Benoît Stroh

COURBES ELLIPTIQUES

Benoît Stroh

2 janvier 2017

COURBES ELLIPTIQUES

Benoît Stroh

TABLE DES MATIÈRES

CHAPITRE 1

COURBES ELLIPTIQUES SUR LES COMPLEXES

1.1. Rappels sur les surfaces de Riemann

Soit X une surface de Riemann compacte connexe de genre g. Notons Ω^1_X le faisceau des 1-formes différentielles holomorphes sur X, qui sont par définition localement de la forme $f(z)dz$ avec z une coordonnée locale sur X et $f(z)$ une fonction holomorphe. D'après la définition du genre, $H^0(X, \Omega^1_X)$ qui est l'espace des 1-formes différentielles holomorphes globales, est un $\mathbb{C}$-espace vectoriel de dimension g.

1.1.1. Faisceau associé à un diviseur. — Soit $D = \sum_{P \in X} n_p \cdot (P)$ un élément du groupe abélien libre $\mathrm{Div}(X) = \mathbb{Z}[X]$ bâti sur les points de X, où $n_P = 0$ pour presque tout $P \in X$. On notera $|D| = \{P \in X \mid n_P \neq 0\}$ le support de D et on dira que D est un diviseur. On notera $\deg(D) = \sum_P n_P \in \mathbb{Z}$. On dira que D est effectif si $D = \sum_{P \in X} n_P \cdot (P)$ avec $n_P \geq 0$ pour tout $P \in X$. Tout diviseur s'écrit comme différence de deux diviseurs effectifs.

On note $\mathcal{O}_X(D)$ le faisceau des fonctions méromorphes sur X dont le diviseur est $\geq -D$. Par convention, la fonction nulle est toujours section locale de $\mathcal{O}_X(D)$. Si $D = -(P)$, $\mathcal{O}_X(D)$ est le faisceau des fonctions holomorphes nulles en P et si $D = 2(Q) - (P)$, $\mathcal{O}_X(D)$ est le faisceau des fonctions méromorphes avec pôle d'ordre ≥ 2 en Q et nulles en P.

Remarque 1.1.1. — Attention au signe $-$ intervenant dans la définition de $\mathcal{O}_X(D)$. Une manière de se rappeler de sa nécessité est qu'on veut que l'application $D \mapsto \mathcal{O}_X(D)$ soit « croissante », c'est à dire qu'il y a plus de sections locales dans $\mathcal{O}_X(D')$ que dans $\mathcal{O}_X(D)$ si $D' - D$ est effectif. Or il y a plus de fonctions méromorphes que de fonctions holomorphes qui s'annulent...

Exercice 1. — Pourquoi le diviseur d'une fonction méromorphe est-il de degré nul ? Pourquoi cela implique-t-il que $\deg(D)$ ne dépend que de la classe d'isomorphisme du faisceau de $\mathcal{O}_X$-modules $\mathcal{O}_X(D)$? Retrouver ce dernier point grâce au théorème de Riemann-Roch.

Le faisceau $\mathcal{O}_X(D)$ est un faisceau de $\mathcal{O}_X$-modules localement libre de rang 1. On a la formule de dualité

$$\mathcal{O}_X(D)^\vee \;=\; \underline{\mathcal{H}om}_{\mathcal{O}_X}(\mathcal{O}_X(D),\mathcal{O}_X) \;\xrightarrow{\sim}\; \mathcal{O}_X(-D)\,. \tag{1.1.\textbf{a}}$$

Lorsque D est effectif, on a une inclusion canonique $\mathcal{O}_X(-D)\subset\mathcal{O}_X$ dont on notera $\mathcal{O}_D$ le conoyau. Le faisceau $\mathcal{O}_D$ est concentré sur le fermé de Zariski $|D|\subset X$: sa fibre en tout $Q\notin|D|$ est nulle. De plus sa fibre en $P\in|D|$ est un $\mathbb{C}$-espace vectoriel complexe de dimension n_P. La surjection canonique $\mathcal{O}_X\to\mathcal{O}_D$ associe à une fonction holomorphe f le vecteur $(f(P),f'(P),\cdots,f^{(n_P-1)}(P))$ pour tout $P\in X$.

Remarque 1.1.2. — La suite exacte $0\to\mathcal{O}_X(-D)\to\mathcal{O}_X\to\mathcal{O}_D\to 0$ est bien à prendre au sens des faisceaux et non pas des préfaiseaux. Ainsi on ne dit pas du tout que pour tout ouvert $U\subset X$ on a $\mathcal{O}_D(U)=\mathcal{O}_X(U)/\mathcal{O}_X(-D)(U)$ mais simplement que cela est vrai si U est assez petit. Au contraire l'interprétation précédente de $\mathcal{O}_D$ montre que $\mathcal{O}_D(U)=\mathcal{O}_X(U)/\mathcal{O}_X(-D)(U)$ si et seulement si pour tout $P\in U$ et tout $(a_0,\cdots,a_{n_P-1})\in\mathbb{C}^{n_P}$ il existe f holomorphe sur U telle que $f^{(i)}(P)=a_i$ pour tout $P\in U$ et tout $0\leq i<n_P$. Cela est évidemment vrai si U est une boule ouverte mais pas si $U=X$ est compact car par le théorème de Liouville, toute fonction holomorphe est alors constante. Le formalisme cohomologique nous apprend que $H^1(X,\mathcal{O}_X(-D))$ est un obstacle à la surjectivité de $\mathcal{O}_X(U)\to\mathcal{O}_D(U)$ et plus précisément que

$$\mathcal{O}_D(U)/\mathcal{O}_X(U)\;\xrightarrow{\sim}\;\mathrm{Ker}\left(H^1(X,\mathcal{O}_X(-D))\to H^1(X,\mathcal{O}_X)\right)\,.$$

Remarque 1.1.3. — Lorsque D est effectif on a aussi une inclusion $\mathcal{O}_X\subset\mathcal{O}_X(D)$ et $\mathcal{O}_X(D)/\mathcal{O}_X$ représente les différentes parties polaires possibles pour une fonction méromorphe le long de D. La situation est exactement opposée à celle de la discussion précédente, et c'est logique vu la formule de dualité 1.1.**a**.

Ainsi calculer les dimensions de $H^0(X,\mathcal{O}_X(D))$ et de $H^1(X,\mathcal{O}_X(D))$ permet de répondre à un problème tout à fait basique : savoir s'il existe des fonctions méromorphes de partie polaire et de développement limité d'ordre fini fixé.

1.1.2. Théorème de Riemann-Roch. — La première partie du théorème de Riemann-Roch est triviale, mais inutile sans la dualité de Serre qu'on verra juste après. On notera $h^i(D)=\dim_{\mathbb{C}}H^i(X,\mathcal{O}_X(D))$ pour tout i et D. D'après la définition de la cohomologie cohérente d'une surface de Riemann (*ie* d'une courbe complexe) ce nombre est nul pour tout $i>\dim_{\mathbb{C}}(X)=1$. On notera $\chi(D)=h^0(D)-h^1(D)$ et $\chi(\mathcal{O}_X)=h^0(0)-h^1(0)$.

Théorème 1.1.4. — *On a* $\chi(D)=\chi(\mathcal{O}_X)+\deg(D)$ *pour tout* D.

Démonstration. — Il suffit de montrer que le théorème pour D est équivalent au théorème pour $D-(P)$ pour tout $P \in X$. Mais on a alors la suite exacte courte de faisceaux

$$0 \to \mathcal{O}_X(D-(P)) \to \mathcal{O}_X(D) \to \mathcal{O}_X(D) \otimes_{\mathcal{O}_X} \mathcal{O}_P \to 0$$

et d'après la suite longue de cohomologie, on trouve bien que $\chi(D) = \chi(D-(P)) - 1$. En effet $\mathcal{O}_X(D) \otimes_{\mathcal{O}_X} \mathcal{O}_P$ est concentré sur P qui est une variété complexe de dimension 0, donc il n'a que du H^0 et son H^0 est de dimension 1 car c'est le cas de $\mathcal{O}_P$. □

Remarque 1.1.5. — On a en fait $\chi(\mathcal{O}_X) = 1-g$ car $H^0(X, \mathcal{O}_X)$ est de dimension un par Liouville puisque X est compacte, et que $H^1(X, \mathcal{O}_X)$ est de dimension g. Cela consiste au choix en un corollaire de la dualité de Serre ou en une définition du genre (alors appelé « genre arithmétique »). Nous sommes dans le premier de ces deux cas puisque nous avons défini le genre *via* les formes différentielles (aussi appelé « genre géométrique »).

Voilà maintenant le théorème de dualité de Serre, qui est à la cohomologie cohérente ce que la dualité de Poincaré est à la cohomologie de Betti (la théorie de Hodge fait d'ailleurs le pont entre ces deux dualités). Il se généralise à des variétés complexes de dimension arbitraire. Nous en donnerons une preuve adélique simple pour les courbes dans le chapitre suivant.

Théorème 1.1.6. — *On a un isomorphisme canonique* $H^1(X, \Omega^1_X) \xrightarrow{\sim} \mathbb{C}$ *et pour tout* D *et tout* $i = 0, 1$ *on a une dualité parfaite*

$$H^{1-i}(X, \mathcal{O}_X(D)) \times H^i(X, \mathcal{O}_X(-D) \otimes \Omega^1_X) \longrightarrow \mathbb{C}\,.$$

Exercice 2. — Comment étendre ce théorème à tout faisceau cohérent ?

Si $\mathcal{F}$ est un faisceau localement libre de rang un sur X, on définit $\deg(\mathcal{F})$ comme le degré de tout diviseur D tel que $\mathcal{O}_X(D) \simeq \mathcal{F}$, et cela ne dépend pas du choix de D. Cette définition repose sur deux points : que tout faisceau localement libre de rang un est isomorphe à un $\mathcal{O}_X(D)$ car X est lisse, puis que le degré de D est nul lorsque D est le diviseur d'une fonction méromorphe sur X.

Corollaire 1.1.7. — *On a* $\deg(\Omega^1_X) = 2g-2$.

Démonstration. — Appliquer le théorème 1.1.4 à Ω^1_X et calculer $\chi(\Omega^1_X)$ par 1.1.6. □

Lemme 1.1.8. — *On a* $h^0(D) = 0$ *si* $\deg(D) < 0$.

Démonstration. — Si $f \in H^0(X, \mathcal{O}_X(D))$ est non nulle, le diviseur de f est $\geq -D$ donc de degré > 0. Mais le degré du diviseur d'une fonction méromorphe est nul. □

Le corollaire suivant constitue l'application la plus fréquente du théorème de Riemann-Roch. On notera qu'il prend une forme particulièrement agréable lorsque $g = 1$.

Corollaire 1.1.9. — *Si* $\deg(D) > 2g - 2$ *on a* $h^0(D) = 1 - g + \deg(D)$ *et* $h^1(D) = 0$.

Remarque 1.1.10. — Ainsi l'intervalle pour $\deg(D)$ dans lequel il n'est pas facile de calculer $h^0(D)$ et $h^1(D)$ individuellement est $[0, 2g-2]$. En fait il faux que dans cet invervalle, $h^0(D)$ et $h^1(D)$ ne dépendent que de $\deg(D)$ et du genre de X ; des informations plus précises sur la courbe sont par exemple requises.

1.1.3. Théorème de Hurwitz. — Ce théorème permet de relier le genre de la source et de l'arrivée lorsqu'on a un revêtement ramifié entre surfaces de Riemann.

Théorème 1.1.11. — *Soient* X *et* Y *des surfaces de Riemann compactes connexes de genre* g_X *et* g_Y. *Soit* $f : X \to Y$ *un revêtement de degré* n *et d'indice de ramification* e_P *en tout* $P \in X$. *Alors*

$$2g_X - 2 \;=\; n \cdot (2g_Y - 2) + \sum_{P \in X} (e_P - 1)\,.$$

Démonstration. — On a par définition de la ramification $h^0(\Omega^1_X / f^*\Omega^1_Y) = \sum_{P \in X}(e_P - 1)$. Il suffit ensuite d'utiliser la formule pour $\chi(\Omega^1)$ en fonction du genre. □

1.1.4. Calcul du genre. — Considérons à présent le cas d'une surface de Riemann compacte algébrique X qui est un fermé de Zariski de $\mathbb{P}^2_{\mathbb{C}}$. Elle est donc définie par l'annulation d'un polynôme homogène P de degré d en 3 variables. Comme on suppose que X est une surface de Riemann, donc lisse, on a que P, $\partial P/\partial X$, $\partial P/\partial Y$ et $\partial P/\partial Z$ ne s'annulent pas simultanément.

Théorème 1.1.12. — *La surface de Riemann* X *est connexe de genre* $\frac{(d-1)(d-2)}{2}$.

Démonstration. — Par définition on a une suite exacte courte de faisceaux

$$0 \to \mathcal{I} \to \mathcal{O}_{\mathbb{P}^2_{\mathbb{C}}} \to \mathcal{O}_X \to 0$$

où $\mathcal{O}_{\mathbb{P}^2_{\mathbb{C}}}$ désigne le faisceau des fonctions holomorphes à deux variables sur $\mathbb{P}^2_{\mathbb{C}}$ et où $\mathcal{I} = P \cdot \mathcal{O}_{\mathbb{P}^2_{\mathbb{C}}}$. Comme la caractéristique d'Euler est additive sur les suites exactes courtes de faisceaux on trouve $1 - g = \chi(\mathcal{O}_X) = \chi(\mathcal{O}_{\mathbb{P}^2_{\mathbb{C}}}) - \chi(\mathcal{I})$. On utilise ensuite des propositions de géométrie complexe sur $\mathbb{P}^2_{\mathbb{C}}$ qui garantissent que $\chi(\mathcal{O}_{\mathbb{P}^2_{\mathbb{C}}}) = 1$ et que $\chi(\mathcal{I}) = (d-1)(d-2)/2$. De même on montre que $H^1(\mathbb{P}^2_{\mathbb{C}}, \mathcal{I}) = 0$ d'où une surjection $H^0(\mathbb{P}^2_{\mathbb{C}}, \mathcal{O}_{\mathbb{P}^2_{\mathbb{C}}}) \to H^0(X, \mathcal{O}_X)$ et la connexité de X. □

Remarque 1.1.13. — C'est un cas particulier de la théorie du complexe de Koszul. Ce complexe résout $\mathcal{O}_X$ comme quotient de $\mathcal{O}_{\mathbb{P}^n_{\mathbb{C}}}$ lorsque X est une variété complexe de dimension arbitraire donnée comme lieu d'annulation de plusieurs équations dans $\mathbb{P}^n$, sous une hypothèse additionnelle qui s'appelle être « intersection complète » et qui est toujours vérifiée lorsqu'il n'y qu'une seule équation. Lorsqu'il n'y a qu'une seule équation de degré d, cas où on dit que X est une *hypersurface* de $\mathbb{P}^n_{\mathbb{C}}$, on trouve que la dimension de $H^1(X, \mathcal{O}_X)$ est le coefficient binômial C^n_{d-1}.

1.2. Tores complexes

Rappelons brièvement la théorie des courbes elliptiques sur $\mathbb{C}$. On suppose connue la théorie des surfaces de Riemann, ainsi que dans une moindre mesure celle des formes modulaires. Nous ne donnerons pas toutes les démonstrations dans cette partie (voir par exemple [**Si**, ch.VI]).

Définition 1.2.1. — Une courbe elliptique E sur $\mathbb{C}$ est une surface de Riemann de la forme $\mathbb{C}/\Lambda$ avec $\Lambda \subset \mathbb{C}$ un réseau, c'est à dire un sous-groupe isomorphe à $\mathbb{Z}^2$ tel que $\mathbb{C} = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$.

On notera en particulier que E est une surface de Riemann compacte connexe de genre 1.

Lemme 1.2.2. — *Toute courbe elliptique E sur $\mathbb{C}$ est canoniquement munie d'une loi de groupe abélien.*

En particulier E est munie d'un point privilégié noté 0, qui est l'image de l'origine de $\mathbb{C}$ et qui est le neutre pour la loi de groupe. Le théorème suivant est un cas particulier facile du théorème d'uniformisation de Riemann, valable pour toutes les surfaces de Riemann compactes connexes.

Théorème 1.2.3. — *Les courbes elliptiques sur $\mathbb{C}$ sont exactement les surfaces de Riemann compactes connexes de genre 1 munies d'un point privilégié.*

Démonstration. — On donne juste la construction de la construction de Λ et du morphisme $X \to \mathbb{C}/\Lambda$ lorsque X est une surface de Riemann compacte de genre 1 munie d'un point P. On veut trouver un réseau $\Lambda \subset \mathbb{C}$ et un isomorphisme $X \xrightarrow{\sim} \mathbb{C}/\Lambda$ qui envoie P sur 0. Comme X est de genre 1 on a que $H^0(X, \Omega^1_X)$ est un $\mathbb{C}$ espace vectoriel de dimension 1 dont on choisit un générateur ω.

On considère alors $\phi : X \to \mathbb{C}$ qui envoie $Q \in X$ sur $\int_P^Q \omega \in \mathbb{C}$. Cette fonction est mal définie car un choix arbitraire est caché dans l'intégrale : celui d'un chemin joignant P et Q. Mais ϕ devient bien définie si on la voit à valeur dans le quotient de $\mathbb{C}$ par l'ensemble des $\int_\gamma \omega$ pour tout lacet γ autour de P. On introduit donc $\Lambda = \{\int_\gamma \omega,\ \gamma \in H_1(X, \mathbb{Z})\} \subset \mathbb{C}$ où

l'on a considéré l'homologie de Betti de X qui dans ce cas est aussi $\pi_1(X,P)$. On obtient bien $\phi : X \to \mathbb{C}/\Lambda$ telle que $\phi(P) = 0$.

Comme $H_1(X,\mathbb{Z}) \simeq \mathbb{Z}^2$ on a $\Lambda \simeq \mathbb{Z}^2$. On veut ensuite vérifier que $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}$. Si (γ_1, γ_2) forme une $\mathbb{Z}$-base de $H_1(X,\mathbb{Z})$ on veut donc voir que $\int_{\gamma_1} \omega$ et $\int_{\gamma_2} \omega \in \mathbb{C}$ sont $\mathbb{R}$-linéairement indépendants. Enfin on veut voir que ϕ est bijective. Aucun des deux points n'est évident ; on renvoie au cours de surfaces de Riemann pour cela. □

Remarque 1.2.4. — L'application ϕ de la démonstration précédente est l'application d'Abel-Jacobi qui existe pour toute surface de Riemann. Elle vérifie $\phi^*(\mathrm{d}z) = \omega$, où $\mathrm{d}z$ est la différentielle canonique sur $\mathbb{C}$ descendue à $\mathbb{C}/\Lambda$, ce qui est possible car $\mathrm{d}(z+\lambda) = \mathrm{d}z$ pour tout $\lambda \in \Lambda$. On dit que Λ est le réseau des *périodes* de X.

Remarque 1.2.5. — Cette application ϕ ainsi que la construction de $\Lambda \subset \mathbb{C}$ dépend du choix de $\omega \in H^0(X, \Omega^1_X)$. On obtient une construction plus canonique en remplaçant $\mathbb{C}$ par le $\mathbb{C}$-espace vectoriel $H^0(X,\Omega^1_X)^\vee = \mathrm{Hom}_{\mathbb{C}}(H^0(X,\Omega^1_X),\mathbb{C})$ de dimension 1. Remarquons que ce dernier est canoniquement isomorphe à $H^1(X,\mathcal{O}_X)$ par le théorème 1.1.6.

Remarque 1.2.6. — La différence entre une courbe elliptique sur $\mathbb{C}$ et une surface de Riemann compact connexe de genre 1 réside donc dans le choix d'un point base. C'est donc une différence de même nature que celle entre espace vectoriel et espace affine. On oublie parfois la donnée de ce point pour simplifier.

1.3. Formes modulaires

Soit $E_\Lambda = \mathbb{C}/\Lambda$ une courbe elliptique sur $\mathbb{C}$. Un point clé de la théorie est que E_Λ est une courbe algébrique, définie par des équations homogènes de degré 3 dans le plan projectif complexe. Rappelons comment on trouve de telles équations. On introduit la fonction de Weierstrass

$$\wp_\Lambda(z) \;=\; \frac{1}{z^2} + \sum_{\omega\in\Lambda-\{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\,.$$

Remarque 1.3.1. — On va voir que $\wp_\Lambda$ est invariante par translation de Λ ie $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$ pour tout $\lambda \in \Lambda$. Le candidat le plus naïf vérifiant cette invariance aurait été $\sum_{\omega\in\Lambda} 1/(z-\omega)^2$. Malheureusement comme on somme sur $\Lambda \simeq \mathbb{Z}^2$ et pas sur $\mathbb{Z}$ comme dans les sommes de Riemann habituelles, cette série ne converge pas. On obtient la convergence en retranchant $1/\omega^2$, d'où la définition de $\wp$.

Lemme 1.3.2. — *La fonction $\wp_\Lambda$ converge absolument et uniformément sur tout compact de $\mathbb{C}-\Lambda$. Elle définit une fonction méromorphe sur $\mathbb{C}$ qui est holomorphe sur $\mathbb{C}-\Lambda$ et qui a un pôle double de résidu nul en tout $\lambda \in \Lambda$.*

Lemme 1.3.3. — *On a* $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)$ *pour tous* $(z,\lambda) \in \mathbb{C} \times \Lambda$.

Démonstration. — On peut donc dériver $\wp_\Lambda$ terme à terme et on trouve $\wp'_\Lambda(z) = -2 \cdot \sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}$ qui est clairement invariante par translation de Λ. On en déduit $\wp_\Lambda(z+\lambda) = \wp_\Lambda(z)+c(\lambda)$ pour tous $(z,\lambda) \in \mathbb{C}\times\Lambda$ avec $c(\lambda) \in \mathbb{C}$ indépendant de z. En posant $z = -\lambda/2$ et en utilisant la parité de $\wp_\Lambda$ on en déduit $c(\lambda) = 0$. □

On introduit ensuite la série d'Eistenstein non normalisée de poids $2k \in \mathbb{N}$

$$G_{2k}(\Lambda) \;=\; \sum_{\omega\in\Lambda-\{0\}} \frac{1}{\omega^{2k}}\,.$$

Remarque 1.3.4. — La fonction G_{2k} est définie sur l'ensemble des réseaux de $\mathbb{C}$ et est homogène de poids $-2k$, c'est à dire que $G_{2k}(c\cdot\Lambda) = c^{-2k}\cdot G_{2k}(\Lambda)$ pour tout $c \in \mathbb{C}^*$. On peut aussi voir G_{2k} comme une fonction sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ en posant

$$G_{2k}(\tau) \;=\; G_{2k}(\mathbb{Z}+\tau\cdot\mathbb{Z}) \;=\; \sum_{(n,m)\neq(0,0)} \frac{1}{(n+m\tau)^{2k}}$$

Alors $G_{2k} : \mathcal{H} \to \mathbb{C}$ est une forme modulaire de poids $2k$ pour le groupe $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, c'est-à-dire qu'elle vérifie l'équation fonctionnelle

$$G_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) \;=\; (c\tau+d)^{2k}\cdot G_{2k}(\tau) \;\;\forall\,\tau\in\mathcal{H},\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)\,.$$

Cette forme est propre pour les opérateurs de Hecke mais non cuspidale.

Remarque 1.3.5. — Les normalisations ne sont pas tout à fait unifiées dans la littérature : certains auteurs posent $G_k(\Lambda) = \sum_{\omega\in\Lambda-\{0\}} 1/\omega^k$ pour tout $k \in \mathbb{N}$ et l'on retrouve exactement notre définition car G_k est nulle si k est impair. L'avantage de cette normalisation est que G_{2k} est modulaire de poids $2k$ pour le groupe $\Gamma(1)$. On rappelle par ailleurs que les formes modulaires de poids impair pour $\Gamma(1)$ sont toutes nulles.

D'autres auteurs notent $G'_k(\Lambda) = \sum_{\omega\in\Lambda-\{0\}} 1/\omega^{2k}$ qui est alors modulaire de poids $2k$ pour $\Gamma(1)$. Cette renumérotation n'est pas forcément une bonne idée. En effet il existe aussi des séries d'Eisenstein définies par une formule analogue mais pour des sous-groupes d'indice fini de $\Gamma(1)$, qui sont donc des formes modulaires de niveau > 1. Le poids de telles formes n'est pas nécessairement pair. La notation G'_k demande alors d'introduire des exposants qui sont demi-entiers.

Enfin on réserve la notation E_{2k} aux séries d'Eisenstein normalisées $E_{2k}(\Lambda) = \frac{G_{2k}(\Lambda)}{2\zeta(2k)}$ où ζ est la fonction de Riemann. Le terme constant de E_{2k} est un, il s'agit donc d'une forme propre normalisée pour les opérateurs de Hecke.

Lemme 1.3.6. — *La série qui définit* $G_{2k}(\Lambda)$ *avec* $\Lambda \subset \mathbb{C}$ *ou* $G_{2k}(\tau)$ *avec* $\tau \in \mathcal{H}$ *converge absolument pour tout* $k > 1$ *et la fonction* $\mathcal{H} \to \mathbb{C}$, $\tau \mapsto G_{2k}(\tau)$ *est holomorphe.*

Remarque 1.3.7. — On a déjà vu apparaître cette philosophie lors de l'introduction de $\wp$: comme on somme sur $\Lambda \simeq \mathbb{Z}^2$, les conditions de convergence des sommes de Riemann ne sont pas les mêmes que dans le cas usuel où on somme sur $\mathbb{Z}$.

On pose enfin comme d'habitude $g_2(\Lambda) = 60 \cdot G_4(\Lambda)$ et $g_3(\Lambda) = 140 \cdot G_6(\Lambda)$.

Proposition 1.3.8. — *On a* $\wp'_\Lambda(z)^2 = 4 \cdot \wp_\Lambda(z)^3 - g_2(\Lambda) \cdot \wp_\Lambda(z) - g_3(\Lambda)$ *pour tout* $z \in \mathbb{C} - \Lambda$.

Démonstration. — On considère $z \mapsto \wp'_\Lambda(z)^2 - 4 \cdot \wp_\Lambda(z)^3 + g_2(\Lambda) \cdot \wp(z) + g_3(\Lambda)$ qui est holomorphe sur $\mathbb{C} - \Lambda$ et qui est Λ-périodique. De plus un développement limité montre qu'elle est holomorphe près de 0 et s'annule en 0. On en déduit qu'elle est holomorphe sur le compact $\mathbb{C}/\Lambda$ donc bornée par le théorème de Liouville, donc nulle. □

On pose $\Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2$ qui est le discriminant usuel du polynôme $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ et il s'annule donc si et seulement si ce polynôme a une racine de multiplicité ≥ 2.

Remarque 1.3.9. — Si par le dictionnaire usuel on voit Δ comme une fonction $\mathcal{H} \to \mathbb{C}$, on obtient une forme modulaire cuspidale de poids 12 pour $\Gamma(1)$. Elle est propre pour les opérateurs de Hecke et c'est d'ailleurs la seule forme modulaire cuspidale de poids ≤ 12 pour $\Gamma(1)$.

Soit $C \subset \mathbb{P}^2_{\mathbb{C}}$ la courbe algébrique projective donnée par l'annulation d'un polynôme homogène $P(X, Y, Z)$ en les variables X, Y et Z. Rappelons que cette courbe est dite lisse si pour tout $[x; y; z] \in \mathbb{P}^2_{\mathbb{C}}$ tel que $P(x, y, z) = 0$, on a $\partial P/\partial X(x, y, z) \neq 0$ ou $\partial P/\partial Y(x, y, Z) \neq 0$ ou $\partial P/\partial Z(x, y, z) \neq 0$. Cela se traduit par le fait que l'espace tangent à C en (x, y, z) est une droite affine. Cela se traduit aussi par le fait que la surface compacte C^{an} associée à C est localement conformément équivalente à une boule ouverte de $\mathbb{C}$, autrement dit est une surface de Riemann.

On note désormais $E^{\mathrm{alg}}_\Lambda \subset \mathbb{P}^2_{\mathbb{C}}$ la courbe algébrique projective donnée par l'annulation de $P(X, Y, Z) = Y^2Z - 4X^3 + g_2(\Lambda) \cdot XZ^2 + g_3(\Lambda) \cdot Z^3$. On voit facilement que E^{alg}_Λ est lisse si et seulement si $\Delta \neq 0$. On notera alors E^{an}_Λ la surface de Riemann compacte associée.

