calculs directs on voit donc que

$$\phi(A_1 + A_2) = \phi(A_1) + \phi(A_2)$$

Si $A_1 = A_2 \neq -A_1$, alors on a la formule de duplication

$$x(2A_1) = (\frac{3x_1^2 + 2ax_1 + b}{2y_1})^2 - a$$

$$y(2A_1) = -(\frac{3x_1^2 + 2ax_1 + b}{2y_1})x(2A_1) - \frac{-x_1^3 + bx_1}{2y_1}$$

et encore des calculs directs montrent que $\phi(2A_1) = 2\phi(A_1)$.

Si $A_1 = -A_2$ on a $x_1 = x_2$ et $y_1 = -y_2$ donc $\lambda_1 = \lambda_2$ et $\mu_1 = -\mu_2$ et donc $\phi(A_1) = -\phi(A_2)$ et bien sûr $\phi(O_E) = O_F$ par définition (avec la notation évidente).

Notez que les conditions sur a et b assurent que F est une courbe elliptique.

Maintenant on répète la construction avec F au lieu de E en utilisant les mêmes formules, et on obtient à partir de λ et μ les nouvelles quantités ρ et σ qui satisfont la relation algébrique

$$\sigma^2 = \rho(\rho^2 + 4a\rho + 16b)$$

et donc si on pose $\xi = \rho/4$ et $\eta = \sigma/8$, on a que ξ et ρ satisfont l'équation définissant E. Alors on peut définir un morphisme $\psi : F \to E$ avec $(\lambda,\mu) \mapsto (\xi,\eta)$ et en composant avec ϕ, un morphisme $\psi \circ \phi : E \to E$ qui est un homomorphisme de groupes. Si un point $(x,y) \in E$ est dans le noyau de ce morphisme, on doit avoir $\phi(x,y) = (0,0) \in F$ et donc (x,y) doit être forcement un point d'ordre 2 de E. Alors le noyau de $\psi \circ \phi$ consiste des points d'ordre 2 de E plus le point à l'infini. Donc, $\psi \circ \phi$ est la multiplication par ± 2.

Jusqu'à maintenant, on a construit deux morphismes $\phi : E \to F$ et $\psi : F \to E$ dont la composition est la multiplication par ± 2. Comme le théorème que l'on est en train de démontrer porte sur les points rationnels, étudions l'effet que ces morphismes ont sur les points rationnels. La stratégie sera de montrer que les quotients $F(\mathbb{Q})/\phi(E(\mathbb{Q}))$ et $E(\mathbb{Q})/\psi(F(\mathbb{Q}))$ sont finis. Alors le théorème suivra du fait que $\psi \circ \phi$ est la multiplication par ± 2.

Montrons donc que le quotient $F(\mathbb{Q})/\phi(E(\mathbb{Q}))$ est fini.

On montre tout d'abord que un point $(u,v) \in F(\mathbb{Q})$ est dans $\phi(E(\mathbb{Q}))$ si et seulement si $u \in (\mathbb{Q}^*)^2$ ou bien $u = 0$ et $a^2 - 4b \in (\mathbb{Q}^*)^2$. En fait, si $u = 0$ et $a^2 - 4b \in (\mathbb{Q}^*)^2$, comme l'équation $x^2 + ax + b = 0$ a une solution dans les nombres rationnels, on peut prendre x une de ces solutions et $y = 0$, alors $\phi(x,y) = (u,v)$. Si pourtant $u \neq 0$ est dans $(\mathbb{Q}^*)^2$, alors on utilise les formules inverses

$$x = \frac{1}{2}(\lambda + \lambda^{-1/2}\mu - a)$$

$$y = \lambda^{1/2}x$$

en spécialisant $\lambda = u$, $\mu = v$ pour obtenir $\phi(x,y) = (u,v)$. L'autre implication est triviale grâce à la formule $\lambda = y^2/x^2$.

