ÉCOLE POLYTECHNIQUE.

ENSEIGNEMENT D'APPROFONDISSEMENT.

Théorème du relèvement canonique de Deuring.

Pierrick Dartois.

Ce mémoire est la continuité de mon sujet de PSC qui portait sur l'étude de l'algorithme de Satoh pour le comptage des points rationnels des courbes elliptiques définies sur $\mathbb{F}_q$. Étant donné une courbe ordinaire E définie sur $\mathbb{F}_q$ et une extension non ramifiée de $\mathbb{Q}_p$ de corps résiduel $\mathbb{F}_q$, notée $\mathbb{Q}_q$, cet algorithme relève E dans $\mathbb{Q}_q$. Dans une courbe $\tilde{E}$ ainsi obtenue, Satoh calcule la trace du morphisme de Frobenius de E relevé sur $\tilde{E}$ pour en déduire $|E(\mathbb{F}_q)|$ à l'aide du théorème de Hasse. L'article originel de Satoh ([1]) admet donc le résultat suivant dû à Deuring :

Toute courbe ordinaire $E/\mathbb{F}_q$ peut-être relevée en $\tilde{E}/\mathbb{Q}_q$ de telle sorte que la réduction modulo p induise un isomorphisme $\mathrm{End}(\tilde{E}) \simeq \mathrm{End}(E)$.

Le but de ce mémoire est de prouver ce résultat en introduisant tous les outils théoriques nécessaires.

Étant donné la difficulté du théorème, et la propension de l'auteur à l'exhaustivité des preuves, ce document est malheureusement assez long. Pour en faciliter la lecture, les résultats principaux sont encadrés :

— En rouge pour les plus importants, qui font figure de conclusion d'un chapitre ou d'une partie.
— En bleu pour les résultats centraux.
— En noir pour les résultats intermédiaires importants ou difficiles mais pas centraux.

Pour distinguer les nouveaux résultats de ceux qui ont déjà été prouvés en PSC, nous avons annoté les résultats et parties qui ont été intégralement ou partiellement repris par la mention entre parenthèse (PSC). Les développements les plus techniques ou les plus périphériques ont été mis en annexe. On y trouvera notamment des compléments d'algèbre commutative et de théorie algébrique des nombres utiles et qui n'ont pas été vus ou approfondis dans le cours de Gaëtan Genevier [10]. On s'y réfèrera librement tout au long de ce rapport, notamment au cours des preuves.

Table des matières

Chapitre 1

L'anneau des endomorphismes d'une courbe elliptique.

Dans tout ce chapitre, K est un corps de caractéristique différente de 2 ou 3 et $\overline{K}$ désigne une clôture algébrique de K. E, E_1, E_2 et E_3 sont des courbes elliptiques sur K de polynômes de Weierstrass respectifs $W(X,Y) := Y^2 - X^3 - aX - b$, $W_1(X,Y) := Y^2 - X^3 - a_1X - b$... On notera $\mathcal{O}$, $\mathcal{O}_1$, $\mathcal{O}_2$ et $\mathcal{O}_3$ leurs points à l'infini respectifs.

1.1 Morphisme dual (PSC).

1.1.1 Définition.

On commence par généraliser la formule de la proposition 6.10 du cours [3] pour obtenir une formule plus manipulable sur le degré des morphismes.

Définition 1.1.1.1. *On appelle* morphisme généralisé *entre deux courbes elliptiques E_1 et E_2 une application $\phi : E_1 \longrightarrow E_2$ telle qu'il existe $f, g \in \overline{K}(E_1)$ vérifiant $W_2(f,g) = 0$ et tels qu'en tout point $P \in E_1$ où f et g sont définies, on ait :*

$$\phi(P) := (f(P), g(P))$$

et $\phi(P) = \mathcal{O}_2$ sinon.

Exemple 1.1.1.2. Un morphisme est un morphisme généralisé. En outre, la formule d'addition des points assure aussi que pour tout $P \in E$ la translation :

$$\tau_P : Q \in E \longmapsto P + Q \in E$$

est un morphisme généralisé. Ce n'est pas un morphisme sauf lorsque $P = \mathcal{O}$ puisque $\tau_P(\mathcal{O}) = P$. C'est en fait la raison d'être de cette définition.

E_2 est une courbe elliptique donc une courbe projective plane. La proposition 4.12 du cours s'applique alors et assure que l'anneau $K[E_2]_Q$ des fonctions rationnelles définies en Q est un anneau de valuation discrète pour tout $Q \in E_2$. On peut donc considérer des uniformisantes en Q et définir l'ordre en Q des fonctions rationnelles.

Remarquons que si $f \in \overline{K}(E_2)$ et si $\phi : E_1 \longrightarrow E_2$ un morphisme généralisé non constant alors $f \circ \phi \in \overline{K}(E_1)$. En outre, si $r_{\phi(P)}$ et $s_{\phi(P)}$ sont des uniformisantes en $\phi(P)$ alors $s_{\phi(P)} = r_{\phi(P)}g$ avec $g \in \overline{K}(E_2)$ dont $\phi(P)$ n'est ni zéro ni pôle donc :

$$\mathrm{ord}_P(s_{\phi(P)} \circ \phi) = \mathrm{ord}_P(g \circ \phi) + \mathrm{ord}_P(r_{\phi(P)} \circ \phi) = \mathrm{ord}_P(r_{\phi(P)} \circ \phi)$$

Ce qui donne un sens à la définition suivante :

Définition 1.1.1.3. *Soient $\phi : E_1 \longrightarrow E_2$ un morphisme généralisé non constant et $P \in E_1$. On définit* l'indice de ramification *de ϕ en P par :*

$$e_\phi(P) := ord_P(r_{\phi(P)} \circ \phi)$$

où $r_{\phi(P)}$ est une uniformisante quelconque en $\phi(P)$.

On obtient aisément les propriétés élémentaires suivantes sur l'indice de ramification.

Proposition 1.1.1.4 (propriétés de l'indice de ramification)**.** *Soient $\phi : E_1 \longrightarrow E_2$, $\psi : E_2 \longrightarrow E_3$ des morphismes généralisés non constants, $P, Q \in E_1$ et $f \in \overline{K}(E_2)$. Alors :*

(i) $ord_P(f \circ \phi) = ord_{\phi(P)}(f)e_\phi(P)$.

(ii) $e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(\phi(P))$.

(ii) *En notant $\tau_Q : P \in E_1 \longmapsto P + Q \in E_1$ la translation de Q, on a $e_{\tau_Q}(P) = 1$ et donc par (i). :*

$$ord_P(f \circ \tau_Q) = ord_{P+Q}(f)$$

Démonstration. Pour (i), on écrit $f = ur^n$ avec r une uniformisante en $\phi(P)$, $u \in K(E_2)$ dont $\phi(P)$ n'est ni zéro ni pôle et $n := \mathrm{ord}_{\phi(P)}(f)$. Vu que $\mathrm{ord}_P(u \circ \phi) = 0$ (puisque $\phi(P)$ n'est ni zéro ni pôle de u), on obtient alors :

$$\mathrm{ord}_P(f \circ \phi) = \mathrm{ord}_P((u \circ \phi)(r \circ \phi)^n) = \mathrm{ord}_P(u \circ \phi) + n\mathrm{ord}_P(r \circ \phi) = \mathrm{ord}_{\phi(P)}(f)e_\phi(P)$$

(ii) est une conséquence de (i) en prenant $f := r \circ \psi$ avec r une uniformisante en $\psi \circ \phi(P)$.

Pour (iii), il suffit de vérifier que $e_{\tau_Q}(P) = 1$ i.e. que $\mathrm{ord}_P(r_{\tau_Q(P)} \circ \tau_Q) = 1$, lorsque $r_{\tau_Q(P)}$ est une uniformisante en $\tau_Q(P)$, ce qui est trivialement vérifié. □

Proposition 1.1.1.5. *Si $\phi : E_1 \longrightarrow E_2$ est une isogénie alors $e_\phi(P)$ est indépendant du point $P \in E_1$ choisi. On peut donc noter e_ϕ l'indice de ramification d'un morphisme, indépendamment du point.*

Démonstration. On sait qu'alors pour tous $P, Q \in E, \phi(P + Q) = \phi(P) + \phi(Q)$, ce qui donne :

$$\forall P \in E, \quad \phi \circ \tau_P = \tau_{\phi(P)} \circ \phi$$

et donc pour tous $P \in E$, $e_{\phi\circ\tau_P}(\mathcal{O}) = e_{\tau_{\phi(P)}\circ\phi}(\mathcal{O})$. Or, d'après les points (ii) et (iii) de la proposition précédente :

$$e_{\phi\circ\tau_P}(\mathcal{O}) = e_\phi(\tau_P(\mathcal{O}))e_{\tau_P}(\mathcal{O}) = e_\phi(P)$$

Et :

$$e_{\tau_{\phi(P)}\circ\phi}(\mathcal{O}) = e_{\tau_{\phi(P)}}(\phi(P))e_\phi(\mathcal{O}) = e_\phi(\mathcal{O})$$

Donc $e_\phi(P) = e_\phi(\mathcal{O})$ et ce pour tout $P \in E$. □

Remarque 1.1.1.6. On pourrait montrer cela pour tout morphisme généralisé non constant mais ce ne sera pas nécessaire. C'est par ailleurs un résultat non trivial qui utilise le fait que tout morphisme généralisé qui envoie le point à l'infini sur le point à l'infini est un morphisme.

Maintenant que l'indice de ramification est bien compris, voici donc la généralisation de la proposition 6.10 tant attendue.

Proposition 1.1.1.7. *Soit $\phi : E_1 \longrightarrow E_2$ une isogénie. Alors :*

$$deg(\phi) = e_\phi|ker(\phi)|$$

Démonstration. Écrivons ϕ sous forme canonique $\phi(X,Y) := (r(X), Ys(X))$ avec $r, s \in K(X)$. ϕ est alors surjectif (d'après la proposition 6.11 du cours). E_1 et E_2 étant infinis, le nombre de points d'ordonnée nulle sur une courbe elliptique étant au plus 3 et $r \neq 0$ ne prenant la même valeur qu'un nombre fini de fois, on dispose donc de $P \in E_1 \setminus \{\mathcal{O}_1\}$ d'ordonnée non nulle tel que $\phi(P)$ est distinct de $\mathcal{O}_2$, d'ordonnée non nulle et tel que $\deg(p(X) - r(x_P)q(X)) = \max(\deg(p), \deg(q)) = \deg(\phi)$ (en ayant écrit $r := \frac{p}{q}$ avec $p, q \in K[X]$ premiers entre eux). Dans ce cas, il est aisé de voir que $X - r(x_P)$ est une uniformisante en $\phi(P)$ (cf. exercice 6.1.a. ou la proposition II.19 de [4] pour une preuve complète). On en déduit que :

$$e_\phi = \mathrm{ord}_P(r(X) - r(x_P))$$

Alors x_P n'est pas racine de q puisque $\phi(P) \neq \mathcal{O}$. Il s'ensuit que e_ϕ est la multiplicité de x_P comme racine de $p(X) - r(x_P)q(X)$.

En outre, $Q := (x, y) \in E_1$ vérifie $\phi(Q) = \phi(P)$ si et seulement si :

$$r(x) = r(x_P) \quad \text{et} \quad s(x)y = s(x_P)y_P$$

Mais si $r(x) = r(x_P)$ i.e. $p(x) - r(x_P)q(x) = 0$ alors l'équation de Weierstrass de E_2 donne que $s(x)y = \pm s(x_P)y_P \neq 0$ donc $s(x) \neq 0$. Si de plus, $\phi(Q) = \phi(P)$, alors nécessairement $y = \frac{s(x_P)y_P}{s(x)}$. Il y a donc autant de racines de $p(X) - r(x_P)q(X)$ que d'éléments de $\phi^{-1}(\phi(P))$. Mais $|\phi^{-1}(\phi(P))| = |\phi^{-1}(\mathcal{O}_2)| = |\ker(\phi)|$ puisque ϕ est un morphisme de groupes. Donc le nombre de racines de $p(X) - r(x_P)q(X)$ vaux $|\ker(\phi)|$.

Enfin, si $Q := (x_Q, y_Q) \in \phi^{-1}(\phi(P))$ alors $\phi(Q) = \phi(P)$ est distinct de $\mathcal{O}_2$ est d'ordonnée non-nulle donc on obtient de même que :

$$e_\phi = \mathrm{ord}_Q(r(X) - r(x_Q)) = \mathrm{ord}_Q(r(X) - r(x_P))$$

qui est la multiplicité de x_Q en tant que racine de $p(X) - r(x_P)q(X)$. Ainsi, toutes les racines de $p(X) - r(x_P)q(X)$ ont même multiplicité égale à e_ϕ, de sorte que :

$$\deg(\phi) = \deg(p(X) - r(x_P)q(X)) = |\ker(\phi)|e_\phi$$

□

Remarque 1.1.1.8. On déduit immédiatement de la proposition précédente et de la proposition 6.10 de [3] assurent que si $\phi : E_1 \longrightarrow E_2$ une isogénie, alors ϕ est séparable si et seulement si $e_\phi = 1$.

Corollaire 1.1.1.9. *Soient $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_2, E_3)$ des isogénies. Alors :*

$$deg(\psi \circ \varphi) = deg(\psi)deg(\varphi)$$

Démonstration. On a $e_{\psi\circ\varphi} = e_\psi e_\varphi$ d'après les propriétés des indices de ramification. En outre :

$$\ker(\psi \circ \varphi) = \bigsqcup_{P \in \ker(\psi)} \varphi^{-1}(\{P\})$$

Or, $|\varphi^{-1}(\{P\})| = |\ker(\varphi)|$ car φ est un morphisme de groupes. Ainsi $|\ker(\psi \circ \varphi)| = |\ker(\varphi)||\ker(\psi)|$ donc $\deg(\psi \circ \varphi) = \deg(\psi)\deg(\varphi)$. □

Corollaire 1.1.1.10. *Supposons que $p := car(K) > 0$. Alors tout isognénie $\varphi : E_1 \longrightarrow E_2$ est de la forme $\varphi = \psi \circ \phi_{p^n}$ avec :*

$$\phi_{p^n} : [x : y : z] \in E_1 \longmapsto [x^{p^n} : y^{p^n} : z^{p^n}] \in E_1^{(p^n)}$$

le n-ième morphisme de Forbenius, $E_1^{(p^n)}$ étant la courbe elliptique d'équation de Weierstrass : $Y^2 = X^3 + a_1^{p^n}X + b^{p^n}$ et $\psi \in Hom(E_1^{(p^n)}, E_2)$ séparable.

Démonstration. On raisonne par récurrence sur e_φ. Si $e_\varphi = 1$ alors φ est séparable et il n'y a rien à prouver.

Supposons donc que $e_\varphi > 1$. Alors φ est inséparable. Écrivons-le sous forme normale $\varphi(X,Y) = (r_1(X), Ys_1(X))$. En multipliant l'ordonnée par $1 = \left(\frac{Y^2}{X^3+a_1X+b_1}\right)^{\frac{p-1}{2}}$, on peut en fait écrire :

$$\varphi(X,Y) = (r_1(X), Y^p s_2(X))$$

Posons $r_1(X) = \frac{p_1(X)}{q_1(X)}$ avec $p_1, q_1 \in K[X]$ premiers entre eux. On a par inséparabilité de φ :

$$0 = r_1'(X) = \frac{p_1'(X)q_1(X) - p_1(X)q_1'(X)}{q_1(X)^2}$$

Donc $p_1'(X)q_1(X) = p_1(X)q_1'(X)$ donc, comme p_1 et q_1 sont premiers entre eux, le théorème de Gauss donne que q_1 divise q_1' et que p_1 divise p_1', donc que $p_1' = q_1' = 0$ (pour raison de degré). Donc $p_1(X) = p(X^p)$ et $q_1(X) = q(X^p)$ avec $p, q \in K[X]$, puis $r_1(X) = r(X^p)$ avec $r := \frac{p}{q}$.

Or, $(Y^p s_2(X))^2 = r(X^p)^3 + Ar(X^p) + B$ donc :

$$s_2(X)^2 = \frac{r(X^p)^3 + a_2r(X^p) + b_2}{Y^{2p}} = \frac{r(X^p)^3 + a_2r(X^p) + b_2}{(X^3 + a_1X + b_1)^p} = \frac{r(X^p)^3 + a_2r(X^p) + b_2}{X^{3p} + a_1^pX^p + b_1^p}$$

Donc $s_2(X)^2$ est une fraction rationnelle en X^p, que l'on écrit $s_2(X) = s(X^p)$ avec :

$$s := \frac{r(X)^3 + a_2r(X) + b_2}{X^3 + a_1^pX + b_1^p}$$

Donc $\varphi(X,Y) = (r(X^p), Y^p s(X^p))$, puis $\varphi = \psi \circ \phi_p$ où ψ est l'isogénie définie sur $E_1^{(p)}$ par $\psi(X,Y) := (r(X), Ys(X))$.

Or, ϕ_p est de degré p est de noyau trivial donc $e_{\phi_p} = p$ d'après la proposition 1.1.1.7. Par multiplicativité des indices de ramifications, on obtient alors $e_\psi = \frac{e_\varphi}{p}$ et on conclut par hypothèse de récurrence. □

Théorème 1.1.1.11. *Si $\varphi \in Hom(E_1, E_2)$ est une isogénie alors il existe $\hat{\varphi} \in Hom(E_2, E_1)$ une isogénie telle que :*

$$\varphi \circ \hat{\varphi} = [deg(\varphi)]_{E_2} \quad et \quad \hat{\varphi} \circ \varphi = [deg(\varphi)]_{E_1}$$

Ce morphisme est unique lorsque φ est non nul et il est donné par la formule :

$$\hat{\varphi}(P) = [e_\varphi]\left(\sum_{Q \in \varphi^{-1}(\{P\})} Q - \sum_{R \in \varphi^{-1}(\{\mathcal{O}_2\})} R\right)$$

pour tout $P \in E_2$. $\hat{\varphi}$ est appelé morphisme dual *de φ.*

Remarque 1.1.1.12. On peut bien sûr définir le morphisme dual du morphisme nul par $\hat{0} := 0$.

Démonstration. Pour démontrer l'existence, on vérifie simplement que la formule précédente convient. Soit $P \in E_2$. Alors comme φ est un morphisme de groupes :

$$\begin{aligned}\varphi \circ \hat{\varphi}(P) &= [e_\varphi]\left(\sum_{Q \in \varphi^{-1}(\{P\})} \varphi(Q) - \sum_{R \in \varphi^{-1}(\{\mathcal{O}_2\})} \varphi(R)\right) = [e_\varphi]\left(\sum_{Q \in \varphi^{-1}(\{P\})} P - \sum_{R \in \varphi^{-1}(\{\mathcal{O}_2\})} \mathcal{O}_2\right) \\ &= [e_\varphi] \circ [|\varphi^{-1}(\{P\})|](P) = [e_\varphi] \circ [|\ker(\varphi)|](P) = [e_\varphi|\ker(\varphi)|](P) \\ &= [\deg(\varphi)]P\end{aligned}$$

Et si $P \in E_1$, alors comme $Q - P$ décrit $\varphi^{-1}(\{\mathcal{O}_2\})$ quand Q décrit $\varphi^{-1}(\{\varphi(P)\})$:

$$\hat{\varphi} \circ \varphi(P) = [e_\varphi] \left(\sum_{Q \in \varphi^{-1}(\{\varphi(P)\})} Q - \sum_{R \in \varphi^{-1}(\{\mathcal{O}_2\})} R \right) = [e_\varphi] \left(\sum_{Q \in \varphi^{-1}(\{\varphi(P)\})} Q - \sum_{Q \in \varphi^{-1}(\{\varphi(P)\})} (Q - P) \right)$$
$$= [e_\varphi] \circ [|\varphi^{-1}(\{\varphi(P)\})|](P) = [\deg(\varphi)]P$$

D'où l'existence.

Pour l'unicité, il suffit de remarquer que si $\hat{\varphi}'$ vérifie les mêmes hypothèses que $\hat{\varphi}$ alors $(\hat{\varphi}' - \hat{\varphi}) \circ \varphi = 0$ donc que $\hat{\varphi} - \hat{\varphi}' = 0$ puisque φ est surjective lorsque φ est non nulle. □

On obtient un corollaire immédiat de l'existence du morphisme dual :

Corollaire 1.1.1.13. *Soit $\varphi : E_1 \longrightarrow E_2$ une isogénie. Posons $p := car(K)$. Si $p \nmid deg(\varphi)$, alors φ est séparable.*

Démonstration. On a $\varphi \circ \hat{\varphi} = [\deg(\varphi)]$ donc par multiplicativité de l'indice de ramification :

$$e_\varphi e_{\hat{\varphi}} = e_{[\deg(\varphi)]}$$

Mais $p \nmid \deg(\varphi)$ donc $[\deg(\varphi)]$ est séparable et $e_{[\deg(\varphi)]} = 1$ d'après le corollaire 6.16 de [3]. Il s'ensuit que $e_\varphi = 1$, puis que φ est séparable. □

1.1.2 Accouplement de Weil.

On introduit ici l'accouplement de Weil comme un outil de calcul qui nous sera utile pour démontrer certaines propriétés du morphisme dual. En raison de la technicité des preuves, nous renvoyons le lecteur à l'annexe A.2.1 pour une preuve de ces résultats.

Fixons $n \geq 2$ non divisible par $\mathrm{car}(K)$ et notons μ_n l'ensemble des racines n-ièmes de l'unité de $\overline{K}$. Comme $\mathrm{car}(K)$ ne divise pas n, $X^n - 1$ est séparable donc μ_n est de cardinal n.

Théorème 1.1.2.1. *Il existe une application $e_n : E[n]^2 \longrightarrow \mu_n$ appelée* accouplement de Weil *et vérifiant les propriétés suivantes :*

(i) *e_n est bilinéaire :*

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q) \quad \text{et} \quad e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2)$$

pour tous $P, P_1, P_2, Q, Q_1, Q_2 \in E[n]$.

(ii) *e_n est alternée $e_n(P, P) = 1$ pour tout $P \in E[n]$ et $e_n(P, Q) = e_n(Q, P)^{-1}$ pour tous $P, Q \in E[n]$.*

(iii) *e_n est non-dégénérée $e_n(P, Q) = 1$ pour tout $P \in E[n]$ si et seulement si $Q = \mathcal{O}$.*

1.1.3 Propriétés du morphisme dual.

A partir des propriétés de l'accouplement de Weil, on peut montrer les propriétés suivantes du morphisme dual. En raison de la technicité des preuves, nous renvoyons à l'annexe A.2.2 pour une preuve détaillée.

Proposition 1.1.3.1. *Soit $\varphi \in Hom(E_1, E_2)$, $\psi \in Hom(E_2, E_3)$ des morphismes. Alors :*

(i) $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$.

(ii) *Si $car(K)$ ne divise pas n alors φ et $\hat{\varphi}$ sont adjointes pour l'accouplement de Weil e_n :*

$$\forall (P, Q) \in E_1[n] \times E_2[n], \quad e_n(\varphi(P), Q) = e_n(P, \hat{\varphi}(Q))$$

(iii) $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\varphi}$.

(iv) $\widehat{[n]} = [n]$ *et* $deg[n] = n^2$ *pour tout* $n \in \mathbb{N}$.

(v) $deg(\hat{\varphi}) = deg(\varphi)$.

(vi) $\hat{\hat{\varphi}} = \varphi$.

1.1.4 Retour au degré.

Nous avons commencé par quelques considérations sur le degré pour construire le morphisme dual. En fait, réciproquement, le morphisme dual nous permet de comprendre le degré et en particulier de montrer que c'est une forme quadratique.

Définition 1.1.4.1. *Soit $(A, +)$ un groupe abélien. Une* forme quadratique sur A *est une application $q : A \longrightarrow \mathbb{R}$ telle que :*

(i) *q est symétrique :* $\forall a \in A, \quad q(a) = q(-a)$.

(ii) *L'application :*

$$B : (a, b) \in A^2 \longmapsto q(a + b) - q(a) - q(b) \in \mathbb{R}$$

est $\mathbb{Z}$-bilinéaire.

q est dite définie positive *si pour tout $a \in A$, $q(a) \geq 0$ avec égalité si et seulement si $a = 0$.*

Proposition 1.1.4.2. *$deg : Hom(E_1, E_2) \longrightarrow \mathbb{Z}$ est une forme quadratique définie positive.*

Démonstration. Les points (i) et (iii) de la définition ci-dessus sont clairs d'après la 1.1.1.7. Le point (ii) découle des propriétés de l'isogénie duale (proposition 1.1.3.1, point (iii)). En effet, si $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$ et si $\langle ., . \rangle$ est l'accouplement associé à deg alors :

$$\begin{aligned}[\langle \varphi, \psi \rangle] &= [\deg(\varphi + \psi)] - [\deg(\varphi)] - [\deg(\psi)] = (\varphi + \psi) \circ \widehat{(\varphi + \psi)} - \varphi \circ \hat{\varphi} - \psi \circ \hat{\psi} \\ &= (\varphi + \psi) \circ (\hat{\varphi} + \hat{\phi}) - \varphi \circ \hat{\varphi} - \psi \circ \hat{\psi} = \varphi \circ \hat{\psi} + \hat{\varphi} \circ \psi\end{aligned}$$

Et cette expression est clairement $\mathbb{Z}$-bilinéaire (d'après les points (iii) et (iv) de la proposition 1.1.3.1). □

1.2 Module de Tate.

Dans ce paragraphe nous introduisons un outil qui permet de voir les morphismes entre courbes elliptiques comme morphismes entre modules, objets mieux compris. Nous verrons que cela présente un intérêt dans l'étude de la structure de $\mathrm{Hom}(E_1, E_2)$.

On supposera que le lecteur est familier des limites projectives et des nombres p-adiques étudiés en détail dans le cours de représentation des groupes compacts MAT 563 (voir [5], exercice 2.10) et sur lesquels nous ferons de brefs rappels.

Définition 1.2.0.1. *On appelle* système projectif *une suite $(G_n, f_n)_{n \geq 1}$ telle que :*

(i) *Pour tout $n \in \mathbb{N}^*$, G_n est un groupe.*

(ii) *Pour tout $n \in \mathbb{N}^*$, $f_n : G_{n+1} \longrightarrow G_n$ est un morphisme de groupes.*

On appelle limite projective *de* $(G_n, f_n)_{n\geq 1}$ *et on note* $\varprojlim G_n$ *le sous-groupe de* $\prod_{n\in\mathbb{N}^*} G_n$ *donné par :*

$$\left\{(x_n)_{n\geq 1} \in \prod_{n\in\mathbb{N}^*} G_n \mid \forall n \in \mathbb{N}^*, \quad f_n(x_{n+1}) = x_n\right\}$$

Dans tout ce paragraphe, ℓ désignera un nombre premier. Pour tout $n \in \mathbb{N}^*$:

$$\begin{array}{rccc} g_n : \mathbb{Z} & \longrightarrow & \mathbb{Z}/\ell^n\mathbb{Z} \\ x & \longmapsto & x\ [\ell^n] \end{array}$$

s'annulle sur $\ell^{n+1}\mathbb{Z}$ donc induit un morphisme de groupes $f_n : \mathbb{Z}/\ell^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$ par propriété universelle du quotient. L'ensemble des *entiers* ℓ*-adiques* $\mathbb{Z}_\ell$ est la limite projective de $(\mathbb{Z}/\ell^n\mathbb{Z}, f_n)_{n\geq 1}$:

$$\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} = \left\{(x_n)_{n\geq 1} \in \prod_{n\in\mathbb{N}^*} \mathbb{Z}/\ell^n\mathbb{Z} \mid \forall n \in \mathbb{N}^*, \quad x_{n+1} \equiv x_n\ [\ell^n]\right\}$$

Pour tout $n \in \mathbb{N}^*$, on considère $E[\ell^n]$ l'ensemble des points de ℓ^n-torsions de E et le morphisme :

$$f_n : P \in E[\ell^{n+1}] \longmapsto [\ell]P \in E[\ell^n]$$

Définition 1.2.0.2. *On appelle* module de Tate ℓ-adique *de* E *et on note* $T_\ell(E)$ *la limite projective de* $(E[\ell^n], f_n)_{n\geq 1}$ *:*

$$T_\ell(E) = \varprojlim E[\ell^n] = \left\{(P_n)_{n\geq 1} \in \prod_{n\in\mathbb{N}^*} E[\ell^n] \mid \forall n \in \mathbb{N}^*, \quad P_{n+1} = [\ell]P_n\right\}$$

Proposition 1.2.0.3 (PSC)**.** *$T_\ell(E)$ est muni d'une structure naturelle de $\mathbb{Z}_\ell$-module libre de rang :*

(i) 2 *si $\ell \neq car(K)$.*

(ii) 1 *si $\ell = car(K)$ et si E n'est pas supersingulière.*

(iii) 0 *si $\ell = car(K)$ et si E est supersingulière.*

Démonstration. La structure de $\mathbb{Z}_\ell$-module est donnée par :

$$\forall (x_n)_{n\geq 1} \in \mathbb{Z}_\ell,\ (P_n)_{n\geq 1} \in T_\ell(E) \quad (x_n)_{n\geq 1} \cdot (P_n)_{n\geq 1} := ([x_n]P_n)_{n\geq 1}$$

La bonne définition de cette structure se vérifie assez facilement. Elle tient essentiellement au fait que pour $n \in \mathbb{N}^*$ $P \in E[\ell^n]$ et $x \in \mathbb{Z}$, $[x]P$ ne dépend que de x modulo ℓ^n.

(i) Supposons $\ell \neq \text{car}(K)$. Alors la proposition 6.17 du polycopié de cours [3] assure que $E[\ell]$ est un $\mathbb{Z}/\ell\mathbb{Z}$-espace vectoriel de dimension 2. Soit donc (P_1, Q_1) une $\mathbb{Z}/\ell\mathbb{Z}$-base de $E[\ell]$. $[\ell]$ étant surjective (d'après la proposition 6.11 de [3]), on peut alors définir des suites $P := (P_n)_{n\geq 1}$ et $Q := (Q_n)_{n\geq 1}$ telles que $P_n = [\ell]P_{n+1}$ et $Q_n = [\ell]Q_{n+1}$ pour tout $n \in \mathbb{N}^*$.

(P, Q) est libre sur $\mathbb{Z}_\ell$ car une relation de liaison entre P et Q sur $\mathbb{Z}_\ell$ donnerait une relation de liaison entre P_1 et Q_1 sur $\mathbb{Z}/\ell\mathbb{Z}$, ce qui est exclus.

Il s'agit maintenant de montrer que (P, Q) est génératrice. On fixe $R := (R_n)_{n\geq 1} \in T_\ell(E)$. On construit par récurrence sur $n \in \mathbb{N}^*$ des suites $(x_n)_{n\geq 1}, (y_n)_{n\geq 1} \in \mathbb{Z}_\ell$ vérifiant $R_n = [x_n]P_n + [y_n]Q_n$.

L'existence de $(x_1, y_1) \in \mathbb{Z}/\ell\mathbb{Z}^2$ convenable est assurée par le caractère $\mathbb{Z}/\ell\mathbb{Z}$-générateur de (P_1, Q_1) dans $E[\ell]$.

Soit $n \in \mathbb{N}^*$. Supposons construits $x_1, \cdots, x_n, y_1, \cdots, y_n$ convenables. On sait que :

$$[\ell]R_{n+1} = R_n = [x_n]P_n + [y_n]Q_n = [x_n][\ell]P_{n+1} + [y_n][\ell]Q_{n+1} = [\ell]([\tilde{x_n}]P_{n+1} + [\tilde{y_n}]Q_{n+1})$$

avec $\tilde{x_n}$ et $\tilde{y_n}$ étant des relèvement respectifs dans $\mathbb{Z}$ de x_n et y_n. Il s'ensuit que :

$$S_{n+1} := R_{n+1} - [\tilde{x_n}]P_{n+1} - [\tilde{y_n}]Q_{n+1}$$

est dans $E[\ell]$. Comme (P_1, Q_1) engendre $E[\ell]$, il existe donc $\alpha, \beta \in \mathbb{Z}$ tels que :

$$S_{n+1} = [\alpha]P_1 + [\beta]Q_1 = [\alpha][\ell^n]P_{n+1} + [\beta][\ell^n]Q_{n+1}$$

Posons donc $x_{n+1} := \tilde{x_n} + \alpha\ell^n \ [\ell^{n+1}]$ et $y_{n+1} := \tilde{y_n} + \beta\ell^n \ [\ell^{n+1}]$. Alors $x_{n+1} \equiv x_n \ [\ell^n]$, $y_{n+1} \equiv y_n \ [\ell^n]$ et :

$$R_{n+1} = [x_{n+1}]P_{n+1} + [y_{n+1}]Q_{n+1}$$

D'où la récurrence.

(ii) Lorsque $\ell = \mathrm{car}(K)$ et que E n'est pas supersingulière, le raisonnement est strictement le même, avec cette fois-ci $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$.

(iii) Lorsque $\ell = \mathrm{car}(K)$ et que E est supersingulière, $E[\ell^n] = \{0\}$ pour tout $n \in \mathbb{N}^*$ donc $T_\ell(E)$ est nul. □

Voyons maintenant l'utilité du module de Tate dans l'étude de $\mathrm{Hom}(E_1, E_2)$. Soit $\varphi \in \mathrm{Hom}(E_1, E_2)$ un morphisme. Alors on peut lui associer un morphisme $\mathbb{Z}_\ell$-linéaire $\varphi_\ell \in \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ donné par :

$$\forall\ (P_n)_{n\geq 1} \in T_\ell(E_1), \quad \varphi_\ell((P_n)_{n\geq 1}) := (\varphi(P_n))_{n\geq 1}$$

En étendant cette formule par $\mathbb{Z}_\ell$-linéarité, on obtient un morphisme de $\mathbb{Z}_\ell$-modules :

$$\Phi_\ell : \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

Proposition 1.2.0.4. *Si $\ell \neq car(K)$ alors Φ_ℓ est injectif.*

Avant d'en venir à la démonstration de la proposition ci-dessus, commençons par montrer le lemme suivant :

Lemme 1.2.0.5. *Soit $M \subset Hom(E_1, E_2)$ un sous-$\mathbb{Z}$-module de type fini de $Hom(E_1, E_2)$. Alors :*

$$M^{div} := \{\varphi \in Hom(E_1, E_2) |\ \exists m \in \mathbb{N}^*, \quad [m] \circ \varphi \in M\}$$

est libre de type fini.

Démonstration. **Étape 1 :** Montrons que M^{div} s'injecte dans $M \otimes_{\mathbb{Z}} \mathbb{R}$ comme $\mathbb{Z}$-module via :

$$\iota : \varphi \in M^{div} \longmapsto ([m_\varphi] \circ \varphi) \otimes \frac{1}{m_\varphi} \in M \otimes_{\mathbb{Z}} \mathbb{R}$$

où pour tout $\varphi \in M^{div}$, $m_\varphi := \min\{m \in \mathbb{N}^* | [m] \circ \varphi \in M\}$. Il s'agit de montrer que ι est $\mathbb{Z}$-linéaire et injective. Pour tout $\varphi \in M^{div}$, $I_\varphi := \{m \in \mathbb{N}^* | [m] \circ \varphi \in M\}$ est l'idéal de $\mathbb{Z}$ engendré par m_φ. Si $\varphi, \psi \in M^{div}$, on a trivialement :

$$I_\varphi \cap I_\psi = \mathrm{ppcm}(m_\varphi, m_\psi)\mathbb{Z} \subset I_{\varphi+\psi} = m_{\varphi+\psi}\mathbb{Z}$$

donc $m_{\varphi+\psi} | \mathrm{ppcm}(m_\varphi, m_\psi)$ et ainsi, en écrivant $\mathrm{ppcm}(m_\varphi, m_\psi) = a m_{\varphi+\psi}$, $\mathrm{ppcm}(m_\varphi, m_\psi) = b m_\varphi$ et

$\text{ppcm}(m_\varphi, m_\psi) = cm_\psi$ pour $a, b, c \in \mathbb{N}^*$, on obtient :

$$\begin{aligned}
\iota(\varphi+\psi) &= ([m_{\varphi+\psi}] \circ (\varphi+\psi)) \otimes \frac{1}{m_{\varphi+\psi}} = ([am_{\varphi+\psi}] \circ (\varphi+\psi)) \otimes \frac{1}{am_{\varphi+\psi}} \\
&= ([\text{ppcm}(m_\varphi, m_\psi)] \circ \varphi + [\text{ppcm}(m_\varphi, m_\psi)] \circ \psi) \otimes \frac{1}{\text{ppcm}(m_\varphi, m_\psi)} \\
&= ([\text{ppcm}(m_\varphi, m_\psi)] \circ \varphi) \otimes \frac{1}{\text{ppcm}(m_\varphi, m_\psi)} + ([\text{ppcm}(m_\varphi, m_\psi)] \circ \psi) \otimes \frac{1}{\text{ppcm}(m_\varphi, m_\psi)} \\
&= ([bm_\varphi] \circ \varphi) \otimes \frac{1}{bm_\varphi} + ([cm_\psi] \circ \psi) \otimes \frac{1}{cm_\psi} = ([m_\varphi] \circ \varphi) \otimes \frac{1}{m_\varphi} + ([m_\psi] \circ \psi) \otimes \frac{1}{m_\psi} \\
&= \iota(\varphi) + \iota(\psi)
\end{aligned}$$

ceci prouve la $\mathbb{Z}$-linéarité. Montrons maintenant l'injectivité de ι. Ceci revient à montrer l'injectivité de :

$$j : \varphi \in M \longmapsto \varphi \otimes 1 \in M \otimes_{\mathbb{Z}} \mathbb{R}$$

En effet, si $\varphi \in M^{div}$ vérifie $\iota(\varphi) = 0$ alors $j([m_\varphi] \circ \varphi) = m_\varphi \iota(\varphi) = 0$ donc $[m_\varphi] \circ \varphi = 0$, puis $\varphi = 0$ car sinon φ serait surjectif (d'après la proposition 6.11 de [3] [1]) et on aurait donc $[m_\varphi] = 0$, ce qui est exclus (d'après la proposition 6.15 de [3]).

On vient de montrer au passage que $\text{Hom}(E_1, E_2)$ est sans torsion. Ainsi, M est de type-fini et sans torsion donc libre d'après le théorème de structure des modules de type-fini (théorème 3.7.3 de [7]). Soit donc $(\varphi_i)_{1 \leq i \leq r}$ une $\mathbb{Z}$-base de M. Alors $(\varphi_i \otimes 1)_{1 \leq i \leq r}$ est une $\mathbb{R}$-base de $M \otimes_{\mathbb{Z}} \mathbb{R}$. En effet, cette famille est clairement $\mathbb{R}$-génératrice. Montrons qu'elle est libre. Soient $\lambda_1, \cdots, \lambda_r \in \mathbb{R}$ tels que :

$$\sum_{i=1}^{r} \lambda_i \varphi_i \otimes 1 = \sum_{i=1}^{r} \varphi_i \otimes \lambda_i = 0 \quad (\star)$$

Considérons :

$$\begin{array}{rcl} f : M \times \mathbb{R} & \longrightarrow & \mathbb{R}^r \\ (\sum_{i=1}^r n_i \varphi_i, \lambda) & \longmapsto & (\lambda n_i)_{1 \leq i \leq r} \end{array}$$

Alors par propriété universelle du produit tensoriel, f se factorise de façon unique sous la forme $f = g \circ \oplus$ avec $g : M \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \mathbb{R}^r$ $\mathbb{Z}$-linéaire et $\oplus : M \times \mathbb{R} \longrightarrow M \otimes_{\mathbb{Z}} \mathbb{R}$, l'application produit tensoriel. Ainsi, en appliquant g à $(\star)$, on obtient que :

$$\sum_{i=1}^{r} g(\varphi_i \otimes \lambda_i) = \sum_{i=1}^{r} f(\varphi_i, \lambda_i) = (\lambda_i)_{1 \leq i \leq r} = 0$$

Ce qu'il fallait démontrer.

Enfin, si $\varphi \in M$ s'écrit $\varphi = \sum_{i=1}^r \lambda_i \varphi_i$ dans $(\varphi_i \otimes 1)_{1 \leq i \leq r}$ alors :

$$j(\varphi) = \sum_{i=1}^{r} \lambda_i \varphi_i \otimes 1$$

donc $j(\varphi) = 0$ donne $\lambda_1 = \cdots = \lambda_r = 0$, puis $\varphi = 0$. Ceci termine l'étape 1.

Étape 2 : Montrons que $\iota(M^{div})$ est un sous-réseau de $M \otimes_{\mathbb{Z}} \mathbb{R}$. En effet, ceci a un sens car M est de type fini et donc $M \otimes_{\mathbb{Z}} \mathbb{R}$ est muni d'une structure de $\mathbb{R}$-espace vectoriel de dimension finie. On le munit de la topologie usuelle de $\mathbb{R}$. Considérons l'application :

$$\begin{array}{rcl} M \times \mathbb{R} \times M \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (\varphi, \lambda, \psi, \mu) & \longmapsto & \lambda\mu(\deg(\varphi+\psi) - \deg(\varphi) - \deg(\psi)) \end{array}$$

1. Les arguments données dans $\text{End}(E)$ étant généralisables à $\text{Hom}(E_1, E_2)$.

Cette application est tétralinéaire d'après la proposition 1.1.4.2. La propriété universelle du produit tensoriel assure qu'elle se factorise en une composée :

$$M \times \mathbb{R} \times M \times \mathbb{R} \xrightarrow{(\otimes,\otimes)} (M \otimes_{\mathbb{Z}} \mathbb{R})^2 \xrightarrow{\langle .,. \rangle} \mathbb{R}$$

la flèche de droite $\langle .,. \rangle$ étant $\mathbb{R}$-bilinéaire. Pour tout $x \in M \otimes_{\mathbb{Z}} \mathbb{R}$, posons $\deg(x) = \frac{1}{2}\langle x, x \rangle$. Cette application est une forme quadratique qui coïncide avec le degré usuel sur $\iota(M^{div})$. $\deg : M \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \mathbb{R}$ est continue car bilinéaire donc :

$$U := \{x \in M \otimes_{\mathbb{Z}} \mathbb{R} \mid \deg(x) < 1\}$$

est un voisinage ouvert de 0 dans $M \otimes_{\mathbb{Z}} \mathbb{R}$. En outre, il est clair que $\iota(M^{div}) \cap U = \{0\}$ puisque la fonction degré est entière. Ceci montre que $\iota(M^{div})$ est un sous-groupe discret de $M \otimes_{\mathbb{Z}} \mathbb{R}$. Puisque $\iota(M^{div})$ continent $M \otimes_{\mathbb{Z}} \mathbb{Z}$ qui engendre $M \otimes_{\mathbb{Z}} \mathbb{R}$ sur $\mathbb{R}$, il s'ensuit que $\iota(M^{div})$ est bien un sous-réseau de $M \otimes_{\mathbb{Z}} \mathbb{R}$. Ainsi, $\iota(M^{div})$, puis M^{div} est libre de type fini d'après le théorème 2.4 de [10]. □

On revoit maintenant à l'annexe A.3 pour une démonstration de ce théorème assez difficile et technique qui nous sera utile dans la preuve de la proposition 1.2.0.4.

Théorème 1.2.0.6. *(de factorisation) Soient E_1, E_2, E_3 des courbes elliptiques sur K, $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_1, E_3)$ des morphismes. Supposons φ séparable et $ker(\varphi) \subset ker(\psi)$. Alors il existe un unique morphisme $\lambda \in Hom(E_2, E_3)$ tel que :*

$$\psi = \lambda \circ \varphi$$

Démonstration. (de la proposition 1.2.0.4) Soit $x \in \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ tel que $\Phi_\ell(x) = 0$. Alors x s'écrit :

$$x = \sum_{i=1}^{r} \varphi_i \otimes \lambda_i$$

avec $\varphi_1, \cdots, \varphi_r \in \mathrm{Hom}(E_1, E_2)$ et $\lambda_1, \cdots, \lambda_r \in \mathbb{Z}_\ell$. Considérons $M := \sum_{i=1}^{r} \mathbb{Z}\varphi_i$. C'est un sous-$\mathbb{Z}$-module de type fini de $\mathrm{Hom}(E_1, E_2)$ tel que $x \in M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Ainsi, le lemme 1.2.0.5 assure que :

$$M^{div} := \{\varphi \in \mathrm{Hom}(E_1, E_2) | \ \exists m \in \mathbb{N}^*, \quad [m] \circ \varphi \in M\}$$

est libre de type fini. Soit $(\psi_j)_{1 \leq j \leq s}$ une $\mathbb{Z}$-base de M^{div}. Comme $M \subset M^{div}$, $(\psi_j)_{1 \leq j \leq s}$ est $\mathbb{Z}$-génératrice de M donc $\mathbb{Z}_\ell$ génératrice de $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. On dispose donc de $\mu_1, \cdots, \mu_s \in \mathbb{Z}_\ell$ tels que :

$$x = \sum_{j=1}^{s} \mu_j \psi_j \otimes 1$$

Soit $n \in \mathbb{N}^*$. Soient $a_1, \cdots, a_s \in \mathbb{Z}$ tels que $a_j \equiv \mu_j \ [\ell^n]$ pour tout $j \in \{1, \cdots, s\}$. Alors en regardant le n-ième terme de la suite définissant $\Phi_\ell(x)(P)$ pour tout $P \in T_\ell(E_1)$, on obtient que $\phi_n := \sum_{j=1}^{s} [a_j] \circ \psi_j$ est nul sur $E[\ell^n]$. Comme $[\ell^n]$ est séparable puisque $\ell \neq \mathrm{car}(K)$ (corollaire 6.16 de [3]), le théorème 1.2.0.6 assure l'existence de $\lambda \in \mathrm{Hom}(E_1, E_2)$ tel que :

$$\phi_n = \lambda \circ [\ell^n] = [\ell^n] \circ \lambda$$

Comme $\phi_n \in \sum_{j=1}^{s} \mathbb{Z}\psi_j = M^{div}$, il est clair que $\lambda \in M^{div}$. Il s'ensuit que :

$$\lambda = \sum_{j=1}^{s} [b_j] \circ \psi_j$$

avec $b_1, \cdots, b_s \in \mathbb{Z}$. La liberté de $(\psi_j)_{1 \leq j \leq s}$ assure que $a_j = b_j \ell^n$ pour tout $j \in \{1, \cdots, s\}$. Ainsi,

$\mu_j \equiv a_j \equiv 0\ [\ell^n]$ et ce pour tous $n \in \mathbb{N}^*$ et $j \in \{1, \cdots, s\}$. D'où $\mu_j = 0$ pour tout $j \in \{1, \cdots, s\}$ et $x = 0$. □

Théorème 1.2.0.7. *$Hom(E_1, E_2)$ est un $\mathbb{Z}$-module libre de rang au plus 4.*

Démonstration. Soit ℓ un nombre premier $\neq \mathrm{car}(K)$. Alors les propositions 1.2.0.4 et 1.2.0.3 assurent que $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ est un $\mathbb{Z}_\ell$-module libre de rang fini (comme sous-module d'un module libre de rang fini) et que :

$$\mathrm{rg}_{\mathbb{Z}_\ell}\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \leq \mathrm{rg}_{\mathbb{Z}_\ell}\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) \leq 4$$

Il suffirait de montrer que $\mathrm{rg}_{\mathbb{Z}}\mathrm{Hom}(E_1, E_2) \leq \mathrm{rg}_{\mathbb{Z}_\ell}\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ pour conclure. Or, si $(\varphi_i)_{1\leq i\leq r}$ est une famille $\mathbb{Z}$-libre de $\mathrm{Hom}(E_1, E_2)$ alors $(\varphi_i \otimes 1)_{1\leq i\leq r}$ est $\mathbb{Z}_\ell$-libre dans $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ en vertu d'un raisonnement déjà vu dans la preuve du lemme 1.2.0.5. Il s'agit de considérer :

$$\begin{array}{ccc} \bigoplus_{i=1}^r \mathbb{Z}\varphi_i \times \mathbb{Z}_\ell & \longrightarrow & \mathbb{Z}_\ell^r \\ (\sum_{i=1}^r n_i\varphi_i, \lambda) & \longmapsto & (\lambda n_i)_{1\leq i\leq r} \end{array}$$

et d'appliquer la propriété universelle du produit tensoriel. Ceci conclut. □

1.3 Structure de End(E).

Nous venons de montrer (théorème 1.2.0.7) que $\mathrm{End}(E)$ est un $\mathbb{Z}$-module libre de rang au plus 4. On a aussi vu (théorème 1.1.1.11 et proposition 1.1.3.1) que $\mathrm{End}(E)$ est muni d'un endomorphisme $\mathbb{Z}$-linéaire $\varphi \longmapsto \hat{\varphi}$ tel que pour tous $\varphi, \psi \in \mathrm{End}(E)$:

(i) $\hat{\hat{\varphi}} = \varphi$ (cet endomorphisme est donc invoultif).

(ii) $\hat{[n]} = [n]$ pour tout $n \in \mathbb{Z}$.

(iii) $\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [\deg(\varphi)] \in \mathbb{N}$ (en voyant $\mathbb{Z}$ comme un sous-anneau de $\mathrm{End}(E)$ via $n \longmapsto [n]$).

(iv) $\varphi \circ \hat{\varphi} = 0$ si et seulement si $\varphi = 0$.

(v) $\varphi \,\hat{\circ}\, \psi = \hat{\psi} \circ \hat{\varphi}$.

On en déduit le :

Théorème 1.3.0.1. *Seuls trois cas sont possibles pour $End(E)$:*

(i) *$End(E) \simeq \mathbb{Z}$.*

(ii) *$End(E)$ est un ordre d'une extension qudratique imaginaire de $\mathbb{Q}$.*

(iii) *$End(E)$ est un ordre d'une algèbre de quaternions.*

Avant d'en venir à la démonstration de ce résultat, rappelons ce qu'est une algèbre de quaternions.

Définition 1.3.0.2. *Une* algèbre de quaternions $\mathcal{K}$ *est une $\mathbb{Q}$-algèbre intègre de la forme :*

$$\mathcal{K} = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\beta \oplus \mathbb{Q}\alpha\beta$$

avec $\alpha^2, \beta^2 \in \mathbb{Q}^*_-$ et $\alpha\beta = -\beta\alpha$.

Remarque 1.3.0.3. Comme toute $\mathbb{Q}$-algèbre intègre de dimension finie, une algèbre de quaternions est une algèbre à division, c'est à dire que chacun de ses éléments non nuls admet un inverse.

Démonstration. (du théorème 1.3.0.1) Si $\mathrm{End}(E) \simeq \mathbb{Z}$ il n'y a rien à faire.

Sinon, considérons $\mathcal{K} := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Alors $\mathcal{K}$ est une $\mathbb{Q}$-algèbre de dimension finie ($\mathrm{End}(E)$ étant de rang fini). Elle est de plus intègre car si $x, y \in \mathcal{K}$ vérifient $xy = 0$ alors on peut écrire :

$$x = \sum_{i=1}^r \varphi_i \otimes \lambda_i \quad \text{et} \quad y = \sum_{j=1}^s \psi_j \otimes \mu_j$$

avec $\varphi_1, \cdots, \varphi_r, \psi_1, \cdots, \psi_s \in \mathrm{End}(E)$ et $\lambda_1, \cdots, \lambda_r, \mu_1, \cdots, \mu_s \in \mathbb{Q}$. Quitte à multiplier x et y par des entiers (le ppcm des numérateurs des λ_i et des μ_j respectivement), on peut supposer que les λ_i et les λ_j sont entiers. Mais alors :

$$xy = \left(\sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} \lambda_i \mu_j \varphi_i \circ \psi_j \right) \otimes 1 = \left(\sum_{i=1}^{r} \lambda_i \varphi_i \right) \circ \left(\sum_{j=1}^{s} \mu_j \psi_j \right) \otimes 1 = 0$$

on conclut alors par injectivité de $j : \varphi \in \mathrm{End}(E) \longmapsto \varphi \otimes 1 \in \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ déjà vue dans la preuve du lemme 1.2.0.5 avec $\mathbb{R}$ au lieu de $\mathbb{Q}$ et par integrité de $\mathrm{End}(E)$ (proposition 6.11 de [3]) que $x = 0$ ou $y = 0$. Ainsi, $\mathcal{K}$ **est une algèbre à division**. Étant engendrée par $\mathrm{End}(E)$, qui est de rang compris entre 2 et 4 sur $\mathbb{Z}$ (puisque l'on suppose $\mathrm{End}(E) \not\simeq \mathbb{Z}$), $\mathcal{K}$ **est de dimension comprise entre** 2 **et** 4 **sur** $\mathbb{Q}$.

On peut de plus voir $\mathrm{End}(E) \simeq j(\mathrm{End}(E))$ comme un sous-anneau de $\mathcal{K}$. Montrons que c'est un ordre de $\mathcal{K}$. Comme $\mathrm{End}(E)$ engendre $\mathcal{K}$, il suffit de prouver que tout élément de $\mathrm{End}(E)$ est entier algébrique. Pour cela, prolongeons le morphisme de dualité à $\mathcal{K}$. On considère l'application $\mathbb{Z}$-bilinéaire :

$$\begin{array}{ccc} \mathrm{End}(E) \times \mathbb{Q} & \longrightarrow & \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \\ (\varphi, \lambda) & \longmapsto & \hat{\varphi} \otimes \lambda \end{array}$$

que l'on factoriste en une application linéaire de $\hat{\mathrm{ffl}} : \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ dans lui-même via l'application produit tensoriel. L'endomorphisme $\mathbb{Q}$-linéaire ainsi défini coïncide avec le morphisme de dualité sur $\mathrm{End}(E)$ donc on vérifie facilement par $\mathbb{Q}$-linéarité que pour tous $x, y \in \mathcal{K}$:

(i) $\hat{\hat{x}} = x$.

(ii) $\hat{q} = q$ pour tout $q \in \mathbb{Q}$ (en voyant $\mathbb{Q}$ comme un sous-corps de $\mathcal{K}$ via $q \in \mathbb{Q} \longmapsto [1] \otimes q \in \mathcal{K}$).

(iii) $x\hat{x} = \hat{x}x \in \mathbb{Q}_+$.

(iv) $x\hat{x} = 0$ si et seulement si $x = 0$.

(v) $\hat{xy} = \hat{y}\hat{x}$.

Considérons les fonctions norme et trace données respectivement par :

$$\forall x \in \mathcal{K}, \quad N(x) := x\hat{x} \quad \text{et} \quad \mathrm{Tr}(x) := x + \hat{x}$$

N est à valeur dans $\mathbb{Q}$ d'après (iii) et Tr aussi d'après l'égalité :

$$\forall x \in \mathcal{K}, \quad \mathrm{Tr}(x) = 1 + N(x) + N(1 - x)$$

N et Tr sont même à valeur dans $\mathbb{Z}$ sur $\mathrm{End}(E)$. L'égalité :

$$\forall x \in \mathcal{K}, \quad (X - x)(X - \hat{x}) = X^2 - \mathrm{Tr}(x)X + N(x)$$

assure alors que tous les éléments de $\mathrm{End}(E)$ sont entiers algébriques, donc que $\mathbf{End}(E)$ **est un ordre de** $\mathcal{K}$.

Étudions maintenant $\mathcal{K}$. Comme $[\mathcal{K} : \mathbb{Q}] \geq 2$, on dispose de $\alpha \in \mathcal{K} \setminus \mathbb{Q}$. Quitte à remplacer α par $\alpha - \frac{1}{2}\mathrm{Tr}(\alpha)$ (qui n'est pas dans $\mathbb{Q}$ car $\frac{1}{2}\mathrm{Tr}(\alpha) \in \mathbb{Q}$), on peut supposer que $\mathrm{Tr}(\alpha) = 0$. On a alors $\hat{\alpha} = -\alpha$ et donc $\alpha^2 = -\alpha\hat{\alpha} \in \mathbb{Q}_-$ d'après (iii) et $\alpha^2 \neq 0$ par (iv). Si $\mathcal{K} = \mathbb{Q}(\alpha)$, alors $\mathcal{K}$ est donc une extension quadratique imaginaire de $\mathbb{Q}$.