Proposition 1.3.10. — *Pour tout réseau* $\Lambda \subset \mathbb{C}$ *on a* $\Delta(\Lambda) \neq 0$. *De plus l'application* $E_\Lambda = \mathbb{C}/\Lambda \to E^{\mathrm{an}}_\Lambda$, $z \mapsto [\wp(z), \wp'(z), 1]$ *induit un isomorphisme* $\Phi : E_\Lambda \xrightarrow{\sim} E^{\mathrm{an}}_\Lambda$ *entre surfaces de Riemann.*

Remarque 1.3.11. — Cet isomorphisme envoie $(\mathbb{C} - \Lambda)/\Lambda$ sur la courbe affine d'équation $y^2 = x^3 - g_2 x - g_3$ dans $\mathbb{C}^2$. Comme $\wp$ et $\wp'$ ont des pôles d'ordres respectifs 2 et 1 en $z \in \Lambda$ on obtient que $\Phi(z) = [0, 1, 0]$, qui est l'unique point de E^{an}_Λ sur l'hyperplan projectif d'équation $Z = 0$. On dira que c'est le point à l'infini de E^{an}_Λ.

Remarque 1.3.12. — Si on savait *a priori* que Φ était un isomorphisme, on en déduirait que E_Λ^{an} est une surface de Riemann puisqu'elle serait isomorphe à $\mathbb{C}/\Lambda$, puis que E_Λ^{an} serait lisse et donc que $\Delta(\Lambda) \neq 0$.

On doit en fait prouver d'abord que E_Λ^{an} est lisse donc que $\Delta(\Lambda) \neq 0$ en utilisant les propriétés des fonctions holomorphes sur $\mathbb{C}/\Lambda$ et on en déduit ensuite que Φ est un isomorphisme en montrant qu'elle est étale, c'est à dire qu'elle induit un isomorphisme sur les droites tangentes. On peut d'ailleurs aussi utilise le théorème de Hurwitz 1.1.11 à ce point, en tenant compte du théorème 1.1.12 pour vérifier que E est de genre 1. Le fait que $\Delta(\Lambda) \neq 0$ a été prouvé dans le cours de formes modulaires.

On a donc réussi à algébriser E_Λ en la courbe projective E_Λ^{alg}. On verra en TD que cela n'a rien de miraculeux car toutes les surfaces de Riemann compactes sont algébrisables. Il s'agit d'une conséquence de plus du théorème de Riemann-Roch.

Remarque 1.3.13. — Si $g \geq 2$ et $\Lambda \subset \mathbb{C}^g$ est un réseau, c'est à dire un sous-$\mathbb{Z}$-module isomorphe à $\mathbb{Z}^{2g}$ tel que $\mathbb{C}^g = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, le tore complexe $\mathbb{C}^g/\Lambda$ n'est pas toujours algébrisable. Lorsqu'il est algébrisable, on dira que c'est une variété abélienne de genre g sur $\mathbb{C}$. Le caractère non automatiquement algébrique explique pourquoi la théorie des variétés abéliennes est plus difficile que celle des courbes elliptiques.

On peut aussi raisonner dans l'autre sens, et c'est plus facile : partant de A, $B \in \mathbb{C}$ tels que $A^3 - 27B^2 \neq 0$, notons E la courbe algébrique projective définie par l'équation homogène $Y^2Z = 4X^3 - AXZ^2 - bZ^3$ et E^{an} la surface de Riemann associée. Il existe alors un réseau $\Lambda \subset \mathbb{C}$ et un isomorphisme $E_\Lambda = \mathbb{C}/\Lambda \xrightarrow{\sim} E^{\mathrm{an}}$. Il suffit pour cela de prouver que E est de genre 1, ce qui résulte du théorème 1.1.12, puis d'utiliser le théorème 1.2.3. On remarque que E est munie du point privilégié $[0; 1; 0]$ que l'on choisit lorsqu'on applique le théorème 1.1.12.

Exercice 3. — Prouver le résultat plus fort affirmant que pour tous A, $B \in \mathbb{C}$ tels que $A^3 - 27B^2 \neq 0$ il existe $\Lambda \in \mathbb{C}$ tel que $g_2(\Lambda) = A$ et $g_3(\Lambda) = B$. On pourra chercher à quelle condition les courbes E et E' définies respectivement par A et B puis A' et B' sont isomorphes.

1.4. Loi de groupe

1.4.1. Groupe de classe. — Dans ce paragraphe, X désigne une surface de Riemann compacte connexe quelconque. Soit D un diviseur de X. On dit qu'il est rationnellement si c'est le diviseur d'une fonction méromorphe sur X. Cela implique par l'exercice 1 que $\deg(D) = 0$. On note $\mathrm{Pic}^0(X)$ le quotient du groupe abélien des diviseurs de degré nul par le sous-groupe des diviseurs principaux. On notera $D \sim D'$ pour dire que D et D'

ont même image dans $\mathrm{Pic}^0(X)$. On note aussi $\mathrm{Pic}(X)$ le quotient du groupe abélien des diviseurs par le sous-groupe des diviseurs principaux. On a une suite exacte courte

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0\,.$$

Remarque 1.4.1. — Cette définition ressemble à celle du groupe de classe d'un corps de nombres et la géométrie algébrique nous apprend que ce n'est pas un hasard. Par contre la nature de ces groupes abéliens est quelque peu différente : le groupe de classe est fini et on verra que $\mathrm{Pic}^0(E)$ est loin d'être fini.

Soit $x_0 \in X$ un point fixé. On dispose alors de l'application d'Abel-Jacobi $\alpha : X \to \mathrm{Pic}^0(X)$ qui envoie $x \in X$ sur la classe de $x_0 - x$ qui est un diviseur de degré nul.

Remarque 1.4.2. — C'est une application entre deux objets de nature très différente : une surface de Riemann à la source et un groupe abstrait à l'arrivée. En fait la théorie de Hodge nous apprend en général que $\mathrm{Pic}^0(X)$ admet une structure de variété complexe et que α est une immersion holomorphe. En fait on montre que $\mathrm{Pic}^0(X)$ s'identifie au quotient du $\mathbb{C}$-espace vectoriel $H^1(X, \mathcal{O}_X)$ par le $\mathbb{Z}$-réseau $H^1(X, \mathbb{Z})$. *Via* cette identification, l'application α redonne bien l'application d'Abel-Jacobi usuelle $x \mapsto \int_{x_0}^{x} \omega$ où $\omega \in H^0(X, \Omega^1_X)$ est vue comme forme linéaire sur $H^1(X, \mathcal{O}_X)$ grâce au théorème 1.1.6.

Exercice 4. — Expliquer l'identification de $\mathrm{Pic}^0(X)$ fournie dans la remarque précédente en utilisant la suite de faisceaux

$$0 \longrightarrow 2i\pi \cdot \mathbb{Z} \longrightarrow \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^* \longrightarrow 0\,.$$

On pourra d'abord montrer que $\mathrm{Pic}(X) \xrightarrow{\sim} H^1(X, \mathcal{O}_X^*)$ en se basant sur une interprétation à la Cech de H^1.

1.4.2. Cas des courbes elliptiques. — Si E est une courbe elliptique sur $\mathbb{C}$ c'est à dire au choix $\mathbb{C}/\Lambda$ avec $\Lambda \subset \mathbb{C}$ un réseau, ou une surface de Riemann compacte connexe de genre 1 munie d'un point marqué, ou la surface de Riemann algébrique donnée par l'équation $ZY^2 = X^3 + aXZ^2 + bZ^3$ avec $A^3 - 27B^2 \neq 0$. On a dans chaque cas un point privilégié que l'on notera $0_E \in E$: l'origine de $\mathbb{C}/\Lambda$ ou $[0;1;0]$ dans le dernier cas. On normalise l'application d'Abel-Jacobi par le choix de 0_E.

Théorème 1.4.3. — *L'application d'Abel-Jacobi induit un isomorphisme* $\alpha : E \xrightarrow{\sim} \mathrm{Pic}^0(E)$ *qui envoie* $x \in X$ *sur* $(x) - (0_E) \in \mathrm{Pic}^0(X)$.

Démonstration. — On commence par vérifier l'injectivité. Si $x, y \in E$ vérifient $\alpha(x) = \alpha(y)$, il existe une fonction méromorphe f dont le diviseur est $(x) - (y)$. En particulier on a $f \in H^0(E, \mathcal{O}_E((y))$. Mais comme E est de genre 1, le corollaire à Riemann-Roch 1.1.9 montre que $h^0((y)) = 1$. Donc $H^0(E, \mathcal{O}_E((y))$ est égal à l'ensemble des fonctions constantes,

et f est constante donc $x = y$. Voir aussi [**Si**, coro.VI.2.3] pour une démonstration analytique.

On montre ensuite la surjectivité : si D est un diviseur de degré nul, on veut trouver $P \in X$ et une fonction méromorphe f dont le diviseur soit $D-(P)+(0_E)$. Par le corollaire 1.1.9 on a $h^0(D + (0_E)) = 1 > 0$ donc il existe une fonction méromorphe f de diviseur $\geq -D - (0_E)$. Comme le degré du diviseur de f est nul, f a un unique zéro qui est le P cherché. □

On a donc canoniquement identifié la surface de Riemann E et le groupe $\mathrm{Pic}^0(E)$. On obtient en particulier une loi de groupe sur E en transportant par α celle de $\mathrm{Pic}^0(E)$. Pour le dire explicitement, si $x, y \in E$, la somme $x + y \in E$ est l'unique point $P \in E$ tel que $(P) - (0_E) \sim (x) + (y) - 2 \cdot (0_E)$. Aussi l'opposé de x est l'unique $P \in E$ tel que $(P) - (0_E) \sim (0_E) - (x)$. Le neutre est bien sûr 0_E.

Remarque 1.4.4. — Il est indispensable dans cette histoire de travailler dans le quotient $\mathrm{Pic}^0(E)$ de $\mathrm{Div}^0(E)$. Dans $\mathrm{Div}^0(E)$ qui est un groupe libre on a jamais $(P)+(Q)-2\cdot(0_E) = (R) - (0_E)$ pour $P, Q, R \in E$.

Il reste à comprendre cette loi de groupe suivant les différentes incarnations de E (soit $\mathbb{C}/\Lambda$ soit une courbe algébrique donnée par une équation cubique). On montrera la proposition suivante en TD. Elle implique que la loi de groupe de E est une application $E \times E \to E$ holomorphe, ce qui n'est pas évident sur la définition.

Proposition 1.4.5. — *Si on identifie E à $\mathbb{C}/\Lambda$ qui est muni de la loi de groupe quotient, l'application d'Abel-Jacobi α est un isomorphisme de groupes.*

Remarque 1.4.6. — Si on note $\mathrm{Div}^0(\mathbb{C}/\Lambda) \subset \mathrm{Div}(\mathbb{C}/\Lambda)$ le sous-groupe des diviseurs de degré nul, il existe une application $\beta' : \mathrm{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$ qui envoie $\sum_P n_P \cdot (P)$ sur $\sum_P n_P \cdot P$, donc qui échange la somme formelle de points de $\mathrm{Div}^0(E)$ contre la somme usuelle des points de $\mathbb{C}/\Lambda$. Il est clair que β' est un morphisme de groupes. Notons $\alpha' : \mathbb{C}/\Lambda \to \mathrm{Div}^0(\mathbb{C}/\Lambda)$ l'application $x \mapsto (x) - (0_E)$ qui relève α de $\mathrm{Pic}^0(E)$ à $\mathrm{Div}^0(E)$. On a clairement $\beta' \circ \alpha' = \mathrm{Id}$. Tout l'enjeu de la proposition est donc de montrer que β' se factorise en $\beta : \mathrm{Pic}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$.

Corollaire 1.4.7. — *Soit $D = \sum_{P \in \mathbb{C}/\Lambda} n_P \cdot (P)$ un diviseur de $\mathbb{C}/\Lambda$. Il existe une fonction méromorphe sur $\mathbb{C}/\Lambda$ de diviseur D si et seulement si $\sum_P n_P = 0$ et $\sum_P n_P \cdot P = 0_{\mathbb{C}/\Lambda}$.*

Démonstration. — C'est une retraduction de l'isomorphisme de groupe $\alpha^{-1} : \mathrm{Pic}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$ qui envoie $\sum_P n_P \cdot (P)$ sur $\sum_P n_P \cdot P$. □

Remarque 1.4.8. — Ce corollaire est en fait équivalent au théorème 1.4.3. Montrons par exemple qu'il implique la surjectivité de α. Il s'agit étant donné $D \in \mathrm{Div}^0(\mathbb{C}/\Lambda)$ de

trouver $x \in \mathbb{C}/\Lambda$ tel que $D \sim (x)-(0_E)$. Si $D = \sum_P n_P \cdot (P)$ il suffit de poser $x = \sum_P n_P \cdot P$. On en verra une démonstration purement analytique en TD à l'aide de la fonction σ de Weierstrass.

Rappelons la loi de groupe folklorique sur le lieu d'annulation E d'un polynôme $Y^2Z - 4X^3 + aXZ^2 + bZ^3$ dans $\mathbb{P}^2_{\mathbb{C}}$ avec $\Delta = a^3 - 27b^2 \neq 0$, vu comme surface de Riemann. Cette loi explicite permet également de prouver l'holomorphie de la loi de groupe $E \times E \to E$. On munit E du point privilégié $0_E = [0;1;0]$. Soit $P, Q \in E$. On trace alors la droite projective de $\mathbb{P}^2_{\mathbb{C}}$ passant par P et Q, qui intersecte E en un troisième point R (qui peut être égal à P ou Q si cette droite est tangente à E). On trace ensuite la droite projective passant par 0_E et par R. Elle recoupe E en un point que l'on notera provisoirement $P \oplus Q$.

Remarque 1.4.9. — On a utilisé le théorème de Bezout, qui dit que deux courbes de $\mathbb{P}^2_{\mathbb{C}}$ donnée par l'annulation de polynômes homogènes de degrés n et m et sans composante irréductible commune ont exactement nm points d'intersection comptés avec multiplicité. Vu qu'ici un des degrés est un, le théorème se vérifie par un calcul direct dans ce cas. Ce théorème admet de vastes généralisations connues sous le nom de « théorie de l'intersection ».

Proposition 1.4.10. — *L'isomorphisme d'Abel-Jacobi $\alpha : E \xrightarrow{\sim} \mathrm{Pic}^0(E)$, $x \mapsto (x) - (0_E)$ envoie $x \oplus y$ sur $\alpha(x) + \alpha(y)$ pour tous $x, y \in E$. En particulier $\oplus$ est une loi de groupe abélien sur E et α est un isomorphisme de groupes.*

Démonstration. — Soit $f(X,Y,Z)$ l'équation homogène de degré 1 de la droite projective de $\mathbb{P}^2_{\mathbb{C}}$ reliant x et y et soit z l'autre point d'intersection de cette droite et de E. La fraction rationnelle f/Z est homogène de degré 0 donc définit une fonction sur l'ouvert de $\mathbb{P}^2_{\mathbb{C}}$ où $Z \neq 0$. On voit f/Z comme une fonction méromorphe sur E par restriction. Son diviseur est donc $(x) + (y) + (z) - 3 \cdot (0_E)$.

De même soit $g(X,Y,Z)$ l'équation de la droite reliant 0_E, z et $x \oplus y$. Le diviseur de g/Z vue comme fonction méromorphe sur E est $(z) + (x \oplus y) - 2 \cdot (0_E)$. Au final le diviseur de g/f est $(x \oplus y) - (x) - (y)$ et on a donc bien $\alpha(x \oplus y) = \alpha(x) + \alpha(y)$. □

Remarque 1.4.11. — On aurait pu définir plus synthétiquement la loi de groupe $\oplus$ en disant que pour tous $x, y, z \in E$ on a $z \oplus y \oplus z = 0_E$ si et seulement si x, y et z sont alignés.

On remarquera néanmoins qu'il n'est pas du tout évident que $\oplus$ soit associative, et en particulier soit une loi de groupes. Aussi les formules explicite pour $\oplus$ que nous verrons en TD ne sont pas très jolies. Dans notre optique, la bonne manière de comprendre la loi de groupes sur E est vraiment d'utiliser α pour transporter la loi de groupe canonique sur $\mathrm{Pic}^0(E)$.

On verra plus loin les courbes elliptiques sur les corps finis, qui sont très utiles pour la cryptographie. Ce n'est n'est que dans cette optique informatique que les équations explicites pour la loi de groupe s'avèrent importantes.

1.5. Invariant modulaire

Le j-invariant est un nombre complexe qui caractérise la classe d'isomorphisme d'une courbe elliptique. Rappelons ses divers incarnations selon les diverses visions possibles de E.

1.5.1. Le cas de $\mathbb{C}/\Lambda$. — Soit $\Lambda \subset \mathbb{C}$ un réseau. Rappelons qu'on a noté $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ qui vérifie $\Delta(c\cdot\Lambda) = c^{-12}\Delta(\Lambda)$. On pose alors $j(\Lambda) = 1728\cdot g_2(\Lambda)^3/\Delta(\Lambda)$ qui vérifie $j(c\cdot\Lambda) = j(\Lambda)$. Ainsi j est une fonction sur l'ensemble des classes d'homothéties de réseau, c'est à dire une fonction $\mathcal{H}/\Gamma(1) \to \mathbb{C}$ qui est holomorphe.

Remarque 1.5.1. — On ne peut pas dire que j est une forme holomorphe de poids 0 car elle n'est pas holomorphe à l'infini. Elle a en fait un pôle simple en l'infini et son q-développement commence par $1/q + 744 + 196884q + \cdots$. L'intérêt de la normalisation par 1728 est de rendre le résidu égal à un. Vous noterez que dans le cours d'Alberto Minguez, la normalisation par 1728 était déjà cachée dans la définition de Δ, ce qui rend Δ normalisée de q-développement $q - 24q^2 + 252q^3 + \cdots$.

Lemme 1.5.2. — *Soient Λ et $\Lambda' \subset \mathbb{C}$ deux réseaux. Les surfaces de Riemann $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes si et seulement s'il existe $c \in \mathbb{C}^*$ tel que $\Lambda' = c\cdot\Lambda$.*

Démonstration. — Un sens est clair. Inversement soit $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ un isomorphisme de surface de Riemann. Il induit un isomorphisme $\mathbb{C}$-linéaire df sur les espaces tangents en $0_{\mathbb{C}/\Lambda}$ et en $0_{\mathbb{C}/\Lambda'}$. Donc $df : \mathbb{C} \to \mathbb{C}$ est la multiplication par un scalaire $c \in \mathbb{C}^*$ et par exponentiation de Lie on trouve que f est aussi la multiplication par c (voir la remarque 1.6.2 pour une autre démonstration n'utilisant pas l'exponentiation de Lie). □

Remarque 1.5.3. — Notons qu'on a pas demandé à f d'être un morphisme de groupes, mais on a comme corollaire que f est toujours un morphisme de groupes. Nous reverrons cela plus tard dans la proposition 1.6.1.

Proposition 1.5.4. — *La fonction j induit une bijection entre l'ensemble des classes d'isomorphismes de courbes elliptiques sur $\mathbb{C}$ et $\mathbb{C}$. Autrement dit les courbes elliptiques $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes si et seulement si $j(\Lambda) = j(\Lambda')$ et pour tout $j \in \mathbb{C}$ il existe $\Lambda \subset \mathbb{C}$ tel que $j(\Lambda) = j$.*

Démonstration. — Le lemme 1.5.2 montre que $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes si et seulement si Λ et Λ' sont homothétiques donc définissent le même point de $\mathcal{H}/\Gamma(1)$. Mais vous avez

vu dans le cours de formes modulaires (conséquence du « lemme $k/12$ ») que j induisait un isomorphisme de surfaces de Riemann $\mathcal{H}/\Gamma(1) \xrightarrow{\sim} \mathbb{C}$. □

Remarque 1.5.5. — On dit que $\mathcal{H}/\Gamma(1) \xrightarrow{\sim} \mathbb{C}$ est l'espace de modules grossier des courbes elliptiques. C'est la courbe modulaire ouverte de niveau $\Gamma(1)$ définie sur $\mathbb{C}$. On définira plus tard les courbes elliptiques sur $\mathbb{Q}$ et sur $\mathbb{Z}$ et cela permettrait de définir cette courbe modulaire sur $\mathbb{Q}$ ou sur $\mathbb{Z}$. De même pour tout sous-groupe d'indice fini de $\Gamma(1)$ lorsqu'on rajoute du niveau.

Exercice 5. — Faisons agir $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{Z}^2$ de la manière standard et faisons agir $\Gamma(1) \ltimes \mathbb{Z}^2$ sur $\mathcal{H} \times \mathbb{C}$ par la formule $(\gamma, (a,b)) \cdot (\tau, z) = (\gamma \cdot \tau, z + a + b\gamma \cdot \tau)$ où $\tau \in \mathcal{H}$, $z \in \mathbb{C}$, $(a,b) \in \mathbb{Z}^2$ et $\gamma \in \Gamma(1)$. Considérons $E^{\mathrm{univ}} = (\mathcal{H} \times \mathbb{C})/(\Gamma_1 \ltimes \mathbb{Z}^2)$ qui est muni d'un morphisme $f : E^{\mathrm{univ}} \to \mathcal{H}/\Gamma(1)$. Pour tout $\tau \in \mathcal{H}/\Gamma(1)$, est-ce que $f^{-1}(\tau)$ est la courbe modulaire d'invariant $j(\tau)$? Autrement dit, existe-t-il une courbe elliptique universelle sur $\mathcal{H}/\Gamma(1)$? Si il y a un problème, d'où vient-il ?

1.5.2. Le cas d'un polynôme de degré 3. — Notons E le lieu d'annulation d'un polynôme $Y^2Z - 4X^3 + aXZ^2 + bZ^3$ dans $\mathbb{P}^2_{\mathbb{C}}$ avec $\Delta = a^3 - 27b^2 \neq 0$, vu comme courbe algébrique. De même notons E' le lieu d'annulation d'un polynôme $Y^2Z - 4X^3 + a'XZ^2 + b'Z^3$ avec $\Delta' = a'^3 - 27b'^2 \neq 0$. On cherche tous les changements de variable donnés par des fractions rationnelles sans pôles sur E et E' qui induisent un isomorphisme $E \xrightarrow{\sim} E'$. On trouve par calcul direct.

Lemme 1.5.6. — *Les seuls changements de variable bijectifs entre l'équation* $Y^2Z - 4X^3 + aXZ^2 + bZ^3$ *et l'équation* $Y'^2Z' - 4X'^3 + a'X'Z'^2 + b'Z'^3$ *s'obtiennent en posant* $X' = c^2 \cdot X$, $Y' = c^3 \cdot Y$, $Z' = Z$ *avec* $c \in \mathbb{C}^*$. *Cela implique que* $a' = c^4 \cdot a$, $b' = c^6 \cdot b$ *et* $\Delta' = c^{12} \cdot \Delta$.

Remarque 1.5.7. — On retrouve de manière algébrique la proposition 1.5.4. On retrouve aussi les propriétés d'homogénéité de poids 4, 6 et 12 des fonctions g_2, g_3 et Δ ainsi que celles de poids 2 et 3 de $\wp$ et $\wp'$.

La traduction directe de la proposition 1.5.4 en terme de surfaces de Riemann définies par des équations dans $\mathbb{P}^2_{\mathbb{C}}$ aurait été de chercher les changements de variable donnés par des applications biholomorphes qui ne sont pas nécessairement des fonctions rationnelles. On peut soit se convaincre par calcul que tout tel changement de variable est aussi de la forme $X' = c^2 \cdot X$, $Y' = c^3 \cdot Y$, $Z' = Z$ donc polynomial, soit appliquer la théorie GAGA générale qui dit que pour toutes variétés algébriques projectives X et Y, on a une bijection entre les applications holomorphes à plusieurs variables $X^{\mathrm{an}} \to Y^{\mathrm{an}}$ et les applications algébriques $X \to Y$, où X^{an} est la variété complexe associée à X.

Exercice 6. — Prouver un comme cas particulier de ce principe GAGA que toute fonction méromorphe $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{C}$ qui est holomorphe hors de ∞ est un polynôme.

On pose alors $j(E) = 1728a^3/\Delta$ et on a prouvé que E est isomorphe à E' si et seulement si $j(E) = j(E')$. De plus il est clair que pour tout $j \in \mathbb{C}$ il existe E telle que $\Delta \neq 0$ et $j(E) = j$.

Remarque 1.5.8. — Si E et E' sont isomorphes, on n'a pas $\Delta = \Delta'$ ce qui est cohérent avec le fait que Δ est une forme modulaire de poids 12 et pas 0. Par contre Δ et Δ' s'annulent simultanément, ce qui est cohérent avec le fait que E est lisse si et seulement si E' l'est.

1.6. Morphismes

Soit E une courbe elliptique sur $\mathbb{C}$. La proposition suivante peut paraître surprenante. Elle montre un lien caché entre holomorphie et respect de la loi de groupe.

Proposition 1.6.1. — *Soient E et E' deux courbes elliptiques sur $\mathbb{C}$ et $f : E \to E'$ un morphisme de surfaces de Riemann tel que $f(0_E) = 0_{E'}$. Alors f est un morphisme de groupes.*

Démonstration. — Prenons E de la forme $\mathbb{C}/\Lambda$ et E' de la forme $\mathbb{C}/\Lambda'$ pour $\Lambda : \Lambda' \subset \mathbb{C}$ des réseaux . On a donc $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ dont la différentielle $df : \mathbb{C} \to \mathbb{C}$ l'origine de E et de E' est $\mathbb{C}$-linéaire. Donc $df(z) = \alpha \cdot z$ avec $\alpha \in \mathbb{C}$. On a alors $f(z+\Lambda) = df(z) + \Lambda' = \alpha \cdot z + \Lambda'$ par exponentiation de Lie donc f est un morphisme de groupes. □

Remarque 1.6.2. — Donnons une autre démonstration de la proposition 1.6.1 qui évite l'exponentiation de Lie. Si $f : E \to E'$ est holomorphe, elle se relève en $\tilde{f} : \mathbb{C} \to \mathbb{C}$ holomorphe vérifiant $\tilde{f}(\Lambda) \subset \Lambda'$ et $\tilde{f}(0) = 0$. On a donc $\tilde{f}(z+\omega) - \tilde{f}(z) \in \Lambda'$ pour tout $z \in \mathbb{C}$ et $\omega \in \Lambda$. Comme Λ' est discret on en déduit que $\tilde{f}(z+\omega) - \tilde{f}(z)$ est constant en z donc que $\tilde{f}'(z+\omega) = \tilde{f}'(z)$. Donc $\tilde{f}' : \mathbb{C} \to \mathbb{C}$ est holomorphe et Λ-périodique donc constante égale à $\alpha \in \mathbb{C}$ par le théorème de Liouville. Donc $\tilde{f}(z) = \alpha \cdot z + \beta$ pour tout $z \in \mathbb{C}$. Comme $\tilde{f}(0) = 0$ on a $\beta = 0$ donc $\tilde{f}(z) = \alpha \cdot z$ puis $f(z) = \alpha \cdot z$.

On appellera désormais *morphisme* entre courbes elliptiques toute application holomorphe préservant le neutre donc la loi de groupe. On a en fait prouvé au cours de la démonstration de la proposition 1.6.1 le lemme suivant.

Lemme 1.6.3. — *Soit $E = \mathbb{C}/\Lambda$ et $E' = \mathbb{C}/\Lambda'$ deux courbes elliptiques sur $\mathbb{C}$. Tout morphisme $f : E \to E'$ s'obtient par passage au quotient de l'application $\mathbb{C} \to \mathbb{C}$, $z \mapsto \alpha \cdot z$ avec $\alpha \cdot \Lambda \subset \Lambda'$.*

La proposition suivante est un cas particulier des théorèmes GAGA qui disent que tout morphisme holomorphe (*resp.* méromorphe) entre variétés complexes projectives est une application algébrique régulière (*resp.* rationnelle). Voir aussi l'exercice 6.

Proposition 1.6.4. — *Soit E^{alg} et E'^{alg} deux courbes projectives lisses de genre 1. Désignons par $(E^{\mathrm{alg}})^{\mathrm{an}}$ et $(E'^{\mathrm{alg}})^{\mathrm{an}}$ les surfaces de Riemann associées. Toute application holomorphe $f : (E^{\mathrm{alg}})^{\mathrm{an}} \to (E'^{\mathrm{alg}})^{\mathrm{an}}$ provient d'une unique application algébrique régulière $f^{\mathrm{an}} : E^{\mathrm{an}} \to E'^{\mathrm{an}}$.*

Démonstration. — Notons $(E^{\mathrm{alg}})^{\mathrm{an}} = \mathbb{C}/\Lambda$ et $(E'^{\mathrm{alg}})^{\mathrm{an}} = \mathbb{C}/\Lambda'$. D'après le lemme 1.6.3, le morphisme f est donnée par la multiplication par $\alpha \in \mathbb{C}$ vérifiant $\alpha \cdot \Lambda \subset \Lambda'$. Aussi l'algébrisation de $\mathbb{C}/\Lambda$ est donnée par le morphisme $z \mapsto [\wp_\Lambda(z); \wp'_\Lambda(z); 1] \in \mathbb{P}^2_{\mathbb{C}}$ et celle de $\mathbb{C}/\Lambda$ par $z \mapsto [\wp_{\Lambda'}(z); \wp'_{\Lambda'}(z); 1] \in \mathbb{P}^2_{\mathbb{C}}$. Il faut donc vérifier que $\wp_{\Lambda'}(\alpha \cdot z)$ et $\wp'_{\Lambda'}(\alpha \cdot z)$ sont des fractions rationnelles en $\wp_\Lambda(z)$ et en $\wp'_\Lambda(z)$. Mais $\wp_{\Lambda'}(\alpha \cdot z)$ et $\wp'_{\Lambda'}(\alpha \cdot z)$ sont méromorphes et Λ-périodique car $\alpha \cdot \Lambda \subset \Lambda'$. Or nous avons vu en TD que toute fonction méromorphe Λ-périodique sur $\mathbb{C}$ est fraction rationnelle en $\wp_\Lambda(z)$ et en $\wp'_\Lambda(z)$. □

Définition 1.6.5. — Un endomorphisme de E est un morphisme de surfaces de Riemann de E dans E qui respecte la loi de groupe.

