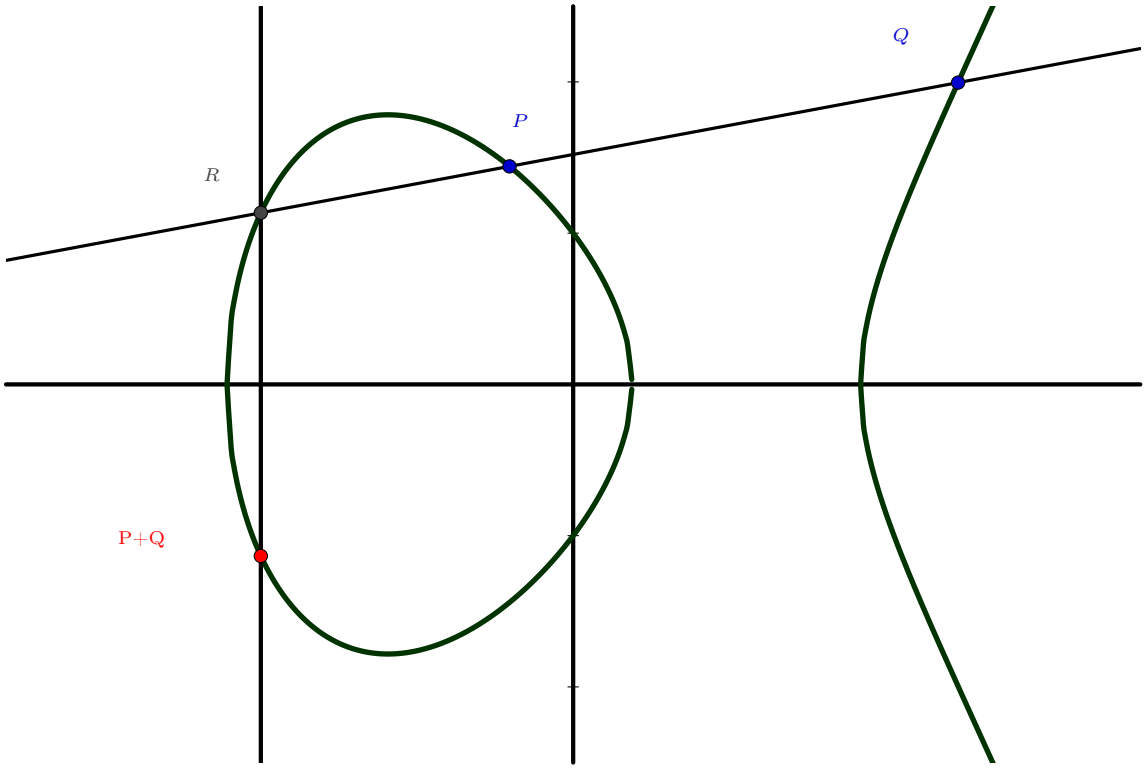
Projet Scientifique Collectif : Comptage de points sur les courbes elliptiques.

Rapport final.

Gustave Billon, Pierrick Dartois, Pedro Freire Mascarenhas Pontes, Minmin Ge, Emmanuel Pinglier, Quentin Yang, Raphaël Yu.

Abstract : Notre groupe de PSC avait pour objectif principal d'étudier un algorithme de comptage de points sur une courbe elliptique qui peut être appliqué à la cryptographie, à travers un article que nous devons à Satoh. Nous présentons donc le fonctionnement de cet algorithme, sa preuve mathématique ainsi qu'une implémentation en Sage.



Remerciements

Nous ne pouvions commencer notre rapport sans remercier Stéphane Bijakowski qui a encadré notre projet en tant que tuteur et coordintateur. Sa disponibilité pour répondre à nos questions, son suivi du projet et les références qu'il nous a indiquées nous ont été indispensables.

Merci aussi à François Morain et Pierrick Gaudry, spécialistes du comptage de points, qui nous ont aidé à faire face à quelques difficultés d'implémentation.

Merci enfin au département de mathématiques pour avoir mis à notre disposition les moyens de faire ce PSC extrêmement enrichissant.

Introduction.

Avant d'entrer dans l'étude de l'algorithme de Satoh en lui même, il nous a fallu acquérir toutes les connaissances mathématiques nécessaires à sa compréhension en profondeur. Nous partions de loin, avec seulement nos connaissances de classes préparatoires ou de premier cycle universitaire. Sans maîtrise des nombres p-adiques, avec seulement quelques rudiments en algèbre générale et en théorie des anneaux et des corps, et sans avoir approché ni de près ni de loin la géométrie algébrique pour la plupart d'entre nous, un important travail préparatoire fut nécessaire pour parvenir au résultat d'aujourd'hui.

Nous avons commencé par un survol des sources à notre disposition, visant à dégager les principales notions à aborder avant de nous concentrer en profondeur dessus. Nous en avons dégagé principalement sept :

- L'étude élémentaire des courbes elliptiques qui fait notamment l'objet de la section 1.
- Les prérequis d'algèbres qui nous manquaient (arithmétique sur les anneaux, modules, algèbres et théorie de Galois) qui font l'objet de l'annexe B (sauf pour la théorie de Galois vue en cours de MAT 451).
- Des éléments de théorie algébrique des nombres, en particulier sur les nombres p-adiques qui font l'objet de la section 2 et des annexes C et D. Le coeur de l'algorithme de Satoh étant un relèvement p-adique de courbes elliptiques définies sur $\mathbb{F}_q$, ceci nous a paru indispensable.
- Des éléments de géométrie algébrique (notion la plus difficile, que nous avons abordée sous l'angle le plus élémentaire possible) qui fait l'objet de la section 3. L'objectif principal de cette étude était de comprendre la notion d'isogénie et de l'utiliser pour comprendre le théorème de Hasse, essentiel pour le comptage de points.
- Le cas particulier des courbes elliptiques définies sur $\mathbb{C}$ (présenté en section 4), reformulant les notions de géométrie algébrique avec le langage de l'analyse complexe, plus aisé à comprendre pour nous (et donc étudié en amont). L'intérêt de ce point de vue est qu'il est transposable à d'autres corps que $\mathbb{C}$, (en particulier aux extensions de $\mathbb{Q}_p$), et qu'il permet de justifier un calcul de relèvement p-adique d'une courbe elliptique à partir d'une équation polynômiale.
- Le groupe formel, très utilisé comme outil de calcul par Satoh, qui fait l'objet de la section 5.
- Les propriétés du relèvement p-adique d'une courbe elliptique (admises en raison de notre insuffisante maîtrise de la théorie des nombres et de la géométrie algébrique pour les comprendre pleinement). Elles font l'objet de la section 6.

Une fois toutes ces notions abordées, nous avons pu étudier pleinement l'algorithme de Satoh (dans la section 7), faire état de certaines approximations et en proposer une implémentation machine avec le langage Sage.

Ce rapport présente une double fonction. Il sert bien sûr à présenter notre travail mais ceci aurait sans doute pu être fait de façon plus concise. Il est donc aussi une compilation de tout le contenu mathématique, auparavant inconnu pour nous, que nous avons abordé au cours de ce projet. Il est conçu comme un outil de travail, auquel nous nous sommes référés continuellement pour partager et actualiser nos connaissances. Pour que l'exhaustivité de ce rapport ne rebute pas le lecteur, nous avons donc mis en annexe les développements les plus techniques et les plus périphériques. Comme nous sommes entrés dans les détails, nous tenons cependant à présenter l'intégralité de ce que nous avons vu.

Nous avons fait tout notre possible pour rendre le parcours de ce rapport agréable. Il y a deux documents : un pour le corps du texte, l'autre pour les annexes. Toutes les notions introduites font l'objet d'une motivation dans la perspective d'une application concrète. Les résultats principaux sont encadrés en bleu et les théorèmes centraux sont encadrés en rouge. Ainsi nous vous souhaitons une bonne lecture.

Une brève histoire de ce PSC : organisation et difficultés rencontrées.

Ce PSC a principalement consisté en un travail de recherche bibliographique. Une fois les références adéquates réunies, il nous a fallu nous organiser pour y comprendre ce qui nous était nécessaire. Nous avons dû régler pour cela différents problèmes organisationnels :

1. Comment partager l'étude des notions indispensables sachant que la compréhension des unes nécessite parfois celles des autres et que nous ne le savons pas a priori ?
2. Comment faire en sorte que tous les membres du PSC aient une vision d'ensemble et connaissent tous les outils mathématiques nécessaires ?
3. Comment s'assurer de la bonne gestion de notre temps ?

Pour répondre à la première question, nous avons tenté une répartition "à première vue", en "pariant" sur les notions prétendument indépendantes [1]. Nous avons construit de petits groupes de deux à trois personnes pour étudier indépendamment ces notions. Voici par exemple la répartition que nous avions adopté dans la proposition détaillée :

Thème	Théorie des corps et théorie de Galois.	Nombres p-adiques et relèvement p-adique d'une courbe elliptique.	Isogénies.
"Spécialistes"	Pierrick Dartois Emmanuel Pinglier	Quentin Yang Raphaël Yu	Gustave Billon Pedro Freire Mascarenhas Pontes Minmin Ge

Il restait bien sûr d'autres notions à étudier, que nous comptions aborder ensuite.

Pour échanger les informations entre les membres du groupe (deuxième question), nous avons adopté la méthode des exposés. Chaque semaine lors des réunions PSC, chacun passait à tour de rôle en début de séance pour expliquer son travail aux autres afin que chacun en maîtrise les fondamentaux. Nous sollicitions aussi des exposés lors des entretiens avec notre tuteur. Ceci a bien fonctionné au début, notamment pour les nombres p-adiques ainsi que la théorie des corps sur laquelle nous avons beaucoup insisté car nous pensions - à raison - qu'il s'agissait d'un prérequis transversal.

Pour la gestion du temps, nous nous sommes donné un échéancier avec l'étude de 3 premières notions de septembre à décembre, l'étude des suivantes de décembre à février et le début de la programation de février à avril.

Toutefois, ce système de répartition par notions indépendantes et exposés réguliers a vite rencontré ses limites.

Tout d'abord, les notions prétendument indépendantes ne l'étaient pas vraiment et nous en avons parfois sous-estimé l'ampleur mathématique. La notion d'anneau de valuation discrète, vue dans l'étude des nombres p-adiques, était par exemple nécessaire à la compréhension de certaines notions de géométrie algébrique élémentaire. Nous nous sommes aussi rendus compte qu'il fallait détacher un groupe pour l'étude de notions profondes de théorie algébrique des nombres avant d'aborder la preuve du théorème de Deuring (6.3.2), résultat tout à fait central pour notre sujet d'étude. Nous avions constamment le souci de maîtriser toute la construction mathématique des outils introduits et utilisés. Aussi, vu le nombre considérable de notions à étudier pour en arriver à comprendre la preuve de ce théorème, nous avons fini par l'admettre. Nous risquions de perdre en rigueur et de creuser les écarts dans le groupe, pour ce résultat théorique. Ceci nous aura ainsi été enseigné : une recherche bibliographique n'est pas un sentier battu. Nous ne pouvons en connaître à l'avance la difficulté. Prévoir une organisation trop formelle était donc voué à l'échec.

Les exposés ont aussi vite rencontré leurs limites. En effet, ils étaient souvent assez chronophages et empêchaient donc le groupe d'avancer de façon effective. Par ailleurs, ces séances traînant souvent en longueur, la concentration de certains membres de notre équipe baissait inévitablement avec les heures.

Nous avons donc décidé d'adopter une organisation moins formalisée dans la répartition du travail. Plutôt que d'affecter des personnes à des grands thèmes, nous nous donnions chaque semaine des missions précises. Chacun avait bien sûr un thème de prédilection mais quand un groupe spécialisé présentait une difficulté, il pouvait par exemple demander du renfort. Ainsi, par exemple, Emmanuel et Pierrick ont "migré" vers la théorie algébrique des nombres une fois la théorie de Galois terminée afin d'envisager la preuve du théorème de Deuring. Les "spécialistes" des nombres p-adiques ont aussi pu répondre aux questions des "spécialistes" de géométrie algébrique sur la notion d'anneau de valuation discrète. De même, au moment d'aborder l'implémentation de l'algorithme, Quentin qui était affecté à l'étude de la

1. à l'exception de la théorie des corps et de la théorie de Galois, comme nous le verrons plus tard.

proposition 4.2. de l'article de Satoh ([1]) est venu aider Minmin et Raphaël à programmer. Au lieu de faire des exposés systématiquement, nous exposions nos connaissances à la demande de ceux qui en avaient besoin. De plus, le rapport servait de référence commune pour certaines questions techniques. Cette organisation flexible est devenue de plus en plus efficace au fur et à mesure que chacun se spécialisait et que notre compréhension du sujet s'améliorait.

Bien sûr, l'inconvénient majeur de cette méthode est que tous les membres du groupe ont des connaissances assez hétérogènes, puisqu'ils sont spécialisés, ce qui peut nuire à la compréhension d'ensemble. La lecture partagée du rapport et le retour à des séances d'exposés et de questions/réponses devrait régler ce problème d'ici la soutenance. Nous sommes confiants sur ce point puisque nous avons su atteindre nos objectifs : comprendre en détail et implémenter l'algorithme de Satoh.

En effet, cette organisation moins formelle nous a permis de respecter les jalons que nous nous étions fixés. Nous avons simplement eu un petit retard dans l'implémentation de l'algorithme, assez rapidement corrigé courant avril. Grâce au travail régulier et à la motivation de chacun, notre PSC n'a pas sombré sous les flots des séances de MIE du mercredi après-midi et autres banalisations des crénaux par l'administration de l'École tant décriées dans le dernier IK Enseignement.

Table des matières

Par convention, dans tout ce document, les corps et les anneaux sont commutatifs et les anneaux sont intègres, sauf mention du contraire.

1 Contexte général du sujet.

Comme nous le verrons, ce sujet requiert un important bagage théorique. Aussi souhaitons-nous commencer par des considérations pratiques.

Le cryptage RSA nous a rendu bien des services jusqu'à présent pour sécuriser nos données. Cependant, si les recherches liées à la factorisation des nombres entiers progressent suffisamment pour casser ce type de cryptosystème, il peut être intéressant de trouver un autre procédé de cryptage. Une des pistes possibles est le logarithme discret dans un groupe fini. Les courbes elliptiques définies sur les corps finis, une fois munies d'une structure de groupe abélien, peuvent donc être utilisées pour la cryptographie. La question est alors de savoir quelles sont les courbes elliptiques dans lesquelles le problème du logarithme discret est suffisament difficile à résoudre. Nous verrons que c'est là que le comptage de points intervient. Présentons d'abord plus en détail les problèmes liés à la cryptographie.

1.1 Quelques considérations sur la cryptographie.

1.1.1 Principe des cryptosystèmes

Le problème est le suivant. Deux interlocuteurs *Alice* et *Bob* veulent communiquer sur un canal de transmission non sécurisé, de sorte qu'un tiers *Eve* est susceptible d'intercepter leurs échanges. Par exemple, *Alice* peut être un consommateur, *Bob* un site d'achats en ligne à qui *Alice* transmet ses données bancaires pour réaliser un paiement et *Eve* un cyber-pirate.

Pour sécuriser ses données bancaires, *Alice* va les chiffrer avant de les envoyer à *Bob*, de telle façon que seul *Bob* puisse les lire. *Alice* et *Bob* vont donc utiliser un *cryptosystème*, c'est-à-dire un ensemble de clés de chiffrement, utilisées pour chiffrer des messages, chacune étant associée à une clé de déchiffrement permettant l'opération inverse, et qui est très difficile à trouver à partir de la seule clé de chiffrement. *Alice* choisit une clé k, de telle sorte que *Bob* connaisse la clé d_k de déchiffrement associée. Elle chiffre ses données bancaires m à l'aide de k, et envoie le cryptogramme obtenu c à *Bob*. Si *Eve* intercepte c, elle ne pourra rien en faire sans connaître la clé d_k (du moins si le cryptosystème est bien conçu). A la fin de la chaîne, *Bob* déchiffrera les coordonnées bancaires de *Alice* en utilisant d_k.

Les cryptosystèmes les plus simples utilisent la même clé pour chiffrer et déchiffrer les messages : on parle alors de cryptographie symétrique. C'est le cas du chiffre de César par exemple, qui consiste à décaler dans l'alphabet les lettres du message à crypter. Il est important pour ce type de chiffrage que la clé soit très difficile à trouver à partir de seuls messages cryptés, même en grand nombre. Ce n'est pas le cas du chiffre de César qui peut être cassé à partir d'une simple analyse fréquentielle du message, mais il existe des cryptosystèmes symétriques très solides, utilisant notamment des réseaux de Feistel. En revanche, la cryptographie symétrique nécessite un premier échange entre *Alice* et *Bob* pour se mettre d'accord sur la clé, qui peut être interceptée par *Eve* à cette occasion. Pour remédier à ce problème, on utilise la cryptographie à clé publique.

1.1.2 La cryptographie à clé publique

La question est de savoir comment *Bob* peut connaître la clé d_k de manière efficace et sécurisée. Le plus simple est de travailler avec des cryptosystèmes dits *à clé publique*. *Bob* publie la clé k (appelée *clé publique*) avec laquelle il veut être joint, mais pas la clé d_k (la *clé privée*) avec laquelle il va déchiffrer ses messages. Si *Alice* veut le joindre, elle doit chiffrer son message avec la clé k. Ainsi il n'y a pas besoin d'une première communication non cryptée entre Alice et Bob pour se mettre d'accord sur k et d_k. De plus, en général, la relation chiffrement / déchiffrement est symétrique, c'est-à-dire qu'un message chiffré avec une clé de déchiffrement peut être déchiffré avec la clé de chiffrement associée. Ainsi, si Alice veut savoir si c'est bien Bob qui lui demande des informations, elle peut exiger de lui qu'il crypte ses messages avec sa clé privée d_k. Si elle peut déchiffrer le cryptogramme obtenu avec la clé publique k, elle est assurée que le message vient de Bob.

L'exemple le plus connu de cryptographie à clé publique est le cryptosystème RSA (encore très largement utilisé aujourd'hui). On se donne un groupe abélien fini G de cardinal n secret. Généralement, on choisit $G = (\mathbb{Z}/N\mathbb{Z})^*$ avec $N = pq$, et p et q sont deux grands nombres premiers, on a alors $n = \varphi(N) = (p-1)(q-1)$. On se donne un exposant k premier à n qui constituera la clé publique et un exposant d gardé secret, qui constituera la clé privée, telle que $kd \equiv 1[n]$ [2], l'existence de d étant

2. n est gardé secret de façon à ce que l'on ne puisse pas remonter facilement à d à partir de k par une simple application de l'algorithme d'Euclide étendu. C'est parfois difficile de trouver un groupe public, dans lequel tout le monde puisse calculer

assurée par le théorème de Bézout. *Alice* s'arrange pour que son message soit traduit en un élément m de G, et envoie le cryptogramme $c = m^k$ à *Bob*. *Bob* le décode avec sa clé privée d :

$$c^d = m^{kd} = m$$

Mais les systèmes à clé publique présentent un inconvénient. *Eve* peut très bien mener une *attaque à clair choisi*, c'est à dire chiffrer des messages de son choix avec la clé publique k, et utiliser les cryptogrammes obtenus pour en déduire la clé de privée d. Elle saura alors comment déchiffrer tous les messages reçus par *Bob*. [3]

C'est pourquoi, dans le protocole HTTPS par exemple, très largement utilisé pour assurer la sécurité des échanges par internet, *Alice* et *Bob* commencent par se mettre d'accord sur une clé commune à l'aide d'un cryptosystème à clé publique, puis ils utilisent cette clé pour crypter leurs échanges de façon symétrique. Cette façon de faire présente également l'avantage d'être plus rapide, la cryptographie symétrique nécessitant moins de temps de calcul que la cryptographie asymétrique. C'est notamment le principe de l'échange de clés de Diffie-Hellman.

1.1.3 L'Échange de clés de Diffie-Hellman

On se donne G un groupe cyclique d'ordre n qui contiendra la clé finale et g un générateur de G. En pratique $G = (\mathbb{Z}/p\mathbb{Z})^*$ pour p un nombre premier assez grand [4]. *Alice* choisit secrètement un entier a au hasard dans $\{0, \cdots, n-1\}$ et *Bob* choisit de la même façon un entier b. *Alice* calcule g^a et l'envoie à *Bob*, qui élève le résultat à la puissance b pour obtenir $k = g^{ab}$. De même, *Bob* calcule g^b et l'envoie à *Alice*, qui élève à son tour le résultat à la puissance a pour trouver k. *Eve* qui épie leurs couversations n'aura connaissance que de g, g^a et g^b. Pour trouver k, elle devra savoir traiter le problème du logarithme discret dans G, c'est à dire savoir retrouver a et b à partir de g, g^a et g^b ; problème à ce jour très difficile à résoudre lorsque $n =\mid G \mid$ assez grand et G bien choisi.

Une fois la clé secrète k échangée, *Alice* et *Bob* peuvent communiquer de façon symétrique en toute sécurité en appliquant le protocole d'El-Gamal. Si *Alice* veut envoyer un message m à *Bob*, elle calcule le cryptogramme $c = km$ et l'envoie à *Bob*, qui le décrypte en calculant $k^{-1}c$. La procédure est identique si *Bob* veut envoyer un message à *Alice*, c'est pour cette raison que le cryptosystème El-Gamal est symétrique.

On retiendra que la plupart des cryptosystèmes à courbes elliptiques fonctionnent selon ce principe. Il faut donc s'assurer que le groupe G dans lequel on travaille soit tel qu'il est très difficile de résoudre le problème du logarithme discret pour trouver la clé k.

1.1.4 Pourquoi compter les points : le problème du logarithme discret.

On voit que l'échange de clés de Diffie-Hellman pose un critère pour savoir si un groupe G est approprié pour faire de la cryptographie : le problème du logarithme discret est-il facile à résoudre dans G ? Précisons d'abord la notion de logarithme discret.

Définition 1.1.1. *Soit G un groupe abélien fini et $g, h \in G$. On appelle, sous réserve d'existence,* logarithme discret en base g de h *le plus petit entier naturel a tel que $h = g^a$. On le note $l_g(h)$.*

L'un des algorithmes les plus efficaces pour résoudre ce problème est l'algorithme de Pohlig-Hellman.

Théorème 1.1.2 (Pohlig-Hellman)**.** *Soient G un groupe cyclique de cardinal n, $g \in G$ un générateur de G et $h \in G$ quelconque. Alors il existe un algorithme permettant de trouver $l_g(h)$ avec :*

$$O\left(\sum_{p|n} \alpha_p(\log(n) + \sqrt{p}) + \log(n)^2\right)$$

opérations arithmétiques élémentaires où $n = \prod_{p|n} p^{\alpha_p}$ est la décomposition de n en produit de facteurs premiers (que l'on suppose connue).

Démonstration. Voir annexe A.1. □

pour crypter des messages mais dont le cardinal reste secret. C'est l'avantage du choix du groupe $G = (\mathbb{Z}/N\mathbb{Z})^*$ car l'on peut connaître $N = pq$ tout en ignorant $n = (p-1)(q-1)$, dont le calcul nécessite de connaître la factorisation de N (question très difficile à résoudre lorsque N devient grand).

3. Il est possible de contourner cette difficulté en changeant de clés souvent, ou en complexifiant le cryptosystème de telle façon qu'un même message ne donne pas toujours le même cryptogramme. En général, les cryptosystèmes type RSA en eux mêmes évitent ce type d'erreur. Il suffit de prendre une clé publique k très grande, de telle façon qu'il soit difficile de remonter aux messages en clairs m, à partir des cryptogrammes m^k.

4. Un sous-groupe cyclique d'une courbe elliptique pourrait tout aussi bien convenir.

On constate donc que le problème du logarithme discret est d'autant plus facile à résoudre lorsque $n = |G|$ n'admet que des petits facteurs premiers. Lorsque le groupe choisi est une courbe elliptique définie sur $\mathbb{F}_q$, il est donc utile d'en compter les points. Tel est l'objet de l'algorithme de Satoh. Mais avant d'aller plus loin, il est indispensable de définir les courbes elliptiques et de les munir d'une structure de groupe abélien.

1.2 Commençons... Généralités sur les courbes elliptiques.

Nous présentons ici ce qu'est une courbe elliptique et comment est construite la loi de groupe sur une courbe elliptique.

Dans ce paragraphe, $\mathbb{K}$ désigne un corps commutatif et $\overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$. Les preuves de cette section sont en annexe A.3.

Définition 1.2.1. *On appelle* plan projectif sur $\mathbb{K}$ *et on note* $\mathbb{P}^2(\overline{\mathbb{K}})$ *l'ensemble des classes d'équivalence de* $\overline{\mathbb{K}}^3 \setminus \{0\}$ *modulo la relation* $\sim$ *donnée par :*

$$\forall A, B \in \overline{\mathbb{K}}^3, \quad x \sim y \Longleftrightarrow \exists \lambda \in \overline{\mathbb{K}}^*,\ A = \lambda B$$

Pour tous $x, y, z \in \overline{\mathbb{K}}$*, on note* $[x : y : z]$ *la classe d'équivalence de* (x, y, z) *modulo* $\sim$*.*

On appelle ensemble des points $\mathbb{K}$-rationnels *l'ensemble :*

$$\mathbb{P}^2(\mathbb{K}) := \{[x : y : z] \mid x, y, z \in \mathbb{K}\}$$

Pour faire simple, le plan projectif peut être vu comme l'ensemble des droites de $\mathbb{K}^3$ passant par l'origine. Il peut aussi être vu comme le plan $\mathbb{K}^2$ auquel on ajoute des points à l'infini.

Définition 1.2.2. *On appelle* courbe de genre 1 sur $\overline{\mathbb{K}}$ *un ensemble* E *de la forme :*

$$E = \{P := [x : y : z] \in \mathbb{P}^2(\overline{\mathbb{K}}) \mid F(x, y, z) = 0\}$$

où $F \in \overline{\mathbb{K}}[X, Y, Z]$ *est un polynôme homogène de la forme :*

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

avec $a_1, \cdots, a_6 \in \overline{\mathbb{K}}$*. On dit que* E est définie sur $\mathbb{K}$ *lorsque tous les coefficients précédents sont dans* $\mathbb{K}$*. On note alors* $E(\mathbb{K}) := E \cap \mathbb{P}^2(\mathbb{K})$ l'ensemble des points de $\mathbb{K}$.

En faisant la substitution $x := \frac{X}{Z}$ et $y := \frac{Y}{Z}$, on voit que :

$$E = \{P := [x : y : 1] \in \mathbb{P}^3(\overline{\mathbb{K}}) \mid f(x, y) = 0\} \cup \{\mathcal{O}\}$$

avec $\mathcal{O} := [0 : 1 : 0]$, appelé *point à l'infini* (heuristiquement équivalent du point $(x, y) = (0, \infty)$ car $Z = 0$) et $f \in \overline{\mathbb{K}}[X, Y]$, le polynôme donné par :

$$f = Y^2 - X^3 + a_1XY - a_2X^2 + a_3Y - a_4X - a_6$$

Définition 1.2.3. *L'équation* $f(x, y) = 0$ *est appelée* équation de Weierstrass *et le polynôme* f *est appelé* polynôme de Weierstrass.

Cette équation peut encore être simplifiée dans le cas où la caractériqtique de $\mathbb{K}$ (que l'on notera $\mathrm{car}(\mathbb{K})$ dans toute la suite) est distincte de 2. En effet, en faisant la substitution :

$$Y' := \frac{Y - a_1X - a_3}{2}$$

On trouve que :

$$\tilde{f} := Y'^2 - 4X^3 - b_2X^2 - 2b_4X - b_6$$

avec :

$$b_2 := a_1^2 + 4a_2, \quad b_4 := 2a_4 + a_1a_3, \quad b_6 := a_3^2 + 4a_6$$

est un polynôme de Weierstrass de la courbe $\tilde{E}$ associée à E définie par :

$$\tilde{E} := \left\{ \left[x : \frac{y - a_1x - a_3}{2} : 1 \right] \mid [x : y : 1] \in E \right\} \cup \{\mathcal{O}\}$$

De la même façon, on peut lorsque car($\mathbb{K}$) ≥ 5, par une substitution analogue, supprimer le terme en X^2 du polynôme de Weierstrass (en changeant les coefficients) pour obtenir un polynôme de Weierstrass de la forme :

$$\hat{f} = Y^2 - X^3 - AX - B$$

Ce constat sera largement utilisé par Satoh en pratique.

Nous allons maintenant définir une loi de groupe sur une courbe de genre 1 E fixée. Deux points P et Q de E différents de $\mathcal{O}$ peuvent être vus comme des points de $\overline{\mathbb{K}}^2$ car ils sont entièrement déterminés par leurs coordonnées x et y. Si P et Q sont distincts, il existe alors une unique droite D du plan passant par ces points. Lorsque D n'est pas verticale (i.e. lorsque $x(P) \neq x(Q)$), déterminer les points d'intersection entre cette droite et la courbe E (entièrement déterminée par le polynôme f) revient à résoudre une équation polynomiale de degré 3 à une variable, qui possède trois solutions (comptées avec multiplicité) dans le corps algébriquement clos $\overline{\mathbb{K}}$. Il existe donc un troisième point d'intersection R entre D et E (qui peut être éventuellement confondu avec P ou Q). On considère alors la droite verticale D', passant par R, ie d'équation $x = x(R)$ (qui peut être vue géométriquement comme la droite d'intersection entre R et $\mathcal{O}$). Cette droite D' a deux points d'intersection avec E (issus de la résolution d'une équation polynomiale d'ordre 2 à une variable) : R, et un autre point que l'on notera $P \oplus Q$.

On veut maintenant généraliser le calcul de $P \oplus Q$ aux autres cas. Si $P = \mathcal{O}$, on remplace D par la droite d'équation $x = x(Q)$ et si $Q = \mathcal{O}$, on remplace D par la droite d'équation $x = x(P)$ dans la construction précédente. Il est clair que dans ces deux cas on obtient respectivement P et Q comme résultat (car alors $D = D'$). $\mathcal{O}$ joue donc le rôle d'élément neutre et on peut donc convenir que $\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$.

Le cas où $P = Q \neq \mathcal{O}$ est plus délicat. On aurait bien envie de prendre pour droite D la tangente à la courbe E (notion à définir). Mais cette tangente ne va pas toujours être bien définie ce qui motive les développements qui vont suivre.

Le dernier cas à traiter et le cas où D est verticale. On conviendra alors dans ce cas que $P \oplus Q = \mathcal{O}$.

On a représenté géométriquement ci-dessous la loi d'addition des points dans le cas réel ($\mathbb{K} = \mathbb{R}$).

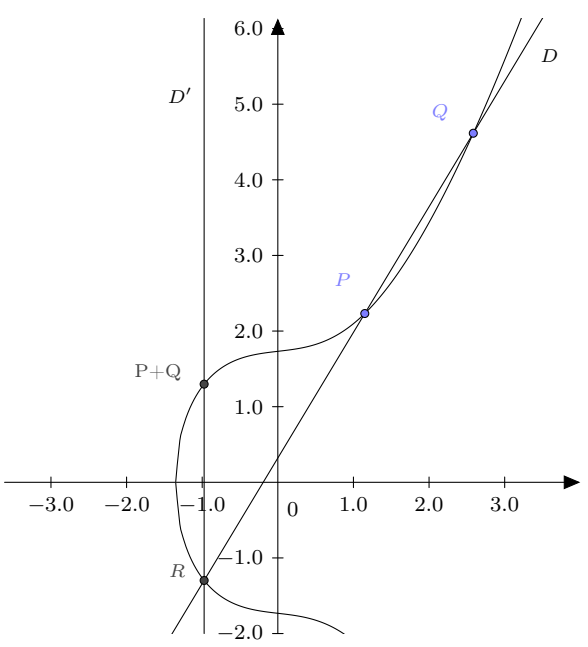


FIGURE 1 – Loi d'addition sur la courbe de genre 1 d'équation $y^2 = x^3 + \frac{2}{5}x + 3$, cas $P \neq Q$.

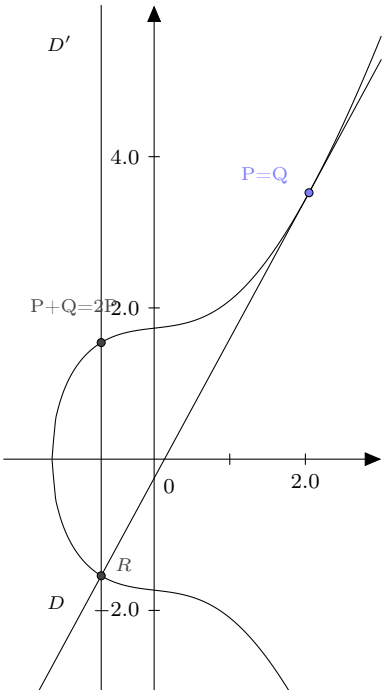


FIGURE 2 – Loi d'addition sur la courbe de genre 1 d'équation $y^2 = x^3 + \frac{2}{5}x + 3$, cas $P = Q$.

Définition 1.2.4. *Soit E une courbe de genre 1 d'équation de Weierstrass $f(x, y) = 0$. On dit qu'un point $P := [x : y : 1] \in E \setminus \{\mathcal{O}\}$ est* singulier *lorsque :*

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

Une courbe de genre 1 est dite singulière *si elle possède au moins un point singulier. Sinon, elle est appelée* courbe elliptique. *Pour une courbe de genre 1 E donnée, on notera E_{ns} l'ensemble de ses points non singuliers.*

Définition 1.2.5. *Soit E une courbe de genre 1 d'équation de Weierstrass $f(x,y)=0$. Soit $P := [x_0 : y_0 : 1] \in E \setminus \{\mathcal{O}\}$ un point non-singulier. Alors on appelle tangente à E en P, la droite d'équation :*

$$(x-x_0)\frac{\partial f}{\partial X}(x_0,y_0)+(y-y_0)\frac{\partial f}{\partial Y}(x_0,y_0)=0$$

Il est possible de caractériser les courbes elliptiques en introduisant les notations suivantes associées à l'équation de Weierstrass :

$$b_8 := a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^3-a_4^2, \quad \Delta := -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6$$

Définition 1.2.6. *La quantité Δ est appelée* discriminant de E.

Proposition 1.2.7. *Si car$(\mathbb{K}) \neq 2$ alors :*

$$\Delta = \frac{1}{16}disc\left(\tilde{f}(X,0)\right) = \frac{1}{16}disc\left(4X^3+b_2X^2+2b_4X+b_6\right)$$

disc désignant la fonction discriminant et $\tilde{f}$ étant le polynôme de Weierstrass alternatif introduit précédemment. Ceci justifie le nom de discriminant donné à la quantité Δ.

On dispose de la caractérisation suivante des courbes singulières :

Proposition 1.2.8. *Soit E une courbe de genre 1 d'équation de Weierstrass $f(x,y)=0$. Alors E est singulière si et seulement si $\Delta = 0$. Dans ce cas, il n'existe qu'un seul point singulier.*

Nous savons donc maintenant comment caractériser les courbes singulières, qui sont en général éliminées dans les applications cryptographiques (de façon à être sûr que tout point de la courbe est un point du groupe). Nous verrons cependant que ce n'est pas absolument nécessaire pour définir une structure de groupe car on peut se restreindre à l'ensemble E_{ns} des points non-singuliers. Pour définir cette loi de groupe, commençons par donner des formules d'addition sur les points non-singuliers.

Proposition 1.2.9 (formules d'addition des points)**.** *Soit E une courbe de genre 1 d'équation de Weierstrass :*

$$f(x,y) := y^2-x^3+a_1xy-a_2x^2+a_3y-a_4y-a_6=0$$

Soient $P_1, P_2 \in E_{ns} \setminus \{\mathcal{O}\}$ et $P_3 := P_1 \oplus P_2$ que l'on écrit $P_i := [x_i : y_i : 1]$ pour $i \in \{1,2\}$, alors :

(1). *P_1 admet un opposé $\ominus P_1 := [x_1 : -y_1-a_1x_1-a_3 : 1]$.*

(2). *Si $x_1 \neq x_2$ alors $P_3 := [x_3 : y_3 : 1]$ avec :*

$$x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2 \quad et \quad y_3 = -(\lambda+a_1)x_3-\nu-a_3$$

où :

$$\lambda := \frac{y_2-y_1}{x_2-x_1}, \nu := \frac{y_1x_2-y_2x_1}{x_2-x_1}$$

(3). *Si $P_1 = P_2$ et $2y_1+a_1x_1+a_3 \neq 0$ alors :*

$$x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2 \quad et \quad y_3 = -(\lambda+a_1)x_3-\nu-a_3$$

avec :

$$\lambda := \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, \nu := \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}$$

On déduit des formules précédentes le résultat suivant :

Corollaire 1.2.10. *$(E_{ns}, \oplus)$ est un groupe abélien. En outre, l'ensemble $E(\mathbb{K}) := E_{ns} \cap \mathbb{P}^2(\mathbb{K})$ des points de $\mathbb{K}$ est un sous-groupe de $(E_{ns}, \oplus)$.*

Dans toute la suite, on ne considèrera que des courbes elliptiques (non singulières). On aura donc $E_{ns} = E$ et on ne se souciera plus des points singuliers. On se placera aussi en caractéristique plus grande que 5, de façon à pouvoir mettre le polynôme de Weierstrass de la courbe elliptique sous la forme :

$$f(X,Y) := Y^2-X^3-AX-B$$

avec $\Delta(E) = -16(A^3+27B^2) \neq 0$. A terme, nous travaillerons avec E définie sur $\mathbb{F}_q$ et nous calculerons le cardinal du groupe fini $E(\mathbb{F}_q)$, utilisé comme cryptosystème.

1.3 Le comptage de points sur les courbes elliptiques.

Maintenant que nous savons ce qu'est une courbe elliptique et que nous avons compris l'intérêt du comptage de points sur une courbe elliptique, nous présentons ici différents algorithmes ainsi que leurs complexités.

1.3.1 La formule de Lang-Trotter

La formule de Lang-Trotter est un algorithme naïf qui permet de calculer le cardinal d'une courbe définie sur $\mathbb{F}_p$ lorsque p est un petit nombre premier. Elle s'appuie sur la formule :

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + Ax + B}{p} \right)$$

. Ici, on utilise le **symbole de Legendre** c'est-à-dire :

$$\forall a \in \mathbb{F}_p, \quad \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$$

Cet algorithme ne s'applique pas tel quel dans $\mathbb{F}_2$ ni dans $\mathbb{F}_q$ mais des adaptations sont possibles. Quoi qu'il en soit, il nécessite $O(p)$ opérations (ou $O(q)$ quand on l'adapte dans $\mathbb{F}_q$), ce qui en fait un algorithme exponentiel. Il est donc loin d'être optimal.

1.3.2 La méthode de Shanks

La méthode de Shanks est un principe général qui permet de calculer le cardinal d'une groupe abélien fini. Pour l'appliquer, il suffit de connaître un majorant du cardinal et de savoir calculer la loi du groupe.

Soit E une courbe elliptique sur $\mathbb{F}_p$ de cardinal m. Par le théorème de Hasse que nous verrons plus tard [5], on a $|m - (p+1)| \leq 2\sqrt{p}$. On pose alors $S = 4\sqrt{p}$ et $r = \lceil \sqrt{S} \rceil$. L'idée est de calculer un entier n tel que $|n - (p+1)| \leq 2\sqrt{p}$ et $nP = 0$ où P est un point aléatoire de la courbe.

- **Pas de bébé :** On calcule P, 2P, ... rP
- **Pas de géant :** On calcule 2rP, 3rP, ... r^2P
- **Collision :** On calcule $H_i = (\lfloor p + 1 - 2\sqrt{q} \rfloor + jr)P \ \forall j \leq r$ et on cherche une collision du type $H_i = jP$. Grâce au théorème de Hasse, on sait qu'une telle collision a toujours lieu. Lorsque l'ordre de P est supérieur à $4\sqrt{q}$, il existe une unique collision et on a $m = \lfloor p+1-2\sqrt{q} \rfloor + ri - j$. Du travail supplémentaire est nécessaire afin de trouver un point P dont l'ordre est suffisamment grand.

La méthode de Shanks permet de calculer le cardinal d'une courbe elliptique définie sur $\mathbb{F}_p$ en $O(\sqrt[4]{p})$. Elle est adaptable dans F_q ($q = p^n$) mais sa complexité est exponentielle en n. Bien qu'elle soit sensiblement plus rapide que l'algorithme naïf, elle nécessite aussi $O(\sqrt[4]{p})$ emplacements mémoire disponible en mémoire vive !

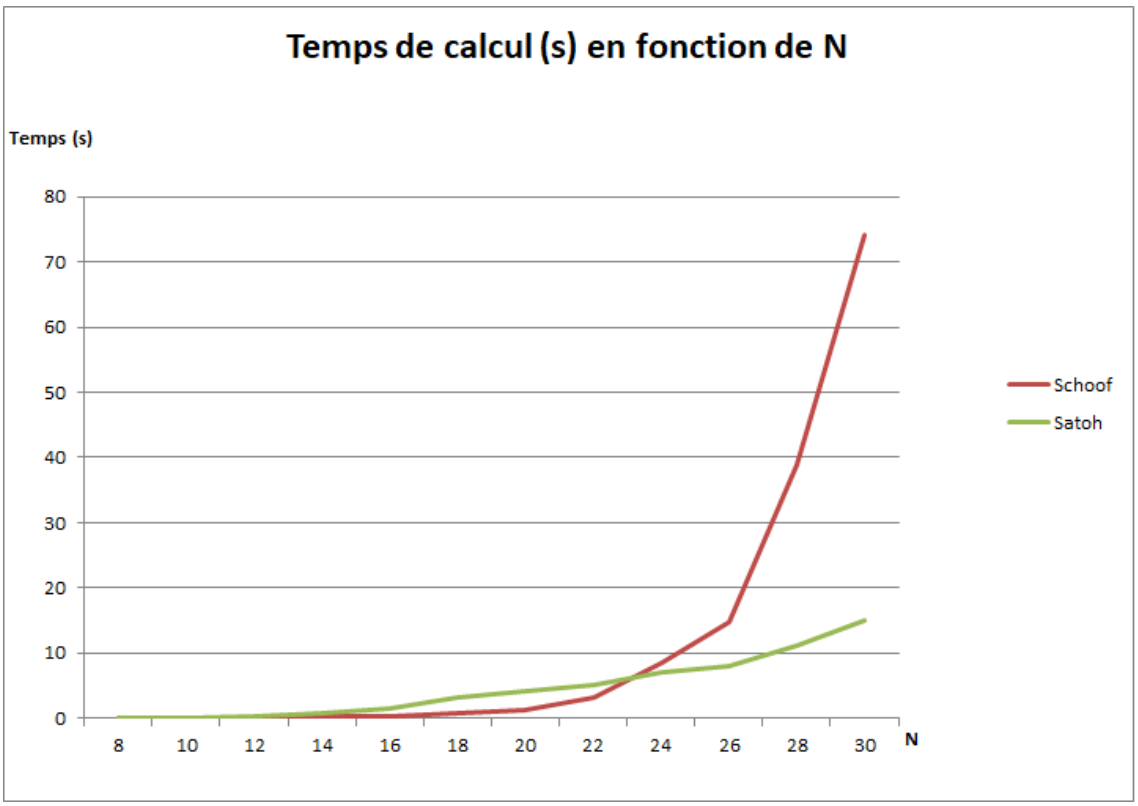
1.3.3 L'algorithme de Schoof

L'algorithme de Schoof est le premier algorithme polynomial (1985) qui répond à notre problème. Il consiste à calculer *mmodl* pour de petits nombres premiers l. Il est cependant trop complexe pour que l'on détaille ici son fonctionnement. Depuis sa parution, il fait l'objet de nombreuses études et d'innombrables raffinements. C'est d'ailleurs l'algorithme de School-Elkies-Atkin (SEA), considéré comme le meilleur, qui est implémenté sur Pari/GP. Il est efficace sur tout type de courbes et permet un calcul en $O(log(q)^4)$ opérations.

1.3.4 L'algorithme de Satoh

En 1999, Satoh, propose une méthode originale qui repose sur le relèvement dans $\mathbb{Q}_q$ et permet un calcul plus rapide en petite caractéristique. Ainsi, à $p \geq 5$ fixé, il permet un calcul en $O(n^{3+\epsilon})$ pour tout $\epsilon > 0$. En petite caractéristique, l'algrotithme de Satoh est donc bien meilleur que celui de Schoof. Dans notre PSC, nous avons décidé d'étudier l'algorithme de Satoh aussi aurons-nous l'occasion de le détailler plus tard dans le rapport. En attendant, voici une courbe qui compare les temps de calcul que nous avons obtenu avec l'algorithme que nous avons programmé, comparés avec l'algorithme SEA implémenté dans Sage.

5. théorème 3.8.2



Les valeurs indiquées ont été obtenues en effectuant une moyenne sur 20 mesures de temps. Lors de chaque mesure de temps, on tire aléatoirement deux coefficients A et B et on applique les deux algorithmes. Les écarts-types mesurés pour l'algorithme de Satoh sont très grands pour $N \leq 10$ (de l'ordre de 5 à 10%) mais négligeables dès que $N > 15$ (moins de 1%).

2 Relèvement p-adique du corps de base $\mathbb{F}_q$.

L'idée principale de Satoh consiste à résoudre le problème du comptage de points en se plaçant en caractéristique nulle, via un relèvement p-adique du problème. En effet, **le souci principal de $\mathbb{F}_q$ est que tous les calculs se font en caractéristique p non nulle ce qui présente une difficulté calculatoire (on perd de l'information dans les calculs). S'il existait un moyen de "conserver l'information contenue dans les restes modulo p", la tache serait simplifiée. D'où l'idée de travailler dans un corps plus gros (que nous baptiserons $\mathbb{Q}_q$) dont la réduction des éléments modulo p donne des éléments de $\mathbb{F}_q$. Dans cette section, nous présentons une construction de ce relèvement du corps de base $\mathbb{F}_q$.**

2.1 Généralités sur les corps valués.

Afin d'être plus adapté aux calculs modulo p, $\mathbb{Q}_q$ est muni d'une topologie particulière, distincte de la topologie archimédienne classique (sur $\mathbb{Q}$ et $\mathbb{R}$). L'idée est de partir de $\mathbb{Q}$ et de le munir de la topologie p-adique. Une fois ceci fait, on étend $\mathbb{Q}$ en un corps complet $\mathbb{Q}_p$.

$\mathbb{Q}_p$ se réduira en $\mathbb{F}_p$ (nous donnerons plus tard un sens à cette notion de réduction). Pour relever $\mathbb{F}_q$, il faudra prendre une "bonne" extension de $\mathbb{Q}_p$.

Dans ce paragraphe, nous présentons quelques généralités sur une classe de corps dont font partie $\mathbb{Q}_p$ et $\mathbb{Q}_q$: les corps valués.

2.1.1 Corps valués.

Définition 2.1.1. *Soit $\mathbb{K}$ un corps. On appelle* valuation *sur $\mathbb{K}$ une application $v : \mathbb{K} \longrightarrow \mathbb{R} \cup \{+\infty\}$ vérifiant pour tous $x, y \in \mathbb{K}$:*

(i). $v(x) = +\infty \Longleftrightarrow x = 0$.

(ii). $v(x \cdot y) = v(x) + v(y)$.

(iii). $v(x + y) \geq \min(v(x), v(y))$.

Un corps muni d'une valuation $(\mathbb{K}, v)$ est appelé corps valué.

On peut constater immédiatement que v induit un morphisme du groupe $(\mathbb{K}^*, \times)$ vers le groupe $(\mathbb{R}, +)$. Ainsi, $v(\mathbb{K}^*)$ est un sous-groupe de $(\mathbb{R}, +)$ qui est donc soit monogène (c'est à dire de la forme $a\mathbb{Z}$ avec $a > 0$) soit dense dans $\mathbb{R}$.

Définition 2.1.2. *L'application v est appelée* valuation discrète *lorsque $v(\mathbb{K}^*)$ est un sous-groupe monogène de $(\mathbb{R}, +)$.*

Définition 2.1.3. *On appelle norme sur $\mathbb{K}$ une application $|.| : \mathbb{K} \longrightarrow \mathbb{R}_+$ telle que pour tous $x, y \in \mathbb{K}$:*

(i). $|x| = 0 \Longleftrightarrow x = 0$.

(ii). $)|x \cdot y| = |x||y|$.

(iii). $|x + y| \leq |x| + |y|$.

Elle est dite ultramétrique*, si de plus la condition suivante, qui implique (iii). est réalisée :*

$$\forall x, y \in \mathbb{K}, \quad |x + y| \leq \max(|x|, |y|)$$

Remarque : Si $(\mathbb{K}, v)$ est un corps valué alors $x \longmapsto a^{v(x)}$ définit une norme ultramétrique pour tout $a \in]0, 1[$. Réciproquement, si $\mathbb{K}$ est muni d'une norme ultramétrique $|.|$ alors $x \longmapsto -b \ln |x|$ définit une valuation sur $\mathbb{K}$ pour tout $b > 0$.

Lemme 2.1.4 (topologie ultramétrique)**.** *On suppose ici que $|.|$ est ultramétrique. Alors :*

(i). *Si, $x, y \in \mathbb{K}$ vérifient $|x| \neq |y|$ alors $|x + y| = \max(|x|, |y|)$. En conséquence, si v est associée à $|.|$ et si $x, y \in \mathbb{K}$ vérifient $v(x) \neq v(y)$ alors $v(x + y) = \min(v(x), v(y))$.*

(ii). *Si $x_0 \in \mathbb{K}$ et $r > 0$ alors pour tout $x \in B(x_0, r)$, $B(x, r) = B(x_0, r)$. Autrement dit, tout point d'une boule est au centre de ladite boule.*

(iii). *Deux boules de $\mathbb{K}$ sont soit disjointes soit contenues l'une dans l'autre.*

(iv). *Les boules de $\mathbb{K}$ sont à la fois ouvertes et fermées.*

(v). *Les composantes connexes de $\mathbb{K}$ sont des singletons. On dira alors que* la topologie de $\mathbb{K}$ est complètement discontinue*.*

Démonstration. Voir annexe C.1.1 □

Exemples :
1). Dans $\mathbb{Q}$ on connait déjà des valuations. Si p est un nombre premier et n un entier relatif, on pose :

$$v_p(n) := \max\{k \in \mathbb{N} \mid p^k | n\}$$

et l'on peut étandre v_p à $\mathbb{Q}$ en posant pour tout $r \in \mathbb{Q}$, $v_p(r) := v_p(a) - v_p(b)$, $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ étant un représentant fractionnaire de r. Il est aisé de vérifier que cette définition ne dépend pas du représentant choisi et que v_p définit bien un valuation discrète sur $\mathbb{Q}$. On l'appelle valuation p-adique et on appelle norme p-adique la norme ultramétrique associée, définie par :

$$|x|_p := p^{-v_p(x)}$$

pour tout $x \in \mathbb{Q}$.
2). Dans le corps des fractions de l'anneau des séries formelles à coefficient dans un corps $\mathbb{K}$:

$$\mathbb{K}((X)) := \left\{ \sum_{n=-\infty}^{+\infty} a_n X^n \mid \forall n \in \mathbb{Z},\, a_n \in \mathbb{K} \text{ et } \exists n_0 \in \mathbb{Z},\, \forall n \leq n_0,\, a_n = 0 \right\}$$

on peut définir une valuation discrète en posant pour tout $f = \sum_{n=-\infty}^{+\infty} a_n X^n \in \mathbb{K}((X))$:

$$v_X(f) := \min\{n \in \mathbb{Z} \mid a_n \neq 0\}$$

Proposition 2.1.5. *Soit $(\mathbb{K}, v)$ un corps valué. On définit :*

$$O_{\mathbb{K},v} := \{x \in \mathbb{K} | v(x) \geq 0\} \quad \text{et} \quad M_{\mathbb{K},v} := \{x \in \mathbb{K} | v(x) > 0\}$$

Alors $O_{\mathbb{K},v}$ est un sous-anneau de $\mathbb{K}$ appelé anneau des entiers de $\mathbb{K}$ *et $M_{\mathbb{K},v}$ est un idéal maximal de $O_{\mathbb{K},v}$. Ainsi, le quotient $K_v := O_{\mathbb{K},v}/M_{\mathbb{K},v}$ est un corps appelé* corps résiduel *de $\mathbb{K}$.*

Démonstration. $O_{\mathbb{K},v}$ est stable par somme et produit d'après les points (ii). et (iii). de la définition d'une valuation. En outre, $v(1) = 0$ et $v(0) = +\infty$ donc $0, 1 \in O_{\mathbb{K},v}$. Donc est bien un sous-anneau de $\mathbb{K}$. Les points (ii). et (iii). de la définition d'une valuation assurent en outre que $M_{\mathbb{K},v}$ est stable par somme et par multiplication par tout élément de $O_{\mathbb{K},v}$. Comme $v(0) = +\infty$, on conclut que $M_{\mathbb{K},v}$ est bien un idéal de $O_{\mathbb{K},v}$.

Pour prouver la maximalité de $M_{\mathbb{K},v}$, il s'agit de montrer que $K_v = O_{\mathbb{K},v}/M_{\mathbb{K},v}$ est bien un corps. Soit $\overline{x} \in K_v^*$. Alors $\overline{x}$ admet un représentant x dans $O_{\mathbb{K},v} \setminus M_{\mathbb{K},v}$, qui est donc non nul et qui vérifie $v(x) = 0$. Mais alors $0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1}) = v(x^{-1})$ donc $x^{-1} \in O_{\mathbb{K},v} \setminus M_{\mathbb{K},v}$ et ainsi la classe de x^{-1} modulo $M_{\mathbb{K},v}$ est un inverse de $\overline{x}$ dans K_v. D'où le résultat. □

Remarque : La preuve précédente nous a permis d'obtenir aussi que le groupe des inversibles $\mathcal{U}(O_{\mathbb{K},v})$ de $O_{\mathbb{K},v}$ est $O_{\mathbb{K},v} \setminus M_{\mathbb{K},v}$, l'ensemble des éléments de valuation nulle.

En outre, l'équivalence entre norme ultramétrique et valuation nous assure que $O_{\mathbb{K},v} = B_f(0, 1)$ et $M_{\mathbb{K},v} = B(0, 1)$. Ce constat sera particulièrement utile dans la preuve du lemme de Hensel.

2.1.2 Anneaux de valuation discrète.

Nous présentons maintenant une classe de corps valués à laquelle appartiennent les corps p-adiques $(\mathbb{Q}_q, \mathbb{Q}_q)$. Le point de vu adopté ici consiste à s'intéresser d'abord à $O_{\mathbb{K},v}$ avant $(\mathbb{K}, v)$.

Définition 2.1.6. *On appelle anneau de valuation discrète un anneau commutatif principal (i.e. un anneau intègre dont tous les idéaux sont engendrés par un seul élément) admettant un unique idéal premier.*

Proposition 2.1.7. ***(i).*** *Soit $\mathbb{K}$ est un corps muni valuation discrète v. Alors $O_{\mathbb{K},v}$ est un anneau de valuation discrète et $\mathbb{K}$ est son corps de fractions.*

(ii). *Soient $\mathbb{A}$ est un anneau de valuation discrète et $\mathbb{K}$ son corps de fractions. Alors $\mathbb{A}$ n'admet qu'un seul élément irréductible r à multiplication par un inversible près. Tout élément x de $\mathbb{A}^*$ s'écrit alors de façon unique $x = ur^k$ avec u inversible dans $\mathbb{A}$ et $k \in \mathbb{N}$. On pose alors $v(x) := k$ et $v(0) = +\infty$. On étend facilement v à $\mathbb{K}$ en posant $v(y) = v(a) - v(b)$ pour tout $y \in \mathbb{K}$, $(a, b) \in \mathbb{A} \times \mathbb{A}^*$ étant un représentant fractionnaire de y. Cette définition est indépendante du représentant choisi, et on obtient ainsi une valuation discrète sur $\mathbb{K}$. Pour cette valuation, $\mathbb{A} = O_{\mathbb{K},v}$ et l'unique idéal premier de $\mathbb{A}$ est $M_{\mathbb{K},v} = r\mathbb{A}$.*

Démonstration. Voir annexe C.1.2. □

Remarque : Nous venons d'établir une équivalence entre corps muni d'une valuation discrète et anneau de valuation discrète. Nous venons en outre de prouver que l'irréductible r (unique à multiplication par un inversible près) qui engendre l'idéal maximal $M_{\mathbb{K},v}$ est toujours tel que $v(r)$ engendre le groupe $v(\mathbb{K}^*)$ et que réciproquement si $v(r)$ est un tel générateur alors r engendre toujours $M_{\mathbb{K},v}$.

Définition 2.1.8. *On appelle* uniformisante *un élément r qui engendre l'idéal maximal $M_{\mathbb{K},v}$ d'un anneau de valuation discrète $(\mathbb{K}, v)$.*

Le point de vue de [4] brièvement évoqué ici (partir des anneaux de valuation discrète au lieu des corps valués) permet de démontrer des résultats profonds à la croisée de la théorie des nombres et de la géométrie algébrique. Ayant pour ambition de démontrer le théorème de Deuring sur l'existence d'un relèvement p-adique canonique d'une courbe elliptique, qui nécessite de bien comprendre les isogénies, nous étions allé plus loin dans l'étude de ces notions. Désormais d'un intérêt limité pour nous puisque nous avons abandonné la preuve du théorème de Deuring (trop difficile à notre niveau), nous avons développé ces aspects dans l'annexe D. Notons toutefois qu'un résultat central de la théorie développée en annexe (la proposition D.3.7) sert à démontrer un théorème reliant degré d'une isogénie et ordre de cette isogénie en un point (voir proposition E.9.1).

2.1.3 Corps locaux et complétion.

Nous introduisons enfin la vraie notion intéressante pour les corps p-adiques.

Définition 2.1.9. *Un corps local est un corps valué complet pour une valuation discrète.*

La complétude est une propriété importante pour le calcul itératif, car elle assure la convergence des suites de Cauchy. Une grande partie du travail pour construire des corps locaux revient donc à compléter des corps déjà existants. Voyons comment faire cela.

Ce développement sur la complétion peut être sauté en première lecture (bien que l'omission des preuves l'ait rendu moins technique). Le lecteur pressé peut donc se reporter immédiatement aux exemples précédant la proposition 2.1.13. Dans ce paragraphe, on fixe $(\mathbb{K}, |.|)$ un corps normé, que l'on cherche à compléter. On note $\mathcal{C}(\mathbb{K})$ l'ensemble des suites de Cauchy à valeurs dans $\mathbb{K}$ et $0(\mathbb{K})$, l'ensemble des suites de $\mathbb{K}$ qui convergent vers 0 (on remarque immédiatement que $0(\mathbb{K}) \subset \mathcal{C}(\mathbb{K})$).

Lemme 2.1.10 (convergence des suites de $\mathcal{C}(\mathbb{K})$)**.** **(i).** *Si $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{K})$ alors $(|a_n|)_{n\in\mathbb{N}}$ converge dans $\mathbb{R}$.*

(ii). *Si $|.|$ est ultramétrique alors toute suite de $\mathcal{C}(\mathbb{K}) \setminus 0(\mathbb{K})$ est de norme constante à partir d'un certain rang.*

(iii). *Si $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{K})$ et si $(a_n - b_n)_{n\in\mathbb{N}} \in 0(\mathbb{K})$ alors $\lim\limits_{n\to+\infty} |a_n| = \lim\limits_{n\to+\infty} |b_n|$.*

Démonstration. Voir annexe C.1.3 □

Proposition 2.1.11. *$\mathcal{C}(\mathbb{K})$ est un anneau commutatif pour les lois $+$ et $\times$ dérivées de $\mathbb{K}$ et $0(\mathbb{K})$ en est un idéal maximal.*

Démonstration. Voir annexe C.1.3 □

Nous venons donc de voir que $\widehat{\mathbb{K}} := \mathcal{C}(\mathbb{K})/0(\mathbb{K})$ est un corps et que la norme $|.|$ de $\mathbb{K}$ peut s'étendre à $\widehat{\mathbb{K}}$ tout entier d'après le point *(iii)*. du lemme C.1.6, en posant pour tout $\overline{a} \in \widehat{\mathbb{K}}$, $|\overline{a}| = \lim\limits_{n\to+\infty} |a_n|$ 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 $\overline{a} \in \widehat{\mathbb{K}}$ 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. $a \in 0(\mathbb{K})$ 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 2.1.12. *$(\widehat{\mathbb{K}}, |.|)$ est un surcorps normé complet de $\mathbb{K}$ et $\mathbb{K}$ est dense dans $\widehat{\mathbb{K}}$. Pour cette raison, $\widehat{\mathbb{K}}$ est appelé* complété de $\mathbb{K}$.

Démonstration. Voir annexe C.1.3 □

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 $v(\mathbb{K}^*) = a\mathbb{Z}$. Ainsi, $v(\mathbb{K}^*)$ est fermé et $v(\widehat{\mathbb{K}}^*)$ qui n'est, par construction, rien d'autre que l'adhérence de $v(\mathbb{K}^*)$ est égal à $v(\mathbb{K}^*)$. Donc le prolongement de la valuation $\mathbb{K}$ à $\widehat{\mathbb{K}}$ reste discret.

Exemples :

1). $\mathbb{R}$ est le complété de $\mathbb{Q}$ pour la norme usuelle. Cependant, $\mathbb{R}$ muni de la norme usuelle n'est pas un corps local.

2). Pour tout nombre premier p on désignera par $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la norme p-adique $|.|_p$ définie en annexe. On l'appelle *corps des nombres p-adiques* C'est un corps local car v_p est une valuation discrète. On note $\mathbb{Z}_p = O_{\mathbb{Q}_p,v_p}$ son anneau d'entiers appelé *anneau des entiers p-adiques.*

Cet exemple est fondammental tant pour la théorie des corps locaux que pour les applications qui nous intéressent. Nous avons travaillé pour cela. Enonçons quelques résultats sur le corps $\mathbb{Q}_p$.

Proposition 2.1.13. *L'idéal maximal de $\mathbb{Z}_p$ est $M_{\mathbb{Q}_p,v_p} = p\mathbb{Z}_p$.*

Démonstration. $v_p(\mathbb{Q}_p^*) = v_p(\mathbb{Q}^*) = \mathbb{Z}$ donc $v_p(p) = 1$ engendre $v_p(\mathbb{Q}_p^*)$ et p est une uniformisante (voir dernière remarque du paragraphe précédent). Ainsi, $M_{\mathbb{Q}_p,v_p} = p\mathbb{Z}_p$. □

Proposition 2.1.14. *Le corps résiduel de $\mathbb{Q}_p$ est $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. On a $1 \in \mathbb{Z}_p$ car $v_p(1) = 0$ donc $\mathbb{Z} \subset \mathbb{Z}_p$ et ainsi, deux entiers congrus modulo p dans $\mathbb{Z}$ sont aussi congrus modulo p dans $\mathbb{Z}_p$, ce qui donne l'inclusion $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}_p/p\mathbb{Z}_p$.

Réciproquement, soient $\overline{x} \in \mathbb{Z}_p/p\mathbb{Z}_p$ et $x \in \mathbb{Z}_p$ un de ses représentants. Par densité de $\mathbb{Q}$ dans $\mathbb{Q}_p$ (prouvée dans le théorème C.1.8), on dispose de $r \in \mathbb{Q}$ tel que $v_p(x - r) \geq 1$. Mais alors $v_p(r) \geq 0$ car sinon, on aurait $v_p(r) < 0 \leq v_p(x)$ et donc $v_p(x - r) = \min(v_p(x), v_p(r)) = v_p(r) < 0$ d'après le lemme 2.1.4. Ecrivons $r := \frac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors $v_p(a) \geq v_p(b)$ donc quitte à diviser numérateur et dénominateur par $p^{v_p(b)}$, on peut supposer $v_p(b) = 0$ et $v_p(a) = v_p(r)$. b est donc premier avec p donc inversible modulo p d'après le théorème de Bézout et on dispose alors de $c \in \mathbb{N}$ tel que $bc \equiv 1\,[p]$. Mais alors :

$$v_p(r - ac) = v_p\left(a\frac{1 - bc}{b}\right) = v_p(a) + v_p(1 - bc) - v_p(b) = v_p(a) + v_p(1 - bc)$$

Avec $v_p(a) = v_p(r) \geq 0$ et $v_p(1 - bc) \geq 1$ vu que $bc \equiv 1\,[p]$. Ainsi, $v_p(r - ac) \geq 1$ et donc :

$$v_p(x - ac) = v_p((x - r) + (r - ac)) \geq \min(v_p(x - r), v_p(r - ac)) \geq 1$$

Donc $\overline{ac} \in \mathbb{Z} \subset \mathbb{Z}_p$ et $\overline{x} = \overline{ac}$ dans $\mathbb{Z}/p\mathbb{Z}$. D'où l'inclusion réciproque. □

Remarque : On a déjà obtenu un premier résultat simple en vu des applications ultérieures : on sait comment relever $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Terminons ce paragraphe avec un résultat de structure des corps locaux.

Théorème 2.1.15. *Soient $\mathbb{K}$ un corps local de corps résiduel K, r une uniformisante et $S(K)$ un système de représentants des éléments de K modulo $rO_{\mathbb{K},v}$. Supposons que $v(r) = 1$. Alors tout élément $x \in \mathbb{K}^*$ s'écrit de manière unique sous la forme :*

$$x = \sum_{n=v(x)}^{+\infty} a_n r^n$$

où $(a_n)_{n \geq v(x)}$ est une suite d'éléments de $S(K)$.

Démonstration. Soit $x \in \mathbb{K}^*$. Alors $x_0 := r^{-v(x)}x \in O_{\mathbb{K},v}$. On peut donc considérer $b_0 \in K$, la réduction de x_0 modulo $rO_{\mathbb{K},v} = M_{\mathbb{K},v}$. Puis, comme $x_0 - b_0 \in rO_{\mathbb{K},v}$, $x_1 := \frac{x_0 - b_0}{r} \in O_{\mathbb{K},v}$ donc on peut considérer b_1, la réduction de x_1 modulo $rO_{\mathbb{K},v} = M_{\mathbb{K},v}$. On définit alors par récurrence les suites $(x_k)_{k\in\mathbb{N}} \in O_{\mathbb{K},v}^{\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}} \in S(K)^{\mathbb{N}}$ déjà initialisées en posant pour tout $k \in \mathbb{N}$:

$$x_{k+1} := \frac{x_k - b_k}{r} \quad \text{et} \quad b_k := x_k \bmod rO_{\mathbb{K},v}$$

On obtient aisément par récurrence que pour tout $k \in \mathbb{N}$:

$$x_0 = \sum_{i=0}^{k-1} b_i r^i + x_k r^k$$

Avec $v(x_k r^k) \geq k$ donc $x_k r_k \underset{k\to+\infty}{\longrightarrow} 0$. Ainsi, la série $\sum_{k\geq 0} b_k r^k$ converge vers $x_0 = r^{-\frac{v(x)}{v(r)}} x$ dans $\mathbb{K}$ et on obtient bien l'existence de la suite $(a_n)_{n\geq \frac{v(x)}{v(r)}}$ désirée en posant pour tout $n \geq v(x)$, $a_n := b_{n+v(x)}$.