Supposons maintenant que $\mathcal{K} \neq \mathbb{Q}(\alpha)$. Soit $\beta \in \mathcal{K} \setminus \mathbb{Q}(\alpha)$. Comme $\hat{\alpha} = -\alpha$ et $\alpha^2 \in \mathbb{Q}^*$, on a :

$$\beta - \frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2\alpha}\mathrm{Tr}(\alpha\beta) = \hat{\beta} - \frac{1}{2}\mathrm{Tr}(\beta) + \frac{1}{2\alpha^2}\mathrm{Tr}(\alpha\beta)\alpha$$

En ajoutant $\beta - \frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2\alpha}\mathrm{Tr}(\alpha\beta)$, on obtient :

$$\mathrm{Tr}\left(\beta - \frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2\alpha}\mathrm{Tr}(\alpha\beta)\right) = 0$$

Et :

$$\alpha\left(\beta - \frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2\alpha}\mathrm{Tr}(\alpha\beta)\right) = \widehat{\alpha\beta} + \alpha\frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2}\mathrm{Tr}(\alpha\beta)$$

De sorte que :

$$\mathrm{Tr}\left(\alpha\left(\beta - \frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2\alpha}\mathrm{Tr}(\alpha\beta)\right)\right) = 0$$

Quitte à remplacer β par $\beta - \frac{1}{2}\mathrm{Tr}(\beta) - \frac{1}{2\alpha}\mathrm{Tr}(\alpha\beta)$ (ce qui ne change pas le fait que $\beta \notin \mathbb{Q}(\alpha)$) on peut donc supposer que :

$$\mathrm{Tr}(\beta) = \mathrm{Tr}(\alpha\beta) = 0$$

Ainsi, on a :

$$\alpha = -\hat{\alpha}, \quad \beta = -\hat{\beta} \quad \text{et} \quad \alpha\beta = -\widehat{\alpha\beta} = -\hat{\beta}\hat{\alpha} = -\beta\alpha$$

En outre, $\beta^2 = -\beta\hat{\beta} \in \mathbb{Q}_-^*$. On obtient donc facilement que :

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

En outre, comme $\alpha \notin \mathbb{Q}$ et $\beta \notin \mathbb{Q}(\alpha)$, on obtient par la formule de la base télescopique :

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2 \times 2 = 4$$

Donc $(1, \alpha, \beta, \alpha\beta)$ est $\mathbb{Q}$-libre. Ceci achève de prouver que $\mathbb{Q}(\alpha, \beta)$ est une algèbre de quaternions. Or, comme $[\mathcal{K} : \mathbb{Q}] \leq 4$, il s'ensuit que $\mathcal{K} = \mathbb{Q}(\alpha, \beta)$, puis que $\mathcal{K}$ est une algèbre de quaternions. □

1.4 End(E) en caractéristique $p \neq 0$.

Dans ce paragraphe, p est un nombre premier $\neq 2, 3$ et q une puissance de p.

Théorème 1.4.0.1. *Soit E une courbe ordinaire définie sur $\mathbb{F}_q$. Alors End(E) est un ordre d'une extension quadratique imaginaire de $\mathbb{Q}$.*

Démonstration. D'après le théorème 1.3.0.1, il suffit de montrer que $\mathrm{End}(E)$ est commutatif et non isomorphe à $\mathbb{Z}$. Pour l'injectivité, commençons par montrer que la flèche naturelle $\mathrm{End}(E) \longrightarrow \mathrm{End}(T_p(E))$ donnée par :

$$\forall \varphi \in \mathrm{End}(E),\ \forall (P_n)_{n\in\mathbb{N}^*} \in T_p(E), \quad \varphi_p((P_n)_{n\in\mathbb{N}^*}) := (\varphi(P_n))_{n\in\mathbb{N}^*}$$

est injective. En effet, si $\varphi \in \mathrm{End}(E)$ vérifie $\varphi_p = 0$ alors $\varphi(E[p^n]) = \{\mathcal{O}\}$ de sorte que $E[p^n] \subset \ker(\varphi)$ pour tout $n \in \mathbb{N}^*$. Or, $|E[p^n]| = p^n$ pour tout $n \in \mathbb{N}^*$ car E est ordinaire donc $\ker(\varphi)$ est infini et nécessairement $\varphi = 0$ d'après la proposition 6.10 de [3]. $\mathrm{End}(E)$ se plonge donc dans $\mathrm{End}(T_p(E))$ avec $T_p(E) \simeq \mathbb{Z}_p$ d'après la proposition 1.2.0.3 (cas ordinaire). Ainsi, $\mathrm{End}(T_p(E)) \simeq \mathbb{Z}_p$ est commutatif et $\mathrm{End}(E)$ aussi.

$\mathrm{End}(E)$ est non isomorphe à $\mathbb{Z}$ car l'isomorphisme de Frobenius $\phi_q : (x, y) \in E \longmapsto (x^q, y^q) \in E$ n'est pas la multiplication par un entier. En effet, si par l'absurde $\phi_q = [n]$ pour un certain $n \in \mathbb{N}$ alors par égalité des degrés :

$$n^2 = \deg(\phi_q) = q$$

Donc $n = p^r$ pour un certain $r \in \mathbb{N}^*$. Donc $\phi_q = [p^r]$ est de noyau $E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}$ car E est ordinaire. C'est absurde car $\ker\phi_q = \{\mathcal{O}\}$. □

Remarque 1.4.0.2. On pourrait aussi montrer que la condition suffisante E ordinaire est en fait nécessaire pour que $\mathrm{End}(E)$ soit l'ordre d'une extension quadratique imaginaire de $\mathbb{Q}$. En effet, dans le cas où E est supersingulière, $\mathrm{End}(E)$ est un ordre d'une algèbre de quaternions. Ce résultat n'étant pas utilisé dans ce document, il ne sera pas prouvé. Le lecteur intéressé pourra consulter la preuve du théorème V.3.1 de [2]. Cependant, nous allons maintenant prouver une condition nécessaire de supersingularité qui nous servira.

Proposition 1.4.0.3. *Si E (définie sur $\mathbb{F}_q$) est supersingulière. Alors $j(E) \in \mathbb{F}_{p^2}$.*

Démonstration. Notons ϕ_p le morphisme de Frobenius et $E^{(p^r)}$ la courbe image de E par ϕ_p^r pour tout $r \in \mathbb{N}^*$. On a :

$$\hat{\phi_p} \circ \phi_p = [p]$$

avec $\ker[p] = E[p] = \{\mathcal{O}\}$ car E est supersingulière donc $\ker\hat{\phi_p}$ est aussi trivial. Mais d'après le point (v) de la proposition 1.1.3.1, $\deg\hat{\phi_p} = \deg\hat{\phi_p} = p$ donc $\hat{\phi_p}$ est inséparable et d'après le corollaire 1.1.1.10, cette isogénie se factorise en $\hat{\phi_p} = \psi \circ \phi_p'^n$ avec $n \in \mathbb{N}^*$ où $\psi : E^{(p^{n+1})} \longrightarrow E$ est séparable et où ϕ_p' est l'isogénie de Frobenius $E^{(p)} \longrightarrow E^{(p^2)}$. Par multiplicativité du degré, on a nécessairement $n = 1$ et $\deg(\psi) = 1$. Mais alors $\hat{\psi} \circ \psi = [1] = \mathrm{id}_{E^{(p^2)}}$ et $\psi \circ \hat{\psi} = [1] = \mathrm{id}_E$ donc ψ est un isomorphisme entre E et $E^{(p^2)}$, de sorte que :

$$j(E) = j(E^{(p^2)}) = 1728\frac{4a^{3p^2}}{4a^{3p^2} + 27b^{2p^2}} = \left(1728\frac{4a^3}{4a^3 + 27b^2}\right)^{p^2} = j(E)^{p^2}$$

Donc $j(E) \in \mathbb{F}_{p^2}$. □

Chapitre 2

Le résultat central : deux bijections.

2.1 Rappels de quelques généralités sur les courbes elliptiques sur $\mathbb{C}$.

On rappelle que toute courbe elliptique E sur $\mathbb{C}$ est isomorphe (en tant que groupe) à un tore $\mathbb{C}/\Lambda$ où $\Lambda := \mathbb{Z} \oplus \tau\mathbb{Z}$ est un réseau de $\mathbb{C}$ avec τ dans $\mathbb{H} := \{z \in \mathbb{C} |\ \mathrm{Im}(z) > 0\}$, le demi-plan de Poincaré (voir 5.12, 5.13 et 5.19 de [3]). L'isomorphisme est donné par la formule :

$$\Phi : z \in \mathbb{C}/\Lambda \longmapsto \begin{cases} \left(\mathfrak{p}_\Lambda(z), \frac{1}{2}\mathfrak{p}'_\Lambda(z)\right) & \text{si } z \neq 0 \\ \mathcal{O} & \text{si } z = 0 \end{cases}$$

$\mathfrak{p}$ étant la fonction de Weierstrass (Λ-périodique) dont l'expression est donnée par :

$$\mathfrak{p}_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

L'ensemble des courbes elliptiques sur $\mathbb{C}$ peut donc être paramétré par la variable $\tau \in \mathbb{H}$. La fonction j-invariant :

$$j : \tau \longmapsto j(\tau) := j(E_\tau)$$

est holomorphe sur $\mathbb{H}$ et invariante sous l'action de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$ donnée par :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ \tau \in \mathbb{H}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau := \frac{a\tau + b}{c\tau + d}$$

On vérifie en effet que $\mathbb{H}$ est stable par cette opération via la formule :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ \tau \in \mathbb{H}, \quad \mathrm{Im}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau \right) = \frac{(ad-bc)\mathrm{Im}(\tau)}{|c\tau + d|^2} = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}$$

j est de plus méromorphe à l'infini, c'est à dire qu'elle peut s'écrire sous la forme $j := F \circ q$ avec $F : \mathbb{D}^* \longmapsto \mathbb{H}$ holomorphe sur le disque épointé $\mathbb{D}^* := \{z \in \mathbb{C} |\ 0 < |z| < 1\}$ et méromorphe en 0 et $q : \tau \in \mathbb{H} \longmapsto e^{2i\pi\tau} \in \mathbb{D}^*$. On a de plus un développement de la forme :

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{+\infty} a_n q^n$$

avec $(a_n)_{n \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ (voir [8], chapitre 4, § 2).

j est en fait une surjection (par le théorème 5.18 de [3]) qui induit par passage au quotient une

surjection :

$$\overline{j} : SL_2(\mathbb{Z}) \setminus \mathbb{H} \longrightarrow \mathbb{C}$$

Nous verrons plus tard que cette application est en fait bijective mais nous aurons besoin pour cela de comprendre comment s'interprétent les morphismes entre courbes elliptiques lorsqu'on les identifie à des tores. Pour le moment, on s'en tient au fait suivant.

Proposition 2.1.0.1. *Il existe une structure de surface de Riemann sur $SL_2(\mathbb{Z}) \setminus \mathbb{H}$ telle que $\overline{j}$ soit une application holomorphe entre surfaces de Riemann.*

Pour démontrer ce résultat, on commence par prouver le lemme suivant :

Lemme 2.1.0.2. *L'action de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$ est :*

(i) Holomorphe *: pour tout $\gamma \in SL_2(\mathbb{Z})$, $\tau \longmapsto \gamma \cdot \tau$ est holomorphe sur $\mathbb{H}$.*

(ii) Proprement discontinue *: pour tout compact $K \subset \mathbb{H}$, l'ensemble :*

$$\{\gamma \in SL_2(\mathbb{Z}) |\ \gamma \cdot K \cap K \neq \emptyset\}$$

est fini.

Démonstration. Pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $\tau \longmapsto \frac{a\tau+b}{c\tau+d}$ est bien holomorphe sur $\mathbb{H}$ car cette fonction n'a éventuellement qu'un pôle en $-\frac{d}{c} \notin \mathbb{H}$ (si $c \neq 0$). D'où (i).

Soient $K \subset \mathbb{H}$ compact et $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ telle que $\gamma \cdot K \cap K \neq \emptyset$. Alors on dispose de $\tau \in \mathbb{H}$ tel que $\gamma \cdot \tau \in K$. On sait qu'alors :

$$\min_{z \in K} \mathrm{Im}(z) \leq \mathrm{Im}(\gamma \cdot \tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2} \leq \frac{\max_{z \in K} \mathrm{Im}(z)}{|c\tau + d|^2}$$

Le minimum et le maximum de $z \longmapsto \mathrm{Im}(z)$ étant atteints sur K car K est compact et que cette fonction est continue. Le minimum est de plus strictement positif car $K \subset \mathbb{H}$. Ainsi :

$$|c\tau + d|^2 \leq \frac{\max_{z \in K} \mathrm{Im}(z)}{\min_{z \in K} \mathrm{Im}(z)}$$

Or :

$$|c\tau + d|^2 = c^2|\tau|^2 + 2cd\mathrm{Re}(\tau) + d^2$$

Et $z \longmapsto \frac{|\mathrm{Re}(z)|}{|z|}$ est continue donc admet son maximum κ sur K qui est nécessairement < 1 puisque $\mathbb{H}$ ne contient pas de nombre réel. Ainsi :

$$\begin{aligned} \frac{\max_{z \in K} \mathrm{Im}(z)}{\min_{z \in K} \mathrm{Im}(z)} &\geq |c\tau + d|^2 \geq c^2|\tau|^2 - 2|c||d|\kappa|\tau| + d^2 = (|c||\tau| - |d|\kappa)^2 + d^2(1 - \kappa^2) \\ &\geq \min((|c| \min_{z \in K} |z| - |d|\kappa)^2, (|c| \max_{z \in K} |z| - |d|\kappa)^2) + d^2(1 - \kappa^2) \end{aligned}$$

Comme le dernier terme de cette égalité tend vers $+\infty$ qand $\max(|c|, |d|) \to +\infty$, il s'ensuit que c et d sont bornés.

En outre :

$$|\gamma \cdot \tau| = \left| \frac{a\tau + b}{c\tau + d} \right| \leq \max_{z \in K} |z|$$

De sorte que :

$$|a\tau + b|^2 \leq |c\tau + d|^2 \max_{z \in K} |z|^2 \leq \frac{\max_{z \in K} \mathrm{Im}(z)^2}{\min_{z \in K} \mathrm{Im}(z)^2} \max_{z \in K} |z|^2$$

On obtient alors exactement par les même calculs que a et b sont bornés.

Comme $a, b, c, d \in \mathbb{Z}$, il s'ensuit que $\{\gamma \in SL_2(\mathbb{Z}) |\ \gamma \cdot K \cap K \neq \emptyset\}$ est fini. D'où (ii). □

Le résultat de la proposition 2.1.0.1 est une conséquence du théorème suivant que nous admettrons (et dont on pourra trouver une preuve dans [11]).

Théorème 2.1.0.3. *(admis) Soit G un groupe agissant holomorphiquement, proprement et discontinûment sur une surface de Riemann S. Alors il existe une structure de surface de Riemann sur S/G telle que l'application quotient $\pi : S \longrightarrow S/G$ soit holomorphe.*

Toute fonction holomorphe $f : S \longrightarrow S'$ invariante sous l'action de G se factorise alors de façon unique sous la forme $f = \overline{f} \circ \pi$ avec $\overline{f} : S/G \longrightarrow S'$ holomorphe.

Remarque 2.1.0.4. Le lemme 2.1.0.2 est trivialement vérifié pour tout sous-groupe $\Gamma \subset SL_2(\mathbb{Z})$. Ainsi, $\Gamma \setminus \mathbb{H}$ est aussi muni d'une structure de surface de Riemann.

2.2 Action sur les tores des morphismes entre courbes elliptiques sur $\mathbb{C}$.

Nous savons maintenant représenter toute courbe elliptique E définie sur $\mathbb{C}$ comme un tore $\mathbb{C}/\Lambda$ où Λ est un réseau de $\mathbb{C}$. La question qui se pose naturellement maintenant est la suivante. Si E_1 et E_2 sont deux courbes elliptiques définies sur $\mathbb{C}$, représentées respectivement par les réseaux Λ_1 et Λ_2, quelle fonction $\mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ peut-on associer à une isogénie entre E_1 et E_2 ?

Pour comprendre cela, on commence par étudier la structure de surface de Riemann sur E_1 et E_2.

2.2.1 Structure de surface de Riemann sur une courbe elliptique sur $\mathbb{C}$.

Soit E une courbe elliptique sur $\mathbb{C}$ de réseau associé Λ. Λ agit par translation sur $\mathbb{C}$. Cette action est holomorphe (car une translation est holomorphe) et il est aisé de voir qu'elle est proprement doscontinue (Λ étant discret). Ainsi, le théorème 2.1.0.3 assure que $\mathbb{C}/\Lambda$ est munie d'une structure de surface de Riemann pour laquelle la projection $\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ est holomorphe. L'action étant de plus sans point fixe, on a en fait un résultat plus fort (conséquence de la proposition 2.8 de [11]).

Lemme 2.2.1.1. *$\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$ est un revêtement, c'est à dire une application continue telle que tout $[z] \in \mathbb{C}/\Lambda$ admette un voisinage ouvert U tel que $\pi^{-1}(U)$ soit une union disjointe d'ouverts $\bigsqcup_{j\in J} V_j$ de $\mathbb{C}$ telle que π induise un homéomorphisme entre V_j et U pour tout $j \in J$.*

Remarque 2.2.1.2. Une application holomorphe bijective étant biholomorphe, ce lemme démontre que π est un biholomorphisme local.

Puisque $\mathbb{C}/\Lambda$ est naturellement munie d'une structure de surface de Riemann, on peut transférer cette structure à E via :

$$\Phi : z \in \mathbb{C}/\Lambda \longmapsto \begin{cases} \left(\mathfrak{p}_\Lambda(z), \frac{1}{2}\mathfrak{p}'_\Lambda(z)\right) & \text{si } z \neq 0 \\ \mathcal{O} & \text{si } z = 0 \end{cases}$$

On va en fait construire une structure de surface de Riemann "à la main" sur E pour laquelle Φ est un biholomorphisme car ceci servira plus tard. Pour cela, il nous faut définir des cartes holomorphes. Tout naturellement, nous prendrons des uniformisantes. Si $P \in E$ alors trois cas sont possibles :

Cas 1 : Si $P \neq \mathcal{O}$ et si $y_P \neq 0$ alors $X - x_P$ est une uniformisante en P ;

Cas 2 : Si $P \neq \mathcal{O}$ et $y_P = 0$ alors Y est une uniformisante en P ;

Cas 3 : Si $P = \mathcal{O}$ alors $\frac{X}{Y}$ est une uniformisante en P.

On pourra trouver une preuve de ce résultat dans [4] (cf. propositions II.19, II.21 et II.23). Dans tout les cas, on notera r_P l'uniformisante en P ainsi choisie. On voit que dans chaque cas, r_P est bien définie sur un voisinage ouvert U_P de P [1].

1. Ici, E est munie de la topologie induite sur E comme sous-ensemble de $\mathbb{P}^2(\mathbb{C})$. En particulier, $\{P = [x : y : z] \in E | y \neq 0\}$ est un visinage ouvert de $\mathcal{O} = [0 : 1 : 0]$, qui s'écrit en coordonnées homogènes $\{(x, y) \in E | y \neq 0\} \cup \mathcal{O}$.

Lemme 2.2.1.3. *$(r_P, U_P)_{P\in E}$ définit un atlas holomorphe sur E.*

Démonstration. Soit $W := Y^2 - X^3 - aX - b$ le polynôme de Weierstrass de E.

Soient $P, Q \in E$ tels que $U_P \cap U_Q \neq \emptyset$.

Si P et Q vérifient le cas 1 alors l'application de transition $r_P \circ r_Q^{-1}$ définie sur $r_Q(U_P \cap U_Q)$ est a translation $z \longmapsto z + x_Q - x_P$ qui est holomorphe.

Supposons que P et Q vérifient respectivement les cas 1 et 2. Comme $y_Q = 0$, x_Q est l'une des trois racines de $X^3 + aX + b$ dont l'expression est donnée par radicaux $x_Q = f(a, b)$ avec f holomorphe par rapport à a et b. Comme $X^3 + aX + b$ est de discriminant non nul, $X^3 + aX + b - y^2$ est de discriminant non nul lorsque y est proche de 0 et ce polynôme a toujours 3 racines distinctes. Quitte à prendre l'ouvert U_Q plus petit, on peut donc supposer que pour tout $R \in U_Q$, $x := f(a, b - y_R^2)$ est l'unique racine de $X^3 + aX + b - y^2$ vérifiant $(x, y_R) \in U_Q$. Ainsi, $r_P(R) = f(a, b - y_R^2) - x_P$ pour tout $R \in U_P \cap U_Q$ et :

$$\forall z \in r_Q(U_P \cap U_Q), \quad r_P \circ r_Q^{-1}(z) = f(a, b - z^2) - x_P$$

qui est holomorphe.

Nous venons en fait de traiter le cas le plus difficile et tous les autres cas se traitent de la même manière. Notons que l'on a imposé des contraintes supplémentaires sur les ouverts U_P. □

Proposition 2.2.1.4. *Φ est un biholomorphisme entre $\mathbb{C}/\Lambda$ et E.*

Démonstration. Il suffit de vérifier que Φ est bijective et holomorphe. La bijectivité a déjà été prouvée dans le théorème 5.12 de [3]. En outre, comme π est un biholomorphisme local, il suffit de prouver que $\Phi \circ \pi$ est holomorphe pour voir que Φ est holomorphe. Or, si $z_0 \notin \Lambda$ alors $P := \Phi(z_0) \neq \mathcal{O}$ et en composant par r_P, on obtient un polynôme en $\mathfrak{p}_\Lambda$ eu $\mathfrak{p}'_\Lambda$ dont les pôles sont en Λ : $r_P \circ \Phi \circ \pi$ est donc holomorphe sur un voisinage de z_0. Puis, si $z_0 \in \Lambda$ alors $\Phi(z_0) = \mathcal{O}$ et :

$$r_{\mathcal{O}} \circ \Phi \circ \pi(z) = \frac{2\mathfrak{p}_\Lambda(z)}{\mathfrak{p}'_\Lambda(z)} \sim \frac{\frac{2}{(z-z_0)^2}}{-\frac{2}{(z-z_0)^3}} = z_0 - z$$

quand $z \longrightarrow z_0$. Donc $r_{\mathcal{O}} \circ \Phi \circ \pi$ est holomorphe sur un voisinage de z_0. Ceci conclut. □

En composant par les cartes de l'atlas du lemme 2.2.1.3, on obtient aussi le :

Lemme 2.2.1.5. *Tout morphisme $E_1 \longrightarrow E_2$ est une application holomorphe.*

2.2.2 Expression des morphismes comme multiplication par un complexe (PSC).

Soit $\alpha \in \mathbb{C}^*$ vérifiant $\alpha\Lambda_1 \subset \Lambda_2$ alors la composée de $z \in \mathbb{C} \longmapsto \alpha z \in \mathbb{C}$ avec π_2 est holomorphe et invariante sous l'action de Λ_1. Elle induit donc une fonction holomorphe :

$$\begin{array}{rccc} \phi_\alpha : & \mathbb{C}/\Lambda_1 & \longrightarrow & \mathbb{C}/\Lambda_2 \\ & z & \longmapsto & \alpha z \bmod \Lambda_2 \end{array}$$

Théorème 2.2.2.1 (PSC). **(i)** *L'application qui à $\alpha \in \mathbb{C}$ vérifiant $\alpha\Lambda_1 \subset \Lambda_2$ associe ϕ_α induit une bijection sur l'ensemble $Hol_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$ des fonctions holomorphes entre $\mathbb{C}/\Lambda_1$ et $\mathbb{C}/\Lambda_2$ qui s'annullent en 0.*

(ii) *Soit $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda_1 \subset \Lambda_2$. Alors ϕ_α est un bijective si et seulement si $\alpha\Lambda_1 = \Lambda_2$. C'est alors un biholomorphisme.*

(iii) *Si E_1 et E_2 sont les courbes elliptiques respectivement associées à $\mathbb{C}/\Lambda_1$ et $\mathbb{C}/\Lambda_2$ et si Φ_1 et Φ_2 désignent respectivement les isomorphismes de groupes entre $\mathbb{C}/\Lambda_1$ et E_1 et entre $\mathbb{C}/\Lambda_2$ et E_2 explicités précédemment, alors :*

$$F : \varphi \in Hom(E_1, E_2) \longmapsto \Phi_2^{-1} \circ \varphi \circ \Phi_1 \in Hol_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$$

est un isomorphisme de $\mathbb{Z}$-modules.

Remarque 2.2.2.2. Ceci prouve que les morphismes entre E_1 et E_2 sont en bijection avec les nombres complexes $\alpha \in \mathbb{C}^*$ tels que $\alpha\Lambda_1 \subset \Lambda_2$.

Avant de prouver ce théorème, montrons un résultat intermédiaire :

Proposition 2.2.2.3 (PSC). *Soit Λ un réseau de $\mathbb{C}$. Alors toute fonction elliptique par rapport à Λ est fraction rationnelle en $\mathfrak{p}_\Lambda$ et $\mathfrak{p}'_\Lambda$.*

Démonstration. Soit f une fonction elliptique par rapport à Λ. Alors f peut s'écrire comme somme d'une fonction paire et d'une fonction impaire, toutes les deux elliptiques. En effet :

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

donc on peut sans perte de généralité supposer f paire ou impaire. En outre, si f est impaire, on obtient que $f\mathfrak{p}'_\Lambda$ est paire, donc on peut supposer qu'en fait f est paire.

On peut alors utiliser le lemme suivant :

Lemme 2.2.2.4. *Si $\omega \in \mathbb{C}$ est un zéro ou pôle de f alors $-\omega$ est un zéro ou un pôle de f de même ordre. Si de plus $-\omega \equiv \omega \mod \Lambda$ alors $ord_\omega(f)$ est pair.*

Démonstration. Il est clair par parité de f que si $\omega \in \mathbb{C}$ est un zéro de f alors $-\omega$ aussi. L'égalité des ordres s'obtient par développement de Taylor au voisinage de ω et de $-\omega$, en remarquant que :

$$f^{(k)}(-\omega) = (-1)^k f^{(k)}(\omega)$$

pour tout $k \in \mathbb{N}$.

Si maintenant $-\omega \equiv \omega \mod \Lambda$ alors par parité de f et Λ-périodicité de f' :

$$f'(\omega) = -f'(-\omega) = -f'(\omega)$$

donc $f'(\omega) = 0$. Donc $\mathrm{ord}_\omega(f) \geq 2$. Posons donc $m := \left\lfloor \frac{\mathrm{ord}_\omega(f)}{2} \right\rfloor$.

Si $\omega \in \mathbb{C} \setminus \Lambda$ alors $\mathfrak{p}_\Lambda(\omega)$ existe et $g := \mathfrak{p}_\Lambda - \mathfrak{p}_\Lambda(\omega)$ est une fonction elliptique paire, qui vérifie donc $\mathrm{ord}_\omega(g) \geq 2$ d'après le résultat précédent. Or, le seul pôle de $\mathfrak{p}_\Lambda$, donc de g dans une maille élémentaire M du réseau Λ est l'unique élément de $M \cap \Lambda$ et il est d'ordre 2 donc d'après la proposition 5.3 de [3], $\mathrm{ord}_\omega(g) = 2$. Donc $\frac{f}{g^m}$ est elliptique et holomorphe en ω. Donc si $\frac{f}{g^m}(\omega) = 0$ alors $\mathrm{ord}_\omega\left(\frac{f}{g^m}(\omega)\right) \geq 2$ d'après ce qui précède, i.e. $\mathrm{ord}_\omega(f) \geq 2m+2$, ce qui contredit le fait que $m := \left\lfloor \frac{\mathrm{ord}_\omega(f)}{2} \right\rfloor$. Ainsi, $\frac{f}{g^m}(\omega) \neq 0$ et $\mathrm{ord}_\omega(f) = 2m$. Si maintenant $\omega \in \Lambda$ alors on peut appliquer le même raisonnement à $g := \frac{1}{\mathfrak{p}_\Lambda}$.

On obtient le même résultat pour les pôles en considérant $\frac{1}{f}$. □

Pour tout $\omega \in \mathbb{C} \setminus \Lambda$, posons :

$$m_\omega := \begin{cases} \frac{1}{2}\mathrm{ord}_\omega(f) & \text{si } \omega \equiv -\omega \mod \Lambda \\ \mathrm{ord}_\omega(f) & \text{sinon} \end{cases}$$

Et considérons pour tout $z \in \mathbb{C} \setminus \Lambda$:

$$g(z) := \prod_{\omega \in \mathbb{C}/\Lambda \setminus \{0\}} (\mathfrak{p}_\Lambda(z) - \mathfrak{p}_\Lambda(\omega))^{m_\omega}$$

Nous avons vu précédemment que pour tout $\omega \in \mathbb{C} \setminus \Lambda$ tel que $\omega \equiv -\omega \mod \Lambda$, $\mathfrak{p}_\Lambda - \mathfrak{p}_\Lambda(\omega)$ admet un zéro d'ordre 2. Si maintenant $\omega \not\equiv -\omega \mod \Lambda$ alors $-\omega$ et ω ont deux classes d'équivalence distinctes dans $\mathbb{C}/\Lambda$ donc le fait que $\mathfrak{p}_\Lambda - \mathfrak{p}_\Lambda(\omega)$ n'ait qu'un seul pôle d'ordre 2 dans toute maille élémentaire du réseau Λ et la propositon 5.3 de [3] assurent que ω est un zéro d'ordre 1 de $\mathfrak{p}_\Lambda - \mathfrak{p}_\Lambda(\omega)$. Ainsi, f et g ont même ordre en tout point de $\mathbb{C} \setminus \Lambda$ et ceci est aussi vrai sur Λ d'après la proposition 5.3 de [3] donc $\frac{f}{g}$ est elliptique et sans pôle ni zéro donc constante d'après le corollaire 5.4 de [3]. Ceci achève la preuve de la proposition. □

Démonstration. (du théorème 2.2.2.1)

(i) Soient $\alpha, \beta \in \mathbb{C}^*$ tels que $\phi_\alpha = \phi_\beta$. Alors $(\beta - \alpha)z = 0 \bmod \Lambda_2$ pour tout $z \in \mathbb{C}$ donc une fonction affine ayant une image soit réduite à $\{0\}$ soit égale à $\mathbb{C}$ tout entier et Λ_2 étant dénombrable, il s'ensuit que $\beta - \alpha = 0$. D'où l'injectivité.

Soit maintenant $f \in \mathrm{Hol}_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$. Alors $f \circ \pi_1$ est holomorphe donc continue sur $\mathbb{C}$ qui est localement et globalement connexe par arcs et $\pi_2 : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda_2$ est un revêtement d'après le lemme 2.2.1.1. Un théorème classique de théorie des revêtements (théorème 2.11 de [11]) assure alors l'existence de $g : \mathbb{C} \longrightarrow \mathbb{C}$ telle que $\pi_2 \circ g = f \circ \pi_1$. π_2 étant un biholomorphisme local, cette formule donne que g est holomorphe. De plus $\pi_2 \circ g = f \circ \pi_1$ se réécrit :

$$\forall z \in \mathbb{C}, \omega \in \Lambda_2, \quad g(z + \omega) = g(z) \bmod \Lambda_2$$

Alors g étant continue sur le connexe par arcs $\mathbb{C}$ et tout point de Λ_2 étant isolé (car Λ_2 est discret), $z \in \mathbb{C} \longmapsto g(z + \omega) - g(z)$ est constante pour tout $\omega \in \Lambda_1$ donc :

$$\forall z \in \mathbb{C}, \quad g'(z + \omega) = g'(z)$$

Écrivons $\Lambda_1 := \mathbb{Z} \oplus \tau_1\mathbb{Z}$. Comme tout élément de $\mathbb{C}/\Lambda_1$ admet un représentant dans le parallélogramme fondamental :

$$P_1 := \{s + t\tau_1 |\ (s,t) \in [0,1]^2\}$$

toutes les valeurs prises par g' sont atteintes sur g'. P_1 étant compact, $|g'|$ admet un maximum global qui est atteint sur P_1. g' n'est donc pas ouverte. Elle est donc constante (toute application holomorphe étant soit constante soit ouverte). On dispose donc de $\alpha \in \mathbb{C}$ tels que $g(z) = \alpha z + g(0)$ pour tout $z \in \mathbb{C}$ avec $g(0) \in \Lambda_2$ car $f(0) = 0$. Il s'ensuit que $f = \phi_\alpha$ avec $\alpha\Lambda_1 \subset \Lambda_2$ (g étant Λ_2-invariante).

(ii) Soit $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda_1 \subset \Lambda_2$ et ϕ_α est bijective. Alors ϕ_α est biholomorphe et par (i), $\phi_\alpha^{-1} : z \in \mathbb{C}/\Lambda_2 \longmapsto \beta z \in \mathbb{C}/\Lambda_2$ avec $\beta \in \mathbb{C}$ tel que $\beta\Lambda_2 \subset \Lambda_1$. Comme $\phi_\alpha \circ \phi_\alpha^{-1} = \mathrm{id}_{\mathbb{C}/\Lambda_2}$, l'injectivité de la bijection de (i) assure que $\alpha\beta = 1$. Ainsi, $\frac{1}{\alpha}\Lambda_2 \subset \Lambda_1$ ie $\Lambda_2 \subset \alpha\Lambda_1$, de sorte que $\alpha\Lambda_1 = \Lambda_2$.

Réciproquement, si $\alpha\Lambda_1 = \Lambda_2$ alors $z \in \mathbb{C}/\Lambda_2 \longmapsto \frac{1}{\alpha}z \in \mathbb{C}/\Lambda_2$ est la réciproque de ϕ_α.

(iii) F est bien définie puisque Φ_1 et Φ_2^{-1} sont holomorphes (d'après la proposition 2.2.1.4), que tout morphisme $\varphi \in \mathrm{Hom}(E_1, E_2)$ est holomorphe (d'après le lemme 2.2.1.5) et que :

$$\Phi_2^{-1} \circ \varphi \circ \Phi_1(0) = \Phi_2^{-1}(\varphi(\mathcal{O})) = \Phi_2^{-1}(\mathcal{O}) = 0$$

La propriété de morphisme de $\mathbb{Z}$-modules de F est une conséquence immédiate de la propriété de morphisme de groupes de Φ_1 et Φ_2^{-1}.

On vérifie alors que :

$$G : f \in \mathrm{Hol}_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) \longmapsto \Phi_2 \circ f \circ \Phi_1^{-1} \in \mathrm{Hom}(E_1, E_2)$$

est bien définie. Une fois ceci fait, nous obtiendrons le résultat voulu puisqu'il sera alors clair que $F \circ G = \mathrm{id}_{\mathrm{Hol}_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)}$ et $G \circ F = \mathrm{id}_{\mathrm{Hom}(E_1,E_2)}$. Soit $f \in \mathrm{Hol}_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$. Justifions que $\Phi_2 \circ f \circ \Phi_1^{-1} \in \mathrm{Hom}(E_1, E_2)$. On sait d'après le point (i) qu'il existe $\alpha \in \mathbb{C}^*$ tel que $\alpha\Lambda_1 \subset \Lambda_2$ et $f = \phi_\alpha$. Si $P \in E_1$ alors on peut écrire $P = \Phi_1(z)$ avec $z \in \mathbb{C}/\Lambda_1$ et donc :

$$\Phi_2 \circ f \circ \Phi_1^{-1}(P) = \left(\mathfrak{p}_{\Lambda_2}(f(z)), \frac{1}{2}\mathfrak{p}'_{\Lambda_1}(f(z))\right) = \left(\mathfrak{p}_{\Lambda_2}(\alpha z), \frac{1}{2}\mathfrak{p}'_{\Lambda_2}(\alpha z)\right)$$

Or, comme $\alpha\Lambda_1 \subset \Lambda_2$, $z \longmapsto \mathfrak{p}_{\Lambda_2}(\alpha z)$ et $z \longmapsto \mathfrak{p}'_{\Lambda_2}(\alpha z)$ sont Λ_1-périodiques et méromorphes donc elliptiques par rapport à Λ_1. On en déduit que ce sont des fractions rationnelles en $\mathfrak{p}_{\Lambda_1}$ et $\mathfrak{p}'_{\Lambda_1}$ d'après la proposition 2.2.2.3. En outre, $\Phi_2 \circ f \circ \Phi_1^{-1}$ est un morphisme de groupes comme composées de morphismes de groupes. C'est donc un morphisme. D'où la bonne définition de G et la bijectivité de F. □

Corollaire 2.2.2.5. *Soit E une courbe elliptique sur $\mathbb{C}$ associée au réseau $\Lambda := \mathbb{Z} \oplus \tau\mathbb{Z}$ ($\tau \in \mathbb{H}$). Alors $End(E) \not\simeq \mathbb{Z}$ si et seulement si τ est racine d'un polynôme de degré 2 à coefficients entiers. Auquel cas, $End(E)$ est un ordre d'une extension quadratique de $\mathbb{Q}$.*

Avant la preuve, faisons une remarque préliminaire que nous utiliserons dans toute la suite :

Remarque 2.2.2.6. Soit Φ l'isomorphisme de groupes entre E et $\mathbb{C}/\Lambda$ explicité au paragraphe précédent. Le point (iii) du théorème 2.2.2.1 nous donne un isomorphisme de $\mathbb{Z}$-modules :

$$F : \varphi \in \mathrm{End}(E) \longmapsto \Phi^{-1} \circ \varphi \circ \Phi \in \mathrm{Hol}_0(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda)$$

C'est en fait un isomorphisme de $\mathbb{Z}$-algèbre. D'après le point (i) du théorème 2.2.2.1, les morphismes de $\mathrm{End}(E)$ peuvent donc être identifiés aux $\alpha \in \mathbb{C}$ tels que $\alpha\Lambda \subset \Lambda$, la somme et la multiplication des morphismes correspondant à la somme et à la multiplication usuelles dans $\mathbb{C}$. Il est par ailleurs assez facile de voir que les entiers de $\mathrm{End}(E)$ correspondent aux entiers de $\mathbb{C}$.

Démonstration. $\Longrightarrow$ Supposons que $\mathrm{End}(E) \not\simeq \mathbb{Z}$. Alors on dispose de $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ tel que $\alpha\Lambda \subset \Lambda$. Ainsi, $\alpha, \alpha\tau \in \Lambda$ ie $\alpha = a\tau + b$ et $\alpha\tau = c\tau + d$ avec $a, b, c, d \in \mathbb{Z}$ donc :

$$a\tau^2 + (b - c)\tau - d = 0$$

Comme $\alpha \notin \mathbb{Z}$, $a \neq 0$. Donc τ est racine d'un polynôme de degré 2 à coefficients entiers.

$\Longleftarrow$ Supposons que τ soit racine d'un polynôme de degré 2 à coefficients entiers, disons $aX^2 + bX + c$ ($a \neq 0$). Quitte à diviser par $\mathrm{pgcd}(a, b, c)$, on peut supposer que a, b et c sont premiers entre eux. De plus, comme $\tau \notin \mathbb{R}$, τ n'est pas racine d'un polynôme de degré 1 donc le polynôme minimal de τ vaut $\pi = X^2 + \frac{b}{a}X + \frac{c}{a}$.

Soit $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda \subset \Lambda$. Alors $\alpha = a'\tau + b'$ et $\alpha\tau = c'\tau + d'$ avec $a', b', c', d' \in \mathbb{Z}$. Donc $a'X^2 + (b' - c')X - d'$ annule τ, de sorte que $\pi = X^2 + \frac{b}{a}X + \frac{c}{a}$ donc $aX^2 + bX + c$ divise ce polynôme dans $\mathbb{Q}[X]$. Il existe donc $q \in \mathbb{Q}$ tel que $a' = qa$, $b' - c' = qb$ et $-d' = qc$. Le dénominateur de q divise donc a, b et c. Comme a, b et c sont premiers entre eux, $q \in \mathbb{Z}$. Ainsi, $\alpha \in \mathbb{Z} + a\tau\mathbb{Z}$.

Réciproquement si $\alpha \in \mathbb{Z}+a\tau\mathbb{Z}$ alors $\alpha = ka\tau+l$ avec $k, l \in \mathbb{Z}$ et donc $\alpha\tau = ka\tau^2+l\tau = k(-b\tau-c)+l \in \Lambda$ de sorte que $\alpha\Lambda \subset \Lambda$. Donc $\mathrm{End}(E) \simeq \mathbb{Z} + a\tau\mathbb{Z}$.

Comme $a\tau$ est racine de $X^2 + abX + ac$, $a\tau$ est entier algébrique. L'ensemble des entiers algébriques étant un sous-anneau de $\mathbb{C}$, tous les éléments de $\mathbb{Z} + a\tau\mathbb{Z}$ sont entiers algébriques. Comme $(1, a\tau)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\tau)$, $\mathbb{Z} + a\tau\mathbb{Z}$ est donc un ordre de ce corps de nombres. Ceci conclut. □

2.3 Courbes elliptiques sur $\mathbb{C}$ à isomorphisme près et quotients de $\mathbb{H}$.

2.3.1 Retour sur la fonction $\overline{j} : SL_2(\mathbb{Z}) \setminus \mathbb{H} \longrightarrow \mathbb{C}$ (PSC).

On commence par le résultat général suivant sur le j-invariant :

$$j(E) := 1728 \frac{4a^3}{4a^3 + 27b^2}$$

lorsque E a pour équation de Weierstrass $Y^2 = X^3 + aX + b$.

Proposition 2.3.1.1 (PSC). *Soit K un corps de caractéristique $\neq 2, 3$. Alors deux courbes elliptiques E_1 et E_2 sur K sont isomorphes (sur $\overline{K}$) si et seulement si elles ont même j-invariant.*

Démonstration. $\Longrightarrow$ Supposons que E_1 et E_2 sont isomorphes. Soient $Y^2 = X^3 + a_i X + b_i$ les équations de Weierstrass de E_i pour $i \in \{1, 2\}$. Ecrivons φ et φ^{-1} sous forme réduite $\varphi(X, Y) := (r_1(X), Y s_1(X))$ et $\varphi^{-1}(X, Y) := (r_2(X), Y s_2(X))$. Comme $\varphi^{-1} \circ \varphi = \mathrm{id}_{E_1}$, on a :

$$r_2(r_1(X)) = X \quad \text{et} \quad Y s_1(X) s_2(r_1(X)) = Y$$

Donc r_1 est de degré 1 et s_1 est constante. Ecrivons donc $r_1(X) = aX + b$ et $s_1(X) = c$, avec $a, b, c \in \overline{K}$, $ac \neq 0$. On sait qu'alors :

$$c^2 Y^2 = (aX + b)^3 + a_2(aX + b) + b_2 \quad (1) \quad \text{et} \quad Y^2 = X^3 + a_1 X + b_1 \quad (2)$$

L'équation $\frac{(1)}{c^2} - (2)$ donne :

$$\frac{a^3}{c^2} = 1 \quad b = 0 \quad a_1 = \frac{a a_2}{c^2} \quad (3) \quad \text{et} \quad b_1 = \frac{b_2}{c^2} \quad (4)$$

en regardant respectivement le terme en X^3, le terme en X^2, le terme en X et le terme constant.

On distingue alors trois cas :

Premier cas : Si $a_1, b_1 \neq 0$ alors $a_2, b_2 \neq 0$ (par (3) et (4)) et donc l'équation $\frac{(3)}{(4)}$ donne $\frac{a a_2}{b_2} = \frac{a_1}{b_1}$ donc $a = \frac{a_1 b_2}{a_2 b_1}$, puis c est une racine de a^3. En fixant γ, une racine de $\frac{a_1 b_2}{a_2 b_1}$, on obtient donc que :

$$\varphi(X, Y) := (\gamma^2 X, \pm \gamma^3 Y)$$

(3) et (4) donnent alors $a_1 = \frac{a_2}{\gamma^4}$ et $b_1 = \frac{b_2}{\gamma^6}$. On obtient alors que :

$$j(E_1) = 1728 \frac{4a_1^3}{4a_1^3 + 27b_1^2} = 1728 \frac{4a_2^3}{4a_2^3 + 27b_2^2} = j(E_2)$$

Deuxième cas : Si $a_1 = 0$ alors $a_2 = 0$ par (3) et $b_1, b_2 \neq 0$ car E_1 et E_2 sont des courbes elliptiques. Donc on a trivialement $j(E_1) = j(E_2) = 0$.

Troisième cas : Si $b_1 = 0$ alors $b_2 = 0$ par (4) et $a_1, a_2 \neq 0$ car E_1 et E_2 sont des courbes elliptiques. Donc on a trivialement $j(E_1) = j(E_2) = 1728$.

$\Longleftarrow$ Supposons que $j(E_1) = j(E_2)$. En multipliant cette équation par $(4a_1^3 + 27b_1^2)(4a_2^3 + 27b_2^2)$ et en simplifaint les entiers (non nuls car $\mathrm{car}(K) \neq 2, 3$), on obtient que :

$$a_2^3 b_1^2 = a_1^3 b_2^2 \quad (5)$$

et donc $A_1 = \frac{A_2}{\gamma^4}$ et $B_1 = \frac{B_2}{\gamma^6}$ où γ est une racine carrée de $\frac{A_1 B_2}{A_2 B_1}$. Donc φ de la forme annoncée est bien un isomorphisme.

On distingue encore trois cas :

Premier cas : Si $a_1, b_1 \neq 0$ alors $a_2, b_2 \neq 0$ car sinon on aurait $j(E_1) = j(E_2) \in \{0, 1728\}$, ce qui n'est possible que lorsque $a_1 b_1 = 0$. En fixant γ, une racine carrée de $\frac{a_1 b_2}{a_2 b_1}$, on obtient par (5) que $a_1 = \frac{a_2}{\gamma^4}$ et $b_1 = \frac{b_2}{\gamma^6}$. Donc l'équation $Y^2 = X^3 + a_1 X + b_1$ est compatible avec $\gamma^6 Y^2 = \gamma^6 X^3 + a_2 \gamma^2 X + b_2$ et $Y^2 = X^3 + a_2 X + b_2$ est compatible avec $\frac{Y^3}{\gamma^6} = \frac{X^3}{\gamma^6} + a_1 \frac{X}{\gamma^2} + b_1$, de sorte que :

$$\varphi : (x, y) \in E_1 \longmapsto (\gamma^2 x, \pm\gamma^3 y) \in E_2$$

définit un isomorphisme de réciproque :

$$\varphi : (x, y) \in E_2 \longmapsto (\gamma^{-2} x, \pm\gamma^{-3} y) \in E_1$$

Deuxième cas : Si $a_1 = 0$ alors $a_2 = 0$ car alors $j(E_1) = j(E_2) = 0$ et $b_1, b_2 \neq 0$ car E_1 et E_2 sont des courbes elliptiques. Considérons γ une racine sixième de $\frac{b_2}{b_1}$. Alors l'équation $Y^2 = X^3 + b_1$ est compatible avec $\gamma^6 Y^2 = \gamma^6 X^3 + b_2$ et $Y^2 = X^3 + b_2$ est compatible avec $\frac{Y^3}{\gamma^6} = \frac{X^3}{\gamma^6} + b_1$ donc comme précédemment :

$$\varphi : (x, y) \in E_1 \longmapsto (\gamma^2 x, \pm\gamma^3 y) \in E_2$$

définit un isomorphisme.

Troisième cas : Si $b_1 = 0$ alors $b_2 = 0$ par car alors $j(E_1) = j(E_2) = 1728$ et $a_1, a_2 \neq 0$ car E_1 et E_2 sont des courbes elliptiques. On conclut de même en prenant pour γ une racine cubique de $\frac{a_2}{a_1}$.

□

Théorème 2.3.1.2. *$\overline{j} : SL_2(\mathbb{Z}) \setminus \mathbb{H} \longrightarrow \mathbb{C}$ est un biholomorphisme.*

Démonstration. $\overline{j}$ est holomorphe est surjective. Il reste à prouver qu'elle est injective. Soient $\tau, \tau' \in \mathbb{H}$ tels que $j(\tau) = j(\tau')$. Alors les courbes elliptiques associées à τ et τ' sont isomorphes d'après la proposition précédente. Notons $\Lambda := \mathbb{Z} \oplus \tau\mathbb{Z}$ et $\Lambda' := \mathbb{Z} \oplus \tau'\mathbb{Z}$. Alors le point (ii) du théorème 2.2.2.1 assure l'existence de $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda = \Lambda'$. Ainsi, $(\alpha, \alpha\tau)$ est une $\mathbb{Z}$-base de Λ' donc la matrice de passage de $(1, \tau)$ à $(\alpha, \alpha\tau)$ est dans $GL_2(\mathbb{Z})$ donc on dispose de $a, b, c, d \in \mathbb{Z}$ tels que $ad - bc = \pm 1$ et :

$$\alpha = c\tau' + d \quad \text{et} \quad \alpha\tau = a\tau' + b$$

On en déduit :

$$\tau = \frac{a\tau' + b}{c\tau' + d} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau'$$

Comme :

$$\mathrm{Im}(\tau) = \frac{(ad - bc)\mathrm{Im}(\tau')}{|c\tau' + d|^2}$$

et que $\tau, \tau' \in \mathbb{H}$, on a en fait $ad - bc = 1$ donc τ et τ' coïncident modulo $SL_2(\mathbb{Z})$, ce qui prouve l'injectivité. □

2.3.2 La première bijection du théorème : $Y_0(N) \simeq S_0(N)$.

Dans ce paragraphe et dans toute la suite, on fixe N un entier naturel ≥ 2.

On considère l'ensemble des paires (E, C) où E est une courbe elliptique sur $\mathbb{C}$ et C un sous-groupe cyclique d'ordre N de E[2]. On munit cet ensemble d'une relation d'équivalence $\sim$ telle que $(E, C) \sim (E', C')$ si et seulement si il existe un isomorphisme $\varphi \in \mathrm{Hom}(E, E')$ tel que $\varphi(C) = C'$. On note $S_0(N)$ l'ensemble quotient pour cette classe d'équivalence.

2. C est nécessairement inclus dans $E[N]$ et C existe car $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ d'après le théorème 6.17 de [3]

Comme nous l'avons vu aux deux précédents paragraphes, $S_0(N)$ s'identifie aux paires $(\mathbb{C}/\Lambda_\tau, C)$ avec $\Lambda_\tau := \mathbb{Z} \oplus \tau\mathbb{Z}$ pour un certain $\tau \in \mathbb{H}$ et C un sous-groupe cyclique d'ordre N de $\mathbb{C}/\Lambda$. On a alors $(\mathbb{C}/\Lambda_\tau, C) \sim (\mathbb{C}/\Lambda_{\tau'}, C')$ si et seulement s'il existe $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda_\tau = \Lambda_{\tau'}$ et $\alpha C = C'$ (cf point (ii) du théorème 2.2.2.1). Nous noterons $[\mathbb{C}/\Lambda_\tau, C]$ la classe de la paire $(\mathbb{C}/\Lambda_\tau, C)$. Pour définir C, nous serons souvent amené à considérer un générateur $P \in \mathbb{C}/\Lambda_\tau$ de C. On notera alors $\langle P \rangle$ (sous-groupe engendré par P) au lieu de C.

Introduisons le sous-groupe de congruence de $SL_2(\mathbb{Z})$ suivant :

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \ [N] \right\}$$

De même que $SL_2(\mathbb{Z})$, $\Gamma_0(N)$ agit par homographie sur $\mathbb{H}$. On notera $Y_0(N) := \Gamma_0(N) \setminus \mathbb{H}$ le quotient ainsi obtenu. Cette action est proprement discontinue et holomorphe (voir remarque 2.1.0.4) donc $Y_0(N)$ est muni d'une structure de surface de Riemann.

Théorème 2.3.2.1 (première bijection)**.** **(i)** *On a :*

$$S_0(N) = \left\{ \left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle \right] \mid \tau \in \mathbb{H} \right\}$$

(ii) $\left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] = \left[\mathbb{C}/\Lambda_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$ *si et seulement si* $\tau' \in \Gamma_0(N)\tau$. *Ainsi, on dispose d'une bijection :*

$$\begin{array}{ccc} Y_0(N) & \longrightarrow & S_0(N) \\ \Gamma_0(N)\tau & \longmapsto & \left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] \end{array}$$

Démonstration. **(i)** On commence par prouver le lemme suivant :

Lemme 2.3.2.2. *La réduction modulo N : $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$ est surjective.*

Démonstration. Soit $\gamma \in SL_2(\mathbb{Z}/N\mathbb{Z})$ que l'on relève arbitrairement en $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$. Alors :

$$ad - bc \equiv 1 \ [N] \quad (1)$$

donc c, d et N sont premiers entre eux.

Montrons qu'il existe $s, t \in \mathbb{Z}$ tels que $c' := c + sN$ et $d' := d + tN$ soient premiers entre eux. Notons $g := c \wedge d$. Alors g et N sont premiers entre eux. Supposons que $c \neq 0$. Alors le théorème des restes chinois assure l'existence de $t \in \mathbb{Z}$ tel que pour tout nombre premier $p|c$, $t \equiv 1 \ [p]$ si $p|g$ et $t \equiv 0 \ [p]$ sinon. Prenons $s = 0$. Alors si p est un nombre premier divisant $c' = c$ et $d' = d + tN$:

— soit il divise g, auquel cas il divise d donc $p|d'$ donne que $N \equiv d + tN \equiv d' \equiv 0 \ [p]$ donc $p|N$ ce qui est exclus car g et N sont premiers entre eux ;

— soit il ne divise pas g, auquel cas $d \equiv d' \equiv 0 \ [p]$ et donc p divise c et d donc g ce qui est absurde.

Donc $c' \wedge d' = 1$. Si $c = 0$ alors $d \neq 0$ car sinon on aurait $0 \equiv 1 \ [N]$ par (1) ce qui est impossible car $N \geq 2$. Un raisonnement symétrique avec d conclut alors de même à l'existence de $s, t \in \mathbb{Z}$ tels que $c' := c + sN$ et $d' := d + tN$ soient premiers entre eux.

Par construction de c' et d' et par (1), on a toujours $ad' - bc' \equiv 1 \ [N]$ donc :

$$ad' - bc' \equiv 1 + kN \quad (2)$$

avec $k \in \mathbb{Z}$. Mais $c' \wedge d' = 1$ donc le théorème de Bézout assure l'existence de $u, v \in \mathbb{Z}$ tels que $ud' - vc' = 1$. On a alors par (2) :

$$(a + uN)d' - (b + vN)c' = 1$$

Donc $\begin{pmatrix} a+uN & b+vN \\ c+sN & d+tN \end{pmatrix}$ relève γ dans $SL_2(\mathbb{Z})$. D'où le résultat. □

Soit $(\mathbb{C}/\Lambda_\tau, C)$ avec $\tau \in \mathbb{H}$ et C un sous-groupe d'ordre N de Λ_τ. Alors C est engendré par un certain P de la forme $P = q\tau + r + \Lambda_\tau$ avec $q, r \in \mathbb{R}$. Comme P est d'ordre N, $Nq \in \mathbb{Z}$ et $Nr \in \mathbb{Z}$ et $\text{pgcd}(Nq, Nr, N) = 1$. Posons donc $q := \frac{c}{N}$ et $r := \frac{d}{N}$ avec $c, d \in \mathbb{Z}$. La condition $\text{pgcd}(c, d, N) = 1$ et le théorème de Bézout assurent l'existence de $a, b \in \mathbb{Z}$ tels que :

$$ad - bc \equiv 1\ [N]$$

donc $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ se réduit modulo N en une matrice de $SL_2(\mathbb{Z}/N\mathbb{Z})$. Comme la réduction modulo $N : SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$ est une surjection (d'après le lemme ci-dessus) et que P ne dépend que des résidus de c et d modulo N, on peut supposer, quitte à changer les coefficients de cette matrice modulo N, que $\gamma \in SL_2(\mathbb{Z})$.

Posons $\tau' := \gamma \cdot \tau = \frac{a\tau+b}{c\tau+b}$ et $\alpha := c\tau + d$. Alors $\alpha\tau' = a\tau + b$ donc $\alpha\Lambda_{\tau'} \subset \Lambda_\tau$ ce qui assure que α définit un morphisme entre $\mathbb{C}/\Lambda_{\tau'}$ et $\mathbb{C}/\Lambda_\tau$. Comme $\gamma \in SL_2(\mathbb{Z})$ est la transposée de la matrice de passage de $(\tau, 1)$ à $(\alpha\tau', \alpha)$, on a même que $(\alpha\tau', \alpha)$ est une $\mathbb{Z}$-base de Λ_τ, et donc que $\alpha\Lambda_{\tau'} = \Lambda_\tau$. Donc α est un isomorphisme d'après le point (ii) du théorème 2.2.2.1. En outre :

$$\alpha\left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle = \left\langle \frac{\alpha}{N} + \alpha\Lambda_{\tau'} \right\rangle = \left\langle \frac{c\tau + d}{N} + \Lambda_\tau \right\rangle = \langle P \rangle = C$$

D'où $[\mathbb{C}/\Lambda_\tau, C] = \left[\mathbb{C}/\Lambda_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$, puis (i).