Cette discussion amène naturellement à définir l'application $q : F(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ donnée par

$$q(u,v) = u(\mathbb{Q}^*)^2 \quad si\ u \neq 0$$

$$q(u,v) = (a^2 - 4b)(\mathbb{Q}^*)^2 \quad si\ u = 0$$
$$q(O) = (\mathbb{Q}^*)^2$$

On vérifie maintenant que cette fonction est un homomorphisme de groupes. Il suffit de montrer que si on a trois points U_1, U_2, U_3 avec $U_1 + U_2 + U_3 = O$, on a aussi l'égalité $q(U_1)q(U_2)q(U_3) = 1$. Soit $Y^2 = X(X^2 + a_1X + b_1)$ l'équation de la courbe F et soient $U_j = (u_j, v_j)$. Si trois points de F ont somme O, ils sont alignés et donc il existe une droite d'équation $Y = lX + m$ qui les contient. En substituant dans l'équation de la courbe, on doit avoir $X(X^2 + a_1X + b_1) - (lX + m)^2 = (X - u_1)(X - u_2)(X - u_3)$ et en regardant les termes de degré 0, on trouve $u_1u_2u_3 = m^2$ et si aucun des u_j est O, on a terminé. Par contre si on a (par exemple) $u_1 = O$, si aussi $u_2 = O$, alors la droite est verticale, $U_3 = O$ et donc on a encore $q(U_1)q(U_2)q(U_3) = 1$. Si non, comme $m = 0$ l'équation devient $X^2 + a_1X + b_1 - l^2X = (X - u_2)(X - u_3)$ donc $u_2u_3 = b_1$, mais en regardant l'équation de F on rappelle que $b_1 = a^2 - 4b$ et donc le résultat suit dans ce cas aussi.

La dernière étape dans l'étude de l'action de ϕ sur les points rationnels est de montrer que l'image de q est finie. Pour faire cela, on garde la notation $Y^2 = X(X^2+a_1X+b_1)$ pour l'équation de la courbe F, dans laquelle on peut supposer que a_1 et b_1 sont des nombres entiers. Tout élément de $(\mathbb{Q})^*/(\mathbb{Q}^*)^2$ peut être écrit $r(\mathbb{Q}^*)^2$ avec r un nombre entier sans facteurs carrés. On montre maintenant que si $r(\mathbb{Q}^*)^2$ est dans l'image de q, alors $r|b_1$. Soit alors $q((u,v)) = r(\mathbb{Q}^*)^2$, c'est à dire qu'il existe deux nombres rationnels s et t tels que

$$u^2 + a_1u + b_1 = rs^2$$

$$u = rt^2$$

Soit $t = l/m$ écrit comme fraction réduite. Alors

$$r^2l^4 + a_1rl^2m^2 + b_1m^4 = rn^2$$

où $n = m^2s$ est entier parce que rs^2 est entier si et seulement si s est entier (r est sans facteurs carrés) et $rn^2 = rm^4s^2$ est entier. On suppose maintenant, par l'absurde, que $r \nmid b_1$ et donc qu'il existe un nombre premier p tel que $p|r$ mais $p \nmid b_1$. L'équation précédente dit alors que $p|m$ et que $p^2|rn^2$. Comme r est sans facteurs carrés, on a alors $p|n$ et par la même équation $p^3|r^2l^4$ donc $p|l$, ce qui est contradictoire à cause du fait que l/m est une fraction réduite.

Il est maintenant clair, en considérant tous les faits précédents, que $F(\mathbb{Q})/\phi E(\mathbb{Q})$ est fini, et donc en répétant le même raisonnement avec ψ au lieu de ϕ, on obtient que $E(\mathbb{Q})/\psi F(\mathbb{Q})$ est fini et par conséquent, comme $\psi \circ \phi$ est la multiplication par ± 2, on obtient la thèse du théorème, c'est à dire que $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini. □

5 La procédure de descente

Dans ce paragraphe on montrera comment "remonter" du groupe $E(\mathbb{Q})/2E(\mathbb{Q})$ au groupe $E(\mathbb{Q})$ en utilisant la procédure de descente. Cet argument n'utilise que de la théorie élémentaire des groupes et est constructif. La définition centrale est la suivante.