D'après la proposition 1.6.1, tout morphisme holomorphe de E dans E qui respecte 0_E est un endomorphisme.

Exemple 1.6.6. — Si $f = [n] : E \to E$ désigne le morphisme $x \mapsto [n] \cdot x$ (qui est n additions successives de x si $n \geq 0$ et de l'opposé $[-1] \cdot x$ de x si $n > 0$) alors f est un endomorphisme pour tout $n \in \mathbb{Z}$. On a bien sûr $[0] = 0_E$ et $[1] = \mathrm{Id}_E$.

Notons $\mathrm{End}(E)$ l'ensemble des endomorphismes. On peut les additionner en utilisant la loi de groupe de E (qui est commutatif) et les multiplier en les composant. Ainsi $\mathrm{End}(E)$ est un anneau. De plus cet anneau contient $\mathbb{Z}$ par le morphisme $n \mapsto [n]$ qui est clairement injectif. Enfin les automorphismes de E sont les inversibles de l'anneau $\mathrm{End}(E)$.

Définition 1.6.7. — Soit K un corps de nombres. Un ordre de K est un sous-anneau $A \subset K$ qui est un sous-$\mathbb{Z}$-module de type fini tel que $K = \mathrm{Frac}(A)$.

Proposition 1.6.8. — *Soit E une courbe elliptique sur $\mathbb{C}$. L'anneau $\mathrm{End}(E)$ est soit isomorphe à $\mathbb{Z}$ par l'application $n \mapsto [n]$, soit isomorphe à un ordre d'un corps quadratique imaginaire. En particulier $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ est un corps de nombres de degré ≤ 2 sur $\mathbb{Q}$. Enfin le groupe des automorphismes $\mathrm{Aut}(E)$ est fini de cardinal 2, 4 ou 6.*

Démonstration. — Supposons $E = \mathbb{C}/\Lambda$ avec $\Lambda = \mathbb{Z} + \mathbb{Z} \cdot \tau$. D'après le lemme 1.6.3, l'anneau des endomorphismes de E est le sous-anneau de $\mathbb{C}$ formé des $\alpha \in \mathbb{C}$ tels que $\alpha \cdot \Lambda \subset \Lambda$. Donc $\alpha \in \Lambda$ s'écrit sous la forme $\alpha = a + b \cdot \tau$ avec $a, b \in \mathbb{Z}$ et la condition devient $\alpha \cdot \tau \in \Lambda$ ce qui impose $\alpha \cdot \tau = c + d \cdot \tau$ avec $c, d \in \mathbb{Z}$. On trouve comme condition $\alpha^2 - (a+d)\alpha + ad - bc = 0$ et en particulier $\mathrm{End}(E)$ est un anneau entier sur $\mathbb{Z}$.

Si $\alpha \notin \mathbb{Z}$ on a $b \neq 0$ donc $b\tau^2 - (a-d)\tau - c = 0$. On voit donc que $\mathbb{Q}(\tau)$ est une extension quadratique de $\mathbb{Q}$, nécessairement imaginaire car $\tau \in \mathcal{H}$. Enfin on trouve que $\mathrm{End}(E)$ est entier sur $\mathbb{Z}$ inclus dans $\mathbb{Q}(\tau)$ donc un ordre de $\mathbb{Q}(\tau)$. La dernière assertion provient de la finitude des unités de $\mathcal{O}_{\mathbb{Q}(\tau)}$ et de leur égalité avec l'ensemble des racines de l'unité. □

Remarque 1.6.9. — On a prouvé que $E = \mathbb{C}/(\mathbb{Z} + \tau \cdot \mathbb{Z})$ a un anneau d'endomorphismes $\neq \mathbb{Z}$ si et seulement si $\tau \in \mathcal{H}$ est quadratique imaginaire, en particulier est dans $\bar{\mathbb{Q}}$. On dira dans ce cas que E a multiplication complexe. De part leurs symétries exceptionnelles, les courbes elliptiques à multiplication complexe s'avèrent bien plus simple à manipuler que les courbes générales. Du point de vue de l'arithmétique, elles sont proches de la théorie du corps de classe alors que les courbes elliptiques générales sont plutôt reliées au programme de Langlands pour le groupe non abélien GL_2.

Remarque 1.6.10. — Le groupe $\mathrm{Aut}(E)$ n'est jamais trivial car il contient toujours $[-1]$. C'est à cause de cela qu'il n'existe pas de courbe elliptique universelle sur $\mathcal{H}/\Gamma(1)$ (voir l'exercice 5). Le groupe $\mathrm{Aut}(E)$ est de cardinal 4 si $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[i]$ donc si $\tau \in \mathbb{Q}[i]$. Le groupe $\mathrm{Aut}(E)$ est de cardinal 6 si $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[j]$ avec $j = e^{2i\pi/3}$ donc si $\tau \in \mathbb{Q}[j]$. On verra en fait en TD que $\mathrm{Aut}(E)$ est de cardinal 4 si et seulement si $j(\tau) = 0$ et que $\mathrm{Aut}(E)$ est de cardinal 6 si et seulement si $j(\tau) = 1728$. Le lecteur pourra d'ailleurs relier ces propriétés à l'action de $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}$ et notamment au cardinal des stabilisateurs.

Exercice 7. — Soit S une variété complexe. On dit qu'une courbe elliptique (relative) E sur S est une variété complexe E munie d'un morphisme holomorphe submersif $f : E \to S$ et d'une section $e : S \to E$ vérifiant $f \circ e = \mathrm{Id}_S$ tels que pour tout $s \in S$, $f^{-1}(\{s\})$ est une courbe elliptique d'origine $e(s)$.

Montrer que pour toute variété complexe S et toute courbe elliptique relative $E \to S$ il existe une unique application holomorphe $g : S \to \mathcal{H}/\Gamma(1)$ telle que pour tout $s \in S$ on ait un isomorphisme $f^{-1}(s) = \mathbb{C}/(\mathbb{Z} + g(s) \cdot \mathbb{Z})$.

Considérons le foncteur $\mathcal{F}$ qui à toute variété complexe S associe l'ensemble des classes d'isomorphismes de courbes elliptiques relatives $E \to S$. Prouver que $\mathcal{F}$ n'est pas un faisceau et n'est en fait même pas un préfaisceau séparé. Autrement dit il existe S et un recouvrement ouvert $S = \cup_i U_i$ tel que l'application de restriction $\mathcal{F}(S) \to \prod_i \mathcal{F}(U_i)$ n'est pas injective. En déduire qu'il n'existe pas de courbe elliptique relative $E \to \mathcal{H}/\Gamma(1)$.

Remarque 1.6.11. — On dit que $\mathcal{H}/\Gamma(1)$ est l'*espace de module grossier* des courbes elliptiques car il paramètre les classes d'isomorphismes de courbes elliptiques. On dit que ce n'est pas un *espace de modules fin* car il n'admet pas de courbe elliptique relative universelle.

On peut corriger la situation en rajoutant des structures de niveau aux courbes elliptiques, ce qui correspond à diviser $\mathcal{H}$ par un sous-groupe d'indice fini assez grand de $\Gamma(1)$,

et ce qui tue les automorphismes (voir l'exercice 8). On peut aussi corriger le problème en remplaçant le quotient naïf $\mathcal{H}/\Gamma(1)$ par un quotient nettement moins naïf noté $[\mathcal{H}/\Gamma(1)]$ et qui n'est pas un ensemble mais une catégorie (plus exactement un faisceau en catégories). Il s'agit d'un champ algébrique ou analytique.

Le problème vu dans l'exercice précédent est absolument général : lorsqu'on cherche à paramétrer des objets possédants des automorphismes non triviaux, on obtient un préfaisceau non séparé et en particulier, il ne peut pas exister d'espace de modules muni d'un objet universel. Il faut soit rigidifier la situation pour tuer les automorphismes soit passer aux champs.

1.7. Points de torsion et isogénies

Soient E et E' deux courbes elliptiques complexes. Dans la défintion suivante on pourrait tenir compte de la proposition 1.6.1 et demander seulement $f(0_E) = 0_{E'}$, ce qui garantit que f est un morphisme de groupes.

Définition 1.7.1. — Une isogénie de E dans E' est un morphisme de groupes holomorphe non nul $E \to E'$.

Remarque 1.7.2. — Dans [**Si**, III.4], les isogénies sont définies comme tous les morphismes de groupes holomorphes. En particulier le morphisme nul est une isogénie avec cette convention, qui n'est pas standard et que nous abandonnerons.

Lemme 1.7.3. — *Une isogénie est un revêtement fini étale de E' par E.*

Démonstration. — Comme une isogénie f est non constante et que sa source et son but ont dimension 1, elle est submersive. Par compacité elle est surjective et c'est donc un revêtement éventuellement ramifié. Mais comme f est un morphisme de groupe, le lieu de ramification de f est stable par addition de n'importe quel $x \in E$. Vu que tout revêtement est non ramifié sur un ouverte dense, on en déduit que f est non ramifié. □

Soit $f : E \to E'$ une isogénie. On notera $\deg(f)$ le degré du revêtement fini étale qu'elle définit.

Lemme 1.7.4. — *Soit f une isogénie. Son noyau* $\mathrm{Ker}(f)$ *est un sous-groupe fini de E de cardinal* $\deg(f)$.

Exemple 1.7.5. — Considérons l'isogénie $[n] : E \to E$ pour $n > 0$. Son degré est n^2 et son noyau $E[n]$ est non canoniquement isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$. On dira que $E[n]$ est l'ensemble des points de n-torsion de E. Si $E = \mathbb{C}/\Lambda$ on a un isomorphisme canonique $E[n] \xrightarrow{\sim} \frac{1}{n} \cdot \Lambda/\Lambda \xrightarrow{\sim} \Lambda/n \cdot \Lambda$.

Exercice 8. — Supposons $n \geq 3$. Soit E une courbe elliptique sur $\mathbb{C}$ et $f \in \mathrm{Aut}(E)$ un automorphisme qui est l'identité sur le sous-ensemble $E[n] \subset E$. Prouver que f est l'identité de E. Donner un contre-exemple si $n \leq 2$. Faire le lien avec l'exercice 7.

Exemple 1.7.6. — Soit $E = \mathbb{C}/\Lambda$, $E' = \mathbb{C}/\Lambda'$ et $f : E \to E'$, $z \mapsto \alpha \cdot z$ avec $\alpha \cdot \Lambda \subset \Lambda'$. On a $\mathrm{Ker}(f) = \frac{1}{\alpha}\Lambda/\Lambda' \xrightarrow{\sim} \Lambda'/\alpha \cdot \Lambda$ et $\deg(f)$ est donc le covolume de l'inclusion de réseaux $\alpha \cdot \Lambda \subset \Lambda'$.

Exemple 1.7.7. — Si $E = E' = \mathbb{C}/\Lambda$ et $f(z) = \alpha \cdot z$ est une isogénie de E dans E, où $\alpha \in \mathbb{C}^*$ vérifie $\alpha \cdot \Lambda \subset \Lambda$, on voit par calcul explicite que $\deg(f) = |\alpha|^2$. En particulier le carré du module de α est entier. Aussi la forme $\mathrm{End}(E) \to \mathbb{N}$, $f \mapsto \deg(f)$ est quadratique. Ce dernier point n'est pas facile à prouver algébriquement.

Définition 1.7.8. — Soit E et E' des courbes elliptiques complexes et $f : E \to E'$ une isogénie de degré n. L'isogénie duale $\hat{f} : E' \to E$ est l'unique isogénie telle que $\hat{f} \circ f = [n]_E$ et $f \circ \hat{f} = [n]_{E'}$.

Remarque 1.7.9. — On dit que E et E' sont isogènes s'il existe une isogénie de E dans E'. Cela implique que les corps $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ et $\mathrm{End}(E') \otimes_{\mathbb{Z}} \mathbb{Q}$ sont isomorphes. L'unicité de l'isogénie duale provient alors du caractère intègre de $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Lorsque $E = \mathbb{C}/\Lambda$ et $E' = \mathbb{C}/\Lambda'$, on voit que E et E' sont isogènes si et seulement si les réseaux Λ et Λ' sont commensurables à homothétie près.

Exemple 1.7.10. — Lorsque $E = E'$ et $f = [n]$ on a tout simplement $\hat{f} = f = [n]$ et $\hat{f} \circ f = [n] \circ [n] = [n^2]$ et effectivement $\deg([n]) = n^2$.

Exemple 1.7.11. — Si E a multiplication complexe par le corps quadratique imaginaire $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ on a $\deg(f) = N_{K/\mathbb{Q}}(f)$ pour tout $f \in \mathrm{End}(E)$ où $\mathrm{End}(E)$ est identifié à un ordre de K. Aussi $\hat{f}$ est simplement égal au conjugué $\bar{f}$ de f vu comme élément de K. On a bien $\hat{f} \circ f = \bar{f} \cdot f = N_{K/\mathbb{Q}}(f)$.

Proposition 1.7.12. — *Toute isogénie admet une isogénie duale.*

Démonstration. — Il s'agit de prouver que pour tous réseaux $\Lambda, \Lambda' \subset \mathbb{C}$ et tout $\alpha \in \mathbb{C}$ tel que $\alpha \cdot \Lambda \subset \Lambda'$ il existe $\beta \in \mathbb{C}$ avec $\beta \cdot \Lambda' \subset \Lambda$ et $\alpha \cdot \beta = n$ où $n = \mathrm{Card}(\Lambda'/\alpha \cdot \Lambda)$ par l'exemple 1.7.6. On pose donc $\beta = n/\alpha$ et on vérifie élémentairement qu'il convient. □

Remarque 1.7.13. — Lorsque $E = E' = \mathbb{C}/\Lambda$ et $f(z) = \alpha \cdot z$ avec $\alpha \cdot \Lambda \subset \Lambda$ on a tout simplement $\hat{f}(z) = \bar{\alpha} \cdot z$ ce qui est conforme à l'exemple 1.7.11.

CHAPITRE 2

COURBES ELLIPTIQUES SUR UN CORPS

2.1. Une preuve du théorème de Riemann-Roch

2.1.1. Bréviaire de géométrie algébrique. — Soit k un corps et X une courbe projective lisse connexe sur k. Par définition il existe donc un entier $n \geq 1$ et une immersion fermée $X \hookrightarrow \mathbb{P}^n_k$. Nous allons maintenant rappeler ce que cela veut dire.

Remarque 2.1.1. — Nous adopterons dans ce cours le point de vue des schémas, même si peu de choses changeraient en considérant celui un peu plus simple des variétés algébriques données localement par le spectre maximal de k-algèbres de tye fini.

Par définition, dans le point de vue des schémas, X est un espace topologique muni d'un faisceau d'anneaux $\mathcal{O}_X$ tel que le couple $(X, \mathcal{O}_X)$ est localement isomorphe au schéma affine $(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$. Ici A est une k-algèbre de type fini et $\mathrm{Spec}(A)$ est l'ensemble des idéaux premiers de A muni de la topologie de Zariski, qui est engendrée par les ouverts de la forme

$$D(f) \;=\; \{\mathfrak{p} \in \mathrm{Spec}(A) \mid f \notin \mathfrak{p}\}$$

pour $f \in A$. On définit le préfaisceau $\mathcal{O}_X$ en posant $\Gamma(D(f), \mathcal{O}_X) = A[\frac{1}{f}]$ et on vérifie qu'il s'agit bien d'un faisceau.

On voit donc que les fermés de $\mathrm{Spec}(A)$ sont exactement les

$$\mathrm{Spec}(A/I) \;=\; \{\mathfrak{p} \in \mathrm{Spec}(A) \mid I \subset \mathfrak{p}\}$$

pour I un idéal de A. On interprète cela en disant que $\mathrm{Spec}(A/I)$ est donné dans $\mathrm{Spec}(A)$ par l'ensemble des équations $f = 0$ pour tout $f \in I$. De plus on a l'inclusion $\mathrm{Spec}(A/I) \subset \mathrm{Spec}(A/J)$ si et seulement si $J \subset I$ (plus il y a d'équations moins il y a de solutions). Ainsi pour tout point $x = \mathfrak{p} \in \mathrm{Spec}(A)$ le singleton $\{x\} \subset \mathrm{Spec}(A)$ n'est pas nécessairement fermé. Au contraire son adhérence est

$$\overline{\{x\}} \;=\; \{\mathfrak{p}' \in \mathrm{Spec}(A) \mid \mathfrak{p} \subset \mathfrak{p}'\}\,.$$

On voit donc que x est fermé si et seulement si $\mathfrak{p}$ est maximal. Si A est intègre et que A n'est pas un corps, on voit que l'idéal $\{0\}$ est premier et définit un point η non fermé dans $\mathrm{Spec}(A)$. Son adhérence est $\overline{\{\eta\}} = \mathrm{Spec}(A)$ et on dit que η est générique.

Pour tout $x \in X$ on notera $k(x)$ son corps résiduel, qui est une extension de k. Lorsque $X = \mathrm{Spec}(A)$ et $x = \mathfrak{p}$ on a par définition $k(x) = \mathrm{Frac}(A/\mathfrak{p})$. Le Nullstellensatz de Hilbert implique que $k(x)/k$ est une extension de degré fini lorsque x est un point fermé (correspondant donc à un idéal maximal de A). Par contre lorsque A est intègre et n'est pas un corps et que $x = \eta$ correspond à l'idéal nul, on a $k(x) = \mathrm{Frac}(A)$ qui n'est pas une k-algèbre de type fini.

Pour tout $x \in X$ on note $\mathcal{O}_{X,x}$ l'anneau local de X en x. Lorsque $X = \mathrm{Spec}(A)$ et $x = \mathfrak{p} \in \mathrm{Spec}(A)$, on a par définition $\mathcal{O}_{X,x} = A_{\mathfrak{p}}$ où $A_{\mathfrak{p}}$ désigne la localisation de A en la partie multiplicative $A - \mathfrak{p}$. Comme le nom l'indique, $\mathcal{O}_{X,x}$ est un anneau local d'idéal maximal $\mathfrak{p}$. Le point éventuellement non fermé $x \in X$ définit donc un point fermé (qui est l'unique point fermé) de $\mathrm{Spec}(\mathcal{O}_{X,x})$. Remplacer X par $\mathrm{Spec}(\mathcal{O}_{X,x})$ permet donc de rendre le point x fermé.

Dans notre cas on suppose de plus que X est une courbe ce qui se traduit par le fait que le degré de transcendance sur k du corps des fractions de A est 1 (le corps des fractions est un produit de corps et c'est un corps si et seulement si A est intègre). Cela se traduit aussi par le fait que tout idéal premier est soit minimal soit maximal. Les chaînes croissantes pour l'inclusion d'idéaux premiers sont donc de longueur ≥ 2.

On suppose aussi que X est lisse sur $\mathrm{Spec}(k)$, ce qui est équivalent à demander que les anneaux A précédents sont réguliers, donc que $\dim_{k(x)}(\mathfrak{m}_x/\mathfrak{m}_x^2) = 1$ pour tout point fermé $x \in X$ correspondant à un idéal maximal $\mathfrak{m}_x \subset A$. Cela implique que $\mathcal{O}_{X,x}$ est un anneau de valuation discrète pour tout point fermé $x \in X$. Soit z_x une uniformisante de $\mathcal{O}_{X,x}$. On a donc $z_x \in \mathfrak{m}_x$ et l'image de z_x dans $\mathfrak{m}_x/\mathfrak{m}_x^2$ forme une $k(x)$-base du $k(x)$-espace vectoriel $\mathfrak{m}_x/\mathfrak{m}_x^2$ de dimension un. On peut voir z_x comme l'analogue direct des coordonnées locales dans la théorie des surfaces de Riemann.

On suppose enfin que X est projective ce qui se traduit par le fait qu'il existe un entier n, un idéal homogène (c'est-à-dire engendré par des polynômes homogènes) $I \subset k[X_0, \cdots, X_n]$ et un isomorphisme entre X et l'ensemble des idéaux premiers homogènes de $k[X_0, \cdots, X_n]/I$ distincts de $(X_0, \ldots, X_n) \bmod I$

Au final tous les points de X sont fermés sauf un unique point générique η dont l'adhérence est X tout entier.

Enfin on dit que X est connexe si pour tout ouvert affine $\mathrm{Spec}(A) \subset X$ l'anneau A ne contient pas d'idempotent non trivial.

Remarque 2.1.2. — Une solution trop naïve aurait été de regarder l'ensemble des coordonnées homogènes $[X_0; \cdots; X_n] \in \mathbb{P}_k^n(k)$ vérifiant par conséquent $X_i \in k$ pour tout

$1 \leq i \leq n$ et telles que $P(X_0, \cdots, X_n) = 0$ pour tout $P \in I$ où $I \subset k[X_0, \cdots, X_n]$ est un idéal homogène.

Lorsque k n'est pas algébriquement clos, cet ensemble de solutions des équations $P(X_0, \cdots, X_n) = 0$ pour tout $P \in I$ peut en effet être vide. Regarder les équations contient donc plus d'informations que regarder leurs solutions dans un corps fixé. C'est la base de la philosophie de la théorie des schémas.

Lorsque k est algébriquement clos, le Nullstellensatz de Hilbert implique que si on définit $X \subset \mathbb{P}^n_k$ comme l'ensemble des idéaux premiers homogènes de $k[X_0, \cdots, X_n]/I$ distincts de $(X_0, \ldots, X_n) \bmod I$ avec $I \subset k[X_0, \cdots, X_n]$ un idéal homogène, l'ensemble des points fermés de X est en bijection canonique avec l'ensemble des $[X_0; \cdots; X_n] \in \mathbb{P}^n_k(k)$ tels que $P(X_0, \cdots, X_n) = 0$ pour tout $P \in I$. Le point de vue naïf est donc le bon, à la considération près des points génériques qui comme on le verra s'avèrent très pratiques.

Remarque 2.1.3. — Le foncteur qui à une k-algèbre A associe le schéma affine $\mathrm{Spec}(A)$ est contravariant. En effet pour tout morphisme d'algèbre $f : A \to B$ et pour tout idéal premier $\mathfrak{p} \subset B$, l'idéal $f^{-1}(\mathfrak{p}) \subset A$ reste premier.

Cela ne marcherait pas dans l'autre direction : si $A = \mathcal{O}_K$ et $B = \mathcal{O}_L$ sont les anneaux d'entiers de corps de nombres L/K, pour tout idéal premier $\mathfrak{q} \subset \mathcal{O}_K$, l'idéal $\mathfrak{q} \cdot \mathcal{O}_L$ n'est pas premier en général (avec la terminologie usuelle de la théorie des nombres, $\mathfrak{q} \cdot \mathcal{O}_K$ est premier si et seulement si $\mathfrak{q}$ est inerte dans L).

On voit enfin que la donnée de $f \in A$, c'est à dire la donnée de $f \in \Gamma(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$ est équivalente à la donnée d'un morphisme de k-algèbres $k[x] \to A$ qui envoie 1 sur f, donc à la donnée d'un morphisme de schémas affines $\mathrm{Spec}(A) \to \mathrm{Spec}(k[x])$. On notera $\mathbb{A}^1_k = \mathrm{Spec}(k[x])$ qu'on appelle « droite affine » sur k. Un théorème général de Grothendieck montre que ces groupes sont nuls si $i > 1$ car $\dim(X) = 1$.

Remarque 2.1.4. — Soit X une courbe algébrique sur k. On a muni X de la topologie de Zariski et d'un faisceau $\mathcal{O}_X$ tel que $H^0(\mathrm{Spec}(A), \mathcal{O}_X) = A$ pour tout ouvert de Zariski $\mathrm{Spec}(A) \subset X$. Le formalisme cohomologique général nous fournit alors des groupes $H^i(X, \mathcal{O}_X)$ pour tout $i \geq 0$. De même si $\mathcal{F}$ est un faisceau de $\mathcal{O}_X$-modules on dispose de $H^i(X, \mathcal{F})$ pour tout $i \geq 0$. On verra une description plus complète de ces groupes de cohomologie dans le paragraphe **2.1.3**.

2.1.2. Diviseurs. — Soit k un corps et X une courbe projective lisse connexe sur k. Notons $|X| \subset X$ l'ensemble des points fermés. On a donc $|X| = X - \{\eta\}$ avec η l'unique point générique de X. On a vu que pour tout $x \in |X|$ le degré de l'extension $k(x)/k$ est fini comme conséquence du Nullstellensatz.

On a note alors $\mathrm{Div}(X) = \mathbb{Z}[|X|]$ le groupe libre sur les points fermés $|X|$ de X. Pour tout $x \in |X|$ on pose $\deg(x) = \deg(k(x)/k)$. Pour tout $D = \sum_P n_P \cdot (P) \in \mathrm{Div}(X)$

on pose $\deg(D) = \sum_P n_P \cdot \deg(P)$. On obtient de la sorte un morphisme de groupes $\deg : \mathrm{Div}(X) \to \mathbb{Z}$. On note $\mathrm{Div}^0(X) = \mathrm{Ker}(\deg)$.

On note η l'unique point générique de X, qui dans le cas d'une courbe comme ici est aussi l'unique point non fermé. On note $k(\eta)$ le corps résiduel de η. Par construction il s'agit de l'ensemble des fonctions rationnelles sur X. Ces fonctions sont définies sur un plus grand ouvert Zariski U de X et ont des pôles sur $X - U$. Il s'agit de l'analogue algébrique des fonctions méromorphes en géométrie complexe.

Pour tout $f \in k(\eta)^*$ on note $\mathrm{div}(f) = \sum_P n_P \cdot (P) \in \mathrm{Div}(X)$ où $P \in |X|$ et $n_P \in \mathbb{Z}$ est l'ordre du zéro ou du pôle de f en P. On utilise plus précisément le fait que $\mathcal{O}_{X,P}$ est un anneau de valuation discrète dont le corps des fractions contient $k(\eta)$. On note alors n_P la valuation de f dans $\mathcal{O}_{X,P}$.

Dans la théorie complexe, nous avons utilisé à de maintes reprises le fait que le degré du diviseur d'une fonction méromorphe f est nul, ce qui se prouve avec le théorème des résidus appliqué à f'/f. Voilà la preuve algébrique du résultat analogue valable sur tout corps. On incitera vivement le lecteur à l'étudier de près, car de nombreux concepts de géométrie algébrique sont utilisés dans la démonstration de ce résultat basique.

Proposition 2.1.5. — *Soit $f \in k(\eta)^*$. On a* $\deg(\mathrm{div}(f)) = 0$.

Démonstration. — Soit $U \subset X$ un ouvert Zariski sur lequel f est régulière, *ie* sans pôles. En notant $\mathbb{A}^1_k = \mathrm{Spec}(k[x])$ on obtient à partir de f un morphisme de schémas $F : U \to \mathbb{A}^1_k$. On a par ailleurs une immersion ouverte $\mathbb{A}^1_k \subset \mathbb{P}^1_k$ qui identifie $\mathbb{A}^1_k$ à l'ouvert de Zariski de $\mathbb{P}^1_k$ où $Y \neq 0$, lorsqu'on note $[X;Y]$ les coordonnées homogènes sur $\mathbb{P}^1_k$. On obtient par composition $F : U \to \mathbb{P}^1_k$ dont on montre qu'il s'étend en un morphisme de schéma $F : X \to \mathbb{P}^1_k$ (c'est par exemple une application du « critère valuatif de propreté » pour lequel on renvoie à la remarque 2.1.6).

On doit alors distinguer deux cas : dans le premier $F : U \to \mathbb{A}^1_k$ est constant, ce qui se traduit par le fait que $f \in k \subset A$. On a alors $\mathrm{div}(f) = 0$ donc clairement $\deg(\mathrm{div}(f)) = 0$.

