Cours fondamental de M2
Introduction à l'arithmétique des courbes elliptiques

Jean-François Dat

2018-2019

Table des matières

1 Introduction

Les courbes elliptiques sont a priori parmi les objets les plus "simples" de la géométrie algébrique. En effet, une définition possible de courbe elliptique $\mathcal{E}$ sur un corps K (disons algébriquement clos pour commencer) est *une courbe projective plane cubique non-singulière.* Si l'on considère que la géométrie algébrique est l'étude des solutions de systèmes d'équations polynômiales à plusieurs variables, on est ici dans le cas d'1 équation de degré 3 en 2 variables, soit le premier cas à considérer au-delà des droites et des coniques. Dans ce langage, on a donc

$$\mathcal{E}(K) = \big\{[x:y:z] \in \mathbb{P}^2(K),\ f(x,y,z) = 0\big\}$$

où $f(X,Y,Z) \in K[X,Y,Z]_3$ est un polynôme homogène de degré 3 irréductible dans l'anneau factoriel $K[X,Y,Z]$. La condition de non-singularité en un point $P = (x,y,z)$ de $\mathcal{E}$ s'écrit selon le critère Jacobien habituel : $(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P), \frac{\partial f}{\partial Z}(P)) \neq (0,0,0)$ et, dans ce cas, la droite de $\mathbb{P}^2$ d'équation

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

est la tangente à $\mathcal{E}$ en P (c'est-à-dire que dans chacune des cartes affines définies par $Z \neq 0$, $Y \neq 0$ et $X \neq 0$ contenant P, la droite est bien la tangente au sens habituel de la géométrie affine. Exercice : le vérifier).

L'inconvénient de ce langage est qu'a priori, plusieurs équations définissent des objets isomorphes au sens de la géométrie algébrique. On peut par exemple faire des changements linéaires de coordonnées (ie faire agir $\mathrm{PGL}_3(K)$ sur $\mathbb{P}^2(K)$), afin de simplifier l'expression de $f(X,Y,Z)$. Voici un exemple.

Proposition. – *Il existe un changement linéaire de coordonnées tel que f prend la forme suivante, dite "forme normale" ou "forme de Weierstrass généralisée"*

$$f(X,Y,Z) = Y^2Z + a_1YXZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^4)$$

Si de plus, $\mathrm{car}(K) \neq 2,3$*, alors on peut même mettre $f = 0$ sous "forme de Weierstrass"*

$$ZY^2 = X^3 + aZ^2X + bZ^3.$$

Démonstration. Passer de la forme normale à la forme courte en caractéristique différente de 2 et 3 est facile ; on pose $Y' = Y + \frac{a_1}{2}X + \frac{a_3}{2}Z$ pour éliminer a_1 et a_3, puis on pose $X' = (X + \frac{a_2}{3}Z)$ pour éliminer a_2.

Avant de continuer, on remarque que lorsque f est sous forme normale, alors le point $O = [0:1:0]$ est le seul point d'intersection de $\mathcal{E}$ avec la droite à l'infini $Z = 0$, qui est donc tangente à $\mathcal{E}$ en O, et la Hessienne $H_f = \det(\frac{\partial^2 f}{\partial X_i X_j})$ de f s'annule en O (autrement dit O est un point d'inflexion : le contact entre la tangente et la courbe est de multiplicité > 2).

Réciproquement, si O annule f alors le coefficients de Y^3 dans le développement de f doit être nul. Si de plus la tangente en O est la droite à l'infini $Z = 0$, alors le coefficient de XY^2 doit être nul. Dans ce cas $H_f(O)$ est 8 fois le coefficient de XY^2 donc celui-ci est nul si $H_f(O) = 0$, au moins en caractéristique $\neq 2$. Mais alors le coefficient de X^3 ne peut être nul car Z ne divise pas f. Après rescaling, on peut le rendre égal à 1 et on voit que f est sous forme normale.

Revenant au cas général, il suffit donc de trouver un point d'inflexion de $\mathcal{E}$, et de l'envoyer par un changement de coordonnées sur O de manière à ce que la tangente soit $Z = 0$. L'ensemble des points d'inflexion est l'intersection de $\mathcal{E}$ et du lieu d'annulation de la Hessienne, qui est aussi une cubique. Cet ensemble est non-vide (le théorème de Bezout nous dit même qu'en comptant les multiplicités, il y a 9 points d'intersection). □

Remarque. – La preuve donnée fournit l'existence d'une forme normale pour K algébriquement clos de caractéristique $\neq 2$. Le résultat est valable en fait pour K parfait, pourvu que $\mathcal{E}(K)$ soit non vide. On en donnera une preuve à partir de la "bonne" définition de courbe elliptique (cf ci-dessous).

Remarque. (Points singuliers) – Si f est un polynôme cubique sous forme de Weierstrass, alors le lieu d'annulation de f dans $\mathbb{P}^2$ est la réunion de $\{O = [0 : 1 : 0]\}$ et du lieu d'annulation dans $\mathbb{A}^2$ de l'équation affine

$$y^2 = x^3 + ax + b.$$

Les seuls points singuliers possibles sont dans $\mathbb{A}^2$ et de la forme $(0, x_0)$ où x_0 est une racine multiple de $X^3 + aX + B$. Ainsi la condition de non-singularité de $\mathcal{E}$ équivaut à la non nullité du discriminant $\Delta = -(4a^3 + 27b^2)$ de ce polynôme. De plus, si celui-ci est nul, on voit qu'il y a exactement 1 point singulier dans la courbe $f = 0$ et qu'il est à coordonnées dans K (même si K n'est pas algébriquement clos). Un changement de variable $x' = x - x_0$ met alors l'équation sous la forme $y^2 = x^2(x - x_1)$ sur K. Sur $\bar{K}$ on peut par changement de variables se ramener à l'une des deux équations $y^2 = x^3$ (cusp) ou $y^2 = x^2(x - 1)$ (point double).

Remarque. (changements de coordonnées) – Le sous-groupe de $\mathrm{PGL}_3(K)$ qui stabilise O et la droite à l'infini $Z = 0$ est un groupe de matrices triangulaires (supérieures si on ordonne la base Y, X, Z). Il agit par automorphismes affines sur le plan affine $Z \neq 0$. En tenant compte que les coefficients de x^3 et y^2 doivent être égaux à 1, on voit que les seuls tels automorphismes qui préservent la propriété d'être sous forme normale sont donnés par $(x, y) \mapsto (u^2x' + r, u^3y' + u^2sx' + t)$. De même les seuls changements de coordonnées affines préservant la propriété d'être sous forme de Weierstrass sont de la forme $x = u^2x'$, $y = u^3y'$. Nous verrons plus tard que si f et f' sous forme normale définissent des courbes elliptiques "isomorphes" (à définir plus loin), alors f' se déduit de f par un changement de coordonnées comme ci-dessus.

Remarque. (Invariant j) – Supposons $\mathrm{car}(K) \neq 2, 3$ et f sous forme de Weierstrass $y^2 = x^3 + Ax + B$. On définit $j = 12^3 \frac{4A^3}{4A^3 + 27B^2}$. On vérifie facilement qu'il est invariant

par changement de coordonnées préservant la forme de Weierstrass. De plus, si $f' = x^3 + A'x + B'$ est une autre forme de Weierstrass avec $j' = j$, alors $A^3 B'^2 = A'^3 B^2$ et, si K est algébriquement clos, on peut trouver un changement de coordonnées transformant f an f' (prendre $u = (B/B')^{1/6}$ si $B' \neq 0$ et $u = (A/A')^{1/4}$ sinon).

Nous verrons bientôt comment utiliser le langage intrinsèque de la géométrie algébrique moderne pour nous affranchir de la présentation de $\mathcal{E}$ comme courbe plane et nous définirons plutôt une courbe elliptique comme une *courbe complète lisse géométriquement connexe de genre 1 et munie d'un K-point.* Nous reprouverons notamment l'existence des formes normales à l'aide du théorème de Riemann-Roch.

1.1 Courbes elliptiques sur $\mathbb{C}$

Lorsque $K = \mathbb{C}$, on sait associer une surface de Riemann à toute courbe algébrique lisse, et cette opération conserve le genre. En particulier, la surface de Riemann associée à une courbe elliptique $\mathcal{E}$ est de genre 1 donc de la forme $\mathbb{C}/\Lambda$ avec $\Lambda = \Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$ un réseau de $\mathbb{C}$. Ici τ est dans le demi-plan supérieur $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$.

Réciproquement, si $\tau \in \mathbb{H}$, la surface de Riemann $\mathbb{C}/\Lambda_\tau$ est algébrisable en une courbe elliptique. Une manière concrète de le voir est d'utiliser les *fonctions de Weierstrass.* La série en $x \in \mathbb{C}$

$$\wp'_\tau(x) = -2 \sum_{\omega \in \Lambda_\tau} \frac{1}{(x-\omega)^3}.$$

converge normalement sur tout domaine fondamental pour Λ_τ, une fois qu'on enlève le nombre fini de termes qui y ont un pôle. Cette fonction est donc Λ_τ-périodique, holomorphe en dehors de Λ_τ et possède des pôles d'ordre 3 en chaque $\omega \in \Lambda$. Elle admet une primitive de la forme

$$\wp_\tau(x) = \frac{1}{x^2} + \sum_{\omega \in \Lambda_\tau \setminus \{0\}} \left(\frac{1}{(x-\omega)^2} - \frac{1}{\omega^2} \right)$$

elle aussi Λ_τ-périodique et méromorphe, mais avec des pôles d'ordre 2 en $\omega \in \Lambda_\tau$. Ainsi $\wp_\tau$ et $\wp'_\tau$ descendent en des fonctions méromorphes sur $\mathbb{C}/\Lambda_\tau$ ayant un pôle d'ordre 2 et 3 en 0. En raisonnant sur les pôles possibles d'une fonction méromorphe générale sur $\mathbb{C}/\Lambda_\tau$, on peut montrer que le corps des fonctions méromorphes sur $\mathbb{C}/\Lambda_\tau$ est $\mathcal{M}_{\mathbb{C}/\Lambda_\tau} = \mathbb{C}(\wp_\tau, \wp'_\tau)$. À l'aide du développement limité de $\wp$ au voisinage de 0 (qui est de la forme $\wp(z) = \frac{1}{z^2} + \frac{g_2}{20} z^2 + \frac{g_3}{70} z^4 + O(z^5)$), on montre que la fonction méromorphe

$$\wp'^2_\tau - 4\wp^3_\tau + g_2(\tau)\wp_\tau + g_3(\tau)$$

est holomorphe, donc constante, puis nulle. Ici g_2 et g_3 sont les *séries d'Eisenstein*

$$g_2(\tau) := 60 \sum_{\omega \in \Lambda_\tau \setminus \{0\}} \frac{1}{\omega^4} \text{ et } g_3(\tau) := 140 \sum_{\omega \in \Lambda_\tau \setminus \{0\}} \frac{1}{\omega^6}.$$

Ceci montre que l'application

$$\mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{P}^2(\mathbb{C}),\ x \neq 0 \mapsto [\wp(x) : \wp'(x) : 1],\ 0 \mapsto [0:1:0]$$

est un isomorphisme de $\mathbb{C}/\Lambda_\tau$ sur la surface de Riemann associée à la courbe elliptique d'équation $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$.

On sait (ou on vérifie) que deux surfaces de Riemann $\mathbb{C}/\Lambda_\tau$ et $\mathbb{C}/\Lambda_{\tau'}$ sont biholomorphes si et seulement si τ' est de la forme $\frac{a\tau+b}{c\tau+d}$, i.e. dans l'orbite de τ pour l'action de $\mathrm{SL}_2(\mathbb{Z})$ par homographies sur $\mathbb{H}$. Par ailleurs, l'*invariant modulaire* $j(\tau) := \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}$ introduit plus haut est ici une fonction holomorphe en $\tau \in \mathbb{H}$ et invariante sous $\mathrm{SL}_2(\mathbb{Z})$. On peut munir le quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ d'une structure naturelle de surface de Riemann (quotient par une action proprement discontinue d'un groupe discret) et montrer que j induit un biholomorphisme $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \xrightarrow{\sim} \mathbb{C}$. Les courbes elliptiques sur $\mathbb{C}$ sont donc paramétrées par leur invariant modulaire, lequel peut prendre n'importe quelle valeur complexe.

Lorsque $g_2(\tau)g_3(\tau) \neq 0$, ce qui équivaut à $j(\tau) \neq 0, 1728$, un changement de variable $(x, y) = ((g_3/g_2)x', (g_3/g_2)^{3/2}y'))$ permet de donner l'équation $E_j : y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}$ pour "la" courbe associée à l'invariant j. Sinon, "la" courbe d'équation $y^2 = x^3 + 1$ a pour invariant $j = 0$ et celle d'équation $y^2 = x^3 + 1$ a pour invariant $j = 1728$

Si K est un sous-corps de $\mathbb{C}$, on dit qu'une courbe elliptique complexe est "définie sur K" si elle peut être définie par une équation cubique plane à coefficients dans K. Si on met cette équation sous la forme de Weierstrass $y^2 = x^3 + Ax + B$, alors son invariant $j = \frac{1728 \cdot 4A^3}{4A^3 + 27B^2}$ est manifestement dans K et, réciproquement, si j est dans K alors E_j définit une courbe elliptique sur K d'invariant j. Néanmoins, il y a en général plusieurs classes d'isomorphisme de courbes elliptiques sur K ayant le même invariant j.

1.2 Loi de groupe

La surface de Riemann associée à une courbe elliptique complexe est visiblement munie d'une structure de groupe dont la multiplication et l'inverse sont holomorphes. De manière remarquable, cette loi est en fait algébrique et définie sur le corps de définition $\mathbb{Q}(j)$ de la courbe. Pour tout corps $K \subset \mathbb{C}$ contenant j, l'ensemble des points rationnels $E_j(K)$ (solution de E_j à valeurs dans K) est donc un sous-groupe de $E_j(\mathbb{C})$.

Plus généralement, sur un corps parfait de caractéristique quelconque, les points rationnels $\mathcal{E}(K)$ sont munis d'une loi de groupe. Lorsqu'on voit $\mathcal{E}$ comme une "courbe de genre 1 munie d'un point rationnel", on se servira du théorème de Riemann-Roch pour définir cette loi, et du point rationnel comme élément neutre.

Lorsqu'on voit $\mathcal{E}$ comme une cubique plane, il y a un procédé géométrique pour construire cette loi. Le point clef est que l'intersection de $\mathcal{E}(\bar{K})$ avec toute droite de $\mathbb{P}^2$ consiste en 3 points (comptés avec multiplicité) P, Q, R. En effet, si $aX + bY + cZ = 0$ est l'équation de la droite et $c \neq 0$ (par exemple) alors $[X : Y]$ sont des coordonnées projectives sur cette droite (ie $[x : y : z] \mapsto [x : y]$ est un isomorphisme de la droite sur $\mathbb{P}^1$) dans lesquelles l'intersection est le lieu d'annulation du polynôme $f(X, Y, -\frac{a}{c}X - \frac{b}{c}Y)$, qui est homogène de degré 3 et *non nul* (sinon l'équation de la droite diviserait f). Remarquons que si P, Q sont deux points K-rationnels alors R aussi. En effet, la droite (PQ) et la courbe étant définies sur K, leur intersection l'est aussi et est stable sous $\mathrm{Gal}(\bar{K}/K)$. Si P et Q sont fixes par Galois, alors R l'est aussi donc est rationnel.

Donnons-nous maintenant un point rationnel O de $\mathcal{E}$ (qu'on suppose exister par définition d'une courbe elliptique). Notons $P \cdot Q$ le troisième point d'intersection de la droite (PQ) avec $\mathcal{E}$ (qui peut éventuellement être P ou Q) et posons $P \oplus Q := O \cdot (P \cdot Q)$. La commutativité de cette opération et le fait que O est élément neutre sont clairs. De plus le point $P \cdot (O \cdot O)$ est inverse de P. Mais l'associativité n'est pas facile à voir dans ce langage. Lorsque f est sous forme de Weierstrass $y^2 = x^3 + Ax + B$ on peut expliciter les coordonnées de $P \oplus Q$ (cf Silverman III....) en fonction de celles de P et Q et vérifier laborieusement l'associativité. Notons que le passage à l'inverse est simplement $P = [x : y : z] \mapsto -P = [x : -y : z]$.

Dans Hüsemoller ou Milne, on trouve une approche géométrique pour prouver l'associativité, qui repose sur le théorème suivant : si 2 cubiques de $\mathbb{P}^2$ (pas nécessairement irréductibles) s'intersectent en 9 points distincts et si une troisième cubique de $\mathbb{P}^2$ passe par 8 de ces points, alors elle passe par le 9ème ! Soient alors P, Q, R trois points de $\mathcal{E}$. On veut montrer que $(P \oplus Q) \cdot R = P \cdot (Q \oplus R)$. On considère la cubique C_1 réunion des trois droites (P, Q), $(O, Q \cdot R)$ et $(R, P \oplus Q)$ ainsi que la cubique C_2 réunion des trois droites (Q, R), $(O, P \cdot Q)$ et $(P, Q \oplus R)$. Les trois coniques C_1, C_2 et $\mathcal{E}$ passent par les 8 points suivants $O, P, Q, R, P \cdot Q, P \oplus Q, Q \cdot R, Q \oplus R$. Le point $(P \oplus Q) \cdot R$ est le 9ème point d'intersection de $\mathcal{E}$ et C_1 et le point $P \cdot (Q \oplus R)$ est le 9ème point d'intersection de $\mathcal{E}$ et C_2. Ils doivent donc être égaux. Bien-sûr tout cela ne fonctionne bien que dans une situation générique où tous les points considérés sont distincts...

1.3 Théorèmes et conjectures célèbres

Un des buts principaux de la géométrie "arithmétique" est d'étudier les ensembles de solutions sur $\mathbb{Q}$ de polynômes sur $\mathbb{Q}$. Par exemple, si C est une conique plane donnée par une équation $f \in \mathbb{Q}[X, Y, Z]$ homogène de degré 2, l'ensemble $C(\mathbb{Q})$ des points rationnels peut être vide (exemple $f = X^2 + Y^2 + Z^2$), mais s'il ne l'est pas et dès qu'on connait un point rationnel $P \in C$, alors on peut trouver tous les autres facilement. En effet, tout droite rationnelle de $\mathbb{P}^2$ passant par P recoupe C en un autre point Q, qui doit être fixe par Galois puisque l'ensemble $\{P, Q\}$ est stable sous Galois. De plus, tout point rationnel de C s'obtient évidemment ainsi. On a donc une paramétisation des points rationnels par $\mathbb{P}^1(\mathbb{Q})$ (exemple : $f = X^2 + Y^2 - Z^2$, appliquer ce principe pour trouver la paramétrisation $[u : v] \mapsto [u^2 - v^2 : 2uv : u^2 + v^2]$ des solutions rationnelles).

Dans le cas des courbes elliptiques, partant de 2 points rationnels, on peut en fabriquer un troisième, et on peut se demander de combien de points il faut disposer pour les trouver tous en itérant ce procédé. Un des résultats phares de ce cours affirme qu'il suffit d'un nombre fini :

THÉORÈME. (Mordell, 1922) – *Le groupe $\mathcal{E}(\mathbb{Q})$ d'une courbe elliptique sur $\mathbb{Q}$ est un groupe abélien de type fini.*

On peut donc décomposer $\mathcal{E}(\mathbb{Q}) = \mathcal{E}(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, où $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ est le sous-groupe (fini) de torsion et r est le *rang* de $\mathcal{E}$. Le premier est assez bien compris, même si la preuve restera hors de portée de ce cours :

THÉORÈME. (Mazur, 1977) – *Le groupe $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ est soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n \leqslant 12$ et $n \neq 11$, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ avec $m \leqslant 4$.*

Le rang r d'une courbe elliptique sur $\mathbb{Q}$ est beaucoup plus mystérieux. On ne connait pas d'algorithme pour le calculer. On pense qu'il peut être arbitrairement grand, mais la meilleure minoration connue est 28. Un théorème de Bhargava (qui lui a valu la médaille Fields) affirme que le rang "moyen" est $\leqslant 1$. Le problème ouvert le plus célèbre sur le rang r est la conjecture de Birch et Swinnerton-Dwyer qui fait intervenir la fonction L de la courbe elliptique. La définition de cette fonction fait intervenir les "réduction modulo p" de $\mathcal{E}$.

Supposons $\mathcal{E}$ donnée par une équation de Weierstrass $y^2 = x^3 + Ax + B$ avec $A, B \in \mathbb{Q}$. Par un changement de coordonnée $y' = u^3 y$ et $x' = u^2 x$, on peut se ramener à $A, B \in \mathbb{Z}$ et ce de manière "minimale", i.e. en gardant $\Delta = 4A^3 + 27B^2$ minimal. On peut alors réduire cette équation modulo p. On trouve une cubique, qui est lisse si p ne divise pas 2Δ, donc une courbe elliptique sur $\mathbb{F}_p$. Le groupe des points rationnels $\mathcal{E}(\mathbb{F}_p)$ est fini et on écrit traditionnellement son cardinal sous la forme $|\mathcal{E}(\mathbb{F}_p)| = 1 + p - a_p$. On a alors l'estimée suivante, due à Hasse :

THÉORÈME. (Hasse, 1933) – $|a_p| \leqslant 2\sqrt{p}$.

Il s'ensuit que le produit Eulérien partiel

$$\prod_{(p,2\Delta)=1} \frac{1}{1 - a_p p^{-s} + p^{-2s}},\ s \in \mathbb{C}$$

converge pour $\Re(s) > 3/2$. On complète ce produit par des facteurs $\frac{1}{1-a_p p^{-s}}$ pour les p divisant Δ, avec $a_p = 1, -1$ ou 0 selon la nature de la singularité de la courbe réduite. On obtient ainsi une fonction $L(E, s)$ a priori définie seulement sur le demi-plan $\Re(s) > 3/2$. Le théorème suivant découle des travaux de Wiles, Taylor, Breuil, Conrad et Diamond.

THÉORÈME. (1993-1998) – *La fonction $L(E, s)$ a un prolongement analytique à $\mathbb{C}$.*

On peut maintenant énoncer la conjecture étonnante de Birch et Swinnerton-Dwyer :

CONJECTURE. – *Le rang r de $\mathcal{E}$ est l'ordre d'annulation r_{an} de $L(E, s)$ en $s = 1$.*

La conjecture est supportée par de nombreux calculs effectués sur ordinateur. Le meilleur résultat général connu est dû à Kolivagin (et Gross-Zagier) et dit que la conjecture est vraie pour $\mathcal{E}$ telle que $r_{an} \leqslant 1$.

Voici un autre résultat récent remarquable, qui était resté ouvert pendant 50 ans (conjecture de Sato-Tate) et qui concerne la distribution des a_p dans l'intervalle $[-2\sqrt{p}, 2\sqrt{p}]$.

THÉORÈME. (Taylor et al., 2008) – *Si $\mathcal{E}$ n'a pas multiplication complexe et si on écrit $a_p = 2\sqrt{p}\cos(\theta_p)$ avec $\theta_p \in [0, \pi]$, alors les θ_p sont équirépartis dans l'intervalle $[0, \pi]$ pour la mesure $\frac{2}{\pi}\sin(\theta)^2 d\theta$.*

1.4 Quelques applications

Théorème de Fermat. La seule démonstration connue du grand théorème de Fermat consiste, suivant une idée originale de Hellegouarch reprise par Frey, à partir d'une éventuelle solution rationnelle non-triviale de $a^n + b^n = c^n$ et démontrer que la courbe $\mathcal{E}$ d'équation $y^2 = x(x - a^n)(x - b^n)$ ne peut pas exister. Serre et Ribet avaient démontré ('80) que la fonction $L(E, s)$ d'une telle courbe ne pouvait pas être égale à une fonction $L(f, s)$ de forme modulaire de poids 2 (cf cours sur les formes modulaires). Mais Wiles, Taylor et al ont montré (1994) que toute courbe elliptique sur $\mathbb{Q}$ est "modulaire" en ce sens.

Nombres congruents. Un entier n est dit congruent s'il est l'aire d'un triangle rectangle dont les côtés sont rationnels, i.e. s'il existe $a, b, c \in \mathbb{Q}^\times$ tels que $a^2 + b^2 = c^2$ et $n = \frac{1}{2}ab$. Déterminer quels nombres sont congruents est un problème très ancien et encore ouvert. En 1983, Tunnel a observé que n est congruent si et seulement si la courbe elliptique $\mathcal{E}_n$ d'équation $y^2 = x^3 - n^2x$ possède un point rationnel avec $y \neq 0$. En effet, il suffit alors de poser $a = \frac{x^2-n^2}{y}$, $b = \frac{2nx}{y}$ et $c = \frac{x^2+n^2}{y}$. Un point rationnel avec $y \neq 0$ ne peut pas être de torsion, donc on voit que n est congruent si et seulement si le rang r de $\mathcal{E}_n$ est > 0. Sous la conjecture de Birch et Swinnerton-Dwyer, Tunnel a ensuite donné des critères calculables pour que n soit congruent ou non.

Algorithmique. Les courbes elliptiques sur $\mathbb{Q}$ sont utilisées dans les algorithmes les plus rapides à ce jour pour la factorisation des entiers et les tests de primalité.

Cryptographie La méthode de Diffie-Hellman pour que deux parties échangent une information secrète d'un observateur extérieur utilise un groupe cyclique C muni d'un générateur P, et fonctionne d'autant mieux qu'il est difficile de trouver, pour $Q \in C$, un entier n tel que $Q = n.P$. Les groupes multiplicatifs de corps finis, $\mathbb{F}_p^\times$ avec p très grand, sont par exemple de bons candidats (les meilleurs algorithmes à ce jour pour calculer le logarithme discret dans ces groupes requièrent un temps "sous-exponentiel" en $\log p$). Mais à ce jour, les meilleurs algorithmes connus pour calculer le logarithme discret dans un groupe $\mathcal{E}(\mathbb{F}_p)$ sont en temps "exponentiel", ce qui rend ces groupes plus sûrs (et plus utilisés d'ailleurs) en cryptographie.

2 Rappels et compléments de géométrie algébrique

Le corps k sera algébriquement clos sauf mention du contraire.

2.1 Variétés

Le but est ici de fixer le langage. Les concepts sont supposés avoir été déjà rencontrés. Si ce n'est pas le cas, on pourra consulter le chapitre I du livre de Hartshorne.

Variété projective. À un idéal premier homogène $\mathfrak{p}$ de $k[X_0, \cdots, X_n]$ est associé un "espace k-annelé", i.e. un couple $(X, \mathcal{O})$ formé d'un espace topologique irréductible et d'un

faisceau d'anneaux de fonctions régulières ($U \subset X$ ouvert) $\mapsto \mathcal{O}(U) \subset \{f : U \longrightarrow k\}$. Rappelons brièvement que :

- $X = V(\mathfrak{p}) := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(k), \forall f \in \mathfrak{p} \text{ homogène }, f(x_0, \cdots, x_n) = 0\}$.
- $V(\mathfrak{p})$ est muni de la topologie de Zariski, dont les fermés sont les $V(I)$ pour I idéal homogène contenant $\mathfrak{p}$. Irréductible signifie que tout ouvert non vide est dense.
- Si U est ouvert dans X, une fonction $U \longrightarrow k$ est "régulière" si pour tout $P \in U$ elle est au voisinage de ce point de la forme $[x_0 : \cdots : x_n] \mapsto \frac{g(x_0,\cdots,x_n)}{h(x_0,\cdots,x_n)}$ avec g et h homogènes de même degré et h ne s'annulant pas en P.

Variété (quasi-projective). Un morphisme d'espaces k-annelé $(X, \mathcal{O}) \longrightarrow (X', \mathcal{O}')$ est une application continue $\varphi : X \longrightarrow X'$ telle que pour tout ouvert U' de X' et toute fonction régulière $f' : U' \longrightarrow k$, la fonction $f' \circ \varphi : f^{-1}(U) \longrightarrow k$ soit régulière. On appellera *variété quasi-projective*, ou simplement *variété*, tout espace annelé isomorphe à un ouvert d'une variété projective muni du faisceau de fonctions régulières restreint à cet ouvert. Un *morphisme de variétés* est par définition un morphisme d'espaces k-annelés. On a ainsi construit une catégorie Var_k.

Exemple. $\mathbb{A}^n$ est un ouvert de $\mathbb{P}^n$, donc une variété quasi-projective, et toute fonction régulière $f : X \longrightarrow k$ induit un morphisme de variétés $X \longrightarrow \mathbb{A}^1$.

Applications et fonctions rationnelles, dimension. Soit $(X, \mathcal{O}_X)$ une variété.

- On note $k(X)$ le quotient de l'ensemble des paires (U, f) avec U ouvert de X et $f \in \mathcal{O}(U)$ par la relation d'équivalence $(U, f) \sim (U', f') \Leftrightarrow f_{|U\cap U'} = f'_{U\cap U'}$. L'ensemble $k(X)$ est clairement une k-algèbre et, puisque X est irréductible, c'est même un corps, appelé *corps des fonctions rationnelles*.
- La dimension de X, notée $\dim(X)$, est le degré de transcendence de $k(X)$ sur k.
- Si $(Y, \mathcal{O}_Y)$ est une autre variété, une *application rationnelle* $X \dashrightarrow Y$ est une classe d'équivalence de paires (U, φ) où U est ouvert de X et $\varphi : U \longrightarrow Y$ est un morphisme de variétés. On dit qu'elle est dominante si l'image $\varphi(U)$ est dense dans Y. Dans ce cas, on obtient une inclusion $k(Y) \hookrightarrow k(X)$ en composant avec les fonctions rationnelles. Ce procédé définit une équivalence de catégories entre variétés munies des applications rationnelles dominantes et extensions de k de type fini.
- Une application *birationnelle* est une application rationnelle qui admet un "inverse", ou encore qui induit un isomorphisme d'un ouvert de X sur un ouvert de Y. Elle induit alors un isomorphisme $k(Y) \xrightarrow{\sim} k(X)$ et, inversement, tout tel isomorphisme provient d'une application birationnelle.

Sous-variétés et immersions. Soit $(X, \mathcal{O}_X)$ une variété et Y un sous-ensemble localement fermé irréductible (pour la topologie induite). Notons $\mathcal{O}(Y)$ l'ensemble des fonctions $Y \longrightarrow k$ qui sont localement restriction d'une fonction rationnelle $f \in k(X)$ et posons $\mathcal{O}_Y(V) = \mathcal{O}(V)$ pour V ouvert de Y. Alors $(Y, \mathcal{O}_Y)$ est une variété (découle des définitions et du fait qu'un fermé irréductible de $\mathbb{P}^n$ est de la forme $V(\mathfrak{p})$ pour $\mathfrak{p}$ premier homogène). Une *immersion* est un morphisme de variétés dont l'image est localement fermée et qui induit un isomorphisme sur l'image munie de sa structure de sous-variété.

Anneaux locaux, régularité.

— Pour $P \in X$, l'anneau des germes de fonctions régulières en P est noté $\mathcal{O}_P$. Il s'identifie à la sous-k-algèbre de $k(X)$ formée des fonctions rationnelles *définies en* P, i.e. qui admettent un représentant (U, f) avec $P \in U$. C'est un anneau local dont l'idéal maximal $\mathfrak{m}_P$ est formé des fonctions rationnelles nulles en P. Le corps résiduel $\mathcal{O}_P/\mathfrak{m}_P$ est k.
— La dimension de Krull de $\mathcal{O}_P$ (longueur d'une chaîne maximale d'idéaux premiers) est $\dim(X)$.
— On dit que P est un point *non-singulier* (ou *lisse* ou encore *simple*) si son anneau local est régulier, au sens où $\dim_k(\mathfrak{m}_P/\mathfrak{m}_P^2) = \dim(\mathcal{O}_P)$ (on a de manière générale l'inégalité $\geqslant$). Lorsque P est non-singulier, le k-dual $(\mathfrak{m}_P/\mathfrak{m}_P^2)^*$ est appelé *espace tangent de X en P.*

Variétés affines. Soit A une k-algèbre de type fini intègre. Notons $X = \mathrm{Max}(A)$ l'ensemble des idéaux maximaux de A. On le munit de la topologie de Zariski dont les fermés sont les $V(I) = \{\mathfrak{m} \in \mathrm{Max}(A), \mathfrak{m} \supset I\}$. Le localisé $A_\mathfrak{m}$ de A en $\mathfrak{m} \in \mathrm{Max}(A)$ est un sous-anneau du corps des fractions $\mathrm{Frac}(A)$ de A et son corps résiduel est égal à k par le Nullstellensatz. Pour chaque ouvert U, notons $\mathcal{O}(U)$ le sous-anneau $\cap_{\mathfrak{m}\in U} A_\mathfrak{m}$ de $\mathrm{Frac}(A)$. On peut voir $f \in \mathcal{O}(U)$ comme une fonction $\mathfrak{m} \in U \mapsto (f \bmod \mathfrak{m}) \in k$. On obtient ainsi un faisceau de fonctions "régulières" dont les anneaux locaux sont les $\mathcal{O}_\mathfrak{m} = A_\mathfrak{m}$. L'espace annelé $(X, \mathcal{O})$ ainsi obtenu est une variété. En effet, un choix de générateurs de la k-algèbre A fournit une présentation $A = k[X_1, \cdots, X_n]/\mathfrak{p}$ avec $\mathfrak{p}$ idéal premier, et le Nullstellensatz identifie $\mathrm{Max}(A)$ à $V(\mathfrak{p})$ et [Hartshorne I.3.2] montre que les faisceaux de fonctions se correspondent, de sorte que $\mathrm{Max}(A)$ s'identifie à la sous-variété fermée $V(\mathfrak{p})$ de $\mathbb{A}^n$.

Remarquons que $k(X) = \mathrm{Frac}(A)$, $\dim(X) = \dim(A)$ et $\mathcal{O}(X) = A$. De plus, pour toute autre variété Y, l'application $\mathrm{Hom}_{\mathrm{Var}}(Y, X) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(A, \mathcal{O}_Y(Y))$ est une bijection. En particulier la catégorie des variétés affines est anti-équivalente à celle des k-algèbres intègres de type fini.

Par ailleurs, toute variété possède un recouvrement fini par des ouverts qui sont des variétés affines, et dont les intersections sont des variétés affines aussi (on utilise le recouvrement habituel de $\mathbb{P}^n$ pour se ramener à un ouvert de $\mathbb{A}^n$, lequel est complémentaire d'un $V(f_1, \cdots, f_r)$ et donc réunion des ouverts affines $\{f_i \neq 0\}$).

Enfin, on a le critère Jacobien de lissité habituel. Si P est un point de $V(\mathfrak{p}) \subset \mathbb{A}^n$ comme ci-dessus et $f_1, \cdots, f_r$ des générateurs de $\mathfrak{p}$, alors P est non-singulier si et seulement si la matrice Jacobienne $(\frac{\partial f_i}{\partial X_j})_{i,j}$ est de rang $n - \dim(X)$ (cf [Hartshorne, I.5.1]).

2.2 Courbes

Une courbe (algébrique !) est une variété de dimension 1. Un fermé d'une courbe est un ensemble fini. En effet, on peut supposer la courbe affine, disons d'anneau de fonctions A, et il faut voir que pour tout $f \in A$ non nul, $\{\mathfrak{m} \in \mathrm{Max}(A), f \in \mathfrak{m}\}$ est fini. Cela découle du fait que la k-algèbre $A/(f)$ est de dimension 0 donc ses idéaux maximaux sont aussi minimaux parmi les idéaux premiers et ceux-ci sont en nombre fini puisque $A/(f)$ est noethérienne. En conséquence, un morphisme entre courbes est soit constant, soit dominant, auquel cas

ses fibres sont finies.

2.2.1 *Anneaux réguliers de dimension* 1. Un anneau local noethérien $(A, \mathfrak{m})$ régulier de dimension 1 est principal, $\mathfrak{m}$ étant engendré par tout élément ϖ de $\mathfrak{m} \setminus \mathfrak{m}^2$ (par le lemme de Nakayama). On a $\mathfrak{m} \setminus \mathfrak{m}^2 = A^\times \varpi$ et plus généralement $\mathfrak{m}^i \setminus \mathfrak{m}^{i+1} = A^\times \varpi^i$. Il s'ensuit que $\mathrm{Frac}(A) = A[\varpi^{-1}]$ et que l'application $v : \mathrm{Frac}(A)^\times \longrightarrow \mathbb{Z}$, $x \mapsto \max\{n \in \mathbb{N}, x \in \mathfrak{m}^n\}$ est une valuation sur $K = \mathrm{Frac}(A)$ (i.e. vérifie $v(xy) = v(x) + v(y)$ et $v(x+y) \geqslant \min\{v(x), v(y)\}$. On dit que A est un *anneau de valuation discrète.* Notons qu'on retrouve A à partir de K et v puisque $A = \{x \in K, v(x) \geqslant 0\}$ (en posant $v(0) = +\infty$). Un anneau local régulier de dimension quelconque est normal (ie intégralement clos). En dimension 1, on a la réciproque :

PROPOSITION. – *Un anneau local $(A, \mathfrak{m})$ noethérien normal de dimension 1 est régulier.*

Démonstration. On veut montrer que $\mathfrak{m}$ est principal. Pour cela, il suffit de trouver $x \in \mathrm{Frac}(A)$ tel que $x\mathfrak{m} = A$; en effet x^{-1} est alors un générateur de $\mathfrak{m}$. Pour tout idéal I de A, posons $I^{-1} := \{x \in \mathrm{Frac}(A),\ xI \subset A\}$. Si $x \in \mathfrak{m}^{-1}$, on a $x\mathfrak{m} \subseteq \mathfrak{m}$ ou $x\mathfrak{m} = A$.

Si $x\mathfrak{m} \subseteq \mathfrak{m}$ alors $x \in A$. En effet, $\mathfrak{m}$ est un A-module de type fini puisque A est noethérien, donc x est entier par Cayley-Hamilton, et $x \in A$ puisque A est normal.

Il nous suffit donc de montrer que $A \subsetneq \mathfrak{m}^{-1}$. L'ensemble des idéaux I tels que $A \subsetneq I^{-1}$ est non-vide (car il contient les idéaux principaux) donc, puisque A est noethérien, admet un élément maximal, disons $\mathfrak{a}$. Si l'on prouve que $\mathfrak{a}$ est premier, alors l'hypothèse $\dim(A) = 1$ impliquera $\mathfrak{a} = \mathfrak{m}$, et on aura gagné.