Définition 11. *Soit A un groupe abélien et $m \geq 2$ un nombre entier. Une* fonction hauteur d'ordre m *sur A est une fonction $h : A \to \mathbb{R}$ avec les trois propriétés suivantes.*

1. *Pour tout $Q \in A$ il existe une constante réelle C_1 telle que, pour tout $P \in A$, on a*

$$h(P + Q) \leq 2h(P) + C_1$$

2. *Il existe une constante réelle C_2 telle que, pour tout $P \in A$ on a*

$$h(mP) \geq m^2h(P) - C_2$$

3. Pour toute constante réelle C_3, l'ensemble

$$\{P \in A | h(P) \leq C_3\}$$

est fini.

L'existence d'une fonction hauteur est suffisante pour démarrer la *procédure de la descente*, qui est représentée par le théorème suivant.

Théorème 11. *Soit A un groupe abélien avec une fonction hauteur $h : A \to \mathbb{R}$ d'ordre m. Si le quotient A/mA est fini, alors le groupe A est de type fini.*

Preuve. Soient $Q_1, \ldots, Q_r$ représentants dans A des classes de A/mA, et soit $P \in A$. On va montrer qu'il existe une combinaison linéaire avec des entiers $\lambda_1, \ldots, \lambda_r$ et une constante C qui est *indépendante de* P tels que $P - \sum \lambda_i Q_i = kQ$ pour quelque entier k et quelque élément $Q \in A$ avec $h(Q) \leq C$. La thèse suivra alors de la propriété 3 de la définition de hauteur.

Soit donc

$$P = mP_1 + Q_{i_1}$$

$$P_1 = mP_2 + Q_{i_2}$$

et par récurrence

$$P_{n-1} = mP_n + Q_{i_n}$$

pour chaque entier positif n, et soit C_1' le maximum des constantes du premier point dans la définition de hauteur appliquée aux éléments $-Q_1$, ..., $-Q_r$.

La seconde propriété des hauteurs dit que pour chaque j on a $h(P_j) \leq \frac{1}{m^2}(h(mP_j) + C_2)$, et puisque $mP_j = P_{j-1} - Q_{i_j}$, par la première propriété on a $h(mP_j) \leq 2h(P_{j-1}) + C_1'$ et donc la formule suivante, valide pour tout j :

$$h(P_j) \leq \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2)$$

Si on utilise cette dernière formule à partir de P_n en remontant jusqu'à P, on obtient

$$h(P_n) \leq (2/m^2)^n h(P) + \frac{1}{m^2}(\frac{1}{m^2} + \frac{2}{m^4} + \ldots + \frac{2^{n-1}}{m^{2n}})(C_1' + C_2)$$

$$< (2/m^2)^n h(P) + \frac{(C_1' + C_2)(1 - (\frac{2}{m^2})^n)}{m^2 - 2}$$

$$\leq \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2)$$

où on a utilisé le fait que $m \geq 2$. Si on prend n grand, on peut donc avoir

$$h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2) = C$$

Mais comme $P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$ on a trouvé la combinaison linéaire cherchée. □

Cette *procédure de descente* peut être appliquée aux courbes elliptiques sur $\mathbb{Q}$ pour démontrer le théorème de Mordell fort à partir de celui faible. On note que la démonstration ci-dessus est *constructive*, c'est à dire qu'à partir des éléments de A/mA on peut trouver effectivement, en façon algorithmique, les générateurs du groupe A. Le fait que l'on ne connaisse pas d'algorithme qui détermine le groupe des points rationnels $E(\mathbb{Q})$ d'une courbe elliptique E découle du fait que le quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ n'est pas totalement connu.

6 Le théorème de Mordell

On est maintenant prêt à démontrer le théorème de Mordell que l'on rappelle maintenant.

Théorème 12. *Soit E une courbe elliptique sur $\mathbb{Q}$. Alors le groupe des points rationnels $E(\mathbb{Q})$ est de type fini.*

Si $t = p/q$ est un nombre rationnel écrit comme fraction réduite, on définit la *hauteur* de t comme $H(t) = \max\{|p|, |q|\}$. Si E est une courbe elliptique et $P \in E$ est un point $P \neq O$, on note $x(P)$ la première coordonnée de P.