(ii) $\Longrightarrow$ Soient $\tau, \tau' \in \mathbb{H}$ tels que $\left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] = \left[\mathbb{C}/\Lambda_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$. Alors on dispose de $\alpha \in \mathbb{C}$ tel que :

$$\alpha\Lambda_{\tau'} = \Lambda_\tau \quad \text{et} \quad \alpha\left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle = \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle$$

Ces conditions donnent que $\alpha\left(\frac{1}{N} + \Lambda_{\tau'}\right) = \frac{\alpha}{N} + \Lambda_\tau$ est d'ordre N donc $\alpha = c\tau + d$ avec $c, d \in \mathbb{Z}$ tels que $\text{pgcd}(c, d, N) = 1$. Or, tous les points de $\left\langle \frac{1}{N} + \Lambda_\tau \right\rangle$ sont de composante en τ nulle modulo Λ_τ ce qui assure que $N|c$.

Puis, la condition $\alpha\Lambda_{\tau'} = \Lambda_\tau$ assure que $(\alpha, \alpha\tau')$ est une $\mathbb{Z}$-base de Λ_τ donc que la transposée de la matrice de passage de $(\tau, 1)$ à $(\alpha\tau', \alpha)$ est dans $GL_2(\mathbb{Z})$. En écrivant $\alpha\tau' = a\tau + b$ avec $a, b \in \mathbb{Z}$ on obtient alors :

$$\tau' = \frac{a\tau + b}{c\tau + d} = \gamma \cdot \tau$$

avec $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ comme $\tau, \tau' \in \mathbb{H}$, la formule :

$$\text{Im}(\tau') = \frac{\det(\gamma)\text{Im}(\tau)}{|c\tau + d|^2}$$

assure que $\gamma \in SL_2(\mathbb{Z})$. Comme $N|c$, on a en fait même $\gamma \in \Gamma_0(N)$.

$\Longleftarrow$ Soient $\tau, \tau' \in \mathbb{H}$ tels que $\tau' := \gamma \cdot \tau$ pour un certain $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Posons $\alpha := c\tau + d$. Alors $\alpha\tau = a\tau + b \in \Lambda_\tau$ et $(\alpha, \alpha\tau)$ est une $\mathbb{Z}$-base de Λ_τ donc $\alpha\Lambda_{\tau'} = \Lambda_\tau$. Puis :

$$\alpha\left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle = \left\langle \frac{\alpha}{N} + \alpha\Lambda_{\tau'} \right\rangle = \left\langle \frac{c\tau + d}{N} + \Lambda_\tau \right\rangle = \left\langle \frac{d}{N} + \Lambda_\tau \right\rangle = \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle$$

Les deux dernières égalités venant du fait que $N|c$, puis que $ad - bc = 1$, de sorte que $d \wedge N = 1$. Ainsi :

$$\left[\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] = \left[\mathbb{C}/\Lambda_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$$

□

2.4 Le revêtement ramifié $p_N : Y_0(N) \longrightarrow \mathbb{C}$ induit par j.

La projection $\mathbb{H} \longrightarrow SL_2(\mathbb{Z}) \setminus \mathbb{H}$ est $\Gamma_0(N)$-invariante. Comme l'action de $\Gamma_0(N) \subset SL_2(\mathbb{Z})$ est holomorphe et proprement discontinue, le théorème 2.1.0.3 assure que cette projection induit une application holomorphe :

$$\pi_N : Y_0(N) = \Gamma_0(N) \setminus \mathbb{H} \longrightarrow SL_2(\mathbb{Z}) \setminus \mathbb{H}$$

qui sera notre objet d'étude dans ce paragraphe.

En fait, en composant π_N par $\overline{j} : SL_2(\mathbb{Z}) \setminus \mathbb{H} \longrightarrow \mathbb{C}$, on obtient une application holomorphe $p_N : Y_0(N) \longrightarrow \mathbb{C}$ que nous utiliserons plus tard. Comme $\overline{j}$ est un biholomorphisme, toute "l'information analytique" de p_N est contenue dans π_N.

Définition 2.4.0.1. *Pour tout $\tau \in \mathbb{H}$, on note $SL_2(\mathbb{Z})_\tau$ le stabilisateur de $\mathbb{H}$ sous l'action de $SL_2(\mathbb{Z})$ par homographie appelé* groupe d'isotropie de τ. *τ est dit* elliptique *si $SL_2(\mathbb{Z})_\tau$ n'est pas réduit à $\{\pm I_2\}$. Dans ce cas, sa classe $SL_2(\mathbb{Z})\tau$ dans $SL_2(\mathbb{Z}) \setminus \mathbb{H}$ est aussi appelée elliptique.*

Proposition 2.4.0.2. *Les seuls points elliptiques de $SL_2(\mathbb{Z})\setminus\mathbb{H}$ sont les classes de i et de $\rho := e^{\frac{2i\pi}{3}}$. Les groupes d'isotropie respectifs de i et ρ sont :*

$$SL_2(\mathbb{Z})_i = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \quad et \quad SL_3(\mathbb{Z})_\rho = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle$$

Démonstration. Soit $\tau \in \mathbb{H}$ un point elliptique. Alors on dispose de $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \setminus \{\pm I_2\}$ stabilisant τ. On a donc $\gamma \cdot \tau = \frac{a\tau+b}{c\tau+d} = \tau$, ce qui conduit à :

$$c\tau^2 + (d-a)\tau - b = 0$$

Comme $\tau \notin \mathbb{R}$, $c \neq 0$ et $\Delta := (d-a)^2 + 4bc < 0$. Or :

$$\Delta = d^2 - 2ad + a^2 + 4bc = d^2 + 2ad + a^2 - 4(ad - bc) = (d+a)^2 - 4$$

Donc $|\mathrm{Tr}(\gamma)| = |a+d| < 2$. Ainsi, le polynôme caractéristique de γ est de la forme X^2+1 ou $X^2 \pm X + 1$. D'après le théorème de Cayley-Hamilton, ce polynôme annule γ donc $\gamma^2 + I_2 = 0$ et donc $\gamma^4 = I_2$ ou $\gamma^2 + \gamma + I_2 = 0$ et donc $\gamma^3 = -\gamma^2 - \gamma = I_2$ ou $\gamma^2 - \gamma + I_2 = 0$ et donc $\gamma^3 = \gamma^2 - \gamma = -I_2$, puis $\gamma^6 = I_2$. Ainsi, γ est d'ordre $1, 2, 3, 4$ ou 6.

Mais si γ est d'ordre au plus 2 alors γ est racine de $X^2 - 1 = (X-1)(X+1)$, un polynôme scindé à racines simples (sur $\mathbb{Q}$) donc γ est diagonalisable sur $\mathbb{Q}$ de valeurs propres incluses dans $\{\pm 1\}$. Comme $\det(\gamma) = 1$, nécessairement ces valeurs propres sont toutes les deux 1 ou toutes les deux -1. Donc $\gamma = \pm I_2$, ce qui est exclus. Donc γ est d'ordre $3, 4$ ou 6.

Lemme 2.4.0.3. *Soit $\gamma \in SL_2(\mathbb{Z})$. Alors :*

(i) *Si γ est d'ordre 3, alors γ est conjuguée (dans $SL_2(\mathbb{Z})$) à $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^{\pm}$.*

(ii) *Si γ est d'ordre 4, alors γ est conjuguée (dans $SL_2(\mathbb{Z})$) à $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{\pm}$.*

(iii) *Si γ est d'ordre 6, alors γ est conjuguée (dans $SL_2(\mathbb{Z})$) à $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm}$.*

Démonstration. On commence par prouver (ii). Supposons que γ soit d'ordre 4. On considère le sous-réseau canonique $\mathbb{Z}^2 \subset \mathbb{R}^2$. γ agit sur ce réseau par multiplication matrice×vecteur colonne. Comme γ est d'ordre 4, on peut penser cette action comme l'action de i (aussi d'ordre 4) sur le réseau $\mathbb{Z}[i]$. Plus précidément, on définit une opération de produit externe $\cdot : \mathbb{Z}[i] \times \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ donnée par :

$$\forall a, b \in \mathbb{Z},\ v \in \mathbb{Z}^2, \quad (a+ib) \cdot v = av + b\gamma \cdot v$$

On vérifie aisément que ce produit externe munit $\mathbb{Z}^2$ d'une structure de $\mathbb{Z}[i]$-module. Or, on sait que $\mathbb{Z}[i]$ est principal (pour une démonstration de ce fait classique de théorie des nombres, voir le théorème 4.11 de [10]). Donc le théorème de structure des modules de type-fini sur un anneau principal (théorème 3.7.7 de [7]) s'applique et donne que :

$$\mathbb{Z}^2 \simeq \bigoplus_{k=1}^{r} \mathbb{Z}[i]/d_k\mathbb{Z}[i]$$

avec $d_1 | \cdots | d_r$ dans $\mathbb{Z}[i]$, la relation d'isomorphisme $\simeq$ étant valable entre $\mathbb{Z}[i]$-modules. Mais $\mathbb{Z}^2$ est libre donc sans torsion comme $\mathbb{Z}$-module et $\mathbb{Z}^2$ et $\mathbb{Z}[i]$ sont de rang 2 sur $\mathbb{Z}$ donc nécéssairement (un morphisme de $\mathbb{Z}[i]$-modules étant en particulier un morphisme de $\mathbb{Z}$-modules), $\mathbb{Z}^2 \simeq \mathbb{Z}[i]$.

Soit donc $\varphi : \mathbb{Z}[i] \longmapsto \mathbb{Z}^2$ un isomorphisme de $\mathbb{Z}[i]$-modules. Alors $u := \varphi(1)$ et $v := varphi(i)$ engendre $\mathbb{Z}^2$ en tant que $\mathbb{Z}$-module. Il s'ensuit que la matrice de passage de la base canonique à (u, v) est dans $GL_2(\mathbb{Z})$, donc de déterminant ± 1. En outre, on a :

$$\gamma \cdot u = i \cdot \varphi(1) = \varphi(i) = v \quad \text{et} \quad \gamma \cdot v = i \cdot \varphi(i) = \varphi(i^2) = -\varphi(1) = -u$$

Donc, selon que $\det(u, v) = 1$ ou $\det(u, v) = -1$, γ est conjuguée dans $SL_2(\mathbb{Z})$ à $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}$ (en inversant l'ordre de u et v dans la base). D'où (ii).

Le point (iii) se prouve exactement de la même manière en remplaçant $\mathbb{Z}[i]$ par $\mathbb{Z}[e^{\frac{i\pi}{3}}]$ (qui est aussi principal d'après le théorème 4.11 de [10]). Pour prouver le point (ii), il suffit de remarquer que si γ est d'ordre 3, alors $-\gamma$ est d'ordre 6. Le résultat s'en déduit alors immédiatement du point (iii). □

D'après, le lemme précédent, quitte à remplacer τ par un élément de son orbite ($P^{-1} \cdot \tau$ étant stabilisé par γ' si $\gamma = P\gamma' P^{-1}$ avec $P, \gamma' \in SL_2(\mathbb{Z})$), on peut supposer que γ est de la forme $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^{\pm}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{\pm}$ ou $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm}$.

Si $\gamma = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^{\pm}$ ou $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{\pm}$, alors $-\frac{1}{\tau+1} = \tau$ donc $\tau^2 + \tau + 1 = 0$ donc $\tau \in \{1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\}$. Comme $\tau \in \mathbb{H}$, $\tau = e^{\frac{2i\pi}{3}} = \rho$.

Si $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{\pm}$ alors $-\frac{1}{\tau} = \tau$ donc $\tau^2 = -1$ donc $\tau = \pm i$ mais $\tau \in \mathbb{H}$, de sorte que $\tau = i$.

□

Théorème 2.4.0.4. *π_N induit un revêtement de degré $d_0(N) := (SL_2(\mathbb{Z}) : \Gamma_0(N))$ entre $Y_0(N) \setminus \{\Gamma_0(N)i, \Gamma_0(N)\rho\}$ et $SL_2(\mathbb{Z}) \setminus \mathbb{H} \setminus \{SL_2(\mathbb{Z})i, SL_2(\mathbb{Z})\rho\}$.*

Démonstration.

Lemme 2.4.0.5. *Pour tout $\tau \in \mathbb{H}$, il existe un disque ouvert centré en τ, $D_\tau \subset \mathbb{H}$ tel que :*

$$\forall \gamma \in SL_2(\mathbb{Z}), \quad \gamma \cdot D_\tau \cap D_\tau \neq \emptyset \Longrightarrow \gamma \in SL_2(\mathbb{Z})_\tau$$

Démonstration. Soit $r > 0$ tel que $D(\tau, r) \subset \mathbb{H}$. Posons pour tout $n \in \mathbb{N}$, $D_n := D\left(\tau, \frac{r}{2^n}\right)$. Alors pour tout $n \in \mathbb{N}$, $\overline{D_n}$ est compact donc le lemme 2.1.0.2 assure que :

$$E_n := \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \cdot D_n \cap D_n \neq \emptyset\} \subset \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \cdot \overline{D_n} \cap \overline{D_n} \neq \emptyset\}$$

est fini. Ainsi, $(E_n)_{n\in\mathbb{N}}$ est une suite décroissante d'ensembles finis donc elle est constante à partir d'un certain rang $n_0 \in \mathbb{N}$. On a alors :

$$E_{n_0} = \bigcap_{n\in\mathbb{N}} E_n = \left\{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \text{ stabilise } \bigcap_{n\in\mathbb{N}} \overline{D_n} = \{\tau\}\right\} = SL_2(\mathbb{Z})_\tau$$

Il suffit donc de prendre $D_\tau := D_{n_0}$. □

Notons $\varpi_N : \mathbb{H} \longrightarrow Y_0(N)$ et $\pi : \mathbb{H} \longrightarrow Y_0(N)$ les projections canoniques. On sait qu'alors $\pi := \pi_N \circ \varpi_N$. Soient $y \in SL_2(\mathbb{Z}) \setminus \mathbb{H} \setminus \{SL_2(\mathbb{Z})i, SL_2(\mathbb{Z})\rho\}$ et $\tau \in \mathbb{H}$ tel que $y = SL_2(\mathbb{Z})\tau$. Alors $\tau \notin SL_2(\mathbb{Z})i \cup SL_2(\mathbb{Z})\rho$, de sorte que $SL_2(\mathbb{Z})_\tau = \{\pm I_2\}$ d'après la proposition 2.4.0.2, puis que :

$$\forall \gamma \in SL_2(\mathbb{Z}), \quad \gamma \cdot D_\tau \cap D_\tau \neq \emptyset \Longrightarrow \gamma = \pm I_2 \quad (\star)$$

d'après le lemme précédent. Posons $V := \pi(D_\tau)$ et $U := \varpi_N(D_\tau)$. Ce sont des voisinages ouverts respectifs de y et τ car π et ϖ_N sont ouvertes. Alors en remarquant que π_N est la projection canonique pour l'action de $SL_2(\mathbb{Z})/\Gamma_0(N)$ sur $Y_0(N)$, on obtient :

$$\pi_N^{-1}(V) = \pi_N^{-1}(\pi(D_\tau)) = \pi_N^{-1}(\pi_N(U)) = \bigcup_{\overline{\gamma}\in SL_2(\mathbb{Z})/\Gamma_0(N)} \overline{\gamma} \cdot U \quad (\star\star)$$

Mais si $\gamma, \gamma' \in SL_2(\mathbb{Z})$ vérifient $\overline{\gamma}\cdot U \cap \overline{\gamma'}\cdot U \neq \emptyset$ alors $\gamma\Gamma_0(N)D_\tau \cap \gamma'\Gamma_0(N)D_\tau \neq \emptyset$ donc $\gamma\gamma_1 \cdot D_\tau \cap \gamma'\gamma_2 \cdot D_\tau \neq \emptyset$ i.e. $D_\tau \cap \gamma_1^{-1}\gamma^{-1}\gamma'\gamma_2 \cdot D_\tau \neq \emptyset$ pour certains $\gamma_1, \gamma_2 \in \Gamma_0(N)$ et ainsi $\gamma_1^{-1}\gamma^{-1}\gamma'\gamma_2 = \pm I_2$ par $(\star)$, de sorte que $\gamma \equiv \gamma' \bmod SL_2(\mathbb{Z})$ i.e. $\overline{\gamma} = \overline{\gamma'}$. Ainsi, l'union de $(\star\star)$ est une union disjointe d'ouverts.

En outre, pour tout $\gamma \in SL_2(\mathbb{Z})$, $(\pi_N)|^V_{\overline{\gamma}\cdot U} : \overline{\gamma} \cdot U \longrightarrow V$ est surjective. De plus, si $x_1, x_2 \in \overline{\gamma} \cdot U$ vérifient $\pi_N(x) = \pi_N(x')$ alors comme φ_N induit une surjection $\gamma \cdot D_\tau \longrightarrow \overline{\gamma} \cdot U$, on a $x_1 = \varphi_N(\gamma \cdot \tau_1)$ et $x_2 = \varphi_N(\gamma \cdot \tau_2)$ pour $\tau_1, \tau_2 \in D_\tau$. On a alors $\pi(\gamma \cdot \tau_1) = \pi(\gamma \cdot \tau_2)$ donc $\gamma'\gamma \cdot \tau_1 = \gamma \cdot \tau_2$ pour un certain $\gamma' \in SL_2(\mathbb{Z})$ et donc $\gamma^{-1}\gamma'\gamma = \pm I_2$ par $(\star)$, puis $\gamma' = \pm I_2$, de sorte que $\gamma \cdot \tau_1 = \gamma \cdot \tau_2$, puis $x_1 = x_2$. $(\pi_N)|^V_{\overline{\gamma}\cdot U}$ est donc bijective. C'est donc un biholomorphisme.

Ceci montre avec $(\star\star)$ que π_N induit un revêtement de degré $d_0(N) := (SL_2(\mathbb{Z}) : \Gamma_0(N))$ entre $Y_0(N) \setminus \{\Gamma_0(N)i, \Gamma_0(N)\rho\}$ et $SL_2(\mathbb{Z}) \setminus \mathbb{H} \setminus \{SL_2(\mathbb{Z})i, SL_2(\mathbb{Z})\rho\}$. □

Corollaire 2.4.0.6. *$p_N := \overline{j} \circ \pi_N$ induit un revêtement de degré $d_0(N) := (SL_2(\mathbb{Z}) : \Gamma_0(N))$ entre $Y_0(N) \setminus \{\Gamma_0(N)i, \Gamma_0(N)\rho\}$ et $\mathbb{C} \setminus \{0, 1728\}$.*

Démonstration. Il s'agit seulement de déterminer $j(i)$ et $j(\rho)$. Le résultat en découlera immédiatement en vertu du théorème précédent. Or, on sait que (voir [3], paragraphe 5.3) :

$$\forall \tau \in \mathbb{H}, \quad j(\tau) = 1728\frac{g_4(\tau)^3}{g_4(\tau)^3 - 27g_6(\tau)^2}$$

avec :

$$\forall \tau \in \mathbb{H}, \quad g_4(\tau) := \sum_{(n,m)\in\mathbb{N}^2\setminus\{(0,0)\}} \frac{1}{(n+\tau m)^4} \quad \text{et} \quad g_6(\tau) := \sum_{(n,m)\in\mathbb{N}^2\setminus\{(0,0)\}} \frac{1}{(n+\tau m)^6}$$

qui vérifient :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \quad g_4\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{-4} g_4(\tau) \quad \text{et} \quad g_6\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{-6} g_4(\tau)$$

En appliquant ces relations à i, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et g_6 donne $g_6(i) = i^{-6} g_6(i) = -g_6(i)$ donc $g_6(i) = 0$, puis $j(i) = 1728$.

De même, en les appliquant à ρ, $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et g_4 donne $g_4(\rho) = (1+\rho)^{-4} g_4(\rho) = (-\rho^2)^{-4} g_4(\rho) = \rho g_4(\rho)$ donc $g_4(\rho) = 0$, puis $j(\rho) = 0$. □

En fait, on peut même calculer explicitement le degré $d_0(N)$ du revêtement ramifié p_N.

Lemme 2.4.0.7.

$$d_0(N) := (SL_2(\mathbb{Z}) : \Gamma_0(N)) = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

Démonstration. Voir annexe E. □

2.5 L'équation modulaire (PSC).

Le polynôme modulaire d'ordre N, noté Φ_N est un polynôme à deux variables qui intervient dans l'étude des isogénies de noyeau cyclique de degré N. Nous nous en servirons pour obtenir une équation polynomiale entre les fonctions j et $j_N : \tau \in \mathbb{H} \longmapsto j(N\tau)$.

2.5.1 Matrices primitives et morphismes.

Définition 2.5.1.1. *Une matrice 2×2 est dite primitive lorsqu'elle est à coefficients entiers tous premiers entre eux. On définit l'ensemble des matrices primitives de déterminant N comme étant :*

$$P_N := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid pgcd(a,b,c,d) = 1 \text{ et } ad - bc = N \right\}$$

Commençons par remarquer que P_N est stable par multiplication à gauche par tout élément de $SL_2(\mathbb{Z})$. En effet, si un entier d divise tous les coefficients de QP pour $P \in P_N$ et $Q \in SL_2(\mathbb{Z})$ alors il divise tous les coefficients de $Q^{-1}QP = P$, qui sont combinaison linéaires de ceux de QP donc $d = 1$. On peut donc faire agir $SL_2(\mathbb{Z})$ sur P_N par multiplication à gauche.

Lemme 2.5.1.2. *Toutes les matrices de P_N sont équivalentes en prenant des matrices de $SL_2(\mathbb{Z})$ pour matrices de passage.*

Démonstration. Soit $P \in P_N$. D'après le théorème de la forme normale de Smith (théorème 3.7.9 de [7]), on dispose de $Q, R \in SL_2(\mathbb{Z})$ tels que $QPR = \mathrm{Diag}(d_1, d_2)$ avec $d_1, d_2 \in \mathbb{Z}$ et $d_1 | d_2$. En outre, $\mathrm{pgcd}(d_1, d_2) = 1$ car un diviseur commun à d_1 et d_2 divise tous les coefficients de $Q^{-1}\mathrm{Diag}(d_1, d_2)R^{-1} = P$. En outre $d_1 d_2 = N$ donc $d_1 = \pm 1$ et $d_2 = \pm N$. On peut supposer que $d_1 = 1$ et $d_2 = N$, quitte à multiplier Q par $-I_2 \in SL_2(\mathbb{Z})$. Il s'ensuit que toutes les matrices de P_N sont équivalentes à la même matrice donc équivalentes entre elles. □

Lemme 2.5.1.3. *L'ensemble :*

$$R_N := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in P_N \mid 0 \leq b < d \right\}$$

contient un unique représentant de toutes les orbites de P_N sous l'action de $SL_2(\mathbb{Z})$ par multiplication à gauche.

Démonstration. Soit $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in P_N$. Soient $g := \frac{c}{a \wedge c}$ et $h := -\frac{a}{a \wedge c}$, qui sont premiers entre eux et vérifient $ga + fc = 0$. Choisissons aussi $e, f \in \mathbb{Z}$ tels que $eh - fg = 1$ (qui existent d'après le théorème de Bézout). Alors :

$$Q := \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in SL_2(\mathbb{Z})$$

et QP est de la forme :

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$$

avec $a_1, b_1, d_1 \in \mathbb{Z}$. Remarquons qu'en outre, pour tout $k \in \mathbb{Z}$:

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 + kd_1 \\ 0 & d_1 \end{pmatrix}$$

donc on peut choisir k de sorte que $0 \leq b_1 + kd_1 < d_1$. Ceci prouve bien que R_N intersecte toutes les orbites de P_N sous l'action de $SL_2(\mathbb{Z})$.

Soient maintenant $P_1 := \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ et $P_2 := \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ des matrices de P_N dans la même orbite sous l'action de $SL_2(\mathbb{Z})$. Alors on dispose de $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ telle que $P_2 = PP_1$. On a alors :

$$\begin{pmatrix} aa_1 & ab_1 + bd_1 \\ ca_1 & cb_1 + dd_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$$

Donc $c = 0$ (puisque $a_1 d_1 = N \neq 0$ et que $cd_1 = 0$). Donc $\det(P) = ad = 1$, puis $a = d = 1$ (vu que $P = -P$ dans $SL_2(\mathbb{Z})$). Ainsi, $a_1 = a_2$, $d_1 = d_2$ et $ba_1 + b_1 = b_2$. Or, $0 \leq b_2 < d_2 = d_1$ et $0 \leq b_1 < d_1$ donc b_1 et b_2 sont restes de b_2 dans la division euclidienne par d_1 donc par unicité du reste, le qotient b est nul et ainsi $b_1 = b_2$. Donc $P_1 = P_2$. R_N intersecte un seul élément de chaque orbite de P_N sous l'action de $SL_2(\mathbb{Z})$. □

Lemme 2.5.1.4.

$$|R_N| = N \prod_{p|N} \left(1 + \frac{1}{p}\right) = d_0(N)$$

Il y a donc $d_0(N)$ orbites de P_N sous l'action de $SL_2(\mathbb{Z})$.

Démonstration. Voir annexe E □

Maintenant que nous comprenons bien P_N, voyons le lien avec les morphismes. Soient E_1 et E_2 sont deux courbes elliptiques représentées respectivement par des réseaux $\Lambda_1 := \mathbb{Z} \oplus \tau_1 \mathbb{Z}$ et $\Lambda_2 := \mathbb{Z} \oplus \tau_2 \mathbb{Z}$ ($\tau_1, \tau_2 \in \mathbb{H}$) alors un morphisme entre E_1 et E_2 correspond à la multiplication par un certain $\alpha \in \mathbb{C}^*$ telle que $\alpha\Lambda_1 \subset \Lambda_2$. Le noyeau de ce morphisme s'identifie alors avec l'ensemble des $z \in \mathbb{C}/\Lambda_1$ tels que $\alpha z \in \Lambda_2$, c'est à dire au groupe quotient $\Lambda_2/\alpha\Lambda_1$.

Notons P la transposée de la matrice de passage de $(\tau_2, 1)$ (base de Λ_2) à $(\alpha\tau_1, \alpha)$ (base de $\alpha\Lambda_1 \subset \Lambda_2$), de sorte que $\tau_1 = P \cdot \tau_2$. P est bien-sûr à coefficients entiers puisque $\alpha\Lambda_1 \subset \Lambda_2$. Alors on a le résultat suivant :

Proposition 2.5.1.5. *Le groupe $\Lambda_2/\alpha\Lambda_1$ est cyclique d'ordre N si et seulement si $P \in P_N$.*

Démonstration. $\Longrightarrow$ Supposons $\Lambda_2/\alpha\Lambda_1$ cyclique d'ordre N. On applique alors le théorème de la forme

normale de Smith à P (théorème 3.7.9 de [7]) :

$$P = Q \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix} R \quad (\star)$$

avec $Q, R \in SL_2(\mathbb{Z})$ et $d, e \in \mathbb{Z}$ tels que $d|e$. Cette transformation fournit des bases (ω_1, ρ_1) et (ω_2, ρ_2) respectivement de $\alpha\Lambda_1$ et Λ_2 telles que $\omega_1 = d\omega_2$ et $\rho_1 = e\rho_2$. Comme $d|e$ et que tout élément de Λ_2 est combinaison linéaire entière de ω_2 et ρ_2, tout élément de $\Lambda_2/\alpha\Lambda_1$ est d'ordre au plus e, cette borne supérieure étant atteinte par la classe de ρ_2. Donc $e = N$.

Puis, P étant de déterminant ed, et P étant la transposée de la matrice de passage de $(\tau_2, 1)$ base de Λ_2 à $(\alpha\tau_1, \alpha)$ base de $\alpha\Lambda_1$, on a en fait :

$$ed = |\Lambda_2/\alpha\Lambda_1| = N$$

d'après un résultat classique de théorie des réseaux (voir proposition 2.17 de [10]). Ainsi, $d = 1$ et P est primitive par $(\star)$ car un diviseur commun à tous les coefficients de P diviserait $Q^{-1}PR^{-1} = \mathrm{Diag}(1, N)$ donc 1. Ainsi, $P \in P_N$.

$\Longrightarrow$ Supposons $P \in P_N$. Alors d'après le théorème de la forme normale de Smith, on dispose de $Q, R \in SL_2(\mathbb{Z})$ tels que $P = Q\mathrm{Diag}(d, e)R$ avec $d, e \in \mathbb{Z}$ et $d|e$. En outre, $\mathrm{pgcd}(d, e) = 1$ car un diviseur commun à d et e divise tous les coefficients de $Q^{-1}\mathrm{Diag}(d, e)R^{-1} = P$. Ainsi, $d = 1$ et $e = N$ (puisque $de = \det(P) = N$).

Comme précédemment, la transformation de Smith fournit des bases (ω_1, ρ_1) et (ω_2, ρ_2) respectivement de $\alpha\Lambda_1$ et Λ_2 telles que $\omega_1 = \omega_2$ et $\rho_1 = N\rho_2$. Comme justifié précédemment aussi, $|\Lambda_2/\alpha\Lambda_1| = \det(P) = N$ et de plus, la classe de ρ_2 est d'ordre N dans $\Lambda_2/\alpha\Lambda_1$ donc $\Lambda_2/\alpha\Lambda_1$ est cyclique d'ordre N. □

2.5.2 Le polynôme modulaire.

Définition 2.5.2.1. *Une fonction holomorphe $f : \mathbb{H} \longrightarrow \mathbb{C}$ est dite* holomorphe à l'infini *lorsqu'il existe $F : \mathbb{D}^* \longrightarrow \mathbb{C}$ ($\mathbb{D}^*$ étant le disque unité ouvert privé de 0) méromorphe en 0 telle que :*

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

F admet alors un développement méromorphe en 0 :

$$F(q) = \sum_{n \geq -n_0} c_n q^n$$

valable sur $\mathbb{D}^*$ tout entier appelé développement de Fourier à l'infini de f. *Une telle fonction F est alors unique et est notée f^*.*

Proposition 2.5.2.2. *Soit f une fonction méromorphe à l'infini invariante sous l'action de $SL_2(\mathbb{Z})$. Alors f est un polynôme en j à coefficients dans le $\mathbb{Z}$-module engendré par ses coefficients de Fourier.*

Démonstration. On procède par récurrence forte sur $m := -\mathrm{ord}_\infty(f) = -\mathrm{ord}_0(f^*)$. Si $m \leq 0$, alors f est une forme modulaire de poids 0 donc f est constante d'après la proposition 5.17 de [3], donc le résultat désiré est immédiat dans ce cas. Si maintenant $m \in \mathbb{N}^*$ et que l'on suppose le résultat vrai aux rangs $\leq m - 1$. Alors on écrit le développement de Fourier de f :

$$f^*(z) = \sum_{n=-m}^{+\infty} c_n z^n$$

avec $c_{-m} \neq 0$. Comme $\mathrm{ord}_0(j^*) = -1$ de résidu associé égale à 1 (voir § 5.3 de [3]), $f - c_{-m}j^m$ est méromorphe à l'infini d'ordre $-(m-1)$ et toujours invariante sous l'action de $SL_2(\mathbb{Z})$ (car j l'est aussi).

Donc c'est un polynôme en j à coefficients dans le $\mathbb{Z}$-module engendré par les coefficients de Fourier de $f - c_{-m}j^m$, qui sont aussi dans le module engendré par les coefficients de Fourier de f (puisque j est à coefficients de Fourier entiers). D'où le résultat. □

Si f est une fonction méromorphe définie sur $\mathbb{H}$ et si $P := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbb{R})$ est une matrice de déterminant strictement positif alors $\mathbb{H}$ est stable sous l'action de P donnée par $P \cdot \tau = \frac{a\tau+b}{c\tau+d}$ et on peut définir la fonction $f \circ P$ par :

$$\forall \tau \in \mathbb{H}, \quad f \circ P(\tau) = f(P \cdot \tau) = f\left(\frac{a\tau + b}{c\tau + d}\right)$$

Définition 2.5.2.3. *On appalle N-ième polynôme modulaire le polynôme donné par :*

$$\Phi_N(X) = \prod_{P \in R_N} (X - j \circ P)$$

Théorème 2.5.2.4. *Φ_N est à coefficients dans $\mathbb{Z}[j]$.*

Pour prouver ce résultat, nous aurons besoin du lemme suivant :

Lemme 2.5.2.5. *Notons $D_1 := \{z \in \mathbb{C} \mid |z| \leq 1 \text{ et } z \notin]-1, 0]\}$. Soit $f : \mathbb{D}^* \longrightarrow \mathbb{C}$ continue sur $\mathbb{D}^*$, holomorphe sur D_1 et telle que $z \in \mathbb{D}^* \longmapsto z^k f(z)$ est bornée au voisinage de 0 pour un certain $k \in \mathbb{N}$. Alors f est holomorphe sur $\mathbb{D}^*$ et méromorphe en 0.*

Démonstration. Quitte à considérer $z \in \mathbb{D}^* \longmapsto z^{k+1} f(z)$ en lieu et place de f (fonction que l'on peut étendre par continuité en 0), on peut supposer f continue sur $\mathbb{D}$, le disque unité tout entier et montrer qu'alors f est holomorphe sur $\mathbb{D}$ (en divisant par z^{k+1}, on obtiendra une fonction méromorphe en 0). D'après le théorème de Morera, il suffit de montrer que :

$$\int_R f(z)dz = 0$$

pour tout rectangle $R \subset \mathbb{D}$ de côtés parallèles aux axes des abscisses et des ordonnées du plan complexe. On sait déjà que c'est vrai lorsque $R \subset D_1$. Il reste à le montrer lorsque R traverse $]-1, 0]$. Or, si $A, B, C, D, E, F \in \mathbb{D}$ sont tels que $ABCD$ et $DCEF$ sont des rectangles de côtés parallèles aux axes des abscisses et des ordonnées alors :

$$\begin{aligned}
\int_{ABEF} f(z)dz &= \int_A^B f(z)dz + \int_B^E f(z)dz + \int_E^F f(z)dz + \int_F^A f(z)dz \\
&= \int_A^B f(z)dz + \int_B^C f(z)dz + \int_C^E f(z)dz + \int_E^F f(z)dz + \int_F^D f(z)dz + \int_D^A f(z)dz \\
&= \int_A^B f(z)dz + \int_B^C f(z)dz + \int_C^D f(z)dz + \int_D^A f(z)dz + \int_D^C f(z)dz + \int_C^E f(z)dz \\
&+ \int_E^F f(z)dz + \int_F^D f(z)dz \\
&= \int_{ABCD} f(z)dz + \int_{DCEF} f(z)dz
\end{aligned}$$

Avec un tel découpage, on se ramène simplement à montrer que $\int_{ABCD} f(z)dz = 0$ lorsque $ABCD$ est un rectangle tel que $A, B \in D_1$ et $C, D \in]-1, 0]$. Supposons pour fixer les idées que $\mathrm{Im}(A) = \mathrm{Im}(B) < 0$ (le cas inverse se traitant de le même manière). Alors pour tout $\varepsilon > 0$ suffisamment petit, $C_\varepsilon := C - i\varepsilon$ et $D_\varepsilon := D - i\varepsilon$ sont tels que $ABC_\varepsilon D_\varepsilon \subset D_1$, de sorte que :

$$\int_{ABC_\varepsilon D_\varepsilon} f(z)dz = 0$$

Or, f est continue sur le pavé P délimité par $ABCD$ qui est compact donc uniformément continue sur P d'après le théorème de Heine. Ainsi, pour $\delta > 0$ fixé, il existe $\varepsilon > 0$ tel que :

$$\forall z, z' \in P, \quad |z - z'| < \varepsilon \Longrightarrow |f(z) - f(z')| < \delta$$

Mais alors :

$$\begin{aligned}\left|\int_{ABCD} f(z)dz - \int_{ABC_\varepsilon D_\varepsilon} f(z)dz\right| &\leq \left|\int_{C_\varepsilon}^{C} f(z)dz\right| + \left|\int_{C}^{D} f(z)dz - \int_{C_\varepsilon}^{D_\varepsilon} f(z)dz\right| + \left|\int_{D}^{D_\varepsilon} f(z)dz\right| \\ &\leq 2\varepsilon \max_{z\in P} |f(z)| + |D - C|\delta\end{aligned}$$

Ainsi $\int_{ABC_\varepsilon D_\varepsilon} f(z)dz \longrightarrow \int_{ABCD} f(z)dz$ quand $\varepsilon \longrightarrow 0$, puis :

$$\int_{ABCD} f(z)dz = 0$$

ce qui conclut. □

Démonstration. (du théorème 2.5.2.4)

Les coefficients de Φ_N sont des polynômes symétriques en $j \circ P$ pour $P \in R_N$. En outre, si $P \in R_N$ et $Q \in SL_2(\mathbb{Z})$ alors $PQ \in P_N$ et donc on dispose de $P' \in R_N$ et de $Q' \in SL_2(\mathbb{Z})$ tellles que $Q'P' = PQ$ d'après le lemme 2.5.1.3, de sorte que $j \circ P \circ Q = j \circ Q' \circ P' = j \circ P'$. Puis, si $P_2 \in R_N$ vérifie $Q_2'P' = P_2Q_2$ avec $Q_2, Q_2' \in SL_2(\mathbb{Z})$ alors P_2 et P sont dans la même orbite sous l'action de $SL_2(\mathbb{Z})$ et donc $P = P_2$ d'après le lemme 2.5.1.3. Donc la composition des fonctions $j \circ P$ par Q ne fait que les permuter et aisni tous les coefficients de Φ_N sont invariants sous l'action de $SL_2(\mathbb{Z})$.

En outre, on a vu que le développement de Fourier de j s'écrit :

$$j^*(q) = \frac{1}{q} + \sum_{k=0}^{+\infty} c_k q^k$$

Donc si $P := \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R_N$ alors en posant $q : \tau \in \mathbb{H} \longmapsto e^{2i\pi\tau} \in \mathbb{D}^*$, on a :

$$j(P \cdot \tau) = j\left(\frac{a\tau + b}{d}\right) = \frac{1}{q(\tau)^{\frac{a}{d}}\zeta_d^b} + \sum_{k=0}^{+\infty} c_k q(\tau)^{\frac{ak}{d}} \zeta_d^{kb} \quad (2)$$

avec $\zeta_d := e^{\frac{2i\pi}{d}} = e^{\frac{2ia\pi}{N}}$. Ainsi, $\tau \longmapsto q(\tau)^N j(P\cdot\tau)$ (2) est bornée quand $\tau \longrightarrow \infty$ (puisque $ad = N$). De même qu'à j nous associons un développement de Fourier, nous allons donner un développement analogue pour $j \circ P$, qui n'est en général pas méromorphe à l'infini. Considérons la fonction logarithme complexe principal log définie et holomorphe sur $\mathbb{C} \setminus \mathbb{R}_-$ et dont l'expression est donnée par :

$$\forall r > 0, \theta \in]-\pi, \pi[, \quad \log(re^{i\theta}) = \log(r) + i\theta$$

On peut étendre log aux valeurs $\theta = \pi$ par cette formule ci-dessus mais on a alors une discontinuité sur $\mathbb{R}_-^*$. Il est alors immédiat que $j^* = j \circ \frac{1}{2i\pi} \log$ (en dépit de la discontinuité puisque j est invariante sous l'action $\tau \longmapsto \tau + 1$ qui correspond à une rotation sur $\mathbb{D}^*$ lorsque l'on compose par q). Considérons la fonction $(j \circ P)^* := j \circ P \circ \frac{1}{2i\pi} \log$, définie sur $\mathbb{D}^*$ mais a priori discontinue sur $]-1, 0[$. Alors (1) assure que sur $D_1 := \mathbb{D}\setminus]-1, 0]$:

$$(j \circ P)^*(q) = \frac{1}{q^{\frac{a}{d}}\zeta_d^b} + \sum_{k=0}^{+\infty} c_k q^{\frac{ak}{d}} \zeta_d^{kb} \quad (3)$$

les puissances étant définies à partir de log via la formule $q^\alpha := \exp(\alpha \log(q))$ pour tout $\alpha \in \mathbb{R}$ et $q \in D_1$.

Cette formule est toujours valide sur $]-1,0[$ via le prolongement de log mais elle n'établit le caractère holomorphe de $(j\circ P)^*$ que sur D_1.

Soit f un coefficient de Φ_N. Comme f est un polynôme symétrique en les $j\circ P$ ($P\in R_N$), $f^*:=f\circ\frac{1}{2i\pi}\log$ est aussi holomorphe sur D_1. Elle est aussi continue sur $]-1,0[$ car on a vu que f est invariante sous l'action de $SL_2(\mathbb{Z})$, donc en particulier sous l'effet de la translation $\tau\longmapsto\tau+1$. Ainsi, vu (2) et le lemme 2.5.2.5, f^* est holomorphe sur $\mathbb{D}^*$ et méromorphe en 0. f^* admet donc un développement en série de Laurent :

$$f^*(q)=\sum_{k\leq -k_0}c_kq^k \quad (4)$$

Or, (3) assure aussi que f^* admet un développement en puissances de $q^{\frac{1}{N}}$:

$$f^*(q)=\sum_{l\leq -l_0}d_lq^{\frac{l}{N}} \quad (5)$$

à coefficents dans $\mathbb{Z}[\zeta_N]$ (où $\zeta_N:=e^{\frac{2i\pi}{N}}$). Il s'ensuit que $g:q\longmapsto q^{\max(Nk_0,l_0)+1}f^*(q^N)$ définit une fonction holomorphe sur $\mathbb{D}$ tout entier et admet donc un développement de Taylor. Or par (4) et (5) :

$$g(q)=\sum_{k\leq -k_0}c_kq^{kN+\max(Nk_0,l_0)+1}=\sum_{l\leq -l_0}d_lq^{l+\max(Nk_0,l_0)+1}$$

L'unicité du développement de Taylor assure que les deux développements (4) et (5) sont égaux donc en particulier que les puissances fractionnaires de q disparaissent de (5) et que les c_k sont tous dans $\mathbb{Z}[\zeta_N]$.

Ainsi, f^* peut être vu comme un série formelle de $\mathbb{Z}[\zeta_N]((q))\subset\mathbb{Q}(\zeta_N)((q))$. Cette identification est licite par unicité du développement en série de Laurent.

Faisons agir $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ sur $\mathbb{Q}(\zeta_N)((q))$ de la manière suivante : si $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ et $g=\sum_{k\geq k_0}a_kq^k\in\mathbb{Q}(\zeta_N)((q))$ alors :

$$\sigma(g):=\sum_{k\geq k_0}\sigma(a_k)q^k$$

Or, on sait (par le théorème 6.3.1 de [7]) que $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ envoie ζ_N sur ζ_N^r pour un certain $r\in\mathbb{Z}$ inversible modulo N. Ainsi, par (3), on a pour $P:=\begin{pmatrix}a&b\\0&d\end{pmatrix}\in R_N$ fixée :

$$\sigma((j\circ P)^*)=\frac{1}{q^{\frac{a}{d}}\zeta_d^{rb}}+\sum_{k=0}^{+\infty}c_kq^{\frac{ak}{d}}\zeta_d^{krb}$$

Or, rb reste premier avec a et d car r est inversible modulo $N=ad$. Ainsi, on voit immédiatement que $\sigma((j\circ P)^*)=j\circ P'$ avec $P':=\begin{pmatrix}a&b'\\0&d\end{pmatrix}\in R_N$, b' étant le reste de rb dans la division euclidienne par d. Donc $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ permutte les fonctions $j\circ P$ ($P\in R_N$). Comme f^* est symétrique en les variables $(j\circ P)^*$ ($P\in R_N$), f^* est donc invariant sous l'action de ce groupe de Galois. Ainsi, $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ fixe tous les coefficients du développement en puissances de q de f qui sont dans $\mathbb{Z}[\zeta_N]$, comme nous l'avons vu. Ainsi, tous ces coefficients sont dans $\mathbb{Z}[\zeta_N]\cap\mathbb{Q}$ (d'après la proposition 5.6.11 de [7]). Mais $\mathbb{Z}[\zeta_N]\cap\mathbb{Q}=\mathbb{Z}$ car tous les éléments de $\mathbb{Z}[\zeta_N]$ sont entiers algébriques puisque ζ_N est entier algébrique. Ainsi, $f^*\in\mathbb{Z}((q))$.

f est donc méromorphe à l'infini et invariante sous l'action de $SL_2(\mathbb{Z})$. On conclut alors avec la proposition 2.5.2.2 que $f\in\mathbb{Z}[j]$. D'où le résultat. □

Remarque 2.5.2.6. Le développement de Fourier :

$$j^*(q)=\frac{1}{q}+\sum_{k\geq 0}a_kq^k$$

assure que j est transcendant sur $\mathbb{C}$ ce qui permet de voir j et X comme deux variables algébriquement indépendantes et Φ_N comme un polynôme à deux variables $\Phi_N(X,j) \in \mathbb{Z}[X,j]$.

Corollaire 2.5.2.7. *$\Phi_N(X,j)$ est irréductible sur $\mathbb{C}(j)$.*

Démonstration. Par définition, $\Phi_N(X,j) = \prod_{P\in R_N}(X - j\circ P)$ est scincé sur $\mathbb{C}(j,(j\circ P)_{P\in R_N})$. Or, pour tout $Q \in SL_2(\mathbb{Z})$, $f \in \mathbb{C}(j,(j\circ P)_{P\in R_N}) \longmapsto f\circ P \in \mathbb{C}(j,(j\circ P)_{P\in R_N})$ est un automorphisme de la $\mathbb{C}(j)$-algèbre $\mathbb{C}(j,(j\circ P)_{P\in R_N})$ et l'action de $SL_2(\mathbb{Z})$ ainsi définie permute transitivement les $j\circ P$ ($P \in R_N$) comme ceci a été justifié dans la preuve du théorème 2.5.2.4. Il s'ensuit que $\mathrm{Gal}(\mathbb{C}(j,(j\circ P)_{P\in R_N})/\mathbb{C}(j))$ permute transitivement les racines de $\Phi_N(X,j)$, donc que ce polynôme est irréductible.

□

Proposition 2.5.2.8. *$\Phi_N(j,j)$ est un polynôme en j à coefficients entiers non constant.*

Démonstration. On sait déjà que $\Phi_N(j,j)$ est un polynôme en j d'après le théorème 2.5.2.4 donc qu'il admet un dévelopement de Fourier à l'infini à coefficients entiers. Pour toute matrice $P := \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R_N$, on a :

$$(j\circ P)^*(q) = \frac{1}{q^{\frac{a}{d}}\zeta_d^b} + \sum_{k=0}^{+\infty} c_k q^{\frac{ak}{d}} \zeta_d^{kb}$$

Comme nous l'avons vu dans la preuve du théorème 2.5.2.4. Ainsi, les termes d'ordre négatif de $j^*(q) - (j\circ P)^*(q)$, à savoir $\frac{1}{q}$ et $-\frac{1}{q^{\frac{a}{d}}\zeta_d^b}$ ne se compensent que lorsque $a = d$ et $b = 0$, auquel cas les entiers a, b et d ne sont pas premiers entre eux, ce qui est impossible car $P \in R_N$. Ainsi, le développement de Fourier à l'infini de $\Phi_N(j,j) = \prod_{P\in R_N}(j - j\circ P)$ admet un terme d'ordre < 0. Comme nous l'avons vu dans la preuve de la proposition 2.5.2.2, c'est donc un polynôme en j de degré > 0. □

2.6 La clôture intégrale de $\overline{\mathbb{Q}}[j]$ dans $\overline{\mathbb{Q}}(j, j_N)$ et la surface de Riemann $X(\mathbb{C})$.

Comme R_N contient la matrice $\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, la fonction :

$$j_N : \tau \in \mathbb{H} \longmapsto j(N\tau) = j\circ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}(\tau)$$

est racine de $\Phi_N(X,j) \in \mathbb{Z}[j][X]$, qui est irréductible sur $\mathbb{C}(j)$ (donc a fortiori sur $\overline{\mathbb{Q}}(j)$) d'après le corollaire 2.5.2.7. Comme $\Phi_N(X,j)$ est unitaire et à coefficients dans $\mathbb{Z}[j] \subset \overline{\mathbb{Q}}(j)$ d'après le théorème 2.5.2.4, c'est le polynôme minimal de j_N sur $\overline{\mathbb{Q}}(j)$. Ainsi, $\overline{\mathbb{Q}}(j,j_N) = \overline{\mathbb{Q}}(j)(j_N)$ est une extension de degré $\deg\Phi_N(X,j) = d_0(N) = N\prod_{p|N}\left(1+\frac{1}{p}\right)$ (comme nous l'avons vu au lemme 2.5.1.4). Comme $\Phi_N(X,j)$ est séparable (car c'est un polynôme irréductible sur un corps de caractéristique nulle), $\overline{\mathbb{Q}}(j,j_N)/\overline{\mathbb{Q}}(j)$ est séparable.

Considérons $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ la clôture intégrale de $\overline{\mathbb{Q}}[j]$ dans $\overline{\mathbb{Q}}(j,j_N)$.

Proposition 2.6.0.1. *$\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est un $\overline{\mathbb{Q}}[j]$-module libre type fini de rang $d_0(N)$ et une $\overline{\mathbb{Q}}$-algèbre de type fini, c'est à dire isomorphe à une $\overline{\mathbb{Q}}$-algèbre de la forme :*

$$\overline{\mathbb{Q}}[X_1,\cdots,X_r]/I$$

avec I un idéal premier de $\overline{\mathbb{Q}}[X_1,\cdots,X_r]$.

Démonstration. $\overline{\mathbb{Q}}(j, j_N)/\overline{\mathbb{Q}}(j)$ est finie et séparable et $\overline{\mathbb{Q}}[j] \simeq \overline{\mathbb{Q}}[X]$ car j est transcendant d'après la remarque 2.5.2.6. Or, $\overline{\mathbb{Q}}[X]$ est principal. Le point (ii) de la proposition B.4.0.1 assure alors que $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est un $\overline{\mathbb{Q}}[j]$-module libre de type fini de rang $d_0(N)$.

Soient $x_1, \cdots, x_{r-1} \in \mathcal{A}_{N,\overline{\mathbb{Q}}}$ des générateurs de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ comme $\overline{\mathbb{Q}}[j]$-module. Alors $x_1, \cdots, x_{r-1}, j$ engendrent $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ comme $\overline{\mathbb{Q}}$-algèbre. Considérons :

$$\begin{array}{rcl} \varphi : \overline{\mathbb{Q}}[X_1, \cdots, X_r] & \longrightarrow & \mathcal{A}_{N,\overline{\mathbb{Q}}} \\ P(X_1, \cdots, X_r) & \longmapsto & P(x_1, \cdots, x_{r-1}, j) \end{array}$$

Alors φ est un morphisme de $\overline{\mathbb{Q}}$-algèbre surjectif et induit donc un isomorphisme de $\overline{\mathbb{Q}}[X_1, \cdots, X_r]/\ker(\varphi)$ vers $\mathcal{A}_{N,\overline{\mathbb{Q}}}$. Mais $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est intègre donc $I := \ker(\varphi)$ est premier, ce qui conclut. □

Comme $\overline{\mathbb{Q}}[X_1, \cdots, X_r]$ est nothérien, il existe $F_1, \cdots, F_s \in \overline{\mathbb{Q}}[X_1, \cdots, X_r]$ une famille de polynôme engendrant l'déal I de la proposition précédente. On définit la variétés algébriques affines suivantes :

$$X(\overline{\mathbb{Q}}) := \{(x_1, \cdots, x_r) \in \overline{\mathbb{Q}}^r \mid \forall 1 \leq i \leq s, \quad F_i(x_1, \cdots, x_r) = 0\}$$

$$X(\mathbb{C}) := \{(x_1, \cdots, x_r) \in \mathbb{C}^r \mid \forall 1 \leq i \leq s, \quad F_i(x_1, \cdots, x_r) = 0\}$$

Proposition 2.6.0.2. *L'application :*

$$\Upsilon : \varphi \in Hom_{\overline{\mathbb{Q}}-alg}(\mathcal{A}_{N,\overline{\mathbb{Q}}}, \mathbb{C}) \longmapsto (\varphi(\overline{X_1}), \cdots, \varphi(\overline{X_r}))$$

où la barre supérieure sur les $\overline{X_i}$ désigne la réduction modulo I dans $\overline{\mathbb{Q}}[X_1, \cdots, X_r]$, est une bijection entre l'ensemble des morphismes de $\overline{\mathbb{Q}}$-algèbres de $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$ vers $\mathbb{C}$, $Hom_{\overline{\mathbb{Q}}}(\mathcal{A}_{N,\overline{\mathbb{Q}}}, \mathbb{C})$, et la variété $X(\mathbb{C})$.

Démonstration. Soit $\varphi \in \mathrm{Hom}_{\overline{\mathbb{Q}}-alg}(\mathcal{A}_{N,\overline{\mathbb{Q}}}, \mathbb{C})$. Alors pour tout $i \in \{1, \cdots, s\}$:

$$F_i(\varphi(\overline{X_1}), \cdots, \varphi(\overline{X_r})) = \varphi(F_i(\overline{X_1}, \cdots, \overline{X_r})) = \varphi(\overline{F_i}) = 0$$

Donc Υ est bien à valeurs dans $X(\mathbb{C})$.

Υ est clairement injective car $\varphi \in \mathrm{Hom}_{\overline{\mathbb{Q}}-alg}(\mathcal{A}_{N,\overline{\mathbb{Q}}}, \mathbb{C})$ est entièrement déterminé par ses valeurs en les $\overline{X_i}$ vu que $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \mathbb{Q}[X_1, \cdots, X_r]/I$.

Soit $(x_1, \cdots, x_r) \in X(\mathbb{C})$. On définit un morphisme de $\overline{\mathbb{Q}}$-algèbre $\psi : \overline{\mathbb{Q}}[X_1, \cdots, X_r] \longrightarrow \mathbb{C}$ donné par $\psi(X_i) := x_i$ pour tout $i \in \{1, \cdots, r\}$. Alors :

$$\forall 1 \leq i \leq s, \quad \psi(F_i) = F_i(\psi(X_1), \cdots, \psi(X_r)) = F_i(x_1, \cdots, x_r) = 0$$

Donc ψ s'annule sur I et induit donc un morphisme $\overline{\psi} : \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I \simeq \mathcal{A}_{N,\overline{\mathbb{Q}}} \longrightarrow \mathbb{C}$. Ainsi, Υ est surjective et réalise donc bien une bijection. □

Théorème 2.6.0.3. *$X(\mathbb{C})$ peut être munie d'une structure de surface de Riemann.*

Démonstration. La preuve consiste à montrer que la matrice jacobienne de $F := (F_1, \cdots, F_s)$ est de rang $r - 1$ et d'appliquer l'analogue complexe du théorème du rang constant pour définir les cartes. Un tel résultat fait appel à la théorie des fonctions holomorphes de plusieurs variables expliquée dans [12]. Nous introduirons ultérieurement les notions nécessaires.

Étape 1 : Pour le moment, calculons $\mathrm{rgJac}_P(F)$ lorsque $P \in X(\overline{\mathbb{Q}})$ (nous verrons à quoi sert cette hypothèse restrictive). Il peut être utile de se reporter à l'annexe D concernant les espaces tangents aux variétés algébriques affines pour bien comprendre ce calcul. On sait que $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X_1, \cdots, X_r]/(F_1, \cdots, F_s) \simeq \overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]$, ce dernier ensemble étant l'algèbre des fonctions polynomiales sur $X(\overline{\mathbb{Q}})$. Comme $\overline{\mathbb{Q}}(j, j_N)/\overline{\mathbb{Q}}(j)$

est finie et séparable, que $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est la clôture intégrale de $\overline{\mathbb{Q}}[j]$ dans cet extension et que $\overline{\mathbb{Q}}[j]$ est de Dedekind, la proposition B.5.0.3 assure que $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]$ est de Dedekind. Comme $\overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]_P$ est la localisation de $\overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]$ par l'idéal premier :

$$M_P := \{f \in \overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})] \mid f(P) = 0\}$$

le corollaire B.6.0.6 assure que c'est un anneau de valuation discrète d'unique idéal maximal principal :

$$\mathfrak{m}_P = \{f \in \overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]_P \mid f(P) = 0\}$$

Soit $t \in \mathfrak{m}_P$ une uniformisante en P, c'est à dire un générateur de $\mathfrak{m}_P$. Alors :

$$f \longmapsto \frac{f}{t}$$

induit un isomorphisme $\overline{\mathbb{Q}}$-linéaire $\mathfrak{m}_P/\mathfrak{m}_P^2 \simeq \overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]_P/\mathfrak{m}_P$. Or, $\overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]_P/\mathfrak{m}_P$ est un corps car $\mathfrak{m}_P$ est maximal et c'est de plus une $\overline{\mathbb{Q}}$-algèbre. De plus, $\mathfrak{m}_P/\mathfrak{m}_P^2$ est un $\overline{\mathbb{Q}}$-espace vectoriel de dimension finie car $\ker(dF_P) \simeq T_P(V) \simeq (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$ aussi d'après la proposition D.0.0.6 et le corollaire D.0.0.5. $\overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]_P/\mathfrak{m}_P$ est donc une extension finie donc algébrique de $\overline{\mathbb{Q}}$, qui est algébriquement clos, de sorte que :

$$\overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]_P/\mathfrak{m}_P \simeq \overline{\mathbb{Q}}$$

Ainsi, $\ker(dF_P) \simeq (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$ est de dimension 1 sur $\overline{\mathbb{Q}}$. On déduit alors immédiatement du théorème du rang que $\mathrm{rgJac}_P(F) = r - 1$.

