THÉORIE DES NOMBRES 1

Par
Nouressadat Touafek
Département de Mathématiques,
Université Mohamed Seddik Ben Yahia, Jijel
Année Universitaire 2019–2020.

N.B. Ce polycopié, est un résumé de cours Théorie des Nombres 1 que je donne aux étudiants du Master 1, Mathématiques Fondamentales et Discrètes, au sein du Département de Mathématiques de l'Université Mohamed Seddik Ben Yahia de Jijel.
Les notions développées ici ne sont pas originales et sont trés connues pour les gens qui travaillent sur les courbes elliptiques.
Pour plus de détails et de notions, on renvoie aux références utilisé pour réaliser ce polycopié et que je liste à la fin de ce résumé.

Tout au long de ce polycopié $\mathbb{K}$ désigne un corps commutatif : $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$.

CHAPITRE 1

COURBES PLANES PROJECTIVES : DÉFINITIONS ET RÉSULTATS GÉNÉRAUX

1.1 Plan projectif

Définition 1.1.1 *Le plan affine noté* $\mathbb{A}^2(\mathbb{K})$*, est l'ensemble des points* $(x, y) \in \overline{\mathbb{K}}^2$.

Définition 1.1.2 *Le plan projectif sur* $\mathbb{K}$ *est defini par*

$$\mathbb{P}_2(\mathbb{K}) := \frac{\{(X, Y, Z) \in \mathbb{K}^3 - 0_{\mathbb{K}^3}\}}{\sim}$$

La relation $\sim$ *est définie par :*

$$(X, Y, Z) \sim (X_1, Y_1, Z_1)$$

si et seulement si

$$\exists\, \lambda \in K^* : \ (X, Y, Z) = \lambda\,(X_1, Y_1, Z_1)\,.$$

L'élément de $\mathbb{P}_2(\mathbb{K})$*, la classe du point* $P = (X, Y, Z)$ *, sera noté* $[X, Y, Z]$ *ou* $(X : Y : Z)$*.*
X, Y, Z sont appelés : coordonnées homogènes du point P.

Remarque 1.1.1 1. *Si* $Z \neq 0$*, alors*

$$[X, Y, Z] = [x_1, y_1, 1],\ x_1 = \frac{X}{Z},\ y_1 = \frac{Y}{Z}.$$

Le point (X, Y, Z) *de* $\mathbb{P}_2(\mathbb{K})$ *peut s'identifier à un de* $\mathbb{A}^2(\mathbb{K})$*. Autrement dit, on a une injection :*

$$i : \ \mathbb{A}^2(\mathbb{K}) \to \mathbb{P}^2(\mathbb{K})\ i(x, y) = [x, y, 1].$$

Cette application n'est pas surjective car la droite $Z = 0$ *n'est pas atteint. i est appelée plongement canonique du plan affine dans le plan projectif.*

2. *Dans le plan projectif on a deux types de points, (points affines) ceux avec* $Z \neq 0$ *et (points á linfini) ceux avec* $Z = 0$ *.*

1.2 Courbes planes projectives

Définition 1.2.1 *Un polynôme* $F \in \mathbb{K}[X_1, X_2, ..., X_n]$ *est dit homogène de degré d si tout monôme de F est de degré totale d. De plus, F est dit irréductible s'il ne peut s'écrire comme le produit non trivial de deux polynômes de* $\mathbb{K}[X_1, X_2, ..., X_n]$*.*

Exemple 1.2.1 *Le polynôme* F_1 *de* $\mathbb{R}[X, Y, Z]$ *avec*

$$F_1(X, Y, Z) = X^3 + XY^2 + XYZ$$

est homogéne de degré 3. Cependant le polynôme F_2 de $\mathbb{R}[X,Y,Z]$ definit par

$$F_2(X,Y,Z) = X^3 + XY^2 + XY$$

est degré 3, mais n'est pas homogène, (deux monômes sont de degrés 3 et l'autre de degré 2).

Exercice 1.2.1 *Considérons le polynôme non nul P de $\mathbb{K}[X_1, X_2, ..., X_n]$.*
Montrer que P est homogène de degré d si et seulement si, pour une variable auxiliaire $t \in \mathbb{K}^*$

$$P\ (tX_1, tX_2, ..., tX_n) = t^d P(X_1, X_2, ..., X_n)$$

Preuve. *1. $\Rightarrow$) Évidente. Il suffit d'écrire :*

$$P(X_1, X_2, ..., X_n) = a_1 X_1^{k_{1,1}} ... X_n^{k_{1,n}} + a_2 X_1^{k_{2,1}} ... X_n^{k_{2,n}} + a_i X_1^{k_{1,1}} ... X_n^{k_{i,n}}$$

avec

$$k_{1,1} + ... + k_{1,n} = k_{2,1} + ... + k_{2,n} = k_{i,1} + ... + k_{i,n} = d.$$

2. $\Leftarrow$) Inversement, écrivons P comme une somme de polynômes homogènes non nuls de degré d_i

$$P = P_{d_1} + P_{d_2} + ... + P_{d_k},\ d_1 \leq d_2 ... \leq d_k.$$

En utilisant le fait que

$$P(tx_1, tx_2, ..., tx_n) = t^d P(x_1, x_2, ..., x_n)$$

on obtient que

$$t^{d_1} P_{d_1} + t^{d_2} P_{d_2} + ... + t^{d_k} P_{d_k} = t^d P = t^d P_{d_1} + t^d P_{d_2} + ... + t^d P_{d_k}$$

donc

$$t^{d_i} = t^d, \forall i = 1, ..., k.$$

Par conséquent $k = 1$ et $P = P_{d_1}$. ■

Définition 1.2.2 *Une courbe plane projective C de $\mathbb{P}_2(K)$ est l'ensemble des points (X,Y,Z) (X, Y, Z non tous nuls) qui satisfont à*

$$F(X,Y,Z) = 0,$$

où F est un polynôme homogène de $\mathbb{K}[X,Y,...,Z]$ de degré $d \geq 1$.

Remarque 1.2.1 *1. Si $d = 1$, alors C est appellée **droite**, et elle prend la forme*

$$C : P(X, Y, Z) = aX + bY + cZ = 0,\ (a, b, c) \neq 0_{\mathbb{K}^3}.$$

*2. Si $d = 2$, alors C est appelée **conique**, et elle prend la forme*

$$C : P(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0,\ (a, b, c, d, e, f) \neq 0_{\mathbb{K}^6}.$$

*3. Si $d = 3$, alors C est appellée **cubique**, et elle prend la forme*

$$\begin{aligned} C : P(X, Y, Z) &= aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z \\ &\quad + hXZ^2 + jYZ^2 + kZ^3 = 0, (a, b, c, d, e, f, g, h, j, k) \neq 0_{\mathbb{K}^{10}}. \end{aligned}$$

4. L'entier d est appelé le degré de la courbe.

N.B *En pratique pour passer de la forme projective (en X, Y, Z) à la forme affine (en x, y) d'une courbe on pose $Z = 1$ et en change X et Y par x et y. Inversement, si une courbe affine (en x, y) est de degré d, on change x par X et y par Y, et on multiplie par des puissances de Z de sortes que tous les monômes serons du même degré d.*

Exemple 1.2.2 *La version affine de $X^3 + Y^2Z + XZ^2 = 0$ est $x^3 + y^2 + x = 0$. Inversement puisque le degré de $x^3 + y^2 + x = 0$ est 3, alors on change x en X et y en Y, puis multiplions le deuxième monôme par Z et le troixième par Z^2 pour avoir $X^3 + Y^2Z + XZ^2 = 0$.*

Exercice 1.2.2 *1. Soient L_1, L_2 deux droites du plan projectif d'équations*

$$L_1 : a_1X + b_1Y + c_1Z = 0,\ L_2 : a_2X + b_2Y + c_2Z = 0.$$

Montrer que si $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$, alors $L_1 \equiv L_2$.