Montrons que $\mathfrak{a}$ est premier. Soient $x, y \in A$ t.q. $xy \in \mathfrak{a}$ et $x \notin \mathfrak{a}$. On doit prouver que $y \in \mathfrak{a}$. Or, on a $(x) + \mathfrak{a} \supsetneq \mathfrak{a}$ et donc, par définition de $\mathfrak{a}$, il s'ensuit $((x) + \mathfrak{a})^{-1} = A$. Soit alors $z \in \mathfrak{a}^{-1} \setminus A$. On a $zy((x) + \mathfrak{a}) \subset \mathfrak{a}\mathfrak{a}^{-1} + y\mathfrak{a}\mathfrak{a}^{-1} \subset A$ donc $zy \in ((x) + \mathfrak{a})^{-1} = A$. Il s'ensuit que $z \in ((y) + \mathfrak{a})^{-1}$ et donc que $((y) + \mathfrak{a}^{-1}) \supsetneq A$. Par définition de $\mathfrak{a}$ on a donc $(y) + \mathfrak{a} = \mathfrak{a}$ et $y \in \mathfrak{a}$. □

COROLLAIRE. – *Si C est une courbe affine d'anneau de fonctions A, alors C est lisse si et seulement si A est normal.*

Un anneau noethérien A de dimension 1 dont tous les localisés sont réguliers est appelé *anneau de Dedekind.* D'après la proposition précédente, c'est la même chose qu'un anneau noethérien normal de dimension 1. Voici une propriété très importante de ces anneaux.

PROPOSITION. – *Soient A un anneau de Dedekind, L une extension séparable finie de $K = \mathrm{Frac}(A)$, et B la clôture intégrale de A dans L. Alors B est aussi de Dedekind, et est un A-module de type fini.*

Démonstration. B est intègre et normal par construction. Montrons qu'il est de type fini comme A-module. Cela impliquera qu'il est noethérien, et aussi de dimension 1 (et donc de Dedekind) car chaque idéal premier non nul $\mathfrak{P}$ de B est maximal, puisque $B/\mathfrak{P}$ est intègre de dimension finie sur le corps $A/(\mathfrak{P} \cap A)$ (noter que $\mathfrak{P} \cap A$ est non nul, et donc maximal, puisqu'il contient le terme constant du polynôme minimal d'un élément non nul de $\mathfrak{P}$).

Soit $b_1, \cdots, b_n$ une base de L sur K contenue dans B (ça existe puisque $L = \mathrm{Frac}(B)$). Puisque L est séparable, la forme K-bilinéaire $(b, b') \mapsto \mathrm{Tr}_{L/K}(bb')$ sur L est non dégénérée. Soit alors $b_1^*, \cdots, b_n^*$ la base de L "duale" pour cette forme. Pour tout $b \in B$, on a donc $b = \sum_{i=1}^n \mathrm{Tr}_{L/K}(bb_i)b_i^*$. Puisque A est normal, on a $\mathrm{Tr}_{L/K}(B) \subset A$ et on en déduit que $B \subset \bigoplus_i Ab_i^*$. Puisque A est noethérien, B est un A-module de type fini. □

COROLLAIRE. – *Si K est une extension finie de $k(X)$, la clôture intégrale A de $k[X]$ dans K est une k-algèbre de type fini et un anneau de Dedekind.*

Démonstration. Comme dans la preuve précédente, il suffit de prouver la finitude de A comme $k[X]$-module. Si l'extension est séparable, on applique la proposition précédente. Si non, on est en caractéristique $p > 0$ et il existe une puissance q de p telle que $K^q \subset K_{sep}$ où K_{sep} est la clôture séparable de $k(X)$ dans K. Il s'ensuit que le composé $k(X)K^q$ est séparable sur $k(X)$. Considérons alors le corps composé $L = k(X^{1/q})K$ dans une clôture algébrique de $k(X)$. Comme k est parfait, le morphisme $x \mapsto x^q$ fournit un isomorphisme de l'extension $k(X^{1/q}) \subset k(X^{1/q})K$ sur l'extension $k(X) \subset k(X)K^q$, montrant que la première est séparable. Maintenant la clôture intégrale de $k[X]$ dans $k(X^{1/q})$ est $k[X^{1/q}]$ qui est visiblement un $k[X]$-module de type fini. Donc sa clôture intégrale dans L est aussi un $k[X]$-module de type fini grâce à la proposition précédente. Et finalement, la clôture intégrale dans K, étant un sous-module de celle dans L, est aussi de type fini sur $k[X]$. □

Remarque. – À l'aide du lemme de normalisation de Noether, on montre que la proposition est vraie sans hypothèse de séparabilité, si A est une k-algèbre de type fini.

Application : normalisation de courbes. Soit C une courbe affine et $A = \mathcal{O}(C)$ son algèbre de fonctions. Notons $\tilde{A}$ la clôture intégrale de A dans $k(C)$. C'est encore une k-algèbre de type fini donc elle définit une courbe $\tilde{C}$. Celle-ci est lisse puisque ses anneaux locaux sont ceux de A. De plus, l'inclusion $A \subset \tilde{A}$ induit un morphisme $\tilde{C} \longrightarrow C$ dominant. Comme $\tilde{A}$ est entière sur A, ce morphisme est même *surjectif*. On peut montrer (exercice) que c'est un isomorphisme au-dessus du lieu non-singulier de C. Le morphisme $\tilde{C} \longrightarrow C$ mérite donc le nom de "désingularisation". La désingularisation existe en dimension supérieure, mais c'est beaucoup plus compliqué...

Comme la normalisation commute à la localisation, on peut l'appliquer à une courbe pas affine en la recouvrant par des courbes affines d'intersections affines et en recollant les normalisations de ces courbes affines. On construit ainsi un espace annelé, mais il n'est pas évident de voir que c'est une variété.

2.2.2 *Courbes projectives lisses.* On se donne une extension K de k de type fini et de degré de transcendence 1. Nous allons construire une courbe projective lisse de corps de fonctions K et montrer qu'elle est unique à isomorphisme près. Pour cela, notons

$$C_K := \{\text{valuations } v : K^\times \twoheadrightarrow \mathbb{Z}\}$$

et munissons cet ensemble de la topologie dont les ouverts sont les complémentaires d'ensemble finis. Pour $v \in C_K$ on note $\mathcal{O}_v$ l'anneau de valuation, $\mathfrak{m}_v$ son idéal maximal et $k_v = \mathcal{O}_v/\mathfrak{m}_v$ son corps résiduel. Ce corps contient k par construction.

LEMME. – *C_K est infini. De plus :*
i) Pour toute valuation $v \in C_K$, on a $k = k_v$.
ii) Pour toute $f \in K^\times$, l'ensemble $\{v \in C_K, v(f) > 0\}$ est fini.

Démonstration. i) Puisque v est non triviale, il existe $f \in K$ tel que $v(f) > 0$. Puisque v est nulle sur k, l'élément f est transcendant sur k et engendre une algèbre $k[f]$ isomorphe à une algèbre de polynômes. L'extension $k(f) \subset K$ est finie, donc d'après le corollaire précédent, la clôture intégrale A de $k[f]$ est une k-algèbre de type fini de dimension 1 et de corps des fractions K. Puisque $k[f] \subset \mathcal{O}_v$ on a aussi $A \subset \mathcal{O}_v$. De plus, l'idéal $\mathfrak{m} := \{a \in A, v(a) > 0\}$ est un idéal maximal de A. En effet, c'est un idéal premier non nul (puisqu'il contient f) dans un anneau de dimension 1. Le localisé $A_\mathfrak{m}$ est contenu dans $\mathcal{O}_v$ et son corps résiduel $A/\mathfrak{m}$ est égal à k par le Nullstellensatz et la type-finitude de A comme k-algèbre. Il ne reste donc plus qu'à prouver que $A_\mathfrak{m} = \mathcal{O}_v$. Or, $A_\mathfrak{m}$ est lui-aussi un anneau de valuation. Donc si $x \in K \setminus A_\mathfrak{m}$, on a $x^{-1} \in A_\mathfrak{m}$ donc $x^{-1} \in \mathcal{O}_v$ et finalement $x \in K \setminus \mathcal{O}_v$, ce qui donne l'inclusion manquante.

ii) On peut supposer $f \in K \setminus k$ et donc transcendant sur k. Le raisonnement du i) montre que $\{v \in C_K, v(f) > 0\}$ est en bijection avec $\{\mathfrak{m} \in \mathrm{Max}(A),\ f \in \mathfrak{m}\}$, lequel est fini puisque $A/(f)$ est de dimension 0 et de type fini sur k (c'est un fermé propre de la courbe affine associée à A).

Reste à montrer que C_K est infini, mais cela découle du fait que $\mathrm{Max}(A)$ l'est. □

Soit maintenant U un ouvert de C_K (donc le complémentaire d'un ensemble fini). Posons

$$\mathcal{O}_K(U) := \{f \in K | \forall v \in U, v(f) \geqslant 0\} = \bigcap_{v \in U} \mathcal{O}_v.$$

D'après le i) du lemme précédent, on a une application

$$f \in \mathcal{O}_K(U) \ \mapsto \ (v \mapsto \bar{f} \in k = k_v)$$

de $\mathcal{O}_K(U)$ dans l'ensemble des fonctions $U \longrightarrow k$. D'après le ii) et le fait que U est infini, c'est une injection. On obtient ainsi un faisceau de fonctions sur C_K dont les anneaux locaux sont les anneaux de valuation discrète $\mathcal{O}_v$, $v \in C_K$. On a donc construit un espace k-annelé $(C_K, \mathcal{O}_K)$ dont le corps de fonctions rationnelles est manifestement K.

THÉORÈME. – *$(C_K, \mathcal{O}_K)$ est isomorphe à une courbe projective lisse.*

Démonstration. Soit $f \in K \setminus k$ et A la clôture intégrale de $k[f]$ comme dans la preuve précédente. Les arguments de cette preuve montrent aussi que l'application

$$C_{K,f} := \{v \in C_K, v(f) \geqslant 0\} \longrightarrow \mathrm{Max}(A),\ v \mapsto \mathfrak{m}_v \cap A$$

est une bijection de l'ouvert $C_{K,f}$ de C_K sur $\mathrm{Max}(A)$. C'est évidemment un homéomorphisme et il découle des définitions que les faisceaux de fonctions régulières se correspondent. On a donc un isomorphisme d'espaces k-annelés de $C_{K,f}$ sur la courbe affine

$\mathrm{Max}(A)$. Si $C_{K,f} = C_K \setminus \{v_1, \cdots, v_r\}$ alors en choissant des f_i tels que $v_i(f_i) > 0$, on obtient un recouvrement ouvert de C_K par les courbes affines $C_i := C_{K,f_i}$ et $C_0 := C_{K,f}$.

Choisissons pour chaque i un plongement affine $C_i \subset \mathbb{A}^{n_i}$ (autrement dit une présentation $k[X_1, \cdots, X_{n_i}] \twoheadrightarrow A_i$) et notons $\bar{C}_i$ la fermeture de C_i dans $\mathbb{P}^{n_i}$ qui est une courbe projective de corps de fonctions rationnelles K. D'après le lemme ci-dessous, il existe pour chaque i un morphisme d'espaces k-annelés. $C_K \xrightarrow{\varphi_i} \bar{C}_i$ qui prolonge l'immersion ouverte $C_i \hookrightarrow \bar{C}_i$. On en déduit un morphisme $C_K \xrightarrow{\varphi} \prod_i \bar{C}_i$ et on note que $\prod_i \bar{C}_i$ est une variété projective. Soit C l'adhérence de $\varphi(C_K)$ dans $\prod_i \bar{C}_i$. C'est encore une courbe algébrique projective de corps de fonctions K. Nous allons montrer que φ induit un isomorphisme $C_K \xrightarrow{\sim} C$.

Comme pour tout morphisme d'espaces k annelé, on a pour chaque point $v \in C_K$, un morphisme local entre germes de fonctions $\varphi^* : \mathcal{O}_{\varphi(v)} \longrightarrow \mathcal{O}_v$. Il s'agit ici simplement d'une inclusion $\mathcal{O}_{\varphi(v)} \subset \mathcal{O}_v$ de deux sous-anneaux de K. Lorsque $v \in C_i$, la projection $C \longrightarrow \bar{C}_i$ envoie $\varphi(v)$ sur v et fournit donc l'autre inclusion, de sorte que $\mathcal{O}_{\varphi(v)} = \mathcal{O}_v$. Soit maintenant P un point de C. Son anneau local $\mathcal{O}_P$ est contenu dans un anneau de valuation $\mathcal{O}_v$ (prendre la valuation associée à un idéal maximal de la clôture intégrale de $\mathcal{O}_P$ dans K). Or, $\mathcal{O}_v = \mathcal{O}_{\varphi(v)}$, on a donc deux points P et $\varphi(v)$ de C tels que $\mathcal{O}_P \subset \mathcal{O}_{\varphi(v)}$. Alors $P = \varphi(v)$. En effet, on peut trouver une carte affine $\mathrm{Max}(A)$ de C contenant les deux points et ils correspondent alors à deux idéaux maximaux $\mathfrak{m}$ et $\mathfrak{n}$ tels que $A_\mathfrak{m} \subset A_\mathfrak{n}$, ce qui implique $\mathfrak{n} \subset \mathfrak{m}$ et donc $\mathfrak{n} = \mathfrak{m}$. On a donc la surjectivité de φ. Son injectivité est claire. C'est donc une bijection et même un homéomorphisme. Puisque les morphismes sur les anneaux locaux sont des isomorphismes, on en conclut que φ est un isomorphisme. □

Lemme. – *Soit C un ouvert de C_K et $v \in C$. Tout morphisme d'espaces k-annelés $\varphi : C \setminus \{v\} \longrightarrow Y$ vers une variété projective Y admet un unique prolongement à C.*

Démonstration. Quitte à composer avec une immersion fermée $Y \subset \mathbb{P}^n$, on peut supposer $Y = \mathbb{P}^n$. En raisonnant par récurrence sur n, on peut supposer que $\varphi(C \setminus \{v\})$ n'est pas contenu dans la réunion des hyperplans de coordonnées. Le complémentaire U de cette réunion est affine et $\mathcal{O}_{\mathbb{P}^n}(U)$ contient les fonctions $X_i X_j^{-1}$ pour $0 \leqslant i, j \leqslant n$. Soient $f_{ij} \in \mathcal{O}_C(\varphi^{-1}(U)) \subset K$ les fonctions obtenues par composition avec φ. Prenons k tel que $v(f_{k0})$ est minimal parmi les $v(f_{i0})$. Alors pour tout i on a $v(f_{ik}) = v(f_{k0}^{-1} f_{i0}) \geqslant 0$ et donc $f_{ik} \in \mathcal{O}_C(\varphi^{-1}(U) \cup \{v\})$. Les $X_i X_k^{-1}$ sont des coordonnées affines sur l'ouvert $X_k \neq 0$ de $\mathbb{P}^n$. Il y a donc un unique morphisme $\varphi^{-1}(U) \cup \{v\} \longrightarrow \{X_k \neq 0\}$ donné par $w \mapsto [f_{0k}(w) : \cdots : f_{nk}(w)]$ (noter que $f_{kk} = 1$). Ce morphisme prolonge $\varphi_{|\varphi^{-1}(U)}$ et se recolle avec φ en un morphisme $C \longrightarrow \mathbb{P}^n$ qui prolonge φ. □

Remarquons que le même résultat avec la même preuve vaut si on remplace C par n'importe quelle courbe et v par un point régulier P de cette courbe. En particulier, on a le résultat suivant :

Corollaire. – *Soit $f : C \dashrightarrow Y$ une application rationnelle entre une courbe et une variété projective. Si C est lisse, alors f est un morphisme (ie est représenté par un couple (C, φ)).*

COROLLAIRE. – *Deux courbes projectives lisses C et C' de corps de fonctions rationnelles K sont isomorphes.*

Démonstration. Puisque $k(C) = k(C')$, il existe des application birationnelles $f : C \dashrightarrow C'$ et $g : C' \dashrightarrow C$ "inverses" l'une de l'autre. Par le corollaire précédent, elles se prolongent en des morphismes $\varphi : C \longrightarrow C'$ et $\psi : C' \longrightarrow C$. La composée $\psi \circ \varphi$ est alors l'identité sur un ouvert de C, donc sur tout C par densité. Idem pour $\psi \circ \varphi$. □

Si maintenant on se donne une extension $K' \subset K$ entre extensions de k de type fini et degré de transcendance 1, alors on a vu qu'il lui correspond une application rationnelle dominante $C_K \longrightarrow C_{K'}$. Par ce qui précède, celle-ci provient d'un morphisme (nécessairement unique). En particulier toute fonction rationnelle non constante $f \in K$ fournit un morphisme $C_K \xrightarrow{\varphi_f} \mathbb{P}^1$. Plus généralement, on a essentiellement prouvé :

COROLLAIRE. – *La catégorie des courbes projectives lisses munies des morphismes dominants est anti-équivalente à la catégorie des extensions de k de type fini et degré de transcendance* 1.

Notons qu'une extension $K' \subset K$ comme ci-dessus est nécessairement finie. On définit le *degré* d'un morphisme dominant $C \xrightarrow{\varphi} C'$ par $\deg(\varphi) := [k(C) : k(C')]$ et le *degré séparable* par $\deg_s(\varphi) : [k(C)_{\text{sep}} : k(C')]$.

PROPOSITION. – *Un morphisme dominant de courbes projectives est surjectif.*

Démonstration. Soit $C \xrightarrow{\varphi} C'$ le morphisme. En remplaçant C par $C_{k(C)}$, on se ramène au cas où C est lisse, et de même pour C'. Soit $P' \in C'$. En identifiant K' à $\varphi^*(K') \subset K$, son anneau local $\mathcal{O}_{P'} \subset K'$ est contenu dans un anneau de valuation de K, lequel est l'anneau local $\mathcal{O}_P$ en un point P de C. L'anneau $\mathcal{O}_P \cap K'$ est un anneau de valuation de K' contenant $\mathcal{O}_{P'}$ qui est aussi de valuation. Ces anneaux sont égaux. De même on a $\mathcal{O}_{\varphi(P)} = (\mathcal{O}_P \cap K')$, et donc $\varphi(P) = P'$. □

COROLLAIRE. – *Tout morphisme de source une courbe projective est d'image fermée.*

Démonstration. Notons que c'est vrai dès que la source est projective (pas nécessairement de dimension 1). Ici la fermeture $C' := \overline{\varphi(C)}$ est une sous-variété de Y et le morphisme $C \longrightarrow C'$ est dominant, donc C' est de dimension 1 et la proposition dit que $\varphi(C) = C'$. □

2.2.3 *Plongements projectifs.* Soit C une courbe projective lisse et $f_0, \cdots, f_n \in K^\times$. Il existe un ouvert affine U de C sur lequel les f_i sont définies et ne s'annulent pas. On a donc un unique morphisme $U \longrightarrow \mathbb{A}^{n+1}$ associé au morphisme de k-algèbres $X_i \mapsto f_i$. L'image de ce morphisme est dans $\mathbb{A}^{n+1} \setminus \{0\}$ et on peut composer pour obtenir $U \longrightarrow \mathbb{P}^n$. D'après la section précédente, ce morphisme se prolonge en un morphisme $C \xrightarrow{\varphi} \mathbb{P}^n$. Nous cherchons ici un critère pour que ce dernier morphisme soit une immersion fermée.

Pour cela notons $\mathcal{L} \subset K$ le k-sev de K engendré par les f_i. Pour $P \in C$ posons $v_P(\mathcal{L}) = \min\{v_P(f), f \in \mathcal{L}\}$ et $U_k := \{P \in C, v_P(f_k) = v_P(\mathcal{L})\}$. C'est un ouvert de C et les fonctions $f_i f_k^{-1}$ sont dans $\mathcal{O}(U_k)$. Il leur est donc associé un unique morphisme

$U_k \xrightarrow{\varphi_k} \{X_k \neq 0\} \simeq \mathbb{A}^n \subset \mathbb{P}^n$ envoyant $\frac{X_i}{X_k}$ sur $f_i f_k^{-1}$. Concrètement $\varphi_k(P) = [(f_0 f_k^{-1})(P) : \cdots : (f_n f_k^{-1})(P)]$ pour tout $P \in U_k$. Il est clair que φ_k et φ_j coïncident sur $U_k \cap U_j$, donc ces morphismes se recollent pour définir le morphisme $C \xrightarrow{\varphi} \mathbb{P}^n$ qui nous intéresse.

LEMME. – *Le morphisme φ est une immersion fermée si et seulement si :*

i) $\forall P \neq Q \in C$, $\exists f \in \mathcal{L}$, $v_P(f) = v_P(\mathcal{L})$ *et* $v_Q(f) > v_Q(\mathcal{L})$

ii) $\forall P \in C$, $\exists f \in \mathcal{L}$, $v_P(f) = v_P(\mathcal{L}) + 1$.

Démonstration. Par définition, φ est une immersion fermée si et seulement si elle réalise un homéomorphisme sur son image fermée et si pour tout $P \in C$, le morphisme local $\varphi^* \mathcal{O}_{\mathbb{P}^n, \varphi(P)} \longrightarrow \mathcal{O}_P$ est surjectif. Montrons d'abord que ceci équivaut à ce que φ soit injective et que pour tout P le morphisme local φ^* induise une surjection $\mathfrak{m}_{\mathbb{P}^n, P} \twoheadrightarrow \mathfrak{m}_P / \mathfrak{m}_P^2$. En effet, on sait déjà que l'image de φ est fermée, et vu que les topologies de C et de son image sont données par les complémentaires de sous-ensembles finis, l'injectivité de φ implique que c'est un homéomorphisme. Lorsqu'on a un morphisme d'anneaux locaux $A \longrightarrow B$ tel que $A/\mathfrak{m}_A \simeq B/\mathfrak{m}_B$ et $\mathfrak{m}_A \twoheadrightarrow \mathfrak{m}_B/\mathfrak{m}_B^2$ il n'est généralement pas vrai que $A \twoheadrightarrow B$, *mais c'est vrai si B est un A-module de type fini* (exercice avec le lemme de Nakayama). Dans notre cas, l'image $\mathcal{O}_{\varphi(P)} := \varphi^*(\mathcal{O}_{\mathbb{P}^n, \varphi(P)})$ est l'anneau local en $\varphi(P)$ de la courbe image $\varphi(C)$. L'anneau $\mathcal{O}_P$ est un localisé de la normalisation $\tilde{\mathcal{O}}_{\varphi(P)}$ de $\mathcal{O}_{\varphi(P)}$ dans K et n'a pas de raison d'être de type fini sauf justement si $\varphi^{-1}(\varphi(P)) = \{P\}$, puisque dans ce cas on a $\tilde{\mathcal{O}}_{\varphi(P)} = \mathcal{O}_P$ et on sait que la normalisation est de type fini. Donc, lorsque φ est injective, la surjectivité de $\mathfrak{m}_{\mathbb{P}^n, P} \twoheadrightarrow \mathfrak{m}_P/\mathfrak{m}_P^2$ implique bien celle de $\mathcal{O}_{\mathbb{P}^n, \varphi(P)} \longrightarrow \mathcal{O}_P$.

Écrivons maintenant $f \in \mathcal{L}$ sous la forme $f = \sum_{i=0}^n \lambda_i f_i$. Alors la condition $(v_P(f) = v_P(\mathcal{L})$ et $v_Q(f) > v_Q(\mathcal{L}))$ équivaut à ce que $\varphi(Q)$ soit dans l'hyperplan d'équation $\sum_i \lambda_i X_i = 0$ et $\varphi(P)$ dans le complémentaire de cet hyperplan. Le point i) est donc équivalent à l'injectivité de φ.

Par ailleurs, si k est tel que $v_P(f_k) = v_P(\mathcal{L})$, la condition $v_P(f) = v_P(\mathcal{L}) + 1$ équivaut à ce que la fonction linéaire $\sum_i \lambda_i \frac{X_i}{X_k}$ sur l'ouvert affine $\{X_k \neq 0\}$ de $\mathbb{P}^n$ soit dans l'idéal maximal au point $\varphi(P)$ et que son image $f f_k^{-1}$ soit une uniformisante en P. La condition ii) au point P équivaut donc à la surjectivité de $\mathfrak{m}_{\mathbb{P}^n, P} \to \mathfrak{m}_P/\mathfrak{m}_P^2$. □

Nous allons voir comment la théorie des diviseurs, et notamment le théorème de Riemann-Roch permet de trouver des espaces vectorels $\mathcal{L}$ vérifiant les conditions du lemme.

2.3 Diviseurs, différentielles, Riemann-Roch

2.3.1 *Diviseurs.* Soit C une courbe lisse. On note $\mathrm{Div}(C)$ le groupe abélien libre de base C. Si $D = \sum_P a_P[P]$ est un diviseur, son *degré* est l'entier $\sum_P a_P$. On note généralement $\mathrm{Div}^0(C)$ le sous-groupe des diviseurs de degré 0. On munit $\mathrm{Div}(C)$ de la relation d'ordre

$$D = \sum_P a_P[P] \leqslant D' = \sum_P a'_P[P] \Leftrightarrow \forall P \in C, a_P \leqslant a'_P.$$

On dit que D est *positif* ou *effectif* si $D \geqslant 0$. L'ensemble $\mathrm{Div}(C)$ ainsi ordonné est très utile pour étudier les espaces de fonctions méromorphes à pôles ou zéros prescrits. Pour cela, on associe à une fonction l'ensemble de ses pôles et zéros comptés avec multiplicités sous forme de diviseur. Formellement, le lemme 2.2.2 ii) permet de définir une application

$$\mathrm{div} : k(C)^\times \longrightarrow \mathrm{Div}(C),\ f \mapsto \sum_P v_P(f)[P]$$

où on a noté v_P la valuation normalisée de $k(C)$ associée à P. Cette application est un morphisme de groupes abéliens. Pour tout diviseur D, l'ensemble

$$\mathcal{L}_D := \{f \in k(C),\ \mathrm{div}(f) + D \geqslant 0\}$$

est un k-espace vectoriel et consiste en toutes les fonctions méromorphes dont l'ordre du pôle en un point P est au plus le coefficient de P dans D. Par exemple, $\mathcal{L}_0$ est l'espace des fonctions définies partout, et on a vu plus haut que $\mathcal{L}_0 = k$ lorsque C est projective.

Lemme. – *Si C est projective (et lisse) $\mathcal{L}_D$ est de dimension finie, notée ℓ_D. De plus, si $D \leqslant D'$ on a $0 \leqslant \ell_{D'} - \ell_D \leqslant \deg(D') - \deg(D)$.*

Démonstration. Il est clair que $D \leqslant D' \Rightarrow \mathcal{L}_D \subset \mathcal{L}_{D'}$. Il suffit donc de prouver la finitude de la dimension dans le cas $D \geqslant 0$. Dans ce cas, nous montrons par récurrence sur $\deg(D)$ que $\ell_D \leqslant \deg(D)+1$. En degré 0, on a $D = 0$ et on vient de voir que $\ell_0 = 1$. Si $\deg(D) > 0$, il existe P tel que $D - [P] \geqslant 0$. Si $\mathcal{L}_D = \mathcal{L}_{D-[P]}$ la finitude de la dimension et la borne sont connues par récurrence. Sinon, soit $f \in \mathcal{L}_D \setminus \mathcal{L}_{D-[P]}$. En simplifiant le pôle en P de $g \in \mathcal{L}_D$ par une combinaison linéaire avec f, on constate que $\mathcal{L}_D = \mathcal{L}_{D-[P]} \oplus kf$. Ceci conclut la récurrence. On vient de montrer l'inégalité annoncée dans le cas $0 \leqslant D$. La même preuve règle le cas de $D \leqslant D'$. □

Remarque. – Si $g \in k(C)^\times$, on a $\ell_{D+\mathrm{div}(g)} = \ell_D$ car l'application $f \mapsto fg$ induit un isomorphime $\mathcal{L}_{D+\mathrm{div}(g)} \xrightarrow{\sim} \mathcal{L}_D$. Ceci est une invitation à considérer les diviseurs modulo les *diviseurs principaux*, qui sont par définitions ceux de la forme $\mathrm{div}(f)$. On introduit donc le *groupe de Picard*

$$\mathrm{Pic}(C) := \mathrm{Coker}(k(C)^\times \longrightarrow \mathrm{Div}(C)).$$

Exercice. – Pour D effectif sur $\mathbb{P}^1$, la borne $\ell_D = \deg(D) + 1$ est atteinte.

Soit maintenant $C \xrightarrow{\varphi} C'$ un morphisme de courbes lisses. On a un morphisme évident

$$\varphi_* : \mathrm{Div}(C) \longrightarrow \mathrm{Div}(C'),\ [P] \mapsto [\varphi(P)]$$

et on définit un morphisme dans l'autre sens

$$\varphi^* : \mathrm{Div}(C') \longrightarrow \mathrm{Div}(C),\ [P'] \mapsto \sum_{\varphi(P)=P'} e_P(\varphi)[P]$$

où $e_P(\varphi)$ est l'*indice de ramification* de φ en P défini par $e_P(\varphi) = v_P(\varphi^*(t_{\varphi(P)}))$ avec $t_{\varphi(P)} \in k(C')$ une uniformisante de $\mathcal{O}_{\varphi(P)}$ (ie un élément tel que $v_{\varphi(P)}(t_{\varphi(P)}) = 1$). On a

bien-sûr aussi $\varphi^* : k(C')^\times \hookrightarrow k(C)^\times$ et on définit $\varphi_* := N_{k(C)/k(C')} : k(C')^\times \hookrightarrow k(C)^\times$. On a alors les propriétés suivantes :

LEMME. – *Supposons C et C' projectives.*

i) $\deg(\varphi^*(D)) = \deg(\varphi)\deg(D)$ *pour tout* $D \in \mathrm{Div}(C')$.

ii) $\mathrm{div}(\varphi^* f) = \varphi^* \mathrm{div}(f)$ *pour toute* $f \in k(C')^\times$.

Démonstration. i) Identifions $k(C')$ à un sous-corps de $k(C)$ via φ^*. Soit P' un point de C'. Considérons la clôture intégrale $A_{P'}$ de $\mathcal{O}_{P'}$ dans $k(C)$. D'après le corollaire 2.2.1, il est de type fini sur $\mathcal{O}_{P'}$. Comme son corps de fractions est $k(C)$ et comme $\mathcal{O}_{P'}$ est principal, il s'ensuit que $A_{P'}$ est libre de rang $\deg(\varphi)$ sur $\mathcal{O}_{P'}$. Le quotient $A_{P'}/(t_{P'})$ est donc de dimension $\deg(\varphi)$ sur k. Par ailleurs, $\varphi^{-1}(P')$ s'identifie à $\mathrm{Max}(A_{P'})$ et la décomposition habituelle des anneaux artiniens s'écrit ici

$$A_{P'}/(t_{P'}) = \prod_{\varphi(P)=P'} \mathcal{O}_P/(t_{P'}).$$

Or, par définition, on a $e_\varphi(P) = v_P(t_{P'}) = \dim_k(\mathcal{O}_P/(t_{P'}))$.

ii) Il s'agit de vérifier que $v_P(f) = e_P(\varphi) v_{P'}(f)$. Exercice. □

Exercice. – Si $C' \xrightarrow{\psi} C''$ est un second morphisme de courbes projectives lisses, alors pour tout $P \in C$ on a $e_P(\psi \circ \varphi) = e_P(\varphi) e_{\varphi(P)}(\psi)$.

COROLLAIRE. – *Pour toute* $f \in k(C)^\times$ *on a* $\deg(\mathrm{div}(f)) = 0$.

Démonstration. Si f est constante, c'est clair, sinon on considère le morphisme $C \xrightarrow{\varphi_f} \mathbb{P}^1$ via le plongement $k(X) \hookrightarrow K$, $X \mapsto f$. Alors le ii) du lemme montre que

$$\mathrm{div}(f) = \varphi_f^*(\mathrm{div}(X)) = \varphi_f^*([0] - [\infty]),$$

et le i) donne l'égalité voulue. □

Application. – S'il existe $P \in C$ tel que $\ell_{[P]} = 2$, alors $C \simeq \mathbb{P}^1$. En effet, soit f non constante dans $\mathcal{L}_{[P]}$ et $\varphi_f : C \longrightarrow \mathbb{P}^1$ le morphisme associé. Alors $\varphi_f^{-1}([\infty]) = [P]$ donc, d'après le i) du lemme, $\deg(\varphi_f) = 1$ et il s'ensuit que $k(C) = k(f)$.

Exercice. – Montrer que $\deg(D) < 0 \Rightarrow \ell_D = 0$.

On peut maintenant définir $\mathrm{Pic}^0(C) := \mathrm{Coker}(k(C)^\times \longrightarrow \mathrm{Div}^0(C))$, qui s'inscrit dans une suite exacte $0 \longrightarrow \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}(C) \longrightarrow \mathbb{Z} \longrightarrow 0$.

Exercice. – Montrer que $\mathrm{Pic}^0(\mathbb{P}^1) = 0$.

Nous avons vu plus haut que $\ell_D \leqslant \deg(D) + 1$ pour tout diviseur D. La proposition suivante nous assure que ℓ_D ne s'éloigne pas trop de $\deg(D)$. C'est le premier pas vers le théorème de Riemann-Roch qui permettra de mieux contrôler ℓ_D.

PROPOSITION. – *La fonction* $D \mapsto r(D) := \deg(D) - \ell_D$ *est bornée supérieurement.*

Démonstration. Remarquons d'abord que le premier lemme ci-dessus nous dit que la fonction $D \mapsto r(D)$ est croissante.

Choisissons maintenant $f \in k(C)$ non constante, notons $\varphi_f : C \longrightarrow \mathbb{P}^1$ le morphisme associé, et considérons le diviseur (effectif) des pôles de f :

$$D_f := \varphi_f^*([\infty]) = \sum_{\varphi_f(P)=\infty} e_{\varphi_f}(P)[P] = -\sum_{P|v_P(f)<0} v_P(f)[P].$$

Soit A la clôture intégrale de $k[f]$ dans $k(C)$. Pour tout $g \in A$ et tout $P \in C$, on a $v_P(f) \geqslant 0 \Rightarrow v_P(g) \geqslant 0$ et donc $\varphi_g(P) = \infty \Rightarrow \varphi_f(P) = \infty$. Il s'ensuit qu'il existe un entier $k \in \mathbb{N}$ tel que $\varphi_g^*([\infty]) \leqslant k\varphi_f^*([\infty])$. Soit $g_1, \cdots, g_n$ une base de A comme $k[f]$-module. Prenons $m \in \mathbb{N}$ tel que $\varphi_{g_i}^*([\infty]) \leqslant m\varphi_f^*([\infty])$ pour tout i. On a donc $g_i \in \mathcal{L}(mD_f)$ pour tout i. Soit maintenant $m' \geqslant m$ et considérons les $n(m'-m+1)$ fonctions

$$g_i f^j,\ i = 1, \cdots, n,\ j = 0, \cdots, m'-m.$$

Ces fonctions sont dans $\mathcal{L}(m'D_f)$ et sont k-linéairement indépendantes. On a donc $\ell_{m'D_f} \geqslant n(m'-m+1)$ et, en se rappelant que $\deg(D_f) = [k(C) : k(f)] = n$, on obtient

$$\forall m' \geqslant m,\ r(m'D_f) \leqslant m'n - n(m'-m+1) = n(m-1).$$

Ainsi la fonction croissante $m' \mapsto r(m'D_f)$ est bornée. Notons B une borne, par exemple $n(m-1)$. Nous allons montrer que $r(D) \leqslant B$ pour tout $D \in \mathrm{Div}(C)$.

Pour cela, on observe que pour toute fonction $g \in k(C)^\times$, on a $r(D + \mathrm{div}(g)) = r(D)$. Il nous suffira donc de construire une fonction g telle que $D + \mathrm{div}(g) \leqslant mD_f$ pour un entier m. De manière équivalente, on veut trouver g telle que $v_P(g) + a_P(D) \leqslant 0$ pour tout $P \in \varphi_f^{-1}(\mathbb{A}^1)$. Soit alors $S \subset C$ l'ensemble (fini) des $P \in \varphi_f^{-1}(\mathbb{A}^1)$ tels que $a_P(D) > 0$. Il suffit de prendre la fonction $g := \prod_{P \in S}(f - f(P))^{-a_P(D)}$ (ici, on note $\varphi_f(P) = [f(P) : 1]$). □

Exemple. – Considérons la cubique projective plane C d'équation

$$Y^2Z = (X - x_1Z)(X - x_2Z)(X - x_3Z),\ x_i \in k.$$

Si les x_i sont distincts, elle est lisse et passe par les points distincts $P_i = [x_i : 0 : 1]$ et $O = [0 : 1 : 0]$. Comme elle n'est pas contenue dans l'hyperplan $\{Z = 0\}$, les fonctions $x = X/Z$ et $y = Y/Z$ induisent des fonctions rationnelles sur C. La fonction y s'annule en chaque P_i et on peut calculer son ordre $v_{P_i}(y) = \dim_k(\mathcal{O}_{P_i}/(y))$ dans la carte affine $Z \neq 0$. On trouve $(k[x,y]_{(P_i)})_{/(y,y^2-\Pi(x-x_i))} = k$ et donc $v_{P_i}(y) = 1$. La fonction $1/y = Z/Y$ s'annule en O avec pour ordre la dimension de $\mathcal{O}_O/(y^{-1})$. On peut calculer cet anneau dans la carte affine $Y \neq 0$ où l'équation de la courbe est $z = \prod(x - x_iz)$. On trouve l'anneau $(k[x,z]_{(x,z)})_{/(z,z-\Pi(x-x_iz))} = (k[x,z]_{(x,z)})_{/(z,x^3)}$ qui est de dimension 3. On en déduit que

$$\mathrm{div}(y) = \sum_i [P_i] - 3[O].$$

Exercice : montrer que $\mathrm{div}(x - x_i) = 2[P_i] - 2[O]$.

Ceci montre que pour cette courbe on a $\ell_{2[O]} \geqslant 2$ puisque $\mathcal{L}_{2[O]}$ contient x et 1, et $\ell_{3[O]} \geqslant 3$ puisque $\mathcal{L}_{3[O]}$ contient y, x, et 1. Pour montrer que ce sont des égalités, il suffit de montrer que $\ell_{[O]} = 1$ (par le premier lemme 2.3.1), i.e. il suffit de montrer que C n'est pas isomorphe à $\mathbb{P}^1$. La prochaine section introduit un outil utile pour discriminer les courbes.