Étape 2 : Calculons maintenant $\mathrm{rg}_{\mathbb{C}}\mathrm{Jac}_P(F)$ lorsque $P \in X(\mathbb{C})$. On ne peut plus ici travailler dans $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I \simeq \overline{\mathbb{Q}}[X(\overline{\mathbb{Q}})]$, mais seulement dans $\mathbb{C}[X(\mathbb{C})] \simeq \mathbb{C}[X_1, \cdots, X_r]/I_{\mathbb{C}}$ où $I_{\mathbb{C}}$ est l'idéal de $\mathbb{C}[X_1, \cdots, X_r]$ engendré par I. Montrons que $I_{\mathbb{C}}$ est toujours premier afin de pouvoir appliquer les résultats de l'annexe D.

Lemme 2.6.0.4. *$\mathbb{C}[X_1, \cdots, X_r]/I_{\mathbb{C}}$ est isomorphe en tant que $\overline{\mathbb{Q}}$-algèbre à $\mathbb{C} \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$*

Démonstration. Considérons :

$$(\lambda, P) \in \mathbb{C} \times \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I \longmapsto \lambda P \in \mathbb{C}[X_1, \cdots, X_r]/I_{\mathbb{C}}$$

Cette application est bien définie et $\overline{\mathbb{Q}}$-bilinéaire donc par propriété universelle du produit tensorille, elle induit une application $\overline{\mathbb{Q}}$-bilinéaire $\varphi : \mathbb{C} \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I \longrightarrow \mathbb{C}[X_1, \cdots, X_r]/I_{\mathbb{C}}$ vérifiant :

$$\forall (\lambda, P) \in \mathbb{C} \times \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I, \quad \varphi(\lambda \otimes P) = \lambda P$$

φ est clairement surjective puisque $\varphi(\lambda \otimes \overline{X_1}^{i_1} \cdots \overline{X_r}^{i_r}) = \lambda \overline{X_1}^{i_1} \cdots \overline{X_r}^{i_r}$ pour tous $\lambda \in \mathbb{C}$ et $i_1, \cdots, i_r \in \mathbb{N}$.

Soit $x \in \mathbb{C} \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$ tel que $\varphi(x) = 0$. Alors $x = \sum_{i=1}^m \lambda_i \otimes P_i$ avec $\lambda_1, \cdots, \lambda_m \in \mathbb{C}$ et $P_1, \cdots, P_m \in \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$. Soit $E := \overline{\mathbb{Q}}(\lambda_1, \cdots, \lambda_m)$. Alors d'après le lemme B.8.0.3, E est une extension finie d'un certain corps $\overline{\mathbb{Q}}(t_1, \cdots, t_n)$ avec $t_1, \cdots, t_n \in E$ algébriquement indépendants. Comme $\overline{\mathbb{Q}}(t_1, \cdots, t_n)$ est de caractéristique nulle, $E/\overline{\mathbb{Q}}(t_1, \cdots, t_n)$ est une extension finie de corps parfaits donc est séparable (corollaire 5.6.12 de [7]) donc $E = \overline{\mathbb{Q}}(t_1, \cdots, t_n)[\alpha]$ pour un certain $\alpha \in E$ algébrique d'après le théorème de l'élément primitif (théorème 5.4.6 de [7]). Quitte à multiplier les λ_i par leurs dénominateurs dans $\overline{\mathbb{Q}}[t_1, \cdots, t_n]$, on peut supposer que $x \in \overline{\mathbb{Q}}[t_1, \cdots, t_n][\alpha] \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$. Mais $\overline{\mathbb{Q}}[t_1, \cdots, t_n][\alpha] \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$ s'identifie à $(\overline{\mathbb{Q}}[X_1, \cdots, X_r]/I)[t_1, \cdots, t_n][\alpha]$ via φ d'après le lemme B.8.0.2. Ainsi, $x = 0$. □

La proposition B.8.0.4 et le lemme précédent assurent que $\mathbb{C}[X_1, \cdots, X_r]/I_{\mathbb{C}}$ est intègre donc que $I_{\mathbb{C}}$ est premier, ce qu'il fallait démontrer. Les résultats de l'annexe D s'appliquent alors toujours et assurent

que $\ker(dF_P) \simeq (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$.

Supposons par l'absurde que $\mathfrak{m}_P/\mathfrak{m}_P^2 = \{0\}$ alors $\mathfrak{m}_P = \mathfrak{m}_P^2$. Mais $\mathfrak{m}_P$ est un idéal de $\mathbb{C}[X(\mathbb{C})]_P$ et un $\mathbb{C}[X(\mathbb{C})]$-module de type fini engendré par les $\overline{X_j - x_j}$ $(1 \leq j \leq r)$ si l'on écrit $P := (x_1, \cdots, x_r)$. Ainsi, le lemme de Nakayama (lemme B.2.0.1) donne que $(1-a)\mathfrak{m}_P = \{0\}$ pour un certain $a \in \mathfrak{m}_P$. Mais $\mathbb{C}[X(\mathbb{C})]_P$ est intègre donc en fait, $\mathfrak{m}_P = \{0\}$.

Ainsi, $\overline{X_j - x_j} = 0$ pour tout $j \in \{1, \cdots, n\}$ donc $\mathbb{C}$ se surjecte dans $\mathbb{C}[X(\mathbb{C})] \simeq \mathbb{C}[X_1, \cdots, X_r]/I_{\mathbb{C}}$. Ainsi, $\mathbb{C}[X(\mathbb{C})] = \{0\}$ ou $\mathbb{C}$. Autrement dit, $I_{\mathbb{C}}$ est maximal ou $I_{\mathbb{C}} = \mathbb{C}[X_1, \cdots, X_r]$. Dans le cas où $I_{\mathbb{C}}$ est maximal, $X(\mathbb{C})$ est un singleton (d'après le corollaire 1.21 de [3], conséquence du théorème des zéros algébrique) donc $X(\overline{\mathbb{Q}}) \subset X(\mathbb{C})$ est vide ou un singleton. $X(\overline{\mathbb{Q}}) \neq \emptyset$ puisque sinon, on aurait $I = \overline{\mathbb{Q}}[X_1, \cdots, X_r]$ d'après la version faible théorème des zéros géométrique (théorème 2.4 de [3]) donc $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I = \{0\}$, ce qui est exclus. Donc $X(\overline{\mathbb{Q}})$ est un singleton et ainsi, I est maximal, et $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$ est de dimension finie sur $\overline{\mathbb{Q}}$ d'après le théorème des zéros algébrique (théorème 1.20 de [3]). Mais $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ contient $\overline{\mathbb{Q}}[j] \simeq \overline{\mathbb{Q}}[X]$ donc c'est impossible. Pour les mêmes raisons, le cas $I_{\mathbb{C}} = \mathbb{C}[X_1, \cdots, X_r]$ est aussi exclus.

On en déduit que $\ker(dF_P) \simeq (\mathfrak{m}_P/\mathfrak{m}_P^2)^* \neq \{0\}$ et donc que $\mathrm{rg}_{\mathbb{C}}\mathrm{Jac}_P(F) \leq r-1$.

Supposons par l'absurde que $\mathrm{rgJac}_P(F) < r-1$. Alors P est non seulement zéro des F_i mais aussi des polynômes qui caractérisent l'inégalité $\mathrm{rg}_{\mathbb{C}}\mathrm{Jac}_P(F) < r-1$, autrement dit, des polynômes :

$$\forall 1 \leq i \leq r,\ J \subset \{1, \cdots, s\}, |J| = r-1, \quad G_{i,J} := \det\left(\frac{\partial F_k}{\partial X_l}\right)_{\substack{1 \leq k \neq i \leq r \\ l \in J}}$$

Notons J et $J_{\mathbb{C}}$ les idéaux engendrés par $I = (F_1, \cdots, F_s)$ et les $G_{i,J}$ respectivement dans $\overline{\mathbb{Q}}[X_1, \cdots, X_r]$ et dans $\mathbb{C}[X_1, \cdots, X_r]$. Alors $P \in V(J_{\mathbb{C}})$ donc $J_{\mathbb{C}} \subsetneq \mathbb{C}[X_1, \cdots, X_r]$ et ainsi, $J \subsetneq \overline{\mathbb{Q}}[X_1, \cdots, X_r]$ et $V(J) \neq \emptyset$ d'après la version faible du théorème des zéros (théorème 2.4 de [3]). Donc on dispose de $Q \in X(\overline{\mathbb{Q}})$ tel que $\mathrm{rgJac}_P(F) < r-1$, ce qui contredit le résultat de l'étape 2. Ainsi, $\mathrm{rgJac}_P(F) = r-1$.

Étape 3 : Appliquons maintenant cela à la construction d'une structure de surface de Riemann sur $X(\mathbb{C})$. Introduisons pour cela la théorie des fonctions holomorphes de plusieurs variables détaillée dans [12]. Une fonction $G : U \longrightarrow V$ où U est un ouvert de $\mathbb{C}^n$ et V un ouvert de $\mathbb{C}^m$ est dite holomorphe si elle est de classe $\mathcal{C}^1$ (via l'identification réelle usuelle) et que sa différentielle est $\mathbb{C}$-linéaire. Ceci équivaut à ce que les composantes G_i de G soient holomorphes en chacunes de leurs variables en fixant toutes les autres (corollaire 2.8 de [12]), ce qui est manifestement le cas pour :

$$F : (x_1, \cdots, x_r) \in \mathbb{C}^r \longmapsto (F_1(x_1, \cdots, x_r), \cdots, F_s(x_1, \cdots, x_r)) \in \mathbb{C}^s$$

car les F_i sont ploynomiales. La composée de deux fonctions holomorphes est holomorphe (théorème 5.3 de [12]). Les fonctions holomorphes de différentielle inversible (comme application $\mathbb{C}$-linéaire) vérifient le théorème d'inversion locale holomorphe (théorème 5.5 de [12]), à partir duquel on démontre le théorème du rang constant (variante du corollaire 5.6 de [12]).

En particulier, l'étape 2 assure donc que pour tout $P \in X(\mathbb{C})$, il existe $U \subset \mathbb{C}^r$ et $V \subset \mathbb{C}^s$ des voisinages ouverts de 0, $\Phi_P : U \longrightarrow \mathbb{C}^r$ et $\Psi_P : V \longrightarrow \mathbb{C}^s$ induisant des biholomorphismes sur leurs images respectives et tels que $\Phi_P(0) = P$ et :

$$\forall (z_1, \cdots, z_r) \in U, \quad \Psi_P \circ F \circ \Phi_P(z_1, \cdots, z_r) = (z_1, \cdots, z_{r-1}, 0, \cdots, 0)$$

On en déduit que :

$$X(\mathbb{C}) \cap \Phi_P(U) = \{\Phi_P(0, \cdots, 0, z_r) \mid (0, \cdots, 0, z_r) \in U\}$$

On définit ainsi un atlas holomorphe sur $X(\mathbb{C})$ en prenant $\varphi_P : x \in X(\mathbb{C}) \cap \Phi_P(U) \longmapsto (\Phi_P^{-1})_r(x) \in \mathbb{C}$ pour tout $P \in X(\mathbb{C})$, la compatibilité des cartes étant assurée par le caractère biholomorphe des Φ_P. $\square$

2.7 Deuxième bijection : l'application holomorphe $\varphi_N : Y_0(N) \longrightarrow X(\mathbb{C})$.

2.7.1 Préliminaire : quotients de courbes elliptiques et morphismes.

Soit K un corps de caractéristique différente de 2 et 3. Commençons par définir le quotient d'une courbe elliptique.

Théorème 2.7.1.1. *Soient E une courbe elliptique sur K et C un sous-groupe fini de E. Alors il existe une courbe elliptique E' unique à isomorphisme près (sur $\overline{K}$) et un morphisme $\phi : E \longrightarrow E'$ séparable tel que $ker(\phi) = C$.*
On pose $E' := E/C$ que l'on appelle courbe elliptique quotient de E par C. *On appellera* projection canonique *un tel morphisme ϕ.*

Démonstration. Dans le cas général, ce théorème utilise des résultats de géométrie algébrique avancés (et hors de notre portée) tels que la formule d'Hurwitz. On trouvera une démonstration dans [2] (proposition 4.12). La preuve est plus simple lorsque $K = \mathbb{C}$, hypothèse que nous ferons. On peut donc travailler avec des réseaux de $\mathbb{C}$.

Existence : Soit $\Lambda_\tau := \mathbb{Z} \oplus \tau\mathbb{Z}$ un réseau de $\mathbb{C}$ avec $\tau \in \mathbb{H}$. Soit C un sous-groupe fini de $\mathbb{C}/\Lambda$. Alors C est engendré par un nombre fini d'éléments $P_1, \cdots, P_m \in C$. Quitte à quotienter par $\langle P_1 \rangle, \langle P_2 \rangle, \cdots, \langle P_m \rangle$ par successivement, on peut supposer C cyclique engendré par P_1. Posons $N := |C|$. Alors d'après le point (i) du théorème 2.3.2.1, $(\mathbb{C}/\Lambda_\tau, C) \simeq (\mathbb{C}/\Lambda_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle)$ pour un certain $\tau' \in \mathbb{H}$. L'isomorphisme en question induit un isomorphisme de groupes :

$$(\mathbb{C}/\Lambda_\tau)/C \simeq \mathbb{C}/\Lambda_{\tau'}/\left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle \simeq \mathbb{C}/(\mathbb{Z} + \tau'\mathbb{Z} + 1/N\mathbb{Z}) = \mathbb{C}/(1/N\mathbb{Z} \oplus \tau'\mathbb{Z})$$

Or, $\mathbb{Z} \oplus N\tau\mathbb{Z}$ est un réseau de $\mathbb{C}$ donc $\mathbb{C}/(1/N\mathbb{Z} \oplus \tau\mathbb{Z})$ est muni d'une structure de courbe elliptique, qui induit une structure de courbe elliptique sur $(\mathbb{C}/\Lambda_\tau)/C$. Le morphisme $\phi_1 : \mathbb{C}/\Lambda_{\tau'} \longrightarrow \mathbb{C}/(1/N\mathbb{Z} \oplus \tau'\mathbb{Z})$ donné par la multiplication par 1 est de noyau $\langle 1/N + \Lambda_{\tau'} \rangle$ et donne le morphisme :

$$\phi : \mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{C}/(1/N\mathbb{Z} \oplus \tau'\mathbb{Z}) \simeq (\mathbb{C}/\Lambda_\tau)/C$$

cherché en composant par l'isomorphisme $(\mathbb{C}/\Lambda_\tau, C) \simeq (\mathbb{C}/\Lambda_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle)$.

Unicité : On peut traiter l'unicité dans le cas général (K quelconque). Soient $\phi : E \longrightarrow E'$ et $\psi : E \longrightarrow E''$ séparables tels que $\ker(\phi) = \ker(\psi) = C$. Alors le théorème 1.2.0.6 assure l'existence d'un morphisme séparable $\lambda : E' \longrightarrow E''$ tel que $\psi = \lambda \circ \phi$. Comme ϕ et ψ sont séparables, on a alors d'après la proposition 6.10 de [3] :

$$|C| = \deg(\psi) = \deg(\lambda \circ \phi) = \deg(\lambda)\deg(\psi) = \deg(\lambda)|C|$$

Ainsi, $\deg(\lambda) = 1$ et donc $\lambda \circ \hat{\lambda} = [1]$, ce qui prouve que λ est un isomorphisme dont l'inverse est le morphisme dual. D'où l'unicité. □

Proposition 2.7.1.2. *Soient E_1 et E_2 deux courbes elliptiques définies sur K. Si End$(E_1) \simeq \mathbb{Z}$ alors Hom$(E_1, E_2) \simeq \{0\}$ ou $\mathbb{Z}$.*

Démonstration. Supposons $\mathrm{Hom}(E_1, E_2) \simeq \{0\}$. Soient $\phi \in \mathrm{Hom}(E_1, E_2) \setminus \{0\}$ et :

$$\iota : \psi \in \mathrm{Hom}(E_1, E_2) \longmapsto \hat{\phi} \circ \psi \in \mathrm{End}(E_1)$$

Alors si $\psi \in \mathrm{Hom}(E_1, E_2)$ vérifie $\iota(\psi) = \hat{\phi} \circ \psi = 0$ alors $\phi \circ \hat{\phi} \circ \psi = 0$ donc $[\deg(\phi)] \circ \psi = 0$ avec $\deg(\phi) \neq 0$ donc $\psi = 0$ car $\mathrm{Hom}(E_1, E_2)$ est libre (d'après le théorème 1.1.1.11). Ainsi, ι est injective et il s'ensuit que $\mathrm{Hom}(E_1, E_2) \simeq \mathbb{Z}$. □

Proposition 2.7.1.3. *Soient E une courbe elliptique telle que $End(E) \simeq \mathbb{Z}$, C et C' des sous-groupes finis de E de même ordre. Si $E/C \simeq E/C'$ alors $C = C'$.*

Démonstration. Soient $\lambda : E/C \longrightarrow E/C'$ un isomorphisme et $\phi : E \longrightarrow E/C$ et $\psi : E \longrightarrow E/C'$ des projections canoniques. Ainsi, λ est de degré $|\ker(\lambda)| = 1$ donc, ϕ et ψ étant séparables de noyaux respectifs C et C' :

$$\deg(\lambda \circ \phi) = \deg(\phi) = |C| = |C'| = \deg(\psi)$$

Remarqons que $\lambda \circ \phi, \psi \in \mathrm{Hom}(E, E/C) \setminus \{0\}$. Ainsi, $\mathrm{Hom}(E, E/C) \simeq \mathbb{Z}$ puisque $\mathrm{End}(E) \simeq \mathbb{Z}$ et d'après la proposition précédente. $\lambda \circ \phi$ et ψ sont donc des entiers de même degré (donc de même carré), de sorte que :

$$\lambda \circ \phi = \pm\psi$$

Il s'ensuit que $C = \ker(\phi) = \ker(\lambda \circ \phi) = \ker(\psi) = C'$. □

2.7.2 L'application $\varphi_N : Y_0(N) \longrightarrow X(\mathbb{C})$.

Lemme 2.7.2.1. *Toute fonction $f \in \mathcal{A}_{N,\overline{\mathbb{Q}}}$ est holomorphe sur $\mathbb{H}$.*

Démonstration. Soit $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est la clôture intégrale de $\overline{\mathbb{Q}}[j]$ dans $\overline{\mathbb{Q}}(j, j_N)$ donc si $f \in \mathcal{A}_{N,\overline{\mathbb{Q}}}$, alors on dispose de $a_0, \cdots, a_{d-1} \in \overline{\mathbb{Q}}[j]$ tels que :

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

Les a_i sont holomorphes sur $\mathbb{H}$ (car j est holomorphe sur $\mathbb{H}$) donc si $\tau \in \mathbb{H}$ est un pôle de f alors τ est un pôle d'ordre $d\mathrm{ord}_\tau(f)$ de $f^d + \sum_{i=0}^{d-1} a_i f^i = 0$. Absurde ! Comme $f \in \mathcal{A}_{N,\overline{\mathbb{Q}}} \subset \overline{\mathbb{Q}}(j, j_N)$, f est méromorphe et sans pôle donc holomorphe sur $\mathbb{H}$. □

Rappelons que $\mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[X_1, \cdots, X_r]/I$ avec j envoyé sur $\overline{X_1}$, la réduite de X_1 modulo I (proposition 2.6.0.1). On peut donc voir les $\overline{X_i}$ comme des fonctions de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ qui engendrent $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ sur $\overline{\mathbb{Q}}$. Elles sont holomorphes d'après le lemme précédent, ce qui assure la bonne définition de :

$$\tau \in \mathbb{H} \longmapsto (\overline{X_1}(\tau), \cdots, \overline{X_r}(\tau)) \in X(\mathbb{C})$$

C'est une application holomorphe (chaque coordonnée étant holomorphe, on peut appliquer la théorie des fonctions holomorphes de plusieurs variables de [12] puisque les cartes sont holomorphes comme fonctions de plusieurs variables). D'après le lemme suivant et le théorème 2.1.0.3, elle induit même une application holomorphe :

$$\varphi_N : Y_0(N) \longrightarrow X(\mathbb{C})$$

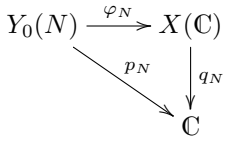
Lemme 2.7.2.2. *j_N est invariante sous l'action de $\Gamma_0(N)$. Il s'ensuit que toute fonction de $\mathcal{A}_{N,\overline{\mathbb{Q}}} \subset \overline{\mathbb{Q}}(j, j_N)$ est invariante sous l'action de $\Gamma_0(N)$.*

Démonstration. Soient $\tau, \tau' \in \mathbb{H}$ tels que $\tau' \in \Gamma_0(N)\tau$. Alors d'après le théorème 2.3.2.1, $(\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau \rangle) \simeq (\mathbb{C}/\Lambda_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle)$. Donc il existe $\alpha \in \mathbb{C}^*$ tel que $\alpha\Lambda_\tau = \Lambda_{\tau'}$ et $\alpha\langle 1/N + \Lambda_\tau \rangle = \langle 1/N + \Lambda_{\tau'} \rangle$, de sorte que :

$$\alpha\left(\frac{1}{N}\mathbb{Z} + \Lambda_\tau\right) = \alpha\left(\frac{1}{N}\mathbb{Z} \oplus \tau\mathbb{Z}\right) = \frac{1}{N}\mathbb{Z} + \Lambda_{\tau'} = \frac{1}{N}\mathbb{Z} \oplus \tau'\mathbb{Z}$$

Donc $\mathbb{C}/(1/N\mathbb{Z} \oplus \tau\mathbb{Z}) \simeq \mathbb{C}/(1/N\mathbb{Z} \oplus \tau'\mathbb{Z})$ en tant que surfaces de Riemann et courbes elliptiques par abus (d'après le point (ii) du théorème 2.2.2.1). Or, $\mathbb{C}/(1/N\mathbb{Z} \oplus \tau\mathbb{Z}) \simeq \mathbb{C}/(\mathbb{Z} \oplus N\tau\mathbb{Z})$ et $\mathbb{C}/(1/N\mathbb{Z} \oplus \tau'\mathbb{Z}) \simeq \mathbb{C}/(\mathbb{Z} \oplus N\tau'\mathbb{Z})$ en considérant la multiplication par N des réseaux. Ainsi, $j(N\tau) = j(N\tau')$ i.e. $j_N(\tau) = j_N(\tau')$ d'après la proposition 2.3.1.1. □

Considérons $q_N : (x_1, \cdots, x_n) \in X(\mathbb{C}) \longmapsto x_1 \in \mathbb{C}$. C'est une application holomorphe (toujours d'après la théorie des applications holomorphes de plusieurs variables). Comme $\overline{X_1}$ s'identifie à j, on a $q_N \circ \varphi = p_N$ ou autrement dit le diagramme suivant commute :



Proposition 2.7.2.3. *Les fibres de q_N sont de cardinal au plus $d_0(N)$.*

Démonstration. Soit $z \in \mathbb{C}$. Alors d'après la proposition 2.6.0.2 :

$$q_N^{-1}(\{z\}) = \{(x_1, \cdots, x_r) \in X(\mathbb{C}) \mid x_1 = z\}$$

s'identifie à :

$$H_z := \{\phi \in \mathrm{Hom}_{\overline{\mathbb{Q}}-alg}(\mathcal{A}_{N,\overline{\mathbb{Q}}}, \mathbb{C}) \mid \phi(j) = z\}$$

puisque $\overline{X_1}$ s'identifie à j.

Poser $\psi(j) := z$ suffit à définir un morphisme de $\overline{\mathbb{Q}}$-algèbre $\psi : \overline{\mathbb{Q}}[j] \longmapsto \mathbb{C}$. Un morphisme de $\overline{\mathbb{Q}}$-algèbre $\phi \in H_z$ est donc un prolongement de ψ. Soit $\mathfrak{p} := \ker(\psi)$. C'est un idéal de $\overline{\mathbb{Q}}[j]$ qui est soit nul, soit égal à $\overline{\mathbb{Q}}[j]$ tout entier, soit propre et premier, auquel cas il est maximal car $\overline{\mathbb{Q}}[j]$ est de Dedekind (j étant transcendant sur $\overline{\mathbb{Q}}$, c'est un anneau principal donc on peut appliquer la proposition C.1.0.9). Remarquons aussi que si $\phi \in H_z$ alors $\mathfrak{P} = \ker(\phi)$ est soit $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ tout entier (auquel cas $\mathfrak{p} = \overline{\mathbb{Q}}[j]$) soit un idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Distinguons trois cas :

Premier cas : Si $\mathfrak{p} = \{0\}$ alors tout idéal premier de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ non nul $\mathfrak{P}|\mathfrak{p}$ n'est pas maximal car sinon $\mathfrak{p}$ le serait (d'après la proposition B.7.1.2). Or, $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est de Dedekind d'après la proposition B.5.0.3 car $\overline{\mathbb{Q}}[j]$ est de Dedekind et que $\overline{\mathbb{Q}}(j, j_N)/\overline{\mathbb{Q}}(j)$ est finie et séparable donc tout idéal premier non nul de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est premier. Ainsi, le seul idéal premier $\mathfrak{P}$ de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ au-dessus de $\mathfrak{p}$ est $\{0\}$. Ainsi, tout élément $\phi \in H_z$ est injectif.

Comme $\overline{\mathbb{Q}}[j, j_N] \subset \mathcal{A}_{N,\overline{\mathbb{Q}}}$ (vu que $\Phi_N(j_N, j) = 0$ et que $\Phi_N(X, j)$ est unitaire dans $\mathbb{Z}[j][X]$), ϕ peut donc être prolongé à $\mathrm{Frac}\overline{\mathbb{Q}}[j, j_N] = \overline{\mathbb{Q}}(j, j_N)$. Comme $\phi(j) = \psi(j) = z$, ϕ est donc entièrement déterminé par sa valeur en j_N. Or, $\phi(\Phi_N(j_N, j)) = \Phi_N(\phi(j_N), \phi(j)) = 0$ donc $\phi(j_N)$ est l'une des $d_0(N)$ racines de $\Phi_N(X, \phi(j)) \in \mathbb{Z}[\phi(j)][X]$. Ainsi, $|q_N^{-1}(\{z\})| = |H_z| \leq d_0(N)$.

Deuxième cas : Si $\mathfrak{p} = \overline{\mathbb{Q}}[j]$ et si $\phi \in H_z$ alors $\phi(1) = \psi(1) = 0$ donc $\phi = 0$. Donc $|q_N^{-1}(\{z\})| = 1 \leq d_0(N)$.

Troisième cas : Si $\mathfrak{p}$ est propre alors le théorème B.7.2.5, il y a au plus $[\overline{\mathbb{Q}}(j, j_N) : \overline{\mathbb{Q}}(j)] = d_0(N)$ idéaux premiers de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ au-dessus de $\mathfrak{p}$. Montrons qu'alors $\phi \in H_z$ est entièrement déterminé par $\mathfrak{P} := \ker(\phi)$ (idéal premier de $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ au-dessus de $\mathfrak{p}$), ce qui conclura.

Remarquons tout d'abord que ϕ induit une injection $\overline{\phi} : \mathcal{A}_{N,\overline{\mathbb{Q}}}/\mathfrak{P} \longrightarrow \mathbb{C}$ qui caractérise ϕ.

On sait d'après la proposition B.7.1.2 que $\mathfrak{P}$ est maximal car $\mathfrak{p}$ l'est aussi. Donc $\mathcal{A}_{N,\overline{\mathbb{Q}}}/\mathfrak{P}$ est un corps un $\overline{\mathbb{Q}}[j]/\mathfrak{p}$-espace vectoriel de dimension finie. Or, $\mathfrak{p}$ est maximal donc $\overline{\mathbb{Q}}/\mathfrak{p}$ est un corps et un $\overline{\mathbb{Q}}$-espace vectoriel de dimension finie donc $\overline{\mathbb{Q}}[j]/\mathfrak{p} \simeq \overline{\mathbb{Q}}$, puis $\mathcal{A}_{N,\overline{\mathbb{Q}}}/\mathfrak{P} \simeq \overline{\mathbb{Q}}$ car $\overline{\mathbb{Q}}$ est algébriquement clos.

Ainsi, $\overline{\phi} : \mathcal{A}_{N,\overline{\mathbb{Q}}}/\mathfrak{P} \longrightarrow \mathbb{C}$ est le morphisme de corps trivial, ce qui prouve bien que ϕ est déterminé par $\mathfrak{P}$.

□

Proposition 2.7.2.4. *φ_N est injective.*

Démonstration. **Étape 1 : Montrons que φ_N est injective en les points transcendants (modulo l'action de $\Gamma_0(N)$).** Soient $\tau \in \mathbb{H}$ transcendant sur $\mathbb{Q}$ et $E_\tau \simeq \mathbb{C}/\Lambda_\tau$ la courbe elliptique associée. Alors le corollaire 2.2.2.5 assure que $\mathrm{End}(E_\tau) \simeq \mathbb{Z}$.

Soit $\tau' \in \mathbb{H}$ tel que $\varphi_N(\Gamma_0(N)\tau) = \varphi_N(\Gamma_0(N)\tau')$. Alors $\overline{X_i}(\tau) = \overline{X_i}(\tau')$ pour tout $i \in \{1, \cdots, r\}$. Comme $\overline{\mathbb{Q}}[j, j_N] \subset \mathcal{A}_{N,\overline{\mathbb{Q}}} \simeq \overline{\mathbb{Q}}[\overline{X_1}, \cdots, \overline{X_r}]$, on a $j(\tau) = j(\tau')$ et $j_N(\tau) = j_N(\tau')$. Ainsi, d'après la proposition 2.3.1.1, $\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda_{\tau'}$ et $\mathbb{C}/\Lambda_{N\tau} \simeq \mathbb{C}/\Lambda_{N\tau'}$. Or, on a vu au cours de la preuve du lemme 2.7.2.2 que :

$$\mathbb{C}/\Lambda_{N\tau} \simeq \mathbb{C}/\Lambda_\tau/C \quad \text{et} \quad \mathbb{C}/\Lambda_{N\tau'} \simeq \mathbb{C}/\Lambda_{\tau'}/C'$$

avec $C := \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle$ et $C' := \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle$. Ainsi, $\mathbb{C}/\Lambda_\tau/C \simeq \mathbb{C}/\Lambda_{\tau'}/C'$.

En outre, comme $j(\tau) = j(\tau')$, on a d'après le théorème 2.3.1.2, $\tau' = \gamma \cdot \tau = \frac{a\tau+b}{c\tau+d}$ avec $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Posons $\alpha := c\tau + d$. Alors :

$$\alpha\Lambda_{\tau'} = \alpha\mathbb{Z} + \alpha\tau'\mathbb{Z} = (c\tau+d)\mathbb{Z} + (a\tau+b)\mathbb{Z} = \mathbb{Z} \oplus \tau\mathbb{Z} = \Lambda_\tau$$

car $\gamma \in SL_2(\mathbb{Z})$. Donc la multiplication par α induit un isomorphisme $\mathbb{C}/\Lambda_{\tau'} \simeq \mathbb{C}/\Lambda_\tau$. Le groupe :

$$\alpha C' = \alpha \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle = \left\langle \frac{\alpha}{N} + \alpha\Lambda_{\tau'} \right\rangle = \left\langle \frac{c\tau+d}{N} + \Lambda_\tau \right\rangle \quad (\star)$$

est alors de rang N. Ainsi α induit un isomorphisme $\mathbb{C}/\Lambda_{\tau'}/C' \simeq \mathbb{C}/\Lambda_\tau/\alpha C'$. On en déduit que :

$$\mathbb{C}/\Lambda_\tau/\alpha C' \simeq \mathbb{C}/\Lambda_\tau/C$$

Comme $\mathrm{End}(E_\tau) \simeq \mathbb{Z}$ la proposition 2.7.1.3 assure que $\alpha C' = C$. On a donc par $(\star)$, $\frac{c\tau+d}{N} = \frac{k}{N} + a'\tau + b'$ avec $k \in \mathbb{Z}$ premier à N et $a', b' \in \mathbb{Z}$. Il est donc nécessaire que $N|c$ donc que $\gamma \in \Gamma_0(N)$. Ceci conclut l'étape 1.

Étape 2 : Soient $\tau, \tau' \in \mathbb{H}$ distincts tels que $\varphi_N(\Gamma_0(N)\tau) = \varphi_N(\Gamma_0(N)\tau')$. Alors d'après le théorème de structure locale des applications holomorphes (théorème 2.4 de [11], légèrement adapté pour avoir les mêmes cartes au but), on dispose de (U, ϕ) et (U', ψ') des cartes disjointes respectivement centrées en $\Gamma_0(N)\tau$ et $\Gamma_0(N)\tau'$ dans $Y_0(N)$, de (V, ψ) une carte centrée en $\varphi_N(\Gamma_0(N)\tau) = \varphi_N(\Gamma_0(N)\tau')$ dans $X(\mathbb{C})$ telles que :

$$\forall z \in \phi(U), \quad \psi \circ \varphi_N \circ \phi^{-1}(z) = z^k \quad \text{et} \quad \forall z \in \phi'(U'), \quad \psi \circ \varphi_N \circ \phi'^{-1}(z) = z^l$$

avec $k, l \in \mathbb{N}^*$. On ne peut avoir $k = 0$ ou $l = 0$ car sinon φ_N serait localement constante et donc constante sur $Y_0(N)$ tout entier (qui est connexe par arcs), et donc $p_N = q_N \circ \varphi_N$ serait constante, puis j serait constante, ce qui est exclus. Sur un voisinage W de 0 tel que $W^l \subset \phi(U)$ et $W^k \subset \phi'(U')$, on a donc :

$$\forall z \in W, \quad \psi \circ \varphi_N \circ \phi^{-1}(z^l) = \psi \circ \varphi_N \circ \phi'^{-1}(z^k) \quad \text{donc} \quad \varphi_N \circ \phi^{-1}(z^l) = \varphi_N \circ \phi'^{-1}(z^k)$$

Comme $\overline{\mathbb{Q}}$ est dénombrable, $\mathbb{H} \setminus \overline{\mathbb{Q}}$ est dense dans $\mathbb{H}$ et donc on peut trouver $z \in W$ tel que $\phi^{-1}(z^l) = \Gamma_0(N)\tau$ avec $\tau \in \mathbb{H} \setminus \overline{\mathbb{Q}}$. C'est absurde d'après le resultat de l'étape 1. □

2.7.3 Conclusion.

Théorème 2.7.3.1 (seconde bijection)**.** *φ_N induit un biholomorphisme :*

$$Y_0(N) \setminus \{\Gamma_0(N)i, \Gamma_0(N)\rho\} \longrightarrow X(\mathbb{C}) \setminus q_N^{-1}(\{0, 1728\})$$

Démonstration. D'après la proposition précédente, comme φ_N est injectif, il s'agit de prouver que si

$P \in X(\mathbb{C}) \setminus q_N^{-1}(\{0, 1728\})$, alors il existe $\tau \in Y_0(N) \setminus \{\Gamma_0(N)i, \Gamma_0(N)\rho\}$ tel que $\varphi_N(\tau) = P$.

Soit donc $P \in X(\mathbb{C}) \setminus q_N^{-1}(\{0, 1728\})$. Alors d'après le théorème 2.4.0.4, $p_N^{-1}(\{q_N(P)\})$ est de cardinal $d_0(N)$. Notons $\tau_1, \cdots, \tau_{d_0(N)}$ les éléments de cet ensemble. Comme φ_N est injectif, $\{\varphi_N(\tau_1), \cdots, \varphi_N(\tau_{d_0(N)})\}$ est de cardinal $d_0(N)$. Or, comme $p_N = q_N \circ \varphi_N$, c'est un sous-ensemble de $q_N^{-1}(\{q_N(P)\})$, qui est de cardinal au plus $d_0(N)$ d'après la proposition 2.7.2.3. Ainsi :

$$q_N^{-1}(\{q_N(P)\}) = \{\varphi_N(\tau_1), \cdots, \varphi_N(\tau_{d_0(N)})\}$$

Comme $P \in q_N^{-1}(\{q_N(P)\})$, on a donc $P = \varphi_N(\tau_i)$ pour un certain $i \in \{1, \cdots, d_0(N)\}$, ce qui conclut. Nécessairement, $\tau_i \notin \{\Gamma_0(N)i, \Gamma_0(N)\rho\}$ car $\{i, \rho\}$ est envoyé sur $\{0, 1728\}$ par la fonction j, comme nous l'avons vu au cours de la preuve du théorème 2.4.0.4. □

Corollaire 2.7.3.2. *Si $\psi : \mathcal{A}_{N,\overline{\mathbb{Q}}} \longrightarrow \mathbb{C}$ est un morphisme de $\overline{\mathbb{Q}}$-algèbres tel que $\psi(j) \notin \{0, 1728\}$ alors il existe $\tau \in \mathbb{H}$ tel que :*

$$\forall f \in \mathcal{A}_{N,\overline{\mathbb{Q}}}, \quad \psi(f) = f(\tau)$$

τ est de plus unique modulo l'action de $\Gamma_0(N)$ sur $\mathbb{H}$.

Démonstration. A ψ, on associe le point $P := (\psi(\overline{X_1}) = \psi(j), \cdots, \psi(\overline{X_r})) \in X(\mathbb{C})$ via la bijection :

$$\Upsilon : \mathrm{Hom}_{\overline{\mathbb{Q}}-alg}(\mathcal{A}_{N,\overline{\mathbb{Q}}}, \mathbb{C}) \longrightarrow X(\mathbb{C})$$

de la proposition 2.6.0.2. Comme $\psi(j) \notin \{0, 1728\}$, d'après le théorème précédent, on dispose alors de $\tau \in \mathbb{H}$ unique modulo $\Gamma_0(N)$ tel que $P = \varphi_N(\tau)$ i.e. $\psi(\overline{X_i}) = \overline{X_i}(\tau)$ pour tout $i \in \{1, \cdots, r\}$. Comme $\mathcal{A}_{N,\overline{\mathbb{Q}}}$ est engendré par les $\overline{X_i}$ comme $\overline{\mathbb{Q}}$-algèbre, on en déduit que :

$$\forall f \in \mathcal{A}_{N,\overline{\mathbb{Q}}}, \quad \psi(f) = f(\tau)$$

Ceci conclut. □

Chapitre 3

La réduction modulo p.

L'annexe C est un préliminaire utile pour l'introduction du vocabulaire et des résultats de base sur l'algèbre p-adique.

Dans ce chapitre, on fixe p un nombre premier distinct de 2 et 3, et $\mathfrak{P}$ un idéal de $\overline{\mathbb{Z}}$ au-dessus de p. On sait qu'alors (voir remarque C.2.0.2) $\mathfrak{P}$ munit $\overline{\mathbb{Q}}$ d'une norme ultramétrique $|.|_{\mathfrak{P}}$ telle que $|p|_{\mathfrak{P}} = 1$ et donc d'une valuation $v_{\mathfrak{P}}$ telle que $v_{\mathfrak{P}}(p) = 1$, que nous noterons v pour abréger. Le corps résiduel de $(\overline{\mathbb{Q}}, v)$ est $\overline{\mathbb{F}_p}$ d'après la remarque C.2.0.6. Nous noterons $\overline{\mathbb{Z}}_{\mathfrak{P}}$ l'anneau local :

$$\overline{\mathbb{Z}}_{\mathfrak{P}} := (\overline{\mathbb{Z}} \setminus \mathfrak{P})^{-1}\overline{\mathbb{Z}} = \{x \in \overline{\mathbb{Q}} \mid v(x) \geq 0\}$$

et :

$$\mathfrak{M}_{\mathfrak{P}} := \{x \in \overline{\mathbb{Q}} \mid v(x) > 0\}$$

son idéal maximal. Enfin, nous noterons $\widehat{\overline{\mathbb{Q}}}$ le complété de $(\overline{\mathbb{Q}}, v)$, $\widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ et $\widehat{\mathfrak{M}}_{\mathfrak{P}}$ les analogues de $\overline{\mathbb{Z}}_{\mathfrak{P}}$ et $\mathfrak{M}_{\mathfrak{P}}$ dans $\widehat{\overline{\mathbb{Q}}}$. En théorie, la réduction $\widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}} \longrightarrow \overline{\mathbb{F}_p}$ sera appelée par abus réduction modulo $\mathfrak{P}$.

Étant donné une courbe elliptique E définie sur un corps fini $\mathbb{F}_q \subset \overline{\mathbb{F}_p}$, il est aisé de trouver un relèvement $\tilde{E}$ de E défini sur $\overline{\mathbb{Z}}_{\mathfrak{P}}$. Il suffit de relever les coefficients a et b de l'équation de Weierstrass $Y^2 = X^3 + aX + b$ de E. Dans ce chapitre, nous allons définir des morphismes de réduction des points $\tilde{E} \longrightarrow E$ et des morphismes $\mathrm{End}(\tilde{E}) \longrightarrow \mathrm{End}(E)$. On pourra montrer assez facilement un résultat de surjectivité pour la réduction des points.

Cependant, la réduction des morphismes est beaucoup plus délicate. On obtiendra naturellement l'injectivité de la réduction des morphismes. Pour autant, la surjectivité n'est pas automatique. Lorsque E est supersingulière, c'est même impossible car $\mathrm{End}(E)$ est un ordre d'une algèbre de quaternions tandis que $\mathrm{End}(\tilde{E})$ est un ordre d'une extension quadratique imaginaire de $\mathbb{Q}$ (d'après le théorème 1.3.0.1). Lorsque E est ordinaire en revanche, $\mathrm{End}(E)$ est aussi un ordre d'une extension quadratique imaginaire de $\mathbb{Q}$ (d'après le théorème 1.4.0.1) et nous montrerons que l'on peut choisir E de telle sorte que le morphisme de réduction soit surjectif (théorème dû à Max Deuring).

3.1 Réduction des points.

On considère E une courbe elliptique définie sur $\overline{\mathbb{Z}}_{\mathfrak{P}}$, d'équation de Weierstrass $Y^2 = X^3 + aX + b$ dont la réduction modulo $\mathfrak{P}$, notée $\overline{E}$, d'équation de Weierstrass :

$$Y^2 = X^3 + \overline{a}X + \overline{b}$$

est une courbe elliptique, c'est-à-dire qu'elle vérifie $\Delta(\overline{E}) = 4\overline{a}^3 + 27\overline{b}^2 \neq 0$. On supposera de plus que $\overline{a}\overline{b} \neq 0$ ($j(\overline{E}) \neq 0, 1728$).

Lemme 3.1.0.1. *Si $P := (x, y) \in E(\widehat{\overline{\mathbb{Q}}}) \setminus \{\mathcal{O}\}$. Alors $v(x) < 0$ si et seulement si $v(y) < 0$ et dans ce cas :*

$$3v(x) = 2v(y)$$

Démonstration. Si $v(x) < 0$ alors comme $v(a) = v(b) = 0$ ($\overline{a}\overline{b} \neq 0$), on a d'après le lemme C.1.0.4 :

$$2v(y) = v(x^3 + ax + b) = \min(3v(x), v(x) + v(a), v(b)) = 3v(x)$$

Réciproquement, si $v(x) \geq 0$, alors :

$$2v(y) = v(x^3 + ax + b) = \max(3v(x), v(x) + v(a), v(b)) = 0$$

Donc $v(y) \geq 0$. □

On définit la réduction modulo $\mathfrak{P}$: $\mathrm{red}_{\mathfrak{P}} : E(\widehat{\overline{\mathbb{Q}}}) \longrightarrow \overline{E}(\overline{\mathbb{F}_p})$ de la façon suivante. Soit $P := (x, y) = [x : y : 1] \in E(\widehat{\overline{\mathbb{Q}}}) \setminus \{\mathcal{O}\}$. Si $v(x) \geq 0$ alors $v(y) \geq 0$ d'après le lemme précédent donc on peut poser :

$$\overline{P} = \mathrm{red}_{\mathfrak{P}}(P) := [\overline{x} : \overline{y} : \overline{1}] = (\overline{x}, \overline{y})$$

Sinon, $v(y) < 0$ donc $v(y^{-1}) > 0$, $3v(x) = 2v(y)$ (d'après le lemme) donc $v(y) < v(x)$ et $v(y^{-1}x) > 0$. On pose alors :

$$\overline{P} = \mathrm{red}_{\mathfrak{P}}(P) := [\overline{y^{-1}x} : \overline{y^{-1}y} : \overline{y^{-1}}] = [0 : 1 : 0] = \mathcal{O}$$

Bien-sûr, $\overline{\mathcal{O}} = \mathrm{red}_{\mathfrak{P}}(\mathcal{O}) := \mathcal{O}$.

Proposition 3.1.0.2. *La réduction $red_{\mathfrak{P}} : E(\widehat{\overline{\mathbb{Q}}}) \longrightarrow \overline{E}(\overline{\mathbb{F}_p})$ est un morphisme de groupes de noyau :*

$$ker(red_{\mathfrak{P}}) = \{(x, y) \in E(\widehat{\overline{\mathbb{Q}}}) \setminus \{\mathcal{O}\} \mid v(x) < 0\} \cup \{\mathcal{O}\}$$

Démonstration. Pour voir que $\mathrm{red}_{\mathfrak{P}}$ est un morphisme de groupes, il s'agit de montrer que si L est une droite projective intersectant $E(\widehat{\overline{\mathbb{Q}}})$ en P, Q et R alors la réduction $\overline{L}$ de L modulo $\mathfrak{P}$ intersecte $\overline{E}$ en $\overline{P}$, $\overline{Q}$ et $\overline{R}$ avec multiplicités. Ceci est long et fastidieux en raison du grand nombre de cas à distinguer. Nous renvoyons le lecteur à l'exercice 7.15 de [2] pour une démonstration complète de ce fait.

Le calcul du noyau est cependant immédiat par définition. □

3.1.1 Surjectivité de la réduction des points.

Proposition 3.1.1.1. *La réduction $red_{\mathfrak{P}} : E(\widehat{\overline{\mathbb{Q}}}) \longrightarrow \overline{E}(\overline{\mathbb{F}_p})$ est surjective.*

Démonstration. Soit $P := (x, y) \in \overline{E} \setminus \{\mathcal{O}\}$. Prenons $\tilde{y} \in \widehat{\overline{\mathbb{Q}}}$ un relèvement de y modulo $\mathfrak{P}$ et considérons le polynôme $Q(X) := X^3 + aX + b - \overline{y}^2 \in \widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}[X]$. Alors $\overline{Q}(x) = 0$. Distinguons deux cas :

- **Premier cas :** Si $\overline{Q}'(x) \neq 0$ alors on applique le lemme de Hensel (théorème C.4.0.1) à Q pour obtenir l'existence de $\tilde{x} \in \widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ se réduisant sur x tel que $\tilde{y}^2 = \tilde{x}^3 + a\tilde{x} + b$. On a alors $\tilde{P} := (\tilde{x}, \tilde{y}) \in E(\widehat{\overline{\mathbb{Q}}})$ et $\mathrm{red}_{\mathfrak{P}}(\tilde{P}) = P$.
- **Deuxième cas :** Si $\overline{Q}'(x) = 0$ alors $3x^2 + \overline{a} = 0$ donc $x = \pm u$ où u est une racine de $-\frac{\overline{a}}{3}$ fixée dans $\overline{\mathbb{F}_p}$ et $y^2 = x^3 + \overline{a}b + \overline{b}$. Comme $p \neq 2, 3$ et $\overline{a} \neq 0$, on a donc $x \neq 0$ et $\overline{Q}'(x) = 6x \neq 0$ donc le lemme de Hensel assure l'existence de $\tilde{x} \in \widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ se réduisant sur x. Le lemme de Hensel appliqué de la même façon à $Y^2 - (\tilde{x}^3 + a\tilde{x} + b)$ donne $\tilde{y}' \in \widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ se réduisant sur y tel que $\tilde{y}'^2 = \tilde{x}^3 + a\tilde{x} + b$. On a alors $\tilde{P} := (\tilde{x}, \tilde{y}') \in E(\widehat{\overline{\mathbb{Q}}})$ et $\mathrm{red}_{\mathfrak{P}}(\tilde{P}) = P$.

□

3.1.2 Réduction des groupes de torsion.

Proposition 3.1.2.1. *Soit $n \in \mathbb{N}^*$ premier à p. Supposons que $\overline{E}[n] \subset \overline{E}$. Alors la réduction modulo $\mathfrak{P}$ induit un insomorphisme de groupes $E[n] \longrightarrow \overline{E}[n]$.*

Démonstration. Notons $\Psi_n(X,Y)$ le n-ième polynôme de division de E défini par récurrence par :

$$\Psi_1(X,Y) := 1, \quad \Psi_2(X,Y) := 2Y, \quad \Psi_3(X,Y) := 3X^4 + 6aX^2 + 12bX - a^2$$

$$\Psi_4(X,Y) := 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3)$$

Pour $m \geq 3$:

$$\Psi_{2m} := \frac{\Psi_{m-1}^2\Psi_m\Psi_{m+2} - \Psi_{m-2}\Psi_m\Psi_{m+1}^2}{2Y}$$

Et pour $m \geq 2$:

$$\Psi_{2m+1} := \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3$$

$\overline{\Psi_n}(X,Y)$ vérifie les mêmes relations de récurrence donc c'est le n-ième polynôme de division de $\overline{E}$. On sait de plus (comme conséquence de la la proposition 6.15 de [3]) qu'un point est de n-torsion si et seulement si c'est un zéro du n-ième polynôme de division. Ceci est valable dans E comme dans $\overline{E}$.

Or, on montre facilement par récurrence que $\Psi_n(X,Y)^2$ s'écrit dans $\overline{\mathbb{Z}}_{\mathfrak{P}}[X,Y]/(Y^2 - X^3 - aX - b)$ comme un polynôme en X de degré $n^2 - 1$ et de coefficient dominant n^2. Distinguons alors deux cas.

Premier cas : Si n est pair alors $\Psi_n(X,Y)$ s'écrit dans $\overline{\mathbb{Z}}_{\mathfrak{P}}[X,Y]/(Y^2 - X^3 - aX - b)$:

$$\Psi_n(X,Y) = nYP_n(X)$$

avec P_n unitaire de degré $\frac{n^2-4}{2}$. Comme $n \wedge p = 1$, on a $|\overline{E}[n]| = |E[n]| = n^2$ (d'après le point (i) du théorème 6.17 de [3]). n étant de plus impair, $E[2] \subset E[n]$. Or, $E[2]$ est formé du point $\mathcal{O}$ et des points d'ordonnée nulle (d'où le facteur Y). Les abscisses des $n^2 - 4$ autres points sont racines de P_n. Comme $-P \in E[n]$ dès que $P \in E[n]$ et que deux points ayant même abscisse sont égaux ou opposés, P_n est scindé à racines simples dans $\overline{\mathbb{Q}}$ et ses racines sont les abscisses des points de $E[n] \setminus E[2]$.

De même $\overline{P_n}$ est scindé à racines simples dans $\overline{\mathbb{F}_p}$ et ses racines sont les abscisses des points de $\overline{E}[n] \setminus \overline{E}[2]$. Donc $\overline{P_n}$ n'a pas de racine double et le lemme de Hensel (théorème C.4.0.1) assure que l'on peut toutes les relever dans $\widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$. Ainsi, toutes les racines de P_n sont dans $\widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$.

Ainsi, pour tout $\overline{P} := (\overline{x}, \overline{y}) \in \overline{E}[n] \setminus \overline{E}[2]$, on dispose d'une racine x de P_n dans $\widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ se réduisant sur $\overline{x}$. Considérons alors le polynôme $Q(Y) := Y^2 - x^3 - ax - b$. Alors $\overline{Q}(\overline{y}) = 0$ et $\overline{Q}'(\overline{y}) = 2\overline{y} \neq 0$ car $P \notin \overline{E}[2]$ donc le lemme de Hensel assure l'existence de $y \in \widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ se réduisant sur y modulo $\mathfrak{P}$ tel que $Q(y) = 0$. On a alors $\Psi_n(x,y) = 0$ donc $P := (x,y) \in E[n] \cap E(\widehat{\overline{\mathbb{Q}}})$.

Puis, si $\overline{P} := (\overline{x}, \overline{y}) \in \overline{E}[2] \setminus \{\mathcal{O}\}$ alors $\overline{y} = 0$. Considérons donc $Q(X) := X^3 + aX + b$. $\overline{x}$ est une racine simple de $\overline{Q}$, ce polynôme n'ayant pas de racine double car il est de discriminant $\Delta(\overline{E}) \neq 0$ donc d'après le lemme de Hensel, $\overline{x}$ admet un relèvement $x \in \widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$ qui est une racine de Q. On a alors $(x,0) \in E[2] \cap E(\widehat{\overline{\mathbb{Q}}})$.

Ainsi, $\mathrm{red}_{\mathfrak{P}}$ induit une surjection entre $E[n]$ et $\overline{E}[n]$. Ces deux groupes ayant même ordre, il s'agit d'un isomorphisme.

Deuxième cas : Si n est impair alors :

$$\Psi_n(X,Y) = nP_n(X)$$

avec P_n unitaire de degré $\frac{n^2-1}{2}$. On applique le même raisonnement que précédemment (lemme de Hensel appliqué à P_n). C'est même plus simple cette fois-ci car il n'y a pas à considérer les points de $E[2]$.

□

On déduit de la proposition ci-dessus le corollaire immédiat ci-dessus.

Corollaire 3.1.2.2. *Notons* $E^{tors} := \bigcup_{p\nmid n} E[n]$ *et* $\overline{E}^{tors}$ *son analogue dans* $\tilde{E}$*. Alors* $red_{\mathfrak{P}}$ *induit un isomorphisme de groupes* $E^{tors} \longrightarrow \overline{E}^{tors}$*.*

3.2 Réduction des morphismes.

On se donne E_1 et E_2 deux courbes elliptiques définies sur $\overline{\mathbb{Z}}_{\mathfrak{P}}$ dont les réductions modulo $\mathfrak{P}$ ($\overline{E_1}$ et $\overline{E_2}$ respectivement) sont des courbes elliptiques de coefficients tous non nuls. On va construire une flèche $\mathrm{Red}_{\mathfrak{P}} : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(\overline{E_1}, \overline{E_2})$.

Si $\varphi \in \mathrm{Hom}(E_1, E_2)$ est une isogénie à coefficients dans $\overline{\mathbb{Q}}$ alors on peut l'écrire sous forme normale :

$$\varphi(X, Y) := (r(X), Y s(X))$$

avec $r, s \in \overline{\mathbb{Q}}(X)$. Pour réduire cette formule, il faut d'abord s'assurer que numérateurs et dénominateurs ont des coefficients de valuation ≥ 0, de façon à pouvoir les réduire après modulo $\mathfrak{P}$, quitte à multiplier par un un élément de $\mathfrak{P}$ les numérateurs et dénominateurs. Toutefois, le risque est grand de se retrouver avec $\frac{0}{0}$ une fois réduit. D'où l'utilité de réduire de façon "optimale". La valuation de Gauss est un outil pour cela.