2. Soient L_1, L_2 deux droites parallèles du du plan affine d'équations

$$L_1 : a_1x + b_1y + c_1 = 0,\ L_2 : a_2x + b_2y + c_2z = 0.$$

Montrer que L_1 et L_2, considérés comme des droites du plan projectif, síntersectent.

Preuve.

1. Il existe $\lambda \in K^*$, tel que $a_1 = \lambda a_2$, $b_1 = \lambda b_2$, $c_1 = \lambda c_2$ ainsi :

$$a_1X + b_1Y + c_1Z = \lambda(a_2X + b_2Y + c_2Z) = 0.$$

2. *Comme les deux droites sont parallèles, alros il* $\exists\, t \in K^*$, *tel que*

$$a_2 = ta_1,\ b_2 = tb_1.$$

Dans le plan projectif les deux droites s'écrivent

$$L_1 : a_1X + b_1Y + c_1Z = 0,\ L_2 : a_2X + b_2Y + c_2Z = 0.$$

Pour $Z = 0$, *on aura*

$$L_1 : a_1X + b_1Y,\ L_2 : t(a_1X + b_1Y) = 0.$$

■

Remarque 1.2.2 *En géométrie projective, tous les droites s'intersectent.*

1.3 Courbes lisses

Définition 1.3.1 *Un point P d'une courbe C du plan projectif* $\mathbb{P}_2(\mathbb{K})$ *d'équation :* $F(X, Y, Z) = 0$, *est dit singulier si*

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

Si non, P est dit non singulier ou simple.

Définition 1.3.2 *La courbe C est dite courbe non singulière (lisse) si tous ses points sont simples.*

Exercice 1.3.1

1. *Montrer que la courbe C définie sur* $\mathbb{R}$ *(i.e., une courbe de* $\mathbb{P}_2(\mathbb{R})$*) par*

$$C/\mathbb{R} : ZY^2 = X^3.$$

est une courbe singulière au point $P = [0, 0, 1]$.

2. *Montrer que la courbe* $C/\mathbb{R}$ *définie par*

$$Y^2Z - X^3 + 3XZ^2 - 3Z^3 = 0$$

est lisse.

Preuve.

1. *Posons* $F(X,Y,Z) = ZY^2 - X^3$. *On a*

$$F(0,0,1) = \frac{\partial F}{\partial X}(0,0,1) = \frac{\partial F}{\partial Y}(0,0,1) = \frac{\partial F}{\partial Z}(0,0,1) = 0.$$

2. *Posons*

$$F(X,Y,Z) = Y^2Z - X^3 + 3XZ^2 - 3Z^3 = 0.$$

Alors un point $P_0 = (X_0, Y_0, Z_0$ *de la courbe C est singulier si*

$$\frac{\partial F}{\partial X}(P_0) = \frac{\partial F}{\partial Y}(P_0) = \frac{\partial F}{\partial Z}(P_0) = 0.$$

Cela donne

$$-3X_0^2 + 3Z_0^2 = 2Y_0Z_0 = Y_0^2 + 6X_0Z_0 - 9Z_0^2 = 0.$$

Le seul point qui satisfait ces équations est le point $P_0 = (0,0,0)$, *donc la courbe est lisse.*

■

Soit C une courbe définie sur $\mathbb{K}$ *par*

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ - a_6Z^3 = 0.$$

On veut déterminer la nature des points singuliers (lorsque existent) de la courbe C.

Exercice 1.3.2 *La courbe C a un seul point à l'infini et il est non singulier.*

Preuve. *Posons* $Z = 0$, *nous obtenons,* $X^3 = 0$, *ainsi* $(X,Y,Z) = (0,Y,0)$, $Y \neq 0$.
i.e., $(0:1:0)$) *et le seul point á l'infini. Comme*

$$\frac{\partial F}{\partial y}(0,1,0) = 1 \neq 0,$$

il résulte que ce point est non singulier. ■

Ainsi, si la courbe C à un point singulier alors ce point sera affine. La version affine de C est

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Supposons que $P = (x_0, y_0)$ *est un tel point. En faisons le devellopement de Taylor de* f *au voisinage de* $P = (x_0, y_0)$ *et en utilisant le fait que*

$$f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0,$$

on obtient

$$f(x,y) - f(x_0,y_0) = [(y-y_0) - \alpha(x-x_0)][(y-y_0) - \beta(x-x_0)] - (x-x_0)^3,\ \alpha,\ \beta \in \overline{K}.$$

Définition 1.3.3 *Le point singulier P est dit :*

1. *Un nœud si $\alpha \neq \beta$. Dans ce cas, la courbe C admet deux tangentes distinctes au point P*

$$y - y_0 = \alpha(x-x_0) \ \ et \ \ \ y - y_0 = \beta(x-x_0)$$

2. *Un point de rebroussement si $\alpha = \beta$. Dans ce cas, la courbe C admet deux tangentes confondues au point P*

$$y - y_0 = \alpha(x-x_0)$$

Exercice 1.3.3 *Considérons sur $\mathbb{R}$ la courbe C d'équation*

$$x(y^2-1) = y(x^2-2).$$

Énumérer les points à l'infini de la courbe C, puis dire qu'elle est la nature de chaque point.

Preuve. *En projectif, la courbe s'écrit :*

$$F(X,Y,Z) = X(Y^2 - Z^2) - Y(X^2 - 2Z^2) = 0.$$

Posons $Z = 0$. Ainsi, on obtient

$$XY(Y-X) = 0.$$

Si $X = 0$, $Y \neq 0$, le point $(X,Y,Z) = (0,Y,0)$, donc on a le point $P_1 = (0:1:0)$. Pour ce point $\frac{\partial F}{\partial X}(P_1) = 1$. On déduit que P_1 est non singulier.
Si $Y = 0$, $X \neq 0$, le point $(X,Y,Z) = (X,0,0)$, donc on a le point $P_2 = (1:0:0)$. Pour ce point $\frac{\partial F}{\partial Y}(P_2) = -1$. On déduit que P_2 est non singulier.
Si $Y = X \neq 0$, le point $(X,Y,Z) = (X,X,0)$, $Y \neq 0$, donc on a le point $P_3 = (1:1:0)$. Pour ce point $\frac{\partial F}{\partial X}(P_3) = -1$. On déduit que P_3 est non singulier. ■

Exercice 1.3.4 *Consiérons les deux courbes*

$$C_1/\mathbb{R} : f_1(x,y) = y^2 - x^3 - 9x^2 = 0,\ C_2/\mathbb{R} : f_2(x,y) = y^2 - (x-1)^3 = 0.$$

Etudier l'existence et la nature des points singuliers de ces deux courbes.