Dans le second cas $F : U \to \mathbb{A}^1_k$ est non constant. On voit alors que l'image de $F : X \to \mathbb{P}^1_k$ est un sous-schéma de $\mathbb{P}^1_k$ qui est connexe (puisque X l'est), qui n'est pas réduit à un point (car F n'est pas constant) et qui est fermé (car X est projectif donc propre, ce qui implique que F est propre). Or les seuls sous-schémas fermés de $\mathbb{P}^1_k$ sont les unions disjointes de points et tout $\mathbb{P}^1_k$. On en déduit que l'image de F est tout $\mathbb{P}^1_k$.

Comme F n'est pas constante, elle envoie le point générique de X sur le point générique de $\mathbb{P}^1_k$. On a donc un morphisme de corps nécessairement injectif $k(\eta_{\mathbb{P}^1_k}) \subset k(\eta_X)$ ainsi que pour tout $x \in X$ des injections $\mathcal{O}_{X,x} \subset k(\eta_X)$ et $\mathcal{O}_{\mathbb{P}^1_k} \subset k(\eta_{\mathbb{P}^1_k})$. On en conclut que $\mathcal{O}_{X,x}$ est $\mathcal{O}_{\mathbb{P}^1_k,F(x)}$-module sans torsion. Comme $\mathcal{O}_{\mathbb{P}^1_k,F(x)}$ est un anneau de valuation discrète, on en déduit que $\mathcal{O}_{X,x}$ est $\mathcal{O}_{\mathbb{P}^1_k,F(x)}$-module plat. On dit alors que F est plat.

Enfin pour tout $y \in \mathbb{P}^1_k$ la fibre $F^{-1}(\{x\})$ est finie car F est non constante et que $\dim(X) = \dim(\mathbb{P}^1_k)$. On dit alors que F est quasi-fini. Mais tout morphisme propre et quasi-fini et fini. On obtient que $\mathcal{O}_{X,x}$ est $\mathcal{O}_{\mathbb{P}^1_k,F(x)}$-module de type fini.

Soit $\mathrm{Spec}(A) \subset \mathbb{P}^1_k$ un ouvert de Zariski affine et $\mathrm{Spec}(B) \subset X$ son image inverse par F (on a utilisé que cette image inverse reste affine car F est un morphisme affine puisqu'il est fini). On a montré que B est un A-module plat de type fini, donc un A-module projectif de rang fini. Quitte à remplacer A par un ouvert affine plus petit on peut donc supposer que B est un A-module libre de rang fini, isomorphe à A^n pour un certain n. On dit que n est le rang de F, et toute la discussion précédente est en fait une présentation de la notion de rang d'un morphisme fini et plat.

Supposons maintenant que $\mathrm{Spec}(A) \subset \mathbb{P}^1_k$ un ouvert de Zariski affine contenant 0 et ∞. C'est possible car $\mathbb{P}^1_k$ privé de n'importe quel nombre ≥ 1 de points fermés est affine (et cela reste vrai pour toute courbe). On a donc deux idéaux maximaux $\mathfrak{m}_0$ et $\mathfrak{m}_\infty$ de A. On a alors des isomorphismes canoniques entre les schémas suivants munis de leur structure éventuellement non réduite (on verra qu'ils sont réduits si et seulement si $n_P \in \{-1, 0, 1\}$ pour tout $P \in |X|$).

$$\begin{aligned} F^{-1}(\{0\}) = X \times_{\mathbb{P}^1_k} \{0\} &= \mathrm{Spec}(B \otimes_A A/\mathfrak{m}_0) \\ F^{-1}(\{\infty\}) = X \times_{\mathbb{P}^1_k} \{\infty\} &= \mathrm{Spec}(B \otimes_A A/\mathfrak{m}_\infty) \end{aligned}$$

Mais l'algèbre $B \otimes_A A/\mathfrak{m}_0$ est artinienne égale à $\sum_{P\,|f(P)=0} \mathcal{O}_{X,P}/\mathfrak{m}_P^{n_P}$ et de même $B \otimes_A A/\mathfrak{m}_\infty$ est artinienne égale à $\sum_{P\,|f(P)=\infty} \mathcal{O}_{X,P}/\mathfrak{m}_P^{-n_P}$. On déduit les égalités

$$\begin{aligned} \deg(F) = n &= \sum_{P\,|f(P)=0} n_P \cdot \deg(P) \\ &= -\sum_{P\,|f(P)=\infty} n_P \cdot \deg(P) \end{aligned}$$

d'où enfin la proposition. □

Exercice 9. — Montrer qu'il est indispensable de normaliser $\deg(D)$ avec les facteurs $\deg(P)$ pour avoir $\deg(\mathrm{div}(f)) = 0$.

Remarque 2.1.6. — Le critère valuatif de propreté affirme qu'un schéma Y de type fini sur k est propre si et seulement si pour tout anneau de valuation discrète A de corps de fractions K, tout K-point de X s'étend en un A-point de X. Lorsque X est une variété projective sur k, on vérifie facilement le critère valuatif sur les coordonnées homogènes.

Lorsque X est une courbe algébrique lisse sur k et Y est propre sur k, on en déduit que toute application rationnelle de X dans Y est régulière. Soit en effet $U \subset X$ un ouvert Zariski et $f : U \to Y$ qu'on veut étendre sur X. Soit $P \in X - U$. L'anneau local $\mathcal{O}_{X,P}$ est un anneau de valuation discrète car X est une courbe lisse. Son corps des fractions

est $k(\eta_X)$. Comme Y est propre sur k, le $k(\eta_X)$-point $f(\eta_X)$ de Y s'étend en un morphisme $\mathrm{Spec}(\mathcal{O}_{X,P}) \to Y$. Ce morphisme se recolle avec f sur U pour donner $f : U \cup \{P\} \to X$ régulière. On fait ensuite varier P dans $X - U$.

Exercice 10. — Construire X, Y et une application rationnelle de X dans Y qui ne s'étend pas en un application régulière de X dans Y dans les cas suivants :

i. Y n'est pas propre.

ii. X est une courbe singulière.

iii. X est lisse de dimension ≥ 2.

2.1.3. Répartitions. — Soit X une courbe algébrique sur k de point générique η, de corps des fractions $k(\eta)$ et de points fermés $|X|$. On note R l'ensemble des collections $(r_P)_{P\in|X|}$ telles que $r_P \in k(\eta)$ pour tout $P \in |X|$ et telles que $r_P \in \mathcal{O}_{X,P}$ pour tout $|X|$ sauf peut-être un nombre fini.

Remarque 2.1.7. — Ainsi R est le produit restreint des $k(\eta) = \mathrm{Frac}(\mathcal{O}_{X,P})$ pour $P \in |X|$ relativement aux sous-anneaux $\mathcal{O}_{X,P}$. On peut voir R comme les collections de germes de fonctions rationnelles en tout $P \in |X|$, ces germes étant presque tous réguliers mais sans aucune de recollement imposée lorsque P varie.

Remarque 2.1.8. — On pourrait introduire un analogue $\hat{R}$ de R faisant intervenir les complétés des anneaux de valuation discrète $\mathcal{O}_{X,P}$ et leur corps des fractions. On alors un analogue direct des adèles des corps de nombres (les places infinies en moins). Les résultats suivants seront toujours valables pour $\hat{R}$ avec la même démonstration.

On dispose d'une injection diagonale $k(\eta) \hookrightarrow R$ qui envoie $f \in k(\eta)$ sur la collection $(f)_{P\in|X|}$. L'image de cette injection consiste en les collections de germes de fonctions rationnelles qui se recollent lorsque P varie. Il est clair que R est un anneau et que $k(\eta) \hookrightarrow R$ est un morphisme d'anneaux.

Soit $D = \sum_{P\in|X|} n_P \cdot (P) \in \mathrm{Div}(X)$ avec $n_P = 0$ pour presque tout $P \in |X|$. On note $R(D)$ le sous-ensemble de R formé des collections $(r_P)_{P\in|X|}$ telles que la valuation en P de r_P est $\geq -n_P$ pour tout $P \in |X|$. On dispose donc d'un diagramme commutatif

$$\begin{array}{ccc} H^0(X, \mathcal{O}_X(D)) & \longrightarrow & R(D) \\ \downarrow & & \downarrow \\ k(\eta) & \longrightarrow & R \end{array}$$

Ce diagramme est de plus cartésien dans le sens où

$$H^0(X, \mathcal{O}_X(D)) \;=\; R(D) \cap_R k(\eta)\,.$$

On voit déjà que répartitions et fonctions rationnelles servent à exprimer le H^0 cohérent. On va voir qu'il en est de même pour le H^1.

Commencer par faisceautiser les anneaux R, $R(D)$ et $k(\eta)$. On note $\underline{k(\eta)}$ le faisceau constant défini sur X muni de sa topologie de Zariski tel que

$$H^0(U, \underline{k(\eta)}) \ = \ k(\eta)$$

pour tout ouvert $U \subset X$. On note $\underline{R}$ le faisceau défini par

$$H^0(U, \underline{R}) \ = \ \prod_{P \in |U|}{}' \ k(\eta)$$

où $\prod'$ désigne un produit restreint. De même on définit le sous-faisceau $\underline{R}(D) \subset \underline{R}$ dont la valeur sur $U \subset X$ est l'ensemble des $(r_P)_{P \in |U|}$ tels que la valuation en P de r_P est $\geq -n_P$ pour tout $P \in |U|$.

Définition 2.2. — Soit X un espace topologique et $\mathcal{F}$ un faisceau sur X. On dit que $\mathcal{F}$ est flasque si pour tout ouvert $U \subset X$ la restriction induit une surjection $H^0(X, \mathcal{F}) \to H^0(U, \mathcal{F})$.

Remarque 2.2.1. — Les faisceaux $\mathcal{O}_X$ ou $\mathcal{O}_X(D)$ ne sont pas du tout flasques : il y a beaucoup plus de fonctions régulières sur un ouvert U que sur tout X car on n'autorise n'importe quel pôles sur $X - U$. Dans ce cas l'application de restriction $H^0(X, \mathcal{O}_X(D)) \to H^0(U, \mathcal{O}_X(D))$ est injective par l'analogue algébrique de l'unicité du prolongement analytique.

La théorie générale de la cohomologie montre que si $\mathcal{F}$ est flasque sur X alors $H^i(X, \mathcal{F}) = 0$ pour tout $i > 0$. Ainsi résoudre un faisceau par des faisceaux flasques permettra de calculer son H^i en terme de H^0 de faisceaux flasques.

Lemme 2.2.2. — *Les faisceaux $\underline{k(\eta)}$, $\underline{R}$ et $\underline{R}(D)$ sont flasques.*

Démonstration. — Conséquence immédiate de la définition. □

Lemme 2.2.3. — *On a une suite exacte courte de faisceaux $0 \to \mathcal{O}_X(D) \to \underline{k}(\eta) \oplus \underline{R} \to \underline{R} \to 0$ dans laquelle le morphisme $\underline{k}(\eta) \oplus \underline{R} \to \underline{R}$ envoie $f \oplus g$ sur $f - g$.*

Démonstration. — Il s'agit de remarquer que pour tout ouvert $U \subset X$ on a $H^0(U, \mathcal{O}_X(D)) = \underline{R}(D)(U) \cap_{\underline{R}(U)} k(\eta)$. □

Proposition 2.2.4. — *On a des isomorphismes canoniques*

$$H^0(X, \mathcal{O}_X(D)) = R(D) \cap_R k(\eta)$$

et

$$H^1(X, \mathcal{O}_X(D)) = R/(k(\eta) + R(D)) .$$

Démonstration. — On a déjà prouvé le cas de H^0. Utilisons la suite longue de cohomologie déduite de la suite exacte courte du lemme 2.2.3, ainsi que l'annulation de la cohomologie supérieure des faisceaux flasques. On trouve la suite exacte longue

$$0 \to H^0(X, \mathcal{O}_X(D)) \to R(D) \oplus k(\eta) \to R \to H^1(X, \mathcal{O}_X(D) \to 0$$

d'où le résultat. □

Remarque 2.2.5. — On a en fait prouvé plus : tout d'abord on a prouvé que $H^i(X, \mathcal{O}_X) = 0$ si $i > 1$. Ensuite, si on accepte le langage et les notations des catégories dérivées, on a construit un quasi-isomorphisme canonique entre le complexe de cohomologie $R\Gamma(X, \mathcal{O}_X(D))$ et le complexe $[R(D) \oplus k(\eta) \to R]$ concentré en degrés 0 et 1.

Remarque 2.2.6. — Comme nous l'avons déjà indiqué le lecteur remarquera que l'énoncé correspondant reste vrai avec les répartitions complétées $\hat{R}$ et $\hat{R}(D)$, c'est à dire les adèles de X. Il reste aussi vrai dans le cas multiplicatif, où les adèles deviennent les idèles. On trouve

$$\mathrm{Pic}(X) \;=\; H^1(X, \mathcal{O}_X^*) \;=\; R^*/(k(\eta)^* \cdot R(D)^*) \;=\; \hat{R}^*/(k(\eta)^* \cdot \hat{R}(D)^*) .$$

On retrouve la formule idélique du groupe de classe vue en cours de théorie des nombres.

On note désormais $I(D) = H^1(X, \mathcal{O}_X(D)) = R/(R(D)+k(\eta))$. On définit $J(D) = I(D)^\vee$ comme l'ensemble des formes k-linéaires sur le k-espace vectoriel de dimension finie $I(D)$. Si $D \leq D'$ (*ie* si $D' - D$ est un diviseur effectif) on a une inclusion $R(D) \subset R(D')$, une surjection $I(D) \to I(D')$ et une injection $J(D') \subset J(D)$. On note alors

$$J \;=\; \bigcup_{D \in \mathrm{Div}(X)} J(D)$$

qui est l'ensemble des formes linéaires $R \to k$ nulles sur $k(\eta)$ et sur un $R(D)$, pour D dépendant de la forme.

Proposition 2.2.7. — *L'ensemble J est naturellement un $k(\eta)$-espace vectoriel. Sa dimension est ≤ 1.*

Démonstration. — Soit $\alpha \in J$ et $f \in k(\eta)$. On veut définir $f \cdot \alpha \in J$. On pose pour cela $(f \cdot \alpha)((r_P)_P) = \alpha((f \cdot r_P)_P)$. On remarque que si α est nulle sur $R(D)$ et si Δ est le diviseur de f alors $f \cdot \alpha$ est nul sur $R(D - \Delta)$.

Montrons que la dimension de J sur $k(\eta)$ est ≤ 1. Par contraposée supposons qu'il existe $\alpha,\ \beta \in J$ linéairement indépendantes sur $k(\eta)$. Soit $D \in \mathrm{Div}(X)$ tel que $\alpha, \beta \in J(D)$. Soit $D_n \in \mathrm{Div}(X)$ n'importe quel diviseur de degré n avec $n \in \mathbb{N}$ un entier que nous

fixerons plus tard. Soit $f \in H^0(X, \mathcal{O}_X(D_n))$. On a alors $f \cdot \alpha \in J(D - D_n)$. Ainsi le morphisme

$$H^0(X, \mathcal{O}_X(D_n))^{\oplus 2} \to J(D - D_n) \ , \ (f, g) \mapsto f \cdot \alpha + g \cdot \beta$$

est injectif par indépendance linéaire de α et β. Mais $J(D-D_n) = H^1(X, \mathcal{O}_X(D-D_n))^\vee$ par la proposition 2.2.4. Ainsi la dimension sur k de $J(D-D_n)$ est égale à $h^0(D-D_n)-\deg(D-D_n)-\chi(X)$ par la partie facile de Riemann-Roch contenue dans le théorème 1.1.4. Bref cette dimension est n plus une constante. Par contre la dimension de $H^0(X, \mathcal{O}_X(D_n))^{\oplus 2}$ est $\geq 2n$ plus une constante toujours par le théorème 2.2.4. On obtient une contradiction lorsque $n \to 0$. □

2.2.1. Dualité de Serre. — Soit X une courbe projective lisse sur k. On dispose sur X du faisceau localement libre de rang un $\Omega^1_{X/k}$ des formes différentielles régulières. On note $\Omega^1_{X/k}(D) = \Omega^1_{X/k} \otimes_{\mathcal{O}_X} \mathcal{O}_X(D)$ que l'on peut interpréter comme le faisceau des formes différentielles rationnelles avec pôles contrôlés par D. On note

$$M = \bigcup_{D \in \mathrm{Div}(X)} H^0(X, \Omega^1_{X/k}(D)) = H^0(\mathrm{Spec}(k(\eta)), \Omega^1_{X/k})$$

qui est l'ensemble des formes différentielles rationnelles sur X. C'est un $k(\eta)$-espace vectoriel de dimension un. On *admet* par analogie avec les surfaces de Riemann qu'il existe pour tout $P \in |X|$ une forme linéaire canonique $\mathrm{res}_P : M \to k(P)$ qui associe à une forme rationnelle son résidu en P. Ici $k(P)$ est le corps résiduel de P ; c'est donc une extension finie de k.

Remarque 2.2.8. — Soit z_P une coordonnée locale en P, donc une fonction définie sur un voisinage ouvert U de P s'annulant à l'ordre un en P, ou bien encore un générateur de l'idéal $\mathfrak{m}_P$. On dispose de sa différentielle $dz_P \in H^0(U, \Omega^1_{X/k})$. L'idée est alors de poser

$$\mathrm{res}_P\left(\lambda \cdot \frac{dz_P}{z_P}\right) = \lambda \, .$$

Il reste à voir que cette définition ne dépend pas du choix de z_P et cela n'est pas facile, surtout en caractéristique positive. Sur $\mathbb{C}$ l'indépendance du choix de z_P résulte du théorème des résidus qui écrit ce terme comme une intégrale curviligne ne dépendant que de la forme différentielle.

Remarque 2.2.9. — Contrairement à ce qu'on pourrait croire, une fonction rationnelle n'a pas de résidu bien défini. En effet poser $\mathrm{res}_P(\lambda/z_P) = \lambda$ dépend complètement du choix de z_P : si on pose $t_P = 2 \cdot z_P$ qui reste un paramètre local en P, le résidu est multiplié par 2 !

Dans le cas des surfaces de Riemann, les exemples $X = \mathbb{C}$, $X = \mathbb{C}/\Lambda$ ou X un ouvert de $\mathbb{C}$ sont trompeurs car si z est la coordonnée de $\mathbb{C}$, le paramètre local $z_P = z - P$ est

un choix canonique pour tout $P \in X$. En fait il serait plus canonique de parler dans ces cas du résidu de la forme différentielle méromorphe $f(z) \cdot dz$ plutôt que celui de la fonction méromorphe $f(z)$ qui dépend du choix de z.

Remarque 2.2.10. — Si k est de caractéristique 0, on peut prouver que res_P est bien défini en utilisant le cas complexe. Il s'agit de l'application suivante du *principe de Lefschetz*. Soit X une courbe projective lisse sur k. Elle est définie par l'annulation d'un nombre fini de polynômes, qui ont chacun un nombre fini de coefficients dans k. Ainsi X est en fait définie sur un sous-corps $k' \subset k$ qui est de degré de transcendance fini sur $\mathbb{Q}$. De plus on peut supposer notre forme méromorphe ω aussi définie sur k'. De même pour les coordonnées locales z_P et z'_P. Mais on peut alors plonger k' dans $\mathbb{C}$. Or il est clair que le résidu est invariant par extension du corps de base. Il suffit bien de prouver $\mathrm{res}_P(\omega) = \mathrm{res}'_P(\omega)$ sur $\mathbb{C}$, où res_P est défini avec la coordonnée locale z_P et res'_P avec z'_P.

Proposition 2.2.11. — *Pour tout $\omega \in M$ on a $\sum_{P\in|X|} \mathrm{tr}_P(\mathrm{res}_P(\omega)) = 0$ où $\mathrm{tr}_P : k(P) \to k$ est la trace de l'extension finie $k(P)/k$.*

Remarque 2.2.12. — Sans prendre la trace, on ne serait pas capable de sommer les expressions $\mathrm{res}_P(\omega)$ qui vivent dans des extensions différentes de k !

Remarque 2.2.13. — Là aussi si k est de caractéristique nulle, le principe de Lefschetz permet de prouver la proposition par réduction au cas complexe.

On définit un accouplement $\langle \cdot, \cdot \rangle : M \otimes_k R \to k$ en posant

$$\langle \omega, (r_P)_P \rangle \ = \ \sum_{P\in|X|} \mathrm{res}_P(r_P \cdot \omega) \, .$$

Cette somme est finie car ω n'a qu'un nombre fini de pôles et r_P est régulier en P pour presque tout P.

Lemme 2.2.14. — *On a $\langle \omega, f \rangle = 0$ pour tout $f \in k(\eta) \subset R$ et $\omega \in M$. On a $\langle \omega, r \rangle = 0$ pour tout $r \in R(D)$ et $\omega \in H^0(X, \Omega^1_{X/k}(-D))$. Enfin $\langle \cdot, \cdot \rangle$ est $k(\eta)$-linéaire.*

Démonstration. — Le premier point est la proposition 2.2.11. Le second résulte du fait que $r_P \cdot \omega$ est régulière en P si $r \in R(D)$ et $\omega \in H^0(X, \Omega^1_{X/k}(-D))$. Le troisième point résulte de l'égalité $\langle f \cdot \omega, r \rangle = \langle \omega, f \cdot r \rangle = \sum_P \mathrm{res}_P(f \cdot r_P \cdot \omega)$ pour tout $f \in k(\eta)$. □

On obtient donc pour tout $\omega \in H^0(X, \Omega^1_{X/k}(-D))$ une forme linéaire $\langle \omega, \cdot \rangle : R/(R(D) + k(\eta)) \to k$. Cela fournit une application canonique

$$\theta : H^0(X, \Omega^1_{X/k}(-D)) \to J(D) = I(D)^\vee = (R/(R(D) + k(\eta))^\vee = H^1(X, \mathcal{O}_X(D))^\vee \, .$$

Lemme 2.2.15. — *Soit $\omega \in M$ tel que $\theta(\omega) \in J(D)$. Alors $\omega \in H^0(X, \Omega^1_{X/k}(-D))$.*

Démonstration. — Il s'agit de voir que si $\sum_P \mathrm{res}_P(r_P \cdot \omega)$ pour tout $(r_P)_P$ avec pôles $\geq -D$ alors ω a un diviseur $\geq D$. C'est clair en fixant d'abord P puis en posant $r_Q = 0$ si $Q \neq P$ et en prenant pour r_P une puissance adéquate d'un paramètre local en P. □

***Théorème 2.2.16* (Dualité de Serre).** — *L'application θ induit un isomorphisme canonique $H^0(X, \Omega^1_{X/k}(-D)) = H^1(X, \mathcal{O}_X(D))^\vee$.*

Démonstration. — On montre d'abord que θ induit un isomorphisme $M \xrightarrow{\sim} J$. Mais l'application $\theta : M \to J$ est injective car si $\theta(\omega) = 0$ on a $\theta \in H^0(X, \Omega^1_{X/k}(-\Delta))$ par le lemme 2.2.15 pour tout $\Delta \in \mathrm{Div}(X)$. On a donc $\omega = 0$.

L'application $\theta : M \to J$ est surjective car c'est une application $k(\eta)$-linéaire injective, car $\dim_{k(\eta)}(J) \leq 1$ par la proposition 2.2.7 et car $M \neq 0$ (en fait on a dit avant que $\dim_{k(\eta)}(M) = 1$ mais on reprouve cela).

On applique alors le lemme 2.2.15 pour vérifier que θ induit bien un isomorphisme $H^0(X, \Omega^1_{X/k}(-D)) = H^1(X, \mathcal{O}_X(D))^\vee$. □

Remarque 2.2.17. — En particulier on obtient un isomorphisme canonique $H^1(X, \Omega^1_{X/k}) = H^0(X, \mathcal{O}_X)^\vee = k^\vee = k$. C'est seulement ici qu'on utilise la connexité de X.

Exercice 11. — Donner une formule explicite pour l'isomorphisme $H^1(X, \Omega^1_{X/k}) = k$.

2.3. Équation

Soit k un corps. Nous allons définir et étudier les courbes elliptiques sur k en copiant le cas complexe déjà traité. Ceci est légitime car le théorème de Riemann-Roch est vrai sur k, comme nous venons de le voir. Bien sûr nous n'utiliserons que les preuves algébriques et pas celles reposant sur l'analyse complexe, les formes modulaires ou les fonctions elliptiques.

Définition 2.3.1. — Une courbe elliptique sur k est une courbe projective lisse connexe de genre un munie d'un point $0_E \in E(k)$.

Remarque 2.3.2. — On dit que 0_E est rationnel sur k. Cela veut dire que son corps résiduel est égal à k et pas juste à une extension de degré fini de k. On se reportera à la discussion du paragraphe 2.4 pour plus de détails. Toute courbe projective lisse de genre un sur k n'admet pas nécessairement de point rationnel. On rencontre de tels contre-exemples dans l'étude de la cohomologie galoisienne des courbes elliptiques *via* les groupes de Selmer ou de Tate-Shafarevitch.

Proposition 2.3.3. — *Soit E la courbe de $\mathbb{P}^2_k$ définie par l'annulation de $ZY^2 - 4X^3 + aXZ^2 + bZ^3$ avec $\Delta = a^3 - 27b^2 \neq 0$. Alors E est une courbe elliptique lorsqu'on la muni du point $0_E = [0; 1; 0]$.*

Il nous reste à prouver la réciproque. Dans le cas complexe, nous avions utilisé l'uniformisation de E par $\mathbb{C}/\Lambda$ et l'équation entre $\wp_\Lambda$ et $\wp'_\Lambda$. Nous allons ici raisonner en deux temps selon que la caractéristique de k est $2, 3$ ou pas.

Théorème 2.3.4. — *Soit E une courbe elliptique sur k de neutre 0_E. Il existe $x, y \in k(\eta_E)$ régulières sur $U \subset E$ tels que la fonction $U \to \mathbb{P}^2_k$, $P \mapsto [x(P); y(P); 1]$ s'étende en un plongement $E \hookrightarrow \mathbb{P}^2_k$ qui envoie 0_E sur $[0; 1; 0]$ et et qui réalise un isomorphisme entre E et la courbe projective C d'équation de Weierstrass*

$$Y^2 \cdot Z + a_1 \cdot X \cdot Y \cdot Z + a_3 \cdot Y \cdot Z^2 = X^3 + a_2 \cdot X^2 \cdot Z + a_4 \cdot X \cdot Z^2 + a_6 \cdot Z^3$$

avec $a_i \in k$ pour $1 \leq i \leq 6$.

Démonstration. — D'après le théorème de Riemann-Roch et la dualité de Serre, on a $h^0(n \cdot (0_E)) = n$ pour tout $n \geq 1$. De plus les constantes k sont dans $H^0(X, \mathcal{O}_X(n \cdot (0_E)))$ pour tout $n \geq 1$. On en déduit qu'il existe $x, y \in k(\eta_E)$ tel que $1, x$ forme une base de $H^0(X, \mathcal{O}_X(2 \cdot (0_E)))$ et $1, x, y$ forme une base de $H^0(X, \mathcal{O}_X(3 \cdot (0_E)))$. On voit aussi que l'ordre de x en 0_E est exactement 2 et celui de y exactement 3.

Puis $H^0(X, \mathcal{O}_X(6 \cdot (0_E)))$ est de dimension 6 et contient les 7 fonctions $1, x, y, x^2, xy, y^2, x^3$. Il existe donc une relation linéaire

$$A_1 + A_2 \cdot x + A_3 \cdot y + A_4 \cdot x^2 + A_5 \cdot xy + A_6 \cdot y^2 + A_7 \cdot x^3 = 0\,.$$

On a nécessairement $A_6 \neq 0$ et $A_7 \neq 0$ car sinon tous les termes de l'équation précédente auraient un pôle d'ordre différent en 0_E, ce qui forcerait chaque terme à être nul. Il suffit alors d'effectuer le changement de variable $x' = -A_6 \cdot A_7 \cdot x$ et $y' = A_6 \cdot A_7^2 \cdot y$, de diviser par $A_6^3 \cdot A_7^4$ et de passer à l'équation homogène associée pour obtenir $\varphi : E \to C$. On a bien $\varphi(0_E) = [0; 1; 0]$ car y a un pôle d'orde supérieur à celui de x en 0_E.

Il faut ensuite prouver que φ est injective donc est une application de degré un entre courbes. Comme $\deg(\varphi)$ est aussi le degré de l'extension de corps $k(\eta_C) \subset k(\eta_E)$ et que $k(\eta_C) = k(x, y)$ est le corps engendré par x et y avec la relation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, on veut prouver que $k(\eta_E) = k(x, y)$. Considérons l'application $\psi : E \to \mathbb{P}^1_k$, $P \mapsto [x(P); 1]$. Comme le seul pôle de x est en 0_E et est double on a $\psi^{-1}(\infty) = 2 \cdot (0_E)$ et on voit d'après la démonstration de la proposition 2.1.5 que ψ est de degré 2. Comme $k(\eta_{\mathbb{P}^1_k}) = k(x)$ on voit que $[k(\eta_E) : k(x)] = 2$. De même $[k(\eta_E) : k(y)] = 3$ en considérant $E \to \mathbb{P}^1_k$, $P \mapsto [y(P), 1]$. Donc $[k(\eta_E) : k(x, y)]$ divise 2 et 3 donc est égal à un.