Définition 3.2.0.1. *On appelle* valuation de Gauss *d'un polynôme* $P := \sum_{i=0}^{d} c_i X^i \in \overline{\mathbb{Q}}[X]$ *l'élément de* $\mathbb{R} \cup \{+\infty\}$ *donné par :*

$$v_G(P) := \min_{0 \leq i \leq d} v(c_i)$$

On étend cette fonction à $\overline{\mathbb{Q}}(X)$ *par la formule :*

$$\forall (P, Q) \in \overline{\mathbb{Q}}[X] \times \overline{\mathbb{Q}}[X] \setminus \{0\}, \quad v_G\left(\frac{P}{Q}\right) = v_G(P) - v_G(Q)$$

A partir des propriétés de v, on obtient le :

Lemme 3.2.0.2. *v_G est une valuation sur $\overline{\mathbb{Q}}(X)$ et le corps résiduel de $\overline{\mathbb{Q}}(X)$ pour cette valuation est $\overline{\mathbb{F}_p}(X)$.*

Lemme 3.2.0.3. *Si $\varphi \in Hom(E_1, E_2)$ est une isogénie écrite sous forme normale $\varphi(X, Y) := (r(X), Y s(X))$ alors on a :*

$$v_G(s) = v_G(r) = 0$$

Démonstration. Notons $Y^2 = X^3 + a_2 X + b_2$ l'équation de Weierstrass de E_2, de sorte que :

$$(X^3 + a_1 X + b_1) s(X)^2 = r(X)^3 + a_2 r(X) + b_2 \quad (\star)$$

Supposons par l'absurde que $v_G(r) > 0$ alors d'une part, d'après le lemme C.1.0.4 :

$$v_G((X^3 + a_1 X + b_1) s(X)^2) = v_G(r(X)^3 + a_2 r(X) + b_2) = v_G(b_2) = 0$$

Et d'autre part :

$$v_G((X^3 + a_1 X + b_1) s(X)^2) = 2 v_G(s(X)) + v_G(X^3 + a_1 X + b_1) = 2 v_G(s(X))$$

Donc $v_G(s(X)) = 0$. En réduisant modulo $\mathfrak{P}$, on obtient alors que :

$$(X^3 + \overline{a_1} X + \overline{b_1}) \overline{s}(X)^2 = \overline{b_2}$$

Ainsi, on peut écrire $X^3+\overline{a_1}X+\overline{b_1}=\overline{b_2}\frac{\overline{B}(X)^2}{\overline{A}(X)^2}$, avec $\overline{A},\overline{B}\in\overline{\mathbb{F}_p}[X]$ non nuls et premiers entre eux. Ainsi, $\overline{A}^2|\overline{B}^2$ donc $\overline{A}$ est constant et $\overline{B}$ est un polynôme de degré $\frac{3}{2}$. Absurde !

De même si par l'absurde $v_G(s)>0$, l'équation $(\star)$ et le lemme C.1.0.4 assurent que $v_G(r)\geq 0$. On peut donc réduire $(\star)$ modulo $\mathfrak{P}$ pour obtenir :

$$\overline{r(X)}^3+\overline{a_2}\overline{r(X)}+\overline{b_2}=0$$

Donc $\overline{r(X)}$ est constante égale à une racine α de $X^3+\overline{a_2}X+\overline{b_2}$. Considérons la composée :

$$\Psi : E_1^{tors}\xrightarrow{\varphi} E_2^{tors}\xrightarrow{\mathrm{red}_{\mathfrak{P}}}\overline{E_2}^{tors}$$

Pour tout $P:=(x,y)\in E_1^{tors}$, $[n]P=\mathcal{O}$ pour un certain $n\in\mathbb{N}^*$ premier à p donc $[n]\varphi(P)=\varphi([n]P)=\mathcal{O}$ et $\varphi(P)\in E_2^{tors}$ donc la composée est bien définie. En outre, si $\varphi(P)\neq\mathcal{O}$, alors $\overline{\varphi(P)}\neq\mathcal{O}$ d'après le corollaire 3.1.2.2 donc $v(r(x))\geq 0$ et $v(ys(x))\geq 0$ d'après la proposition 3.1.0.2, de sorte que :

$$\overline{\varphi(P)}=(\overline{r(x)},\overline{ys(x)})$$

Comme $\varphi(P)\neq\mathcal{O}$, $P\neq\mathcal{O}$ donc la proposition 3.1.2.1 et la proposition 3.1.0.2 donnent que $v(x)\geq 0$. $\overline{r(X)}=\alpha$ n'ayant pas de pôle, $\overline{x}$ n'en est pas un et on a donc :

$$\overline{r(x)}=\overline{r}(\overline{x})=\alpha$$

Et par suite $\overline{ys(x)}=0$, donc :

$$\overline{\varphi(P)}=(\alpha,0)$$

Ainsi, Ψ est à valeurs dans $\overline{E_2}[2]$. Mais φ induit une surjection $E_1^{tors}\longrightarrow E_2^{tors}$ car $\varphi : E_1\longrightarrow E_2$ est surjective comme toute isogénie (proposition 6.11 de [3]) et que φ envoie un point de E_1^{tors} sur E_2^{tors} comme nous l'avons justifié plus haut. De plus, la proposition 3.1.2.1 assure que $E_2^{tors}\xrightarrow{\mathrm{red}_{\mathfrak{P}}}\overline{E_2}^{tors}$ est surjective. Donc Ψ est surjective et $\overline{E_2}^{tors}=\overline{E_2}[2]$. C'est absurde ! Ainsi, $v_G(r)\leq 0$ et $v_G(s)\leq 0$.

Or, $(\star)$ et le lemme C.1.0.4 donnent que $v_G(r)<0\iff v_G(s)<0$ et qu'alors $2v_G(s)=3v_G(r)$ (la preuve est la même que pour les points). Supposons par l'absurde que ce soit le cas. Plaçons-nous alors dans le sous-corps K de $\overline{\mathbb{Q}}$ engendré par les coefficients de E_1, E_2, r et s. K est un corps de nombres donc (K,v) est à valuation discrète (voir C.2.0.2) donc on dispose d'une uniformisante $\pi\in\mathcal{O}_K$. On peut alors écrire $r(X)=\frac{A(X)}{\pi^{3n}B_0(X)}$ et $s(X)=\frac{C(X)}{\pi^{2n}D_0(X)}$ avec $A,B_0,C,D_0\in K[X]\setminus\{0\}$ tels que $A\wedge B_0=1$, $C\wedge D_0=1$, et $v_G(A)=v_G(B_0)=v_G(C)=v_G(D_0)=0$. $(\star)$ devient alors :

$$(X^3+a_2X+b_2)C(X)^2\pi^{6n}B_0(X)^3=(A(X)^3+a_2A(X)\pi^{4n}B_0(X)^2+b_2\pi^{6n}B(X)^3)\pi^{6n}D_0(X)^2$$

En simplifiant par π^{6n} et en réduisant modulo $\mathfrak{P}$, on obtient alors :

$$(X^3+\overline{a_2}X+\overline{b_2})\overline{C}(X)^2\overline{B_0}(X)^3=\overline{A}(X)^3\overline{D_0}(X)^2$$

Comme $X^3+\overline{a_2}X+\overline{b_2}$ est à racines simples (puisque E_2 est une courbe elliptique), ceci est impossible. □

Si $\varphi\in\mathrm{Hom}(E_1,E_2)$ est une isogénie écrite sous forme normale $\varphi(X,Y):=(r(X),Ys(X))$ alors le lemme ci-dessus permet de poser :

$$\mathrm{Red}_{\mathfrak{P}}(\varphi)(X,Y)=\overline{\varphi}(X,Y):=(\overline{r}(X),Y\overline{s}(X))$$

On pose aussi bien-sûr $\mathrm{Red}_{\mathfrak{P}}(\mathcal{O}):=\mathcal{O}$. Voyons maintenant les propriétés de cette flèche $\mathrm{Red}_{\mathfrak{P}}:\mathrm{Hom}(E_1,E_2)\longrightarrow\mathrm{Hom}(\overline{E_1},\overline{E_2})$. Pour commencer, vérifions que cette flèche est bien définie, c'est à dire à valeurs dans les

morphismes.

Lemme 3.2.0.4. *Si $\varphi \in Hom(E_1, E_2)$ alors $\overline{\varphi} \in Hom(\overline{E_1}, \overline{E_2})$.*

Démonstration. Si $\varphi = \mathcal{O}$ alors $\overline{\varphi} = \mathcal{O} \in \mathrm{Hom}(\overline{E_1}, \overline{E_2})$. Supposons donc $\varphi \neq \mathcal{O}$ et écrivons sous forme normale $\varphi(X, Y) := (r(X), Ys(X))$. Alors :

$$(X^3 + a_1X + b_1)s(X)^2 = r(X)^3 + a_2r(X) + b_2$$

Donc en réduisant modulo $\mathfrak{P}$, on obtient :

$$(X^3 + \overline{a_1}X + \overline{b_1})\overline{s}(X)^2 = \overline{r}(X)^3 + a_2\overline{r}(X) + \overline{b_2}$$

Donc $\overline{\varphi}(X, Y) = (\overline{r}(X), Y\overline{s}(X))$ définit un morphisme généralisé. D'après le théorème A.1.0.1, il suffit donc de vérifier que $\overline{\varphi}(\mathcal{O}) = \mathcal{O}$, c'est à dire de le degré du numérateur de $\overline{r}$ est strictement supérieur à celui de son dénominateur.

Écrivons donc $r := \frac{A_1}{B_1}$ avec $A_1, B_1 \in \overline{\mathbb{Q}}[X]$ non nuls, premiers entre eux et de valuation de Gauss nulle (ce qui est possible d'après le lemme précédent). Écrivons aussi sous forme normale l'isogénie duale $\hat{\varphi}(X, Y) := (t(X), Yu(X))$ et $t := \frac{A_2}{B_2}$ avec $A_2, B_2 \in \overline{\mathbb{Q}}[X]$ non nuls, premiers entre eux et de valuation de Gauss nulle. Vu que $\hat{\varphi} \circ \varphi = [n]$ (où $n := \deg(\varphi)$), on a :

$$t(r(X)) = \frac{\phi_n(X)}{\Psi_n^2(X)}$$

où Ψ_n est le n-ième polynôme de division de E_1 et $\phi_n(X) := X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}$. Comme pour tout $m \in \mathbb{N}^*$, ψ_m^2 est un polynôme en X de degré $m^2 - 1$ et de coefficient dominant m^2 (d'après [3], page 76), on obtient que ϕ_n est un polynôme en X unitaire de degré n^2. En réduisant modulo $\mathfrak{P}$, on obtient toujours :

$$\overline{t}(\overline{r}(X)) = \frac{\overline{\phi_n}(X)}{\overline{\Psi_n}^2(X)}$$

Bien-sûr, $v_G(\psi_n^2(X)) = 0$ car $\overline{\Psi_n}$ est le n-ième polynôme de division de $\overline{E_1}$, ce qui rend la réduction légale. Mais alors $\overline{\phi_n}(X)$ est encore de degré n^2, de même que le numérateur de $\overline{t}(\overline{r}(X))$.

En outre, d'après le lemme A.1.0.4, $\deg(A_1) = \deg(A_2) = n$ et $\deg(B_1) = \deg(B_2) = n - 1$ ($\hat{\varphi}$ étant aussi de degré n). On peut donc écrire $A_2 := \sum_{i=0}^{n} a_iX^i$ et $B_2 := \sum_{i=0}^{n} b_iX^i$, puis :

$$\overline{t}(\overline{r}(X)) = \frac{\sum_{i=0}^{n} \overline{a_i}\overline{A_1}(X)^i\overline{B_1}(X)^{n-i}}{\overline{B_1}(X)\sum_{i=0}^{n-1} \overline{b_iA_1}(X)^i\overline{B_1}(X)^{n-1-i}}$$

avec $\deg(\overline{A_1}) \leq \deg(A_1) = n$ et $\deg(\overline{B_1}) \leq \deg(B_1) = n - 1$, de sorte que :

$$\deg\left(\sum_{i=0}^{n} \overline{a_i}\overline{A_1}(X)^i\overline{B_1}(X)^{n-i}\right) \leq \deg(\overline{A_1}(X)^n) \leq n^2$$

Comme le numérateur de $\overline{t}(\overline{r}(X))$ est de degré n^2, il y a en fait égalité, ce qui donne $\deg(\overline{A_1}) = n$, puis $\deg(\overline{B_1}) < \deg(\overline{A_1})$, de sorte que $\overline{\varphi}(\mathcal{O}) = \mathcal{O}$. □

Proposition 3.2.0.5. *Soient $\varphi, \psi \in End(E)$. Alors :*

$$\overline{\varphi + \psi} = \overline{\varphi} + \overline{\psi} \quad et \quad \overline{\varphi \circ \psi} = \overline{\varphi} \circ \overline{\psi}$$

Démonstration. On prouve seulement la multiplicativité, la preuve de l'additivité étant analogue à celle l'additivité pour les points (voir [2], exercice 7.15).

Supposons φ et ψ non nulles (l'autre cas étant trivial). Alors on peut les écrire sous forme normale :

$$\varphi(X,Y) = (r_1(X), Ys_1(X)) \quad \text{et} \quad \psi(X,Y) = (r_2(X), Ys_2(X))$$

avec $r_1, r_2, s_1, s_2 \in \overline{\mathbb{Q}}(X)$ et $r_1 := \frac{A_1}{B_1}, r_2 := \frac{A_2}{B_2}, s_1 := \frac{C_1}{D_1}, s_2 := \frac{C_2}{D_2}$ avec les numérateurs et dénominateurs premiers entre eux dans $\overline{\mathbb{Z}}_{\mathfrak{P}}[X]$. Quitte à simplifier par p, on peut toujours supposer les valuations de Gauss des numérateurs nulles et les valuations de Gauss des dénominateurs positives ou nulles.

Pour montrer que la réduction se compose, il suffit de montrer que les dénominateurs $\overline{B_1} \circ \overline{r_2}(X)$ et $\overline{D_1} \circ \overline{r_2}(X)$ sont non nuls. Supposons par l'absurde que $\overline{B_1} \circ \overline{r_2}(X) = 0$. Alors $\overline{B_1} = 0$ ou $\overline{r_2}$ est constante égale à une racine de $\overline{B_1}$. Le cas $\overline{B_1} = 0$ est exclus car $\overline{\varphi} \neq 0$. Le cas $\overline{r_2}$ constante aussi car les isogénies sont surjectives et ne peuvent donc être constantes (d'après la proposition 6.11 de [3]). Pour la même raison $\overline{D_1} \circ \overline{r_2}(X)$ est non-nul. □

Proposition 3.2.0.6. *Soit $\varphi \in Hom(E_1, E_2)$ une isogénie de degré non divisible par p. Alors la réduction des points $red_{\mathfrak{P}}$ induit un isomorphisme entre $ker(\varphi)$ et $ker(\overline{\varphi})$.*

Démonstration. Posons $n := \deg(\varphi)$. On a :

$$\widehat{\varphi} \circ \varphi = [n]_{E_1}$$

Ce qui donne en réduisant modulo $\mathfrak{P}$:

$$\overline{\widehat{\varphi}} \circ \overline{\varphi} = \overline{[n]_{E_1}}$$

d'après la proposition précédente. Or, $[n]_{E_1}$ s'exprime en fonction du polynôme de division $\Psi_n(X,Y)$ et que $\overline{\Psi_n}(X,Y)$ est le polynôme de division de $\overline{E_1}$, comme nous l'avons vu au cours de la preuve de la proposition 3.1.2.1. Ainsi, on obtient par multiplicativité du degré :

$$\deg(\overline{\varphi})\deg(\overline{\widehat{\varphi}}) = \deg([n]_{\overline{E_1}}) = n^2$$

Or, en écrivant $\overline{\varphi}$ et $\overline{\widehat{\varphi}}$ sous forme normale et en réduisant modulo $\mathfrak{P}$ les numérateurs et dénominateurs de leurs abscisses, on obtient que $\deg(\overline{\varphi}) \leq \deg(\varphi) = n$ et $\deg(\overline{\widehat{\varphi}}) \leq \deg(\hat{\varphi}) = n$, de sorte que $\deg(\overline{\varphi}) = \deg(\varphi)$.

Comme $p \not| \deg(\varphi)$, $\overline{\varphi}$ est séparable (d'après le corollaire 1.1.1.13) et bien-sûr φ est séparable car $\overline{\mathbb{Q}}$ est de caractéristique nulle. On a donc $|\ker(\varphi)| = |\ker(\overline{\varphi})|$. Écrivons φ sous forme normale $\varphi(X,Y) := (r(X), Ys(X))$ et $r := \frac{A}{B}$ avec $A, B \in \overline{\mathbb{Q}}[X]$ non nuls, premiers entre eux et de valuation de Gauss nulle. Alors :

$$\overline{r}(X) = \frac{\overline{A}(X)}{\overline{B}(X)}$$

Or, B est scindé dans $\overline{\mathbb{Q}}$ et ses racines sont les abscisses des éléments de $\ker(\varphi) \setminus \{\mathcal{O}\}$. Mais $p \not| n$ donc $\ker(\varphi) \subset E_1[n] \subset E_1^{tors}$. Comme $\mathrm{red}_{\mathfrak{P}}$ est injective sur E_1^{tors}, le 3.1.2.2 assure que les coefficients des points de $\ker(\varphi) \setminus \{\mathcal{O}\}$ sont dans $\widehat{\overline{\mathbb{Z}}}_{\mathfrak{P}}$. Ainsi, les racines de $\overline{B}$ sont des réduites des racines de B. Or, comme les abscisses des éléments de $\ker(\overline{\varphi}) \setminus \{\mathcal{O}\}$ sont pôles de $\overline{r}$, ce sont des racines de $\overline{B}$. On en déduit que $\mathrm{red}_{\mathfrak{P}}$ induit une surjection $\ker(\varphi) \longrightarrow \ker(\overline{\varphi})$. Par égalité des cardinaux, c'est un isomorphisme, ce qui conclut. □

3.3 Le théorème de Deuring.

3.3.1 Remarques préliminaires.

On se donne une courbe elliptique E ordinaire définie sur un corps fini $\mathbb{F}_q$, q étant une puissance d'un nombre premier $p \neq 2, 3$. Nous noterons $Y^2 = X^3 + aX + b$ son équation de Weierstrass.

Relever E est facile. En prenant des relevés dans $\overline{\mathbb{Z}}$ de a et b, notés respectivement $\tilde{a}$ et $\tilde{b}$, on obtient une courbe elliptique $\tilde{E}$ définie sur $\overline{\mathbb{Z}}$ et se réduisant sur E.

Dans les sections précédentes, nous avons construit des flèches de réduction $\mathrm{red}_{\mathfrak{P}} : \tilde{E}(\widehat{\overline{\mathbb{Q}}}) \longrightarrow E$ et $\mathrm{Red}_{\mathfrak{P}} : \mathrm{End}(\tilde{E}) \longrightarrow \mathrm{End}(E)$. Nous avons prouvé facilement que l'on pouvait relever les points, c'est-à-dire que la flèche $\mathrm{red}_{\mathfrak{P}}$ est surjective. Peut-on de même relever les morphismes ? Nous allons montrer que si E est ordinaire (hypothèse indispensable que nous ferons), on pourra trouver un relèvement $\tilde{E}_0$ de E sur lequel la réduction des morphismes est surjective.

Nous avons vu (théorème 1.4.0.1) que $\mathrm{End}(E)$ s'identifie à un ordre d'une extension quadratique imaginaire de $\mathbb{Q}$, disons $\mathbb{Q}(\alpha)$ (avec $\alpha \in \mathbb{C} \setminus \mathbb{R}$, de degré 2 sur $\mathbb{Q}$). La proposition B.1.0.1 assure alors l'existence d'un entier $c \in \mathbb{Z} \setminus \{0\}$ tel que $\mathrm{End}(E) \simeq \mathbb{Z} + c\alpha\mathbb{Z}$. Par linéarité et multiplicativité de la réduction (proposition 3.2.0.5) et puisque la réduction et le relèvement de la multiplication par un entier est maîtrisée (c'est fait dans [3] en considérant les polynômes de division), il suffit de relever le morphisme φ_0 associé à $c\alpha$.

Remarquons que $\varphi_0 + [n]$ engendre aussi $\mathrm{End}(E)$ pour tout $n \in \mathbb{Z}$. D'après le lemme qui suit, nous pouvons donc utiliser ce degré de liberté supplémentaire pour supposer que $p \not| \deg(\varphi_0)$ donc que φ_0 est séparable d'après le corollaire 1.1.1.13, quitte à remplacer φ_0 par $\varphi_0 + [n]$.

Lemme 3.3.1.1. *Il existe $n \in \mathbb{Z}$ tel que $p \not| \deg(\varphi_0 + [n])$.*

Démonstration. On sait d'après la proposition 1.1.4.2, deg est une forme quadratique donc pour tout $n \in \mathbb{Z}$:

$$\begin{aligned}\deg(\varphi_0 + [n]) = \deg(\varphi_0 + n[1]) &= \deg(\varphi_0) + n^2\deg([1]) + n(\deg(\varphi_0 + [1]) - \deg(\varphi_0) - \deg([1])) \\ &= n^2 + n(\deg(\varphi_0 + [1]) - \deg(\varphi_0) - 1) + \deg(\varphi_0) \quad (\star)\end{aligned}$$

Supposons que $p|\deg(\varphi_0)$. On a donc :

$$\forall n \in \mathbb{Z}, \quad \deg(\varphi_0 + [n]) \equiv n(n + \deg(\varphi_0 + [1]) - 1) \ [p]$$

Il suffit donc que $p \not| n$ et $p \not| n + \deg(\varphi_0 + [1]) - 1$. Soit r le reste de $\deg(\varphi_0 + [1]) - 1$ dans la division euclidienne par p. Alors $r \in \{0, \cdots, p-1\}$. Si $r \in \{0, 1\}$ alors comme $p \geq 5$, $n \equiv 1 \ [p]$ convient. Sinon, $n \equiv -1 \ [p]$ convient. □

Si φ_0 se factorise dans $\mathrm{End}(E)$ sous la forme $\varphi_0 = [m] \circ \lambda$, alors la proposition 3.2.0.5 assure qu'il suffit de relever le facteur λ. D'après le lemme suivant et par multiplicativité du degré (corollaire 1.1.1.9), on peut donc supposer que $\ker(\varphi_0)$ est cyclique et que $p \not| \deg(\varphi_0)$.

Lemme 3.3.1.2. *Il existe $\lambda \in End(E)$ de noyau cyclique et $m \in \mathbb{Z}$ tels que $\varphi_0 = [m] \circ \lambda$.*

Démonstration. On sait que $\ker(\varphi_0)$ est un groupe abélien fini donc il existe $d_1 | \cdots | d_r$ des entiers ≥ 2 tels que :

$$\ker(\varphi_0) \simeq \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$$

Si $r = 1$, c'est terminé. Sinon, on remarque que le groupe de d_1-torsion de $\mathbb{Z}/d_2\mathbb{Z}$ est :

$$\mathbb{Z}/d_2\mathbb{Z}[d_1] = \frac{d_2}{d_1}\mathbb{Z}/d_2\mathbb{Z} \simeq \mathbb{Z}/d_1\mathbb{Z}$$

Il s'ensuit que $(\mathbb{Z}/d_1\mathbb{Z})^2$ se plonge dans $\ker(\varphi_0)$. Or, $E[d_1] \simeq (\mathbb{Z}/d_1\mathbb{Z})^2$ d'après le théorème 6.17 de [3] car :

$$|\ker(\varphi_0)| = \prod_{i=1} d_i | \deg(\varphi_0)$$

d'après la proposition 1.1.1.7 et que $p \not| \deg(\varphi_0)$, de sorte que $p \not| d_1$. Donc $E[d_1] \subset \ker(\varphi_0)$. De plus, $[d_1]$ est séparable (car $p \not| d_1$) et le théorème 1.2.0.6 assure alors l'existence de $\lambda \in \mathrm{End}(E)$ tel que $\varphi_0 = \lambda \circ [d_1]$.

Considérons le morphisme de groupes :

$$f : P \in \ker(\varphi_0) \longmapsto [d_1]P \in \ker(\lambda)$$

Alors $\ker(f) = E[d_1]$ et f est surjectif car si $Q \in \ker(\lambda)$ et $[d_1]$ est surjectif comme tout morphisme non nul (proposition 6.11 de [3]) donc on dispose de $P \in E$ tel que $Q = [d_1]P$. Mais alors :

$$\varphi_0(P) = \lambda([d_1]P) = \lambda(Q) = \mathcal{O}$$

donc $P \in \ker(\varphi)$, ce qui prouve la surjectivité de f. Par propriété universelle du quotient, f induit donc un isomorphisme $\ker(\varphi_0)/E[d_1] \simeq \ker(\lambda)$. On en déduit que :

$$\ker(\lambda) \simeq \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}/(\mathbb{Z}/d_1\mathbb{Z})^2 \simeq (\mathbb{Z}/d_2\mathbb{Z})/(\mathbb{Z}/d_1\mathbb{Z}) \times \prod_{i=3}^{r} \mathbb{Z}/d_i\mathbb{Z} \simeq \mathbb{Z}/\frac{d_1}{d_2}\mathbb{Z} \times \prod_{i=3}^{r} \mathbb{Z}/d_i\mathbb{Z}$$

On conclut alors par récurrence sur r en appliquant le même raisonnement à λ pour obtenir finalement une isogénie de noyau cyclique. □

D'après la discussion ci-dessus, relever tous les morphismes de $\mathrm{End}(E)$ revient à relever φ_0 de degré non divisible par p (donc séparable) et de noyau cyclique. Nous noterons $C := \ker(\varphi_0)$ et $N := \deg(\varphi_0)$ dans toute la suite. On a alors :

$$C \simeq \mathbb{Z}/N\mathbb{Z} \subset E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$$

La proposition 3.2.0.6 assure alors que si $\tilde{E}$ est un relèvement de E et si $\tilde{\varphi_0}$ relève φ_0 alors la réduction des points induit un isomorphisme :

$$\tilde{C} := \ker(\tilde{\varphi_0}) \longrightarrow C$$

Comme $\mathrm{red}_{\mathfrak{P}}$ induit en fait un isomorphisme $\tilde{E}[N] \longrightarrow E[N]$ (d'après la proposition 3.1.2.1), on a nécessairement $\tilde{C} = (\pi_p)^{-1}_{|\tilde{E}[N]}(C)$. En fait, cette formule détermine même $\tilde{\varphi_0}$ à un isomorphisme près d'après le lemme suivant :

Lemme 3.3.1.3. *Soient E_1, E_2 et E_3 des courbes elliptiques définies sur un corps K de caractéristique $\neq 2, 3$. Soient $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_1, E_3)$ des isogénies séparables tels que $ker(\varphi) = ker(\psi)$. Alors il existe un automorphisme $\lambda \in Hom(E_2, E_3)$ tel que $\psi = \lambda \circ \varphi$.*

Démonstration. Comme φ et ψ sont séparables et que $\ker(\varphi) = \ker(\psi)$, le théorème 1.2.0.6 assure l'existence de $\lambda \in \mathrm{Hom}(E_2, E_3)$ et $\mu \in \mathrm{Hom}(E_3, E_2)$ telles que $\psi = \lambda \circ \varphi$ et $\varphi = \mu \circ \psi$. Ainsi :

$$\psi = \lambda \circ \mu \circ \psi \quad \text{et} \quad \varphi = \mu \circ \lambda \circ \varphi$$

Une isogénie étant surjective (proposition 6.11 de [3]), on en déduit que $\lambda \circ \mu$ et $\mu \circ \lambda$ sont égales à l'identité. Ainsi, λ est un isomorphisme. □

Remarque 3.3.1.4. Si de plus $E_2 = E_3$ et $j(E_2) \notin \{0, 1728\}$ (ce qui est toujours le cas si E_2 est ordinaire d'après la proposition 1.4.0.3), alors les calculs faits dans la preuve de la proposition 2.3.1.1 donnent que $\lambda = \pm \mathrm{id}_{E_2}$, de sorte que $\varphi = \pm\psi$.

Ainsi, il suffit de trouver $\varphi \in \mathrm{End}(\tilde{E})$ de noyau $\tilde{C}$. On aura alors automatiquement $\overline{\varphi} = \varphi_0$, quitte à changer φ en $-\varphi$.

On connait déjà un morphisme de noyau $\tilde{C}$ d'après le théorème 2.7.1.1, donné par la réduction $\varphi : \tilde{E} \longmapsto \tilde{E}/\tilde{C}$. Cependant, cette réduction n'est pas a priori un endomorphisme puisque $\tilde{E}/\tilde{C}$ n'est pas isomorphe à $\tilde{E}$ en général. Nous sommes donc amenés à résoudre le problème suivant :

Problème : Trouver $\tilde{E}$ relevant E telle que $\tilde{E}/\tilde{C} \simeq \tilde{E}$.

Comme $\tilde{E}$ est définie sur $\overline{\mathbb{Z}}_{\mathfrak{P}} \subset \mathbb{C}$, le couple $(\tilde{E}, \tilde{C})$ s'identifie d'après le théorème 2.3.2.1 à $(\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau \rangle)$ pour un certain $\tau \in \mathbb{H}$ défini modulo $\Gamma_0(N)$, de sorte que :

$$j(\tilde{E}) = j(\tau) \quad \text{et} \quad j(\tilde{E}/\tilde{C}) = j(N\tau)$$

Le problème ci-dessus revient donc à trouver $\tau' \in \mathbb{H}$ tel que $j(\tau') = j(N\tau')$ et tel que $j(\tau')$ se réduise sur $j(E)$ (la réduite étant alors isomorphe à E).

3.3.2 Conclusion : preuve du théorème de Deuring.

Soit $\tau \in \mathbb{H}$ tel que $j(\tilde{E}) = j(\tau)$, $(\tilde{E}, \tilde{C})$ étant rappelons-le, un relèvement de (E, C).

Notons $\mathcal{A}_{N,\overline{\mathbb{Z}}}$ la clôture intégrale de $\overline{\mathbb{Z}}[j]$ dans $\overline{\mathbb{Q}}(j, j_N)$. Alors $\mathcal{A}_{N,\overline{\mathbb{Z}}} \subset N, \overline{\mathbb{Q}}$, la clôture intégrale de $\overline{\mathbb{Q}}[j]$ dans $\overline{\mathbb{Q}}(j, j_N)$ donc d'après le lemme 2.7.2.1, toute fonction $f \in \mathcal{A}_{N,\overline{\mathbb{Z}}}$ est holomorphe. On peut donc définir un morphisme d'anneaux :

$$f \in \mathcal{A}_{N,\overline{\mathbb{Z}}} \longmapsto f(\tau) \in \mathbb{C}$$

Lemme 3.3.2.1. *Ce morphisme est en fait à valeurs dans $\overline{\mathbb{Z}}_{\mathfrak{P}}$.*

Démonstration. Si $f \in \mathcal{A}_{N,\overline{\mathbb{Z}}}$ alors f est entier sur $\overline{\mathbb{Z}}[j]$ donc $f(\tau)$ est entier sur $\overline{\mathbb{Z}}[j(\tau)]$. Mais $j(\tau) \in \overline{\mathbb{Z}}_{\mathfrak{P}}$ par hypothèse. En effet, $\tilde{E}$ relève E donc :

$$\Delta(E) = 4a^3 + 27b^2 = 4\tilde{a}^3 + 27\tilde{b}^2 \bmod \mathfrak{P} \neq 0$$

De sorte que :

$$j(\tilde{E}) = 1728\frac{4\tilde{a}^3}{4\tilde{a}^3 + 27\tilde{b}^2} \in \overline{\mathbb{Z}}_{\mathfrak{P}}$$

Ainsi, $f(\tau)$ est entier sur $\overline{\mathbb{Z}}_{\mathfrak{P}}$.

De plus, $f \in \overline{\mathbb{Q}}(j, j_N)$ donc $f(\tau) \in \overline{\mathbb{Q}}(j(\tau), j_N(\tau))$. Mais $j(\tau) \in \overline{\mathbb{Z}}_{\mathfrak{P}} \subset \overline{\mathbb{Q}}$ et j_N est racine du polynôme modulaire $\Phi_N(X, j) \in \mathbb{Z}[j][X]$ (unitaire) donc $j_N(\tau)$ est entier sur $\mathbb{Z}[j(\tau)] \subset \overline{\mathbb{Z}}_{\mathfrak{P}}$. Or, $\overline{\mathbb{Q}}$ est algébriquement clos donc $j_N(\tau) \in \overline{\mathbb{Q}}$, puis $f(\tau) \in \overline{\mathbb{Q}}$.

Comme $\overline{\mathbb{Z}}_{\mathfrak{P}}$ est intégralement clos dans $\overline{\mathbb{Q}}$ d'après la proposition C.1.0.9, il s'ensuit que $f(\tau) \in \overline{\mathbb{Z}}_{\mathfrak{P}}$. □

En composant avec la réduction modulo $\mathfrak{P}$, on obtient un morphisme :

$$\begin{array}{rcl} \Psi : \mathcal{A}_{N,\overline{\mathbb{Z}}} & \longrightarrow & \overline{\mathbb{Z}}_{\mathfrak{P}} \\ f & \longmapsto & f(\tau) \bmod \mathfrak{M}_{\mathfrak{P}} \end{array}$$

Lemme 3.3.2.2. *On a $\Psi(j) = \Psi(j_N)$.*

Démonstration. Cette égalité a bien un sens car $j_N \in \mathcal{A}_{N,\overline{\mathbb{Z}}}$. En effet, j_N est racine de $\Phi_N(X, j)$, qui est unitaire à coefficients dans $\mathbb{Z}[j] \subset \overline{\mathbb{Z}}[j]$.

On sait que tous les éléments de $\tilde{C}$ sont à coordonnées dans $\overline{\mathbb{Z}}_{\mathfrak{P}}$. Les formules de Vélu (voir [15]) donnant l'équation de Weeirstrass de $\tilde{E}/\tilde{C}$ à partir de cette de $\tilde{E}$ assurent alors que $\tilde{E}/\tilde{C}$ est à coefficients dans $\overline{\mathbb{Z}}_{\mathfrak{P}}$, ce qui assure qu'on peut réduire $\tilde{E}/\tilde{C}$ modulo $\mathfrak{P}$. Il reste à montrer que la courbe réduite $E' := \overline{\tilde{E}/\tilde{C}}$ est bien une courbe elliptique, à savoir qu'elle est de discriminant non nul. Pour le voir, on applique de nouveau les formules de Vélu, mais cette fois-ci à (E, C) et l'on remarque que E/C a même équation de Weierstrass que E', de sorte que $E' = E/C$. Il s'ensuit que :

$$j(E/C) = j(\tilde{E}/\tilde{C}) \bmod \mathfrak{M}_{\mathfrak{P}} = j_N(\tau) \bmod \mathfrak{M}_{\mathfrak{P}}$$

Or, la réduction canonique $E \longmapsto E/C$ et φ_0 sont séparables et ont même noyau donc le lemme 3.3.1.3 assure que E et E/C sont isomorphes, de sorte que $j(E) = j(E/C)$, puis que :

$$\Psi(j) = j_N(\tau) \bmod \mathfrak{M}_{\mathfrak{P}} = j(E/C) = j(E) = j(\tau) \bmod \mathfrak{M}_{\mathfrak{P}} = \Psi(j_N)$$

□

Ainsi, on a vu que $(j - j_N) \subset \ker\Psi$. Nous allons maintenant prouver le résultat essentiel qui nous permettra de conclure.

Lemme 3.3.2.3. *Il existe un idéal premier $\mathfrak{R}$ de $\mathcal{A}_{N,\overline{\mathbb{Z}}}$ tel que :*

(i) $(j - j_N) \subset \mathfrak{R} \subset ker(\Psi)$.

(ii) $\mathfrak{R} \cap \overline{\mathbb{Z}} = \{0\}$.

Démonstration. $\ker(\Psi)$ est premier donc radical. Ainsi, $\sqrt{(j - j_N)} \subset \sqrt{\ker(\Psi)} \subset \ker(\Psi)$. Le corollaire B.3.0.5 s'applique donc et donne que :

$$\sqrt{j - j_N} = \bigcap_{\substack{\mathfrak{p} \text{ premier} \\ (j-j_N)\subset\mathfrak{p}\subset\ker(\Psi)}} \mathfrak{p}$$

Il s'agit de montrer que l'un des idéaux premiers de cette intersection vérifie $\mathfrak{p} \cap \overline{\mathbb{Z}} = \{0\}$ donc que $\sqrt{j - j_N} \cap \overline{\mathbb{Z}} = \{0\}$.

Supposons par l'absurde qu'il existe $x \in \sqrt{j - j_N} \cap \overline{\mathbb{Z}}$ non nul. Alors $x^n \in (j - j_N)$ pour un certain $n \in \mathbb{N}$. Alors on dispose de $y \in \mathcal{A}_{N,\overline{\mathbb{Z}}}$ tel que $x^n = (j - j_N)y$. Notons $\mathcal{N}$ la norme sur l'extension $\overline{\mathbb{Q}}(j, j_N)/\overline{\mathbb{Q}}(j)$. Comme $\overline{\mathbb{Q}}(j, j_N)/\overline{\mathbb{Q}}(j)$ est séparable, on a classiquement (voir la proposition 5.14 de [10] pour une preuve) :

$$\forall z \in \overline{\mathbb{Q}}(j, j_N), \quad \mathcal{N}(z) = \prod_{\sigma\in\Sigma} \sigma(z)$$

où Σ est l'ensemble des morphismes de corps définis sur $\overline{\mathbb{Q}}(j, j_N)$ à valeurs dans une certaine clôture algébrique de ce corps et fixant $\overline{\mathbb{Q}}(j)$. Par multiplicativité de la norme, on a :

$$\mathcal{N}(x^n) = \mathcal{N}(j - j_N)\mathcal{N}(y)$$

Or, $x^n \in \overline{\mathbb{Q}}[j]$ donc $\mathcal{N}(x^n) = [\overline{\mathbb{Q}}(j, j_N) : \overline{\mathbb{Q}}(j)]x^n = d_0(N)x^n$. De plus, $y \in \mathcal{A}_{N,\overline{\mathbb{Z}}} \subset \mathcal{A}_{N,\overline{\mathbb{Q}}}$ donc y est entier sur $\overline{\mathbb{Q}}[j]$ et il en est de même de tous ses $\overline{\mathbb{Q}}(j)$ conjugués $\sigma(y)$ ($\sigma \in \Sigma$), de sorte que $\mathcal{N}(y) = \prod_{\sigma\in\Sigma} \sigma(y)$ soit entier sur $\overline{\mathbb{Q}}[j]$. Or, $\mathcal{N}(y) \in \overline{\mathbb{Q}}(j)$ et $\overline{\mathbb{Q}}[j]$ est intégralement clos puisque, j étant transcendant, il est isomorphe à $\overline{\mathbb{Q}}[X]$ donc principal donc de Dedekind d'après la proposition C.1.0.9. Ainsi, $\mathcal{N}(y) \in \overline{\mathbb{Q}}[j]$. Enfin :

$$\mathcal{N}(j - j_N) = \prod_{\sigma\in\Sigma} (\sigma(j) - \sigma(j_N)) = \prod_{\sigma\in\Sigma} (j - \sigma(j_N)) = \Phi_N(j, j)$$

les $\sigma(j_N)$ ($\sigma \in \Sigma$) étant les $\overline{\mathbb{Q}}(j)$-conjugués distincts de j_N et $\Phi_N(j, X)$ étant le polynôme minimal de j_N (d'après le corollaire 2.5.2.7). Il s'ensuit que :

$$x^n = \Phi_N(j, j)Q(j)$$

avec $Q \in \overline{\mathbb{Q}}[X]$. Or, la proposition 2.5.2.8 assure que $\Phi_N(j, j)$ est un polynôme non constant en j. Ceci contredit la transcendance de j puisque $x \neq 0$. D'où le résultat. □

Énonçons et prouvons maintenant un dernier résultat mineur.

Lemme 3.3.2.4. *On a $\mathcal{A}_{N,\overline{\mathbb{Q}}} = \overline{\mathbb{Q}} \cdot \mathcal{A}_{N,\overline{\mathbb{Z}}}$.*

Démonstration. L'inclusion $\supset$ est triviale. Prouvons l'inclusion réciproque. Soit $x \in \mathcal{A}_{N,\overline{\mathbb{Q}}}$. Alors il est entier sur $\overline{\mathbb{Q}}[j]$ donc on dispose de $d \in \mathbb{N}^*$ et de $P_0, \cdots, P_{d-1} \in \overline{\mathbb{Q}}[X]$ tels que :

$$x^d + \sum_{i=0}^{d-1} P_i(j) x^i = 0$$

Soit K le sous-corps de $\overline{\mathbb{Q}}$ engendré par les coefficients des P_i $(0 \leq i \leq d-1)$. Alors K est un corps de nombres donc le lemme B.4.0.3 assure qu'il existe $c \in \mathbb{N}^*$ tel que $cP_i \in \mathcal{O}_K[X] \subset \overline{\mathbb{Z}}[X]$ pour tout $i \in \{0, \cdots, d-1\}$. Ainsi, on a :

$$(cx)^d + \sum_{i=0}^{d-1} c^{d-i} P_i(j)(cx)^i = 0$$

Donc cx est entier sur $\overline{\mathbb{Z}}[j]$, et ainsi $cx \in \mathcal{A}_{N,\overline{\mathbb{Z}}}$, ce qui conclut. □

Tous les ingrédients sont maintenant en place.

Théorème 3.3.2.5 (Deuring)**.** *Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ (q étant une puissance d'un nombre premier $p \neq 2, 3$). Soit $\mathfrak{P}$ un idéal maximal de $\overline{\mathbb{Z}}$ contenant p. Alors il existe une courbe elliptique $\tilde{E}_0$ définie sur $\overline{\mathbb{Z}}_{\mathfrak{P}}$ se réduisant sur E modulo $\mathfrak{P}$ et telle que le morphisme de groupes :*

$$Red_{\mathfrak{P}} : End(\tilde{E}_0) \longmapsto End(E)$$

soit un isomorphisme.

Démonstration. On a déjà vu que $\mathrm{Red}_{\mathfrak{P}}$ est injective lors de sa construction (et ce quelle que soit la courbe $\tilde{E}$ choisie). La question est donc de trouver $\tilde{E}$ telle qu'il y ait injectivité.

Considérons un idéal $\mathfrak{R}$ donné par le lemme 3.3.2.3 et la réduction canonique modulo $\mathfrak{R}$:

$$\Pi : \mathcal{A}_{N,\overline{\mathbb{Z}}} \longrightarrow \mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R}$$

Comme $\mathfrak{R}$ est premier, $\mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R}$ est intègre donc on peut considérer sont corps de fractions $L := \mathrm{Frac}(\mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R})$. Comme $\mathfrak{R} \cap \overline{\mathbb{Z}} = \{0\}$, $\overline{\mathbb{Z}}$, s'injecte dans $\mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R}$ donc L est une extension de $\overline{\mathbb{Q}} = \mathrm{Frac}(\overline{\mathbb{Z}})$. En outre, tous les éléments de $\mathcal{A}_{N,\overline{\mathbb{Z}}}$ sont entiers sur $\overline{\mathbb{Z}}[j]$ donc les éléments de $\mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R}$ sont entiers sur $\overline{\mathbb{Z}}[\Pi(j)]$. Mais $(j - j_N) \subset \mathfrak{R}$ donc modulo $\mathfrak{P}$:

$$\Phi_N(j, j) \equiv \Phi_N(j_N, j) = 0$$

Mais $\Phi_N(j, j)$ est un polynôme en j non constant d'après la proposition 2.5.2.8. Ainsi, $\Pi(j)$ est algébrique sur $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$. Ainsi, tout élément de $\mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R}$, donc de L est algébrique sur $\overline{\mathbb{Q}}$. Comme $\overline{\mathbb{Q}}$ est algébriquement clos, L se plonge dans $\overline{\mathbb{Q}}$. Ainsi, $L \simeq \overline{\mathbb{Q}}$.

Comme $\mathfrak{R} = \ker\Pi$ intersecte trivialement $\overline{\mathbb{Z}}$, on peut étendre Π à $\overline{\mathbb{Q}}\mathcal{A}_{N,\overline{\mathbb{Z}}} = \mathcal{A}_{N,\overline{\mathbb{Q}}}$, pour obtenir un morphisme de $\overline{\mathbb{Q}}$-algèbre $\Pi : \mathcal{A}_{N,\overline{\mathbb{Q}}} \longrightarrow \overline{\mathbb{Q}}$. Comme E est ordinaire, son j-invariant n'est ni 0 ni 1728 (d'après la proposition 1.4.0.3) et il en est de même du j-invariant du relevé quelconque $\tilde{E}$ choisi dans ce paragraphe. On peut donc appliquer le corollaire 2.7.3.2 du théorème de la deuxième bijection (théorème 2.7.3.1) pour obtenir l'existence de $\tau' \in \mathbb{H}$ défini modulo $\Gamma_0(N)$ tel que :

$$\forall f \in \mathcal{A}_{N,\overline{\mathbb{Q}}}, \quad \Pi(f) = f(\tau')$$

Soit $\tilde{E}_0$ la courbe elliptique sur $\mathbb{C}$ associée à $\tau' \in \mathbb{H}$. Alors :

$$j(\tau') = j_N(\tau') \quad (\star)$$

puisque $(j - j_N) \subset \mathfrak{R}$.

Comme $\mathfrak{R} \subset \ker(\Psi)$, Ψ se factorise par Π par propriété universelle du quotient. Ainsi, $\Phi : \mathcal{A}_{N,\overline{\mathbb{Z}}} \longrightarrow \mathcal{A}_{N,\overline{\mathbb{Z}}}/\mathfrak{R}$ est à valeurs dans $\overline{\mathbb{Z}}_{\mathfrak{P}}$, de sorte que $j(\tilde{E}_0) = j(\tau') \in \overline{\mathbb{Z}}_{\mathfrak{P}}$. On peut donc supposer que $\tilde{E}_0$ est définie sur $\overline{\mathbb{Z}}_{\mathfrak{P}}$, ce qui permet de la réduire modulo $\mathfrak{P}$. Ψ se factorisant par Π, on a de plus :

$$j(\tilde{E}_0) = j(\tau') = \Pi(j) \equiv \Psi(j) \bmod \mathfrak{M}_{\mathfrak{P}} = j(\tau) \bmod \mathfrak{M}_{\mathfrak{P}} = j(E)$$

$\tilde{E}_0$ se réduit donc sur une courbe elliptique isomorphe à E, donc par changement de variable, on peut supposer que $\tilde{E}_0$ se réduit sur E. Comme expliqué à la fin du paragraphe précédent, ceci prouve avec $(\star)$ le théorème de Deuring. □

Annexe A

Compléments sur les morphismes.

Dans ce chapitre, on fixe K un corps de caractéristique $\neq 2, 3$ et $\overline{K}$ une clôture algébrique de K.

A.1 Lemmes techniques sur les isogénies.

On commence par un résultat qui permet de vérifier qu'un morphisme généralisé est une isogénie. Avant cela, donnons quelques précisions sur l'évaluation des fonctions rationnelles, puis des morphismes.

Soit E une courbe elliptique définie sur K d'équation de Weierstrass $Y^2 = X^3 + aX + b$.

Si $p \in \overline{K}[E]$ est une fonction polynomiale définie sur E, alors on peut l'écrire sous la forme normale :

$$p(X, Y) := p_1(X) + Y p_2(X)$$

avec $p_1, p_2 \in \overline{K}[X]$ uniques et considérer sa norme :

$$N(p) = (p_1(X) + Y p_2(X))(p_1(X) - Y p_2(X)) = p_1(X)^2 - Y^2 p_2(X)^2 = p_1(X)^2 - (X^3 + aX + b)p_2(X)^2$$

Et noter $\deg(p)$ le degré usuel en X de $N(p)$.

Si $f \in \overline{K}(E)$ est une fonction rationnelle et si $P \in E$ on sait évaluer $f(P)$ lorsque $P \neq \mathcal{O}$. Si P n'est pas un pôle de f, autrement dit si $f = \frac{p}{q}$ avec $p, q \in \overline{K}[E]$ avec $q(P) \neq 0$ alors l'évaluation est aisée $f(P) = \frac{p(P)}{q(P)}$. Sinon, on pose $f(P) = \infty$. Lorsque $P = \mathcal{O}$, on distingue trois cas :

- Si $\deg(p) > \deg(q)$ alors $f(\mathcal{O}) = 0$.
- Si $\deg(p) < \deg(q)$ alors $f(\mathcal{O}) = \infty$.
- Si $\deg(p) = \deg(q)$ alors $f(\mathcal{O})$ est le rapport des coefficients des monômes de plus haut degré de p et q.

On peut vérifier que ce procédé est indépendant du représentant de f choisi.

Si $\phi : E_1 \longrightarrow E_2$ est un morphisme généralisé non nul entre deux courbes elliptiques définies sur K alors on peut l'écrire sous la forme $\phi := (f, g)$. Si $P \in E_1$, on évalue $f(P)$ et $g(P)$ pour décider de la valeur $\phi(P)$. Si aucune des deux valeurs n'est infinie, on pose $\phi(P) := (f(P), g(P))$. Sinon, on peut montrer qu'alors $f(P) = g(P) = \infty$ (avec l'équation de Weierstrass et l'étude de l'ordre des pôles) ce qui nous autorise à poser $\phi(P) = \mathcal{O}$.

Théorème A.1.0.1. *Soit $\phi : E_1 \longrightarrow E_2$ un morphisme généralisé entre deux courbes elliptiques E_1 et E_2 définies sur K. Supposons que $\phi(\mathcal{O}) = \mathcal{O}$. Alors ϕ est un morphisme.*

Démonstration. On commence par montrer que ϕ est impaire, c'est à dire qu'elle vérifie $\phi(-P) = -\phi(P)$ pour tout $P \in E_1$. Pour cela, on prouve le lemme suivant.

Lemme A.1.0.2. *Tout morphisme généralisé $\psi : E_1 \longrightarrow E_2$ pair, c'est à dire vérifiant $\psi(-P) = \psi(P)$ pour tout $P \in E_1$ est constant.*

Démonstration. Si $\phi = \mathcal{O}$ alors c'est terminé. Sinon, on peut écrire le morphisme généralisé sous la forme $\psi = (f, g)$ avec $f, g \in K(E)$ et on écrit f et g sous forme réduite $f = f_1(X) + Yf_2(X)$ et $g = g_1(X) + Yg_2(X)$ avec $f_1, f_2, g_1, g_2 \in \mathbb{K}(X)$. Comme $\psi(P) = \psi(-P)$ pour tout $P \in E_1$, on a $f(X, Y) = f(X, -Y)$ ce qui donne $f_2 = g_2 = 0$ et donc $W_2(f_1, f_2) = 0$, W_2 étant le polynôme de Weierstrass de la courbe E_2. On peut alors en déduire que f_1 et f_2 sont constantes d'après le lemme technique suivant que nous ne prouverons pas (le lecteur intéressé pourra trouver une preuve dans [4]).

Lemme A.1.0.3. *Il n'existe pas de couple $(r, s) \in K(X)^2$ non constant solution de l'équation de Weierstrass $Y^2 = X^3 + a_2X + b_2$.*

Ainsi, ϕ est constante. □

Considérons :

$$\phi_+ : P \in E_1 \longmapsto \frac{\phi(P) + \phi(-P)}{2} \quad \text{et} \quad \phi_- : P \in E_1 \longmapsto \frac{\phi(P) - \phi(-P)}{2}$$

ϕ_+ est pair donc constant égal à $\phi_+(\mathcal{O}) = \mathcal{O}$. Donc $\phi = \phi_+ + \phi_- = \phi_-$ est impaire.

On montre maintenant que pour tout $Q \in E_1$, le morphisme généralisé :

$$\alpha_Q : P \in E_1 \longmapsto \phi(P + Q) - \phi(P) - \phi(Q)$$

est nul. On considère pour $Q \in E_1$ le morphisme généralisé :

$$\beta_Q : P \in E_1 \longmapsto \phi(P + Q) - \phi(P - Q)$$

Comme ϕ est impaire, β_Q est paire donc constante égale à $\beta_Q(\mathcal{O}) = 2\phi(Q)$. On a donc pour tout $n \in \mathbb{N}^*$:

$$\phi((n + 1)Q) = \phi((n - 1)Q) + \beta_Q(nQ) = \phi((n - 1)Q) + 2\phi(Q)$$

Ceci permet de montrer par récurrence sur $n \in \mathbb{N}$ que $\phi(nQ) = n\phi(Q)$. Et ceci est vrai pour tout $Q \in E_1$.

Soit maintenant $Q \in E_1$. Pour $n \in \mathbb{N}^*$, comme $[n]$ est non constante, elle est surjective (proposition 6.11 de [3]) et Q admet donc un antécédant par $[n]$, noté P. On a alors :

$$\alpha_Q(P) = \phi(P + Q) - \phi(P) - \phi(Q) = \phi((n + 1)P) - \phi(P) - \phi(nP) = (n + 1)\phi(P) - \phi(P) - n\phi(P) = \mathcal{O}$$

Comme pour tout $R \in E[n]$, on a $[n](P + R) = Q$ donc $\alpha_Q(P + R) = \mathcal{O}$. Ceci étant valable pour tout $n \in \mathbb{N}^*$, et $E[n]$ étant de cardinal n^2 (puisqu'ici $\text{car}(K) = 0$), on en déduit que α_Q prend une infinité de fois la valeur $\mathcal{O}$.

Supposons par l'absurde que $\alpha_Q \neq \mathcal{O}$. Alors l'une des coordonnées de α_Q admet une infinité de pôles ce qui n'est le cas pour aucune fonction rationnelle. Donc $\alpha_Q = \mathcal{O}$ et ce pour tout $Q \in E_1$, ce qui donne le résultat. □

Voici maintenant un résultat nous donnant des informations utiles sur la forme normale d'une isogénie.

Lemme A.1.0.4. *Supposons K de caractéristique nulle. Soit $\varphi \in Hom(E_1, E_2)$ une isogénie entre deux courbes elliptiques E_1 et E_2 définies sur K. Écrivons φ sous forme normale :*

$$\varphi(X, Y) := \left(\frac{A(X)}{B(X)}, Y\frac{C(X)}{D(X)}\right)$$

avec $A, B, C, D \in \overline{K}[X] \setminus \{0\}$ tels que $A \wedge B = C \wedge D = 1$. Alors :

$$deg(A) = deg(\varphi) \quad et \quad deg(B) = deg(\varphi) - 1$$

Démonstration. Posons $n := \deg(\varphi)$. Comme $\varphi(\mathcal{O}) = \mathcal{O}$, on a $\deg(A) > \deg(B)$, de sorte que $n = \max(\deg(A), \deg(B)) = \deg(A)$, puis que :

$$\deg(B) < n \quad (1)$$

Or, on sait que :

$$(X^3 + a_1X + b_1)C(X)^2B(X)^3 = (A(X)^3 + a_2A(X)B(X)^2 + b_2B(X)^3)D(X)^2 \quad (2)$$

Considérons alors $U(X)$ le polynôme unitaire simple dont l'ensemble des racines est :

$$S := \{x_P \mid P := (x_P, y_P) \in \ker(\varphi) \setminus E_1[2]\}$$

Alors $U(X)|B(X)$ car tout élément du noyau est pôle de la fonction rationnelle $\frac{A}{B}$ et de plus $U \wedge (X^3 + a_1X + b_1) = 1$ (car les racines de $X^3 + a_1X + b_1$ sont les abscisses des points de $E_1[2] \setminus \{\mathcal{O}\}$). Comme $A \wedge B = 1$, $U \wedge B = 1$ et (2) donne que $U(X)|D(X)^2$, donc $U(X)|D(X)$ car U est à racines simples. Mais alors $U(X)^2|B(X)^3$ par (2) et puisque U est premier avec C et $X^3 + a_1X + b_1$. Puis $U(X)^2|B(X)$ encore par simplicité de U.

Puis, comme $E_1[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ (théorème 6.17 de [3]), $E_1[2] \cap \ker(\varphi) \simeq \{0\}, \mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$. On distingue alors trois cas :

Premier cas : Si $E_1[2] \cap \ker(\varphi) = \{\mathcal{O}\}$ donc $|S| = \frac{n-1}{2}$ (car pour tout $x \in S$, si $P \in \ker(\varphi)$ est d'abscisse x, $-P \neq P$ aussi et ce sont les deux seuls points d'abscisse x) et ainsi, $\deg(B) \geq 2\deg(U) = n - 1$, puis $\deg(B) = n - 1$ par (1).

Deuxième cas : Si $E_1[2] \cap \ker(\varphi) \simeq \mathbb{Z}/2\mathbb{Z}$ alors $|S| = \frac{n-2}{2}$ et de plus B admet une racine qui n'est pas dans S, correspondant à l'abscisse de l'unique point de $E_1[2] \cap \ker(\varphi) \setminus \{\mathcal{O}\}$. D'où $\deg(B) \geq 2\deg(U) + 1 = n - 1$, puis $\deg(B) = n - 1$ par (1).

Troisième cas : Si $E_1[2] \cap \ker(\varphi) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ alors $|S| = \frac{n-4}{2}$ et de plus B admet trois autres racines qui ne sont pas dans S, correspondant à l'abscisse des 3 points de $E_1[2] \cap \ker(\varphi) \setminus \{\mathcal{O}\}$. D'où $\deg(B) \geq 2\deg(U) + 3 = n - 1$, puis $\deg(B) = n - 1$ par (1).

□

A.2 Accouplement de Weil et propriétés du morphisme dual (PSC).

A.2.1 Accouplement de Weil.

Pour rappel, K est un corps de caractéristique $\neq 2, 3$, n est un entier ≥ 2 et μ_n est l'ensemble des racines n-ièmes de l'unité dans $\overline{K}$, la clôture algébrique de K.

Théorème A.2.1.1. *Il existe une application $e_n : E[n]^2 \longrightarrow \mu_n$ appelée* accouplement de Weil *et vérifiant les propriétés suivantes :*

(i) *e_n est bilinéaire :*

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q) \quad \text{et} \quad e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2)$$

pour tous $P, P_1, P_2, Q, Q_1, Q_2 \in E[n]$.