2.3.2 *Différentielles.* Soit $K \subset L$ une extension de corps, on peut définir le L-espace vectoriel $\Omega_{L/K}$ des différentielles de Kähler comme le quotient du L-espace vectoriel de base les symboles dx, $x \in L$, par les relations $d(x+y) = dx + dy$, $d(xy) = xdy + ydx$ et $dx = 0$ si $x \in K$. Il est donc muni d'une application K-linéaire $x \mapsto dx$. On peut aussi le définir ainsi :

$$\Omega_{L/K} := I/I^2, \text{ où } I := \mathrm{Ker}(L \otimes_K L \xrightarrow{\text{mult}} L),$$

auquel cas, $dx = (x \otimes 1 - 1 \otimes x) \bmod I^2$. Plus généralement, on définit $\Omega_{B/A}$ pour n'importe quel morphisme d'anneaux de la même manière. Le couple $(\Omega_{B/A}, d)$ est universel parmi les B-modules munis d'une dérivation A-linéaire. Voici quelques propriétés très générales, laissées en exercice (sinon voir tout livre d'algèbre commutative, par exemple [Matsumura]).

i) Si B est engendrée comme A-algèbre par des éléments $x_1, \cdots, x_n$, alors $\Omega_{B/A}$ est engendré par les dx_i comme B-module.

ii) Si $B = A[X_1, \cdots, X_n]$, alors $\Omega_{B/A}$ est libre sur B de base $dX_1, \cdots, dX_n$.

iii) Si S est une partie multiplicative de B, alors $S^{-1}\Omega_{B/A} = \Omega_{S^{-1}B/A} = \Omega_{S^{-1}B/(S\cap A)^{-1}A}$.

iv) Si A' est une B-algèbre et $A' = A \otimes_B B'$, alors $\Omega_{B'/A'} \simeq B' \otimes_B \Omega_{B/A}$.

v) Pour $A \longrightarrow B \longrightarrow C$, on a une suite exacte $C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0$

vi) Pour I idéal de B, on a une suite exacte $I/I^2 \longrightarrow B/I \otimes_B \Omega_{B/A} \longrightarrow \Omega_{(B/I)/A} \longrightarrow 0$ où le premier morphisme est induit par $i \mapsto 1 \otimes di$.

Dans le cas des extensions de corps, on a les propriétés suivantes :

vii) Pour une extension finie L/K, on a $\Omega_{L/K} = 0 \Leftrightarrow L$ est séparable sur K. C'est immédiat sur la deuxième définition puisque L est séparable sur K si et seulement si $L \otimes_K L$ est réduite.

Exemple. – Si $L = \mathbb{F}_p(X)$ et $K = \mathbb{F}_p(X^p)$, comme toute dérivation $\mathbb{F}_p$-linéaire de L est nulle sur K, on a $\Omega_{L/K} = \Omega_{L/\mathbb{F}_p} = L \cdot dX$.

viii) Si de plus L et K sont des extensions de type fini de k, alors le morphisme $L \otimes_K \Omega_{K/k} \longrightarrow \Omega_{L/k}$ est un isomorphisme si et seulement si $L \supset K$ est séparable. Cela découle de vii) et v) plus un petit argument, cf [Matsumura, 27.A case 2].

Proposition. – *i) Soit K un corps de fonctions de courbe sur k, v un point de C_K, et t une uniformisante en v. Alors $\Omega_{\mathcal{O}_v/k}$ est libre de rang 1 sur $\mathcal{O}_v$, engendré par dt.*

ii) Si $K' \subset K$ est une extension finie et si $t' \in K'$ est une uniformisante de $v' = v_{|K'}$, alors $\Omega_{\mathcal{O}_v/\mathcal{O}_{v'}} \simeq (\mathcal{O}_v/\frac{dt'}{dt}\mathcal{O}_v).dt$ est de longueur finie $\geqslant v(t') - 1$ avec égalité si et seulement si $v(t') \neq 0$ dans k. En particulier, ce module est nul si et seulement si $v(t') = 1$.

Démonstration. i) Soit A la clôture intégrale de $k[t]$ dans K. On a déjà vu que A est une k-algèbre de type fini, donc $\Omega_{A/k}$ est un A-module de type fini par la propriété i). On sait aussi que $\mathcal{O}_v$ est le localisé de A en l'idéal maximal $\mathfrak{m}_v \cap A$, donc $\Omega_{\mathcal{O}_v/k}$ est de type fini comme $\mathcal{O}_v$-module par la propriété iii). Les propriétés iii) et viii) impliquent que $K \otimes_{\mathcal{O}_v} \Omega_{\mathcal{O}_v/k} = \Omega_{K/k}$ est de dimension $\geqslant 1$. Maintenant, si on fait $A = k$, $B = \mathcal{O}_v$ et $I = \mathfrak{m}_v$ dans vi), on obtient une surjection $\mathfrak{m}_v/\mathfrak{m}_v^2 \twoheadrightarrow k \otimes_{\mathcal{O}_v} \Omega_{\mathcal{O}_v/k}$. Comme $\mathfrak{m}_v/\mathfrak{m}_v^2$ est engendré par l'image de t, ceci montre que $\Omega_{\mathcal{O}_v/k}$ est engendré par dt. Comme $\mathcal{O}_v$ est principal et que $\Omega_{\mathcal{O}_v/k}$ a rang $\geqslant 1$, on conclut.

ii) La suite exacte v) nous donne ici $\mathcal{O}_v \otimes_{\mathcal{O}_{v'}} \Omega_{\mathcal{O}_{v'}/k} \longrightarrow \Omega_{\mathcal{O}_v/k} \longrightarrow \Omega_{\mathcal{O}_v/\mathcal{O}_{v'}} \longrightarrow 0$, qui d'après le i) s'écrit encore $\mathcal{O}_v dt' \longrightarrow \mathcal{O}_v dt \longrightarrow \Omega_{\mathcal{O}_v/\mathcal{O}_{v'}} \longrightarrow 0$, d'où l'isomorphisme annoncé. Écrivons maintenant $t' = ut^{v(t')}$ avec $u \in \mathcal{O}_v^\times$. On a donc $dt' = v(t')ut^{v(t')-1}dt + t^{v(t')}du$. Il s'ensuit que $\frac{dt'}{dt}\mathcal{O}_v dt \subset t^{v(t')-1}\mathcal{O}_v dt$ avec égalité dès que $v(t')$ est non nul dans k, d'où la deuxième assertion. Notons que $\Omega_{\mathcal{O}_v/\mathcal{O}_{v'}}$ est de torsion et donc de longueur finie, puisque son localisé $\Omega_{K/K'}$ est nul par hypothèse de séparabilité. □

Voici un corollaire du point ii), que l'on démontre plus classiquement avec la théorie des discriminants dans les anneaux de Dedekind.

COROLLAIRE. – *Soit $\varphi : C \longrightarrow C'$ un morphisme dominant* séparable *de courbes lisses. Alors le lieu de ramification $\{P \in C, e_P(\varphi) > 1\}$ est fini.*

Démonstration. Identifions $k(C')$ à un sous-corps de $k(C)$ via φ^*. Alors d'après le ii) de la proposition précédente, on a $e_P(\varphi) > 1 \Leftrightarrow \Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}} \neq 0$. Soit t' une uniformisante en $\varphi(P)$, A' la normalisation de $k[t']$ dans K' et A sa normalisation dans K. Par la compatibilité des différentielles avec la localisation, on a $\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}} = \mathcal{O}_P \otimes_A \Omega_{A/A'}$, donc P est dans le support de $\Omega_{A/A'}$. Mais on sait que $\Omega_{A/A'}$ est un A-module de type fini, donc son support est fermé. Or $K \otimes_A \Omega_{A/A'} = \Omega_{K/K'} = 0$ car $K' \subset K$ est séparable, donc ce fermé est propre et par conséquent fini. □

DÉFINITION. – *Sous les hypothèses du corollaire, on note $R_\varphi := \sum_{P \in C} \dim_k(\Omega_{P/\varphi(P)})[P]$ et on l'appelle* diviseur de ramification *de φ.*

Le ii) de la proposition précédente montre que

$$R_\varphi \geqslant \sum_P (e_P(\varphi) - 1)[P], \quad \text{avec égalité si } e_P(\varphi) \neq 0 \text{ dans } k, \text{ pour tout } P.$$

Par localisation, le point i) de la proposition implique que $\Omega_{K/k}$ est de dimension 1 engendré par dt. Ceci permet la définition suivante.

PROPOSITION - DÉFINITION. – *Soit C une courbe lisse. On note $\Omega_C := \Omega_{k(C)/k}$ et on l'appelle* espace des (formes) différentielles méromorphes *sur C.*

i) Pour chaque point $P \in C$ et pour toute $\omega \in \Omega_C$, l'entier

$$v_P(\omega) := v_P(\omega/dt)$$

ne dépend pas du choix d'une uniformisante $t \in k(C)$ en P.

ii) Pour toute $\omega \in \Omega_C$, l'ensemble $\{P \in C, v_P(\omega) \neq 0\}$ est fini. On peut donc poser

$$\mathrm{div}(\omega) := \sum_P v_P(\omega)[P] \ \in \mathrm{Div}(C).$$

iii) L'image K_C de $\mathrm{div}(\omega)$ dans $\mathrm{Pic}(C)$ est indépendente de ω et est appelée classe canonique. *Si C est propre, on définit le* genre *de la courbe C par $g = g(C) := \ell_{K_C}$.*

Démonstration. i) Si t' est une autre uniformisante en P, le i) de la proposition précédente implique que $dt' \in \mathcal{O}_P dt$ et $dt \in \mathcal{O}_P dt'$, et donc que $dt' \in \mathcal{O}_P^\times dt$.

ii) Puisque $v_P(f\omega) = v_P(f) + v_P(\omega)$, il suffit de traiter une seule forme différentielle ω. Prenons $\omega = dt$ où t est une uniformisante en un point Q. Soit $\varphi_t : C \longrightarrow \mathbb{P}^1$ le morphisme défini par t. Notons que ce morphisme est séparable puisque dt engendre $\Omega_{k(C)/k}$, ce qui implique $\Omega_{k(C)/k(t)} = 0$ par la suite exacte v). Pour tout $P \in \varphi_t^{-1}(\mathbb{A}^1)$, écrivons $\varphi_t(P) = [t(P) : 1]$ avec $t(P) \in k$. La fonction $t - t(P)$ est alors une uniformisante en $\varphi_t(P)$. D'après le dernier corollaire, le lieu de ramification de φ_t est fini. Donc, pour presque tout $P \in \varphi_t^{-1}(\mathbb{A}^1)$, la fonction $t - t(P)$ est une uniformisante en P. En un tel point, on a donc $v_P(dt) = v_P(d(t - t(P))) = 0$.

iii) est clair. □

Exercice. – Soit $C = \mathbb{P}^1$ et $t = \frac{X}{Y}$. Montrer que $\mathrm{div}(dt) = -2[\infty]$, puis que $g(\mathbb{P}^1) = 0$.

Définition. – *Pour U ouvert de C on pose $\Omega_C(U) := \{\omega \in \Omega_C,\ v_P(\omega) \geqslant 0, \forall P \in U\}$. C'est le $\mathcal{O}_C(U)$-module des "formes différentielles régulières" sur U.*

Si on choisit $\omega \neq 0$ dans Ω_C, on a $\Omega_C(C) \simeq \{f \in k(C),\ \mathrm{div}(f\omega) \geqslant 0\} = \mathcal{L}_{\mathrm{div}(\omega)}$. Ainsi, pour une courbe propre et lisse, l'espace $\Omega_C(C)$ des formes différentielles partout régulières est de dimension finie égale au genre g de la courbe.

Exemple. – Soit C la cubique d'équation $Y^2Z = (X - x_1Z)(X - x_2Z)(X - x_3Z)$. Pour calculer dx, on remarque d'abord que $x - x_0$ est une uniformisante en tout point $P = [x_0 : y_0 : 1]$ de $C \cap \mathbb{A}^2$ tel que $x_0 \neq x_i$, d'où $v_P(dx) = v_P(d(x - x_0)) = 0$ en un tel point. Pour $P_i = [x_i : 0 : 1]$, on a vu que $v_{P_i}(x - x_i) = 2$ donc $v_{P_i}(dx) = v_{P_i}(d(x - x_i)) = 1$. Enfin on a vu que $v_O(x) = -2$, donc $v_O(dx) = v_O(-x^{-2}d(x^{-1})) = 3$. On a donc $\mathrm{div}(dx) = \sum_i [P_i] - 3[O]$. Par le calcul précédent de $\mathrm{div}(y)$, on en déduit que $\mathrm{div}(\frac{dx}{y}) = 0$, c'est-à-dire que $\frac{dx}{y}$ est une différentielle partout régulière et ne s'annulant nulle part. En particulier, $K_C = 0$ et $g(C) = 1$.

Étudions maintenant l'application $k(C')$-linéaire $\Omega_{C'} \xrightarrow{\varphi^*} \Omega_C$ associée à un morphisme $\varphi : C \longrightarrow C'$. D'après la propriété viii) plus haut, cette application est non-nulle (et donc injective) si et seulement si l'extension $k(C') \xrightarrow{\varphi^*} k(C)$ est séparable.

Proposition. (Formule de Hurwitz) – *Supposons φ séparable. Alors on a l'égalité $\deg(K_C) = \deg(\varphi)\deg(K_{C'}) + \deg(R_\varphi)$. On a de plus $\deg(R_\varphi) \geqslant \sum_{P \in C}(e_P(\varphi) - 1)$, avec égalité si les indices de ramification sont premiers à la caractéristique de k.*

Démonstration. Soit $\omega' \in \Omega_{C'}$. Il suffit de prouver que $\mathrm{div}(\varphi^*\omega') = \varphi^*(\mathrm{div}(\omega')) + R_\varphi$, ou autrement dit que $v_P(\varphi^*(\omega')) = e_P(\varphi)v_{\varphi(P)}(\omega') + \dim_k(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})$ pour tout $P \in C$. Soit $t' \in k(C')$ une uniformisante en $\varphi(P)$ et $t \in k(C)$ une uniformisante en P. En posant $e = e_P(\varphi)$, il existe $u \in \mathcal{O}_P^\times$ telle que $t' = t^e u$. Écrivons alors $\omega' = f dt'$, de sorte que $v_{\varphi(P)}(\omega') = v_{\varphi(P)}(f)$. On a $\varphi^*\omega' = f[et^{e-1} + t^e \frac{du}{dt}]dt$ et donc $v_P(\varphi^*\omega) = v_P(et^{e-1}f + t^e f\frac{du}{dt}) = v_P(f) + \dim_k(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})$ d'après la preuve du ii) de la première proposition. L'inégalité sur R_φ a déjà été vue plus haut. □

2.3.3 *Résidus.* Fixons un corps de fonctions K sur k. Si $v \in C_K$, et si $t \in K$ est une uniformisante en v, le morphisme de k-algèbres $k[X] \longrightarrow \mathcal{O}_v$, $X \mapsto t$ induit pour tout $n > 0$ un isomorphisme $k[X]/(X^n) \xrightarrow{\sim} \mathcal{O}_v/\mathfrak{m}_v^n$, d'où à la limite un isomorphisme

$$k[[X]] \xrightarrow{\sim} \hat{\mathcal{O}}_v := \lim_{\longleftarrow n\in\mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$$

de l'anneau des séries formelles en X sur le complété $\mathfrak{m}_v$-adique de $\mathcal{O}_v$. On écrira informellement $\hat{\mathcal{O}}_v = k[[t]]$. Via cet isomorphisme, le corps K se plonge dans le corps $k((t)) = \mathrm{Frac}(k[[t]])$, ce qui permet de "développer" toute fonction méromorphe $f \in K$ comme une série $f = \sum_{n\in -N} a_{n,t}(f)t^n$ dans $k((t))$.

Proposition - Définition. – *Soit $\omega \in \Omega_{K/k}$. Le scalaire $a_{-1,t}(\frac{\omega}{dt})$ ne dépend pas du choix de l'uniformisante t en v. On le note* $\mathrm{Res}_v(\omega)$ *et on l'appelle* résidu *de f en v.*

Démonstration. Soit $t' = tu$ une autre uniformisante, avec donc $u \in \mathcal{O}_v^\times$. Quitte à multiplier u par un scalaire de k, on peut supposer que $u \in 1 + \mathfrak{m}_v$. Dans $k[[t]]$ on peut écrire $u \in 1 + tk[[t]]$ sous la forme $u = 1 + \sum_{n\geqslant 1} b_n t^n$. Notons $u' = \sum_{n\geqslant 1} n b_n t^{n-1}$. On a donc $dt' = [u + tu']dt$. Écrivons $\omega = \sum_{n>-N} a_{n,t}t^n dt = \sum_{n>-N} a_{n,t'}(t')^n dt'$. On a donc l'égalité dans $k((t))$

$$\sum_{n>-N} a_{n,t}t^n = \sum_{n>-N} a_{n,t'}[u^{n+1} + tu'u^n]t^n.$$

Puisqu'on s'intéresse au terme en t^{-1} on peut travailler dans le $k[[t]]$-module quotient $k((t))/k[[t]]$ qui est aussi un k-espace vectoriel de base les t^n pour $n > 0$. Puisque $tu'u^{-1}t^{-1} \in k[[t]]$, on a dans ce quotient l'égalité

$$\sum_{0>n>-N} a_{n,t}t^n dt = a_{-1,t'}t^{-1} + \sum_{-1>n>-N} a_{n,t'}[u^{n+1} + tu'u^n]t^n.$$

Il s'agit donc de montrer que pour tout $n < -1$, le développement t-adique de $[u^{n+1} + tu'u^n]t^n$ n'a pas de terme en t^{-1} (ou plutôt que celui-ci est nul). Si k est de caractéristique 0, c'est facile car $[u^{n+1} + tu'u^n]t^n = \frac{1}{n+1}(u^{n+1}t^{n+1})'$ et la dérivée d'une série formelle n'a jamais de terme en t^{-1}. Pour obtenir le cas général, on peut travailler dans l'anneau $A[[t]][t^{-1}]$ avec $A = \mathbb{Z}[B_i]_{i\geqslant 1}$ et $u = 1 + \sum_{i\geqslant 1} B_i t^i$. Alors le coefficient de t^{-1} dans le développement de $[u^{n+1} + tu'u^n]t^n$ est un élément de A. On vient de voir que cet élément est nul dans $\mathrm{Frac}(A)$ qui est de caractéristique 0, donc il est nul. On conclut par spécialisation $B_i \mapsto b_i$. □

Il est clair sur la définition que pour toute valuation on a $v(\omega) \geqslant 0 \Rightarrow \mathrm{Res}_v(\omega) = 0$. Ainsi la somme $\sum_{v \in C_K} \mathrm{Res}_v(\omega)$ est bien définie.

THÉORÈME. (Théorème des résidus) – *Pour toute $\omega \in \Omega_{K/k}$ on a $\sum_{v \in C_K} \mathrm{Res}_v(\omega) = 0$.*

Démonstration. Traitons d'abord le cas $K = k(t)$ (géométriquement, $C = \mathbb{P}^1$ et $t = \frac{X}{Y}$). Dans ce cas on peut écrire $\omega = f(t)dt$ et $f(t) \in k(t)$ est combinaison k-linéaire de fonctions de la forme $\frac{t^n}{(t-x)^m}$ avec $n, m \in \mathbb{N}$. Comme le résidu est k-linéaire, on peut donc supposer f de cette forme. Alors f a deux pôles possibles : $P = [x : 1]$ et $\infty = [1 : 0]$. On calcule $\mathrm{Res}_P(f) = \binom{n}{m-1} x^{n-m+1} = -\mathrm{Res}_\infty(f)$.

Revenons au cas général et choisissons $t \in K$ telle que K soit séparable sur $k(t)$ (par exemple une uniformisante en un point). Notons $\varphi_t : C_K \longrightarrow \mathbb{P}^1$ le morphisme associé. Il nous suffira de prouver la formule suivante :

$$\forall f \in K, \forall P \in \mathbb{P}^1, \quad \sum_{\varphi_t(v)=P} \mathrm{Res}_v(f dt) = \mathrm{Res}_P(\mathrm{tr}(f)dt),$$

où $\mathrm{tr} = \mathrm{Tr}_{K/k(t)}$ est la trace. En fait, il suffit de le faire pour le point $P = [0 : 1]$ (quitte à ensuite changer t en $t - \lambda$ ou $1/t$). Soit A le normalisé de $k[t]$ dans K. Par passage à la limite projective des isomorphismes $A/t^n A \simeq \prod_{v \mapsto P} \mathcal{O}_v/t^n\mathcal{O}_v$, on obtient que $A \otimes_{k[t]} k[[t]] = \prod_{\varphi_t(v)=P} \hat{\mathcal{O}}_v$. Soit alors $\hat{K}_v = \mathrm{Frac}(\hat{\mathcal{O}}_v)$, on est ramené au problème local suivant :

$$\forall f \in \hat{K}_v, \mathrm{Res}_v(f dt) = \mathrm{Res}_P(\mathrm{tr}_v(f)dt),$$

où tr_v est la trace $\mathrm{Tr}_{\hat{K}_v/k((t))}$. Soit t_v une uniformisante en v, et écrivons $t = t_v^e u$ avec $e = v(t)$ et $u \in \hat{\mathcal{O}}_v^\times = k[[t_v]]^\times$.

Si k est de caractéristique nulle (ou plus généralement si e est inversible dans k), $u = \lambda(1 + t_v g(t_v))$ admet une racine e-ème, donnée par la formule habituelle du développement limité de $(1+x)^{1/e}$. On peut donc modifier notre choix de t_v pour avoir $t_v^e = t$. Dans ce cas, si $f = \sum a_n t_v^n$, on a $f dt = e \sum_n a_n t_v^{n+e-1} dt_v$ d'où l'on tire $\mathrm{Res}_v(f dt) = e a_{-e}$. Par ailleurs, en calculant dans la base $1, t_v, \cdots, t_v^{e-1}$ de $k((t_v))$ sur $k((t))$ on voit que $\mathrm{tr}_v(t_v^n)$ est nul si e ne divise pas n et $\mathrm{tr}_v(t_v^{ne}) = e t^n$. On en tire $\mathrm{Res}_P(\mathrm{tr}_v(f)dt) = e a_{-e}$ comme voulu.

Pour passer à k de caractéristique positive, on procède comme dans la proposition précédente. On note $A = \mathbb{Z}[B_i]_{i \in \mathbb{N}}$ et on travaille dans une extension $A[[t]][t^{-1}] \subset A[[t_v]][t_v^{-1}]$ avec $t = t_v^e u$ et $u = 1 + \sum_i B_i t_v^i$. La formule qu'on veut démontrer est une égalité d'éléments de A, et on a déjà montré cette égalité dans $\mathrm{Frac}(A)$ qui est de caractéristique nulle. □

2.3.4 *Riemann-Roch.* Voici un théorème qui permet de contrôler les dimensions ℓ_D introduites plus haut. Il a de nombreuses applications.

THÉORÈME. – *Soit C une courbe projective lisse. Pour tout $D \in \mathrm{Div}(C)$ on a*

$$\ell_D - \ell_{K_C - D} = \deg(D) + 1 - g(C).$$

Pour la preuve on introduit l'anneau des adèles de $K = k(C)$:

$$\mathbb{A} = \prod_{P\in C}{}' \hat{K}_P := \left\{ (f_P)_{P\in C} \in \prod_{P\in C} \hat{K}_P,\ f_P \in \hat{\mathcal{O}}_P \text{ pour presque tout } P \right\},$$

dans lequel K se plonge diagonalement. Pour toute adèle $(f_P)_P$ et toute forme différentielle $\omega \in \Omega_C$, la somme $\sum_P \mathrm{Res}_P(f_P\omega)$ est finie, et le théorème des résidus dit qu'elle est nulle si $(f_P)_P$ est dans K diagonal. On a donc une forme k-bilinéaire

$$\mathbb{A}/K \times \Omega_K \longrightarrow k, \text{ définie par } \langle (f_P)_P, \omega\rangle = \sum_{P\in C} \mathrm{Res}_P(f_P\omega),$$

que l'on peut voir aussi comme une application k-linéaire $\Omega_K \xrightarrow{\rho} \mathrm{Hom}_k(\mathbb{A}/K, k)$.

Pour un diviseur $D = \sum_P a_P$, on introduit maintenant

$$\mathbb{A}_D := \{(f_P)_P,\ v_P(f_P) + a_P \geqslant 0\} \text{ et } \Omega_D := \{\omega \in \Omega_K,\ \mathrm{div}(\omega) \geqslant D\}.$$

Voici quelques observations :

i) Pour $D \leqslant D'$, on a $\dim_k(\mathbb{A}_{D'}/\mathbb{A}_D) = \deg(D') - \deg(D)$.

ii) $K \cap \mathbb{A}_D = \mathcal{L}_D$.

iii) Pour $D \leqslant D'$, on a $\dim_k((\mathbb{A}_{D'} + K)/(\mathbb{A}_D + K)) = (\deg(D') - \ell_{D'}) - (\deg(D) - \ell_D)$.

iv) $\dim_k(\Omega_D) = \ell_{K_C - D}$. En effet, l'application $\mathcal{L}_{\mathrm{div}(\omega)-D} \longrightarrow \Omega_D$, $f \mapsto f\omega$ est un isomorphisme de k-ev.

v) $\langle \mathbb{A}_D + K, \Omega_D\rangle = 0$, et donc $\rho(\Omega_D) \subset \mathrm{Hom}_k(\mathbb{A}/(\mathbb{A}_D + K), k)$, puisque le résidu d'une fonction régulière est nul.

Le théorème de Riemann-Roch découlera facilement du résultat suivant.

PROPOSITION. – *ρ induit un isomorphisme $\Omega_D \xrightarrow{\sim} \mathrm{Hom}_k(\mathbb{A}/(\mathbb{A}_D + K), k)$.*

Démonstration. Posons $H_D := \mathrm{Hom}_k(\mathbb{A}/(\mathbb{A}_D + K), k)$ et $h_D := \dim_k(H_D)$. Notons que H_D est bien de dimension finie en vertu de la propriété iii) et de la borne sur $\deg(D') - \ell_{D'}$ donnée par la proposition 2.3.1. Montrons que $\rho^{-1}(H_D) = \Omega_D$. En effet, soit ω telle qu'il existe un point Q avec $v_Q(\omega) < a_Q(D)$. Alors pour une adèle $(f_P)_P$ telle que $P \neq Q \Rightarrow f_P = 0$ et $v_Q(f_Q) = -v_Q(\omega_Q) - 1$, on a $\langle (f_P)_P, \omega\rangle \neq 0$ et $(f_P)_P \in \mathbb{A}_D$. Ceci montre aussi que ρ est injective et donc que $h_D \geqslant \ell_{K_C - D}$.

Supposons ρ non surjective et soit $\alpha \in H_D \setminus \rho(\Omega_D)$. Remarquons que via l'action de K sur Ω_K on a $\mathcal{L}(E) \cdot \Omega_D \subset \Omega_{D-E}$ pour tout diviseur E. De même, l'action naturelle de K sur $\mathrm{Hom}_k(\mathbb{A}/K, k)$ vérifie $\mathcal{L}(E) \cdot H_D \subset H_{D-E}$. Ces actions sont compatibles avec ρ (i.e. ρ est K-linéaire), et on en déduit que $\mathcal{L}(E) \cdot \alpha \cap \rho(\Omega_{D-E}) = \{0\}$. Il s'ensuit l'inégalité

$$h_{D-E} \geqslant \ell_E + \ell_{K_C - D + E}.$$

Par ailleurs, si E est positif, l'observation iii) montre que

$$h_{D-E} = h_D + \deg(E) + \ell_{D-E} - \ell_D \leqslant h_D + \deg(E).$$

Mais la proposition 2.3.1 montre que pour $E >> 0$ ces deux inégalités sont contradictoires. □

Fin de la démonstration du théorème de Riemann-Roch. D'après la proposition, on a $\dim_k(\mathbb{A}/(\mathbb{A}_D+K)) = \ell_{K_C-D}$. Pour $D \leqslant D'$, l'égalité $\dim_k(\mathbb{A}/(\mathbb{A}_D+K)) = \dim_k(\mathbb{A}/(\mathbb{A}_{D'}+K)) + \dim_k((\mathbb{A}_{D'}+K)/(\mathbb{A}_D+K))$ s'écrit

$$\ell_{K_C-D} = \ell_{K_C-D'} + (\deg(D') - \ell_{D'}) - (\deg(D) - \ell_D).$$

Ainsi, l'énoncé de Riemann-Roch est vrai pour D si et seulement si il l'est pour D'. En prenant $D' \geqslant 0$, on obtient qu'il est vrai pour D si et seulement si il l'est pour 0. Or, pour 0 il découle de la définition du genre. □

COROLLAIRE. – *i)* $\deg(K_C) = 2g-2$.
ii) $\deg(D) \geqslant 2g-1 \Rightarrow \ell_D = \deg(D)+1-g$.

2.3.5 COROLLAIRE.– *Supposons* $\deg(D) \geqslant 2g+1$. *Alors le morphisme* $C \xrightarrow{\varphi} \mathbb{P}^{\ell_D-1}$ *associé à un choix de base* $f_0, \cdots, f_{\ell_D-1}$ *de* $\mathcal{L}_D$ *(cf section 2.2.3) est une immersion fermée.*

Démonstration. Montrons d'abord qu'avec les notation du lemme 2.2.3, on a $v_P(\mathcal{L}_D) = -a_P(D)$ pour tout $P \in C$. En effet, ceci équivaut à l'inégalité $\ell_{D-[P]} < \ell_D$, laquelle découle du ii) du corollaire ci-dessus (il suffirait même que $\deg(D) \geqslant 2g$).

Ceci étant, la condition i) du lemme équivaut à demander que pour tous $P \neq Q$, on ait l'inégalité $\ell_{D-[Q]} > \ell_{D-[Q]-[P]}$, et la condition ii) équivaut à demander que pour tout P, on ait l'inégalité $\ell_{D-[P]} > \ell_{D-2[P]}$. Ces deux inégalités découlent encore de la formule de Riemmann-Roch (via le ii) du précédent corollaire) sous l'hypothèse $\deg(D) \geqslant 2g+1$. □

Remarque. – La formule de Hurwitz pour un morphisme $\varphi : C \longrightarrow C'$ non constant séparable s'écrit donc $2g_C - 2 = \deg(\varphi)(2g_{C'}-2) + \deg(R_\varphi)$, et se simplifie en $2g_C - 2 = \deg(\varphi)(2g_{C'}-2) + \sum_P (e_P(\varphi)-1)$ si les indices de ramification de φ sont inversibles dans k. Dans tous les cas, on voit que si $g_C < g_{C'}$ alors tout morphisme $C \longrightarrow C'$ est constant.

2.3.6 PROPOSITION.– *Le genre d'une courbe projective plane lisse* $C \subset \mathbb{P}^2$ *de degré* d *est donné par la formule* $g = \frac{(d-1)(d-2)}{2}$.

Démonstration. Supposons $d > 1$ et notons $f \in k[X,Y,Z]$ un polynôme homogène de degré d qui définit C. Soit $O = [X_0 : Y_0 : Z_0]$ un point de $\mathbb{P}^2 \setminus C$ et $L \subset \mathbb{P}^2$ une droite ne contenant pas O. Considérons la projection $\mathbb{P}^2 \setminus \{O\} \longrightarrow L$, $P \mapsto (OP) \cap L$ et restreignons-là à C. On obtient un morphisme $C \xrightarrow{\varphi} L \simeq \mathbb{P}^1$ de degré visiblement égal à d. Pour $P \in C$, on vérifie que $e_P(\varphi)$ est la multiplicité d'intersection (cf TD) de (OP) et C. En particulier, on a donc $e_P(\varphi) > 1$ si et seulement si (OP) est la tangente à C en P, c'est-à-dire si et seulement si P est dans l'intersection de C et de la courbe C' d'équation $\frac{\partial f}{\partial X}X_0 + \frac{\partial f}{\partial Y}Y_0 + \frac{\partial f}{\partial Z}Z_0 = 0$. Mieux, dans ce cas la multiplicité d'intersection de C et C' en P est $\dim_k(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})$ (voir ci-dessous). Par le théorème de Bezout, il s'ensuit donc que $\deg(R_\varphi) = d(d-1)$. La formule de Hurwitz permet alors de conclure.

Pour calculer la multiplicité, on peut supposer après changement de coordonnées que $O = [0:1:0]$, $P = [0:0:1]$ et $L = \{Y + \lambda Z = 0\}$ pour un $\lambda \in k$. Dans ce cas, la projection d'un point de $\mathbb{A}^2 = \{Z \neq 0\}$ depuis O sur L est donnée par $[x:y:1] \mapsto [x:-\lambda:1]$ et x

est donc une uniformisante de $\mathcal{O}_{L,\varphi(P)}$. La condition $e := e_P(\varphi) > 1$ implique alors que y est une uniformisante de $\mathcal{O}_{C,P}$ puisque $\mathfrak{m}_{C,P}$ est engendré par x et y. On peut donc écrire $x = y^e u$ dans $\mathcal{O}_{C,P}$, avec $u \in \mathcal{O}_{C,P}^\times$. Par ailleurs, on peut certainement écrire $f(x, y, 1)$ sous la forme $f(x, y, 1) = xv(x, y) + y^f w(y)$ dans $k[x, y]$ et avec $w(0) \neq 0$. En regardant dans $\mathcal{O}_{C,P}$ et en prenant les valuations, on voit que $f = e + v_P(v(x, y))$, et en particulier $f > 1$. Comme P est régulier, on doit avoir $v(0, 0) \neq 0$ et $f = e$. Il s'ensuit que v est inversible dans $\mathcal{O}_{\mathbb{P}^2,P}$ (tout comme w) et que $u = -wv^{-1}$ dans $\mathcal{O}_{C,P}$. Maintenant, l'équation de C' est $\frac{\partial f}{\partial y}(x, y) = 0$, et la multiplicité de l'intersection de C et C' en P est la dimension sur k de $\mathcal{O}_{C,P}/(\frac{\partial f}{\partial y})$, qui est aussi la valuation de $\frac{\partial f}{\partial y}$ dans $\mathcal{O}_{C,P}$. Or, on a dans $\mathcal{O}_{C,P}$

$$\frac{\partial f}{\partial y} = x\frac{\partial v}{\partial y} + ey^{e-1}w + y^e\frac{\partial w}{\partial y} = v\frac{\partial}{\partial y}(y^e w v^{-1}) = -v\frac{dx}{dy}.$$

On a donc $v_P(\frac{\partial f}{\partial y}) = v_P(\frac{dx}{dy}) = \dim_k(\Omega_{\mathcal{O}_P/\mathcal{O}_{\varphi(P)}})$. □

2.4 Questions de rationnalité et d'inséparabilité

2.4.1 *Rationnalité.* On souhaite étudier les solutions de systèmes d'équations sur un corps k non nécessairement algébriquement clos (par exemple $k = \mathbb{Q}$ ou $\mathbb{F}_p$). Le meilleur cadre pour ce faire est celui des schémas. Néanmoins, lorsque k est parfait, on peut garder le langage classique et l'enrichir d'une action de Galois. Supposons donc k parfait, choisissons une clôture algébrique $\bar{k}$ de k, et notons $G_k := \mathrm{Gal}(\bar{k}/k)$.

Variétés projectives définies sur k. On dit qu'une sous-variété $V(\mathfrak{p}) \subset \mathbb{P}^n_{\bar{k}}$ est *définie sur k* si son idéal $\mathfrak{p}$ est engendré par des polynômes à coefficients dans k, i.e. si on a $\mathfrak{p} = (\mathfrak{p} \cap k[X_i])\bar{k}[X_i]$. Dans ce cas, le sous-ensemble $X = V(\mathfrak{p})$ de $\mathbb{P}(\bar{k})$ est stable sous l'action de G_k et le faisceau des fonctions régulières est aussi muni d'une action semi-linéaire [1] de G_k. En d'autres termes, on a une action de G_k sur le corps des fonctions $\bar{k}(X)$ qui prolonge celle sur $\bar{k}$, et pour tout ouvert $U \subset X$ et tout $\sigma \in G_k$, on a $\sigma(\mathcal{O}(U)) \subset \mathcal{O}(\sigma^{-1}(U))$. On a donc enrichi l'espace $\bar{k}$-annelé $(X, \mathcal{O}_X)$ d'une action de Galois (sur l'espace et sur le faisceau). Notons que cette action est *continue* au sens où tout élément de X ou de $k(X)$ est fixé par un sous-groupe ouvert de G_k (i.e. un sous-groupe de la forme G_ℓ pour une extension finie $\ell \supset k$). Dans la suite, toutes les actions de G_k seront supposées continues.

Variétés sur k. Une variété sur k sera un espace annelé $(X, \mathcal{O}_X)$ muni d'une action de Galois, qui est isomorphe à un ouvert Galois-stable d'une variété projective définie sur k. Un morphisme est ici un morphisme d'espaces $\bar{k}$-annelés compatible aux actions de Galois. Pour une telle variété on définit

$$X(k) := X^{G_k} \text{ et } k(X) := \bar{k}(X)^{G_k}.$$

Dans le cas où $X = V(\mathfrak{p})$ avec $\mathfrak{p}$ idéal premier homogène de $k[X_0, \cdots, X_n]$, on a bien

$$X(k) = \{P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(k),\ \forall f \in \mathfrak{p}, f(P) = 0\}$$

1. Une action semi-linéaire de G_k sur un $\bar{k}$-ev V est une action additive et qui vérifie $\sigma(\lambda v) = \sigma(\lambda)\sigma(v)$ pour tous $\sigma \in G_k$, $\lambda \in \bar{k}$ et $v \in V$.

et on a aussi

$$k(X) = (k[X_0, \cdots, X_n]/\mathfrak{p})_{(0)} \text{ (éléments de degré 0 dans le localisé homogène).}$$

En particulier, on a $\bar{k} \otimes_k k(X) = \bar{k}(X)$. La dimension de X se lit aussi comme le degré de transcendence de $k(X)$ sur k. Pour X une variété sur k, on notera $X_{\bar{k}}$ la variété sur $\bar{k}$ sous-jacente (oubli de l'action de Galois). Si $k \subset \ell \subset \bar{k}$ est une extension intermédiaire, on notera aussi X_ℓ la variété sur ℓ obtenue en restreignant l'action de Galois à $G_\ell \subset G_k$.