Pour montrer l'unicité de la suite $(a_n)_{n\geq v(x)}$, il suffit de montrer l'unicité de la suite $(b_k)_{k\in\mathbb{N}}$ associée. Soit donc $(c_k)_{k\in\mathbb{N}} \in S(K)^{\mathbb{N}}$ telle que $x_0 = \sum_{k=0}^{+\infty} c_k r^k = \sum_{k=0}^{+\infty} b_k r^k$. Alors en réduisant cette égalité modulo $rO_{\mathbb{K},v}$ on obtient que $c_0 = b_0$, puis en supposant que $c_0 = b_0, \cdots, b_k = c_k$ pour $k \in \mathbb{N}$ et en réduisant l'égalité modulo $r^{k+1}O_{\mathbb{K},v}$, on obtient que $c_{k+1} = b_{k+1}$. On en déduit donc l'unicité par récurrence. □

Exemple : Nous venons d'obtenir en particulier que tout élément x de $\mathbb{Q}_p^*$ s'écrit de manière unique comme série :

$$x = \sum_{n=v_p(x)}^{+\infty} a_n p^n$$

où $(a_n)_{n\geq v_p(x)}$ est une suite d'éléments de $S(\mathbb{Z}/p\mathbb{Z}) = \{0, \cdots, p-1\}$.

Nous avons même une méthode algorithmique pour trouver cette série. Regardons par exemple l'écriture de -1 dans $\mathbb{Z}_p$. L'unique élément de $\{0, \cdots, p-1\}$ qui relève $\overline{-1}$ est $p-1$, puis l'unique élément de $\{0, \cdots, p-1\}$ qui relève $\frac{\overline{-1-(p-1)}}{p} = \overline{-1}$ est $p-1$ etc. On en déduit :

$$-1 = \sum_{n=0}^{+\infty} (p-1)p^n$$

dans $\mathbb{Z}_p$.

Cette écriture semble bien pratique mais elle présente toutefois une difficulté technique. Si l'on veut additionner et multiplier dans $\mathbb{Q}_p$, on ne peut pas simplement le faire terme à terme ou avec un produit de Cauchy. Il faut faire en sorte que les coefficients restent dans $\{0, \cdots, p-1\}$, ce qui revient à reporter des retenues de chaque coefficient sur les suivants. Nous n'implémenterons pas cela nous-même car il existe des algorithmes efficaces pour le faire déjà implémentés en Sage.

Trève de considérations pratiques. Soit $x \in \mathbb{Z}_p$. On peut alors écrire (quitte à prendre les premiers termes nuls) :

$$x = \sum_{n=0}^{+\infty} a_n p^n$$

On remarque alors que $x = \lim_{n\to+\infty} x_n$ pour la topologie induite par la valuation p-adique, avec :

$$\forall n \in \mathbb{N}, \quad x_n := \sum_{k=0}^{n} a_k p^k$$

On peut en outre remarquer que pour tous entiers $m \leq n$, on a $x_m \equiv x_n \,[p^{m+1}]$. On constate donc que $\mathbb{Z}_p$ a une structure de limite projective au sens de la définition suivante :

Définition 2.1.16. *Soient $(I, \leq)$ un ensemble totalement ordonné et $(E_i)_{i\in I}$ une famille d'ensembles telle que pour tout $i, j \in I$ tels que $i \leq j$, il existe une fonction $f_j^i : E_j \longrightarrow E_i$, la famille de fonctions $(f_j^i)_{\substack{i,j\in I \\ i\leq j}}$ vérifiant :*

$$\forall i, j, k \in I, i \leq j \leq k \Longrightarrow f_j^i \circ f_k^j = f_k^i$$

On dit alors que $\left((E_i)_{i\in I}, (f_j^i)_{\substack{i,j\in I \\ i\leq j}}\right)$ est un système projectif *et on appelle* limite projective de $(E_i)_{i\in I}$ *l'ensemble :*

$$\varprojlim E_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} E_i \mid \forall i, j \in I, i \leq j \Longrightarrow x_i = f_j^i(x_j) \right\}$$

Considérons le système projectif $\left((\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}^*}, (f_m^n)_{\substack{n,m\in\mathbb{N}^* \\ n\leq m}}\right)$ où pour tous $n, m \in \mathbb{N}^*$ tels que $n \leq m$, $f_m^n : \mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ est la réduction modulo p^{n+1}. Alors nous venons de voir que :

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

On pourrait travailler avec cette définition pour $\mathbb{Z}_p$.

2.2 Polynômes dans les corps locaux, lemme de Hensel.

Supposons que l'on connaisse une racine d'un polynôme modulo p (par exemple dans $\mathbb{F}_p$). La question est de savoir comment relever cette racine dans un corps p-adique (par exemple $\mathbb{Q}_p$). Ceci est un point crucial pour les calculs de satoh, mais aussi pour la construction de $\mathbb{Q}_q$.

Dans tout ce paragraphe, $(\mathbb{K}, v)$ sera un corps valué complet, même lorsque ce n'est pas précisé dans les hypothèses des résultats énoncés.

Théorème 2.2.1 (Hensel)**.** *Soient $(\mathbb{K}, v)$ un corps valué complet et $P \in O_{\mathbb{K},v}[X]$. On suppose qu'il existe $x \in O_{\mathbb{K},v}$ tel que $|P(x)| < |P'(x)|^2$. Alors il existe $\xi \in O_{\mathbb{K},v}$, une racine de P telle que $|x - \xi| \leq \left|\frac{P(x)}{P'(x)}\right| < |P'(x)|$. C'est par ailleurs la seule racine de P contenue dans $B(x, |P'(x)|)$.*

Démonstration. Voir annexe C.2. □

Remarque : Ce théorème possède une application algorithmique qui permet de trouver la racine ξ. C'est une simple application de la méthode de Newton que le lecteur peut trouver en annexe.

On peut traduire cette version technique du lemme de Hensel en terme de relèvement de racines.

Corollaire 2.2.2. *Soient $P \in O_{\mathbb{K},v}[X]$ unitaire et $\overline{P}$ sa réduction modulo $M_{\mathbb{K},v}$. Supposons que $\overline{P}$ admette une racine simple $\overline{\alpha}$ dans K_v (le corps résiduel de $\mathbb{K}$). Alors il existe une unique racine $\alpha \in O_{\mathbb{K},v}$ de P dont la réduction modulo $M_{\mathbb{K},v}$ soit égale à $\overline{\alpha}$.*

Démonstration. Prenons $\alpha_0 \in O_{\mathbb{K},v}$ un représentant de $\overline{\alpha}$ modulo $M_{\mathbb{K},v}$. Alors modulo $M_{\mathbb{K},v}$: $\overline{P(\alpha_0)} = \overline{P}(\overline{\alpha}) = \overline{0}$ et donc $P(\alpha_0) \in M_{\mathbb{K},v}$, de sorte que $|P(\alpha_0)| < 1$. En outre, $\overline{P'(\alpha_0)} = \overline{P}'(\overline{\alpha}) \neq \overline{0}$ car $\overline{\alpha}$ est racine simple de $\overline{P}$. Ainsi, $P'(\alpha_0) \in O_{\mathbb{K},v} \setminus M_{\mathbb{K},v}$ et ainsi $|P'(\alpha_0)| = 1$. Donc $\left|\frac{P(\alpha_0)}{P'(\alpha_0)^2}\right| < 1$ et le lemme de Hensel assure l'existence d'un unique $\alpha \in B(\alpha_0, |P'(\alpha_0)|) \cap O_{\mathbb{K},v} = B(\alpha_0, 1) \cap O_{\mathbb{K},v}$ tel que $P(\alpha) = 0$. On peut donc écrire $\alpha = \alpha_0 + h$ avec $h \in B(0,1) = M_{\mathbb{K},v}$ donc la réduction modulo $M_{\mathbb{K},v}$ de α vaut bien $\overline{\alpha_0} = \overline{\alpha}$.

En outre, si $\beta \in O_{\mathbb{K},v}$ vérifie les mêmes hypothèses alors $\overline{\beta} = \overline{\alpha}$ modulo $M_{\mathbb{K},v}$ donc d'après le point (ii). du lemme 2.1.4, $\beta \in B(\alpha, 1) \cap O_{\mathbb{K},v} = B(\alpha_0, 1) \cap O_{\mathbb{K},v}$ et ainsi $\beta = \alpha$ par unicité d'un tel $\alpha \in B(\alpha_0, 1) \cap O_{\mathbb{K},v}$. □

On pourra trouver en annexe C.2 quelques compléments sur le relèvement de facteurs polynomiaux (et non plus seulement de racines).

Nous terminons ce paragraphe par des considérations très utiles sur les polynômes à coefficients dans $\mathbb{K}$, et sur les $\mathbb{K}$-espaces vectoriels de dimension finie.

Définition 2.2.3. *Pour tout $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$, on définit la* valuation de Gauss *de P par :*

$$v_G(P) := \min_{0 \leq i \leq n} v(a_i)$$

Remarque : On peut facilement vérifier que la valuation de Gauss suit les axiomes (i). et (iii). d'une valuation sur $\mathbb{K}[X]$, l'axiome (ii). étant remplacé par un axiome de sous-multiplicativité. Cet axiome (ii). est cependant vérifié lorsque la valuation v sur $\mathbb{K}$ est discrète.

On peut associer une norme à v_G en prenant $\|.\| := a^{v_G}$ pour $a \in]0,1[$. Mais $\mathbb{K}[X]$ ne peut pas être un corps normé car ce n'est pas un corps. C'est en fait un $\mathbb{K}$-espace vectoriel normé au sens suivant (tout à fait analogue à celui de $\mathbb{R}$ et $\mathbb{C}$) :

Définition 2.2.4. *Si $(\mathbb{K}, |.|)$ est un corps normé, et si E est un $\mathbb{K}$-espace vectoriel on dit que $\|.\| : E \longrightarrow \mathbb{R}_+$ est une norme sur E lorsqu'elle vérifie pour tous $x, y \in E$ et $\lambda \in \mathbb{K}$:*

(i). $\|x\| = 0 \iff x = 0$.

(ii). $\|\lambda \cdot x\| = |\lambda| \|x\|$.

(iii). $\|x + y\| \leq \|x\| + \|y\|$.

On retrouve alors plein de résultats qui sont vrais sur $\mathbb{R}$ et $\mathbb{C}$ lorsque $\mathbb{K}$ est complet (hypothèse faite dans tout le présent paragraphe). Entre autres, on peut étendre la définition d'un espace de Banach comme $\mathbb{K}$-espace vectoriel normé complet et obtenir qu'ainsi le théorème du point fixe de Banach reste vrai avec les mêmes hypothèses. De même, on peut aussi montrer que toutes les normes sont équivalentes en dimension finie.

Finissons cette remarque en notant que, sur $\mathbb{K}_n[X]$, il est facile de vérifier que si $\mathbb{K}$ est complet pour v alors $\mathbb{K}_n[X]$ est complet pour v_G. Ces constats sont importants pour la suite.

Terminons ce paragraphe avec un lemme que nous utiliserons pour prolonger les valuations dans le paragraphe qui suit :

Lemme 2.2.5. *Soit $P \in \mathbb{K}[X]$ irréductible tel que $P(0) \in O_{\mathbb{K},v}$. Alors $P \in O_{\mathbb{K},v}[X]$.*

Démonstration. Voir annexe C.2 □

2.3 Extension non ramifiée de corps locaux et application au relèvement de $\mathbb{F}_q$.

Nous avons vu au paragraphe 2.1.3 comment relever $\mathbb{F}_p$, en construisant le corps local $\mathbb{Q}_p$. Nous savons que $\mathbb{F}_q$ est une extension finie de degré n de $\mathbb{F}_p$ (avec la convention habituelle $q = p^n$). Il est donc naturel de prendre une extension finie de degré n de $\mathbb{Q}_p$ pour relever $\mathbb{F}_q$. Cela pose cependant des difficultés techniques, comme par exemple le prolongement de la valuation p-adique, que nous traiterons dans le paragraphe qui suit.

2.3.1 Prolongement d'une valuation.

Introduisons tout d'abord un outil technique pour prolonger la valuation d'un corps valué.

Définition 2.3.1. *Soit $\mathbb{L}$ une extension finie d'un corps $\mathbb{K}$. Pour tout $x \in \mathbb{L}$, on définit* la norme de x sur $\mathbb{L}$, *notée $N_{\mathbb{L}/\mathbb{K}}(x)$, et* la trace de x sur $\mathbb{L}$, *notée $T_{\mathbb{L}/\mathbb{K}}(x)$, respectivement comme le déterminant et la trace de l'endomorphisme $\mathbb{K}$-linéaire $y \in \mathbb{L} \longmapsto xy \in \mathbb{L}$.*

En fait, c'est à partir de la norme de $N_{\mathbb{L}/\mathbb{K}}$ que nous définirons la norme prolongée sur $\mathbb{L}$. Voyons maintenant un calcul de cette quantité.

Lemme 2.3.2. *Si l'on note a_0 le coefficient constant du polynôme minimal de $x \in \mathbb{L}$ sur $\mathbb{K}$ et d son degré, alors $d|[\mathbb{L} : \mathbb{K}]$,*

$$N_{\mathbb{L}/\mathbb{K}}(x) = (-1)^{[\mathbb{L}:\mathbb{K}]} a_0^{[\mathbb{L}:\mathbb{K}]/d} \quad \text{et} \quad T_{\mathbb{L}/\mathbb{K}}(x) = -\frac{[\mathbb{L} : \mathbb{K}] a_{d-1}}{d}$$

Démonstration. Voir annexe C.3.1 □

Avant d'aborder le prolongement de la valuation, commençons par caractériser l'équivalence des normes sur un corps normé.

Définition 2.3.3. *On dira que deux normes sur un corps normé sont équivalentes si elles définissent la même topologie (i.e. les mêmes ouverts et les mêmes fermés).*

Proposition 2.3.4. *Soit $\mathbb{K}$ un corps muni de deux normes $|.|_1$ et $|.|_2$. Alors $|.|_1$ et $|.|_2$ sont équivalentes si et seulement si il existe $\alpha \in \mathbb{R}_+^*$ tel que $|.|_2 = |.|_1^\alpha$.*

Démonstration. Voir annexe C.3.1 □

Théorème 2.3.5 (prolongement des valuations)**.** *Soient $(\mathbb{K}, v)$ un corps valué complet et $\mathbb{L}$ une extension finie de $\mathbb{K}$. Alors v se prolonge de manière unique en $\tilde{v}$ sur $\mathbb{L}$ donnée par :*

$$\tilde{v}(x) = \frac{1}{[\mathbb{L} : \mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(x))$$

pour tout $x \in \mathbb{L}$.

Démonstration. Voir annexe C.3.1 □

Corollaire 2.3.6. *Soit $\overline{\mathbb{K}}$ la clôture algébrique du corps valué $(\mathbb{K}, v)$. Alors il existe une unique manière de prolonger v à $\overline{\mathbb{K}}$.*

Démonstration. Si $x \in \overline{\mathbb{K}}$, alors $\mathbb{K}[x]$ est une extension finie de $\mathbb{K}$ puisque x est algébrique. Donc il n'y a qu'un seul prolongement de v à $\mathbb{K}[x]$ d'après la proposition précédente, défini par $v(x) := v(N_{\mathbb{K}[x]/\mathbb{K}}(x))$. Ceci étant vrai pour tout $x \in \overline{\mathbb{K}}$, on en déduit immédiatement l'existence et l'unicité. □

2.3.2 Extension non-ramifiée d'un corps local et relèvement de $\mathbb{F}_q$.

Dans ce paragraphe, on fixe $(\mathbb{K}, v)$ un corps local dont le corps résiduel K est parfait (c'est à dire un corps de caractéristique nulle ou de caractéristique non nulle dont le morphisme de Frobenius est surjective). On fixe aussi $\mathbb{L}$ une extension finie de $\mathbb{K}$ dont on note L le corps résiduel (pour la valuation qui prolonge v sur $\mathbb{L}$, encore notée v). v étant fixée, la dépendance en v de $O_{\mathbb{K},v}$, $M_{\mathbb{K},v}$ etc... ne sera plus précisée.

Proposition 2.3.7. *L est une extension finie de K de degré au plus $[\mathbb{L} : \mathbb{K}]$.*

Démonstration. Voir annexe C.3.2 □

Définition 2.3.8. *On dit que $\mathbb{L}/\mathbb{K}$ est une extension* non-ramifiée *lorsque $[\mathbb{L} : \mathbb{K}] = [L : K]$.*

Théorème 2.3.9. *Soit M une extension finie d'un corps parfait K, corps résiduel de $\mathbb{K}$. Alors il existe une extension finie non-ramifiée $W(M)/\mathbb{K}$ de corps résiduel M.*

Démonstration. Comme ce résultat est crucial, nous en donnons la preuve ici même. K étant un corps parfait et M étant une extension finie de K, le théorème de l'élément primitif (tel qu'il est énoncé dans [6]) assure l'existence de $\overline{\alpha} \in M$ tel que $M = K[\overline{\alpha}]$. Soit $\overline{P}$ le polynôme minimal de $\overline{\alpha}$ sur K et $P \in O_{\mathbb{K}}[X]$ un représentant unitaire de $\overline{P}$ modulo $M_{\mathbb{K}}$.

Alors comme $\overline{P}$ est irréductible dans $K[X]$, P est aussi irréductible dans $O_{\mathbb{K}}[X]$. En effet, si $P = QR$ avec $Q, R \in O_{\mathbb{K}}[X]$ et $1 \leq \deg(Q), \deg(R) \leq \deg(P)$ alors $\overline{P} = \overline{Q}\overline{R}$ avec $1 \leq \deg(\overline{Q}), \deg(\overline{R}) \leq \deg(\overline{P})$, car P étant unitaire, les coefficients dominants de Q et R sont inversibles donc non nuls modulo $M_{\mathbb{K}}$. P est donc irréductible dans $\mathbb{K}[X]$. En effet, si $Q, R \in \mathbb{K}[X]$ vérifient $P = QR$ avec $1 \leq \deg(Q), \deg(R) \leq \deg(P)$, alors on a $v_G(QR) = v_G(P) \geq 0$. Or, v étant une valuation discrète $v_G(QR) = v_G(Q) + v_G(R)$ (d'après la remarque qui suit la définition d'une valuation de Gauss, faite en 2.2) et l'on dispose d'une uniformisante r sur $\mathbb{K}$. Donc quitte à quitte à multiplier Q par $r^{-v_G(Q)}$ et R par $r^{v_G(Q)}$, on peut supposer que $v_G(Q), v_G(R) \geq 0$, donc que $Q, R \in O_{\mathbb{K}}[X]$. Ceci contredit l'irréductibilité de P sur $O_{\mathbb{K}}[X]$.

Ainsi, $\mathbb{M} := \mathbb{K}[X]/(P)$ est un corps et une extension finie de $\mathbb{K}$ de degré $\deg(P) = [M : K]$. Mais alors le corps résiduel $\tilde{M}$ de $\mathbb{M}$ (muni de la valuation v qui prolonge celle de $\mathbb{K}$) contient ζ, la classe du monôme X de $K[X]$ modulo $\overline{P}$ (réduite de P modulo $M_{\mathbb{K}}$, qui coïncide avec celle modulo $M_{\mathbb{M}}$). Ainsi $K[\zeta] \subset \tilde{M}$. Mais ζ est une racine de $\overline{P}$, qui est irréductible et unitaire, donc égal au polynôme minimal de ζ. Ainsi, $[\tilde{M} : K] \geq [K[\zeta] : K] = \deg(P) = [M : K]$ et d'après la proposition précédente $[\tilde{M} : K] \geq [\mathbb{M} : \mathbb{K}] = [M : K]$. Donc $\tilde{M}$ est une extension de degré $[M : K]$ de K, que l'on peut donc identifier à M. Ains, $\mathbb{M}/\mathbb{K}$ est non ramifiée et on peut poser $W(M) := M$. □

Application : Nous pouvons donc appliquer le travail entrepris au cas qui nous intéresse. On prend $\mathbb{K} := \mathbb{Q}_p$, qui est un corps local lorsqu'il est muni de la valuation p-adique v_p. $\mathbb{Q}_p$ a pour corps résiduel $K = \mathbb{F}_p$, qui est parfait. On sait que $\mathbb{F}_q$ est une extension finie de degré n de $\mathbb{F}_p$ (car $q = p^n$). Le théorème précédent assure alors l'existence de $W(\mathbb{F}_q)$, une extension non-ramifiée de $\mathbb{Q}_p$ (donc de degré n), de corps résiduel $\mathbb{F}_q$.

Pour simplifier on notera $\mathbb{Q}_q := W(\mathbb{F}_q)$ et $\mathbb{Z}_q := O_{W(\mathbb{F}_q)}$ son anneau d'entiers.

Terminons avec la notion d'extension non ramifiée maximale, que Satoh utilise aussi dans son article.

Définition 2.3.10. *Soit $\mathbb{K}$ un corps local de corps résiduel parfait K. Considérons l'ensemble $\mathcal{E}(K)$ de toutes les extensions finies L de K dans $\overline{K}$, la clôture algébrique de K. Alors on appelle extension non ramifiée maximale de $\mathbb{K}$, et on note $\mathbb{K}^{nr}$ l'ensemble :*

$$\mathbb{K}^{nr} := \bigcup_{L \in \mathcal{E}(K)} W(L)$$

Proposition 2.3.11. *$\mathbb{K}^{nr}$ est un sous-corps de $\overline{\mathbb{K}}$, la clôture algébrique de $\mathbb{K}$.*

Démonstration. Voir annexe C.3.2 □

Remarque : Nous avons vu au paragraphe précédent que l'on pouvait prolonger la valuation v définie sur $\mathbb{K}$ de façon unique sur $W(L)$ pour toute extension L finie de K ($W(L)$ étant une extension finie de $\mathbb{K}$). On peut donc prolonger v de façon unique sur $\mathbb{K}^{nr}$ vu son écriture, ce qui fait de $\mathbb{K}^{nr}$ un corps valué.

Introduisons enfin un lemme qui nous servira pour établir certains résultats techniques de Satoh.

Lemme 2.3.12. *Soit $P \in O_{\mathbb{K}}[X]$ un polynôme unitaire dont la réduction $\overline{P}$ modulo $M_{\mathbb{K}}$ est sans facteur carré. Alors toutes les racines de P sont dans $O_{\mathbb{K}^{nr}}$.*

Démonstration. Voir annexe C.3.2 □

⋆

Nous avons introduit ici un prérequis d'algèbre majeur : la construction de $\mathbb{Q}_q$. Nous nous servirons aussi beaucoup de la notion d'anneau de valuation discrète au cours du rapport. Le lecteur pourra trouver d'autres développements d'algèbres assez généraux dans les annexes B et D. Mais il est grand temps de rentrer dans le vif du sujet en nous concentrant plus spécifiquement sur les courbes elliptiques.

3 Isogénies et géométrie algébrique élémentaire sur les courbes elliptiques.

Cette section est le coeur mathématique du sujet car elle comprend en substance, toute les propriétés algébriques et géométriques des courbes elliptiques. Il s'agit d'étudier des fonctions rationnelles définies sur une courbe elliptique, à partir desquelles on peut notamment caractériser la structure de groupe de cette courbe (voir théorème 3.2.11) et définir des morphismes entre courbes elliptiques. Ces morphismes enrichissent la structure et donnent des informations sur les courbes elliptiques. Sur les corps finis par exemple, l'étude de certains de ces morphismes donne accès au nombre de points (théorème de Hasse). Pour comprendre l'algorithme de satoh, la géométrie algébrique en genre 1 est donc un passage obligé.

Au départ, notre référence sur le sujet était [7]. Mais le haut niveau de connaissance mathématique attendu du lecteur sur le sujet ainsi que le renvoi récurrent à des ouvrages généraux et très difficiles de géométrie algébrique nous ont empêché de saisir les concepts introduits en profondeur. Depuis le précédent rapport, nous avons trouvé une référence plus accessible que [7] pour introduire ces prérequis de géométrie algébrique. Cette référence [8], est en fait un cours donné à l'Université Paris VIII qui introduit ces notions de façon élémentaire en substituant les résultats d'algèbre profonds au calcul, ce qui a le mérite de les clarifier à ce stade de nos études. La plupart des résultats seront donc prouvés en annexe E, à l'exception de ceux qui sont manifestement trop calculatoires.

Dans toute cette section, $\mathbb{K}$ désignera un corps de caractéristique différente de 2 et 3 [6] et E une courbe elliptique sur $\mathbb{K}$. On sait qu'alors le polynôme de Weierstrass associée à E peut s'écrire :

$$W(X,Y) = Y^2 - X^3 - AX - B$$

avec $A, B \in \mathbb{K}$ et $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$.

3.1 Fonctions rationnelles définies sur E.

3.1.1 Généralités.

Remarquons tout d'abord que le polynôme de Weierstrass W est irréductible dans $\mathbb{K}[X,Y]$. En effet, sinon, on aurait une factorisation de la forme $W(X,Y) = (Y - p(X))(Y - q(X))$ avec $p, q \in \mathbb{K}[X]$ et donc on aurait :

$$p(X)q(X) = X^3 + AX + B \quad \text{et} \quad p(X) + q(X) = 0$$

Donc p et q ont même degré, ce qui est incompatible avec le fait que pq soit de degré 3. Ainsi, l'anneau :

$$\mathbb{K}[E] = \mathbb{K}[X,Y]/(W(X,Y))$$

des classes de polynômes modulo l'annulation sur E est un anneau intègre.

Définition 3.1.1. *On appelle* anneau des polynômes sur E *l'anneau* $\mathbb{K}[E]$. *Son corps de fractions, noté* $\mathbb{K}(E)$ *est appelé* corps des fonctions *de* E.

Commençons par voir à quoi ressemblent les polynômes sur E :

Proposition 3.1.2. *Si* $f \in \mathbb{K}[E]$ *alors il existe un unique couple* $(p,q) \in \mathbb{K}[X]^2$ *tel que :*

$$f(X,Y) = p(X) + Yq(X)$$

Cette écriture est appelée la forme réduite de f.

Démonstration. Pour l'existence, il suffit de remplacer Y^k par $(X^3 + AX + B)^{\frac{k}{2}}$ pour k pair et $Y(X^3 + AX + B)^{\frac{k-1}{2}}$ pour k impair pour tout monôme X^kY^l apparaissant dans l'écriture de f. Pour l'unicité, on remarque que si $(p_1,q_1),(p_2,q_2) \in \mathbb{K}[X]^2$ vérifie $p_1 + Yq_1 = p_2 + Yq_2$ dans $\mathbb{K}[E]$, alors W divise $(p_1 - p_2) + Y(q_1 - q_2)$ donc en regardant le degré en Y, on obtient nécessairement que $(p_1 - p_2) + Y(q_1 - q_2) = 0$, ie $p_1 = p_2$ et $q_1 = q_2$. □

Définition 3.1.3. *Pour* $f := p + Yq \in \mathbb{K}[E]$, *on appelle conjugué de* f *et on note* $\overline{f}$ *le polynôme :*

$$\overline{f} = p(X) - Yq(X)$$

On appelle norme de f, *le polynôme :*

$$N(f) = f\overline{f} = p(X)^2 - Y^2q(X)^2$$

qui peut être vu comme un polynôme de $\mathbb{K}[X]$ *en remplaçant* Y^2 *par* $X^3 + AX + B$.

6. Ces cas induisent des complications techniques et pour cette raison, Satoh ne les traite pas.

On vérifie facilement les propriétés suivantes sur le conjugué et la norme :

Proposition 3.1.4. **(i).** *La conjugaison est additive et multiplicative.*

(ii). *Si $f \in \mathbb{K}[E]$ et $P \in E$ alors $\overline{f}(P) = f(-P)$.*

(iii). *La norme est multiplicative.*

(iv). *Si $f \in \mathbb{K}[E]$ vérifie $N(f) = 0$, alors $f = 0$.*

Démonstration. Les trois premiers points sont immédiats. Pour le quatrième, il suffit de remarquer que si $f(X, Y) = p(X) + Yq(X) \in \mathbb{K}[E]$ vérifie $N(f) = 0$ alors :

$$p(X)^2 = (X^3 + AX + B)q(X)^2$$

donc un polynôme de degré pair égalise un polynôme de degré impair et donc $p = q = 0$. □

Remarquons que la norme permet aussi de définir une forme réduite dans $\mathbb{K}(E)$. En effet, si $f, g \in \mathbb{K}(E)$ et $g \neq 0$ alors :

$$\frac{f}{g} = \frac{f\overline{g}}{N(g)}$$

et en écrivant la forme réduite de $f\overline{g}$, on trouve une forme réduite pour $\frac{f}{g}$:

$$\frac{f}{g} = r(X) + Ys(X)$$

avec $r, s \in \mathbb{K}(X)$. Il est aisé de vérifier que cette écriture est unique. On peut donc de la même façon définir le conjugué et la norme d'une fonction sur E.

L'introduction de la notion de norme permet de définir une "bonne" notion de degré dans $\mathbb{K}[E]$ et $\mathbb{K}(E)$.

Définition 3.1.5. *On appelle* degré *d'un polynôme $f \in \mathbb{K}[E]$ le degré de $N(f)$ comme polynôme de $\mathbb{K}[X]$. Etant donné une fonction de E, $F \in \mathbb{K}(E)$ et un de ses représentants $\frac{f}{g}$ avec $f, g \in \mathbb{K}[E]$, on définit aussi le degré de F par :*

$$deg(F) = deg(f) - deg(g)$$

qui ne dépend pas du représentant choisi.

On dispose d'une formule simple pour le degré d'un polynôme :

Proposition 3.1.6. *Si $f \in \mathbb{K}[E]$ a pour forme réduite $p(X) + Yq(X)$ alors :*

$$deg(f) = \begin{cases} \max(2deg(p), 2deg(q) + 3) & si\ q \neq 0 \\ 2deg(p) & sinon \end{cases}$$

En outre, le degré ainsi défini vérifie les mêmes propriétés que le degré usuel des polynômes (la multiplicativité notamment).

3.1.2 Évaluation d'une fonction de E en un point, anneau local des fonctions en un point.

On veut maintenant évaluer les fonctions de E en des points de E. Remarquons que comme les points de E sont à coordonnées dans la clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$, le résultat est a priori dans $\overline{\mathbb{K}} \cup \{\infty\}$, la valeur ∞ étant réservée aux cas où la division par 0 est inévitable. Tenant compte de cette difficulté et afin de ne pas perdre en généralité, on s'autorise à considérer des polynômes et des fonctions sur E à coefficients dans $\overline{\mathbb{K}}$. On notera donc $\overline{\mathbb{K}}[E]$ et $\overline{\mathbb{K}}(E)$ les objets analogues à $\mathbb{K}[E]$ et $\mathbb{K}(E)$ pour $\overline{\mathbb{K}}$.

Définition 3.1.7. *Si $f \in \overline{\mathbb{K}}[E]$ alors le point $P \in E \setminus \{\mathcal{O}\}$ est dit régulier lorsqu'il existe un représentant $\frac{g}{h}$ de f tel que $h(P) \neq 0$. Sinon P est appelé pôle de f. Si P est régulier et que $g(P) = 0$, P est un zéro de f.*

Le degré va nous donner un critère pour évaluer une fonction sur E.

Règles d'évaluation : Soient $f \in \overline{\mathbb{K}}(E)$, $\frac{g}{h}$ un représentant de f et $P \in E$.

(i). Si $P \neq \mathcal{O}$ n'est pas un pôle de f, on peut supposer $h(P) \neq 0$, et on pose alors $f(P) := \frac{g(P)}{h(P)}$.

(ii). Si $P \neq \mathcal{O}$ est un pôle de f, alors on pose $f(P) := \infty$.

(iii). Si $P = \mathcal{O}$ alors $f(P)$ vaut respectivement 0, le rapport des termes de plus haut degré de g et h, ou ∞ selon que $\deg(f) < 0$, $\deg(f) = 0$ ou $\deg(f) > 0$.

Définition 3.1.8. *Etant donné $P \in E$, on* appelle anneau local de E en P *l'anneau $\overline{\mathbb{K}}[E]_P$ des fonctions sur E dont P n'est pas pôle. On appelle* idéal local de E en P *l'idéal $M(E)_P = \{f \in \overline{\mathbb{K}}[E]_P, f(P) = 0\}$.*

Proposition 3.1.9. *$\overline{\mathbb{K}}[E]_P$ est un anneau de valuation discrète d'idéal maximal $M(E)_P$.*

Démonstration. Voir annexe E.1 □

Remarque : Notons au passage que la preuve du résultat précédent a permis d'obtenir que $\text{ord}_{\mathcal{O}}(f) = -\deg(f)$ pour toute fonction $f \in \overline{\mathbb{K}}(E)$.

Proposition 3.1.10. *Le corps des fractions de $\overline{\mathbb{K}}[E]_P$ est $\overline{\mathbb{K}}(E)$, qui est donc un corps valué pour l'unique valuation discrète normalisée relative à $\overline{\mathbb{K}}[E]_P$ et M_P, que l'on notera ord_P.*

Démonstration. Ceci est clair puisque les polynômes sont des éléments de $\overline{\mathbb{K}}[E]_P$. □

Remarque : La notion d'anneau localisé en un idéal fractionnaire est introduite dans l'annexe D.2. Nous avons illustré cette notion dans un cas particulier en faisant les preuves à la main au lieu d'appliquer des résultats généraux. Nous avons jugé que l'exposé était plus clair ainsi.

Voyons une application simple mais très utile du travail mené sur $\overline{\mathbb{K}}[E]_P$.

Proposition 3.1.11. *Si $f \in \mathbb{K}(E)$ et $P \in E \setminus \{\mathcal{O}\}$ alors P est un pôle de f si et seulement si f admet un représentant $\frac{g}{h}$ tel que $h(P) = 0$ et $g(P) \neq 0$.*

Démonstration. Le sens $\Longleftarrow$ est trivial. Supposons que P soit un pôle de f. Alors on peut écrire $f = r_P^{\text{ord}_P(f)} u$ avec r_P une uniformisante en P (que l'on peut prendre polynomiale d'après la preuve de la proposition précédente puisque $P \neq \mathcal{O}$) et $u \in \overline{\mathbb{K}}[E]_P$ dont P n'est pas pôle. Puisque $f \notin \overline{\mathbb{K}}[E]_P$ car P est un pôle de f, on a $\text{ord}_P(f) < 0$ donc en prenant $\frac{g}{h_0}$ un représentant de u, on obtient que g et $h := r_P^{-\text{ord}_P(f)} h_0$ conviennent. □

Proposition 3.1.12. *Soit $f \in \overline{\mathbb{K}}[E] \setminus \{0\}$. Alors :*

(i). *f n'a qu'un nombre fini de pôles et de zéros.*

(ii). *$\sum_{P \in E} ord_P(f) = 0$.*

(iii). *Si f n'a ni zéro ni pôle, alors f est constante.*

(iv). *Si f est non constante, alors f est surjective.*

Démonstration. Voir annexe E.1 □

3.2 Groupe des diviseurs de E.

Définition 3.2.1. *On appelle groupe des diviseurs d'une courbe elliptique E le groupe libre composé des sommes formelles :*

$$\sum_{P \in E} n_P(P)$$

avec $(n_P)_{P \in E}$ famille d'entiers à support fini. On note $Div(E)$ ce groupe.

Définition 3.2.2. *Pour $D = \sum_{P \in E} n_P(P) \in Div(E)$, on définit son* ordre *et sa* norme *respectivement par :*

$$ord(D) := \sum_{P \in E} n_P \quad \text{et} \quad |D| := \sum_{P \in E \setminus \{\mathcal{O}\}} |n_P|$$

On définit aussi $Div^0(E) := \{D \in Div(E), ord(D) = 0\}$.

Définition 3.2.3. *On peut assossier un diviseur à une fonction rationnelle $f \in \overline{\mathbb{K}}(E)$ par la formule :*

$$div(f) = \sum_{P \in E} ord_P(f)(P)$$

Notons que la famille $(\text{ord}_P(f))_{P \in E}$ est bien à support fini d'après le point (i). de la proposition 3.1.12. Le diviseur d'une fonction vérifie les propriétés suivantes :

Proposition 3.2.4. *Soient $f, g \in \overline{\mathbb{K}}(E) \setminus \{0\}$. Alors :*

(i). *$ord(div(f)) = 0$*

(ii). *$div(fg) = div(f) + div(g)$.*

(iii). *$div(f) = div(g)$ si et seulement si f et g sont colinéaires.*

Démonstration. Le point (i). est une conséquence immédiate du point (ii). de la proposition 3.1.12 et le point (ii). découle de la multiplicativité de l'ordre en un point d'une fonction de E (qui est une valuation discrète). Puis, le point (ii). assure que :

$$\text{div}\left(\frac{f}{g}\right) = \text{div}(f) - \text{div}(g) = 0$$

donc $\frac{f}{g}$ n'a ni zéro ni pôle, donc elle est constante d'après le point (iii). de la proposition 3.1.12. D'où (iii). □

Il s'agit maintenant de savoir si réciproquement, un diviseur $D \in \text{Div}(E)$ est le diviseur d'une fonction. Nous savons déjà qu'il est nécessaire que $\text{ord}(D) = 0$ i.e. que $D \in \text{Div}^0(E)$ pour cela. Nous verrons que D doit vérifier une hypothèse supplémentaire pour cela.

Définition 3.2.5. *Un diviseur $D \in Div^0(E)$ est dit* principal *lorsqu'il existe $f \in \overline{\mathbb{K}}(E)$ telle que $D = div(f)$. On note $Princ(E)$ le groupe des diviseurs principaux et $Pic(E)$ le groupe quotient $Div(E)/Princ(E)$ appelé* groupe de Picard de E. *On définit de la même manière $Pic^0(E) := Div^0(E)/Princ(E)$.*

Définition 3.2.6. *On dira que deux diviseurs D_1 et D_2 sont équivalents lorsque $D_1 - D_2$ est principal, c'est à dire lorsqu'ils ont la même classe dans le groupe de Picard.*

Pour chercher des conditions de "principalité", on commence par réduire les diviseurs à des formes les plus simples possibles à équivalence près.

Proposition 3.2.7. *Si $D \in Div(E)$ alors il existe $D_1 \in Div(E)$ tel que $|D_1| \leq 1$, $ord(D_1) = ord(D)$ et $D \sim D_1$.*

Démonstration. Voir annexe E.2. □

Proposition 3.2.8. *Soient $P, Q \in E$. Alors le diviseur $(P) - (Q)$ est prinicpal si et seulement si $P = Q$.*

Démonstration. Voir annexe E.2. □

A ce stade, nous pouvons aisément donner une condition nécessaire et suffisante de principalité d'un diviseur. Pour cela, introduisons la notion de somme d'un diviseur :

Définition 3.2.9. *Soit $D = \sum_{P \in E} n_P(P) \in Div(E)$. On appelle* somme *de D et on note $sum(D)$, l'évaluation de D dans E :*

$$sum(D) = \sum_{P \in E} n_P P$$

Théorème 3.2.10. *D est principal si et seulement si son ordre et sa somme sont nuls.*

Démonstration. Voir annexe E.2 □

Remarque : Il peut être utile pour certaines applications de se restreindre aux points rationnels de la courbe elliptique E, c'est-à-dire aux points à coordonnées dans $\mathbb{K}$. En particulier, si D est un diviseur à support dans l'ensemble des points rationnels de somme et d'ordre nuls, on voudrait savoir s'il existe $f \in \mathbb{K}(E)$ telle que $D = \text{div}(f)$. C'est en fait toujours le cas car la fonction f construite dans la preuve de la proposition 3.2.7 est à coefficients dans $\mathbb{K}$ lorsque le diviseur est à support dans $E(\mathbb{K})$, l'ensemble des points rationnels. En effet, les formules d'addition des points montrent que si droite passe par deux points de $E(\mathbb{K})$ alors le troisième est dans $E(\mathbb{K})$. En outre, une droite qui passe par deux points rationnels est à coefficients dans $\mathbb{K}$.

Les outils développés ici permettent aussi de prouver que la loi d'addition des points introduite dans la section 1 est une loi de groupe abélien, en particulier qu'elle est associative (point délicat à vérifier).

Théorème 3.2.11. *L'application :*

$$\begin{array}{rccc} \Phi : & E & \longrightarrow & Pic^0(E) \\ & P & \longmapsto & (P) - (\mathcal{O}) + Princ(E) \end{array}$$

est une bijection telle que $\Phi(P+Q) = \Phi(P) + \Phi(Q)$ pour tous $P, Q \in E$. Ceci montre en particulier que E est un groupe pour l'addition des points isomorphes au groupe $Pic^0(E)$.

Démonstration. L'injectivité de Φ est une conséquence immédiate de la proposition 3.2.8. Soit $D \in \mathrm{Div}^0(E)$. Alors comme D est de degré nul la proposition 3.2.7 assure que $D \sim 0 = (\mathcal{O})-(\mathcal{O})$, $D \sim (P)-(\mathcal{O})$ ou $D \sim -(P)+(\mathcal{O})$ avec $P \in E \setminus \{\mathcal{O}\}$. Dans le dernbier cas, on peut remarquer que :

$$\mathrm{div}(X - x_P) = (P) + (-P) - 2(\mathcal{O})$$

et donc que $(P) + (-P) - 2(\mathcal{O}) \sim 0$ pour obtenir par somme dans $\mathrm{Pic}^0(E)$:

$$D \sim (-P) - (\mathcal{O})$$

D'où la surjectivité de Φ.

Soient $P, Q \in E$. Alors :

$$\Phi(P+Q) = (P+Q) - (\mathcal{O}) + \mathrm{Princ}(E)$$

Or, on a vu dans le développemnt précédent sur les droites que :

$$(P+Q) \sim (P) + (Q) - (\mathcal{O})$$

D'où $\Phi(P+Q) = \Phi(P) + \Phi(Q)$. □

3.3 Morphismes, isogénies.

3.3.1 Généralités.

Définition 3.3.1. *Soient E_1 et E_2 deux courbes elliptiques sur $\mathbb{K}$. On appelle morphisme une application :*

$$\begin{array}{rcl} \phi : E_1 & \longrightarrow & E_2 \\ P & \longmapsto & (f(P), g(P)) \end{array}$$

avec $f, g \in \mathbb{K}(E_1)$ vérifiant $W_2(f,g) = 0$, W_2 étant le polynôme de Weierstrass de E_2.

Remarque : Précisons une petite difficulté dans la définition précédente. Lorsque P est un pôle de l'une des deux fonctions f et g, on convient que $\phi(P) = \mathcal{O}_{E_2}$.

Un morphisme peut aussi être vu comme un point fini de la courbe elliptique $E_2(\mathbb{K}(E_1))$ constituée des points à coordonnées dans le corps $\mathbb{K}(E_1)$ des fonctions rationnelles sur E_1 vérifiant l'équation de Weierstrass de E_2. On peut donc additionner les morphismes en utilisant la loi d'addition des points sur $E_2(\mathbb{K}(E_1))$. On peut alors vérifier en utilisant les formules d'addition que si ϕ, ψ sont deux morphismes alors pour tout $P \in E_1$:

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

On aimerait aussi ajouter un point à l'infini pour compléter la structure des morphismes. On ajoute donc le morphisme constant égal à $\mathcal{O}$ à l'ensemble des morphismes donnés par la définition précédente.

Commençons par une propriété importante des morphismes :

Proposition 3.3.2. *Un morphisme est soit constant soit surjectif.*

Démonstration. Soit ϕ un morphisme non constant entre deux courbes elliptiques E_1 et E_2. Ecrivons $\phi := (f, g)$ avec $f, g \in \mathbb{K}(E_1)$. Si par l'absurde f était constante, alors g serait racine d'une équation polynomiale d'ordre 2 donc g prendrait au plus deux valeurs donc elle ne pourrait être surjective dans $\overline{\mathbb{K}} \cup \{\infty\}$ et le point (iv). de la proposition 3.1.12. Donc g serait constante et ϕ aussi. Donc f n'est pas constante. Elle admet donc un pôle, en lequel ϕ vaut $\mathcal{O}$. Donc tout morphisme prend la valeur $\mathcal{O}$.

Ceci suffit à conclure en considérant le morphisme $\phi - Q$ pour tout $Q \in E_2$. □

Définition 3.3.3. *Une isogénie est un morphisme entre deux courbes elliptiques, qui est aussi un morphisme de groupes. L'ensemble des isogénies entre deux courbes elliptiques E_1 et E_2 forme un groupe additif noté $Hom(E_1, E_2)$. On note $End(E) = Hom(E, E)$ qui est muni d'une structure d'anneau non commutatif pour l'addition et la composition.*

On dira qu'une isogénie $\varphi \in Hom(E_1, E_2)$ est définie sur $\mathbb{K}$ *lorsqu'elle est nulle ou lorsqu'elle est de la forme $\varphi := (f, g)$ avec $f, g \in \mathbb{K}(E_1)$.*

Exemples : morphismes et isogénies usuelles

1). La translation $\tau_Q : P \in E \longmapsto P + Q \in E$ est un morphisme mais ce n'est pas une isogénie.

2). La multiplication par $n \in \mathbb{Z}$:

$$[n] : P \in E \longmapsto nP \in E$$

est une isogénie. Son noyau que nous étudierons en détail ultérieurement est appelé *le groupe des points de n-torsions de E* et noté $E[n]$.

3). Lorsque $\mathbb{K}$ est un corps de caractéristique p, on définit la p^n*-ième isogénie de Frobenius* (pour $n \in \mathbb{N}^*$) par :

$$\begin{array}{rcl} \mathrm{Fr}_{p^n} : E & \longrightarrow & E_{p^n} \\ (x,y) & \longmapsto & (x^{p^n}, y^{p^n}) \\ \mathcal{O} & \longmapsto & \mathcal{O} \end{array}$$

avec E_{p^n} la courbe elliptique de polynôme de Weierstrass :

$$W_{p^r}(X,Y) = Y^2 - X^3 - A^{p^n}X - B^{p^n}$$

et de discriminant $\Delta(E)^{p^n} \neq 0$. Nous verrons que l'isogénie de Frobenius joue un rôle essentiel dans l'algorithme de Satoh.

Proposition 3.3.4 (forme réduite d'une isogénie)**.** *Toute isogénie $\varphi \in Hom(E_1, E_2)$ admet une unique forme réduite :*

$$\varphi = (r(X), Ys(X))$$

avec $r, s \in \mathbb{K}(X)$.

Démonstration. On écrit $\varphi = (f, g)$ avec $f, g \in \mathbb{K}(E_1)$ et on décompose f et g en forme réduite :

$$f(X,Y) = r(X) + Yr_1(X) \quad \text{et} \quad g(X,Y) = s_1(X) + Ys(X)$$

avec $r, r_1, s, s_1 \in \mathbb{K}(X)$. Comme φ est un morphisme de groupes, on a $\varphi(X, -Y) = -\varphi(X,Y)$ ce qui donne que $r_1 = s_1 = 0$. D'où l'existence d'une forme réduite pour φ. L'unicité est une conséquence immédiate de l'unicité de la forme réduite des fonctions rationnelles sur E_1. □

Théorème 3.3.5. *Pour qu'un morphisme ϕ soit une isogénie, il faut et il suffit que $\phi(\mathcal{O}) = \mathcal{O}$.*

Démonstration. Voir annexe E.3.1. □

3.3.2 Isomorphismes, j-invariant.

Définition 3.3.6. *Une isogénie $\varphi \in Hom(E_1, E_2)$ est un isomorphisme s'il existe $\psi \in Hom(E_1, E_2)$ telle que $\psi \circ \varphi = id_{E_1}$ et $\varphi \circ \psi = id_{E_2}$. On note alors $\psi := \varphi^{-1}$ et on dit que E_1 et E_2 sont isomorphes.*

Définition 3.3.7. *Soit E une courbe elliptique de polynôme de Weierstrass $W := Y^2 - X^3 - AX - B$. On appelle* j-invariant *la quantité :*

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

Pour simplifier la preuve du résultat suivant, on se place dans le cas où les coefficients A et B des courbes considérées sont non-nuls. Ce résultat se généralise bien-sûr lorsque cela n'est plus vérifié.

Proposition 3.3.8. *Deux courbes elliptiques E_1 et E_2 sont isomorphes sur $\overline{\mathbb{K}}$ si et seulement si elles ont même j-invariant. Si E_1 et E_2 sont sous forme canonique, il n'existe que deux isomorphismes $\varphi : E_1 \longmapsto E_2$, qui sont de la forme :*

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

avec γ est une racine de $\frac{A_1B_2}{A_2B_1}$, où $W_1 := Y^2 - X^3 - A_1X - B_1$ et $W_2 := Y^2 - X^3 - A_2X - B_2$ sont les polynômes de Weierstrass de E_1 et E_2.

Démonstration. Voir annexe E.3.2. □

3.3.3 Ramification.

De même que pour les fonctions rationnelles, on aimerait pouvoir étudier "les pôles et les zéros des morphismes", ceci motive l'introduction de la notion de la notion d'indice de ramification.

Remarquons que si $f \in \overline{\mathbb{K}}(E_2)$ et si $\phi : E_1 \longrightarrow E_2$ un morphisme alors $f \circ \phi \in \mathbb{K}(E_1)$. 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 $g \in \overline{\mathbb{K}}(E_2)$ 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 3.3.9. *Soient $\phi : E_1 \longrightarrow E_2$ un morphisme 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 en $\phi(P)$.

On obtient aisément avec les propriétés de l'ordre la :

Proposition 3.3.10 (propriétés de l'indice de ramification)**.** *Soient $\phi : E_1 \longrightarrow E_2$, $\psi : E_2 \longrightarrow E_3$ des morphismes, $P, Q \in E_1$ et $f \in \overline{\mathbb{K}}(E_2)$. Alors :*

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

(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). :*

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

Proposition 3.3.11. *Si $\phi : E_1 \longrightarrow E_2$ est un morphisme 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. Voir annexe E.4 □

Définition 3.3.12. *On dira qu'un morphisme ϕ est* ramifié *ou* inséparable *lorsque $e_\phi > 1$ et qu'il est* non ramifié *ou* séparable *lorsque $e_\phi = 1$.*

Proposition 3.3.13. *Soit $\varphi \in Hom(E_1, E_2)$ une isogénie de forme réduite $(r(X), Ys(X))$. Alors φ est séparable si et seulement si la fraction rationelle dérivée $r'(X)$ est non nulle.*

Démonstration. Voir annexe E.4 □

Corollaire 3.3.14. *En caractéristique nulle toutes les isogénies non-nulles sont séparables. Si $car(\mathbb{K}) = p > 0$, une isogénie φ définie sur E est inséparable si et seulement si elle s'écrit sous la forme $\varphi(X, Y) = (r(X^p), Y^p s(X^p))$.*

Démonstration. Voir annexe E.4 □

Remarque : En particulier, en caractéristique $p > 0$, Fr_{p^n} est inséparable pour tout $n \in \mathbb{N}^*$.

Remarquons qu'une isogénie non nulle admet un nombre fini de pôles, puisqu'une fonction rationnelle non nulle admet un nombre fini de pôle et de zéros. Ainsi, le noyau d'une isogénie non nulle est fini ce qui donne un sens à la définition suivante.

Définition 3.3.15. *On définit le* degré *d'une isogénie $\varphi : E_1 \longrightarrow E_2$ non nulle par la formule :*

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

On convient que l'isogénie nulle est de degré 0.

Remarque : Silverman donne une autre définition du degré dans [7] mais celle donnée ici semble plus facile à utiliser en pratique. On pourra trouver cette définition en annexe E.9 et son exploitation dans l'obtention de résultats plus profonds sur les isogénies que ceux évoqués ici.

Proposition 3.3.16. *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 $\deg(\psi \circ \varphi) = \deg(\psi)\deg(\varphi)$. □

Exemple : Nous allons calculer le degré du q-ième Frobenius dans un corps $\mathbb{K}$ de caractéristque p ($q = p^n$). Il est clair que $|\ker(\mathrm{Fr}_q)| = 1$. En outre, pour un point $P = (x, y) \in E \setminus \{\mathcal{O}\}$ tel que $y \neq 0$, on a :

$$e_{\mathrm{Fr}_q} = e_{\mathrm{Fr}_q}(P) = \mathrm{ord}_P((X - x^q) \circ \Phi_q) = \mathrm{ord}_P(X^q - x^q)$$

Mais $X^q - x^q$ est de degré $2q$ et ses seuls zéros sont P et $-P$ et cette fonction n'a que $\mathcal{O}$ comme pôle. Donc d'après le point (ii). de la proposition 3.1.12 :

$$\mathrm{ord}_P(X^q - x^q) + \mathrm{ord}_{-P}(X^q - x^q) = -\mathrm{ord}_{\mathcal{O}}(X^q - x^q) = 2q$$

Mais $\mathrm{ord}_P(X^q - x^q) = \mathrm{ord}_{-P}(\overline{X^q - x^q}) = \mathrm{ord}_{-P}(X^q - x^q)$ donc $\mathrm{ord}_P(X^q - x^q) = q$, puis $\boxed{\deg(\mathrm{Fr}_q) = q}$.

Compléments : On pourra trouver en annexe E.4.1 un développement sur les polynômes d'annulation des isogénies. Ces polynômes caractérisent le noyau des isogénie, et ont donc une importance cruciale dans l'étude de ces objets. En effet, ils donnent une équation polynomiale dont sont solution les abscisses des éléments du noyau. A partir de la connaissance de tels polynômes, on peut donc obtenir de précieuses informations sur le noyau et à l'inverse construire des isogénies de noyau donné (c'est l'objet des formules de Vélu, cf. [10]).

3.4 L'isogénie $[n]$ et le groupe de n-torsion $E[n]$.

L'isogénie $[n]$ est avec le Frobenuis, une isogénie très utile à Satoh. Mais elle présente aussi un intérêt théorique, notamment parce qu'elle intervient dans une formule d'inversion des isogénies (que nous verrons en 3.6) et dans la construction du module de Tate. Cette sous-section, bien qu'un peu technique, est donc cruciale.

Dans toute ce paragraphe, n désignera un entier naturel non nul.

3.4.1 L'isogénie $[n]$.

Lemme 3.4.1. *$|E[2^m]| = 4^m$ pour tout $m \in \mathbb{N}$.*

Démonstration. On prouve le résultat par récurrence sur $m \in \mathbb{N}$.

Initialisation : Pour $m = 0$, $|E[1]| = |\{\mathcal{O}\}| = 1$. Pour $m = 1$, on sait déjà que $E[2]$ contient l'ensemble des points tels que $P = -P$, c'est à dire $\mathcal{O}$ et les trois points finis d'ordonée nulle (dont les abscisses sont racines distinctes du polynôme $X^3 + AX + B$). Donc $|E[2]| = 4$.

Hérédité : Soit $m \geq 2$. Supposons le résultat au rang $m - 1$. Comme nous l'avons vu dans la preuve de multiplicativité des degrés :

$$|E[2^m]| = |\ker([2^m])| = |\ker([2^{m-1}] \circ [2])| = |\ker([2^{m-1}])||\ker([2])| = |E[2^{m-1}]||E[2]| = 4^{m-1}4 = 4^m$$

D'où l'itération et le résultat.

□

Proposition 3.4.2. *L'isogénie $[n]$ est non nulle.*

Démonstration. Il s'agit là de vérifier que $|E[n]| < +\infty$. Comme $|E[ab]| = |E[a]||E[b]|$ pour tous $a, b \in \mathbb{N}^*$, d'après la preuve de multiplicativité des degrés, on sait d'après le lemme précédent qu'il suffit de prouver que $|E[n]| < +\infty$ pour n impair. Comme $|E[2]| = 4$, on dispose de $P \in E[2] \setminus \{\mathcal{O}\}$ on a alors :

$$nP = \left(2\frac{n-1}{2} + 1\right) P = P + \frac{n-1}{2}2P = P + \frac{n-1}{2}\mathcal{O} = P \neq \mathcal{O}$$

Donc $[n] \neq 0$ et ainsi $|E[n]| < +\infty$. □

Proposition 3.4.3. *(admise) Notons $(r_n(X), Ys_n(X))$ la forme réduite de $[n]$. Alors :*

$$r_n'(X) = ns_n(X)$$

ainsi $[n]$ est séparable si et seulement si car$(\mathbb{K})$ ne divise pas n.

Démonstration. Ce résultat qui se prouve par une récurrence très calculatoire est admis. Le lecteur intéressé trouvera une preuve dans [8]. □

Pour $S \subset E$, on notera (S) le diviseur donné par :

$$(S) = \sum_{P \in S} (P)$$

Lemme 3.4.4 (propriétés de la forme réduite)**.** **(i).** *Si n n'est pas multiple de car($\mathbb{K}$) alors :*

$$deg(r_n) = 2, \quad deg(s_n) = 0, \quad \frac{r_n}{X}(\mathcal{O}) = \frac{1}{n^2}, \quad \text{et } s_n(\mathcal{O}) = \frac{1}{n^3}$$

(ii). *On a pour tous $n, m \in \mathbb{N}^*$ tels que car($\mathbb{K}$) ne divise pas $n, m, n+m$ et $n-m$:*

$$div(r_n - r_m) = (E[n+m]) + (E[n-m]) - 2(E[m]) - 2(E[n])$$

Démonstration. Voir annexe E.5.1 □

Proposition 3.4.5. *Si car($\mathbb{K}$) ne divise pas n, alors :*

$$|E[n]| = n^2$$

Démonstration. On prouve le résultat par récurrence sur $n \in \mathbb{N}^*$. On a trivialement $|E[1]| = 1$ et l'on sait déjà avec le lemme 3.4.1 que $|E[2]| = 4$.

Soit $q \geq 3$ non divisible par car($\mathbb{K}$). Supposons le résultat aux rangs $1, \cdots, q-1$. Appliquons le point (ii). du lemme précédent. On montre donc l'existence de $n, m \in \mathbb{N}^*$ tels que $n+m = q$, $m < n$ et tels que car($\mathbb{K}$) ne divise pas n, m et $n-m$. Si car($\mathbb{K}$) ne divise pas $q-1$ et $q-2$, $n = q-1$ et $m = 1$ conviennent. Si car($\mathbb{K}$)$|q-1$, alors car($\mathbb{K}$) ne divise pas $q-2$ ni $q-4$ car car($\mathbb{K}$) ≥ 5 donc $n = q-2$ et $m = 2$ conviennent. Si car($\mathbb{K}$)$|q-2$, alors car($\mathbb{K}$) ne divise pas $q-3$ et $q-6$ donc $n = q-3$ et $m = 3$ conviennent. Le point (ii). du lemme précédent ainsi que le point (i). de la proposition 3.2.4 assurent alors que :

$$0 = \text{ord}(\text{div}(r_n - r_m)) = |E[n+m]| + |E[n-m]| - 2|E[n]| - 2|E[m]|$$

Donc $|E[q]| = |E[n+m]| = 2|E[n]| + 2|E[m]| - |E[n-m]| = 2n^2 + 2n^2 - (n-m)^2 = (n+m)^2 = q^2$. D'où l'itération et le résultat. □

Proposition 3.4.6 (Structure du groupe de torsion.)**.** *Si car($\mathbb{K}$) ne divise pas n alors $E[n]$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$.*

Démonstration. On sait par la proposition précédente que $|E[n]| = n^2$ et que si d divise n, alors $|E[d]| = d^2$. Or on a le résultat suivant :

Lemme 3.4.7. *Si A est un groupe abélien fini d'ordre N^r tel que pour D divisant N, $A[D]$ est d'ordre D^r, alors A est isomorphe à $(\frac{\mathbb{Z}}{N\mathbb{Z}})^r$.*

Démonstration. En effet, on a $A \approx \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_n\mathbb{Z}$ avec $q_1 \dots q_n = N^r$ et $q_i = p_i^{\alpha_i}$ où les p_i sont des nombres premiers distincts d'après le théorème de structure des groupes abéliens finis prouvé en annexe (voir corollaire B.2.14). On a $\mathbb{Z}/N\mathbb{Z}[D] = \mathbb{Z}/q_1\mathbb{Z}[D] \times \cdots \times \mathbb{Z}/q_n\mathbb{Z}[D]$ et $|\mathbb{Z}/q_i\mathbb{Z}|[D] = \text{pgcd}(q_i, D)$.

Donc pour D divisant N, on a $N^r = \text{pgcd}(D, q_1) \dots \text{pgcd}(D, q_2)$. Donc pour p premier divisant N, il y a exactement r indices $i_1 \dots i_r$ tels que $q_{i_k} = p^{\alpha_{i_k}}$. On a si $v = v_p(n)$: $\alpha_{i_k} \leqslant v$ et $\alpha_{i_1} + \cdots + \alpha_{i_k} \geqslant v$. Par conséquent $\alpha_{i_k} = v$, ce qui montre le résultat intermédiaire. □

L'isomorphisme entre $E[n]$ et $(\mathbb{Z}/n\mathbb{Z})^2$ découle directement de ce résultat. □

3.4.2 Polynômes de division.

La problématique évoquée ici est celle de l'annexe E.4.1 : trouver une équation polynomiale dont sont solution les abscisses des points du noyau. Dans le cas de l'isogénie $[n]$, ceci revient à étudier le n-ième polynôme de division.

On se donne $n \in \mathbb{N}^*$, un entier non divisible par car($\mathbb{K}$). On considère le diviseur $D := (E[n]) - n^2(\mathcal{O})$. On a bien $\text{ord}(D) = 0$ d'après la proposition 3.4.5. En outre, d'après la proposition 3.4.6, $E[n] \approx (\mathbb{Z}/n\mathbb{Z})^2$ donc on dispose d'un isomorphisme de groupes $\alpha : E[n] \longrightarrow (\mathbb{Z}/n\mathbb{Z})^2$:

$$\begin{aligned} \text{sum}(D) &= \sum_{P \in E[n]} P = \sum_{(k,l) \in (\mathbb{Z}/n\mathbb{Z})^2} \alpha(k,l) \\ &= \alpha\left(\sum_{k \in (\mathbb{Z}/n\mathbb{Z})} k, \sum_{l \in (\mathbb{Z}/n\mathbb{Z})} l \right) = \alpha\left(\frac{n(n+1)}{2}, \frac{n(n+1)}{2} \right) = \alpha(0,0) = \mathcal{O} \end{aligned}$$

Donc d'après le théorème E.2.4, on dispose de $\psi_n \in \overline{\mathbb{K}}(E)$ telle que $D = \mathrm{div}(\psi_n)$ et de coefficient dominant n.

Définition 3.4.8. *La fonction Ψ_n est appelé* n-ième polynôme de division.

Proposition 3.4.9. *ψ_n est un polynôme de $\mathbb{K}[E]$ donné par :*

$$\Psi_n(X,Y) := \begin{cases} nf_{[n]}(X) & \text{si } n \text{ est impair} \\ nY\frac{f_{[n]}(X)}{f_{[2]}(X)} & \text{si } n \text{ est pair} \end{cases}$$

où $f_{[n]}(X)$ est le polynôme d'annulation de $[n]$ dont l'ensemble des racines est l'ensemble des abscisses des points de $E[n] \setminus \{\mathcal{O}\}$.

Démonstration. Voir annexe E.5.2 □

Complément : On pourra trouver plus de détails au sujet des polynômes de division dans l'annexe E.5.2, notamment une relation de récurrence très utile dans les calculs de Satoh.

3.5 Couplage de Weil.

On introduit ici un outil de démonstration qui aide à mieux comprendre les isogénies : le couplage de Weil. Cet outil ne sera pas utilisé à d'autres fins dans le rapport, c'est pourquoi ce passage requiert peu d'attention du lecteur. On pourra en première lecture ne retenir que les propriétés de la proposition 3.5.2 qui seront utiles par la suite.

On fixe n non divisible par $\mathrm{car}(\mathbb{K})$. Soit $Q \in E[n]$. Alors le théorème E.2.4 assure l'existence de $f_Q \in \overline{\mathbb{K}}(E)$ telle que :

$$\mathrm{div}(f_Q) = n(Q) - n(\mathcal{O})$$

Soit $Q' \in E$ tel que $[n]Q' = Q$ (Q' existe car $[n]$ est non nulle donc surjective). Soit $D := \sum_{R \in E[n]}[(Q'+R)-(R)]$. Alors :

$$\mathrm{ord}(D) = |E[n]| - |E[n]| = 0 \quad \text{et} \quad \mathrm{sum}(D) = [|E[n]|]Q'$$

On sait que $|E[n]| = n^2$ puisque $\mathrm{car}(\mathbb{K})$ ne divise pas n. On a donc $\mathrm{sum}(D) = [n]Q = \mathcal{O}$. Le théorème E.2.4 assure alors l'existence de $g_Q \in \overline{\mathbb{K}}(E)$ telle que :

$$div(g_Q) = \sum_{R \in E[n]} [(Q'+R)-(R)]$$

On alors :

$$div(g_Q^n) = ndiv(g_Q) = \sum_{R \in E[n]} [n(Q'+R) - n(R)]$$

Par ailleurs, $[m]S = Q$ si et seulement si $S = Q' + R$ avec $R \in E[n]$ et de même $[n]S = \mathcal{O}$ si et seulement si $S \in E[n]$. 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 :

$$div(f_Q \circ [n]) = \sum_{R \in E[n]} [n(Q'+R) - n(R)] = div(g_Q^n)$$

D'après le point (iii). de la proposition 3.2.4, on peut donc supposer :

$$f_Q \circ [n] = g_Q^n$$

quitte à multiplier g_Q par une constante de $\overline{\mathbb{K}}^*$ (ce qui ne change pas son diviseur). 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 $T \longmapsto \frac{g_Q(T+P)}{g_P(T)}$ est à valeurs dans l'ensemble des racines n-ièmes de l'unité de $\overline{\mathbb{K}}$, noté $\mu_n(\overline{\mathbb{K}})$, qui est de cardinal n. Le point (iii). de la proposition 3.1.12 assure alors que cette fonction est constante, que nous noterons $e_n(P,Q)$.