(ii) *e_n est alternée $e_n(P, P) = 1$ pour tout $P \in E[n]$ et $e_n(P, Q) = e_n(Q, P)^{-1}$ pour tous $P, Q \in E[n]$.*

(iii) *e_n est non-dégénérée $e_n(P, Q) = 1$ pour tout $P \in E[n]$ si et seulement si $Q = \mathcal{O}$.*

Démonstration. Soit $Q \in E[n]$. Alors le théorème d'Abel-Jacobi (théorème 4.28 des notes de cours [3]) assure l'existence de $f_Q \in \overline{K}(E)$ telle que :

$$\mathrm{div}(f_Q) = n(Q) - n(\mathcal{O})$$

Soit $Q' \in E \setminus \{\mathcal{O}\}$ tel que $[n]Q' = Q$. Un tel Q' existe car $[n]$ est non nul donc surjectif d'après la proposition 6.11 de [3] et que $|[n]^{-1}(\{Q\})| = |E[n]| = n^2 > 1$ puisque $\mathrm{car}(K)$ ne divise pas n d'après le théorème 6.17 de [3]. Soit $D := \sum_{R \in E[n]}[(Q' + R) - (R)]$. Alors :

$$\mathrm{ord}(D) = |E[n]| - |E[n]| = 0 \quad \text{et} \quad \mathrm{sum}(D) = [|E[n]|]Q' = [n] \circ [n]Q = \mathcal{O}$$

Le théorème d'Abel-Jacobi assure alors l'existence de $g_Q \in \overline{K}(E)$ telle que :

$$div(g_Q) = \sum_{R \in E[n]} [(Q' + R) - (R)]$$

On a alors :

$$div(g_Q^n) = n div(g_Q) = \sum_{R \in E[n]} [n(Q' + R) - n(R)]$$

Par ailleurs, $[n]S = \mathcal{O}$ si et seulement si $S \in E[n]$ et de même $[m]S = Q$ si et seulement si $S = Q' + R$ avec $R \in E[n]$. Ainsi, $f_Q \circ [n]$ a des zéros d'ordre n, qui sont les $Q' + R$ pour $R \in E[n]$ et des pôles d'ordre n qui sont les $R \in E[n]$ et donc :

$$div(f_Q \circ [n]) = \sum_{R \in E[n]} [n(Q' + R) - n(R)] = div(g_Q^n)$$

Or, le théorème d'Abel-Jacobi (4.28 de [3]) assure aussi qu'à diviseur donné, une fonction rationnelle de E est déterminée à une constante près. Quitte à renormaliser f_Q, on peut donc supposer que :

$$f_Q \circ [n] = g_Q^n$$

On en déduit que pour $P \in E[n]$ tout $T \in E \setminus \{-Q\}$:

$$g_Q(T + P)^n = f_Q([n]T + [n]P) = f_Q([n]T) = g_Q(T)^n$$

Donc $T \longmapsto \frac{g_Q(T+P)}{g_Q(T)}$ est à valeurs dans l'ensemble des racines n-ièmes de l'unité de $\overline{K}$ qui est fini de cardinal n (cette fonction valant 1 en $-Q$ puisque les pôles de g_Q sont tous d'ordre -1). Cette fonction ne peut donc pas être surjective puisque $\overline{K}$ est infini. Le lemme suivant assure alors que cette fonction est une constante, que nous noterons $e_n(P, Q)$.

Lemme A.2.1.2. *Une fonction rationnelle de E est soit constante soit surjective.*

Démonstration. Soit $f \in \overline{K}(E)$ non constante. Alors pour tout $\lambda \in \overline{K}$, $f - \lambda$ n'est pas constante donc la remarque 4.35 de [3] assure que cette fonction admet un zéro, ce qui conclut. □

Il s'agit maintenant de montrer que e_n ainsi construite vérifie (i), (ii) et (iii). Ces démonstrations un peu techniques peuvent être sautées en première lecture.

(i) Soient $P, P_1, P_2, Q, Q_1, Q_2 \in E[n]$. Alors comme $T \longmapsto \frac{g_P(T+Q)}{g_P(T)}$ est indépendante de $T \in E \setminus \{-Q\}$. On applique donc la formule définissant le couplage de Weil à T et $T + P_1$:

$$e_n(P_1 + P_2, Q) = \frac{g_Q(T + P_1 + P_2)}{g_Q(T)} = \frac{g_Q(T + P_1)}{g_Q(T)} \frac{g_Q(T + P_1 + P_2)}{g_Q(T + P_1)} = e_n(P_1, Q) e_n(P_2, Q)$$

Le théorème d'Abel-Jacobi assure l'existence de $f \in \overline{K}(E)$ telle que $\mathrm{div}(f) = (Q_1 + Q_2) - (Q_1) - (Q_2) + (\mathcal{O})$.

Soient Q_1' et Q_2' des antécédents respectifs de Q_1 et Q_2 par $[n]$. Alors l'ensemble des zéros de $f \circ [n]$ est $(Q_1' + Q_2' + E[n]) \cup E[n]$ et l'ensemble des ses pôles est $(Q_1' + E[n]) \cup (Q_2' + E[n])$. Tous ces zéros et ces pôles sont d'ordre 1 donc :

$$\begin{aligned}\operatorname{div}(f \circ [n]) &= \sum_{R \in E[n]} (R + Q_1' + Q_2') - \sum_{R \in E[n]} (R + Q_1') - \sum_{R \in E[n]} (R + Q_1') + \sum_{R \in E[n]} (R) \\ &= \sum_{R \in E[n]} [(R + Q_1' + Q_2') - (R)] - \sum_{R \in E[n]} [(R + Q_1') - (R)] - \sum_{R \in E[n]} [(R + Q_1') - (R)] \\ &= \operatorname{div}(g_{Q_1+Q_2}) - \operatorname{div}(g_{Q_1}) - \operatorname{div}(g_{Q_2})\end{aligned}$$

Donc quitte à multiplier f par une constante non nulle, on peut supposer que :

$$f \circ [n] = \frac{g_{Q_1+Q_2}}{g_{Q_1} g_{Q_2}} \quad \text{et donc} \quad g_{Q_1+Q_2} = g_{Q_1} g_{Q_2} (f \circ [n])$$

D'où, en appliquant la formule définissant l'accouplement de Weil en $\mathcal{O}$:

$$e_n(P, Q_1 + Q_2) = \frac{g_{Q_1+Q_2}(P)}{g_{Q_1+Q_2}(\mathcal{O})} = \frac{g_{Q_1}(P) g_{Q_2}(P) f([n]P)}{g_{Q_1}(\mathcal{O}) g_{Q_2}(\mathcal{O}) f([n]\mathcal{O})}$$

Comme $[n]P = \mathcal{O}$, les facteurs en f s'éliminent et on obtient $e_n(P, Q_1 + Q_2) = e_n(P, Q_1) e_n(P, Q_2)$.

(ii) Soient $P \in E[n]$ et P' un antécédant de P par $[n]$. Pour tout $Q \in E$, on rappelle que τ_Q est la translation de Q. Comme $\operatorname{div}(f_P) = n(P) - n(\mathcal{O})$, on a $\operatorname{div}(f_P \circ \tau_{[i]P}) = n(-[i-1]P) - n(-[i]P)$ donc :

$$\begin{aligned}\operatorname{div}\left(\prod_{i=0}^{n-1} f_P \circ \tau_{[i]P}\right) &= \sum_{i=0}^{n-1} \operatorname{div}(f_P \circ \tau_{iP}) = \sum_{i=0}^{n-1} [n(-[i-1]P) - n(-[i]P)] \\ &= \sum_{i=-1}^{n-2} n(-[i]P) - \sum_{i=0}^{n-1} n(-[i]P) = 0\end{aligned}$$

La dernière égalité venant du fait que $[-1]P = [n-1]P$ puisque $P \in E[n]$. Ainsi, $\prod_{i=0}^{n-1} f_P \circ \tau_{[i]P}$ est constante d'après la remarque 4.35 de [3]. Comme $f_P \circ [n] = g_P^n$, et $\tau_{[i]P} \circ [n] = [n] \circ \tau_{[i]P'}$, on a :

$$\left(\prod_{i=0}^{n_1} g_P \circ \tau_{[i]P'}\right)^n = \prod_{i=0}^{n_1} f_P \circ [n] \circ \tau_{[i]P'} = \left(\prod_{i=0}^{n_1} f_P \circ \tau_{[i]P}\right) \circ [n]$$

Et $\left(\prod_{i=0}^{n_1} g_P \circ \tau_{[i]P'}\right)^n$ est donc constante. Donc $\prod_{i=0}^{n_1} g_P \circ \tau_{[i]P'}$ prend un nombre fini de valeurs et ne peut être surjective, donc elle est constante. On a donc en évaluant cette fonction en T et $T + P'$ pour $T \in E$ tel que $T + iP'$ ne soit ni zéro ni pôle de g_P pour tout $i \in \{0, \cdots, n-1\}$:

$$\prod_{i=0}^{n_1} g_P(T + iP') = \prod_{i=0}^{n_1} g_P(T + (i+1)P')$$

Donc en simplifiant $g_P(T) = g_P(T + nP') = g_P(T + P)$ et ainsi $e_n(P, P) = 1$ par définition de e_n.

En combinant (i). et ce que nous venons de montrer, on obtient pour $P, Q \in E[n]$:

$$1 = e_n(P + Q, P + Q) = e_n(P, P) e_n(P, Q) e_n(Q, P) e_n(Q, Q) = e_n(P, Q) e_n(Q, P)$$

Donc $e_n(P, Q) = e_n(P, Q)^{-1}$.

(iii) On commence par prouver le lemme suivant.

Lemme A.2.1.3. *Soit $f \in \overline{K}(E)$ telle que pour tous $P \in E[n]$ et $Q \in E$, on ait $f(Q + P) = f(Q)$. Alors il existe $g \in \overline{K}(E)$ telle que $f = g \circ [n]$.*

Démonstration. Considérons les sous-corps de $\overline{K}(E)$ suivants :

$$L := \{f \in \overline{K}(E) \mid \forall P \in E[n], \quad f \circ \tau_P = f\} \quad \text{et} \quad M := \{g \circ [n] \mid g \in \overline{K}(E)\}$$

et le groupe G formé par les automorphismes $\sigma_P : f \in \overline{K}(E) \longmapsto f \circ \tau_P \in \overline{K}(E)$ pour $P \in E[n]$. Ce groupe est d'ordre n^2 puisque $E[n]$ est d'ordre n^2 (théorème 6.17). L étant un sous-corps $\overline{K}(E)$ invariant sous l'action de G, le lemme d'Artin assure alors que $[\overline{K}(E) : L] = n^2$. Sachant qu'il est clair que $M \subset L$, il suffit de montrer que $[\overline{K}(E) : M] \leq n^2$ pour obtenir que $L = M$ et conclure.

En écrivant $[n] = (r_n(X), Ys_n(X))$ sous forme canonique, on obtient que $r_n(X) = X \circ [n]$ et que $Ys_n(X) = Y \circ [n]$. Ces fonctions sont donc dans M. En outre, on a d'après la proposition 6.15 de [3] :

$$r_n = \frac{X\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2} \quad \text{donc} \quad X\psi_n^2 - \psi_{n-1}\psi_{n+1} - \psi_n^2 r_n = 0$$

Comme ψ_n^2 et $\psi_{n-1}\psi_{n+1}$ sont des polynômes en X de degrés respectifs $n^2 - 1$ et $\frac{(n-1)^2+(n+1)^2-2}{2} = n^2$, on obtient que X est racine d'un polynôme de degré au plus n^2 à coefficients dans M. Donc $M(X)$ est une extension de degré $\leq n^2$ de M.

Mais $\overline{K}(E) = M(X,Y)$ et $Y = \frac{Y \circ [n]}{s_n(X)} \in M(X)$ car $Y \circ [n] \in M$. Donc $\overline{K}(E) = M(X)$ et ainsi $[\overline{K}(E) : M] = [M(X) : M] \leq n^2$. D'où le résultat. □

On a $e_n(P,Q) = 1$ pour tout $P \in E[n]$ par hypothèse donc $g_Q(P+R) = g_Q(R)$ pour tout $R \in E$ et donc le lemme précédent assure l'existence de $h_Q \in \overline{K}(E)$ telle que $g_Q = h_Q \circ [n]$. Il s'ensuit que $(h_Q \circ [n])^n = g_Q^n = f_Q \circ [n]$ donc par surjectivité de $[n]$, $h_Q^n = f_Q$. Donc :

$$n\mathrm{div}(h_Q) = \mathrm{div}(h_Q^n) = \mathrm{div}(f_Q) = n(Q) - n(\mathcal{O})$$

Donc $\mathrm{div}(h_Q) = (Q) - (\mathcal{O})$. La réciproque du théorème d'Abel-Jacobi (admise et dont on trouvera une démonstration dans [4], théorème II. 50) assure alors que $Q = \mathcal{O}$.

□

A.2.2 Propriétés du morphisme dual.

Proposition A.2.2.1. *Soit $\varphi \in Hom(E_1, E_2)$, $\psi \in Hom(E_2, E_3)$ des morphismes. Alors :*

(i) $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$.

(ii) *Si car(K) ne divise pas n alors φ et $\hat{\varphi}$ sont adjointes pour l'accouplement de Weil e_n :*

$$\forall (P,Q) \in E_1[n] \times E_2[n], \quad e_n(\varphi(P), Q) = e_n(P, \hat{\varphi}(Q))$$

(iii) $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\varphi}$.

(iv) $\widehat{[n]} = [n]$ *et* $deg[n] = n^2$ *pour tout* $n \in \mathbb{N}$.

(v) $deg(\hat{\varphi}) = deg(\varphi)$.

(vi) $\hat{\hat{\varphi}} = \varphi$.

Démonstration. **(i)** On a d'après les propriétés de l'isogénie duale et du degré :

$$\begin{aligned}\hat{\varphi} \circ \hat{\psi} \circ \psi \circ \varphi &= \hat{\varphi} \circ [\deg(\psi)] \circ \varphi = [\deg(\psi)] \circ \hat{\varphi} \circ \varphi \\ &= [\deg(\psi)] \circ [\deg(\varphi)] = [\deg(\psi)\deg(\varphi)] = [\deg(\psi \circ \varphi)]\end{aligned}$$

On montre de même que $\psi \circ \varphi \circ \hat{\varphi} \circ \hat{\psi} = [\deg(\psi \circ \varphi)]$, et on conclut par unicité de l'isogénie duale.

(ii) On a pour $R \in E$ donné $e_n(\varphi(P), Q) = \frac{g_Q(R+\varphi(P))}{g_Q(R)}$ avec les notations du paragraphe précédent. Considérons :

$$D := e_\varphi \sum_{R\in\varphi^{-1}(\{Q\})} (R) - e_\varphi \sum_{R\in\varphi^{-1}(\{\mathcal{O}\})} (R) - \left([e_\varphi] \sum_{R\in\varphi^{-1}(\{Q\})} R - [e_\varphi] \sum_{R\in\varphi^{-1}(\{\mathcal{O}\})} R \right) + (\mathcal{O})$$

Alors $\mathrm{sum}(D) = 0$ et $\mathrm{ord}(D) = 0$ donc le théorème d'Abel-Jacobi assure l'existence de $h \in \overline{K}(E)$ telle que $D = \mathrm{div}(h)$. Mais alors, comme $\mathrm{div}(f) = n(P) - n(\mathcal{O})$, on a :

$$\begin{aligned}
\mathrm{div}\left(\frac{f_Q \circ \varphi}{h^n}\right) &= \mathrm{div}(f \circ \varphi) - n\mathrm{div}(h) \\
&= \sum_{R\in\varphi^{-1}(\{Q\})} \mathrm{ord}_R(f\circ\varphi)(R) - \sum_{R\in\varphi^{-1}(\{\mathcal{O}\})} \mathrm{ord}_R(f\circ\varphi)(R) - n\mathrm{div}(h) \\
&= n e_\varphi \left(\sum_{R\in\varphi^{-1}(\{Q\})} (R) - \sum_{R\in\varphi^{-1}(\{\mathcal{O}\})} (R) \right) - n\mathrm{div}(h) \\
&= n \left([e_\varphi] \sum_{R\in\varphi^{-1}(\{Q\})} R - [e_\varphi] \sum_{R\in\varphi^{-1}(\{\mathcal{O}\})} R \right) - n(\mathcal{O}) \\
&= n\left(\hat{\varphi}(Q)\right) - n\left(\mathcal{O}\right)
\end{aligned}$$

Et :

$$\left(\frac{g_Q \circ \varphi}{h \circ [n]}\right)^n = \frac{f_Q \circ [n] \circ \varphi}{(h\circ[n])^n} = \frac{f_Q \circ \varphi \circ [n]}{(h\circ[n])^n} = \frac{f_Q \circ \varphi}{h^n} \circ [n]$$

On peut donc prendre $f_{\hat{\varphi}(Q)} = \frac{f_Q \circ \varphi}{h^n}$ et $g_{\hat{\varphi}(Q)} = \frac{g_Q \circ \varphi}{h \circ [n]}$. Alors comme $[n]P = \mathcal{O}$:

$$\begin{aligned}
e_n(P, \hat{\varphi}(Q)) &= \frac{g_Q \circ \varphi(R+P)}{g_Q \circ \varphi(R)} \frac{h\circ[n](R)}{h\circ[n](R+P)} \\
&= \frac{g_Q(\varphi(R)+\varphi(P))}{g_Q(\varphi(R))} \frac{h([n]R)}{h([n]R+[n]P)} = \frac{g_Q(\varphi(R)+\varphi(P))}{g_Q(\varphi(R))} = e_n(\varphi(P), Q)
\end{aligned}$$

D'où le résultat.

(iii) Par hypothèse, $\mathrm{car}(K) \neq 2$ donc on peut appliquer la proposition précédente avec $n = 2^m$ pour $m \in \mathbb{N}^*$. On obtient alors pour tout $(P, Q) \in E_1[n] \times E_2[n]$, avec la bilinéarité du couplage de Weil et le théorème précédent :

$$\begin{aligned}
e_n(P, \widehat{\varphi+\psi}(Q)) &= e_n((\varphi+\psi)(P), Q) = e_n(\varphi(P)+\psi(P), Q) = e_n(\varphi(P), Q) e_n(\psi(P), Q) \\
&= e_n(P, \hat{\varphi}(Q)) e_n(P, \hat{\psi}(Q)) = e_n(P, \hat{\varphi}(Q) + \hat{\psi}(Q))
\end{aligned}$$

Donc $e_n(P, \widehat{\varphi+\psi}(Q) - \hat{\varphi}(Q) - \hat{\psi}(Q)) = 1$ par antisymétrie et bilinéarité de e_n. Ceci étant valable pour tout $P \in E_1[n]$, la non-dégénérescence de e_n assure que $\widehat{\varphi+\psi}(Q) - \hat{\varphi}(Q) - \hat{\psi}(Q) = \mathcal{O}$ et ce pour tous $Q \in E_2[n]$ et tout $m \in \mathbb{N}^*$ (avec $n = 2^m$). Or, $|E[2^m]| = 4^m$ d'après la proposition 6.17 de [3]. Donc $\widehat{\varphi+\psi} - \widehat{\varphi} - \widehat{\psi}$ est un morphisme de noyau infini. Il est donc nul d'après la proposition 1.1.1.7. D'où le résultat.

(iv) On procède par récurrence sur $n \in \mathbb{N}$ pour prouver que $\widehat{[n]} = [n]$. Il est clair que $\widehat{[0]} = [0]$ et que $\widehat{[1]} = [1]$ (vu que $[1]$ est séparable vu que $X' = 1 \neq 0$ donc de degré $|\ker[1]| = |\{\mathcal{O}\}| = 1$ et que $[1] \circ [1] = [1]$). Soit $n \in \mathbb{N}^*$. Supposons que $\widehat{[n]} = [n]$. Le point (ii) assure alors que :

$$\widehat{[n+1]} = \widehat{[n]+[1]} = \widehat{[n]} + \widehat{[1]} = [n] + [1] = [n+1]$$

Donc on a bien $\widehat{[n]} = [n]$ pour tout $n \in \mathbb{N}$. Ainsi :

$$[\deg([n])] = \widehat{[n]} \circ [n] = [n] \circ [n] = [n^2]$$

Donc $[\deg([n]) - n^2] = 0$ et ainsi $\deg([n]) - n^2 = 0$ puisque $[m]$ est non constante dès que $m \neq 0$. Donc $\deg([n]) = n^2$.

(v) On a d'après le point précédent :

$$(\deg(\varphi))^2 = \deg([\deg(\varphi)]) = \deg(\varphi \circ \hat{\varphi}) = \deg(\varphi)\deg(\hat{\varphi})$$

Donc lorsque $\varphi \neq 0$, $\deg(\varphi) \neq 0$ et $\deg(\hat{\varphi}) = \deg(\varphi)$. Et ceci est encore vrai pour $\varphi = 0$ puisqu'on a alors $\hat{\varphi} = 0$.

(vi) Le point précédent assure que l'on a dans E_1 :

$$\hat{\varphi} \circ \varphi = [\deg(\varphi)] = [\deg(\hat{\varphi})]$$

De même $\varphi \circ \hat{\varphi} = [\deg(\hat{\varphi})]$ dans E_2. Donc $\hat{\hat{\varphi}} = \varphi$ par définition et unicité de l'isogénie duale. □

A.3 Théorème de factorisation (PSC).

Comme toujours, K est un corps commutatif de caractéristique $\neq 2, 3$ et $\overline{K}$ est une clôture algébrique de K et E_1, E_2, E_3 sont des courbes elliptiques définies sur K.

Nous allons ici prouver le résultat suivant :

Théorème A.3.0.1. *(théorème 1.2.0.6) Soient $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_1, E_3)$ des morphismes. Supposons φ séparable et $ker(\varphi) \subset ker(\psi)$. Alors il existe un unique morphisme $\lambda \in Hom(E_2, E_3)$ tel que :*

$$\psi = \lambda \circ \varphi$$

Si $\phi : E_1 \longrightarrow E_2$ est un morphisme généralisé alors on peut définir un morphisme de corps :

$$\begin{array}{rcl} \phi^* : \overline{K}(E_2) & \longrightarrow & \overline{K}(E_1) \\ f & \longmapsto & f \circ \phi \end{array}$$

Ainsi, $\phi^*\overline{K}(E_2)$ est un sous-corps de $\overline{K}(E_1)$. On peut en fait même calculer le degré de l'extension $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ lorsque ϕ est un morphisme.

Théorème A.3.0.2. *Si $\varphi \in Hom(E_1, E_2)$ non nul alors :*

$$[\overline{K}(E_1) : \varphi^*\overline{K}(E_2)] = deg(\varphi)$$

Démonstration. Notons X_i, Y_i les variables de E_i pour $i \in \{1, 2\}$.

Comme φ est non nul, on peut l'écrire sous forme normale $\varphi(X_1, Y_1) := (r(X_1), Y_1 s(X_1))$ avec $r, s \in \overline{K}(X)$. Ainsi, pour tout $g \in \overline{K}(E_2)$ écrite sous forme normale $g(X_2, Y_2) := p(X_2) + Y_2 q(X_2)$ avec $p, q \in \overline{K}(X)$, on a :

$$\varphi^* g(X_1, Y_1) = g \circ \varphi(X_1, Y_1) = p(r(X_1)) + Y_1 s(X_1) q(r(X_1)) \quad (\star)$$

Ainsi, $\varphi^* Y_2 = Y_1 s(X_1)$ et donc $Y_1 = \frac{\varphi^* Y_2}{s(X_1)} \in \varphi^*\overline{K}(E_2)(X_1)$. Il s'ensuit que $\overline{K}(E_1) = \varphi^*\overline{K}(E_2)(X_1)$.

Ecrivons $r := \frac{P}{Q}$ avec $P, Q \in \overline{K}[X]$ non nuls et premiers entre eux. $\chi(X) = P(X) - r(X_1)Q(X)$ est aors un polynôme annulateur non nul (il n'y a pas de compensation des coefficients puisque $r \notin \overline{K}$) de X_1 à coefficients dans $\varphi^*\overline{K}(E_2)$ (puisque $r = \varphi^* X_2$). Il est de degré $\max(\deg(P), \deg(Q)) = \deg(\varphi)$ puisque $r \notin \overline{K}$.

Montrons que c'est le polynôme minimal de X_1 sur $\varphi^*\overline{K}(E_2)$, ce qui conclura. Soit $R(X)$ un polynôme annulateur de X_1 à coefficients dans $\varphi^*\overline{K}(E_2)$ que l'on peut écrire sous la forme :

$$R(X) := \sum_{i=0}^{d} (p_i(r(X_1)) + Y_1 s(X_1) q_i(r(X_1)))X^i$$

par avec $d \in \mathbb{N}^*$ et $p_0, \cdots, p_d, q_0, \cdots, q_d \in \overline{K}(X)$ (d'après $(\star)$). Ainsi, par unicité de la forme normale d'une fonction rationnelle $R_1(X) := \sum_{i=0}^{d} p_i(r(X_1))X^i$ et $R_2(X) := \sum_{i=0}^{d} q_i(r(X_1))X^i$ annulent X_1.

Soit S_1 le reste de R_1 par la division euclidienne par χ dans $\overline{K}(r(X_1))$. Supposons par l'absurde $S_1 \neq 0$. Ecrivons S_1 est un polynôme de degré $< \deg(\varphi)$ à coefficients dans $\overline{K}(r(X_1))$ que l'on peut écrire sous la forme :

$$S_1(X) = \sum_{i=0}^{\deg(\varphi)-1} s_i(r(X_1))X^i$$

avec $s_0, \cdots, s_{\deg(\varphi)-1} \in \overline{K}(X)$. Comme R_1 et χ annullent X_1, S_1 aussi. Quitte à multiplier s_1 par la composée des dénominateurs des s_i avec r_i, on peut donc supposer que les s_i sont dans $\overline{K}[X]$. On peut alors rééctire S_1 en :

$$S_1(X) = \sum_{j=0}^{e} T_j(X) r(X_1)^j$$

avec $T_0, \cdots, T_e \in \overline{K}[X]$ de degré $< \deg(\varphi)$ et $T_e \neq 0$. Quitte à diviser S_1 par r autant de fois que nécessaire, on peut supposer que $T0 \neq 0$. La variable X_1 étant transendante sur $\overline{K}$, on a en fait dans $\overline{K}(X)$:

$$\sum_{j=0}^{e} T_j(X) r(X)^j = 0 \quad \text{i.e.} \quad \sum_{j=0}^{e} T_j(X) Q(X)^{e-j} P(X)^j = 0$$

Comme P et Q sont premiers entre eux, on a donc $P|T_0$ et $Q|T_e$. Mais, T_0 et T_e sont de degré $< \deg(\varphi) = \max(\deg(P), \deg(Q))$ donc T_0 ou T_e est nul. C'est absurde ! Donc $S_1 = 0$ et ainsi $\chi|R_1$. De même, $\chi|R_2$ et $\chi|R$, ce qui prouve que χ est le polynôme minimal de X_1. □

Proposition A.3.0.3. *Soit $\varphi \in Hom(E_1, E_2)$ non-nul et séparable. Alors l'application :*

$$\begin{array}{rcl} \Phi : ker(\varphi) & \longrightarrow & Aut_{\varphi^*\overline{K}(E_2)}(\overline{K}(E_1)) \\ P & \longmapsto & \tau_P^* \end{array}$$

où τ_P désigne la translation de P, définit un isomorphisme de groupes. En conséquence, l'extension $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$ est galoisienne.

Démonstration. On commence par vérifier la bonne définition de Φ. Soit $P \in \ker(\phi)$. Alors $\varphi = \varphi \circ \tau_p$ donc pour tout $f \in \overline{K}(E_2)$:

$$\tau_P^*(\varphi^*(f)) = f \circ \varphi \circ \tau_P = f \circ \varphi = \varphi^*(f)$$

Donc τ_P^* fixe $\varphi^*\overline{K}(E_2)$ donc c'est un morphisme de $\varphi^*\overline{K}(E_2)$-algèbres. En outre, τ_P^* est bijectif de reciproque τ_{-P}^*, ce qui prouve bien que $\tau_P^* \in \mathrm{Aut}_{\varphi^*\overline{K}(E_2)}(\overline{K}(E_1))$.

Puis, si $P, Q \in \ker(\varphi)$, alors pour tout $g \in \overline{K}(E_1)$:

$$\Phi(P+Q)(g) = g \circ \tau_{P+Q} = g \circ \tau_Q \circ \tau_P = \Phi(P) \circ \Phi(Q)(g)$$

Donc Φ est un morphisme de groupes.

Soit $P \in \ker(\varphi)$ tel que $\Phi(P) = id_{\overline{K}(E_1)}$. Alors pour tout $f \in \overline{K}(E_1)$, $f \circ \tau_P = f$ donc en prenant $f = X$ et $f = Y$, on obtient $\tau_P = id_{E_1}$ donc $P = \mathcal{O}$ (en évaluant cette égalité en $\mathcal{O}$). Donc Φ est injective.

La séparabilité de φ assure que $[\overline{K}(E_1) : \varphi^*\overline{K}(E_2)] = \deg(\varphi) = |\ker(\varphi)|$ (la première égalité résulte

du théorème A.3.0.2 et la deuxième de la proposition 6.11 de [3]). Un résultat classique de théorie de Galois (théorème 5.4.1 de [7]) donne alors que :

$$|\mathrm{Aut}_{\varphi^*\overline{K}(E_2)}(\overline{K}(E_1))| \leq [\overline{K}(E_1) : \varphi^*\overline{K}(E_2)]_s \leq [\overline{K}(E_1) : \varphi^*\overline{K}(E_2)] = |\ker(\varphi)|$$

Ce qui permet de conclure à la bijectivité de Φ. L'inégalité ci-dessus est donc en fait une égalité et $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$ est donc séparable puisque $[\overline{K}(E_1) : \varphi^*\overline{K}(E_2)]_s = [\overline{K}(E_1) : \varphi^*\overline{K}(E_2)]$ (corollaire 5.6.3 de [7]) et normale puisque $|\mathrm{Aut}_{\varphi^*\overline{K}(E_2)}(\overline{K}(E_1))| = [\overline{K}(E_1) : \varphi^*\overline{K}(E_2)]_s$, ce qui veut dire que tous les plongements de $\varphi^*\overline{K}(E_2)$-algèbre définis sur $\overline{K}(E_1)$ sont des automorphismes de $\overline{K}(E_1)$. Ainsi, $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$ est galoisienne. □

Démonstration. (du théorème 1.2.0.6) Tout point $P \in \ker(\varphi)$ est aussi dans $\ker(\psi)$, donc τ_P^* est dans $\mathrm{Gal}(\overline{K}(E_1)/\psi^*\overline{K}(E_3))$ d'après la propostion précédente et donc que τ_P^* fixe $\psi^*\overline{K}(E_3)$. Mais comme tous les éléments du groupe de Galois $\mathrm{Gal}(\overline{K}(E_1)/\varphi^*\overline{K}(E_2))$ sont de la forme τ_P^* pour $P \in \ker(\varphi)$ d'après la proposition précédente, on obtient que $\mathrm{Gal}(\overline{K}(E_1)/\varphi^*\overline{K}(E_2))$ fixe $\psi^*\overline{K}(E_3)$ et donc que :

$$\psi^*\overline{K}(E_3) \subset \varphi^*\overline{K}(E_2)$$

par correspondance de Galois (théorème 6.1.1 de [7]).

Considérons donc le plongement :

$$\iota := {\varphi^*}^{-1} \circ i \circ \psi^* : \overline{K}(E_3) \longrightarrow \overline{K}(E_2)$$

où i est l'inclusion canonique de $\psi^*\overline{K}(E_3)$ dans $\varphi^*\overline{K}(E_2)$. Posons alors $\lambda := (\iota(X_3), \iota(Y_3))$ où X_3 et Y_3 sont respectivement les fonctions abscisse et ordonnée de E_3. Si l'on note $W_2(X_2, Y_2)$ et $W_3(X_3, Y_3)$ respectivement les polynômes de Weierstrass de E_2 et E_3 on obtient l'égalité suivante dans $\overline{K}(E_3)$:

$$W_3(\iota(X_3), \iota(X_3)) = \iota(W_3(X_3, Y_3)) = \iota(0) = 0$$

Donc λ est bien un morphisme de E_2 dans E_3. En outre, pour tout $f \in \overline{K}(E_3)$:

$$\lambda^*(f) = f \circ \lambda = f(\iota(X_3), \iota(Y_3)) = \iota(f(X_2, Y_2)) = \iota(f)$$

De sorte que :

$$f \circ \lambda = {\varphi^*}^{-1} \circ i \circ \psi^*(f) \quad \text{i.e.} \quad \varphi^*(f \circ \lambda) = \psi^*(f) \quad \text{i.e.} \quad f \circ \lambda \circ \varphi = f \circ \psi$$

Donc en particulier $X_3 \circ \lambda \circ \varphi = X_3 \circ \psi$ et $Y_3 \circ \lambda \circ \varphi = Y_3 \circ \psi$, puis finalement $\lambda \circ \varphi = \psi$. □

Annexe B

Compléments utiles de théorie algébrique des nombres et d'algèbre commutative.

On reprend ici quelques notions de théorie algébrique des nombres utiles détaillées dans le chapitre 1 de [9] et non développées dans le cours de Gaëtan Genevier [10]. Nous partons des notions les plus élémentaires avant d'aborder des résultats plus ambitieux. Dans cette section, les anneaux sont commutatifs, unitaires et intègres (sauf mention du contraire).

B.1 Ordres des extensions quadratiques imaginaires et conducteur.

Soit K une extension quadratique imaginaire de $\mathbb{Q}$. Soit $x \in K$ un élément primitif de K, qui est donc de partie imaginaire non nulle. Le discriminant d du polynôme minimal π_x de x sur $\mathbb{Q}$ est donc < 0. Avec des manipulations algébriques élémentaires, on obtient alors immédiatement que $K = \mathbb{Q}(\sqrt{d})$. Quitte simplifier et à multiplier $\sqrt{d}$ par le dénominateur de d, on peut supposer de plus que $d \in \mathbb{Z}$ est sans facteur carré.

On peut alors montrer en considérant la norme et la trace que l'anneau d'entiers de K est $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z} + \alpha\mathbb{Z}$ avec :

$$\alpha = \begin{cases} \sqrt{d} & \text{si } d \equiv 2, 3 \ [4] \\ \frac{1+\sqrt{q}}{2} & \text{si } d \equiv 1 \ [4] \end{cases}$$

On pourra trouver une preuve dans la proposition 5.23 de [10].

Proposition B.1.0.1. *Soit $A \subset \mathcal{O}_K$ un ordre de K. Alors il existe un unique $c \in \mathbb{N}^*$ tel que $A = \mathbb{Z} + c\mathcal{O}_K = \mathbb{Z} + c\alpha\mathbb{Z}$. Cet entier est appelé* le conducteur de A.

Démonstration. Considérons $A \cap \alpha\mathbb{Z}$. C'est un idéal de l'anneau $\alpha\mathbb{Z}$, qui est principal de même que $\mathbb{Z}$. $A \not\subset \mathbb{Z}$ car A est un ordre, donc $n + m\alpha \in A$ pour certains entiers $n, m \in \mathbb{Z}$ et $m \neq 0$, puis $m\alpha \in A$ car $\mathbb{Z} \subset A$ et donc $A \cap \alpha\mathbb{Z} \neq \{0\}$. Ainsi, il existe un unique $c \in \mathbb{N}^*$ tel que $A \cap \alpha\mathbb{Z} = c\alpha\mathbb{Z}$.

Montrons qu'un tel c convient. Soit $x \in A$. Alors $x = n + m\alpha$ avec $n, m \in \mathbb{Z}$ et $m\alpha = x - n \in A \cap \alpha\mathbb{Z}$, de sorte que $c|m$. D'où $x \in \mathbb{Z} + c\alpha\mathbb{Z}$. Ainsi, $A = \mathbb{Z} + c\mathcal{O}_K = \mathbb{Z} + c\alpha\mathbb{Z}$. □

B.2 Lemme de Nakayama.

Lemme B.2.0.1 (Nakayama)**.** *Soit A un anneau commutatif unitaire, I un idéal de A et M un A-module de type fini tel que $M \subset IM$. Alors il existe $a \in I$ tel que $(1-a)M = \{0\}$.*

Démonstration. Soit $(m_1, \cdots, m_n)$ une famille A-génératrice de M. Alors comme $M \subset IM$, on a :

$$\forall i \in \{1, \cdots, n\}, \quad m_i = \sum_{j=1}^{n} a_{i,j} m_j$$

avec $a_{i,j} \in I$ pour tous $i, j \in \{1, \cdots, n\}$. Posons $A := (a_{i,j})_{1 \leq i,j \leq n}$, et $m := (m_i)_{1 \leq i \leq n}$. Alors $(I_n - A)m = 0$. Mais la formule de Laplace assure que :

$$^t\mathrm{Com}(I_n - A)(I_n - A) = dI_n$$

avec $d := \det(I_n - A)$. Ainsi, $dm = {}^t\mathrm{Com}(A - I_n)(A - I_n)m = 0$. Comme $(m_1, \cdots, m_n)$ engendre M, il s'ensuit que $dM = 0$. Mais en développant le déterminant, on obtient que $d \equiv 1 \bmod I$ donc $d = 1 - a$ avec $a \in I$, ce qui conclut. □

B.3 Nilradical et radical d'un anneau.

Définition B.3.0.1. *Soit A un anneau commutatif et unitaire (non intègre a priori). Alors on appelle* nilradical *de A et on note $Nil(A)$ l'ensemble des éléments nilpotents de A :*

$$Nil(A) = \{x \in A \mid \exists n \in \mathbb{N}^*, \quad x^n = 0\}$$

Si I est un idéal de A, on appelle nilradical *de I et on note $Nil(I)$ l'intersection $I \cap Nil(A)$.*

Proposition B.3.0.2. *Si I est un idéal de A alors $Nil(I)$ est un idéal de A et c'est même l'intersection de tous les idéaux premiers de A inclus dans I.*

Démonstration. $\mathrm{Nil}(A)$ est bien un idéal de A car c'est le radical de l'idéal nul (on applique la proposition 2.11 de [3]). Le point le moins évident est la stabilité par addition qui se prouve avec la formule du binôme de Newton. Ainsi, $\mathrm{Nil}(I)$ est un idéal comme intersection d'idéeaux.

Soit $\mathfrak{p}$ un idéal premier de A inclus dans I. Alors si $x \in \mathrm{Nil}(I)$, on a $x^n = 0$ pour un certain entier $n \in \mathbb{N}^*$ donc $x^n \in \mathfrak{p}$ donc $x \in \mathfrak{p}$ puisque $\mathfrak{p}$ est premier. Il s'ensuit que :

$$\mathrm{Nil}(I) \subset \bigcap_{\mathfrak{p} \subset I \text{ premier}} \mathfrak{p}$$

Réciproquement, si $x \in A \setminus \mathrm{Nil}(A)$, il s'agit de montrer qu'il existe un idéal $\mathfrak{p}$ premier de A inclus dans I tel que $x \notin \mathfrak{p}$. Considérons l'ensemble E des idéaux de A inclus dans I ne contenant aucune puissance de x. Alors E est inductif pour l'inclusion au sens de la définition suivante :

Définition B.3.0.3. *Un ensemble ordonnée $(E, \leq)$ est dit* inductif *s'il est non-vide et si toute partie totalement ordonnée de E admet un plus grand élément.*

E est non vide car il contient 0 (puisque x n'est pas nilpotent). En outre, si $(I_j)_{j \in J}$ est une famille totalement ordonnée d'idéaux de E, c'est à dire une telle que $(J, \leq)$ est totalement ordonnée telle que $I_j \subset I_k$ dès que $j \leq k$ dans J, alors on peut considérer l'idéal somme :

$$\mathcal{I} = \sum_{j \in J} I_j = \left\{ \sum_{k \in K} x_k \mid K \subset J \quad \text{fini} \quad \text{et} \quad \forall k \in K, \quad x_k \in I_k \right\}$$

$\mathcal{I}$ contient tous les I_j et ne contient aucune puissance de x car si $x^n \in \mathcal{I}$ pour un certain $n \in \mathbb{N}^*$ alors $x^n = \sum_{k\in K} x_k$ pour $K \subset J$ fini et $x_k \in I_k$ pour tout $k \in K$, de sorte que $x^n \in I_{k_0}$ où k_0 est le plus grand élément de K. De plus $\mathcal{I} \subset I$ car tous les I_j sont inclus dans I. C'est donc un majorant dans E de $(I_j)_{j\in J}$. On peut alors appliquer le lemme de Zorn :

Théorème B.3.0.4 (lemme de Zorn)**.** *Si $(E, \leq)$ est un ensemble ordonné inductif, alors E admet un élément maximal.*

Soit donc $\mathfrak{p}$ un élément maximal de E. Alors il ne contient aucune puissance de x donc en particulier, il ne contient pas x. Il reste à montrer que $\mathfrak{p}$ est premier. Soient $y, z \in A \setminus \mathfrak{p}$. Montrons que $yz \notin \mathfrak{p}$. Comme $y \notin \mathfrak{p}$, $\mathfrak{p} \subsetneq \mathfrak{p} + (y)$, de sorte que $\mathfrak{p} + (y) \notin E$ par maximalité de $\mathfrak{p}$. Ainsi, on dispose de $k \in \mathbb{N}^*$, $q \in \mathfrak{p}$ et $a \in A$ tels que :

$$x^k = q + ay$$

Pour la même raison, on dispose de $l \in \mathbb{N}^*$, $r \in \mathfrak{p}$ et $b \in A$ tels que :

$$x^l = r + bz$$

De sorte que :

$$x^{k+l} = qr + qbz + ray + abyz$$

Comme $x^{k+l} \notin \mathfrak{p}$ et que $qr + qbz + ray \in \mathfrak{p}$, nécessairement $yz \notin \mathfrak{p}$, ce qui conclut. □

Corollaire B.3.0.5. *Soient A un anneau et $I \subset J$ deux idéaux de A tels que $\sqrt{I} \subset J$. Alors le radical de I est l'intersection de tous les idéaux premiers $I \subset \mathfrak{p} \subset J$.*

Démonstration. Cela découle de la proposition précédente puisque la projection canonique $A \longrightarrow A/I$ induit une bijection entre les idéaux de A contenant I inclus dans J et les idéaux de A/I inclus dans J/I, le caractère premier des idéaux étant conservé. On conclut en remarquant que I est envoyé sur 0 dans A/I et $\sqrt{I}$ est envoyé sur $\mathrm{Nil}(J/I)$ dans A/I (l'hypothèse $\sqrt{I} \subset J$ étant ici cruciale). □

B.4 Sur la clôture intégrale.

Proposition B.4.0.1. *Soient A un anneau et K son corps de fractions. Soient L/K une extension de corps et B la clôture intégrale de A dans L.*

- **(i)** *Supposons que A est noethérien, intégralement clos (dans K) et que L/K est finie et séparable. Alors B est un A-module de type fini.*
- **(ii)** *Supposons de plus A principal. Alors B est libre de rang $[L : K]$.*

Démonstration. **(i)** Commençons par prouver le lemme suivant :

Lemme B.4.0.2. *L'application :*

$$\begin{array}{rcl} \Phi : L & \longrightarrow & L^* = Hom(L, K) \\ x & \longmapsto & \phi_x : y \in L \longmapsto Tr_{L/K}(xy) \in K \end{array}$$

est un isomorphisme.

Démonstration. Supposons par l'absurde que la fonction $\mathrm{Tr}_{L/K}$ soit identiquement nulle. Alors comme L/K est séparable, on a d'après un résultat classique de théorie des nombres prouvé dans [10] (voir proposition 5.14) :

$$\mathrm{Tr}_{L/K} = \sum_{\sigma\in\Sigma(L/K)} \sigma = 0$$

où $\Sigma(L/K)$ est l'ensemble des K-plongements sur L i.e. des automorphismes de K-algèbres définis sur L (à valeurs dans $\overline{K}$, une clôture algébrique de K).

Or, les éléments de $\Sigma(L/K)$ forment une famille libre sur K. En effet, si $\sigma_1, \cdots, \sigma_n$ sont n K-plongements distincts de L, alors ils forment une famille libre sur K. Montrons-le par récurrence sur n. Si $n = 1$ alors c'est trivial car un morphisme de corps est injectif donc non nul. Sinon, on écrit et $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$ pour $\lambda_1, \cdots, \lambda_n \in K$. On a alors pour tous $x, y \in L$:

$$\sum_{i=1}^{n} \lambda_i(\sigma_i(x) - \sigma_n(x))\sigma(y) = \sum_{i=1}^{n} \lambda_i \sigma_i(xy) - \sigma_n(x) \sum_{i=1}^{n} \lambda_i \sigma_i(y) = 0$$

Donc pour tout $x \in L$, $\sum_{i=1}^{n-1} \lambda_i(\sigma_i(x) - \sigma_n(x))\sigma_i = 0$ et donc $\lambda_i(\sigma_i(x) - \sigma_n(x)) = 0$ par hypothèse de récurrence donc $\lambda_i = 0$ puisque σ_n est distinct des σ_i pour tout $i \in \{1, \cdots, n-1\}$. On en déduit $\lambda_n \sigma_n = 0$, puis $\lambda_n = 0$ puisque $\sigma_n \neq 0$. Ceci termine la récurrence.

Ainsi, l'égalité $\mathrm{Tr}_{L/K} = \sum_{\sigma \in \Sigma(L/K)} \sigma = 0$ est impossible car elle contredit la liberté des éléments de $\Sigma(L/K)$. Donc on dispose de $z \in L$ tel que $\mathrm{Tr}_{L/K}(z) \neq 0$. Donc si $x \in L \setminus \{0\}$ alors $\phi_x\left(\frac{z}{x}\right) = \mathrm{Tr}_{L/K}\left(x\frac{z}{x}\right) \neq 0$. Donc Φ est injective donc bijective par égalité des dimensions. □

Fixons $\mathcal{B} := (e_1, \cdots, e_n)$ une K-base de L. L/K étant algébrique, quitte à multiplier tous les éléments de $\mathcal{B}$ par un certain élément non nul de A, on peut les supposer tous entiers sur A, d'après le lemme qui suit :

Lemme B.4.0.3. *Soit $x \in L$ algébrique sur K. Alors il existe $c \in A \setminus \{0\}$ tel que $cx \in B$.*

Démonstration. Comme x est algébrique sur K, on peut écrire $\sum_{i=0}^{d} \lambda_i x^i = 0$ avec $\lambda_0, \cdots, \lambda_d \in K$ et $\lambda_d \neq 0$. Quitte à diviser par λ_d, on peut supposer $\lambda_d = 1$. Comme K est le corps des fractions de A, on peut écrire $\lambda_i = \frac{a_i}{b_i}$ avec $(a_i, b_i) \in A \times A \setminus \{0\}$ pour tout $i \in \{1, \cdots, d-1\}$. Mais alors, en posant $c := \prod_{i=0}^{d-1} b_i$ et en multipliant l'équation par c^d, con obtient :

$$(cx)^d + \sum_{i=0}^{d-1} a_i b_i^{d-1-i} \prod_{0 \leq j \neq i \leq d-1} b_j^{d-i} (cx)^i = 0$$

donc cx est entier sur A donc $cx \in B$. □

Le lemme B.4.0.2 assure l'existence de $f_1, \cdots, f_n \in L$ tels que :

$$\forall 1 \leq i, j \leq n, \quad \mathrm{Tr}_{L/K}(e_i f_j) = \delta_{i,j} \quad (\star)$$

Il suffit de prendre $f_i := \Phi^{-1}(e_i^*)$ pour tout $i \in \{1, \cdots, n\}$. Le lemme B.4.0.3 assure que pour tout $i \in \{1, \cdots, n\}$, il existe $c_i \in A \setminus \{0\}$ tel que $c_i f_i$ soit entier sur A. En posant $c := \prod_{i=1}^{n} c_i$, on obtient que les cf_i sont entiers sur A, la clôture intégrale de A dans L étant un sous-anneau de L (d'après le lemme B.4.0.3).

Soit $x \in B$. Alors d'après le lemme B.4.0.3, les cxf_i, puis les $\mathrm{Tr}_{L/K}(cxf_i) = \sum_{\sigma \in \Sigma(L/K)} \sigma(cxf_i)$ sont entiers sur A. En outre en écrivant $x = \sum_{i=1}^{n} \lambda_i e_i$ avec $\lambda_1, \cdots, \lambda_n \in K$, on obtient par $(\star)$:

$$\forall i \in \{1, \cdots, n\}, \quad \mathrm{Tr}_{L/K}(cxf_i) = c\lambda_i$$

Comme les $c\lambda_i$ sont entiers sur A et dans K et que A est intégralement clos (dans son corps de fractions K), on a $c\lambda_i \in A$ pour tout $i \in \{1, \cdots, n\}$. Nous venons donc de montrer que $B \subset \sum_{i=1}^{n} Ac^{-1}e_i$.

On conclut avec le lemme classique de théorie des modules qui suit.

Lemme B.4.0.4. *Un sous-module d'un module de type fini sur un anneau noethérien A est de type fini.*

Démonstration. Soit M un A-module de type fini. Considérons $(m_1, \cdots, m_n)$ une famille génératrice de M et le morphisme surjectif de A-modules :

$$f : (a_1, \cdots, a_n) \in A^n \longmapsto \sum_{i=1}^{n} a_i m_i \in M$$

Comme f est surjectif, la propriété universelle du quotient assure qu'il induit un isomorphisme entre $A^n/\ker(f)$ et M. Donc $M \simeq A^n/\ker(f)$ et tout sous-module N de M est isomorphe à $P/\ker(f)$ où P est un sous-A-module de A^n. Comme un quotient d'un module de type fini est de type-fini, il suffit de montrer que P est de type fini. On le prouve par récurrence sur n.

Si $n = 1$ alors P est un idéal de A donc il est de type fini comme A-module car A est noethérien.

Soit $n \geq 2$. Supposons le résultat au rang $n-1$. Soit P un sous-A-module de A^n. Considérons le sous-module de A^n : $M_1 := \{(a, 0, \cdots, 0) | a \in A\}$ et posons $P_1 := P \cap M_1$. Alors d'après le cas $n = 1$, P_1 est de type fini donc on dispose de $x_1, \cdots, x_p \in P_1$ engendrant P_1 comme A-module. Soit la projection canonique $\pi : A^n \longrightarrow A^n/M_1$. Comme $A^n/M_1 \simeq A^{n-1}$, $\pi(P) = P/P_1$ est de type fini par hypothèse de récurrence donc on dispose de $y_1, \cdots, y_q \in P$ tels que $\pi(y_1), \cdots, \pi(y_q)$ engendrent $\pi(P)$ comme A module. Si $x \in P$, $\pi(x) = \sum_{i=1}^{q} a_i \pi(y_i)$ pour $a_1, \cdots, a_q \in A$. On a donc $x - \sum_{i=1}^{q} a_i y_i \in \ker(\pi) \cap P = P_1$ et donc $x - \sum_{i=1}^{q} a_i y_i = \sum_{j=1}^{p} b_j x_j$ pour $b_1, \cdots, b_p \in A$. Nous venons donc de montrer que $(x_1, \cdots, x_p, y_1, \cdots, y_q)$ est génératrice de P, donc que P est de type fini. D'où l'itération et le résultat. □

(ii) Comme A est principal, A est en particulier factoriel donc A est intégralement clos par (ii). A est de plus noethérien donc B, la clôture intégrale de A dans L est un A-module de type fini par (i). B est sans torsion comme sous-anneau de L qui est sans torsion (car c'est un corps). Donc B est libre. Si $(e_1, \cdots, e_n)$ est une K-base de L alors comme L/K est algébrique, le point (i) du lemme B.4.0.3 assure l'existence de $c_i \in A \setminus \{0\}$ tel que $c_i e_i \in B$ pour tout $i \in \{1, \cdots, n\}$. Mais alors $(c_i e_i)_{1 \leq i \leq n}$ est A-libre sur B car K-libre et donc B est de rang $\geq n = [L : K]$. De plus, si $(b_1, \cdots, b_m)$ est une A-base de B et si $\sum_{i=1}^{m} \lambda_i b_i = 0$ pour $\lambda_1, \cdots, \lambda_m \in K$, on a, en prenant c, un dénominateur commun des λ_i, $\sum_{i=1}^{m} c\lambda_i b_i = 0$ avec $c\lambda_i \in A$ pour tout $i \in \{1, \cdots, m\}$ donc $c\lambda_i = 0$, puis $\lambda_i = 0$ pour tout $i \in \{1, \cdots, m\}$. Donc $(b_1, \cdots, b_m)$ est K-libre et $m \leq [L : K]$. Donc B est de rang $[L : K]$. □

B.5 Sur les anneaux de Dedekind.

Définition B.5.0.1. *Un anneau A est de Dedekind s'il est (intègre, commutatif, unitaire), noethérien, intégralement clos et que tout idéal premier non nul de A est maximal.*

Proposition B.5.0.2. *Un anneau principal est de Dedekind.*

Démonstration. Soit A un anneau principal. Alors il est trivialement noethérien. Il est de plus factoriel.

Soit K le corps de fractions de A et soit $x \in K$ entier sur A. Alors on dispose de $d \in \mathbb{N}^*$ et $a_0, \cdots, a_{d-1} \in A$ tels que :

$$x^d + \sum_{i=0}^{d-1} a_i x^i = 0$$

Comme A est factoriel, on peut écrire $x = \frac{p}{q}$ avec $p \in A$ et $q \in A \setminus \{0\}$ premiers entre eux. On a alors :

$$p^d = -\sum_{i=0}^{d-1} a_i p^i q^{d-i} = -q \sum_{i=0}^{d-1} a_i p^i q^{d-1-i}$$

de sorte que $q | p^d$. Comme p et q sont premiers entre eux, q est inversible dans A et $x \in A$. Ainsi, A est intégralement clos.

Soit $\mathfrak{p}$ un idéal premier non nul de A. Alors $\mathfrak{p} = (\pi)$ pour un certain irréductible $\pi \in A$. Si $x \in A \setminus \mathfrak{p}$, considérons l'idéal $\mathfrak{p} + (x) = (\pi) + (x)$. Alors il est principal donc on dispose de $y \in A \setminus \{0\}$ tel que

$(\pi)+(x)=(y)$. Mais alors $y|x$ et $y|\pi$. Mais $x \in A \setminus \mathfrak{p}$ donc $\pi \not| x$ donc π et x sont premiers entre eux, et par suite, $x \in A^\times$. Ainsi, $\mathfrak{p}+(x)=A$, ce qui montre la maximalité de $\mathfrak{p}$ et termine la preuve. □

Proposition B.5.0.3. *Soient A un anneau de Dedekind, K son corps de fractions L/K une extension finie séparable et B est la clôture intégrale de A dans L. Alors B est un anneau de Dedekind.*

Démonstration. Il s'agit de prouver que B est noethérien, intégralement clos et que tout idéal premier non nul de B est maximal.

Le fait que B soit intégralement clos est une conséquence immédiate de la proposition B.4.0.1. Puis, tout idéal de B est un sous-A-module de B sur un anneau noethérien (l'anneau A) donc est de type fini d'après le lemme B.4.0.4. B est donc noethérien.

Enfin, soit $\mathfrak{P}$ un idéal premier non nul de B. Alors $\mathfrak{p} := \mathfrak{P} \cap A$ est un idéal premier de A. Il est de plus non nul car si $x \in \mathfrak{P} \setminus \{0\}$, le lemme B.4.0.2 assure que $cx \in A$ pour un certain $c \in A \setminus \{0\}$, de sorte que cx soit un élément non nul de $\mathfrak{p}$. Donc $\mathfrak{p}$ est maximal puisque A est de Dedekind.

B étant entier sur A, on obtient que $B/\mathfrak{P}$ est algébrique sur $A/\mathfrak{p}$ (en réduisant modulo $\mathfrak{P}$ les équations polynomiales unitaires à coefficients dans A satisfaites par les éléments de B).

Soit donc $x \in B/\mathfrak{P}$ non nul. Alors x est algébrique sur $A/\mathfrak{p}$, de sorte que $A/\mathfrak{p}[x] \subset B/\mathfrak{P}$ soit un corps (isomorphe à $A/\mathfrak{p}[X]/(\pi)$, π étant le polynôme minimal de x sur $A/\mathfrak{p}$). En particulier, x est inversible dans $A/\mathfrak{p}[x]$ donc dans $B/\mathfrak{P}$. Ainsi, $B/\mathfrak{P}$ est un corps et $\mathfrak{P}$ est maximal. □

Théorème B.5.0.4 (Van Der-Waerden)**.** *Soit A un anneau de Dedekind. Alors :*

- **(i)** *L'ensemble des idéaux fractionnaires non nuls de A est un groupe pour la multiplication.*
- **(ii)** *Tout idéal de A admet une décomposition en produit de facteurs premiers et cette décomposition est essentiellement unique (à l'ordre des facteurs près).*

Démonstration. **(i) Étape 1 :** Montrons que si I est un idéal non nul de A alors il existe un produit d'idéaux premiers non nuls inclus dans $\mathfrak{a}$.