Il reste à prouver que C est lisse. Supposons par contraposée que C est singulière. Quitte à changer de variable on suppose que $[0; 0; 1]$ est singulier. Un calcul explicite montre alors que $C \to \mathbb{P}^1_k$, $P \mapsto [x(P), y(P)]$ est de degré 1. Par composition avec φ on en déduit $E \to \mathbb{P}^1_k$ de degré un. Mais cela est incompatible avec la formule de Hurwitz et le fait que E est de

genre 1. Finalement $\varphi : E \to C$ est un morphisme de degré un entre courbes projectives lisses donc est un isomorphisme. □

Remarque 2.3.5. — On a utilisé qu'un morphisme $\varphi : E \to C$ de degré un entre courbes projectives lisses est un isomorphisme. On peut voir cela de la même manière qu'avec les surfaces de Riemann, en introduisant un paramètre local z_C et en vérifiant que $\varphi^*(z_C)$ reste un paramètre local sur E. Une autre manière d'expliquer cela est d'utiliser l'égalité $k(\eta_E) = k(\eta_C)$ et le fait qu'une courbe projective lisse sur k est complètement caractérisée par son corps des fractions car ses points fermés correspondent aux valuations sur $k(\eta)$ triviales sur k (point de vue de Zariski sur la géométrie algébrique).

Exercice 12. — Construire un morphisme entre courbes qui est ramifié en chaque point.

Exercice 13. — Construire un morphisme bijectif entre courbes, donc de degré un, qui n'est pas un isomorphisme.

Remarque 2.3.6. — On a en particulier prouvé que $k(\eta_E) = k(x, y)$. Le lecteur fera le lien avec un exercice du TD1 dans lequel on prouvait que $k(\mathbb{C}/\Lambda) = k(\wp_\Lambda, \wp'_\Lambda)$.

Proposition 2.3.7. — *Supposons que k est de caractéristique $\neq 2, 3$. La courbe C du théorème 2.3.4 (et donc aussi la courbe E qui lui est isomorphe) peut s'obtenir comme lieu d'annulation de $ZY^2 - 4X^3 + aXZ^2 + bZ^3$ avec $\Delta = a^3 - 27b^2 \neq 0$.*

Démonstration. — Il suffit d'effectuer successivement les changements de variables $Y \mapsto \frac{1}{2}(Y - a_1X - a_3Z)$ pour obtenir l'équation $Y^2Z = 4X^3 + b_2X^2Z + 2b_4XZ^2 + b_6Z^3$ puis $X \mapsto \frac{1}{3}(X - 3b_2 \cdot Z)$ pour conclure. □

Si la caractéristique de k est $\neq 2, 3$, tout marche comme sur les complexe. Ainsi les courbes E et E' d'équations $Y^2Z = 4X^3 - aXZ^2 - bZ^3$ et $Y^2Z = 4X^3 - a'XZ^2 - b'Z^3$ sont isomorphes sur k si et seulement s'il existe $c \in k^*$ tel que $a' = c^4a$ et $b' = c^6b$. Si l'on pose $j(E) = 1728a^3/\Delta = 1728a^3/(a^3 - 27b^2)$ on voit que $j(E) = j(E')$ si E et E' sont isomorphes sur k.

Lemme 2.3.8. — *Soit $\bar{k}$ une clôture algébrique de k. Les courbes elliptiques E et E' sur k sont isomorphes sur $\bar{k}$ si et seulement si $j(E) = j(E')$.*

Démonstration. — En introduisant les coefficients a, b de l'équation de E et a', b' de E' on se rend compte que $j(E) = j(E')$ implique que $b^2/a^3 = b'^2/a'^3$ donc qu'il existe $c \in \bar{k}^*$ tel que $a' = c^4a$ et $b' = c^6b$. □

Remarque 2.3.9. — Nous n'avons pas dit que E et E' sont isomorphes sur k ! Comme $c^4 = a'/a$ et $c^6 = b'/b$ on voit que E et E' deviennent isomorphes (si $j(E) = j(E')$) sur

une extension de degré ≤ 24 de k contenant une racine 4-ième de a'/a et une racine 6-ième de b'/b.

Exemple 2.3.10. — Lorsque $D \in k^*$, les courbes d'équations (affines) $y^2 = 4x^3 - ax - b$ et $Dy^2 = 4x^3 - ax - b$ deviennent isomorphes sur $k(\sqrt{D})$.

Exemple 2.3.11. — Si $2a \neq 0$ et $D \in k^*$, les courbes d'équations (affines) $y^2 = x^3 + ax$ et $y^2 = x^3 + Dax$ deviennent isomorphes sur $k(\sqrt[4]{D})$.

Exemple 2.3.12. — Si $6b \neq 0$ et $D \in k^*$, les courbes d'équations (affines) $y^2 = x^3 + b$ et $y^2 = x^3 + Db$ deviennent isomorphes sur $k(\sqrt[6]{D})$.

Exercice 14. — Soit k un corps de caractéristique $\neq 2, 3$, soit l/k une extension et soit E, E' deux courbes elliptiques sur k telles que $E_l \simeq E'_l$. Montrer que la paire (E, E') est isomorphe sur k à la paire de courbes elliptiques décrite dans un des trois exemples précédents.

Lemme 2.3.13. — *Pour tout $j \in k$ il existe une courbe elliptique E sur k telle que $j(E) = j$.*

Remarque 2.3.14. — Si k est de caractéristique 2 ou 3, on doit utiliser les équations de Weierstrass plus générales données dans le théorème 2.3.4. On peut toujours caractériser lorsque deux courbes définies par de telles équations sont isomorphes sur $\bar{k}$ et on peut aussi définir explicitemment le j-invariant. Pour plus de détails, voir **[Si**, III.1]. En vérité le cas de caractéristique 2 et 3 n'est plus compliqué que parce qu'on utilise les équations. Avec plus de géométrie algébrique (voir par exemple 2.4.6) il n'y aurait aucune différence en petite caractéristique.

2.4. Loi de groupes

Une précision de notation : $\mathbb{P}^1_k$ et $\mathbb{P}^2_k$ sont des schémas sur $\mathrm{Spec}(k)$, donc des espaces topologiques avec la topologie de Zariski munis d'un faisceau d'anneau et qui sont localement de la forme $\mathrm{Spec}(k[x])$ et $\mathrm{Spec}(k[x, y])$. Il s'agit donc d'objets un peu abstraits, mais naturels du point de vue de la géométrie algébrique. Nous noterons par opposition $\mathbb{P}^1(k) = (k^2 - \{0\})/k^*$ et $\mathbb{P}^2(k) = (k^3 - \{0\})/k^*$ qui sont juste des ensembles. Par exemple $\mathbb{P}^1_k$ est l'ensemble des coordonnées homogènes $[X; Y]$ avec $X, Y \in k$. Les ensembles $\mathbb{P}^1(k)$ et $\mathbb{P}^1(k)$ ne sont pas munis d'une topologie ni d'un faisceau d'anneau. Même s'ils sont concrets, ils ne sont donc pas « géométriques ».

Il y a en fait un plongement naturel $\mathbb{P}^1(k) \subset \mathbb{P}^1_k$ dont l'image consiste en des points fermés. On a donc une inclusion $\mathbb{P}^1(k) \subset |\mathbb{P}^1_k|$ et son image est exactement l'ensemble des $P \in |\mathbb{P}^1_k|$ tels que $k(P) = k$. On dit que $\mathbb{P}^1(k)$ est l'ensemble des k-points de $\mathbb{P}^1_k$, ou encore l'ensemble de ses points rationnels sur k. De même pour $\mathbb{P}^2_k$.

Remarque 2.4.1. — Ainsi si k est algébriquement clos on a $\mathbb{P}^1(k) = |\mathbb{P}^1_k|$ et de même pour $\mathbb{P}^2_k$. À la considération des points génériques près, l'ensemble $\mathbb{P}^1(k)$ et le schéma $\mathbb{P}^1_k$ sont identifiés. Tous les problèmes psychologiques disparaissent ! C'est le point de vue qui prévalait dans la définition des surfaces de Riemann : on travaille avec l'ensemble des solutions sur $\mathbb{C}$ d'équations holomorphes et cet ensemble est muni d'une topologie et d'un faisceau de fonctions holomorphes.

Malheureusement tous les corps intéressants ne sont pas algébriquement clos : ne serait-ce si l'on veut faire de la cryptographie, on est amené à considérer $k = \mathbb{F}_p$. L'ensemble $\mathbb{P}^1(\mathbb{F}_p)$ est un ensemble fini de cardinal $p+1$, qui ne peut pas avoir d'autre topologie que la topologie discrète. Il est donc non connexe. Par opposition $\mathbb{P}^1_{\mathbb{F}_p}$ est un ensemble infini muni d'un topologie intéressante pour laquelle il est connexe. Regarder l'inclusion $\mathbb{P}^1(\mathbb{F}_p) \subset \mathbb{P}^1_{\mathbb{F}_p}$ permet en quelque sorte d'épaissir l'ensemble fini $\mathbb{P}^1(\mathbb{F}_p)$ en l'espace topologique connexe $\mathbb{P}^1_{\mathbb{F}_p}$.

On notera $E(k)$ l'ensemble des $P \in |E|$ tels que $k(P) = k$. C'est aussi l'ensemble des solutions concrètes $[X;Y;Z] \in \mathbb{P}^2(k)$ de l'équation cubique qui définit E. C'est enfin l'ensemble des morphismes de schémas $\mathrm{Spec}(k) \to E$ qui sont des sections du morphisme structural $E \to \mathrm{Spec}(k)$. On appelle $E(k)$ l'ensemble des points rationnels de E sur k ou l'ensemble des k-points de E. Pour tout $P \in E(k)$ on a $\deg(P) = 1$. Par définition, on a $0_E \in E(k)$.

Théorème 2.4.2. — *L'application d'Abel-Jacobi* $\alpha : E(k) \to \mathrm{Pic}^0(E)$, $x \mapsto (x) - (0_E)$ *est une bijection. En particulier l'ensemble* $E(k)$ *est muni d'une loi de groupe abélien de neutre* 0_E.

Démonstration. — Il suffit de reprendre la démonstration du théorème 1.4.3 puisque le théorème de Riemann-Roch est vrai sur tout corps. Pour rappel, montrons que α est surjective. Si $D \in \mathrm{Div}^0(E)$ on considère un élément non nul $f \in H^0(E, \mathcal{O}_E(D + (0_E)))$, sachant que ce k-espace vectoriel est de dimension un. On a donc $\mathrm{div}(f) \geq -D - (0_E)$ et $\deg(\mathrm{div}(E)) = 0$. Donc f a un unique pôle $P \in |E|$. De plus on a $\deg(P) = 1$ donc $k(P) = k$. On a donc trouvé $P \in E(k)$ tel que $\mathrm{div}(f) = -D + (P) - (0_E)$ d'où $\alpha(P) \sim D$. □

Rien n'empêche que le groupe $E(k)$ soit trivial réduit à $\{0_E\}$. Par contre si k est algébriquement clos, on a $E(k) = |E|$ et $E(k)$ est loin d'être trivial. L'intérêt du théorème précédent est qu'il s'applique non seulement à E sur k mais aussi à toutes les extensions des scalaires qui s'en déduisent : si l/k est une extension de corps, on note E_l la courbe elliptique sur l définie dans $\mathbb{P}^2_l$ par la même équation que E. On obtient alors un morphisme

$$\alpha_l : E_l(l) \to \mathrm{Pic}^0(E_l)$$

et bien sûr $E_l(l) \neq \{0_E\}$ si l est assez grand. On note aussi $E_l(l) = E(l)$ et c'est l'ensemble des morphismes de schémas $\mathrm{Spec}(l) \to E$ dont la composée avec le morphisme structural

$E \to \mathrm{Spec}(k)$ est égale au morphisme $\mathrm{Spec}(l) \to \mathrm{Spec}(k)$ provenant de l'inclusion $k \subset l$. En termes plus simples, c'est l'ensemble des solutions dans $\mathbb{P}^2(l)$ de l'équation cubique. Enfin si l/k est galoisienne (en particulier séparable) on peut identifier le quotient de $E(l)$ par l'action de $\mathrm{Gal}(l/k)$ à l'ensemble des $P \in |E|$ tels que $k \subset k(P) \subset l$. Enfin si k est parfait et que $\bar{k}$ est une clôture algébrique de k, on a des bijections canoniques

$$|E| \;=\; |E_{\bar{k}}|/\mathrm{Gal}(\bar{k}/k) \;=\; E_{\bar{k}}(\bar{k})/\mathrm{Gal}(\bar{k}/k) \;=\; E(\bar{k})/\mathrm{Gal}(\bar{k}/k)$$

ainsi que

$$E(k) \;=\; E(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}$$

où pour tout ensemble M muni d'une action d'un groupe G on note

$$M^G = \{m \in M \mid g \cdot m = m \;\; \forall\, g \in G\}$$

les invariants et $M/G = M/\sim$ le quotient, où $m \sim n$ s'il existe $g \in G$ tel que $m = g \cdot n$. Cette action de $\mathrm{Gal}(\bar{k}/k)$ permet de relier l'ensemble $E(k)$ et les points fermés $|E|$ du schéma E.

Remarque 2.4.3. — Dans le langage des variétés lorsque k est parfait, rappelons qu'un diviseur est un élément $\mathrm{Gal}(\bar{k}/k)$-invariant de $\mathbb{Z}[E(\bar{k})]$. Si l'on écrit la démonstration du théorème 2.4.2 dans ce langage, on trouve alors $P \in E(\bar{k})$ et $f \in k(\eta_E)^*$ tels que $\mathrm{div}(f) = -D+(P)-(0_E)$ et il faut montrer que $P \in E(k)$. On veut donc vérifier que $\sigma(P) = P$ pour tout $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Il suffit pour cela d'écrire $\sigma(f) = f$ et $\sigma(\mathrm{div}(f)) = \mathrm{div}(\sigma(f)) = \mathrm{div}(f)$ puis $\sigma(D) = D$ et $\sigma(0_E) = 0_E$.

Remarque 2.4.4 **(working definition)**. — Pour résumé de la manière la plus simple possible : une courbe elliptique E sur k est la donnée d'une équation cubique lisse $P(X,Y,Z) = 0$ à coefficients dans k. On note ensuite $E(k)$ l'ensemble des solutions $[X,Y,Z] \in (k^3-\{0\})/k^*$ de l'équation $P(X,Y,Z) = 0$. De même pour toute extension de corps l/k on note $E(l)$ l'ensemble des solutions $[X,Y,Z] \in (l^3 - \{0\})/l^*$. Si l/k est galoisienne on a $E(k) = E(l)^{\mathrm{Gal}(l/k)}$. Si l est algébriquement clos, la donnée de $E(l)$ permet de retrouver l'équation P. Si l est quelconque, on peut par contre avoir $E(l) = \{[0;1;0]\}$. Si k est parfait de clôture algébrique $\bar{k}$ on note $|E| = E(\bar{k})/\mathrm{Gal}(\bar{k}/k)$ et on dit que c'est l'ensemble des points fermés de E.

Ce point de vue est concret mais il évite de définir un espace topologique E muni d'un faisceau d'anneau. Sans cela, il sera dur de faire de la géométrie et d'appliquer la cohomologie des faisceaux. Si l'on avance suffisamment en géométrie algébrique, on se rend néanmoins compte que ce point de vue naïf est le bon : c'est la philosophie du foncteur des points d'un schéma et du lemme de Yoneda.

Introduisons le produit fibré $E \times_k E$ de deux copies de E au dessus de $\mathrm{Spec}(k)$. Si $E \subset \mathbb{P}^2_k$ est définie par l'équation $P(X,Y,Z) = 0$, ce produit $E \times_k E$ est tout simplement défini dans $\mathbb{P}^2_k \times_k \mathbb{P}^2_k$ par les deux équations $P(X,Y,Z) = P(X',Y',Z') = 0$. Ici $[X;Y;Z]$ est

la coordonnée homogène sur le premier facteur $\mathbb{P}^2_k$ et $[X';Y';Z']$ la seconde. On a donc clairement

$$|E \times_k E| \;=\; |E| \times |E|$$

où le second membre désigne le produit usuel des ensembles. La subtilité concerne les points génériques : il y a dans $E \times_k E$ beaucoup plus de points génériques que ceux de la forme $\eta_E \times P$, $P \times \eta_E$ ou $\eta_E \times \eta_E$. Cela est relié à l'existence de courbes dans $E \times E$ qui ne sont pas de la forme $E \times \{P\}$ ou $\{P\} \times E$, *ie* qui ne sont pas des axes de coordonnés. Pour ceux qui ne sont pas intéressés par la géométrie algébrique, il suffit de retenir que l'ensemble $E \times_k E$ est plus gros que $E \times E$ mais qu'ils ont même sous-ensemble de points fermés. Le produit ensembliste naïf $E \times E$ n'est pas muni d'une structure de schéma et n'intervient jamais en géométrie algébrique. Rappelons aussi que si k est séparable, on a une identification canonique $(E(\bar{k}) \times E(\bar{k}))/\mathrm{Gal}(\bar{k}/k) = |E \times_k E|$.

Proposition 2.4.5. — *Supposons k séparable. Soit $\bar{k}$ une clôture algébrique de k. L'application d'addition $E(\bar{k}) \times E(\bar{k}) \to E(\bar{k})$ induit une application*

$$|E \times_k E| \;=\; \big(E(\bar{k}) \times E(\bar{k})\big)\,/\mathrm{Gal}(\bar{k}/k) \;\longrightarrow\; |E| \;=\; E(\bar{k})/\mathrm{Gal}(\bar{k}/k)$$

qui s'étend canoniquement en une application algébrique $m_E : E \times_k E \to E$. De même, l'application d'opposé $[-1] : |E| \to |E|$ s'étend canoniquement en une application algébrique $[-1] : E \to E$.

Démonstration. — Grâce au théorème 2.4.2, on a muni $E(\bar{k})$ de la loi de groupe obtenue par image inverse par α de celle de $\mathrm{Pic}^0(E_{\bar{k}})$. On a montré dans la proposition 1.4.10 que cette loi de groupe peut se réinterpréter géométriquement avec les intersections de cordes à E. Or cette loi géométrique est donnée par des résolutions d'équations linéaires donc par des formules rationnelles en les coordonnées homogènes des points de E. La subtilité est que ces fonctions rationnelles peuvent des pôles sur E. Voir **[Si**, th.III.3.6] pour l'argument complet. □

Remarque 2.4.6. — On a donc utilisé la vision géométrique de la loi de groupe (avec les cordes en plusieurs points) pour montrer construire une loi interne algébrique et l'isomorphisme d'Abel-Jacobi pour vérifier que c'est une loi de groupe. On aurait pu en fait utiliser uniquement l'application d'Abel-Jacobi, mais cela demande plus de connaissance en géométrique. Aussi cela permet de voir que l'hypothèse que k soit parfait est superflue. En fait il existe un schéma $\underline{\mathrm{Pic}}^0(E)$ dont les k-points est l'ensemble $\mathrm{Pic}^0(E)$. Mais le schéma $\underline{\mathrm{Pic}}^0(E)$ est naturellement muni d'une structure de schéma en groupes, donc en particulier d'un morphisme d'addition

$$\underline{\mathrm{Pic}}^0(E) \times_k \underline{\mathrm{Pic}}^0(E) \to \underline{\mathrm{Pic}}^0(E)$$

De plus il existe une version schématique $\underline{\alpha} : E \to \underline{\mathrm{Pic}}^0(E)$ de l'application d'Abel-Jacobi qui est toujours un isomorphisme. On en déduit l'existence d'une loi $E \times_k E \to E$.

Remarque 2.4.7. — Comme nous l'avons dit, le théorème 2.4.2 fournit une loi de groupe abélien sur $E(k)$. En particulier si $P, Q \in E(k)$ on a $P + Q \in E(k)$ et pas seulement $P + Q \in E(\bar{k})$. Cela n'est pas tout à fait évident lorsqu'on pense à la loi de groupes en termes géométriques avec les intersections de la droite (PQ) avec le graphe de E. On le prouve à la main en remarquant qu'un polynôme de degré 3 à coefficients dans k et à racines disctintes qui a deux racines dans k a sa troisième racine également dans k.

Remarque 2.4.8. — Nous n'avons jamais dit que $|E \times_k E| = |E| \times |E|$ et c'est d'ailleurs faux dès que k n'est pas algébriquement clos puisque $|E \times_k E| = (E(\bar{k})^2)/\mathrm{Gal}(\bar{k}/k)$ et $|E| \times |E| = (E(\bar{k})^2)/\mathrm{Gal}(\bar{k}/k)^2$. Donc nous n'avons jamais dit qu'il existe une loi de groupe $|E| \times |E| \to |E|$!

Exercice 15. — Soit $\mathbb{A}^1_k = \mathrm{Spec}(k[t])$. On a donc un isomorphisme de schémas $\mathbb{A}^1_k \times_k \mathbb{A}^1_k = \mathrm{Spec}(k[x, y])$. Vérifier qu'on a une loi d'addition qui est un morphisme de schéma $\mathbb{A}^1_k \times_k \mathbb{A}^1_k \to \mathbb{A}^1_k$. Écrire le morphisme correspondant $k[t] \to k[x, y]$ sur les anneaux de fonctions. Vérifier que $|\mathbb{A}^1_k|$ n'est *pas* un groupe si k n'est pas algébriquement clos.

2.5. Morphismes

Soit k un corps et E, E' deux courbes elliptiques sur k de neutres 0_E et $0_{E'}$.

Définition 2.5.1. — Un morphisme de courbes elliptiques de E dans E' est une application régulière $f : E \to E'$ entre courbes algébriques sur k telle que $f(0_E) = 0_{E'}$.

Proposition 2.5.2. — *Soit l/k une extension de corps. Tout morphisme f de courbes elliptiques induit un morphisme de groupes $f(l) : E(l) \to E'(l)$. De plus f rend commutatif le diagramme*

$$\begin{array}{ccc} E \times_k E & \xrightarrow{(f,f)} & E' \times_k E' \\ \downarrow{\scriptstyle m_E} & & \downarrow{\scriptstyle m_{E'}} \\ E & \xrightarrow{\quad f \quad} & E' \end{array}$$

où m_E et $m_{E'}$ sont les lois de groupes de E et de E', ce qu'on peut reformuler en disant que f est un morphisme de schémas en groupes.

Démonstration. — On peut supposer que f est non nul. Dans ce cas c'est un morphisme fini de E dans E'. Il induit donc $f_* : \mathrm{Div}(E) \to \mathrm{Div}(E')$ en posant $f_*(\sum_{P \in |E|} n_P \cdot (P)) = \sum n_P \cdot (f(P))$. Ce morphisme préserve l'annulation du degré et on a donc $f_* : \mathrm{Div}^0(E) \to$

$\mathrm{Div}^0(E')$. Il induit aussi une injection de corps $k(\eta_{E'}) \hookrightarrow k(\eta_E)$ qui réalise $k(\eta_E)$ comme extension de degré finie de $k(\eta_{E'})$. On obtient donc une norme

$$f_* = N_{k(\eta_E)/k(\eta_{E'})} : k(\eta_E)^* \to k(\eta_{E'})^* .$$

Au final on obtient un morphisme $f_* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(E')$. On a alors un diagramme commutatif

$$\begin{array}{ccc} E(k) & \xrightarrow{\alpha_E} & \mathrm{Pic}^0(E) \\ \downarrow{\scriptstyle f(k)} & & \downarrow{\scriptstyle f_*} \\ E'(k) & \xrightarrow{\alpha_{E'}} & \mathrm{Pic}^0(E') \end{array}$$

où les morphismes horizontaux sont des isomorphismes de groupes d'après le théorème 2.4.2. De plus f_* est clairement un morphisme de groupe. On en déduit que $f(k)$ est bien un morphisme de groupes. De même pour toute extension l/k. On en déduit que f est un morphisme de schémas en groupes en considérant les points génériques (voir **[Ne]**). □

Définition 2.5.3. — Soient E et E' des courbes elliptiques sur k. Une isogénie $f : E \to E'$ est un morphisme non nul.

En particulier une isogénie est un morphisme fini et plat entre courbes qui a un degré $\deg(f) \in \mathbb{N}^*$. Un exemple d'isogénie est l'automorphisme $[-1]_E$.

Lemme 2.5.4. — *Soit $n \in \mathbb{Z} - \{0\}$. Alors l'application $[n]_E$ est une isogénie.*

Démonstration. — Il faut voir qu'elle n'est pas constante. C'était évident sur $\mathbb{C}$ et donc en caractéristique 0 par le principe de Lefschetz. Esquissons une preuve en toute caractéristique. On peut supposer $n > 0$ puisque $[-1]_E$ est un automorphisme de E. Si $\mathrm{car}(k) \neq 2$, un calcul explicite sur les équations montre que $E(\bar{k})[2] = \{P \in E(\bar{k}) \mid [2]_E(P) = 0_E\}$ est fini de cardinal 4. Donc $[2]$ n'est pas constant et par récurrence $[2^k]$ n'est pas constant pour tout $k > 0$. Soit $P \neq 0_E \in E(\bar{k})[2]$. Pour tout m impair on a $[m]_E(P) = P$ en utilisant une relation de Bezout, donc $[m]_E(P) \neq 0_E$ et $[m]$ n'est pas constant. Au final $[n]_E = [2^k \cdot m]_E$ n'est pas constant. Si $\mathrm{car}(k) = 2$ on recommence en utilisant $[3]_E$. □

Corollaire 2.5.5. — *Soit k un corps et E une courbe elliptique sur k. On a une injection d'anneau $\mathbb{Z} \to \mathrm{End}_k(E)$, $n \mapsto [n]_E$.*

Remarque 2.5.6. — D'après le principe de Lefschetz, si k est de caractéristique nulle la proposition 1.6.8 et la remarque 1.6.9, on a $\mathbb{Z} = \mathrm{End}_{\bar{k}}(E)$ pour la plupart des E. On verra par opposition dans la remarque 2.5.14 que sur les corps finis on a toujours $\mathbb{Z} \neq \mathrm{End}_{\bar{k}}(E)$.

2.5.1. Exemples d'isogénies. — Donnons quelques exemples explicites avec des équations.

Exemple 2.5.7. — Soit E d'équation affine $y^2 = x^3 + ax + b$ avec $\Delta \neq 0$. D'après la vision géométrique de la loi de groupe on a $[-1](x, y) = (x, -y)$. Sur $\mathbb{C}$, cela est équivalent au fait que $\wp_\Lambda$ est paire et $\wp'_\Lambda$ impaire.

Exemple 2.5.8 **(CM)**. — Soit k de caractéristique $\neq 2$. Notons $i \in \bar{k}$ une racine primitive 4-ème de 1. On a donc $i^2 = -1$. Soit E la courbe elliptique sur k d'équation affine $y^2 = x^3 - x$. L'application $[i] : E \to E$, $(x, y) \mapsto (-x, iy)$ est alors un endomorphisme de $E_{k(i)}$. De plus $[i] \circ [i] = [-1]$ par calcul immédiat. On en déduit un morphisme de $\mathbb{Z}[i]$ dans $\mathrm{End}(E_{k(i)})$. On a aussi $[-i](x, y) = [-1] \circ [i](x, y) = (-x, -iy)$.

On voit déjà dans cet exemple que l'endomorphisme $[i]$ n'est pas défini sur k. Ainsi pour l/k une extension de corps, on a *a priori* une inclusion stricte $\mathrm{End}(E) \subset \mathrm{End}(E_l)$.

Si k est de caractéristique nulle, on a en fait $\mathrm{End}(E_{k(i)}) = \mathbb{Z}[i]$. On est donc dans un cas de multiplication complexe et ici $j(E) = 1728$. Le groupe $\mathrm{Aut}(E_{k(i)})$ est de cardinal 4, égal $\{[\pm 1], [\pm i]\}$.