Définition 3.5.1. *L'application ainsi définie :*

$$e_n : E[n] \times E[n] \longrightarrow \mu_n(\overline{\mathbb{K}})$$

est appelée couplage de Weil.

Proposition 3.5.2 (propriétés du couplage de Weil). **(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 $Q=\mathcal{O}$.*

(iv). *Le couplage de Weil est compatible. C'est à dire que :*

$$e_{nm}(P,Q)=e_n([m]P,Q)$$

pour tous $n,m\in\mathbb{N}^*$ non divisibles par car($\mathbb{K}$), $P\in E[nm]$ et $Q\in E[m]$.

Démonstration. Voir annexe E.6. □

3.6 Isogénie duale.

Une question naturelle à se poser sur les isogénies est la suivante : peut-on "inverser" une isogénie ? Plus précisément, étant donné $\varphi\in\mathrm{Hom}(E_1,E_2)$, peut-on construire une isogénie $\hat{\varphi}\in\mathrm{Hom}(E_2,E_1)$? Même s'il n'y a pas toujours d'inverse, le résultat suivant donne néanmoins une réponse positive à la question précédente.

Proposition 3.6.1. *Si $\varphi\in Hom(E_1,E_2)$ alors il existe $\hat{\varphi}\in Hom(E_2,E_1)$ telle que :*

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

Cette isogénie est unique lorsque φ est non nulle et elle est donnée par la formule :

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

pour tout $P\in E_2$. $\hat{\varphi}$ est appelée l'isogénie duale *de φ.*

Démonstration. Voir annexe E.7 □

On dispose des propriétés suivantes sur l'isogénie duale :

Proposition 3.6.2. *Soit $\varphi\in Hom(E_1,E_2)$, $\psi\in Hom(E_2,E_3)$ des isogénies. Alors :*

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

(ii). *Si car($\mathbb{K}$) ne divise pas n alors φ et $\hat{\varphi}$ sont adjointes pour 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). $\widehat{\varphi+\psi}=\hat{\varphi}+\hat{\psi}$.

(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. Voir annexe E.7 □

L'introduction de la notion d'isogénie duale n'est cependant pas seulement purement théorique et désintéressée. Nous verrons en effet que l'étude de l'isogénie duale du Frobenius présente un intérêt pour Satoh. De plus, la notion d'isogénie duale nous permet d'obtenir le résultat suivant, ingrédient essentiel de la preuve du théorème de Hasse :

Proposition 3.6.3. *Le degré :*

$$deg : Hom(E_1,E_2)\longrightarrow\mathbb{N}$$

est une forme quadratique définie positive, c'est à dire que :

(i). $deg(\varphi)=deg(-\varphi)$ *pour tout* $\varphi\in Hom(E_1,E_2)$.

(ii). *L'application :*

$$\langle , \rangle : (\varphi, \psi) \in Hom(E_1, E_2)^2 \longmapsto deg(\varphi + \psi) - deg(\varphi) - deg(\psi)$$

est $\mathbb{Z}$-bilinéaire. Ceci assure en particulier que $deg(n\varphi) = n^2 deg(\varphi)$ pour tous $\varphi \in Hom(E_1, E_2)$ et $n \in \mathbb{Z}$.

(iii). *Pour tout $\varphi \in Hom(E_1, E_2)$, $deg(\varphi) \geq 0$ et $deg(\varphi) = 0$ si et seulement si $\varphi = 0$.*

Démonstration. Les points (i). et (iii). sont clairs. Le point (ii). découle des propriétés de l'isogénie duale. En effet, si $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$, alors on a d'après le point (iii). de la proposition précédente :

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

Et cette expression est clairement $\mathbb{Z}$-bilinéaire. □

Définition 3.6.4. *Si Fr_p désigne la p-ième isogénie de Frobenius (ici $car(\mathbb{K}) = p$), on désigne par V_p son isogénie duale appelée* isogénie de Verschiebung.

Remarque (fondamentale) : Comme $\mathrm{Fr}_p \circ V_p = [\deg(\mathrm{Fr}_p)] = [p]$ et que $\ker(\mathrm{Fr}_p) = \{\mathcal{O}\}$, on a $\ker(V_p) = E[p]$. Satoh se sert beaucoup de ce fait.

Théorème 3.6.5 (structure du groupe de torsion)**.** *Soient $p := car(\mathbb{K})$ et $n \in \mathbb{N}^*$.*

(i). *Si p ne divise pas n alors $E[n]$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$.*

(ii). *Deux cas peuvent se produire selon la séparabilité de V_p :*

(a). *Si V_p est séparable alors $E[p^n]$ est isomorphe à $\mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \in \mathbb{N}^*$. On dit alors que E est* ordinaire.

(b). *Si V_p est inséparable alors $E[p^n] = \{\mathcal{O}\}$ pour tout $n \in \mathbb{N}^*$. On dit alors que E est* super-singulière.

Démonstration. Le point (i). a déjà été prouvé dans la proposition 3.4.6. Pour le point (ii)., on remarque que pour tout $n \in \mathbb{N}^*$:

$$|E[p^n]| = |\ker([p^n])| = |\ker([p]^n)| = |\ker([p])|^n = |E[p]|^n = |\ker(V_p)|^n$$

avec $\deg(V_p) = \deg(\mathrm{Fr}_p) = p$ et donc $|\ker(V_p)|e_{V_p} = p$. Si V_p est séparable on a donc $e_{V_p} = 1$ et ainsi $|\ker(V_p)| = p$. Donc $|E[p^n]| = p^n$. On applique alors le lemme 3.4.7 pour conclure.

Si V_p est inséparable alors $e_{V_p} = p$ et $|\ker(V_p)| = 1$ on conclut donc trivialement dans ce cas. □

3.7 Module de Tate et trace d'une isogénie.

3.7.1 Généralités sur le module de Tate.

L'idée maîtresse ici est de traiter les isogénies comme des applications linéaires (entre modules [7]), objets mieux maîtrisés. On fixe l un nombre premier. On considère le système projectif (voir définition 2.1.16) $((E[l^n])_{n\in\mathbb{N}^*}, (f_m^n)_{1\leq n\leq m})$ avec :

$$\forall 1 \leq n \leq m, \quad f_m^n : P \in E[l^m] \longmapsto [l^{m-n}]P \in E[l^n]$$

Définition 3.7.1. *On appelle* module de Tate l-adique de E *la limite projective :*

$$T_l(E) = \varprojlim E[l^n]$$

On munit $T_l(E)$ d'une structure de $\mathbb{Z}_l$-module en posant pout tous $x := (x_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}_l = \varprojlim \mathbb{Z}/l^n\mathbb{Z}$ et $P := (P_n)_{n\in\mathbb{N}^*} \in T_l(E)$:

$$x \cdot P := ([x_n]P_n)_{n\in\mathbb{N}^*}$$

pour définir la loi externe.

Proposition 3.7.2. *Si $l \neq car(\mathbb{K})$ alors $T_l(E)$ est isomorphe à $\mathbb{Z}_l^2$ en tant que $\mathbb{Z}_l$-module.*

Démonstration. Voir annexe E.8 □

7. Etant donné nos connaissances étaient limitées à l'algèbre linéaire vectorielle, nous avons étudié les modules en annexe A.

Soit $\varphi \in \mathrm{Hom}(E_1, E_2)$ une isogénie. Alors φ agit comme un morphisme de $\mathbb{Z}_l$-modules via l'application $\mathbb{Z}_l$-linéaire associée :

$$\begin{array}{rccc} \varphi_l : & T_l(E_1) & \longrightarrow & T_l(E_2) \\ & (P_n)_{n\in\mathbb{N}^*} & \longmapsto & (\varphi(P_n))_{n\in\mathbb{N}^*} \end{array}$$

Lorsque $E_1 = E_2 = E$, ce point de vue nous autorise à considérer des objets tels que le polynôme caractéristique, la trace et le déterminant de φ dans $T_l(E)$ (en considérant ces quantités pour φ_l). Nous allons montrer par la suite que ces quantités ne dépendent pas de l.

Pour cela, nous allons utiliser le couplage de Weil. Nous allons construire un couplage de Weil sur $T_l(E)^2$, à partir des couplages de Weil $e_{l^n} : E[l^n]^2 \longrightarrow \mu_{l^n}(\overline{\mathbb{K}})$ pour $n \in \mathbb{N}^*$ définis au paragraphe 3.5, $\mu_{l^n}(\overline{\mathbb{K}})$ désignant le groupe des racines l^n-ièmes de l'unité de $\overline{\mathbb{K}}$.

On considère le système projectif $((\mu_{l^n})_{n\in\mathbb{N}^*}, (f_m^n)_{1\leq n\leq m})$ avec :

$$\forall 1 \leq n \leq m, \quad f_m^n : \zeta \in \mu_{l^m}(\mathbb{K}) \longmapsto \zeta^{l^{m-n}} \in \mu_{l^n}(\mathbb{K})$$

Et la limite projective :

$$T_l(\mu) = \varprojlim \mu_{l^n}(\overline{\mathbb{K}})$$

Définition 3.7.3. *On définit* le couplage de Weil sur $T_l(E)$ *par :*

$$\begin{array}{rccc} e^{(l)} : & T_l(E)^2 & \longrightarrow & T_l(\mu) \\ & ((P_n)_{n\in\mathbb{N}^*}, (Q_n)_{n\in\mathbb{N}^*}) & \longmapsto & (e_{l^n}(P_n, Q_n))_{n\in\mathbb{N}^*} \end{array}$$

Ceci est bien défini car si $((P_n)_{n\in\mathbb{N}^*}, (Q_n)_{n\in\mathbb{N}^*}) \in T_l(E)^2$ alors pour tous $1 \leq n \leq m$, on a d'après la bilinéarité et la compatibilité du couplege de Weil (points (i). et (iv). de la proposition 3.5.2) :

$$e_{l^n}(P_n, Q_n) = e_{l^n}([l^{m-n}]P_m, [l^{m-n}]Q_m) = e_{l^n}([l^{m-n}]P_m, Q_m)^{l^{m-n}} = e_{l^m}(P_m, Q_m)^{l^{m-n}}$$

Les propriétés du couplage de Weil classique s'étendent au nouveau couplage de Weil défini sur $T_l(E)$.

Proposition 3.7.4. **(i).** *$e^{(l)}$ est bilinéaire :*

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

pour tous $P, P_1, P_2, Q, Q_1, Q_2 \in T_l(E)$.

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

(iii). *$e^{(l)}$ est non-dégénérée $e^{(l)}(P, Q) = 1$ pour tout $P \in T_l(E)$ si et seulement si $Q = O_{T_l(E)}$.*

(iv). *$\varphi \in Hom(E_1, E)$ et $\hat{\varphi}$ sont adjointes pour $e^{(l)}$:*

$$\forall (P, Q) \in T_l(E_1) \times T_l(E), \quad e^{(l)}(\varphi_l(P), Q) = e^{(l)}(P, \hat{\varphi}_l(Q))$$

Proposition 3.7.5. *Si $\varphi \in End(E)$ et si φ_l est l'application $\mathbb{Z}_l$-linéaire associée à φ sur $T_l(E)$, alors on a $\det \varphi_l = deg\varphi$.*

Démonstration. Soient (v_1, v_2) une $\mathbb{Z}_l$-base de $T_l(E)$ et A la représentation matricielle de φ_l dans la base (v_1, v_2) :

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

On utilise la bilinéarité et l'antisymétrie de $e^{(l)}$:

$$\begin{aligned} e^{(l)}([\deg(\varphi)]_l(v_1), v_2) &= e^{(l)}((\widehat{\varphi} \circ \varphi)_l(v_1), v_2) \\ &= e^{(l)}(\widehat{\varphi}_l(\varphi_l(v_1)), v_2) \\ &= e^{(l)}(\varphi_l(v_1), \varphi_l(v_2)) \\ &= e^{(l)}(av_1 + cv_2, bv_1 + dv_2) \\ &= e^{(l)}(v_1, v_1)^{ab} e(v_1, v_2)^{ad} e(v_2, v_1)^{cb} e(v_2, v_2)^{cd} \\ &= e^{(l)}(v_1, v_2)^{ad-bc} = e^{(l)}([\det(A)]_l v_1, v_2) \end{aligned}$$

Donc par linéarité à gauche $e^{(l)}([\deg(\varphi) - \det(A)]_l v_1, v_2) = 1$. De même $e^{(l)}([\deg(\varphi) - \det(A)]_l v_1, v_1) = 1$ puisque $e^{(l)}(v_1, v_1) = 1$ et par linéarité à gauche. Donc (v_1, v_2) étant une base de $T_l(E)$, on obtient que $e^{(l)}([\deg(\varphi) - \det(A)]_l v_1, u) = 1$ pour tout $u \in T_l(E)$ et donc que $[\deg(\varphi) - \det(A)]_l v_1 = 0$ par non dégénerscence de $e^{(l)}$. On montre de même que $[\deg(\varphi) - \det(A)]_l v_2 = 0$, ce qui donne $[\deg(\varphi) - \det(A)]_l = 0$, puis $\deg(\varphi) = \det(A) = \det(\varphi_l)$. □

3.7.2 Trace d'une isogénie.

Définition 3.7.6. *On appelle trace d'une isogénie $\varphi \in End(E)$ pour l premier différent de $Car(\mathbb{K})$ la trace de φ_l dans $T_l(E) \approx \mathbb{Z}_l^2$.*

On peut montrer avec la proposition 3.7.5 que **la trace d'une isogénie, qui a priori est dans $\mathbb{Z}_l$, est en fait entière et ne dépend pas de l.** En effet, pour tout $n \in \mathbb{N}^*$:

$$\deg([n] - \varphi) = \det([n] - \varphi_l) = n^2 - \mathrm{Tr}(\varphi_l)n + \det(\varphi_l) \quad (\star)$$

Il est alors immédiat que $\mathrm{Tr}(\phi_l) \in \mathbb{N}$ et que cette quantité est indépendante de l. On peut donc poser :

$$\mathrm{Tr}(\varphi) = \mathrm{Tr}(\varphi_l)$$

Une première propriété de la trace que l'on peut obtenir simplement avec les calculs précédents est la suivante :

Proposition 3.7.7.

$$Tr(\varphi) = Tr(\hat{\varphi})$$

Démonstration. Commençons par remarquer que pour $n \in \mathbb{N}^*$, $\hat{[n]} = [n]$, de sorte que $[n]\hat{} - \phi = [n] - \hat{\phi}$ et :

$$n^2 - \mathrm{Tr}(\varphi)n + \deg(\varphi) = deg([n] - \varphi) = deg([n] - \hat{\varphi}) = \mathrm{Tr}(\hat{\varphi})n + \deg(\hat{\varphi})$$

Donc $\mathrm{Tr}(\varphi) = \mathrm{Tr}(\hat{\varphi})$ puisque $\deg(\hat{\varphi}) = \deg(\varphi)$. □

Remarque : Cette dernière propriété est cruciale pour Satoh car elle substitue le calcul de la trace du Vershiebung à celle du Forbenius, plus simple à calculer car le Vershiebung est séparable. En effet, comme nous le verrons dans la section suivante, le calcul de la trace du Frobenius est un ingrédient du comptage de points.

3.8 Isogénies à valeurs dans $\mathbb{F}_q$.

3.8.1 Isogénie de Frobenius et théorème de Hasse.

Proposition 3.8.1. *L'isogénie de Frobenius Fr_{p^n} est inséparable tandis que $[m] - Fr_{p^n}$ est séparable si et seulement si p ne divise pas m. En particulier, $[1] - Fr_q$ est séparable.*

Démonstration. Voir annexe E.10.1 □

Remarque : Ce résultat est fondammental car il est au coeur de l'idée même du relèvement p-adique de Satoh. Comme nous le verrons, le Frobenius est important dans le comptage de points mais il est "dur à manipuler" car inséparable. L'une des vertus du relèvement p-adique est donc de rendre les isogénies séparables en se plaçant en caractéristique nulle.

On suppose que $p := \mathrm{car}(\mathbb{K})$ est un nombre premier. On note Fr_q le q-ième isomorphisme de Fobenius pour $q = p^n$ pour $n \in \mathbb{N}^*$. La relation $(\star)$ du paragraphe précédent appliquée à Fr_q, qui est de degré q donne que :

$$\mathrm{Tr}(\mathrm{Fr}_q) = 1 + q - \deg([1] - \mathrm{Fr}_q)$$

On peut en déduire l'un théorème les plus importants de ce rapport, directement utilisé par Satoh dans son algorithme de comptage de points :

Théorème 3.8.2 (Hasse)**.** *Le nombre de points rationnels de la courbe s'obtient avec le calcul de la trace du q-ième morphisme de Frobenius par la formule :*

$$|E(\mathbb{F}_q)| = q + 1 - Tr(Fr_q)$$

On a en outre $|Tr(Fr_q)| \leq 2\sqrt{q}$, de sorte que :

$$||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}$$

Démonstration. On sait que $[1] - \mathrm{Fr}_q$ est séparable, ce qui assure que :

$$|\ker([1] - \mathrm{Fr}_q)| = \deg([1] - \mathrm{Fr}_q) = 1 + q - \mathrm{Tr}(\mathrm{Fr}_q)$$

Pour relier $\ker([1] - \mathrm{Fr}_q)$ à $|E(\mathbb{F}_q)|$, il est plus simple de voir les points de E comme des points du plan projectif $\mathbb{P}^3(\overline{\mathbb{F}_q})$ et détudier l'action du Frobenius sur ces points. On a :

$$\mathrm{Fr}_q : [x : y : z] \in E \longmapsto [x^q : y^q : z^q] \in E$$

Donc $[x : y : z] \in \ker(\mathrm{Fr}_q)$ si et seulement si $[x^q - x : y^q - y : z^q - z] = [0 : 1 : 0]$. Mais le thèorème de Lagrange appliqué à $\mathbb{F}_q^*$ assure que tout élément $x \in \mathbb{F}_q$ vérifie $x^q = x$. Comme $X^q - X$ est de degré $q = |\mathbb{F}_q|$, il est donc sciendé à racines simples dans $\mathbb{F}_q$:

$$X^q - X = \prod_{\zeta \in \mathbb{F}_q} (X - \zeta)$$

Donc $[x : y : z] \in \ker(\mathrm{Fr}_q)$ si et seulement si x et z sont racines de $X^q - X$ donc dans $\mathbb{F}_q$, ce qui équivaut à dire que $[x : y : z] \in E(\mathbb{F}_q)$. Donc $|\ker(\mathrm{Fr}_q)| = |E(\mathbb{F}_q)|$.

Il reste à prouver que $|\mathrm{Tr}(\mathrm{Fr}_q)| \leq 2\sqrt{q}$. Comme $\deg([1]) = 1$ et $\deg(\mathrm{Fr}_q) = q$, on a :

$$\mathrm{Tr}(\mathrm{Fr}_q) = \deg([1] - \mathrm{Fr}_q) - \deg([1]) - \deg(\mathrm{Fr}_q) = \langle [1], -\mathrm{Fr}_q \rangle$$

Puisque deg est une forme quadratique définie positive (d'après la proposition 3.6.3), on peut donc appliquer l'équivalent suivant de l'inégalité de Cauchy-Schwartz qui donne immédiatement le résultat voulu.

Lemme 3.8.3. *Soit $(G, +)$ un groupe abélien et d une forme quadratique définie positive $d : G \longrightarrow \mathbb{N}$. Considérons la forme bilinéaire associée :*

$$\langle , \rangle : (g, h) \in G^2 \longmapsto d(g + h) - d(g) - d(h)$$

Alors :

$$\forall (g, h) \in G^2, \quad |\langle g, h \rangle| \leq 2\sqrt{d(g)d(h)}$$

Démonstration. Soient $g, h \in G$. Alors pour tous $n, m \in \mathbb{Z}$:

$$\begin{aligned} d(ng + mh) &= \frac{1}{2}\langle ng + mh, ng + mh \rangle = \frac{1}{2}\left(n^2\langle g, g \rangle + 2nm\langle g, h \rangle + m^2\langle h, h \rangle\right) \\ &= n^2 d(g) + nm\langle g, h \rangle + m^2 d(h) \end{aligned}$$

Cette expression est donc positive pour tous $n, m \in \mathbb{Z}$. En évaluant ceci en $m = -\langle g, h \rangle$ et $n = 2d(h)$, on obtient alors :

$$d(h)(4d(g)d(h) - \langle g, h \rangle^2) \geq 0$$

Ce qui donne immédiatement le résultat du lemme (si $h \neq 0$ on simplifie par $d(h)$, sinon, l'inégalité à démontrer est triviale). □

□

3.8.2 Critère pratique de supersingularité.

On se reportera utilement à l'annexe E.11 pour trouver une méthode alternative de comptage de points (moins efficace en pratique) menant à un critère de supersingularité (quant-à-lui très utilisé en pratique et en particulier pour l'algorithme de Satoh qui ne traite pas les courbes supersingulières).

Théorème 3.8.4. *Soit A_p le coefficient devant X^{p-1} du polynômes $(X^3 + AX + B)^{\frac{p-1}{2}}$. Alors E est supersingulière si et seulement si $A_p = 0$.*

⋆

Nous venons de voir en substance le coeur mathématique du sujet. Etant donné le grand nombre de notions introduites et de résultats, on peut se demander s'il n'existe pas une formulation plus simple de ces mêmes concepts et résultats. Lorsque l'on prend $\mathbb{C}$ comme corps de base, l'analyse complexe répond positivement à cette question.

4 Courbes elliptiques sur $\mathbb{C}$ et polynômes modulaires.

La première question qui vient probablement à l'esprit en commençant cette étude est : à quoi cela sert-il de travailler avec des courbes elliptiques définies sur $\mathbb{C}$ alors que celles que nous étudions sont dans $\mathbb{F}_q$ ou $\mathbb{Z}_q$? En fait, on dispose d'un résultat théorique qui nous permet de plonger $\overline{\mathbb{Q}_p}$ dans $\mathbb{C}$. Ainsi, les résultats de cette section, valables sur $\mathbb{C}$, le seront aussi sur $\overline{\mathbb{Q}_p}$.

L'objet de cette section est d'obtenir une équation polynomiale liant les j-invariants des courbes elliptiques entre lesquelles il existe une isogénie de noyau cyclique (théorème 4.6.9). Nous le verrons, cette équation est primordiale pour relever "correctement [8]" les courbes elliptiques de $\mathbb{F}_q$ dans $\mathbb{Q}_q$. Aussi avons-nous cherché à savoir d'où elle provient, et ce fut l'occasion de faire de très jolies mathématiques. **Toutefois, le lecteur pressé peut tout à fait ne retenir de cette section que le théorème 4.6.9 ainsi que les propositions 4.6.7 et 4.6.8.**

On constatera que certains arguments, idées et techniques de preuves sont assez semblables à celles de la section précédente, en particulier dans les discussions sur les fonctions elliptiques, qui sont des objets analogues aux fonctions rationnelles. Nous avons cependant conservé cette partie pour plus de clarté, au risque de nous répéter. Indiquons en outre à toutes fins utiles que l'analyse complexe, présentée dans [5] semblait plus accessible que la géométrie algébrique présentée par [7]. C'est pourquoi nous avons commencé par étudier [5] avant de bien comprendre la géométrie algébrique avec [8].

L'idée qui guide cette étude est d'identifier chaque courbe elliptique E définie sur $\mathbb{C}$ à un tore $\mathbb{C}/\Lambda$ (où Λ est un réseau) et d'identifier les fonctions rationnelles sur E à des fonctions méromorphes Λ-périodiques (dites elliptiques). C'est l'objet des quatre premiers paragraphes. Une fois ce fait acquis, on l'utilise pour identifier les isogénies entre les courbes $E_1 \approx \mathbb{C}/\lambda_1$ et $E_2 \approx \mathbb{C}/\lambda_2$ à des nombres complexes $\alpha \in \mathbb{C}^*$ tels que $\alpha\Lambda_1 \subset \Lambda_2$. Le noyau de l'isogénie représentée par α s'identifie alors à $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ et on étudie les matrices de passage entre des bases de Λ_1 et λ_2 lorsque ce noyau est cyclique pour obtenir l'équation polynomiale voulue. C'est l'objet des deux derniers paragraphes.

4.1 Préliminaires d'analyse complexe : fonctions elliptiques.

Définition 4.1.1. *Un réseau de $\mathbb{C}$ est un sous-$\mathbb{Z}$-module de $\mathbb{C}$ de type fini et de rang 2, non inclus dans une droite du plan complexe.*

Remarque : Si Λ est un réseau de $\mathbb{C}$, alors Λ admet des $\mathbb{Z}$-bases à deux éléments libre sur $\mathbb{R}$ (car sion Λ serait inclus dans une droite). Ces bases engendrent donc $\mathbb{C}$ tout entier comme $\mathbb{R}$-espace vectoriel.

Définition 4.1.2. *Un* parallélogramme fondammental *du réseau Λ est un ensemble de la forme :*

$$P := \{\alpha + s\omega_1 + t\omega_2 \mid s, t \in [0, 1[\}$$

avec $\alpha \in \mathbb{C}$ et (ω_1, ω_2) une $\mathbb{Z}$-base de Λ.

Remarque : Tout parallélogramme fondammental P est naturellement en bijection avec le quotient $\mathbb{C}/\Lambda$. Ainsi, une somme à support fini d'éléments indexés par un parralélogramme fondammental P, qui ne dépend pas de ce parrallélogramme sera notée simplement $\sum_{\omega\in\mathbb{C}/\Lambda}$.

Définition 4.1.3. *Une fonction elliptique f par rapport au réseau Λ est une fonction méromorphe sur $\mathbb{C}$, Λ-périodique, c'est à dire telle que pour tout point $\omega \in \Lambda$ et tout complexe z qui n'est pas pôle de f :*

$$f(z + \omega) = f(z)$$

Pour tout $\omega \in \mathbb{C}$, on notera $ord_\omega(f)$ et $res_\omega(f)$ respectivement l'ordre de ω comme zéro ou pole de f et le résidu associé.

On notera aussi $\mathbb{C}(\Lambda)$ l'ensemble des fonctions elliptiques par rapport au réseau Λ.

Proposition 4.1.4. *Si f est une fonction elliptique non constante sur un réseau Λ alors f admet des zéros et des pôles en nombre fini sur $\mathbb{C}/\Lambda$.*

Démonstration. Si f n'admet pas de pôle alors f est holomorphe et de plus par Λ-périodicité :

$$\sup_{x\in\overline{P}}|f(x)| = \sup_{x\in\mathbb{C}}|f(x)|$$

pour tout parallélogramme fondammental P de Λ. Comme f est continue (car holomorphe) et que Λ est compact, $\sup_{x\in\overline{P}}|f(x)|$ est fini et atteint donc f est bornée sur $\mathbb{C}$. Le théorème de Liouville assure alors que f est constante. Donc f admet des pôles.

8. Le sens de cet adverbe sera précisé dans la section 6.

De même, si f n'admet pas de zéros alors $\frac{1}{f}$ est elliptique et holomorphe donc constante. Donc f admet des zéros.

En outre, f étant méromorphe, les pôles de f sont isolés donc en nombre finis dans le compact $\overline{P}$ qui contient $P \approx \mathbb{C}/\Lambda$. Il en est de même pour les zéros de f d'après le principe des zéros isolés. □

Remarque : Si f est une fonction elliptique sur un réseau Λ alors $\sum_{\omega \in P} \mathrm{ord}_\omega(f)$ et $\sum_{\omega \in P} \mathrm{res}_\omega(f)$ sont donc des sommes à support fini qui ne dépendent pas du parralélogramme fondammental P de Λ donné. On peut donc indexer ces sommes par $\mathbb{C}/\Lambda$.

Proposition 4.1.5. *Soit f une fonction elliptique par rapport à un réseau Λ. Alors :*

$$\sum_{\omega \in \mathbb{C}/\Lambda} res_\omega(f) = \sum_{\omega \in \mathbb{C}/\Lambda} ord_\omega(f) = 0$$

Démonstration. Voir annexe F.1 □

On en déduit immédiatement le résultat suivant :

Corollaire 4.1.6. *Si f est une fonction elliptique non-constante sur un réseau Λ, alors elle admet au moins deux pôles dans $\mathbb{C}/\Lambda$.*

Proposition 4.1.7. *Soit f une fonction elliptique par rapport à un réseau Λ. Alors pour tout parallélogramme fondammental P de Λ :*

$$\sum_{\omega \in P} \omega \cdot ord_\omega(f) \in \Lambda$$

Démonstration. Voir annexe F.1. □

4.2 Fonction $\mathcal{P}_\Lambda$ de Weierstrass et paramétrage des courbes elliptiques.

Proposition 4.2.1. *Considérons la fonction définie sur $\mathbb{C} \setminus \Lambda$ définie par :*

$$\mathcal{P}_\Lambda(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

Cette fonction est bien définie, paire et elliptique par rapport à Λ. En outre, la série de fonctions définissant $\mathcal{P}_\Lambda$ converge normalement sur tout compact de $\mathbb{C} \setminus \Lambda$. Cette fonction est appellée fonction de Weierstrass associée à Λ.

Démonstration. Voir annexe F.2 □

Proposition 4.2.2. *$\mathbb{C}(\Lambda)$ est un corps engendré par $\mathcal{P}$ et $\mathcal{P}'$.*

Démonstration. Voir annexe F.2 □

Proposition 4.2.3. **(i).** *$\mathcal{P}_\Lambda$ admet pour développement en série de Laurent au voisinage de 0 :*

$$\mathcal{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1) s_{2n+2} z^{2n}$$

avec pour tout $n \geq 3$:

$$s_n(\Lambda) = s_n := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^n}$$

qui est bien définie d'après le lemme F.2.2.

(ii). *Posons $g_4(\Lambda) = g_4 := 60 s_4(\Lambda)$ et $g_6(\Lambda) = g_6 := 140 s_6(\Lambda)$. Alors :*

$$\mathcal{P}'^2_\Lambda = 4\mathcal{P}^3_\Lambda - g_4 \mathcal{P}_\Lambda - g_6$$

Démonstration. Voir annexe F.2 □

Remarque : Nous venons d'obtenir que $(\mathcal{P}_\Lambda, \mathcal{P}'_\Lambda)$ paramétrise une équation de courbes elliptiques. Nous verrons dans le prochain paragraphe que ce paramétrage est bijectif et permet d'identifier la courbe elliptique ainsi définie à $\mathbb{C}/\Lambda$.

4.3 Courbes elliptiques et réseaux de $\mathbb{C}$

Théorème 4.3.1 (paramétrage). **(i).** *Si Λ est un réseau de $\mathbb{C}$ alors $\Delta(\Lambda) := g_4(\Lambda)^3 - 27g_6(\Lambda)^2 \neq 0$. En d'autre termes, la courbe $E(\Lambda)$ d'équation de Weierstrass :*

$$y^2 = 4x^3 - g_4(\Lambda)x - g_6(\Lambda)$$

définit bien une courbe elliptique sur $\mathbb{C}$.

(ii). *L'application :*

$$\begin{array}{rccc} \Phi : & \mathbb{C}/\Lambda & \longrightarrow & E(\Lambda) \\ & z & \longmapsto & (\mathcal{P}_\Lambda(z), \mathcal{P}'_\Lambda(z)) \end{array}$$

est alors un isomorphisme additif de groupes (en prenant la convention $\Phi(0) = \mathcal{O}$).

Démonstration. Voir annexe F.3 □

4.4 Courbes elliptiques, réseaux de $\mathbb{C}$ et groupe modulaire.

Dans cette sous-section, nous montrons qu'en fait, toute courbe elliptique sur $\mathbb{C}$ peut s'identifier à un réseau de $\mathbb{C}$.

4.4.1 j-invariant et groupe modulaire

Si Λ est un réseau de $\mathbb{C}$ alors on peut définir son j-invariant, égal au j-invariant de la courbe elliptique associée :

$$j(\Lambda) := j(E(\Lambda)) = 1728\frac{g_4(\Lambda)^3}{\Delta(\Lambda)} = 1728\frac{g_4(\Lambda)^3}{g_4(\Lambda)^3 - 27g_6(\Lambda)^2}$$

Si Λ_1 et Λ_2 sont deux réseaux de $\mathbb{C}$ tels que $\Lambda_2 = \alpha\Lambda_1$ avec $\alpha \in \mathbb{C}^*$ alors $g_4(\Lambda_2) = \frac{g_4(\Lambda_1)}{\alpha^4}$ et $g_6(\Lambda_2) = \frac{g_6(\Lambda_1)}{\alpha^6}$ donc $j(\Lambda_1) = j(\Lambda_2)$ ce qui montre que les courbes représentées par Λ_1 et Λ_2 sont isomorphes.

Donc si Λ est un réseau de $\mathbb{C}$ dont (ω_1, ω_2) est une base *orientée* (c'est à dire choisie de sorte que (ω_2, ω_1) soit directe quitte à échanger ω_1 et ω_2) alors $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ représente la même courbe que $\frac{1}{\omega_2}\Lambda = \mathbb{Z} + \frac{\omega_1}{\omega_2}\mathbb{Z}$ à isomorphisme près. Il s'ensuit que j (et donc la courbe représentée) ne dépend que du paramètre $\tau := \frac{\omega_1}{\omega_2}$, qui est toujours à valeurs dans le demi plan de Poincaré :

$$\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

Nous disposons donc d'une fonction (que nous noterons j), qui associe à tout point τ de $\mathbb{H}$ une classe d'équivalence de courbes elliptiques à isomorphisme près. L'objet de cette sous-section sera de montrer que j est surjective mais commençons par remarquer avant cela que j n'est pas injective.

En effet, si (ω_1, ω_2) et (ω'_1, ω'_2) sont deux bases orientiées d'un même réseau de $\mathbb{C}$ alors la transposée de la matrice de passage de l'une à l'autre est une matrie $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ inversible à coefficients dans $\mathbb{Z}$. On en déduit qu'elle est de déterminant ± 1. On a alors :

$$\frac{\omega'_1}{\omega'_2} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d}$$

Un calcul facile donne alors que :

$$\mathrm{Im}\left(\frac{\omega'_1}{\omega'_2}\right) = \mathrm{Im}\left(\frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d}\right) = \frac{\det(P)\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right)}{\left|c\frac{\omega_1}{\omega_2} + d\right|^2}$$

Donc que $\det(P) = 1$ car (ω_1, ω_2) et (ω'_1, ω'_2) sont orientiées.

Réciproquement, si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et si $\tau \in \mathbb{H}$ alors $\tau' = \frac{a\tau+b}{c\tau+d} \in \mathbb{H}$ et $\mathbb{Z} + \tau\mathbb{Z} = \mathbb{Z} + \tau'\mathbb{Z}$.

Nous venons donc d'obtenir que j **est invariant par l'acion de** $SL_2(\mathbb{Z})$, c'est à dire que :

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

Nous étudierons donc l'action du groupe $SL_2(\mathbb{Z})$ [9] sur le demi-plan de Poincaré $\mathbb{H}$, définie par :

$$P \cdot z = \frac{az+b}{cz+d}$$

pour tous $z \in \mathbb{H}$ et $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, dont les orbites nous donneront toutes les courbes elliptiques à isomorphisme près. Comme l'action de $-I_2$ est triviale, on considère en fait l'action de $\Gamma := SL_2(\mathbb{Z})/\{\pm I_2\}$ sur $\mathbb{H}$.

Définition 4.4.1. *Le groupe* $\Gamma := SL_2(\mathbb{Z})/\{\pm I_2\}$ *est appelé* groupe modulaire.

Par abus, on adoptera la notation matricielle pour les éléments de Γ, quitte à confondre une matrice avec son opposée.

Définition 4.4.2. *On appelle* domaine fondammental *de* Γ *dans* $\mathbb{H}$ *une partie* S *de* $\mathbb{H}$ *telle que toute orbite de* $\mathbb{H}$ *sous l'action de* Γ *admette un élément dans* S *et telle que si deux éléments* z *et* z' *de* S *sont dans la même orbite, alors ils sont soit égaux soit dans le bord de* S.

Si l'on trouve un domaine fondammental de Γ dans $\mathbb{H}$, j sera donc presque injective sur ce domaine.

Proposition 4.4.3. **(i).** Γ *est engendré par :*

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(ii). *Soit :*

$$\mathcal{F} := \left\{ z \in \mathbb{H} \mid Re(z) \in \left[-\frac{1}{2}, \frac{1}{2}\right] \text{ et } |z| \geq 1 \right\}$$

Alors $\mathcal{F}$ *est un domaine fondammental de* Γ *dans* $\mathbb{H}$.

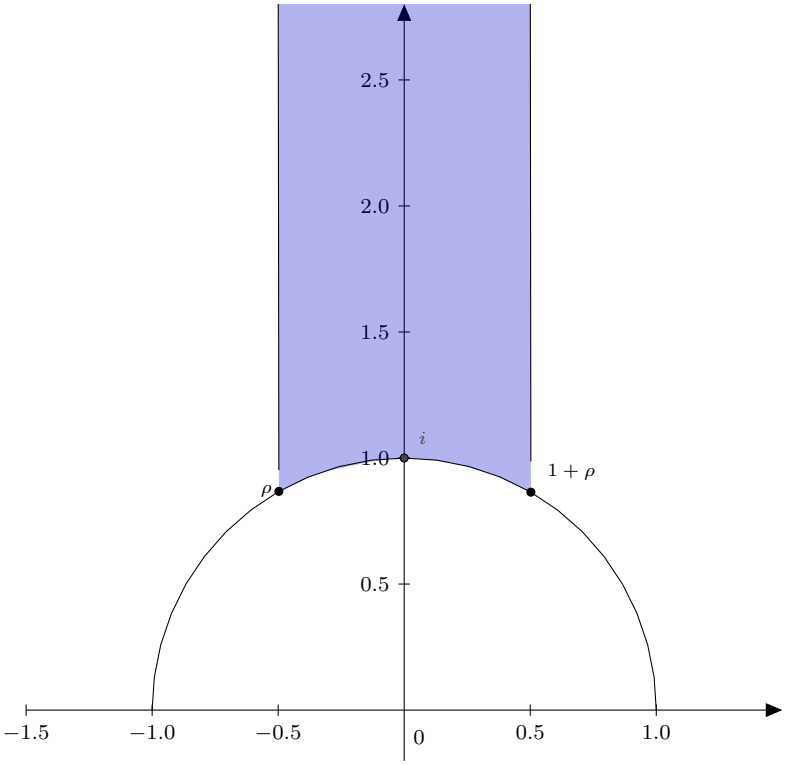


FIGURE 3 – Domaine fondammental $\mathcal{F}$ de Γ dans $\mathbb{H}$ représenté en bleu avec $\rho := e^{\frac{2i\pi}{3}}$.

Démonstration. Voir annexe F.4.1 □

9. Les actions de groupes sont supposées connues par les membres du groupe de PSC donc le prérequis n'est pas introduit ici.

4.4.2 Fonctions méromorphes à l'infini.

Si l'on considère une fonction méromorphe f définie sur $\mathbb{H}$ et 1-périodique alors :

$$f^* : z \longmapsto f\left(\frac{1}{2i\pi}\ln(z)\right)$$

est bien définie et méromorphe sur D^*, le disque unité privé de 0 (la définition sur $\mathbb{R}_- \cap D^*$ ne posant pas de difficulté puisque ln est déterminé à $2i\pi$ près sur $\mathbb{R}_-$ et que f est 1-périodique).

Définition 4.4.4. *On dit que f est* méromorphe à l'infini *lorsque* 0 *est un pôle de f^*.*

Si c'est le cas f^* est développable en série de Laurent au voisinage de 0 :

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

avec $N \in \mathbb{Z}$ et $c_N \neq 0$. Les c_n sont appelés les *coefficients de Fourier* de f et N, l'ordre de f à l'infini noté $\mathrm{ord}_\infty(f)$.
Remarque : Par ce procédé, nous venons de ramener l'étude du pôle à l'infini de f en l'étude d'un pôle en zéro de f^*, notion bien maîtrisée.

Proposition 4.4.5. *Soit f une fonction méromorphe à l'infini sur $\mathbb{H}$ invariante sous l'action de Γ, c'est à dire telle que pour tout $z \in \mathbb{H}$ qui n'est pas pôle de f et pour tout $P \in \Gamma$, on ait $f(P \cdot z) = f(z)$. Alors :*

$$ord_\infty(f) + \frac{1}{3}ord_\rho(f) + \frac{1}{2}ord_i(f) + \frac{1}{2}\sum_{\omega \in \partial\mathcal{F}\setminus\{\rho,i,\rho+1\}} ord_\omega(f) + \sum_{\omega \in \mathring{\mathcal{F}}} ord_\omega(f) = 0$$

avec $\rho := e^{\frac{2i\pi}{3}}$.

Démonstration. Voir annexe F.4.2 □

Nous allons appliquer le résultat précédent à j. Mais pour cela, il faut montrer que j est méromorphe à l'infini. On développe donc j^* en zéro grâce au lemme suivant :

Lemme 4.4.6. **(i).** *Pour tout $k \in \mathbb{N}^*$ la fonction donnée pour tout $\tau \in \mathbb{H}$ par :*

$$s_{2k}(\tau) := s_{2k}(\mathbb{Z} + \tau\mathbb{Z}) = \sum_{n,m \in \mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(n+\tau m)^{2k}}$$

introduite dans la proposition 4.2.3 admet le développement de Fourier suivant sur $\mathbb{H}$ tout entier :

$$s_{2k}(\tau) = 2\zeta(2k) + \frac{2(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{+\infty}\left(\sum_{d|n} d^{2k-1}\right)e^{2in\pi\tau}$$

(ii). *j est méromorphe à l'infini, de développement de Fourier à l'infini donné par :*

$$j^*(z) = \frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n$$

où $(c_n)_{n\in\mathbb{N}}$ est une suite d'entiers.

Démonstration. Voir annexe F.4.2 □

La combinaisons de ces deux résultats nous permet de démontrer le théorème attendu.

Théorème 4.4.7. **(i).** *La fonction j induit une surjection entre $\mathcal{F}$, le domaine fondammental du groupe modulaire dans $\mathbb{H}$ et $\mathbb{C}$. Deux éléments $\mathcal{F}$ ont la même image par j si et seulement si ils sont dans le bord de $\mathcal{F}$.*

(ii). *Toute courbe elliptique sur $\mathbb{C}$ peut ainsi être représentée par un groupe de la forme $\mathbb{C}/\Lambda$, où Λ est un réseau de $\mathbb{C}$.*

Démonstration. Voir annexe F.4.2 □

4.5 Courbes elliptiques, réseaux de $\mathbb{C}$ et isogénies.

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 ?

Commençons par remarquer que si Λ_1 et Λ_2 sont deux réseaux de $\mathbb{C}$ et si $\alpha \in \mathbb{C}^*$ vérifie $\alpha\Lambda_1 \subset \Lambda_2$ alors on peut définir :

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

Théorème 4.5.1. **(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 f sur $\mathbb{C}$, s'annulant en 0 et vérifiant :*

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

(ii). *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 dans le théorème 4.3.1, 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 bien définie et c'est une bijection.

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

Démonstration. Voir annexeF.5 □

4.6 Polynômes modulaires.

Le polynôme modulaire d'ordre n, noté Φ_n est un polynôme à deux variables qui intervient dans l'étude des isogénies de noyau cyclique de degré n. On montrera notamment dans ce paragraphe qu'il existe une telle isogénie entre deux courbes elliptiques E et F définies sur $\mathbb{C}$ si et seulement si $\Phi_n(j(E), j(F)) = 0$. Ceci est aussi valable sur $\mathbb{Q}_p$ d'après l'argument donné en début de section.

4.6.1 Matrices primitives et isogénies.

Définition 4.6.1. *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 [10] par tout élément de Γ. En effet, si un entier d divise tous les coefficients de QP pour $P \in P_n$ et $Q \in \Gamma$ 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 Γ sur P_n par multiplication à droite.

La raison pour laquelle nous introduisons ces matrices est l'existence d'une correspondance entre les isogénies de noyau cyclique d'ordre n et les orbites des éléments de P_n sous l'action de Γ par multiplication à gauche.

Proposition 4.6.2. *Toutes les matrices de P_n sont équivalentes en prenant des matrices de Γ pour matrices de passage.*

Démonstration. Soit $P \in P_n$. D'après la proposition B.2.11, on dispose de $Q, R \in GL_2(\mathbb{Z})$ tels que $QPR = \mathrm{Diag}(d_1, d_2)$ avec $d_1, d_2 \in \mathbb{Z}$ et $d_1 | d_2$. Comme P et Q sont obtenues par des opérations élémentaires dans $SL_2(\mathbb{Z})$, on a en fait $P, Q \in \Gamma$. 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 $d_2 = \pm n$. Mais dans Γ, $-I_2 = I_2$ donc on peut supposer que $d_1 = 1$ et $d_2 = n$, quitte à multiplier Q par -1. Il s'ensuit que toutes les matrices de P_n sont équivalentes à la même matrice donc équivalentes entre elles. □

10. Ceci est vrai aussi pour la multiplication à droite, mais sans pour autant faire de politique, nous nous limiterons à l'action à gauche.

Proposition 4.6.3. *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 Γ par multiplication à gauche.

Démonstration. Voir annexe F.6.1 □

Maintenant que nous comprenons bien P_n, voyons le lien avec les isogénies. Comme nous l'avons vu dans la sous-section précédente, si E_1 et E_2 sont des courbes elliptiques représentées respectivement par des réseaux Λ_1 et Λ_2 alors une isogénie 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 noyau de cette isogénie 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 $\frac{1}{\alpha}\Lambda_2/\Lambda_1$.**

Il s'agit donc d'étudier ce groupe. On se donne (ω_1, ω_2) une base de Λ_1 et (ω_3, ω_4) une base de $\frac{1}{\alpha}\Lambda_2$.Notons P la transposée de la matrice de passage de (ω_3, ω_4) à (ω_1, ω_2). Alors on a le résultat suivant :

Proposition 4.6.4. *Le groupe $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ est cyclique d'ordre n si et seulement si $P \in P_n$.*

Démonstration. Voir annexe F.6.1 □

4.6.2 Le polynôme modulaire.

Proposition 4.6.5. *Soit f une fonction méromorphe à l'infini invariante sous l'action de Γ. 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 $N := -\mathrm{ord}_\infty(f)$. Si $N \leq 0$, alors f^* est bornée au voisinage de 0 donc f est bornée sur $\mathbb{C}$ (car elle ne peut diverger en l'infini) et ainsi f est constante, donc le résultat désiré est immédiat dans ce cas. Si maintenant $N \in \mathbb{N}^*$ et que l'on suppose le résultat vrai aux rangs $\leq N-1$. Alors on écrit le développement de Fourier de f :

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

avec $c_{-N} \neq 0$. D'après le lemme 4.4.6, $f - c_{-N} j^N$ est méromorphe à l'infini et invariante sous l'action de Γ d'ordre $-(N-1)$ à l'infini. Donc c'est un polynôme en j à coefficients dans le $\mathbb{Z}$-module engendré par les coefficients de Fourier de $f - c_{-N} j^N$, qui sont aussi dans le module engendré par les coefficients de Fourier de f (puisque j est à coefficients de Fourier entiers d'après le lemme 4.4.6). 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 4.6.6. *On appelle n-ième polynôme modulaire le polynôme donné par :*

$$\Phi_n(X) = \prod_{P \in R_n} (X - j \circ P)$$

Proposition 4.6.7. *Φ_n est à coefficients dans $\mathbb{Z}[j]$.*

Démonstration. L'idée clé est d'utiliser la proposition 4.6.5. Le lecteur peut voir les détails en annexe F.6.2 □

On peut donc remplacer j par une indéterminée Y, et voir Φ_n comme un polynôme à deux variables.

Proposition 4.6.8 (relation de Kronecker)**.** *On a pour tout nombre premier p :*

$$\Phi_p(X, Y) \equiv (X - Y^p)(X^p - Y)\,[p]$$

Démonstration. Voir annexe F.6.2 □

4.6.3 Polynôme modulaire et isogénies.

Théorème 4.6.9. *Soient E_1 et E_2 deux courbes elliptiques sur $\mathbb{C}$. Alors il existe une isogénie de degré n entre E_1 et E_2 si et seulement si :*

$$\Phi_n(j(E_1), j(E_2)) = 0$$

Démonstration. Soient Λ_1 et Λ_2 les réseaux de $\mathbb{C}$ respectivement associés à E_1 et E_2. Ecrivons $j(E_1) = j(\Lambda_1) = j(\tau')$ et $j(E_2) = j(\Lambda_2) = j(\tau)$ avec $\tau, \tau' \in \mathcal{F}$, comme le théorème 4.4.7 nous autorise à le faire. On a alors :

$$\Phi_n(j(E_1), j(E_2)) = \Phi_n(j(\tau), j(\tau')) = \prod_{P \in R_n} (j(\tau') - j(P \cdot \tau))$$

qui vaut 0 si et seulement si $j(\tau') = j(P \cdot \tau)$ pour une certaine matrice $P \in R_n$, ce qui équivaut à $\tau' = P \cdot \tau$ pour une certaine matrice $P \in P_n$ (puisque j est injective modulo l'action de Γ).

S'il existe une isogénie de degré n entre E_1 et E_2, alors comme dans le paragraphe 4.6.1, on peut prendre un représentant $\alpha \in \mathbb{C}^*$ de cette isogénie vérifiant $\alpha\Lambda_1 \subset \Lambda_2$, (ω_1, ω_2) et (ω_3, ω_4) des bases respectives de Λ_1 et $\frac{1}{\alpha}\Lambda_2$. $(\alpha\omega_3, \alpha\omega_4)$ est alors une base de Λ_2. On peut donc choisir ces bases de sorte que $\tau = \frac{\alpha\omega_3}{\alpha\omega_4} = \frac{\omega_3}{\omega_4}$ et $\tau' = \frac{\omega_1}{\omega_2}$. Si P désigne la matrice de passage de (ω_3, ω_4) à (ω_1, ω_2), on a alors $\tau' = P \cdot \tau$ et $P \in P_n$ d'après la proposition 4.6.4, donc $\Phi_n(j(E_1), j(E_2)) = 0$ d'après le raisonnement précédent.

Réciproquement, si $\Phi_n(j(E_1), j(E_2)) = 0$ alors $\tau' = P \cdot \tau$ pour une certaine matrice $P \in P_n$. On peut donc considérer (ω_1, ω_2) et (ω_3, ω_4) des bases respectives de Λ_1 et Λ_2 telles que $\tau' = \frac{\omega_1}{\omega_2}$ et $\tau = \frac{\omega_3}{\omega_4}$. On a alors :

$$\frac{\omega_1}{\omega_2} = \frac{a\omega_3 + b\omega_4}{c\omega_3 + d\omega_4}$$

En posant $\alpha := \frac{c\omega_3 + d\omega_4}{\omega_2}$, on a alors $\omega_1 = a\frac{\omega_3}{\alpha} + b\frac{\omega_4}{\alpha}$ et $\omega_2 = c\frac{\omega_3}{\alpha} + d\frac{\omega_4}{\alpha}$ donc $\alpha\Lambda_1 \subset \Lambda_2$ et P est la matrice de passage de $\left(\frac{\omega_3}{\alpha}, \frac{\omega_4}{\alpha}\right)$ (base de $\frac{1}{\alpha}\Lambda_2$) à (ω_1, ω_2) donc l'isogénie entre E_1 et E_2 représentée par α est de noyau cyclique d'ordre n d'après la proposition 4.6.4.

□

⋆

Dans cette section, nous avons introduit un outil de calcul utile à Satoh. Tel sera aussi l'objet de la section suivante sur le groupe formel.

5 Groupe formel

Nous avons vu précédemment l'intérêt de pouvoir calculer les objets manipulés pour mieux les comprendre (fonctions rationnelles, isogénies, j-invariant etc) en faisant des développement en série. Dans le même esprit, nous "développons en série la loi de groupe" d'une courbe elliptique (au troisième paragraphe) avant d'appliquer ces résultats aux calculs des isogénies (dans les deux derniers paragraphes).

La définition d'un groupe formel en général et du groupe formel d'une courbe elliptique en particulier est faite dans [7] et [12].

5.1 Généralités sur les groupes formels.

Définition 5.1.1. *Soit $\mathbb{A}$ un anneau. On appelle groupe formel sur $\mathbb{A}$ une série formelle $F \in \mathbb{A}[\![X,Y]\!]$ telle que :*

1. $F(X,Y) = F(Y,X)$
2. $F(F(X,Y),Z) = F(X,F(Y,Z))$
3. $F(X,0) = X$

Remarquons qu'on ne manipule que des séries formelles sans terme constant, ce qui permet de donner un sens à la composée de deux séries formelles.

Proposition 5.1.2. *Soit F un groupe formel sur $\mathbb{A}$. F vérifie de plus les deux proporiétés suivantes :*

1. $F(X,Y) = X + Y +$ *(termes de degré* $\geqslant 1$*)*
2. *Il existe $i(X) \in \mathbb{A}[\![X]\!]$ telle que $F(X,i(X)) = F(i(X),X) = 0$*

Démonstration. Voir annexe G.1 □

Remarque : $i(X)$ joue le rôle de l'inversion. C'est pourquoi un groupe formelle s'identifie bien à une loi de groupe.

Exemples :

— La série formelle somme : $F(X,Y) = X + Y, i(X) = -X$

— La série formelle produit : $F(X,Y) = (X+1)(Y+1) - 1, i(X) = -X + X^2 - X^3 + \cdots$

On voit qu'un groupe formel F sur $\mathbb{A}$ induit une loi de groupe sur l'ensemble $X\mathbb{A}[\![X]\!]$ en posant $f \oplus g = F(f,g)$. On montre la réciproque dans le lemme suivant.

Lemme 5.1.3. *Soit $F \in \mathbb{A}[\![X,Y]\!]$ sans terme constant. Posons pour $f,g \in X\mathbb{A}[\![X]\!]$, $f \oplus g = F(f,g)$. Si $\oplus$ est associative, commutative et admet 0 comme élément neutre, alors F est un groupe formel.*

Démonstration. Voir annexe G.1 □

On peut maintenant énoncer une proposition qui nous sera utile pour construire le groupe formel d'une courbe elliptique.

Proposition 5.1.4. *Soit G un groupe abélien et $F \in \mathbb{A}[\![X,Y]\!]$ sans terme constant. S'il existe une injection $Q : X\mathbb{A}[\![X]\!] \to G$ telle que $Q(0) = 0$ et pour $f,g \in X\mathbb{A}[\![X]\!]$, on a $Q(f) + Q(g) = Q(F(f,g))$, alors F est un groupe formel.*

Démonstration. Définissons $\oplus$ comme dans le lemme 5.1.3. On a $Q(f \oplus g) = Q(f) + Q(g) = Q(g) + Q(f) = Q(g \oplus f)$ donc $\oplus$ commutative par injectivité de Q. De même, $\oplus$ est associative par associativité de la loi de G. Enfin, on a $Q(f \oplus 0) = Q(f) + Q(0) = Q(f) + 0$ puis $f \oplus 0 = f$. $\oplus$ vérifie donc les hypothèses du lemme 5.1.3, puis F est un groupe formel. □

5.2 Morphismes de groupes formels.

Nous calculerons dans la section suivante le groupe formel associé à une courbe elliptique. **Comme la finalité est d'utiliser ce groupe formel pour calculer des isogénies, il est tout à fait naturel de chercher à savoir si cette notion admet un analogue formel.**

Définition 5.2.1. *Soient F,G des groupes formels sur $\mathbb{A}$. On appelle morphisme de groupes formels de F vers G une série formelle $f \in \mathbb{A}[\![X]\!]$ telle que $f(F(X,Y)) = G(f(X),f(Y))$. On note $Hom(F,G)$ l'ensemble de ces morphismes. On dit que F et G sont isomorphes s'il existe f un morphisme de F vers G et g un morphisme de G vers F tels que $g(f(x)) = f(g(X)) = X$.*

Exemple Pour $m \in \mathbb{Z}$, on définit $[m]$ par :

$$\begin{cases} [0](X) = 0 \\ [m+1](X) = F([m](X), X) \\ [m-1](X) = F([m](X), i(X)) \end{cases}$$

On a alors :

Proposition 5.2.2. **(i).** *$[m](X)$ est un homomorphisme sur F*

(ii). *$[m](X) = mX + O(X^2)$*

(iii). *Si $m \in \mathcal{U}(\mathbb{A})$, alors $[m](X)$ est un isomorphisme.*

Démonstration. Voir annexe G.2 □

5.3 Groupe formel d'une courbe elliptique.

Soit E une courbe elliptique sur un corps $\mathbb{K}$ de polynôme de Weierstrass général

$$W(X,Y) := Y^2 - X^3 + a_1XY - a_2X^2 + a_3Y - a_4X - a_6$$

Notons $\mathbb{K}((T))$ le corps des fractions de l'anneau $\mathbb{K}[\![T]\!]$.

L'idée derrière l'introduction du paramètre local $\tau = -\frac{X}{Y}$ d'une courbe elliptique est de pouvoir considérer un "développement en série entière"de la courbe autour de son élément neutre $[0:1:0]$.

Remarquons tout d'abord que pour $f \in \mathbb{K}(E)$, on dispose d'un "développement en série entière en $\mathcal{O}$" de f.

Proposition 5.3.1. *Munissons $\mathbb{K}(E)$ de la norme associée à l'ordre en $\mathcal{O}$. Il existe un morphisme de corps isométrique $\Phi : \mathbb{K}(E) \to \mathbb{K}((T))$ (pour les valuations $ord_{\mathcal{O}}$ au départ et v_T à l'arivée).*

Démonstration. Soit τ une uniformisante en $\mathcal{O}$. D'après le théorème 2.1.15, appliqué avec K une complétion de $\mathbb{K}(E)$ et $S(K) = \mathbb{K}$, tout $f \in \mathbb{K}(E)$ s'écrit de manière unique

$$f = \sum_{n \geq ord_{\mathcal{O}}(f)} a_n \tau^n$$

avec le a_n dans $\mathbb{K}$. On pose donc $\Phi : \mathbb{K}(E) \to \mathbb{K}((X))$ qui à f associe $\sum_{n \geq ord_{\mathcal{O}}(f)} a_n X^n$ avec les a_n définis comme ci-dessus. On vérifie aisément que f est une isométrie (donc f injective) et un morphisme de corps. □

On voudrait à présent définir une loi de groupe formel sur $\mathbb{K}$ à partir de la loi de groupe de E. Pour cela, on considère la courbe $E(\mathbb{K}((T)))$, munie d'une structure de groupe et qui contient $E(\mathbb{K})$. D'après la proposition 5.1.4, il suffit de disposer d'une injection Q de $T\mathbb{K}[\![T]\!]$ dans $E(\mathbb{K}((T)))$ et d'une série formelle $F \in \mathbb{K}[\![X,Y]\!]$ tels que pour $f, g \in T\mathbb{K}[\![T]\!]$, on ait $Q(f) + Q(g) = Q(F(f,g))$. Les constructions de Q et de F étant assez techniques, on renvoit le lecteur à l'annexe G.3 pour plus de détails.

5.4 Les Formules de Vélu.

Soit E une courbe elliptique sur un corps $\mathbb{K}$ et G un sous-groupe fini de E. Les développements sur le groupe formel nous permettent de fournir des formules explicites pour la courbe E/G et l'isogénie $\phi : E \to E/G$ de noyau G dont l'existence est affirmée dans le théorème E.9.5 rappelé ci-dessous :

Théorème 5.4.1 (admis)**.** *(théorème E.9.5) Soit G un sous-groupe fini d'une courbe elliptique E. Alors il existe un couple (φ, E') où E' est une courbe elliptique et φ une isogénie de $Hom(E, E')$ telle que $ker(\varphi) = G$. Le couple (φ, E') est unique à isomorphisme près.*

Ces formules, les formules de Vélu, sont exposées avec précision dans [10]. Elles nous seront utiles pour le calcul des premiers coefficients des Verschiebungs utilisés par l'algorithme de Satoh. Comme ces formules ne sont pas essentielles à la compréhension du reste du document, nous ne les avons pas reproduites ici. Le lecteur pourra les consulter en annexe G.4.

5.5 Groupe formel et isogénies.

Soient E_1 et E_2 deux courbes elliptiques de polynômes de Weierstrass respectifs W_1 et W_2, de paramètres locaux en $\mathcal{O}$ τ_1 et τ_2 et de groupes formels associés respectifs F_1 et F_2. Si $\varphi \in \mathrm{Hom}(E_1, E_2)$ est une isogénie alors $\tau_2 \circ \varphi$ est une fonction rationnelle sur E_1, développable en série formelle par rapport à τ_1 (puique les fonctions X et Y de E_1 le sont, comme nous l'avons vu précédemment). En outre, $\varphi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$, de sorte que $\tau_2 \circ \varphi(\mathcal{O}_{E_1}) = 0$, et donc que $\tau_2 \circ \varphi$ est de valuation ≥ 1 dans l'anneau de valuation discrète $\mathbb{K}[E_1]_{\mathcal{O}}$, dont τ_1 est une uniformisante. On a donc un développement de la forme :

$$\tau_2 \circ \varphi = \sum_{n=1}^{+\infty} a_n \tau_1^n$$

pour $(a_n)_{n\in\mathbb{N}^*} \in \mathbb{K}^{\mathbb{N}}$. On peut donc définir l'application :

$$\begin{array}{rcl} \Psi : \mathrm{Hom}(E_1, E_2) & \longrightarrow & T\mathbb{K}[\![T]\!] \\ \varphi & \longmapsto & \Phi_1(\tau_2 \circ \varphi) \end{array}$$

où $\Phi_1 : \mathbb{K}(E_1) \longrightarrow T\mathbb{K}[\![T]\!]$ est l'application définie à la proposition 5.3.1.

Théorème 5.5.1 (isogénies et groupe formel). **(i).** *L'application Ψ précédente est à valeurs dans $Hom(F_1, F_2)$, l'ensemble des morphismes de groupes formels entre F_1 et F_2 et c'est un morphisme injectif de groupes.*

(ii). *Si E_3 est une courbe elliptique de paramètre local en $\mathcal{O}$ τ_3 et si $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_2, E_3)$ alors on a la formule :*

$$\tau_3 \circ (\psi \circ \varphi) = (\tau_3 \circ \psi) \circ (\tau_2 \circ \varphi)$$

où la composition du milieu à droite est la composition des séries formelles, tandis que celle de gauche est la composition de l'isogénie $\psi \circ \varphi$ par la fonction τ_3.

Démonstration. Voir annexe G.5 □

⋆

La liste des ingrédients mathématiques de l'algorithme de Satoh est très longue, et pas encore terminée... Et pour cause ! Il manque un ingrédient essentiel : la notion de relèvement p-adique d'une courbe elliptique. Ceci nous donnera aussi l'occasion d'appliquer quelques résultats de la section précédente.

6 Relèvement d'une courbe elliptique définie sur $\mathbb{F}_q$.

Dans cette section, on étudie la notion de relèvement p-adique d'une courbe elliptique, tout à fait centrale dans l'algorithme de Satoh.

Le premier paragraphe définit la notion de relèvement p-adique et de réduction. Dans le deuxième paragraphe, on "évalue" le groupe formel afin d'étudier le comportement du paramètre local lorsque l'on réduit modulo p. On y présente aussi une application du groupe formel au calcul de la trace. Enfin, le troisième paragraphe définit ce qu'est un "bon" relèvement p-adique et énonce les conditions de son existence.

6.1 Relèvement de la courbe et réduction modulo p.

Dans toute la suite de cette section, on fixe une courbe elliptique E définie sur $\mathbb{F}_q$. Comme $\text{car}(\mathbb{F}_q) = p \neq 2, 3$, le polynôme de Weierstrass de E est à changement de variables près :

$$f(X, Y) := Y^2 - X^3 - AX - B$$

avec $A, B \in \mathbb{F}_q$ avec $\Delta = -16(4A^3 + 27B^2) \neq 0$. On suppose que $AB \neq 0$.

Définition 6.1.1. *On appelle* relèvement p-adique de E, *toute courbe $\tilde{E}$, d'équation de Weierstrass :*

$$Y^2 = X^3 + \tilde{A}X + \tilde{B}$$

définie sur $\mathbb{Z}_q$ dont la réduction modulo p des coefficients donne E.

On peut considérer la réduction modulo p des points entre $\tilde{E}$ et E :

$$\pi : [x : y : z] \in \tilde{E} \longrightarrow [\overline{x} : \overline{y} : \overline{z}] \in E$$

précisons que dans le cas où l'une des coordonnées, x, y, z est de valuation négative, on peut considérer $k := -\min(v_p(x), v_p(y), v_p(z))$ et utiliser le fait que :

$$[x : y : z] = [p^k x : p^k y : p^k z]$$

avant de réduire le terme de droite, dont les composantes sont de valuation positive.

Faisons une première remarque sur la réduction des points de $\tilde{E}$. Soit $P := (x, y) \in E \setminus \{\mathcal{O}\}$, que l'on peut écrire $P := [x : y : 1]$ dans $\mathbb{P}^3(\overline{\mathbb{Q}_q})$. Si $v_p(x) < 0$ alors comme :

$$y^2 = x^3 + \tilde{A}x + \tilde{B}$$

avec $v_p(\tilde{A}), v_p(\tilde{B}) = 0$ car $AB \neq 0$ et $v_p(x) < 0$; on a d'après le point (i). du lemme 2.1.4 :

$$2v_p(y) = v_p(x^3 + \tilde{A}x + \tilde{B}) = 3v_p(x)$$

Donc $v_p(x) = -2k$ et $v_p(y) = -3k$ avec $k \in \mathbb{N}^*$. On a donc $P = [p^{3k}x : p^{3k}y : p^{3k}]$ avec $p^{3k}x$ et $p^{3k}y$ de valuation positive donc la réduction de P s'écrit :

$$\overline{P} = [\overline{p^{3k}x} : \overline{p^{3k}y} : \overline{p^{3k}}] = [0 : \overline{p^{3k}y} : 0] = [0 : 1 : 0] = \mathcal{O}$$

A l'inverse, si $v_p(x) \geq 0$, alors $v_p(y) = 0$ d'après l'équation de Weierstrass et donc on peut directement réduire modulo p pour obtenir un point distinct de $\mathcal{O}$. Nous venons donc de montrer la :

Proposition 6.1.2.

$$ker(\pi) = \{P \in E \mid v_p(x(P)) < 0\} \cup \{\mathcal{O}\}$$

6.2 Réduction modulo p et groupe formel.

Dans ce paragraphe $(\mathbb{A}, v)$ désignera un anneau de valuation discrète normalisée (i.e. telle que $v(\mathbb{A}) = \mathbb{N}$), $M_{\mathbb{A}}$ son idéal maximal formé des éléments de valuation ≥ 1, et $F(X, Y) \in \mathbb{A}[\![X, Y]\!]$, un groupe formel à coefficients dans $\mathbb{A}$.