Preuve. *Les point singuliers (lorque existent) seront affines. Il est facile de voir que* $P = (0,0)$ *le seul point singulier pour la courbe* C_1*. Le dévloppement de Taylor au voisinage de ce point nous donne :*

$$f(x,y) = (y-3x)(y+3x) - x^3,\ \alpha = 3 \neq \beta = -3.$$

Il résulte que P est un noued, et on a les deux droites tangentes $y = 3x$, $y = -3x$.
De même on démontre que $Q = (1,0)$ *est le seul point singulier pour la courbe* C_2*. Le dévloppement de Taylor au voisinage de ce point nous donne :*

$$f(x,y) = y^2 - x^3 = (y-0.x)(y-0.x) - x^3,\ \alpha = \beta = 0.$$

Il résulte que Q est point de rebroussement, et on a deux droites tangentes confondues déquations $y = 0$. ■

Remarque 1.3.1 *Parmi les points qui satisfont à une courbe C, on a ceux avec* $(X,Y,Z) \in \mathbb{K}^3$ *et d'autres avec* $(X,Y,Z) \in \overline{\mathbb{K}}^3 - \mathbb{K}^3$.

Définition 1.3.4 *L'ensemble des points* $\mathbb{K}$*-rationnels d'une courbe C de* $\mathbb{P}_2(\mathbb{K})$ *est l'ensemble, notée* $C(\mathbb{K})$*, défini par*

$$C(\mathbb{K}) := \left\{(X,Y,Z) \in \mathbb{K}^3 : F(X,Y,Z) = 0.\right\}.$$

Exemple 1.3.1 *Soit la courbe* $C/\mathbb{R}$ *défnie par*

$$ZY^2 = X^3.$$

Les point $(0,0,1)$, $(1,-1,1)$ *sont des points* $\mathbb{R}$*-rationnels. Cependant le point* $(-1,i,1)$ *n'est pas* $\mathbb{R}$*-rationnel.*

Exercice 1.3.5 *Consiérons la courbe* $C/\mathbb{F}_2$ *défnie par*

$$Y^2 + X^2 + XZ + YZ = 0.$$

Donner l'ensemble $C(\mathbb{F}_2)$.

Preuve. *Pour les points à l'infini, posons* $Z = 0$*, on obient*

$$Y^2 + X^2 = 0.$$

Le seul point satisfait cette relation est $(1,1,0)$. *Pour les points affines* ($Z \neq 0$), *divisons par* Z^2, *puisque le degré de la courbe est* 2. *Posons*

$$x = \frac{X}{Z},\ y = \frac{Y}{Z},$$

on obtient

$$y^2 + x^2 + x + y = 0.$$

En tenant compte de la caractéristique du corps, nous obtenons

$$(x+y)^2 + x + y = (x+y)(x+y+1) = 0.$$

Ce qui donne $x + y = 0$ *ou* $x + y + 1 = 0$. *La premiere équation nous donne les points* $(0,0,1)$, $(1,1,1)$ *et la deuxième donne les points* $(1,0,1)$, $(0,1,1)$. *Ainsi*

$$C/\mathbb{F}_2 = \{(1,1,0),(0,0,1),(1,1,1),(1,0,1),(0,1,1)\}.$$

■

CHAPITRE 2

COURBES ELLIPTIQUES

2.1 Forme de Weierstrass

Définition 2.1.1 *Une courbe elliptique sur un corps* $\mathbb{K}$ *est une paire* (E, O) *où* E *désigne une cubique* $(d = 3)$ *irréductible, non-singulière et* O *un point de* E.

Une courbe elliptique peut être définie comme suit.

Définition 2.1.2 *Une courbe elliptique du plan projectif* $\mathbb{P}_2(\mathbb{K})$ *est une cubique lisse de la forme*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,\ a_i \in \mathbb{K}.$$

Il est claire que le point $O = (0 : 1 : 0)$ *est un point de la courbe.*

Remarque 2.1.1 *la version affine de la courbe elliptique E est donnée par*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

plus le point à l'infini $O = (0 : 1 : 0)$.
Cette forme est appelée forme de Weierstrass (généralisée). On verra plus loin que le point à l'infini $O = (0 : 1 : 0)$ *jouera le rôle de l'élément neutre.*

Définition 2.1.3 *Le genre d'une courbe plane projective C de degré d est l'entier positif g défini*

par :

$$g = \frac{(d-1)(d-2)}{2} - \sum_P \frac{m_P(m_P-1)}{2}$$

avec P désigne un point singulier de la courbe C de multiplicité m_P. Lorsque C est une courbe elliptique E (donc lisse), alors on a pas de points singuliers et $d = 3$ puisque E est une cubique, d'où

$$g = \frac{(d-1)\,(d-2)}{2} = 1.$$

Remarque 2.1.2 *La non-singularité d'une courbe donnée par une forme de Weierstrass est détecté par la valeur non-nulle d'une quantitée qu'on note $\triangle$ et qu'on l'appelle discriminant.*

Définition 2.1.4 *Le discriminant $\triangle$ d'une courbe E donnée par une équation de Weierstrass*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{K}$$

est la quantité

$$\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

Lorsque ($\triangle \neq 0$, i.e., E est une courbe elliptique), on d'éfinit le j-invariant de la courbe elliptique E par

$$j = \frac{c_4^3}{\triangle}.$$

avec

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2,\ c_4 = b_2^2 - 24b_4.$$

Théorème 2.1.3 *Soit $E/\mathbb{K}$ une courbe elliptique d'équation de Weierstrass généralisée*

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

Supposons que Car $(\mathbb{K}) \neq 2$, alors la courbe E prend la forme

$$Y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,\ Y = y + \frac{1}{2}(a_1x + a_3).$$