Définition 12. *Soit E une courbe elliptique sur $\mathbb{Q}$ et $P \in E$ un point rationnel. La* hauteur logarithmique *de P est définie comme*

$$h_x(P) = \log H(x(P)) \quad si\ P \neq O$$

$$h_x(P) = 0 \quad si\ P = O$$

Dans une section précédente, on a montré le théorème de Mordell faible, qui dit que le quotient $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini. Grâce à la procédure de descente, la preuve du théorème de Mordell se réduit au lemme suivant.

Lemme 4. *La fonction h_x est une fonction hauteur d'ordre 2.*

Preuve. On écrira à partir de maintenant l'équation de Weierstrass de la courbe E comme

$$Y^2 = X^3 + AX + B$$

avec A et B entiers. On veut alors montrer la propriété 1 des fonctions hauteurs, c'est à dire qu'on fixe un point $P_0 \in E(\mathbb{Q})$ et on veut trouver une constante C_1 (qui dépend éventuellement de P_0) telle que pour tout $P \in E(\mathbb{Q})$, on a $h_x(P + P_0) \leq 2h_x(P) + C_1$. On suppose que $P \neq O, \pm P_0$, et on note $P = (\frac{a}{d^2}, \frac{b}{d^3})$ (on peut toujours écrire un point rationnel comme ça, à cause de l'équation de Weierstrass) et $P_0 = (\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3})$. Alors la formule d'addition dit que $x(P + P_0) = (\dfrac{y - y_0}{x - x_0})^2 - x - x_0$ et donc, en substituant l'équation de Weierstrass, $x(P + P_0) = \dfrac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0^2 d) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_o d^2)^2}$ d'où on obtient $H(x(P + P_0)) \leq C_1' \max\{|a|^2,\ |d|^4,\ |bd|\}$ avec C_1' qui dépend seulement de A, B, a_0, b_0, d_0. Bien sûr on a aussi $b^2 = a^3 + Aad^4 + Bd^6$ et donc naturellement $|b| \leq C_1'' \max\{|a|^{3/2},\ |d|^3\}$ avec C_1'' qui dépend seulement de A et B. Alors $|bd| \leq C_1'' \max\{|a|^{3/2}|d|,\ |d|^4\}$. Or, si $|d| \leq |a|^{1/2}$ on a $|a|^{3/2}|d| \leq |a|^2$ et si $|d| > |a|^{1/2}$, on a $|d|^4 > |a|^{3/2}|d|$ et donc, dans tous les cas, $\max\{|a|^2,\ |d|^4,\ |bd|\} \leq C_1''' \max\{|a|^2,\ |d|^4\}$ et enfin $H(P + P_0) \leq C_1 \max\{|a|^2,\ |d|^4\} = C_1 H(P)^2$ et en prenant les logarithmes on obtient $h_x(P + P_0) \leq 2h_x(P) + \log C_1$ ce qui est la première propriété dans la définition de hauteur. Si enfin $P = O, \pm P_0$, on peut choisir (sans perte de généralité) $C_1 > \max\{h_x(P_0), h_x(2P_0)\}$ et la propriété est encore vraie.

Pour la seconde propriété on prend $P \in E(\mathbb{Q})$ tel que $2P \neq O$ (on peut bien ne pas considérer les points de 2-torsion car ils sont en nombre fini, et donc il suffit de choisir un C_2 assez grand). On écrit $x(P) = x = a/b$ et on utilise la formule de duplication pour écrire

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx - A^2}{4x^3 + 4Ax + 4B} = \frac{F(a,b)}{G(a,b)}$$

où on a définit les polynômes homogènes $F(X, Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4$ et $G(X, Z) = 4X^3Z + 4AXZ^3 + 4BZ^4$ (noter que G n'est pas le polynôme homogène associé au dénominateur dans la formule de duplication : il y a un facteur Z en plus, pour que ce polynôme ait le même degré que F).