On suppose que pour tous $x, y \in M_{\mathbb{A}}$, la série $F(x, y)$ converge dans $M_{\mathbb{A}}$. Ceci est vrai lorsque $\mathbb{A}$ est complet pour la topologie associée à v mais nous verrons qu'une hypothèse plus faible suffit. On munit alors $M_{\mathbb{A}}$ de la loi de groupe $\oplus_F$ donnée par :

$$\forall x, y \in M_{\mathbb{A}}, \quad x \oplus_F y = F(x, y)$$

Notons τ le paramètre local à l'infini $\mathcal{O}$ de $\tilde{E}$ donné par :

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

pour tout $P \in E\backslash\{\mathcal{O}\}$ et $\tau(\mathcal{O}) = 0$. On munit l'ensemble $M_{\overline{\mathbb{Q}_q}}$ des éléments de $\overline{\mathbb{Q}_q}$ de valuation strictement positive muni des lois d'additions sur le groupe formel de la loi de groupe $\oplus_{F_{\tilde{E}}}$ où $F_{\tilde{E}}$ est le groupe formel associé à $\tilde{E}$. On vérifie que cette loi de groupe est bien définie à l'aide du lemme suivant.

Lemme 6.2.1. *Soient $x, y \in M_{\overline{\mathbb{Q}_q}}$. Alors $F_{\tilde{E}}(x, y)$ est bien défini et c'est un élément de $M_{\overline{\mathbb{Q}_q}}$.*

Démonstration. Voir H. □

Proposition 6.2.2.

$$\tau : ker(\pi) \longmapsto M_{\overline{\mathbb{Q}_q}}$$

est un isomorphisme de groupes.

Démonstration. Voir H. □

Remarque : La discussion précédente reste valable en remplaçant $\overline{\mathbb{Q}_q}$ par $\mathbb{Q}_q^{nr}$ et les arguments sont les mêmes. En particulier :

$$\tau : \ker(\pi) \cap \tilde{E}(\mathbb{Q}_q^{nr}) \longmapsto p\mathbb{Z}_q^{nr}$$

est un isomorphisme de groupes pour l'addition $\oplus_{F_{\tilde{E}}}$ à l'arrivée. C'est surtout dans $\mathbb{Q}_q^{nr}$ que nous utiliserons ces résultats.

Puisque $M_{\overline{\mathbb{Q}_p}}$ et $p\mathbb{Z}_q^{nr}$ sont munies des mêmes lois que le groupe formel $F_{\tilde{E}}$, on peut définir des morphismes sur ces groupes en évaluant les morphismes de groupes formels définis au paragraphe 5.1. C'est ainsi que l'on peut définir le morphisme $[m]$ pour tout $m \in \mathbb{N}^*$ qui coincide avec la multiplication par m des points de la courbe, c'est à dire que :

$$\forall P \in \tilde{E}, \quad \tau([m]P) = [m]\tau(P)$$

La proposition 5.2.2 donne alors immédiatement que :

Proposition 6.2.3. *$[m]$ est un isomorphisme de $M_{\overline{\mathbb{Q}_p}}$ dans lui-même (et de $p\mathbb{Z}_q^{nr}$ dans lui-même).*

Le point de vue groupe formel pour les morphismes permet d'effectuer certains calculs. Pour comprendre le résultat qui suit, on gardera bien à l'esprit le paragraphe 5.5

Proposition 6.2.4. *Soit $\varphi \in End(\tilde{E})$ une isogénie non nulle de développement en $\mathcal{O}$ associé $\tau \circ \phi := \sum_{n=1}^{+\infty} c_n \tau^n$. Alors :*

$$Tr(\varphi) = c_1 + \frac{deg(\varphi)}{c_1}$$

Démonstration. D'après le théorème de Cayley Hamilton appliqué dans $T_l(\tilde{E})$, on obtient l'égalité suivante dans $\mathrm{End}(\tilde{E})$ (par injectivité de l'application $\phi \in \mathrm{End}(\tilde{E}) \longmapsto \phi_l \in \mathrm{End}(T_l(\tilde{E}))$) :

$$\varphi^2 + \mathrm{Tr}(\varphi)\varphi + \deg(\varphi) = 0$$

En composant par τ et en réinjectant le développement $\tau \circ \phi := \sum_{n=1}^{+\infty} c_n \tau^n$ dans cette égalité, on obtient grâce au théorème 5.5.1 que :

$$(c_1^2 + c_1\mathrm{Tr}(\varphi) + \deg(\varphi))\tau + O(\tau^2) = 0$$

Donc $c_1^2 + c_1\mathrm{Tr}(\varphi) + \deg(\varphi) = 0$. Comme φ est non nulle, $\deg(\varphi) \neq 0$ et donc $c_1 \neq 0$. On en déduit que :

$$\mathrm{Tr}(\varphi) = c_1 + \frac{\deg(\varphi)}{c_1}$$

□

6.3 Comment bien relever les isogénies ?

Relever la courbe E n'est pas suffisant pour l'algorithme de Satoh, puisqu'il est aussi intéressant de "bien" relever les isogénies.

Définition 6.3.1. *Si E_1 et E_2 sont deux courbes elliptiques, $\tilde{E}_1$, $\tilde{E}_2$ des relèvements p-adiques respectifs de ces courbes et si $\phi \in Hom(E_1, E_2)$ est une isogénie entre E_1 et E_2 alors on appelle* relèvement de ϕ *une isogénie $\tilde{\phi}$ telle que :*

$$\phi \circ \pi = \pi \circ \tilde{\phi}$$

Lorsque l'on dispose d'une isogénie Ψ entre $\tilde{E}_1$ et $\tilde{E}_2$, il est facile de lui associer une isogénie $\pi(\Psi)$ entre E_1 et E_2 vérifiant l'égalité ci-dessus en posant pour tout $P \in E_1$:

$$\pi(\Psi)(P) := \pi(\Psi(\tilde{P}))$$

où $\tilde{P}$ est un relèvement quelconque de P. Ψ étant défini par des fractions racionnelles, il est aisé de vérifier que $\pi(\Psi(\tilde{P}))$ ne dépend pas du relèvement $\tilde{P}$ de P choisi. Réciproquement, on aimerait bien savoir si toute isogénie $\phi \in \mathrm{Hom}(E_1, E_2)$ admet un relèvement. Le théorème de Deuring, dont la preuve est fort difficile, assure que ceci est possible.

Théorème 6.3.2 (Deuring)**.** *(admis) Si la courbe elliptique E est ordinaire, alors il existe un relèvement $E^{\uparrow}$ de E tel que la réduction modulo p :*

$$\Psi \in End(E^{\uparrow}) \longmapsto \pi(\Psi)$$

induise un isomorphisme d'anneaux entre $End(E^{\uparrow})$ et $End(E)$. Ce relèvement est unique à isomorphisme près et on l'appelle relèvement canonique.

Nous utiliserons en outre les résultats suivants, admis aussi car difficiles :

Théorème 6.3.3 (Messing)**.** *(admis) Soient E_1 et E_2 des courbes elliptiques ordinaires sur $\mathbb{F}_q$. Alors la réduction modulo p induit un isomorphisme d'anneaux entre $Hom(E_1^{\uparrow}, E_2^{\uparrow})$ et $Hom(E_1, E_2)$.*

Ceci assure que toute isogénie ϕ entre E_1 et E_2 admet un unique relèvement $\phi^{\uparrow}$ entre $E_1^{\uparrow}$ et $E_2^{\uparrow}$. Cependant, il n'est pas intéressant de relever des isogénies sans connaître les propriétés géométriques du relèvement.

Proposition 6.3.4 (propriétés géométriques du relèvement des isogénies)**.** *Soient E_1 et E_2 des courbes elliptiques ordinaires sur $\mathbb{F}_q$ et $\phi \in Hom(E_1, E_2)$. Alors :*

(i). $deg(\phi) = deg(\phi^{\uparrow})$.

(ii). $Tr(\phi) = Tr(\phi^{\uparrow})$.

(iii). $\pi(ker(\phi^{\uparrow})) = ker(\phi)$.

$\star$

Nous disposons désormais tous les ingrédients mathématiques pour comprendre l'algorithme de Satoh. Voici donc le grand *finale* de ce rapport.

7 L'algorithme de Satoh.

Cette section a pour objet de faire la synthèse de tous les résultats vus jusqu'ici, afin d'étudier l'algorithme de Satoh. On présentera donc l'article originel de Satoh [1], publié en 1999. Pour les preuves et résultats techniques, on se reportera avec profit à l'annexe I.

Dans toute cette section, p sera un nombre premier ≥ 5 (le cas de la caractéristique 2 et 3 n'ayant pas été traité par Satoh). On posera $q := p^N$, et on désignera par $\mathbb{Q}_q$ une extension non ramifiée de $\mathbb{Q}_p$ de corps résiduel $\mathbb{F}_q$ (et donc de degré n). On désignera aussi par $\mathbb{Z}_q := O_{\mathbb{Q}_q}$ son anneau d'entiers, $\mathbb{Q}_q^{nr}$ son extension non ramifiée maximale et $\mathbb{Z}_q^{nr} := O_{\mathbb{Q}_q^{nr}}$ l'anneau d'entiers de cet extension. On notera enfin v_p la valuation p-adique et v_G la valuation de Gauss associée.

Nous savons que nous disposons d'une décomposition des éléments de $\mathbb{Q}_q$ sous forme de séries à coefficients dans le corps résiduel $\mathbb{F}_q$ (voir théorème 2.1.15). Bien sûr, comme il est impossible de travailler sur machine avec de tels entités mathématiques, nous devons les approcher à une certaine précision $u \in \mathbb{N}^*$, en tronquant les termes d'indice $\geq u$ dans la série, ce qui revient à travailler dans $\mathbb{Z}_q/p^u\mathbb{Z}_q$.

Dans toute la suite de cette section, on considère pour tout $i \in \{0, \cdots, N\}$, E_i la courbe elliptique d'équation de Weierstrass :

$$f_i(X,Y) := Y^2 - X^3 - A^{p^i}X - B^{p^i}$$

E_{i+1} est donc l'image de E_i par la p-ième isogénie de Frobenius :

$$\begin{array}{rcl} \mathrm{Fr}_i : E_i & \longrightarrow & E_{i+1} \\ (x,y) & \longmapsto & (x^p, y^p) \\ \mathcal{O} & \longmapsto & \mathcal{O} \end{array}$$

et E_i est l'image de E_{i+1} par l'isogénie de Verschiebung V_i, qui n'est autre que l'isogénie duale de Fr_i. Il est clair que $E_0 = E = E_N$.

Pour tout $i \in \{0, \cdots, N\}$, on note $E_i^\uparrow$, $V_i^\uparrow$ et $\mathrm{Fr}_i^\uparrow$ les relèvements p-adiques canoniques respectifs de E_i, V_i et Fr_i dont l'existence est assurée par le théorème de Deuring. Le but est de construire une approximation de ces objets afin de pouvoir calculer $\mathrm{Tr}(V_0^\uparrow \circ \cdots \circ V_{N-1}^\uparrow)$, qui nous donnera le nombre de points de E par un calcul facile. En effet, la trace d'une isogénie étant égale à celle de son isogénie duale, le théorème de Hasse assure que :

$$|E(\mathbb{F}_q)| = q + 1 - \mathrm{Tr}(V_0^\uparrow \circ \cdots \circ V_{N-1}^\uparrow)$$

Le schéma ci-dessous résumme le principe du relèvement p-adique de Satoh :

$$\begin{array}{ccccccccc} E^\uparrow & \xrightarrow{V_{N-1}^\uparrow} & E_{N-1}^\uparrow & \xrightarrow{V_{N-2}^\uparrow} & E_{N-2}^\uparrow & \cdots & E_1^\uparrow & \xrightarrow{V_0^\uparrow} & E^\uparrow \\ \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ E & \xrightarrow{V_{N-1}} & E_{N-1} & \xrightarrow{V_{N-2}} & E_{N-2} & \cdots & E_1 & \xrightarrow{V_0} & E \end{array}$$

7.1 Relèvement des j-invariants à l'aide du polynôme modulaire.

Afin de pouvoir relever correctement la courbe E_i pour tout $i \in \{0, \cdots, N\}$, il faut relever le j-invariant $j(E_i)$ en $j(E_i^\uparrow)$. Ceci peut se faire de façon peu coûteuse à l'aide du polynôme modulaire Φ_p, en utilisant le théorème 4.6.9. Les deux résultats suivants dus à Satoh donnent une implémentation efficiente de cette méthode.

Proposition 7.1.1. *Soient $m \in \mathbb{N}^*$ et $z_0, \cdots, z_{N-1} \in \mathbb{Z}_q$ vérifiant pour tout $i \in \{0, \cdots, N-1\}$:*

(i). $z_i \equiv z_{i+1}^p \,[p]$.

(ii). $\overline{z_i}^{p^2} \neq \overline{z_i}$.

(iii). $\Phi_p(z_i, z_{i+1}) \equiv 0 \,[p^m]$.

en convenant que $z_N := z_0$. Alors il existe $\zeta_0, \cdots, \zeta_{N-1} \in \mathbb{Z}_q$ dont les coefficients sont déterminés de façon unique modulo p^{2m}, vérifiant pour tout $i \in \{0, \cdots, N-1\}$:

(i). $\zeta_i \equiv z_i \,[p^m]$.

(ii). $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0 \,[p^{2m}]$.

en convenant de nouveau que $\zeta_N := \zeta_0$.

De plus, connaissant le résidu modulo p^{2m} de Φ_p, on peut calculer les $\zeta_i \,[p^{2m}]$ en $O(N)$ opérations sur $\mathbb{Z}_q/p^{2m}\mathbb{Z}_q$.

Démonstration. Voir annexe I.3 □

On en déduit du résultat précédent la méthode d'approximation des j-invariants $j(E_i^{\uparrow})$. Le résultat qui suit nous assure la convergence de cette méthode.

Proposition 7.1.2. *Supposons que $j(E) \neq j(E)^{p^2}$. Soient $(a_n)_{n\in\mathbb{N}}$ une suite strictement croissante d'entiers naturels non nuls et $(z_{0,n})_{n\in\mathbb{N}}, \cdots, (z_{N-1,n})_{n\in\mathbb{N}}$, N suites d'éléments de $\mathbb{Z}_q$ telles que pour tout $i \in \{0, \cdots, N-1\}$:*

(i). $\overline{z_{i,0}} = j(E_i)$.

(ii). $z_{i,n+1} \equiv z_{i,n}\,[p^{a_n}]$.

(iii). $\Phi_p(z_{i,n}, z_{i+1,n}) \equiv 0\,[p^{a_n}]$.

En convenant toujours que $(z_{N,n})_{n\in\mathbb{N}} = (z_{0,n})_{n\in\mathbb{N}}$. Alors pour tout $i \in \{0, \cdots, N-1\}$, $z_{i,n} \underset{n\to+\infty}{\longrightarrow} j(E_i^{\uparrow})$ et pour tout $n \in \mathbb{N}$, $z_{i,n} \equiv j(E_i^{\uparrow})\,[p^{a_n}]$.

Démonstration. Voir annexe I.3 □

Décrivons maintenant l'algorithme du relèvement des j-invariants :

	Relèvement des j-invariants.
ENTRÉES :	le vecteur $(j(E_i))_{0\leq i\leq N-1} = (j(E)^{p^i})_{0\leq i\leq N-1}$.
	la précision M à laquelle on souhaite approcher $(j(E_i^{\uparrow}))_{0\leq i\leq N-1}$ modulo p^M.
INITIALISATION :	$u := 1$ compteur de précision effective.
	$Z := (j(E_i))_{0\leq i\leq N-1}$
TRAITEMENT :	Tant que $u < M$:
	• $F(Z) := (\Phi_p(Z_0, Z_1), \Phi_p(Z_1, Z_2), \cdots, \Phi_p(Z_{N-1}, Z_0))$.
	• $Z := Z - Jac_Z(F)^{-1}F(Z)$.
	• $u := 2u$.
SORTIE :	$Z = (j(E_i^{\uparrow}))_{0\leq i\leq N-1}\,[p^M]$.

Cet algorithme est correct d'après les deux résultats précédents.

7.2 Algorithme de calcul du cycle de relèvements p-adiques.

Soit $\tilde{E}$ un relèvement p-adique quelconque de E, de polynôme de Weierstrass $Y^2 - X^3 - \tilde{A}X - \tilde{B}$. Notons pour toute partie S de $\overline{\mathbb{Q}_q}$, $\tilde{E}(S)$ l'ensemble des points de $\tilde{E}$ à coordonnées dans S ($\mathcal{O}$ inclus).

La question est de savoir à quelle précision $\tilde{E}$ doit-elle approcher $E^{\uparrow}$ pour que $\tilde{E}[p]$ se réduise sur $E[p]$. Pourquoi ceci est-il important ? Parce qu'en fait, $\ker(V_p) = E[p]$. Ainsi, comme $V_p^{\uparrow}$ est séparable et de même degré que V_p, la proposition 6.1.2 nous donne que $\ker(V_p^{\uparrow})$ est l'ensemble des points de $E^{\uparrow}[p]$ dont les coordonnées sont de valuation positive. On connait alors la réduction de ces points [11] donc en les relevant, on peut en théorie avoir accès à$\ker(V_p^{\uparrow})$

Comme $\ker(V_p^{\uparrow})$ est un groupe cyclique d'ordre p, il suffit en fait que $\tilde{E}[p] \cap \tilde{E}[\mathbb{Z}_q^{nr}] \neq \{\mathcal{O}\}$ pour que $\tilde{E}[p]$ se réduise sur $E[p]$. Le théorème suivant nous dit quand cela se produit.

Théorème 7.2.1. *Les assertions suivantes sont équivalents :*

(i). $\tilde{E}[p] \cap \tilde{E}[\mathbb{Z}_q^{nr}] \neq \{\mathcal{O}\}$.

(ii). *Il existe $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ tel que $\tau(pP) \in p^2\mathbb{Z}_q^{nr}$.*

(iii). *Il existe $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ tel que $\Psi_p(x(P), \tilde{A}, \tilde{B}) \equiv 0\,[p^2]$.*

(iv). $j(\tilde{E}) \equiv j(E^{\uparrow})\,[p^2]$.

Démonstration. Voir annexe □

Lemme 7.2.2. *Supposons que $\tilde{E}$ satisfasse l'une des conditions du théorème précédent. Alors pour tout $P \in \tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$:*

$$v_p\left(\frac{\partial \Psi_p}{\partial X}(x(P), \tilde{A}, \tilde{B})\right) = 1$$

Démonstration. Voir annexe I.4 □

11. C'est justement parce que le Frobenius est inséparable que nous perdons cette connaissance si l'on remplace V_p par Fr_p. D'où l'intérêt de considérer V_p dans l'algorithme de Satoh.

A partir des deux résultats précédents, on peut prouver le résultat central de l'algorithme de satoh, qui contient en substance toutes les étapes difficiles.

Théorème 7.2.3. *Soit $E : Y^2 = X^3 + AX + B$ une courbe elliptique sur $\mathbb{F}_q (q = p^N)$ telle que $j(E) \notin \mathbb{F}_{p^2}$, $E_i (0 \leq i \leq N-1)$ son image par Fr_p^i, $M \geq 2$ un entier. Alors on dispose d'un algorithme pour construire des courbes elliptiques $E^{((i))}$ sur $\mathbb{Z}_q$ et un polynôme $h^{((i))}$ à coefficients dans $\mathbb{Z}_q$ tels que :*

(i).

$$h^{((i))} \equiv \prod_{P \in \frac{G^{((i))} \setminus \{\mathcal{O}\}}{\{-1,1\}}} (X - x(P)) \text{ modulo } p^{M-1}$$

avec $G^{((i))} = E^{((i))}[p] \cap E^{((i))}(\mathbb{Z}_q^{nr})$

(ii). $j(E^{((i))}) \equiv j(E^{(i)\uparrow})$ modulo p^M

(iii). $\overline{A^{((i))}} = A^{p^i}$ et $\overline{B^{((i))}} = B^{p^i}$

(iv). $G^{((i))}$ est un groupe d'ordre p dont la réduction modulo p est la p-torsion de E_i

Les polynômes $h^{((i))}$ et les coefficients $A^{((i))}$ et $B^{((i))}$ peuvent être calculés avec $O(N \ln(M))$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$.

Démonstration. Voir annexe I.4 □

Voici l'algorithme décrit dans la preuve du théorème précédent. La correction théorique de ces programmes n'a rien d'évident. C'est pourquoi le lecteur intéressé est invité à se reporter en annexe I pour en voir une justification.

	Méthode de Newton.
ENTRÉES :	précision M. $P \in \mathbb{Z}_q[X]$ tel que $\overline{P}$ est séparable. $\xi \in \mathbb{F}_q$ une racine de $\overline{P}$.
INITIALISATION :	$u := 1$ compteur de précision effective. ζ relèvement quelconque de ξ.
TRAITEMENT :	Tant que $u < M$. • $\zeta := \zeta - \frac{P(\zeta)}{P'(\zeta)}$. • $u := 2u$.
SORTIE :	$\zeta \in \mathbb{Z}_q$ tel que $\zeta \equiv \xi\,[p]$ et $P(\zeta) \equiv 0[p^M]$.

	Relèvement de A, B.
ENTRÉES :	les coefficients $A, B \in \mathbb{F}_q$. la précision M.
INITIALISATION :	$Z := (j(E_i^{(i)\uparrow}))_{0 \leq i \leq N-1}$ calculé avec l'algorithme de relèvement des j-invariants.
TRAITEMENT :	Pour i allant de 0 à $N-1$ • $B^{((i))}$ est un relèvement quelconque de B^{p^i} modulo p^M. • $A^{((i))}$ est le relèvement à la précision M. de la racine A^{p^i} du polynôme $(4j(E_i^{(i)\uparrow}) - 1728)X^3 + 27j(E_i^{(i)\uparrow})B^{((i))3}$ calculée par méthode de Newton.
SORTIE :	$(A^{((i))}, B^{((i))})_{0 \leq i \leq N-1}$.

	Relèvement de facteurs polynomiaux (décrit par le lemme I.1.3)
ENTRÉES :	précision M. $P \in \mathbb{Z}_q[X]$ unitaire et $U \in \mathbb{Z}_q[X]$ et $t := v_G(U')$ tels que. (i). $\overline{P}$ est séparable. (ii). $\overline{P} \wedge \overline{p^{-t}U'(X)} = 1$. hspace0.5cm (iii). P divise U modulo p^{1+t}.
INITIALISATION :	$u := 1$ compteur de précision effective. $Q := P$ R reste dans la division euclidienne de U par Q $R_0 := p^{-t-u}R$ $R_1(X) = p^{-t}U'(X)$
TRAITEMENT :	Tant que $u < M$ • (U, V) couple de Bézout tel que $UQ + VR_1 \equiv 1[p^M]$ obtenu par l'algorithme d'Euclide étendu modulo p^M. • $B_1 := VR_0$ • R_2 reste de la division euclidienne de $Q'(X)B_1(X)$ par Q • $Q := Q + p^u R_2$ • $u := 2u$ R reste dans la division euclidienne de U par Q • $R_0 := p^{-t-u}R$
SORTIE :	$Q \in \mathbb{Z}_q[X]$ tel que Q divise U modulo p^M.

	Calcul des polynômes $h^{((i))}$.
ENTRÉES :	$(A^{((i))}, B^{((i))})_{0\leq i\leq N-1}$ calculé avec la fonction relèvement de A, B. la précision M.
INITIALISATION :	Calculer $(\Psi_i)_{0\leq i\leq N-1} := (\Psi_p(X, A^{((i))}, B^{((i))}))_{0\leq i\leq N-1}$.
TRAITEMENT :	Pour i allant de 0 à $N-1$ [12] • $f(X) = \sum_{k=0}^{\frac{p-1}{2}} \frac{u_k}{u_{\frac{p-1}{2}}} X^k$ où pour tout $k \in [\![0, \frac{p-1}{2}]\!]$ u_k est le coefficient devant X^{pk} de $\overline{\Psi_{i-1}}$ • $h^{((i))}$ relèvement du facteur f avec $U := \Psi_i$, $t := 1$ et $P := f$ dans l'algorithme précédent.
SORTIE :	$(h^{((i))})_{0\leq i\leq N-1}$.

7.3 Calcul effectif de la trace du Frobenius et comptage de points.

Proposition 7.3.1. *Soient $i \in \{1, \cdots, N\}$ et $\tau_i := -\frac{X}{Y}$ le paramètre local en $\mathcal{O}$ de $E_i^{\uparrow}$ et $c_{i,1} \in \mathbb{Z}_q$ le premier coefficient du développement du Verschiebung V_i :*

$$\tau_{i-1} \circ V_i = \sum_{n=1}^{\infty} c_{i,n} \tau_i^n$$

On suppose connus les coefficients $A_i^{\uparrow}$, $B_i^{\uparrow}$ et le polynôme unitaire et séparable $h_i^{\uparrow}(X)$ dont les racines sont les abscisses des points du groupe $G_i := E_i^{\uparrow}[p] \cap E_i^{\uparrow}(\mathbb{Z}_q^{nr})$ privé de $\mathcal{O}$. Alors on peut calculer $c_{i,1}^2$ avec $O(1)$ opérations sur $\mathbb{Z}_q$.

Démonstration. Voir annexe I.5 □

Remarque : Si l'on connait $A_i^{\uparrow}$, $B_i^{\uparrow}$ et $h_i^{\uparrow}(X)$ seulement à la précision p^M, alors on peut connaître $c_{i,1}^2$ à la précision p^M en $O(1)$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$.

Théorème 7.3.2. *Soit E une courbe elliptique non supersingulière définie sur $\mathbb{F}_q$, avec $q := p^N$. Si $j(E)^{p^2} \neq j(E)$, alors on il existe un algorithme permettant de déterminer $|E(\mathbb{F}_q)|$ avec $O(N \ln(M))$ opérations dans $\mathbb{Z}_q/p^M\mathbb{Z}_q$ (pour $M := \lfloor \frac{N}{2} \rfloor + 3$) et $O(N^2)$ opérations dans $\mathbb{F}_q$.*

Démonstration. Voir annexe I.5 □

Remarque : Rappelons que la complexité idiquée en section 1.3.4. est en $O(N^{3+\varepsilon})$. Comme le coût dominant concerne les opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$, cela signifie que les opérations arithmétiques sur cet anneau coûtent en $O(N^2)$.

Nous avons donc un algorithme efficient de comptage de points. Le seul ennui est qu'il ne fonctionne pas dans le cas $j(E) \in \mathbb{F}_{p^2}$. Satoh propose un algorithme qui fonctionne (mais pas toujours) dans ce cas-ci. Il est présenté en annexe I.6. En attendant, voici l'algorithme de Satoh générique.

	Calcul de la Trace modulo p.
ENTRÉES :	les coefficients $A, B \in \mathbb{F}_q$. la précision M.
INITIALISATION :	t_1 coefficient devant X^{p-1} de $(X^3 + AX + B)^{\frac{p-2}{2}}$. $t := t_1$.
TRAITEMENT :	Pour i allant de 1 à $N-1$ • $t := tt_1^{p^i}$
SORTIE :	t, trace de Fr_q modulo p.

	Algorithme de satoh.
ENTRÉES :	les coefficients $A, B \in \mathbb{F}_q$. la précision M.
INITIALISATION :	Calculer $(A^{((i))}, B^{((i))}, h^{((i))}(X))_{0 \leq i \leq N-1}$ avec les algorithmes précédents. $c_2 = 1$.
TRAITEMENT :	Pour i allant de 0 à $N-1$ • s_1 coefficient devant $X^{\frac{p-1}{2}-1}$ de $h^{((i))}(X)$. • s_2 coefficient devant $X^{\frac{p-1}{2}-2}$ de $h^{((i))}(X)$. • s_3 coefficient devant $X^{\frac{p-1}{2}-3}$ de $h^{((i))}(X)$. • $\alpha := (6-5p)A^{((i))} - 30(s_1^2 - 2s_2)$. • $\beta := (15-14p)B^{((i))} + 70(s_1^3 - 3s_1s_2 + 3s_3) + 42A^{((i))}s_1$. • $c_2 := c_2 \frac{A^{((i-1))}\beta}{B^{((i-1))}\alpha}$. • c, revelèvement de t modulo p^M avec la méthode de Newton appliquée à $\xi := t$ et $P := X^2 - c2$. • d est la conversion de c en entier. Si $d > 2\sqrt{q}$: • d est l'opposé de la conversion de $-c$ en entier. [13]
SORTIE :	$\lvert E(\mathbb{F}_q)\rvert = q + 1 - d$.

Conclusion.

Seule la présention de l'algorithme de Satoh pouvait conclure ce rapport de façon éloquente mais nous ne pouvions terminer sans ces quelques mots. Ce PSC nous a fait visiter de nombreuses contrées du beau pays des mathématiques, mais l'histoire s'arrête-t-elle ici ? Tant de choses ont été vues. Mais tout n'a pas été fait. Nous aurions par exemple aimé pouvoir comprendre le théorème de Deuring. Peut-être qu'une étude plus approfondie de la géométrie algébrique nous aurait servi. Puisque nous avons étudié le polynôme modulaire, il eût été naturel de prolonger cette étude avec l'article de Nakamura [13], qui intervient dans la preuve du théorème 7.2.3. D'un point de vue algorithmique, nous aurions aussi pu pousser l'étude de la complexité plus loin en nous intéressant aux méthodes de calcul efficients sur les nombres p-adiques (notamment la multiplication par transformée de Fourier rapide). Enfin, nous aurions aimé trouver une preuve complète de la proposition I.2.6 [14]. Puisque certains PSC sont repris d'une année à l'autre, pourquoi ne pas proposer à la promotion X2017 de reprendre le nôtre ?

14. Nous n'avons trouvé aucune référence qui la prouve complètement. Satoh se réfère à [11] qui ne la prouve qu'en partie.

Références

[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] FAVRE Thierry. *Comptage de points sur les courbes elliptiques* [en ligne]. Mémoire de Master en Mathématiques. Lausanne : École Polytechnique Fédérale de Lausanne, 2012, 46 p. Disponible sur : http ://csag.epfl.ch/files/content/sites/csag/files/travdipl/thierryfavre.pdf (23/08/2017).

[3] BUCHMANN Johannes. *Introduction à la cryptographie*. Traduit de l'anglais par Jacques Vélu. Paris : Dunod, 2006, 261 p. (Sciences Sup) ISBN 2 10 049622 0

[4] SERRE Jean Pierre. *Local Fields* [en ligne]. Translated from the French by Marvin Jay Greenberg. 1rst Ed. New York, USA : Springer, 1979, 248 p. Disponible sur : http ://en.bookfi.net/ (consulté le 10/09/2017). ISBN 978-1-4757-5673-9

[5] LANG Serge. *Elliptic Functions* [en ligne]. 2nd Ed. New York, USA : Springer, 1987, 328 p. Disponible sur : http ://en.bookfi.net/ (consulté le 20/09/2017). ISBN 978-1-4612-4752-4

[6] HERNANDEZ David et LASZLO Yves. *Cours de Théorie de Galois*. [document électronique]. Paris, 2012, 167 p. Disponible sur : https :/gargantua.polytechnique.fr/siatel-web/linkto/mICYYYS8ZJW (consulté le 21/09/2017).

[7] SILVERMAN Joseph. *The Arithmetic of Elliptic Curves* [en ligne]. 2nd Ed. New York, USA : Springer, 2009, 522 p. Disponible sur : http ://en.bookfi.net/ (consulté le 21/06/2017). ISBN 978-0-387-09494-6

[8] 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 (consulté le 26/01/2018).

[9] CASSELS J.W.S. *Lectures on Elliptic Curves*. 1rst Ed. Cambridge, UK : Cambridge University Press, 1991, 142 p. (London Mathematical Society, Students Texts 24) ISBN 0521 42530 1.

[10] VÉLU Jacques. *Isogénies entre Courbes Elliptiques* [en ligne]. Palaiseau, France : Comptes rendus hebdomadaires des séances de l'Académie des sciences, 1971, 6 p. Disponible sur : gallica.bnf.fr

[11] CASSELS, J. W. S. *A note on the division values of $\mathcal{P}(u)$*. [en ligne]. Cambridge, UK : Cambridge Philosophical Society, 1949, 6 p. Disponible sur : https ://www.cambridge.org/core/journals/mathematical-proceedings-of-the-cambridge-philosophical-society/article/note-on-the-division-values-of-u/3D61C507E27970D284F6548FD1066631.

[12] BLUHER, Antonia W. *Formal Groups, Elliptic Curves, and Some Theorems of Couveignes*, 1997 : National Security Agency, 9800 Savage Road, Fort George G. Meade, MD 20755-6000, 20 p. Disponible sur : https ://arxiv.org/abs/math/9708215v1

[13] Nakamura, T. : *A note on elliptic curves with ordinary reduction.* Arch. Math. 60, 440-445 (1980), 6 p. Disponible sur : https ://link.springer.com/content/pdf/10.1007/BF01202309.pdf

A Preuves de la section 1.

A.1 L'algorithme de Pohlig-Hellman.

On rappelle le problème initial. On veut prouver le théorème suivant :

Théorème A.1.1 (Pohlig-Hellman)**.** *Soient G un groupe cyclique de cardinal n, $g \in G$ un générateur de G et $h \in G$ quelconque. Alors il existe un algorithme permettant de trouver $l_g(h)$ avec :*

$$O\left(\sum_{p|n} \alpha_p(\ln(n) + \sqrt{p}) + \ln(n)^2\right)$$

opérations arithmétiques élémentaires où $n = \prod_{p|n} p^{\alpha_p}$ est la décomposition de n en produit de facteurs premiers (que l'on suppose connue).

On commence par montrer que le calcul de $l_g(h)$ se ramène au calcul d'un logarithme discret dans un groupe de taille p^{α_p} pour tout diviseur premier p de n. Pour tout diviseur premier p de n, on définit $n_p := \frac{n}{p^{\alpha}_p}$, $g_p := g^{n_p}$ et $h_p := h^{n_p}$, et on remarque que h_p est bien dans le sous groupe engendré par g_p car $h_p = g_p^{l_g(h)}$. Ainsi, $l_{g_p}(h_p)$ existe et le théorème suivant nous permet de calculer $l_g(h)$ à partir des $l_{g_p}(h_p)$:

Proposition A.1.2. *Soit $x \in \{0, \cdots, n-1\}$, l'unique solution du système de congruence :*

$$\left(x \equiv l_{g_p}(h_p) \quad [p^{\alpha_p}]\right)_{p|n}$$

dont l'existence est assurée par le théorème des restes chinois. Alors $x = l_g(h)$.

Démonstration. Si n n'admet qu'un seul diviseur premier alors le résultat est trivial ($x = l_{g_p}(h_p) = l_g(h)$). Supposons donc que n ait au moins deux diviseurs premiers distincts p et q. Alors, vu que g_p est d'ordre p^{α_p} et que $x \equiv l_{g_p}(h_p) \quad [p^{\alpha_p}]$, on a :

$$(g^{-x}h)^{n_p} = g^{-xn_p}h^{n_p} = g_p^{-x}h_p = g_p^{-l_{g_p}(h_p)}h_p = h_p^{-1}h_p = 1$$

Et de même, $(g^{-x}h)^{n_q} = 1$. Ainsi, l'ordre de $g^{-x}h$ divise n_p et n_q donc 1 car ces deux entiers sont premiers entre eux. Il s'ensuit que $g^{-x}h = 1$ i.e. $g^x = h$. Mais g étant d'ordre n, il n'y a qu'un seul entier x de $\{0, \cdots, n-1\}$ qui vérifie cette relation (il s'agit de $l_g(h)$). Donc $x = l_g(h)$. □

On est donc ramené par le théorème précédent au cas où $|G| = n = p^{\alpha}$ (en substituant le sous-groupe engendré par g_p à G). On montre qu'en fait, on peut même se ramener au calcul du logarithme discret dans un groupe d'ordre p. On sait que $l_g(h) < p^{\alpha}$ donc on peut décomposer $l_g(h)$ en base p avec α chiffres :

$$l_g(p) = \sum_{k=0}^{\alpha-1} a_k p^k$$

avec pour tout $i \in \{0, \cdots, \alpha-1\}$, $a_i \in \{0, \cdots, p-1\}$. Ainsi, on a $p^{\alpha-1}l_g(p) \equiv a_0 p^{\alpha-1} \quad [p^{\alpha}]$ et comme G est supposé être d'ordre p^{α} :

$$\left(g^{p^{\alpha-1}}\right)^{a_0} = h^{p^{\alpha-1}}$$

$g^{p^{\alpha-1}}$ étant d'ordre p, il s'ensuit que a_0 est l'unique entier de $\{0, \cdots, p-1\}$ qui vérifie cette relation, c'est à dire que :

$$a_0 = l_{g^{p^{\alpha-1}}}(h^{p^{\alpha-1}})$$

On détermine les chiffres suivants par récurrence. Supposons $a_0, \cdots, a_i$ déterminés (pour $i \in \{0, \cdots, \alpha-2\}$). Alors en remarquant que :

$$l_g(p)p^{\alpha-i-2} \equiv \sum_{k=0}^{i+1} a_k p^{\alpha+k-i-2} \quad [p^{\alpha}]$$

De sorte que :

$$\left(g^{p^{\alpha-1}}\right)^{a_{i+1}} = h_i^{p^{\alpha-i-1}}$$

avec $h_i := hg^{\sum_{k=0}^{i} a_k p^k}$, et que :

$$a_i = l_{g^{p^{\alpha-1}}}(h_i^{p^{\alpha-i-1}})$$

Nous nous sommes ramenés maintenant au cas où G est d'ordre p. Nous ne pouvons donc plus continuer à "descendre" et il nous faut un algorithme explicite pour calculer $l_g(h)$. Cette tâche peut être effectuée en temps $O(\sqrt{p})$, par l'algorithme "pas de bébés-pas de géant" décrit dans le paragraphe suivant.

Terminons avec le calcul de la complexité. En utilisant l'exponentiation rapide, le calcul de g_p et h_p nécessite $O(\ln(n_p)) = O(\ln(n))$ multiplications dans G pour tout $p|n$. Le calcul de chacun des α_p chiffres a_i de $l_{g_p}(h_p)$ nécessite $O(\ln(p^{alpha_p})) = O(\ln(n))$ opérations pour calculer les puissances $g_p^{alph_p - 1}$ et les h_i et $O(\sqrt{p})$ opérations pour l'algorithme de calcul du logarithme discret. Ceci donne au total :

$$O\left(\sum_{p|n} \alpha_p(\ln(n) + \sqrt{p})\right)$$

opérations dans le groupe G. En outre, le nombre de facteurs premiers de n étant un $O(\ln(n))$, et la résolution d'un système de m équations modulaires par le théorème Chinois étant de complexité $O(m^2)$ [15], il faut $O(\ln(n)^2)$ opérations arithmétiques élémentaires pour résoudre le système de congruence donnant $l_g(h)$.

A.2 L'Algorithme "Pas de bébés - pas de géants".

Soient G un groupe cyclique, d'ordre n et g un générateur de G. On cherche pour $h \in G$ donné, $l_g(h)$, le logarithme discret en base g de h. On pourrait penser à l'algorithme naïf qui consiste à calculer toutes les puissances de g et à reconnaître h, et qui nécessite $O(n)$ opérations. Dans des groupes de grande taille, c'est quasiment impossible. Il existe en fait un peu mieux : l'algorithme "pas de bébés-pas de géant" par exemple trouve le logarithme discret en $O(\sqrt{n})$ opérations. Expliquons comment.

On commence par calculer $m := \lceil \sqrt{n} \rceil$. Ecrivons la division euclidienne de $l_g(h)$ par m :

$$l_g(h) = qm + r \quad \text{avec } q \in \mathbb{N} \quad \text{et } r \in \{0, \cdots, m-1\}$$

Cet algorithme trouve $l_g(h)$ en calculant q et r. L'idée est de calculer les puissances de g (pas de bébé) et de $k := g^m$ (pas de géant) jusqu'à trouver le couple (q, r). L'algorithme porte donc bien son nom...

Plus concrètement, on stocke en mémoire l'ensemble des "pas de bébé" :

$$B := \{(hg^{-s}, s) \mid s \in \{0, \cdots, m-1\}\}$$

Si l'on y trouve un couple de la forme $(1, r)$ alors $l_g(h) = r$. Sinon, on calcule les puissances successives de k, jusqu'à trouver un entier q tel que $k^q = hg^{-r}$ avec $(hg^{-r}, r) \in B$. On a alors :

$$g^{qm+r} = h \quad \text{i.e.} \quad l_g(h) = qm + r$$

En termes de complexité, on effectue m multiplications pour calculer successivement les éléments de B, m multiplications pour calculer k, et $q \geq \frac{n}{m} + 1$ multiplications pour calculer les puissances de k, chaque puissance étant comparée aux éléments de B (opération pouvant être réalsée à coût constant en utilisant une table de hachage). Le nombre d'opérations est donc de l'ordre de $2m + q = O(\sqrt{n})$. On gagene donc nettement en complexité par rapport à l'algorithme naïf, mais il faut garder à l'esprit que l'on doit stocker les éléments de B (ce qui représente un coût spatial en $O(\sqrt{n})$). Notons qu'il existe un autre algorithme avec les mêmes performances temporelles, mais un coût spatial constant, l'algorithme ρ de Pollard, non présenté ici.

A.3 Généralités sur les courbes elliptiques.

Proposition A.3.1. *Soit E une courbe de genre 1 d'équation de Weierstrass $f(x, y) = 0$. Alors E est singulière si et seulement si $\Delta = 0$. Dans ce cas, il n'existe qu'un seul point singulier.*

Démonstration. **Premier cas :** On prouve dans un premier temps le résultat lorsque $\text{car}(\mathbb{K}) \neq 2$. Il est alors aisé de remarquer que E est singulière si et seulement si la courbe $\tilde{E}$ de polynôme de Weierstrass simplifié :

$$\tilde{f} := Y'^2 - 4X^3 - b_2X^2 - 2b_4X - b_6$$

l'est aussi. En effet :

$$\frac{\partial \tilde{f}}{\partial X}(X, Y') = \frac{\partial f}{\partial X}(X, Y') - a_1 \frac{\partial f}{\partial Y}(X, Y')$$

15. On pourra se référer au théorème 2.15.3. de [3] pour une preuve de ce résultat.

Et :

$$\frac{\partial \tilde{f}}{\partial Y'}(X,Y') = \frac{\partial Y}{\partial Y'}\frac{\partial \tilde{f}}{\partial Y} = 2\frac{\partial f}{\partial Y}(X,Y')$$

De sorte que $[x:y:1]$ est un point singulier de E si et seulement si $\left[x:\frac{y-a_1x-a_3}{2}:1\right]$ est un point singulier de $\tilde{E}$.

Or, un point $[x_0,y_0':1] \in \tilde{E}$ est singulier si et seulement si :

$$\tilde{f}(x_0,y_0') = \frac{\partial \tilde{f}}{\partial X}(x_0,y_0') = \frac{\partial \tilde{f}}{\partial Y'}(x_0,y_0') = 0$$

Mais $\frac{\partial \tilde{f}}{\partial Y'}(x_0,y_0') = 0$ équivaut à $2y_0' = 0$ i.e. $y_0' = 0$ ($\text{car}(\mathbb{K}) \neq 2$) et la condition $\tilde{f}(x_0,y_0') = \frac{\partial \tilde{f}}{\partial X}(x_0,y_0') = 0$ équivaut donc à :

$$P(x_0) = P'(x_0) = 0$$

avec $P := \tilde{f}(X,0) = 4X^3 + b_2X^2 + 2b_4X + b_6$.

Donc si E est singulière, alors $\tilde{E}$ est aussi singulière et P admet une racine double, de sorte que $\Delta = 0$. On obtient alors immédiatement l'uncicité du point singulier lorsqu'il existe puisqu'un polynôme de degré 3 ne peut avoir deux racines doubles distintes.

Réciproquement, si $\Delta = 0$ il suffit de considérer une racine double x_0 de P et $y_0' = 0$, pour obtenir un point sigulier de $\tilde{E}$, donc de E.

Deuxième cas : Traitons maintenant le cas où $\text{car}(\mathbb{K}) = 2$.

Premier sous-cas : Supposons que $a_1 \neq 0$. On fait alos la substitution :

$$X := a_1^2X' + \frac{a_3}{a_1}, Y := a_1^3Y' + \frac{a_1^2a_4 + a_3^2}{a_1^3}$$

Ce qui définit une nouvelle courbe de genre 1 $\tilde{E}$ de polynôme de Weierstrass :

$$\tilde{f} := Y'^2 + X'Y' - X'^3 - a_2'X'^2 - a_6'$$

Avec :

$$a_2' := \frac{a_1a_2 + a_3}{a_1^3}, a_6' := \frac{a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3 + a_1^4a_4^2 + a_1^3a_3^3 + a_3^4}{a_1^{10}}$$

On obtient par un raisonnement analogue à celui mené en caractéristique $\neq 2$ que E est singulière si et seulement si $\tilde{E}$ l'est aussi. Un calcul en caractéristique 2 assure aussi le discriminant de $\tilde{E}$ et celui de E sont liés par la relation :

$$\tilde{\Delta} = a_6' = \frac{\Delta}{a_1^{10}}$$

De sorte que $\tilde{\Delta} = 0$ si et seulement si $\Delta = 0$.

Si E est singulière, alors $\tilde{E}$ aussi et on dispose donc de $[x_0:y_0:1] \in \tilde{E}$ tel que $\tilde{f}(x_0,y_0) = \frac{\partial \tilde{f}}{\partial X'}(x_0,y_0) = \frac{\partial \tilde{f}}{\partial Y'}(x_0,y_0) = 0$, c'est à dire :

$$y_0^2 + x_0y_0 - x_0^3 - a_2'x_0^2 - a_6' = y_0 - 3x_0^2 = x_0 = 0$$

Et donc $x_0 = y_0 = a_6' = 0$, puis $\Delta = a_6' = 0$.

Réciproquement, si $\Delta = 0$ on voit clairement avec les calculs précédents que le point $[0:0:1] \in \tilde{E}$ est un point singulier de $\tilde{E}$ et donc que E est singulière.

Deuxième sous-cas : Supposons que $a_1 = 0$. Alors la substitution $X := X' + a_2$ donne une nouvelle courbe elliptique $\tilde{E}$ de polynôme de Weierstrass :

$$\tilde{f} := Y^2 + a_3Y - X'^3 - a_4'X' - a_6'$$

avec $a_4' := a_4 + a_2^2$ et $a_6' := a_2a_4 + a_6$, de discriminant $\tilde{\Delta} = a_3^4 = \Delta$. On conclut alors de la même façon que précédemment.

Lorsque $\text{car}(\mathbb{K}) = 2$, il y a unicité du point singulier lorsqu'il y en a un, car $[0:0:1]$ est le seul point singulier de $\tilde{E}$ dans les deux cas précédents.

□

Proposition A.3.2 (formules d'addition des points)**.** *Soit E une courbe de genre 1 d'équation de Weierstrass :*

$$f(x,y) := y^2 - x^3 + a_1xy - a_2x^2 + a_3y - a_4y - a_6 = 0$$

Soient $P_1, P_2 \in E_{ns} \setminus \{\mathcal{O}\}$ et $P_3 := P_1 \oplus P_2$ que l'on écrit $P_i := [x_i : y_i : 1]$ pour $i \in \{1,2\}$, alors :

(1). *P_1 admet un opposé $\ominus P_1 := [x_1 : -y_1 - a_1x_1 - a_3 : 1]$.*

(2). *Si $x_1 \neq x_2$ alors $P_3 := [x_3 : y_3 : 1]$ avec :*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{et} \quad y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

où :

$$\lambda := \frac{y_2 - y_1}{x_2 - x_1}, \nu := \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

(3). *Si $P_1 = P_2$ et $2y_1 + a_1x_1 + a_3 \neq 0$ alors :*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{et} \quad y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

avec :

$$\lambda := \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \nu := \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

Démonstration. **(1).** On vérifie par le calcul que $f(x_1, -y_1 - a_1x_1 - a_3) = 0$, ce qui assure que $\ominus P_1$ est un point de E. Comme P_1 et $\ominus P_1$ ont même abscisse, la définition de $\oplus$ assure qu'ils sont opposés lorsqu'ils sont distincts, i.e. lorsque $-y_1 - a_1x_1 - a_3 \neq y_1$.
Si maintenant $P_1 = \ominus P_1$, alors on a :

$$\frac{\partial f}{\partial Y}(x_1, y_1) = 2y_1 + a_1x_1y_1 + a_3y_1 = 0$$

Donc la tangente à E en $P_1 = \ominus P_1$ est horizontale et il s'ensuit par définition de $\oplus$ que P_1 et $\ominus P_1$ sont encore opposés.

(2). La droite D reliant P_1 à P_2 a pour équation :

$$y = \lambda x + \nu$$

Comme $P_1, P_2 \in E \cap D$, x_1 et x_2 sont des racines distinctes du polynôme $f(X, \lambda X + \nu)$, de coefficient dominant -1, qui s'écrit donc :

$$f(X, \lambda X + \nu) = -(X - x_0)(X - x_1)(X - x_2)$$

x_0 étant l'abscisse du troisième point d'intersection R entre D et E, dont on notera $y_0 := \lambda x_0 + \nu$ l'ordonnée. L'écriture du terme en X^2 du polynôme précédent donne :

$$x_0 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

On sait qu'alors $x_3 = x_0 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$.
En outre, vu que P_3 est le "deuxième" point d'intersection entre E et la droite d'équation $x = x_0 = x_3$ (le premier étant R), y_3 est la "deuxième" solution de l'équation polynomiale $f(x_3, Y) = 0$. Or, on vérifie facilement la factorisation suivante :

$$f(x_3, Y) = Y^2 + a_1x_0Y + a_3Y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = (Y - y_0)(Y + y_0 + a_1x_0 + a_3)$$

Qui nous donne immédiatement que :

$$y_3 = -y_0 - a_1x_0 - a_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

(3). Comme précédemment, la tangente D à E en P_1 a pour équation $y = \lambda x + \nu$ (voir définition 6). Ainsi, x_1 est racine du polynôme $f(X, \lambda X + \nu)$, de dérivée en x_1 :

$$\frac{\partial f}{\partial X}(x_1, \lambda x_1 + \nu) + \lambda \frac{\partial f}{\partial Y}(x_1, \lambda x_1 + \nu)$$

avec $\lambda = -\frac{\frac{\partial f}{\partial X}(x_1, \lambda x_1 + \nu)}{\frac{\partial f}{\partial Y}(x_1, \lambda x_1 + \nu)}$ par définition. Donc la dérivée de $f(X, \lambda X + \nu)$ s'annule en x_1, qui en est donc une racine double. On a donc :

$$f(X, \lambda X + \nu) = -(X - x_0)(X - x_1)^2$$

Et le raisonnement qui suit est tout à fait analogue à celui du point (2)..

□

Corollaire A.3.3. *$(E_{ns}, \oplus)$ est un groupe abélien. En outre, l'ensemble $E(\mathbb{K}) := E_{ns} \cap \mathbb{P}^2(\mathbb{K})$ des points rationnels de E est un sous-groupe de $(E_{ns}, \oplus)$.*

Démonstration. Commençons par vérifier que $\oplus$ est une loi de composition interne, c'est à dire que la somme de deux points non-singuliers n'est jamais un point singulier. Pour vérifier cela, il suffit de montrer que toute droite D coupant E en deux points distincts de E_{ns} ou tangente à E en un point de E_{ns} n'intersecte pas de point singulier S de E. En effet, les abscisses (ou les ordonnées) des points d'intersection entre D et E sont solution d'une équation polynomiale de degré au plus 3 et les deux points d'intersection de D et de E_{ns} sont solution de cette équation (quitte à les compter avec multiplicité dans le cas de tangence, comme nous l'avons fait dans la preuve du point (3). du résultat précédent).

Or, un point singulier $S := [x_0 : y_0 : 1] \in E \cap D$ est de multiplicitée au moins 2. En effet, si D a pour équation $y = ax + b$ alors x_0 est racine de $f(X, aX + b)$ de dérivée en x_0 :

$$\frac{\partial f}{\partial X}(x_0, y_0) + a\frac{\partial f}{\partial Y}(x_0, y_0) = 0$$

vu que S est singulier. Le raisonnement est le même si l'équation de D est du type $x = c$. Ainsi, D n'intersecte pas S car sinon on obtiendrait une équation polynomiale d'ordre au plus 3 avec 4 solutions.

On peut alors vérifier que $(E_{ns}, \oplus)$ est un groupe abélien. $\mathcal{O}$ est un élément neutre. L'associativité est garantie par les formules d'additions ci-dessus (mais la preuve, trop lourde n'est pas présentée ici). En outre, la commutativité est claire avec ces mêmes formules d'addition (on peut aussi donner un argument géométrique : la droite D intersectant P et Q est la même que celle intersectant Q et P). Pour finir, tout élement admet un opposé.

$E(\mathbb{K})$ est un sous-groupe de $(E_{ns}, \oplus)$ car il contient le neutre $\mathcal{O}$ et qu'il est stable par somme d'après les formules d'addition.

Dans le cas où E est une courbe elliptique, notons qu'une preuve moins élémentaire mais plus élégante de ce résultat est donné à la section 3.2. (voir théorème 3.2.11). □

B Prérequis d'algèbre générale.

Nous exposons ici les prérequis algébriques de base qui nous servent tout au long du document à l'exception de la théorie de Galois (car elle fait l'objet du cours de l'X : voir [6]). Il s'agit de notions que nous n'avons pas étudié dans notre scolarité antérieure mais qui sont suffisamment élémentaires pour être considérées comme des prérequis.

B.1 Arithmétique sur les anneaux.

Définition B.1.1. *Soit $\mathbb{A}$ un anneau et I un idéal de $\mathbb{A}$. I est* principal *s'il existe un élément $a \in \mathbb{A}$ tel que $I = a\mathbb{A}$. Autrement dit, I est généré par un unique élément de $\mathbb{A}$. $\mathbb{A}$ est* principal *si tout idéal de $\mathbb{A}$ est principal.*

Définition B.1.2. *Un anneau $\mathbb{A}$ est* noetherien *si toute suite croissante d'idéaux de $\mathbb{A}$ est stationnaire.*

Proposition B.1.3. *Un anneau principal est noetherien.*

Démonstration. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux d'un anneau principal $\mathbb{A}$. Alors $I = \bigcup_{i\in\mathbb{N}} I_n$ est un idéal de $\mathbb{A}$ comme réunion croissante d'idéaux. Comme $\mathbb{A}$ est principal, il est de la forme $a\mathbb{A}$ où $a \in \mathbb{A}$. $a \in I$ donc (par définition) il existe $n \in \mathbb{N}$ tel que $a \in I_n$. Par suite $I \subset I_n$ puis $I_i = I$ pour tout $i \geq n$. La suite est bien stationnaire. □

Lemme B.1.4. *Dans un ensemble ordonné $(E, \leq)$, les deux propriétés suivantes sont équivalentes :*

(i). *Toute suite croissante est stationnaire.*

(ii). *Tout sous-ensemble non vide de E admet un élément maximal.*

Démonstration. Supposons (ii). et dotons-nous d'une suite croissante $(a_i)_{i\in\mathbb{N}}$ de E. Alors il existe $i_0 \in \mathbb{N}$ tel que a_{i_0} est un élément maximal de la suite. Comme la suite est croissante, elle est donc stationnaire à partir du rang i_0.

Réciproquement, munissons-nous d'un sous-ensemble non vide $F \subset E$. Supposons que F n'admet pas d'élement maximal : $\forall a \in F$, $\exists b \in F / a < b$. Montrons qu'il existe une suite croissante non stationnaire de F :

Comme $F \neq \emptyset$, il existe $a_0 \in F$.

Soit $n \in \mathbb{N}$. Supposons qu'il existe un tuple strictement croissant $(a_i)_{0\leq i\leq n} \in F^{n+1}$. a_n n'est pas un élément maximal de F donc il existe $a_{n+1} \in F$ tel que $a_n < a_{n+1}$.

On a donc construit par récurrence une suite strictement croissante d'éléments de F, ce qui démontre la réciproque par contraposée. □

De ce lemme on déduit la propriété suivante : toute famille non vide d'idéaux d'un anneau principal admet un élément maximal. Cela nous permet de démontrer le théorème fondamental de l'arithmétique dans les anneaux principaux.

Définition B.1.5. *Un anneau $\mathbb{A}$ est dit* ***factoriel*** *si tout élément non nul de $\mathbb{A}$ se décompose en un produit d'un élément inversible et d'éléments irréductibles. Cette décomposition est alors unique à l'élément inversible près.*

Proposition B.1.6. *Un anneau principal est factoriel.*

Démonstration. Soit $\mathbb{A}$ un anneau principal. On raisonne par l'absurde : supposons qu'il existe un élément non nul $a \in \mathbb{A}$ qui n'est pas produit d'éléments irréductibles. Soit $\mathcal{F}$ la famille d'idéaux engendrés par de tels éléments. Par hypothèse, $\mathcal{F} \neq \emptyset$ donc elle possède un élément maximal $F = f\mathbb{A}$.

f est non nul et n'est pas irréductible (sinon il serait produit d'éléments irréductibles) donc il existe un couple d'éléments non inversibles $(x, y) \in \mathbb{A}^2$ tel que $f = xy$. On a clairement $F \subsetneq x\mathbb{A}$ car y n'est pas inversible donc, par maximalité de F et comme $x \neq 0, x$ est un produit d'éléments irréductibles, de même pour y. Comme $f = xy$, on en déduit que f lui-même est un produit d'éléments irréductibles, ce qui aboutit à une contradiction. □

On a donc retrouvé le théorème fondamental de l'arithmétique pour les anneaux principaux. On se propose maintenant de donner quelques propriétés générales vérifiées dans un anneau principal :

Proposition B.1.7 (Bézout.)**.** *Soit $\mathbb{A}$ un anneau principal. $\forall (a, b) \in \mathbb{A}^2$, $\exists d \in \mathbb{A} / a\mathbb{A} + b\mathbb{A} = d\mathbb{A}$. d est un pgcd de a et de b, noté $a \wedge b$. Deux éléments a et b sont premiers entre eux si 1 est un pgcd de a et de b. Si p est irréductible, $\forall a \in \mathbb{A}$, $p \wedge a \in \{1, p\}$.*

Lemme B.1.8 (Gauss.). *Soit $\mathbb{A}$ un anneau principal et p un irréductible de $\mathbb{A}$. Pour tout $(a,b) \in \mathbb{A}^2$, si $p \mid a$ mais $p|ab$, alors $p|b$.*

Proposition B.1.9. **(i).** *Les idéaux premiers sont les idéaux engendrés par un élément irréductible.*

(ii). *Les idéaux maximaux sont les idéaux premiers.*

B.2 Modules, algèbres.

Ici, il s'agit de voir comment se généralisent les résultats classiques de l'algèbre linéaire dans les espaces vectoriels et les algèbres, lorsque la structure de base n'est plus un corps mais un anneau tel que $\mathbb{Z}$, $\mathbb{Z}_p$ ou $\mathbb{Z}_q$. Nous introduisons donc la notion de module sur un anneau commutatif intègre et principal (propriétés que vérifient $\mathbb{Z}$, $\mathbb{Z}_p$ ou $\mathbb{Z}_q$). Dans tout ce paragraphe, $\mathbb{A}$ désignera donc un tel anneau.

Définition B.2.1. *Soit $(\mathbb{M},+)$ un groupe abélien. On dit que $\mathbb{M}$ est un $\mathbb{A}$-module si il existe une application externe $\cdot : \mathbb{A}\times\mathbb{M}\to\mathbb{M}$ vérifiant pour tous $a,b\in\mathbb{A}$ et $x,y\in\mathbb{M}$:*

(i). $a\cdot(x+y)=a\cdot x+a\cdot y$.

(ii). $(a+b)\cdot x=a\cdot x+b\cdot y$.

(iii). $(ab)\cdot x=a\cdot(b\cdot x)$.

(iv). $1\cdot x=x$.

Si de plus, $\mathbb{M}$ est muni d'une structure d'anneau pour une certaine loi $\times$ vérifiant pour tous $x,y\in\mathbb{M}$ et $a,b\in\mathbb{A}$:

(i). $(a+b)\cdot x\times y=a\cdot x\times y+b\cdot x\times y$.

(ii). $a\cdot(x\times y)=(a\cdot x)\times y=x\times(a\cdot y)$.

On dit que $\mathbb{M}$ est une $\mathbb{A}$-algèbre.

Exemples :

1). L'ensemble $\mathbb{A}[X]$ des polynômes à coefficients dans $\mathbb{A}$ et l'ensemble $M_{n,m}(\mathbb{A})$ des matrices à coefficients dans $\mathbb{A}$ sont naturellement munis d'une structure de $\mathbb{A}$-algèbre.

2). Tout groupe abélien $(G,+)$ est naturellement muni d'une structure de $\mathbb{Z}$-module. Ce constat nous permettra d'obtenir un théorème de structure des groupes abéliens de type fini à partir de notre étude de la théorie des modules.

3). De même que dans les espaces vectoriels, on définit la notion d'application $\mathbb{A}$-linéaire entre deux modules $\mathbb{M}$ et . On note alors $\mathrm{Hom}_{\mathbb{A}}(\mathbb{M},\mathbb{L})$ (ou $\mathrm{Hom}(\mathbb{M},\mathbb{L})$ lorsqu'il n'y a pas d'ambiguïté sur $\mathbb{A}$), l'ensemble des applications $\mathbb{A}$-linéaires de $\mathbb{M}$ dans $\mathbb{L}$ et $\mathrm{End}(\mathbb{M}) := \mathrm{Hom}(\mathbb{M},\mathbb{M})$ l'ensemble des endomorphismes de $\mathbb{M}$. On peut munir $\mathrm{Hom}(\mathbb{M},\mathbb{L})$ (et $\mathrm{End}(\mathbb{M})$ de même), d'une structure naturelle de $\mathbb{A}$-module. L'hypothèse de commutativité de $\mathbb{A}$ est cruciale ici pour que la multiplication par un scalaire d'une application $\mathbb{A}$-linéaire reste $\mathbb{A}$-linéaire.

$\mathrm{End}(\mathbb{M})$ est même une $\mathbb{A}$-algèbre pour la composition.

Une application $\mathbb{A}$-linéaire bijective est appelée isomorphisme. Si $\mathrm{Hom}(\mathbb{M},\mathbb{L})$ en contient une, on dit que $\mathbb{M}$ et $\mathbb{N}$ sont isomorphes. Comme la composée de deux applications $\mathbb{A}$-linéaires reste $\mathbb{A}$-linéaire, cette notion est transitive.

4). Nous verrons d'autres exemples (qui font tout l'intérêt de cette digression) tels que le module de Tate et le groupe des isogénies d'une courbe elliptique.

Sous-modules, modules engendrés :

Les notions de sous-module et de sous-algèbre sont définies de la même manière qu'en algèbre linéaire classique (présence des neutres et stabilité). On vérifie ainsi facilement que les intersections et les sommes de sous-modules sont des sous-modules, et qu'une intersection de sous-algèbre définit une sous-algèbre. La notion de somme directe est la même qu'en algèbre vectorielle. Enfin, l'image et le noyau d'une application $\mathbb{A}$-linéaire sont des sous-modules.

On peut définir aussi la notion de module et d'algèbre engendrées par une partie $P\subset\mathbb{M}$ (plus petite structure contenant ladite partie). On peut vérifier qu'il s'agit de l'ensemble des combinaisons linaires des éléments de P pour la structure de module et l'enesmble des combinaisons linéaires des produits des éléments de P pour la structure d'algèbre.

Modules quotient :

Soient $\mathbb{M}$ un $\mathbb{A}$-module et $\mathbb{L}$ un sous-module de $\mathbb{M}$. Alors $\mathbb{L}$ est un sous-groupe distingué de $\mathbb{M}$ pour la loi $+$, car $\mathbb{M}$ est abélien. Ainsi, $\mathbb{M}/\mathbb{L}$ est muni d'une structure de groupe pour la loi $+$. En fait, on peut aussi construire une loi externe $\cdot$ sur $\mathbb{M}/\mathbb{L}$ en posant :

$$a \cdot \overline{x} := \overline{a \cdot x}$$

pour tous $a \in \mathbb{A}$ et $\overline{x} \in \mathbb{M}/\mathbb{L}$ choisi. On peut facilement vérifier que $\cdot$ est bien définie car $a \cdot \overline{x}$ ne dépend pas du représentant de $\overline{x}$ modulo $\mathbb{L}$ choisi.

Par exemple, $\mathbb{A}$ est un $\mathbb{A}$-module et tout idéal I de $\mathbb{A}$ est un sous-module de $\mathbb{A}$ donc $\mathbb{A}/I$ est un $\mathbb{A}$-module.

Comme pour les groupes, quotienter est un moyen de rendre injectives des applications linéaires.

Lemme B.2.2. *Si f est une application $\mathbb{A}$-linéaire entre deux $\mathbb{A}$-modules $\mathbb{M}$ et $\mathbb{L}$ alors il existe une unique application $\mathbb{A}$-linéaire $\overline{f} : \mathbb{M}/ker(f) \longrightarrow \mathbb{L}$ telle que $f = \overline{f} \circ \pi$, π étant l'application $\mathbb{A}$-linéaire de projection de $\mathbb{M}$ sur $\mathbb{M}/ker(f)$. $\overline{f}$ induit un isomorphisme entre $\mathbb{M}/ker(f)$ et $im(f)$.*

Démonstration. f est constante sur chaque classe d'équivalence de $\mathbb{M}/\ker(f)$. On peut alors poser :

$$\forall x \in \mathbb{M}, \quad \overline{f}(\overline{x}) := f(x) \quad (\star)$$

Ceci définit bien une application $\mathbb{A}$-linéaire entre $\mathbb{M}/\ker(f)$ et $\mathbb{L}$ qui vérifie $f = \overline{f} \circ \pi$. En outre, si $x \in \mathbb{M}$ vérifie $\overline{f}(\overline{x}) = 0$ alors $f(x) = 0$ donc $x \in \ker(f)$ et $\overline{x} = \overline{0}$ donc $\overline{f}$ est injective, et induit donc un isomorphisme entre $\mathbb{M}/\ker(f)$ et $\mathrm{im}(f)$. L'unicité est claire car toute application convenable vérifie $(\star)$. □

Modules libres de type-fini :

Les notions de famille libre et de famille génératrice sont les mêmes que dans l'algèbre linéaire vectorielle. Cependant, l'existence d'une base n'est pas toujours assurée. D'où la définition suivante.