Remarque 2.5.9. — Si $k = \mathbb{C}$ et E est la courbe elliptique d'équation $y^2 = x^3 - x$ comme dans l'exemple précédent, on vérifie que $E = \mathbb{C}/\Lambda$ avec $\Lambda = \mathbb{Z} + i \cdot \mathbb{Z}$, qui a effectivement multiplication complexe par $\mathbb{Z}[i]$. On a $g_3(\Lambda) = 0$ car $g_3(\Lambda) = g_3(i \cdot \Lambda) = i^6 \cdot g_3(\Lambda) = -g_3(\Lambda)$. Une subtilité est qu'on a pas $g_2(\Lambda) = 4$ ni même $g_2(\Lambda) \in \mathbb{Q}$. Les courbes elliptiques d'équation $y^2 = x^3 - x$ et $y^2 = 4x^3 - g_2(\Lambda)$ sont isomorphes mais pas égales. En fait un théorème de Hurwitz affirme que

$$g_2(\Lambda) \;=\; 64 \cdot \left(\int_0^1 \frac{dt}{\sqrt{1 - t^4}} \right)^4$$

Exemple 2.5.10 **(Isogénie duale)**. — Soit k de caractéristique $\neq 2$. Soient $a, b \in k$ avec $b \neq 0$ et $r = a^2 - 4b \neq 0$. Notons E la courbe d'équation affine $y^2 = x^3 + ax^2 + bx$ et E' celle d'équation affine $y^2 = x^3 - 2ax^2 + rx$. On a alors deux isogénies de degré 2

$$\phi : E \to E', \;\; (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

et

$$\phi' : E' \to E, \;\; (x, y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(r - x^2)}{8x^2} \right)$$

On vérifie par calcul que $\phi' \circ \phi = [2]_E$ et $\phi \circ \phi' = [2]_{E'}$. On en déduit que $\phi' = \hat{\phi}$ est l'isogénie duale de ϕ dans le sens qu'on verra dans le paragraphe **2.5.1.1**. On peut aussi en déduire une expression facile de $[2]_E$. De même on peut trouver par itération $[4]_E$ ou $[2^r]_E$!

Exemple 2.5.11 **(Frobenius)**. — Soit k de caractéristique $p > 0$ et soit $q = p^r$. Soit E une courbe elliptique sur k définie par l'équation affine $y^2 = x^3 + ax + b$. Rappelons que

$k \to k$, $t \mapsto t^q$ est un morphisme d'algèbre fondamental appelé *morphisme de Frobenius* arithmétique relativement à q. On note $E^{(q)}$ la courbe sur k définie par l'équation affine $y^2 = x^3 + a^q x + b^q$. On a alors $\Delta(E^q) = \Delta(E)^q$ et $j(E^q) = j(E)^q$. En particulier $E^{(q)}$ est lisse et est une courbe elliptique munie du point privilégié $0_{E^{(q)}} = [0;1;0] = \phi_q(0_E)$. On définit alors un morphisme

$$\phi_q : E \to E^{(q)}, \quad (x,y) \mapsto (x^q, y^q)$$

appelé morphisme de Frobenius relatif de E (arithmétique, relativement au choix de q). Le cas où $k \subset \mathbb{F}_q$ est spécialement intéressant. En effet on a alors $t^q = t$ pour tout $t \in k$ et donc $E^{(q)} = E$. Dans ce cas $\phi_q \in \mathrm{End}(E)$.

Rappelons qu'une extension de corps L/K est dite séparable si elle est algébrique et que pour tout $x \in L$, son polynôme minimal sur K a une dérivée non nulle. On dit qu'elle est inséparable si elle n'est pas séparable. On dit que L/K est purement inséparable si pour tout $K \subset M \subset L$ tel que M/K soit séparable, on ait $M = K$. On dit que K est parfait s'il n'a pas d'extensions inséparable.

Si K est de caractéristique nulle ou plus généralement de caractéristique première à $[L : K]$ alors L/K est toujours inséparable et K est donc toujours parfait (mais on réserve plutôt cette terminologie à la caractéristique positive). Si $p = \mathrm{car}(K) > 0$ et $q = p^r$ on note K^q le sous-corps de K formé des puissances q-èmes d'éléments de K. L'extension $K^q \subset K$ est alors purement inséparable. Si K est parfait elle est triviale, si $K = \mathbb{F}_p(t)$ elle est de degré q, si $K = \mathbb{F}_p(t_1, t_2)$ elle est de degré q^2. Plus généralement si k est parfait et K/k est purement transcendante de degré de transcendance r, l'extension $K^q \subset K$ est purement inséparable de degré q^r.

Les corps finis sont parfaits mais $\mathbb{F}_p(t)$ n'est pas parfait puisque l'extension $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ est purement inséparable, et elle est isomorphe à l'extension $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ où $\mathbb{F}_p(t^p) = \mathbb{F}_p(t)^p$.

Proposition 2.5.12. — *Soit k un corps parfait de caractéristique $p > 0$ et $q = p^r$. Soit E une courbe elliptique sur k. Le degré du morphisme $\phi_q : E \to E^{(q)}$ défini précédemment est q. L'inclusion de corps $k(\eta_{E^{(q)}}) \subset k(\eta_E)$ déduit de ϕ_q identifie $k(\eta_{E^{(q)}})$ à $k(\eta_E)^q$. L'extension $k(\eta_{E^{(q)}}) \subset k(\eta_E)$ est donc purement inséparable de degré q. Enfin le morphisme $\phi_q : E \to E^{(q)}$ est totalement ramifié en tout point de $E^{(q)}$.*

Démonstration. — On a $k(\eta_E) = k(x,y)$ qui est le corps à deux variables transcendantes où on impose la relation $y^2 = x^3 + ax + b$ si telle est l'équation de E. De même on a $k(\eta_{E^{(q)}}) = k(X,Y)$ si l'équation de $E^{(q)}$ est $Y^2 = X^3 + \alpha X + \beta$. Comme par construction $\phi_q : E \to E^{(q)}$ envoie (x,y) sur $(X,Y) = (x^q, y^q)$ on en déduit que $k(\eta_{E^{(q)}}) = k(x^q, y^q) = k(x,y)^q$ comme k est parfait. On voit donc que l'inclusion $k(\eta_{E^{(q)}}) \subset k(\eta_E)$ est purement inséparable. Comme $k(\eta_E)$ est de degré de transcendance 1 sur k qui est parfait, le degré de l'extension $k(\eta_E)/k(\eta_{E^{(q)}})$ est donc q. Comme $\deg(\phi_q) = [k(\eta_E) : k(\eta_{E^{(q)}})]$ on en déduit que ϕ_q est de degré q. □

Exercice 16. — Soit $P \in E$ de corps résiduel $k(P)$ et d'image $\phi_q(P) \in E^{(q)}$. D'écrire explicitement le morphisme induit au niveau des corps résiduels $k(\phi_q(P)) \to k(P)$. Est-ce un morphisme de k-algèbres ?

Remarque 2.5.13. — La situation est spécialement agréable si $k \subset \mathbb{F}_q$ donc si $u \mapsto u^q$ est l'identité de k. On a alors un isomorphisme canonique $E^{(q)} = E$ puisqu'ils sont définis par la même équation. Ainsi ϕ_q est un endomorphisme de E.

Remarque 2.5.14. — On a montré que si $k = \mathbb{C}$ le degré de $[n]_E$ est n^2. D'après le principe de Lefschetz, cela reste vrai si k est de caractéristique nulle. On verra que c'est en fait vrai en toute caractéristique dans la proposition 2.5.27. En particulier on voit que ϕ_p ou plus généralement ϕ^q avec $q = p^{2r+1}$ n'est pas de la forme $[n]_E$ si $k \subset \mathbb{F}_q$ (cas où ϕ_q est bien un endomorphisme de E). On a donc $\mathrm{End}_k(E) \neq \mathbb{Z}$ si k est fini.

Supposons que $a, b \in \mathbb{Z}_p$. On peut alors définir une courbe elliptique relative $E \to \mathrm{Spec}(\mathbb{Z}_p)$ par l'équation affine $y^2 = x^3 + ax + b$. Elle « met en famille » sur le trait $\mathrm{Spec}(\mathbb{Z}_p)$ la courbe elliptique $E_{\mathbb{F}_p}$ sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + ax + b$ et celle $E_{\mathbb{Q}_p}$ de même équation sur $\mathbb{Q}_p$. On a $\phi_p \in \mathrm{End}_{\mathbb{F}_p}(E_{\mathbb{F}_p})$. D'après le principe de Lefschetz on trouve que $\mathrm{End}_{\mathbb{Q}_p}(E)$ est soit isomorphe à $\mathbb{Z}$ soit à $\mathfrak{a}$ un ordre d'un corps quadratique imaginaire. On en déduit que s'il existe $\varphi \in \mathrm{End}_{\mathbb{Z}_p}(E)$ qui relève ϕ_q alors on a $\mathrm{End}_{\mathbb{Q}_p}(E) = \mathfrak{a}$ et $\mathfrak{a}$ contient un élément de norme p. Si $\mathrm{Frac}(\mathfrak{a}) = \mathbb{Q}(\sqrt{-d})$ l'équation $u^2 - dv^2 = p$ a donc une solution. On trouve que p est inerte dans $\mathbb{Q}(\sqrt{-d})$ donc que d est un carré dans $\mathbb{F}_p$ et le symbole de Legendre (d/p) est égal à 1. Cela fait un premier lien, qui peut être poursuivi, entre l'arithmétique des corps quadratique imaginaires et celle des courbes elliptiques sur les corps finis.

Définition 2.5.15. — Soit k un corps et $\lambda : E \to E'$ une isogénie entre courbes elliptiques sur k. On dit que f est séparable si l'extension $k(\eta_{E'}) \subset k(\eta_E)$ est séparable.

Remarque 2.5.16. — Si k est de caractéristique nulle toute isogénie est séparable. De même si $\deg(\lambda)$ est premier à la caractéristique de k, l'isogénie λ est toujours séparable. Par contre l'isogénie de Frobenius ϕ_q n'est jamais inséparable.

On peut aussi appeler *isogénie étale* une isogénie inséparable. En effet, une isogénie est un morphisme étale de schéma si et seulement si elle est séparable. La notion de morphisme étale joue un rôle clé en géométrie algébrique et elle sert à définir les ouverts étales d'un schéma qui permettent de définir sa cohomologie étale. Un morphisme est étale si le déterminant de sa différentielle est inversible en tout point. En géométrie complexe, le théorème d'inversion locale s'applique alors, et on voit que les morphismes étales sont exactement les isomorphismes locaux. En géométrie algébrique le théorème d'inversion locale n'est pas vraie, et remplacer les ouverts Zariski par les ouverts étales est une manière de forcer ce théorème à devenir vrai.

Proposition 2.5.17. — *Soit k un corps parfait de caractéristique $p > 0$ et $\lambda : E \to E'$ une isogénie. Il existe un unique $q = p^r$ et une unique isogénie séparable $\mu : E^{(q)} \to E'$ tel que $\lambda = \mu \circ \phi_q$. En particulier q divise* $\deg(\lambda)$.

Démonstration. — Considérons l'extension de corps $k(\eta_E)/k(\eta_{E'})$. Soit L la sous-extension séparable maximale. Alors $k(\eta_E)/L$ est purement inséparable donc son degré est de la forme $q = p^r$. On a alors $k(\eta_E)^q \subset L$. Comme $[k(\eta_E) : L] = q = [k(\eta_E) : k(\eta_E)^q]$ on en déduit $L = k(\eta_E)^q$. On obtient donc une inclusion $k(\eta_{E'}) \subset k(\eta_E)^q$ qui induit un morphisme $U \to E'$ avec U un ouvert de $E^{(q)}$. Par propreté ce morphisme s'étend en le morphisme $\lambda : E^{(q)} \to E'$ cherché. L'inclusion $k(\eta_{E'}) \subset k(\eta_E)^q \subset k(\eta_E)$ induit bien la factorisation $\lambda = \mu \circ \phi_q$ sur un ouvert Zariski de E. Par densité des ouverts Zariski, l'égalité $\lambda = \mu \circ \phi_q$ est vraie sur E. Enfin λ est une isogénie par la proposition 2.5.2 car elle est non constante et respecte le neutre. Elle est séparable car elle correspond à l'extension séparable $L/k(\eta_{E'})$. □

Corollaire 2.5.18. — *Soit k un corps parfait de caractéristique $p > 0$ et $\lambda : E \to E'$ une isogénie telle que $k(\eta_E)/k(\eta_{E'})$ est purement inséparable de degré q. Alors il existe un isomorphisme $E' \simeq E^{(q)}$ qui fait se correspondre λ et ϕ_q.*

À isomorphisme près, l'unique isogénie purement inséparable de degré $q = p^r$ est le Frobenius $\phi_q : E \to E^{(q)}$. Étudions à présent son noyau.

Lemme 2.5.19. — *L'isogénie ϕ_q de degré q induit une injection $E(\bar{k}) \hookrightarrow E^{(q)}(\bar{k})$. Son noyau est donc trivial.*

Démonstration. — C'est clair sur la formule $\phi_q(x, y) = (x^q, y^q)$ car l'équation $x^q = 0$ n'a que la solution $x = 0$ dans $\bar{k}$. □

Remarque 2.5.20. — Ainsi l'application $\phi_q : E(\bar{k}) \xrightarrow{\sim} E^{(q)}(\bar{k})$ est une bijection car elle est surjective (c'est vrai pour toute isogénie) et injective. Néanmoins le morphisme algébrique $\phi_q : E \to E^{(q)}$ est loin d'être un isomorphisme car il est de degré q. C'est en fait un revêtement ramifié en tout point avec indice de ramification q.

La même situation arrive déjà pour la droite affine $\mathbb{A}^1_k = \mathrm{Spec}(k[x])$ lorsque k est de caractéristique p et $q = p^r$. On dispose là encore d'un morphisme de Frobenius $\phi_q : \mathbb{A}^1_k \to (\mathbb{A}^1_k)^{(q)} = \mathbb{A}^1_k$ qui envoie x sur x^q. Ce morphisme est surjectif de degré q et n'est pas un isomorphisme. Par contre il induit une bijection $\phi_q : \bar{k} = \mathbb{A}^1_k(\bar{k}) \to \bar{k} = \mathbb{A}^1_k(\bar{k})$.

Remarque 2.5.21. — Le morphisme de Frobenius ϕ_q explique clairement pourquoi il est insuffisant de regarder les solutions dans $\bar{k}$ des équations définissant les variétés algébriques.

Dans le cas de $\mathbb{A}^1_k$, il paraît naturel de définir le noyau de ϕ_q comme le schéma non réduit donné par l'équation $\phi_q(x) = 0$, c'est à dire par l'équation $x^q = 0$, donc de poser

$$\mathrm{Ker}(\phi_q) \ = \ \mathrm{Spec}(k[x]/x^q)\,.$$

Ainsi $\mathrm{Ker}(\phi_q)$ est un schéma non trivial, différent de $\mathrm{Spec}(k)$, ce qui correspond au fait que ϕ_q n'est pas un isomorphisme. De plus, on lit sur la taille de $\mathrm{Ker}(\phi_q)$ le degré de ϕ_q. En effet le rang de la k-algèbre finie $k[x]/x^q$ est q, qui est le degré de ϕ_q. La situation dégénère par contre lorsqu'on considère les $\bar{k}$-points de $\mathrm{Ker}(\phi_q)$. On a alors $\mathrm{Ker}(\phi_q)(\bar{k}) = \{0\}$ car l'équation $x^q = 0$ n'a que 0 comme solution dans $\bar{k}$ ou plus généralement dans un anneau réduit. Le schéma non réduit $\mathrm{Ker}(\phi_q)$ n'est donc pas caractérisé par ses $\bar{k}$-points. Il serait caractérisé par ses points à valeurs dans des anneaux non réduits (c'est par exemple une conséquence du lemme de Yoneda). Le schéma $\mathrm{Ker}(\phi_q)$ est le premier exemple de schéma en groupe fini et plat. Ce sont des schémas typiquement non réduits qui interviennent dans l'étude de la géométrie algébrique en caractéristique positive.

Remarque 2.5.22. — Le morphisme de Frobenius existe en fait pour toute variété algébrique sur un corps de caractéristique p. Par exemple si $X = \mathbb{A}^1_k = \mathrm{Spec}(k[x])$, on a $\phi_q : X \to X$, $x \mapsto x^q$. Dans ce cas ϕ_q n'a aucune rapport avec l'isogénie $[q]_{\mathbb{A}^1}$ provenant de la loi de groupe de $\mathbb{A}^1_k$ car $[q]_{\mathbb{A}_1}(x) = qx = 0$. Si $X = \mathrm{G}_{mk} = \mathrm{Spec}(k[x, x^{-1}])$, on a $\phi_q : X \to X$, $x \mapsto x^q$. Dans ce cas on a $\phi_q = [q]_{\mathrm{G}_m}$. Pour les courbes elliptiques, on verra plus tard que ϕ_q est un facteur de $[q]_E$, c'est-à-dire qu'il existe une isogénie $\hat{\phi_q}$ telle que $\hat{\phi_q} \circ \phi_q = [q]_E$.

2.5.1.1. *Isogénie duale.* — Sur les complexes, on a construit l'isogénie duale de manière analytique (si f était la multiplication par $\alpha \in \mathbb{C}$ alors $\hat{f}$ est la multiplication par le conjugué $\bar{\alpha}$). Dans le cas algébrique, on va utiliser le théorème 2.4.2.

Théorème 2.5.23. — *Soit $f : E \to E'$ une isogénie de degré n. Il existe une unique isogénie $\hat{f} : E' \to E$ telle que $\hat{f} \circ f = [n]_E$ et $f \circ \hat{f} = [n]_{E'}$. On dit que $\hat{f}$ est l'isogénie duale de f.*

Démonstration. — Montrons l'unicité. Si $\hat{f}$ et $\hat{f}'$ sont deux isogénies duales on a $(\hat{f} - \hat{f}') \circ f = 0_E$. Comme f est non constant on en déduit que $\hat{f} - \hat{f}'$ est constant. Vu sa valeur en $0_{E'}$, cette différence est bien nulle.

Montrons l'existence. L'application non constante $f : E \to E'$ induit une injection de corps $f^* : k(\eta_{E'}) \hookrightarrow k(\eta_E)$. Elle induit aussi un morphisme $f^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$ en posant $f^*((P')) = \sum_{P \in f^{-1}(\{P'\})} e_P \cdot (P)$ pour tout $P' \in |E'|$, où on a noté e_P le degré de ramification de f en P. L'application f^* induit un morphisme $f^* : \mathrm{Div}^0(E') \to \mathrm{Div}^0(E)$ puis un morphisme $f^* : \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E)$. En appliquant le théorème 2.4.2 on en déduit un morphisme $\hat{f}(k) : E'(k) \to E(k)$. On a de même $\hat{f}(l) : E'(l) \to E(l)$ pour toute extension l/k. On utilise la notion de point générique et de spécialisation pour montrer

qu'il existe une application algébrique $\hat{f} : E' \to E$ qui induit $\hat{f}(l)$ sur les l-points pour toute extension l/k. Choisissons en effet $l = k(\eta_{E'}) = k(x, y)$. On dispose de $\hat{f}(l) : E'(l) \to E(l)$. Mais on dispose aussi d'un point canonique (appelé point tautologique, ou point générique) $\eta_{E'}$ de $E'(l)$: il correspond à la solution $(x, y) \in l = k(x, y)$ de l'équation $y^2 = x^3 + a'x + b'$. Le $k(\eta_{E'})$-point $\hat{f}(l)(\eta_{E'})$ de E défini alors une application rationnelle $\hat{f} : U' \to E$ pour U' un ouvert de Zariski de E'. Cette application s'étend en une application régulière $\hat{f} : E' \to E$ par propreté de E et E'.

Vérifions qu'on a bien $f \circ \hat{f} = [n]_{E'}$. D'après la démonstration de la proposition 2.5.2, l'application $f : E(k) \to E'(k)$ s'obtient après application des isomorphismes d'Abel-Jacobi α et α' à partir de l'application $f_* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(E')$, qui s'obtient elle-même à partir de $f_* : \mathrm{Div}^0(E) \to \mathrm{Div}^0(E')$ qui envoie $\sum_P n_P \cdot (P)$ sur $\sum_P n_P \cdot (f(P))$. Il suffit donc de vérifier que $f_* \circ f^*$ est la multiplication par n sur $\mathrm{Div}^0(E')$. Mais

$$f_* \circ f^*(P') \;=\; f_* \left(\sum_{P \in f^{-1}(\{P'\})} e_P \cdot (P) \right) \;=\; \sum_{P \in f^{-1}(\{P'\})} e_P \cdot (f(P)) = n \cdot (P')$$

De même pour tout extension l/k. On a donc $f(l) \circ \hat{f}(l) = [n]_E$ comme endomorphisme de $E'(l)$. On en déduit que $f \circ \hat{f} = [n]_E$.

On montre enfin que $\hat{f} \circ f = [n]_E$ en écrivant $(\hat{f} \circ f) \circ \hat{f} = \hat{f} \circ (f \circ \hat{f}) = \hat{f} \circ [n]_{E'} = [n]_E \circ \hat{f}$ où la dernière égalité provient du fait que $\hat{f}$ est un morphisme de groupes. On en déduit que $(\hat{f} \circ f - [n]_E) \circ \hat{f}$ est nulle puis comme $\hat{f}$ est non constante que $\hat{f} \circ f = [n]_E$. □

Remarque 2.5.24. — De manière explicite, $\hat{f}(P')$ est donc l'unique point $P \in E(k)$ tel que $(P) - (0_E) \sim f^*((P') - (0_{E'}))$ pour tout $P' \in E$.

Remarque 2.5.25. — Le morphisme $f^* : \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E)$ se comprend très bien en termes de faisceaux inversibles. Rappelons que $\mathrm{Pic}(E) = \mathrm{Div}(E)/k(\eta_E)^*$ s'identifie naturellement à l'ensemble des classes d'isomorphismes de $\mathcal{O}_E$-modules localement libre et que le sous-ensemble $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/k(\eta_E)^*$ consiste par définition en les classes d'isomorphismes de $\mathcal{O}_E$-modules localement libre de degré nul. Comme la notation le suggère, le morphisme $f^* : \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E)$ est simplement le foncteur d'image inverse des faisceaux cohérents. En ces termes on a donc $f^*(\mathcal{L}') = f^{-1}(\mathcal{L}) \otimes_{f^{-1}(\mathcal{O}_{E'})} \mathcal{O}_E$.

Remarque 2.5.26. — On voit que même si on suppose k parfait, on a utilisé dans la preuve le corps non parfait $k(x, y) = k(\eta_{E'})$. Cela justifie l'intérêt de considérer aussi des corps non parfaits. Le lecteur pourra par ailleurs se reporter à [**Ne**, 12.6] pour plus de détails sur l'utilisation des points génériques.

L'isogénie duale $f \mapsto \hat{f}$ n'est définie que pour f une isogénie, c'est à dire un morphisme non nul. On pose $\hat{0} = 0$ ce qui permet d'étendre $f \mapsto \hat{f}$ en une application $\mathrm{Hom}(E, E') \to \mathrm{Hom}(E', E)$.

Proposition 2.5.27. — *Les points suivants sont vérifiés.*

i. *Soit $f : E \to E'$ une isogénie. On a $\deg(f) = \deg(\hat{f})$ et $\hat{\hat{f}} = f$.*

ii. *Soient $f : E \to E'$ et $g : E' \to E''$ deux isogénies. On a $\widehat{g \circ f} = \hat{f} \circ \hat{g}$.*

iii. *Soient $f : E \to E'$ et $g : E \to E'$ deux isogénies. On a $\widehat{f +_{E'} g} = \hat{f} +_E \hat{g}$.*

iv. *Pour tout $n \in \mathbb{Z}$ on a $\widehat{[n]}_E = [n]_E$ et $\deg([n]_E) = n^2$.*

Démonstration. — Admettons le point 3 pour l'instant et prouvons le dernier. On en déduit $\widehat{[n]}_E = [n]_E$ par récurrence sur n. On a ensuite $[\deg(n)] = [n] \circ \widehat{[n]} = [n] \circ [n] = [n^2]$ donc $\deg([n]) = n^2$ puisque $[\bullet] : \mathbb{Z} \to \mathrm{End}(E)$ est injective.

Montrons le second point. Soit $r = \deg(f)$ et $s = \deg(g)$. On a $g \circ f \circ \hat{f} \circ \hat{g} = g \circ [r] \circ \hat{g} = [r] \circ g \circ \hat{g}$ car g est un morphisme de groupes donc $g \circ [r] = [r] \circ g$. On trouve donc $g \circ f \circ \hat{f} \circ \hat{g} = [r] \circ [s] = [rs] = [\deg(g \circ f)]$ d'où $\widehat{g \circ f} = \hat{f} \circ \hat{g}$.

Montrons le premier point. On a $\deg(f) \cdot \deg(\hat{f}) = \deg(f \circ \hat{f}) = \deg([\deg(f)]) = \deg(f)^2$ d'où $\deg(f) = \deg(\hat{f})$. On a ensuite en notant $n = \deg(f) = \deg(\hat{f})$ les égalités

$$[n] \circ \hat{\hat{f}} = f \circ \hat{f} \circ \hat{\hat{f}} = f \circ [n] = [n] \circ f$$

donc $f = \hat{\hat{f}}$.

La démonstration du point 3 est authentiquement difficile. Elle demande de considérer des diviseurs sur la surface $E \times_k E$, et de considérer la courbe elliptique $E_{k(\eta_E)}$ sur le corps non parfait $k(\eta_E)$. Pour plus de détails, voir [**Ne**, 3.1.6]. □

Corollaire 2.5.28. — *L'application* $\deg : \mathrm{End}(E, E') \to \mathbb{Z}$ *est quadratique. Ainsi l'application* $\mathrm{End}(E, E') \times \mathrm{End}(E, E') \to \mathbb{Z}$ *qui envoie* (f, g) *sur* $\deg(f +_E g) - \deg(f) - \deg(g)$ *est bilinéaire.*

Démonstration. — C'est clair car on a dit que $f \mapsto \hat{f}$ est linéaire et que $[\deg(f)] = \hat{f} \circ f$ est donc quadratique. □

2.6. Différentielles invariantes

Soit k un corps de caractéristique $\neq 2, 3$ et E une courbe elliptique sur k d'équation affine $y^2 = x^3 + ax + b$. Notons $\omega_E = \frac{dx}{2y} = \frac{dy}{3x^2+a}$ qui est une forme différentielle rationnelle sur E. Rappelons que si $P \in |E|$ admet la fonction z_P comme paramètre local (ainsi z_P est un générateur de l'idéal maximal de l'anneau de valuation discrète $\mathcal{O}_{E,P}$) on pose $\mathrm{ord}_P(f \cdot dz_P) = \mathrm{ord}_P(f)$ pour tout $f \in k(\eta_E)^*$. On dit que $f \cdot dz_P$ est régulière en P si son ordre est ≥ 0 et qu'elle est non nulle en P si son ordre est nul.

Lemme 2.6.1. — *La forme différentielle ω_E est régulière sans zéros. On a donc $H^0(E, \Omega^1_{E/k}) = k \cdot \omega_E$.*

Démonstration. — Soit $P = (x_P, y_P) \in E(\bar{k}) - \{0_E\}$. Comme E est lisse en P, on a $2y_P \neq 0$ ou $3x_P^2 + a \neq 0$. Si $2y_P \neq 0 \neq 0$ on en déduit que $\omega_E = \frac{dx}{2y}$ est régulière non nulle en P. Si $3x_P^2 + a \neq 0$ on utilise l'expression $\omega_E = \frac{dy}{3x^2+a}$ pour conclure la même chose. Enfin si $P = 0_E$ on utilise le fait que $\deg(\mathrm{div}(\omega_E)) = 0$ pour conclure que ω_E est régulière non nulle en 0_E. Enfin $H^0(E, \Omega^1_{E/k})$ est de dimension 1 puisque E est de genre 1. On en déduit qu'il est engendré par n'importe quelle forme différentielle régulière sans zéros. □

Remarque 2.6.2. — Si la caractéristique de k est 2 ou 3 et que l'équation de E prend donc une forme compliquée, on peut néanmoins définir ω_E. Tous les résultats de cette partie restent vrais.

Lemme 2.6.3. — *La multiplication par ω_E induit un isomorphisme $\mathcal{O}_E \xrightarrow{\sim} \Omega^1_{E/k}$. En particulier le faisceau localement libre $\Omega^1_{E/k}$ est en fait libre de rang un muni d'une trivialisation canonique.*

Démonstration. — La section ω_E de $\Omega^1_{E/k}$ est définie sur E et n'a pas de zéros. On a donc $\omega_E \cdot \mathcal{O}_{E,P} = \Omega^1_{E/k} \otimes_{\mathcal{O}_E} \mathcal{O}_{E,P}$ pour tout $P \in E$. □

Remarque 2.6.4. — Soit G une variété lisse sur k qui a une structure de schéma en groupes. En particulier $G(\bar{k})$ est un groupe. On dispose alors du faisceau $\Omega^1_{G/k}$ qui est localement libre de rang $\dim(G/k)$. Notons $e : \mathrm{Spec}(k) \to G$ la section neutre Il existe alors un isomorphisme canonique $\Omega^1_{G/k} \xrightarrow{\sim} \mathcal{O}_G \otimes_k (e^*\Omega^1_{G/k})$. En particulier le faisceau localement libre $\Omega^1_{G/k}$ est en fait libre associé au k-espace vectoriel $e^*\Omega^1_{G/k}$. C'est ce qu'on appelle le « transport parallèle » sur le fibré cotangent d'un groupe.