Maintenant on remarque que $F(X,1)$ et $G(X,1)$ sont des polynômes de $\mathbb{Q}[X]$ qui sont premiers entre eux, et donc ils engendrent tout $\mathbb{Q}[X]$. En particulier, si $\Delta = 4A^3 + 27B^2$, il existe des polynômes f_1, g_1, f_2, g_2 homogènes tels que

$$f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) = 4\Delta Z^7$$

$$f_2(X,Z)F(X,Z) - g_2(X,Z)G(X,Z) = 4\Delta X^7$$

Soit $\delta = \mathrm{pgcd}(F(a,b), G(a,b))$, alors les équations ci-dessus montrent que δ divise 4Δ (car a et b sont bien sûr premiers entre eux) et donc trivialement $|\delta| \leq |4\Delta|$, d'où $H(x(2P)) \geq \dfrac{\max\{|F(a,b)|,\ |G(a,b)|\}}{|4\Delta|}$.

Encore par les équations ci-dessus, on a que

$$|4\Delta b^7| \leq 2\max\{|f_1(a,b)|,\ |g_1(a,b)|\}\max\{|F(a,b)|,\ |G(a,b)|\}$$

$$|4\Delta a^7| \leq 2\max\{|f_2(a,b)|,\ |g_2(a,b)|\}\max\{|F(a,b)|,\ |G(a,b)|\}$$

et comme f_1, g_1, f_2 et g_2 sont des polynômes de degré 3 (regarder les équations qui les définissent), on a aussi la relation

$$\max\{|f_1(a,b)|,\ |g_1(a,b)|,\ |f_2(a,b)|,\ |g_2(a,b)|\} \leq C\max\{|a|^3,\ |b|^3\}$$

pour quelque constante réelle C. En mettant ensemble les trois relations trouvées, on obtient enfin

$$\max\{|4\Delta a^7|,\ |4\Delta b^7|\} \leq 2C\max\{|a|^3,\ |b|^3\}\max\{|F(a,b)|,\ |G(a,b)|\}$$

d'où l'inégalité finale

$$H(x(2P)) \geq \frac{\max\{|F(a,b)|,\ |G(a,b)|\}}{|4\Delta|} \geq (2C)^{-1}\max\{|a|^4,\ |b|^4\}$$

et en prenant les logarithmes on obtient la propriété 2 des hauteurs.

L'ensemble des nombres rationnels avec hauteur plus petite qu'un nombre réel donné est clairement fini. Comme pour tout x rationnel, il y a au plus deux y tels que (x,y) soit sur la courbe elliptique, on a aussi la propriété 3 des hauteurs et le lemme est démontré. □

7 Le calcul du groupe

7.1 Procédure de calcul

Soit (E,O) une courbe elliptique avec point à l'infini O et avec un point rationnel d'ordre 2. Elle peut donc être définie, après une translation, par l'équation

$$E : y^2 = x^3 + ax^2 + bx$$

et soit r le rang de la partie libre de $E(\mathbb{Q})$. En utilisant le théorème de structure des groupes abéliens de type fini, on voit facilement que

$$(E(\mathbb{Q}) : 2E(\mathbb{Q})) = 2^r \cdot |E[2]|$$

où on écrit $E[m]$ pour les points de m-torsion. En regardant l'équation, on voit que les points de 2-torsion sont 2 si $a^2 - 4b$ n'est pas un nombre carré, et ils sont 4 si $a^2 - 4b$ est un nombre carré.

On appelle $\overline{E}$ la courbe auxiliaire définie par

$$\overline{E} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x = x^3 + \overline{a}x^2 + \overline{b}x$$

On a montré dans la preuve du théorème de Mordell faible que l'on a deux morphismes $\phi : E \to \overline{E}$ et $\psi : \overline{E} \to E$ dont la composition est la multiplication par 2. Alors

$$(E(\mathbb{Q}) : 2E(\mathbb{Q})) = (E(\mathbb{Q}) : \psi \circ \phi(E(\mathbb{Q}))) = (E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q})))(\psi(\overline{E}(\mathbb{Q})) : \psi \circ \phi E(\mathbb{Q}))$$