Supposons de plus que Car $(\mathbb{K}) \neq 3$, alors E prend une forme simplifiée

$$Y^2 = X^3 + AX + B,\ Y = y + \frac{1}{2}(a_1x + a_3),\ X = x + \frac{b_2}{12}.$$

et on a

$$\triangle = -16\left(4A^3 + 27B^2\right),\ j = -1728\frac{(4A)^3}{\triangle},$$

avec

$$A = -\frac{c_4}{48},\ B = -\frac{c_6}{864},\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Preuve. *Supposons Car* $(\mathbb{K}) \neq 2$. *Alors, par complétion du carré, nous obtenons*

$$\begin{aligned}\left(y + \frac{1}{2}(a_1x + a_3)\right)^2 &= x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{4}(a_1x + a_3)^2 \\ &= x^3 + \frac{1}{4}(a_1 + 4a_2)x^2 + \frac{1}{2}(a_1a_3 + 2a_4)x + \frac{1}{4}\left(a_3^2 + 4a_6\right) \\ &= x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}\end{aligned}$$

d'où

$$Y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

avec

$$Y = y + \frac{1}{2}(a_1x + a_3).$$

Supposons de plus que Car $(\mathbb{K}) \neq 3$, *par complétion du cube dans*

$$Y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

on obtient

$$\begin{aligned}Y^2 &= (x + \frac{b_2}{12})^3 - \frac{b_2^2}{48}x - \frac{b_2^3}{1728} + \frac{b_4}{2}x + \frac{b_6}{4} \\ &= (x + \frac{b_2}{12})^3 - \frac{1}{48}(b_2^2 - 24b_4)x - \frac{1}{1728}(b_2^3 - 432b_6) \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)(x - \frac{b_2}{12}) - \frac{1}{1728}(b_2^3 - 432b_6) \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)x + \frac{1}{576}b_2^3 - \frac{1}{24}b_2b_4 - \frac{1}{1728}b_2^3 + \frac{432}{1728}b_6) \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)x + \frac{1}{864}b_2^3 - \frac{1}{24}b_2b_4 + \frac{1}{4}b_6 \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)x - \frac{1}{864}(-b_2^3 + 36b_2b_4 - 216b_6)\end{aligned}$$

donc, la forme simplifiée de Weierstrass est

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

avec

$$X = x + \frac{b_2}{12}.$$

De plus

$$A = -\frac{c_4}{48},\ B = -\frac{c_6}{864},\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

d'où

$$\triangle = -16(4A^3 + 27B^2),\ j = \frac{c_4^3}{\triangle} = -1728\frac{(4A)^3}{\triangle}.$$

■

Lemme 2.1.1 *Soit $E/\mathbb{K}$ une courbe d'équation de Weierstrass*

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

dont le discriminant est $\triangle$ et le $j-$invariant j (lorsque $\Delta \neq 0$).
Le changement de variables

$$x = u^2X + r,\ y = u^3Y + u^2sX + t,\ r,\ s,\ t,\ u(\neq 0) \in \mathbb{K}(\overline{\mathbb{K}})$$

transforme l'équation de Weierstrass précédente en l'équation

$$E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6',\ a_i' \in \mathbb{K}(\overline{\mathbb{K}}),$$

avec

$$\begin{aligned}
ua_1' &= a_1 + 2s\ ,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t\ ,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)\,a_1 + 3r^2 - 2st\ ,\\
u^6a_6' &= a_6 + ra_4 + r^2a_2 - ta_3 - rta_1 + r^3 - t^2.
\end{aligned}$$

De plus,

$$u^{12}\Delta' = \Delta,$$

et lorque $\Delta \neq 0$, on aura aussi

$$j' = j.$$

Preuve. *Il suffit de remplacer par les nouvelles expressions de x et y.* ■

Définition 2.1.5 *Tout changement de coordonnées de la forme*

$$x = u^2X + r,\ y = u^3Y + u^2sX + t$$

est dit admissible.

Théorème 2.1.4 *Soit $E/\mathbb{K}$ une courbe elliptique donnée par l'équation de Weierstrass*

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

alors,

$$E \text{ est lisse (non-singulière)} \Leftrightarrow \ \Delta \neq 0.$$

Preuve. *En projectif, la courbe E s'écrit*

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

On sait que le seul point à l'infinit $O = [0,1,0]$ n'est pas point singulier de E, et que si un point singulier existe, il sera affine.

1. *Supposons que $\Delta \neq 0$, et montrons que E est lisse. Si, E admet un point singulier $P_0 = (x_0, y_0)$, alors par le changement de variable*

   $$(x,y) \leftarrow (x - x_0, y - y_0)$$

   nous ramenons le point P_0 en le point $(0,0)$, ce changement de varibles est admissible (avec $u = 1$) et donc ne modifie pas le discriminant, i.e.,

   $$\Delta' = \Delta$$

   avec Δ' le discriminant de la courbe E'd'é quation

   $$E' : f'(x,y) = y^2 + a'_1\ xy + a'_3y - x^3 - a'_2x^2 - a'_4x - a'_6$$

   On a

   $$a'_6 = f'(0,0) = 0\ \ , a'_3 = \frac{\partial f'}{\partial y}(0,0) = 0, a'_4 = \frac{\partial f'}{\partial y}(0,0) = 0$$

   donc, E' s'écrit

   $$E' : f'(x,y) = y^2 + a'_1\ xy - x^3 - a'_2x^2.$$

   Le disctiminant de cette équation est nul, ce qui contredit l'hypothèse ; c'est-à-dire E

n'admet pas des points singuliers.

2. *Inversement, supposons que notre courbe E est lisse, et montrons que* $\Delta \neq 0$.
Pour raison de simplification, on se restraint au cas $Car(\mathbb{K}) \neq 2, 3$.

Si $Car(\mathbb{K}) \neq 2$, *alors E s'écrit*

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Le point $P_0 = (x_0, y_0)$ *de E sera singulier* $\Leftrightarrow 2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$. *C'est -à-dire, les points singuliers de E sont les points de la forme de cordonnées* $(x_0, 0)$, *avec* x_0 *est une racine double de l'équation*

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0.$$

Notons que cette dernière équation admet une racine double si est seulement si son discriminant qui égale $16\triangle$ *est nul.*
Si de plus, $Car(\mathbb{K}) \neq 3$, *nous obtenons la forme simplifier de E,*

$$E : y^2 = x^3 + Ax + B.$$

Si $P_0 = (x_0, y_0)$ *est un point singulier de E, alors*

$$2y_0 = 0,\ 3x_0^2 + A = 0 \Leftrightarrow y_0 = 0,\ x_0^2 = -\frac{A}{3}.$$

Il résulite que

$$y_0^2 = 0 = x_0^3 + Ax_0 + B = \frac{2}{3}Ax_0 + B$$

donc

$$x_0 = -\frac{3B}{2A}$$

ainsi,

$$x_0^2 = \frac{9B^2}{4A^2} = -\frac{A}{3} \Leftrightarrow -16\left(4A^3 + 27B^2\right) = 0 = \Delta.$$

■

2.2 Loi de Groupe

Le but de cette partie est de définir une loi de composition pour la courbe ellipitique E définie sur $\mathbb{K}$ *par la forme de Weierstrass avec* $O = (0 : 1 : 0)$ *son seul point à l'infini. Cette loi confère*

à E et en particulier à $E(K) \subseteq E$ la structure d'un groupe abélien.