Variétés affines sur k. Si A est une k-algèbre de type fini, on dit qu'elle est *géométriquement intègre* si $A_{\bar{k}} := \bar{k} \otimes_k A$ est intègre. Dans ce cas, on voit aisément que $X := \mathrm{Max}(A_{\bar{k}})$, muni de l'action de Galois évidente, est une variété sur k. De plus, on récupère A à partir de X par la formule $A = \mathcal{O}(X)^{G_k}$. On obtient ainsi une anti-équivalence de catégories entre variétés affines sur k et k-algèbres de type fini géométriquement intègres. Plus généralement, si $(X, \mathcal{O})$ est une variété sur k, alors l'application $\mathrm{Hom}_{k-\mathrm{Var}}(X, \mathrm{Max}(A_{\bar{k}})) \longrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(A, \mathcal{O}(X)^{G_K})$ est une bijection. On prendra garde au fait que, en général on a $\mathrm{Max}(A_{\bar{k}})^{G_k} \neq \mathrm{Max}(A)$. En fait, on a une application évidente $\mathrm{Max}(A_{\bar{k}}) \longrightarrow \mathrm{Max}(A)$ et celle-ci identifie $\mathrm{Max}(A)$ à l'ensemble quotient $\mathrm{Max}(A_{\bar{k}})/G_k$. Via cette application, $\mathrm{Max}(A_{\bar{k}})^{G_k}$ s'identifie au sous-ensemble $\{\mathfrak{m} \in \mathrm{Max}(A),\ A/\mathfrak{m} = k\}$ des idéaux maximaux de A de corps résiduel k.

Courbes projectives (géométriquement) lisses sur k. Une courbe $(C, \mathcal{O})$ sur k est dite lisse si elle est lisse comme $\bar{k}$-variété. On laisse le lecteur se convaincre que les constructions de la section ... s'adaptent et fournissent une anti-équivalence de catégories entre courbes lisses sur k munies des morphismes non constants et corps de fonction K de type fini sur k, de degré de transcendance 1, et tels que k soit algébriquement clos dans K (cette condition implique que $K_{\bar{k}} = \bar{k} \otimes_k K$ est un corps. Comme ci-dessus, on prendra garde au fait que l'application de restriction $v \mapsto v_{|K}$ identifie l'ensemble des valuations $K^\times \twoheadrightarrow \mathbb{Z}$ au quotient de $C_{K_{\bar{k}}}$ par G_k, alors que l'ensemble des points rationnels $C(k) = (C_{K_{\bar{k}}})^{G_k}$ correspond aux valuations sur K de corps résiduel k.

Diviseurs rationnels. Soit C une courbe sur k. On a une action de G_k évidente sur $\mathrm{Div}(C)$ et on dit que D est "défini sur k" ou "k-rationnel" s'il est fixe par G_k. Le sous-groupe $\mathrm{Div}_k(C) = \mathrm{Div}(C)^{G_k}$ des diviseurs définis sur k s'identifie au groupe abélien libre de base les G_k-orbites de C. De plus, le sous $\bar{k}$-ev $\mathcal{L}_D$ de $\bar{k}(C)$ associé à un tel diviseur est stable sous l'action de G_k.

LEMME. (Hilbert 90) – *Soit D un diviseur k-rationnel. Alors $\mathcal{L}_D$ admet une base formée de fonctions dans $k(C)$.*

Démonstration. Plus généralement, si V est un $\bar{k}$-ev muni d'une action semi-linéaire continue de G_k, alors l'application $\bar{k}$-linéaire

$$\bar{k} \otimes_k V^{G_k} \longrightarrow V,\ \lambda \otimes v \mapsto \lambda v$$

est un isomorphisme de $\bar{k}$-ev.

Montrons d'abord que toute famille k-libre de V^{G_k} est aussi $\bar{k}$-libre dans V, ce qui assurera l'injectivité de l'application ci-dessus. Soit donc $v_1, \cdots, v_n \in V^{G_k}$ et $\lambda_1, \cdots, \lambda_n \in \bar{k}$ tels que $\sum_i \lambda_i v_i = 0$, avec disons $\lambda_j \neq 0$ pour au moins un j. Si $\ell \supset k$ désigne une extension finie contenant les λ_i, on sait qu'il existe $x \in \ell$ tel que $\mathrm{Tr}_{\ell/k}(x\lambda_j) \neq 0$ (puisque ℓ est séparable sur k). On en déduit une relation de dépendance non triviale à coefficients dans k :

$$\sum_{\sigma \in \mathrm{Gal}(\ell/k)} \sigma\left(\sum_i x\lambda_i v_i\right) = \sum_i \mathrm{Tr}_{\ell/k}(\lambda_i x) v_i = 0.$$

Montrons maintenant que V^{G_k} engendre V linéairement sur $\bar{k}$, ce qui assurera la surjectivité de l'application ci-dessus. Pour $v \in V \setminus \{0\}$, notons V_v le $\bar{k}$-sev de V engendré par l'orbite de v, qui est stable sous G_k. Si on montre que $V_v^{G_k}$ engendre V_v pour tout v, on aura gagné. Pour cela, soit ℓ une extension finie Galoisienne de k telle que v soit fixe par G_ℓ. Soit $\lambda_1, \cdots, \lambda_n$ une k-base de ℓ et soit $\sigma_1, \cdots, \sigma_n$ une énumération de $\mathrm{Gal}(\ell/k)$. On sait que la matrice $(\sigma_j(\lambda_i))_{i,j}$ est inversible. Puisque V_v est $\bar{k}$-linéairement engendré par les $\sigma_i(v)$, il l'est donc aussi par les $\sum_j \sigma_j(\lambda_i)\sigma_j(v) = \sum_{\sigma \in \mathrm{Gal}(\ell/k)} \sigma(\lambda_i v)$, lesquels sont bien fixes par G_k. □

2.4.2 Corollaire. (Plongements projectifs définis sur k.)– *Soit C une courbe projective lisse définie sur k, et D un diviseur défini sur k. Supposons* $\deg(D) \geqslant 2g+1$. *Alors le morphisme $C \longrightarrow \mathbb{P}^n$ associé à un choix de k-base $f_0, \cdots, f_{\ell_D - 1}$ de $\mathcal{L}_D \cap k(C)$ est une immersion fermée définie sur k.*

Démonstration. Découle du lemme et du corollaire 2.3.5. □

2.4.3 *Inséparabilité.* On suppose ici que k est de caractéristique $p > 0$, mais *toujours parfait*. Si q est une puissance de p, l'application $a \mapsto a^q$ définit un endomorphisme de n'importe quelle k-algèbre A. On note A^q l'image de cet endomorphisme.

Lemme. – *Soit $K' \subset K$ une extension purement inséparable de degré q de corps de fonctions de courbes sur k. Alors $K' = K^q$.*

Démonstration. Notons que q est nécessairement une puissance de p, disons $q = p^r$. De plus, on a $K^q \subset K'$ puisque le polynôme minimal sur K' d'un élément de K est de la forme $X^{q'} - f$ avec $f \in K'$ et $q'|q$. Il nous suffira donc de montrer que $[K : K^q] = q$. Puisque k est parfait, il est contenu dans K^q et $\bar{k} \otimes_k K^q = (\bar{k} \otimes_k K)^q$. On peut donc étendre les scalaires à $\bar{k}$, ce qui nous ramène au cas $k = \bar{k}$. Dans ce cas, soit $t \in K$ une uniformisante pour une valuation $v \in C_K$. On sait que l'extension $K \supset k(t)$ est séparable. Donc K est une extension à la fois séparable et inséparable du corps composé $K^q(t)$ et, par conséquent, $K = K^q(t)$. Le degré $[K : K^q]$ est donc le degré du polynôme minimal de t sur K^q, c'est-à-dire le plus petit $q'|q$ tel que $t^{q'} \in K^q$. Or on a $v(t^{q'}) = q'$ et $q|v(f)$ pour tout $f \in K^q$. Donc $q' = q$. □

Corollaire. – *Soit $C \xrightarrow{\varphi} C'$ un morphisme purement inséparable de courbes projectives lisses. Alors φ est un homéomorphisme et $g(C) = g(C')$.*

Démonstration. Identifions $\varphi^*(k(C'))$ à $k(C)^q$. Alors, en termes de valuations, φ s'identifie à l'application $v \mapsto \frac{1}{q} v_{|k(C)^q}$ qui est visiblement une bijection, et donc un homéomorphisme, dont l'inverse est $w \mapsto w \circ (-)^q$. L'application $\Omega_{C'} \xrightarrow{\varphi^*} \Omega_C$ est nulle mais l'isomorphisme dans l'autre sens $k(C) \xrightarrow{\sim} k(C)^q$, $f \mapsto f^q$ induit un isomorphisme $k(C)^q \otimes_{k(C)} \Omega_{k(C)/k} \xrightarrow{\sim} \Omega_{k(C)^q/k}$ qu'on note $\omega \mapsto \omega^{(q)}$. On voit que pour tout $P \in C$, on a $v_P(\omega) = v_{\varphi(P)}(\omega^{(q)})$, et on en déduit que l'isomorphisme précédent respecte la régularité des formes différentielles. Il s'ensuit que $g(C') = g(C)$. □

Soit C une courbe projective lisse sur k. On notera $C^{(q)}$ la courbe de corps $k(C)^q$. On a donc un morphisme $C \longrightarrow C^{(q)}$ purement inséparable de degré q, et le lemme nous dit que tout morphisme inséparable de degré q est de cette forme à isomorphisme près. Notons que l'isomorphisme de corps $k(C) \xrightarrow{\sim} k(C)^q$, $f \mapsto f^q$ est $(k, (-)^q)$-semi-linéaire. Il induit donc un morphisme de k-extensions

$$k \otimes_{k,(-)^q} k(C) \xrightarrow{\sim} k(C)^q,$$

qui montre que $C^{(q)}$ est aussi la courbe déduite de C par "extension" des scalaire via $\lambda \mapsto \lambda^q$.

Remarque. – Sur un corps non parfait, c'est de cette manière que l'on définit $C^{(q)}$.

Exercice. – Supposons que $C = V(\mathfrak{p}) \subset \mathbb{P}^n$. Montrer que $C^{(q)} = V(\mathfrak{p}^{(q)})$ où $\mathfrak{p}^{(q)}$ est l'image de $\mathfrak{p}$ par $k[X_0, \cdots, X_n] \longrightarrow k[X_0, \cdots, X_n]$, $X_i \mapsto X_i$, $\lambda \mapsto \lambda^q$. Montrer aussi que le morphisme $C \longrightarrow C^{(q)}$ est donné par $[x_0 : \cdots : x_n] \mapsto [x_0^q : \cdots : x_n^q]$.

Exemple. – Supposons que $k = \mathbb{F}_q$. Dans ce cas, l'isomorphisme de corps $(-)^q : k(C) \xrightarrow{\sim} k(C)^q$ est k-linéaire, et fournit donc un isomorphisme de courbes $C^{(q)} \xrightarrow{\sim} C$ défini sur k. En composant avec le morphisme $C \longrightarrow C^{(q)}$, on obtient un endomorphisme ϕ_q défini sur k de la courbe C, appelé *endomorphisme de Frobenius*. Les points fixes de cet endomorphisme dans $C(\bar{\mathbb{F}}_q)$ sont aussi les points fixes sous $G_{\mathbb{F}_q}$, c'est-à-dire les points rationnels $C(\mathbb{F}_q)$.

2.4.4 Corollaire.– *Si $g(C) < g(C')$, tout morphisme $C \longrightarrow C'$ est constant.*

Démonstration. Soit $C \xrightarrow{\varphi} C'$ un morphisme non constant, et soit q son degré inséparable. On a donc une extension séparable $\varphi^*(k(C')) \subset k(C)^q$ qui nous fournit une factorisation $\varphi : C \longrightarrow C^{(q)} \xrightarrow{\varphi_s} C'$ avec φ_s séparable. Or, $g(C^{(q)}) = g(C)$, donc la formule de Hurwitz et l'effectivité du diviseur de ramification R_{φ_s} impliquent $g(C) \geqslant 1 + \deg(\varphi_s)(g(C') - 1)$. □

3 Courbes elliptiques

Le corps de base k est supposé parfait, et on en fixe une clôture algébrique $\bar{k}$.

Définition. – *Une courbe elliptique sur k est une courbe projective lisse $\mathcal{E}$ de genre 1 définie sur k et munie d'un point k-rationnel O.*

D'après la proposition 2.3.6, une cubique plane lisse est de genre 1. Si elle est définie sur k et possède un point rationnel, c'est donc une courbe elliptique.

3.1 Loi de groupe.

On rappelle que $\mathrm{Pic}^0(C)$ désigne le quotient de $\mathrm{Div}^0(C)$ (diviseurs de degré 0) par $\mathrm{div}(\bar{k}(C)^\times)$ (diviseurs principaux).

3.1.1 Proposition.– *Soit $(\mathcal{E}, O)$ une courbe elliptique. L'application d'Abel-Jacobi*

$$\mathcal{E} \longrightarrow \mathrm{Pic}^0(\mathcal{E}),\ P \mapsto \overline{[P] - |O]}$$

est une bijection G_k-équivariante.

Démonstration. L'application est clairement G_k-équivariante puisque O est fixe par G_k.

i) injectivité. Supposons $\overline{[P] - [Q]} = 0$. Il existe donc $f \in \bar{k}(\mathcal{E})^\times$ telle que $[P] - [Q] = \mathrm{div}(f)$. En particulier, $f \in \mathcal{L}_{[Q]}$. Or, par Riemann-Roch, on a $\ell_{[Q]} = 1$ et comme $k \subset \mathcal{L}_{[Q]}$, on en déduit que f est constante. On a donc $[P] - [Q] = 0$, d'où $P = Q$.

ii) surjectivité. Soit D un diviseur de degré 0. Par Riemann-Roch on a $\ell_{[O]+D} = 1$. Soit donc $f \in \mathcal{L}_{[O]+D}$ non nulle. On a $\mathrm{div}(f) + D + [O] \geqslant 0$ et $\deg(\mathrm{div}(f) + D + [O]) = 1$, donc il existe un point P tel que $\mathrm{div}(f) + D + [O] = [P]$. D'où $\overline{D} = \overline{[P] - [O]}$ dans $\mathrm{Pic}^0(\mathcal{E})$. □

Puisque $\mathrm{Pic}^0(\mathcal{E})$ est un groupe abélien, on peut munir $\mathcal{E}$ de la structure de groupe abélien transportée via la bijection d'Abel-Jacobi. Cette loi est compatible à l'action de Galois. Par construction, l'élément neutre est O et la somme et la multiplication par $n \in \mathbb{Z}$ sont caractérisées par les congruences suivantes modulo les diviseurs principaux :

$$[P + Q] \sim [P] + [Q] - [O], \quad [nP] \sim n[P] - (n-1)[O].$$

Notre définition est a priori ensembliste.

3.1.2 Lemme.– *L'application inverse $\mathcal{E} \longrightarrow \mathcal{E}$, $R \mapsto -R$ est sous-jacente à un automorphisme involutif et défini sur k de la variété $\mathcal{E}$. De plus, pour tout $Q \in \mathcal{E}$, l'application de translation $t_Q : \mathcal{E} \longrightarrow \mathcal{E}$, $R \mapsto R + Q$ est sous-jacente à un automorphisme de variétés, qui est défini sur k si Q l'est.*

Démonstration. Nous commençons par la remarque suivante. Si P et Q sont deux points de $\mathcal{E}$ éventuellement égaux, Riemann-Roch assure que $\mathcal{L}_{[P]+[Q]}$ contient une fonction $f \in \bar{k}(\mathcal{E})^\times$ non constante. Soit $\varphi_f : \mathcal{E} \longrightarrow \mathbb{P}^1$ le morphisme associé. Puisque $\mathcal{L}_{[P]} = \mathcal{L}_{[Q]} = k$, on a $\varphi_f^*([\infty]) = [P] + [Q]$ donc φ_f est de degré 2. Notons que l'extension $\bar{k}(\mathcal{E}) \supset \bar{k}(f)$ est séparable, sinon on aurait $\bar{k}(\mathcal{E}) = \bar{k}(f^{1/2})$ et $\mathcal{E} \simeq \mathbb{P}^1$. Cette extension est donc Galoisienne ; notons $\sigma_{P,Q}^*$ l'élément non trivial de $\mathrm{Gal}(\bar{k}(\mathcal{E})/\bar{k}(f))$. Puisque $\mathcal{E}$ est projective lisse, il existe un unique automorphisme involutif $\sigma = \sigma_{P,Q}$ de la variété $\mathcal{E}$ qui induit $\sigma_{P,Q}^*$ sur $\bar{k}(\mathcal{E})$. On a $\varphi_f \circ \sigma = \varphi_f$ donc les fibres de φ_f sont stables sous σ. Mieux, *l'action de σ sur chaque fibre est transitive* [cf exercice ci-dessous pour un énoncé plus général] : en effet, supposons

$\varphi_f^{-1}(R) = \{R, S\}$ avec $R \neq S$ et fixons $r \in \bar{k}(\mathcal{E})$ telle que $v_R(r) = 1$ et $v_S(r) = 0$. Si $\sigma(R) = R$ alors $v_R(\sigma(r)) = 1$ et $v_S(\sigma(r)) = 0$, et donc $v_R(r\sigma(r)) = 2$ et $v_S(r\sigma(r)) = 0$, ce qui est absurde car $r\sigma(r) \in \bar{k}(\mathcal{E})^\sigma$ donc $v_{\varphi_f(R)}(r\sigma(r)) = e_R(\varphi_f)^{-1} v_R(r\sigma(r)) = e_S(\varphi_f)^{-1} v_S(r\sigma(r))$.

En particulier, on a $\sigma(P) = Q$ et, pour tout $R \in C$, on a $\varphi_f^*[\varphi_f(R)] = [R] + [\sigma(R)]$. Si $R \neq P, Q$ on a donc $[R] + [\sigma(R)] = [P] + [Q] + \mathrm{div}(f - f(R))$, et dans tous les cas on a

$$(*) \quad [R] + [\sigma_{P,Q}(R)] \sim [P] + [Q].$$

Notons que pour tout $\tau \in G_k$ on a $\tau(\sigma_{P,Q}(R)) = \sigma_{\tau(P),\tau(Q)}(\tau(R))$, donc en particulier si P et Q sont k-rationnels alors $\sigma_{P,Q}$ est défini sur k.

Appliquons maintenant ceci à $P = Q = O$. L'égalité $(*)$ nous dit que $\sigma_{O,O}(R) = -R$, donc l'inverse est donnée par l'automorphisme $\sigma_{O,O}$ qui est défini sur k. Appliquons ensuite à $P = O$ et Q un point comme dans l'énoncé. Alors l'égalité $(*)$ dit que $\sigma_{O,Q}(R) = Q - R = -t_{-Q}(R)$, et il s'ensuit que l'application t_Q est sous-jacente au morphisme $\sigma_{O,O} \circ \sigma_{O,Q} \circ \sigma_{O,O}$, lequel est bien défini sur k si Q est k-rationnel. □

Exercice. – Soit $K \supset K'$ une extension Galoisienne de corps de fonctions de courbes, et $C \xrightarrow{\varphi} C'$ le morphisme de courbes projectives lisses correspondant. La correspondance entre courbes et corps de fonctions fournit une action de $\mathrm{Gal}(K/K')$ sur C par automorphismes de variétés.

i) Montrer que les fibres de φ sont les $\mathrm{Gal}(K/K')$-orbites dans C.

ii) Montrer plus précisément $\varphi^*[\varphi(P)] = \sum_{\sigma \in \mathrm{Gal}(K/K')} \sigma^*[P] = \sum_{\sigma \in \mathrm{Gal}(K/K')} [\sigma^{-1}(P)]$.

iii) En déduire que l'indice de ramification est constant sur les fibres, et divise $\deg(\varphi)$.

Nous aimerions aussi montrer que la somme $\mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ est un morphisme de variétés. Pour cela, nous faisons le lien avec la loi de groupe introduite au début de ce cours.

3.1.3 Théorème.– *i) Soit $(\mathcal{E}, O)$ une courbe elliptique sur k. Il existe un plongement $\iota : \mathcal{E} \hookrightarrow \mathbb{P}^2$ défini sur k dont l'image est la courbe définie par une équation de Weierstrass*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

et qui envoie le point O sur le point $[0 : 1 : 0]$.

ii) Tout autre tel plongement s'obtient en composant ι avec un changement de coordonnées linéaire $\mathbb{P}^2 \longrightarrow \mathbb{P}^2$ donné par une matrice de la forme $\begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}$. En d'autres termes, deux équations de Weierstrass définissent des courbes elliptiques isomorphes si et seulement si elles se déduisent l'une de l'autre par un changement de coordonnées $x' = u^2x + r$, $y' = u^3y + u^2sx + t$.

iii) Pour $P, Q, R \in \mathcal{E}$, on a $P+Q+R = O$ si et seulement si il existe une droite $L \subset \mathbb{P}^2$ telle que $[L \cap \iota(\mathcal{E})] = [\iota(P)] + [\iota(Q)] + [\iota(R)]$. (Ici $[L \cap \iota(\mathcal{E})]$ désigne le diviseur des points d'intersection de L et $\iota(\mathcal{E})$ comptés avec multiplicités).

Démonstration. i) Puisque O est un point k-rationnel, le diviseur $3[O]$ est défini sur k. Son degré $\deg(3[O]) = 3$ étant $\geqslant 2g+1$, on sait que tout choix de k-base de $\mathcal{L}_{3[O]}$ fournit un plongement dans $\mathbb{P}^{\ell_{3[O]}-1}$. Or, d'après Riemann-Roch on a $\ell_{3[O]} = 3$, et aussi $\ell_{2[O]} = 2$. Choisissons une k-base $\{1, x, y\}$ de $\mathcal{L}_{3[O]}$ telle que $\{1, x\}$ soit une base de $\mathcal{L}_{2[O]}$. On a donc une immersion fermée $\iota_{x,y} : \mathcal{E} \longrightarrow \mathbb{P}^2$. Pour en calculer une équation, on remarque que la famille de 7 fonctions $\{y^2, x^3, yx, x^2, y, x, 1\}$ vit dans $\mathcal{L}_{6[O]}$ qui est de dimension 6. Cette famille est donc k-linéairement liée. Par ailleurs, les familles obtenues en retirant y^2 ou x^3 sont libres, puisque ayant des pôles d'ordre distinct en O. Toute relation de dépendance linéaire non triviale doit donc avoir un coefficient non nul en y^2 et en x^3. En remplaçant x et y par des multiples convenables, on obtient une relation de dépendance sous forme de Weierstrass. Ainsi $\iota_{x,y}(\mathcal{E})$ est contenue dans une cubique de Weierstrass C. Comme $\iota_{x,y}(\mathcal{E})$ ne peut pas être une conique ni une droite (genre 0), on doit avoir $\iota_{x,y}(\mathcal{E}) = C$. Enfin, remarquons que O est envoyé sur un pôle de $x = X/Z$ et $y = Y/Z$, donc sur un point de la droite $\{Z = 0\}$, mais $[0 : 1 : 0]$ est le seul point de $C \cap \{Z = 0\}$.

ii) Réciproquement, si $\iota : \mathcal{E} \hookrightarrow \mathbb{P}^2$ est un plongement sur une cubique de Weierstrass envoyant O sur $[0 : 1 : 0]$, alors les fonctions $x' = \iota^*(X/Z)$ et $y' = \iota^*(Y/Z)$ forment une autre base $\{1, x', y'\}$ de $\mathcal{L}_{3[O]}$ telle que $x' \in \mathcal{L}_{2[O]}$. On peut donc écrire $x' = \lambda x + r$ et $y' = \mu y + sx + t$. Pour que les coefficients de x'^3 et $y'3$ soient égaux, on doit avoir $\mu^2 = \lambda^3$ et donc $\mu = u^3$ et $\lambda = u^2$ pour $u := \mu\lambda^{-1}$.

iii) Supposons $P+Q+R = O$. Alors il existe $f \in \bar{k}(\mathcal{E})^\times$ telle que $[P]+[Q]+[R]-3[O] = \mathrm{div}(f)$. Une telle fonction f s'annule en P, Q, R et est dans $\mathcal{L}_{3[O]}$ donc s'écrit $f = ax+by+c$. Soit alors $L \subset \mathbb{P}^2$ la droite d'équation $aX + bY + cZ = 0$. Pour calculer le diviseur intersection $[L \cap \iota(\mathcal{E})]$ on remarque que si S est un point de $\mathcal{E} \setminus \{O\}$, alors on calcule dans les coordonnées affines (x, y) que $\mathrm{mult}_{\iota(S)}(L \cap \iota(\mathcal{E})) = v_S(f)$, tandis que pour $S = O$, on voit dans les coordonnées affines $(\frac{X}{Y}, \frac{Z}{Y})$ que $\mathrm{mult}_{\iota(O)}(L \cap \iota(\mathcal{E})) = v_O(fy^{-1}) = v_O(f) + 3$. Il s'ensuit que

$$\iota^*[L \cap \iota(\mathcal{E})] = \sum_{S \in \mathcal{E}} v_S(f)[S] + 3[O] = \mathrm{div}(f) + 3[O] = [P] + [Q] + [R].$$

Réciproquement, soit L la droite d'équation $aX + bY + cZ = 0$ et posons $f := ax + by + c$ vue comme fonction rationnelle sur E. Comme ci-dessus, on a $\iota^*[L \cap \iota(\mathcal{E})] = \mathrm{div}(f) + 3[O]$. Par ailleurs, on sait que $[L \cap \iota(\mathcal{E})]$ est de la forme $[\iota(P)] + [\iota(Q)] + [\iota(R)]$ (forme facile de Bézout), donc on a l'égalité $\mathrm{div}(f) = [P]+[Q]+[R]-3[O]$ qui assure que $P+Q+R = O$. □

3.1.4 Corollaire.– *La loi de groupe $\mathcal{E} \times \mathcal{E} \xrightarrow{\mu_\mathcal{E}} \mathcal{E}$ est un morphisme de k-variétés.*

Démonstration. Choisissons un plongement de Weierstraß de $\mathcal{E}$ comme dans le i) du théorème et identifions $\mathcal{E} = \iota(\mathcal{E})$. L'ensemble

$$U := \{(P, Q) \in \mathcal{E} \setminus \{O\} \times \mathcal{E} \setminus \{O\},\ P \neq \pm Q\}$$

est un ouvert de $\mathcal{E} \times \mathcal{E}$ puisqu'on sait que $R \mapsto -R$ est un morphisme. Si $(P, Q) \in U$ alors $P \neq Q$ donc la droite (PQ) est bien définie et, par le iii) du théorème, $-(P + Q)$ est le

"troisième" point d'intersection de $(QP) \cap \mathcal{E}$, formellement défini par

$$[-(P+Q)] = [(QP) \cap \mathcal{E}] - [P] - [Q].$$

De plus, on a $P, Q \in \{Z \neq 0\} \subset \mathbb{P}^2$ et, puisque $P \neq (-Q)$, on a aussi $-(P+Q) \in \{Z \neq 0\}$. Ecrivons tout point $R \in \{Z \neq 0\}$ sous la forme $[x(R) : y(R) : 1]$. Alors la droite (PQ) a pour équation $aX + bY + cZ = 0$ avec

$$a = y(P) - y(Q),\ b = x(Q) - x(P),\ c = x(Q)y(P) - x(P)y(Q).$$

Puisque $O \notin (PQ)$ on a $b \neq 0$. En remplaçant y par $-b^{-1}ax - b^{-1}c$ dans l'équation de Weierstraß affine de $\mathcal{E}$, on obtient un polynôme de degré 3 en x

$$x^3 + (a_2 - b^{-2}a^2 + a_1b^{-1}a)x^2 + \text{ termes de degré } \leqslant 1$$

dont les trois racines sont $x(P)$, $x(Q)$ et $x(-(P+Q))$. En particulier on a

$$x(P+Q) = x(-(P+Q)) = -a_2 + \frac{(y(P)-y(Q))^2}{(x(P)-x(Q))^2} + a_1\frac{y(P)-y(Q)}{x(P)-x(Q)} - x(P) - x(Q),$$

d'où l'on tire ensuite

$$y(-(P+Q)) = \frac{y(P)-y(Q)}{x(P)-x(Q)}x(P+Q) - \frac{y(P)x(Q)-y(Q)x(P)}{x(P)-x(Q)}$$

puis, en utilisant le fait que $y(P+Q)$ et $y(-(P+Q))$ sont racines d'un trinôme $y^2 + (a_1x(P+Q)+a_3)y + c$

$$y(P+Q) = -\left(a_1 + \frac{y(P)-y(Q)}{x(P)-x(Q)}\right)x(P+Q) - a_3 + \frac{y(P)x(Q)-y(Q)x(P)}{x(P)-x(Q)}.$$

Il est maintenant clair que les fonctions $(P,Q) \mapsto x(P+Q)$ et $(P,Q) \mapsto y(P+Q)$ sont des fonctions régulières sur U et donc, l'application $(P,Q) \mapsto P+Q$ est un morphisme $\oplus$ de $U \times U$ dans $\mathcal{E}$.

Maintenant, rappelons les morphismes de translation t_R du lemme 3.1.2. En observant que $P + Q = t_{-R}(t_R(P) + Q)$, on constate que l'addition est donnée par le morphisme $t_{-R} \circ \oplus \circ (t_R \times \mathrm{id})$ sur l'ouvert $V_R := (t_R \times \mathrm{id})^{-1}(U)$. Puisque les V_R recouvrent $\mathcal{E} \times \mathcal{E}$, on en conclut que l'addition est donnée par un morphisme sur $\mathcal{E} \times \mathcal{E}$. □

Remarque. – L'associativité de l'addition sur $\mathcal{E}$ se traduit par l'égalité $\mu_\mathcal{E} \circ (\mu_\mathcal{E} \times \mathrm{id}) = \mu_\mathcal{E} \circ (\mathrm{id} \times \mathcal{E}) : \mathcal{E} \times \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$, et le fait que l'inverse soit donné par un morphisme $[-] : \mathcal{E} \longrightarrow \mathcal{E}$ se traduit par $\mu_\mathcal{E} \circ (\mathrm{id} \times [-]) = \mu_\mathcal{E} \circ ([-] \times \mathrm{id}) = \mathrm{id} : \mathcal{E} \longrightarrow \mathcal{E}$. Il s'ensuit que pour toute variété sur k (ou $\bar{k}$), les ensembles $\mathrm{Hom}_{k-\mathrm{Var}}(Y, \mathcal{E})$ (ou $\mathrm{Hom}_{\bar{k}-\mathrm{Var}}(Y, \mathcal{E})$) sont naturellement munis de structures de groupe abéliens, définies par $\varphi + \psi := \mu_\mathcal{E} \circ (\varphi, \psi)$.

3.2 Morphismes et isogénies

3.2.1 LEMME.– *Soient $(\mathcal{E}, O)$ et $(\mathcal{E}', O')$ deux courbes elliptiques, et soit $\varphi : \mathcal{E} \longrightarrow \mathcal{E}'$ un morphisme de variétés.*

i) Si φ est non constant, alors $e_P(\varphi) = \deg_i(\varphi)$ pour tout $P \in \mathcal{E}$.

ii) Si $\varphi(O) = O'$ alors φ est un morphisme de groupes, et $\mu_{\mathcal{E}'} \circ (\varphi \times \varphi) = \varphi \circ \mu_{\mathcal{E}}$.

Démonstration. i) Si φ est non constant séparable, la formule de Hurwitz nous assure que $\deg(R_\varphi) = 0$. Or, le diviseur de ramification R_φ est effectif, donc il est nul. En général, on factorise $\varphi = \psi \circ \phi_q$ avec ψ séparable et ϕ_q le morphisme de Frobenius $\mathcal{E} \longrightarrow \mathcal{E}^{(q)}$ associé à $q = \deg_i(\varphi)$. Celui-ci est partout ramifié d'indice q.

ii) Le morphisme φ induit un homomorphisme de groupes abéliens $\varphi_* : \mathrm{Div}(\mathcal{E}) \longrightarrow \mathrm{Div}(\mathcal{E}')$. On laisse en exercice le fait que pour toute fonction $f \in k(\mathcal{E})^\times$ on a $\varphi_*(\mathrm{div}(f)) = \mathrm{div}(N_{k(\mathcal{E})|k(\mathcal{E}')}f)$, ce qui montre que φ_* passe au quotient $\mathrm{Pic}(\mathcal{E}) \longrightarrow \mathrm{Pic}(\mathcal{E}')$. Mais alors, l'égalité $\varphi_*([P]-[O]) = [\varphi(P)]-[O']$ et la définition des lois de groupe sur $\mathcal{E}$ et $\mathcal{E}'$ montrent que φ est un morphisme de groupes. En particulier les deux morphismes $\mu_{\mathcal{E}'} \circ (\varphi \times \varphi)$ et $\varphi \circ \mu_{\mathcal{E}}$, $\mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}'$ coïncident sur les espaces topologiques sous-jacents, donc sont égaux. □

DÉFINITION. – *Un* morphisme de courbes elliptiques $(\mathcal{E}, O) \xrightarrow{\varphi} (\mathcal{E}', O')$ *est un morphisme de variétés $\mathcal{E} \longrightarrow \mathcal{E}'$ tel que $\varphi(O) = O'$. Une* isogénie *est un morphisme de courbes elliptiques non constant. Les morphismes forment un groupe abélien* $\mathrm{Hom}(\mathcal{E}, \mathcal{E}')$ *via l'addition $(\varphi + \psi)(P) := \varphi(P) +_{\mathcal{E}'} \psi(P)$, et les endomorphismes forment un anneau* $\mathrm{End}(\mathcal{E})$ *avec pour produit la composition.*

Notons qu'une composition d'isogénies est une isogénie.

Remarque. – Le fait qu'un endomorphisme non nul de $(\mathcal{E}, O)$ est surjectif montre que l'anneau $\mathrm{End}(\mathcal{E})$ est sans diviseur de zéro.

D'après le lemme 3.2.1 i), le noyau $\mathrm{Ker}\,\varphi = \varphi^{-1}(O')$ d'une isogénie est un sous-groupe de $\mathcal{E}$ d'ordre $\deg_s(\varphi)$ (le degré séparable). L'action par translation de $\mathrm{Ker}\,\varphi$ sur $\mathcal{E}$ induit une action par automorphismes de corps sur $\bar{k}(\mathcal{E})$, et $\varphi^*(\bar{k}(\mathcal{E}')) \subset \bar{k}(\mathcal{E})^{\mathrm{Ker}\varphi}$. Lorsque φ est séparable, cette inclusion est une égalité pour des raisons de degré. Dans ce cas, $\bar{k}(\mathcal{E})$ est une extension Galoisienne de $\bar{k}(\mathcal{E}')$ de groupe $\mathrm{Ker}\,\varphi$. Réciproquement, on a le résultat suivant.

LEMME. – *Soit $\Gamma \subset \mathcal{E}$ un sous-groupe fini. Alors Γ est le noyau d'une isogénie $\mathcal{E} \xrightarrow{\varphi} \mathcal{E}'$.*

Démonstration. La théorie de Galois nous dit que $\bar{k}(\mathcal{E})$ est Galoisienne de groupe Γ sur le sous-corps $\bar{k}(\mathcal{E})^\Gamma$. En particulier, ce dernier a pour degré de transcendance 1 sur $\bar{k}$, donc est le corps de fonctions d'une courbe projective lisse C. De plus, l'inclusion de corps provient d'un morphisme $\mathcal{E} \xrightarrow{\varphi} C$ de degré $|\Gamma|$. Montrons que φ est constante sur les Γ-orbites dans $\mathcal{E}$. En effet, si $\varphi(\gamma + P) \neq \varphi(P)$ alors on peut trouver $f \in \bar{k}(C)$ avec un pôle en $\varphi(P)$ et sans pôle en $\varphi(\gamma + P)$. Alors f, vue comme fonction sur $\mathcal{E}$, aurait un pôle en P mais pas en $\gamma + P$, ce qui est absurde puique f est Γ-invariante. Cela implique que les fibres

de φ sont de cardinal $|\Gamma|$ et, par conséquent, que φ est non ramifiée. Mais alors la formule de Hurwitz assure que $g(C) = 1$. En posant $O' := \varphi(O)$, on a donc une courbe elliptique (C, O') munie d'une isogénie $\mathcal{E} \xrightarrow{\varphi} C$ de noyau Γ. □

3.2.2 *La multiplication par m.* C'est l'exemple fondamental d'isogénie (si $m \neq 0$). On la notera $[m]$ ou $[m]_{\mathcal{E}}$. Mais encore faut-il prouver qu'elle est non-constante ! Il suffit de le faire pour m premier. Si m est impair et qu'on connait l'existence d'un point P d'ordre 2 (i.e $2P = O$ et $P \neq O$), alors $mP = P$ donc P et O sont dans l'image de $[m]$ qui n'est pas constante. Voici comment prouver que $\mathcal{E}$ possède un point d'ordre 2 lorsque $\mathrm{car}(k) \neq 2$. On considère le morphisme $\mathcal{E} \longrightarrow \mathbb{P}^1$ donné par $x \in \mathcal{L}_{2[O]} \setminus \bar{k}$, qui est de degré 2 et dont les fibres sont les $\{P, -P\}$, pour $P \in \mathcal{E}$. Ce morphisme est séparable et, si $\mathrm{car}(k) \neq 2$, ses indices de ramifications 1 ou 2 sont inversibles dans k, donc la formule de Hurwitz montre qu'il y a exactement 4 points de ramifications, i.e. 4 points tels que $P = -P$. Cela montre aussi que $[2]$ n'est pas constante, au moins lorsque $\mathrm{car}(k) \neq 2$. On a donc prouvé

Proposition. – *Si* $\mathrm{car}(k) \neq 2$, *alors* $[m]_{\mathcal{E}}$ *est une isogénie.*

Ce résultat est encore vrai en caractéristique 2, comme on le verra sous (3.3.2).

Remarque. – Le fait que $[m]_{\mathcal{E}}$ soit une isogénie pour tout m équivaut à l'injectivité du morphisme d'anneaux $\mathbb{Z} \longrightarrow \mathrm{End}(\mathcal{E})$.