Supposons par l'absurde que ce ne soit pas le cas. Alors le lemme de Zorn assure l'existence d'un idéal I qui ne contient aucun produit d'idéaux premiers non-nul de A et qui est maximal pour cette propriété. Alors I n'est bien-sûr pas premier. Ainsi, on dispose de $a, b \in A$ tels que $ab \in I$ mais ni a ni b ne soient dans I. Posons $J := I + aA$ et $J' := I + bA$. Alors $JJ' \subset I$ (car $ab \in I$) et $I \subsetneq J, J'$. Par maximalité de I, J et J' contiennent chacun un produit d'idéaux premiers non-nuls donc I aussi. C'est absurde !

Étape 2 : Montrons que tout idéal premier non-nul de A est inversible (pour le produit des idéaux fractionnaires).

Soient $\mathfrak{p}$ un idéal premier non-nul de A et :

$$\mathfrak{p}^{-1} := \{x \in K | x\mathfrak{p} \subset A\}$$

On voit que $\mathfrak{p}^{-1}$ est un idéal fractionnaire de A dans K (il est stable par somme, par multiplication par A et vérifie $c\mathfrak{p}^{-1} \subset A$ pour tout $c \in \mathfrak{p}$) et qu'il contient A. En outre, $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A$. Mais $\mathfrak{p}$ est premier donc maximal (car A est de Dedekind) et $\mathfrak{p}\mathfrak{p}^{-1}$ est un idéal de A (comme idéal fractionnaire de A inclus dans A) donc $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ ou $\mathfrak{p}\mathfrak{p}^{-1} = A$.

Supposons par l'absurde que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Alors $\mathfrak{p}^{-1}$ stabilise $\mathfrak{p}$ qui est un A-module de type fini (A étant noethérien) et la proposition 1.1.1.7 assure que $\mathfrak{p}^{-1}$ est entier sur A donc inclus dans A car A est intégralement clos.

Il s'agit donc de montrer que $A \subsetneq \mathfrak{p}^{-1}$. Soit $a \in \mathfrak{p} \setminus \{0\}$. Alors l'étape 1 assure l'existence d'idéaux premiers non nuls de A : $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ tels que $\prod_{i=1}^r \mathfrak{p}_i \subset aA$. Supposons r minimal pour cette propriété. Comme $aA \subset \mathfrak{p}$ et que $\mathfrak{p}$ est premier, l'un des $\mathfrak{p}_i$ est contenu dans $\mathfrak{p}$. Quitte à changer l'ordre des facteurs, on peut supposer qu'il s'agit de $\mathfrak{p}_1$. Alors $\mathfrak{p} = \mathfrak{p}_1$ par maximalité de $\mathfrak{p}_1$ (A étant de Dedekind). Mais alors $\prod_{i=2}^r \mathfrak{p}_i \not\subset aA$ car r est minimal et donc on dispose de $b \in \prod_{i=2}^r \mathfrak{p}_i \setminus aA$. Mais alors $b\mathfrak{p} \in \prod_{i=1}^r \mathfrak{p}_i \subset aA$

donc $ba^{-1}\mathfrak{p} \in A$ et $ba^{-1} \in \mathfrak{p}^{-1}$. Mais $ba^{-1} \notin A$ car $b \notin aA$. Ceci conclut l'étape 2 en montrant que $\mathfrak{p}\mathfrak{p}^{-1} = A$.

Étape 3 : Montrons que tout idéal non nul I de A est inversible (dans l'ensemble des idéaux fractionnaires) et son inverse est donné par :

$$I^{-1} := \{x \in K | xI \subset A\}$$

Supposons qu'il existe un idéal non nul I de A qui ne soit pas inversible et prenons I maximal pour cette propriété (comme le lemme de Zorn le permet). Alors I est contenu dans un idéal maximal de A : $\mathfrak{p}$.

En outre, $A \subset \mathfrak{p}^{-1}$ et $I \subset \mathfrak{p}$ donc $I \subset I\mathfrak{p}^{-1} \subset A$. Mais $I\mathfrak{p}^{-1} \neq I$ car sinon $\mathfrak{p}^{-1}$ stabiliserait un A-module de type fini donc serait entier sur A donc inclus dans A, ce qui est exclus comme nous l'avons vu à l'étape 2. Ainsi, $I \subsetneq I\mathfrak{p}^{-1}$ donc $I\mathfrak{p}^{-1}$ est inversible par maximalité de I. Notons $\mathfrak{a}$ son inverse. Alors $\mathfrak{p}^{-1}\mathfrak{a}$ est un inverse de I. Absurde !

Ainsi, tout idéal non-nul I de A admet un inverse fractionnaire. Soit J un inverse de I. Alors $JI = A$ donc tout $x \in J$ vérifie $xI \in A$, de sorte que $J \subset I^{-1}$. Réciproquement, si $x \in I^{-1}$ alors $xI \subset A$ donc $xIJ \subset J$ donc $xA \subset J$ puis $x \in J$. Ainsi, $J = I^{-1}$.

Conclusion : Si $\mathfrak{a}$ est un idéal fractionnaire non-nul de A dans K alors $\mathfrak{a} = c^{-1}I$ pour un certain $c \in A \setminus \{0\}$ et pour un certain idéal non nul I de A. Ainsi, $\mathfrak{a}cI^{-1} = A$ et donc $\mathfrak{a}$ est inversible d'inverse cI^{-1}. Ceci prouve que l'ensemble des idéaux fractionnaires non nuls de A forme un groupe pour la multiplication.

Remarque B.5.0.5. On voit que $cI^{-1} = \mathfrak{a}^{-1} := \{x \in K | x\mathfrak{a} \subset A\}$. En effet, pour tout $x \in K$, on a :

$$x\mathfrak{a} \subset A \iff xc^{-1}I \subset A \iff xc^{-1} \in I^{-1} \iff x \in cI^{-1}$$

(ii) Existence : On suppose par l'absurde qu'il existe un idéal premier non nul I de A qui ne soit pas produit d'idéaux premiers non nuls de A. Prenons I maximal pour cette propriété. Alors il existe un idéal maximal $\mathfrak{p}$ de A contenant I. On a alors $I \subsetneq I\mathfrak{p}^{-1}$ (comme nous l'avons vu dans la preuve du (i)) puisque $I \neq \mathfrak{p}$. En outre, $I\mathfrak{p}^{-1} \subsetneq A$ car $I \neq \mathfrak{p}$. Donc $I\mathfrak{p}^{-1}$ est produit d'idéaux premiers par maximalité de I, puis I est produit d'idéaux premiers. C'est absurde !

Unicité : Soient $\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{q}_1, \cdots, \mathfrak{q}_s$ des idéaux premiers non nuls de A tels que :

$$\prod_{i=1}^{r} \mathfrak{p}_i = \prod_{j=1}^{s} \mathfrak{q}_j$$

Alors $\mathfrak{p}_1 \supset \prod_{j=1}^{s} \mathfrak{q}_j$ donc par primalité de $\mathfrak{p}_1$, $\mathfrak{q}_j \subset \mathfrak{p}_1$ pour un certain $j \in \{1, \cdots, s\}$ et donc $\mathfrak{q}_j = \mathfrak{p}_1$ par maximalité de $\mathfrak{q}_j$ (A étant de Dedekind). Ainsi, en multipliant par $\mathfrak{p}_1^{-1}$, en en appliquant le même raisonnement à $\mathfrak{p}_2$, puis $\mathfrak{p}_3$ etc..., on montre par récurrence que $r \geq s$ et que les $\mathfrak{p}_i$ sont dans le produit $\prod_{j=1}^{s} \mathfrak{q}_j$. Par symétrie, $s \geq r$ et les $\mathfrak{q}_j$ sont dans le produit $\prod_{i=1}^{r} \mathfrak{p}_i$. Ainsi, $r = s$ et les facteurs premiers sont les mêmes. D'où l'unicité. □

B.6 Sur le localisé d'un anneau de Dedekind.

Soient A un anneau, K son corps de fractions et $\mathfrak{p}$ un idéal premier non nul de A. Alors $A \setminus \mathfrak{p}$ est stable par multiplication (par primalité de $\mathfrak{p}$) et ne contient pas 0, ce qui assure que :

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A = \left\{ \frac{a}{s} \mid x \in A \text{ et } a \in A \setminus \mathfrak{p} \right\}$$

est un sous-anneau de K (contenant A). On l'appelle *l'anneau localisé de A en $\mathfrak{p}$*. Il porte effectivement bien son nom :

Proposition B.6.0.1. *$A_\mathfrak{p}$ est un anneau local, c'est à dire qu'il contient un unique idéal maximal qui s'écrit :*

$$\mathfrak{m}_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}\mathfrak{p} = \left\{ \frac{a}{s} | a \in \mathfrak{p} \text{ et } s \in A \setminus \mathfrak{p} \right\}$$

Démonstration. Remarquons que l'ensemble des inversibles de $A_\mathfrak{p}$ est le complémentaire de $\mathfrak{m}_\mathfrak{p}$. En effet, si $x \in A_\mathfrak{p}^\times$ alors $xy = 1$ pour un certain $y \in A_\mathfrak{p}^\times$ et on écrit alors $x := \frac{a}{s}$, $y := \frac{b}{t}$ avec $a, b \in A$ et $s, t \in A \setminus \mathfrak{p}$ donc $ab = ts \in A \setminus \mathfrak{p}$ donc $a \in A \setminus \mathfrak{p}$ (car sinon $ts \in \mathfrak{p}$) ie $x \notin \mathfrak{m}_\mathfrak{p}$. Réciproquement, si $x \in A_\mathfrak{p} \setminus \mathfrak{m}_\mathfrak{p}$ alors $x := \frac{a}{s}$ avec $a, s \in A \setminus \mathfrak{p}$ et $x\frac{s}{a} = 1$ donc $x \in A_\mathfrak{p}^\times$.

Il s'ensuit que tout idéal de $A_\mathfrak{p}$ est inclus dans $\mathfrak{m}_\mathfrak{p}$ ou contient un inversible de $A_\mathfrak{p}$ donc est $A_\mathfrak{p}$ tout entier. Donc $\mathfrak{m}_\mathfrak{p}$ est un idéal maximal de $A_\mathfrak{p}$.

Si $\mathfrak{m}$ est un (autre) idéal maximal de $A_\mathfrak{p}$, on a donc $\mathfrak{m} \subset \mathfrak{m}_\mathfrak{p}$ (puisque $\mathfrak{m} \neq A_\mathfrak{p}$) et donc $\mathfrak{m} = \mathfrak{m}_\mathfrak{p}$ par maximalité de $\mathfrak{m}$. D'où l'unicité. □

Proposition B.6.0.2. *Si A est un anneau de Dedekind et si $\mathfrak{p}$ est un idéal premier non nul de A, alors $A_\mathfrak{p}$ est de Dedekind.*

Démonstration. Soit $x \in K = \mathrm{Frac}(A)$ entier sur $A_\mathfrak{p}$. Alors en multipliant une équation polynomiale unitaire à coefficients dans $A_\mathfrak{p}$ vérifiée par x, par la bonne quantité, on obtient que sx est entier sur A pour un certain $s \in A \setminus \mathfrak{p}$. Donc $sx \in A$ car A est intégralement clos. D'où $x \in (A \setminus \mathfrak{p})^{-1}A = A_\mathfrak{p}$. $A_\mathfrak{p}$ est donc intégralement clos.

Lemme B.6.0.3. *Etant donné un idéal I' de $A_\mathfrak{p}$, on a :*

$$I' = (A \setminus \mathfrak{p})^{-1}(I' \cap A)$$

Démonstration. Soit $x \in I'$. Alors $x = \frac{a}{s}$ avec $(a, s) \in A \times A \setminus \mathfrak{p}$ donc $sx = a \in A$ et $sx \in I'$ (car I' est un idéal de $A_\mathfrak{p}$). Donc $sx \in I' \cap A$, puis $x \in (A \setminus \mathfrak{p})^{-1}(I' \cap A)$.

Réciproquement, si $x \in (A \setminus \mathfrak{p})^{-1}(I' \cap A)$ alors $x = \frac{a}{s}$ avec $(a, s) \in I' \cap A \times A \setminus \mathfrak{p}$ donc $x = \frac{1}{s}a$ avec $a \in I'$ donc $x \in I'$. □

Le lemme ci-dessus assure que tout idéal I' de $A_\mathfrak{p}$ s'écrit $I' = (A \setminus \mathfrak{p})^{-1}(I' \cap A)$, avec $I' \cap A$ idéal de A, donc de type fini comme A-module (car A est noethérien). Ainsi, $A_\mathfrak{p}$ est noethérien.

Enfin, si $\mathfrak{q}$ est un idéal premier non nul de $A_\mathfrak{p}$, alors $\mathfrak{q} \cap A$ est premier non nul dans A donc maximal et tout idéal I' de $A_\mathfrak{p}$ tel que $\mathfrak{q} \subset I'$ vérifie $\mathfrak{q} \cap A \subset I' \cap A$ donc $I' \cap A = \mathfrak{q} \cap A$ ou A, de sorte que $I' = (A \setminus \mathfrak{p})^{-1}(I' \cap A) = \mathfrak{q}$ ou $A_\mathfrak{p}$. Ainsi, $\mathfrak{q}$ est maximal. Ceci achève de montrer que $A_\mathfrak{p}$ est de Dedekind. □

Proposition B.6.0.4. *Si A est de Dedekind et admet un nombre fini d'idéaux premiers, alors A est principal.*

Démonstration. On commence par prouver le lemme suivant :

Lemme B.6.0.5. *Si I et J sont des idéaux de A tels que $I + J = A$ alors $I^\alpha + J^\beta = A$ pour tous $\alpha, \beta \in \mathbb{N}$ (avec la convention $I^0 = J^0 = A$).*

Démonstration. On raisonne par récurrence sur $\alpha + \beta \in \mathbb{N}$. On connaît le résultat pour $\alpha + \beta \leq 2$.

Soit $N \geq 3$. Suppposons le résultat vrai pour tous $\alpha, \beta \in \mathbb{N}$ tels que $\alpha + \beta \leq N - 1$. Soient $\alpha, \beta \in \mathbb{N}$ tels que $\alpha + \beta = N$. Si $\alpha = 0$ ou $\beta = 0$, il est clair que $I^\alpha + J^\beta = A$. Sinon, l'hypothèse de récurrence donne que $I^{\alpha-1} + J^{\beta-1} = A$. En multipliant ceci par $I + J$, on obtient :

$$I^\alpha + IJ^{\beta-1} + JI^{\alpha-1} + J^\beta = A \quad (\star)$$

Or, en multipliant $I + J = A$ par $I^{\alpha-1}$ et par $J^{\beta-1}$, on obtient :

$$I^\alpha + JI^{\alpha-1} = I^{\alpha-1} \quad \text{et} \quad IJ^{\beta-1} + J^\beta = J^{\beta-1}$$

Ainsi, $JI^{\alpha-1} = I^{\alpha-1} + I^{\alpha}$ et $IJ^{\beta-1} = J^{\beta-1} + J^{\beta}$, de sorte que par somme :

$$JI^{\alpha-1} + IJ^{\beta-1} = I^{\alpha-1} + I^{\alpha} + J^{\beta-1} + J^{\beta} = A + I^{\alpha} + J^{\beta} = A$$

En substituant dans $(\star)$, il vient que $I^{\alpha} + J^{\beta} = A$. D'où l'itération et le résultat. □

Soit $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$ l'ensemble des idéaux premiers de A. Soit I un idéal de A que l'on peut décomposer de façon unique en produit de $\mathfrak{p}_i$ (d'après le point (ii) du théorème B.5.0.4) :

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$$

On sait qu'alors $\mathfrak{p}_i^2 \neq \mathfrak{p}_i$ pour tout $i \in \{1, \cdots, r\}$ (car sinon on obtientdrait $\mathfrak{p}_i = A$ en multipliant par $\mathfrak{p}_i^{-1}$). On dispose donc de $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$ pour tout $i \in \{1, \cdots, r\}$. Les idéaux premiers de A étant maximaux, on sait que $\mathfrak{p}_i + \mathfrak{p}_j = A$ pour tous $1 \leq i \neq j \leq r$, de sorte que $\mathfrak{p}_i^{\alpha_i+1} + \mathfrak{p}_j^{\alpha_j+1} = A$ pour tous $1 \leq i \neq j \leq r$, d'après le lemme ci-dessus. Le théorème des restes chinois s'applique alors et fournit $y \in A$ tel que :

$$\forall i \in \{1, \cdots, r\}, \quad y \equiv x_i^{\alpha_i} \bmod \mathfrak{p}_i^{\alpha_i+1}$$

Factorisons yA en produit d'idéaux premiers :

$$yA = \prod_{i=1}^{r} \mathfrak{p}_i^{\beta_i}$$

Soit $i \in \{1, \cdots, r\}$. Alors $y \equiv 0 \bmod \mathfrak{p}_i^{\beta_i}$ donc $\beta_i < \alpha_i + 1$ car $x_i^{\alpha_i} \notin \mathfrak{p}_i^{\alpha_i+1}$ vu que $x_i \notin \mathfrak{p}_i^2$. Mais $y \equiv 0 \bmod \mathfrak{p}_i^{\alpha_i}$ donc $yA \subset \mathfrak{p}_i^{\alpha_i}$, de sorte que $\beta_i \geq \alpha_i$ d'après la proposition 2.5.1.5. Ainsi :

$$yA = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i} = I$$

Donc A est principal.

□

Corollaire B.6.0.6. *Si A est de Dedekind et si $\mathfrak{p}$ est un idéal premier non nul de A alors $A_{\mathfrak{p}}$ est un anneau de valuation discrète.*

Démonstration. Ceci découle directement des trois propositions qui précèdent. □

B.7 Idéaux premiers et extensions d'anneaux de Dedekind.

B.7.1 Cas Général.

On fixe A un anneau, K son corps de fractions, B un anneau contenant A et $\mathfrak{p}$ un idéal premier de A. En considérant l'ensemble multiplicatif $A \setminus \mathfrak{p}$, on notera $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$ la localisation de A en $\mathfrak{p}$ et $B_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}B$.

Définition B.7.1.1. *On dira qu'un idéal premier $\mathfrak{P}$ de B est* au-dessus de $\mathfrak{p}$ *lorsque $\mathfrak{p} = \mathfrak{P} \cap A$ et on notera alors $\mathfrak{P}|\mathfrak{p}$.*

Proposition B.7.1.2. *Soient B un anneau entier sur A et $\mathfrak{P}$ un idéal premier de B au-dessus de $\mathfrak{p}$. Alors $\mathfrak{p}$ est maximal si et seulement si $\mathfrak{P}$ est maximal.*

Démonstration. $\Longrightarrow$ Supposons $\mathfrak{p}$ maximal. B étant entier sur A, on obtient que $B/\mathfrak{P}$ est algébrique sur $A/\mathfrak{p}$ (en réduisant modulo $\mathfrak{P}$ les équations polynomiales unitaires à coefficients dans A satisfaites par les éléments de B).

Soit donc $x \in B/\mathfrak{P}$ non nul. Alors x est algébrique sur $A/\mathfrak{p}$, de sorte que $A/\mathfrak{p}[x] \subset B/\mathfrak{P}$ soit un corps (isomorphe à $A/\mathfrak{p}[X]/(\pi)$, π étant le polynôme minimal de x sur $A/\mathfrak{p}$). En particulier, x est inversible dans $A/\mathfrak{p}[x]$ donc dans $B/\mathfrak{P}$. Ainsi, $B/\mathfrak{P}$ est un corps et $\mathfrak{P}$ est maximal.

$\Longleftarrow$ Supposons $\mathfrak{P}$ maximal. Alors $B/\mathfrak{P}$ est un corps entier sur $A/\mathfrak{p}$. Si par l'absurde $A/\mathfrak{p}$ n'était pas un corps alors on disposerait d'un idéal maximal (donc premier) $\mathfrak{m}$ de $A/\mathfrak{p}$ et la proposition précédente assurerait l'existence de $\mathfrak{M}$, idéal premier de $B/\mathfrak{P}$ au-dessus de $\mathfrak{m}$. Le sens $\Longrightarrow$ assure la maximalité de $\mathfrak{M}$. Mais $\mathfrak{m} \subset \mathfrak{M}$ et $\mathfrak{m} \neq \{0\}$ donc $\mathfrak{M} \neq \{0\}$ donc, $B/\mathfrak{P}$ étant un corps, $\mathfrak{M} = B/\mathfrak{P}$ et $\mathfrak{m} = \mathfrak{M} \cap A/\mathfrak{p} = A/\mathfrak{p}$, ce qui est exclus. Ainsi, $A/\mathfrak{p}$ est un corps et $\mathfrak{p}$ est maximal. □

Proposition B.7.1.3. *Supposons A intégralement clos (dans son corps de fractions K) et L/K finie et galoisienne de groupe de Galois G. Soient $\mathfrak{P}$ et $\mathfrak{Q}$ des idéaux premiers de B (la clôture intégrale de A dans L) au-dessus de $\mathfrak{p}$ (idéal premier de A). Alors il existe $\sigma \in G$ tel que $\mathfrak{Q} = \sigma(\mathfrak{P})$.*

Démonstration. Quitte à localiser en $\mathfrak{p}$ (ce qui est possible car G stabilise $A \setminus \mathfrak{p} \subset A \subset K$), on peut supposer $\mathfrak{p}$ maximal. Supposons par l'absurde $\mathfrak{Q} \neq \sigma(\mathfrak{P})$ pour tout $\sigma \in G$. Commençons par remarquer que $\mathfrak{P}$ et $\mathfrak{Q}$ sont maximaux (d'après la proposition B.7.1.2) et que pour tout $\sigma \in G$, $\sigma(\mathfrak{P})$ est maximal. Ainsi, pour tout $\sigma \in G$, $\mathfrak{Q} \subsetneq \mathfrak{Q} + \sigma(\mathfrak{P})$ donc $\mathfrak{Q} + \sigma(\mathfrak{P}) = B$ par maximalité de $\mathfrak{Q}$ et de même $\sigma(\mathfrak{P}) + \tau(\mathfrak{P}) = B$ dès que $\sigma(\mathfrak{P}) \neq \tau(\mathfrak{P})$ (pour $\sigma, \tau \in G$). Le théorème des restes Chinois s'applique alors et assure l'existence de $x \in B$ tel que :

$$x \equiv 0 \bmod \mathfrak{Q} \quad \text{et} \quad \forall \sigma \in G, \quad x \equiv 1 \bmod \sigma(\mathfrak{P}) \qquad (\star)$$

x est entier sur A et il en est de même de $\sigma(x)$ pour tout $\sigma \in G$ donc $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in B$. Or, on sait que $N_{L/K}(x) \in K$ et que A est intégralement clos (dans K), donc $N_{L/K}(x) \in A$. Mais x divise $N_{L/K}(x)$ dans B et $x \in \mathfrak{Q}$ par $(\star)$ donc $N_{L/K}(x) \in \mathfrak{Q}$. Ainsi, $N_{L/K}(x) \in A \cap \mathfrak{Q} = \mathfrak{p}$. Comme $\mathfrak{p} \subset \mathfrak{P}$ et que $\mathfrak{P}$ est premier, il existe donc $\sigma \in G$ tel que $\sigma(x) \in \mathfrak{P}$.

Or, $(\star)$ assure que $x \notin \sigma(\mathfrak{P})$ pour tout $\sigma \in G$ donc $\sigma(x) \notin \mathfrak{P}$ pour tout $\sigma \in G$. C'est absurde ! □

Corollaire B.7.1.4. *Si L/K est finie et séparable alors il existe un nombre fini d'idéaux premiers de L au-dessus de $\mathfrak{p}$.*

Démonstration. L/K étant finie et séparable, le théorème de l'élément primitif (théorème 5.4.6. de [7]) assure l'existence de $\alpha \in L$ tel que $L = K[\alpha]$. α est alors algébrique sur K et on peut considérer M le sous-corps d'une clôture algébrique de K engendré (sur K) par tous les K-conjugués de α. M est une extension galoisienne finie de K qui contient L. Notons C la clôture intégrale de B dans M.

Si $\mathfrak{P}_1$ et $\mathfrak{P}_2$ sont deux idéaux premiers distincts de B au-dessus de $\mathfrak{p}$ et si $\mathfrak{Q}_1$ et $\mathfrak{Q}_2$ sont des idéaux premiers de C respectivement au-dessus de $\mathfrak{P}_1$ et $\mathfrak{P}_2$ alors $\mathfrak{Q}_1 \cap A = \mathfrak{P}_1 \neq \mathfrak{Q}_2 \cap A = \mathfrak{P}_2$ donc $\mathfrak{Q}_1$ et $\mathfrak{Q}_2$ sont distincts. Ils sont de plus au-dessus de $\mathfrak{p}$. Ainsi, l'ensemble des idéaux premiers de B au-dessus de $\mathfrak{p}$ s'injecte dans l'ensemble des idéaux de C au-dessus de $\mathfrak{p}$. Or, cet ensemble est fini majoré par $[M : K]$ car le groupe de Galois de M/K permute transitivement les idéaux de C au-dessus de $\mathfrak{p}$ d'après la proposition précédente. □

B.7.2 Cas des anneaux de Dedekind.

On fixe A un anneau, K son corps de fractions, B un anneau contenant A et $\mathfrak{p}$ un idéal premier de A. En considérant l'ensemble multiplicatif $A \setminus \mathfrak{p}$, on notera $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$ la localisation de A en $\mathfrak{p}$ et $B_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}B$.

Définition B.7.2.1. *On dira qu'un idéal premier $\mathfrak{P}$ de B est* au-dessus de $\mathfrak{p}$ *lorsque $\mathfrak{p} = \mathfrak{P} \cap A$ et on notera alors $\mathfrak{P}|\mathfrak{p}$.*

On fixe dans la suite de ce paragraphe un anneau de Dedekind A, $\mathfrak{p}$ un idéal premier non nul de A, K le corps de fractions de A, une extension finie et séparable L/K et B la clôture intégrale de A dans L. On sait qu'alors B est de Dedekind (par la proposition B.5.0.3).

$\mathfrak{p}B$, l'idéal de B engendré par $\mathfrak{p}$ admet une décomposition (unique) en produit d'idéaux premiers :

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

avec $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ distincts deux à deux et $e_1, \cdots, e_r \in \mathbb{N}^*$.

Les $\mathfrak{P}_i$ sont tous les idéaux premiers de B contenant $\mathfrak{p}B$ (donc $\mathfrak{p}$). On a donc pour tout $i \in \{1, \cdots, r\}$, $\mathfrak{p} \subset \mathfrak{P}_i \cap A$ avec $\mathfrak{p}$ maximal donc $\mathfrak{P}_i \cap A = \mathfrak{p}$ i.e. $\mathfrak{P}_i | \mathfrak{p}$. Ainsi :

Proposition B.7.2.2. *Les idéaux premiers intervenant dans la décomposition de $\mathfrak{p}B$ sont les idéaux premiers de B au-dessus de $\mathfrak{p}$.*

Pour tout $i \in \{1, \cdots, r\}$, l'indice e_i est appelé *indice de ramification de $\mathfrak{p}$ en $\mathfrak{P}_i$* et noté $e(\mathfrak{P}_i/\mathfrak{p})$ ou $e_{\mathfrak{P}_i}$. Bien-sûr, cette dénomination s'étend aux idéaux premiers de B qui ne sont pas au-dessus de $\mathfrak{p}$, auquel cas l'indice de ramification est nul.

On sait par ailleurs que pour tout $\mathfrak{P}|\mathfrak{p}$, $B/\mathfrak{P}$ est une extension du corps $A/\mathfrak{p}$ ($\mathfrak{p}$ et $\mathfrak{P}$ étant maximaux). On note :

$$f(\mathfrak{P}/\mathfrak{p}) = f_{\mathfrak{P}} := [B/\mathfrak{P} : A/\mathfrak{p}]$$

quantité que l'on appelle *degré d'inertie de $B/\mathfrak{P}$ sur $A/\mathfrak{p}$*.

Définition B.7.2.3. *Pour tout $\mathfrak{P}|\mathfrak{p}$, on définit la* norme *de $\mathfrak{P}$ par :*

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$$

On étend cette formule à tous les idéaux fractionnaires non nuls de B par multiplicativité (sachant qu'ils se décomposent de façon unique en produit d'idéaux premiers).

Proposition B.7.2.4. *Soit A un anneau de Dedekind, K son corps de factions, $M/L/K$ une tour d'extensions finies séparables B la clôture intégrale de A dans L et C la clôture intégrale de B dans M. Alors si $\mathfrak{p}, \mathfrak{P}$ et $\mathfrak{Q}$ sont des idéaux premiers non-nuls respectifs de A, B et C tels que $\mathfrak{Q}|\mathfrak{P}$ et $\mathfrak{P}|\mathfrak{p}$ alors :*

$$e(\mathfrak{Q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p}) \quad \text{et} \quad f(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$$

Démonstration. Dans (i), la multiplicativité des degrés d'inertie est une conséquence du théorème de la base téléscopique. On prouve donc la multiplicativité des indices de ramicication. On sait que :

$$\begin{aligned}\mathfrak{p}C = \mathfrak{p}BC &= \left(\prod_{\mathfrak{P}'|\mathfrak{p}} \mathfrak{P}'^{e(\mathfrak{P}'/\mathfrak{p})}\right) C = \prod_{\mathfrak{P}'|\mathfrak{p}} (\mathfrak{P}'C)^{e(\mathfrak{P}'/\mathfrak{p})} \\ &= \prod_{\mathfrak{P}'|\mathfrak{p}} \left(\prod_{\mathfrak{Q}'|\mathfrak{P}'} \mathfrak{Q}'^{e(\mathfrak{Q}'/\mathfrak{P}')}\right)^{e(\mathfrak{P}'/\mathfrak{p})} = \prod_{\mathfrak{P}'|\mathfrak{p}} \prod_{\mathfrak{Q}'|\mathfrak{P}'} \mathfrak{Q}'^{e(\mathfrak{Q}'/\mathfrak{P}')e(\mathfrak{P}'/\mathfrak{p})} \quad (\star)\end{aligned}$$

Or, si par l'absurde $\mathfrak{Q}'$ est un idéal premier non nul de C au-dessus de $\mathfrak{P}_1$ et $\mathfrak{P}_2$, idéaux premiers non nuls distincts de B, alors $\mathfrak{Q}'$ contient $\mathfrak{P}_1 + \mathfrak{P}_2 = A$ ($\mathfrak{P}_1$ et $\mathfrak{P}_2$ étant maximaux car B est de Dedekind) donc 1, donc C, ce qui est exclus. Ainsi, les idéaux premiers intervenant dans $(\star)$ sont tous distincts et on a donc bien :

$$e(\mathfrak{Q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$$

□

Théorème B.7.2.5. *Si A est de Dedekind, que L/K est finie et séparable et si $\mathfrak{p}$ est un idéal premier non nul de A alors :*

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$$

Démonstration. Posons $S_\mathfrak{p} := A \setminus \mathfrak{p}$ et $B_\mathfrak{p} := S_\mathfrak{p}^{-1}B$ et $\mathfrak{m}_\mathfrak{p} := S_\mathfrak{p}^{-1}\mathfrak{p}$, l'unique idéal premier de $A_\mathfrak{p} = S_\mathfrak{p}A$. Si la décomposition de $\mathfrak{p}B$ s'écrit $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$ alors celle de $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p}$ dans $B_\mathfrak{p}$ (qui reste un anneau de Dedekind d'après la proposition B.5.0.3) s'écrit :

$$\mathfrak{m}_\mathfrak{p}B_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} S_\mathfrak{p}^{-1}\mathfrak{P}^{e_\mathfrak{P}}$$

les idéaux $S_\mathfrak{p}^{-1}\mathfrak{P}$ restant maximaux, de même que $\mathfrak{P}$ et deux à daux distincts (car d'intersection avec B deux à deux distincts). Donc les indices de ramification sont invariants par localisation. Montrons que c'est aussi le cas des degrés d'inertie. C'est une conséquence du lemme suivant :

Lemme B.7.2.6. **(i)** *$A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ et $A/\mathfrak{p}$ sont isomorphes (en tant qu'anneaux).*

(ii) *Si $\mathfrak{P}$ est un idéal premier de B au-dessus de $\mathfrak{p}$, alors $B_\mathfrak{p}/S_\mathfrak{p}^{-1}\mathfrak{P}$ et $B/\mathfrak{P}$ sont isomorphes (en tant qu'anneaux).*

Démonstration. **(i)** On a un morphisme naturel $\varphi : A \longrightarrow A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ induit par l'inclusion de A dans $A_\mathfrak{p}$. φ est surjectif. En effet, $\mathfrak{p}$ est maximal donc si $s \in S_\mathfrak{p}$ alors $\mathfrak{p} + sA = A$ et donc pour tout $a \in A$, il existe $b \in A$ tel que $a - sb \in \mathfrak{p}$ i.e. $\frac{a}{s} - b \in \mathfrak{p}$. Ceci montre la surjectivité de φ.

En outre, $\ker(\varphi) = \mathfrak{p}$. En effet, l'inclusion $\supset$ est triviale et réciproquement si $x \in A$ vérifie $\varphi(x) = 0$ alors $x \in \mathfrak{m}_\mathfrak{p}$ donc $x = \frac{a}{s}$ avec $a \in \mathfrak{p}$ et $s \in S_\mathfrak{p}$ donc $sx \in \mathfrak{p}$ avec $s \in A \setminus \mathfrak{p}$ et donc $x \in \mathfrak{p}$ par primalité de $\mathfrak{p}$. φ induit donc un isomorphisme entre $A/\mathfrak{p}$ et $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$.

(ii) se prouve de la même manière. □

Ainsi, quitte à localiser en $\mathfrak{p}$, on peut supposer que A est un anneau de valuation discrète. Ainsi, A est principal donc le point (ii) de la proposition B.4.0.1 assure que B est un A-module libre de rang $[L : K]$. Le lemme suivant assure alors que $B/\mathfrak{p}B$ est un $A/\mathfrak{p}$-espace vectoriel de dimension $[L : K]$.

Lemme B.7.2.7. *Si A est un anneau de valuation discrète d'unique idéal premier $\mathfrak{p}$ et si M est un A-module libre de rang n alors $M/\mathfrak{p}M$ est un $A/\mathfrak{p}$-espace vectoriel de dimension n.*

Démonstration. Considérons donc $(e_1, \cdots, e_n)$ une A-base de M et $(\overline{e_1}, \cdots, \overline{e_r})$ sa réduite modulo $\mathfrak{p}M$. Alors elle engendre trivialement $M/\mathfrak{p}M$ (en tant que $A/\mathfrak{p}$-espace vectoriel).

Soient $\lambda_1, \cdots, \lambda_n \in A$ vérifient $\sum_{i=1}^n \overline{\lambda_i}\overline{e_i} = \overline{0}$ (les $\overline{\lambda_i}$ étant les réduites modulo $\mathfrak{p}$ des λ_i). Alors $\sum_{i=1}^n \lambda_i e_i \in \mathfrak{p}M$. Mais $\mathfrak{p} = \pi A$ pour une certaine uniformisante π donc on dispose de $x \in M$ tel que :

$$\sum_{i=1}^n \lambda_i e_i = \pi x$$

Ecrivons $x = \sum_{i=1}^n \mu_i e_i$ dans la A-base $(e_1, \cdots, e_n)$. Alors :

$$\sum_{i=1}^n (\lambda_i - \pi\mu_i)e_i = 0$$

donc $\lambda_i = \pi\mu_i \in \mathfrak{p}$ de sorte que $\overline{\lambda_i} = \overline{0}$, pour tout $i \in \{1, \cdots, n\}$ par liberté sur A des e_i. Donc $(\overline{e_1}, \cdots, \overline{e_r})$ est une $A/\mathfrak{p}$-base de $M/\mathfrak{p}M$, ce qui conclut. □

On dispose d'un morphisme :

$$\psi : B \longrightarrow \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_\mathfrak{P}}$$

donné par la réduction modulo $\mathfrak{P}^{e_\mathfrak{P}}$ pour tout $\mathfrak{P}|\mathfrak{p}$. Comme les $\mathfrak{P}|\mathfrak{p}$ sont maximaux, le théorème des restes chinois et le lemme B.6.0.5 assure que ψ est surjective. En outre, on a :

$$\ker(\psi) = \bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$$

Mais on a clairement $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}} \subset \bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$ et réciproquement pour tout $\mathfrak{Q}|\mathfrak{p}$, $\bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}} \subset \mathfrak{Q}^{e_\mathfrak{Q}}$ donc $\mathrm{ord}_\mathfrak{Q}\left(\bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}\right) \geq e_\mathfrak{Q}$, ce qui prouve que $\bigcap_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}} \subset \mathfrak{p}B$, d'après la proposition 2.5.1.5. Ainsi, $\ker(\psi) = \mathfrak{p}B$ et ψ induit un isomorphisme d'anneaux entre $B/\mathfrak{p}B$ et $\prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_\mathfrak{P}}$.

Cet isomorphisme est $A/\mathfrak{p}$-linéaire, donc on obtient en passant aux dimensions :

$$[L:K] = [B/\mathfrak{p}B : A/\mathfrak{p}] = \sum_{\mathfrak{P}|\mathfrak{p}} [B/\mathfrak{P}^{e_\mathfrak{P}} : A/\mathfrak{p}] \quad (\star)$$

Il reste donc à calculer les dimensions $[B/\mathfrak{P}^{e_\mathfrak{P}} : A/\mathfrak{p}]$ pour tout $\mathfrak{P}|\mathfrak{p}$. Fixons $\mathfrak{P}|\mathfrak{p}$. Pour tout $j \in \mathbb{N}^*$, on dispose d'un morphisme surjectif $A/\mathfrak{p}$-linéaire $B/\mathfrak{P}^{j+1} \longmapsto B/\mathfrak{P}^j$ donné par la réduction modulo $\mathfrak{P}^j$ dont le noyau est $\mathfrak{P}^j/\mathfrak{P}^{j+1}$. Il s'ensuit par le théorème du rang que :

$$[B/\mathfrak{P}^{j+1} : A/\mathfrak{p}] = [B/\mathfrak{P}^j : A/\mathfrak{p}] + [\mathfrak{P}^j/\mathfrak{P}^{j+1} : A/\mathfrak{p}] \quad (\star\star)$$

Mais A est un anneau de valuation discrète dont $\mathfrak{p}$ est l'unique idéal maximal et tout idéal premier non-nul de B est donc au-dessus de $\mathfrak{p}$. Comme L/K est séparable, B n'admet donc qu'un nombre fini d'idéaux premiers d'après le corollaire B.7.1.4. Comme B est de Dedekind, le proposition B.6.0.4 assure donc que B est principal. Ainsi, $\mathfrak{P}$ admet un générateur Π. La multiplication par Π^j induit un isomorphisme $A/\mathfrak{p}$-linéaire $B/\mathfrak{P} \longrightarrow \mathfrak{P}^j/\mathfrak{P}^{j+1}$, qui nous donne :

$$[\mathfrak{P}^j/\mathfrak{P}^{j+1} : A/\mathfrak{p}] = [B/\mathfrak{P} : A/\mathfrak{p}] = f_\mathfrak{P}$$

Ainsi, par $(\star\star)$, $[B/\mathfrak{P}^{j+1} : A/\mathfrak{p}] = [B/\mathfrak{P}^j : A/\mathfrak{p}] + f_\mathfrak{P}$. On obtient donc par récurrence que :

$$[B/\mathfrak{P}^{e_\mathfrak{P}} : A/\mathfrak{p}] = e_\mathfrak{P} f_\mathfrak{P}$$

et ce pour tout $\mathfrak{P}|\mathfrak{p}$. Par $(\star)$, on conclut que :

$$[L:K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}$$

□

B.8 Produit tensoriel d'algèbres.

On commence par vérifier qu'un produit tensoriel d'algèbres est une algèbre.

Proposition B.8.0.1. *Soient R un anneau et A et B des R-algèbres. Alors $A \otimes_R B$ peut être munie d'une structure de R-algèbre telle que :*

$$\forall a, a' \in A,\ b, b' \in B, \quad (a \otimes b)(a' \otimes b) = (aa') \otimes (bb')$$

Démonstration. Soient $a \in A$ et $b \in B$. Considérons :

$$\phi_{a,b} : (a', b') \in A \times B \longmapsto (aa') \otimes (bb') \in A \otimes_R B$$

Alors $\phi_{a,b}$ est R-bilinéaire donc par propriété universelle du produit tensoriel elle se factorise en une application R-linéaire $m_{a,b} : A \otimes_R B \longrightarrow A \otimes_R B$ telle que :

$$\forall a' \in A,\ b' \in B, \quad m_{a,b}(a' \otimes b) = \phi_{a,b}(a', b') = (aa') \otimes (bb')$$

Mais $(a, b) \in A \times B \longrightarrow m_{a,b} \in \mathrm{End}_R(A \otimes_R B)$ est R-bilinéaire donc elle se factorise en $M : A \otimes_R B \longrightarrow$

$\mathrm{End}_R(A \otimes_R B)$ telle que :

$$\forall a \in A,\ b \in B, \quad M(a \otimes b) = m_{a,b}$$

On a donc :

$$\forall a, a' \in A,\ b'b \in B, \quad M(a \otimes b)(a' \otimes b') = m_{a,b}(a' \otimes b') = (aa') \times (bb') \quad (\star)$$

Ainsi :

$$(x, y) \in (A \otimes_R B) \times (A \otimes_R B) \longmapsto M(x)(y) \in A \otimes_R B$$

est une l'application R-bilinéaire voulue qui définit bien un produit sur $A \otimes_R B$ par $(\star)$. □

Lemme B.8.0.2. *Soient K un corps, A une K-algèbre et α un élément algébrique sur $K(X_1, \cdots, X_n)$. alors $K[X_1, \cdots, X_n][\alpha] \otimes_K A$ est isomorphe (en tant que K-algèbre) à $A[X_1, \cdots, X_n][\alpha]$.*

Démonstration. Considérons :

$$\phi : (x, \lambda) \in K[X_1, \cdots, X_n][\alpha] \otimes_K A \longmapsto \lambda x \in A[X_1, \cdots, X_n][\alpha]$$

C'est une application K-bilinéaire qui se factorise par propriété universelle du produit tensoriel en une application K-linéaire $\Phi : K[X_1, \cdots, X_n][\alpha] \otimes_K A \longrightarrow A[X_1, \cdots, X_n]$ telle que :

$$\forall (x, \lambda) \in K[X_1, \cdots, X_n][\alpha] \otimes_K A, \quad \Phi(x \otimes \lambda) = \lambda x \quad (\star)$$

Comme ϕ est un morphisme de K-algèbres, il est aisé de vérifié que Φ aussi.

Φ est de plus surjective puisque $\Phi\left(\lambda \otimes X_1^{i_1} \cdots X_n^{i_n} \alpha^i\right) = \lambda X_1^{i_1} \cdots X_n^{i_n} \alpha^i$ pour tous $\lambda \in A$ et $i_1, \cdots, i_n, i \in \mathbb{N}$. En outre, en notant d le degré d'algébricité de α sur $K(X_1, \cdots, X_n)$, si $y \in K[X_1, \cdots, X_n][\alpha] \otimes_K A$, on peut écrire de façon unique :

$$y = \sum_{i=0}^{d-1} \left(\sum_{\substack{(i_1, \cdots, i_n) \in \mathbb{N}^n \\ \sum_{j=1}^n i_j \leq e}} a_{i_1, \cdots, i_n} \otimes X_1^{i_1} \cdots X_n^{i_n} \right) \alpha^i$$

pour un certain $e \in \mathbb{N}$ et des coefficients $a_{\alpha_1, \cdots, \alpha_n} \in K$. Si de plus $\Phi(y) = 0$ alors :

$$\sum_{i=0}^{d-1} \left(\sum_{\substack{(i_1, \cdots, i_n) \in \mathbb{N}^n \\ \sum_{j=1}^n i_j \leq e}} a_{i_1, \cdots, i_n} \otimes X_1^{i_1} \cdots X_n^{i_n} \right) \alpha^i = 0$$

donc par $K(X_1, \cdots, X_n)$-liberté de $(1, \cdots, \alpha^{d-1})$ et K-liberté des monômes de $K[X_1, \cdots, X_n]$, les $a_{\alpha_1, \cdots, \alpha_n}$ sont tous nuls. Ainsi Φ est injective. C'est l'isomorphisme cherché. □

Lemme B.8.0.3. *Soient K un corps algébriquement clos et L/K une extension de corps engendrée par un nombre fini d'éléments sur K ($L = K(y_1, \cdots, y_m)$ pour $y_1, \cdots, y_m \in L$). Alors L est soit une extension algébrique de K, soit une extension finie d'un sous corps $K(x_1, \cdots, x_n)$ avec $x_1, \cdots, x_n \in L$ algébriquement indépendants (de sorte que $K(x_1, \cdots, x_n) \simeq K(X_1, \cdots, X_n)$).*

Démonstration. Soient $y_1, \cdots, y_m \in L$ tels que $L = K(y_1, \cdots, y_m)$. Si tous les y_i sont algébriques sur K, alors L/K est algébrique. Sinon, on considère $(y_i)_{i \in I}$ avec $I \subset \{1, \cdots, m\}$ non vide, une sous-famille de $(y_i)_{1 \leq i \leq m}$ algébriquement indépendante et maximale pour cette propriété. Alors pour tout $i \in \{1, \cdots, m\} \setminus I$, y_i est algébrique sur $K((y_j)_{j \in I})$, par maximalité de I. Ainsi, $L/K((y_j)_{j \in I})$ est une extension algébrique. Ceci conclut. □

Proposition B.8.0.4. *Soient K un corps algébriquement clos de caractéristique nulle, A une K-algèbre intègre et L une extension de K. Alors $L \otimes_K A$ est une L-algèbre intègre.*

Démonstration. Soient $x, y \in L \otimes_K A$ tels que $xy = 0$. Ecrivons $x = \sum_{i=1}^{n} \lambda_i \oplus a_i$ et $y = \sum_{j=1}^{m} \mu_j \oplus b_j$ avec $\lambda_1, \cdots, \lambda_n, \mu_1, \cdots, \mu_m \in L$ et $a_1, \cdots, a_n, b_1, \cdots, b_m \in A$. Alors $E := K(\lambda_1, \cdots, \lambda_n, \mu_1, \cdots, \mu_m)$ est une extension de K engendrée par un nombre fini d'éléments. Donc le lemme B.8.0.3 assure que E/K est algébrique i.e. que $E = K$ car K est algébriquement clos ou que E s'identifie à une extension finie de $K(X_1, \cdots, X_q)$. Dans le premier cas, on peut donc supposer $x, y \in A$, ce qui donne immédiatement $x = 0$ ou $y = 0$ par intégrité de A. Plaçons nous donc dans le deuxième cas. Comme K est de caractéristique nulle, $K(X_1, \cdots, X_q)$ aussi. $E/K(X_1, \cdots, X_q)$ est donc une extension finie de corps parfaits donc une extension séparable (corollaire 5.6.12 de [7]) et le théorème de l'élément primitif (théorèmes 5.4.6 de [7]) assure que $E = K(X_1, \cdots, X_q)[\alpha]$ pour un certain $\alpha \in E$ algébrique.

On peut alors voir x et y comme des éléments de $K(X_1, \cdots, X_q)[\alpha] \otimes_K A$, voire même comme des éléments de $K[X_1, \cdots, X_q][\alpha] \otimes_K A$ en les multipliant par leurs plus petits communs dénominateurs dans $K[X_1, \cdots, X_q]$. Or, le lemme B.8.0.2 assure que $K[X_1, \cdots, X_q][\alpha] \otimes_K A \simeq A[X_1, \cdots, X_q][\alpha]$ et $A[X_1, \cdots, X_q][\alpha]$ est un sous-anneau de $\mathrm{Frac}(A)(X_1, \cdots, X_q)[\alpha]$, qui est un corps. Ainsi, $A[X_1, \cdots, X_q][\alpha]$ est intègre et ceci conclut ($x = 0$ ou $y = 0$). □

Annexe C

Nombres p-adiques (PSC).

La théorie des nombres p-adiques et de ses extensions est assez riche et ne sera donc pas abordée en profondeur car ce n'est pas l'objet de ce rapport. Nous nous intéresserons surtout aux places finies des corps de nombres. Le lecteur intéressé pourra se reporter à [14] pour une présentation détaillée de la théorie.

C.1 Corps valués.

Définition C.1.0.1. *Soit K un corps. On appelle* valeur absolue *ou* norme *sur K une application $|.| : K \longrightarrow \mathbb{R}_+$ telle que pour tous $x, y \in K$:*

(i) $|x| = 0 \Longleftrightarrow x = 0$.

(ii) $|x \cdot y| = |x||y|$.

(iii) $|x + y| \leq |x| + |y|$.

Un tel corps K est alors appelé corps valué. *On dira que $|.|$ est* ultramétrique *ou* non-archimédienne *si de plus la condition suivante, qui implique (iii) est réalisée :*

(iv) $\forall x, y \in K, \quad |x + y| \leq \max(|x|, |y|)$.

Une norme non-ultramétrique sera dite archimédienne.

La valeur absolue donnée par $|x| = 1$ pour tout $x \in K \setminus \{0\}$ et $|0| = 0$ sera appelée valeur absolue triviale.

Définition C.1.0.2. *Soit K un corps. On appelle* valuation *sur K une application $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ telle que pour tous $x, y \in K$:*

(i) $v(x) = \infty \Longleftrightarrow x = 0$.

(ii) $v(x \cdot y) = v(x) + v(y)$.

(iii) $v(x + y) \geq \min(v(y), v(y))$.

(K, v) sera alors appelé corps valué.

$v(K^*)$ est alors un sous-groupe de $(\mathbb{R}, +)$ qui est donc soit monogène, soit dense dans $\mathbb{R}$. Si $v(K^*)$ est monogène on dira que v est discrète. *Si de plus, $v(K^*) = \mathbb{Z}$ on dira que v est* normalisée.

Remarque C.1.0.3. Soit K un corps. Alors il est équivalent de se donner une valuation sur K et une norme ultramétrique. En effet, si v est une valuation sur K, alors pour tout $a > 1$:

$$x \in K \longmapsto a^{-v(x)}$$

définit une norme ultramétrique sur K.

Réciproquement, si $|.|$ est une norme ultramétrique sur K alors pour tout $b > 0$:

$$x \in K \longmapsto -b \log |x|$$

définit une valuation sur K.

Noter que la topologie utlramétrique est assez différente de la topologie archimédienne usuelle, notamment à cause du lemme suivant :

Lemme C.1.0.4. *Soient $x, y \in K$ tels que $v(x) \neq v(y)$. Alors :*

$$v(x+y) = \min(v(x), v(y))$$

Démonstration. Quitte à échanger les rôles de x et de y (parfaitement symétriques), on peut supposer que $v(x) < v(y)$. On a alors :

$$v(x+y) \geq \min(v(x), v(y)) = v(x)$$

Donc $\min(v(y), v(x+y)) \geq v(x)$. Mais :

$$v(x) = v((x+y) - y) \geq \min(v(y), v(x+y))$$

Donc $v(x) = \min(v(y), v(x+y))$. Or, $v(y) > v(x)$ donc nécessairement $v(x) = \min(v(y), v(x+y)) = v(x+y)$. Ainsi, $v(x+y) = v(x) = \min(v(x), v(y))$. □

Exemple C.1.0.5. La valeur absolu usuelle définit une norme archimédienne sur $\mathbb{Q}$. $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour cette norme.

Exemple C.1.0.6. Soit p un nombre premier. Alors la valuation p-adique sur $\mathbb{Q}$ définie sur $\mathbb{Z}$ par :

$$\forall n \in \mathbb{Z}, \quad v_p(n) := \sup\{k \in \mathbb{N} \mid p^k | n\}$$

s'étend à $\mathbb{Q}$ par la formule $v_p\left(\frac{n}{m}\right) = v_p(n) - v_p(m)$ pour tous $n \in \mathbb{Z}$ et $m \in \mathbb{Z} \setminus \{0\}$. C'est une valuation discrète normalisée sur $\mathbb{Q}$ donc on peut définir une norme ultramétrique sur $\mathbb{Q}$ par :

$$\forall r \in \mathbb{Q}, \quad |r|_p := \frac{1}{p^{v_p(r)}}$$

Le corps des nombres p-adiques $\mathbb{Q}_p$ est la complétion de $\mathbb{Q}$ pour la norme $|.|_p$.

Dans la suite, nous nous intéresserons donc naturellement surtout aux corps munis de valuations discrètes.

Proposition C.1.0.7. *Soit (K, v) un corps valué.*

(i) *Alors $A := \{x \in K \mid v(x) \geq 0\}$ est un anneau local d'idéal maximal $\mathfrak{m} := \{x \in K \mid v(x) > 0\}$.*

(ii) *Si de plus v est discrète alors A est un anneau de valuation discrète. Autrement dit, $\mathfrak{m}$ est principal. Tout générateur de $\mathfrak{m}$ sera appelé une* uniformisante.

(iii) *Réciproquement, soient A un anneau de valuation discrète d'idéal maximal $\mathfrak{m} := (t)$ et K son corps de fractions. Alors on définit une valuation discrète normalisée sur K par la formule :*

$$\forall x \in A, \quad v(x) := \sup\{k \in \mathbb{N} \mid x \in \mathfrak{m}^k\} = \sup\{k \in \mathbb{N} \mid t^k | x\}$$

étendue à K via $v\left(\frac{x}{y}\right) := v(x) - v(y)$ pour tous $x \in A$ et $y \in A \setminus \{0\}$.

Démonstration. **(i)** $1, -1 \in A$ car $v(1) = v(1) + v(1)$ donc $v(1) = 0$, puis $0 = v(1) = v(-1) + v(-1)$ donc $v(-1) = 0$. Puis, si $x, y \in A$ alors :

$$v(xy) = v(x) + v(y) \geq 0 \quad \text{et} \quad v(x+y) \geq \min(v(x), v(y)) \geq 0$$

Donc $xy, x+y \in A$. A est donc bien un sous-anneau de K.

Si $x \in \mathfrak{m}$ et $y \in A$ alors $v(xy) = v(x) + v(y) \geq v(x) > 0$ donc $xy \in \mathfrak{m}$ et $\mathfrak{m}$ est bien un idéal de A. De plus, si $x \in \mathfrak{m} \setminus A$ alors $v(x) = 0$ donc $x \neq 0$ puis $v(x^{-1}) = v(1) - v(x) = -v(x) = 0$ donc $x^{-1} \in A$. Ainsi, $A^\times = \mathfrak{m} \setminus A$. Ceci prouve que tout idéal $I \subset A$ contenant strictement $\mathfrak{m}$ contient un inversible donc est A tout entier, donc que $\mathfrak{m}$ est maximal. On obtient en outre que si M est un (autre) idéal maximal de A alors $M \subsetneq A$ donc $M \subset \mathfrak{m}$, puis $M = \mathfrak{m}$ par maximalité. Ainsi, A est un anneau local.

(ii) Si v est discrète on peut supposer v normalisée, quitte à la multiplier par un réel > 0. Soit donc $t \in K$ tel que $v(t) = 1$. Alors $t \in \mathfrak{m}$ et pour tout $x \in \mathfrak{m}$, $v(xt^{-1}) = v(x) - 1 \geq 0$ donc $xt^{-1} \in A$ et $t|x$, ce qui prouve que t engendre $\mathfrak{m}$. A est donc un anneau de valuation discrète.

(iii) est laissée au lecteur. Il suffit de vérifier que l'application définie dans l'énoncé de la proposition est bien une valuation. □

Corollaire C.1.0.8. *Soient (K, v) un corps valué $A := \{x \in K \mid v(x) \geq 0\}$ et $\mathfrak{m} := \{x \in K \mid v(x) > 0\}$. Alors $A/\mathfrak{m}$ est un corps appelé* corps résiduel *de K.*

Proposition C.1.0.9. *Si (K, v) est un corps valué alors l'anneau local A de K est intégralement clos.*

Démonstration. Soit $x \in K$ entier sur A. Alors on peut écrire :

$$x^d + \sum_{i=0}^{d-1} a_i x^i = 0$$

avec $a_0, \cdots, a_{d-1} \in A$. Si par l'absurde $x \notin A$ alors $v(x) < 0$, de sorte que $v(x^d) = dv(x) < v(a_i) + iv(x) = v(a_i x^i)$ pour tout $i \in \{0, \cdots, d-1\}$, puis que :

$$v(0) = v\left(x^d + \sum_{i=0}^{d-1} a_i x^i\right) = \min(v(x^d), v(a_{d-1}x^{d-1}), \cdots, v(a_0)) = dv(x)$$

d'après le lemme C.1.0.4. C'est absurde ! Donc $v(x) \geq 0$ et $x \in A$. □

C.2 Places finies sur un corps de nombre.