Définition B.2.3. *Un $\mathbb{A}$-module $\mathbb{M}$ est dit libre s'il admet une base.*

Comme dans les espaces vectoriels, l'algèbre linéaire est plus simple en dimension finie. On se restreint donc à ce cas ici.

Définition B.2.4. *Un $\mathbb{A}$-module $\mathbb{M}$ est dit de type-fini s'il admet une famille génératrice finie.*

Nous allons maintenant construire l'analogue de la dimension sur un $\mathbb{A}$ module libre de type fini, que nous appellerons rang.

Proposition B.2.5. *Si $\mathbb{M}$ est un $\mathbb{A}$-module libre de type fini alors $\mathbb{M}$ admet une base finie.*

Démonstration. Soit $\mathcal{B} := (e_i)_{i \in I}$ une base de $\mathbb{M}$. Comme $\mathbb{M}$ est de type fini on dispose de $x_1, \cdots, x_n \in \mathbb{M}$ qui engendrent $\mathbb{M}$ et qui sont combinaisons linéaires (nécessairement finies) d'éléments de $\mathcal{B}$. Soit donc $J \subset I$ le support de toutes ces combinaisons linéaires (qui est fini). Alors comme $(x_1, \cdots, x_n)$ est génératrice, $(e_i)_{i \in J}$ l'est aussi. Etant en particulier libre comme sous-famille de $\mathcal{B}$, c'est une base de $\mathbb{M}$. □

Fixons donc $\mathbb{M}$ un $\mathbb{A}$-module libre de type fini et $\mathcal{B} := (b_1, \cdots, b_r)$ une base de $\mathbb{M}$. Alors :

$$f : (a_1, \cdots, a_r) \in \mathbb{A}^r \longmapsto \sum_{i=1}^{r} a_i b_i \in \mathbb{M}$$

définit un isomorphisme linéaire entre $\mathbb{A}^r$ et $\mathbb{M}$. Donc $\mathbb{M} \approx \mathbb{A}^r$. Il reste à vérifier l'unicité d'un tel entier r (qui définira le rang de $\mathbb{M}$).

Supposons que $\mathbb{A}^r$ soit isomorphe à $\mathbb{A}^s$ pour un certain entier s et soit g un certain isomorphisme entre les deux. Rappelons un résultat de [6] (corollaire 9.1.4), qui est une conséquence du lemme de Zorn :

Proposition B.2.6. *Tout anneau admet un idéal maximal.*

Soit M un idéal maximal de $\mathbb{A}$. Alors $\mathbb{A}/M$ est un corps et $(\mathbb{A}/M)^r$ et $(\mathbb{A}/M)^s$ peuvent être munis d'une structure de $\mathbb{A}/M$-espace vectoriel. g peut alors être vue comme une application $\mathbb{A}/M$-linéaire de $(\mathbb{A}/M)^r$ dans $(\mathbb{A}/M)^s$, qui devient alors un isomorphisme de $\mathbb{A}/M$-espaces vectoriels. Mais la famille $(e_1, \cdots, e_r)$ de $(\mathbb{A}/M)^r$ donnée par :

$$e_i := (\delta_{i,j})_{1 \leq j \leq r}$$

est une $\mathbb{A}/M$-base de $(\mathbb{A}/M)^r$ qui est donc de dimension r comme $\mathbb{A}/M$-espace vectoriel. De même, $(\mathbb{A}/M)^s$ est de dimension s comme $\mathbb{A}/M$-espace vectoriel. Donc $r = s$.

Définition B.2.7. *Si $\mathbb{M}$ est un $\mathbb{A}$-module libre de type fini alors* le rang *de $\mathbb{M}$ est l'unique entier r tel que $\mathbb{M} \approx \mathbb{A}^r$. C'est aussi le cardinal de toute base de $\mathbb{M}$. On le note rg($\mathbb{M}$).*

Pour que la théorie du rang soit analogue à celle de l'algèbre vectorielle, il ne nous manque plus que le résultat suivant.

Proposition B.2.8. *Si $\mathbb{L}$ est un sous-module d'un module libre de type fini $\mathbb{M}$, alors il est libre de type fini de rang $\leq$ rg($\mathbb{M}$).*

Démonstration. On raisonne par récurrence sur $r := \text{rg}(\mathbb{M})$.

Initialisation : Si $r = 0$ alors $\mathbb{M}$ est engendrée par la famille vide donc $\mathbb{M} = \{0\}$ et donc $\mathbb{L} = \{0\}$ qui est aussi engendré par la famille vide donc libre de type fini et de rang 0.

Hérédité : Soit $r \in \mathbb{N}^*$. Supposons le résultat vrai au rang r. Soient $\mathbb{M}$ un $\mathbb{A}$-module libre de type fini de rang $r+1$ et $\mathbb{L}$ un sous-module de $\mathbb{M}$. Soient $\mathcal{U} = (u_1, \cdots, u_{r+1})$ une base de $\mathbb{M}$ et $\mathbb{M}'$ le sous-module de $\mathbb{M}$ engendré par $(u_1, \cdots, u_r)$. $\mathbb{M}'$ est un module libre de type fini et de rang r car $(u_1, \cdots, u_r)$ en est une base (elle est libre comme sous famille de $\mathcal{U}$ et génératrice par définition de $\mathbb{M}'$). $\mathbb{L} \cap \mathbb{M}'$ est alors un sous-module de $\mathbb{M}'$ et on peut alors appliquer l'hypothèse de récurrence pour obtenir l'existence d'une base $\mathcal{V}' = (v_1, \cdots, v_k)$ de $\mathbb{L} \cap \mathbb{M}'$ avec $k \leq r$.
Soit I l'ensemble des coordonnées des éléments de $\mathbb{L}$ selon u_{r+1}. I contient 0 et I est stable par somme et par multiplication par tout élément de $\mathbb{A}$ donc c'est un idéal de $\mathbb{A}$. On distingue deux cas.

Premier cas Si $I = \{0\}$ alors $\mathbb{L} \subset \mathbb{M}'$ donc $\mathcal{V}'$ est une base de $\mathbb{L}$ qui est donc libre de type fini et de rang $\text{rg}(\mathbb{L}) \leq k \leq r \leq r+1$.

Second cas Sinon, $I \neq \{0\}$ donc comme $\mathbb{A}$ est principal, on dispose de $d \in \mathbb{A} \setminus \{0\}$ tel que $I = d\mathbb{A}$.
Soit $x_0 \in \mathbb{M}'$ tel que $v_{k+1} := x_0 + du_{r+1} \in \mathbb{L}$, qui existe par définition de I. Montrons qu'alors $\mathcal{V} := (v_1, \cdots, v_{k+1})$ est une base de $\mathbb{L}$.
Soit $x \in \mathbb{L}$. Alors sa coordonnée selon u_{r+1} est dans I donc elle est de la forme $a_{k+1}d$ avec $a_{k+1} \in \mathbb{A}$ et donc la coordonnée de $y := x - a_{k+1}v_{k+1}$ selon u_{r+1} est nulle donc $y \in \mathbb{M}'$. Mais $x \in \mathbb{L}$ et $v_{k+1} \in \mathbb{L}$ donc $y \in$. Donc on dispose de $a_1, \cdots, a_k \in \mathbb{A}$ tels que $y = \sum_{i=1}^{k} a_i v_i$ i.e. $x = \sum_{i=1}^{k+1} a_i v_i$.
Soient maintenant $b_1, \cdots, b_{k+1} \in \mathbb{A}$ tels que $\sum_{i=1}^{k+1} b_i v_i = 0$. Alors :

$$b_{k+1}v_{k+1} = -\sum_{i=1}^{k} b_i v_i \in \mathbb{M}'$$

Donc si par l'absurde $b_{k+1} \neq 0$ alors $b_{k+1}v_{k+1}$ a pour composante $b_{k+1}d \neq 0$ (par intégrité de $\mathbb{A}$) selon u_{r+1} ce qui contredit son appartenance à $\mathbb{M}'$. Ainsi, $b_{k+1} = 0$ et $\sum_{i=1}^{k} b_i v_i = 0$ donc par liberté de $\mathcal{V}'$, $\forall i \in \{1, \cdots, k\}$, $b_i = 0$.
Donc $\mathcal{V}$ est bien une base de et donc $\text{rg}() = k+1 \leq r+1 = \text{rg}(\mathbb{M})$.

D'où l'itération et le résultat.

□

Remarque : Au cours de la preuve, nous avons pleinement utilisé le fait que $\mathbb{A}$ est intègre et principal. C'est pourquoi cette hypothèse est nécessaire pour avoir une notion de rang analogue à cette de l'algèbre vectorielle. Toutefois, on dispose d'une version affaiblie de ce résultat lorsque l'hypothèse de principalité est un peu affaiblie, plus précisément lorsque l'anneau $\mathbb{A}$ est simplement supposé noethérien.

Définition B.2.9. *Un anneau est dit noethérien si tous ses idéaux sont de type finis, c'est à dire engendrés par un nombre fini d'éléments.*

Proposition B.2.10. *Si $\mathbb{A}$ est intègre et noethérien, si $\mathbb{M}$ est un $\mathbb{A}$-module de type fini et un sous-module de $\mathbb{M}$ alors est de type fini.*

Démonstration. C'est une récurrence sur le rang de $\mathbb{M}$ analogue à celle de la proposition B.2.8. □

Structure des modules de type fini :

Nous prouvons ici un résultat de théorie des groupes, qui nous est utile pour l'étude des isogénies (cf. théorème **??**) en nous plaçant dans le cadre plus génbéral de la théorie des modules de type fini sur un anneau commutatif, intègre et principal.

Commençons avec quelques remarques de calcul matriciel sous de telles hypothèses. Sur des modules libres de type fini, une application linéaire peut être représentée par une matrice dans des bases dans

l'espace d'arrivée et de départ. On peut aussi définir des matrices de changement de base, de la même façon qu'en algèbre vectorielle. Ces matrices sont toujours inversibles et on dispose des mêmes formules de changement de base. En outre, la matrice d'une application linéaire est inversible si et seulement si c'est un isomorphisme.

On peut définir aussi la notion de rang d'une application linéaire ou d'une matrice (comme rang de l'image par cette application linéaire ou par cette matrice comme sous-module d'un module libre de type fini, comme nous l'assure la proposition B.2.8). Les propriétés de l'algèbre vectorielle restent encore une fois valables (invarance par changement de base notamment et équivalence entre l'inversibilité et l'égalité entre le rang et la taille d'une matrice carré).

Les propriétés du déterminant sur des matrices carrées restent aussi invariantes et termes de calculs issus de la multilinéarité. Notons cependant qu'une matrice $M \in M_n(\mathbb{A})$ n'est inversible que lorsque son déterminant est dans le groupe des inversibles de $\mathbb{A}$. On peut par ailleurs prouver le théorème de Cayley-Hamilton.

Indiquons aussi que l'on peut faire les mêmes opérations élémentaires sur les matrices qu'en algèbre linéaire classique (échanges de lignes et de colonnes, addition d'une ligne ou d'une colonne à une autre ligne ou colonne multipliée par un scalaire) sans chager le rang, car ceci revient à multiplier la matrice sur laquelle on travaille par des matrices de déterminant 1. Ceci nous permettra d'obtenir le résultat suivant :

Proposition B.2.11 (forme normale de Smith)**.** *Toute matrice $M \in M_{n,m}(\mathbb{A})$ est équivalente à une matrice de $M_{n,p}(\mathbb{A})$, contenant un bloc diagonal $Diag(d_1, \cdots, d_r)$ en haut à gauche et des 0 partout ailleurs, où r est le rang de M et $d_1, \cdots, d_r \in \mathbb{A} \setminus \{0\}$ vérifient :*

$$d_1 | \cdots | d_r$$

Démonstration. On prouve ce résultat par récurrence sur $\max(n, m)$, la taille de la matrice.

Initialisation : Si $M \in M_{n,m}(\mathbb{A})$ vérifie $\max(n, m) = 1$ alors $n = m = 1$ et la matrice est déjà sous forme de Smith.

Hérédité : Soit $M \in M_{n,m}(\mathbb{A})$ avec $\max(n, m) \geq 2$. Supposons le résultat aux rangs $1, \cdots, \max(n, m) - 1$. On commence par mettre la première ligne de M sous la forme $(d \quad 0 \quad \cdots \quad 0)$ en effectuant des opérations élémentaires. On élimine les derniers $M_{1,j}$ par récurrence finie descendante. Soit $j \in \{2, \cdots, m\}$. Supposons que $M_{1,j+1} = \cdots = M_{1,m} = 0$. Distinguons alors deux cas :

Premier cas : Si $M_{1,j-1}$ divise $M_{1,j}$ alors on fait l'opération élémentaire $C_j \longleftarrow C_j - \frac{M_{1,j}}{M_{1,j-1}} C_{j-1}$ (sauf dans le cas où $M_{1,j-1} = 0$ où l'on n'a rien à faire).

Deuxième cas : Supposons que $M_{1,j-1}$ ne divise pas $M_{1,j}$. $\mathbb{A}$ étant principal, on peut définir le pgcd de toute paire d'éléments de $\mathbb{A}$ à multiplication par un inversible près (comme générateur de l'idéal somme de la paire de ces deux éléments). Soit donc d un pgcd de $M_{1,j-1}$ et $M_{1,j}$. On dispose alors de $u, v \in \mathbb{A}$ tels que $uM_{1,j-1} + vM_{1,j} = d$ (ceci résultant directement de la définition du pgcd). Soient $a, b \in \mathbb{A}$ tels que $M_{1,j-1} = ad$ et $M_{1,j} = bd$. Alors $ua + vb = 1$ (en simplifiant par d, ce qui est possible car $\mathbb{A}$ est intègre et commutatif) et $M_{1,j-1}b = adb = aM_{1,j}$. Ainsi, la matrice :

$$\mathrm{Diag}\left(\begin{pmatrix} u & -b \\ v & a \end{pmatrix}, 1, \cdots, 1\right)$$

est de déterminant 1 donc inversible. Donc en multipliant M par S, on obtient que M est équivalente à une matrice dont les deux premiers coefficients de la première ligne s'écrivent :

$$(M_{1,j-1} \quad M_{1,j}) \begin{pmatrix} u & -b \\ v & a \end{pmatrix} = (d \quad 0)$$

Ceci termine la démonstration dans le cas $n = 1$. Sinon, on peut de manière analogue, annuler tous les coefficients $M_{i,1}$ pour $i \geq 2$ de M en multipliant M à gauche par des matrices inversibles. On obtient alors que M est équivalente à une matrice de la forme :

$$M' := \begin{pmatrix} d & 0 \\ 0 & M_1 \end{pmatrix}$$

avec $d \in \mathbb{A}$ et $M_1 \in M_{n-1,m-1}(\mathbb{A})$. Par hypothèse de récurrence, on dispose alors de $P_1 \in GL_{n-1}(\mathbb{A})$, de $Q_1 \in GL_{m-1}(\mathbb{A})$ et de D_1 contenant un bloc diagonal $\mathrm{Diag}(d_2, \cdots, d_r)$ en haut à gauche avec $d_2 | \cdots | d_r$, telles que $M_1 = P_1 D_1 Q_1$. On pose alors :

$$P := \begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix}, \quad Q := \begin{pmatrix} 1 & 0 \\ 0 & Q_1 \end{pmatrix} \quad \text{et} \quad D := \begin{pmatrix} d & 0 \\ 0 & D_1 \end{pmatrix}$$

qui vérifient $M' = PDQ$ avec P et Q inversibles (car de même déterminant que P_1 et Q_1 respectivement). Si $d|d_2$ on a terminé (r étant bien le rang de M car celui-ci est invariant par équivalence). Dans le cas contraire, on fait $L_1 \longleftarrow L_1 + L_2$ sur la matrice D et on considère d', un pgcd de d et d_2, $u, v \in \mathbb{A}$ tels que $ud + vd_2 = d'$ et $a, b \in \mathbb{A}$ tels que $d = ad'$ et $d_2 = bd'$. Alors :

$$\text{Diag}\left(\begin{pmatrix} u & -b \\ v & a \end{pmatrix}, 1, \cdots, 1\right)$$

est inversible et en multipliant D par cette matrice, on obtient comme bloc 2×2 en haut à gauche :

$$\begin{pmatrix} d & d_2 \\ 0 & d_2 \end{pmatrix}\begin{pmatrix} u & -b \\ v & a \end{pmatrix} = \begin{pmatrix} d' & 0 \\ d_2 v & d_2 a \end{pmatrix}$$

sans changer les autres coefficients de D. Comme, $d'|d_2$, on fait alors $L_2 \longleftarrow L_2 - \frac{d_2 v}{d'} L_1$, pour transformer ce bloc en :

$$\begin{pmatrix} d' & 0 \\ 0 & d_2 a \end{pmatrix}$$

Si $d_2 a | d_3$ c'est terminé. Sinon on est ramené au même problème que précédement et on peut procéder par récursivement sur l'indice $i \in \{2, \cdots, r\}$ problématique. D'où l'itération et le résultat.

□

Corollaire B.2.12 (théorème de la base adaptée)**.** *Si $\mathbb{M}$ est un $\mathbb{A}$-module libre de type fini et si est un sous-module de $\mathbb{M}$ alors il existe une base $(e_1, \cdots, e_n)$ de $\mathbb{M}$ et des scalaires $d_1, \cdots, d_r \in \mathbb{A} \setminus \{0\}$ tels que $d_1 | \cdots | d_r$ et $(d_1 e_1, \cdots, d_r e_r)$ soit une base de .*

Démonstration. est un sous-module du module libre de type fini $\mathbb{M}$ donc la proposition B.2.8 assure que est libre de rang $r \leq \text{rg}(\mathbb{M}) := n$ et on dispose donc d'une base $(f_1, \cdots, f_r)$ de . Considérons l'application $\mathbb{A}$-linéaire :

$$f : (a_1, \cdots, a_r) \in \mathbb{A}^r \longmapsto \sum_{i=1}^{r} a_i f_i \in \mathbb{M}$$

Son image est exactemnt , donc elle est de rang r et d'après la proposition B.2.11, il existe une base de $\mathcal{B}$ de $\mathbb{A}^r$ et une base de $\mathcal{E} := (e_1, \cdots, e_n)$ de $\mathbb{M}$ telles que :

$$\text{Mat}_{\mathcal{B},\mathcal{E}}(f) = \begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots & & \vdots \\ 0 & \cdots & d_r & 0 & \cdots & 0 \end{pmatrix}$$

avec $d_1, \cdots, d_r \in \mathbb{A} \setminus \{0\}$ tels que $d_1 | \cdots | d_r$. $(d_1 e_1, \cdots, d_r e_r)$ est alors une famille génératrice de l'image de f, donc de et cette famille est libre par liberté de $(e_1, \cdots, e_r)$ et intégrité de $\mathbb{A}$. Donc c'est une base de . □

Théorème B.2.13 (structure des modules de type fini)**.** *Si $\mathbb{M}$ est un $\mathbb{A}$-module de type fini alors il existe des entiers naturels r et q et des scalaires $d_1, \cdots, d_r \in \mathbb{A} \setminus \{0\}$ non inversibles tels que $d_1 | \cdots | d_r$ vérifiant :*

$$\mathbb{M} \approx \mathbb{A}^q \times \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_r\mathbb{A}$$

Démonstration. $\mathbb{M}$ étant de type fini, on dispose de $x_1, \cdots, x_n \in \mathbb{M}$ engendrant $\mathbb{M}$. Considérons l'application $\mathbb{A}$-linéaire :

$$f : (a_1, \cdots, a_n) \in \mathbb{A}^n \longmapsto \sum_{i=1}^{n} a_i x_i \in \mathbb{M}$$

Soit $\mathbb{L} := \ker(f)$. Alors $\mathbb{L}$ est un sous-module du module libre de type fini $\mathbb{A}^n$. Donc d'après le théorème de la base adaptée, on dispose d'une base $(e_1, \cdots, e_n)$ de $\mathbb{A}^n$ et de $d_1, \cdots, d_r \in \mathbb{A} \setminus \{0\}$ tels que $d_1 | \cdots | d_r$ et que $(d_1 e_1, \cdots, d_r e_r)$ soit une base de $\mathbb{L}$.

En outre, f étant surjective, le lemme précédent assure que $\mathbb{M} \approx \mathbb{A}^n/$. Posons $q := n - r$. Pour terminer la preuve, il reste à montrer que :

$$\mathbb{A}^n/\mathbb{L} \approx \mathbb{A}^q \times \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_r\mathbb{A}$$

Pour cela, on considère l'application $\mathbb{A}$-linéaire :

$$g : (a_1, \cdots, a_q, b_1, \cdots, b_r) \in \mathbb{A}^q \times \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_r\mathbb{A} \longmapsto \sum_{i=1}^{r} a_i e_{q+i} + \sum_{i=1}^{q} b_i e_i \in \mathbb{A}^n/\mathbb{L}$$

g est bien définie et surjective. En effet, si $x \in \mathbb{A}^n$, on peut décomposer x dans $(e_1, \cdots, e_n)$:

$$x := \sum_{i=1}^{n} x_i e_i$$

avec $x_1, \cdots, x_n \in \mathbb{A}$. En notant pour tout $i \in \{1, \cdots, r\}$, b_i la classe de x_i modulo d_i, et en posant $a_j := x_{r+j}$ pour tout $j \in \{1, \cdots, q\}$, on obtient que :

$$\overline{x} := \sum_{i=1}^{r} a_i e_{q+i} + \sum_{i=1}^{q} b_i e_i = g(a_1, \cdots, a_q, b_1, \cdots, b_r)$$

g est de plus injective car si $(a_1, \cdots, a_q, b_1, \cdots, b_r) \in \mathbb{A}^q \times \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_r\mathbb{A}$ vérifie :

$$\sum_{i=1}^{r} a_i e_{q+i} + \sum_{i=1}^{q} b_i e_i = \overline{0}$$

alors pour tout $i \in \{1, \cdots, q\}$, il existe $\tilde{b}_i$ un représentant de b_i dans $\mathbb{A}/d_i\mathbb{A}$, tel que :

$$\sum_{i=1}^{r} a_i e_{q+i} + \sum_{i=1}^{q} \tilde{b}_i e_i = 0$$

Donc par liberté de $(e_1, \cdots, e_n)$, tous les a_i et tous les $\tilde{b}_i$ (donc tous les b_i) sont nuls. Ainsi, g est l'isomorphisme cherché entre $\mathbb{A}^n/$ et $\mathbb{A}^q \times \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_r\mathbb{A}$.

Si l'un des d_i est inversible alors $\mathbb{A}/d_i\mathbb{A} \approx \{0\}$ donc on peut supposer que tous les d_i sont non inversibles quitte à retirer les facteurs triviaux inutiles dans le produit direct précédent. Ceci termine la preuve. □

Rappellons que si $(G, +)$ est un groupe abélien, alors G est un $\mathbb{Z}$-module. Donc si G est de type fini, le théorème précédent s'applique et on obtient que :

$$G \approx \mathbb{Z}^q \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_1, \cdots, d_r \geq 2$ tels que $d_1 | \cdots | d_r$. L'isomorphisme ayant lieu en tant que $\mathbb{Z}$-modules (donc en tant que groupes additifs). Si G est de plus fini, alors $q = 0$ (sinon $\mathbb{Z}$ se plongerait dans G) et l'on peut décomposer les d_i en facteurs premiers et appliquer le théorème des restes chinois pour obtenir le résultat suivant :

Corollaire B.2.14 (théorème de structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini. Alors il existe des nombres premiers distincts deux à deux $p_1, \cdots, p_r$, des entiers naturels non nuls $\alpha_1, \cdots, \alpha_r$, $n_1, \cdots, n_r$ tels que :*

$$G \approx (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^{n_1} \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^{n_r}$$

En fait, cette décomposition est unique à l'ordre des facteurs près, car l'unicité est vraie aussi pour les modules, la base adaptée et la forme de Smith. Cepedant, l'unicité n'est pas utilisée dans ce rapport. C'est pourquoi nous ne l'avons pas prouvée.

C Preuves et compléments de la section 2.

C.1 Généralités sur les corps valués.

C.1.1 Corps valués.

Lemme C.1.1 (topologie ultramétrique)**.** *(lemme 2.1.4) On suppose ici que $|.|$ est ultramétrique. Alors :*

(i). *Si, $x, y \in \mathbb{K}$ vérifient $|x| \neq |y|$ alors $|x+y| = \max(|x|, |y|)$. En conséquence, si v est associée à $|.|$ et si $x, y \in \mathbb{K}$ vérifient $v(x) \neq v(y)$ alors $v(x+y) = \min(v(x), v(y))$.*

(ii). *Si $x_0 \in \mathbb{K}$ et $r > 0$ alors pour tout $x \in B(x_0, r)$, $B(x, r) = B(x_0, r)$. Autrement dit, tout point d'une boule est au centre de ladite boule.*

(iii). *Deux boules de $\mathbb{K}$ sont soit disjointes soit contenues l'une dans l'autre.*

(iv). *Les boules de $\mathbb{K}$ sont à la fois ouvertes et fermées.*

(v). *Les composantes connexes de $\mathbb{K}$ sont des singletons. On dira alors que* la topologie de $\mathbb{K}$ est complètement discontinue.

Démonstration. **(i).** Quitte à échanger les rôles de x et de y (parfaitement symétriques), on peut supposer que $|x| > |y|$. On a alors, comme $|.|$ est ultramétrique :

$$|x+y| \leq \max(|x|, |y|) = |x|$$

Donc $\max(|y|, |x+y|) \leq |x|$. Mais :

$$|x| = |(x+y) - y| \leq \max(|y|, |x+y|)$$

Donc $|x| = \max(|y|, |x+y|)$. Or, $|y| < |x|$ donc nécessairement $|x| = \max(|y|, |x+y|) = |x+y|$. Ainsi, $|x+y| = |x| = \max(|x|, |y|)$.

(ii). Soient $x_0, x \in \mathbb{K}$ et $r > 0$ tels que $x \in B(x_0, r)$. Alors $|x - x_0| < r$ si $y \in B(x, r)$, on a $|y - x| < r$ et donc :

$$|y - x_0| \leq \max(|y - x|, |x - x_0|) < r$$

de sorte que $y \in B(x_0, r)$. Ainsi, $B(x_0, r) \subset B(x, r)$ et comme $x_0 \in B(x, r)$, on peut appliquer le raisonnement précédent pour obtenir l'inclusion réciproque.

(iii). Soient $B_1 := B(x_1, r_1)$ et $B_2 := B(x_2, r_2)$ deux boules de $\mathbb{K}$. Alors si $B_1 \cap B_2 \neq \emptyset$, on peut prendre $x \in B_1 \cap B_2$, qui vérifie d'après le point prcédédent $B(x, r_1) = B_1$ et $B(x, r_2) = B_2$. Donc si $r_1 \leq r_2$, $B_1 \subset B_2$ et si $r_1 > r_2$ alors $B_2 \subset B_1$.

(iv). Soit $B := B(x, r)$ une boule ouverte de $\mathbb{K}$. Elle est clairement ouverte. En outre, si $y \in \mathbb{K} \setminus B$ alors $B(y, r)$ n'est pas incluse dans B et B n'est pas incluse dans $B(x, r)$ non plus donc $B(y, r) \subset \mathbb{K} \setminus B$ d'après le point précédent. Donc $\mathbb{K} \setminus B$ est ouvert et ainsi B est fermée.
Le point (ii). étant aussi valable pour les boules fermées en vertu d'un raisonnement strictement analogue, on en déduit que toute boule fermée est ouverte.

(v). Soit C un connexe de $\mathbb{K}$. Supposons par l'absurde que C contienne deux éléments distincts x et y. Alors $B := B\left(x, \frac{|x-y|}{2}\right)$ contient x et ne contient pas y donc $B \cap C, (\mathbb{K} \setminus B) \cap C \neq \emptyset$ et le point précédent assure que ces deux ensembles sont des ouverts de C, ce qui contredit la connexité de C.

□

C.1.2 Anneau de valuation discrète

Proposition C.1.2. ***(i).*** *Soit $\mathbb{K}$ est un corps muni valuation discrète v. Alors $O_{\mathbb{K},v}$ est un anneau de valuation discrète et $\mathbb{K}$ est son corps de fractions.*

(ii). *Soient $\mathbb{A}$ est un anneau de valuation discrète et $\mathbb{K}$ son corps de fractions. Alors $\mathbb{A}$ n'admet qu'un seul élément irréductible r à multiplication par un inversible près. Tout élément x de $\mathbb{A}^*$ s'écrit alors de façon unique $x = ur^k$ avec u inversible dans $\mathbb{A}$ et $k \in \mathbb{N}$. On pose alors $v(x) := k$ et $v(0) = +\infty$. On étend facilement v à $\mathbb{K}$ en posant $v(y) = v(a) - v(b)$ pour tout $y \in \mathbb{K}$, $(a, b) \in \mathbb{A} \times \mathbb{A}^*$ étant un représentant fractionnaire de y. Cette définition est indépendante du représentant choisi, et on obtient ainsi une valuation discrète sur $\mathbb{K}$. Pour cette valuation, $\mathbb{A} = O_{\mathbb{K},v}$ et l'unique idéal premier de $\mathbb{A}$ est $M_{\mathbb{K},v} = r\mathbb{A}$.*

Démonstration. **(i).** Supposons que $\mathbb{K}$ soit un corps muni d'une valuation discrète v. Alors $v(\mathbb{K}^*)$ est un sous-groupe monogène de $(\mathbb{R}, +)$ donc on dispose de $r \in \mathbb{K}^*$ tel que $v(r)$ soit un générateur strictement positif de $v(\mathbb{K}^*)$.

Soit I un idéal non nul de $O_{\mathbb{K},v}$. Soient $k_0 := \min\left\{\frac{v(x)}{v(r)} \mid x \in I\right\}$ et x_0 réalisant ce minimum. Alors on peut écrire $x_0 := u_0 r^{k_0}$ avec $v(u_0) = 0$ donc u_0 inversible dans $O_{\mathbb{K},v}$, d'après une remarque faite plus haut. Donc $r^{k_0} = u^{-1}x_0 \in I$, puis $r^{k_0}O_{\mathbb{K},v} \in I$. Réciprquement, si $x \in I \setminus \{0\}$, on peut écrire $v(x) = kv(r)$ avec $k \geq k_0$ et on a alors $x = ur^k = ur^{k-k_0}r^{k_0}$ avec u inversible dans $O_{\mathbb{K},v}$, donc $x \in r^{k_0}O_{\mathbb{K},v}$. Ainsi, $I = r^{k_0}O_{\mathbb{K},v}$.

Ceci est en particulier vrai pour $I = M_{\mathbb{K},v}$ (on a alors $k_0 = 1$). Le seul idéal plus grand que $M_{\mathbb{K},v}$ pour l'inclusion est donc $O_{\mathbb{K},v}$. Ainsi, $M_{\mathbb{K},v}$ est un idéal maximal donc premier de $O_{\mathbb{K},v}$. Il est par ailleurs clair que c'est le seul idéal premier. En effet, si I est un autre idéal de $O_{\mathbb{K},v}$ alors il est soit $O_{\mathbb{K},v}$ soit de la forme $r^k O_{\mathbb{K},v}$ pour $k \geq 2$, de sorte que les $\overline{r}\overline{r^{k-1}} = 0$ dans $O_{\mathbb{K},v}/I$ avec $\overline{r}, \overline{r^{k-1}} \neq 0$. Ainsi, $O_{\mathbb{K},v}$ est un anneau de valuation discrète.

Il reste à vérifier que $\mathbb{K}$ est le corps des fractions de $O_{\mathbb{K},v}$. $\mathbb{K}$ contient clairement le corps des fractions de $O_{\mathbb{K},v}$. Réciproquement, si $x \in \mathbb{K} \setminus O_{\mathbb{K},v}$ alors $v(x) < 0$ donc on peut écrire $v(x) = -kv(r)$ avec $k \in \mathbb{N}^*$. On a alors $x = \frac{u}{r^k}$ avec $u \in \mathcal{U}(O_{\mathbb{K},v})$. Ceci prouve que $\mathbb{K}$ est bien le corps des fractions de $O_{\mathbb{K},v}$.

(ii). Soit $M_{\mathbb{A}}$ l'unique idéal maximal de $\mathbb{A}$. Comme $\mathbb{A}$ est principal, $M_{\mathbb{A}}$ admet un générateur $r \in \mathbb{A}$ qui est irréductible (un idéal maximal étant toujours premier). Si $s \in \mathbb{A}$ est un autre irréductible alors $s\mathbb{A}$ est premier donc $s\mathbb{A} = r\mathbb{A}$ et ainsi, $s = ur$ et $r = u's$ avec $u, u' \in \mathbb{A}^*$. Donc $s = uu's$ puis $uu' = 1$ par intégrité de $\mathbb{A}$ donc u est inversible dans $\mathbb{A}$. Donc r est bien l'unique irréductible à multiplication par un inversible près.

Comme $\mathbb{A}$ est principal, il est factoriel donc on peut écrire tout élément x de $\mathbb{A}$ de façon unique sous la forme $x = ur^k$ avec $u \in \mathcal{U}(\mathbb{A})$ et $k \in \mathbb{N}$. En définissant la valuation v comme dans l'énoncé de la proposition, on obtient alors le reste des résultats attendus en vertu du point (i). (étant bien entendu que $\mathbb{A} = O_{\mathbb{K},v}$ pour la valuation ainsi définie).

□

Pour plus de précisions sur ce qui suit, on renvoit à l'annexe B donnant des compléments d'arithmétique sur les anneaux (anneaux néothériens, factoriels... etc).

Proposition C.1.3 (Caractérisation des anneaux de valuation discrète.)**.** *Soit $\mathbb{A}$ un anneau commutatif. $\mathbb{A}$ est un anneau de valuation discrète si et seulement si c'est un anneau local (qui possède un unique idéal maximal) noetherien dont l'idéal maximal est engendré par un élément non nilpotent.*

Démonstration. Le sens direct étant immédiat, on ne s'intéresse qu'à la réciproque : soit $\mathbb{A}$ un anneau commutatif local noetherien dont l'idéal maximal est engendré par $r \in \mathbb{A}$ non nilpotent. Soit I un idéal de $\mathbb{A}$. Montrons dans un premier temps que l'une des deux propriétés est vérifiée :

— $I = \mathbb{A}$

— $I \subset r\mathbb{A}$.

En effet, si $I \neq \mathbb{A}$, soit I est maximal et $I = r\mathbb{A}$ par unicité, soit I n'est pas maximal est il existe I_1 un idéal de $\mathbb{A}$ tel que $I \subset I_1 \neq \mathbb{A}$. Supposons $I \not\subset r\mathbb{A}$. Soit $n \geq 1$. On suppose qu'il existe $(I_i)_{1 \leq i \leq n}$ tel que $I \subsetneq I_1 \subsetneq \cdots \subsetneq I_n \neq \mathbb{A}$. Comme $I \not\subset r\mathbb{A}$, I_n n'est pas maximal donc il existe I_{n+1} un idéal distinct de $\mathbb{A}$ qui le contient. On peut donc construire une suite strictement croissante d'idéaux, ce qui contredit le caractère noetherien de $\mathbb{A}$.

Dans un deuxième temps, montrons que I est de la forme $r^n\mathbb{A}$. De nouveau, raisonnons par l'absurde : $I \subset r\mathbb{A}$ donc on peut poser $I_1 = \frac{1}{r}I$, vérifier qu'il s'agit d'un idéal de $\mathbb{A}$ et construire une suite d'idéaux strictement croissante telle que $I = r^n I_n$. En effet, comme I n'est pas de la forme $r^n\mathbb{A}$, aucun de ces idéaux n'est maximal ou égal à $\mathbb{A}$ ce qui permet de construire cette suite par récurrence.

Nous avons donc montré que I est principal. De plus I est local et r n'est pas nilpotent donc on déduit du théorème fondamental de l'arithmétique que $\mathbb{A}$ est intègre. Cela achève la démonstration : un anneau commutatif local noetherien dont l'idéal maximal est engendré par un élément non nilpotent est bien un anneau de valuation discrète. □

Définition C.1.4. *Un annneau $\mathbb{A}$ est dit* intégralement clos dans un anneau $\mathbb{B}$ *contenant $\mathbb{A}$ si toute racine d'un polynôme unitaire de $\mathbb{A}[X]$ contenue dans $\mathbb{B}$ est en fait un élément de $\mathbb{A}$. Si $\mathbb{A}$ est intègre, on dit simplement qu'il est* intégralement clos *lorsqu'il est intégralement clos dans son corps de fractions.*

Théorème C.1.5 (Caractérisation des anneaux de valuation discrète)**.** *Soit $\mathbb{A}$ un anneau commutatif intègre noetherien. $\mathbb{A}$ est un anneau de valuation discrète si et seulement s'il vérifie les deux propriétés suivantes :*

(i). *$\mathbb{A}$ est intégralement clos.*

(ii). *$\mathbb{A}$ possède un unique idéal premier non nul.*

Démonstration. Un anneau de valuation $\mathbb{A}$ respecte bien évidemment (ii). Soit de plus $x \in \mathbb{K}$ et $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{A}[X]$. Si x $\notin \mathbb{A}$, $v(x) < 0$ donc $v(x^n) = nv(x) < v(a_k) + kv(x) = v(a_k x^k)$ pour tout $k < n$. D'après le lemme 2.1.4 (point (i).), $v(P(x)) = v(x^n) < 0$ donc $P(x) \notin \mathbb{A}$ puis $P(x) \neq 0$. Cela montre que $\mathbb{A}$ est intégralement clos.

Réciproquement, si $\mathbb{A}$ est un anneau commutatif intègre et noethérien qui vérifie (i) et (ii), on va montrer que $\mathbb{A}$ est un anneau de valuation discrète. Pour cela, il suffit de montrer que $\mathbb{A}$ est principal. Comme A est déjà noethérien et local, il suffit de montrer que son idéal maximal m est principal. Pour cela, nous faisons appel à un résultat d'algèbre : dans un anneau local, tout idéal inversible est principal. De plus, il est également connu que l'inverse d'un idéal (ici m), quand il existe, est donné par la construction suivante :

$$m' = \{x \in K / xm \subset A\}$$

Il suffit donc de montrer que m' est bien l'inverse de $m \cdot m'$ est un sous-$\mathbb{A}$-module de K qui contient $\mathbb{A}$ et, par construction, $m \cdot m' \subset \mathbb{A}$ donc c'est un idéal de $\mathbb{A}$. Or $A \subset m'$ donc $m \subset m \cdot m'$. Par maximalité de m, $m \cdot m' = m$ ou $m \cdot m' = \mathbb{A}$.

Commençons par montrer le fameux résultat d'algèbre : si $m \cdot m' = \mathbb{A}$, m est principal. Par définition, si $m \cdot m' = \mathbb{A}$, il existe $n \in \mathbb{N}$ et $(x_i, y_i)_{0 \leq i \leq n} \in m \times m'$ tel que $\sum_{i=0}^{n} x_i y_i = 1$. Comme $m \cdot m' \subset \mathbb{A}$, chaque $x_i y_i$ est dans $\mathbb{A}$ mais comme $m \neq \mathbb{A}$, au moins un (mettons xy) n'est pas dans m. m étant l'idéal maximal de $\mathbb{A}$, xy est un inversible de $\mathbb{A}$, d'inverse $u \in \mathbb{A}$. Alors il existe $y \in m'$ et $x' = ux \in \mathbb{A}$ tel que $\forall a \in m$, $a = x'(ay)$ où $ay \in \mathbb{A}$ par définition de m'. Ainsi $m = x'\mathbb{A}$ donc m est principal.

Montrons ensuite que $m \cdot m' = \mathbb{A}$. Pour cela, il suffit de montrer que $m \cdot m' \neq m$. Pour cela, remarquons que si $m \cdot m' = m$, alors $m' = \mathbb{A}$.

On suppose $m \cdot m' = m$ et on se munit de $x \in m'$. Une récurrence immédiate montre que $\forall n \in \mathbb{N}$, $x^n m \subset m$ puis, par définition : $x^n \in m'$. Pour $n \in \mathbb{N}$, on note a_n le sous-$\mathbb{A}$-module de $\mathbb{K}$ engendré par les $(x^i)_{0 \leq i \leq n}$ alors les $(a_n)_{n \in \mathbb{N}}$ forment une suite croissante de $\mathbb{A}$-module de m'. Comme $\mathbb{A}$ est noetherien, cette suite est stationnaire donc, pour n assez grand, on peut écrire $x^n \in a_n \subset a_{n-1}$ donc x^n est combinaison linéaire sur $\mathbb{A}$ des $(x^i)_{0 \leq i < n}$ donc **x est entier sur** A. Comme $\mathbb{A}$ est intégralement clos, cela montre $x \in \mathbb{A}$ puis $m' \subset \mathbb{A}$.

Enfin, Jean Pierre Serre fournit la démonstration suivante : si $\mathbb{A}$ possède un unique idéal premier non nul, $m' \neq \mathbb{A}$, ce qui achève la démonstration.

Soit x un élément non nul de m et $\mathbb{A}_x$ l'anneau des fractions de la forme $\frac{p}{x^n}$ où $p \in \mathbb{A}$ et $n \in \mathbb{N}$. Supposons que $\mathbb{A}_x$ n'est pas un coprs. Alors il contient un idéal maximal non nul $\mathcal{P}$. Comme x est inversible dans $\mathbb{A}_x$, $x \notin \mathcal{P}$ donc $\mathcal{P} \bigcap \mathbb{A} \neq m$. Soit alors $\frac{p}{x^n}$ un élément non nul de $\mathcal{P}$. $p \in \mathcal{P} \bigcap \mathbb{A}$ donc $\mathcal{P} \bigcap \mathbb{A} \neq \{0\}$. On a donc construit un idéal premier non nul de $\mathbb{A}$ différent de m, ce qui est absurde ! On en déduit que $\mathbb{A}_x$ est un corps. Or $\mathbb{A} \subset \mathbb{A}_x \subset \mathbb{K}$ donc $\mathbb{A}_x = \mathbb{K}$, le plus petit surcorps de $\mathbb{A}$.

Ainsi, pour τ un élément non nul de m, il existe $n \in \mathbb{N}$ et $p \in \mathbb{A}$ tels que $\frac{1}{\tau} = \frac{p}{x^n}$ soit $x^n = y\tau \in \tau\mathbb{A}$. Cela étant vrai pour tout x $\in$ m, on peut se donner une famille $(x_i)_{0 \leq i \leq k}$ génératrice de m (finie car A est noetherien) et n assez grand pour que $x_i^n \in \tau\mathbb{A}$ pour tout i. Pour tout $N > k(n-1)$, $m^N \subset \tau\mathbb{A}$ car tout monôme en les (x_i) de degré supérieur à N contient au moins un facteur en $x_i^n \in \tau\mathbb{A}$. On choisit N le plus petit entier tel que $m^N \subset \tau\mathbb{A}$. Soit alors $y \in m^{N-1}$ tel que $y \notin \tau\mathbb{A}$. Par construction, $ym \in \tau\mathbb{A}$ donc par définition, $\frac{y}{\tau} \in m'$. On a bien $m' \neq \mathbb{A}$. □

C.1.3 Corps locaux et complétion.

Lemme C.1.6 (convergence des suites de $\mathcal{C}(\mathbb{K})$). **(i).** *Si $(a_n)_{n \in \mathbb{N}} \in \mathcal{C}(\mathbb{K})$ alors $(|a_n|)_{n \in \mathbb{N}}$ converge dans $\mathbb{R}$.*

(ii). *Si $|.|$ est ultramétrique alors toute suite de $\mathcal{C}(\mathbb{K}) \setminus 0(\mathbb{K})$ est de norme constante à partir d'un certain rang.*

(iii). *Si $(a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}} \in \mathcal{C}(\mathbb{K})$ et si $(a_n - b_n)_{n \in \mathbb{N}} \in 0(\mathbb{K})$ alors $\lim_{n \to +\infty} |a_n| = \lim_{n \to +\infty} |b_n|$.*

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 $(a_n)_{n \in \mathbb{N}} \in \mathcal{C}(\mathbb{K}) \setminus 0(\mathbb{K})$. 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 2.1.4 $|a_N - a_n| = \max(|a_n|, |a_N|) \geq \min(|a_n|, |a_N|)$).

(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.1.7. *$\mathcal{C}(\mathbb{K})$ est un anneau commutatif pour les lois $+$ et $\times$ dérivées de $\mathbb{K}$ et $0(\mathbb{K})$ 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 $(a_n b_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{K})$ car une suite de Cauchy est toujours bornée (ce qui s'obtient comme conséquence du point (i). du lemme précédent). Donc $\mathcal{C}(\mathbb{K})$ est un anneau commutatif.

$0(\mathbb{K})$ contient la suite nulle (neutre additif), est stable par somme et par produit par tout élément de $\mathcal{C}(\mathbb{K})$ car le produit d'une suite bornée par une suite convergente vers 0 converge vers 0. Ainsi, $0(\mathbb{K})$ en est un idéal de $\mathcal{C}(\mathbb{K})$.

Montrons enfin que $0(\mathbb{K})$ est maximal. Soient $\overline{a} \in \mathcal{C}(\mathbb{K})/0(\mathbb{K}) \setminus 0$ et $a := (a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{K}) \setminus 0(\mathbb{K})$ 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 $(b_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{K})$. En outre, pour tout $n \geq N$, $a_n b_n - 1 = 0$ donc $(a_n b_n - 1)_{n\in\mathbb{N}} \in 0(\mathbb{K})$, et donc $\overline{a}\overline{b} = \overline{1}$ dans $\mathcal{C}(\mathbb{K})/0(\mathbb{K})$, ce qui prouve que $\overline{a}$ est inversible. Donc $\mathcal{C}(\mathbb{K})/0(\mathbb{K})$ est bien un corps et $0(\mathbb{K})$ un idéal maximal de $\mathcal{C}(\mathbb{K})$. □

Théorème C.1.8. *$(\widehat{\mathbb{K}}, |.|)$ est un surcorps normé complet de $\mathbb{K}$ et $\mathbb{K}$ est dense dans $\widehat{\mathbb{K}}$. Pour cette raison, $\widehat{\mathbb{K}}$ est appelé* complété de $\mathbb{K}$.

Démonstration. Par abus, on peut considérer $\widehat{\mathbb{K}}$ comme un surcorps de $\mathbb{K}$ en l'identifiant avec les classes d'équivalence des suites constantes.

On commence par montrer que $\mathbb{K}$ est dense dans $\widehat{\mathbb{K}}$. Soient $\overline{a}$ un élément de $\hat{\mathbb{K}}$ et $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{K})$ 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 $\widehat{\mathbb{K}}$. D'où la densité de $\mathbb{K}$ dans $\widehat{\mathbb{K}}$.

Ce raisonnement permet aussi de montrer que toute suite de Cauchy de $\mathbb{K}$ converge dans $\widehat{\mathbb{K}}$ car si $(a_n)_{n\in\mathbb{N}}$ en est une, alors on a vu qu'elle convergeait vers sa réduction modulo $0(\mathbb{K})$, $\overline{a}$, dans $\widehat{\mathbb{K}}$.

On en déduit finalement que $\widehat{\mathbb{K}}$ est complet. En effet, si $(\overline{a}_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\widehat{\mathbb{K}}$ alors par densité de $\mathbb{K}$ dans $\widehat{\mathbb{K}}$, 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 $\mathbb{K}$ 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 $\widehat{\mathbb{K}}$ 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 $\widehat{\mathbb{K}}$. □

C.2 Le lemme de Hensel et ses applications au relèvement de racines et de facteurs polynomiaux.

Théorème C.2.1 (Hensel). *Soient $(\mathbb{K}, v)$ un corps valué complet et $P \in O_{\mathbb{K},v}[X]$. On suppose qu'il existe $x \in O_{\mathbb{K},v}$ tel que $|P(x)| < |P'(x)|^2$. Alors il existe $\xi \in O_{\mathbb{K},v}$, une racine de P telle que $|x - \xi| \leq \left|\frac{P(x)}{P'(x)}\right| < |P'(x)|$. C'est par ailleurs la seule racine de P contenue dans $B(x, |P'(x)|)$.*

Démonstration. Ce théorème repose sur la méthode de Newton pour approcher les zéros d'une fonction. On pose $x_0 := x$ et pour tout $n \in \mathbb{N}$:

$$x_{n+1} := x_n - \frac{P(x_n)}{P'(x_n)}$$

Posons $a := \left|\frac{|P(x)|}{|P'(x)|^2}\right|$ et montrons par récurrence forte sur $n \in \mathbb{N}$ le résultat suivant :

$$H_n : x_{n+1} \text{ est bien défini et dans } O_{\mathbb{K},v},\ |P'(x_{n+1})| = |P'(x)|,\ |x_{n+1} - x_n| \leq a^{2^n}|P'(x)| \text{ et } |P(x_{n+1})| \leq a^{2^{n+1}}|P'(x)|^2.$$

Initialisation : Par hypothèse $|P'(x)|^2 > |P(x)| \geq 0$ donc $P'(x) \neq 0$ et ainsi, x_1 est bien défini. En outre :

$$|x_1 - x_0| = \left|\frac{P(x)}{P'(x)}\right| = a|P'(x)|$$

Or, $a = \left|\frac{|P(x)|}{|P'(x)|^2}\right| < 1$ par hypothèse et $P'(x) \in O_{\mathbb{K},v}$ car $P \in O_{\mathbb{K},v}[X]$ et $x \in O_{\mathbb{K},v}$ donc $v(P'(x)) \geq 0$ et $|P'(x)| \leq 1$, puis $|x_1 - x_0| < 1$, donc $v(x_1 - x_0) > 0$ et ainsi, $x_1 - x_0 \in O_{\mathbb{K},v}$ i.e. $x_1 \in O_{\mathbb{K},v}$ (car $x_0 = x \in O_{\mathbb{K},v}$).

Pour montrer les deux résultats qu'il reste à vérifier, on prouve le lemme suivant :

Lemme C.2.2. *Si $P \in O_{\mathbb{K},v}[X]$ alors pour tout $k \in \mathbb{N}$, $\frac{1}{k!}P^{(k)} \in O_{\mathbb{K},v}[X]$.*

Démonstration. Par linéarité, il suffit de vérifier que ceci est vrai pour les monômes. Soient $k, l \in \mathbb{N}$. Alors on sait que :

$$\frac{\left(X^l\right)^{(k)}}{k!} = \binom{l}{k} X^{l-k} \in O_{\mathbb{K},v}[X]$$

D'où le résultat. □

La formule de Taylor-Young appliquée à P' nous assure alors l'existence de $d \in O_{\mathbb{K},v}$ (de sorte que $|d| \leq 1$) tel que :

$$P'(x_1) = P'(x_0) + (x_1 - x_0)d$$

Ainsi :

$$|P'(x_1) - P'(x_0)| = |d||x_1 - x_0| \leq |x_1 - x_0| = a|P'(x_0)| < |P'(x_0)|$$

Donc comme $|.|$ est ultramétrique et que $|P'(x_1) - P'(x_0)| \neq |P'(x_0)|$, le lemme 2.1.4 assure que :

$$|P'(x_1)| = |(P'(x_1) - P'(x_0)) + P'(x_0)| = \max(|P'(x_1) - P'(x_0)|, |P'(x_0)|) = |P'(x_0)|$$

Enfin, le lemme précédent appliqué à P assure l'existence de $c \in O_{\mathbb{K},v}$ (de sorte que $|c| \leq 1$) tel que :

$$P(x_1) = P(x_0) + (x_1 - x_0)P'(x_0) + (x_1 - x_0)^2 c$$

Or, $P(x_0) + (x_1 - x_0)P'(x_0) = 0$ par définition de x_1 donc :

$$|P(x_1)| \leq |x_1 - x_0|^2|c| \leq |x_1 - x_0|^2 = a^2|P'(x)|^2$$

D'où H_0.

Hérédité : Soit $n \in \mathbb{N}^*$. Supposons $H_0, \cdots, H_{n-1}$. Alors par H_{n-1}, $P'(x_n) \neq 0$ donc x_{n+1} est bien défini et :

$$\left|\frac{P(x_n)}{P'(x_n)^2}\right| = \left|\frac{P(x_n)}{P'(x)^2}\right| \leq a^{2^n}\frac{|P'(x)|^2}{|P'(x)|^2} = a^{2^n} < 1$$

De sorte que $x_{n+1} \in O_{\mathbb{K},v}$ en vertu d'un raisonnement déjà vu à l'initialisation. Les autres résultats s'obtiennent ensuite par les mêmes calculs que ceux de l'initialisation en utilisant l'hypothèse H_{n-1}. D'où H_n, l'itération et le résultat.

D'après ce que nous venons de prouver, nous avons donc, vu que $a<1$, $P(x_n) \underset{n\to+\infty}{\longrightarrow} 0$ et :

$$\forall m \geq n \in \mathbb{N}, \quad |x_m - x_n| \leq \sum_{k=n}^{m-1} |x_{k+1}-x_k| = \sum_{k=n}^{m-1} a^{2^k}|P'(x)| \leq \sum_{k=n}^{+\infty} a^{2^k}|P'(x)|$$

avec $\sum_{k=n}^{+\infty} a^{2^k} \underset{n\to+\infty}{\longrightarrow} 0$ vu que $\sum_{k\geq 0} a^{2^k}$ converge (car $a<1$). Donc $(x_n)_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{K}$ qui est complet donc elle converge vers un certain $\xi \in \mathbb{K}$. Or, $O_{\mathbb{K},v} = B_f(0,1)$ est fermé donc $\xi \in O_{\mathbb{K},v}$.

En outre, il est facile de vérifier que les polynômes sont des fonctions continues de $\mathbb{K}$ dans lui-même (ceci s'obtient par les mêmes arguments que dans le cas réel), donc $P(x_n) \underset{n\to+\infty}{\longrightarrow} P(\xi)$ et ainsi $P(\xi)=0$.

P' est de même continue et ainsi $|P'(x)| = |P'(x_n)| \underset{n\to+\infty}{\longrightarrow} |P'(\xi)|$ et donc $|P'(\xi)| = |P'(x)|$.

Puis, comme $|.|$ est ultramétrique, on a pour tout $n \in \mathbb{N}$:

$$|x_n - x| = \left|\sum_{k=0}^{n-1}(x_{k+1}-x_k)\right| \leq \max_{0\leq k\leq n-1}|x_{k+1}-x_k| = a|P'(x)| = \left|\frac{P(x)}{P'(x)}\right|$$

Donc $n\to+\infty$ donne que $|\xi - x| \leq \left|\frac{P(x)}{P'(x)}\right| < |P'(x)|$.

Si $\zeta \in \mathbb{K}$ est une autre racine de P dans $B(x,|P'(x)|)$ alors d'après le point (ii). du lemme 2.1.4, $B(\zeta,|P'(x)|) = B(x,|P'(x)|)$ et donc $\xi \in B(\zeta,|P'(x)|)$. On peut donc écrire $\zeta = \xi + h$ avec $h \in \mathbb{K}$ vérifiant $|h| < |P'(x)|$ avec $P'(x) \in O_{\mathbb{K},v}$ donc $|P'(x)| \leq 1$. Donc $|h|<1$, puis $h \in O_{\mathbb{K},v}$ et $\zeta \in O_{\mathbb{K},v}$. Il s'ensuit avec le lemme précédent que :

$$0 = P(\zeta) = P(\xi) + hP'(\xi) + h^2 s = h(P'(x) + hs)$$

avec $s \in O_{\mathbb{K},v}$ donc $|s| \leq 1$. Avec $|hs| \leq |h| < |P'(x)|$ donc $P'(x) + hs \neq 0$ et donc $h=0$ par intégrité de $\mathbb{K}$. Ainsi, $\zeta = \xi$. D'où le résultat. □

Travaillons maintenant pour relever des facteurs polynomiaux. On commence pour cela par rappeler la définition ainsi qu'une propriété du résultant.

Définition C.2.3. *Soient $P,Q \in \mathbb{K}[X]$ de degrés respectifs $deg(P) \leq n$ et $deg(Q) \leq m$. On définit :*

$$\Phi_{P,Q} : (U,V) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] \longmapsto UP + QV \in \mathbb{K}_{n+m-1}[X]$$

On appelle résultant (m,n) de P et Q *et on note $Res_{m,n}(P,Q)$ le déterminant de $\Phi_{P,Q}$ dans les bases canoniques $((X^k,X^l))_{0\leq k\leq m-1, 0\leq l\leq n-1}$ de $\mathbb{K}_{m-1}[X]\times\mathbb{K}_{n-1}[X]$ et $(X^k)_{0\leq k\leq n+m-1}$ de $\mathbb{K}_{n+m-1}[X]$.*

Proposition C.2.4. *Si $(P,Q) \in \mathbb{K}_n[X]\times\mathbb{K}_m[X]$ alors $Res_{m,n}(P,Q)=0$ si et seulement si $deg(P)\leq n-1$ et $deg(Q)\leq m-1$ ou $deg(P\wedge Q)\geq 1$.*

Théorème C.2.5 (Hensel version forte)**.** *Supposons que $(\mathbb{K},v)$ soit un corps valué complet. Soient $P,Q,R \in O_{\mathbb{K},v}[X]$ et $C>0$ tels que :*

(i). *$deg(Q)\leq n$, $deg(R)\leq m$ et $deg(P-QR)\leq n+m-1$.*

(ii). *$v_G(P-QR) \geq C + 2v(Res_{m,n}(Q,R))$.*

Alors il existe $\tilde{Q},\tilde{R} \in O_{\mathbb{K},v}[X]$ tels que :

(i). *$P = \tilde{Q}\tilde{R}$.*

(ii). *$deg(\tilde{Q}-Q)\leq n-1$ et $deg(\tilde{R}-R)\leq m-1$.*

(iii). *$v_G(\tilde{Q}-Q) \geq C + v(Res_{m,n}(Q,R))$ et $v_G(\tilde{R}-R) \geq C + v(Res_{m,n}(Q,R))$.*

Démonstration. Commençons par associer une norme à v_G en posant $|S| := a^{v_G(S)}$ pour tout $S \in \mathbb{K}[X]$ (pour un certaint $a \in]0,1[$).

Si $\mathrm{Res}_{m,n}(Q,R)=0$ alors l'hypothèse (ii). assure que $P=QR$ et le résultat est immédiat. Supposons donc que $\mathrm{Res}_{m,n}(Q,R)\neq 0$. Nous allons alors tenter de transformer le problème pour nous ramener à l'application du théorème de point fixe de Banach.

En effet, le point (ii). du résultat à prouver impose que $V := \tilde{Q} - Q \in \mathbb{K}_{n-1}[X]$ et $U := \tilde{R} - R \in \mathbb{K}_{m-1}[X]$. Ainsi, comme $\mathrm{Res}_{m,n}(Q,R)\neq 0$, $\Phi_{P,Q}$ est inversible et (i). est vérifié si et seulement si :

$$(Q+V)(R+U) = P \Longleftrightarrow QU + RV = P - QR - UV \Longleftrightarrow (U,V) = \Phi_{P,Q}^{-1}(P-QR-UV)$$

On cherche donc un point fixe de l'application :

$$\Psi : (U,V) \in \mathbb{K}_{m-1}[X]\times\mathbb{K}_{n-1}[X] \longmapsto \Phi_{P,Q}^{-1}(P-QR-UV) \in \mathbb{K}_{m-1}[X]\times\mathbb{K}_{n-1}[X]$$

dans la boule fermée de $\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$ munie de la norme produit des normes associées à v_G sur $\mathbb{K}_{m-1}[X]$ et $\mathbb{K}_{m-1}[X]$:

$$B := B_f\left(0, a^{C+v(\mathrm{Res}_{m,n}(Q,R))}\right) = \{(U,V) \in \mathbb{K}_{m-1}[X]\times\mathbb{K}_{n-1}[X] \mid \min(v_G(U), v_G(V)) \geq C+v(\mathrm{Res}_{m,n}(Q,R))\}$$

Comme $(\mathbb{K}, v)$ est complet alors $\mathbb{K}_{m-1}[X]$ et $\mathbb{K}_{n-1}[X]$ sont complets (voir remarque ci-dessus) donc $\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$ est complet. B étant un fermé d'un espace de Banach, c'est aussi un espace de banach donc il suffit donc de vérifier que Ψ est contractante pour appliquer le théorème du point fixe de Banach.

Soit $(U,V) \in B$. Alors :

$$\begin{aligned} v_G(P-QR-UV) &\geq \min(v_G(P-QR), v_G(UV)) \geq \min(C+2v(\mathrm{Res}_{m,n}(Q,R)), 2C+2v(\mathrm{Res}_{m,n}(Q,R))) \\ &\geq C+2v\left(\mathrm{Res}_{m,n}(Q,R)\right) \end{aligned}$$

Soient Φ_1, Ψ_1 et Φ_2, Ψ_2 les projetés de $\Phi_{P,Q}^{-1}$ et Ψ sur $\mathbb{K}_{m-1}[X] \times \{0\}$ et $\{0\} \times \mathbb{K}_{n-1}[X]$ respectivement. Comme P et Q sont à coefficients dans $O_{\mathbb{K},v}$, la matrice canoniquement associée à $\Phi_{P,Q}$ est à coefficients dans $O_{\mathbb{K},v}$ et la formule d'inversion d'une matrice à l'aide de ses cofacteurs assure alors que la matrice canoniquement associée à $\Phi_{P,Q}^{-1}$ est à coefficients dans $\frac{1}{\mathrm{Res}_{m,b(Q,R)}} O_{\mathbb{K},v}$. Ainsi, $\min(v_G(\Phi_1(S)), v_G(\Phi_2(S))) \geq v_G(S) - v(\mathrm{Res}_{m,n}(Q,R))$ pour tout $S \in \mathbb{K}_{n+m-1}[X]$. Ainsi :

$$\min(v_G(\Phi_1(P-QR-UV)), v_G(\Phi_2(P-QR-UV))) \geq C + v(\mathrm{Res}_{m,n}(Q,R))$$

Et donc Φ est définie de B dans elle même.

Soient $(U,V), (U',V') \in B$. Alors :

$$\begin{aligned} v_G(\Phi_1(U,V) - \Phi_1(U',V')) &= v_G(\Phi_{P,Q}^{-1}(UV-U'V')) \geq v_G(UV-U'V') - v(\mathrm{Res}_{m,n}(Q,R)) \\ &= v_G(U(V-V') + V'(U-U')) - v(\mathrm{Res}_{m,n}(Q,R)) \\ &\geq \min(v_G(U(V-V')), v_G(V'(U-U'))) - v(\mathrm{Res}_{m,n}(Q,R)) \\ &= \min(v_G(U)+v_G(V-V'), v_G(V')+v_G(U-U')) - v(\mathrm{Res}_{m,n}(Q,R)) \\ &\geq \min(v_G(U), v_G(V')) + \min(v_G(V-V'), v_G(U-U')) - v(\mathrm{Res}_{m,n}(Q,R)) \\ &\geq C + \min(v_G(V-V'), v_G(U-U')) \end{aligned}$$

Et de même pour Ψ_2. Donc :

$$\begin{aligned} |\Psi(U,V) - \Psi(U',V')| &= \max(a^{v_G(\Phi_1(U,V)-\Phi_1(U',V'))}, a^{v_G(\Phi_2(U,V)-\Phi_2(U',V'))}) \leq a^C |(U,V)-(U',V')| \\ &< |(U,V)-(U',V')| \end{aligned}$$

Et Ψ est bien contractante. D'où le résultat. □

Après ces quelques préliminaires, on peut prouver un résultat qui découle du lemme de Hensel et qui dit en substance que si l'on dispose d'une "presque factorisation" d'un polynôme de $O_{\mathbb{K},v}[X]$ alors on dispose effectivement d'une factoristion dans $O_{\mathbb{K},v}[X]$, qui n'est pas trop loin de la factorisation initiale.

On peut illustrer une application de ce lemme technique avec le relèvement de facteurs polynomiaux.

Corollaire C.2.6. *Soient $P, Q, R \in O_{\mathbb{K},v}[X]$ tels que :*

(i). *Q est unitaire de degré n.*

(ii). *$deg(R) \leq m$ et $deg(P-QR) \leq n+m-1$.*

(iii). *Les réductions $\overline{Q}$ et $\overline{R}$ de Q et R modulo $M_{\mathbb{K},v}$ sont premières entre elles.*

(iv). *$\overline{P} = \overline{QR}$ modulo $M_{\mathbb{K},v}$.*

Alors il existe un unique couple $(\tilde{P}, \tilde{Q}) \in O_{\mathbb{K},v}[X]^2$ tel que :

(i). *$deg(\tilde{Q}-Q) \leq n-1$ et $deg(\tilde{R}-R) \leq m-1$.*

(ii). *$\overline{\tilde{Q}} = \overline{Q}$ et $\overline{\tilde{R}} = \overline{R}$ modulo $M_{\mathbb{K},v}$.*

(iii). *$P = \tilde{Q}\tilde{R}$.*

Démonstration. Comme $\overline{Q}$ et $\overline{R}$ sont premiers entre eux, on a $\mathrm{Res}_{m,n}(\overline{Q}, \overline{R}) \neq \overline{0}$ modulo $M_{\mathbb{K},v}$ et donc Q et R étant à coefficients dans $O_{\mathbb{K},v}$, $\mathrm{Res}_{m,n}(Q,R) \in O_{\mathbb{K},v} \setminus M_{\mathbb{K},v}$, i.e. $v(\mathrm{Res}_{m,n}(Q,R)) = 0$. Comme $\overline{P} = \overline{QR}$ modulo $M_{\mathbb{K},v}$, on a $v_G(P-QR) > 0$ et on peut donc appliquer le théorème précédent en prenant nimporte quel $C \in]0, v_G(P-QR)[$. Ceci prouve l'existence.