Maintenant, si on a un homomorphisme entre groupes abéliens $\psi : A \to A'$ et $B \subseteq A$ est un sous-groupe, on peut utiliser les théorèmes d'homomorphisme pour obtenir la formule

$$(\psi(A) : \psi(B)) = \frac{(A : B)}{(\ker(\psi) : \ker(\psi) \cap B)}$$

Si on applique cette formule avec $A = \overline{E}(\mathbb{Q})$ et $B = \phi(E(\mathbb{Q}))$ on obtient

$$(E(\mathbb{Q}) : 2E(\mathbb{Q})) = \frac{(E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q})))(\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q})))}{(\ker(\psi) : \ker(\psi) \cap \phi(E(\mathbb{Q})))}$$

et on vérifie avec aise en utilisant les définitions de ψ et de la courbe auxiliaire, que le dénominateur $(\ker(\psi) : \ker(\psi) \cap \phi(E(\mathbb{Q})))$ est 2 si $\overline{b}$ n'est pas un carré, et 1 si c'est un carré.

En mettant ensemble tout cela, on obtient la formule

$$2^r = \frac{(E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q})))(\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q})))}{4}$$

donc, pour calculer le rang de la partie libre du groupe des points rationnels, on doit calculer les indices au numérateur.

On rappelle l'homomorphisme q défini pendant la preuve du théorème de Mordell faible, c'est-à-dire $q : \overline{E}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ donné par

$$q(u, v) = u(\mathbb{Q}^*)^2 \quad si\ u \neq 0$$
$$q(u, v) = \overline{b}(\mathbb{Q}^*)^2 \quad si\ u = 0$$
$$q(O) = (\mathbb{Q}^*)^2$$

Dans la même preuve, on a montré que le noyau de q est exactement $\phi(E(\mathbb{Q}))$, et en définissant q sur $E(\mathbb{Q})$ avec les mêmes formules on obtient la formule finale

$$2^r = \frac{|q(E(\mathbb{Q})| \cdot |q(\overline{E}(\mathbb{Q}))|}{4}$$

On veut donc calculer les cardinaux ci-dessus, c'est-à-dire on veut trouver les nombres rationnels qui peuvent apparaître, modulo $(\mathbb{Q}^*)^2$, comme première coordonnée d'un point de E. On écrit $(x, y) = (\frac{m}{e^2}, \frac{n}{e^3})$ avec $e > 0$ et les fractions réduites.

Si $x = 0$, on a $(x, y) = (0, 0)$ et $q(x, y) = b$ est toujours dans l'image $q(E(\mathbb{Q}))$.

Si $a^2 - 4b = d^2$ est un carré, alors $(\frac{-a+d}{2}, 0)$ et $(\frac{-a-d}{2}, 0)$ sont des points d'ordre deux différents de $(0, 0)$ en général. Dans ce cas là on a donc $\frac{-a \pm d}{2} \in q(E(\mathbb{Q}))$.

On considère donc les points avec m et n non nuls. Alors on a l'équation

$$n^2 = m(m^2 + ame^2 + be^4)$$

Soit $b_1 = \pm \text{pgcd}(b, m)$ où on choisit pour b_1 le même signe de m, et soient $b_2 = b/b_1$ et $m_1 = m/b_1$. Comme on voit facilement que $b_1 | n$ on écrit $n = b_1 n_1$ aussi. En substituant dans l'équation ci-dessus on obtient donc

$$n_1^2 = m_1(b_1 m_1^2 + a m_1 e^2 + b_2 e^4)$$

Mais maintenant m_1 et $(b_1 m_1^2 + a m_1 e^2 + b_2 e^4)$ sont premiers entre eux et comme leur produit est un carré, chaque terme doit être un carré. Alors on peut factoriser $n = MN$ avec $M^2 = m_1$ et $N^2 = (b_1 m_1^2 + a m_1 e^2 + b_2 e^4)$, qui satisfont l'équation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$$

On a donc une façon directe pour calculer ce qu'on veut. Si on trouve des nombres entiers M et N tous les deux non nuls qui satisfont l'équation ci-dessus, on obtient aussi un point rationnel (x, y) en faisant la procédure inverse et alors $x = \frac{b_1 M^2}{e^2}$. Donc, modulo $(\mathbb{Q}^*)^2$, les nombres rationnels qui apparaissent comme première coordonnée d'un point de E sont les valeurs des b_1 pour lesquelles il y a une solution à l'équation ci-dessus avec M et N entiers non nuls. On constate *a posteriori* que M et N sont premiers entre eux, et donc dans la recherche des b_1 conduisants à une équation résoluble, on peut imposer M et N premiers entre eux sans perte de généralité. De même, on peut supposer M et b_1 premiers entre eux.