Théorème 2.2.1 **Théorème de Bezout.** *Soient C_1 et C_2 deux courbes planes projectives, sans composantes communes, définies respectivement par deux polynômes homogènes $F_1(X, Y, Z)$ et $F_2(X, Y, Z)$ de $\overline{\mathbb{K}}[X, Y, Z]$, de degrés respectifs d_1 et d_2 Alors C_1 et C_2 s'intersectent en $d_1 d_2$ points.*

On définit sur E, la loi de composition interne qu'on note $\oplus$ comme suit :
Soient deux points distincts P, Q de E, et L la droite passant par P et Q. Alos par le Théorème de Bezout, L s'intersecte avec E en trois points P, Q et le troisième point R (Les points P, Q, R peuvent être identiques). Soit L_1 la droite passant par R et le point à l'infini $\boldsymbol{O}$. Il résulte par le Théorème de Bezout que L_1 et E s'intersectent aussi en un troisième point qu'on le note $P \oplus Q$, i.e.,

$$(P \oplus Q) \oplus R = \boldsymbol{O}.$$

Ainsi la loi est interne et on a :

1. $\forall$ *P, Q* $\in E$ *:* $P \oplus Q = Q \oplus P$. *Commutativité.*
2. $\forall$ $P \in E$ *:* $P \oplus \boldsymbol{O} = P$. *Élément neutre.*
3. $\ominus P = R$. *Élément symétrique.*
4. $\forall$ *P, Q, R* $\in E$ *:* $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$. *Associativité.*

Théorème 2.2.2 *La loi $\oplus$ confère à*

$$E = \left\{(x, y) \in \overline{K}^2 : \ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\right\} \cup \{\boldsymbol{O}\}$$

la structure d'un groupe abélien.

Dans toute la suite on écrit + (resp. −) au lieu de $\oplus$ (resp. $\ominus$).

2.3 Formules Explicites

Soient P et Q deux point de coordonnées $P = (x_P, y_P)$, $Q = \left(x_Q, y_Q\right)$. On va donné des formules explicites des coordonnées de $-P = (x_{-P}, y_{-P})$ et $P + Q = (x_{P+Q}, y_{P+Q})$.

2.3.1 Coordonnées de $-P$

Soit (L) *la droite passant par* P *et* O*, alors*

$$L : aX + bY + cZ = 0,\ (a, b, c) \neq 0_{\mathbb{K}^3}.$$

Comme O *est un point de* (L)*, alors elle prend la forme* $L : aX + cZ = 0$*, mais* $P \in L$*, donc* $ax_P + c = 0$*. Ainsi* $c = -ax_P$*, et donc*

$$L : x - x_P = 0.$$

Ainsi,

$$f(x_P, y) = y^2 + (a_1 x_P + a_3)\, y - \left(x_P^3 + a_2 x_P^2 + a_4 x_P + a_6\right) = (y - y_P)(y - y_{-P}).$$

Par identification, on obtient que

$$y_{-P} = -y_P - a_1 x_P - a_3.$$

Donc,

$$-P = \left(x_P, -y_P - a_1 x_P - a_3\right).$$

2.3.2 Coordonnées de $P + Q$ avec $P \neq Q$

1. *Si*

$$x_P = x_Q,\ y_P + y_Q + a_1 x_P + a_3 = 0,$$

alors

$$P + Q = O.$$

2. *Si* $x_P \neq x_Q$*, la droite passant par* P *et* Q *a pour équation*

$$y = \alpha x + \beta,$$

avec $\alpha = \frac{y_Q - y_P}{x_Q - x_P}$ *et* $\beta = y_P - \alpha x_P$*, ou bien* $\beta = y_Q - \alpha x_Q$*. En portant dans l'équation de* E*, on obtient*

$$f(x, \alpha x + \beta) = -x^3 + \left(\alpha^2 + \alpha a_1 - a_2\right) x^2 + \left(2\alpha\beta + \beta a_1 + \alpha a_3 - a_4\right) x + \beta^2 + \beta a_3 - a_6 = 0.$$

Les racines de cette équations sont x_P*,* x_Q *et* x_R *où* $R = (x_R, y_R)$ *est le troisième point*

d'intersection entre la droite passant par P et Q et la courbe E. Ainsi

$$f(x, \alpha x + \beta) = \gamma (x - x_P)\left(x - x_Q\right)(x - x_R).$$

Il résulte que

$$\gamma = -1,\ x_P + x_Q + x_R = \alpha^2 + \alpha a_1 - a_2.$$

Ainsi

$$\begin{aligned} x_R &= x_{P+Q} = \alpha^2 + \alpha a_1 - a_2 - x_P - x_Q \\ y_R &= y_{P+Q} = \alpha x_R + \beta \end{aligned}$$

i.e.,

$$R = \left(\alpha^2 + \alpha a_1 - a_2 - x_P - x_Q, \alpha x_R + \beta\right) = (x_R, y_R) \tag{2.2}$$

donc

$$\begin{aligned} P + Q &= -R = (x_R, -y_R - a_1 x_R - a_3) \\ &= \left(x_R, -(\alpha + a_1) x_R - (a_3 + \beta)\right). \end{aligned}$$

2.3.3 Coordonnées de $2P$

C'est le cas P = Q, et la droite passant par P et Q sera la droite tangente T à la courbe E en le point P. Soit

$$T := y = \alpha x + \beta$$

on a,

$$df = \frac{\partial f}{\partial y}(x, y)dy + \frac{\partial f}{\partial x}(x, y)dx = 0$$

et donc

$$\frac{dy}{dx} = -\frac{\frac{\partial f}{\partial x}(x, y)}{\frac{\partial f}{\partial y}(x, y)} = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}.$$

Ainsi

$$\alpha = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3}$$

en portant dans (2.2)*, on obtient les coordonées du troisième point d'intersection*

$$R = (\overline{x}_{2P}, \overline{y}_{2P}).$$

c'est -à-dire que

$$2P = -R = \left(\overline{x}_{2P}, -\overline{y}_{2P} - a_1\overline{x}_{2P} - a_3\right).$$

Exercice 2.3.1 *1. Soit E la courbe elliptique définie sur* $\mathbb{Q}$ *par*

$$E : y^2 = x^3 - 25x.$$

Soient $P = (5, 0)$ *et* $Q = (-4, 6)$ *deux points de la courbe E.*
Calculer $-P$ *et déduire que* $2P = \mathcal{O}$*, puis calculer* $P + Q$*.*

Preuve. *On a* $-P = (x_P, -y_P - a_1x_P + a_3) = (5, 0)$*, ainsi* $P = -P$ *ce qui donne* $2P = \mathcal{O}$*.*
Il n'est pas difficile de voir que la droite L passant par P et Q a pour équation

$$L : y = \frac{-2}{3}(x - 5).$$

Remplaçant par

$$y = \frac{-2}{3}(x - 5)$$

dans l'équation de la courbe, nous obtenons

$$(x - 5)(x + 4)(9x + 5) = 0.$$

Ce qui donne

$$x_R = -\frac{5}{9},\ y_R = \frac{100}{27}.$$

Ainsi,

$$P + Q = -R = \left(-\frac{5}{9}, -\frac{100}{27}\right).$$

■

Exercice 2.3.2 *Considérons la courbe elliptique E définie sur* $\mathbb{Q}$ *par*

$$E : f(x, y) = y^2 - x^3 - 1 = 0.$$

Calculer $2P$*, avec* $P = (2, 3)$*.*

Preuve. *La droite tangente T en P a pour équation*

$$y = -\frac{\frac{\partial f}{\partial x}(P)}{\frac{\partial f}{\partial y}(P)}x + b,$$

ainsi $y = 2x - 1$. *L'abscisse* x_R *du troisiè point d'intersection, sera une racine de*

$$f(x, 2x - 1) = (x - 2)^2 x = 0.$$

Donc $x_R = 0$ *et* $y_R = 2x_R - 1 = -1$, *il résulte que* $R = (0, -1)$ *et* $2P = -R = (0, 1)$. ■