Dans ce paragraphe, on fixe K un corps de nombre et $\mathcal{O}_K$ son anneau d'entiers. Comme $\mathcal{O}_K$ est la clôture intégrale de $\mathbb{Z}$ dans K, que $\mathbb{Z}$ est de Dedekind et que $K/\mathbb{Q}$ est finie et séparable, la proposition B.5.0.3 assure que $\mathcal{O}_K$ est de Dedekind.

Soit p un nombre premier. Alors tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_K$ au-dessus de p est en fait maximal. $(\mathcal{O}_K)_\mathfrak{P}$, le localisé de $\mathcal{O}_K$ en $\mathfrak{P}$ est donc un anneau de valuation discrète dont K est le corps de fractions (proposition B.6.0.2). Ainsi, on peut définir sur K une valuation $v_\mathfrak{P}$ selon la méthode du point *(iii)* de la proposition C.1.0.7. Elle est appelée *valuation $\mathfrak{P}$-adique*. Puisque $(\mathcal{O}_K)_\mathfrak{P}$ est un anneau local, pour cette valuation, l'idéal maximal est nécessairement :

$$\mathfrak{m}_\mathfrak{P} := (\mathcal{O}_K \setminus \mathfrak{P})^{-1}\mathfrak{P}$$

et le corps résiduel vaut $k := (\mathcal{O}_K)_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}$.

On peut définir une norme $|.|_\mathfrak{P}$ à partir de $v_\mathfrak{P}$ en posant :

$$\forall x \in K, \quad |x|_\mathfrak{P} := a^{-v_\mathfrak{P}(x)}$$

pour un certain réel $a > 1$. Par convention, la constante a définissant $|.|_{\mathfrak{P}}$ est choisie de telle sorte que :

$$|p|_{\mathfrak{P}} := \frac{1}{p}$$

Par multiplicativité, on obtient alors que $|.|_{\mathfrak{P}}$ prolonge la norme p-adique sur $\mathbb{Q}$, ce qui rend cette normalisation assez intéressante. De plus, cette normalisation est compatible aux extensions de corps

Lemme C.2.0.1. *Si L/K est une extension finie et si $\mathfrak{Q}$ est un idéal premier de $\mathcal{O}_L$ au-dessus de $\mathfrak{P}$. Alors $|.|_{\mathfrak{P}}$ et $|.|_{\mathfrak{Q}}$ coïncident sur K.*

Démonstration. Il suffit de vérifier la coïncidence sur des uniformisantes. Soient s et t respectivement des uniformisantes en $\mathfrak{P}$ et $\mathfrak{Q}$. Alors par factorisation dans un anneau de Dedekind :

$$p\mathcal{O}_K = \prod_{\mathfrak{P}'|p} \mathfrak{P}'^{e(\mathfrak{P}'/p)} \quad \text{et} \quad p\mathcal{O}_L = \prod_{\mathfrak{Q}'|p} \mathfrak{Q}'^{e(\mathfrak{Q}'/p)}$$

On a par définition :

$$v_{\mathfrak{P}}(p) = e(\mathfrak{P}/p) \quad \text{et} \quad v_{\mathfrak{Q}}(p) = e(\mathfrak{Q}/p)$$

D'où :

$$|s|_{\mathfrak{P}} = \frac{1}{p^{1/e(\mathfrak{P}/p)}} \quad \text{et} \quad |t|_{\mathfrak{Q}} = \frac{1}{p^{1/e(\mathfrak{Q}/p)}}$$

Mais $\mathfrak{P} = \prod_{\mathfrak{Q}'|p} \mathfrak{Q}'^{e(\mathfrak{Q}'/\mathfrak{P})}$ donc :

$$s\mathfrak{O}_L = \mathfrak{m}_{\mathfrak{P}} = \prod_{\mathfrak{Q}'|p} \mathfrak{Q}'^{e(\mathfrak{Q}'/\mathfrak{P})}_{\mathfrak{P}}$$

De sorte que :

$$v_{\mathfrak{Q}}(s) = e(\mathfrak{Q}/\mathfrak{P})$$

Puis que, par multiplicativité des indices de ramification (proposition B.7.2.4) :

$$|s|_{\mathfrak{Q}} = |t|_{\mathfrak{Q}}^{e(\mathfrak{Q}/\mathfrak{P})} = |t|_{\mathfrak{Q}} = \frac{1}{p^{e(\mathfrak{Q}/\mathfrak{P})/e(\mathfrak{Q}/p)}} = \frac{1}{p^{1/e(\mathfrak{P}/p)}} = |s|_{\mathfrak{P}}$$

□

Remarque C.2.0.2. On se donne un idéal maximal $\mathfrak{P}$ de $\overline{\mathbb{Z}}$ contenant p (qui existe d'après le lemme de Zorn). Pour tout corps de nombres K, $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$ au-dessus de p qui induit donc une norme ultramétrique $|.|_{\mathfrak{p}}$ sur K. Ainsi, avec la normalisation vue précédemment, on a défini une norme ultramétrique sur tout corps de nombre compatible aux extensions finies donc une norme ultramétrique sur $\overline{\mathbb{Q}}$ qui ne dépend que de la donnée de $\mathfrak{P}$.

Réciproquement, si $|.|$ est une norme ultramétrique sur K prolongeant $|.|_p$, on peut montrer que $|.|$ est une norme $\mathfrak{P}$-adique pour un certain idéal premier $\mathfrak{P}$ de $\mathcal{O}_K$ au-dessus de p. Ce résultat ne nous étant pas absolument nécessaire, nous ne le démontrerons pas. Cependant, il nous donne une équivalence très instructive entre idéeaux premiers au-dessus de p et normes prolongeant la norme p-adique qui justifie la terminologie adoptée.

Définition C.2.0.3. *On appellera* place au-dessus de p *indistinctement un idéal $\mathfrak{P}$ au-dessus de p de $\mathcal{O}_K$ et une norme prolongeant la norme p-adique.*

Remarque C.2.0.4. Usuellement dans la littérature, une place est une classe d'équivalence topologique de normes sur un corps. La définition ci-dessus, très peu générale, conserve cependant l'idée de ce qu'est une place.

Voyons maintenant un résultat sur le corps résiduel modulo les places finies.

Théorème C.2.0.5. **(i)** *Soient K un corps et $\mathfrak{P}$ une place finie de $\mathcal{O}_K$ au-dessus de p. Alors le corps résiduel de $(K, |.|_{\mathfrak{P}})$ est :*

$$k = (\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}} \simeq \mathcal{O}_K/\mathfrak{P}$$

avec $\mathfrak{m}_{\mathfrak{P}} := (\mathcal{O}_K \setminus \mathfrak{P})^{-1}\mathfrak{P}$. C'est un corps fini de caractéristique p.

(ii) *Si q est une puissance de p alors $\mathbb{F}_q$ est le corps résiduel d'un certain corps de nombre K muni d'une place finie $\mathfrak{P}$ au-dessus de p dont p est une uniformisante dans $(K, |.|_{\mathfrak{P}})$. $\mathfrak{P}$ est alors la seule place finie de K au-dessus de p. Un tel corps de nombres est dit* non ramifié au dessus de p.

Démonstration. **(i)** On sait par définition que le corps résiduel vaut $k = (\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}$. Il s'agit donc de montrer que $(\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}} \simeq \mathcal{O}_K/\mathfrak{P}$. On peut déjà remarquer que $\mathcal{O}_K/\mathfrak{P}$ se plonge dans $(\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}$. En effet, la réduction modulo $\mathfrak{m}_{\mathfrak{P}}$ donne un morphisme d'anneaux naturels :

$$\mathcal{O}_K \longrightarrow (\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}$$

dont le noyau est $\mathfrak{P} \subset \mathfrak{m}_{\mathfrak{P}}$. En effet, si $x \in \mathcal{O}_K$ est congru à 0 modulo $\mathfrak{m}_{\mathfrak{P}}$ alors $x \in \mathfrak{m}_{\mathfrak{P}} = (\mathcal{O}_K \setminus \mathfrak{P})^{-1}\mathfrak{P}$ donc $x = \frac{y}{s}$ avec $y \in \mathfrak{P}$ et $s \in \mathcal{O}_K \setminus \mathfrak{P}$ donc $xs = y \in \mathfrak{P}$. Or, $\mathfrak{P}$ est premier et $s \notin \mathfrak{P}$ donc $x \in \mathfrak{P}$. On a donc un morphisme injectif d'anneaux :

$$\mathcal{O}_K/\mathfrak{P} \longrightarrow (\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}$$

qui donne notre plongement. C'est même un morphisme de corps car $\mathfrak{P}$ est maximal.

Réciproquement, soit $\pi : (\mathcal{O}_K)_{\mathfrak{P}} \longrightarrow k$ la projection canonique. Alors il est immédiat que $\pi(\mathcal{O}_K) = \mathcal{O}_K/\mathfrak{P}$ (via l'identification de $\mathcal{O}_K/\mathfrak{P}$ à un sous-corps de k avec le plongement précédent). Il s'agit donc de montrer que $\pi(\mathcal{O}_K) = k$. Soit $x \in (\mathcal{O}_K)_{\mathfrak{P}}$. Alors $x = \frac{y}{s}$ avec $y \in \mathcal{O}_K$ et $s \in \mathcal{O}_K \setminus \mathfrak{P}$. Comme $s \notin \mathfrak{P}$, $\pi(s) \neq 0$ donc $\pi(s)$ est inversible dans $\mathcal{O}_K/\mathfrak{P}$. Soit $z \in \pi^{-1}(\pi(s)^{-1})$. Alors $\pi(yz - x) = \pi(y)\pi(s)^{-1} - \pi(y)\pi(s)^{-1} = 0$ de sorte que $\pi(x) = \pi(yz) \in \pi(\mathcal{O}_K)$. Ainsi :

$$k = (\mathcal{O}_K)_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}} \simeq \mathcal{O}_K/\mathfrak{P}$$

Comme $p \in \mathfrak{P}$, p est nul dans le corps $k \simeq \mathcal{O}_K/\mathfrak{P}$ et donc c'est la caractéristique de k. En outre, $\mathfrak{P}$ est d'indice fini dans $\mathcal{O}_K$ (voir [10] p. 96 pour une preuve). Donc k est un corps fini.

(ii) $\mathbb{F}_q/\mathbb{F}_p$ est finie et séparable comme extension de corps parfaits. Ainsi, le théorème de l'élément primitif assure que $\mathbb{F}_q = \mathbb{F}_p[\overline{\alpha}]$ pour $\overline{\alpha} \in \mathbb{F}_q$ de degré $d := [\mathbb{F}_q : \mathbb{F}_p]$ sur $\mathbb{F}_p$. Soient $\overline{\Pi}$ le polynôme minimal de $\overline{\alpha}$ sur $\mathbb{F}_p$ et $\Pi \in \mathbb{Z}[X]$ un polynôme unitaire de degré d tel que $\Pi \equiv \overline{\Pi}\ [p]$. Soit $\alpha \in \overline{\mathbb{Q}}$ une racine de Π. Alors Π est irréductible dans $\mathbb{Z}[X]$ puisque $\overline{\Pi}$ est irréductible dans $\mathbb{F}_p[X]$. Ainsi, Π est irréductible sur $\mathbb{Q}[X]$ car unitaire (d'après la théorie des contenus). Π est donc le polynôme minimal de α sur $\mathbb{Q}$, qui est donc de degré d sur $\mathbb{Q}$.

Considérons $K := \mathbb{Q}(\alpha)$ et $\mathfrak{P}$ une place finie de K au-dessus de p. Posons $A := \mathbb{Z}[\alpha] \subset \mathcal{O}_K$ et $\mathfrak{p} := A \cap \mathfrak{P}$. Alors A est un ordre de $\mathcal{O}_K$ et $\mathfrak{p}$ est maximal dans A d'après la proposition B.7.1.2 donc $A/\mathfrak{p}$ est un corps qui se plonge dans le corps résiduel de K : $\mathcal{O}_K/\mathfrak{P}$, d'après des manipulations élémentaires analogues à celles du point précédent. Or, $\overline{\Pi}$ est irréductible dans $\mathbb{F}_p[X]$ et $\mathfrak{p}$ contient p donc $A/\mathfrak{p}$ un corps fini de cardinal $p^d = q$ d'après la proposition 6.10 de [10]. On en déduit que $f(\mathfrak{P}/p\mathbb{Z}) \geq d = [K : \mathbb{Q}]$. On conclut par le théorème B.7.2.5 :

$$d = [K : \mathbb{Q}] = \sum_{\mathfrak{P}'|p} e(\mathfrak{P}'/p\mathbb{Z}) f(\mathfrak{P}'/p\mathbb{Z})$$

que $f(\mathfrak{P}/p\mathbb{Z}) = d$ donc que $k = \mathfrak{P}/p\mathbb{Z} = \mathbb{F}_q$ et que $e(\mathfrak{P}/p\mathbb{Z}) = 1$ donc que p est de valuation 1 donc une uniformisante. De plus, $\mathfrak{P}$ est clairement le seul idéal premier de $\mathcal{O}_K$ au-dessus de p d'après la formule du théorème B.7.2.5.

□

Remarque C.2.0.6. Soit $\mathfrak{P}$ un idéal maximal de $\overline{\mathbb{Z}}$ au-dessus de p. On a vu à la remarque C.2.0.2 que $\mathfrak{P}$ induit une place finie sur tout corps de nombres. Comme $\overline{\mathbb{Q}}$ est l'union de tous les corps de nombres, le corps résiduel de $\overline{\mathbb{Q}}$ est l'union de tous les corps finis de caractéristique p d'après le théorème précédent donc c'est $\overline{\mathbb{F}_p}$.

C.3 Complétion.

Dans ce paragraphe, on fixe $(K, |.|)$ un corps normé, que l'on cherche à compléter. On note $\mathcal{C}(K)$ l'ensemble des suites de Cauchy à valeurs dans K et $0(K)$, l'ensemble des suites de K qui convergent vers 0 (on remarque immédiatement que $0(K) \subset \mathcal{C}(K)$).

On commence par prouver quelques résultats intermédiaires :

Lemme C.3.0.1 (convergence des suites de $\mathcal{C}(K)$). **(i).** *Si $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$ alors $(|a_n|)_{n\in\mathbb{N}}$ converge dans $\mathbb{R}$.*

(ii). *Si $|.|$ est ultramétrique alors toute suite de $\mathcal{C}(K) \setminus 0(K)$ est de norme constante à partir d'un certain rang.*

(iii). *Si $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$ et si $(a_n - b_n)_{n\in\mathbb{N}} \in 0(K)$ alors $\lim\limits_{n\to+\infty} |a_n| = \lim\limits_{n\to+\infty} |b_n|$.*

Démonstration. **(i).** Remarquons que par inégalité triangulaire on a $||a_n| - |a_m|| \leq |a_n - a_m|$ pour tous $n, m \in \mathbb{N}$, ce qui donne immédiatement que $(|a_n|)_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{R}$ donc convergente.

(ii). Soit $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)\setminus 0(K)$. On sait alors par le point précédent que $(|a_n|)_{n\in\mathbb{N}}$ converge vers $\ell > 0$. On dispose donc de $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0$, $|a_n| \geq \frac{\ell}{2}$. Et comme $(a_n)_{n\in\mathbb{N}}$ est de Cauchy, on dispose de $N_1 \in \mathbb{N}$ tel que pour tous $m \geq n \geq N_1$, $|a_n - a_m| \leq \frac{\ell}{4}$. Mais alors en posant $N := \max(N_0, N_1)$, on obtient que pour tout $n \geq N$, $|a_N - a_n| < \min(|a_n|, |a_N|)$ et donc que $|a_n| = |a_N|$ (sinon, $|.|$ étant ultramétrique, on aurait d'après le lemme C.1.0.4 $|a_N - a_n| = \max(|a_n|, |a_N|) \geq \min(|a_n|, |a_N|)$).

(iii). Les limites $\lim\limits_{n\to+\infty} |a_n|$ et $\lim\limits_{n\to+\infty} |b_n|$ existent par le point (i). et sont égales car $||a_n| - |b_n|| \leq |a_n - b_n|$ pour tout $n \in \mathbb{N}$ et que $|a_n - b_n| \underset{n\to+\infty}{\longrightarrow} 0$.

□

Proposition C.3.0.2. *$\mathcal{C}(K)$ est un anneau commutatif pour les lois $+$ et $\times$ dérivées de K et $0(K)$ en est un idéal maximal.*

Démonstration. Le fait que les lois $+$ et $\times$ respectent les axiomes d'un anneau commutatif (associativité, commutativité, distributivité, éléments neutres) est clair. La difficulté consiste à montrer que ces lois sont bien des lois de composition internes. Il est immédiat qu'une somme de suites de Cauchy est de Cauchy. En revanche, pour le produit de deux suites de Cauchy $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, il suffit de remarquer que pour tous $n, m \in \mathbb{N}$:

$$|a_n b_n - a_m b_m| = |a_n(b_n - b_m) - (a_m - a_n)b_m| \leq |a_n||b_n - b_m| + |a_m - a_n||b_m|$$

Ce qui permet de conclure que $(a_n b_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$ car une suite de Cauchy est toujours bornée (ce qui s'obtient comme conséquence du point (i). du lemme précédent). Donc $\mathcal{C}(K)$ est un anneau commutatif.

$0(K)$ contient la suite nulle (neutre additif), est stable par somme et par produit par tout élément de $\mathcal{C}(K)$ car le produit d'une suite bornée par une suite convergente vers 0 converge vers 0. Ainsi, $0(K)$ en est un idéal de $\mathcal{C}(K)$.

Montrons enfin que $0(K)$ est maximal. Soient $\overline{a} \in \mathcal{C}(K)/0(K) \setminus 0$ et $a := (a_n)_{n\in\mathbb{N}} \in \mathcal{C}(K) \setminus 0(K)$ un représentant de $\overline{a}$. Alors d'après le point (i). du lemme précédent, $(|a_n|)_{n\in\mathbb{N}}$ converge vers $\ell > 0$ donc on

dispose de $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|a_n| \geq \frac{\ell}{2}$. On pose alors pour tout $n \in \mathbb{N}$:

$$b_n := \begin{cases} 0 & \text{si } n < N \\ \frac{1}{a_n} & \text{si } n \geq N \end{cases}$$

On a alors pour tous $n, m \geq N$:

$$|b_n - b_m| = \frac{|a_m - a_n|}{|a_n a_m|} \leq \frac{4|a_m - a_n|}{\ell^2}$$

et il est alors clair que $(b_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$. En outre, pour tout $n \geq N$, $a_n b_n - 1 = 0$ donc $(a_n b_n - 1)_{n\in\mathbb{N}} \in 0(K)$, et donc $\overline{a}\overline{b} = \overline{1}$ dans $\mathcal{C}(K)/0(K)$, ce qui prouve que $\overline{a}$ est inversible. Donc $\mathcal{C}(K)/0(K)$ est bien un corps et $0(K)$ un idéal maximal de $\mathcal{C}(K)$. □

Nous venons donc de montrer que $\widehat{K} := \mathcal{C}(K)/0(K)$ est un corps et que la norme $|.|$ de K peut s'étendre à $\widehat{K}$ tout entier d'après le point (iii). du lemme C.3.0.1, en posant pour tout $\overline{a} \in \widehat{K}$, $|\overline{a}| = \lim\limits_{n\to+\infty} |a_n|$ pour un représentant $(a_n)_{n\in\mathbb{N}}$ quelconque de $\overline{a}$ (dont la valeur de $|\overline{a}|$ ne dépend pas).

Ceci définit bien une norme car l'inégalité triangulaire et la multiplicativité passent à la limite. En outre, si $\overline{a} \in \widehat{K}$ est de norme nulle alors $\overline{a}$ admet un représentant $(a_n)_{n\in\mathbb{N}}$ tel que $\lim\limits_{n\to+\infty} |a_n| = 0$. On a alors $a_n \underset{n\to+\infty}{\longrightarrow} 0$ i.e. $a \in 0(K)$ i.e. $\overline{a} = \overline{0}$.

On peut enfin remarquer en passant à la limite que le caractère ultramétrique est conservé. On a en fait des résultats topologiques encore meilleurs.

Théorème C.3.0.3. *$(\widehat{K}, |.|)$ est un surcorps normé complet de K et K est dense dans $\widehat{K}$. Si $(L, |.|_1)$ est un (autre) surcorps normé complet de K dont la norme prolonge celle de K et tel que K est dense dans L, alors il existe un isomorphisme de corps isométrique $\widehat{K} \longrightarrow L$. Pour cette raison, $\widehat{K}$ est appelé "le"* complété de K *ou "la"* complétion de K.

Démonstration. Par abus, on peut considérer $\widehat{K}$ comme un surcorps de K en l'identifiant avec les classes d'équivalence des suites constantes.

On commence par montrer que K est dense dans $\widehat{K}$. Soient $\overline{a}$ un élément de $\hat{K}$ et $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(K)$ un représentant de $\overline{a}$. Alors pour tout $n \in \mathbb{N}$:

$$|\overline{a} - a_n| = \lim_{m\to+\infty} |a_m - a_n| \leq \sup_{m\geq n} |a_m - a_n|$$

Et $\sup\limits_{m\geq n} |a_m - a_n| \underset{n\to+\infty}{\longrightarrow} 0$ car $(a_n)_{n\in\mathbb{N}}$ est de Cauchy, de sorte que $a_n \underset{n\to+\infty}{\longrightarrow} \overline{a}$ dans $\widehat{K}$. D'où la densité de K dans $\widehat{K}$.

Ce raisonnement permet aussi de montrer que toute suite de Cauchy de K converge dans $\widehat{K}$ car si $(a_n)_{n\in\mathbb{N}}$ en est une, alors on a vu qu'elle convergeait vers sa réduction modulo $0(K)$, $\overline{a}$, dans $\widehat{K}$.

On en déduit finalement que $\widehat{K}$ est complet. En effet, si $(\overline{a}_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\widehat{K}$ alors par densité de K dans $\widehat{K}$, on dispose pour tout $n \in \mathbb{N}$ de $b_n \in \mathbb{K}$ tel que $|\overline{a}_n - b_n| \leq 2^{-n}$. On obtient alors que $(b_n)_{n\in\mathbb{N}}$ est de Cauchy dans K car si $\varepsilon > 0$ alors on dispose de $N \in \mathbb{N}$ tel que pour tous $m \geq n \geq N$:

$$|\overline{a}_n - \overline{a}_m| \leq \frac{\varepsilon}{2}$$

Et donc pour tous $m \geq n \geq \max\left(N, \left\lceil \frac{\ln\left(\frac{4}{\varepsilon}\right)}{\ln(2)} \right\rceil\right)$:

$$|b_n - b_m| \leq |b_n - \overline{a}_n| + |\overline{a}_n - \overline{a}_m| + |\overline{a}_m - b_m| \leq \frac{\varepsilon}{2} + 2^{-n} + 2^{-m} \leq \varepsilon$$

Donc $(b_n)_{n\in\mathbb{N}}$ converge vers $\overline{b}$ dans $\widehat{K}$ et $(\overline{a}_n)_{n\in\mathbb{N}}$ aussi puisque $|\overline{a}_n - b_n| \underset{n\to+\infty}{\longrightarrow} 0$. D'où la complétude de $\widehat{K}$.

Soit $(L, |.|_1)$ un (autre) surcorps normé complet de K dont la norme prolonge celle de K et tel que K est dense dans L. Soit $\varphi : \mathcal{C}(K) \longrightarrow L$ donné par :

$$\forall (a_n)_{n\in\mathbb{N}} \in \mathcal{C}(K), \quad \varphi((a_n)_{n\in\mathbb{N}}) := \lim_{n\to+\infty} a_n \in L$$

Alors φ est un morphisme d'anneaux une surjection de $\mathcal{C}(K)$ dans L par densité de K dans L et son noyau est exactement l'idéal $0(K)$. Donc φ induit un isomorphisme de corps $\widehat{K} = \mathcal{C}(K)/0(K) \longrightarrow L$. Cet isomorphisme est isométrique car :

$$\forall a := (a_n)_{n\in\mathbb{N}} \in \mathcal{C}(K), \quad |\varphi(a)|_1 := |\lim_{n\to+\infty} a_n|_1 = \lim_{n\to+\infty} |a_n|_1 = \lim_{n\to+\infty} |a_n| = |\overline{a}|$$

□

Remarque C.3.0.4. Dans le cas où la norme $|.|$ est ultramétrique, on peut lui associer une valuation v. Nous avons travaillé ici dans le but d'obtenir des corps valués complets.

Dans le cas où v est discrète on dispose de $a > 0$ tel que $v(K^*) = a\mathbb{Z}$. Ainsi, $v(K^*)$ est fermé et $v(\widehat{K}^*)$ qui n'est, par construction, rien d'autre que l'adhérence de $v(K^*)$ est égal à $v(K^*)$. Donc le prolongement de la valuation K à $\widehat{K}$ reste discret. On obtient même que la complétion préserve les uniformisantes.

C.4 Lemme de Hensel.

Théorème C.4.0.1 (Lemme de Hensel)**.** *Soient (K, v) un corps valué complet de corps résiduel k, $A := \{x \in K \mid v(x) \geq 0\}$ son anneau local, $\mathfrak{m} := \{x \in K \mid v(x) > 0\}$ son idéal maximal et $P \in A[X]$. Supposons que la réduction modulo $\mathfrak{m}$ de P notée $\overline{P} \in k[X]$ admette une racine simple $\overline{a} \in k$ ($\overline{P}'(\overline{a}) \neq 0$). Alors il existe un unique $a \in A$ se réduisant sur $\overline{a}$ modulo $\mathfrak{m}$ tel que $P(a) = 0$.*

Démonstration. **Existence :** L'ingrédient essentiel de la preuve est l'approximation des zéros des fonctions par la méthode de Newton. Soit $a_0 \in A$ quelconque tel que $\overline{a_0} = \overline{a}$. Montrons que l'on peut alors construire une suite récurrente $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$:

$$v(P(a_n)) \geq 2^n v(P(a_0)) \quad \text{et} \quad v(P'(a_n)) = 0$$

Soit $n \in \mathbb{N}$. Supposons construits $a_0, \cdots, a_n \in A$. Appliquons la formule de Taylor polynomiale :

$$P(X + a_n) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a_n)}{k!} X^k$$

avec pour tout $k \in \mathbb{N}$, $v\left(\frac{P^{(k)}(a_n)}{k!}\right) \geq 0$ car $P(X + a_n) \in A[X]$ vu que $P \in A[X]$ et $a_n \in A$. Ainsi, en évaluant cette équation en $X := -\frac{P(a_n)}{P'(a_n)}$, on trouve :

$$P\left(a_n - \frac{P(a_n)}{P'(a_n)}\right) = \sum_{k\geq 2}^{+\infty} \frac{P^{(k)}(a_n)}{k!} \left(-\frac{P(a_n)}{P'(a_n)}\right)^k$$

avec $v\left(-\frac{P(a_n)}{P'(a_n)}\right) = 2^n v(P(a_0)) > 0$ par hypothèse et donc par inégalité ultramétrique :

$$v\left(P\left(a_n - \frac{P(a_n)}{P'(a_n)}\right)\right) \geq v\left(\frac{P''(a_n)}{2}\left(-\frac{P(a_n)}{P'(a_n)}\right)^2\right) \geq 2^{n+1} v(P(a_0))$$

Puis, toujours avec la formule de Taylor :

$$P'\left(a_n - \frac{P(a_n)}{P'(a_n)}\right) = \sum_{k=0}^{+\infty} \frac{P^{(k+1)}(a_n)}{k!} (-\frac{P(a_n)}{P'(a_n)})^k$$

avec pour tout $k \in \mathbb{N}^*$:

$$v\left(\frac{P^{(k+1)}(a_n)}{k!}\left(-\frac{P(a_n)}{P'(a_n)})^k\right)\right) \geq kv\left(-\frac{P(a_n)}{P'(a_n)}\right) > 0$$

Donc d'après le lemme C.1.0.4 :

$$v\left(P'\left(a_n - \frac{P(a_n)}{P'(a_n)}\right)\right) = v(P'(a_n)) = 0$$

Posons donc :

$$a_{n+1} := a_n - \frac{P(a_n)}{P'(a_n)}$$

qui convient. D'où la construction.

Pour tous $n \leq m \in \mathbb{N}$, on a par le lemme C.1.0.4 :

$$v(a_m - a_n) = v\left(\sum_{k=n}^{m-1}(a_{k+1} - a_k)\right) = v\left(\sum_{k=n}^{m-1} -\frac{P(a_k)}{P'(a_k)}\right) = v\left(-\frac{P(a_k)}{P'(a_k)}\right) \geq 2^n v(P(a_0)) \underset{n\to+\infty}{\longrightarrow} +\infty$$

Donc $(a_n)_{n\in\mathbb{N}}$ est de Cauchy dans K qui est complet donc c'est une suite convergente. Posons $a := \lim_{n\to+\infty} a_n$. Alors comme $P(a_n) \underset{n\to+\infty}{\longrightarrow} 0$, on conclut avec le lemme suivant que $P(a) = 0$.

Lemme C.4.0.2. *Les fonctions polynomiales sont continues pour la topologie induite sur K par v.*

Démonstration. Il suffit de prouver ce résultat pour les monômes. Le résultat général s'obtient par linéarité et inégalité ultramétrique. Soient $n \in \mathbb{N}^*$ et $a, h \in K$. Alors :

$$v((a+h)^n - a^n) = v\left(h\sum_{k=0}^{n-1} a^k h^{n-1-k}\right) \geq v(h) + \min_{0\leq k\leq n-1}(kv(a) + (n-1-k)v(h)) = v(h) + (n-1)\min(v(a), v(h))$$

La continuité de $x \longmapsto x^n$ s'en déduit immédiatement. □

Unicité : Soit $b \in A$ une (autre) racine de P telle que $\overline{b} = \overline{a}$. Posons $h := b - a$. Alors $v(h) > 0$ et d'après la formule de Taylor :

$$0 = P(a+h) = P(a) + \sum_{k=1}^{+\infty}\frac{P^{(k)}(a)}{k!}h^k = \sum_{k=1}^{+\infty}\frac{P^{(k)}(a)}{k!}h^k$$

Comme $\overline{P}'(\overline{a}) \neq 0$, $v(P'(a)) = 0$ et donc :

$$v(h) = v(P'(a)h) = v\left(-\sum_{k=1}^{+\infty}\frac{P^{(k)}(a)}{k!}h^k\right) \geq v\left(-\frac{P''(a)}{2}h^2\right) \geq 2v(h)$$

Comme $v(h) > 0$, ceci implique que $v(h) = +\infty$ donc que $h = 0$ et $a = b$. □

Annexe D

L'espace tangent à une variété algébrique affine.

Dans cette section, on fixe K un corps algébriquement clos et V une variété algébrique affine irréductible d'idéal annulateur premier $I \subset K[X_1, \cdots, X_r]$. On se donne $F_1, \cdots, F_s \in K[X_1, \cdots, X_r]$ des générateurs de I, de sorte que :

$$V = \{(x_1, \cdots, x_r) \in K^r \mid \forall 1 \leq i \leq s, \quad F_i(x_1, \cdots, x_r) = 0\}$$

Définir l'espace tangent à V en $P := (x_1, \cdots, x_r) \in V$, c'est développer les équations $F_i(P) = 0$ qui définissent V "au premier ordre". Formellement, on regarde les équations $F_i(P + \varepsilon Q) = 0$ avec ε "très petit" et $Q := (y_1, \cdots, y_r) \in K^r$ un "vecteur tangent", on obtient :

$$\forall 1 \leq i \leq s, \quad F_i(P + \varepsilon Q) = F_i(P) + \varepsilon \sum_{j=1}^{r} y_j \frac{\partial F_i}{\partial X_j}(P) + O(\varepsilon^2) = 0$$

avec les équations $F_i(P) = 0$ et en négligeant les termes d'ordre 2, on obtient :

$$\forall 1 \leq i \leq s, \quad \sum_{j=1}^{r} y_j \frac{\partial F_i}{\partial X_j}(P) = 0$$

Donc $Q \in \ker dF_P$ si l'on note $F := (F_1, \cdots, F_s)$. C'est l'équation usuelle de la tangente.

On ne peut cependant définir la tangente directement ainsi puisque la "petitesse" de ε n'a a priori pas de sens dans le corps K (qui n'a même pas de topologie en général). On peut résoudre ce problème assez simplement en remplaçant lors du développement K par $K[X]/(X^2) = K[\varepsilon]$ (avec $\varepsilon = \overline{X}$ vérifiant $\varepsilon^2 = 0$), ce qui revient à travailler au premier ordre car tous les termes en ε^2 s'éliminent. Nous verrons ainsi une définition alternative de la tangente, tout à fait analogue à la précédente, mais conceptuellement plus facile à manipuler.

Définition D.0.0.1. *Soit $P \in V$. On appelle* vecteur tangent *à V en P toute forme K-linéaire $v : K[V]_P \longrightarrow K$ ($K[V]_P$ étant l'anneau local de $K[V]$ en P) qui est une* dérivation en P, *c'est à dire que :*

$$\forall f, g \in K[V]_P, \quad v(fg) = f(P)v(g) + g(P)v(f)$$

La tangente à V en P *est l'espace des vecteurs tangents à V en P. On la note $T_P(V)$.*

Définition D.0.0.2. *Soient $P \in V$, $p : K[\varepsilon] \longrightarrow K$ la projection canonique donnée par :*

$$\forall \lambda, \mu \in K, \quad p(\lambda + \varepsilon\mu) = \lambda$$

Pour rappel, $\varepsilon^2 = 0$. On appelle déformation de V en P *un morphisme de K-algèbre $\varphi : K[V]_P \longrightarrow K[\varepsilon]$ telle que $p \circ \varphi = ev_P$ où ev_P est le morphisme d'évaluation en P :*

$$\forall P \in K[V]_P, \quad ev_P(f) = f(P)$$

On note Def(V, P) l'ensemble des déformations de V en P.

Remarque D.0.0.3. Les déformations sont les analogues algébriques des fonctions $\varepsilon \longmapsto P + \varepsilon Q$ définies au voisinage de 0 introduites précédemment. Elles portent donc bien leur nom, puisqu'elles mesurent la "déformation" de la courbe au voisinage de P (via le paramètre Q). La proposition qui suit n'a donc rien d'étonnant.

Proposition D.0.0.4. *Soit $P \in V$. Alors l'application :*

$$\begin{array}{ccc} T_P(V) & \longrightarrow & Def(V, P) \\ v & \longmapsto & v^* := ev_P + \varepsilon v \end{array}$$

est une bijection.

Démonstration. On commence par vérifier la bonne définition de cette application. Il s'agit de vérifier que si $v \in T_P(V)$ est un vecteur tangent à V en P alors $v^* = \mathrm{ev}_P + \varepsilon v$ est un morphisme de K-algèbres. Cette application est clairement K-linéaire car v et ev_P le sont. En outre, si $f, g \in K[V]_P$ alors :

$$\begin{aligned} v^*(f)v^*(g) &= (f(P) + \varepsilon v(f))(g(P) + \varepsilon v(g)) = f(P)g(P) + (f(P)v(g) + g(P)v(f))\varepsilon + v(f)v(g)\varepsilon^2 \\ &= f(P)g(P) + (f(P)v(g) + g(P)v(f))\varepsilon = f(P)g(P) + v(fg)\varepsilon = v^*(fg) \end{aligned}$$

Donc v^* est bien un morphisme de K-algèbres et ainsi $v^* \in \mathrm{Def}(V, P)$.

L'injectivité de l'application en question est claire. Il s'agit donc de vérifier sa surjectivité. Soient $\varphi \in \mathrm{Def}(V, P)$, $q : K[V]_P \longrightarrow K[\varepsilon]$ la projection canonique telle que :

$$\forall \lambda, \mu \in K, \quad p(\lambda + \varepsilon\mu) = \mu$$

et $f, g \in K[V]_P$. Alors :

$$\begin{aligned} f(P)g(P) + q \circ \varphi(fg)\varepsilon = \varphi(fg) = \varphi(f)\varphi(g) &= (f(P) + q \circ \varphi(f)\varepsilon)(g(P) + q \circ \varphi(g)\varepsilon) \\ &= f(P)g(P) + (f(P)q \circ \varphi(g) + g(P)q \circ \varphi(f))\varepsilon + q \circ \varphi(f)q \circ \varphi(g)\varepsilon^2 \\ &= f(P)g(P) + (f(P)q \circ \varphi(g) + g(P)q \circ \varphi(f))\varepsilon \end{aligned}$$

Ainsi, $q \circ \varphi$ est bien une dérivation i.e. $q \circ \varphi \in T_P(V)$, puis $\varphi = (q \circ \varphi)^*$. D'où la surjectivité. □

Corollaire D.0.0.5. *Soit $P \in V$. $T_P(V)$ est isomorphe en tant que K-espace vectoriel à $ker(dF_P)$, où $F := (F_1, \cdots, F_s)$ (de sorte que $V = F^{-1}(\{0\})$).*

Démonstration. On sait que $K[V] \simeq K[X_1, \cdots, X_r]/I$ avec I idéal annulateur de V. $K[V]_P$ est alors une K-algèbre engendré par les $\overline{X_j}$, réduites des X_j modulo I donc tout morphismes de $K[V]_P \longrightarrow K[\varepsilon]$ est entièrement déterminé par ses valeurs en les $\overline{X_j}$. Ainsi, la proposition D.0.0.4 assure que $v \in T_P(V)$ est entièrement déterminé par $v^* \in \mathrm{Def}(V, P)$ donc par $(v^*(\overline{X_j}))_{1 \leq j \leq r}$. Mais on sait que :

$$\forall 1 \leq i \leq s, \quad F_i(v^*(\overline{X_1}), \cdots, v^*(\overline{X_r})) = v^*(\overline{F_i}) = v^*(0) = 0 \quad (\star)$$

Or, en écrivant $P := (x_1, \cdots, x_r)$ et $v(\overline{X_j}) := y_j$ pour tout $j \in \{1, \cdots, r\}$, on obtient que $v^*(\overline{X_j}) = x_j + \varepsilon y_j$

pour tout $j \in \{1, \cdots, r\}$ et donc par $(\star)$:

$$\forall 1 \leq i \leq s, \quad \sum_{j=1}^{r} y_j \frac{\partial F_i}{\partial X_j}(P) = 0$$

i.e. $(y_1, \cdots, y_r) \in \ker(dF_P)$. On définit ainsi une application K-linéaire injective :

$$v \in T_P(V) \longmapsto (v(\overline{X_j}))_{1 \leq j \leq r} \in \ker(dF_P)$$

Il s'agit de voir que cette application est sujective. Soit $(y_1, \cdots, y_r) \in \ker(dF_P)$. Alors on définit un morphisme de K-algèbres $\varphi : K[X_1, \cdots, X_r] \longrightarrow K[\varepsilon]$ par :

$$\forall 1 \leq j \leq r, \quad \varphi(X_j) := x_j + \varepsilon y_j$$

Alors :

$$\forall 1 \leq i \leq s, \quad \varphi(F_i) = F_i(\varphi(X_1), \cdots, \varphi(X_r)) = F(P) + \varepsilon \sum_{j=1}^{r} y_j \frac{\partial F_i}{\partial X_j}(P) + \varepsilon^2 \cdots + \cdots = 0$$

Puisque $(y_1, \cdots, y_r) \in \ker(dF_P)$. Ainsi, par passage au quotient, φ induit un un morphisme de K-algèbres $\overline{\varphi} : K[X_1, \cdots, X_r]/I \simeq K[V] \longrightarrow K[\varepsilon]$, qui s'étend sans peine à $K[V]_P$. $v := q \circ \overline{\varphi}$ est alors l'antécédant de $(y_1, \cdots, y_r)$ cherché. □

Proposition D.0.0.6. *Soit $P \in V$. Alors $T_P(V)$ est isomorphe en tant que K-espace vectoriel au dual $(\mathfrak{m}_P/\mathfrak{m}_P^2)^*$, où $\mathfrak{m}_P$ est l'idéal maximal de $k[V]_P$ donné par :*

$$\mathfrak{m}_P = \{f \in k[V]_P \mid f(P) = 0\}$$

Démonstration. Soit $v \in T_P(V)$. Alors pour tous $f, g \in \mathfrak{m}_P$, on a $f(P) = g(P) = 0$ donc :

$$v(fg) = f(P)v(g) + g(P)v(f) = 0$$

v s'annule donc sur $\mathfrak{m}_P^2$ et la propriété universelle du quotient assure que v induit une application K-linéaire $\overline{v} : \mathfrak{m}_P/\mathfrak{m}_P^2 \longrightarrow K$. On définit ainsi un morphisme K-linéaire :

$$v \in T_P(V) \longmapsto \overline{v} \in (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$$

Montrons que ce morphisme est injectif. En effet, si $v \in T_P(V)$ vérifie $\overline{v} = 0$ alors v s'annulle sur $\mathfrak{m}_P$ donc :

$$\forall f \in K[V]_P, \quad v(f) = v(f(P)) \quad (\star)$$

(puisque $f - f(P) \in \mathfrak{m}_P$). Mais pour tout $\lambda \in K$:

$$v(\lambda) = v(\lambda \cdot 1) = \lambda v(1) + v(\lambda)$$

Donc $\lambda v(1) = 0$. Mais par K-linéarité $\lambda v(1) = v(\lambda)$. Ainsi, v est nulle sur K donc nulle par $(\star)$.

Montrons maintenant la surjectivité. Soit $\alpha \in (\mathfrak{m}_P/\mathfrak{m}_P^2)^*$. Posons pour tout $f \in K[V]_P$, $v(f) := \alpha(\overline{f - f(P)})$ où $\overline{f - f(P)}$ est la classe de $f - f(P) \in \mathfrak{m}_P$ modulo $\mathfrak{m}_P^2$. Alors par K-linéarité de α, on obtient que pour tous $f, g \in K[V]_P$:

$$f(P)v(g) + g(P)v(f) = f(P)\alpha(\overline{g - g(P)}) + g(P)\alpha(\overline{f - f(P)}) = \alpha(\overline{f(P)g + g(P)f - 2f(P)g(P)})$$

Mais $v(fg) = \alpha(\overline{fg - f(P)g(P)})$ et :

$$f(P)g + g(P)f - 2f(P)g(P) - (fg - f(P)g(P)) = -(f - f(P))(g - g(P)) \in \mathfrak{m}_P^2$$

De sorte que $\overline{f(P)g + g(P)f - 2f(P)g(P)} = \overline{fg - f(P)g(P)}$ et $v(fg) = f(P)v(g) + g(P)v(f)$. v étant clairement K-linéaire, on a donc montré $v \in T_P(V)$. On a alors clairement $\alpha = \overline{v}$, d'où la surjectivité. $\square$

Annexe E

Calcul de $d_0(N) = (SL_2(\mathbb{Z}) : \Gamma_0(N))$.

Lemme E.0.0.1. *(lemme 2.4.0.7)*

$$d_0(N) := (SL_2(\mathbb{Z}) : \Gamma_0(N)) = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

Démonstration. Nous calculerons cet indice en plusieurs étapes, en calculant d'abord des indices intermédiaires (c'est la démarche suivie dans l'exercice 1.2.2 de [13]).

Étape 1 : Notons :

$$\Gamma(N) := \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I_2 \ [N]\}$$

$\Gamma(N)$ est le noyeau de la réduction modulo $N : SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$, qui est surjective d'après le lemme 2.3.2.2. Ainsi, $(SL_2(\mathbb{Z}) : \Gamma(N)) = |SL_2(\mathbb{Z}/N\mathbb{Z})|$. Mais en écrivant la décomposition de N en produit de facteurs premiers :

$$N = \prod_{i=1}^{r} p_i^{\alpha_i}$$

avec $p_1, \cdots, p_r$ des nombres premiers distincts et $\alpha_1, \cdots, \alpha_r \in \mathbb{N}^*$, on obtient un isomorphisme d'anneaux :

$$\psi : \mathbb{Z}/N\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

en résuisant modulo $p_i^{\alpha_i}$ sur chacun des facteurs $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ (d'après le théorème des restes chinois). On considère alors :

$$\phi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z}) \longmapsto \left(\begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(c) & \psi_i(d) \end{pmatrix} \right)_{1 \leq i \leq r} \in \prod_{i=1}^{r} SL_2(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

Comme ψ est un isomorphisme, on a pour tous $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$:

$$ad - bc = 1 \Longleftrightarrow \forall 1 \leq i \leq r, \quad \psi_i(a)\psi_i(d) - \psi_i(b)\psi_i(c) = \psi_i(ad - bc) = 1 \quad (1)$$

ce qui prouve que ϕ est bien défini. C'est en outre un morphisme de groupes car ψ est un morphisme d'anneaux. Comme ψ est injective, ϕ l'est clairement aussi. En outre, si $\left(\begin{pmatrix} a_i & b_i \\ b_i & d_i \end{pmatrix} \right)_{1 \leq i \leq r} \in \prod_{i=1}^{r} SL_2(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$, alors la surjectivité de ψ assure l'existence de $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$ tels que $a_i = \psi_i(a), b_i = \psi_i(b), c_i = \psi_i(c)$ et $d_i = \psi_i(d)$ pour tout $i \in \{1, \cdots, r\}$. Mais alors $ad - bc = 1$ par (1). Ainsi, ϕ est un isomorphisme de groupes et donc :

$$(SL_2(\mathbb{Z}) : \Gamma(N)) = |SL_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{i=1}^{r} |SL_2(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})| \quad (2)$$

Il suffit donc de calculer $|SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})|$ pour tout nombre premier p et tout $\alpha \in \mathbb{N}^*$. On procède par récurrence sur α. Pour $\alpha = 1$, il est classique que :

$$|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{|(\mathbb{Z}/p\mathbb{Z})^*|} = \frac{(p^2-1)(p^2-p)}{p-1} = p(p-1)(p+1) \quad (3)$$

On obtient $|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$ en comptant les familles libres à deux éléments de $(\mathbb{Z}/p\mathbb{Z})^2$ (p^2-1 choix pour le premier élément et p^2-p pour le deuxième car il doit être linéairement indépendant du premier) ; et $|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{|(\mathbb{Z}/p\mathbb{Z})^*|}$ en remarquant que $SL_2(\mathbb{Z}/p\mathbb{Z})$ est le noyau du morphisme surjectif de groupes $\det : GL_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$.

Soit $\alpha \in \mathbb{N}^*$. Considérons la réduction modulo p^α qui induit un morphisme de groupes :

$$\varphi_\alpha : SL_2(\mathbb{Z}/p^{\alpha+1}\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})$$

La surjectivité de φ_α est une conséquence immédiate du lemme 2.3.2.2. On a donc :

$$|SL_2(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})| = |\ker(\varphi_\alpha)||SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})|$$

Soit donc $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \ker(\varphi_\alpha)$. Notons toujours a, b, c, d les revelés de a, b, c, d dans $\{0, \cdots, p^{\alpha+1} - 1\}$. Alors :

$$a = 1 + kp^\alpha,\ d = 1 + lp^\alpha,\ b = mp^\alpha,\ c = np^\alpha$$

avec $k, l, m, n \in \{0, \cdots, p-1\}$. En outre :

$$ad - bc = (1 + kp^\alpha)(1 + lp^\alpha) - nmp^{2\alpha} \equiv 1 + (k+l)p^\alpha \ [p^{\alpha+1}]$$

Ainsi, $p|k+l$ et donc $k + l = 0$ ou p. Dans les deux cas, le choix de k détermine (i.e. de a) entièrement l (i.e. de d) et les choix de n et m (i.e. de b et c) sont indépendants. On en déduit que $|\ker(\varphi_\alpha)| = p^3$, puis que :

$$|SL_2(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})| = p^3|SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})|$$

Par récurrence et par (3), on en déduit que :

$$|SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})| = p^{3(\alpha-1)+1}p(p-1)(p+1) = p^{3\alpha}\left(1 - \frac{1}{p^2}\right)$$

Puis, par (2) :

$$(SL_2(\mathbb{Z}) : \Gamma(N)) = N^3 \prod_{p|N}\left(1 - \frac{1}{p^2}\right) \quad (4)$$

Étape 2 : Considérons le groupe :

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \ [N] \text{ et } a \equiv d \equiv 1 \ [N] \right\}$$

Qui est un sous-groupe de $\Gamma_0(N)$ dont $\Gamma(N)$ est un sous-groupe. Soit :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \longmapsto b \in \mathbb{Z}/N\mathbb{Z}$$

C'est un morphisme de groupes (pour la multiplication à la source et l'addition au but). Il est surjectif

(car $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$ pour tout $b \in \mathbb{Z}$) et de noyau $\Gamma(N)$. Ainsi :

$$(\Gamma_1(N) : \Gamma(N)) = |\mathbb{Z}/N\mathbb{Z}| = N$$

Par (4), on en déduit que :

$$(SL_2(\mathbb{Z}) : \Gamma_1(N)) = \frac{(SL_2(\mathbb{Z}) : \Gamma(N))}{(\Gamma_1(N) : \Gamma(N))} = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \quad (5)$$

Étape 3 : Considérons l'application :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \longmapsto d \in (\mathbb{Z}/N\mathbb{Z})^*$$

C'est un morphisme de groupes multiplicatifs de noyau $\Gamma_1(N)$. Il est de plus surjectif car si $d \in \mathbb{Z}$ est inversible modulo N, $a \in \mathbb{Z}$ un iverse de d modulo N. On a alors $ad = 1 + bN$ pour un certain $b \in \mathbb{Z}$. Ainsi, $\begin{pmatrix} a & b \\ N & d \end{pmatrix} \in \Gamma_0(N)$ et son image est d $[N]$. Ainsi :

$$(\Gamma_0(N) : \Gamma_1(N)) = |(\mathbb{Z}/N\mathbb{Z})^*| = N \prod_{p|N} \left(1 - \frac{1}{p}\right)$$

et donc par (5) :

$$d_0(N) = (SL_2(\mathbb{Z}) : \Gamma_0(N)) = \frac{(SL_2(\mathbb{Z}) : \Gamma_1(N))}{(\Gamma_0(N) : \Gamma_1(N))} = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

□

Lemme E.0.0.2. *(lemme 2.5.1.4)*

$$|R_N| = N \prod_{p|N} \left(1 + \frac{1}{p}\right) = d_0(N)$$

Il y a donc $d_0(N)$ orbites de P_N sous l'action de $SL_2(\mathbb{Z})$.

Démonstration. Rappelons que :

$$R_N := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad = N \text{ et } 0 \leq b < d \right\}$$

Lorsque d est choisi (nécessairement parmi les diviseurs de N), $a = \frac{N}{d}$ est fixé et il reste à choisir $0 \leq b < d$ premier avec $e_d(N) := d \wedge \frac{N}{d}$ i.e. que b est inversible modulo e_d. Ainsi, b est de la forme $ke_d + l$ avec $0 \leq k < \frac{d}{e_d(N)}$ et l l'un des $\varphi(e_d(N))$ relèvements dans $\{0, \cdots, e_d(N) - 1\}$ d'un inversible modulo $e_d(N)$ (φ étant la fonction indicatrice d'Euler). Il y a donc $\frac{d}{e_d(N)}\varphi(e_d(N))$ choix possibles pour b à d fixé. Ainsi :

$$|R_N| = \sum_{d|N} \frac{d}{e_d(N)} \varphi(e_d(N)) \quad (\star)$$

Or, par multiplicativité du pgcd (que l'on obtient aisément en regardant les facteurs premiers), on a pour $N_1, N_2 \geq 2$ sont premiers entre eux, $d_1|N_1$ et $d_2|N_2$:

$$e_{d_1 d_2}(N_1 N_2) = e_{d_1}(N_1) e_{d_2}(N_2)$$

En outre, φ est multiplicative et $(d_1, d_2) \longmapsto d_1 d_2$ est une bijection entre les couples d'entiers naturels (d_1, d_2) tels que $d_1 | N_1$ et $d_2 | N_2$ et l'ensemble des entiers $d | N$. Donc par changement d'indice :

$$\begin{aligned} |R_{N_1 N_2}| &= \sum_{\substack{d_1 | N_1 \\ d_2 | N_2}} \frac{d_1 d_2}{e_{d_1 d_2}(N_1 N_2)} \varphi(e_{d_1 d_2}(N_1 N_2)) \\ &= \left(\sum_{d_1 | N_1} \frac{d_1}{e_{d_1}(N_1)} \varphi(e_{d_1}(N_1)) \right) \left(\sum_{d_2 | N_2} \frac{d_2}{e_{d_2}(N_2)} \varphi(e_{d_2}(N_2)) \right) = |R_{N_1}||R_{N_2}| \end{aligned}$$

Ainsi, $N \longmapsto |R_N|$ est multiplicative donc il suffit de calculer $|R_{p^\alpha}|$ pour p premier et $\alpha \in \mathbb{N}^*$. On a par $(\star)$:

$$\begin{aligned} |R_{p^\alpha}| &= \sum_{k=0}^{\alpha} \frac{p^k}{p^k \wedge p^{\alpha-k}} \varphi(p^k \wedge p^{\alpha-k}) = 1 + p^\alpha + \sum_{k=1}^{\alpha-1} \frac{p^k}{p^{\min(k,\alpha-k)}} (p^{\min(k,\alpha-k)} - p^{\min(k,\alpha-k)-1}) \\ &= 1 + p^\alpha + \sum_{k=1}^{\alpha-1} p^k \left(1 - \frac{1}{p}\right) = 1 + p^\alpha + p \frac{p^{\alpha-1} - 1}{p-1} \left(1 - \frac{1}{p}\right) = p^\alpha + p^{\alpha-1} = p^\alpha \left(1 + \frac{1}{p}\right) \end{aligned}$$

En décomposant N en produit de facteurs premiers, on obtient donc finalement :

$$|R_N| = N \prod_{p | N} \left(1 + \frac{1}{p}\right) = d_0(N)$$

□

Bibliographie

[1] SATOH Takakazu. *The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting . Journal of the Ramanujan Mathematical Society*, December 2000.

[2] SILVERMAN Joseph. *The Arithmetic of Elliptic Curves*. 2nd Ed. New York, USA : Springer, 2009, 522 p.

[3] SCHRAEN Benjamin. *Introduction à la géométrie algébrique et courbes elliptiques*. École polytechnique, 2019.

[4] GUILLOT Philippe. *Introduction aux courbes elliptiques pour la cryptographie* [en ligne]. Saint Denis, 2013, 89 p. Disponible sur : http ://ufr6.univ-paris8.fr/Math/sitemaths2/spip/IMG/pdf/PolyECCCourt.pdf.

[5] STROH Benoît. *Représentations des groupes compacts*. École Polytechnique, 2018-2019.

[6] SHAFAREVICH I. R. *Basic algebraic geometry 1*. Springer-Verlag, Berlin, third edition, 2013. Translation of the 3rd Russian edition entitled "Osnovy algebraicheskoj geometrii". MCCME, Moscow 2007, originally published in one volume.

[7] LANG Serge. *Algèbre*. 3ème édition, traduit de l'anglais par Christos Grammatikas. Paris, France : Dunod, 2014, 912 p.

[8] LANG Serge. *Elliptic Functions*. 2nd Ed. New York, USA : Springer, 1987, 328 p.

[9] LANG Serge. *Algebraic Number Theory*. 2nd Ed. New York, USA : Springer, 1994, 357 p.

[10] CHENEVIER Gaëtan. *Théorie Algébrique des Nombres*. Palaiseau, École polytechnique, 2018, 149 p.

[11] FAVRE Charles. *Surfaces de Riemann et théorie des revêtements*. Palaiseau, École polytechnique, 2019, 120 p.

[12] LAURENT-THIÉBAUT Christine. *Fonctions holomorphes de plusieurs variables - Une introduction*. Paris, CNRS Éditions et InterEditions, 1997, 244 p.

[13] DIAMOND Fred, SHURMAN Jerry. *A First Course of Modular Forms*. New-York, Springer-Verlag, 2005, 447 p.

[14] AMICE Yvette. *Les nombres p-adiques*. Paris, Presses Universitaires de France, 1975, 193 p.

[15] VÉLU Jacques. *Isogénies entre courbes elliptiques*. Compte Rendu de l'Académie des Sciences de Paris. Paris, BnF, Gallica, 1971, 6 p.