Pour l'unicité, on reprend les notations du théorèmes précédent et on utilise le fait que pour tout $C \in]0, v_G(P-QR)[$, l'application Φ admet un unique point fixe dans $B_f(0, a^C)$ d'après le théorème de Banach, ce qui prouve en faisant tendre C vers 0 que l'unicité reste valable sur $B(0,1)$ (boule ouverte). Mais les couples $(U,V) = (\tilde{R}-R, \tilde{Q}-Q) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$ solutions du problème de point fixe de norme 1 sont tels que $v_G(U) = v_G(V) = 0$ ce qui contredit le point (ii). que le couple $(\tilde{P}, \tilde{Q})$ doit vérifier. Les solutions de norme > 1 étant exclues car elles ne sont pas à coefficients dans $O_{\mathbb{K},v}$, on obtient bien l'unicité. □

Prouvons enfin comme annoncé un petit lemme technique.

Lemme C.2.7. *Soit $P \in \mathbb{K}[X]$ irréductible tel que $P(0) \in O_{\mathbb{K},v}$. Alors $P \in O_{\mathbb{K},v}[X]$.*

Démonstration. Supposons par l'absurde que P n'est pas à coefficient dans $O_{\mathbb{K},v}$. Soit a le coefficient de P de degré d maximal parmi ceux qui ont une valuation minimale, c'est à dire qui réalisent $v_G(P)$. Alors $v(a) = v_G(P) < 0$ et donc $a \neq 0$. On peut donc considérer $a^{-1}P$, qui est à coefficients dans $O_{\mathbb{K},v}$. Ecrivons :

$$a^{-1}P = \sum_{k=0}^{d-1} b_k X^k + X^d + \sum_{k=d+1}^{n} b_k X^k$$

avec $b_0, \cdots, b_{d-1}, b_{d+1}, \cdots, b_n \in O_{\mathbb{K},v}$. Notons que $v(b_k) > 0$ pour tout $k \in \{d+1, \cdots, n\}$ et posons $Q := \sum_{k=0}^{d-1} b_k X^k + X^d$, $R := 1 + b_n X^{n-d}$. Alors Q est unitaire de degré d, $\deg(R) = n-d$, $\deg(P-QR) \leq n-1$, $Q \equiv 1$ modulo $M_{\mathbb{K},v}$, de sorte que $QR \equiv a^{-1}P$ modulo $M_{\mathbb{K},v}$ et que les réduites de Q et R modulo $M_{\mathbb{K},v}$ soient premières entre elles. Donc on peut appliquer le corrollaire précédent et obtenir l'existence de $(\tilde{P}, \tilde{Q}) \in O_{\mathbb{K},v}[X]^2$ tel que $P = a\tilde{Q}\tilde{R}$ et $\deg(\tilde{Q}-Q) \leq d-1$ et $\deg(\tilde{R}-R) \leq n-d-1$. Mais alors ni $\tilde{Q}$, ni $\tilde{R}$ ne sont constants. Ceci contredit l'irréductibilité de P. □

C.3 Extension non ramifiée de corps locaux et application au relèvement de $\mathbb{F}_q$.

C.3.1 Prolongement d'une valuation.

Lemme C.3.1. *Si l'on note a_0 le coefficient constant du polynôme minimal de $x \in \mathbb{L}$ sur $\mathbb{K}$ et d son degré, alors $d|[\mathbb{L}:\mathbb{K}]$,*

$$N_{\mathbb{L}/\mathbb{K}}(x) = (-1)^{[\mathbb{L}:\mathbb{K}]} a_0^{[\mathbb{L}:\mathbb{K}]/d} \quad \text{et} \quad T_{\mathbb{L}/\mathbb{K}}(x) = -\frac{[\mathbb{L}:\mathbb{K}]a_{d-1}}{d}$$

Démonstration. $\mathbb{L}$ est une extension finie de $\mathbb{K}[x]$, qui est une extension finie (de degré d) de $\mathbb{K}$ donc le théorème de la base télescopique assure que :

$$[\mathbb{L}:\mathbb{K}] = [\mathbb{L}:\mathbb{K}[x]][\mathbb{K}[x]:\mathbb{K}] = [\mathbb{L}:\mathbb{K}[x]]d$$

Donc $d|[\mathbb{L}:\mathbb{K}]$. Notons $\Pi_x := \sum_{k=0}^{d-1} a_k X^k + X^d$ avec $a_0, \cdots, a_{d-1} \in \mathbb{K}$, le polynôme minimal de x sur $\mathbb{K}$ et posons $e := [\mathbb{L}:\mathbb{K}[x]] = \frac{[\mathbb{L}:\mathbb{K}]}{d}$. Soit $(u_1, \cdots, u_e)$ une $\mathbb{K}[x]$-base de $\mathbb{L}$. On sait que $(x^i)_{0 \leq i \leq d-1}$ est une $\mathbb{K}$-base de $\mathbb{K}[x]$, et donc que $\mathcal{B} := (x^i u_j)_{\substack{0 \leq i \leq d-1 \\ 1 \leq j \leq e}}$ est une $\mathbb{K}$-base de $\mathbb{L}$ (en vertu du théorème de la base téléscopique). Dans cette base, l'endomorphisme $y \in \mathbb{L} \longmapsto xy$ a une matrice diagonale par blocs, consitituée de e blocs compagnons de la forme :

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & 1 & -a_{d-1} \end{pmatrix}$$

Dont le déterminant vaut $(-1)^d a_0$ (comme on le voit en développant suivant la première ligne). Ainsi, le déterminant de $y \in \mathbb{L} \longmapsto xy$ vaut :

$$N_{\mathbb{L}/\mathbb{K}}(x) = ((-1)^d a_0)^e = (-1)^{[\mathbb{L}:\mathbb{K}]} a_0^{[\mathbb{L}:\mathbb{K}]/d}$$

Et sa trace vaut $T_{\mathbb{L}/\mathbb{K}}(x) = -ea_{d-1} = -\frac{[\mathbb{L}:\mathbb{K}]a_{d-1}}{d}$. □

Proposition C.3.2. *Soit $\mathbb{K}$ un corps muni de deux normes $|.|_1$ et $|.|_2$. Alors $|.|_1$ et $|.|_2$ sont équivalentes si et seulement si il existe $\alpha \in \mathbb{R}_+^*$ tel que $|.|_2 = |.|_1^\alpha$.*

Démonstration. Lorsqu'il existe $\alpha \in \mathbb{R}_+^*$ tel que $|.|_2 = |.|_1^\alpha$, il est immédiat que $|.|_1$ et $|.|_2$ sont équivalentes. Réciproquement, supposons que $|.|_1$ et $|.|_2$ soient équivalentes. Alors la notion de convergence est la même pour $|.|_1$ et $|.|_2$ et donc pour tout $x \in \mathbb{K}$, $(x^n)_{n\in\mathbb{N}}$ converge pour $|.|_1$ si et seulement si elle converge pour $|.|_2$. Or, $(x^n)_{n\in\mathbb{N}}$ ne converge que si x est de norme < 1 (quelle que soit la norme). Donc $|x|_1 < 1 \iff |x|_2 < 1$.

On distingue alors deux cas. Supposons que tous les éléments de $\mathbb{K}^*$ soient de norme ($|.|_1$ et $|.|_2$) ≥ 1. Alors ils sont tous de norme 1 (car $|x||x^{-1}| = 1$ pour tout $x \in \mathbb{K}$ et toute norme $|.|$ sur $\mathbb{K}$). Ainsi, $|.|_2 = |.|_1 (= 1 \text{ sur } \mathbb{K}^*)$.

Supposons maintenant qu'il existe $x_0 \in \mathbb{K}^*$ tel que $|x_0|_1 < 1$ et $|x_0|_2 < 1$. Soit $y \in \mathbb{K}^*$. Alors pour tout $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$:

$$|x_0^{-a} y^b|_1 < 1 \iff |x_0^{-a} y^b|_2 < 1$$

Alors en passant au ln, comme $|x_0|_1 < 1$ et $|x_0|_2 < 1$:

$$\frac{\ln |y|_1}{\ln |x_0|_1} > \frac{a}{b} \iff \frac{\ln |y|_2}{\ln |x_0|_2} > \frac{a}{b}$$

De sorte que :

$$\left\{ r \in \mathbb{Q} \mid \frac{\ln |y|_1}{\ln |x_0|_1} > r \right\} = \left\{ r \in \mathbb{Q} \mid \frac{\ln |y|_2}{\ln |x_0|_2} > r \right\}$$

Et donc en passant au sup ($\mathbb{Q}$ étant dense dans $\mathbb{R}$), de ces ensembles, on obtient que : $\frac{\ln |y|_1}{\ln |x_0|_1} = \frac{\ln |y|_2}{\ln |x_0|_2}$, puis que $\frac{\ln |y|_2}{\ln |y|_1} = \frac{\ln |x_0|_2}{\ln |x_0|_1}$, et ce pour tout $y \in \mathbb{K}^*$. Donc en posant $\alpha := \frac{\ln |x_0|_2}{\ln |x_0|_1}$, on obtient bien que $|.|_2 = |.|_1^\alpha$. □

Théorème C.3.3 (prolongement des valuations)**.** *Soient $(\mathbb{K}, v)$ un corps valué complet et $\mathbb{L}$ une extension finie de $\mathbb{K}$. Alors v se prolonge de manière unique en $\tilde{v}$ sur $\mathbb{L}$ donnée par :*

$$\tilde{v}(x) = \frac{1}{[\mathbb{L} : \mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(x))$$

pour tout $x \in \mathbb{L}$.

Démonstration. Commençons par vérifier que $\tilde{v}$ définit bien une valuation. Si $x \in \mathbb{L}$ vérifie $\tilde{v}(x) = +\infty$ alors $N_{\mathbb{L}/\mathbb{K}}(x) = 0$ donc d'après le lemme C.3.1, le coefficient constant du polynôme minimal de x est nul et $x = 0$. Si $x, y \in \mathbb{L}$ alors la multiplicativité du déterminant assure que :

$$\begin{aligned}\tilde{v}(x \cdot y) &= \frac{1}{[\mathbb{L} : \mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(x \cdot y)) = \frac{1}{[\mathbb{L} : \mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(x) N_{\mathbb{L}/\mathbb{K}}(y)) = \frac{1}{[\mathbb{L} : \mathbb{K}]} (v(N_{\mathbb{L}/\mathbb{K}}(x)) + v(N_{\mathbb{L}/\mathbb{K}}(y))) \\ &= \tilde{v}(x) + \tilde{v}(y)\end{aligned}$$

Il reste à vérifier que pour tous $x, y \in \mathbb{L}$, $\tilde{v}(x + y) \geq \min(\tilde{v}(x), \tilde{v}(y))$, ce qui est trivial si $y = 0$ et équivaut à $\tilde{v}\left(1 + \frac{x}{y}\right) \geq \min\left(\tilde{v}\left(\frac{x}{y}\right), 0\right)$ sinon (par soustraction de $\tilde{v}(y)$). Ceci revient à montrer que si $x \in \mathbb{L}$ vérifie $\tilde{v}(x) \geq 0$ alors $\tilde{v}(1 + x) \geq 0$. Mais si $v(N_{\mathbb{L}/\mathbb{K}}(x)) \geq 0$, alors d'après le lemme C.3.1, $\tilde{v}(\Pi_x(0)) = \frac{\deg(\Pi_x)}{[\mathbb{L}:\mathbb{K}]} \tilde{v}(N_{\mathbb{L}/\mathbb{K}}(x)) \geq 0$ et donc $\Pi_x(0) \in O_{\mathbb{K},v}$ et comme Π_x est irréductible, le lemme C.2.7 assure que $\Pi_x \in O_{\mathbb{K},v}[X]$. Mais Π_{1+x} divise $\Pi_x(X - 1)$, qui est un polynôme annulateur de $1 + x$ et si par l'absurde il n'était pas égal à $\Pi_x(X - 1)$, alors comme il est unitaire, il serait de degré $< \deg(\Pi_x)$ et alors $\Pi_{1+x}(1 + X)$ serait un polynôme annulateur de x de degré $< \deg(\Pi_x)$, ce qui contredirait la minimalité de Π_x. Donc $\Pi_{1+x} = \Pi_x(X - 1)$ et donc d'après le lemme C.3.1 :

$$N_{\mathbb{L}/\mathbb{K}}(1 + x) = (-1)^{[\mathbb{L}:\mathbb{K}]} \Pi_x(-1)^{[\mathbb{L}:\mathbb{K}]/\deg(\Pi_x)} \in O_{\mathbb{K},v}$$

et ainsi, $\tilde{v}(N_{\mathbb{L}/\mathbb{K}}(1 + x)) \geq 0$. Donc $\tilde{v}$ est bien une valuation sur $\mathbb{L}$.

Vérifions qu'elle prolonge v. En effet, si $x \in \mathbb{K}$ alors $\Pi_x = X - x$ donc d'après le lemme C.3.1 :

$$\tilde{v}(x) = \frac{1}{[\mathbb{L} : \mathbb{K}]} v((-1)^{[\mathbb{L}:\mathbb{K}]} (-x)^{[\mathbb{L}:\mathbb{K}]}) = v(x)$$

On prouve maintenant l'unicité. Si v_2 est une autre valuation qui prolonge v alors comme $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie et que $\mathbb{K}$ est complet, les normes $|.|_1 := a^{\tilde{v}}$ et $|.|_2 := a^{v_2}$ (pour $a \in]0, 1[$ quelconque) sont équivalentes sur $\mathbb{L}$ donc d'après la proposition précédente, on dispose de $\alpha \in \mathbb{R}_+^*$ tel que $|.|_2 = |.|_1^\alpha$. Mais alors $v_2 = \alpha \tilde{v}$ et donc sur $\mathbb{K}$: $\tilde{v} = v = v_2 = \alpha \tilde{v}$, puis $\alpha = 1$. Donc $v_2 = \tilde{v}$. □

C.3.2 Extension non-ramifiée d'un corps local et relèvement de $\mathbb{F}_q$.

Proposition C.3.4. *L est une extension finie de K de degré au plus $[\mathbb{L} : \mathbb{K}]$.*

Démonstration. K s'injecte dans L en prenant pour tout $\overline{\alpha} \in K$ un représentant $\alpha \in O_{\mathbb{K}} \subset O_{\mathbb{L}}$ et en le réduisant modulo $M_{\mathbb{L}}$ (ce qui redonne $\overline{\alpha}$). Ainsi, L est une extension finie de K.

Soit $(\overline{x_1}, \cdots, \overline{x_d})$ est une K-base de L et $(x_1, \cdots, x_d)$ un relevé de cette base modulo $M_{\mathbb{L}}$. Alors si $\lambda_1, \cdots, \lambda_d \in \mathbb{K}$ non tous nuls vérifient :

$$\sum_{k=1}^{d} \lambda_k x_k = 0$$

on peut supposer que tous les λ_i sont dans $O_{\mathbb{K}}$ et que l'un d'entre eux est de valuation nulle, donc dans $O_{\mathbb{L}} \setminus M_{\mathbb{L}}$, quitte à multiplier les λ_i par l'élément de plus petite valuation. Ceci qui donne en réduisant modulo $M_{\mathbb{L}}$ une K-relation de liaison non-triviale sur L pour $(\overline{x_1}, \cdots, \overline{x_d})$, un élément de valuation nulle étant non nul modulo $M_{\mathbb{L}}$. Ceci contredit la liberté de $(\overline{x_1}, \cdots, \overline{x_d})$. Donc $(x_1, \cdots, x_d)$ est $\mathbb{K}$-libre sur $\mathbb{L}$ et ainsi :

$$[\mathbb{L} : \mathbb{K}] \geq d = [L : K]$$

□

Proposition C.3.5. *$\mathbb{K}^{nr}$ est un sous-corps de $\overline{\mathbb{K}}$, la clôture algébrique de $\mathbb{K}$.*

Démonstration. Soit $x \in \mathbb{K}^{nr}$. Alors $x \in W(L)$ pour une certaine extension finie L de K. K étant parfait, le théorème de l'élément primitif assure l'existence de $\overline{\alpha} \in L$ tel que $L = K[\overline{\alpha}]$. Mais $\overline{\alpha}$ est algébrique sur K donc c'est une racine de son polynôme minimal $\Pi_{\overline{\alpha}} \in K[X]$. Mais K étant parfait et $\Pi_{\overline{\alpha}}$ étant irréductible, le théorème 4.5.3 de [6] assure que $\overline{\alpha} \in L$ est une racine simple de $\Pi_{\overline{\alpha}}$. Soit $\tilde{\Pi}_{\overline{\alpha}} \in O_{\mathbb{K}}[X]$ un représentant de $\Pi_{\overline{\alpha}}$ modulo $M_{\mathbb{K}}$. On peut donc, d'après le corollaire 2.2.2 relever $\overline{\alpha}$ en $\alpha \in O_{W(L)}$, de telle sorte que $\tilde{\Pi}_{\overline{\alpha}}(\alpha) = 0$. Mais alors $\tilde{\Pi}_{\overline{\alpha}}$ est le polynôme minimal de α (sinon on contredirait la minimalité de $\Pi_{\overline{\alpha}}$ en réduisant modulo $M_{W(L)}$). Ainsi :

$$[\mathbb{K}[\alpha] : \mathbb{K}] = \deg(\tilde{\Pi}_{\overline{\alpha}}) = \deg(\Pi_{\overline{\alpha}}) = [L : K] = [W(L) : \mathbb{K}]$$

et donc $W(L) = \mathbb{K}[\alpha]$. Donc $x \in K[\alpha] \subset \overline{\mathbb{K}}$, la dernière inclusion venant du fait que $\tilde{\Pi}_{\overline{\alpha}}$ est un polynôme annulateur de α à coefficients dans $\mathbb{K}$. Ainsi, $\mathbb{K}^{nr} \subset \overline{\mathbb{K}}$.

Il est par ailleurs clair que $\mathbb{K}^{nr}$ contient 0 et 1 (qui sont dans $W(L)$ pour toute extension finie L de K). Si maintenant, $x, y \in \mathbb{K}^{nr}$ alors $x \in W(L)$ et $y \in W(M)$ pour L et M des extensions finies de K. K étant parfait, le théorème de l'élément primitif assure alors l'existence de $\overline{\alpha} \in M$ tel que $M = K[\overline{\alpha}]$. Considérons alors $N := L[\overline{\alpha}]$. Comme $\overline{\alpha}$ est algébrique sur K, il est algébrique sur L (qui est un extension de K) et donc N est bien un corps qui contient L et $K[\overline{\alpha}] = M$. C'est de plus une extension finie de L (car $\overline{\alpha}$ est algébrique), qui est elle-même une extension finie de K, donc une extension finie de K d'après le théorème de la base télescopique. On peut donc considérer $W(N)$. Or, en vertu d'un raisonnement déjà vu ci-dessus (appliquant le corollaire 2.2.2 au polynôme minimal de $\overline{\alpha}$ relevé dans $O_{W(N)}$), on peut écrire $W(M) = \mathbb{K}[\alpha]$ pour un certain représentant $\alpha \in O_{W(N)} \subset W(N)$ de $\overline{\alpha}$ modulo $M_{\mathbb{K}}$. Il est donc clair que $W(M) \subset W(N)$. Pour la même raison, $W(L) \subset W(N)$. Ainsi, $x, y \in W(N)$ et donc $x + y, x - y, xy \in W(N) \subset \mathbb{K}^{nr}$. Enfin, si $x \neq 0$ alors $x^{-1} \in W(L) \subset \mathbb{K}^{nr}$. Donc $\mathbb{K}^{nr}$ est bien un sous-corps de $\overline{\mathbb{K}}$. □

Lemme C.3.6. *Soit $P \in O_{\mathbb{K}}[X]$ un polynôme unitaire dont la réduction $\overline{P}$ modulo $M_{\mathbb{K}}$ est sans facteur carré. Alors toutes les racines de P sont dans $O_{\mathbb{K}^{nr}}$.*

Démonstration. Comme $\overline{P}$ est sans facteurs carré, on peut décomposer $\overline{P}$ en produit d'irréductibles unitaires de $K[X]$:

$$\overline{P} := \prod_{i=1}^{k} \overline{P}_i$$

Comme les $\overline{P}_i$ sont premiers entre eux deux à deux et unitaires, on peut les relever en $P_1, \cdots, P_r \in O_{\mathbb{K}}[X]$ unitaires tels que :

$$P = \prod_{i=1}^{k} P_i$$

en appliquant le corollaire C.2.6. On a vu dans la preuve du théorème 2.3.9 que les P_i étaient encore irréductibles dans $\mathbb{K}[X]$.

Soit $x \in \overline{\mathbb{K}}$ une racine de P. Alors x est racine de l'un des P_i, qui est son polynôme minimal (car c'est un polynôme annulateur irréductible unitaire de x). Ainsi, on obtient que $\mathbb{K}[x]$ est une extension

de degré $\deg(P_i)$ de $\mathbb{K}$. Mais alors $\overline{x}$, la réduite de x modulo $M_{\mathbb{K}[x]}$ est une racine de $\overline{P_i}$, qui est son polynôme minimal sur K. Ainsi, $K[\overline{x}]$ est une extension de degré $\deg(P_i)$ de K, qui est contenue dans le corps résiduel L de $\mathbb{K}[x]$. Ainsi $[L : K] \geq \deg(P_i) = [\mathbb{K}[x] : \mathbb{K}]$. Mais d'après la proposition C.3.4, il y a en fait égalité dans l'inégalité précédente. Ainsi, $\mathbb{K}[x]$ est une extension non ramifiée de $\mathbb{K}$, qui se plonge donc dans $\mathbb{K}^{nr}$, et ainsi x s'identifie à un élément de $\mathbb{K}^{nr}$.

En outre, vu que $P \in O_{\mathbb{K}}[X] \subset O_{\mathbb{K}^{nr}}[X]$ et que $O_{\mathbb{K}^{nr}}$ est intégralement clos dans $\mathbb{K}^{nr}$ d'après la proposition **??**, on a $x \in O_{\mathbb{K}^{nr}}$. D'où le résultat. □

D Compléments de théorie algébrique des nombres.

Cette section est un complément non essentiel à la compréhension générale du ducument. Nous l'avions introduite pour étudier la preuve du théorème de Deuring que nous avons abandonnée. Pour cette raison, les notions abordées ici ne sont pas bien maîtrisées par l'ensemble du groupe. Nous présentons ces notions simplement par souci de compte-rendu de notre travail.

D.1 Idéaux fractionnaires.

Définition D.1.1. *Un* idéal fractionnaire *de $\mathbb{A}$ est une partie de $\mathbb{K}$ de la forme $d^{-1}J$ où $d \in \mathbb{A}\backslash\{0\}$ et J un idéal de $\mathbb{A}$. Autrement dit, m est un idéal fractionnaire si et seulement si il existe $d \in \mathbb{A}\backslash\{0\}$ tel que $dm \subset \mathbb{A}$. (Car un $\mathbb{A}$-module inclu dans $\mathbb{A}$ est un idéal de $\mathbb{A}$.)*

*m est dit **principal** si J est principal. m est dit de type fini si J est de type fini (engendré par un nombre fini d'éléments).*

Sur les idéaux fractionnaires, il est possible de définir un "quotient" : $(a : b)$ est l'idéal $\{x \in \mathbb{K}/xb \subset a\}$. Le quotient de deux idéaux fractionnaires est un idéal fractionnaire. Quand a est inversible, multiplier par a^{-1} revient à diviser par a.

Proposition D.1.2. *Un idéal fractionnaire d'un anneau noetherien $\mathbb{A}$ est un sous-A-module de K de type fini et réciproquement.*

Démonstration. En effet, si a est un sous-$\mathbb{A}$-module de type fini de $\mathbb{K}$, on se donne $G = (g_i)_{0\leq i\leq n-1}$ une famille génératrice de a, d un dénominateur commun à G et J l'idéal engendré par dG. Réciproquement, J est un idéal donc a est un sous-$\mathbb{A}$-module. Comme $\mathbb{A}$ est noetherien, on se donne G une famille génératrice finie de J et $d^{-1}G$ est une famille génératrice de a donc a est de type fini. □

Proposition D.1.3. *Tout sous-$\mathbb{A}$-module inversible est un idéal fractionnaire.*

Démonstration. En effet, si M et N sont des sous-$\mathbb{A}$-modules de $\mathbb{K}$ tels que $N \cdot M = \mathbb{A}$, alors il existe un élément $d \in N$ qui est aussi un élément de $A\backslash\{0\}$ (du simple fait que N est un sous-$\mathbb{A}$-module de $\mathbb{K}$) et bien sûr $dM \subset \mathbb{A}$. □

Nous venons donc de montrer la :

Proposition D.1.4. *L'ensemble des idéaux fractionnaires inversibles forme un groupe abélien.*

Proposition D.1.5. *Un idéal fractionnaire inversible est de type fini.*

D.2 Anneaux de Dedekind.

Définition D.2.1. *Soit $\mathbb{A}$ un anneau intègre et $\mathbb{K}$ son corps de fractions. Soit S une partie de $\mathbb{A}$ stable par produit contenant 1 et ne contenant pas 0. L'ensemble :*

$$\{x \in \mathbb{K}/\exists y, s \in \mathbb{A} \times S, x = \frac{y}{s}\}$$

est un anneau noté $S^{-1}\mathbb{A}$ et l'application $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathbb{A}$ est une bijection de l'ensemble des idéaux premiers de $S^{-1}\mathbb{A}$ vers l'ensemble des idéaux premiers de $\mathbb{A}$ ne rencontrant pas S.

Lorsque $S = \mathbb{A}\backslash\mathfrak{p}$ où $\mathfrak{p}$ est un idéal premier de $\mathbb{A}$, $S^{-1}\mathbb{A}$ se note $A_\mathfrak{p}$. C'est un anneau local d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$ et de cors résiduel le corps des fractions de $\mathbb{A}/\mathfrak{p}$; les idéaux premiers de $\mathbb{A}_\mathfrak{p}$ correspondant aux idéaux premiers de $\mathbb{A}$ contenus dans $\mathfrak{p}$. $\mathbb{A}_\mathfrak{p}$ est le localisé de $\mathbb{A}$ en $\mathfrak{p}$.

Proposition D.2.2. *Si $\mathbb{A}$ est un anneau intègre noetherien, les deux propriétés suivantes sont équivalentes :*

(i). *Pour tout idéal premier non nul $\mathfrak{p}$, $\mathbb{A}_\mathfrak{p}$ est un anneau de valuation discrète.*

(ii). *$\mathbb{A}$ est intégralement clos et tout idéal premier non nul de $\mathbb{A}$ est maximal.*

Démonstration. Supposons d'abord que la propriété (i). est vérifiée. Soient alors $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers tels que $\mathfrak{p} \subset \mathfrak{p}'$. Supposons de plus $\mathcal{P}'$ non nul. Alors l'idéal premier $\mathcal{P}\mathbb{A}_{\mathcal{P}'} \subset \mathfrak{p}'\mathbb{A}_{\mathfrak{p}'} \subset \mathbb{A}_{\mathfrak{p}'}$. Comme $\mathbb{A}_{\mathfrak{p}'}$ est un avd d'après (i)., il possède un unique idéal premier non nul donc $\mathfrak{p}\mathbb{A}_{\mathfrak{p}'} = \{0\}$ ou $\mathfrak{p}\mathbb{A}_{\mathfrak{p}'} = \mathfrak{p}'\mathbb{A}_{\mathfrak{p}'}$, d'où $\mathfrak{p} = \{0\}$ ou $\mathfrak{p} = \mathfrak{p}'$. Tout idéal premier non nul de $\mathbb{A}$ est maximal.

Par ailleurs, si $a \in \mathbb{K}$ est entier sur $\mathbb{A}$, on se donne $\mathfrak{p}$ un idéal premier non nul. $\mathbb{A}_\mathfrak{p}$ contient $\mathbb{A}$ donc a est entier sur $\mathbb{A}_\mathfrak{p}$ et constitue un élément de son corps de fractions. De plus, d'après (i)., $\mathbb{A}_\mathfrak{p}$ est intégralement clos donc $a \in \mathbb{A}_\mathfrak{p}$. Soit $(b, c) \in \mathbb{A}^2$ tel que $a = \frac{b}{c}$. Par définition, il existe $s \in \mathbb{A}\backslash\mathfrak{p}$ et $y \in \mathbb{A}$ tels que $bs = yc$. Alors l'idéal :

$$\mathcal{I} = \{x \in \mathbb{A} / bx \in c\mathbb{A}\}$$

contient $s \notin \mathcal{P}$ donc $\mathcal{I} \not\subset \mathfrak{p}$. Cela étant valable pour tout $\mathfrak{p}$, on déduit $\mathcal{I} = \mathbb{A}$. En particulier $b \in c\mathbb{A}$ donc $a = \frac{b}{c} \in \mathbb{A}$. $\mathbb{A}$ est donc intégralement clos.

Réciproquement, supposons (ii). et munissons-nous d'un idéal premier non nul $\mathfrak{p}$. Comme $\mathbb{A}_\mathfrak{p}$ est local, il suffit de démontrer qu'il est intégralement clos d'après le théorème **??**. Soit x un élement du corps des fractions de $\mathbb{A}_\mathfrak{p}$ entier sur $\mathbb{A}_\mathfrak{p}$. Et $(a_k)_{0\leq k\leq n} \in \mathbb{A}_\mathfrak{p}^{n+1}$ tel que $\sum_{k=0}^{n} a_k X^k = 0$. En multipliant par s^n où $s \in \mathbb{A}$ est un dénominateur commun aux a_k, on a $(sx)^n + \sum_{k=0}^{n-1} b_k (sX)^k = 0$ où les b_k sont des éléments de $\mathbb{A}$. $sx \in \mathbb{K}$ et sx est entier sur $\mathbb{A}$ donc, d'après (ii)., $sx \in \mathbb{A}$ puis $x \in \mathbb{A}_\mathfrak{p}$. Les $\mathbb{A}_\mathfrak{p}$ sont bien intégralement clos, ce qui termine la démonstration. □

Définition D.2.3. *Un anneau intègre et noetherien qui vérifie ces deux propriétés équivalentes est un* ***anneau de Dedekind****.*

Théorème D.2.4. *Soit $\mathbb{A}$ un anneau commutatif intègre et unitaire. Les propriétés suivantes sont équivalentes :*

(1). $\mathbb{A}$ est un anneau de Dedekind
(2). Tout idéal premier non nul de $\mathbb{A}$ est inversible.
(3). Tout idéal non nul de $\mathbb{A}$ est inversible.
(4). Tout idéal non nul de $\mathbb{A}$ est produit d'éléments maximaux.
(5). Tout idéal non nul de $\mathbb{A}$ est produit d'éléments premiers.

De plus, la décomposition en produits d'idéaux premiers est alors unique.

Démonstration. Dans toute cette démonstration, $\mathbb{A}$ est un anneau commutatif intègre et unitaire.

Soit $\mathbb{A}$ un anneau de Dedekind et $\mathcal{I}$ un idéal premier non nul de $\mathbb{A}$. On pose $S = \mathbb{A}\backslash\mathcal{I}$. $\mathbb{A}_\mathcal{I}$ est un anneau de valuation discrète donc il est principal. Il existe $p \in \mathbb{A}_\mathcal{I}$ qui engendre l'idéal $\mathcal{I}\mathbb{A}_\mathcal{I}$. Ainsi $\mathcal{I}\mathbb{A}_\mathcal{I} = p\mathbb{A}_\mathcal{I}$ donc $\mathcal{I} \subset p\mathbb{A}_\mathcal{I}$. Comme $\mathbb{A}$ est de Dedekind, $\mathbb{A}$ est noetherien et on peut se donner une famille génératrice $(g_i)_{1\leq i\leq n}$ de $\mathcal{I}$. $\forall i, g_i \in p\mathbb{A}_\mathcal{I}$ donc il existe $s_i, y_i \in S \times \mathbb{A} g_i = p s_i^{-1} y_i$. Soit $a = \prod_{i=1}^{n} s_i \in S$. Alors $\forall i, \frac{a}{p} g_i \in \mathbb{A}$ donc $\frac{a}{p}\mathcal{I} \subset \mathbb{A}$. On montre alors que $\mathcal{I}$ est inversible, d'inverse $Q = \mathbb{A} + \frac{a}{p}\mathbb{A}$: par construction, $Q \cdot \mathcal{I}$ est un idéal de $\mathbb{A}$ qui contient $\mathcal{I}$ ainsi que $a \notin \mathcal{I}$. Comme $\mathcal{I}$ est un idéal premier non nul, on en déduit que $Q \cdot \mathcal{I} = \mathbb{A}$, ce qui prouve que $\mathcal{I}$ est inversible.

Soit $\mathbb{A}$ un anneau dont tout idéal premier non nul est inversible. Raisonnons par l'absurde et supposons qu'il existe un idéal $\mathcal{I}$ non nul non inversible. Montrons alors qu'une réunion totalement ordonnée d'idéaux non nuls non inversibles est encore un idéal non nul non inversible : Soit $(\mathcal{J}_i)_I$ un ensemble totalement ordonné d'idéaux non nuls non inversible et $\mathcal{J}$ leur réunion. Si $\mathcal{J}$ n'est pas de type fini, il n'est pas inversible. S'il est de type fini, il existe $(j_i)_{1\leq i\leq n}$ n éléments de $\mathbb{A}$ qui l'engendrent. Or chaque j_i est inclus dans un certain J_{n_i} donc $\mathcal{J} = \bigcup_{i=1}^{n} J_{n_i}$. Comme la famille est totalement ordonnée, il s'agit de l'un des J_{n_i} donc $\mathcal{J}$ n'est pas inversible. Cela montre que l'ensemble des éléments non inversibles est inductif. D'après le lemme de Zorn, il existe $\mathfrak{p}$ un idéal non nul non inversible maximal au sens de l'inclusion. Montrons que cet idéal est premier. Soit $a \in \mathbb{A}\backslash\mathfrak{p}$ et $b \in \mathfrak{p}$ tel que $ab \in \mathfrak{p}$. L'idéal $Q = \mathfrak{p} + a\mathbb{A}$ contient strictement $\mathfrak{p}$ donc est inversible par maximalité de $\mathfrak{p}$. Comme $\mathfrak{p}$ n'est pas inversible, $\mathfrak{p} \cdot Q^{-1}$ n'est pas inversible. Mais comme $Q \subset \mathbb{A}$, $1 \in Q^{-1} = \{x \in \mathbb{K} / xQ \subset \mathbb{A}\}$ donc $\mathfrak{p} \subset \mathfrak{p} \cdot Q^{-1}$ puis $\mathfrak{p} = \mathfrak{p} \cdot Q^{-1}$ par maximalité. Or $ab \in \mathfrak{p}$ donc $\mathfrak{p}$ contient bQ donc $b \in \mathfrak{p} \cdot Q^{-1} = \mathfrak{p}$. Cela montre que $\mathfrak{p}$ est premier et aboutit à une contradiction.

Supposons maintenant que tout idéal non nul de $\mathbb{A}$ est inversible. Tout idéal inversible étant de type fini, $\mathbb{A}$ est donc noetherien. Soit $\mathcal{I}$ un idéal non nul de $\mathbb{A}$. Si $\mathcal{I} \neq \mathbb{A}$, il existe un idéal maximal M_1 de $\mathbb{A}$ qui le contient. $\mathcal{I} \subset M_1 \subset \mathbb{A}$ donc $\mathcal{I} \cdot M_1^{-1}$ est un idéal de $\mathbb{A}$ qui contient $\mathcal{I}$. On peut donc construire une suite croissante d'idéaux $\mathcal{I} \subset \mathcal{I} \cdot M_1^{-1} \subset \cdots \subset \mathcal{I} \cdot M_1^{-1} \cdots M_n^{-1}$. Comme $\mathbb{A}$ est noetherien, cette suite est stationnaire et il existe $M_1, \cdots, M_n$ des idéaux maximaux tels que $\mathcal{I} = M_1 \cdots M_n$.

Les idéaux de la décomposition précédentes étant maximaux, ils sont aussi premiers. On déduit de plus l'unicité de cette décomposition par une itération immédiate.

Supposons maintenant que tout idéal non nul se décompose de manière unique en un produit d'idéaux premiers. Montrons qu'alors tout idéal premier non nul est maximal, ce qui fixera l'équivalence (4) ⇔ (5). Soit $\mathfrak{p}$ un idéal premier non nul et $\mathcal{I}$ un idéal maximal qui le contient. $\mathcal{I}$ se décompose en un produit

d'idéaux premiers et comme $\mathfrak{p}$ est premier, il apparaît dans cette décomposition. Mais $\mathcal{I}$ lui-même premier donc, par unicité de la décomposition, $\mathcal{I} = \mathfrak{p}$ ce qui montre que $\mathfrak{p}$ est maximal.

On va ensuite montrer que si tout idéal non nul se décompose de manière unique en produits d'idéaux maximaux, alors tout idéal premier non nul est inversible. Pour cela, il suffit de montrer que tout idéal maximal est inversible. Soit $\mathcal{M}$ un idéal maximal et $a \in \mathcal{M}\backslash\{0\}$. On se donne $M_1 \cdots M_n$ la décomposition de $a\mathbb{A}$ en idéaux maximaux. Comme $a\mathbb{A}$ est inversible, tous les M_i le sont. Mais $\mathcal{M}$ est un idéal qui contient a donc $a\mathbb{A} = M_1 \cdots M_n$. $\mathcal{M}$ étant maximal, il est en particulier premier donc $\mathbb{A}\backslash\mathcal{M}$ est stable par produit. Si on suppose que pour tout i, il existe $m_i \in M_i$ tel que $m_i \notin \mathcal{M}$, alors $m_1 \cdots m_n \notin \mathcal{M}$, ce qui contredit la propriété précédente. On en déduit que $\mathcal{M}$ contient l'un des M_i puis, par maximalité, $\mathcal{M}$ est égal à l'un des M_i. Ainsi $\mathcal{M}$ est bien inversible.

Pour terminer la démonstration, il ne nous reste plus qu'à montrer (2) $\implies$ (1). Supposons alors que tout idéal premier non nul est inversible. Comme on l'a vu précédemment, un résultat d'algèbre nous garantit que $\mathbb{A}$ est alors noetherien. De plus, on a aussi montré deux paragraphes plus haut que tout idéal premier non nul est alors maximal. Nous disposons par ailleurs des propriétés équivalentes (2), (3), (4) et (5). Il ne reste plus qu'à montrer que $\mathbb{A}$ est intégralement clos. Soit $\mathfrak{p}$ un idéal premier non nul. Tout idéal de $\mathbb{A}$ se décomposant de manière unique en un produit d'idéaux premiers, on peut associer à un idéal I de $\mathbb{A}$ la valuation p-adique $v_\mathfrak{p}(I)$ et étendre cette valuation sur l'ensemble des idéaux fractionnaires de $\mathbb{A}$. On peut ensuite construire une valuation sur $\mathbb{K}$ que nous appelerons encore $v_\mathfrak{p}$ par abus de notation : $\forall x \in \mathbb{K}, v_\mathfrak{p}(x) = v_\mathfrak{p}(x\mathbb{A})$. Il n'est pas difficile de montrer qu'il s'agit bien d'une valuation. L'anneau $\mathbb{A}$ correspond alors à l'intersection des anneaux de valuation correspondants. Il est donc intégralement clos comme intersection d'anneaux intégralement fermés sur $\mathbb{K}$. □

Proposition D.2.5. *Dans un anneau de Dedekind, tout idéal fractionnaire non nul est inversible. Les idéaux fractionnaires non nuls d'un anneau de Dedekind forment donc un groupe multiplicatif. Il s'appel le* ***groupe des idéaux*** *de l'anneau.*

Démonstration. En effet, si a est un idéal fractionnaire non nul, il existe $d \in \mathbb{A}$ et J un idéal de $\mathbb{A}$ tel que $a = d^-1J$. J est non nul donc inversible donc a est inversible. □

Proposition D.2.6. *Soit $\mathbb{A}$ un anneau de Dedekind. Pour tout élément non nul $x \in \mathbb{A}$, il n'y a qu'un nombre fini d'idéaux premiers contenant x.*

Démonstration. Soit $(p_i)_\mathbb{N}$ des idéaux premiers de $\mathbb{A}$ contenant x. On peut alors construire une suite décroissante d'idéaux contenant x : pour $n \in \mathbb{N}$, $a_n = \bigcap_{i=0}^{n} p_i$ avec pour convention $a_0 = \mathbb{A}$. Comme tous ces idéaux contiennent x, ils sont non nuls donc inversibles. Par passage à l'inverse, on peut construire une suite croissante d'idéaux fractionnaires $(a_n^{-1})_{n\in\mathbb{N}}$ tous inclus dans le sous-$\mathbb{A}$-module de type fini $x^{-1}\mathbb{A}$. Cette suite est donc stationnaire (il existe un rang à partir duquel tous les générateurs du $\mathbb{A}$-module de type fini sont inclus dans la réunion). En repassant à l'inverse, on obtient qu'il existe $r \in \mathbb{N}$ tel que, $\forall k \geq r$, $\bigcap_{i=0}^{k} p_i = \bigcap_{i=0}^{r} p_i$. Une récurrence immédiate montre que : $\forall k > r$, $p_1 \cdots p_r \subset \bigcap_{i=0}^{r} p_i \subset p_k$. Comme les p_k sont premiers, on en déduit que, pour tout k, p_k est l'un des $p_1 \cdots p_r$. Ainsi x n'est contenu que dans un nombre fini d'idéaux premiers. □

Proposition D.2.7. *Tout idéal fractionnaire d'un anneau de Dedekind s'écrit de manière unique sous la forme :*

$$a = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a)}$$

où les $v_\mathfrak{p}(a)$ sont des entiers relatifs presque tous nuls. Par ailleurs, on a les formules suivantes :

(i). $v_\mathfrak{p}(a \cdot b) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b)$

(ii). $v_\mathfrak{p}(b : a) = v_\mathfrak{p}(b) - v_\mathfrak{p}(a)$

(iii). $v_\mathfrak{p}(a + b) = inf(v_\mathfrak{p}(a), v_\mathfrak{p}(b))$

Lemme D.2.8 (Lemme d'approximation)**.** *Soit $\mathbb{A}$ un anneau de Dedekind, $k \in \mathbb{N}$, $(\mathfrak{p}_i)_{1\leq i\leq n}$ des idéaux premiers deux-à-deux distincts de $\mathbb{A}$, $(x_i)_{1\leq i\leq n}$ des éléments de $\mathbb{K}$ et $(n_i)_{1\leq i\leq n}$ des entiers. Alors il existe $x \in \mathbb{K}$ tel que : $\forall i, v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ et $v_\mathfrak{q} \geq 0$ pour tout idéal premier $\mathfrak{q}$ disctincts des $\mathfrak{p}_i$.*

Démonstration. Cela découle directement du théorème du même nom sur les valeurs absolues non équivalentes d'un corps $\mathbb{K}$. En effet, pour $i \in \{1, \cdots, n\}$, on fixe $p_i \in \mathfrak{p}_i\backslash\{0\}$ et on définit la valeur absolue p_i-adique comme suit : $\forall x \in \mathbb{K}, |x|_{p_i} = p_i^{-v_{\mathfrak{p}_i}(x)}$ avec pour convention $|0|_{p_i} = 0$ pour tout i. On pose $b_i = \frac{\prod_{k\neq i} p_k}{p_i}$ et il n'est pas difficile de voir que $|b_i|_{p_i} > 1$ avec $|b_i|_{p_j} < 1$ pour tout $j \neq i$. On en déduit

$\frac{b_i^m}{1+b_i^m} \xrightarrow[m\to+\infty]{|.|_{p_i}} 1$ et $\frac{b_i^m}{1+b_i^m} \xrightarrow[m\to+\infty]{|.|_{p_j}} 0$ pour $j \neq i$. Il suffit donc de choisir $x_0 = \sum_{i=1}^{n} \frac{b_i^m}{1+b_i^m} x_i$ avec m assez grand. Alors $|x_0 - x_i|_{p_i}$ peut être rendue arbitrairement petit, ce qui assure $v_{p_i}(x_0 - x_i) \geq n_i$. Enfin, il existe un nombre fini d'idéaux premiers $\mathfrak{q}$ distincts des $\mathfrak{p}_i$ pour lesquels $v_\mathfrak{q}(x) \neq 0$. Quitte à remplacer x_0 par $x = x_0 \prod_\mathfrak{q} q_\mathfrak{q}^{v_\mathfrak{q}(x)}$ où les $q_\mathfrak{q}$ sont des éléments arbitraires non nuls des idéaux premiers non nuls $\mathfrak{q}$, on a également $v_\mathfrak{q}(x) \geq 0$ pour tout idéal premier $\mathfrak{q}$ disctint des $\mathfrak{p}_i$, ce qui termine la démonstration. □

D.3 Extension d'anneaux de Dedekind.

Dans cette sous-section, on se donne $\mathbb{A}$ un anneau intègre, noethérien et intégralement clos dont on note $\mathbb{K}$ le corps des fractions, $\mathbb{L}$ une extension finie de $\mathbb{K}$ de degré n et $\mathbb{B}$ l'ensemble des éléments de $\mathbb{L}$ *entiers sur* $\mathbb{A}$, c'est à dire admettant un polynôme annunaleur unitaire dans $\mathbb{A}[X]$. $\mathbb{B}$ est appellée *clôture intégrale de* $\mathbb{A}$. On suppose en outre que $\mathbb{K}$ est un corps parfait, ce qui nous assure que l'extension $\mathbb{L}/\mathbb{K}$ est séparable (d'après le théorème 4.5.3 de [6]).

Proposition D.3.1. *$\mathbb{B}$ est un sous-anneau de $\mathbb{L}$ et $\mathbb{L}$ est son corps de fractions.*

Démonstration. Dans cette preuve, nous utilisons abondamment les résultants (on renvoit le lecteur à la proposition C.2.4 et à la définition C.2.3). $\mathbb{B}$ contient trivialement $0, -1$ et 1 (dont $X, X+1$ et $X-1$ sont des polynômes annulateurs unitaires dans $\mathbb{A}[X]$). Soient $x, y \in \mathbb{A}$. Considérions $P, Q \in \mathbb{A}[X]$ des polynômes annulateurs unitaires respectifs de x et y, de degrés respectifs m et n. Considérons les polynômes en l'indéterminée Y :

$$R(Y) := \mathrm{Res}_{m,n}(P(X), Q(Y-X)) \quad \text{et} \quad S(Y) := \mathrm{Res}_{m,n}\left(P(X), X^n Q\left(\frac{Y}{X}\right)\right)$$

On voit en développant les déterminants de Sylvester que R et S sont unitaires. En outre, comme x est une recine commune de $P(X)$, $Q(x+y-X)$ et $X^n Q\left(\frac{xy}{X}\right)$, la proposition C.2.4 assure que $R(x+y) = S(xy) = 0$. Mais R et S sont des polynômes non nuls de $\mathbb{A}[X]$ donc $xy \in \mathbb{B}$ et $x + y \in \mathbb{B}$. Donc $\mathbb{B}$ est un sous-anneau de $\mathbb{L}$.

Soit $x \in \mathbb{L}$. Comme $\mathbb{L}/\mathbb{K}$ est finie, $\mathbb{L}/\mathbb{K}$ est algébrique donc si $x \in \mathbb{L}$, alors on peut définir son polynôme minimal sur $\mathbb{K}$:

$$\Pi_x := X^d + \sum_{i=0}^{d-1} a_i X^i \in \mathbb{K}[X]$$

Ecrivons alors pour tout $i \in \{0, \cdots, d-1\}$, $a_i := \frac{\alpha_i}{\beta_i}$ avec $(\alpha_i, \beta_i) \in \mathbb{A} \times \mathbb{A}^*$. Alors en multipliant l'équation $\Pi_x(x) = 0$ par $\left(\prod_{j=0}^{d-1} \beta_j\right)^d$, on obtient que $x \prod_{j=0}^{d-1} \beta_j$ est racine de :

$$P := X^d + \sum_{i=0}^{d-1} \alpha_i \left(\prod_{0 \leq j \neq i \leq d-1} \beta_j\right) \left(\prod_{j=0}^{d-1} \beta_j\right)^{d-i-1} X^i$$

Or, P est un polynôme unitaire à coefficients dans $\mathbb{A}$. Donc $x \prod_{j=0}^{d-1} \beta_j \in \mathbb{B}$. Donc $x = \frac{b}{a}$ avec $b \in \mathbb{B}$ et $a \in \mathbb{A}$. Nous venons donc de montrer que $\mathbb{L}$ est le corps de fractions de $\mathbb{B}$ (et même que l'on peut prendre des dénominateurs dans $\mathbb{A}$).

□

Proposition D.3.2. *$\mathbb{B}$ est un sous-module de type fini (sur $\mathbb{A}$) de $\mathbb{L}$.*

Démonstration. Nous renvoyons le lecteur au début de la section 2.3.1 pour les précisions nécessaires sur la fonction trace $T_{\mathbb{L}/\mathbb{K}}$.

Comme $\mathbb{L}/\mathbb{K}$ est finie et que $\mathbb{K}$ est parfait, le théorème de l'élément primitif (théorème 4. 6. 2. de [6]) assure l'existence de $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$. Mais alors $(1, \alpha, \cdots, \alpha^{n-1})$ est une $\mathbb{K}$-base de $\mathbb{L}$. En outre, on a vu précédemment que $\alpha = \frac{\beta}{a}$ avec $a \in \mathbb{A} \setminus \{0\}$ et $\beta \in \mathbb{B}$. Ainsi, $\mathcal{B} := (1, \beta, \cdots, \beta^{n-1})$ est une $\mathbb{K}$-base de $\mathbb{L}$ constituée d'éléments de $\mathbb{B}$. On considère alors M le sous-module de $\mathbb{L}$ (sur $\mathbb{A}$) engendré par $\mathcal{B}$. On sait qu'alors $M \subset \mathbb{B}$.

Par ailleurs, si $x \in \mathbb{B}$ et $y \in M$ alors $xy \in \mathbb{B}$, donc on dispose de $P \in \mathbb{A}[X]$ unitaire annulant xy. Donc le polynôme minimal de xy sur $\mathbb{K}$ divise P, et ainsi tous les $\mathbb{K}$-conjugués de xy dans $\overline{\mathbb{K}}$ sont annulés par P. Or, la proposition précédente reste vraie lorsque l'on remplace $\mathbb{L}$ par $\overline{\mathbb{K}}$ (qui est une extension algébrique de $\mathbb{K}$), ce qui assure que la somme des $\mathbb{K}$-conjugués de xy est toujours entière sur $\mathbb{A}$. Ainsi, d'après la proposition C.2.4 et les relations coefficients racines, $T_{\mathbb{L}/\mathbb{K}}(xy)$ est entier sur $\mathbb{A}$. Mais $T_{\mathbb{L}/\mathbb{K}}(xy) \in \mathbb{K}$ (car c'est la trace d'un endomorphisme $\mathbb{K}$-linéaire) et $\mathbb{A}$ est intégralement clos donc $T_{\mathbb{L}/\mathbb{K}}(xy) \in \mathbb{A}$. On définit donc une application linéaire :

$$x \in \mathbb{B} \longmapsto u_x \in \mathrm{Hom}_\mathbb{A}(M, \mathbb{A})$$

en posant :

$$\forall (x,y) \in \mathbb{B} \times M, \quad u_x(y) = T_{\mathbb{L}/\mathbb{K}}(xy)$$

Cette application est de plus injective car si $x \in \mathbb{B}$ vérifie $u_x = 0$ alors :

$$\forall i \in \{1, \cdots, n\}, \quad T_{\mathbb{L}/\mathbb{K}}(xe_i) = 0$$

Comme $\mathcal{B}$ est une $\mathbb{K}$-base de $\mathbb{L}$, on dispose de $x_0, \cdots, x_{n-1} \in \mathbb{K}$ tels que $x = \sum_{j=0}^{n-1} x_j \beta^j$. Donc en notant pour tout $j \in \{0, \cdots, n-1\}$, $T_j := (T_{\mathbb{L}/\mathbb{K}}(\beta^{i+j}))_{0 \leq i \leq n-1}$, on obtient que :

$$\sum_{j=0}^{n-1} x_j T_j = 0$$

Or, d'après le lemme suivant, $(T_j)_{1 \leq j \leq n}$ est libre donc $x_1 = \cdots = x_n = 0$, et $x = 0$.

Lemme D.3.3. *La matrice $(T_{\mathbb{L}/\mathbb{K}}(\beta^{i+j}))_{0 \leq i,j \leq n-1}$ est inversible.*

Démonstration. Comme $\mathcal{B} = (1, \beta, \cdots, \beta^{n-1})$ est une $\mathbb{K}$-base de $\mathbb{L}$, le polynôme minimal sur $\mathbb{K}$ de β est de degré n. C'est aussi le polynôme minimal de l'endomorphisme $x \in \mathbb{L} \longmapsto \beta x$. Comme il est unitaire et de degré n, c'est en fait le polynôme caractériqtique de cet endomorphisme. Or, le polynôme minimal de β est irréductible donc scindé à racines simples dans $\overline{\mathbb{K}}$. Ainsi, les valeurs propres $\lambda_0, \cdots, \lambda_{n-1} \in \overline{\mathbb{K}}$ de la matrice de $x \in \mathbb{L} \longmapsto \beta x$ dans $\mathcal{B}$ sont distinctes deux à deux. En outre, l'invariance de la trace d'une matrice par extension de corps assure que :

$$\forall i,j \in \{0, \cdots, n-1\}, \quad T_{\mathbb{L}/\mathbb{K}}(\beta^{i+j}) = \sum_{k=0}^{n-1} \lambda_k^{i+j}$$

Donc en notant $\Lambda := (\lambda_k^i)_{0 \leq i,k \leq n-1}$, on obtient que :

$$(T_{\mathbb{L}/\mathbb{K}}(\beta^{i+j}))_{0 \leq i,j \leq n-1} = \Lambda \, {}^t\Lambda$$

De sorte que (les λ_i étant deux à deux distincts) :

$$\det(T_{\mathbb{L}/\mathbb{K}}(\beta^{i+j}))_{0 \leq i \neq j \leq n-1} = (\det \Lambda)^2 = \prod_{0 \leq i,j \leq n-1} (\lambda_i - \lambda_j)^2 \neq 0$$

□

Donc $\mathbb{B}$ se plonge dans $\mathrm{Hom}_{\mathbb{A}}(M, \mathbb{A})$ qui est un $\mathbb{A}$-module libre de type fini engendrée par la base duale de $\mathcal{B}$, $\mathcal{B}^* := (e_1^*, \cdots, e_n^*)$, donnée par :

$$\forall 1 \leq i,j \leq n, \quad e_i^*(e_j) = \delta_{i,j}$$

donc on peut identifier $\mathbb{B}$ à un sous-module (sur $\mathbb{A}$) de $\mathrm{Hom}_{\mathbb{A}}(M, \mathbb{A})$ et ainsi, $\mathbb{B}$ est de type fini d'après la proposition B.2.10. □

Proposition D.3.4. *$\mathbb{B}$ est un sous-anneau noethérien et intégralement clos de $\mathbb{L}$. En outre, si $\mathbb{A}$ est de Dedekind, alors $\mathbb{B}$ aussi.*

Démonstration. Si I est un idéal de $\mathbb{B}$ alors I est un sous-module de $\mathbb{B}$, qui est de type fini comme $\mathbb{A}$-module donc comme $\mathbb{A}$ est noethérien la proposition B.2.10 assure que I est de type fini. Ainsi, $\mathbb{B}$ est noethérien.

Soit $x \in \mathbb{L}$ admettant un polynôme annulateur unitaire dans $\mathbb{B}[X]$. Si $x = 0$ alors $x \in \mathbb{B}$. Sinon, on considère $P := X^d + \sum_{i=0}^{d-1} b_i X^i \in \mathbb{B}[X]$ annulant $\mathbb{A}$. Considérons la $\mathbb{A}$-algèbre $C := \mathbb{A}[b_0, \cdots, b_{d-1}]$, qui est de type-fini comme $\mathbb{A}$-module (comme sous-module de $\mathbb{B}$, qui est de type fini sur l'anneau neothérien $\mathbb{A}$). $D := C[x]$ est un C-module de type fini (engendré par $(1, x, \cdots, x^{d-1})$) donc un $\mathbb{A}$-module de type fini (engendré par exemple par $(c_i x^j)_{1 \leq i \leq m, 0 \leq j \leq d-1}$, où $(c_i)_{1 \leq i \leq m}$ est une famille $\mathbb{A}$-génératrice de C).

Considérons donc $(d_1, \cdots, d_k)$ une famille $\mathbb{A}$-génératrice de D. Alors pour tout $i \in \{1, \cdots, k\}$, $d_i x \in D$ peut s'écrire sous la forme :

$$d_i x = \sum_{j=1}^{k} a_{i,j} d_j$$

avec $(a_{i,j})_{1 \leq i,j \leq k} \in M_k(\mathbb{A})$. Ainsi :

$$(a_{i,j} - \delta_{i,j} x)_{1 \leq i,j \leq k} (d_i)_{1 \leq i \leq k} = 0$$

Donc en multipliant cette égalité par la comatrice de $(a_{i,j} - \delta_{i,j}x)_{1\leq i,j\leq k}$, on obtient que :

$$\forall i \in \{1, \cdots, k\}, \quad \det(\delta_{l,j}x - a_{l,j})_{1\leq l,j\leq k} d_i = 0$$

Donc par intégrité de $\mathbb{A}$, $\det(\delta_{l,j}x - a_{l,j})_{1\leq l,j\leq k} = 0$ ou $d_i = 0$ pour tout $i \in \{1, \cdots, k\}$ i.e. $D = \{0\}$. Or, ce dernier cas est exclus puisque $x \neq 0$ et que $x \in D$. Ainsi, $\det(\delta_{l,j}x - a_{l,j})_{1\leq l,j\leq k} = 0$. $\det(\delta_{l,j}X - a_{l,j})_{1\leq l,j\leq k}$ est alors un polynôme unitaire à coefficients dans $\mathbb{A}$ annulant x. Ainsi, $x \in \mathbb{B}$. Ceci prouve que $\mathbb{B}$ est intégralement clos.

Supposons maintenant que $\mathbb{A}$ est de Dedekind. Soient $\mathfrak{P} \subset \mathfrak{Q}$ des idéaux premiers de $\mathbb{B}$. Alors $\mathfrak{P}' := \mathfrak{P} \cap \mathbb{A}$ et $\mathfrak{Q}' := \mathfrak{Q} \cap \mathbb{A}$ sont des idéaux premiers de $\mathbb{A}$, et donc $\mathfrak{P}' = 0$ (et donc $\mathfrak{P} = 0$) ou $\mathfrak{P}' = \mathfrak{Q}'$. Supposons que $\mathfrak{P}' = \mathfrak{Q}'$. Plaçons nous dans $A := \mathbb{A}/\mathfrak{P}'$ et $B := \mathbb{B}/\mathfrak{P}$, qui restent intègre car $\mathfrak{P}$ est premier. Alors si par l'absurde $\mathfrak{P} \neq \mathfrak{Q}$, on dispose de $x \in \mathfrak{Q}/\mathfrak{P}$ non nul modulo $\mathfrak{P}$. Mais alors $x \in B$, donc x est entier sur A. Considérons le polynôme unitaire annulateur de x : $P := X^d + \sum_{i=0}^{d-1} a_i X^i \in A[X]$, de degré minimal. Alors $a_0 \neq 0$ (sinon on disposerait d'un polynôme unitaire annulant x de degré $d-1$). En outre, $P(x) = 0$ donc a_0 est dans l'idéal de B engendré par x, qui est inclus dans $\mathfrak{Q}/\mathfrak{P}$. On a alors $x \in \mathfrak{Q}/\mathfrak{P} \cap A = \mathfrak{Q}'/\mathfrak{P}' = \mathfrak{P}'/\mathfrak{P}' = \{0\}$. Donc $x = 0$. C'est absurde ! Donc $\mathfrak{P} = \mathfrak{Q}$. Ainsi, $\mathfrak{P} = \{0\}$ ou $\mathfrak{P} = \mathfrak{Q}$. D'après la définition D.2.3, ceci montre que $\mathbb{B}$ est de Dedekind. □

On suppose désormais que $\mathbb{A}$ est un anneau de Dedekind, de sorte que $\mathbb{B}$ soit aussi de Dedekind.

Définition D.3.5. *Etant donné un idéal premier $\mathfrak{p}$ de $\mathbb{A}$ et un idéal premier $\mathfrak{B}$ de $\mathbb{B}$ tous deux non nuls, on dit que* $\mathfrak{B}$ divise $\mathfrak{p}$ *et on note* $\mathfrak{B}|\mathfrak{p}$ *lorsque* $\mathfrak{p} = \mathfrak{B} \cap \mathbb{A}$.

Remarque : $\mathfrak{B}|\mathfrak{p}$ si et seulement si $\mathfrak{B}$ contient l'idéal $\mathfrak{p}\mathbb{B}$ de $\mathbb{B}$ engendré par $\mathfrak{p}$. En effet, cette condition est clairement nécessaire. Réciproquement, si $\mathfrak{p}\mathbb{B} \subset \mathfrak{B}$ alors $\mathfrak{p} = \mathfrak{p}\mathbb{B} \cap \mathbb{A} \subset \mathfrak{B} \cap \mathbb{A}$ donc $\mathbb{A}$ étant de Dedekind et $\mathfrak{B} \cap \mathbb{A}$ étant un idéal premier de $\mathbb{A}$, $\mathfrak{p} = \mathfrak{B} \cap \mathbb{A}$.

Si $\mathfrak{p}$ est un idéal premier non-nul de $\mathbb{A}$, alors $\mathfrak{p}\mathbb{B}$ est un idéal non nul de $\mathbb{B}$, qui est de Dedekind, donc $\mathfrak{p}\mathbb{B}$ se décompose en produits d'idéaux premiers non-nuls :

$$\mathfrak{p}\mathbb{B} = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{v_{\mathfrak{B}}(\mathfrak{p}\mathbb{B})}$$

Pour tout idéal premier $\mathfrak{B}|\mathfrak{p}$, on sait qu'en outre $\mathbb{B}/\mathfrak{B}$ est une $\mathbb{A}/\mathfrak{p}$-algèbre et que $\mathbb{A}/\mathfrak{p}$ et $\mathbb{B}/\mathfrak{B}$ sont des corps (car $\mathfrak{p}$ et $\mathfrak{B}$ sont maximaux). En outre, $\mathbb{B}/\mathfrak{B}$ est de dimension finie sur $\mathbb{A}/\mathfrak{p}$ car $\mathbb{B}$ est un $\mathbb{A}$-module de type fini.

Définition D.3.6. *Si $\mathfrak{p}$ est un idéal premier non nul de $\mathbb{A}$ et si $\mathfrak{B}|\mathfrak{p}$ alors on note $e_{\mathfrak{B}/\mathfrak{p}} := v_{\mathfrak{B}}(\mathfrak{p}\mathbb{B})$ et $f_{\mathfrak{B}/\mathfrak{p}} := [\mathbb{B}/\mathfrak{B} : \mathbb{A}/\mathfrak{p}]$, que l'on appelle respectivement* indice de ramification *et* indice d'inertie *de $\mathfrak{B}$ sur $\mathfrak{p}$.*

Remarque : Cela nous ramène à la question de la ramification. Nous voyons bien que ce qui est fait ici est une généralisation du travail de la section 1, un anneau de valuation discrète étant en particulier un anneau de Dedekind. Cependant, cherchant à rester au niveau le plus élémentaire possible dès qu'un pré-requis doit être introduit, nous n'avons pas jugé nécessaire d'aller aussi loin au moment ou nous avons construit $\mathbb{Q}_q$.

Proposition D.3.7. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbb{A}$. Alors $\mathbb{B}/\mathfrak{p}\mathbb{B}$ est une $\mathbb{A}/\mathfrak{p}$ algèbre de dimension $n = [\,:\mathbb{K}]$ isomorphe en tant que $\mathbb{A}/\mathfrak{p}$-algèbre au produit $\prod_{\mathfrak{B}|\mathfrak{p}} \mathbb{B}/\mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$. En outre :*

$$n = \sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}/\mathfrak{p}} f_{\mathfrak{B}/\mathfrak{p}}$$

Démonstration. Considérons $\mathbb{A}_{\mathfrak{p}} = (\mathbb{A} \setminus \mathfrak{p})^{-1}\mathbb{A}$, la localisation de $\mathbb{A}$ à $\mathfrak{p}$ et $B := (\mathbb{A} \setminus \mathfrak{p})^{-1}\mathbb{B}$.

Commençons par montrer que B est la clôture intégrale de $\mathbb{A}_{\mathfrak{p}}$ dans . Si x est entier sur $\mathbb{A}_{\mathfrak{p}}$, alors en multipliant l'équation polynomiale unitaire à coefficients dans $\mathbb{A}_{\mathfrak{p}}$ vérifiée par x par une certaine puissance $a \in \mathbb{A} \setminus \mathfrak{p}$ du dénominateur commun des coefficients, on obtient comme dans la proposition D.3.1 que $ax \in \mathbb{B}$, et donc que $x \in B$. Réciproquement, si $x \in B$ alors $x = \frac{b}{a}$ avec $b \in \mathbb{B}$ et $a \in \mathbb{A} \setminus \mathfrak{p}$. En divisant une équation polynomiale unitaire à coefficients dans $\mathbb{A}$ vérifiée par b par une certaine puissance de a, on obtient que x est entier sur $\mathbb{A}_{\mathfrak{p}}$.

$\mathbb{A}_{\mathfrak{p}}$ est en outre un anneau de valuation discrète, donc en particulier un anneau de Dedekind. Ainsi, la proposition D.3.2 assure que B est un $\mathbb{A}_{\mathfrak{p}}$ module de type fini. Or, on a vu dans la preuve de cette même proposition que B contient un $\mathbb{A}_{\mathfrak{p}}$-module M, libre de type fini et de rang n et que B se plonge dans $M^* := \mathrm{Hom}_{\mathbb{A}_{\mathfrak{p}}}(M, \mathbb{A}_{\mathfrak{p}})$, qui est aussi libre de type fini et de rang n. Comme $\mathbb{A}_{\mathfrak{p}}$ est un anneau de valuation discrète, il est principal et la B.2.8 assure que $\mathbb{M}$ est libre de type fini et de rang n.