On note $\mathcal{E}[m] := \mathrm{Ker}\,[m]_{\mathcal{E}}$ et on l'appelle le *sous-groupe de m-torsion* de $\mathcal{E}$. Comme $[m]_{\mathcal{E}}$ est définie sur k, ce sous-groupe est stable sous G_k. Si l'on pense au cas complexe $k = \mathbb{C}$ où l'on sait qu'une courbe elliptique est, en tant que surface de Riemann, isomorphe à $\mathbb{C}/\Lambda$ avec Λ un réseau cocompact de $\mathbb{C}$, alors on voit que $\mathcal{E}[m] = \frac{1}{m}\Lambda/\Lambda \simeq (\mathbb{Z}/m\mathbb{Z})^2$. On en déduit facilement que la même propriété est vraie sur $\bar{\mathbb{Q}}$ ou sur tout corps algébriquement clos de caractéristique 0 (exercice). En particulier, lorsque $k = \mathbb{Q}$, on obtient des "représentations Galoisiennes continues" extrêmement intéressantes $G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ (cf plus loin).

Nous allons voir que la situation est plus compliquée en caractéristique positive. Le premier problème qui se pose est l'éventuelle inséparabilité de $[m]_{\mathcal{E}}$. Nous prouverons à l'aide des différentielles le théorème fondamental suivant, cf (3.3.2).

Théorème. – *L'isogénie* $[m]_{\mathcal{E}}$ *est séparable si et seulement si* $(m, \mathrm{car}(k)) = 1$.

Voici par exemple comment on en déduit la structure de la 2-torsion de $\mathcal{E}$ en caractéristique $\neq 2$.

Corollaire. – *Si* $\mathrm{car}(k) \neq 2$, *alors* $\mathcal{E}[2^n] \simeq (\mathbb{Z}/2^n\mathbb{Z})^2$ *pour tout* $n > 0$.

Démonstration. On vient de voir que $|\mathcal{E}[2]| = 4$. Puisque $[2]_{\mathcal{E}}$ est séparable, elle non ramifiée et donc de degré 4. Il s'ensuit que $[2^n]_{\mathcal{E}}$ est de degré 4^n, et puisqu'elle est aussi non ramifiée, on a $|\mathcal{E}[2^n]| = (2^n)^2$. C'est un exercice de théorie des groupes d'en déduire, par récurrence, que $\mathcal{E}[2^n] \simeq (\mathbb{Z}/2^n\mathbb{Z})^2$. □

Plus généralement, le théorème implique que si $(p, \mathrm{car}(k)) = 1$, le groupe $\mathcal{E}[p]$ est un p-groupe dont le cardinal est le degré de $[p]_{\mathcal{E}}$. Nous allons voir plus loin que ce degré est

toujours p^2. On pourrait montrer assez rapidement que ce degré est > 1 en vérifiant, sur une équation de Weierstraß, que le groupe d'automorphisme de $\mathcal{E}$ est fini, car si $[p]$ était de degré 1, et donc un automorphisme, il ne pourrait pas être d'ordre fini puisque $[p^r] \neq \mathrm{id}$ ($[p^r - 1]_{\mathcal{E}}$ n'est pas constante). On a donc $|\mathcal{E}[p]| = p^k$ avec $k \geqslant 1$, et on a en particulier l'existence d'un point d'ordre p sur $\mathcal{E}$, puis, en prenant des préimages successives, l'existence de points d'ordre p^n, et finalement, celle de points d'ordre m pour tout m premier à $\mathrm{car}(k)$.

3.2.3 *Isogénies duales.* Si $\varphi : \mathcal{E} \longrightarrow \mathcal{E}'$ est une isogénie, le pull-back des diviseurs fournit un morphisme de groupes $\varphi^* : \mathrm{Pic}^0(\mathcal{E}') \longrightarrow \mathrm{Pic}^0(\mathcal{E})$, qui via la bijection d'Abel-Jacobi 3.1.1 fournit donc une application $\hat{\varphi} : \mathcal{E}' \longrightarrow \mathcal{E}$. Explicitement, on a

$$\forall T' \in \mathcal{E}',\ [\hat{\varphi}(T')] - [O] \sim \varphi^*([T'] - [O']).$$

Nous allons montrer que cette application $\hat{\varphi}$ est aussi une isogénie.

Pour analyser le problème, choisissons T tel que $\varphi(T) = T'$. La préimage de T' est $\{T + R, R \in \mathrm{Ker}(\varphi)\}$, où $\mathrm{Ker}\,\varphi = \varphi^{-1}(O')$ est un sous-groupe de $\mathcal{E}$ d'ordre $\deg_s(\varphi)$ (le degré séparable). De plus, tous les points de $\mathcal{E}$ sont d'indice de ramification égal au degré inséparable $\deg_i(\varphi)$. On obtient donc

$$\varphi^*([T'] - [O']) = \sum_{R \in \mathrm{Ker}(\varphi)} \deg_i(\varphi)([T + R] - [R])$$

Puisque $[T + R] - [R] \sim [T] - [O]$, on en déduit, en posant $m = \deg(\varphi)$:

$$\varphi^*([T'] - [O']) \sim \deg_i(\varphi) \sum_{R \in \mathrm{Ker}(\varphi)} ([T] - [O]) = \deg(\varphi)([T] - [O]) = [[m]_{\mathcal{E}} T] - [O].$$

Le théorème suivant montre donc, entre autres, que l'application $\hat{\varphi}$ est une isogénie.

Théorème. – *Soit $\varphi : \mathcal{E} \longrightarrow \mathcal{E}'$ une isogénie de degré m. Il existe une unique isogénie $\hat{\varphi} : \mathcal{E}' \longrightarrow \mathcal{E}$ telle que $\hat{\varphi} \circ \varphi = [m]_{\mathcal{E}}$. De plus, on a aussi $\varphi \circ \hat{\varphi} = [m]_{\mathcal{E}'}$ ainsi que $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$ pour toute autre isogénie $\psi : \mathcal{E}' \longrightarrow \mathcal{E}''$.*

Démonstration. L'unicité est claire, vu la surjectivité de φ. De même, supposant l'existence de $\hat{\varphi}$, l'égalité $\varphi \circ \hat{\varphi} \circ \varphi = \varphi \circ [m]_{\mathcal{E}} = [m]_{\mathcal{E}'} \circ \varphi$ montre que $\varphi \circ \hat{\varphi} = [m]_{\mathcal{E}'}$. Supposons maintenant l'existence de $\hat{\varphi}$ et $\hat{\psi}$ comme dans l'énoncé, alors on a

$$(\hat{\varphi} \circ \hat{\psi}) \circ (\psi \circ \varphi) = \hat{\varphi} \circ [\deg \psi]_{\mathcal{E}'} \circ \varphi = \hat{\varphi} \circ \varphi \circ [\deg \psi]_{\mathcal{E}} = [\deg \varphi]_{\mathcal{E}} [\deg \psi]_{\mathcal{E}} = [\deg(\varphi \circ \psi)]_{\mathcal{E}}$$

d'où l'existence de $\widehat{\psi \circ \varphi}$ et l'égalité $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$. Cela nous permet de traiter séparément les isogénies séparables et purement inséparables.

Dans le cas où φ est séparable, on a $\varphi^*(\bar{k}(\mathcal{E}')) = \bar{k}(\mathcal{E})^{\ker \varphi}$ tandis que $[m]^*_{\mathcal{E}}(\bar{k}(\mathcal{E})) \subset \bar{k}(\mathcal{E})^{\ker [m]_{\mathcal{E}}}$. Or $\mathrm{Ker}\,\varphi$ est d'ordre $m = \deg(\varphi)$, donc contenu dans $\mathrm{Ker}[m]_{\mathcal{E}}$, et on a donc des inclusions

$$\bar{k}(\mathcal{E}) \supset \varphi^* \bar{k}(\mathcal{E}') \supset [m]^* \bar{k}(\mathcal{E}).$$

On en déduit un morphisme de corps $(\varphi^*)^{-1} \circ [m]^* : \bar{k}(\mathcal{E}) \longrightarrow \bar{k}(\mathcal{E}')$, auquel correspond un morphisme de variétés $\hat{\varphi} : \mathcal{E}' \longrightarrow \mathcal{E}$ tel que $\hat{\varphi} \circ \varphi = [m]_{\mathcal{E}}$. On a nécessairement $\hat{\varphi}(O') = O$, donc $\hat{\varphi}$ est une isogénie.

Dans le cas où φ est purement inséparable, elle est de la forme $\mathcal{E} \xrightarrow{\phi_q} \mathcal{E}^{(q)}$ avec $q = p^r$ (isogénie "de Frobenius"), et se décompose en $\mathcal{E} \xrightarrow{\phi_p} \mathcal{E}^{(p)} \xrightarrow{\phi_p^{(p)}} \mathcal{E}^{(p^2)} \longrightarrow \cdots \longrightarrow \mathcal{E}^{(q)}$, donc il suffit de traiter le cas $q = p$. Mais alors le théorème 3.2.2 nous dit que $[p]_{\mathcal{E}}$ est inséparable, donc se factorise $[p]_{\mathcal{E}} = \psi \circ \phi_{p^{r'}}$ avec ψ inséparable, et donc se factorise aussi $[p]_{\mathcal{E}} = \psi' \circ \phi_p$ et il n'y a plus qu'à poser $\hat{\phi}_p := \psi$. □

Exercice. – Soient $\varphi : \mathcal{E} \longrightarrow \mathcal{E}'$ et $\psi : \mathcal{E} \longrightarrow \mathcal{E}''$ deux isogénies. Supposons φ séparable et $\operatorname{Ker}\varphi \subset \operatorname{Ker}\psi$. Alors il existe une unique isogénie $\lambda : \mathcal{E}' \longrightarrow \mathcal{E}''$ telle que $\lambda \circ \varphi = \psi$.

Lorsque $k = \mathbb{C}$, on voit sur les surfaces de Riemann C/Λ que $[m]_{\mathcal{E}}$ est de degré m^2. Il s'ensuit que $\deg(\hat{\varphi}) = m$ et $\hat{\hat{\varphi}} = \varphi$, et aussi que $\widehat{[m]} = [m]$. Toutes ces propriétés sont vraies en général et découlent du théorème difficile suivant, qui sera prouvé en 3.4.4.

3.2.4 Théorème.– *Pour $\varphi, \psi : \mathcal{E} \longrightarrow \mathcal{E}'$ deux isogénies, on a $\widehat{(\varphi + \psi)} = \hat{\varphi} + \hat{\psi}$.*

Admettons ce théorème pour l'instant.

3.2.5 Corollaire.– *Pour tout $m \in \mathbb{N}^*$, on a $\deg([m]_{\mathcal{E}}) = m^2$ et $\widehat{[m]} = [m]$. De plus,*

i) Si $(m, \operatorname{car}(k)) = 1$ alors $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

ii) Si $p = \operatorname{car}(k)$ alors soit $\mathcal{E}[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$ pour tout n, soit $\mathcal{E}[p^n] = \{O\}$ pour tout n.

Démonstration. Puisque $\widehat{[1]} = [1]$, le théorème implique en sommant que $\widehat{[m]} = [m]$, d'où l'on tire que $[\deg(m)]_{\mathcal{E}} = [m]_{\mathcal{E}} \circ [m]_{\mathcal{E}} = [m^2]_{\mathcal{E}}$. Mais alors $[\deg(m) - m^2]_{\mathcal{E}} = [0]_{\mathcal{E}} = 0$ dans $\operatorname{End}(\mathcal{E})$ et par conséquent $\deg(m) = m^2$.

Lorsque $(m, \operatorname{car}(k)) = 1$, on a donc $|\mathcal{E}[m]| = m^2$. En écrivant $\mathcal{E}[m]$ comme produit de groupes cycliques et en utilisant $|\mathcal{E}[m']| = (m')^2$ pour $m'|m$, on obtient le i).

Si $p = \operatorname{car}(k)$, écrivons $[p]_{\mathcal{E}} = \hat{\phi}_p \circ \phi_p$ où $\phi_p : \mathcal{E} \longrightarrow \mathcal{E}^{(p)}$ est l'isogénie de Frobenius. Si $\hat{\phi}_p$ est séparable, alors $|\mathcal{E}[p]| = \deg_s([p]_{\mathcal{E}}) = p$ et plus généralement $|\mathcal{E}[p^n]| = \deg_s([p^n]_{\mathcal{E}}) = p^n$, d'où l'on tire par récurrence que $\mathcal{E}[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$. Si $\hat{\phi}_p$ est inséparable alors $\deg_s([p]_{\mathcal{E}}) = \deg([p^n]_{\mathcal{E}}) = 1$ et $\mathcal{E}[p] = \mathcal{E}[p^n] = \{O\}$ pour tout n. □

Remarque. – Si $\mathcal{E}[p] = \{O\}$, $\mathcal{E}$ est dite *supersingulière*. Sinon, elle est dite *ordinaire*.

Exercice. – Montrer que $\hat{\hat{\varphi}} = \varphi$ pour toute isogénie.

Voici une autre conséquence, qui nous sera utile dans la preuve du théorème de Hasse.

3.2.6 Corollaire.– *L'application degré* $\deg : \operatorname{Hom}(\mathcal{E}, \mathcal{E}') \longrightarrow \mathbb{N}$ *est une forme quadratique définie positive.*

Démonstration. La positivité et le caractère défini sont clairs. Ce qui l'est beaucoup moins est la bilinéarité de l'application $(\varphi,\psi)\mapsto \deg(\varphi+\psi)-\deg(\varphi)-\deg(\psi)$. Regardons cette expression dans $\mathrm{End}(\mathcal{E})$, à travers l'injection $\mathbb{Z}\hookrightarrow\mathrm{End}(\mathcal{E})$. On a :

$$\begin{aligned}[\deg(\varphi+\psi)]_{\mathcal{E}}-[\deg(\varphi)]_{\mathcal{E}}-[\deg(\psi)]_{\mathcal{E}} &= \widehat{(\varphi+\psi)}\circ(\varphi+\psi)-\hat{\varphi}\circ\varphi-\hat{\psi}\circ\psi\\ &= (\hat{\varphi}+\hat{\psi})\circ(\varphi+\psi)-\hat{\varphi}\circ\varphi-\hat{\psi}\circ\psi\\ &= \hat{\varphi}\circ\psi+\hat{\psi}\circ\varphi.\end{aligned}$$

La dernière expression est bien $\mathbb{Z}$-bilinéaire en (φ,ψ). □

3.2.7 Théorème. (Hasse)– *Supposons $k=\mathbb{F}_q$. Alors $||\mathcal{E}(\mathbb{F}_q)|-q-1|\leqslant 2\sqrt{q}$.*

Démonstration. Comme dans le dernier exemple de 2.4.3, on a $\mathcal{E}^{(q)}=\mathcal{E}$ et l'isogénie de Frobenius ϕ_q est donc un endomorphisme de $\mathcal{E}$. De plus, son action sur $\mathcal{E}$ est la même que celle d'un générateur de $G_{\mathbb{F}_q}$ donc on a $\mathcal{E}(\mathbb{F}_q)=\mathcal{E}^{\phi_q}=\mathrm{Ker}(\mathrm{id}-\phi_q)$. Puisque ϕ_q est inséparable, on a $\phi_q^*\omega=0$ pour toute différentielle $\omega\in\Omega_{\mathcal{E}}$, et il s'ensuit que $(\mathrm{id}-\phi_q)^*\omega=\omega$, donc $\mathrm{id}-\phi_q$ est une isogénie séparable. En particulier, $|\mathrm{Ker}(\mathrm{id}-\phi_q)|=\deg(\mathrm{id}-\phi_q)$. Or, le corollaire précédent nous dit que $\varphi\mapsto\deg(\varphi)$ est une forme quadratique définie positive sur $\mathrm{End}(\mathcal{E})$. Une version de l'inégalité de Cauchy-Schwartz nous dit alors que

$$|\deg(\mathrm{id}-\phi_q)-\deg(\mathrm{id})-\deg(\phi_q)|\leqslant 2\sqrt{\deg(\mathrm{id})\deg(\phi_q)}.$$

Les égalités $\deg(\mathrm{id})=1$ et $\deg(\phi_q)=q$ achèvent la preuve. □

3.3 Différentielles invariantes et isogénies

Soit $(\mathcal{E},O)$ une courbe elliptique sur k. Puisque $\mathcal{E}$ est de genre 1, le k-ev $\Omega_{\mathcal{E}}(\mathcal{E})$ des différentielles partout régulières est de dimension 1. Soit $\omega\in\Omega_{\mathcal{E}}(\mathcal{E})\setminus\{0\}$. Si θ est un automorphisme de la courbe $\mathcal{E}$, alors $\theta^*\omega\in\Omega_{\mathcal{E}}(\mathcal{E})$ donc il existe $\lambda_\theta\in\bar{k}^\times$ tel que $\theta^*\omega=\lambda_\theta\omega$. Par exemple, pour tout point $P\in\mathcal{E}$, il existe $\lambda_P\in\bar{k}^\times$ tel que $t_P^*\omega=\lambda_P\omega$. Plus généralement, si $\varphi:\mathcal{E}'\longrightarrow\mathcal{E}$ est un morphisme et ω' une différentielle régulière sur $\mathcal{E}'$, il existe $\lambda_\varphi\in\bar{k}$ tel que $\varphi^*\omega=\lambda_\varphi\omega'$. On a alors $\lambda_\varphi\neq 0$ si et seulement si φ est non-constant et séparable.

3.3.1 Théorème.– *Avec les notations ci-dessus :*
i) Pour tout $P\in\mathcal{E}$, on a $\lambda_P=1$ (i.e. $t_P^*\omega=\omega$).
ii) Pour $\varphi,\psi:\mathcal{E}'\longrightarrow\mathcal{E}$, on a $\lambda_{\varphi+\psi}=\lambda_\varphi+\lambda_\psi$ (i.e. $(\varphi+\psi)^*\omega=\varphi^*\omega+\psi^*\omega$).

La propriété i) exprime le fait que ω est invariante par translations, on parle de *différentielle invariante.* La propriété ii) implique que

$$\forall m\in\mathbb{Z},\ \text{on a}\ [m]_{\mathcal{E}}^*\omega=m\omega, \tag{3.3.2}$$

d'où l'on déduit le théorème 3.2.2 comme annoncé, ainsi que le fait que $[m]_{\mathcal{E}}$ est une isogénie aussi en caractéristique 2 si m est impair. Pour voir que $[2]_{\mathcal{E}}$ est non-constante en

caractéristique 2, il suffit alors de remarquer que si P est un point d'ordre 3 (qui existe d'après la fin de 3.2.2), alors $2P \neq O$.

Démonstration. Les deux points sont conséquences d'une même formule que nous expliquons maintenant. On dispose de trois morphismes $\pi_1, \pi_2, \mu : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ (première et seconde projections, et addition) surjectifs. Ces morphismes induisent des morphismes de corps $\pi_1^*, \pi_2^*, \mu^* : k(\mathcal{E}) \longrightarrow k(\mathcal{E} \times \mathcal{E})$ ainsi que des morphismes sur les différentielles $\pi_1^*, \pi_2^*, \mu^* : \Omega_{\bar{k}(\mathcal{E})/\bar{k}} \longrightarrow \Omega_{\bar{k}(\mathcal{E}\times\mathcal{E})/\bar{k}}$. Le point crucial est la formule suivante :

$$(*) \quad \mu^*\omega = \pi_1^*\omega + \pi_2^*\omega.$$

Afin de mieux comprendre ce que cela signifie, prenons un ouvert affine V de $\mathcal{E}$ et notons $\bar{k}[V]$ son algèbre de fonctions régulières. Par exemple, si t est une uniformisante en P et $\varphi_t : \mathcal{E} \longrightarrow \mathbb{P}^1$ le morphisme associé, on peut prendre $V = \varphi_t^{-1}(\mathbb{A}^1)$ et $\bar{k}[V]$ est alors la clôture intégrale de $\bar{k}[t]$ dans $\bar{k}(\mathcal{E})$. L'image réciproque $\mu^{-1}(V)$ est ouverte dans $\mathcal{E}\times\mathcal{E}$ donc contient un ouvert de la forme $V_1 \times V_2$ avec V_i ouvert affine de $\mathcal{E}$, que l'on peut supposer contenus dans V. L'algèbre des fonctions régulières sur $V_1 \times V_2$ est alors $\bar{k}[V_1 \times V_2] = \pi_1^*\bar{k}[V_1] \otimes_{\bar{k}} \pi_2^*\bar{k}[V_2]$ et le $\bar{k}[V_1 \times V_2]$-module des différentielles de Kähler de cette algèbre est donné par

$$\Omega_{\bar{k}[V_1\times V_2]/\bar{k}} = \left(\pi_1^*\bar{k}[V_1] \otimes_{\bar{k}} \pi_2^*\Omega_{\bar{k}[V_2]/\bar{k}}\right) \oplus \left(\pi_1^*\Omega_{\bar{k}[V_1]/\bar{k}} \otimes_{\bar{k}} \pi_2^*\bar{k}[V_2]\right).$$

(Exercice : montrer que $\Omega_{A\otimes_{\bar{k}}B/\bar{k}} = (A \otimes_{\bar{k}} \Omega_{B/\bar{k}}) \oplus (\Omega_{A/\bar{k}} \otimes_{\bar{k}} B)$ comme $A \otimes_{\bar{k}} B$-modules.) Notons encore ω pour sa restriction à V_i. On sait que ω est une $\bar{k}[V_i]$-base de $\Omega_{\bar{k}[V_i]/\bar{k}}$. La décomposition ci-dessus s'écrit donc aussi

$$\Omega_{\bar{k}[V_1\times V_2]/\bar{k}} = \bar{k}[V_1 \times V_2]\pi_1^*\omega \oplus \bar{k}[V_1 \times V_2]\pi_2^*\omega.$$

En restreignant μ à $V_1 \times V_2$, on obtient par pull-back une différentielle $\mu^*\omega \in \Omega_{\bar{k}[V_1\times V_2]/\bar{k}}$. Vu la décomposition ci-dessus, il existe des fonctions $f_1, f_2 \in \bar{k}[V_1 \times V_2]$ uniques telle que

$$\mu^*\omega = f_1 \cdot \pi_1^*\omega + f_2 \cdot \pi_2^*\omega.$$

Il s'agit alors de montrer que $f_1 = f_2 = 1$. Pour cela, nous utilisons l'observation suivante :

$$t_P \text{ est la composée } \mathcal{E} \xrightarrow{(\mathrm{id},\, c_P)} \mathcal{E} \times \mathcal{E} \xrightarrow{\mu} \mathcal{E}$$

où $c_P : \mathcal{E} \longrightarrow \mathcal{E}$ désigne le morphisme constant d'image $\{P\}$. Si $P \in V_2$, cela implique que sur l'ouvert V_1 on a

$$\begin{aligned} t_P^*\,\omega = (\mathrm{id}, c_P)^*\mu^*\omega &= f_{1,|V_1\times\{P\}} \cdot (\mathrm{id}, c_P)^*\pi_1^*\omega + f_{2,|V_1\times\{P\}} \cdot (\mathrm{id}, c_P)^*\pi_2^*\omega \\ &= f_{1,|V_1\times\{P\}} \cdot \omega \qquad\qquad + 0 \end{aligned}$$

Ici on a $(\mathrm{id}, c_P)^*\pi_2^*\omega = 0$ puisque $\pi_2 \circ (\mathrm{id}, c_P)$ est constante. Or on a vu plus haut que $t_P^*\omega = \lambda_P\omega$ pour un scalaire $\lambda_P \in \bar{k}^\times$. Il s'ensuit que $f_{1,|V_1\times\{P\}}$ est constante sur $V_1 \times \{P\}$ de valeur λ_P, et aussi que $P \mapsto \lambda_P$ est régulière sur V_2 puisque $\lambda_P = f_1(Q, P)$ pour tout

$Q \in V_1$. En faisant varier V, V_1 et V_2 on obtient que $P \mapsto \lambda_P$ est une fonction régulière sur $\mathcal{E}$, donc constante, et en faisant $P = O$ on voit que $\lambda_P = 1$ pour tout P.

On a donc montré le i), ainsi que $f_1 = 1$. Un raisonnement symétrique montre $f_2 = 1$, d'où l'égalité

$$(**) : \quad \mu^*\omega = \pi_1^*\omega + \pi_2^*\omega \quad \text{dans } \Omega_{\bar{k}[V_1 \times V_2]/\bar{k}}.$$

Bien-sûr, en localisant, on en déduit la formule $(*)$ dans $\Omega_{\bar{k}(\mathcal{E}\times\mathcal{E})/\bar{k}}$.

Pour prouver ii), on observe maintenant que

— $(\varphi + \psi)$ est la composée $\mathcal{E}' \xrightarrow{(\varphi,\,\psi)} \mathcal{E} \times \mathcal{E} \xrightarrow{\mu} \mathcal{E}$.

— φ est la composée $\mathcal{E}' \xrightarrow{(\varphi,\,\psi)} \mathcal{E} \times \mathcal{E} \xrightarrow{\pi_1} \mathcal{E}$.

— ψ est la composée $\mathcal{E}' \xrightarrow{(\varphi,\,\psi)} \mathcal{E} \times \mathcal{E} \xrightarrow{\pi_2} \mathcal{E}$.

Grâce à $(**)$, il s'ensuit que sur l'ouvert $\varphi^{-1}(V_1) \cap \psi^{-1}(V_2)$ de $\mathcal{E}'$, on a

$$(\varphi + \psi)^*\omega = (\varphi, \psi)^*(\pi_1^*\omega + \pi_2^*\omega) = \varphi^*\omega + \psi^*\omega,$$

comme annoncé dans le ii). □

Citons un corollaire intéressant, même en caractéristique 0. On rappelle que pour φ un endomorphisme de $(\mathcal{E}, O)$ on note $\lambda_\varphi \in \bar{k}$ le scalaire tel que $\varphi^*\omega = \lambda_\varphi\omega$.

3.3.3 Corollaire.– *L'application* $\mathrm{End}\,(\mathcal{E}) \longrightarrow \bar{k}$, $\varphi \mapsto \lambda_\varphi$ *est un morphisme d'anneaux dont le noyau est formé de* 0 *et des isogénies inséparables. En particulier, si* $\mathrm{car}(k) = 0$, *alors* $\mathrm{End}\,(\mathcal{E})$ *est un anneau commutatif intègre.*

En caractéristique p, nous verrons que l'anneau $\mathrm{End}\,(\mathcal{E})$ peut être non commutatif.

Exercice. – Supposons que $\mathcal{E}$ est donnée par une équation de Weierstraß. Montrer que $\frac{dx}{2y+a_1x+a_3}$ est une différentielle partout régulière, et donc invariante par translations.

3.4 Accouplement de Weil

On se donne ici une courbe elliptique $(\mathcal{E}, O)$ et un entier m pour lequel on sait que $[m]_\mathcal{E}$ est de degré m^2. On suppose aussi que $(m, \mathrm{car}(k)) = 1$, de sorte que $[m]_\mathcal{E}$ est séparable et donc non ramifiée et $|\mathcal{E}[m]| = m^2$. Nous allons définir une forme bilinéaire alternée non-dégénérée sur le groupe de m-torsion $\mathcal{E}[m]$.

3.4.1 *Construction.* Partons de $T \in \mathcal{E}[m]$ et considérons le diviseur $[m]^*([T] - [O])$. Si T' est n'importe quel point tel que $mT' = T$, on a

$$[m]^*([T] - [O]) = \sum_{R \in \mathcal{E}[m]} ([T' + R] - [R]) \sim \sum_{R \in \mathcal{E}[m]} ([T'] - [O]) \sim m^2([T'] - [O]) \sim 0.$$

Ici la première égalité est dans $\mathrm{Div}^0(\mathcal{E})$, et les $\sim$ désignent des égalités dans $\mathrm{Pic}^0(\mathcal{E})$, lesquelles découlent de la définition de la loi de groupe sur $\mathcal{E}$. Il existe donc une fonction $g_T \in$

$\bar{k}(\mathcal{E})^\times$, unique à un facteur scalaire près, telle que $\mathrm{div}(g_T) = [m]^*([T] - [O])$. Remarquons maintenant que

$$\mathrm{div}(g_T^m) = [m]^*(m[T] - m[O]) \quad \text{et} \quad m[T] - m[O] \sim [mT] - [O] \sim 0$$

Ainsi, il existe $f \in \bar{k}(\mathcal{E})^\times$ telle que $\mathrm{div}(g_T^m) = [m]^*\mathrm{div}(f) = \mathrm{div}(f \circ [m])$. En particulier, $g_T^m \in k^\times \cdot (f \circ |m])$ est invariante par translation sous $\mathcal{E}[m]$.

Soit alors $S \in \mathcal{E}[m]$ un autre point, et t_S le morphisme de translation par S. On a $(t_S^* g_T)^m = t_S^* g_T^m = g_T^m$, donc il existe une unique racine de l'unité

$$e_m(S,T) \in \mu_m(\bar{k}) \text{ telle que } t_S^* g_T = e_m(S,T) g_T.$$

Notons que ce facteur ne dépend pas du choix de g_T.

3.4.2 Proposition.– *L'application $\mathcal{E}[m] \times \mathcal{E}[m] \longrightarrow \mu_m$, $(S,T) \mapsto e_m(S,T)$ est bilinéaire, alternée, non-dégénérée et compatible à l'action de Galois.*

La non-dégénérescence signifie ici l'injectivité de l'application $\mathcal{E}[m] \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{E}[m], \mu_m)$, $T \mapsto e_m(-,T)$. Pour des raisons de cardinalité, cette application est alors surjective.

Démonstration. La linéarité en la première variable est claire puisque

$$t_{S+S'}^* g_T = (t_S \circ t_{S'})^* g_T = t_{S'}^*(t_S^* g_T) = t_{S'}^*(e_m(S,T) g_T) = e_m(S,T) e_m(S',T) g_T.$$

Pour la linéarité en la seconde variable, le diviseur $[T] + [T'] - [T+T'] - [O]$ est nul dans $\mathrm{Pic}^0(\mathcal{E})$ donc de la forme $\mathrm{div}(f)$ pour $f \in \bar{k}(\mathcal{E})^\times$. On a alors

$$\mathrm{div}(g_T g_{T'} g_{T+T'}^{-1}) = [m]^*([T] + [T'] - [T+T'] - [O]) = \mathrm{div}(f \circ [m]),$$

ce qui implique que $g_T g_{T'} g_{T+T'}^{-1}$ est invariante par translation par $\mathcal{E}[m]$, d'où l'égalité $e_m(S,T) e_m(S,T') e_m(S,T+T')^{-1} = 1$.

Montrons maintenant que $e(T,T) = 1$ (et donc que l'application bilinéaire est alternée). Remarquons d'abord que pour tout $P \in \mathcal{E}$, on a

$$\mathrm{div}(t_P^* g_T) = t_P^*[m]^*([T] - [O]) = [m]^* t_{mP}^*([T] - [O]) = [m]^*([T - mP] - [-mP]).$$

Soit alors $T' \in \mathcal{E}$ tel que $mT' = T$. On a donc dans $\mathrm{Div}(\mathcal{E})$ l'égalité

$$\mathrm{div}\left(\prod_{i=0}^{m-1} t_{iT'}^* g_T\right) = [m]^* \sum_{i=0}^{m-1} ([(1-i)T] - [-iT]) = 0,$$

qui montre que $\prod_{i=0}^{m-1} t_{iT'}^* g_T$ est une fonction constante. On a donc en particulier

$$1 = t_{T'}^*(\prod_{i=0}^{m-1} t_{iT'}^* g_T)(\prod_{i=0}^{m-1} t_{iT'}^* g_T)^{-1} = (\prod_{i=1}^{m} t_{iT'}^* g_T)(\prod_{i=0}^{m-1} t_{iT'}^* g_T)^{-1} = t_T^* g_T \cdot g_T^{-1},$$

d'où $e(T,T)=1$.

Montrons maintenant la non-dégénérescence. Soit T tel que $e(S,T)=1$ pour tout S. Alors g_T est invariante par translation sous $\mathcal{E}[m]$, donc est de la forme $g_T=\tilde{g}_T\circ[m]$. On a alors $[m]^*(\mathrm{div}(\tilde{g}_T))=[m]^*([T]-[O])$ d'où l'on tire $\mathrm{div}(\tilde{g}_T)=[T]-[O]$, ce qui implique $T=O$.

La compatibilité à l'action de Galois, à savoir $e(\sigma S,\sigma T)=\sigma(e(S,T))$ pour tout $\sigma\in G_k$ est laissée en exercice. □

Exercice. – Montrer que $e_m(\mathcal{E}[m]\times\mathcal{E}[m])=\mu_m$.

Notons que notre hypothèse que $[m]_{\mathcal{E}}$ est de degré m^2 implique que $\deg([p]_{\mathcal{E}})=p^2$ pour tout diviseur p (cf discussion à la fin de 3.2.2), et donc $|\mathcal{E}[m']|=\deg([m']_{\mathcal{E}})=m'^2$ pour tout diviseur m' de m. On en déduit que $\mathcal{E}[m]\simeq(\mathbb{Z}/m\mathbb{Z})^2$, et idem pour $m'|m$.

Exercice. – Si $m=dm'$, montrer $e_m(S,T)=e_{m'}([d]S,T)$ pour $S\in\mathcal{E}[m]$ et $T\in\mathcal{E}[m']$.

Donnons-nous maintenant une autre courbe elliptique $(\mathcal{E}',O')$ telle que $\deg([m]_{\mathcal{E}'})=m^2$, ainsi qu'une isogénie $\varphi:\mathcal{E}\longrightarrow\mathcal{E}'$.

3.4.3 Proposition.– *On a $e_m(S,\hat{\varphi}(T'))=e_m(\varphi(S),T')$ pour tous $S\in\mathcal{E}$ et $T'\in\mathcal{E}'$.*

Démonstration. On a par définition de l'accouplement de Weil

$$e_m(\varphi(S),T')=t_{\varphi(S)}^*g_{T'}\cdot g_{T'}^{-1}=\varphi^*(t_{\varphi(S)}^*g_{T'}\cdot g_{T'}^{-1})=t_S^*\varphi^*(g_{T'})\cdot\varphi^*(g_{T'})^{-1}$$
$$e_{m(S,\hat{\varphi}(T'))}=t_S^*g_{\hat{\varphi}(T')}\cdot g_{\hat{\varphi}(T')}^{-1}$$

Par ailleurs, les définitions de $g_{T'}$, $g_{\hat{\varphi}(T')}$ et de l'isogénie duale donnent

$$\begin{aligned}\mathrm{div}(\varphi^*g_{T'})=\varphi^*[m]_{\mathcal{E}'}^*([T']-[O']) &= [m]_{\mathcal{E}}^*\varphi^*([T']-[O])\\ &\sim [m]_{\mathcal{E}}^*([\hat{\varphi}(T')]-[O])=\mathrm{div}(g_{\hat{\varphi}(T')}).\end{aligned}$$

Soit $f\in\bar{k}(\mathcal{E})^\times$ une fonction telle que $\mathrm{div}(f)=\varphi^*([T']-[O])-([\hat{\varphi}(T')]-[O])$. Alors il existe $\lambda\in\bar{k}^\times$ tel que $\varphi^*g_{T'}\cdot g_{\hat{\varphi}(T')}^{-1}=\lambda(f\circ[m]_{\mathcal{E}})$, donc la fonction $\varphi^*g_{T'}\cdot g_{\hat{\varphi}(T')}^{-1}$ est invariante par translations sous $\mathcal{E}[m]$, et on en déduit l'égalité souhaitée. □

3.4.4 *Preuve du théorème 3.2.4.* On suppose $\mathrm{car}(k)\neq 2$. Alors le corollaire de 3.2.2 nous assure que le degré de $[2^n]_{\mathcal{E}}$ est $(2^n)^2$ pour tout n. On dispose donc de l'accouplement de Weil sur chaque $\mathcal{E}[2^n]$. Soient alors $\varphi,\psi:\mathcal{E}\longrightarrow\mathcal{E}'$ deux isogénies comme dans le théorème 3.2.4. Pour tout $n\in\mathbb{N}$, tout $T'\in\mathcal{E}'[2^n]$ et tout $S\in\mathcal{E}[n]$, on a

$$\begin{aligned}e_{2^n}\left(S,\widehat{(\varphi+\psi)}(T')-\hat{\varphi}(T')-\hat{\psi}(T')\right) &= e_{2n}\left(S,\widehat{(\varphi+\psi)}(T')\right)e_{2n}(S,\hat{\varphi}(T'))^{-1}e_{2n}(S,\hat{\psi}(T'))^{-1}\\ &= e_{2n}\left((\varphi+\psi)(S),T'\right)e_{2n}(\varphi(S),T')^{-1}e_{2n}(\psi(S),T')^{-1}\\ &= e_{2n}\left((\varphi+\psi)(S)-\varphi(S)-\psi(S),T'\right)\\ &= e_{2n}(O',T')=1\end{aligned}$$

Par non-dégénérescence de e_{2n}, il s'ensuit que $(\widehat{\varphi+\psi})(T') = \hat{\varphi}(T') + \hat{\psi}(T')$ pour tout $T' \in \mathcal{E}[2^n]$. Or, le sous-groupe $\bigcup_{n\in\mathbb{N}} \mathcal{E}[2^n]$ est un ensemble infini, donc Zariski-dense dans $\mathcal{E}$. L'égalité $(\widehat{\varphi+\psi})(T') = \hat{\varphi}(T') + \hat{\psi}(T')$ est donc vraie pour tout $T' \in \mathcal{E}$.

Pour le cas $\mathrm{car}(k) = 2$, on peut procéder de la même manière, à condition de prouver au préalable que $[3]_{\mathcal{E}}$ est de degré 9, ce qui peut se faire de manière calculatoire à partir d'une équation de Weierstraß (bon courage). □

3.5 Modules de Tate

On fixe ici un nombre premier ℓ tel que $(\ell, \mathrm{car}(k)) = 1$.

3.5.1 *Rappels sur le caractère cyclotomique.* Pour tout entier m premier à $\mathrm{car}(k)$, l'action de G_k sur le groupe des racines m-èmes de l'unité $\mu_m(\bar{k})$ fournit un homomorphisme

$$\chi_m : G_k \longrightarrow \mathrm{Aut}(\mu_m) = (\mathbb{Z}/m\mathbb{Z})^\times = \mathrm{GL}_1(\mathbb{Z}/m\mathbb{Z})$$

qui est continu puisqu'il se factorise par $\mathrm{Gal}(k(\mu_m)/k)$. Cette factorisation est d'ailleurs injective et permet parfois de calculer $\mathrm{Gal}(k(\mu_m)/k)$. Un résultat classique affirme par exemple que si $k = \mathbb{Q}$, χ_m induit un isomorphisme $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$.