CHAPITRE 3

EQUIVALENCES ENTRE COURBES ET ISOMORPHES DE COURBES ELLIPTIQUES

3.1 Courbes birationnellement équivalentes

Définition 3.1.1 *Soient C_1, C_2 deux courbes de $P_2(\mathbb{K})$ et soient P, Q , R trois polynômes homogènes de $\mathbb{K}[X, Y, Z]$ de même degré d. L'application Φ de C_1 dans C_2 qui à $(X, Y, Z) \in C_1(\overline{\mathbb{K}})$ fait correspondre*

$$\Phi(X, Y, Z) = (P(X, Y, Z), Q(X, Y, Z), R(X, Y, Z)$$

est dite application rationnelle (morphisme) si elle est definie et à valeur dans $C_2(\overline{\mathbb{K}})$, sauf peut être en un nombre fini de points. En affine Φ s'écrit

$$\phi(x, y) = \left(\frac{P(x, y, 1)}{R(x, y, 1}, \frac{Q(x, y, 1)}{R(x, y, 1}\right).$$

Définition 3.1.2 *Soient C_1, C_2 deux courbes de $P_2(\mathbb{K})$. L'application rationnelle Φ de C_1 dans C_2 est dite birationnelle s'il existe une application rationnelle Ψ de C_2 dans C_1 de sorte que en tout point, sauf peut-être en un nombre fini de points, les applications composées $\Phi \circ \Psi$ et $\Psi \circ \Phi$ sont les identitées coorespondantes. Dans ce cas, on dit que C_1 et C_2 sont birationnellement équivalentes.*

Proposition 3.1.1 *Considérons sur le corps $\mathbb{K}$ de caractéristique différente de 2, la courbe C d'équation*

$$y^2 = f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4,$$

avec f_4 est un carré dans $\mathbb{K}$. Alors, la courbe C est birationnellement équivalante à la courbe donnée par la forme de Weierstrass

$$Y^2 + 2g_1XY + 2h_1Y = X^3 - 4g_0X^2 - 4h_0X.$$

Preuve. *Sans perdre de généralité, on peut supposer que $f_4 = 1$, si non on divise par f_4. Posons*

$$y^2 = G(x)^2 + H(x),\ G(x) = x^2 + g_1x + g_0,\ H(x) = h_1x + h_0.$$

Par devloppement et identification dans

$$(x^2 + g_1x + g_0)^2 + h_1x + h_0 = f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4,$$

on obtient les valeurs de g_1, g_0, h_1, h_0.
On a,

$$(Y - G)(Y + G(x)) = H(x),$$

posons $T = Y + G$, *ainsi* $Y - G = \frac{H}{T}$ *et donc*

$$2G = T - \frac{H}{T} \tag{3.1}$$

multiplions (3.1) *par* T^2 *et posaons* $S = Tx$, *on obtient ainsi*

$$2S^2 + 2g_1TS + h_1S = T^3 + 2g_0T^2 - h_0T$$

multiplions (3.1)*par* 2^3 *et posons* $X = 2T$, $Y = 4S$, *nous obtenons la forme de Weierstrass*

$$Y^2 + 2g_1XY + 2h_1Y = X^3 - 4g_0X^2 - 4h_0X.$$

Les changements de variables sont

$$X = 2(y + x^2 + g_1x + g_0),\ Y = 4x(y + x^2 + g_1x + g_0.$$

(Donner l'écriture projective de ces changements). ■

Exercice 3.1.1 *Donner une forme de Weierstrass de la courbe (de Jacobi) sur* $\mathbb{Q}$ *d'équation*

$$y^2 = x^4 + 3x^2 + 1.$$

Preuve. *Une forme de Weierstrass est donnée par*

$$Y^2 + 2g_1XY + 2h_1Y = X^3 - 4g_0X^2 - 4h_0X,\ g_1 = 0,\ g_0 = \frac{3}{2},\ h_1 = 0,\ h_0 = -\frac{5}{4}$$

ce qui donne

$$Y^2 = X^3 - 6X^2 + 5X.$$

Les changemnts sont donnés par

$$X = 2y + 2x^2 + 3,\ Y = 4xy + 4x^3 + 6x.$$

■

Exercice 3.1.2 *Écrire les courbes suivantes sous la forme de Weierstrass des courbes suivants : La famille des courbes de Nekovâr :*

$$C_a :\ (3a + 1)y^2 = x^3 - (3a^2 + 1)x + 2a^3 + a + 1,\ a \in \mathbb{Q} - \left\{-\frac{1}{3}\right\}.$$

La famille des courbes de Huff :

$$H_{a,b} : ax(y^2 - 1) = by(x^2 - 1),\ a,\ b \in \mathbb{Q},\ a^2 \neq b^2.$$

3.2 Isogénie et isomorphisme de courbes elliptiques

Définition 3.2.1 *Soient (E_1, O_1), (E_2, O_2) deux courbes elliptiques définies sur $\mathbb{K}$. Une isogénie (homomorphisme de courbes elliptiques) sur $\mathbb{K}$ ($\overline{\mathbb{K}}$) de E_1 dans E_2 est une application rationnelle Φ non identiquement nulle telle que $\Phi(O_1) = O_2$.*

Théorème 3.2.1 *Tout isomorphisme (isogénie bijective), sur $\mathbb{K}$ ($\overline{\mathbb{K}}$), entre deux courbes elliptiques E_1 et E_2 données par leurs formes de Weierstrass prend la forme*

$$(x_2, y_2) = (u^2x_1 + r, u^3y_1 + u^2sx_1 + t),\ u(\neq 0),\ r,\ s,\ t \in \mathbb{K}(\overline{\mathbb{K}}).$$

En coordonnées homogènes, on écrit

$$(X_2, Y_2, Z_2) = (u^2X_1 + rZ_1, u^3Y_1 + u^2sX_1 + tZ_1).$$

Exercice 3.2.1 *Considérons sur $\mathbb{Q}$ les courbes elliptiques (E_1, O_1), (E_2, O_2) d'équations*

$$E_1 : y_1^2 = x_1^3 - x_1,\ E_2 : y_2^2 + 2y_2 = x_2^3 - x_2 - 1.$$

Montrer que les deux courbes sont isiomorphe.