En considérant la réduction modulo $\mathfrak{p}$ d'une $\mathbb{A}_\mathfrak{p}$-base de B, il est alors aisé de vérifier que $B/\mathfrak{p}B$ est un $\mathbb{A}_\mathfrak{p}/\mathfrak{p}\mathbb{A}_\mathfrak{p}$-espace vectoriel de dimension n. Or, on vérifie aussi facilement que $\mathbb{A}_\mathfrak{p}/\mathfrak{p}\mathbb{A}_\mathfrak{p} = \mathbb{A}/\mathfrak{p}$ et $B/\mathfrak{p}B = \mathbb{B}/\mathfrak{p}\mathbb{B}$. Ainsi, $\mathbb{B}/\mathfrak{p}\mathbb{B}$ est une $\mathbb{A}/\mathfrak{p}$ algèbre de dimension n.

Comme $\mathfrak{p}\mathbb{B} = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$, on a clairement $\mathfrak{p}\mathbb{B} \subset \bigcap_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$. En outre, $I := \bigcap_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$ est un idéal de $\mathbb{B}$ dont les facteurs premiers sont les $\mathfrak{B}|\mathfrak{p}$ et les valuations supérieures à $e_{\mathfrak{B}/\mathfrak{p}}$ (car $I \subset \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$ pour tout $\mathfrak{B}|\mathfrak{p}$). Ainsi :

$$I = \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{v_\mathfrak{B}(I)} \subset \prod_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}} = \mathfrak{p}\mathbb{B}$$

et donc $\mathfrak{p}\mathbb{B} = I = \bigcap_{\mathfrak{B}|\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$. Il s'ensuit que l'application :

$$\Phi : \mathbb{B}/\mathfrak{p}\mathbb{B} \longrightarrow \prod_{\mathfrak{B}|\mathfrak{p}} \mathbb{B}/\mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$$

qui à $x \mod \mathfrak{p}\mathbb{B}$ associe $(x \mod \mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}})_{\mathfrak{B}|\mathfrak{p}}$ est bien définie et injective. C'est de plus clairement un morphisme de $\mathbb{A}/\mathfrak{p}$-algèbre. Enfin, le lemme d'approximation, prouvé dans le paragraphe précédent assure que Φ est surjective. Donc en tant que $\mathbb{A}/\mathfrak{p}$-algèbre :

$$\mathbb{B}/\mathfrak{p}\mathbb{B} \approx \prod_{\mathfrak{B}|\mathfrak{p}} \mathbb{B}/\mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}}$$

Ce qui donne en passant aux dimensions (d'après ce que nous avons prouvé ci-dessus) :

$$n = [\mathbb{B}/\mathfrak{p}\mathbb{B} : \mathbb{A}/\mathfrak{p}] = \sum_{\mathfrak{B}|\mathfrak{p}} [\mathbb{B}/\mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}} : \mathbb{A}/\mathfrak{p}]$$

Or, pour tout $\mathfrak{B}|\mathfrak{p}$, $\mathbb{B}/\mathfrak{B}$ est une extension de degré $f := f_{\mathfrak{B}/\mathfrak{p}}$ sur $\mathbb{A}/\mathfrak{p}$ et de plus, en considérant une $\mathbb{A}/\mathfrak{p}$-base $(b_1, \cdots, b_n)$ de $\mathbb{B}/\mathfrak{B}$, on obtient que $\left(\prod_{j=1}^{e} b_{i_j}\right)_{1 \leq i_1, \cdots, i_e \leq f}$ est une $\mathbb{A}/\mathfrak{p}$-base de $\mathbb{B}/\mathfrak{B}^e$ (avec $e := e_{\mathfrak{B}/\mathfrak{p}}$), de sorte que $[\mathbb{B}/\mathfrak{B}^{e_{\mathfrak{B}/\mathfrak{p}}} : \mathbb{A}/\mathfrak{p}] = e_{\mathfrak{B}/\mathfrak{p}} f_{\mathfrak{B}/\mathfrak{p}}$, puis que :

$$n = \sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}/\mathfrak{p}} f_{\mathfrak{B}/\mathfrak{p}}$$

□

E Preuves et compléments de la section 3.

E.1 Fonctions rationnelles définies sur E.

Proposition E.1.1. *$\overline{\mathbb{K}}[E]_P$ est un anneau de valuation discrète d'idéal maximal $M(E)_P$.*

Démonstration. Le fait que $\overline{\mathbb{K}}[E]_P$ est un anneau sous-anneau de $\overline{\mathbb{K}}(E)$ et que M_P est un idéal de $\overline{\mathbb{K}}[E]_P$ est trivial. Pour vérifier que c'est un anneau de valuation discrète, il s'agit de montrer l'existence d'une uniformisante engendrant M_P, i.e. d'un élément $r \in M(E)_P$ tel que toute fonction $f \in \overline{\mathbb{K}}[E]_P$ non nulle s'écrive sous la forme $f = r^k u$ avec $k \in \mathbb{N}$ et $u \in \overline{\mathbb{K}}[E]_P$ inversible dans cet anneau, c'est à dire dont P n'est pas un zéro. En effet, si c'est le cas $f \in M_P$ équivaut à $k \geq 1$ et donc $\overline{\mathbb{K}}[E]_P$ est engendré par r. En outre, si I est un idéal de $\overline{\mathbb{K}}[E]_P$, on obtient que $I = r^{k_0}\overline{\mathbb{K}}[E]_P$ en prenant pour k_0 l'exposant k minimal des éléments de I, ce qui justifie la maximalité de $M(E)_P$ et la principalité de $\overline{\mathbb{K}}[E]_P$. Pour obtenir l'existence de l'uniformisante, on distingue trois cas :

Premier cas : Supposons que $P := (x_P, y_P) \neq \mathcal{O}$ et $y_P \neq 0$. Commençons par le cas où $f \in \overline{\mathbb{K}}[E]_P \setminus \{0\}$ est polynomiale. Ecrivons f sous forme réduite $f = p + Yq$ et considérons $(X - x_P)^\alpha$ le plus grand facteur de $X - x_P$ commun à p et q. Considérons $p_0 := \frac{p}{(X-x_P)^\alpha}$ et $q_0 := \frac{q}{(X-x_P)^\alpha}$. Alors x_P est zéro d'au plus un seul de ces deux éléments. Posons $f_0(X, Y) := p_0(X) + Yq_0(X)$. Alors comme p_0 et q_0 ne s'annulent pas simultanément et que $y_P \neq 0$, $\overline{f}_0(P) \neq 0$. En outre :

$$f_0 = \frac{N(f_0)}{\overline{f}_0}$$

Donc en écrivant dans $\mathbb{K}[X]$: $N(f_0) = (X - x_P)^\beta g$ avec $\beta \in \mathbb{N}$ et $g \in \overline{\mathbb{K}}[X]$ dont x_P n'est pas zéro, on obtient que :

$$f = (X - x_P)^\alpha f_0 = (X - x_P)^{\alpha+\beta} \frac{g}{\overline{f}_0}$$

avec $\frac{g}{\overline{f}_0} \in \overline{\mathbb{K}}(E)$ une fonction dont P n'est ni zéro ni pôle. Si maintenant $f \in \overline{\mathbb{K}}[E]_P$ est une fonction rationnelle sur E alors on écrit $f = \frac{g}{h}$ avec $g, h \in \overline{\mathbb{K}}[E]$ et $h(P) \neq 0$ et en écrivant $g = (X - x_P)^k u$ avec $k \in \mathbb{N}$ et $u \in \overline{\mathbb{K}}[E]_P$ dont P n'est pas zéro :

$$f = (X - x_P)^k \frac{u}{h}$$

avec $\frac{u}{h} \in \overline{\mathbb{K}}[E]_P$ dont P n'est pas zéro, donc inversible. Donc $X - x_P$ est une uniformisante convenable.

Deuxième cas : Supposons $P := (\alpha, 0) \neq \mathcal{O}$ avec $\alpha \in \overline{\mathbb{K}}$. α est donc une racine du polynôme $X^3 + AX + B$, qui admet deux autres racines $\beta, \gamma \in \overline{\mathbb{K}}$, distinctes et différentes de α puisque $\Delta(E) \neq 0$. Comme dans le cas précédent, on commence par traiter la situation où f est polynomiale et on conclut de la même façon lorsque f est une fraction. Ecrivons $f(X, Y) := p(X) + Yq(X)$ sous forme réduite et $p = (X - \alpha)^k p_0$ et $q = (X - \alpha)^l q_0$ avec $k, l \in \mathbb{N}$ et $p_0, q_0 \in \overline{\mathbb{K}}[X]$ dont α n'est pas pôle. Comme :

$$Y^2 = X^3 + AX + B = (X - \alpha)(X - \beta)(X - \gamma)$$

dans $\overline{\mathbb{K}}[E]$, on a :

$$f(X, Y) = Y^{\min(2k,2l+1)} \underbrace{\left(\frac{Y^{2k-\min(2k,2l+1)}}{(X-\beta)^k (X-\gamma)^k} p_0(X) + \frac{Y^{2l+1-\min(2k,2l+1)}}{(X-\beta)^l (X-\gamma)^l} q_0(X) \right)}_{u}$$

Avec u définie en P car $\alpha \neq \beta, \gamma$ et $u(P) \neq 0$ car p_0 et q_0 ne s'annullent pas en α et qu'un seul des exposants $2k - \min(2k, 2l + 1)$ et $2l + 1 - \min(2k, 2l + 1)$ est non nul pour une raison évidente de parité. Donc Y est une uniformisante convenable.

Troisième cas : Supposons $P = \mathcal{O}$. Alors si $f \in \overline{\mathbb{K}}[E]_P \setminus \{0\}$, on écrit :

$$f(X, Y) = \left(\frac{Y}{X}\right)^d g(X, Y)$$

avec $d = -\deg(f)$ et $g(X, Y) \in \overline{\mathbb{K}}(E)$. On a alors d'après la proposition 3.1.6 :

$$-d = d\deg\left(\frac{X}{Y}\right) + \deg(g) = 2d - 3d + \deg(g) = -d + \deg(g)$$

donc $\deg(g) = 0$ et ainsi $g(\mathcal{O}) \neq 0$ d'après les règles d'évaluation. En outre $\deg\left(\frac{X}{Y}\right) = -1$ donc $\frac{X}{Y}(\mathcal{O}) = 0$ et ainsi $\frac{X}{Y} \in M_P$ est une uniformisante convenable.

□

Proposition E.1.2. *Soit $f \in \overline{\mathbb{K}}[E] \setminus \{0\}$. Alors :*

(i). *f n'a qu'un nombre fini de pôles et de zéros.*

(ii). *$\sum_{P\in E} ord_P(f) = 0$.*

(iii). *Si f n'a ni zéro ni pôle, alors f est constante.*

(iv). *Si f est non constante, alors f est surjective.*

Démonstration. **(i).** Ecrivons $f = \frac{g}{h}$ avec g, h des polynômes non nuls sur E. Remarquons que tout zéro de f est zéro de g et que tout pôle de f est zéro de h. Donc si $P \in E \setminus \{0\}$ est zéro de f, alors x_P est racine de $N(g) = g\overline{g}$, qui admet un nombre fini de racines et comme P et $-P$ sont les seuls points d'abscisse x_P, il s'ensuit que l'ensemble des zéros de f est fini. Il en est de même pour les pôles.

(ii). Commençons par montrer le lemme suivant :

Lemme E.1.3.

$$ord_P(f) = ord_{-P}(\overline{f})$$

Démonstration. Si $P = (x_P, y_P) \neq \mathcal{O}$ vérifie $y_P \neq 0$ alors $f = (X - x_P)^{\mathrm{ord}_P(f)} g$ avec $g \in \overline{\mathbb{K}}(E)$ dont P n'est ni zéro ni pôle donc $\overline{f} = (X - x_P)^{\mathrm{ord}_P(f)}\overline{g}$ avec $\overline{g}(-P) = g(P) \neq 0, \infty$ et le résultat s'ensuit immédiatement.
Si $P = (\alpha, 0)$ avec $\alpha \in \overline{\mathbb{K}}$ alors $f = Y^{\mathrm{ord}_P(f)} g$ avec $g \in \overline{\mathbb{K}}(E)$ dont P n'est ni zéro ni pôle donc $\overline{f} = Y^{\mathrm{ord}_P(f)}(-1)^{\mathrm{ord}_P(f)}\overline{g}$ avec $\overline{g}(-P) \neq 0, \infty$ comme précédemment et le résultat s'ensuit immédiatement.
Si $P = \mathcal{O}$ alors $P = -P$ et d'après le troisième cas de la preuve de la proposition 3.1.12 : $\mathrm{ord}_P(f) = -\deg(f) = -\deg(\overline{f}) = \mathrm{ord}_{-P}(\overline{f})$. □

On a donc d'après ce lemme :

$$\sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_P(f) = \sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_{-P}(\overline{f})$$

Donc par multiplicativité de l'ordre :

$$2\sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_P(f) = \sum_{P\in E\setminus\{\mathcal{O}\}} (\mathrm{ord}_P(f) + \mathrm{ord}_{-P}(\overline{f})) = \sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_P(N(f))$$

Factorisons $N(f)$ dans $\overline{\mathbb{K}}(X)$:

$$N(f) = \lambda \prod_{i=1}^{m} (X - x_i)^{n_i}$$

avec $\lambda \in \overline{\mathbb{K}}^*$, $m \in \mathbb{N}^*$, $x_1, \cdots, x_m \in \overline{\mathbb{K}}$ distincts et $n_1, \cdots, n_m \in \mathbb{Z}^*$.
Donc si P est un point d'abscisse x_i pour $1 \leq i \leq m$, et d'ordonnée non nulle, on a :

$$\mathrm{ord}_P(N(f)) = n_i \mathrm{ord}_P(X - x_i) = n_i$$

car $X - x_i$ est une uniformisante. Mais n_i est compté deux fois dans la somme puisque $-P \neq P$ a aussi x_i pour abscisse.
Si maintenant P est un point d'ordonnée nulle, on écrit $P = (\alpha, 0)$ et on note β, γ les autres racines de $X^3 + AX + B$ distinctes de α (cf. deuxième cas de la preuve de la proposition 3.1.12). On a alors :

$$\mathrm{ord}_P(N(f)) = n_i \mathrm{ord}_P(X - x_i) = n_i \mathrm{ord}_P(X - \alpha) = n_i \mathrm{ord}_P\left(\frac{Y^2}{(X-\beta)(X-\gamma)}\right) = 2n_i$$

Mais cette contribution n'est comptée qu'une seule fois car $P = -P$.
Ainsi :

$$2\sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_P(f) = \sum_{P\in E\setminus\{\mathcal{O}\}} \mathrm{ord}_P(N(f)) = \sum_{i=1}^{m} 2n_i = 2\deg(f)$$

Donc :

$$\sum_{P\in E} \mathrm{ord}_P(f) = \deg(f) + \mathrm{ord}_{\mathcal{O}}(f) = 0$$

(iii). D'après ce qui précède, si f est une fonction polynomiale sans zéro (et trivialement sans pôle non plus), alors :

$$\deg(f) = \sum_{P \in E \setminus \{\mathcal{O}\}} \mathrm{ord}_P(f) = 0$$

Et donc $N(f)$ est constante et ainsi, f l'est aussi par un argument de degré dans $\overline{\mathbb{K}}[X,Y]$. Donc si $f = \frac{g}{h}$ est une fonction sur E sans zéro ni pôle, g et h n'ont pas de zéros donc sont constantes et f est constante.

(iv). Si f n'est pas constante alors pour tout $\lambda \in \overline{\mathbb{K}}$, $f - \lambda$ ne l'est pas non plus donc elle admet un zéro ou un pôle d'après le point (iii). Or, la formule de (ii). assure qu'une fonction admettant un pôle admet aussi un zéro.

□

E.2 Groupe des diviseurs de E.

Proposition E.2.1. *Si $D \in Div(E)$ alors il existe $D_1 \in Div(E)$ tel que $|D_1| \leq 1$, $ord(D_1) = ord(D)$ et $D \sim D_1$.*

Démonstration. L'idée principale derrière la preuve est de rassembler les points dans l'expression des diviseurs comme séries formelles en exprimant $(P) + (Q)$ à l'aide de $(P + Q)$. On est alors amené à considérer les droites, qui sont des fonctions polynômiales sur E de la forme :

$$d(X,Y) = aX + bY + c$$

avec $a, b, c \in \overline{\mathbb{K}}$ et $(a,b) \neq (0,0)$. En général, deux cas se présentent :

Premier cas : Lorsque $b \neq 0$, les pôles finis de d sont d'abscisse x, racine du polynôme d'ordre 3 :

$$X^3 - \left(\frac{aX+c}{b}\right)^2 + AX + B$$

et d'ordonnée $-\frac{ax+c}{b}$ donc ils sont au nombre de 3 (en comptant les éventuelles multiplicité) et ainsi :

$$\mathrm{div}(d) = (P) + (Q) + (-R) - 3(\mathcal{O})$$

en ayant noté P, Q et $-R$ ces pôles. On sait qu'alors $P + Q = R$.

Deuxième cas : Lorsque $b = 0$, les pôles finis de d sont d'ordonnée y, racine du polynôme d'ordre 2 :

$$Y^2 + \frac{c^3}{a^3} + \frac{cA}{a} - B$$

et d'abscisse $x = -\frac{c}{a}$ donc ils sont au nombre de 2 (en comptant les éventuelles multiplicité) et ainsi :

$$\mathrm{div}(d) = (P) + (Q) - 2(\mathcal{O})$$

en ayant noté P et Q ces pôles. On peut cependant prendre $R = \mathcal{O}$ et ainsi se ramener à la formule du premier cas.

Voyons maintenant comment ceci sert à rassembler deux points P et Q non nuls. On définit la droite (PQ) passant par les points P et Q (c'est à dire dont P et Q sont pôles) par l'équation :

$$d(X,Y) := (X - x_P)(y_P - y_Q) - (Y - y_P)(x_P - x_Q)$$

En notant $R = P + Q$, on sait qu'alors R est un pôle de d. On a alors :

$$\mathrm{div}(d) = (P) + (Q) + (-R) - 3(\mathcal{O})$$

En outre, si $x_P \neq x_Q$, i.e. $P \neq \pm Q$ alors $R \neq \mathcal{O}$ et $\mathrm{div}(X - x_R) = (R) + (-R) - 2(\mathcal{O})$. Dans ce cas :

$$\mathrm{div}\left(\frac{d(X,Y)}{X - x_R}\right) = \mathrm{div}(d(X,Y)) - \mathrm{div}(X - x_R) = (P) + (Q) - (P+Q) - (\mathcal{O})$$

Donc $(P) + (Q) \sim (P+Q) + (\mathcal{O})$. Dans le cas où $x_P = x_Q$, i.e. $P = \pm Q$, on est ramené au deuxième cas ci-dessus et donc :

$$\mathrm{div}(d(X,Y)) = (P) + (Q) - 2(\mathcal{O})$$

Donc $(P) + (Q) \sim 2(\mathcal{O})$. Notons que cette formule peut encore s'écrire $(P) + (Q) \sim (P+Q) + (\mathcal{O})$ puisque $P + Q = \mathcal{O}$.

On raisonne par récurrence sur la norme de D.

Initialisation : Si D est de norme 0 ou 1 le résultat est immédiat. Pour D de norme 2, D est soit de la forme $D = (P) + (Q) + m(\mathcal{O})$ soit de la forme $D = (P) - (Q) + m(\mathcal{O})$ avec $m \in \mathbb{Z}$. Dans le premier cas, on utilise la formule $(P) + (Q) \sim (P + Q) + (\mathcal{O})$, démontrée ci-dessus pour conclure. Dans le deuxième cas, on applique la formule $\mathrm{div}(X - x_Q) = (Q) + (-Q) - 2(\mathcal{O})$ pour obtenir $(Q) + (-Q) - 2(\mathcal{O}) \sim 0$ et donc :

$$D \sim (P) + (-Q) + (m-2)(\mathcal{O})$$

par somme dans le groupe de Picard. Bien sûr, ces transformations ne changent pas l'ordre de D.

Hérédité : Supposons le résultat aux rangs $\leq n-1$ pour $n \geq 3$ et considérons $D \in \mathrm{Div}(E)$ de norme n.

Si D est de la forme $D = n_1(P) - n_2(Q) + m(\mathcal{O})$ avec $m \in \mathbb{Z}$ et $n_1, n_2 \in \mathbb{N}^*$ tels que $n_1 + n_2 = n$ alors $n_1 \geq 2$ ou $n_2 \geq 2$. On suppose que $n_1 \geq 2$ sans perte de généralité (l'autre cas se traitant de la même manière), puis on utilise le fait que $(P) + (P) \sim 2(\mathcal{O})$ démontré ci-dessus pour obtenir que :

$$D \sim (n_1 - 2)(P) - n_2(Q) + (m-2)(\mathcal{O})$$

qui est de norme $n-2$ et de même ordre que D. On conclut alors par hypothèse de récurrence.

Sinon, D est de la forme $D = n_1(P) + n_2(Q) + D' + m(\mathcal{O})$ avec $m \in \mathbb{Z}$ et $n_1, n_2 \in \mathbb{N}^*$ tels que $n_1 + n_2 \leq n$ et $D' \in \mathrm{Div}(E)$ de norme $n - n_1 - n_2$ et dont le coefficient associé à $\mathcal{O}$ est nul. En utilisant le fait que $(P) + (P) \sim 2(\mathcal{O})$, on obtient alors que :

$$D \sim (n_1 - 1)(P) + (n_2 - 1)(Q) + D' + (m-2)(\mathcal{O})$$

qui est de norme $n-2$ et de même ordre que D. On conclut par hypothèse de récurrence.

□

Proposition E.2.2. *Soient $P, Q \in E$. Alors le diviseur $(P) - (Q)$ est prinicpal si et seulement si $P = Q$.*

Démonstration. On raisonne par l'absurde en supposant que $P \neq Q$. On a alors $(P) - (Q) = \mathrm{div}(f_0)$ pour une certaine fonction rationnelle $f_0 \in \overline{\mathbb{K}}(E)$ de degré zéro, admettant un zéro en P et un pôle en Q. Nous allons montrer que toute fonction rationnelle $f \in \overline{\mathbb{K}}(E)$ est une fraction rationnelle en f_0, ce qui conduira à une contradiction. Soit $f \in \overline{\mathbb{K}}(E)$. On distingue alors deux cas :

Premier cas : Supposons que Q n'est ni zéro ni pôle de f. Alors f_0 est définie en tous les pôles de f (car Q est son unique pôle) et donc on peut considérer :

$$g := \prod_{\substack{R \in E \\ \mathrm{ord}_R(f) \neq 0}} (f_0 - f_0(R))^{\mathrm{ord}_R(f)}$$

Mais pour tout $R \in E$ tel que $\mathrm{ord}_R(f) \neq 0$, $f_0 - f_0(R)$ n'admet que Q comme pôle et elle est de degré 0 donc elle n'admet qu'un seul zéro qui est R d'après le point (ii). de la proposition 3.1.12 donc :

$$\mathrm{div}(f_0 - f_0(R)) = (R) - (Q)$$

Puis, d'après le point (ii). de la proposition 3.1.12 :

$$\begin{aligned}\mathrm{div}(g) &= \sum_{\substack{R \in E \\ \mathrm{ord}_R(f) \neq 0}} \mathrm{ord}_R(f)\mathrm{div}(f_0 - f_0(R)) = \sum_{\substack{R \in E \\ \mathrm{ord}_R(f) \neq 0}} \mathrm{ord}_R(f)(R) - \left(\sum_{\substack{R \in E \\ \mathrm{ord}_R(f) \neq 0}} \mathrm{ord}_R(f) \right)(Q) \\ &= \sum_{\substack{R \in E \\ \mathrm{ord}_R(f) \neq 0}} \mathrm{ord}_R(f)(R) = \mathrm{div}(f)\end{aligned}$$

Donc f est proportionnelle à g d'après le point (iii). de la proposition 3.1.12 et c'est donc une faction rationnelle en f_0, de même que g.

Deuxième cas : Supposons maintenant que Q est zéro ou pôle de f. On a alors :

$$\mathrm{ord}_Q(f f_0^{-\mathrm{ord}_Q(f)}) = \mathrm{ord}_Q(f) - \mathrm{ord}_Q(f)\mathrm{ord}_Q(f_0) = 0$$

Donc $f f_0^{-\mathrm{ord}_Q(f)}$ est une fraction rationnelle en f_0 d'après le cas précédent et c'est aussi le cas pour f.

En particulier, nous venons de montrer que X et Y sont des fractions rationnelles en f_0, donc il existe $r, s \in \overline{\mathbb{K}}(X)$ telles que :

$$r(f_0)^2 = s(f_0)^3 + As(f_0) + B$$

Comme f_0 est non constante, le point (iv). de la proposition 3.1.12 assure que f_0 est surjective donc on a :

$$r(X)^2 = s(X)^3 + As(X) + B$$

Or, ceci n'est possible que si r et s sont constantes, donc si X et Y sont constantes d'après le lemme suivant.

Lemme E.2.3. *Soient $r, s \in \overline{\mathbb{K}}(X)$ telles que :*

$$r(X)^2 = s(X)^3 + As(X) + B$$

Alors r et s sont constantes.

La démonstration de ce lemmme est élémentaire mais longue et technique. C'est pourquoi nous ne la donnerons pas ici. Le lecteur intéressé pourra consulter les pages 32 et 33 de [8]. □

Théorème E.2.4. *D est principal si et seulement si son ordre et sa somme sont nuls.*

Démonstration. $\Longrightarrow$ Si D est principal, on sait déjà par le point (ii). de la proposition 3.1.12 qu'il est d'ordre nul. En outre, la proposition 3.2.7 assure que $D = \epsilon(P) + n(\mathcal{O}) + \mathrm{div}(f)$ avec $P \in E \setminus \{\mathcal{O}\}$, $\epsilon \in \{-1, 0, 1\}$, $n \in \mathbb{Z}$, $f \in \overline{\mathbb{K}}(E)$ et $\mathrm{ord}((P) + n(\mathcal{O})) = \mathrm{ord}(D) = 0$. Ainsi, $n = -\epsilon$. Donc $\epsilon((P) - (\mathcal{O}))$ est principal, ce qui ne peut se produire que si $\epsilon = 0$ ou si $(P) - (\mathcal{O})$ est principal. Si par l'absurde c'est le deuxième cas qui se produit, alors $P = \mathcal{O}$ d'après la proposition 3.2.8, ce qui est exclus. Donc $\epsilon = 0$ et $D = \mathrm{div}(f)$. Or, en repranant la preuve de la proposition 3.2.7, on voit que f est un produit de fonctions dont les sommes des diviseurs sont nulles. Il s'ensuit que $\mathrm{sum}(D) = 0$.

$\Longleftarrow$ Réciproquement, supposons que D est d'ordre et de somme nulle. La prropsition 3.2.7 assure déjà que $D = \epsilon(P) + n(\mathcal{O}) + \mathrm{div}(f)$ avec $\epsilon \in \{-1, 0, 1\}$, $n \in \mathbb{Z}$, $f \in \overline{\mathbb{K}}(E)$ et $\mathrm{ord}((P) + n(\mathcal{O})) = \mathrm{ord}(D) = 0$. On a de même $n = -\epsilon$. Comme on sait que $\mathrm{sum}(\mathrm{div}(f)) = 0$, on a alors :

$$\mathcal{O} = \mathrm{sum}(D) = \epsilon(P - \mathcal{O}) = \epsilon P$$

donc $\epsilon = 0$ puisque $P \neq \mathcal{O}$. On a donc $D = \mathrm{div}(f)$ et donc D est principal. □

E.3 Morphismes, isogénies.

E.3.1 Généralités.

Théorème E.3.1. *Pour qu'un morphisme ϕ soit une isogénie, il faut et il suffit que $\phi(\mathcal{O}) = \mathcal{O}$.*

Démonstration. Si ϕ est une isogénie, on sait que $\phi(\mathcal{O}) = \mathcal{O}$. Réciproquement, supposons que $\phi(\mathcal{O}) = \mathcal{O}$. 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 E.3.2. *Tout morphisme $\psi : E_1 \longrightarrow E_2$ pair, c'est à dire vérifiant $\psi(-P) = \psi(P)$ pour tout $P \in E_1$ est constant.*

Démonstration. En effet, on peut écrire le morphisme sous la forme $\psi = (f, g)$ avec $f, g \in \mathbb{K}(E)$ et on écrit f et g sous forme réduite $f = f_1(X) + Y f_2(X)$ et $g = g_1(X) + Y g_2(X)$ 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. Ainsi, f_1 et f_2 sont constantes d'après le lemme E.2.3. Donc 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 :

$$\alpha_Q : P \in E \longmapsto \phi(P + Q) - \phi(P) - \phi(Q)$$

est nul. On considère pour $Q \in E$ l'application :

$$\beta_Q : P \in E \longmapsto \phi(P + Q) - \phi(P - Q)$$

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 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 lorsque $\mathrm{car}(\mathbb{K}) = 0$ ou lorsque n est premier avec $\mathrm{car}(\mathbb{K})$ [16], 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 contredit le point (i). de la proposition 3.1.12. Donc $\alpha_Q = \mathcal{O}$ et ce pour tout $Q \in E_1$, ce qui donne le résultat. □

E.3.2 Isomorphismes et j-invariant.

Pour simplifier la preuve du résultat suivant, on se place dans le cas où les coefficients A et B des courbes considérées sont non-nuls. Ce résultat se généralise bien-sûr lorsque cela n'est plus vérifié.

Proposition E.3.3. *Deux courbes elliptiques E_1 et E_2 sont isomorphes sur $\overline{\mathbb{K}}$ si et seulement si elles ont même j-invariant. Si E_1 et E_2 sont sous forme canonique, il n'existe que deux isomorphismes $\varphi : E_1 \longmapsto E_2$, qui sont de la forme :*

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

avec γ est une racine de $\frac{A_1B_2}{A_2B_1}$, où $W_1 := Y^2 - X^3 - A_1X - B_1$ et $W_2 := Y^2 - X^3 - A_2X - B_2$ sont les polynômes de Weierstrass de E_1 et E_2.

Démonstration. $\Longrightarrow$ Supposons que E_1 et E_2 sont isomorphes. Ecrivons φ et φ^{-1} sous forme réduite $\varphi(X,Y) := (r_1(X), Ys_1(X))$ et $\varphi^{-1}(X,Y) := (r_2(X), Ys_2(X))$. Comme $\varphi^{-1} \circ \varphi = \mathrm{id}_{E_1}$, on a :

$$r_2(r_1(X)) = X \quad \text{et} \quad Ys_1(X)s_2(r_1(X)) = Y$$

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 $a, b, c \in \overline{\mathbb{K}}$. On sait qu'alors :

$$c^2Y^2 = (aX+b)^3 + A_2(aX+b) + B_2 \quad (1) \quad \text{et} \quad Y^2 = X^3 + A_1X + B_1 \quad (2)$$

L'équation $\frac{(1)}{c^2} - (2)$ donne que $\frac{a^3}{c^2} = 1$ (en regardant le terme en X^3), $b = 0$ (en regardant le terme en X^2), $A_1 = \frac{aA_2}{c^2}$ (3) (en regardant le terme en X) et $B_1 = \frac{B_2}{c^2}$ (4) (en regardant le terme constant). L'équation $\frac{(3)}{(4)}$ donne $\frac{aA_2}{B_2} = \frac{A_1}{B_1}$ donc $a = \frac{A_1B_2}{A_2B_1}$, puis c est une racine de a^3. En fixant γ, une racine de $\frac{A_1B_2}{A_2B_1}$, 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 :

$$j(E_1) = \frac{1728A_1^3}{4A_1^3 + 27B_1^2} = \frac{1728A_2^3}{4A_2^3 + 27B_2^2} = j(E_2)$$

$\Longleftarrow$ 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 $p \geq 5$), on obtient que $A_2^3B_1^2 = A_1^3B_1^2$ et donc $A_1 = \frac{A_2}{\gamma^4}$ et $B_1 = \frac{B_2}{\gamma^6}$ où γ est une racine carrée de $\frac{A_1B_2}{A_2B_1}$. Donc φ de la forme annoncée est bien un isomorphisme. □

E.4 Ramification.

Proposition E.4.1. *Si $\phi : E_1 \longrightarrow E_2$ est un morphisme 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.*

16. Ce résultat sera prouvé ultérieurement

Démonstration. Commençons dans le cas où ϕ est une isogénie. 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 $P \in E$.

Supposons maintenant que ϕ soit simplement un morphisme et notons $Q := \phi(\mathcal{O})$. Alors $\tau_{-Q} \circ \phi$ fixe $\mathcal{O}$ donc c'est une isogénie d'après le théorème 3.3.5. On a donc $e_{\tau_{-Q}\circ\phi}(P) = e_{\tau_{-Q}\circ\phi}(\mathcal{O})$ pour tout $P \in E$. Or, d'après les points (ii). et (iii). de la proposition précédente :

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

D'où le résultat. □

Proposition E.4.2. *Soit $\varphi \in Hom(E_1, E_2)$ une isogénie de forme réduite $(r(X), Ys(X))$. Alors φ est séparable si et seulement si la fraction rationelle dérivée $r'(X)$ est non nulle.*

Démonstration. $\Longrightarrow$ Supposons que φ séparable. Alors $e_\varphi = 1$. En outre, φ n'est pas constante car sinon elle serait nulle et on aurait $e_\varphi = 0$ donc elle est surjective. Comme il n'existe que trois points d'ordonnée nulle et qu'il y a une infinité de points dans E_1 et E_2, on peut donc trouver $P \in E_1 \setminus \{\mathcal{O}\}$ d'ordonnée non nulle tel que $\varphi(P)$ est distinct de $\mathcal{O}$ et d'ordonnée non nulle. D'après le premier cas de la preuve de la proposition 3.1.12, $X - r(x_P)$ est donc une uniformisante en $\varphi(P)$ et ainsi :

$$1 = e_\varphi = e_\varphi(P) = \mathrm{ord}_P(r(X) - r(x_P))$$

Donc x_P est zéro d'ordre 1 de $r(X) - r(x_P)$ ce qui donne $r'(x_P) \neq 0$ donc $r'(X) \neq 0$.

$\Longleftarrow$ Supposons que $r'(X)$ soit non nulle. Alors on dispose d'une infinité de points $P \in E_1 \setminus \{\mathcal{O}\}$ tels que $r'(x_P) \neq 0$ et un nombre fini de points de $E_1 \setminus \{\mathcal{O}\}$ d'ordonnée nulle ou tels que $\varphi(P)$ soit nul ou d'ordonnée nulle puisque φ n'est pas nulle. On dispose donc de $P \in E_1 \setminus \{\mathcal{O}\}$ d'ordonnée non nulle tel que $\varphi(P)$ soit nul et d'ordonnée non nulle vérifiant de surcroît, $r'(x_P) \neq 0$. $X - r(x_P)$ est donc une uniformisante en $\varphi(P)$ tandis que x_P est un zéro d'ordre 1 de $r(X) - r(x_P)$, ce qui donne :

$$e_\varphi = e_\varphi(P) = \mathrm{ord}_P(r(X) - r(x_P)) = 1$$

Donc φ est séparable. □

Corollaire E.4.3. *En caractéristique nulle toutes les isogénies non-nulles sont séparables. Si $car(\mathbb{K}) = p > 0$, une isogénie φ définie sur E est inséparable si et seulement si elle s'écrit sous la forme $\varphi(X, Y) = (r(X^p), Y^p s(X^p))$.*

Démonstration. En caractéristique nulle, une isogénie $\varphi(X, Y) = (r(X), Ys(X))$ telle que $r'(X) = 0$, r est une constante donc φ est constante donc nulle. On suppose donc que $\mathrm{car}(\mathbb{K}) = p > 0$.

$\Longleftarrow$ Si $\varphi(X, Y) = (r(X^p), Y^p s(X^p))$ alors $\frac{dr(X^p)}{dX} = pX^{p-1}r'(X^p) = 0$ donc φ est inséparable.

$\Longrightarrow$ Réciproquement, si φ est inséparable alors on peut l'écrire sous la forme $\varphi(X, Y) = (r_1(X), Ys_1(X))$ donc en multipliant l'ordonnée par $1 = \left(\frac{Y^2}{X^3+AX+B}\right)^{\frac{p-1}{2}}$, 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 $p_1, q_1 \in \mathbb{K}[X]$ premiers entre eux. On a :

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

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 $p, q \in \mathbb{K}[X]$, 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 :

$$s_2(X)^2 = \frac{r(X^p)^3 + Ar(X^p) + B)}{Y^{2p}} = \frac{r(X^p)^3 + Ar(X^p) + B)}{(X^3 + AX + B)^p} = \frac{r(X^p)^3 + Ar(X^p) + B)}{X^{3p} + A^p X^p + B^p}$$

Donc $s_2(X)^2$ est une fraction rationnelle en X^p, donc sa dérivée $2s_2'(X)s_2(X)$ est nulle. Donc $s_2(X) = 0$ ou $s_2'(X) = 0$. Dans les deux cas $s_2(X) = s(X^p)$ pour un certain $s \in \mathbb{K}(X)$. Donc $\varphi(X, Y) = (r(X^p), Y^p s(X^p))$. □

E.4.1 Polynôme d'annulation d'une isogénie.

Définition E.4.4. *Si $\varphi \in Hom(E_1, E_2)$ est une isogénie non nulle, alors appelle* polynôme d'annulation *de φ et on note :*

$$f_\varphi = \prod_{i=1}^{m}(X - x_i)$$

où les x_i sont les abscisses des points de $ker(\varphi) \setminus \{\mathcal{O}\}$ comptées une seule fois.

On peut faire agir le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ sur les points de E en prenant pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$:

$$\sigma \cdot P := \begin{cases} (\sigma(x_P), \sigma(y_P)) & \text{si } P \neq \mathcal{O} \\ \mathcal{O} & \text{si } P = \mathcal{O} \end{cases}$$

On remarque immédiatement que $P \in E(\mathbb{K})$ si et seulement si P est invariant sous l'action du groupe de Galois (comme conséquence de la proposition 5.4.1. de [6]). On vérifie aisément avec les formules d'addition des points et la propriété de morphisme de corps des éléments de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$, que :

$$\forall P, Q \in E, \forall \sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}), \quad \sigma \cdot (P + Q) = \sigma \cdot P + \sigma \cdot Q$$

Proposition E.4.5. *φ est définie sur $\mathbb{K}$ si et seulement si $ker(\varphi)$ est invariant sous l'action de $Gal(\overline{\mathbb{K}}/\mathbb{K})$. Si tel est le cas alors f_φ est dans $\mathbb{K}[X]$.*

Démonstration. Ecrivons la forme réduite : $\varphi(X, Y) := (r(X), Ys(X))$.

$\Longrightarrow$ Supposons que φ est définie sur $\mathbb{K}$. Alors pour tous $P \in E(\mathbb{K}) \setminus \ker(\varphi)$, $Q \in \ker(\varphi)$ et $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$:

$$\varphi(P) = \sigma\varphi(P) = \sigma \cdot \varphi(P + Q) = \sigma \cdot \varphi(P) + \sigma \cdot \varphi(Q)$$

Or $P + Q \in E_1 \setminus \ker(\varphi)$ donc $P + Q$ n'est pas pôle de r et Ys et ces fonctions sont dans $\mathbb{K}(E)$, de sorte que pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ et :

$$\begin{aligned}\sigma \cdot \varphi(P + Q) &= (\sigma(r(x_{P+Q})), \sigma(y_{P+Q}s(x_{P+Q}))) = (r(\sigma(x_{P+Q})), \sigma(y_{P+Q})r(\sigma(x_{P+Q}))) = \varphi(\sigma \cdot (P + Q)) \\ &= \varphi(\sigma \cdot P) + \varphi(\sigma \cdot Q)\end{aligned}$$

On a donc $\mathcal{O} = \sigma \cdot \varphi(Q) = \varphi(\sigma \cdot Q)$ donc $\sigma \cdot Q \in \ker(\varphi)$ et ce pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ et $Q \in \ker(\varphi)$. Donc $\ker(\varphi)$ est invariant sous l'action de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$.

$\Longleftarrow$ Cette implication, qui ne sera pas utilisée, est admise.

En outre, si $\ker(\varphi)$ est stable sous l'action de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$, alors les racines de f_φ sont aussi stables sous l'action de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ et donc $f_\varphi \in \mathbb{K}[X]$. Ceci termine la preuve. □

E.5 L'isogénie $[n]$ et le groupe de n-torsion $E[n]$.

E.5.1 L'isogénie $[n]$.

Lemme E.5.1 (propriétés de la forme réduite)**.** **(i).** *Si n n'est pas multiple de $car(\mathbb{K})$ alors :*

$$deg(r_n) = 2, \quad deg(s_n) = 0, \quad \frac{r_n}{X}(\mathcal{O}) = \frac{1}{n^2}, \quad \text{et } s_n(\mathcal{O}) = \frac{1}{n^3}$$

(ii). *On a pour tous $n, m \in \mathbb{N}^*$ tels que $car(\mathbb{K})$ ne divise pas $n, m, n + m$ et $n - m$:*

$$div(r_n - r_m) = (E[n + m]) + (E[n - m]) - 2(E[m]) - 2(E[n])$$

Démonstration. **(i).** On prouve le résultat par récurrence forte sur $n \in \mathbb{N}^*$ non divisible par $\mathrm{car}(\mathbb{K})$. Le résultat est trivial pour $n = 1$. On a d'après les formules d'addition, pour $n = 2$:

$$r_2 = \frac{(3X^2 + A)^2}{4Y^2} - 2X = \frac{X^4 - 2AX^2 - 8BX + A^2}{4(X^3 + AX + B)}$$

Et :

$$s_2 = \frac{r_2'}{2} = \frac{X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - A^3}{8(X^3 + AX + B)^2}$$

Comme, $\deg(X) = 2$ et $\deg(Y) = 3$, on a $\deg(r_2) = 2$ et $\deg(s_2) = 0$. Puis, en évaluant ces expressions en $\mathcal{O}$, on trouve bien $\frac{r_2}{X}(\mathcal{O}) = \frac{1}{4}$ et $s_2(\mathcal{O}) = \frac{1}{8}$. Notons que tous les calculs faits ici sont légaux puisque $\mathrm{car}(\mathbb{K}) \geq 5$.

Pour prouver l'hérédité, commençons par vérifier que si $q \geq 3$ n'est pas divisible par $\mathrm{car}(\mathbb{K})$ alors il existe $n, m \in \mathbb{N}^*$ distincts tels que $n+m=q$ et $\mathrm{car}(\mathbb{K})$ ne divise pas n et m. Si $q-1$ n'est pas divisible par $\mathrm{car}(\mathbb{K})$, il suffit de prendre $n=q-1$ et $m=1$. Sinon, $n=q-2$ et $m=2$ conviennent. Comme $\mathrm{car}(\mathbb{K}) \geq 5$, le cas $q=2$ ne pose aucun problème. On a d'après les formules d'addition :

$$r_q(X) = Y^2 \left(\frac{s_n - s_m}{r_n - r_m}\right)^2 - r_n - r_m$$

Comme $\deg(r_n) = \deg(r_m) = 2$, $\deg(s_n) = \deg(s_m) = 0$ par hypothèse et $\deg(Y^2) = 6$, on obtient qu'alors $\deg(r_q) \leq 2$. Mais :

$$\begin{aligned}
\frac{r_q}{X}(\mathcal{O}) &= \frac{Y^2}{X}\left(\frac{s_n - s_m}{r_n - r_m}\right)^2(\mathcal{O}) - \frac{r_n}{X}(\mathcal{O}) - \frac{r_m}{X}(\mathcal{O}) \\
&= \frac{X^3 + AX + B}{X^3}\left(\frac{s_n - s_m}{\frac{r_n}{X} - \frac{r_m}{X}}\right)^2(\mathcal{O}) - \frac{r_n}{X}(\mathcal{O}) - \frac{r_m}{X}(\mathcal{O}) \\
&= \left(\frac{\frac{1}{n^3} - \frac{1}{m^3}}{\frac{1}{n^2} - \frac{1}{m^2}}\right)^2 - \frac{1}{n^2} - \frac{1}{m^2} = \frac{1}{(n+m)^2} = \frac{1}{q^2}
\end{aligned}$$

Donc $\deg(r_q) = 2$ puisque ce dernier terme n'est pas nul. En outre, $s_q = \frac{r_q'}{q}$ et donc $\deg(s_q) = \deg(r_q) - 2 = 0$. Puis, le rapport des coefficients dominants du numérateur et du dénominateur de r_q' égalise celui de r_q en vertu d'un calcul facile donc $r_q'(\mathcal{O}) = \frac{r_q}{X}(\mathcal{O}) = \frac{1}{q^2}$, puis $s_q(\mathcal{O}) = \frac{1}{q^3}$. D'où l'itération et le résultat.

(ii). Ce fait ne sera pas prouvé en entier car la preuve est simplement très calculatoire. Le lecteur intéressé pourra la trouver aux pages 46 et 47 de [8]. Nous ne donnons ici que l'idée principale : la détermination des zéros et des pôles de $r_n - r_m$. On voit que si $P \in E$ est zéro de $r_n - r_m$ alors $x_{[n]P} = x_{[m]P}$ donc $[n]P = \pm[m]P$ ie $[n \pm m]P = \mathcal{O}$ donc $P \in E[n+m] \cup E[n-m]$. Si maintenant P est un pôle de $r_n - r_m$ alors P est pôle de l'une des deux fonctions c'est à dire dans $E[n]$ ou $E[m]$. Il reste maintenant à calculer les ordres, ce qui se fait par une disjonction de cas assez longue et pénible où l'hypothèse $\mathrm{car}(\mathbb{K})$ ne divise pas $n+m$ et $n-m$ intervient pour pouvoir utiliser les relations $r_n' = ns_n$ et $r_m' = ms_m$.

□

E.5.2 Compléments sur le polynôme de division.

Proposition E.5.2. *ψ_n est un polynôme de $\mathbb{K}[E]$ donné par :*

$$\Psi_n(X,Y) := \begin{cases} nf_{[n]}(X) & \text{si } n \text{ est impair} \\ nY\frac{f_{[n]}(X)}{f_{[2]}(X)} & \text{si } n \text{ est pair} \end{cases}$$

où $f_{[n]}(X)$ est le polynôme d'annulation de $[n]$ dont l'ensemble des racines est l'ensemble des abscisses des points de $E[n] \setminus \{\mathcal{O}\}$.

Démonstration. Supposons n est impair. Alors $E[n] \cap E[2] = \{\mathcal{O}\}$ donc tous les zéros de Ψ_n sont d'ordonnée non-nulle. Donc si $P \in E[n]$ est un zéro de Ψ_n, on a $P \neq \mathcal{O}$ et $y_P \neq 0$. On sait qu'alors :

$$\mathrm{div}(X - x_P) = (P) + (-P) - 2(\mathcal{O})$$

avec P et $-P$ distincts. Il s'ensuit que $f_{[n]}$ et Ψ_n ont même diviseur donc que $\Psi_n(X,Y) = nf_{[n]}(X)$ en regardant le coefficient dominant.

Supposons n pair. On a toujours pour tout $P \in E[n] \setminus E[2]$:

$$\mathrm{div}(X - x_P) = (P) + (-P) - 2(\mathcal{O})$$

Et en outre, comme Y est de degré 3 et que ses zéros sont tous les points de $E[2] \setminus \{mO\}$, on a :

$$\mathrm{div}(Y) = \sum_{P \in E[2]} (P) - 4(\mathcal{O})$$

Donc $Y\frac{f_{[n]}(X)}{f_{[2]}(X)}$ et Ψ_n ont même diviseur donc que $\Psi_n(X,Y) = nY\frac{f_{[n]}(X)}{f_{[2]}(X)}$ en regardant le coefficient dominant. □

Proposition E.5.3. *Soient $n, m \in \mathbb{N}^*$ vérifiant $n > m$. Si car($\mathbb{K}$) ne divise pas $n, m, n-m$ et $n+m$ alors :*

$$r_n - r_m = -\frac{\Psi_{n+m}\Psi_{n-m}}{\Psi_n^2 \Psi_m^2}$$

Démonstration. D'après le point (ii). du lemme 3.4.4, on voit que $\mathrm{div}(r_n - r_m) = \mathrm{div}\left(\frac{\Psi_{n+m}\Psi_{n-m}}{\Psi_n^2\Psi_m^2}\right)$. Ces fonctions sont donc proportionnelles d'après la proposition le point (iii). de la 3.2.4. Or, d'après le point (i). du lemme 3.4.4, le coefficient dominant de $r_n - r_m$ (qui est de degré 2) vaut :

$$\frac{r_n - r_m}{X}(\mathcal{O}) = \frac{1}{n^2} - \frac{1}{m^2}$$

Tandis que le coefficient dominant de $\frac{\Psi_{n+m}\Psi_{n-m}}{\Psi_n^2\Psi_m^2}$ vaut :

$$\frac{(n+m)(n-m)}{n^2m^2} = \frac{1}{m^2} - \frac{1}{n^2}$$

D'où l'égalité. □

En appliquant ceci avec $m = 1$, on obtient le :

Corollaire E.5.4. *Soit $n \in \mathbb{N}^*$ tel que car($\mathbb{K}$) ne divise ni n, ni $n-1$. Alors :*

$$r_n = \frac{X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}$$

On peut aussi obtenir une définition de la suite des polynômes de division par récurrence en exprimant $r_{2n} - r_n$ et $r_{2n+1} - r_n$ de deux façons différentes.

Proposition E.5.5. *Supposons que car($\mathbb{K}$) $= 0$. Alors :*

$$\Psi_1 := 1, \quad \Psi_2 := 2Y, \quad \Psi_3 := 3X^4+6AX^2+12BX-A^2, \quad \Psi_4 := 4Y(X^6+5AX^4+20BX^3-4ABX-A^3+8B^2)$$

Et :

$$\Psi_{2n+1} := \Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3 \quad \textit{pour } n \geq 2$$

$$\Psi_{2n} := \frac{\Psi_n(\Psi_{n-1}^2\Psi_{n+2} - \Psi_{n-2}\Psi_{n+1}^2)}{2Y} \quad \textit{pour } n \geq 3$$

A partir de ces relations de récurrence et des formules d'addition des points, on obtient aussi le :

Corollaire E.5.6. *Soit $n \in \mathbb{N}^*$ tel que car($\mathbb{K}$) ne divise pas $n-2, n-1, n, n+1$. Alors :*

$$s_n = \frac{\Psi_{2n}}{2\Psi_n^4} = \frac{\Psi_{n-1}^2\Psi_{n+2} - \Psi_{n-2}\Psi_{n+1}^2}{4Y\Psi_n^3}$$

Remarque : Il est possible de définir la suite des polynômes de division par récurrence même lorsque car($\mathbb{K}$) $\neq 0$ en prenant les relations de la proposition précédente. On peut alors montrer que les corollaires E.5.4 et E.5.6 sont vrais pout tout $n \in \mathbb{N}^*$. Cela fait l'objet de l'exercice 3.7. de [7].

Notons que ces polynômes dépendent à priori de X, Y, A et B. On peut donc les considérer comme des polynômes de $\mathbb{Z}[X, Y, A, B]$.

A partir des formules récursives, on peut aussi montrer par récurrence le :

Lemme E.5.7. *On a dans $\mathbb{Z}[X, Y, Z, A, B]$:*

$$\Psi_n(Z^2X, Z^3Y, Z^4A, Z^6B) = Z^{n^2-1}\Psi_n(X, Y, A, B)$$

E.6 Couplage de Weil.

Proposition E.6.1 (propriétés du couplage de Weil)**.** **(i).** *e_n est bilinéaire :*

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

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

(ii). *e_n est altéernée $e_n(P, P) = 1$ 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 $Q = \mathcal{O}$.*

(iv). *Le couplage de Weil est compatible. C'est à dire que :*

$$e_{nm}(P,Q) = e_n([m]P,Q)$$

pour tous $n,m \in \mathbb{N}^*$ non divisibles par car($\mathbb{K}$), $P \in E[nm]$ et $Q \in E[m]$.

Démonstration. **(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 E.2.4 assure l'existence de $f \in \overline{\mathbb{K}}(E)$ 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 :

$$\begin{aligned}
\mathrm{div}(f\circ[n]) &= \sum_{R\in E[n]}(R+Q_1'+Q_2') - \sum_{R\in E[n]}(R+Q_1') - \sum_{R\in E[n]}(R+Q_1') + \sum_{R\in E[n]}(R) \\
&= \sum_{R\in E[n]}[(R+Q_1'+Q_2')-(R)] - \sum_{R\in E[n]}[(R+Q_1')-(R)] - \sum_{R\in E[n]}[(R+Q_1')-(R)] \\
&= \mathrm{div}(g_{Q_1+Q_2}) - \mathrm{div}(g_{Q_1}) - \mathrm{div}(g_{Q_2})
\end{aligned}$$

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 le couplage 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 $\mathrm{div}(f_P) = n(P) - n(\mathcal{O})$, on a $\mathrm{div}(f_P\circ\tau_{iP}) = n(-[i-1]P) - n(-[i]P)$ donc :

$$\begin{aligned}
\mathrm{div}\left(\prod_{i=0}^{n-1} f_P\circ\tau_{iP}\right) &= \sum_{i=0}^{n-1}\mathrm{div}(f_P\circ\tau_{iP}) = \sum_{i=0}^{n-1}[n(-[i-1]P) - n(-[i]P)] \\
&= \sum_{i=-1}^{n-2} n(-[i]P) - \sum_{i=0}^{n-1} n(-[i]P) = 0
\end{aligned}$$

La dernière égalité venant du fait que $[-1]P = [n-1]P$ puisque $P \in E[n]$. Ainsi, $\prod_{i=0}^{n-1} f_P\circ\tau_{iP}$ est constante d'après le point (iii). de la proposition 3.1.12. Comme $f_P\circ[n] = g_P^n$, et $\tau_{[i]P}\circ[n] = [n]\circ\tau_{[i]P'}$, on a :

$$\left(\prod_{i=0}^{n_1} g_P\circ\tau_{iP'}\right)^n = \prod_{i=0}^{n_1} f_P\circ[n]\circ\tau_{iP'} = \left(\prod_{i=0}^{n_1} f_P\circ\tau_{iP}\right)\circ[n]$$

Et $\left(\prod_{i=0}^{n_1} g_P\circ\tau_{iP'}\right)^n$ est donc constante. Donc $\prod_{i=0}^{n_1} g_P\circ\tau_{iP'}$ 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 difficile suivant.

Lemme E.6.2. *Soit $f \in \overline{\mathbb{K}}(E)$ telle que pour tous $P \in E[n]$ et $Q \in E$, on ait $f(Q+P) = f(Q)$. Alors il existe $g \in \overline{\mathbb{K}}(E)$ telle que $f = g \circ [n]$.*

Démonstration. Considérons les sous-corps de $\overline{\mathbb{K}}(E)$ suivants :

$$L := \{f \in \overline{\mathbb{K}}(E) \mid \forall P \in E[n], \quad f \circ \tau_P = f\} \quad \text{et} \quad M := \{g \circ [n] \mid g \in \overline{\mathbb{K}}\}$$

et le groupe G formé par les automorphismes $\sigma_P : f \in \overline{\mathbb{K}}(E) \longmapsto f \circ \tau_P \in \overline{\mathbb{K}}(E)$ pour $P \in E[n]$. Ce groupe est d'ordre n^2 par hypothèse. L étant un sous-corps $\overline{\mathbb{K}}(E)$ invariant sous l'action de G, le lemme d'Artin (voir théorème 5.4.2. de [6]) assure alors que $[\overline{\mathbb{K}}(E) : L] = n^2$. Sachant qu'il est clair que $M \subset L$, il suffit de montrer que $[\overline{\mathbb{K}}(E) : M] \leq n^2$ pour obtenir que $L = M$ et conclure.
En reprenant les notations du paragraphe 3.4.1, on obtient que $r_n(X) = X \circ [n]$ et que $Y s_n(X) = Y \circ [n]$. Ces fonctions sont donc dans M. En outre, on a d'après le corollaire E.5.4 :

$$r_n = \frac{X\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2} \quad \text{donc} \quad X\psi_n^2 - \psi_{n-1}\psi_{n+1} - \psi_n^2 r_n = 0$$

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 $\overline{\mathbb{K}}(X)$.
Mais $\overline{\mathbb{K}}(E) = M(X,Y)$ et $Y = \frac{Y \circ [n]}{s_n(X)} \in M(X)$ car $Y \circ [n] \in M$. Donc $\overline{\mathbb{K}}(E) = M(X)$ et ainsi $[\overline{\mathbb{K}}(E) : M] = [M(X) : M] \leq n^2$. 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 $h_Q \in \overline{\mathbb{K}}(E)$ 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 $\mathrm{div}(h_Q) = (Q) - (\mathcal{O})$ et ainsi $(Q) - (\mathcal{O})$ est principal donc $Q = \mathcal{O}$ d'après la 3.2.8.

(iv). On a :

$$\mathrm{div}(f_Q^m) = m\mathrm{div}(f_Q) = nm(Q) - nm(\mathcal{O})$$

Et :

$$(g_Q \circ [m])^{nm} = (g_Q^n)^m \circ [m] = (f_Q \circ [n])^m \circ [m] = f_Q^m \circ [nm]$$

Donc on peut substituer $(f_Q^m, g_Q \circ [m])$ à (f_Q, g_Q) pour définir e_{nm} d'après la définition du couplage de Weil. Ainsi, pour $R \in E$ quelconque, on a :

$$e_{nm}(P,Q) = \frac{g_Q \circ [m](P+R)}{g_Q \circ [m](R)} = \frac{g_Q([m]P + [m]R)}{g_Q([m]R)} = e_n([m]P, Q)$$

□

E.7 Isogénie duale.

Proposition E.7.1. *Si $\varphi \in Hom(E_1, E_2)$ alors il existe $\hat{\varphi} \in Hom(E_2, E_1)$ telle que :*

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

Cette isogénie est unique lorsque φ est non nulle et elle est donnée par la formule :

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

pour tout $P \in E_2$. $\hat{\varphi}$ est appelée l'isogénie duale *de φ.*

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 :

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

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

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

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. □

Proposition E.7.2. *Soit $\varphi \in Hom(E_1, E_2)$, $\psi \in Hom(E_2, E_3)$ des isogénies. Alors :*

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

(ii). *Si car($\mathbb{K}$) ne divise pas n alors φ et $\hat{\varphi}$ sont adjointes pour 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). $deg(\hat{\varphi}) = deg(\hat{\varphi})$.

(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 $e_n(\varphi(P), Q) = \frac{g_Q(R + \varphi(P))}{g_Q(R)}$. 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 E.2.4 assure que D est principal. Soit donc $h \in \overline{\mathbb{K}}(E)$ 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, car$(\mathbb{K}) \neq 2$ 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 le lemme 3.4.1. Donc $\widehat{\varphi+\psi} - \widehat{\varphi} - \widehat{\psi}$ est une isogénie de noyau infini, donc nulle. 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 $m \neq 0$ (fait que nous prouverons dans le paragraphe suivant). 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.

□

E.8 Module de Tate.

Proposition E.8.1. *Si $l \neq$ car$(\mathbb{K})$ alors $T_l(E)$ est isomorphe à $\mathbb{Z}_l^2$ en tant que $\mathbb{Z}_l$-module.*

Démonstration. D'après le théorème 3.6.5, on dispose pour tout $n \in \mathbb{N}^*$, d'un isomorphisme de groupes à $\Phi_n := (\phi_n, \psi_n) : E[l^n] \longrightarrow (\mathbb{Z}/l^n\mathbb{Z})^2$. On amerait pouvoir prendre comme morphisme de $\mathbb{Z}_p$-modules :

$$\begin{array}{rccc} \Phi : & T_l(E) & \longrightarrow & \mathbb{Z}_l^2 \\ & (P_n)_{n\in\mathbb{N}^*} & \longmapsto & ((\phi_n(P_n))_{n\in\mathbb{N}^*}, (\psi_n(P_n))_{n\in\mathbb{N}^*}) \end{array}$$

Toutefois, rien ne prouve que ce morphisme est bien défini, puisqu'il faudrait vérifier que :

$$\forall 1 \leq n \leq m, \quad \phi_m(P_m) \equiv \phi_n(P_n)\,[l^{n+1}] \quad \text{et} \quad \psi_m(P_m) \equiv \psi_n(P_n)\,[l^{n+1}] \quad (\star)$$

Nous allons construire par récurrence sur $n \in \mathbb{N}^*$ une suite de morphismes de groupes $(\tilde{\Phi}_n)_{n\in\mathbb{N}^*}$ qui vérifie $(\star)$.

Initialisation : On prend $\tilde{\Phi}_1 = \Phi_1$.

Hérédité : Supposons construits les n premiers termes de la suite pour $n \in \mathbb{N}^*$. Posons $P := \tilde{\Phi}_n^{-1}((1,0))$ et $Q := \tilde{\Phi}_n^{-1}((0,1))$. Alors P et Q sont d'ordre l^n et engendrent $E[l^n]$. Soient $P_1, Q_1 \in E$ des antécédants respectifs de P et Q par $[l]$ (qui existent car $[l]$ est surjective). Montrons que P_1 et Q_1 engendrent $E[l^{n+1}]$. Soient $a, b \in \mathbb{Z}/l^{n+1}\mathbb{Z}$ tels que $aP_1 + bQ_1 = \mathcal{O}$. Alors en multipliant par l, et en composant par Φ_n, on obtient que $a, b \equiv 0\,[l^n]$. Mais alors a et b valent soit 0 soit l^n dans $\mathbb{Z}/l^n\mathbb{Z}$. Le cas $(a,b) \in \{(0,l^n), (l^n,0)\}$ est exlus car il donnerait que P_1 ou Q_1 est d'ordre l^n et donc que P ou Q est d'ordre l^{n-1}. Le cas $(a,b) = (l^n, l^n)$ est aussi exclus car il donne en composant par Φ_n que $l^{n-1} \equiv 0\,[l^n]$. Donc $a = b = 0$. Ainsi, $(a,b) \in (\mathbb{Z}/l^{n+1}\mathbb{Z})^2 \longmapsto aP_1 + bQ_1 \in E[l^{n+1}]$ est

injective donc surjective par égalité des cardinaux et aisni P_1 et Q_1 engendrent $E[l^{n+1}]$. On pose alors :

$$\tilde{\Phi}_{n+1}(P_1) := (1,0) \quad \text{et} \quad \tilde{\Phi}_{n+1}(Q_1) := (0,1)$$

dans $(\mathbb{Z}/l^{n+1}\mathbb{Z})^2$, ce qui suffit à définir $\tilde{Phi}_{n+1}$. C'est bien un isomorphisme de $E[l^{n+1}]$ vers $(\mathbb{Z}/l^{n+1}\mathbb{Z})^2$, qui vérifie en outre :

$$\forall P \in E[l^{n+1}], \quad \Phi_{n+1}(P) \equiv \Phi_n([l]P)\,[l^{n+1}]$$

par construction.

Il est aisé de vérifier que la suite ainsi construite vérifie $(\star)$, ce qui donne bien le résultat voulu. □

E.9 Résultats profonds de géométrie algébrique.

Nous sommes jusque là resté à un niveau d'algèbre assez élémentaire pour faciliter les démonstrations. En particulier, la notion de dégré introduite était plus analytique qu'algébrique afin d'être plus manipulable.

Toutefois, nous avons désormais besoin de résultats plus forts sur les isogénies, notamment ceux démontrés par Jacques Vélu dans [10]. Nous nous référons donc cette fois-ci à [**?**] en faisant le lien avec le point de vue de [8]. Comme les résultats invoqués sont plus difficiles, nous omettrons certaines preuves.

Pour raison technique, nous supposerons dans tout ce paragraphe que $\mathbb{K}$ est de caractéristique nulle, ce qui nous assure que tous les corps considérés ici sont aussi de caractéristique nulle, donc parfaits (cadre idéal pour appliquer les résultats de l'annexe C et de [6]). On sait aussi par ailleurs que toute isogénie φ non nulle est non ramifiée (voir corollaire E.4.3), de sorte que $\deg(\varphi) = |\ker(\varphi)|$.

Etant données deux courbes elliptiques E_1 et E_2 et un morphisme $\phi : E_1 \longrightarrow E_2$, on définit l'application :

$$\phi^* : f \in \overline{\mathbb{K}}(E_2) \longmapsto f \circ \phi \in \overline{\mathbb{K}}(E_1)$$

qui est un morphisme de $\overline{\mathbb{K}}$-algèbres. Si ϕ est non constant, ϕ^* est induit même injective car si $f, g \in \overline{\mathbb{K}}(E_2)$ vérifient $f \circ \phi = g \circ \phi$ alors $f(P) = g(P)$ pour tout $P \in E_2$ (ϕ étant surjective) et donc $f = g$. Ainsi, ϕ^* induit un isomorphisme de $\overline{\mathbb{K}}$-algèbres entre $\overline{\mathbb{K}}(E_2)$ et $\phi^*\overline{\mathbb{K}}(E_2)$ et on peut donc définir un isomorphisme réciproque ϕ^{*-1}.

Proposition E.9.1. *Si $\varphi \in Hom(E_1, E_2)$ alors :*

$$deg(\varphi) = [\overline{\mathbb{K}}(E_1) : \varphi^*\overline{\mathbb{K}}(E_2)]$$

Démonstration. Nous allons appliquer la proposition D.3.7 en prenant $\varphi^*\overline{\mathbb{K}}(E_2)$ pour $\mathbb{K}$, $\overline{\mathbb{K}}(E_1)$ pour $\mathbb{L}$, $\varphi^*\overline{\mathbb{K}}[E_2]_{\mathcal{O}}$ pour $\mathbb{A}$ et $\varphi^*M(E_2)_{\mathcal{O}}$ pour $\mathfrak{p}$. Toujours dans l'esprit des notations de la proposition D.3.7, on note $\mathbb{B}$ la clôture intégrale de $\varphi^*\overline{\mathbb{K}}[E_2]_{\mathcal{O}}$ dans $\overline{\mathbb{K}}(E_1)$. Les idéaux de $\mathbb{B}$ divisant $\mathfrak{p}$ sont de la forme $\mathfrak{B} := M(E_1)_P$ pour $P \in \ker(\varphi)$. On a donc d'après la proposition D.3.7 :

$$[\overline{\mathbb{K}}(E_1) : \varphi^*\overline{\mathbb{K}}(E_2)] = \sum_{\mathfrak{B}|\mathfrak{p}} e_{\mathfrak{B}/\mathfrak{p}} f_{\mathfrak{B}/\mathfrak{p}}$$

Mais pour tout $\mathfrak{B} := M(E_1)_P|\mathfrak{p}$, $e_{\mathfrak{B}/\mathfrak{p}}$ est la valuation ord_P minimale de $\mathfrak{p}$ donc :

$$e_{\mathfrak{B}/\mathfrak{p}} = e_\varphi(P)$$

d'après la formule du point (i). de la proposition 3.3.10.