Si l'on considère $\mu_m = \mathbb{G}_m[m]$ comme le groupe des points de m-torsion du groupe multiplicatif $\mathbb{G}_m$ (qui est aussi une courbe algébrique), on comprend alors l'intérêt d'étudier l'action de Galois sur $\mathcal{E}[m]$ pour une courbe elliptique, qui d'après le corollaire 3.2.5 est ici une "représentation linéaire" de G_k

$$\rho_{\mathcal{E},m} : G_k \longrightarrow \mathrm{Aut}(\mathcal{E}[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Notons que l'isomorphisme ci-dessus n'a rien de canonique puisqu'il dépend du choix d'une $\mathbb{Z}/m\mathbb{Z}$-base de $\mathcal{E}[m]$, mais sa classe de conjugaison est canonique. Une difficulté dans l'étude de $\rho_{\mathcal{E},m}$ est que la théorie des représentations linéaires de groupes à valeurs dans un anneau comme $\mathbb{Z}/m\mathbb{Z}$ est a priori compliquée. Néanmoins, on peut produire des représentations linéaires sur des corps de caractéristique 0 en regardant toutes les puissances d'un premier ℓ à la fois.

Pour le cas de $\mathbb{G}_m$, on regarde le système projectif

$$\cdots \longrightarrow \mu_{\ell^n} \xrightarrow{(-)^\ell} \mu_{\ell^{n-1}} \longrightarrow \cdots \longrightarrow \mu_\ell$$

et on pose $T_\ell\mathbb{G}_m := \varprojlim_n \mu_{\ell^n}$ la limite projective de ce système. Un élément de $T_\ell\mathbb{G}_m$ est donc un système compatible de racines de l'unité $(\zeta_n)_n$ avec $\zeta_n \in \mu_{\ell^n}$ et $\zeta_n^\ell = \zeta_{n-1}$. Alors $T_\ell\mathbb{G}_m$ est naturellement un $\mathbb{Z}_\ell$-module libre de rang 1, et un élément $(\zeta_n)_n$ en forme une base si et seulement si $\zeta_1 \neq 1$. Le groupe de Galois G_k agit *continûment* sur $T_\ell\mathbb{G}_m$ si on munit ce dernier de la topologie produit. Cette action est donnée par une représentation $\mathbb{Z}_\ell$-linéaire

$$\chi_{\ell^\infty} : G_k \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell\mathbb{G}_m) = \mathbb{Z}_\ell^\times = \mathrm{GL}_1(\mathbb{Z}_\ell).$$

3.5.2 *Module de Tate de $\mathcal{E}$.* Appliquons la même idée à $\mathcal{E}$. Considérons le système projectif

$$\cdots \longrightarrow \mathcal{E}[\ell^n] \xrightarrow{[\ell]_{\mathcal{E}}} \mathcal{E}[\ell^{n-1}] \longrightarrow \cdots \longrightarrow \mathcal{E}[\ell]$$

et posons $T_\ell\mathcal{E} := \varprojlim_n \mathcal{E}[\ell^n]$ la limite projective de ce système. Un élément de $T_\ell\mathcal{E}$ est donc un système compatible de points de torsion $(P_n)_n$ avec $P_n \in \mathcal{E}[\ell^n]$ et $[\ell]_{\mathcal{E}} P_n = P_{n-1}$. Alors $T_\ell\mathcal{E}$ est naturellement un $\mathbb{Z}_\ell$-module libre de rang 2, et une paire d'éléments $\{(P_n)_n, (Q_n)_n\}$ en forme une $\mathbb{Z}_\ell$-base si et seulement si $\{P_1, Q_1\}$ est une $\mathbb{F}_\ell$-base de $\mathcal{E}[\ell]$. L'action du groupe de Galois G_k sur $T_\ell\mathbb{G}_m$ est donnée par une représentation $\mathbb{Z}_\ell$-linéaire *continue*

$$\rho_{\mathcal{E},\ell^\infty} : G_k \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell\mathcal{E}) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

En inversant ℓ (ie en tensorisant par $\mathbb{Q}_\ell$) on obtient une représentation $G_k \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$ sur un corps de caractéristique nulle, qui est continue pour la topologie ℓ-adique. Cette représentation contient beaucoup d'information arithmétique, par exemple on verra comment on retrouve le nombre de points de $\mathcal{E}$ lorsque k est fini, ou comment on en tire la fonction L de $\mathcal{E}$ si $k = \mathbb{Q}$.

Exercice. – Montrer que $T_\ell\mathcal{E} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathcal{E})$.

Remarque. – Le module de Tate a aussi une motivation topologique. En effet, si $k = \mathbb{C}$ et $\mathcal{E} = \mathbb{C}/\Lambda$, on voit que $T_\ell\mathcal{E} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \Lambda$ (exercice). Or, puisque $\mathbb{C}$ est simplement connexe, on a $\pi_1(\mathcal{E}, O) = \Lambda$ et a fortiori $H_1(\mathcal{E}, \mathbb{Z}) = \pi_1(\mathcal{E}, O)_{\mathrm{ab}} = \Lambda$. Ainsi $T_\ell\mathcal{E}$ joue le rôle, sur un corps quelconque, du groupe d'homologie $H_1(\mathcal{E}, \mathbb{Z}_\ell)$. En fait, ceci est plus qu'une analogie, on peut en effet définir une "topologie" appelée "topologie étale" sur les schémas dont la cohomologie des faisceaux fournit des analogues de l'homologie usuelle en topologie. Le module de Tate $T_\ell\mathcal{E}$ est, de fait, le premier groupe d'homologie étale de $\mathcal{E}$.

La construction du module de Tate est fonctorielle en $\mathcal{E}$ en le sens suivant. Un homomorphisme $\varphi : \mathcal{E} \longrightarrow \mathcal{E}'$ envoie $\mathcal{E}[\ell^n]$ dans $\mathcal{E}'[\ell^n]$, donc induit à la limite une application $\mathbb{Z}_\ell$-linéaire $T_\ell\varphi : T_\ell\mathcal{E} \longrightarrow T_\ell\mathcal{E}'$. La composition $T_\ell\hat{\varphi} \circ T_\ell\varphi$ est donc la multiplication par $\deg(\varphi)$.

Exercice. – À l'aide du deuxième exercice de la section 3.4, montrer que les accouplements de Weil $e_{\ell^n}(-,-)$ fournissent une application $\mathbb{Z}_\ell$-bilinéaire alternée et non dégénérée

$$e(-,-) : T_\ell\mathcal{E} \times T_\ell\mathcal{E} \longrightarrow T_\ell\mathbb{G}_m,$$

et que si $\varphi : \mathcal{E} \longrightarrow \mathcal{E}'$ est une isogénie alors les applications $\mathbb{Z}$-linéaires $T_\ell\varphi$ et $T_\ell\hat{\varphi}$ sont adjointes l'une de l'autre.

3.5.3 Théorème.– *Avec les notations ci-dessus,*

i) L'application $\mathbb{Z}_\ell$-linéaire $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(\mathcal{E}, \mathcal{E}') \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell\mathcal{E}, T_\ell\mathcal{E}')$ est injective. En particulier, le groupe abélien $\mathrm{Hom}(\mathcal{E}, \mathcal{E}')$ est libre de rang au plus 4.

ii) Pour tout $\varphi \in \mathrm{End}(\mathcal{E})$, on a dans $\mathbb{Z}_\ell$ les égalités

$$\det(T_\ell\varphi) = \deg(\varphi) \text{ et } \mathrm{tr}(T_\ell\varphi) = t(\varphi) := 1 + \deg(\varphi) - \deg(\mathrm{id} - \varphi).$$

iii) Le polynôme $X^2 - t(\varphi)X + \deg(\varphi) \in \mathbb{Z}[X]$ *annule* φ *dans l'anneau* $\mathrm{End}(\mathcal{E})$. *De plus, son discriminant* $t(\varphi)^2 - 4\deg(\varphi)$ *est négatif.*

Démonstration. i) Soit $x = \sum_{i=1}^r \alpha_i \otimes \varphi_i$ un élément de $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(\mathcal{E}, \mathcal{E}')$. Notons Φ le sous-groupe de $\mathrm{Hom}(\mathcal{E}, \mathcal{E}')$ engendré par $\varphi_1, \cdots, \varphi_r$, et notons Φ^{sat} son "saturé" défini par

$$\Phi^{\mathrm{sat}} := (\mathbb{Q} \otimes \Phi) \cap \mathrm{Hom}(\mathcal{E}, \mathcal{E}') = \{\varphi \in \mathrm{Hom}(\mathcal{E}, \mathcal{E}'),\ \exists m \in \mathbb{N}, \varphi \circ [m]_{\mathcal{E}} \in \Phi\}.$$

(Rappelons que le $\mathbb{Z}$-module $\mathrm{Hom}(\mathcal{E}, \mathcal{E}')$ est sans torsion, donc s'envoie injectivement dans $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(\mathcal{E}, \mathcal{E}')$). Alors Φ^{sat} est un groupe libre de type fini. En effet, d'après le corollaire 3.2.6, l'application deg définit une forme quadratique définie positive sur $\mathbb{R} \otimes \Phi$ telle que $\deg_{|\Phi^{\mathrm{sat}} \setminus \{0\}} \geqslant 1$, ce qui signifie que Φ^{sat} est discret dans l'espace euclidien $\mathbb{R} \otimes \Phi$. Prenons donc une base $\psi_1, \cdots, \psi_s$ de Φ^{sat} et écrivons l'élément x sous la forme $x = \sum_{i=1}^s \beta_i \otimes \psi_i$.

Supposons maintenant que $\sum_{i=1}^s \beta_i T_\ell \psi_i = 0$ dans $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell\mathcal{E}, T_\ell\mathcal{E}')$. Pour n fixé, approximons β_i par un entier $b_i \in \mathbb{N}$ tel que $v_\ell(\beta_i - b_i) \geqslant n$, et posons $\psi := \sum_{i=1}^s b_i\psi_i \in \Phi^{\mathrm{sat}}$. Le fait que $T_\ell\psi$ envoie $T_\ell\mathcal{E}$ dans $\ell^n T_\ell\mathcal{E}'$ signifie que ψ induit l'application nulle $\mathcal{E}[\ell^n] \longrightarrow \mathcal{E}'[\ell^n]$, et donc que ψ se factorise en $\psi' \circ [\ell^n]$ (cf exercice du paragraphe 3.2.3). Par définition de Φ^{sat}, on a $\psi' \in \Phi^{\mathrm{sat}}$, et en l'écrivant dans la base des ψ_i on constate que que $\ell^n | b_i$ et $\psi' = \sum_i (\ell^{-n} b_i)\psi_i$. Il s'ensuit que $\ell^n | \beta_i$ dans $\mathbb{Z}_\ell$. Faisant maintenant varier n, on voit que $\beta_i = 0$ pour tout i.

ii) Choisissons une $\mathbb{Z}_\ell$-base $P_\bullet, Q_\bullet$ de $T_\ell\mathcal{E}$, et notons $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ la matrice de $T_\ell\varphi$ dans cette base. En notant additivement l'accouplement de Weil sur $T_\ell\mathcal{E}$ (ie en identifiant $T_\ell\mathbb{G}_m$ à $\mathbb{Z}_\ell$), on calcule.

$$\begin{aligned} \deg(\varphi) e(P_\bullet, Q_\bullet) &= e(\deg(\varphi) \cdot P_\bullet, Q_\bullet) = e(T_\ell\hat{\varphi} \circ T_\ell\varphi(P_\bullet), Q_\bullet) = e(T_\ell\varphi(P_\bullet), T_\ell\hat{\varphi} \circ (Q_\bullet)) \\ &= e(aP_\bullet + cQ_\bullet, bP_\bullet + dQ_\bullet) = (ad - bc) e(P_\bullet, Q_\bullet) \end{aligned}$$

Comme $e(P_\bullet, Q_\bullet)$ est nécessairement non nul dans $T_\ell\mathbb{G}_m = \mathbb{Z}_\ell$, on en déduit $\deg(\varphi) = ad - bc = \det(T_\ell\varphi)$ comme voulu. La formule pour $\mathrm{tr}(T_\ell\varphi)$ découle alors de la formule $\mathrm{tr}(A) = 1 + \det(A) - \det(I_2 - A)$ valable pour toute matrice 2×2.

iii) D'après le ii), le polynôme $f(X) = X^2 - t(\varphi)X + \det(\varphi)$ est le polynôme caractéristique de $T_\ell\varphi \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell\mathcal{E})$. Le théorème de Cayley-Hamilton implique donc que $f(T_\ell) = 0$ dans $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell\mathcal{E})$, puis le point i) appliqué à $\mathcal{E}' = \mathcal{E}$ implique que $f(\varphi) = 0$ dans $\mathrm{End}(\mathcal{E})$. Pour voir que le discriminant de f est négatif, il suffit de voir que $f(x) \geqslant 0$ pour tout $x \in \mathbb{R}$. Par continuité, il suffit de le vérifier pour $x = \frac{r}{s} \in \mathbb{Q}$ et on est donc amené à montrer la positivité de $r^2 - t(\varphi)rs + \deg(\varphi)s^2$. Or, puisque $f(X) = \det(X - T_\ell\varphi)$, on a dans $\mathbb{Z}_\ell$ l'égalité $r^2 - t(\varphi)rs + \deg(\varphi)s^2 = \det(r - sT_\ell\varphi)$. Mais d'après le ii) de la proposition, on a $\det(r - sT_\ell\varphi) = \deg(r - s\varphi) \geqslant 0$. □

3.5.4 *Fonction zêta sur un corps fini.* Soit V une variété définie sur $\mathbb{F}_q$. Notons $|V(\mathbb{F}_{q^n})|$ le nombre de points de V à valeurs dans $\mathbb{F}_{q^n}$. Afin de chercher les propriétés combinatoires de ces entiers, il serait naturel de former une série génératrice du type $\sum_{n \in \mathbb{N}^*} |V(\mathbb{F}_{q^n})| T^{n-1}$.

Néanmoins, il s'avère plus judicieux d'utiliser la variante suivante, dont la dérivée logarithmique redonne la série génératrice ci-dessus :

$$Z(V/\mathbb{F}_q, T) := \exp\left(\sum_{n\in\mathbb{N}^*} |V(\mathbb{F}_{q^n})|\frac{T^n}{n}\right) \in \mathbb{Q}[[T]].$$

Pour comprendre cette normalisation, il faut réarranger cette définition selon les "points fermés" du schéma associé à V qui, dans notre langage, correspondent aux orbites de $G_{\mathbb{F}_q}$ agissant sur $V = V(\bar{\mathbb{F}}_q)$. Notons $\mathcal{V}$ l'ensemble des points fermés et, pour $x \in \mathcal{V}$, notons $q_x = q^{n_x}$ le cardinal de son corps résiduel (si on voit x comme une $G_{\mathbb{F}_q}$-orbite, n_x est le cardinal de cette orbite). Alors on a

$$|V(\mathbb{F}_{q^n})| = \sum_{x\in\mathcal{V}, n_x|n} n_x \text{ et donc } \sum_{n\in\mathbb{N}^*} |V(\mathbb{F}_{q^n})|\frac{T^n}{n} = \sum_{x\in\mathcal{V}}\sum_{m\in\mathbb{N}^*} \frac{T^{mn_x}}{m} = -\sum_{x\in\mathcal{V}} \log(1-T^{n_x}),$$

d'où l'on tire que

$$Z(V/\mathbb{F}_q, T) = \prod_{x\in\mathcal{V}} \frac{1}{1-T^{n_x}}.$$

Si l'on pose "formellement" $T = q^{-s}$, on obtient une expression

$$\zeta_{V/\mathbb{F}_q}(s) := \prod_{x\in\mathcal{V}} \frac{1}{1-q_x^{-s}}$$

qui est un analogue clair de la fonction zêta de Riemann. C'est un bon exercice de montrer que $|V(\mathbb{F}_{q^n})| = O(q^{n.\dim(V)})$ (en utilisant le lemme de normalisation de Noether ou une récurrence sur $\dim(V)$), et on en déduit facilement que le produit ci-dessus converge normalement pour $\Re(s) > \dim(V)$.

Exemple. – $Z(\mathbb{A}^n/\mathbb{F}_q, T) = \frac{1}{1-q^nT}$, $Z(\mathbb{P}^n/\mathbb{F}_q, T) = \frac{1}{\prod_{i=0}^n (1-q^iT)}$.

Avant de calculer la fonction zêta d'une courbe elliptique, voici un exercice utile.

Exercice. – Soit R une $\mathbb{Q}$-algèbre et $A \in M_d(R)$ une matrice $d \times d$. On a dans $R[[T]]$

$$\exp\left(\sum_{n\in\mathbb{N}^*} \mathrm{tr}(A^n)\frac{T^n}{n}\right) = \frac{1}{\det(1-T\cdot A)}$$

Théorème. (Hasse) – *Soit $\mathcal{E}$ une courbe elliptique sur $\mathbb{F}_q$ et a l'entier tel que $|\mathcal{E}(\mathbb{F}_q)| = q+1-a$. Alors $Z(\mathcal{E}/\mathbb{F}_q, T)$ est une fraction rationnelle (i.e. est dans $\mathbb{Q}(T)$) et*

$$Z(\mathcal{E}/\mathbb{F}_q, T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}.$$

De plus, on a l'équation fonctionnelle $Z(\mathcal{E}/\mathbb{F}_q, T) = Z(\mathcal{E}/\mathbb{F}_q, 1/qT)$, et les racines de $T^2 - aT + q$ dans $\mathbb{C}$ sont de module $q^{\frac{1}{2}}$.

Démonstration. Soit ϕ_q l'endomorphisme de Frobenius de $\mathcal{E}$. On a déjà vu que $a = q+1-|\mathcal{E}(\mathbb{F}_q)| = \deg(\phi_q)+1-\deg(1-\phi_q)$, donc d'après le ii) du théorème 3.5.3 on a $a = \mathrm{tr}(T_\ell\phi_q)$. De même, puisque $\phi_{q^n} = \phi_q^n$, on a $|\mathcal{E}(\mathbb{F}_{q^n})| = 1+q^n-\mathrm{tr}(T_\ell\phi_q^n)$ pour tout $n \geqslant 1$. Comme le polynôme caractéristique $\det(T - T_\ell\phi_q)$ est $T^2 - aT + q$, on déduit la formule donnée pour $Z(\mathcal{E}/\mathbb{F}_q, T)$ à l'aide de l'exercice précédent. L'équation fonctionnelle se vérifie facilement. Par ailleurs, le iii) du théorème 3.5.3 nous dit que le discriminant de $T^2 - aT + q$ est négatif, donc ses racines α, β dans $\mathbb{C}$ sont conjuguées (par la conjugaison complexe). Comme $\alpha\beta = q$, on en déduit que $|\alpha| = |\beta| = q^{\frac{1}{2}}$. □

Remarque. – La fonction ζ de $\mathcal{E}$ est donc une fonction méromorphe sur $\mathbb{C}$ de la forme

$$\zeta_{\mathcal{E}/\mathbb{F}_q}(s) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})},$$

qui satisfait la même équation fonctionnelle $\zeta_{\mathcal{E}/\mathbb{F}_q}(s) = \zeta_{\mathcal{E}/\mathbb{F}_q}(1-s)$ que la fonction xi de Riemann (une variante de zêta). Le fait que les racines du polynôme au numérateur de $Z(\mathcal{E}/\mathbb{F}_q, T)$ soient de modules $q^{\frac{1}{2}}$ se traduit par le fait que les zéros de $\zeta_{\mathcal{E}/\mathbb{F}_q}(s)$ sont sur la droite $\Re(s) = \frac{1}{2}$, ce qui constitue un analogue frappant de l'hypothèse de Riemann.

Conjectures de Weil. – Lorsque V est une variété projective et lisse de dimension n, Weil avait conjecturé que la fonction zêta devait avoir la forme

$$Z(V/\mathbb{F}_q, T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)}, \quad \text{avec } P_i(T) \in \mathbb{Z}[T],$$

devait satisfaire l'équation fonctionnelle $Z(V/\mathbb{F}_q, 1/q^nT) = \pm q^{\chi\frac{n}{2}}T^\chi Z(V/\mathbb{F}_q, T)$ pour un certain entier χ, et que les racines de $P_i(T)$ dans $\mathbb{C}$ devaient être de module $q^{\frac{i}{2}}$ pour tout i. Une des raisons de croire à la forme rationnelle de $Z(V/\mathbb{F}_q, T)$ venait du fait que $\mathcal{E}(\mathbb{F}_{q^n})$ est l'ensemble des points fixes du Frobenius ϕ_q^n, et donc, par analogie avec les formules de comptage de points fixes en topologie, on pouvait s'attendre à ce que le cardinal de $\mathcal{E}(\mathbb{F}_{q^n})$ soit donné par la trace de ϕ_q^n sur l'espace vectoriel gradué fourni par une "bonne" théorie cohomologique. L'équation fonctionnelle était censée découler d'une dualité de type Poincaré. La théorie cohomologique putative a été développée par Grothendieck et son école, et appelée "cohomologie étale ℓ-adique". Ils ont montré la rationnalité et l'équation fonctionnelle. La partie "hypothèse de Riemann" des conjectures de Weil (l'estimation des modules des racines) a été prouvée par Deligne en munissant la cohomologie ℓ-adique d'une "théorie des poids", ce qui lui a valu la médaille Fields.

3.6 L'anneau des endomorphismes

Nous savons maintenant beaucoup de choses sur l'anneau $\mathrm{End}(\mathcal{E})$ des endomorphismes d'une coube elliptique. Nous savions depuis le début qu'il n'a pas de diviseurs de 0, le fait que $[m]_\mathcal{E}$ est un isogénie pour tout m implique qu'il est sans torsion comme groupe abélien, et le théorème 3.5.3 nous apprend qu'il est libre de rang au plus 4. La $\mathbb{Q}$-algèbre $\mathrm{End}(\mathcal{E})\otimes\mathbb{Q}$ qu'il engendre est donc de dimension au plus 4 et sans diviseurs de zéro. Comme

toute algèbre de dimension finie et sans diviseurs de zéro, c'est donc une *algèbre à division* (tout élément non nul est inversible). D'après le corollaire 3.2.6, on dispose aussi d'une anti-involution $\varphi \mapsto \hat{\varphi}$ sur $\mathrm{End}\,(\mathcal{E})$ telle que $\hat{\varphi}\varphi = \deg(\varphi)\,\mathrm{id}$ avec $\varphi \mapsto \deg(\varphi)$ une forme quadratique définie positive. Cette anti-involution se prolonge par linéarité à $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{Q}$ et fournit une forme quadratique deg qui est encore définie positive.

3.6.1 Lemme.– *La $\mathbb{R}$-algèbre $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{R}$ est une algèbre à division, et est donc isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$ (quaternions).*

Notons que cela n'a rien d'automatique. Par exemple $\mathbb{Q}[\sqrt{2}]$ est un corps mais $\mathbb{Q}[\sqrt{2}] \otimes \mathbb{R} = \mathbb{R}[X]/(X^2 - 2) = \mathbb{R} \times \mathbb{R}$ n'est pas intègre.

Démonstration. Prolongeons l'anti-involution $\varphi \mapsto \hat{\varphi}$ par $\mathbb{R}$-linéarité à $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{R}$. On obtient une anti-involution de la $\mathbb{R}$-algèbre $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{R}$, continue pour la topologie de $\mathbb{R}$-ev de dimension finie. En particulier on a par continuité $\deg(\varphi) := \hat{\varphi}\varphi \in \mathbb{R}_+$ pour tout $\varphi \in \mathrm{End}\,(\mathcal{E}) \otimes \mathbb{R}$. L'application $\varphi \mapsto \deg(\varphi)$ est quadratique, de forme polaire $(\varphi, \psi) \mapsto \frac{1}{2}(\hat{\psi}\varphi + \hat{\varphi}\psi)$. Elle est donc non dégénérée, puisqu'elle était non-dégénérée sur $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{Q}$ et que la non dégénérescence se lit sur le même déterminant. Puisqu'elle est positive, elle est donc définie. Toujours par continuité et densité, l'égalité $\deg(\varphi\psi) = \deg(\varphi)\deg(\psi)$ vraie pour $\varphi, \psi \in \mathrm{End}\,(\mathcal{E}) \otimes \mathbb{Q}$ est aussi vraie dans $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{R}$. On en déduit donc que $\varphi\psi = 0 \Rightarrow \varphi = 0$ ou $\psi = 0$, i.e. que $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{R}$ est une $\mathbb{R}$-algèbre à division. □

3.6.2 Corollaire.– *La $\mathbb{Q}$-algèbre $\mathrm{End}\,(\mathcal{E}) \otimes \mathbb{Q}$ est de l'une des formes suivantes :*
— *soit égale à $\mathbb{Q}$,*
— *soit une extension quadratique imaginaire de $\mathbb{Q}$,*
— *soit une algèbre de quaternions définie de centre $\mathbb{Q}$.*
De plus, si k est de caractéristique 0, alors seules les deux premières formes sont possibles.

Démonstration. La première assertion découle du lemme. La seconde découle du corollaire 3.3.3. □

Remarque. – Une extension quadratique imaginaire K de $\mathbb{Q}$ est de la forme

$$K = \mathbb{Q} \oplus \mathbb{Q}\alpha, \quad \text{avec } \alpha^2 \in \mathbb{Q}_{<0}.$$

Une algèbre de quaternions D sur $\mathbb{Q}$ est une algèbre à division de dimension 4 sur $\mathbb{Q}$ et de centre $\mathbb{Q}$. Si K est une extension de $\mathbb{Q}$, alors la K-algèbre $D \otimes_{\mathbb{Q}} K$ est soit une algèbre à division, soit isomorphe à $M_2(K)$. Dans ce cas on dit que D est *déployée* sur K. Lorsque D n'est pas déployée sur $\mathbb{R}$, on dit qu'elle est *définie*. Dans ce cas on a $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{H}$. Une algèbre de quaternions sur $\mathbb{Q}$ qui est définie est de la forme suivante :

$$D = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\beta \oplus \mathbb{Q}\alpha\beta, \quad \text{avec } \alpha^2, \beta^2 \in \mathbb{Q}_{<0} \text{ et } \beta\alpha = -\alpha\beta.$$

Remarque. – Si $\mathrm{End}(\mathcal{E}) \otimes \mathbb{Q}$ est une algèbre de quaternions, alors k est de caractéristique $p > 0$. D'après i) du théorème 3.5.3, on a pour tout premier $\ell \neq p$ un morphisme injectif

de $\mathbb{Q}_\ell$-algèbres $\mathrm{End}(\mathcal{E}) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(T_\ell\mathcal{E} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$. Par égalité des dimensions, c'est donc un isomorphisme. On voit donc que l'algèbre des quaternions $\mathrm{End}(\mathcal{E}) \otimes \mathbb{Q}$ se déploie sur $\mathbb{Q}_\ell$ pour tout $\ell \neq p$. On peut montrer qu'il existe une unique (à isomorphisme près) algèbre de quaternions D_p sur $\mathbb{Q}$ qui soit définie et déployée sur $\mathbb{Q}_\ell$ pour tout $\ell \neq p$. De plus, D_p est non déployée sur $\mathbb{Q}_p$.

Remarque. – On voit donc que $\mathrm{End}(\mathcal{E})$ est un sous-anneau $\mathcal{D}$ d'une $\mathbb{Q}$-algèbre à division D (éventuellement commutative) qui est aussi un réseau dans le $\mathbb{Q}$-ev sous-jacent. Un tel sous anneau $\mathcal{D}$ est appelé *un ordre* de D.

3.6.3 *Multiplication complexe.* Supposons ici que k est de caractéristique nulle. On dit que $\mathcal{E}$ a *multiplication complexe* si $\mathrm{End}(\mathcal{E}) \neq \mathbb{Z}$.

Le cas $k = \mathbb{C}$. Dans ce cas, on sait d'après le cours "Surfaces de Riemann" qu'on peut uniformiser $\mathcal{E}$ par un bi-holomorphisme $\mathbb{C}/\Lambda \xrightarrow{\sim} \mathcal{E}(\mathbb{C})$. On sait aussi que les endomorphismes analytiques de $\mathbb{C}/\Lambda$ sont les homothéties respectant Λ, c'est-à-dire $\mathrm{End}_{\mathrm{an}}(\mathbb{C}/\Lambda) = \{z \in \mathbb{C}, z\Lambda \subset \Lambda\}$. Pour voir que ces endomorphismes analytiques dont algébriques, il suffit de remarquer qu'ils induisent des endomorphismes du corps $\mathcal{M}(\mathbb{C}/\Lambda)$ des fonctions méromorphes sur $\mathbb{C}/\Lambda$, et que ce corps $\mathcal{M}(\mathbb{C}/\Lambda) = \mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ coïncide avec le corps des fonctions rationnelles $\mathbb{C}(\mathcal{E})$, et enfin rappeler que tout endomorphisme de $\mathbb{C}(\mathcal{E})$ provient d'un endomorphisme de $\mathcal{E}$. On a donc $\mathrm{End}(\mathcal{E}) \simeq \{z \in \mathbb{C}, z\Lambda \subset \Lambda\}$.

Soit maintenant une extention quadratique imaginaire $K \subset \mathbb{C}$ de $\mathbb{Q}$. Si R est un *ordre* de K, i.e. un sous-anneau libre de rang 2 sur $\mathbb{Z}$, c'est aussi un réseau de $\mathbb{C}$, et on a visiblement $\mathrm{End}(\mathbb{C}/R) = R$. On voit ainsi que tout ordre quadratique R est l'anneau des endomorphismes d'au moins une courbe elliptique sur $\mathbb{C}$. Plus généralement, si $\Lambda \subset K$ est un R-module *inversible*[2], on a encore $\mathrm{End}(\mathbb{C}/\Lambda) = R$. Deux R-modules inversibles Λ et Λ' sont isomorphes si et seulement si ils sont K-homothétiques (exercice) et donc si et seulement si $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$. On peut montrer qu'on établit ainsi une bijection

$$\{\text{Courbes ell. sur } \mathbb{C} \text{ avec } \mathrm{End}(\mathcal{E}) = R\}_{/\sim} \longleftrightarrow \mathrm{Pic}(R) = \{R\text{-modules inversibles}\}_{/\sim}.$$

Exercice. – Notons $\mathcal{O}_K$ l'anneau des entiers de K, i.e. la clôture intégrale de $\mathbb{Z}$ dans K.

i) Montrer que $\mathcal{O}_K$ est l'unique ordre maximal de K (pour l'inclusion) et que tout ordre est de la forme $R = \mathbb{Z} + n\mathcal{O}_K$ avec $n \in \mathbb{N}^*$.

ii) Montrer qu'il existe un unique $D \in \mathbb{N}$ sans facteur carré tel que $K = \mathbb{Q}[\sqrt{-D}]$, puis montrer que $\mathcal{O}_K$ est donné par

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-D}], \text{ si } D \equiv 1[4], \quad \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-D}}{2}], \text{ si } D \equiv 3[4].$$

Dans le deuxième cas, $\mathbb{Z}[\sqrt{-D}] = \mathbb{Z} + 2\mathcal{O}_K$ est un ordre non maximal de $\mathbb{Q}[\sqrt{-D}]$.

2. i.e. tel qu'il existe un autre R-module $\Lambda' \subset K$ tel que $\Lambda \cdot \Lambda' = R$.

Remarque. – Si $\mathcal{E}$ est définie sur $\mathbb{R}$, il faut prendre garde au fait que les endomorphismes de $\mathcal{E}$ définis sur $\mathbb{C}$ ne sont pas nécessairement définis sur $\mathbb{R}$. En fait, via son action sur une différentielle invariante définie sur $\mathbb{R}$ (par exemple $\frac{dx}{y}$ si $\mathcal{E}$ est donnée par une équation de Weierstraß $y^2 = x^3 + ax + b$), on a un plongement $\mathrm{End}\,(\mathcal{E}_{/\mathbb{R}}) \hookrightarrow \mathbb{R}$ qui montre que $\mathrm{End}(\mathcal{E}_{/\mathbb{R}}) = \mathbb{Z}$ même si $\mathcal{E}$ a multiplication complexe sur $\mathbb{C}$. En d'autres termes, l'action du générateur de $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ sur $\mathrm{End}\,(\mathcal{E})$ est l'unique automorphisme non-trivial de l'anneau $\mathrm{End}\,(\mathcal{E})$, si celui-ci contient strictement $\mathbb{Z}$.

Exemple. – Soit $k = \mathbb{Q}$ et $\mathcal{E}$ la courbe d'équation affine $y^2 = x^3 + x$. L'application $(x, y) \mapsto (-x, iy)$ définit un automorphisme de $\mathcal{E}$ défini sur $\mathbb{Q}[i]$. C'est un automorphisme d'ordre 4, qui montre que $\mathrm{End}\,(\mathcal{E}_{/\mathbb{Q}[i]}) = \mathbb{Z}[i]$. En utilisant le fait que $\mathbb{Z}[i]$ est principal, on en déduit que $\mathcal{E}(\mathbb{C}) \simeq \mathbb{C}/\mathbb{Z}[i]$.

Proposition. – *Supposons que $\mathcal{E}$ a multiplication complexe définie sur k. Alors l'image de G_k dans $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell\mathcal{E})$ est abélienne pour tout premier ℓ, et l'action de G_k sur $\mathcal{E}[m]$ se factorise par l'abélianisé $G_{k,\mathrm{ab}}$ de G_k pour tout entier m.*

Démonstration. Notons $R = \mathrm{End}\,(\mathcal{E}_{/k})$, qui est donc un ordre dans une extension quadratique imaginaire K de $\mathbb{Q}$. Alors $T_\ell(\mathcal{E})$ est un $R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module fidèle (par le i) du théorème 3.5.3), et donc $T_\ell(\mathcal{E}) \otimes \mathbb{Q}_\ell$ est un $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module fidèle aussi. Puisque $T_\ell(\mathcal{E}) \otimes \mathbb{Q}_\ell$ est de dimension 2 sur $\mathbb{Q}_\ell$, il est libre de dimension 1 sur $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Ainsi la représentation Galoisienne $\rho_{\mathcal{E},\ell^\infty}$ se factorise en

$$\rho_{\mathcal{E},\ell^\infty} : G_k \longrightarrow (K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times = \mathrm{GL}_1(K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell),$$

ce qui montre que son image est abélienne. Il s'ensuit que l'action de G_k sur $\mathcal{E}[\ell^n]$ est abélienne aussi, ainsi que celle sur $\mathcal{E}[m] = \prod_\ell \mathcal{E}[\ell^{v_\ell(m)}]$. □

Remarque. – Si dans la preuve du lemme on a $K = \mathbb{Q}[\sqrt{-D}]$ et $(\ell, 2D) = 1$, alors on a $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathbb{Q}_\ell \times \mathbb{Q}_\ell$ si $-D$ est un carré modulo ℓ. Sinon, $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ est l'extension quadratique non ramifiée de $\mathbb{Q}_\ell$.

Remarque. – Lorsque $\mathcal{E}$ n'a pas multiplication complexe et k est une extension finie de $\mathbb{Q}$, un théorème de Serre affirme que $\rho_{\mathcal{E},\ell^\infty}(G_k)$ est d'indice fini dans $\mathrm{GL}_2(\mathbb{Z}_\ell)$, et donc, en quelque sorte aussi peu abélien que possible.

Remarque culturelle sur le "Kronecker's Jugendtraum". – Si K est une extension finie de $\mathbb{Q}$, notons K_{ab} son *extension abélienne maximale*. C'est la réunion de toutes les extensions finies Galoisiennes de K de groupe de Galois abélien sur K. C'est aussi le sous-corps de $\bar{\mathbb{Q}}$ fixe par le sous-groupe des commutateurs de $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$. C'est donc une extension Galoisienne a priori infinie de groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/K)_{\mathrm{ab}}$. Le théorème de Kronecker-Weber affirme que $\mathbb{Q}_{\mathrm{ab}}$ est l'extension cyclotomique de $\mathbb{Q}$, c'est-à-dire l'extension engendrée par toutes les racines de l'unité. On peut voir cela de plusieurs manières :

— L'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur $(\mathbb{G}_m)_{\mathrm{tors}}$ se factorise fidèlement par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})_{\mathrm{ab}}$.

— $\mathbb{Q}_{\mathrm{ab}}$ est engendrée par les points de torsion de $\mathbb{G}_m$.

— $\mathbb{Q}_{\mathrm{ab}}$ est engendrée par les valeurs "spéciales" $\exp(2i\pi z)$, $z \in \mathbb{Q}$ de la fonction analytique $\mathbb{Z}$-périodique exponentielle.

Les courbes à multiplication complexe permettent de généraliser ceci à toute extension quadratique imaginaire K. C'est plus facile lorsque $\mathcal{O}_K$ est principal, comme c'est le cas par exemple pour $K = \mathbb{Q}[i]$. Dans ce cas précis, soit $\mathcal{E}$ la courbe elliptique sur $\mathbb{Q}$ de l'exemple ci-dessus, alors on peut montrer que :

— L'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[i])$ sur $\mathcal{E}_{\mathrm{tors}}$ se factorise fidèlement par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[i])_{\mathrm{ab}}$.

— $\mathbb{Q}[i]_{\mathrm{ab}}$ est engendrée par les coordonnées x, y des points de torsion de $\mathcal{E}$.

— $\mathbb{Q}[i]_{\mathrm{ab}}$ est engendrée par les valeurs spéciales $\wp_i(z)$ et $\wp_i'(z)$, $z \in \mathbb{Q}[i]$, des fonctions $\mathbb{Z}[i]$-périodiques analytiques de Weierstraß.

Pour plus de détails, cf les cours "Formes modulaires" et "Corps de classe", ou [Silverman C.11].

3.6.4 *Courbes elliptiques supersingulières.* Supposons maintenant k de caractéristique p. Rappelons que $\mathcal{E}$ est dite supersingulière si $\hat{\phi}_p$ est inséparable, ce qui équivaut à $[p]_{\mathcal{E}} = \hat{\phi}_p \circ \phi_p$ purement inséparable, ou encore à $\mathcal{E}[p] = \{0\}$.