Preuve. *On a,*

$$y_2^2 + 2y_2 = x_2^3 - x_2 - 1 \Leftrightarrow y_2^2 + 2y_2 + 1 = x_2^3 - x_2 \Leftrightarrow (y_2 + 1)^2 = x_2^3 - x_2.$$

Posons

$$x_1 = x_2,\ y_1 = y_2 + 1$$

on obient

$$y_1^2 = x_1^3 - x_1$$

qui est l'équation de la courbe E_1. Donc les deux courbes se ramènent l'une à l'autre par le changement de variables admissible (et inversible)

$$(x_1 = x_2,\ y_1 = y_2 + 1),\ (x_2 = x_1,\ y_2 = y_1 - 1).$$

En projectif le changemet de variable admissible s'écrit

$$\Phi : E_2 \to E_1 : \Phi(X_2, Y_2, Z_2) = (X_1, Y_1, Z_1) = (X_2, Y_2 + 1, Z_2).$$

On a $\Phi(O_2) = O_1$. *Ainsi, les courbes* E_1, E_2 *sont isomorphes* ■

Théorème 3.2.2 *Soit* $\mathbb{K}$ *un coprs de caractéristique (Car* $(K) = p$*). Deux courbes elliptiques* E_1, E_2 *sur* $\mathbb{K}$ *données par leurs équations de Weierstrass sont isomorphes sur* $\mathbb{K}$ $(\overline{\mathbb{K}})$ *si et seulement si elles ont le même* $j-$*invariant.*

Preuve. *On se restient au cas* $p \neq 2, 3$.

1. *Supposons que* E_1 *est isomorphe à* E_2, *donc il éxiste un changement de coordonnées admissible sur* $\mathbb{K}(\overline{\mathbb{K}})$, *ainsi on obtient* $j_1 = j_2$ *car* j *est invariant par les changement de variables admissibles.*
2. *Supposons que* $j_1 = j_2$ *et montrons que* E_1 *et* E_2 *sont isomorphes sur* $\mathbb{K}$ $(\overline{\mathbb{K}})$. *Supposons que les équations de Weierstrass des deux courbes* E_1 *et* E_2 *sont*

$$E_1 \ : \ y^2 = x^3 + ax + b, \ j_1 = -1728\frac{(4a)^3}{\triangle},$$
$$E_2 \ : \ y^2 = x^3 + Ax + B, \ j_2 = -1728\frac{(4A)^3}{\triangle'}.$$

En utilisant le fait que $j_1 = j_2$, *on obtient*

$$a^3B^2 = b^2A^3.$$

Cherchons un changement de variables admissible de la forme

$$(x, y) \leftarrow \left(u^2x, u^3y\right)$$

— *Supposons que* $a = 0$, *comme* $\Delta \neq 0$, *il résulte que* $b \neq 0$ *et donc* $A = 0$, $B \neq 0$. *Ainsi, il suffit de prendre*

$$u = \left(\frac{b}{B}\right)^{\frac{1}{6}} \in \overline{K}.$$

Si $u \in \mathbb{K}$, *alors l'isomorphisme sera sur* $\mathbb{K}$.

— *Supposons que* $b = 0$, *comme* $\Delta \neq 0$, *il résulte que* $a \neq 0$ *et donc* $B = 0$, $A \neq 0$. *Dans ce cas on peut prendre*

$$u = \left(\frac{a}{A}\right)^{\frac{1}{4}} \in \overline{K}.$$

Si $u \in \mathbb{K}$, alors l'isomorphisme sera sur $\mathbb{K}$.

— *Supposons que $a.b \neq 0$, alors $A.B \neq 0$. Ainsi, il suffit de prendre*

$$u = \left(\frac{a}{A}\right)^{\frac{1}{4}} = \left(\frac{b}{B}\right)^{\frac{1}{6}} \in \overline{K}.$$

Si $u \in \mathbb{K}$, alors l'isomorphisme sera sur $\mathbb{K}$.

■

CHAPITRE 4

GROUPE DE MORDELL-WEIL ET CARACTÉRISATION DU GROUPE DE TORSION

4.1 Théorème de Mordell-Weill

Soit E une courbe elliptique définie par

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{K}.$$

L'ensemble des points $\mathbb{K}$-rationnels, $E(\mathbb{K})$ muni de la loi définie sur E est un groupe abélien (sous groupe de E).

Définition 4.1.1 *Un point P de $E(\mathbb{K})$ est dit d'ordre fini $m \in \mathbb{N}^*$ si*

$$mP = \underbrace{P + P + ... + P}_{m\ fois} = \mathcal{O} \text{ et } nP \neq \mathcal{O} \text{ dèsque } n < m.$$

Si un tel m n'existe pas le point P est dit point d'ordre infini.

Théorème 4.1.1 *Pour tout entier m fini, les points d'ordre m forme un sous-groupe abélien de $E(\mathbb{K})$ noté $E(\mathbb{K})[m]$.*

Définition 4.1.2 *On définit l'ensemble de tous les points d'ordre fini de $E(\mathbb{K})$, et on le note $E_{tors}(\mathbb{K})$ par*

$$E_{tors}(\mathbb{K}) := \{P \in E(\mathbb{K})\},\ \exists m \in \mathbb{N}^* : mP = \mathcal{O}.$$

Théorème 4.1.2 *$E_{tors}(\mathbb{K})$ est un sous groupe abélien de $E(\mathbb{K})$.*

Théorème 4.1.3 *(**Mordell-Weil**) Le groupe abélien $E(\mathbb{K})$, $\mathbb{K}$ est un corps des nombres, est de type fini, c'est-à-dire, $\exists P_1, ..., P_n \in E(\mathbb{K})$ tel que tout point Q de $E(\mathbb{K})$, s'écrit*

$$Q = m_1P_1 + ... + m_nP_n,\ m_i \in \mathbb{Z},\ i = \overline{1, n},$$

i.e.,

$$E(\mathbb{K}) = \langle P_1, ..., P_n \rangle_{\mathbb{Z}},$$

de plus

$$E(K) \simeq E(K)_{tors} \oplus \mathbb{Z}^r,$$

r est un entier positif.

Remarque 4.1.4 *1. L'entier r est appelé le rang de la courbe elliptique E, qui est le nombre de copies de $\mathbb{Z}$ c'est donc le nombre de points d'ordre infini indépendant.*

2. *Ce théorème à été démontré en premier lieu par Mordell en 1922 dans le cas où* $\mathbb{K} = \mathbb{Q}$, *puis généralisé par Weil en 1928, dans sa thèse, pour* $\mathbb{K}$ *corps des nombres. Le groupe* $E(\mathbb{K})$ *est appelé, groupe de Mordell-Weil, comme honneur pour ces deux mathématiciens.*
3. *Lorsque* $r = 0$, *alors* $E(\mathbb{K}) = E_{tors}(\mathbb{K})$.

4.2 Le groupe de Torsion

Le théorème suivant permet de décrire $E(\mathbb{Q})_{tors}$.

Théorème 4.2.1 *(**Nagell-Lutz**) Soit* $P = (x(P), y(P))$ *un point de torsion d'une courbe elliptique E définie sur* $\mathbb{Q}$ *d'équation de Weierstrass simplifiée*

$$y^2 = x^3 + Ax + B,\ A,\ B \in \mathbb{Z}$$

Supposons que $P \neq O$.