On ne connaît pas d'algorithme pour résoudre l'équation ci-dessus, mais on montrera dans un exemple un calcul explicite du groupe des points rationnels qui utilise le raisonnement effectué.

7.2 Exemple

On considère maintenant la courbe elliptique définie par l'équation

$$C : y^2 = x^3 - 5x$$

Sa courbe auxiliaire est

$$\overline{C} : y^2 = x^3 + 20x$$

Pour C, on a $b = -5$ et $a = 0$, et si on écrit $b = b_1 b_2$ de toute les façons possibles, on a quatre équations à résoudre.

$$N^2 = M^4 - 5e^4$$
$$N^2 = -M^4 + 5e^4$$
$$N^2 = 5M^4 - e^4$$
$$N^2 = -5M^4 + e^4$$

Les deux premières équations peuvent être résolues par $(N, M, e) = (1, 3, 2)$ et $(N, M, e) = (2, 1, 1)$ respectivement, et les deux dernières sont les mêmes avec M et e échangés. Donc on obtient $q(C(\mathbb{Q})) = \{\pm 1, \pm 5\} \pmod{\mathbb{Q}^{*2}}$ et on trouve les points rationnels correspondants avec les formules

$$x = \frac{b_1 M^2}{e^2} \qquad y = \frac{b_1 M N}{e^3}$$

Pour $\overline{C}$ on a $\overline{b} = 20$ et donc les seules possibilités pour $\overline{b_1}$ sont ± 1, ± 2, ± 5, ± 10. Comme $\overline{b_1 b_2} = \overline{b}$, les deux facteurs ont le même signe et s'ils sont négatifs, les équations correspondantes $N^2 = \overline{b_1} M^4 + \overline{b_2} e^4$ ne peuvent pas être résolues, on en déduit alors :

$$q(\overline{C}(\mathbb{Q})) \subseteq \{1,\ 2,\ 5,\ 10\} \pmod{\mathbb{Q}^{*2}}$$

Or, $q(\overline{O}) = 1$ et $q(0, 0) = \overline{b} = 20 = 5 \pmod{\mathbb{Q}^{*2}}$. On considère donc l'équation

$$N^2 = 2M^4 + 10e^4$$

et on cherche ses solutions parmi les nombres entiers tels que $\operatorname{pgcd}(M, 10) = 1$. Par le petit théorème de Fermat, on a $M^4 \equiv 1 \pmod 5$ et donc en regardant l'équation modulo 5, on doit avoir $N^2 \equiv 2 \pmod 5$, qui n'a pas de solution. Comme la condition $\operatorname{pgcd}(M, 10) = 1$ doit quand même être satisfaite, on déduit que $2 \notin q(\overline{C}(\mathbb{Q}))$. Comme $q(\overline{C}(\mathbb{Q}))$ est un sous-groupe de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ qui contient 5 mais pas 2, il ne peut pas contenir 10 non plus.

On a enfin que $q(\overline{C}(\mathbb{Q})) = \{1,\ 5\} \pmod{\mathbb{Q}^{*2}}$ et donc $2^r = \dfrac{4 \cdot 2}{4} = 2$ c'est-à-dire $r = 1$.

Pour calculer la torsion, on utilise le fait que si $(x, y) \in C(\mathbb{Q})$ est de torsion, alors x et y sont des entiers et soit $y = 0$ soit $y^2 | (4a^3 + 27b^2) = 27 \cdot 25 = 3^3 \cdot 5^2$. On vérifie directement qu'on n'a pas de point rationnel de ce type pour $y \neq 0$, et donc les seuls points de torsion sont de 2-torsion et ils sont $(0, 0)$ et le point à l'infini O. On peut donc écrire

$$C(\mathbb{Q}) \backsimeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Références

[1] J.W.S. Cassels. *Lectures on Elliptic Curves.* Cambridge university press, 1991.

[2] Marc Hindry. *Arithmetics.* Springer, 2011.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves.* Springer, 2009.