Lemme. – *Toute courbe elliptique supersingulière sur k peut être définie sur $\mathbb{F}_{p^2}$. En particulier, il n'y a qu'un nombre fini de telles courbes à isomorphisme près.*

Démonstration. Si $\mathcal{E}$ est supersingulière, alors $\hat{\phi}_p : \mathcal{E}^{(p)} \longrightarrow \mathcal{E}$ est inséparable, donc se factorise en $\mathcal{E}^{(p)} \xrightarrow{\phi_p^{(p)}} \mathcal{E}^{(p^2)} \xrightarrow{\psi} \mathcal{E}$, où $\phi_p^{(p)}$ désigne l'isogénie de Frobenius de $E^{(p)}$. Par comparaison des degrés, on a $\deg(\psi) = 1$, donc ψ est un isomorphisme $\mathcal{E}^{(p^2)} \xrightarrow{\sim} \mathcal{E}$. Comme nous le verrons dans la prochaine section ...., on a $j(\mathcal{E}^{(p)}) = j(\mathcal{E})^p$, donc cet isomorphisme implique que $j(\mathcal{E}) \in \{\lambda \in k, \lambda^{p^2} = \lambda\} \subset \mathbb{F}_{p^2}$ et finalement que $\mathcal{E}$ peut être définie sur $\mathbb{F}_{p^2}$. Il est clair qu'il n'y a qu'un nombre fini de cubiques planes définies sur $\mathbb{F}_{p^2}$. □

Nous allons voir plus loin que le nombre de courbes supersingulières est non nul !

Proposition. – *Supposons que $k = \bar{\mathbb{F}}_p$. Alors $\mathcal{E}$ est supersingulière si et seulement si* $\mathrm{End}(\mathcal{E})$ *est une algèbre de quaternions. Si $\mathcal{E}$ est ordinaire,* $\mathrm{End}(\mathcal{E})$ *est quadratique.*

Démonstration. Montrons d'abord que si $\mathcal{E}$ est ordinaire alors $\mathrm{End}(\mathcal{E})$ est commutatif. Pour cela, on regarde l'action de $\mathrm{End}(\mathcal{E})$ sur le module de Tate $T_p\mathcal{E} = \varprojlim_n \mathcal{E}[p^n]$. Puisque $\mathcal{E}$ est ordinaire, on a $T_p\mathcal{E} \simeq \mathbb{Z}_p$ donc l'action en question est donnée par un morphisme $\mathrm{End}(\mathcal{E}) \longrightarrow \mathrm{End}_{\mathbb{Z}_p}(T_p\mathcal{E}) = \mathbb{Z}_p$. Or ce morphisme est injectif car $\bigcup_{n\in\mathbb{N}} \mathcal{E}[p^n]$ est infini et donc Zariski dense. Pour voir que $\mathrm{End}(\mathcal{E})$ est quadratique, on choisit q tel que $\mathcal{E}$ est définie sur $\mathbb{F}_q$ (il suffit par exemple de prendre $\mathbb{F}_q$ contenant tous les coefficients d'une équation de Weierstraß de $\mathcal{E}$). On dispose alors d'un endomorphisme de Frobenius ϕ_q de $\mathcal{E}$ et nous allons montrer qu'il n'est pas dans $\mathbb{Z}$. En effet, si ϕ_q était dans $\mathbb{Z}$ alors, puisque $\deg(\phi_q) = q$, on devrait avoir $\phi_q = [p^r]_{\mathcal{E}}$ avec $q = p^{2r}$. Mais alors $[p^r]_{\mathcal{E}}$ serait purement inséparable et donc $[p]_{\mathcal{E}}$ aussi, ce qui contredit l'ordinarité de $\mathcal{E}$.

Supposons maintenant que $R := \mathrm{End}(\mathcal{E})$ est commutatif. Alors on peut trouver un ensemble infini $\mathcal{L}$ de nombres premiers $\ell \neq p$ tel que ℓR soit un idéal premier de R (si

$R = \mathbb{Z} + n\mathbb{Z}[\sqrt{-D}]$, il suffit de prendre ℓ premier à $2nD$ et tel que $-D$ ne soit pas un carré modulo ℓ). Dans ce cas $R \otimes \mathbb{Z}_\ell$ est un anneau de valuation discrète d'uniformisante ℓ, et donc tout endomorphisme φ de $\mathcal{E}$ s'écrit $\varphi = \varphi' \circ [\ell]_{\mathcal{E}}^v$ avec $T_\ell \varphi'$ inversible, i.e. $(\deg(\varphi'), \ell) = 1$. En particulier, pour tout endomorphisme $\varphi \in \mathrm{End}(\mathcal{E})$ et tout $\ell \in \mathcal{L}$, la valuation ℓ-adique $v_\ell(\varphi)$ du degré de φ est paire. Choisissons alors pour chaque $\ell \in \mathcal{L}$ une isogénie $\mathcal{E} \xrightarrow{\varphi_\ell} \mathcal{E}_\ell$ de degré ℓ (par exemple, un "quotient" au sens du lemme 3.2 de $\mathcal{E}$ par le sous-groupe engendré par un point non nul de $\mathcal{E}[\ell]$). Alors si $\ell \neq \ell'$, les courbes elliptiques $\mathcal{E}_\ell$ et $\mathcal{E}_{\ell'}$ ne sont pas isomorphes, puisque si elles l'étaient on aurait un endomorphisme $\hat{\varphi}_{\ell'} \circ \varphi_\ell$ de $\mathcal{E}$ de degré $\ell\ell'$, ce qui est impossible. Nous avons donc construit une infinité de courbes elliptiques $\mathcal{E}_\ell$ toutes isogènes à $\mathcal{E}$ mais deux à deux non isomorphes. Or, si $\mathcal{E}$ était supersingulière, chaque $\mathcal{E}_\ell$ le serait aussi, puisque l'égalité $[p]_{\mathcal{E}_\ell} \circ \varphi_\ell = \varphi_\ell \circ [p]_{\mathcal{E}}$ implique $\deg_i [p]_{\mathcal{E}_\ell} = \deg_i [p]_{\mathcal{E}} = p^2$. Mais ceci contredirait le lemme ci-dessus, donc $\mathcal{E}$ est ordinaire. □

Tout cela ne nous dit pas encore que les courbes supersingulières existent. Voici un critère utile.

LEMME. – *Si $k = \mathbb{F}_q$, $\mathcal{E}$ est supersingulière si et seulement si $|\mathcal{E}(\mathbb{F}_q)| \equiv 1[p]$.*

Démonstration. On a dans $\mathrm{End}(\mathcal{E})$ l'égalité $[|\mathcal{E}(\mathbb{F}_q)|] = [\deg(1 - \phi_q)] = (1 - \hat{\phi}_q)(1 - \phi_q) = 1 - \hat{\phi}_q - \phi_q + [\deg(\phi_q)]$. En écrivant $|\mathcal{E}(\mathbb{F}_q)| = 1 + q - a$, on a donc $\hat{\phi}_q = [a] - \phi_q$. Si ω est une différentielle régulière sur $\mathcal{E}$, il vient $\hat{\phi}_q^* \omega = a\omega$, et donc $\hat{\phi}_q$ est inséparable si et seulement si a est nul dans k, i.e. $p|a$. □

Application. – La courbe elliptique $y^2 + y = x^3$ sur $\mathbb{F}_2$ a 3 points rationnels O, $[0 : 0 : 1]$ et $[0 : 1 : 1]$, donc est supersingulière.

Supposons maintenant $p > 2$. On sait alors qu'une courbe elliptique $\mathcal{E}$ sur $k = \mathbb{F}_q$ admet une équation de Weierstraß de la forme $y^2 = f(x)$ avec $f \in k[X]$ unitaire de degré 3. On peut compter les $\mathbb{F}_q$-points de $\mathcal{E}$ en remarquant que pout tout $x \in \mathbb{F}_q$, on a 2 (resp. 1, resp. 0) points de $\mathcal{E}$ d'abscisse x selon que $f(x)$ est un carré non nul (resp. nul, resp. pas un carré). Soit donc $\chi : \mathbb{F}_q^\times \longrightarrow \{\pm 1\}$ l'unique caractère non trivial d'ordre 2 de $\mathbb{F}_q^\times$, que l'on prolonge par $\chi(0) := 0$. On a (en n'oubliant pas le point à l'infini)

$$|\mathcal{E}(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x)).$$

LEMME. – *$\mathcal{E}$ est supersingulière $\Leftrightarrow$ le coefficient de x^{p-1} dans $f(x)^{\frac{(p-1)}{2}}$ est nul.*

Démonstration. En utilisant le lemme précédent et le fait que $\chi(t) = t^{\frac{(q-1)}{2}}$ dans $\mathbb{F}_q$, on voit que $\mathcal{E}$ est supersingulière si et seulement si $\sum_{x \in \mathbb{F}_q} f(x)^{\frac{(q-1)}{2}} = 0$.

Pour $n \in \mathbb{N}$, posons $e = (n, q-1)$ et $d = \frac{q-1}{e}$. Alors la somme $\sum_{x \in \mathbb{F}_q} x^n$ est e fois la somme des racines d-èmes de l'unité dans $\mathbb{F}_q$. Cette somme est donc non nulle si et seulement si $d = 1$, i.e. $(q-1)|n$, auquel cas elle vaut $q - 1 = -1$.

Puisque $\deg(f) = 3$, on en déduit que $\sum_{x\in\mathbb{F}_q} f(x)^{\frac{(q-1)}{2}} = -c_q$, où c_q est le coefficient de x^{q-1} dans $f(x)^{\frac{(q-1)}{2}}$. Mais en écrivant $f(x)^{\frac{(p^r-1)}{2}} = f(x)^{\frac{(p^{r-1}-1)}{2}}(f(x)^{\frac{(p-1)}{2}})^{p^{r-1}}$, on vérifie (exercice) que $c_{p^r} = c_{p^{r-1}}c_p^{p^{r-1}}$, ce qui montre que $c_q = 0$ si et seulement si $c_p = 0$. □

Après extension du corps $\mathbb{F}_q$, le polynôme $f(x)$ se scinde, et un changement de coordonnées permet de mettre l'équation de $\mathcal{E}$ sous forme de Legendre $y^2 = x(x-1)(x-\lambda)$ avec $\lambda \in \bar{\mathbb{F}}_p$. En posant $m = \frac{p-1}{2}$, un calcul montre que $c_p = (-1)^m \sum_{i=0}^m \binom{m}{i}^2 \lambda^i$.

Corollaire. – *Une courbe elliptique de Legendre $y^2 = x(x-1)(x-\lambda)$ est supersingulière si et seulement si $H_p(\lambda) = 0$ où $H_p(\lambda) = \sum_{i=0}^m \binom{m}{i}^2 \lambda^i$*

Le polynôme H_p étant visiblement non nul, on en déduit l'existence de courbes supersingulières. On peut même les compter, cf [Silverman, V.4.1 (c)].

Remarque historique : à l'époque où les mathématiciens cherchaient une bonne théorie cohomologique sur les variétés sur $\bar{\mathbb{F}}_p$ afin d'estimer le nombre de $\mathbb{F}_{p^n}$-points, Serre a remarqué que l'existence de courbes supersingulières empêchait l'existence d'une telle cohomologie à coefficients dans $\mathbb{Q}$ ou même $\mathbb{R}$. En effet, le H^1 d'une telle théorie doit être de dimension 2 pour toute courbe elliptique $\mathcal{E}$ (comme sur $\mathbb{C}$), mais par ailleurs le H^1 doit être muni d'une action de $\mathrm{End}(\mathcal{E})$. Or l'algèbre des quaternions $\mathbb{H}$ n'agit sur aucun $\mathbb{R}$-ev de dimension 2. Cette obstruction disparaît si on remplace $\mathbb{R}$ par $\mathbb{Q}_\ell$ avec $\ell \neq p$, puisque, comme on l'a vu, $\mathrm{End}(\mathcal{E})$ est déployée sur $\mathbb{Q}_\ell$.

Remarque. – On vient de voir que les courbes supersingulières sont rares sur $\overline{\mathbb{F}}_p$ (et même en nombre fini). Néanmoins, lorsqu'on part d'une courbe elliptique $\mathcal{E}$ sur $\mathbb{Q}$ et qu'on considère sa réduction modulo p (que l'on définira proprement plus loin), un résultat de Elkies dit qu'il existe une infinité de premiers pour lesquels la réduction est supersingulière. Mais la situation est très différente selon que $\mathcal{E}$ a multiplication complexe ou non. Dans le premier cas, on peut montrer que l'ensemble des premiers où $\mathcal{E}$ a réduction supersingulière est de densité $\frac{1}{2}$, dans le second cas, Serre a montré qu'il a densité 0.

Exemple. – Soit $\mathcal{E}$ la courbe sur $\mathbb{Q}$ d'équation $y^2 = x^3 + 1$. Le coefficient c_p du terme en x^{p-1} de $(x^3+1)^{\frac{p-1}{2}}$ est 0 si $p \equiv 2[3]$, auquel cas la réduction de $\mathcal{E}$ est donc supersingulière, $c_p = \binom{(p-1)/2}{(p-1)/3}$ si $p \equiv 1[3]$, auquel cas la réduction de $\mathcal{E}$ est ordinaire.

3.7 Équations de Weierstraß

3.7.1 *Discriminant et invariant j.* Pour une équation de Weierstraß générale $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ on trouve dans [Silverman, III.1] des formules pour le discriminant Δ et l'invariant j (qui n'est défini que si $\Delta \neq 0$). Des calculs fastidieux mais élémentaires montrent que pour tout changement de coordonnées préservant la forme de Weierstraß, c'est-à-dire de la forme $x' = u^2x + r$, $y' = u^3y + u^2sx + t$, ces quantités varient de la manière suivante : $\Delta' = u^{12}\Delta$ et $j' = j$ (d'où son nom d'invariant).

Plutôt que de donner ces formules dans le cas général, on les donne pour les équations de Weierstraß simplifiées par un changement de coordonnées adéquate, selon la caractéristique

de k. Il est alors immédiat de vérifier la variance de Δ et j.

i) Si $\mathrm{car}(k) \neq 2, 3$, on peut se ramener à $y^2 = x^3 + a_4x + a_6$, de manière unique modulo un changement de coordonnées $(x, y) \to (u^2x, u^3y)$. On pose alors

$$\Delta = -16(4a_4^3 + 27a_6^2) \text{ et } j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

ii) Si $\mathrm{car}(k) = 3$, on peut se ramener à l'une des deux formes suivantes
   (a) $y^2 = x^3 + a_4x + a_6$, de manière unique modulo $(x, y) \to (u^2x + r, u^3y)$. On pose alors $\Delta = -a_4^3$ et $j = 0$.
   (b) $y^2 = x^3 + a_2x^2 + a_6$, de manière unique modulo $(x, y) \to (u^2x, u^3y)$. On pose alors $\Delta = -a_2^3a_6$ et $j = -\frac{a_2^3}{a_6}$.

iii) Si $\mathrm{car}(k) = 2$, on peut se ramener à l'une des deux formes suivantes
   (a) $y^2 + a_3y = x^3 + a_4x + a_6$, de manière unique modulo $(x, y) \to (u^2x + s^2, u^3y + u^2sx + t)$. On pose alors $\Delta = a_4^3$ et $j = 0$.
   (b) $y^2 + xy = x^3 + a_2x^2 + a_6$, de manière unique modulo $(x, y) \to (x', y' + sx')$. On pose alors $\Delta = a_6$ et $j = \frac{1}{a_6}$.

Remarque. – Dans le cas où l'équation est de la forme $y^2 = f(x)$, on constate que $\Delta = 16.\mathrm{disc}(f)$. En particulier, si $f(x) = (x - x_1)(x - x_2)(x - x_3)$ on a

$$\Delta = 16(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

LEMME. – *Une équation de Weierstraß définit une courbe non singulière (et donc une courbe elliptique avec $O = [0 : 1 : 0]$ comme élément neutre) si et seulement si $\Delta \neq 0$.*

Démonstration. On vérifie d'abord facilement que O n'est jamais singulier. Dans le cas où l'équation est de la forme $y^2 = f(x)$ (i.e. en caractéristique $\neq 2$), on peut supposer f scindé $f = (x-x_1)(x-x_2)(x-x_3)$ puisque la non-singularité se teste sur la clôture algébrique de k. Alors les seuls points singuliers possibles sont en $(0, x_i)$ et un tel point est singulier si et seulement si x_i est racine multiple de f, i.e. si et seulement si $\Delta = 0$. En caractéristique 2 : exercice. □

L'invariant j introduit plus haut est donc bien défini lorsque l'équation définit une courbe elliptique. Comme il ne varie pas par changement de coordonnées "admissible", le théorème 3.1.3 assure que *si $\mathcal{E}$ est une courbe elliptique sur k, l'invariant j associé à toute équation de Weierstraß de $\mathcal{E}$ ne dépend que de $\mathcal{E}$*. En particulier, si $\mathcal{E}'$ est isomorphe (sur k ou sur $\bar{k}$) à $\mathcal{E}'$, on a $j(\mathcal{E}) = j(\mathcal{E}')$.

Remarque. – Si k est de caractéristique p et $\mathcal{E}$ est donnée par une équation de Weierstraß associée à $a_1, \cdots, a_6$, alors $\mathcal{E}^{(p)}$ est, par définition, donnée par l'équation associée à $a_1^p, \cdots, a_6^p$. Donc $j(\mathcal{E}^{(p)}) = j(\mathcal{E})^p$.

Exercice. – Si $\mathcal{E}$ est donnée par une équation de Legendre $y^2 = x(x-1)(x-\lambda)$, alors

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

3.7.2 Proposition.– *Avec les notations introduites ci-dessus.*
i) Pour tout $j \in k$, il existe une courbe elliptique $\mathcal{E}$ sur k telle que $j(\mathcal{E}) = j$.
ii) Si $j(\mathcal{E}) = j(\mathcal{E}')$ alors $\mathcal{E}$ et $\mathcal{E}'$ sont isomorphes sur $\bar{k}$.
iii) $\operatorname{Aut}\mathcal{E}_{/\bar{k}}$ *est un groupe fini. Son ordre est donné par le tableau*

$j(\mathcal{E})$	$\operatorname{car}(k)$	$\lvert\operatorname{Aut}\mathcal{E}\rvert$
$\neq 0, 1728$		2
1728	$\neq 2, 3$	4
0	$\neq 2, 3$	6
0	3	12
0	2	24

Démonstration. i) En caractéristique 2 ou 3, c'est clair vu les formules données plus haut. En caractéristique $\neq 2, 3$ et lorsque $j \neq 0, 1728$, on peut prendre $\mathcal{E}$ donnée par $y^2 = 4x^3 - \frac{27j}{j-1728}x^2 - \frac{27j}{j-1728}$. De plus, la courbe $y^2 = x^3 + 1$ a pour invariant $j = 0$ et la courbe $y^2 = x^3 + x$ a pour invariant $j = 1728$.

ii) Si k est de caractéristique $\neq 2, 3$, et $\mathcal{E}$, resp. $\mathcal{E}'$, donnée par l'équation courte associée à (a_4, a_6), resp. à (a'_4, a'_6), alors on a plusieurs cas :

– si $a_4 a_6 \neq 0$, on doit avoir $a'_4 a'_6 \neq 0$ et $a_6^2 a_4^{-3} = a_6'^2 a_4'^{-3}$. Il suffit alors de changer de coordonnées $x' = u^2 x$, $y' = u^3 y$ avec $u = (a'_4 a_4^{-1})^{1/4}$.

– si $a_6 = 0$, alors $a_4 \neq 0$ donc $a'_6 = 0$ et le même changement de coordonnées convient.

– si $a_4 = 0$, alors $a'_4 = 0$ et il suffit de changer de coordonnées avec $u = (a'_6 a_6^{-1})^{1/6}$.

Lorsque k est de caractéristique 2 ou 3 c'est un peu plus compliqué mais tout aussi élémentaire, voir [Silverman, appendice A].

iii) Si $\iota_{x,y}$ est un isomorphisme de $\mathcal{E}$ sur une cubique de Weierstraß, alors pour tout automorphisme σ de $\mathcal{E}$, $\iota_{x,y} \circ \sigma$ est un autre isomorphisme de $\mathcal{E}$ sur la même cubique. D'après le ii) du théorème 3.1.3, on sait que $\iota_{x,y} \circ \sigma$ se déduit de $\iota_{x,y}$ par un changement de coordonnées linéaire sur $\mathbb{P}^2$, et celui-ci doit préserver l'équation de Weierstraß fixée. Il s'agit donc de trouver les changements de coordonnées qui préservent une équation de l'une des formes ci-dessus.

Lorsque k de caractéristique $\neq 2, 3$ et $\mathcal{E}$ donnée par $y^2 = x^3 + a_4 x^2 + a_6$, les seuls automorphismes sont de la forme $(x', y') = (ux, uy)$ avec $u^4 a_4 = a_4$ et $u^6 a_6 = a_6$. On en déduit donc que $\operatorname{Aut}\mathcal{E}$ est cyclique d'ordre donné dans l'énoncé.

Calculer l'ordre pour $j = 0$ en caractéristique 2 et 3 est encore élémentaire. Les groupes obtenus ne sont pas abéliens. □

Exercice. – Vérifier que si $j(\mathcal{E}) = j(\mathcal{E}') \neq 0, 1728$, les courbes $\mathcal{E}$ et $\mathcal{E}'$ sont isomorphes sur une extension quadratique de k. En utilisant que $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ est infini, en déduire que pour chaque $j \in \mathbb{Q}$, il y a une infinité de courbes elliptiques sur $\mathbb{Q}$ d'invariant j et 2 à 2 non $\mathbb{Q}$-isomorphes .

3.7.3 *Équations de Weierstraß singulières.* On suppose ici que $\Delta = 0$. On a vu dans la preuve du premier lemme ci-dessus qu'il y a exactement un point singulier dans $\mathbb{A}^2(\bar{k})$. Comme G_k stabilise le lieu régulier, ce point est k-rationnel et, par un changement de coordonnées, on peut supposer que c'est $(0,0)$. L'équation n'est alors plus de la forme simplifiée mais est nécessairement de la forme

$$y^2 + a_1xy - a_2x^2 = x^3.$$

Appelons C la courbe définie par cette équation, et notons $C^* := C \setminus \{(0,0)\}$ le lieu lisse. Le cône tangent à C en $(0,0)$ est le lieu d'annulation de la forme quadratique du membre de gauche. Soit k' un corps de décomposition de $T^2 + a_1T - a_2$ sur k et soient λ, μ les deux racines de ce polynôme dans k'. L'équation de C sur k' est donc

$$(y - \lambda x)(y - \mu x) = x^3.$$

Deux cas se présentent.

– si $\lambda \neq \mu$ alors $(0,0)$ est un point de croisement avec deux tangentes $y = \lambda x$ et $y = \mu x$. De plus l'application $[X : Y : Z] \mapsto \frac{Y-\lambda X}{Y-\mu X}$ définit un isomorphisme de k'-variétés

$$C^* \xrightarrow{\sim} \mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\} = \bar{k}^\times$$

dont l'inverse est donné par $t \mapsto P(t) := [t - 1 : \mu t - \lambda : \frac{(t-1)^3}{t(\mu-\lambda)^2}]$. Ce morphisme est défini sur k si l'on tord l'action de Galois naturelle sur $\mathbb{G}_m$ en posant $\sigma \cdot z := \sigma(z)^{\chi(\sigma)}$ où $\chi : G_k \twoheadrightarrow \mathrm{Gal}(k'/k) \longrightarrow \{\pm 1\}$ est le caractère associé à k' (qui est trivial si $k' = k$). Dans ce cas, on obtient au niveau des k-points une bijection $C^*(k) \xrightarrow{\sim} \mathrm{Ker}\, N_{k'/k} = \{z \in (k')^\times, z\tau(z) = 1\}$ avec τ le générateur de $\mathrm{Gal}(k'/k)$.

– si $\lambda = \mu$ alors $(0,0)$ est un point de rebroussement (un "cusp") et on a une seule tangente $y = \lambda x$. Dans ce cas, $k' = k$ et on a un isomorphisme de k-variétés

$$C^* \xrightarrow{\sim} \mathbb{A}^1, \ [X : Y : Z] \mapsto \frac{X}{Y - \lambda X}$$

dont l'inverse est donné par $u \mapsto P(u) := [u : 1 + \lambda u : u^3]$.

Dans chacun des cas, on voit donc que C est birationnelle à $\mathbb{P}^1$. On remarque aussi que la cible de l'isomorphisme est une variété-groupe (groupe multiplicatif $\mathbb{G}_m$ ou groupe additif $\mathbb{A}^1$). Ceci n'est pas un hasard.

Lemme. – *Il existe sur C^* une unique loi de groupe telle que pour tout triplet de points $P, Q, R \in C^*$, on a $P + Q + R = O$ si et seulement si $[P, Q, R]$ est l'intersection (comptée avec multiplicité) de C^* avec une droite. De plus, les isomorphismes de variétés décrits ci-dessus sont des isomorphismes de groupes.*

Démonstration. Remarquons qu'une droite passant par le point singulier $(0,0)$ y coupe C avec multiplicité $\geqslant 2$. Ainsi, dès lors qu'une droite intersecte C^* en 2 points distincts ou est tangente en 1 point, alors le troisième point donné par le théorème de Bezout est

encore dans C^*. Ceci permet de définir une loi commutative d'élément neutre O de la même manière que pour une cubique de Weierstraß non-singulière. Montrons que cette loi est compatible avec les isomorphismes donnés ci-dessus. Cela montrera aussi qu'elle est associative.

Le cas $\lambda \neq \mu$. Les points $P(t_1), P(t_2), P(t_3)$ sont l'intersection de la droite $aX + bY + cZ = 0$ avec C si et seulement si t_1, t_2, t_3 sont les 3 racines du polynôme

$$a(\mu - \lambda)^2 t(t-1) + b(\mu - \lambda)^2 t(\mu t - \lambda) + c(t-1)^3.$$

Notons que $c \neq 0$ car la droite ne doit pas passer par le point singulier $(0, 0)$. On voit donc que t_1, t_2, t_3 sont les trois racines d'un polynôme unitaire de degré 3 de terme constant -1. Donc $t_1 t_2 t_3 = 1$.

Le cas $\lambda = \mu$. De même, $P(u_1)$, $P(u_2)$ et $P(u_3)$ sont l'intersection de la droite $aX+bY+cZ = 0$ avec C si et seulement si u_1, u_2, u_3 sont les 3 racines du polynôme $au+b(1+\lambda u)+cu^3$, dont le terme en u^2 est nul. Donc $u_1 + u_2 + u_3 = 0$. □

3.8 Sur un corps non Archimédien

Le corps de base k est ici muni d'une valuation discrète v non triviale. On note R l'anneau de valuation discrète $\{x \in k, v(x) \geqslant 1\}$ et $\tilde{k}$ son corps résiduel. Les cas qui nous intéressent principalement sont $k = \mathbb{Q}$, $v = v_p$ pour p premier, et $\tilde{k} = \mathbb{F}_p$. Néanmoins, il sera utile de considérer des extensions finies de $\mathbb{Q}$ et des valuations qui étendent la valuation p-adique. Il sera aussi utile de compléter ces corps, et donc de considérer des extensions finies de $\mathbb{Q}_p$.

Pour tout $x \in R$, on note $\tilde{x}$ l'image de x dans $\tilde{k}$ et on l'appelle "réduction" de x (sous-entendu "modulo v"). Tout point $P \in \mathbb{P}^n(k)$ possède des coordonnées homogènes $[x_0 : \cdots : x_n]$ telles que $\mathrm{Min}\{v(x_i)\} = 0$. Le point $\tilde{P} \in \mathbb{P}^n(\tilde{k})$ de coordonnées $[\tilde{x}_0 : \cdots : \tilde{x}_n]$ est alors bien défini et ne dépend pas du choix des x_i. On obtient ainsi une application de réduction

$$\mathbb{P}^n(k) \longrightarrow \mathbb{P}^n(\tilde{k}).$$

Soit $C_f \subset \mathbb{P}^2$ une courbe plane définie sur k par un polynôme homogène $f \in k[X, Y, Z]$. On peut multiplier f par un scalaire de sorte que le minimum des valuations de ses coefficients soit 0. Alors, comme ci-dessus, $\tilde{f} \in \tilde{k}[X, Y, Z]$ est un polynôme homogène de même degré et qui ne dépend pas du scalaire choisi. Il définit une courbe plane $C_{\tilde{f}}$ sur $\tilde{k}$, et l'application de réduction ci-dessus induit

$$C_f(k) \longrightarrow C_{\tilde{f}}(\tilde{k}).$$

Rappelons que v peut se prolonger à la clôture algébrique $\bar{k}$ (et ce prolongement est unique si k est complet). La valuation ainsi prolongée n'est plus discrète mais on peut toujours définir une application de réduction qui prolonge la précédente

$$C_f(\bar{k}) \longrightarrow C_{\tilde{f}}(\bar{\tilde{k}}).$$

Rappelons aussi que dans cette situation $\tilde{\bar{k}}$ est une clôture algébrique de $\tilde{k}$. De plus, si $G_{k,v} := \{\sigma \in G_k, \forall x \in \bar{k}, v(\sigma(x)) = v(x)\}$ est le "groupe de décomposition" en v, on a un morphisme canonique $G_{k,v} \longrightarrow G_{\tilde{k}} = \mathrm{Gal}(\tilde{\bar{k}}/\tilde{k})$ compatible avec la réduction $\bar{R} \longrightarrow \tilde{\bar{k}}$. De même, l'application de réduction $C_f(\bar{k}) \longrightarrow C_{\tilde{f}}(\tilde{\bar{k}})$ est compatible avec l'action de $G_{k,v}$ donnée par l'inclusion $G_{k,v} \subset G_k$ du côté gauche et la surjection $G_{k,v} \longrightarrow G_{\tilde{k}}$ du côté droit.

3.8.1 *Réduction d'une cubique de Weierstraß.* On suppose ici que $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ avec $v(a_i) \geqslant 0$ pour tout i. Notons C_f^* le lieu non-singulier de C_f et, de même, $C_{\tilde{f}}^*$ le lieu non-singulier de $C_{\tilde{f}}$. On sait que ces courbes lisses (non projectives en général) sont des groupes. Notons que si P est le point singulier de C_f alors $\tilde{P}$ est celui de $C_{\tilde{f}}$. En revanche, il y a beaucoup de points non-singuliers de C_f qui se réduisent sur le point singulier de $C_{\tilde{f}}$. Introduisons

$$C_f^0 := \{P \in C_f,\ \tilde{P} \in C_{\tilde{f}}^*\}.$$

Bien-sûr, si $\tilde{\Delta} \neq 0$, les courbes $C_{\tilde{f}}$ et C_f sont des courbes elliptiques et on a $C_f^0 = C_f^* = C_f$.

Lemme. – *C_f^0 est un sous-groupe de C_f^* et l'application de réduction $C_f^0 \longrightarrow C_{\tilde{f}}^*$ est un homomorphisme de groupes.*

Démonstration. Puisque la réduction envoie l'élément neutre $O = [0:1:0]$ de C_f^* sur l'élément neutre $\tilde{O} = [0:1:0]$ de $C_{\tilde{f}}^*$, il suffit de montrer que si L est une droite de $\mathbb{P}_k^2$ et $[L \cap C_f] = [P_1] + [P_2] + [P_3]$ dans $\mathrm{Div}(C_f)$ avec $P_1, P_2 \in C_f^0$, alors il existe une droite $\tilde{L}$ de $\mathbb{P}_{\tilde{k}}^2$ telle que $[\tilde{L} \cap C_{\tilde{f}}] = [\tilde{P}_1] + [\tilde{P}_2] + [\tilde{P}_3]$ dans $\mathrm{Div}(C_{\tilde{f}})$. Dans ce cas, on a nécessairement $\tilde{P}_3 \in C_{\tilde{f}}^*$ puisque $\tilde{P}_1, \tilde{P}_2 \in C_{\tilde{f}}^*$, et donc $P_3 \in C_f^0$.

Bien sûr, $\tilde{L}$ n'est pas mystérieuse. On choisit une équation $aX + bY + cZ = 0$ de L avec $\mathrm{Min}(v(a), v(b), v(c)) = 0$ et on prend pour $\tilde{L}$ la droite sur $\tilde{k}$ d'équation $\tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0$, qui ne dépend pas du choix effectué. Il est alors clair que pour tout point P d'intersection de L et C_f avec multiplicité m_P, le point $\tilde{P}$ est un point d'intersection de $\tilde{L}$ et $C_{\tilde{f}}$ avec multiplicité $m_{\tilde{P}} \geqslant m_P$. L'inégalité devient stricte si deux points distincts P, Q de $L \cap C_f$ se réduisent sur le même point $\tilde{P} = \tilde{Q}$. Il s'agit donc de montrer que

$$(*)\ \ \forall \tilde{Q} \in \tilde{L} \cap C_{\tilde{f}},\ \text{on a } m_{\tilde{Q}} = \sum_{P \in L \cap C_f, \tilde{P} = \tilde{Q}} m_P.$$

Si l'application de réduction est injective sur l'intersection $L \cap C_f$, c'est clair car les inégalités $m_{\tilde{P}} \geqslant m_P$ et l'égalité $\sum_{\tilde{Q}} m_{\tilde{Q}} = \sum_P m_P = 3$ impliquent $m_{\tilde{P}} = m_P$ pour tout P.

Supposons l'application de réduction non injective et soient P, Q distincts dans $L \cap C_f$ d'image $\tilde{P} = \tilde{Q}$. Quittes à faire un changement de variables, on suppose de plus que $\tilde{P} = (0,0)$, auquel cas P, Q sont dans la carte affine $Z \neq 0$, de coordonnées (x_P, y_P) et (x_Q, y_Q). La droite affine (PQ) a pour équation

$$(PQ) : (y_Q - y_P)(x - x_P) + (x_P - x_Q)(y - y_P) = 0.$$

Soit $\nu := \mathrm{Min}(v(y_Q - y_P), v(x_P - x_Q))$ et π une uniformisante de v. Posons

$$x_{QP} := \pi^{-\nu}(x_Q - x_P) \text{ et } y_{QP} := \pi^{-\nu}(y_Q - y_P).$$

Alors la droite réduite $\widetilde{(PQ)}$ a pour équation

$$\widetilde{(PQ)} : \tilde{y}_{QP} \cdot x - \tilde{x}_{QP} \cdot y = 0.$$

Considérons maintenant le développement

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

où f_P est une somme de polynôme homogènes de degré 2 et 3. En faisant $(x,y) = (x_Q, y_Q)$, on constate que $v(f_P) > \nu$, donc en divisant par π^ν et en réduisant on obtient l'égalité

$$0 = \tilde{x}_{QP} \cdot \frac{\partial \tilde{f}}{\partial x}(\tilde{P}) + \tilde{y}_{QP} \cdot \frac{\partial \tilde{f}}{\partial y}(\tilde{P}).$$

Puisque les couples $(\tilde{x}_{QP}, \tilde{y}_{QP})$ et $(\frac{\partial \tilde{f}}{\partial x}(\tilde{P}), \frac{\partial \tilde{f}}{\partial y}(\tilde{P}))$ sont non nuls (le second par régularité en $\tilde{P}$), on en déduit que l'équation de $\widetilde{(PQ)}$ est

$$\widetilde{(PQ)} : \frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \cdot x + \frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \cdot y = 0,$$

qui est l'équation de la tangente à $C_{\tilde{f}}$ en $\tilde{P}$. Il s'ensuit en particulier que $m_{\tilde{P}} \geqslant 2$. Ainsi, on en déduit $(*)$ lorsque $m_P = m_Q = 1$ et le troisième point R de $L \cap C_f$ ne se réduit pas sur $\tilde{P}$.

Considérons maintenant le cas où $m_P = 2$ (et donc $m_Q = 1$ et il n'y a pas d'autre point d'intersection). Si on écrit $f_P = f_P^{(2)} + f_P^{(3)}$ avec $f_P^{(i)}$ homogène de degré i, cela équivaut à ce que l'équation de (PQ) divise $f_P^{(2)}$. Mais alors, en réduisant, on constate que l'équation de la tangente en $\tilde{P}$ divise le terme quadratique $\tilde{f}_{\tilde{P}}^{(2)}$ du développement de $\tilde{f}$ en $\tilde{P}$ (qui n'est autre que la réduction de $f_P^{(2)}$). Il s'ensuit que la tangente intersecte $C_{\tilde{f}}$ avec multiplicité 3 en $\tilde{P}$, et on en déduit encore $(*)$ dans ce cas.

Il reste à traiter le cas où $L \cap C_f$ consiste en 3 points distincts P, Q, R se réduisant sur $\tilde{P}$. Reprenons l'égalité

$$0 = f(x_Q, y_Q) = x_{QP}\frac{\partial f}{\partial x}(P) + y_{QP}\frac{\partial f}{\partial y}(P) + \pi^\nu f_P^{(2)}(x_{QP}, y_{QP}) + \pi^{2\nu} f_P^{(3)}(x_{QP}, y_{QP}).$$

On a une égalité similaire pour R

$$0 = f(x_R, y_R) = x_{RP}\frac{\partial f}{\partial x}(P) + y_{RP}\frac{\partial f}{\partial y}(P) + \pi^\mu f_P^{(2)}(x_{RP}, y_{RP}) + \pi^{2\mu} f_P^{(3)}(x_{RP}, y_{RP}).$$

Puisque les points P, Q, R sont alignés, il existe $u \in R^\times$ tel que $(x_{RP}, y_{RP}) = u(x_{QP}, y_{QP})$. On en déduit que

$$(\pi^\nu - u\pi^{\mu-\nu})f^{(2)}(x_{QP}, y_{QP}) + (\pi^{2\nu} - u^2\pi^{2\mu})f^{(3)}(x_{QP}, y_{QP}) = 0,$$

et finalement,

$$f^{(2)}(x_{QP}, y_{QP}) + (\pi^\nu + u\pi^\mu)f^{(3)}(x_{QP}, y_{QP}) = 0,$$

ce qui montre que $\tilde{f}^{(2)}(\tilde{x}_{QP}, \tilde{y}_{QP}) = 0$. Donc l'équation de $\widetilde{(QP)}$, qui est aussi la tangente à $C_{\tilde{f}}$ en $\tilde{P}$ comme on l'a vu plus haut, divise $f^{(2)}$, et on a bien $m_{\tilde{P}} = 3$. □

3.8.2 *Equations de Weierstraß minimales.* Soit $\mathcal{E}$ une courbe elliptique sur k. On aimerait lui associer une courbe $\tilde{\mathcal{E}}$ "canonique" sur $\tilde{k}$ et une application de réduction. Si on voit $\mathcal{E}$ comme une cubique $\mathcal{E} = C_f$, alors la courbe $C_{\tilde{f}}$ dépend en général du choix de f.