1. $x(P), y(P) \in \mathbb{Z}$.
2. *Si P est d'ordre 2, alors*

$$y(P) = 0,\ x(P)^3 + Ax(P) + B = 0.$$

3. *Si P est d'ordre* ≥ 3, *alors :*

$$y(P)^2 \text{ divise } \left(4A^3 + 27B^2\right).$$

Exercice 4.2.1 *Considérons la courbe elliptique sur* $\mathbb{Q}$ *d'équation*

$$E_1 : y^2 = x^3 - 2$$

Montrer que $E(\mathbb{Q})_{tors} = O$.

Preuve. *Si* $(x_0, 0)$ *est un point d'ordre deux, alors* $x_0^3 - 2 = 0$. *Cette n'admet pas de racines rationnelles, donc on a pas de points points d'ordre 2.*
supposons que $P = (x(P), y(P))$ *est un point de torsion P d'ordre* ≥ 3. *Alors* $y(P)$ *sera un entier et* $y(P)^2$ *divise* $4A^3 + 27B^2 = 4 \times 27$, *ainsi*

$$y(P) = \pm 1,\ \pm 2,\ \pm 3 \text{ ou } \pm 6.$$

En portant dans l'équation de la courbe, x_P doit être racine de l'une des équations

$$x(P)^3 = 3,\ 6,\ 11,\ 38.$$

Aucune de ces équations n'a de racines entiers. On déduit que $E(\mathbb{Q})_{tors}$ est le groupe trivial, i.e.,

$$E(\mathbb{Q})_{tors} = \{O\}.$$

■

Exercice 4.2.2 *Considérons la courbe elliptique E d'éfinie sur $\mathbb{Q}$ par*

$$E_2 : y^2 = x^3 - 43x + 166.$$

Déterminer $E(\mathbb{Q})_{tors}$.

Preuve. *L'équation*

$$x^3 - 43x + 166 = 0$$

n'a pas de racines rationnlles, donc $E(\mathbb{Q})$ ne contient aucun points d'ordre 2. On a

$$4A^3 + 27B^2 = 2^{15}.13.$$

Alors, si $P = (x(P), y(P))$ est un point de torsion d'ordre ≥ 3, on aura

$$y(P) \in \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 8,\ \pm 16,\ \pm 32,\ \pm 64,\ \pm 128\}.$$

En dans l'équation de E, nous obtenons

$$x_P = 3,\ y_P = \pm 8,\ x_P = -5,\ y_P \pm 16,\ x_P = 11,\ y_P = \pm 32.$$

Ainsi

$$E(\mathbb{Q})_{tors} = \{O,\ (3,-8),\ (3,8),\ (-5,-16),\ (-5,16),\ (11,-32),\ (11,32)\}.$$

■

Le théorème suivant décrit la structure possible de $E(\mathbb{Q})_{tors}$.

Théorème 4.2.2 (Mazur, Conjecture de Ogg) *Soit E une courbe elliptique sur $\mathbb{Q}$. Alors : $E(\mathbb{Q})_{tors}$ est isomorphe à l'un des groupes suivants*

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z}, && 1 \leq n \leq 10,\ n = 12 \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, && 1 \leq m \leq 4. \end{aligned}$$

Remarque 4.2.3 *Il résulte du du théorème de* ***Mazur*** *que si un point d'une courbe elliptique à un d'ordre* ≥ 13*, alors ce point sera d'ordre infini.*

Exercice 4.2.3 *Considérons sur* $\mathbb{Q}$ *la courbe elliptique d'équation*

$$y^2 = x^3 - 4x.$$

Déterminer $E(\mathbb{Q})_{tors}$ *et déduire que* $E(\mathbb{Q})_{tors}$ *est isomorphe à*

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Preuve. *Il n'est pas difficile de voir que*

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0), (2,0), (-2,0)\}.$$

Posons

$$P = (0,0),\ Q = (2,0),\ R = (-2,0).$$

On a

$$-P = (0,0) = P,\ -Q = (2,0) = Q,\ -R = (-2,0) = R,$$

c'est-à dire

$$2P = 2Q = 2R = \mathcal{O}.$$

De plus $P + Q = R$*, donc*

$$E(\mathbb{Q})_{tors} = \langle P \rangle \oplus \langle Q \rangle$$

qui est isomorphe à

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

■

Exercice 4.2.4 *Soit* $E(\mathbb{Q})$ *la courbe elliptique d'équation*

$$y^2 - xy + 2y = (x-1)^3$$

avec son point $P = (1,0)$*. Quel est l'ordre de* P*?.*

Preuve. *On a*

$$2P = (1,-1),\ -P = (1,-1).$$

Il r'ésulte que

$$2P = -P \Leftrightarrow 3P = \mathcal{O}.$$

Donc P est d'ordre 3. ■

BIBLIOGRAPHIE

[1] *A. A. Ciss, D. Sow, On a new generalisation of Huff, 2011. https ://eprint.iacr.org/2011/580.pdf.*

[2] *S. Allalouche, H. Zatout, Quelques modéles de courbes elliptiques, Mémoire de Master, Université de Jijel, 2013.*

[3] *L. R., Alvaro, Elliptic curves, Modular Forms and their L-functions, Student Mathematical Library Volume : 58 ; 2011.*

[4] *L. Benferhat, Variations sur la mesure de Mahler de polynômes de deux variables. Thèse de doctorat, USTHB Alger, 2011.*

[5] *M. J. Bertin, O. Lecacheux, Courbes elliptiques, Cours de D.E.A, Université Paris 06, (1997).*

[6] *J. W. S. Cassels, Lectures on elliptic curves,London Mathematical Society Student Texts, vol. 24. Cambridge University Press, Cambridge, 1991.*

[7] *J. Devigne, M. Joye, Binary Huff Curves. In : Kiayias A. Eds., Topics in Cryptology CT-RSA 2011. Lecture Notes in Computer Science, vol. 6558. Springer, Berlin, Heidelberg, 2011.*

[8] *, R. Kenane, Quelques éléments de l'arithmétique des courbes elliptiques. Mémoire de Magistère, Université de Jijel, 2013.*

[9] *M. Joye, Introduction élémentaire à la théorie des courbes elliptiques, 1995. https ://www.yumpu.com/fr/document/view/43533787/introduction-elementaire-a-la-theorie-des-courbes-elliptiques.*

[10] *J. Launay, Points rationnels sur les courbes elliptiques, 2011. http ://www.fichier.pdf.fr/2011/07/30/ter/ter.pdf.*

[11] J. S. Mile, Elliptic Curves, Kea Books 2006.

[12] , K. Rolshausen, Éléments explicites dans le K_2 d'une courbe elliptique, Université Louis Pasteur, Strasbourg, 1996.

[13] J. H. Silverman, The Arithmetic of Elliptic Curves, Second Edition. Graduate Texts in Mathematics 106. Springer, 2009.

[14] N. Touafek, Feuilles de cours théorie des nombres 1 et 2. Université de Jijel.

[15] , N. Touafek, Mesure de Mahler et régulateur elliptique : quelques nouvelles relations exotique. Thése de doctorat, Université de Constantine, 2008.

[16] B. Winckier, Les courbes elliptiques ; théorème de Mordell-Weil, 2009. http ://www.mathem.all.fr/bw/Memoire. BrunoWinckler.pdf.