L'hypothèse de lissité est en fait gratuite pour un groupe : si G est réduit sur k et admet une structure de schéma en groupes, il est lisse. En effet comme G est réduit, le lieu lisse de G est un ouvert dense. Mais il est stable par translation par la loi de groupe, donc est égal à tout G. Les groupes non réduits sont néanmoins intéressants. De tels exemples de groupes s'obtiennent en considérant $E[p]$ ou $\mathrm{Ker}(\phi_p)$ vus comme schémas en groupes sur un corps de caractéristique p (voir la remarque 2.5.21).

Lorsque G est une courbe projective réduite sur k qui est un groupe, on a donc $\Omega^1_{X/k} \xrightarrow{\sim} \mathcal{O}_X$. On a donc $2g_X - g = \deg(\Omega^1_{X/k}) = \deg(\mathcal{O}_X) = 0$. On retrouve qu'une courbe projective est un groupe si et seulement si elle est de genre 1, donc si c'est une courbe elliptique. Par contre si on relaxe l'hypothèse de propreté, $\mathbb{G}_a = \mathbb{A}^1 = \mathrm{Spec}(k[x]))$ et $\mathbb{G}_m = \mathbb{A}^1 - \{0\} = \mathrm{Spec}(k[x, x^{-1}])$ sont des groupes. Comme on l'a vu en TD, on les obtient d'ailleurs comme lieu lisse des courbes définies par des équations $y^2 = x^3 + ax + b$ avec $\Delta = 0$, munis de la loi de groupe géométrique définie avec les cordes au lieu lisse de la courbe.

Proposition 2.6.5. — *Si m, p_1, p_2 désignent les trois applications de $E \times_k E$ dans E on a $m^*(\omega) = p_1^*(\omega) + p_2^*(\omega)$ pour tout $\omega \in H^0(E, \Omega^1_{E/k})$.*

Démonstration. — De la même manière que $\mathcal{O}_E \to \Omega^1_{E/k}$, $f \mapsto f \cdot \omega_E$ est un isomorphisme, l'application

$$\mathcal{O}^2_{E\times_k E} \longrightarrow \Omega^1_{E\times_k E/k}$$

qui envoie (f_1, f_2) sur $f_1 \cdot p_1^*(\omega_E) + f_2 \cdot p_2^*(\omega_E)$ est un isomorphisme, où $p_i : E \times_k E \to E$ est la projection sur le i-ème facteur. En prenant les sections globales on obtient un isomorphisme $k^2 \xrightarrow{\sim} H^0(E \times_k E, \Omega^1_{E\times_k E/k})$, $(c_1, c_2) \mapsto c_1 \cdot p_1^*(\omega_E) + c_2 \cdot p_2^*(\omega_E)$. Mais

$$m^*(\omega) \in H^0(E \times_k E, \Omega^1_{E\times_k E/k})$$

donc il existe $c_1, c_2 \in k$ tels que $m^*(\omega) = c_1 \cdot p_1^*(\omega_E) + c_2 \cdot p_2^*(\omega_E)$. En évaluant un des points de $E \times E$ de la forme $P \times 0_E$ et $0_E \times P$ avec $P \in E$ on trouve $c_1 = c_2 = 1$ d'où le résultat. □

Remarque 2.6.6. — On dit que tout $\omega \in H^0(E, \Omega^1_{E/k})$ est une forme différentielle invariante par la loi de groupe de E. C'est en particulier vrai pour ω_E. On a donc $\omega(P) +_k \omega(Q) = \omega(P +_E Q)$ pour tous $P, Q \in E(k)$. On remarque que la formulation de cette égalité utilise déjà le fait que le fibre cotangent dont les sections sont $\Omega^1_{E/k}$ est canoniquement trivialisé d'après le lemme 2.6.3. On a ainsi un isomorphisme canonique $(\Omega^1_{E/k})_P = k$ pour tout $P \in E(k)$. On peut ainsi additionner les éléments $\omega(P)$ et $\omega(Q)$ qui sinon vivraient dans des espaces vectoriels différents.

Remarque 2.6.7. — Si $G = \mathbb{G}_a = \mathrm{Spec}(k[x])$, la forme dx est invariante car $d(x + y) = dx + dy$. La forme $f(x)dx$ est invariante si et seulement si f est constante. Si $G = \mathbb{G}_m = \mathrm{Spec}(k[x, x^{-1}])$, la forme dx/x est invariante car

$$\frac{d(xy)}{xy} = \frac{dx}{x} \cdot \frac{dy}{y}\,.$$

La forme $f(x)dx/x$ est invariante si et seulement si f est constante. On voit donc que pour un schéma en groupes G c'est la propreté qui permet de montrer que toutes les formes différentielles sont invariantes : il faut que les seules fonctions globales soient constantes.

Remarque 2.6.8. — Si $k = \mathbb{C}$ et $E = \mathbb{C}/\Lambda$ pour $\Lambda \subset \mathbb{C}$ un réseau, la surjection $\pi : \mathbb{C} \to E$ est un revêtement non ramifié (on dit encore qu'elle est étale). On a donc $\pi^*(\Omega^1_E) = \Omega^1_{\mathbb{C}} = \mathcal{O}_{\mathbb{C}} \cdot dz$. On alors $\pi^*(\omega_E) = dz$, ce qui permet de comprendre d'une autre manière pourquoi ω_E est invariante. En effet, l'algébrisation de E se fait en posant $x = \wp_\Lambda(z)$ et $y = \wp'_\Lambda(z)$. On obtient alors une équation de la forme $y^2 = 4x^3 - ax - b$ qu'il faut transformer en $y^2 = x^3 + Ax + B$. On trouve $\omega_E = dx/y = d(\wp_\Lambda(z))/\wp'_\Lambda(z)$ et $d(\wp_\Lambda(z)) = \wp'_\Lambda(z) \cdot dz$.

Remarque 2.6.9. — Soit E une courbe elliptique sur k vue comme une courbe de genre 1 munie d'un point rationnel $0_E \in E(k)$. On n'a pas de forme différentielle canonique ω_E. En effet $\omega_E = dx/2y$ dépend d'un choix de coordonnées, c'est à dire d'une équation de E. Mais x et y ne sont définies qu'à une constante près (voir par exemple leur construction avec $x \in H^0(E, \mathcal{O}_E(-2(0_E))) - H^0(E, \mathcal{O}_E)$).

De même si E est une courbe elliptique sur $\mathbb{C}$, la forme différentielle dz n'est canonique que lorsqu'on a fixé une uniformisation $E = \mathbb{C}/\Lambda$. Mais comme on l'a dit dans la remarque 1.2.5, cette uniformisation provient elle-même du choix d'une forme différentielle sur E... Au final ce qui est canonique est l'uniformisation expliquée dans la remarque 1.2.5 et la trivialisation du faisceau des formes différentielles $\Omega^1_{E/k} = (e^*\Omega^1_{E/k}) \otimes_k \mathcal{O}_E$ expliquée dans la remarque 2.6.4.

Corollaire 2.6.10. — *Soient $f, g : E \to E'$ deux isogénies. On a $(f +_{E'} g)^*(\omega') = f^*(\omega') +_k g^*(\omega')$ pour tout $\omega' \in H^0(E', \Omega^1_{E'/k})$.*

Démonstration. — Notons $h = (f, g) : E \to E' \times_k E'$. On a $f +_{E'} g = m \circ h$, $f = p_1 \circ h$ et $g = p_2 \circ h$. Il suffit donc d'appliquer la proposition 2.6.5. □

Corollaire 2.6.11. — *On a $[n]^*_E(\omega) = n \cdot \omega$ pour tout $n \in \mathbb{Z}$ et $\omega \in H^0(E, \Omega^1_{E/k})$.*

Démonstration. — Récurrence sur $|n|$ avec le corollaire précédent. □

2.6.1. Isogénies séparables et formes différentielles. — Nous avons défini la notion d'isogénie séparable dans la définition 2.5.15. Si k est de caractéristique nulle, toute isogénie est séparable. Si k est de caractéristique p toute isogénie de degré premier à p est séparable. D'après la proposition 2.5.17, si k est de caractéristique p, à isomorphisme près toute isogénie se factorise comme composé du Frobenius et d'une isogénie séparable.

Proposition 2.6.12. — *Soit k un corps et $f : E \to E'$ une isogénie entre courbes elliptiques sur k. Alors f est séparable si et seulement si $f^*(\omega_{E'}) = 0$.*

Démonstration. — On utilise la suite longue des différentielles de Kaehler associée aux compositions $k \subset k(\eta_{E'}) \subset k(\eta_E)$. On trouve une suite exacte

$$\begin{array}{ccccc}
\Omega^1_{k(\eta_{E'})/k} \otimes_{k(\eta_{E'})} k(\eta_E) & \xrightarrow{f^*} & \Omega^1_{k(\eta_E)/k} & \longrightarrow & \Omega^1_{k(\eta_E)/k(\eta_{E'})} \\
\downarrow = & & \downarrow = & & \downarrow \\
k(\eta_E) \cdot \omega_{E'} & \xrightarrow{f^*} & k(\eta_E) \cdot \omega_E & \longrightarrow & \Omega^1_{k(\eta_E)/k(\eta_{E'})}
\end{array}$$

On en déduit que $f^*(\omega_{E'}) = 0$ si et seulement si $\Omega^1_{k(\eta_E)/k(\eta_{E'})} = 0$ donc si et seulement si l'extension $k(\eta_{E'}) \subset k(\eta_E)$ est engendrée par éléments dont le polynôme minimal est de dérivée nul, donc si et seulement cette extension est inséparable. □

Exemple 2.6.13. — Si k est de caractéristique p et $q = p^r$, l'isogénie $\phi_q : E \to E^{(q)}$, $(x, y) \mapsto (x^q, y^q)$ est non séparable (elle est purement inséparable, donc n'admet aucune factorisation non triviale faisant intervenir une isogénie séparable) et en effet $\phi_q^*(\omega_{E^{(q)}}) = \phi_q^*(dx/(2y)) = d\phi_q(x)/2\phi_q(y) = 0$ car $d\phi_q(x) = \phi_q'(x) \cdot dx = qx^{q-1} \cdot dx = 0$.

Proposition 2.6.14. — *Soit $f : E \to E'$ une isogénie séparable entre courbes elliptiques sur k. Soient $k \subset k^{\mathrm{sep}} \subset \bar{k}$ des clôtures séparable algébrique de k.*

i. *Pour tout $P \in E$, le morphisme f est non ramifié en P.*

ii. *Pour tout $P' \in E'(\bar{k})$, l'ensemble des antécédents $f^{-1}(\{P'\}) \subset E(\bar{k})$ est de cardinal $\deg(f)$.*

iii. *Pour tout $P' \in E'(k^{\mathrm{sep}})$ et tout $P \in f^{-1}(\{P'\})$, on a $P \in E(k^{\mathrm{sep}})$, ie $f^{-1}(\{P'\})$ est défini sur k^{sep}.*

iv. *Le groupe abélien fini $\ker(f)(\bar{k})$ est de cardinal $\deg(f)$, égal à $\ker(f)(k^{\mathrm{sep}})$ et est muni d'une action canonique de $\mathrm{Gal}(k^{\mathrm{sep}}/k)$.*

Démonstration. — Comme f est séparable, il induit un morphisme non ramifié $\eta_E \to \eta_{E'}$. Il existe donc un ouvert $U \subset E$ tel que $f|_U$ soit non ramifié, car par définition n'importe quelle propriété vraie au point générique s'étend à un ouvert Zariski assez petit. Mais f est un morphisme de groupe donc en translatant U par E on voit que f est non ramifiée. Cela démontre le premier point.

Soit $P' \in E'(\bar{k})$ et $P \in f^{-1}(\{P'\})$. L'indice de ramification de f en P est donc égal à 1 et on a bien $\deg(f) = \sum_{P \in f^{-1}(\{P'\})} e_P = \mathrm{Card}(f^{-1}(\{P'\}))$. Cela montre le point 2.

Le point 3 résulte du fait que comme f est non-ramifié en p, l'extension de corps $f_P^* : k(P) \hookrightarrow k(P')$ est séparable. Le point 4 résulte du fait que f est défini sur k et donc que pour tout $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ et tout $P \in \ker(f)(k^{\mathrm{sep}})$ on a $f(\sigma(P)) = \sigma(f(P)) = \sigma(0_{E'}) = 0_{E'}$ et donc que σ stabilise $\ker(f)(k^{\mathrm{sep}})$. □

Remarque 2.6.15. — La réciproque de la proposition est vraie : une isogénie $f : E \to E'$ est séparable si et seulement si $\ker(f)(k^{\mathrm{sep}})$ est de cardinal $\deg(f)$. Par exemple si k est de caractéristique p et $q = p^r$, alors le Frobenius $\phi_q : E \to E^{(q)}$, $(x, y) \mapsto (x^q, y^q)$ est purement inséparable de degré q et on a $\ker(\phi_q)(\bar{k}) = \{0\}$. Voir la remarque 2.5.21 dans laquelle on explique qu'il faut considérer $\ker(\phi_q)$ comme un schéma en groupes non réduit, qui n'est pas déterminé par ses $\bar{k}$-points.

2.7. Points de torsion

On s'intéresse ici au groupe abélien fini $E[n](\bar{k})$ muni de son action galoisienne.

Proposition 2.7.1. — *Pour tout n premier à la caractéristique de k, l'isogénie $[n]_E$ est séparable. On a $E[n](\bar{k}) = E[n](k^{\mathrm{sep}})$ qui est un groupe abélien fini de cardinal n^2 muni d'une action de $\mathrm{Gal}(k^{\mathrm{sep}}/k)$.*

Démonstration. — D'après le corollaire 2.6.11, on a $[n]_E^*(\omega_E) = n \cdot \omega_E$ qui est non nul dans le k-espace vectoriel $k \cdot \omega_E$ lorsque n est premier à la caractéristique de k. On en déduit que $[n]_E$ est séparable d'après la proposition 2.6.12. Il suffit alors d'appliquer la proposition 2.6.14. □

Remarque 2.7.2. — On aurait aussi pu montrer que $[n]_E$ est séparable en remarquant que son degré est n^2 d'après la proposition 2.5.27 donc est premier à la caractéristique de k. Mais d'après la proposition 2.5.17, cela implique la séparabilité de $[n]_E$.

Proposition 2.7.3. — *Le groupe abélien fini $E[n](\bar{k})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$ pour tout entier n premier à la caractéristique de k.*

Démonstration. — Soit m un diviseur de n. Alors la m-torsion de $E[n](\bar{k})$ est égale à $E[m](\bar{k})$ qui est donc de cardinal m^2. Mais le seul groupe abélien de cardinal n^2 donc la m-torsion est de cardinal m^2 pour tout diviseur m de n est $(\mathbb{Z}/n\mathbb{Z})^2$. □

Remarque 2.7.4. — Supposons k de caractéristique > 2. Nous avons donné dans l'exemple 2.5.10 des formules de $[2]_E$ donc aussi de $[4]_E$ et de $[2^r]_E$ par itération. Le lecteur voit donc la complexité très grande des équations qui définissent $E[2^r](\bar{k})$ muni de son action galoisienne. Il n'est absolument pas évident sur des formules qu'on obtient en résolvant de telles équations une représentation galoisienne à valeurs dans $\mathrm{GL}_2(\mathbb{Z}/2^r\mathbb{Z})$!

Définition 2.8 **(module de Tate)**. — Soit ℓ un nombre premier premier à la caractéristique de k. On note $T_\ell E$ la limite projective sur r de $E[\ell^r](\bar{k})$. On obtient de la sorte un groupe abélien isomorphe à $\mathbb{Z}_\ell^2$ muni d'une action continue de $\mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Lemme 2.8.1. — *Soient E et E' des courbes elliptiques sur k et $f : E \to E'$ un morphisme défini sur k. Il induit $f[\ell^n] : E[\ell^n](\bar{k}) \to E'[\ell^n](\bar{k})$ et $f_\ell : T_\ell(E) \to T_l(E')$ qui sont des morphismes de $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-représentations pour tout $\ell \neq \mathrm{car}(k)$.*

Remarque 2.8.2. — On obtient donc un morphisme

$$\varphi : \mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}(k^{\mathrm{sep}}/k)]}\left(T_\ell E_1[1/\ell], T_\ell E_2[1/\ell]\right)$$

qui est toujours injectif comme on l'a mentionné en TD [**Si**, th.III.7.4]. D'après un théorème de Tate, c'est un isomorphisme si k est fini (étape importante de la démonstration de la

conjecture de Tate pour les diviseurs des variétés abéliennes) et d'après un théorème de Faltings, c'est un isomorphisme si k est un corps de nombres (étape clé de la démonstration de la conjecture de Mordell qui affirme que les courbes de genre > 1 ont un nombre fini de points sur les corps de nombres). Ainsi lorsque k est un corps fini ou un corps de nombres, la classe d'isogénie d'une courbe elliptique est déterminée par la représentation galoisienne sur le module de Tate. C'est bien sûr faux (et φ n'est pas un isomorphisme) lorsque k est algébriquement clos car il n'y a plus de groupe de Galois. C'est aussi faux (et φ n'est pas un isomorphisme) lorsque k est une extension finie de $\mathbb{Q}_p$.

Remarque 2.8.3. — Si $k = \mathbb{C}$ et $E = \mathbb{C}/\Lambda$ on a $E[n](\mathbb{C}) = \Lambda/n \cdot \Lambda$ et un isomorphisme canonique $T_\ell E = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Si k est général on ne sait pas définir Λ mais on sait moralement définir $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = T_\ell E$ pour tout ℓ premier à la caractéristique de k.

Comme nous l'avons dit dans la remarque 1.2.5, si $k = \mathbb{C}$ l'uniformisation canonique de E est plutôt $E = H^0(E, \Omega^1)^\vee/\Lambda$ où $H^0(E, \Omega^1)^\vee$ est un $\mathbb{C}$-espace vectoriel de dimension un. En fait la base ω_E de $H^0(E, \Omega^1)$ détermine une base duale de $H^0(E, \Omega^1)^\vee$ donc un isomorphisme canonique $H^0(E, \Omega^1)^\vee \xrightarrow{\sim} \mathbb{C}$. Mais le k-espace vectoriel $H^0(E, \Omega^1)$, la forme ω_E et l'isomorphisme $H^0(E, \Omega^1)^\vee \xrightarrow{\sim} k$ sont définis lorsque k est quelconque d'après les résultats de la partie 2.6.

Si k est quelconque, on ne peut pas définir $E = \mathbb{C}/\Lambda$ mais on peut définir $\Lambda \otimes \mathbb{Z}_\ell = T_\ell(E)$ pour tout $\ell \neq \mathrm{car}(k)$ et $k = H^0(E, \Omega^1)^\vee$. On peut se demander s'il existe un morphisme $T_\ell(E) \to H^0(E, \Omega^1)^\vee$ qui généraliserait l'inclusion $\Lambda \subset \mathbb{C}$ valable lorsque $k = \mathbb{C}$. Il y a bien sûr un problème de caractéristique : si k est de caractéristique p, un $\mathbb{Z}_\ell$-module libre ne se plonge pas dans un $\mathbb{F}_p$-espace vectoriel. Néanmoins lorsque E est une courbe elliptique sur $\mathbb{Q}_p$, on peut définir une application appelée de *Hodge-Tate* de $T_p(E)$ dans $H^0(E, \Omega^1)^\vee$.

Proposition 2.8.4. — *Soit k un corps de caractéristique p. L'isogénie $[p^r]_E$ est inséparable pour tout $r \geq 1$. Il existe un entier $a(E) = 0, 1$ indépendant de r tel que $E[p^r](\bar{k}) \simeq (\mathbb{Z}/p^r \cdot \mathbb{Z})^{a(E)}$.*

Démonstration. — L'isogénie $[p]_E$ est inséparable d'après la proposition 2.6.12 car $[p]_E^*(\omega_E) = p \cdot \omega_E = 0$. D'après la proposition 2.5.17, on obtient une factorisation $[p]_E = \mu \circ \phi_q$ avec $q = p^b$, $b > 0$ et $\mu : E^{(q)} \to E$ une isogénie séparable. Comme $\deg([p]_E) = p^2$ et $\deg(\phi_q) = q$ on en déduit $b = 1, 2$. On a donc $\deg(\mu) = p^a$ avec $a = 2 - b$. On applique la proposition 2.6.14 à μ et on en déduit $\mathrm{Ker}(\mu)(\bar{k}) = (\mathbb{Z}/p)^a$. Donc $E[p](\bar{k}) = (\mathbb{Z}/p)^a$ car $\mathrm{Ker}(\phi_q)(\bar{k}) = 0$. On traite ensuite le cas $r > 1$ par récurrence. □

Définition 2.8.5. — On dit que E est ordinaire si $a(E) = 1$ et que E est supersingulière si $a(E) = 0$.

Remarque 2.8.6. — Ainsi E est ordinaire si et seulement si $E[p](\bar{k}) \neq 0$ et E est supersingulière si $E[p](\bar{k}) = 0$. On notera qu'en caractéristique p, les courbes elliptiques

n'ont *jamais* p^2 points de p-torsion. Comme nous l'avons déjà mentionné, le bon objet à considérer est un schéma en groupes non réduit de rang p^2 noté $E[p]$, qui peut soit avoir p-points avec indice de nilpotence p dans le cas ordinaire, soit un seul point avec indice de nilpotence p^2 dans le cas supersingulier.

Lemme 2.8.7. — *La courbe E est ordinaire si et seulement si $[p]_E$ est inséparable mais pas purement inséparable, si et seulement si $\hat{\phi}_p$ est séparable.*

Démonstration. — La première équivalence est claire. Pour la seconde on utilise $\hat{\phi}_p \circ \phi_p = [p]_E$ par définition de l'isogénie duale. □

Lemme 2.8.8. — *Supposons $k = \mathbb{F}_q$ avec $q = p^r$. Si une courbe elliptique E sur k est supersingulière, on a $\hat{\phi}_q = \phi_q \circ \alpha$ pour $\alpha \in \mathrm{Aut}(E)$.*

Démonstration. — Comme E est supersingulière, $\hat{\phi}_q = \hat{\phi}_p^r$ est inséparable. Par ailleurs $E^{(p)} = E$ puisque $k = \mathbb{F}_q$. D'après la proposition 2.5.17 il existe un isomorphisme entre $(E, \hat{\phi}_q)$ et (E, ϕ_q). C'est exactement ce qu'on voulait montrer. □

Exemple 2.8.9. — Si E est définie par $y^2 = x^3 - x$ sur $\mathbb{F}_p$ et si p est inerte dans $\mathbb{Q}(i)$ (donc si $p \equiv 3$ modulo 4), la courbe E est supersingulière sur $\mathbb{F}_{p^2} = \mathbb{Z}[i]/p$. En effet nous admis en TD que dans ce cas $\phi_p^2 = [-p]_E$ donc $\hat{\phi}_p = [-1]_E \circ \phi_p$. Remarquons que si on savait *a priori* que E était supersingulière, on pourrait en déduire la formule $\hat{\phi}_p = \alpha \circ \phi_p$ avec $\alpha \in \mathrm{Aut}(E)$.

Si par contre p est totalement décomposé dans $\mathbb{Q}(i)$ (donc si $p \equiv 1$ modulo 4) écrivons $p = x \cdot \bar{x}$ avec $x \in \mathbb{Z}[i]$. Posons $x = u + iv$ avec $u, v \in \mathbb{Z}$. Fixons $I \in \mathbb{F}_p$ tel que $I^2 = -1$. Le morphisme $\mathbb{Z}[i] \to \mathbb{F}_p$ qui envoie i sur I induit un isomorphisme $\mathbb{Z}[i]/x \xrightarrow{\sim} \mathbb{F}_p$. Le choix de I permet de définir une action de $\mathbb{Z}[i]$ sur E par multiplication complexe, ce qui permet de définir $[x]_E$ et $[\bar{x}]_E$. On a $[x]_E \circ [\bar{x}]_E = [p]_E$. On a alors $[x]_E^*(\omega_E) = (u + Iv) \cdot \omega_E$ qui est nul dans $\mathbb{F}_p = \mathbb{Z}[I]/(u + Iv)$, et on a $[\bar{x}]_E^*(\omega_E) = (u - Iv) \cdot \omega_E = 2u \cdot \omega_E$ qui est non nul car $p \neq 2$. On en déduit que $[p]_E$ n'est pas purement inséparable et donc que E est ordinaire. Remarquons aussi que $\phi_p = \alpha \circ [x]_E$ pour $\alpha \in \mathrm{Aut}(E)$.

Remarque 2.8.10. — Dans le cas supersingulier général, on a $\alpha \circ \phi_p^2 = [p]_E$ avec les notations du lemme 2.8.8. En particulier, à l'automorphisme α près (et l'on classifiera les différents automorphismes possibles à la fin de ce cours) on a la formule simple $[p]_E(x, y) = (x^{p^2}, y^{p^2})$. Inversement une telle formule implique la supersingularité car on voit alors que $[p]_E$ est purement inséparable.

La proposition suivante jouera un rôle crucial lorsqu'on comptera le nombre de points des courbes elliptiques sur un corps fini.

Proposition 2.8.11. — *Soit $k \subset \mathbb{F}_q$ un corps fini et E une courbe elliptique sur k. L'isogénie $\mathrm{Id}_E - \phi_q : E \to E$ est séparable.*

Démonstration. — On a $(\mathrm{Id}_E - \phi_q)^*(\omega_E) = \omega_E$. □

2.9. Points sur les corps finis

Soit p un nombre premier et $q = p^r$. Soit E une courbe elliptique sur $\mathbb{F}_q$ munie de son endomorphisme de Frobenius ϕ_q. On s'intéresse dans cette partie au cardinal du groupe fini $E(\mathbb{F}_q)$.

Lemme 2.9.1. — *Soit X une variété de type fini sur $\mathbb{F}_q$. Alors $X(\mathbb{F}_q)$ est un ensemble fini.*

Démonstration. — Comme X est recouvert par un nombre fini de schéma affines, on se ramène à supposer X affine. Alors X est un fermé de Zariski dans $\mathbb{A}^n_{\mathbb{F}_q}$. Mais $\mathbb{A}^n_{\mathbb{F}_q}(\mathbb{F}_q) = \mathbb{F}_q^n$ est fini. □

Remarque 2.9.2. — Soit X une variété de type fini intègre de dimension d sur $\mathbb{F}_q$ et $U \subset X$ un ouvert affine. Par le lemme de normalisation de Noether, il existe un morphisme fini surjectif $U \to \mathbb{A}^d_{\mathbb{F}_q}$ donc $U(\mathbb{F}_{q^s}) = O(q^{sd})$ lorsque $s \to \infty$. Comme $X - U$ est une variété de dimension $< d$ sur $\mathbb{F}_q$, on peut lui appliquer le même argument en raisonnant par récurrence sur d. On en déduit que $X(\mathbb{F}_{q^s}) = O(q^{sd})$ lorsque $s \to \infty$.

Proposition 2.9.3. — *On a* $\mathrm{Card}(E(\mathbb{F}_q)) = \deg(\mathrm{Id}_E - \phi_q)$.

Démonstration. — D'après la proposition 2.8.11, l'isogénie $\mathrm{Id}_E - \phi_q$ est séparable donc d'après la proposition 2.6.14, $E(\mathbb{F}_q) = \ker(\mathrm{id}_E - \phi_q)(\bar{\mathbb{F}}_q)$ a pour cardinal $\deg(\mathrm{Id}_E - \phi_q)$. □

Proposition 2.9.4. — *Si E et E' sont deux courbes elliptiques isogènes sur $\mathbb{F}_q$, on a* $\mathrm{Card}(E(\mathbb{F}_q)) = \mathrm{Card}(E'(\mathbb{F}_q))$.

Démonstration. — Soit $f : E \to E'$ une isogénie. On applique le lemme du serpent au diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E(\bar{\mathbb{F}}_q) & \xrightarrow{f} & E'(\bar{\mathbb{F}}_q) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \mathrm{id}_E - \phi_q} & & \downarrow{\scriptstyle \mathrm{id}_{E'} - \phi'_q} & & \\ 0 & \longrightarrow & A & \longrightarrow & E(\bar{\mathbb{F}}_q) & \xrightarrow{f} & E'(\bar{\mathbb{F}}_q) & \longrightarrow & 0 \end{array}$$

où on a noté $A = \ker(f)(\bar{\mathbb{F}}_q)$ qui est un groupe fini de cardinal $\deg(f)$, on a noté g la restriction de $\mathrm{id}_E - \phi_q$ à A, on a noté $\phi_q : E \to E$ et $\phi'_q : E' \to E'$ les morphismes de

Frobenius et on a utilisé $f \circ \phi_q = \phi'_q \circ f$ car f est défini sur $\mathbb{F}_q$. On obtient une suite exacte courte

$$0 \to \ker(g) \to E(\mathbb{F}_q) \to E'(\mathbb{F}_q) \to \operatorname{coker}(g) \to 0\,.$$

Mais $\operatorname{Card}(\operatorname{coker}(g)) = \operatorname{Card}(\ker(g))$ par finitude de A. □

Remarque 2.9.5. — Si E, E' et f ne sont plus définis sur $\mathbb{F}_q$ (*ie* si k est un corps de caractéristique p quelconque) on a $\phi_q : E \to E^{(q)}$, $\phi'_q : E' \to E'^{(q)}$ et $f^{(q)} \circ \phi_q = \phi'_q \circ f$ où $f^{(q)} : E^{(q)} \to E'^{(q)}$ est définie en prenant les puissances q-ièmes des coefficients des formules polynomiales définissant f.