Définition. – *On dit qu'une équation de Weierstraß est* minimale *si ses coefficients sont entiers et son discriminant est de valuation minimale parmi toutes les équations de Weierstraß à coefficients entiers qui définissent la même courbe.*

Exercice. – ii) Montrer que si $a_i \in R$ et $v(\Delta) < 12$ alors l'équation est minimale.
iii) Si $\mathrm{car}(\tilde{k}) \neq 2, 3$, montrer qu'une équation de Weierstraß courte est minimale si et seulement si $v(\Delta) < 12$ ou $v(a_4) < 4$.

Lemme. – *i) $\mathcal{E}$ admet une équation minimale de l'une des formes simplifiées de 3.7.1, selon* la caractéristique de $\tilde{k}$ *(et pas celle de k).*
ii) Deux équations minimales simplifiées de $\mathcal{E}$ se déduisent par un changement de coordonnées avec $u \in R^\times$ et $r, s, t \in R$.

Démonstration. Exercice. On remarquera que pour pouvoir simplifier les équations de Weierstraß entières, il faut en genéral que 2 ou 3 soit inversible dans R, donc dans $\tilde{k}$. □

Corollaire. – *La courbe $\tilde{\mathcal{E}}$ obtenue par réduction d'une équation minimale de $\mathcal{E}$ ne dépend pas de cette équation minimale, à isomorphisme près.*

Définition. – *On dit que $\mathcal{E}$ a*
— bonne réduction *si $\tilde{\mathcal{E}}$ est non-singulière.*
— réduction multiplicative *si $\tilde{\mathcal{E}}$ a un point de croisement.*
— réduction additive *si $\tilde{\mathcal{E}}$ a un point de rebroussement (cusp).*

Il est clair que $\mathcal{E}$ a bonne réduction si et seulement si elle admet une équation de Weierstraß à coefficients dans R et avec $v(\Delta) = 0$. Voici un résultat clef pour la preuve du théorème de Mordell.

3.8.3 Théorème.– *Supposons que $\mathcal{E}$ a bonne réduction et soit $m \in \mathbb{N}$ premier à la caractéristique résiduelle $p := \mathrm{car}(\tilde{k})$ de k. Alors l'application de réduction $\mathcal{E} \longrightarrow \tilde{\mathcal{E}}$ induit un isomorphisme $\mathcal{E}[m] \xrightarrow{\sim} \tilde{\mathcal{E}}[m]$.*

Démonstration. Quittes à faire une extension finie de k, on supposera que les points de m-torsion de $\mathcal{E}$ et $\tilde{\mathcal{E}}$ sont rationnels, i.e. $\mathcal{E}[m] \subset \mathcal{E}(k)$ et $\tilde{\mathcal{E}}[m] \subset \tilde{\mathcal{E}}(\tilde{k})$. Comme on sait que $|\mathcal{E}[m]| = |\mathcal{E}'[m]| = m^2$, il suffira de prouver l'injectivité de l'application de réduction $\mathcal{E}[m] \longrightarrow \tilde{\mathcal{E}}[m]$. En d'autres termes, en notant $\mathcal{E}^1 := \mathrm{Ker}(\mathcal{E} \longrightarrow \tilde{\mathcal{E}})$ le noyau de l'application de réduction, on veut montrer que $\mathcal{E}^1(k) \cap \mathcal{E}[m] = \{0\}$. Pour cela, *nous pouvons supposer que k est complet* (puisque $\mathcal{E}^1(k) \subset \mathcal{E}^1(\hat{k})$), et nous allons donner une description de $\mathcal{E}^1(k)$.

Puisque $\mathcal{E}^1(k)$ est en quelque sorte "centré" autour de O, il convient de travailler dans la carte affine $\{Y \neq 0\}$ avec coordonnées affines $x = \frac{X}{Y}$ et $z = \frac{Z}{Y}$. Le point O est donc le point $(0,0)$ et une équation de Weierstraß s'écrit

$$f(x,z) := z - (x^3 - a_1xz + a_2x^2z - a_3z^2 + a_4xz^2 + a_6z^3) = 0.$$

On voit que x est une coordonnée locale de $\mathcal{E}$ en O, car l'idéal de l'anneau local $\mathcal{O}_{\mathbb{P}^2,O} = k[x,z]_{(x,z)}$ engendré par x, f est égal à l'idéal engendré par x, z dans ce même anneau, de sorte que

$$\mathcal{O}_{\mathcal{E},O}/(x) = \mathcal{O}_{\mathbb{P}^2,O}/(x,f) = \mathcal{O}_{\mathbb{P}^2}/(x,z) = k.$$

On peut donc identifier le complété $\widehat{\mathcal{O}}_{\mathcal{E},O}$ à $k[[x]]$, et la fonction z y admet un développement

$$z = z(x) = \sum_{n>0} c_n x^n \in k[[x]]$$

et on a $f(x, z(x)) = 0$ dans $k[[x]]$. Notons que, vu la forme de $f(x,z)$, les premiers termes sont donnés par $c_1 = c_2 = 0$ et $c_3 = 1$.

3.8.4 Lemme.– *i) On a $z(x) \in R[[x]]$ (i.e. $c_n \in R$ pour tout n).*
ii) En évaluant z sur l'idéal maximal $\mathfrak{m}_R$ de R, on obtient une bijection

$$\varepsilon : \mathfrak{m}_R \xrightarrow{\sim} \mathcal{E}^1(k), \quad a \mapsto (a, z(a)).$$

Démonstration. Rappelons d'abord le lemme de Hensel. Soit A un anneau commutatif, I un idéal de A et $f \in A[X]$ un polynôme dont on se donne une "racine α modulo I", ie $\alpha \in A$ et $f(\alpha) \in I$. On suppose que

— A est complet pour la topologie I-adique (engendrée par les $a + I^n$, $a \in A$ et $n \in \mathbb{N}$)
— et $f'(\alpha) \in A^\times$.

Alors il existe une unique racine β de f dans A telle que $\beta - \alpha \in I$.

i) Appliquons ceci à $A = R[[x]]$, $I = (x)$, $f = f(x,X)$ et $\alpha = 0$. Puisque $f'(\alpha) = 1$, le lemme de Hensel nous fournit un élément $\beta = \sum_{n>0} b_n x^n \in R[[x]]$ tel que $f(x, \beta(x)) = 0$. Par unicité dans le même lemme appliqué à $A' = k[[x]]$ etc, on doit avoir $z = \beta$ dans $k[[x]]$.

ii) Puisque R est complet pour la valuation v, la série $z(a) := \sum_{n>0} c_n a^n$ converge dans R et fournit un élément de $\mathfrak{m}_R$. L'égalité $f(x, z(x)) = 0$ dans $R[[x]]$ implique $f(a, z(a)) = 0$ dans R, donc le point $P_a = (a, z(a))$ de $\mathbb{A}^2$ est bien dans $\mathcal{E}(k)$. Puisque $a, f(a) \in \mathfrak{m}_R$, on a $P_a \in \mathcal{E}^1(k)$. L'application de l'énoncé est donc bien définie, et son injectivité est évidente. Pour voir la surjectivité, prenons $(a,b) \in \mathcal{E}^1(k)$. Alors $b \in \mathfrak{m}_R$ est une racine du polynôme

$f(a,X) \in R[X]$ dont la dérivée en b est 1. Le lemme de Hensel avec $A = R$, $I = \mathfrak{m}_R$, $f = f(a,X)$ et $\alpha = b$ assure que b est l'unique racine de $f(a,X)$ dans $\mathfrak{m}_R$. Or $z(a)$ en est une autre, donc $b = z(a)$. □

Remarque. – L'argument du i) montre en fait que $z(x) \in \mathbb{Z}[a_1, \cdots, a_6][[x]]$.

Maintenant que nous avons une description commode de $\mathcal{E}^1(k)$, il faut comprendre la multiplication par m et, plus généralement, la loi de groupe sur $\mathcal{E}^1(k)$. Rappelons que $[m] = [m]_{\mathcal{E}} : \mathcal{E} \longrightarrow \mathcal{E}$ est un morphisme qui envoie O sur O. Il induit donc un morphisme d'anneaux locaux $[m]^* : \mathcal{O}_{\mathcal{E},O} \longrightarrow \mathcal{O}_{\mathcal{E},O}$ et, par là, un morphisme sur les complétés $[m]^* : \hat{\mathcal{O}}_{\mathcal{E},O} = k[[x]] \longrightarrow \hat{\mathcal{O}}_{\mathcal{E},O} = k[[x]]$. Ce morphisme est entièrement déterminé par l'image de x qui est une série

$$[m]^*(x) = \sum_{n>0} \mu_n x^n \in k[[x]].$$

3.8.5 Lemme.– *i) On a $[m]^*(x) \in mx + x^2R[[x]]$ (i.e. $\mu_n \in R$ pour tout n et $\mu_1 = m$).*
ii) Notons $\langle m \rangle : \mathfrak{m}_R \longrightarrow \mathfrak{m}_R$ l'application d'évaluation $a \mapsto [m]^*(a)$. Alors

$$[m]_{\mathcal{E}} \circ \varepsilon = \varepsilon \circ \langle m \rangle : \mathfrak{m}_R \longrightarrow \mathcal{E}^1(k).$$

Ce lemme sera une conséquence du théorème 3.8.6 ci-dessous. Admettons-le momentanément et terminons la preuve du théorème 3.8.3 On veut donc prouver l'injectivité de $[m]_{\mathcal{E}}$ sur $\mathcal{E}^1(k)$. D'après les deux lemmes ci-dessus, il suffit de montrer que l'application $\langle m \rangle : \mathfrak{m}_R \longrightarrow \mathfrak{m}_R$ est injective. Pour cela, il suffit de trouver une série formelle $M(X) \in R[[X]]$ inverse de $[m]^*$ au sens de la composition, c'est-à-dire telle que $M([m]^*(x)) = x$. Or on a

$$[m]^* \in mx(1 + R[[x]]) \subset xR[[x]]^\times \text{ car } m \in R^\times$$

donc $t := [m]^*$ est un générateur de l'idéal $xR[[x]]$ et il s'ensuit que $R[[x]] = R[[t]]$. On peut donc exprimer $x = M(t)$ et M est la série formelle cherchée. □

3.8.6 *Loi de groupe formelle.* Selon la même idée que ci-dessus, on s'intéresse à la loi de groupe de $\mathcal{E}$ "au voisinage formel" de O. Concrètement, cette loi est donnée par un morphisme de k-variétés $\mathcal{E} \times \mathcal{E} \xrightarrow{\mu} \mathcal{E}$ qui induit sur les anneaux locaux complétés en O un morphisme (continu)

$$\mu^* : \hat{\mathcal{O}}_{\mathcal{E},O} = k[[x]] \longrightarrow \hat{\mathcal{O}}_{\mathcal{E}\times\mathcal{E},(O,O)} = k[[x_1, x_2]]$$

entièrement déterminé par l'image de x, qui est une série formelle $\mu^* = \mu^*(x_1, x_2) \in k[[x_1, x_2]]$ à deux variables et sans terme constant (car elle doit appartenir à l'idéal maximal). De même, l'inverse est donné par un morphisme $i : \mathcal{E} \longrightarrow \mathcal{E}$ dont le morphisme $i^* : k[[x]] \longrightarrow k[[x]]$ associé est déterminé par une série formelle $i^* = i^*(x) \in k[[x]]$ sans terme constant. Les axiomes de groupe satisfaits par μ et i se traduisent ainsi :

— L'associativité de μ implique $\mu^*(\mu^*(x_1, x_2), x_3) = \mu^*(x_1, \mu^*(x_2, x_3))$.
— La commutativité de μ implique $\mu^*(x_1, x_2) = \mu^*(x_2, x_2)$.

— L'axiome d'inverse implique $\mu^*(x, i^*(x)) = 0$.
— Le fait que O est élément neutre implique $\mu^*(x, 0) = \mu^*(0, x) = x$.
Notons que la dernière égalité équivaut à

$$\mu^*(x_1, x_2) \in x_1 + x_2 + x_1 x_2 k[[x_1, x_2]]$$

et on en déduit aussi que $i^*(x) \in -x + x^2 k[[x]]$. Enfin, la série $[m]^*$ correspondant à la multiplication par m comme dans le lemme 3.8.5 est donnée par

$$[m]^*(x) = \mu(\mu(\cdots(\mu(x, x), x)\cdots, x), x) \in mx + x^2 k[[x]].$$

THÉORÈME. – *Avec les notations ci-dessus :*

i) *On a* $\mu^*(x_1, x_2) \in R[[x_1, x_2]]$ *et* $i^*(x) \in R[[x]]$.

ii) *L'application d'évaluation* $\mathfrak{m}_R \times \mathfrak{m}_R \longrightarrow \mathfrak{m}_R$, $(a_1, a_2) \mapsto \mu^*(a_1, a_2)$ *est bien définie et est une loi de groupe sur* $\mathfrak{m}_R$ *dont l'inverse est donné par* $\mathfrak{m}_R \longrightarrow \mathfrak{m}_R$, $a \mapsto i^*(a)$.

iii) *L'application* $\varepsilon : \mathfrak{m}_R \longrightarrow \mathcal{E}^1(k)$ *du lemme 3.8.4 est un morphisme de groupes.*

Démonstration. i) Considérons le morphisme $i \circ \mu : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$. Comme ci-dessus, il induit au niveau des complétés en O un morphisme $k[[x]] \longrightarrow k[[x_1, x_2]]$ entièrement déterminé par l'image de x, qui est une série formelle $(i \circ \mu)^*(x_1, x_2) \in k[[x_1, x_2]]$ sans terme constant. Grâce aux égalités $\mu \circ (\mathrm{id}, O) = \mathrm{id}$ et $i \circ \mu \circ (i, i) = \mu$, on retrouve $\mu^*(x_1, x_2)$ et $i^*(x)$ par les formules

$$i^*(x) = (i \circ \mu)^*(x, 0) \quad \text{puis} \quad \mu^*(x_1, x_2) = (i \circ \mu)^*(i^*(x_1), i^*(x_2)).$$

Il nous suffira donc de prouver que $(i \circ \mu)^*(x_1, x_2) \in R[[x_1, x_2]]$.

Soit V l'ouvert de $\mathcal{E} \times \mathcal{E}$ formé des points (P_1, P_2) tels que $P_1 \neq P_2$ et $P_1, P_2, (i \circ \mu)(P_1, P_2) \in \mathcal{E} \cap \{Y \neq 0\}$. Notons $P_1 = (x_1, z_1)$, $P_2 = (x_2, z_2)$ et $(i \circ \mu)(P_1, P_2) =: P_3 = (x_3, z_3)$ les coordonnées de ces points dans la carte affine $\{Y \neq 0\}$. Par définition, le point P_3 est le troisième point d'intersection de $(P_1 P_2)$ et $\mathcal{E}$. On a donc les égalités

$$z_3 = z_1 + (x_3 - x_1)\frac{z_2 - z_1}{x_2 - x_1} \quad \text{et} \quad f(x_3, z_3) = 0.$$

Considérons maintenant x et z comme des fonctions rationnelles sur $\mathcal{E}$, i.e. des éléments de $k(\mathcal{E})$. Posons $x_i = \pi_i^*(x)$ et $x_3 = (i \circ \mu)^*(x)$, et de même $z_i = \pi_i^*(z)$ et $z_3 = (i \circ \mu)^*(z)$, qui sont des éléments de $k(\mathcal{E} \times \mathcal{E})$. Alors les égalités ci-dessus, étant valables après évaluation en tout point de l'ouvert V, sont des égalités dans $k(\mathcal{E} \times \mathcal{E})$ et donc, a fortiori, dans le corps des fractions $k((x_1, x_2))$ de $k[[x_1, x_2]] = \widehat{\mathcal{O}}_{\mathcal{E}\times\mathcal{E},(O,O)}$. Mais en tenant compte du fait que $z_i = z(x_i) = \sum_{n>0} c_n x_i^n$, on voit que

$$\frac{z_2 - z_1}{x_2 - x_1} = \sum_{n>0} c_n \left(\sum_{k=0}^{n} x_1^k x_2^{n-k} \right) =: \lambda(x_1, x_2) \in R[[x_1, x_2]].$$

Posons aussi $\nu = \nu(x_1, x_2) := z(x_1) - x_1\lambda(x_1, x_2)$ et considérons le polynôme

$$f(X, \lambda X + \nu) = \alpha_3 X^3 + \alpha_2 X^2 + \alpha_1 X + \alpha_0 \in R[[x_1, x_2]][X].$$

Par construction, ses 3 racines sont x_1, x_2 et x_3, ce qui nous donne l'expression

$$x_3 = -x_1 - x_2 + \frac{\alpha_2(x_1, x_2)}{\alpha_3(x_1, x_2)} \text{ dans } k((x_1, x_2)).$$

Or, un petit calcul montre que $\alpha_3 = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$, donc $\alpha_3 \in R[[x_1, x_2]]^\times$ et finalement $(i \circ \mu)^* = x_3 \in R[[x_1, x_2]]$.

ii) Puisqu'elles sont à coefficients dans R qui est complet, les séries formelles $\mu^*(x_1, x_2)$ et $i^*(x)$ convergent lorsqu'on les évalue sur $\mathfrak{m}_R \times \mathfrak{m}_R$ ou $\mathfrak{m}_R$. Le fait qu'on obtient une loi de groupe et son inverse découle des propriétés listées au-dessus du théorème.

iii) Prenons deux points $P_1 = (x_1, z(x_1))$ et $P_2 = (x_2, z(x_2))$ de $\mathcal{E}^1$ avec $x_1, x_2 \in \mathfrak{m}_R$, et notons $(i \circ \mu)(P_1, P_2) =: P_3 = (x_3, z(x_3))$ le troisième point d'intersection de (P_1P_2) et $\mathcal{E}$, qui appartient encore à $\mathcal{E}^1$. En répétant l'argument précédent et en prenant en compte la convergence de chacune des séries apparaissant $\lambda(x_1, x_2)$, $\alpha_2(x_1, x_2)$ et $\alpha_3(x_1, x_2)^{-1}$, on constate que x_3 est bien donné par l'élément $-x_1 - x_2 + \alpha_3^{-1}\alpha_2$. On en déduit que ε est un morphisme de groupes. □

Remarque. – L'argument du i) montre que $\mu^* \in \mathbb{Z}[a_1, \cdots a_6][[x_1, x_2]]$ et $i^* \in \mathbb{Z}[a_1, \cdots a_6][[x]]$.

3.9 Le théorème de Mordell

Le théorème de Mordell affirme que pour $\mathcal{E}$ courbe elliptique sur un corps de nombres $K \supset \mathbb{Q}$, le groupe $\mathcal{E}(K)$ des points K-rationnels est de type fini. On peut remarquer que si on remplace $\mathcal{E}$ par $\mathbb{G}_m$ (qui est aussi une courbe-groupe, mais qui n'est pas projective), le résultat est faux : $K^\times$ n'est pas de type fini. Néanmoins, un théorème classique de Dirichlet affirme que le groupe multiplicatif $\mathcal{O}_K^\times$ est de type fini, et plus généralement, pour tout $N \in \mathbb{N}$, le groupe $(\mathcal{O}_K[\frac{1}{N}])^\times$ est de type fini. Si on se rappelle que $\mathcal{E}(K) = \mathcal{E}(\mathcal{O}_K)$ (tout point de $\mathbb{P}^2(K)$ a un représentant à coordonnées projectives entières), on peut considérer le théorème de Mordell comme une généralisation de celui de Dirichlet. (Notons tout de même que le théorème de Dirichlet est immédiat lorsque $K = \mathbb{Q}$, contrairement au théorème de Mordell !). La première étape vers Mordell est de prouver :

3.9.1 Théorème. (Mordell "faible")– *$\forall m \in \mathbb{N}$, le groupe $\mathcal{E}(K)/[m](\mathcal{E}(K))$ est fini.*

En fait, le cas $m = 2$ sera suffisant pour la deuxième étape vers le théorème "fort". Mais l'idée pour prouver le cas $m = 2$ est la même pour m général et repose sur un joli analogue de la théorie de Kummer pour les extensions Galoisiennes radicielles.

3.9.2 *Théorie de Kummer sur $\mathbb{G}_m$.* Rappelons comment marche la théorie de Kummer classique. Soit m un entier, et supposons que K contient μ_m. On définit un accouplement

$$\begin{array}{ccc} K^\times \times \mathrm{Gal}(\bar{K}/K) & \to & \mu_m \\ (x, \sigma) & \mapsto & \frac{\sigma(\sqrt[m]{x})}{\sqrt[m]{x}} \end{array} .$$

Notons que le quotient $\frac{\sigma(\sqrt[m]{x})}{\sqrt[m]{x}}$ ne dépend pas du choix de la racine m-ème de x. Soit alors

$$L := K(\sqrt[m]{x}, x \in K)$$

l'extension engendrée par les racines m-èmes d'éléments de K. La théorie de Kummer montre que l'accouplement ci-dessus descend en un accouplement *non dégénéré*

$$K^\times/(K^\times)^m \times \mathrm{Gal}(L/K) \longrightarrow \mu_m.$$

Elle montre aussi que toute extension cyclique d'ordre divisant m est obtenue par extraction de racine m-ème. On peut donc caractériser L comme *l'extension abélienne d'exposant m maximale de K*. Tout ceci est valable sur un corps K de caractéristique première à m. Lorsque K est un corps de nombres et N un entier, notons L_N l'extension engendrée par les racines m-èmes des éléments de $\mathcal{O}_K[\frac{1}{N}]^\times$. L'accouplement ci-dessus se restreint alors en un accouplement toujours non dégénéré

$$\mathcal{O}_K[N^{-1}]^\times/(\mathcal{O}_K[N^{-1}]^\times)^m \times \mathrm{Gal}(L_N/K) \longrightarrow \mu_m.$$

Le théorème de Dirichlet évoqué plus haut implique que le groupe de gauche est fini. Par non dégénérescence, on en déduit que L_N *est une extension finie* de K.

On veut maintenant caractériser L_N comme on l'a fait pour L. Puisque le discriminant de $X^m - x$ est $\pm m^m x^{m-1}$, on voit que L_N est non ramifiée en dehors de mN (c'est-à-dire en dehors des places v de K au-dessus des diviseurs premiers de mN). Réciproquement, si une extension $K(\sqrt[m]{x})$ est non ramifiée en dehors de mN alors pour toute valuation w de K telle que $w(mN) = 0$ on a $m|w(x)$. Si de plus $\mathcal{O}_K[\frac{1}{N}]$ est principal, on peut alors trouver $y \in (K^\times)^m$ tel que $w(xy^m) = 0$ pour toutes ces valuations, i.e. tel que $xy^m \in \mathcal{O}[\frac{1}{N}]^\times$. On a alors $K(\sqrt[m]{x}) = K(\sqrt[m]{x'})$ et on voit que, dans ce cas, L_N *est la sous-extension maximale de L non ramifiée en dehors de mN*. Le théorème de Minkowski sur la finitude du nombre de classes de K assure l'existence d'un entier M_K tel que $\mathcal{O}_K[\frac{1}{M_K}]$ est principal, et cette propriété reste clairement vraie pour tout multiple de M_K. En résumé, nous avons montré (modulo Minkowski et Dirichlet)

Proposition. – *Pour tout entier N, la sous-extension maximale abélienne L'_N d'exposant m et non-ramifiée en dehors de mN de K est de degré fini sur K.*

Rappelons encore que les théorèmes de Minkowski et Dirichlet sont immédiats sur $\mathbb{Q}$.

3.9.3 *Théorie de Kummer sur $\mathcal{E}$.* On suppose que les points de m-torsion sont rationnels, i.e. $\mathcal{E}[m] \subset \mathcal{E}(K)$. On définit alors un accouplement

$$\begin{array}{ccc} \mathcal{E}(K) \times \mathrm{Gal}(\bar{K}/K) & \to & \mathcal{E}[m] \\ (P, \sigma) & \mapsto & \sigma(Q) - Q \end{array},$$

où $Q \in \mathcal{E}(\bar{K})$ est un point tel que $[m](Q) = P$. On voit aisément que $\sigma(Q) - Q$ ne dépend pas du choix de Q. Soit maintenant $\mathcal{L}$ l'extension de K engendrée par les coordonnées de Weierstraß de tous les points $Q \in \mathcal{E}(\bar{K})$ tels que $[m](Q) \in \mathcal{E}(K)$. En d'autres termes, on a

$$\mathcal{L} = \bar{K}^H \text{ où } H := \{\sigma \in \mathrm{Gal}(\bar{K}/K), \forall Q \in [m]^{-1}(\mathcal{E}(K)), \sigma(Q) = Q\}.$$

On prouve facilement (exercice ou cf [Silverman VIII.1]) que l'accouplement ci-dessus descend en un accouplement *non dégénéré*

$$\mathcal{E}(K)/[m]\mathcal{E}(K) \times \mathrm{Gal}(\mathcal{L}/K) \longrightarrow \mathcal{E}[m].$$

Ainsi pour prouver le théorème de Mordell faible dans le cas considéré ($\mathcal{E}[m] \subset \mathcal{E}(K)$), il suffit de prouver que $\mathcal{L}$ est une extension finie de K. Notons que, toujours par non-dégénérescence, $\mathrm{Gal}(\mathcal{L}/K)$ est abélien d'exposant m, donc $\mathcal{L}$ est contenue dans l'extension L du paragraphe précédent. Le point clef est maintenant l'existence d'un entier N tel que $\mathcal{L}$ est contenu dans, dont la finitude est assurée par le théorème de Dirichlet. l'extension L'_N de la proposition précédente. D'après la proposition ci-dessous, on peut prendre $N = N_{K/\mathbb{Q}}(\Delta)$ où Δ est le discriminant d'une équation de Weierstraß minimale.

Proposition. – *Supposons K non archimédien complet de caractéristique résiduelle première à m, et que $\mathcal{E}$ a bonne réduction. Alors $\mathcal{L}$ est une extension non ramifiée de K.*

Démonstration. Notons k le corps résiduel de K. Les applications de réduction $\mathcal{E}(K) \longrightarrow \mathcal{E}(k)$ et $\mathrm{Gal}(\bar{K}/K) \twoheadrightarrow \mathrm{Gal}(\bar{k}/k)$ fournissent un diagramme commutatif

$$\begin{array}{ccc} \mathcal{E}(K) \times \mathrm{Gal}(\bar{K}/K) & \longrightarrow & \mathcal{E}(K)[m] \\ \downarrow & & \downarrow \\ \mathcal{E}(k) \times \mathrm{Gal}(\bar{k}/k) & \longrightarrow & \mathcal{E}(k)[m] \end{array}.$$

Mais d'après le théorème 3.8.3, la flèche de droite est un isomorphisme. Il s'ensuit que l'accouplement du haut est trivial sur $\mathcal{E}(K) \times I_K$ où $I_K = \mathrm{Ker}(\mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(\bar{k}/k)$ est le groupe d'inertie et, par conséquent, que $\mathcal{L}$ est contenue dans $\bar{K}^{I_K}$, qui est l'extension non ramifiée maximale de K. □

3.9.4 *Preuve de Mordell faible.* Nous venons de le prouver sous l'hypothèse que $\mathcal{E}[m] \subset \mathcal{E}(K)$ et en utilisant le théorème de Dirichlet. Notons que si $K = \mathbb{Q}$, le théorème de Dirichlet est trivial. Mais pour se débarasser de l'hypothèse $\mathcal{E}[m] \subset \mathcal{E}(\mathbb{Q})$ il faut de toutes manières passer à une extension finie de $\mathbb{Q}$.

Donc, choisissons une extension Galoisienne finie K' de K telle que $\mathcal{E}[m] \subset \mathcal{E}(K')$. On a une suite exacte courte

$$0 \longrightarrow \left(\mathcal{E}(K) \cap [m]\mathcal{E}(K')\right)/[m]\mathcal{E}(K) \longrightarrow \mathcal{E}(K)/[m]\mathcal{E}(K) \longrightarrow \mathcal{E}(K')/[m]\mathcal{E}(K').$$

On sait que le groupe de droite est fini, il suffira donc de prouver que celui de gauche l'est aussi. Soit $P \in \mathcal{E}(K) \cap [m]\mathcal{E}(K')$. Choisissons $Q \in \mathcal{E}(K')$ tel que $P = [m](Q)$ et considérons l'application

$$\lambda_P : \mathrm{Gal}(K'/K) \longrightarrow \mathcal{E}[m], \;\; \sigma \mapsto \sigma(Q) - Q.$$

Cette application *dépend* du choix de Q. Quoi qu'il en soit, si P' est un autre point de $\mathcal{E}(K) \cap [m]\mathcal{E}(K')$ tel que $\lambda_P = \lambda_{P'}$, alors $Q - Q' \in \mathcal{E}(K)$ donc $P - P' \in [m]\mathcal{E}(k)$. On a donc construit une injection

$$\left(\mathcal{E}(K) \cap [m]\mathcal{E}(K')\right)/[m]\mathcal{E}(K) \hookrightarrow \{\mathrm{Gal}(K/K') \longrightarrow \mathcal{E}[m]\}.$$

Comme l'ensemble de droite est fini, celui de gauche aussi.

3.9.5 *Descente.* Pour un groupe abélien A quelconque, la propriété $|A/mA| < \infty$ est loin d'assurer que A est de type fini. Par exemple, $A = \mathbb{R}$ satisfait $\mathbb{R}/m\mathbb{R} = \{0\}$. Par contre, on se souvient que lorsqu'on prouve que tout sous-groupe *discret* de $\mathbb{R}^n$ est de type fini, un des points clef est la finitude du nombre d'éléments dans une boule ouverte. Ceci peut donner une intuition de ce qui se passe dans le lemme suivant.

LEMME. – *Soit A un groupe abélien, et $m \geqslant 2$ un entier tel que A/mA est fini. Supposons qu'il existe une fonction $h : A \longrightarrow \mathbb{R}$ telle que*

i) $\forall N > 0$, $\{P \in A, h(P) \leqslant N\}$ *est fini.*

ii) $\exists C > 0$, $\forall P \in A$, $h(mP) \geqslant m^2 h(P) - C$.

iii) $\forall Q \in A$, $\exists C_Q > 0$, $\forall P \in A$, $h(P + Q) \leqslant 2h(P) + C_Q$.

Alors A est un groupe de type fini.

Démonstration. Soit Γ un ensemble de représentants des classes module mA. Pour un point $P = P_0 \in A$, on définit inductivement une suite $(P_n)_{n\in\mathbb{N}}$ par la condition

$$P_{n-1} - mP_n \in \Gamma.$$

Notons $C_\Gamma := \mathrm{Max}\{\mathrm{C_Q}, \mathrm{Q} \in \Gamma\}$, on a alors

$$h(P_n) \leqslant \frac{1}{m^2}(h(mP_n) + C) \leqslant \frac{1}{m^2}(2h(P_{n-1}) + C_\Gamma + C).$$

On en déduit par récurrence, puis en utilisant $m \geqslant 2$, que

$$h(P_n) \leqslant \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_\Gamma + C}{m^2 - 2} \leqslant \frac{1}{2^n}h(P) + \frac{1}{2}(C_\Gamma + C).$$

Il s'ensuit que A est engendré par $\Gamma \cup \Gamma'$ où $\Gamma' := \{Q \in A, h(Q) \leqslant C_\Gamma + C\}$. □

3.9.6 *Preuve du théorème de Mordell sur $\mathbb{Q}$.* On suppose ici $K = \mathbb{Q}$. On définit la *hauteur* $H(P)$ et la *hauteur logarithmique* $h(P)$ d'un point de $P \in \mathbb{P}^n(\mathbb{Q})$ par les formules

$$H(P) := \mathrm{Max}(|x_0|, \cdots, |x_n|) \text{ et } h(P) = \log(H(P))$$
$$\text{où } P = [x_0 : \cdots : x_n] \text{ avec } x_i \in \mathbb{Z} \text{ et } \mathrm{pgcd}(x_0, \cdots, x_n) = 1.$$

Pour $x \in \mathbb{Q}$, on pose $H(x) = H([x : 1])$. On a donc $H(x) = \mathrm{Max}(|r|, |s|)$ si $x = \frac{r}{s}$ avec $(r, s) = 1$.

Soit maintenant $\mathcal{E}$ une courbe elliptique sur $\mathbb{Q}$ et $y^2 = x^3 + ax + b$ une équation de Weierstrasß de $\mathcal{E}$ avec $a, b \in \mathbb{Z}$ (on peut toujours s'y ramener par un changement de variables). On se sert de la fonction rationnelle $x : \mathcal{E} \longrightarrow \mathbb{P}^1$ pour définir une hauteur sur $\mathcal{E}(\mathbb{Q})$ par la formule

$$\forall P \in \mathcal{E}(\mathbb{Q}),\ H_x(P) := H(x(P)) \text{ et } h_x(P) = \log(H_x(P)).$$

Le lemme suivant est clair :

LEMME. – $\forall N > 0$, $\{P \in \mathcal{E}(\mathbb{Q}), h_x(P) < N\}$ *est fini.*

Pour tout $P = (x, y) = (\frac{r}{s}, \frac{u}{t}) \in \mathcal{E}(\mathbb{Q})$ (les fractions sont supposées irréductibles), l'égalité $y^2 = x^3 + ax + b$ montre que $t^2 = s^3$, donc en posant $e = ts^{-1}$, on a $t = e^3$ et $s = e^2$ et en particulier $e \in \mathbb{Z}$. L'égalité $u^2 = r^3 + ae^4 + be^6$ montre la troisième inégalité de

$$(*) \quad r \leqslant H_x(P),\ e \leqslant H_x(P)^{1/2},\ u \leqslant c.H_x(P)^{3/2}$$

LEMME. – $\forall Q \in \mathcal{E}(\mathbb{Q})$, $\exists C_Q > 0$, $\forall P \in \mathcal{E}(\mathbb{Q})$, $h_x(P+Q) \leqslant 2h_x(P) + C_Q$.

Démonstration. Le cas $Q = O$ étant trivial, on suppose que $Q = (x_Q, y_Q) \in \{Z \neq 0\}$. Lorsque $P = (x, y) \neq Q, -Q, O$, nous avons obtenu dans la preuve du corollaire 3.1.4 la formule

$$x(P+Q) = \left(\frac{y - y_Q}{x - x_Q}\right)^2 - x - x_Q$$

Tenant compte de l'égalité $y^2 = x^3 + ax + b$, on voit qu'il existe des entiers A, B, C, D, E, F ne dépendant que de Q tels que

$$x(P+Q) = \frac{Ay + Bx^2 + Cx + D}{x^2 + Ex + F} = \frac{Aue + Br^2 + Cre^2 + De^4}{r^2 + Ere^2 + Fe^4}.$$

Grâce à $(*)$, on en déduit que

$$H_x(P+Q) \leqslant \mathrm{Max}(|A| + |B| + |C| + |D|, 1 + |E| + |F|) \cdot H_x(P)^2,$$

d'où l'existence de C_Q en prenant les log, et en incorporant le nombre fini de cas délaissés au début $P = O, Q, -Q$. □

LEMME. – $\exists C > 0$, $\forall P \in \mathcal{E}(\mathbb{Q})$, $h([2](P)) \geqslant 4h(P) - C$.

Démonstration. On peut supposer $2P \neq O$ puisque l'ensemble des points de 2-torsion est fini. On a alors $y_P \neq 0$ et l'équation de la tangente en P est

$$y = \lambda x + k \quad \text{avec} \quad \lambda = \frac{3x_P^2 + a}{2y_P} \quad \text{et} \quad k = y_P - \frac{3x_P^3 + ax_P}{2y_P}$$

Par construction de la loi de groupe, x_{2P}, x_P, x_P sont les racines du polynôme cubique $x^3 - (\lambda x + k)^2 + ax + b$, donc on a

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

Un point important est que les polynômes

$$g(X) = X^3 + aX + b \quad \text{et} \quad f(X) = X^4 - 2aX - 8bX + a^2 = g'(X)^2 - 8Xg(X)$$

sont premiers entre eux puisque g n'a pas de racine multiple. On peut donc leur appliquer le lemme suivant, qui achève la preuve du théorème de Mordell sur $\mathbb{Q}$. □

LEMME. – *Soient $f, g \in \mathbb{Z}[X]$ premiers entre eux, et d le max de leurs degrés. Alors la fonction $x \in \mathbb{Q} \mapsto h([f(x) : g(x)]) - d.h(x)$ est bornée.*

Démonstration. Notons $x = \frac{r}{s}$ avec $(r, s) = 1$, de sorte que $s^d f(x)$ et $s^d g(x)$ sont entiers. On veut majorer leur pgcd, afin de minorer $H([f(x) : g(x)]$. Choisissons pour cela $u, v \in \mathbb{Q}[X]$ tels que $uf + vg = 1$, notons e le max de leurs degrés, et notons N le plus petit entier positif tel que $Nu, Nv \in \mathbb{Z}[X]$. Alors on a

$$(Ns^e u(x)) \cdot (s^d f(x)) + (Ns^e v(x)) \cdot (s^d g(x)) = Ns^{d+e}$$

On en déduit que $pgcd(s^d f(x), s^d g(x)) | Ns^{d+e}$. Par ailleurs, on a $s^d f(x) = \sum_{i=0}^{d} a_i s^{d-i} r^i$, donc le pgcd de $s^d f(x)$ et de s divise le terme dominant $a = a_{deg(f)}$ de f. On a donc

$$\mathrm{pgcd}(s^d f(x), s^d g(x)) | Na^{d+e}.$$

Il s'ensuit que

$$H([f(x) : g(x)]) \geqslant \frac{s^d}{Na^e} \mathrm{Max}(|f(x)|, |g(x)|) \geqslant H(x)^d \frac{\mathrm{Max}(|f(x)|, |g(x)|)}{Na^e \mathrm{Max}(|x|^d, 1)}.$$

Or la fonction $x \mapsto \frac{\mathrm{Max}(|f(x)|, |g(x)|)}{Na^e \mathrm{Max}(|x|^d, 1)}$ tend vers une limite non nulle lorsque $|x| \to \infty$ et ne s'annule pas puisque f et g n'ont pas de zero commun. Donc cette fonction est minorée. On en déduit que la fonction de l'énoncé et minorée, ce qui suffit pour la preuve de Mordell. L'autre inégalité (majoration) est laissée au lecteur (et est plus facile). □

Il est temps de conclure : les trois lemmes ci-dessus et le lemme de descente précédent montrent que le théorème de Mordell "faible" implique le "fort", au moins sur $\mathbb{Q}$. Nous avons montré Mordell faible à l'aide du théorème de Dirichlet sur un corps de nombres. Signalons que si $\mathcal{E}[2] \subset \mathcal{E}(\mathbb{Q})$, nous n'avons besoin de ce théorème que sur $\mathbb{Q}$, où il est facile.