Théorème 2.9.6 **(Hasse)**. — *Soit E une courbe elliptique sur $\mathbb{F}_q$ avec $q = p^r$. Alors*

i. *On a $\phi_q + \hat{\phi}_q = a \in \mathbb{Z}$ avec $|a| \leq 2\sqrt{q}$.*

ii. *On a $\phi_q^2 - a \cdot \phi_q + q = 0$ et $\hat{\phi}_q^2 - a \cdot \hat{\phi}_q + q = 0$ dans $\operatorname{End}(E)$. Ainsi par définition $\phi_q \circ \phi_q - [a]_E \circ \phi_q + [q]_E = [0]_E$.*

iii. *Si $|a| = 2\sqrt{q}$ alors r est pair, $\phi_q = \hat{\phi}_q = a/2 = \pm p^{r/2} = \pm\sqrt{q}$ et $\mathbb{Z}[\phi_q] = \mathbb{Z}$ comme sous-anneau de $\operatorname{End}(E)$.*

iv. *Si $|a| < 2\sqrt{q}$ alors $\mathbb{Q}[\phi_q] = \mathbb{Q}(\sqrt{a^2 - 4q})$ est un corps quadratique imaginaire.*

v. *Les deux racines $\alpha, \beta \in \mathbb{C}$ du polynôme $T^2 - aT + q$ sont conjuguées complexes et vérifient $|\alpha| = |\beta| = \sqrt{q}$.*

Démonstration. — Soient $u, v \in \mathbb{Z}$. On obtient $\deg(u + v\phi_q) = (u + v\phi_q)(u + v\hat{\phi}_q) = u^2 + (\phi_q + \hat{\phi}_q)uv + qv^2$ en tenant compte du fait que $\phi_q \cdot \hat{\phi}_q = \deg(\phi_q) = q$. Comme $\deg(u + v\phi_q) \in \mathbb{Z}$ on en déduit $\phi_q + \hat{\phi}_q = a \in \mathbb{Z}$. En particulier $\hat{\phi}_q = a - \phi_q \in \mathbb{Z}[\phi_q]$. On en déduit que ϕ_q et $\hat{\phi}_q$ sont annulées par $P(T) = T^2 - aT + q$ car

$$\phi_q^2 - a\phi_q + q = \phi_q^2 - (\phi_q + \hat{\phi}_q) \cdot \phi_q + \hat{\phi}_q\phi_q = 0\,.$$

De plus $\deg(u + v\phi_q) \geq 0$ donc la forme quadratique $(u, v) = u^2 + auv + qv^2$ est semi-définie positive et son discriminant $Q(a) = a^2 - 4q$ est positif. On en déduit $|a| \leq 2\sqrt{q}$ d'où les points 1 et 2.

Si $|a| = 2\sqrt{q}$, comme $a \in \mathbb{Z}$ l'entier r est bien pair donc $a/2 = \pm\sqrt{q}$ est entier et $(a/2 - \phi_q)(a/2 - \hat{\phi}_q) = 0$. On en déduit le point 3.

Si $|a| < 2\sqrt{q}$, la forme quadratique $(u, v) \mapsto \deg(u + v\phi_q)$ est définie positive donc $\mathbb{Q}[\phi_q] \neq \mathbb{Q}$. De plus le discriminant de $T^2 - aT + q$ est < 0 et les deux racines $\alpha, \beta \in \mathbb{C}$ de ce polynômes sont conjuguées. On obtient un isomorphisme $\mathbb{Q}[\phi_q] \xrightarrow{\sim} \mathbb{Q}[\alpha]$ en envoyant ϕ_q sur α, ce qui est légitime car ils ont même polynôme minimal. □

Proposition 2.9.7. — *Notons comme précédemment $a = \phi_q + \hat{\phi}_q \in \mathbb{Z}$ et α, β les racines complexes de $T^2 - aT + q$. On a $\beta = \bar{\alpha}$ et $|\alpha| \leq \sqrt{q}$. Pour tout $n \geq 1$ on a* $\mathrm{Card}(E(\mathbb{F}_{q^n})) = (1-\alpha^n)(1-\beta^n) = q^n + 1 - \alpha^n - \beta^n$. *On a enfin l'estimation de Hasse-Weil*

$$|\mathrm{Card}(E(\mathbb{F}_{q^n})) - 1 - q^n| \ \leq \ 2 \cdot q^{n/2} \, .$$

Démonstration. — Nous avons vu dans le théorème précédent que $\beta = \bar{\alpha}$ car soit $a^2 = q$ et $\alpha = \beta$ soit $a^2 < q$ et $\beta = \bar{\alpha}$. L'estimation $|\alpha| \leq \sqrt{q}$ est claire car $|a| = |\alpha + \beta| \leq 2\sqrt{q}$. Si $a^2 = q$ on a $\alpha = \beta = a/2 \in \mathbb{Z}$ et $\phi_q = \hat{\phi}_q = a$ donc $\phi_{q^n} = \phi_q^n = \alpha^n$ et $\hat{\phi}_{q^n} = \hat{\phi}_q^n = \beta^n$. Si $a^2 < q$ on a un isomorphisme $\mathbb{Q}[T]/(T^2 - aT + q) \xrightarrow{\sim} \mathbb{Q}(\phi_q)$ qui envoie T sur ϕ_q et un isomorphisme $\mathbb{Q}[T]/(T^2 - aT + q) \xrightarrow{\sim} \mathbb{Q}(\alpha)$ qui envoie T sur α (cela dépend du choix de α parmi les deux racines de $T^2 - aT + q$, on aurait aussi bien prendre β). On a donc *via* ces isomorphismes $\alpha^n = \phi_q^n$. De plus $\hat{\phi}_q = a - \phi_q = a - \alpha = \beta$ donc $\hat{\phi}_q^n = \beta^n$. Dans tous les cas on a $\mathrm{Card}(E(\mathbb{F}_{q^n})) = \deg(1 - \phi_q^n) = (1 - \phi_q^n)(1 - \hat{\phi}_q^n) = (1-\alpha^n)(1-\beta^n)$ ce qui permet de conclure. □

Remarque 2.9.8. — Ainsi si on connaît $\mathrm{Card}(E(\mathbb{F}_q))$ on connaît α et β par les règles $\alpha\beta = q$ et $\mathrm{Card}(E(\mathbb{F}_{q^n})) - 1 - q^n = a = \alpha + \beta$. On connaît donc aussi $\mathrm{Card}(E(\mathbb{F}_{q^n}))$ pour tout n ! Il y a donc des relations profondes entre le nombre de solutions des équations du type $y^2 = x^3 + ax + b$ avec $\Delta \neq 0$ sur tous les corps finis de caractéristique p. Cela se généralise *via* les conjectures de Weil à toutes les courbes et mêmes à toutes les variétés de type fini sur les corps fini. Par exemple lorsque X est une courbe projective lisse de genre g sur $\mathbb{F}_q$, la connaissance du cardinal de $X(\mathbb{F}_{q^n})$ pour $1 \leq n \leq g$ permet de déterminer le cardinal de $X(\mathbb{F}_{q^n})$ pour tout $n \geq 1$.

Remarque 2.9.9. — Supposons que E est une courbe elliptique définie sur $\mathbb{Z}_p$ par une équation $y^2 = x^3 + ax + b$ avec $\Delta \in \mathbb{Z}_p^*$. Elle définit donc une courbe elliptique sur $\mathbb{Z}/p^n$ pour tout n. Nous n'avons pas dit qu'il y a un lien simple entre les cardinaux de $E(\mathbb{Z}/p^n)$ lorsque n varie !

Remarque 2.9.10. — Nous avons vu dans la remarque 2.9.2 que $\mathrm{Card}(E(\mathbb{F}_{q^n})) = O(q^n)$ lorsque $n \to \infty$ car E est une courbe. La borne de Hasse-Weil permet d'améliorer grandement cette asymptotique (et d'obtenir une information pour tout n, pas seulement pour $n \to \infty$).

Remarque 2.9.11. — La théorie de l'accouplement de Weil [**Si**, ch.III.8] fournit une dualité parfaite $T_\ell(E) \otimes_{\mathbb{Z}_\ell} T_\ell(E) \to T_\ell(\mathbb{G}_m)$ où $T_\ell(\mathbb{G}_m)$ désigne les suites compatibles de racines ℓ^n-ièmes de l'unité dans $\bar{k}$. Cet autodualité identifie le dual de f_ℓ avec $(\hat{f})_\ell$ pour tout isogénie f de E d'isogénie duale $\hat{f}$, où f_ℓ et $(\hat{f})_\ell$ sont les endomorphismes induits sur $T_\ell(E)$. On en déduit que $\deg(f) = f \circ \hat{f} = \det(f_\ell)$. De même $f + \hat{f} \in \mathbb{Z}$ (voir l'exercice 2 du TD 5) est égal à $\mathrm{tr}(f_\ell)$. On peut donc réinterpréter α et β comme les valeurs propres de $(\phi_q)_\ell$ agissant

sur $T_\ell(E)$ pour tout $l \neq p$. En particulier on trouve $\mathrm{Card}(E(\mathbb{F}_{q^n})) = 1 + q^n - \mathrm{tr}((\phi_q)_\ell^n)$. Cette reformulation du comptage des solutions par le module de Tate est le point de départ de la cohomologie étale ℓ-adique. Elle vise à associer des $\mathbb{Z}_\ell$-modules munis d'action du groupe de Galois absolu à toute variété de type fini sur un corps, généralisant $E \mapsto T_\ell(E)$, puis à compter les points de la variété sur $\mathbb{F}_{q^n}$ en termes du polynôme caractéristique du Frobenius agissant sur ces groupes de cohomologie.

Remarque 2.9.12. — Ainsi si E et E' sont deux courbes elliptiques sur $\mathbb{F}_q$ qui ont même nombre de points, *via* des choix de base $T_\ell(E) \simeq \mathbb{Z}_l^2$ et $T_\ell(E') \simeq \mathbb{Z}_\ell^2$, les matrices $(\phi_q)_\ell$ et $(\phi'_q)_\ell$ ont même trace et même polynôme caractéristique. Comme on vérifie par ailleurs qu'elles sont diagonalisables, elles sont conjuguées. On a donc un isomorphisme $T_\ell(E)[1/\ell] \xrightarrow{\sim} T_\ell(E')[1/\ell]$ qui commute à l'action de $\mathrm{Gal}(\bar{F}_q/\mathbb{F}_q)$. D'après le théorème de Tate énoncé dans la remarque 2.8.2, cet isomorphisme Galois-équivariant provient d'un élément f de $\mathrm{Hom}(E, E') \otimes \mathbb{Q}_\ell$. En particulier $\mathrm{Hom}(E, E')$ est non nul, donc il existe une isogénie de E dans E'.

En tenant compte du lemme 2.9.4, on a montré que deux courbes elliptiques sur $\mathbb{F}_q$ sont isogènes si et seulement si elles ont même nombre de points sur $\mathbb{F}_q$!

2.10. Fonction zéta

La fonction $\zeta_\mathbb{Z}$ de Riemann est naturellement associée à la courbe des nombres premiers $\mathrm{Spec}(\mathbb{Z})$, dont les corps résiduels sont tous de caractéristique différente. Si maintenant X est une courbe sur $\mathbb{F}_q$, on peut aussi lui associer une fonction ζ_X. La première partie des conjectures de Weil prédit que cette fonction est une fraction rationnelle en q^{-s}. La situation est donc bien plus simple que pour $\zeta_\mathbb{Z}$. De plus on sait prouver dans ce contexte l'hypothèse de Riemann. De plus il n'y a aucune raison de se cantonner aux courbes : la fonction ζ_X est définie pour toute variété de type fini X sur $\mathbb{F}_q$ et c'est une fraction rationnelle qui vérifie une équation fonctionnelle et une variante de l'hypothèse de Riemann. La démonstration est due à Grothendieck et Deligne et utilise de manière essentielle la cohomologie étale. Nous traiterons ici le cas d'une courbe elliptique qui est élémentaire. Si l'on connaissait la théorie des variétés abéliennes, et en particulier celle des jacobiennes de courbes, on pourrait de même traiter le cas où X est une courbe projective lisse sur $\mathbb{F}_q$.

Définition 2.10.1. — Soit X une variété de type fini sur $\mathrm{Spec}(\mathbb{F}_q)$. On pose

$$\zeta_X(s) = \prod_{x \in |X|} \frac{1}{1 - N(x)^{-s}}$$

où $|X|$ désigne l'ensemble des points fermés de X, où $k(x)$ est le corps résiduel de x qui est une extension de degré fini de $\mathbb{F}_q$ et $N(x) = \mathrm{Card}(k(x))$ qui est donc une puissance de q.

On considère pour l'instant ζ_X comme un produit formel dépendant de $s \in \mathbb{C}$. Quitte à développer $1/(1-x)$ en série formelle, on peut aussi voir ζ_X comme une série formelle. On verra ses propriétés de convergence dans la proposition 2.10.4. Commençons par voir le lien entre ζ_X et une série génératrice obtenue à partir du nombre de points de X sur $\mathbb{F}_{q^n}$ pour tout $n \geq 1$. Cette série génératrice est concrète mais on perd un peu de vue l'analogie avec $\zeta_{\mathbb{Q}}$.

Proposition 2.10.2. — *On a l'égalité entre séries formelles*

$$\zeta_X(s) \;=\; \exp\left(\sum_{n=1}^{\infty} \mathrm{Card}(X(\mathbb{F}_{q^n})) \cdot \frac{q^{-sn}}{n}\right) .$$

Démonstration. — On utilise le lien entre points fermés et $\bar{\mathbb{F}}_q$-points rappelés dans le paragraphe 2.4. On obtient que pour tout $n \geq 1$, l'ensemble $X(\mathbb{F}_{q^n})$ se partitionne selon le corps de définition des points qui est de la forme $\mathbb{F}_{q^d}$ avec $d|n$. De plus comme $|X| = X(\bar{\mathbb{F}}_q)/\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, tout élément de degré d de $|X|$ définit d éléments de $X(\mathbb{F}_{q^d})$, à savoir son orbite sous le groupe de Galois. On obtient donc $\mathrm{Card}(X(\mathbb{F}_{q^n})) = \sum_{d|n} d \cdot \mathrm{Card}(|X|_d)$ où $|X|_d \subset |X|$ est l'ensemble des points fermés tels que $[k(x) : \mathbb{F}_q] = d$. On a donc

$$\begin{aligned}
\log \zeta_X(s) &= \sum_{n=1}^{\infty} \sum_{x \in |X|} \frac{N(x)^{-ns}}{n} \\
&= \sum_{n=1}^{\infty} \sum_{d=1}^{\infty} \sum_{x \in |X|_d} \frac{q^{-nds}}{n} \\
&= \sum_{N=1}^{\infty} \sum_{d=1}^{\infty} \mathrm{Card}(|X|_d) \cdot d \cdot \frac{q^{-Ns}}{N} \\
&= \sum_{N=1}^{\infty} \mathrm{Card}(X(\mathbb{F}_{q^N})) \cdot \frac{q^{-Ns}}{N}
\end{aligned}$$

□

De même que $\zeta_{\mathbb{Q}}$ peut s'écrire comme somme de Riemann ou comme produit eulérien, on a l'écriture additive suivante de ζ_X.

Lemme 2.10.3. — *On a l'égalité formelle* $\zeta_X(s) = \sum_{D \in \mathrm{Div}(X)} \frac{1}{N(D)^s}$ *où* $N(D) = q^{\deg(D)}$.

Proposition 2.10.4. — *Le produit formel ζ_X converge pour $s \in \mathbb{C}$ tel que $\Re(s) > \dim(X)$ et il définit une fonction holomorphe dans ce domaine.*

Démonstration. — On utilise l'estimation fournie dans la remarque 2.9.2 et les conditions usuelles de convergence des sommes de Riemann. □

Exemple 2.10.5. — Les calculs suivants sont vérifiés

i. Si $X = \mathrm{Spec}(\mathbb{F}_q)$ on a $\zeta_X(s) = 1/(1-q^{-s})$.

ii. Si $X = \mathbb{A}^1_{\mathbb{F}_q}$ on a $\mathrm{Card}(X(\mathbb{F}_{q^n})) = q^n$ et $\zeta_X(s) = 1/(1-q^{1-s})$.

iii. Si $X = \mathbb{A}^d_{\mathbb{F}_q}$ on a $\mathrm{Card}(X(\mathbb{F}_{q^n})) = q^{nd}$ et $\zeta_X(s) = 1/(1-q^{d-s})$.

iv. Si $X = \mathbb{P}^1_{\mathbb{F}_q}$ on a $\mathrm{Card}(X(\mathbb{F}_{q^n})) = 1+q^n$ et $\zeta_X(s) = 1/(1-q^{1-s})(1-q^{-s})$.

v. Si $X = \mathbb{G}_{m,\mathbb{F}_q}$ on a $\mathrm{Card}(X(\mathbb{F}_{q^n})) = q^n - 1$ et $\zeta_X(s) = (1-q^{-s})/(1-q^{1-s})$.

vi. Si $X = U \cup V$ alors $\zeta_X(s) = \zeta_U(s) \cdot \zeta_V(s)/\zeta_{U\cap V}(s)$.

Théorème 2.10.6. — *Soit E une courbe elliptique sur $\mathbb{F}_q$. Notons $a = \phi_q + \hat{\phi}_q \in \mathbb{Z}$. On a*

$$\zeta_E(s) \;=\; \frac{1 - a\cdot q^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$$

qui est en particulier une fraction rationnelle. On a l'équation fonctionnelle

$$\zeta_E(s) \;=\; \zeta_E(1-s)\,.$$

De plus les racines de ζ_E sont de partie réelle $1/2$.

Démonstration. — Soient $\alpha, \beta \in \mathbb{C}$ les racines de $T^2 - aT + q$. On utilise le théorème de Hasse qui garantit que $\mathrm{Card}(E(\mathbb{F}_{q^n})) = 1 + q^n - \alpha^n - \beta^n$. Le fait que les racines de ζ_E sont de partie réelle $1/2$ est équivalent à la borne de Hasse-Weil $|\alpha| = |\beta| = \sqrt{q}$. □

Remarque 2.10.7. — C'est comme on l'a dit à plusieurs reprises la cohomologie étale qui permet de comprendre la structure de toutes les formules précédentes pour ζ_X. Les degrés des polynômes en q^{-s} qui apparaissent sont par exemple égaux aux dimensions de $H^i_c(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$. Ces polynômes apparaissent en numérateur ou en dénominateur selon la parité de i. Ainsi $\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}$ n'a pas de numérateur car

$$H^1_c(\mathbb{P}^1_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = H^1(\mathbb{P}^1_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = 0$$

alors que le numérateur de ζ_E est de degré 2 en q^{-s} car

$$H^1_c(E_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = H^1(E_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \mathrm{Hom}(T_\ell(E), \mathbb{Q}_\ell)$$

est de dimension 2. Si X est une courbe projective lisse de genre g sur $\mathbb{F}_q$ on trouverait que ζ_X a un numérateur polynomial de degré $2g$ en q^{-s} et a $(1-q^{-s})(1-q^{1-s})$ comme dénominateur.

2.11. Endomorphismes et automorphismes

On a prouvé le théorème en TD. Rappelons que si k est de caractéristique nulle, d'après le principe de Lefschetz seul les deux premiers cas peuvent apparaître.

Théorème 2.11.1. — *Soit E une courbe elliptique sur k. Alors l'anneau* $\mathrm{End}(E)$ *est isomorphe soit à $\mathbb{Z}$, soit à un ordre d'un corps quadratique imaginaire, soit à un ordre d'une algèbre de quaternions sur $\mathbb{Q}$.*

Exemple 2.11.2. — Si E est définie par $y^2 = x^3 - x$ sur $k = \mathbb{F}_{p^2}$ avec $p \equiv 3 \bmod 4$. On a vu explicitement en TD que $\mathrm{End}(E)$ est l'anneau non commutatif

$$\mathbb{Z} < I, J > /(I^2 = -1, J^2 = -p)$$

où $I = [i]_E$ est la multiplication complexe et $J = \phi_p$, la relation $\phi_p^2 = [-p]_E$ montrant que $[p]_E$ est purement inséparable donc que E est supersingulière.

Remarque 2.11.3. — Les algèbres de quaternions R sur $\mathbb{Q}$ sont classifiées par une famille $(\mathrm{inv}_v)_v \in \mathbb{Z}/2$ pour toute place v de $\mathbb{Q}$ (c'est à dire un nombre premier ou ∞) tel que $\sum_v \mathrm{inv}_v = 0$. De plus $\mathrm{inv}_v = 0$ si et seulement si $R \otimes_{\mathbb{Q}} \mathbb{Q}_v \simeq \mathrm{Mat}_2(\mathbb{Q}_v)$. Or on a vu en TD que dans le cas quaternionique $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \mathrm{Mat}_2(\mathbb{Q}_\ell)$ pour tout $\ell \neq \infty, p$ si $p = \mathrm{car}(k)$. On en déduit que $\mathrm{inv}_p = \mathrm{inv}_\infty = 1$. En particulier étant donné p seule une algèbre de quaternions apparaît.

Remarque 2.11.4. — Insistons sur le fait que même si k est de caractéristique p, l'anneau $\mathrm{End}(E)$ est sans diviseurs de zéro. C'est n'est donc *pas* une k-algèbre ! On a par exemple $[p]_E \neq 0$ car $[\cdot]_E : \mathbb{Z} \hookrightarrow \mathrm{End}(E)$ est injective.

On déduit du théorème 2.11.1 la proposition suivante par classification explicite des éléments inversibles des ordres d'algèbres de quaternions.

Proposition 2.11.5. — *Soit k un corps algébriquement clos et E une courbe elliptique sur k.*

i. $\mathrm{Aut}(E)$ *est de cardinal 2 (donc est égal $[\pm 1]_E$) si $j(E) \neq 0, 1728$.*

ii. $\mathrm{Aut}(E)$ *est de cardinal 4 si $j(E) = 1728$ et $\mathrm{car}(k) \neq 2, 3$.*

iii. $\mathrm{Aut}(E)$ *est de cardinal 6 si $j(E) = 0$ et $\mathrm{car}(k) \neq 2, 3$.*

iv. $\mathrm{Aut}(E)$ *est de cardinal 12 si $j(E) = 1728 = 0$ et $\mathrm{car}(k) = 3$.*

v. $\mathrm{Aut}(E)$ *est de cardinal 24 si $j(E) = 1728 = 0$ et $\mathrm{car}(k) = 2$.*

On peut maintenant faire un lien entre supersingularité et endomorphismes quaternioniques.

Proposition 2.11.6. — *Soit k un corps de caractéristique p et E une courbe elliptique sur k. Alors E est supersingulière si et seulement* $\mathrm{End}_{\bar{k}}(E)$ *est un ordre d'une algèbre de quaternions sur* $\mathbb{Q}$.

Démonstration. — On se ramène au cas où k est algébriquement clos quitte à remplacer k par $\bar{k}$, ce qui ne change pas le fait d'être supersingulier.

On suppose que E est ordinaire et on montre que $\mathrm{End}(E)$ est commutatif. Comme E est ordinaire on a $T_p(E) \neq 0$ et en fait $T_p(E) = \mathbb{Z}_p$. On dispose d'un morphisme $\mathrm{End}(E) \to \mathrm{End}_{\mathbb{Z}_p}(T_pE)$, $f \mapsto f_p$. De plus ce morphisme est injectif car si $f_p = 0$ alors f est nulle sur $E[p^n](k)$ pour tout $n \geq 1$. Cela contredit le fait que si $f \neq 0$ alors f est une isogénie donc $\ker(f)$ est fini. On conclut car $\mathrm{End}_{\mathbb{Z}_p}(T_pE) \simeq \mathbb{Z}_p^*$ est commutatif.

On admet l'assertion réciproque qui est un peu plus longue à démontrer. Voir **[Si**, th.V.3.1]. □

Remarque 2.11.7. — Si E est supersingulière on n'a pas dit que $\mathrm{End}(E)$ est un ordre d'une algèbre de quaternion. Par exemple on peut prendre $k = \mathbb{F}_p$ et E définir par l'équation $y^2 = x^3 - x$. Elle n'acquiert pas sa multiplication complexe sur k mais seulement sur $\mathbb{F}_{p^2}$. On a donc $\mathrm{End}(E) = \mathbb{Z}[\phi_p] = \mathbb{Z}[\sqrt{-p}]$.

Cela nous permet de revenir sur la courbe E définie par l'équation $y^2 = x^3 - x$ sur $k = \mathbb{Z}[i]/p \xrightarrow{\sim} \mathbb{F}_{p^2}$ lorsque $p \equiv 3 \bmod 4$. Rappelons que, même si nous l'avons mentionné à plusieurs reprises, nous n'avons jamais prouvé que $\phi_p^2 = [-p]_E$ ni que E est supersingulière.

On raisonne de la manière suivante. On a $\deg(\phi_p) = p$. Or pour tout $x \in \mathbb{Z}[i]$ on a $\deg([x]_E) = N_{\mathbb{Q}(i)/\mathbb{Q}}(x)$. En effet $\deg : \mathbb{Z}[i] \to \mathbb{N}$ et $N_{\mathbb{Q}(i)/\mathbb{Q}} : \mathbb{Z}[i] \to \mathbb{N}$ sont deux formes quadratiques qui coïncident sur $\mathbb{Z}$ et sur i. Mais il n'existe aucun $x \in \mathbb{Z}[i]$ de norme p. En effet l'idéal $x \cdot \mathbb{Z}[i]$ serait alors premier contenu strictement dans $p \cdot \mathbb{Z}[i]$, ce qui contredit le fait que p est inerte dans $\mathbb{Z}[i]$. De manière équivalente, si $x = u + vi$ avec $u, v \in \mathbb{Z}$ on aurait $p = u^2 + v^2$ ce qui contredit l'hypothèse $p \equiv 3 \bmod 4$ par analyse explicite des sommes de carrés modulo 4. Donc $\phi_p \in \mathrm{End}(E) - \mathbb{Z}[i]$. Or $\mathbb{Z}[i]$ est un ordre maximal de $\mathbb{Q}(i)$ (c'est vrai pour tout anneau d'entier d'un corps de nombres) puisqu'il est intégralement clos. Donc $\mathrm{End}(E)$ n'est pas un ordre d'un corps quadratique imaginaire. Donc $\mathrm{End}(E)$ est un ordre d'une algèbre de quaternions et E est supersingulière d'après la proposition 2.11.6.

Remarque 2.11.8. — On verra en TD une autre manière de prouver que E est supersingulière.

On en déduit d'après la définition de la supersingularité que $\hat{\phi}_p$ est purement inséparable puis que $\hat{\phi}_p = u \circ \phi_p$ pour $u \in \mathrm{Aut}(E)$. On a donc $\phi_p^2 = [p]_E \circ u^{-1}$. Il reste à prouver que $u = [-1]_E$. Supposons pour simplifier $p > 3$. Dans ce cas $\mathrm{Aut}(E)$ est un groupe de cardinal 4 par la proposition 2.11.5 car $j(E) = 1728$. On a donc $u = [\pm 1]_E$ ou $u = [\pm i]_E$.

Mais rappelons en général que $\phi_p + \hat{\phi}_p \in \mathbb{Z} \subset \mathrm{End}(E)$. Donc $\phi_p \circ (1+u) = n \in \mathbb{Z}$. Donc $n^2 = \deg(\phi_p) \cdot |1+u| = p \cdot |1+u|$. La seule possibilité est $u = [-1]$!

Remarque 2.11.9. — On aurait pu argumenter de la même manière pour toute courbe elliptique supersingulière E sur $\mathbb{F}_p$ telle que $j(E) \neq 0, 1728$ si $p \neq 2, 3$. On en déduit $\phi_p^2 = [-p]_E$ car $\hat{\phi}_p = [-1]_E \circ \phi_p$. C'est même plus facile car $u \in \mathrm{Aut}(E) = \{[\pm 1]_E\}$. C'est en fait vrai quelque soit le j-invariant, voir [**Si**, exo.V.5.16]

BIBLIOGRAPHIE

[Ne] J. Nekovar, *Algebraic theory of elliptic curves*, cours de M2, disponible sur sa page web.

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, volume 106 of Graduate Texts in Mathematics, Springer.