Puis, $f_{\mathfrak{B}/\mathfrak{p}} = [\mathbb{B}/\mathfrak{B} : \mathbb{A}/\mathfrak{p}] = 1$ puisque $\mathbb{B}/\mathfrak{B} = \mathbb{A}/\mathfrak{p} = \overline{\mathbb{K}}$. Pour une démonstration de ce fait, il s'agit de développer toutes les fonctions de $\overline{\mathbb{K}}(E_1)$ en série formelle à coefficients dans $\overline{\mathbb{K}}$, en prenant une uniformisante en P comme paramètre. Le développement est fait dans le cas $P = \mathcal{O}$ dans la section concernant le groupe formel.

Comme e_φ est constante, on obtient donc finalement que :

$$[\overline{\mathbb{K}}(E_1) : \varphi^*\overline{\mathbb{K}}(E_2)] = \sum_{P \in \ker(\varphi)} e_\varphi(P) = |\ker(\varphi)| e_\varphi = \deg(\varphi)$$

□

Remarque : Le résultat précédent et sa preuve sont toujours valables en caractéristique non nulle et lorsque φ est inséparable.

Proposition E.9.2. *L'application :*

$$\begin{array}{rccc} \Phi : & ker(\varphi) & \longrightarrow & Aut_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1)) \\ & P & \longmapsto & \tau_P^* \end{array}$$

où τ_P désigne la translation de P, définit un isomorphisme de groupes. En conséquence, l'extension $\overline{\mathbb{K}}(E_1)/\varphi^*\overline{\mathbb{K}}(E_2)$ 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 $f \in \overline{\mathbb{K}}(E_2)$:

$$\tau_P^*(\varphi^*(f)) = f \circ \varphi \circ \tau_P = f \circ \varphi = \varphi^*(f)$$

Donc τ_P^* fixe $\varphi^*\overline{\mathbb{K}}(E_2)$ donc c'est un morphisme de $\varphi^*\overline{\mathbb{K}}(E_2)$-algèbres. En outre, τ_P^* est bijectif de reciproque τ_{-P}^*, ce qui prouve bien que $\tau_P^* \in \mathrm{Aut}_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1))$.

Puis, si $P, Q \in \ker(\varphi)$, alors pour tout $g \in \overline{\mathbb{K}}(E_1)$:

$$\Phi(P+Q)(g) = g \circ \tau_{P+Q} = g \circ \tau_Q \circ \tau_P = \Phi(P) \circ \Phi(Q)(g)$$

Donc Φ est un morphisme de groupes.

Soit $P \in \ker(\varphi)$ tel que $\Phi(P) = id_{\overline{\mathbb{K}}(E_1)}$. Alors pour tout $f \in \overline{\mathbb{K}}(E_1)$, $f \circ \tau_P = f$ donc en prenant $f = 1$, on obtient $\tau_P = id_{E_1}$ donc $P = \mathcal{O}$ (en évaluant cette égalité en $\mathcal{O}$). Donc Φ est injective.

La proposition précédente et la séparabilité de φ ($\mathrm{car}(\mathbb{K}) = 0$) assurent que $[\overline{\mathbb{K}}(E_1) : \varphi^*\overline{\mathbb{K}}(E_2)] = \deg(\varphi) = |\ker(\varphi)|$ et un résultat classique de théorie de Galois donne alors que :

$$|\mathrm{Aut}_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1))| \leq [\overline{\mathbb{K}}(E_1) : \varphi^*\overline{\mathbb{K}}(E_2)] = |\ker(\varphi)|$$

Ce qui permet de conclure à la bijectivité de Φ. Rappelons simplement le résultat de théorie de Galois invoqué. $\overline{\mathbb{K}}(E_1)/\varphi^*\overline{\mathbb{K}}(E_2)$ est une extension finie de corps parfait de degré $|\ker(\varphi)|$ donc le théorème de l'élément primitif (théorème 4.6.2 de [6]) assure l'existence de $f \in \overline{\mathbb{K}}(E_1)$ de degré $|\ker(\varphi)|$ tel que $\overline{\mathbb{K}}(E_1) = \varphi^*\overline{\mathbb{K}}(E_2)[f]$. Un élément $\sigma \in \mathrm{Aut}_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1))$ est donc entièrement déterminé par sa valeur $\sigma(f)$ qui est forcément un $\varphi^*\overline{\mathbb{K}}(E_2)$-conjugué de f (qui est de degré $|\ker(\varphi)|$) et il y a donc au plus $|\ker(\varphi)|$ éléments dans $\mathrm{Aut}_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1))$.

Comme Φ est bijective, l'inégalité $|\mathrm{Aut}_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1))| \leq |\ker(\varphi)|$ est en fait une égalité et on obtient donc que tous les $\varphi^*\overline{\mathbb{K}}(E_2)$-conjugués de f sont les $\sigma(f) \in \overline{\mathbb{K}}(E_1)$ pour $\sigma \in \mathrm{Aut}_{\varphi^*\overline{\mathbb{K}}(E_2)}(\overline{\mathbb{K}}(E_1))$ et donc que $\overline{\mathbb{K}}(E_1)/\varphi^*\overline{\mathbb{K}}(E_2)$ est galoisienne. □

Proposition E.9.3. *Soient E_1, E_2, E_3 des courbes elliptiques définies sur $\mathbb{K}$, $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_1, E_3)$ des isogénies telles que $ker(\varphi) \subset ker(\psi)$. Alors il existe une unique isogénie $\lambda \in Hom(E_2, E_3)$ telle que :*

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

Démonstration. Tout point $P \in \ker(\varphi)$ est aussi dans $\ker(\psi)$, de sorte que $\tau_P^* \in \mathrm{Gal}(\overline{\mathbb{K}}(E_1)/\psi^*\overline{\mathbb{K}}(E_3))$ d'après la propostion précédente et donc que τ_P^* fixe $\overline{\mathbb{K}}(E_3)$. Mais comme tous les éléments du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{K}}(E_1)/\varphi^*\overline{\mathbb{K}}(E_2))$ sont de la forme τ_P^* pour $P \in \ker(\varphi)$ d'après la proposition précédente, on obtient que $\mathrm{Gal}(\overline{\mathbb{K}}(E_1)/\varphi^*\overline{\mathbb{K}}(E_2))$ fixe $\psi^*\overline{\mathbb{K}}(E_3)$ et donc que :

$$\psi^*\overline{\mathbb{K}}(E_3) \subset \varphi^*\overline{\mathbb{K}}(E_2)$$

d'après un résultat classique de théorie de Galois (proposition 5.4.1 de [6]).

Considérons donc le plongement :

$$\iota := {\varphi^*}^{-1} \circ i \circ \psi^* : \overline{\mathbb{K}}(E_3) \longrightarrow \overline{\mathbb{K}}(E_2)$$

où i est l'inclusion canonique de $\psi^*\overline{\mathbb{K}}(E_3)$ dans $\varphi^*\overline{\mathbb{K}}(E_2)$. 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 et W_3 respectivement les polynômes de Weierstrass de E_2 et E_3 on obtient l'égalité suivante dans $\overline{\mathbb{K}}(E_3)$:

$$W_3(\iota(X_3), \iota(X_3)) = \iota(W_3(X_3, Y_3)) = \iota(0) = 0$$

Donc λ est bien un morphisme de E_2 dans E_3. En outre, pour tout $f \in \overline{\mathbb{K}}(E_3)$:

$$\lambda^*(f) = f \circ \lambda = f(\iota(X_3), \iota(Y_3)) = \iota(f(X_2, Y_2)) = \iota(f)$$

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 $\lambda \circ \varphi = \psi$. □

Le nouveau formalisme introduit permet de montrer rapidement un résultat très pratique sur les isomorphismes.

Proposition E.9.4. *Soit $\varphi \in Hom(E_1, E_2)$ une isogénie de degré 1. Alors φ est un isomorphisme.*

Démonstration. Comme φ est de degré 1, on sait qu'alors $\overline{\mathbb{K}}(E_1) = \varphi^*\overline{\mathbb{K}}(E_2)$. $\varphi^* : \overline{\mathbb{K}}(E_2) \longrightarrow \overline{\mathbb{K}}(E_1)$ est donc un automorphisme de $\overline{\mathbb{K}}$-algèbres. En posant $\psi := (\phi^{*-1}(X_1), \phi^{*-1}(Y_1))$, on obtient que ψ est une isogénie telle que $\psi^* = \phi^{*-1}$, X_1 et Y_1 étant respectivement les fonctions abscisses et ordonnées de E_1. On en déduit que $(\varphi \circ \psi)^* = \varphi^* \circ \psi^* = \mathrm{id}_{\overline{\mathbb{K}}(E_1)}$ et que $(\psi \circ \varphi)^* = \mathrm{id}_{\overline{\mathbb{K}}(E_2)}$. En évaluant ces égalités en les fonctions abscisses et ordonnées, on en déduit que $\psi \circ \varphi = \mathrm{id}_{E_1}$ et $\varphi \circ \psi = \mathrm{id}_{E_2}$. Donc φ est un isomorphisme. □

Voici un résultat plus difficile qui est le point de départ des travaux de Vélu. Nous n'en donnerons pas la preuve puisqu'elle requiert la maitrise d'un peu de géométrie algébrique en genre quelconque qui est assez périphérique pour le travail que nous menons.

Théorème E.9.5 (admis)**.** *Soit G un sous-groupe fini d'une courbe elliptique E. Alors il existe un couple (φ, E') où E' est une courbe elliptique et φ une isogénie de $Hom(E, E')$ telle que $ker(\varphi) = G$. Le couple (φ, E') est unique à isomorphisme près.*

Remarque : Par propriété universelle du quotient, φ induit un isomorphisme de groupes entre E/G et E'. Ainsi, E/G a une structure de courbe elliptique (ce qui n'a rien d'évident a priori).

E.10 Courbes elliptiques sur $\mathbb{F}_q$.

E.10.1 Isogénie de Frobenius et théorème de Hasse.

Proposition E.10.1. *L'isogénie de Frobenius Fr_{p^n} est inséparable tandis que $[m] - Fr_{p^n}$ est séparable si et seulement si p ne divise pas m. En particulier, $[1] - Fr_q$ est séparable.*

Démonstration. Posons $\varphi = [m] - \mathrm{Fr}_{p^n}$. Si φ est inséparable alors φ s'écrit comme fonction de X^p d'après le corollaire E.4.3 et d'après la formule d'additions des points, il en est de même pour $\varphi + \mathrm{Fr}_{p^n} = [m]$, qui est donc inséparable. Réciproquement, si $[m]$ est inséparable alors $\varphi = [m] - \mathrm{Fr}_{p^n}$ l'est aussi en vertu du même argument (expression comme fonction de X^p et formule d'addition des points). Ainsi, φ est inséparable si et seulement si $[m]$ est inséparable.

Or, $[m]$ est inséparable si et seulement si elle s'écrit sous la forme $[m] = \phi \circ \mathrm{Fr}_p$ avec $\phi \in \mathrm{Hom}(\mathrm{Fr}_p(E), E)$, d'après le corollaire E.4.3. Si c'est le cas on a alors :

$$m^2 = \deg([m]) = \deg(\phi)\deg(\mathrm{Fr}_p) = p\deg(\phi)$$

donc $p|m$. Réciproquement, si $p|m$ alors $[m] = \left[\frac{m}{p}\right] \circ [p] = \left[\frac{m}{p}\right] \circ V_p \circ \mathrm{Fr}_p$ et donc $[m]$ est inséparable. Ceci termine la preuve. □

E.11 Critère pratique de supersingularité.

Nous donnons ensuite une formule alternative de comptage de points, bien moins utilisée en pratique pour le comptage de points que celle de Hasse mais utile pour déterminer si une courbe elliptique est supersingulière.

Lemme E.11.1. *Soit $\chi : \mathbb{F}_q^* \longrightarrow \{\pm 1\}$ l'unique caractère non trivial d'ordre 2 (morphisme de groupes à valeurs dans $\mathbb{C}$). Soit $x \in \mathbb{F}_q^*$. Alors $\chi(x) = 1$ si et seulement si x est un carré dans $\mathbb{F}_q^*$. En outre, dans $\mathbb{F}_q$ on a $\chi(x) = x^{\frac{q-1}{2}}$ pour tout $x \in \mathbb{F}_q^*$. Il y a par ailleurs $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^*$.*

Démonstration. Commençons par compter les carrés de $\mathbb{F}_q^*$. Soit $g : x \in \mathbb{F}_q^* \longmapsto x^2 \in \mathbb{F}_q^*$. Alors pour tout $y \in \mathrm{im}(g)$ (que l'on peut écrire $y = x^2$ (pour $x \in \mathbb{F}_q^*$), on a deux antécédants de y par g : x et $-x$, qui sont distincts car $p = \mathrm{car}(\mathbb{F}_q) \neq 2$. Le lemme des bergers donne donc que $2|\mathrm{im}(g)| = |\mathbb{F}_q^*| = q - 1$ donc il y a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^*$.

Si $x \in \mathbb{F}_q^*$ est un carré dans $\mathbb{F}_q^*$ alors $x = y^2$ pour un certain $y \in \mathbb{F}_q^*$. Donc $\chi(x) = \chi(y^2) = \chi(y)^2 = 1$. Donc $\ker(\chi)$ contient le groupe $\mathrm{im}(g)$ des carrés dans $\mathbb{F}_q^*$, qui est d'ordre $\frac{q-1}{2}$. D'après, le théorème de Lagrange, on a donc $\ker(\chi) = \mathrm{im}(g)$ ou $\ker(\chi) = \mathbb{F}_q^*$. Donc $\ker(\chi) = \mathrm{im}(g)$ puisque χ est non trivial. Donc seuls les carrés étant dans $\ker(\chi)$, on en déduit que $\chi(x) = 1$ si et seulement si x est un carré dans $\mathbb{F}_q^*$.

Enfin, d'après le théorème de Lagrange, tout élément de $\mathbb{F}_q^*$ est racine de $X^{q-1} - 1 = (X^{\frac{q-1}{2}} - 1)(X^{\frac{q-1}{2}} + 1)$, polynôme scindé dans $\mathbb{F}_q^*$. Donc il y a $\frac{q-1}{2}$ éléments $x \in \mathbb{F}_q^*$ vérifiant $x^{\frac{q-1}{2}} = 1$ et $\frac{q-1}{2}$

autres vérifiant $x^{\frac{q-1}{2}} = -1$. Si x est un carré, on écrit $x = y^2$ avec $y \in \mathbb{F}_q^*$ et on obtient $x^{\frac{q-1}{2}} = y^{q-1} = 1$. Comme il y a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q^*$, on en déduit donc que $x^{\frac{q-1}{2}} = 1$ si et seulement si x est un carré dans $\mathbb{F}_q^*$. Ainsi, dans $\mathbb{F}_q$: $\chi(x) = x^{\frac{q-1}{2}}$ pour tout $x \in \mathbb{F}_q^*$. □

Proposition E.11.2. *Posons $f(X) := X^3 + AX + B$ et étendons χ à $\mathbb{F}_q$ en posant $\chi(0) := 0$. Alors :*

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

Démonstration. On cherche à compter les couples $(x, y) \in \mathbb{F}_q^2$ tels que $f(x) = y^2$. Selon la valeur de x, cette équation a 0 solution si $f(x)$ n'est pas un carré dans $\mathbb{F}_q$, une solution si $f(x) = 0$ et 2 solutions si $f(x)$ est un carré dans $\mathbb{F}_q^*$. D'après le lemme précédent, le nombre de solutions est donc toujours égal à $1 + \chi(f(x))$. Sans omettre le point à l'infini $\mathcal{O}$, on obtient donc que :

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

□

Lemme E.11.3. *Notons pour tout $r \in \mathbb{N}^*$, A_{p^r} le coefficient devant X^{p^r-1} du polynôme $f(X)^{\frac{p^r-1}{2}} = (X^3 + AX + B)^{\frac{p^r-1}{2}}$. Alors on a $Tr(Fr_q) \equiv A_q\,[p]$.*

Démonstration. La proposition et le lemme qui précèdent assurent que dans $\mathbb{F}_q$, on a l'égalité :

$$|E(\mathbb{F}_q)| = 1 + q + \sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}}$$

En outre, le théorème de Hasse donne $|E(\mathbb{F}_q)| = 1 + q - \mathrm{Tr}(\mathrm{Fr}_q)$ et donc :

$$\mathrm{Tr}(\mathrm{Fr}_q) = -\sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}}$$

En outre, $\mathbb{F}_q^*$ est un groupe cyclique donc si l'on prend un générateur $\xi \in \mathbb{F}_q^*$ de $\mathbb{F}_q^*$, on obtient que pour tout $k \in \mathbb{N}$:

$$\sum_{x \in \mathbb{F}_q} x^k = \sum_{i=0}^{q-1} \xi^{ik} = \begin{cases} q-1 = -1 & \text{si } q-1 | k \\ \frac{\xi^{k(q-1)}-1}{\xi^k - 1} = 0 & \text{sinon} \end{cases}$$

Donc :

$$\mathrm{Tr}(\mathrm{Fr}_q) = -\sum_{x \in \mathbb{F}_q} A_q x^{q-1} = A_q$$

dans $\mathbb{F}_q$ et ainsi $\mathrm{Tr}(\mathrm{Fr}_q) \equiv A_q\,[p]$, comme annoncé. □

Théorème E.11.4. *E est supersingulière si et seulement si $A_p = 0$.*

Démonstration. On a vu dans la preuve du théorème de Hasse que :

$$\begin{aligned}[\mathrm{Tr}(\mathrm{Fr}_q)] &= [1] + [\deg(\mathrm{Fr}_q)] - [\deg([1] - \mathrm{Fr}_q)] = [1] + \mathrm{Fr}_q \circ V_p^n - ([1] - \mathrm{Fr}_q) \circ ([1] - V_p^n) \\ &= \mathrm{Fr}_q + V_p^n\end{aligned}$$

Donc $V_p^n = [\mathrm{Tr}(\mathrm{Fr}_q)] - \mathrm{Fr}_q$ donc E est supersingulière si et seulement si V_p^n est inséparable, ce qui équivaut à $p | \mathrm{Tr}(\mathrm{Fr}_q)$ d'après la proposition 3.8.1, ce qui équivaut à $A_q = 0$ d'après le lemme précédent. Il reste donc à montrer l'équivalence $A_q = 0 \iff A_p = 0$.

Or, pour $r \in \mathbb{N}^*$, on a :

$$f(X)^{\frac{p^{r+1}-1}{2}} = f(X)^{\frac{p^r-1}{2}} \left(f(X)^{\frac{p-1}{2}}\right)^{p^r}$$

Donc $A_{p^{r+1}} = A_p^{p^r} A_{p^r}$ et ainsi par une récurrence facile, on obtient que $A_q = A_p^{\frac{q-1}{p-1}}$ et on conclut facilement que $A_q = 0 \iff A_p = 0$. Ceci termine la preuve. □

F Preuves de la section 4.

F.1 Préliminaires d'analyse complexe : fonctions elliptiques.

Proposition F.1.1. *(proposition 4.1.5) Soit f une fonction elliptique par rapport à un réseau Λ. Alors :*

$$\sum_{\omega\in\mathbb{C}/\Lambda} res_\omega(f) = \sum_{\omega\in\mathbb{C}/\Lambda} ord_\omega(f) = 0$$

Démonstration. Soit $P := \{a + s\omega_1 + t\omega_2 \mid s,t \in [0,1[\}$ un parallélogramme fondammental de Λ ((ω_1,ω_2) étant une base de Λ orientée dans le sens direct) choisi de telle façon qu'aucun pôle de f ne se trouve sur P (c'est possible car les pôles de f sont isolés). Alors d'après la formule des résidus :

$$\sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{res}_\omega(f) = \sum_{\omega\in P} \mathrm{res}_\omega(f) = \frac{1}{2i\pi}\int_{\partial P} f(z)dz$$

où ∂P est parcouru dans le sens trigonométrique. On a donc :

$$\partial P = P_1^+ \cup P_2^+ \cup P_1^- \cup P_2^-$$

avec :

$$P_1^+ := [0,\omega_1], \quad P_1^- := [\omega_2+\omega_1,\omega_2], \quad P_2^+ := [\omega_1,\omega_1+\omega_2], \quad P_2^- := [\omega_2,0]$$

intervalles parcourus dans le sens de leurs bornes. Mais l'intégrale de f sur P_1^+ compense celle sur P_1^- par Λ-périodicité de f et, de même, celle de f sur P_2^+ compense celle sur P_2^-. Ainsi :

$$\sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{res}_\omega(f) = \frac{1}{2i\pi}\int_{\partial P} f(z)dz = 0$$

En outre, si ω est un pôle ou un zéro de f dans P alors f admet un développement en série entière au voisinage de ω de la forme :

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

où $m \in \mathbb{Z}^*$ est l'ordre de ω (de sorte que $a_m \neq 0$). Ainsi, au voisinage de ω :

$$f'(z) = \sum_{n=m}^{+\infty} n a_n(z-\omega)^{n-1}$$

D'où :

$$\frac{f'(z)}{f(z)} = \frac{\sum_{n=m}^{+\infty} n a_n(z-\omega)^{n-1}}{\sum_{n=m}^{+\infty} a_n(z-\omega)^n} = \frac{m}{z-\omega}\frac{1+\sum_{n=m+1}^{+\infty}\frac{na_n}{ma_m}(z-\omega)^{n-m}}{1+\sum_{n=m+1}^{+\infty}\frac{a_n}{a_m}(z-\omega)^{n-m}} \sim \frac{m}{z-\omega}$$

Donc $\mathrm{res}_\omega\left(\frac{f'}{f}\right) = m = \mathrm{ord}_\omega(f)$. Le résultat précédent appliqué à $\frac{f'}{f}$ (qui est elliptique par rapport à Λ) donne alors le résultat voulu :

$$\sum_{\omega\in\mathbb{C}/\Lambda} \mathrm{ord}_\omega(f) = 0$$

□

Proposition F.1.2. *(proposition 4.1.7) Soit f une fonction elliptique par rapport à un réseau Λ. Alors pour tout parallélogramme fondammental P de Λ :*

$$\sum_{\omega\in P} \omega \cdot ord_\omega(f) \in \Lambda$$

Démonstration. Considérons la fonction méromorphe $g : z \longmapsto z\frac{f'(z)}{f(z)}$. Soit $P := \{a + s\omega_1 + t\omega_2 \mid s,t \in [0,1[\}$ un parallélogramme fondammental de Λ ((ω_1,ω_2) étant une base de Λ orientée dans le sens direct) ne contenant aucun pôle de f. Alors la formule des résidus donne que :

$$\frac{1}{2i\pi}\int_{\partial P} g(z)dz = \sum_{\omega\in P} \mathrm{res}_\omega(g) \quad (1)$$

avec pour tout $\omega \in P$:

$$\mathrm{res}_\omega(g) = \omega \cdot \mathrm{ord}_\omega(f)$$

d'après un développement au voisinage de ω déjà vu dans la preuve de la proposition précédente. On découpe alors ∂P en :

$$\partial P = P_1^+ \cup P_2^+ \cup P_1^- \cup P_2^-$$

avec :

$$P_1^+ := [a, a+\omega_1], \quad P_1^- := [a+\omega_2+\omega_1, a+\omega_2], \quad P_2^+ := [a+\omega_1, a+\omega_1+\omega_2], \quad P_2^- := [a+\omega_2, a]$$

comme dans la proposition précédente. La Λ-périodicité de f assure que :

$$\begin{aligned}\int_{P_1^+} g(z)dz + \int_{P_1^-} g(z)dz &= \int_{P_1^+} z\frac{f'(z)}{f(z)}dz + \int_{P_1^-} z\frac{f'(z)}{f(z)}dz = \int_{P_1^+} z\frac{f'(z)}{f(z)}dz - \int_{P_1^+} (z+\omega_2)\frac{f'(z+\omega_2)}{f(z+\omega_2)}dz \\ &= \int_{P_1^+} z\frac{f'(z)}{f(z)}dz - \int_{P_1^+} (z+\omega_2)\frac{f'(z+\omega_2)}{f(z+\omega_2)}dz = \int_{P_1^+} z\frac{f'(z)}{f(z)}dz - \int_{P_1^+} (z+\omega_2)\frac{f'(z)}{f(z)}dz \\ &= -\omega_2 \int_{P_1^+} \frac{f'(z)}{f(z)}dz \quad (2)\end{aligned}$$

Montrons qu'alors $\int_{P_1^+} \frac{f'(z)}{f(z)}dz \in 2i\pi\mathbb{Z}$. Pour cela, on considère la fonction :

$$I : t \in [0,1] \longmapsto \exp\left(\int_{[a+t\omega_1]} \frac{f'(z)}{f(z)}dz\right) = \exp\left(\int_0^t \frac{f'(a+s\omega_1)}{f(a+s\omega_1)}ds\right)$$

I est dérivable et :

$$\forall t \in [0,1], \quad I'(t) = \frac{f'(a+t\omega_1)}{f(a+t\omega_1)} I(t)$$

donc pour tout $t \in [0,1]$, $\frac{d}{dt}\left(\frac{I(t)}{f(a+t\omega_1)}\right) = 0$. Ainsi :

$$\frac{I(0)}{f(a)} = \frac{I(1)}{f(a+\omega_1)} = \frac{I(1)}{f(a)}$$

Puis, $I(0) = I(1)$. D'où l'on tire que $\int_{P_1^+} \frac{f'(z)}{f(z)}dz \in 2i\pi\mathbb{Z}$, comme annoncé, puis par (2) :

$$\frac{1}{2i\pi}\left(\int_{P_1^+} g(z)dz + \int_{P_1^-} g(z)dz\right) \in \mathbb{Z}\omega_2$$

En vertu des mêmes arguments :

$$\frac{1}{2i\pi}\left(\int_{P_2^+} g(z)dz + \int_{P_2^-} g(z)dz\right) \in \mathbb{Z}\omega_1$$

Donc finalement (1) donne que $\sum_{\omega\in P} \omega \cdot \mathrm{ord}_\omega(f) \in \Lambda$. Si maintenant P' est un autre parallélogramme fondammental de Λ, alors $\sum_{\omega\in P'} \omega \cdot \mathrm{ord}_\omega(f)$ diffère de $\sum_{\omega\in P} \omega \cdot \mathrm{ord}_\omega(f)$ d'un élément de Λ donc nous venons en fait de montrer le résultat dans le cas général. □

F.2 Fonction $\mathcal{P}_\Lambda$ de Weierstrass et paramétrage des courbes elliptiques.

Proposition F.2.1. *Considérons la fonction définie sur $\mathbb{C}\setminus\Lambda$ définie par :*

$$\mathcal{P}_\Lambda(z) := \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Cette fonction est bien définie, paire et elliptique par rapport à Λ. En outre, la série de fonctions définissant $\mathcal{P}_\Lambda$ converge normalement sur tout compact de $\mathbb{C}\setminus\Lambda$. Cette fonction est appellée fonction de Weierstrass associée à Λ.

Démonstration. Soit $\mathcal{K} \subset \mathbb{C}\setminus\Lambda$ un compact. Alors la distance δ de $\mathcal{K}$ à Λ est non nulle et $\mathcal{K}$ est inclus dans une certaine boule $B(0,M)$ avec $M > 0$. Remarquons que pour tous $\omega \in \Lambda\setminus\{0\}$ et $z \in \mathcal{K}$:

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{z(2\omega - z)}{\omega^4\left(\frac{z}{\omega} - 1\right)^2}$$

De sorte que :

$$\forall z \in \mathcal{K},\, \omega \in \Lambda \setminus \{0\}, \quad \left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \frac{M(\delta + |\omega|)}{|\omega|^4 \left|\frac{z}{\omega} - 1\right|^2}$$

Mais :

$$\eta := \inf_{z \in \mathcal{K}} \min_{\omega \in \Lambda \cap B(0,2M)} \left|\frac{z}{\omega} - 1\right|$$

est atteint (comme minimisation d'une fonction continue sur un compact) et c'est une quantité strictement positive (car $\mathcal{K} \subset \mathbb{C} \setminus \Lambda$). On a donc :

$$\forall z \in \mathcal{K},\, \omega \in \Lambda \setminus \{0\}, \quad \left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \frac{M(\delta + |\omega|)}{|\omega|^4 \min\left(\eta^2, \frac{1}{4}\right)} \leq \frac{C}{|\omega|^3}$$

Pour une certaine constante $C > 0$ indépendante de z et de ω. On conclut alors à l'aide du lemme suivant :

Lemme F.2.2. *Pour tout $\alpha > 2$, $\left(\frac{1}{|\omega|^\alpha}\right)_{\omega \in \Lambda}$ est sommable.*

Démonstration. Soit (ω_1, ω_2) une base de Λ. Alors tout $\omega \in \mathbb{C} \setminus \Lambda$ peut s'écrire de façon unique sous la forme $\omega = k\omega_1 + l\omega_2$ avec $k, l \in \mathbb{Z}$ donc il s'agit de montrer que la famille $\left(\frac{1}{|k\omega_1 + l\omega_2|^\alpha}\right)_{(k,l) \in \mathbb{Z}^2 \setminus \{(0,0)\}}$ est sommable. Pour cela, on munit $\mathbb{C}$ de la norme Manhattan associée à (ω_1, ω_2) (qui est une $\mathbb{R}$-base de $\mathbb{C}$ rappelons-le), définie par :

$$\|z\| := \max(|z_1|, |z_2|)$$

pour tout $z := z_1\omega_1 + z_2\omega_2 \in \mathbb{C}$. Par équivalence des normes en dimension finie, on dispose de $\alpha > 0$ tel que $\|.\| \leq \alpha|.|$. Il suffit donc de montrer que $\left(\frac{1}{\max(|k|,|l|)^\alpha}\right)_{(k,l) \in \mathbb{Z}^2 \setminus \{(0,0)\}}$ est sommable. Or, on a pour tout $N \in \mathbb{N}$:

$$\sum_{\substack{(k,l) \in \mathbb{Z}^2 \setminus \{(0,0)\} \\ \max(|k|,|l|) \leq N}} \frac{1}{\max(|k|,|l|)^\alpha} = \sum_{n=1}^{N} \sum_{\substack{(k,l) \in \mathbb{Z}^2 \\ \max(|k|,|l|) = n}} \frac{1}{n^\alpha} = \sum_{n=1}^{N} \frac{8n}{n^\alpha} \leq 8\zeta(\alpha - 1)$$

Ce qui prouve la sommabilité. □

D'où la définition et la convergence normale de $\mathcal{P}_\Lambda$ sur tout compact $\mathcal{K} \subset \mathbb{C} \setminus \Lambda$.

Remarquons enfin que si $\omega \in \Lambda$, $z \in \mathbb{C} \setminus \Lambda$ et $h \in \mathbb{C}^*$ vérifie $z + h \in \mathbb{C} \setminus \Lambda$ alors :

$$\left|\frac{1}{h}\left(\frac{1}{(z+h-\omega)^2} - \frac{1}{(z-\omega)^2}\right) + \frac{2}{(z-\omega)^3}\right| = \frac{|h|^2}{|z-\omega|^2|z+h-\omega|^2}$$

Donc si d désigne la distance de z à Λ (qui est non nulle car Λ est fermé et que $z \notin \Lambda$), et si $h \in B\left(0, \frac{d}{2}\right)$, alors :

$$\left|\frac{1}{h}\left(\frac{1}{(z+h-\omega)^2} - \frac{1}{(z-\omega)^2}\right) + \frac{2}{(z-\omega)^3}\right| = \frac{|h|}{|z-\omega|^2\left(|z-\omega| - \frac{d}{2}\right)^2} \leq \frac{4|h|}{|z-\omega|^4}$$

Montrons que $\left(\frac{1}{(z-\omega)^3}\right)_{\omega \in \Lambda}$ et est sommable (ce qui donnera aussi par comparaison que $\left(\frac{1}{(z-\omega)^4}\right)_{\omega \in \Lambda}$ est sommable). Par équivalence des normes en dimension finie, nous avons vu que ceci revient à montrer que $\left(\frac{1}{\max(|z_1-k|,|z_2-l|)^3}\right)_{(k,l) \in \mathbb{Z}^2 \setminus \{(0,0)\}}$ est sommbale (z_1 et z_2 étant les coordonnées de z dans la base (ω_1, ω_2)). Or, $\max(|z_1 - k|, |z_2 - l|) \geq \max(|k|, |l|) - \max(|z_1|, |z_2|)$ pour tout $(k, l) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ donc les mêmes estimées que celles du lemme précédent permettent de conclure.

Donc en faisant $h \longrightarrow 0$, on obtient que :

$$\left|\frac{1}{h}(\mathcal{P}_\Lambda(z+h) - \mathcal{P}_\Lambda(z)) + \sum_{\omega \in \Lambda} \frac{2}{(z-\omega)^3}\right| \leq 4|h| \sum_{\omega \in \Lambda} \frac{1}{|z-\omega|^4} \underset{h \to 0}{\longrightarrow} 0$$

donc que $\mathcal{P}_\Lambda$ est dérivable au sens complexe, de dérivée donnée par :

$$\mathcal{P}'_\Lambda(z) = -\sum_{\omega \in \Lambda} \frac{2}{(z-\omega)^3}$$

Donc $\mathcal{P}$ est méromorphe.

$\mathcal{P}_\Lambda$ est clairement paire et $\mathcal{P}'_\Lambda$ est clairement Λ-périodique. Donc $\mathcal{P}'_\Lambda(z + \omega_1) = \mathcal{P}'_\Lambda(z)$ pour tout $z \in \mathbb{C} \setminus \Lambda$. Comme $\mathcal{P}_\Lambda(. + \omega_1) - \mathcal{P}_\Lambda$ est holomorphe sur $\mathbb{C} \setminus \Lambda$, qui est connexe, cette fonction est donc constante, disons égale à β. Mais alors en prenant $z = -\frac{\omega_1}{2}$, on trouve :

$$0 = \mathcal{P}_\Lambda\left(\frac{\omega_1}{2}\right) - \mathcal{P}_\Lambda\left(-\frac{\omega_1}{2}\right) = \beta$$

car $\mathcal{P}_\Lambda$ est paire. Donc $\mathcal{P}_\Lambda(z+\omega_1) = \mathcal{P}_\Lambda(z)$ pour tout $z \in \mathbb{C}\setminus\Lambda$ et pour la même raison $\mathcal{P}_\Lambda(z+\omega_2) = \mathcal{P}_\Lambda(z)$ pour tout $z \in \mathbb{C} \setminus \Lambda$, ce qui suffit à prouver la Λ-périodicité de $\mathcal{P}_\Lambda$. Donc $\mathcal{P}_\Lambda$ est elliptique par rapport à Λ. □

Proposition F.2.3. *(proposition 4.2.2)* $\mathbb{C}(\Lambda)$ *est un corps engendré par* $\mathcal{P}$ *et* $\mathcal{P}'$.

Démonstration. Le fait que $\mathbb{C}(\Lambda)$ soit un corps est clair. Soit $f \in \mathbb{C}(\Lambda)$. 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 $f\mathcal{P}'_\Lambda$ est paire, donc on peut supposer qu'en fait f est paire.

On peut alors utiliser le lemme suivant :

Lemme F.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 $\mathcal{P}_\Lambda(\omega)$ existe et $g := \mathcal{P}_\Lambda - \mathcal{P}_\Lambda(\omega)$ est une fonction elliptique paire, qui vérifie donc $\mathrm{ord}_\omega(g) \geq 2$ d'après le résultat précédent. Or, le seul pôle de $\mathcal{P}_\Lambda$, donc de g dans $\mathbb{C}/\Lambda$ est 0 et il est d'ordre 2 donc d'après la proposition 4.1.5, $\mathrm{ord}_\omega(g) = 2$. 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. $\mathrm{res}_\omega(f) \geq 2m+2$, 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 $\mathrm{res}_\omega(f) = 2m$. Si maintenant $\omega \in \Lambda$ alors on peut appliquer le même raisonnement à $g := \frac{1}{\mathcal{P}_\Lambda}$.

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 $z \in \mathbb{C} \setminus \Lambda$:

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

Nous avons vu précédemment que pour tout $\omega \in \mathbb{C} \setminus \Lambda$ tel que $\omega \equiv -\omega \mod \Lambda$, $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(\omega)$ 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 $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(\omega)$ n'ait qu'un seul pôle d'ordre 2 dnas $\mathbb{C}/\Lambda$ et la propositon 4.1.5 assurent que ω est un zéro d'ordre 1 de $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(\omega)$. 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 4.1.5 donc $\frac{f}{g}$ est elliptique et sans pôle ni zéro donc constante d'après la proposition 4.1.4. Ceci achève la preuve de la proposition. □

Proposition F.2.5. *(proposition 4.2.3)*

(i). $\mathcal{P}_\Lambda$ *admet pour développement en série de Laurent au voisinage de* 0 *:*

$$\mathcal{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1) s_{2n+2} z^{2n}$$

avec pour tout $n \geq 3$ *:*

$$s_n(\Lambda) = s_n := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^n}$$

qui est bien définie d'après le lemme F.2.2.

(ii). *Posons* $g_4(\Lambda) = g_4 := 60s_4(\Lambda)$ *et* $g_6(\Lambda) = g_6 := 140s_6(\Lambda)$. *Alors :*

$$\mathcal{P}'^2_\Lambda = 4\mathcal{P}^3_\Lambda - g_4\mathcal{P}_\Lambda - g_6$$

Démonstration. **(i).** Soit $r := \inf_{\omega\in\Lambda\setminus\{0\}} |\omega|$, qui est une quantité positive puisque $\Lambda\setminus\{0\}$ est un fermé qui ne contient pas 0. Pour tous $z \in B(0,r)$ et $\omega \in \Lambda\setminus\{0\}$, on dispose du développement :

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{\left(\frac{z}{\omega}-1\right)^2} - 1\right) = \frac{1}{\omega^2}\sum_{n=1}^{+\infty}\frac{(n+1)z^n}{\omega^n}$$

De sorte que :

$$\mathcal{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}}\sum_{n=1}^{+\infty}\frac{(n+1)z^n}{\omega^{n+2}}$$

Nous aimerions intervertir les deux sommes. Pour cela, on prouve que $\left(\frac{(n+1)z^n}{\omega^{n+2}}\right)_{\substack{n\in\mathbb{N}^*\\ \omega\in\Lambda\setminus\{0\}}}$ est sommable. On sait déjà que pour tout $\omega\in\Lambda\setminus\{0\}$, $\sum_{n\geq 1}\frac{(n+1)|z|^n}{|\omega|^{n+2}}$ converge de somme $\frac{1}{(|z|-|\omega|)^2} - \frac{1}{|\omega|^2}$. Des estimées analogues à celles obtenues au début de la preuve de la proposition précédente permettent en outre de montrer que $\left(\frac{1}{(|z|-|\omega|)^2} - \frac{1}{|\omega|^2}\right)_{\omega\in\Lambda\setminus\{0\}}$ est sommable. Donc $\left(\frac{(n+1)z^n}{\omega^{n+2}}\right)_{\substack{n\in\mathbb{N}^*\\ \omega\in\Lambda\setminus\{0\}}}$ est bien sommable d'après le théorème de sommation par paquets. D'où :

$$\mathcal{P}_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty}\sum_{\omega\in\Lambda\setminus\{0\}}\frac{(n+1)z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{+\infty}(n+1)s_{n+1}z^n$$

Or, comme $\omega\in\Lambda\setminus\{0\} \longmapsto -\omega\in\Lambda\setminus\{0\}$ est une bijection, on a pour tout $n\in\mathbb{N}$:

$$s_{2n+1} = \sum_{\omega\in\Lambda}\frac{1}{\omega^{2n+1}} = \sum_{\omega\in\Lambda}\frac{1}{(-\omega)^{2n+1}} = -\sum_{\omega\in\Lambda}\frac{1}{\omega^{2n+1}} = -s_{2n+1} = 0$$

Donc seuls les termes d'ordre pair interviennent dans la série et on obtient le résultat voulu.

(ii). Considérons $\varphi := \mathcal{P}'^2_\Lambda - 4\mathcal{P}^3_\Lambda + g_4\mathcal{P}_\Lambda + g_6$ qui est une fonction elliptique par rapport à Λ, n'admettant de pôles éventuels qu'aux points de Λ. En dérivant le développement en série entière précédent (ce qui donne bien $\mathcal{P}'_\Lambda$ au voisinage de 0) et en faisant un développement assymptotique à l'ordre 1 de φ au voisinage de 0, on obtient que 0 est un zéro de φ. Il en est alors de même pour tout autre point de Λ par Λ-périodicité de φ. Ainsi, φ est une fonction elliptique sans pôles, nulle au voisinage de zéro donc la proposition 4.1.4 assure que φ est identiquement nulle, ce qui donne le résultat voulu.

□

F.3 Courbes elliptiques et réseaux de $\mathbb{C}$

Théorème F.3.1 (paramétrage)**.** *(théorème 4.3.1)*

(i). *Si* Λ *est un réseau de* $\mathbb{C}$ *alors* $\Delta(\Lambda) := g_4(\Lambda)^3 - 27g_6(\Lambda)^2 \neq 0$. *En d'autre termes, la courbe* $E(\Lambda)$ *d'équation de Weierstrass :*

$$y^2 = 4x^3 - g_4(\Lambda)x - g_6(\Lambda)$$

définit bien une courbe elliptique sur $\mathbb{C}$.

(ii). *L'application :*

$$\begin{array}{rccc}\Phi : & \mathbb{C}/\Lambda & \longrightarrow & E(\Lambda)\\ & z & \longmapsto & (\mathcal{P}_\Lambda(z), \mathcal{P}'_\Lambda(z))\end{array}$$

est alors un isomorphisme additif de groupes (en prenant la convention $\Phi(0) = \mathcal{O}$*).*

Démonstration. **(i).** Soient (ω_1,ω_2) une base de Λ et $\omega_3 := \omega_1 + \omega_2$. Posons pour tout $i\in\{1,2,3\}$, $e_i := \mathcal{P}_\Lambda\left(\frac{\omega_i}{2}\right)$. Comme $\mathcal{P}'_\Lambda$ est Λ-périodique et impaire, on a pour tout $i\in\{1,2,3\}$:

$$\mathcal{P}'_\Lambda\left(\frac{\omega_i}{2}\right) = -\mathcal{P}'_\Lambda\left(-\frac{\omega_i}{2}\right) = -\mathcal{P}'_\Lambda\left(\frac{\omega_i}{2}\right) = 0$$

Comme $\mathcal{P}'_\Lambda$ admet dans $\mathbb{C}/\Lambda$ un seul pôle d'ordre 3, la proposition 4.1.5 assure que les $\frac{\omega_i}{2}$ sont des zéros d'ordre 1 de $\mathcal{P}'_\Lambda$. Or, $\mathcal{P}_\Lambda - e_i$ est admet un zéro d'ordre pair en $\frac{\omega_i}{2}$ d'après le lemme

F.2.4, donc exactement d'ordre 2 d'après la proposition 4.1.5 (puisque 0 est le seul pôle de $\mathbb{C}/\Lambda$ de $\mathcal{P}_\Lambda - e_i$ et qu'il est d'ordre 2). Ainsi, la fonction :

$$h : z \longmapsto 4\prod_{i=1}^{3}(\mathcal{P}_\Lambda(z) - e_i)$$

admet les mêmes zéros et même pôles que ${\mathcal{P}'}_\Lambda^2$ avec la même multiplicité. Il s'ensuit que $\frac{{\mathcal{P}'}_\Lambda^2}{h}$ est une fonction elliptique sans zéro ni pôle donc une fonction constante. En étudiant cette fonction au voisinage de zéro, on voit qu'en fait il y a égalité. Donc :

$${\mathcal{P}'}_\Lambda^2 = 4\prod_{i=1}^{3}(\mathcal{P}_\Lambda - e_i)$$

et donc d'après le premier point de la proposition 4.2.3, les e_i sont les racines du polynôme $4X^3 - g_4X - g_6$, de discriminant $\Delta(\Lambda)$. Mais la proposition 4.1.5 assure que $\mathcal{P}_\Lambda - e_i$ admet $\frac{\omega_i}{2}$ comme unique zéro dans $\mathbb{C}/\Lambda$ pour tout $i \in \{1,2,3\}$ donc que les e_i sont deux à deux distincts puisqu'il en est de même des $\frac{\omega_i}{2}$. Donc $\Delta(\Lambda) \neq 0$.

(ii). Montrons que Φ est surjective. Soit $(x,y) \in E(\Lambda)$. Comme $\mathcal{P}_\Lambda - x$ est une fonction effiptique non constante, elle admet un zéro $z \in \mathbb{C}/\Lambda$ d'après la proposition 4.1.4. Le point (ii). de la proposition 4.2.3 assure alors que $y^2 = {\mathcal{P}'}_\Lambda^2(z)$, donc que $y = \pm{\mathcal{P}'}_\Lambda(z)$. Quitte à changer z en $-z$, on peut supposer qu'en fait $y = \pm{\mathcal{P}'}_\Lambda(z)$ par parité de $\mathcal{P}_\Lambda$. On a alors $(x,y) = \Phi(z)$.

Montrons que Φ est injective. Soient $z_1, z_2 \in \mathbb{C}$ tels que $(\mathcal{P}_\Lambda(z_1), \mathcal{P}'_\Lambda(z_1)) = (\mathcal{P}_\Lambda(z_2), \mathcal{P}'_\Lambda(z_2))$. Alors on distingue deux cas :

Premier cas : Supposons que $z_1 \equiv -z_1 \mod \Lambda$. Alors le lemme F.2.4 assure que $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(z_1)$ admet un zéro d'ordre ≥ 2 en z_1. En outre, $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(z_1)$ n'admet qu'un seul pôle dans $\mathbb{C}/\Lambda$ qui est d'ordre 2, donc d'après la proposition 4.1.5, $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(z_1)$ ne peut admettre un autre zéro dans $\mathbb{C}/\Lambda$ et aisni $z_1 \equiv z_2 \mod \Lambda$.

Deuxième cas : Supposons que $z_1 \not\equiv -z_1 \mod \Lambda$. Alors $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(z_1)$ s'annule en trois points de $\mathbb{C}/\Lambda$: $z_1, -z_1$ et z_2. La proposition 4.1.5 assure alors que deux d'entre eux sont confondus, donc que $z_2 \equiv \pm z_1 \mod \Lambda$. Or, si par l'absurde $z_2 \equiv -z_1 \mod \Lambda$, alors par imarité de $\mathcal{P}'_\Lambda$:

$$\mathcal{P}'_\Lambda(z_2) = \mathcal{P}'_\Lambda(-z_1) = -\mathcal{P}'_\Lambda(z_1) = -\mathcal{P}'_\Lambda(z_2) = 0$$

Donc z_2 est zéro double de $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(z_1)$ et ceci contredit alors la proposition 4.1.5 (car $z_1 \not\equiv -z_1 \mod \Lambda$). Donc $z_1 \equiv z_2 \mod \Lambda$.

Terminons par la preuve de l'additivité. Soient $z_1, z_2 \in \mathbb{C}/\Lambda$. Il s'agit de voir que :

$$\Phi(z_1 + z_2) = \Phi(z_1) \oplus \Phi(z_2)$$

$\oplus$ désignant la loi de groupe sur la courbe elliptique $E(\Lambda)$ associée à Λ. Supposons dans un premier temps que z_1, z_2 et $-z_2$ distincts deux à deux. Alors $\mathcal{P}_\Lambda(z_1) \neq \mathcal{P}_\Lambda(z_1)$ car sinon $\mathcal{P}_\Lambda - \mathcal{P}_\Lambda(z_1)$ aurait 3 zéros distincts et un pôle d'ordre 2. Considérons donc la droite d'équation $y = ax + b$ qui relie $(\mathcal{P}_\Lambda(z_1), \mathcal{P}'_\Lambda(z_1))$ et $(\mathcal{P}_\Lambda(z_2), \mathcal{P}'_\Lambda(z_2))$ avec :

$$a := \frac{\mathcal{P}'_\Lambda(z_2) - \mathcal{P}'_\Lambda(z_1)}{\mathcal{P}_\Lambda(z_2) - \mathcal{P}_\Lambda(z_1)} \quad \text{et} \quad b := \frac{\mathcal{P}'_\Lambda(z_1)\mathcal{P}_\Lambda(z_2) - \mathcal{P}'_\Lambda(z_2)\mathcal{P}_\Lambda(z_1)}{\mathcal{P}_\Lambda(z_2) - \mathcal{P}_\Lambda(z_1)}$$

et la fonction elliptique $f : z \in \mathbb{C} \setminus \Lambda \longmapsto \mathcal{P}'_\Lambda(z) - (a\mathcal{P}_\Lambda(z) + b)$. f possède un pôle d'ordre 3 en 0 et des zéros en z_1 et z_2. Donc f admet un troisième zéro $z_3 \in \mathbb{C}/\Lambda$, distinct de z_1 et z_2, qui vaut $z_3 = -(z_1 + z_2)$ d'après la proposition 4.1.7. On a alors :

$$\mathcal{P}'_\Lambda(z_3) = a\mathcal{P}_\Lambda(z_3) + b \quad (1)$$

En outre, le polynôme $4X^3 - g_4(\Lambda)X - g_6(\Lambda) - (aX+b)^2$ possède exactement 3 racines qui sont $\mathcal{P}_\Lambda(z_1), \mathcal{P}_\Lambda(z_2)$ et $\mathcal{P}_\Lambda(z_3)$. Donc :

$$4X^3 - g_4(\Lambda)X - g_6(\Lambda) - (aX+b)^2 = 4\prod_{i=1}^{3}(X - \mathcal{P}_\Lambda(z_i))$$

En identifiant le coefficient en X^2, on obtient :

$$\mathcal{P}_\Lambda(z_1) + \mathcal{P}_\Lambda(z_2) + \mathcal{P}_\Lambda(z_3) = \frac{a^2}{4}$$

Donc :

$$\mathcal{P}_\Lambda(z_3) = -\mathcal{P}_\Lambda(z_1) - \mathcal{P}_\Lambda(z_2) + \frac{1}{4}\left(\frac{\mathcal{P}'_\Lambda(z_2) - \mathcal{P}'_\Lambda(z_1)}{\mathcal{P}_\Lambda(z_2) - \mathcal{P}_\Lambda(z_1)}\right)^2 \quad (2)$$

En outre par parité de $\mathcal{P}_\Lambda$:

$$\mathcal{P}_\Lambda(z_3) = \mathcal{P}_\Lambda(-(z_1+z_2)) = \mathcal{P}_\Lambda(z_1+z_2)$$

D'où, par (1) et (2) et d'après les formules d'additions sur une courbe elliptique :

$$\Phi(z_1+z_2) = \Phi(z_1) \oplus \Phi(z_2)$$

Cette formule se généralise quand $z_1 = z_2$ car on obtient alors en passant à la limite $z_2 \to z_1$ dans (2) :

$$\mathcal{P}_\Lambda(z_3) = -2\mathcal{P}_\Lambda(z_1) + \frac{1}{4}\left(\frac{\mathcal{P}''_\Lambda(z_1)}{\mathcal{P}'_\Lambda(z_1)}\right)^2$$

Et que $\mathcal{P}''_\Lambda$ peut facilement s'exprimer en fonction de $\mathcal{P}_\Lambda$ et $\mathcal{P}'_\Lambda$ à l'aide de l'équation :

$$\mathcal{P}'^{\,2}_\Lambda = 4\mathcal{P}^{\,3}_\Lambda - g_4(\Lambda)\mathcal{P}_\Lambda - g_6(\Lambda)$$

Enfin, quand $z_1 = -z_2$, on obtient que $z_1 + z_2 = 0$, donc que $\Phi(z_1+z_2) = \mathcal{O}$, puis que $\mathcal{P}_\Lambda(z_1) = \mathcal{P}_\Lambda(z_2)$ et $\mathcal{P}'_\Lambda(z_1) = -\mathcal{P}'_\Lambda(z_2)$ donc que $\Phi(z_1) \oplus \Phi(z_2) = \mathcal{O}$. Ainsi, Φ est bien un morphisme de groupes, comme annoncé.

□

F.4 Courbes elliptiques, réseaux de $\mathbb{C}$ et groupe modulaire.

F.4.1 j-invariant et groupe modulaire

Proposition F.4.1. **(i).** *Γ est engendré par :*

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(ii). *Soit :*

$$\mathcal{F} := \left\{ z \in \mathbb{H} \mid Re(z) \in \left[-\frac{1}{2}, \frac{1}{2}\right] \text{ et } |z| \geq 1 \right\}$$

Alors $\mathcal{F}$ est un domaine fondammental de Γ dans $\mathbb{H}$.

Démonstration. **(i).** D'après la proposition B.2.11, toute matrice $M \in \Gamma$ est de la forme :

$$M = P \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} Q$$

où $d_1, d_2 \in \mathbb{Z}^*$, $d_1 | d_2$ et où P et Q sont produits de matrices de transvection de la forme :

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = T^m \quad \text{ou} \quad \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} = (STS^{-1})^{-m}$$

avec $m \in \mathbb{Z}^*$. Ainsi, P et Q sont de déterminant 1 donc comme M est de déterminant 1 :

$$d_1 d_2 = \det \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} = 1$$

et ainsi, on peut prendre $d_1 = d_2 = 1$ puisque toute matrice de Γ s'identifie à son opposé. Donc S et T engendrent bien Γ.

(ii). Commençons par montrer que toute orbite de $\mathbb{H}$ sous l'action de Γ admet un élément de $\mathcal{F}$. Soit $z \in \mathbb{H}$. Alors pour tout $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, on a :

$$\mathrm{Im}(P \cdot z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

qui tend vers 0 quand $\max(|c|,|d|) \longrightarrow +\infty$. Donc on dispose de $N \in \mathbb{N}^*$ tel que pout tout $P \in \Gamma$ telle que $\max(|c|,|d|) \geq N$, $\mathrm{Im}(P \cdot z) < \mathrm{Im}(z)$. En considérant :

$$\max_{\max(|c|,|d|)\leq N} \frac{\mathrm{Im}(z)}{|cz+d|^2}$$

qui existe car il est indexé par un ensemble fini et qui est atteint par une certaine matrice $P_0 \in \Gamma$, on obtient alors un maximum global des parties imaginaires des éléments de l'orbite $\Gamma \cdot z$ de z : il suffit de prendre $P_0 \cdot z$. Mais alors pour un certain $m \in \mathbb{Z}$ bien choisi, $\zeta := (T^m P_O) \cdot z = P_0 \cdot z + m$ a même partie imaginaire que $P_0 \cdot z$ et une partie réelle dans $\left[-\frac{1}{2}, \frac{1}{2}\right]$. $\zeta \in \Gamma \cdot z$ est donc toujours de partie imaginaire maximale et donc :

$$\mathrm{Im}\,(S \cdot \zeta) = \frac{\mathrm{Im}(\zeta)}{|\zeta|^2} \leq \mathrm{Im}(\zeta)$$

Donc $|\zeta| \geq 1$. Ainsi, $\zeta \in \mathcal{F}$.

Montrons maintenant le résultat d'"unicité". Soient $z, z' \in \mathcal{F}$ dans la même orbite sous l'action de Γ. Alors on dispose de $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ telle que $z' = P \cdot z$. Quitte à inverser les rôles de z et de z' (en changeant P en P^{-1}), on peut supposer que $\mathrm{Im}(z) \leq \mathrm{Im}(z')$. Quitte à changer P en $-P$ (qui est égale à P dans Γ), on peut aussi supposer que $c \geq 0$.

Comme :

$$\mathrm{Im}(z') = \mathrm{Im}(P \cdot z) = \frac{\mathrm{Im}(z)}{|cz+d|^2} \geq \mathrm{Im}(z)$$

on a $|cz+d| \leq 1$. Or, $z \in \mathcal{F}$ donc :

$$\mathrm{Im}(z) = \sqrt{|z|^2 - \mathrm{Re}(z)^2} \geq \sqrt{1 - \frac{1}{4}} = \frac{\sqrt{3}}{2}$$

Et ainsi $|c\frac{\sqrt{3}}{2}| \leq \mathrm{Im}(cz+d) \leq |cz+d| \leq 1$ et donc $c = 0$ ou $c = 1$.

Premier cas : Si $c = 0$ alors $ad = 1$ donc quitte à changer P en $-P$, on peut supposer que $a = d = 1$. On a alors $z' = z + b$. Or, $z, z' \in \mathcal{F}$ donc $b \in \{-1, 0, 1\}$ et ainsi $z = z'$ ou z et z' sont dans les bords de $\mathcal{F}$ d'équations $\mathrm{Re} = \pm\frac{1}{2}$.

Deuxième cas : Supposons maintenant que $c = 1$. Alors :

$$|\Re(z) + d| = |\mathrm{Re}(z+d)| \leq |z+d| \leq 1$$

donc $d \in \{-1, 0, 1\}$ puisque $|\mathrm{Re}(z)| \leq \frac{1}{2}$. On distingue alors les trois sous-cas :

Premier sous-cas : Supposons que $d = 0$. Alors $bc = -1$ donc $b = -1$ puisque $c \geq 0$. Ainsi :

$$z' = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \cdot z = a - \frac{1}{z}$$

donc $\mathrm{Im}(z') = \frac{\mathrm{Im}(z)}{|z|^2}$ et ainsi $|z| = 1$ et $\mathrm{Im}(z') = \mathrm{Im}(z)$ puisque $\mathrm{Im}(z) \leq \mathrm{Im}(z')$ et $|z| \geq 1$. Puis, $\mathrm{Re}(z') = a - \mathrm{Re}(z)$ et $a \in\in \{-1, 0, 1\}$ puisque $\mathrm{Re}(z), \mathrm{Re}(z') \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. Si $a = \pm 1$ alors $\mathrm{Re}(z) = \mathrm{Re}(z') = \pm\frac{1}{2}$ donc $z = z' = \pm e^{i\frac{\pi}{3}} \in \partial\mathcal{F}$. Si $a = 0$ alors $\mathrm{Re}(z) = -\mathrm{Re}(z')$ donc $|z| = |z'| = 1$ et donc $z, z' \in \partial\mathcal{F}$.

Deuxième sous-cas : Supposons que $d = 1$. Alors :

$$1 \geq |z+1|^2 = |z|^2 + 2\mathrm{Re}(z) + 1 \geq 2(\mathrm{Re}(z) + 1)$$

et donc $\mathrm{Re}(z) = -\frac{1}{2}$ et $|z| = 1$ de sorte que $z = e^{\frac{2i\pi}{3}}$. En outre, $a - b = 1$ car $\det(P) = 1$. Ainsi :

$$z' = \frac{ae^{\frac{2i\pi}{3}} + a - 1}{e^{\frac{2i\pi}{3}} + 1} = e^{-\frac{i\pi}{3}}(ae^{\frac{2i\pi}{3}} + a - 1) = a - e^{-\frac{i\pi}{3}}$$

En regardant les parties réelle et imaginaire de z', on obtient alors que $z' = e^{\frac{2i\pi}{3}}$ ou $e^{\frac{i\pi}{3}}$. Ainsi, $z, z' \in \partial\mathcal{F}$.

Troisième sous-cas : Le cas $d = -1$ se traite comme le précédent.

□

F.4.2 Fonctions méromorphes à l'infini.

Proposition F.4.2. *Soit f une fonction méromorphe à l'infini sur $\mathbb{H}$ invariante sous l'action de Γ, c'est à dire telle que pour tout $z \in \mathbb{H}$ qui n'est pas pôle de f et pour tout $P \in \Gamma$, on ait $f(P \cdot z) = f(z)$. Alors :*

$$ord_\infty(f) + \frac{1}{3} ord_\rho(f) + \frac{1}{2} ord_i(f) + \frac{1}{2} \sum_{\omega \in \partial\mathcal{F} \setminus \{\rho, i, \rho+1\}} ord_\omega(f) + \sum_{\omega \in \mathring{\mathcal{F}}} ord_\omega(f) = 0$$

avec $\rho := e^{\frac{2i\pi}{3}}$.

Démonstration. Par commodité, on appellera pôle un zéro ou un pôle de f. Pour prouver le résultat nous allons intégrer la fonction $\frac{f'}{f}$ sur le contour $\mathcal{C}$ représenté en bleu sur la figure ci-dessous, qui n'est autre que le domaine fondammental du groupe modulaire tronqué (par le segment $[e-1, e]$ sur la figure) et modifié par des arcs de cercles autour des pôles de f situés sur le bord. Ce contour sera parcouru dans le sens trigonométrique et on fera tendre la partie imaginaire de e et les rayons des arcs de cercles autour des pôles au bord du contour vers 0.

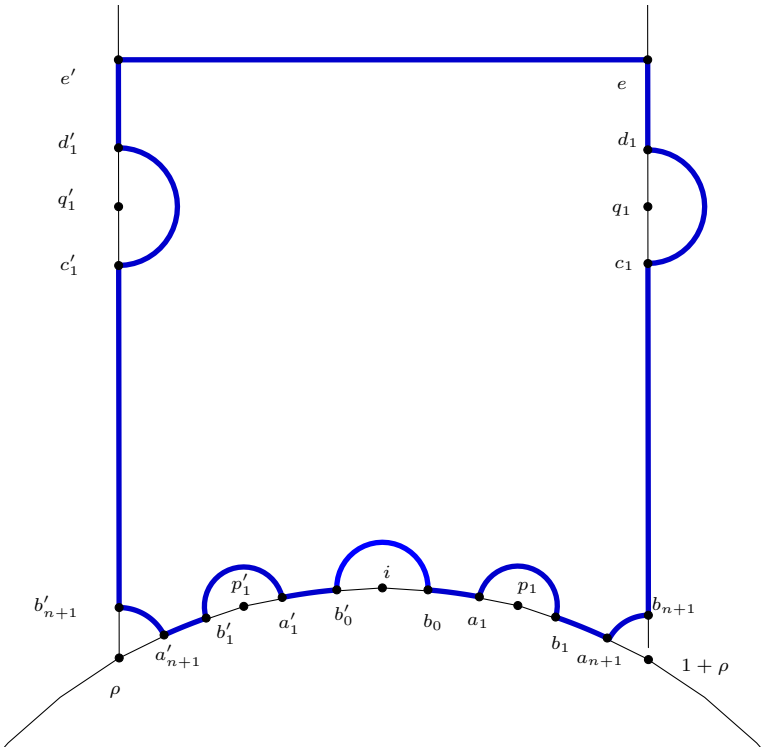


FIGURE 4 – Contour d'intégration $\mathcal{C}$ de $\frac{f'}{f}$

Nous noterons $p_0 := i, p_1, \cdots, p_n, p_{n+1} = \rho$ les pôles de l'arc de cercle inférieur d'abscisse positive et $\widehat{b'_0 b_0}, \widehat{a_1 b_1}, \cdots, \widehat{a_{n+1} b_{n+1}}$ les arcs de cercles respectifs tracés autour de ces pôles (voir figure ci-dessus). Nous noterons aussi $q_1, \cdots, q_m$ les pôles situés sur le segment $[b_{n+1}, e]$ et $\widehat{c_1 d_1}, \cdots, \widehat{c_m d_m}$ les arcs de cerles associés. Par hypothèse :

$$f(z) = f(S \cdot z) = f\left(-\frac{1}{z}\right) \quad \text{et} \quad f(z) = f(T^{-1} \cdot z) = f(z-1)$$

Donc $a'_i := -\overline{a_i}$ et $q'_j := q_j - 1$ sont des pôles de f de même ordre que a_i et b_j respectivement pour tous $i \in \{1, \cdots, n\}$ et $j \in \{1, \cdots, m\}$.On suppose qu'il n'y a pas de pôle de f sur le segment $[e, e']$ (on peut choisir e ainsi car les pôles de f sont isolés). On dispose ainsi de tous les pôles de f

Si l'on note $\omega_1, \cdots, \omega_l$, les pôles de f à l'intérieur du contour, on obtient par la formule des résidus et d'après un calcul déjà vu dans la preuve de la proposition 4.1.5 :

$$\int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = 2i\pi \sum_{k=1}^{l} \mathrm{ord}_{\omega_k}(f) \quad (\star)$$

On découpe maintenant l'intégrale :

$$\begin{aligned}\int_{\mathcal{C}} \frac{f'(z)}{f(z)}dz = \sum_{k=0}^{n} \left(\int_{[b_k,a_{k+1}]} \frac{f'(z)}{f(z)}dz + \int_{\widehat{a_{k+1}b_{k+1}}} \frac{f'(z)}{f(z)}dz + \int_{[a'_{k+1},b'_k]} \frac{f'(z)}{f(z)}dz + \int_{\widehat{b'_{k+1}a'_{k+1}}} \frac{f'(z)}{f(z)}dz \right) \\ + \int_{\widehat{b'_0b_0}} \frac{f'(z)}{f(z)}dz + \int_{[e,e']} \frac{f'(z)}{f(z)}dz + \int_{[b_{n+1},c_1]} \frac{f'(z)}{f(z)}dz + \int_{[c'_1,b'_{n+1}]} \frac{f'(z)}{f(z)}dz \\ + \sum_{k=1}^{m-1} \left(\int_{\widehat{c_kd_k}} \frac{f'(z)}{f(z)}dz + \int_{[d_{k+1},c_{k+1}]} \frac{f'(z)}{f(z)}dz + \int_{\widehat{d'_kc'_k}} \frac{f'(z)}{f(z)}dz + \int_{[c'_{k+1},d'_{k+1}]} \frac{f'(z)}{f(z)}dz \right) \\ + \int_{[d_m,e]} \frac{f'(z)}{f(z)}dz + \int_{[e',d'_m]} \frac{f'(z)}{f(z)}dz\end{aligned}$$

Par 1-périodicité de f, les termes en tilde (qui correspondent à la droite d'équation $x = -\frac{1}{2}$) se simplifient avec les autres (qui correspondent à la droite d'équation $x = \frac{1}{2}$) dans les deux dernière lignes de l'expression.

On traite maintenant le terme $\int_{[e,e']} \frac{f'(z)}{f(z)}dz$. On a en notant $R := \mathrm{Im}(e)$:

$$\begin{aligned}\int_{[e,e']} \frac{f'(z)}{f(z)}dz &= -\int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{f'(t+iR)}{f(t+iR)}dt = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{f'\left(\frac{1}{2i\pi}\ln(e^{2i\pi(t+iR)})\right)}{f\left(\frac{1}{2i\pi}\ln(e^{2i\pi(t+iR)})\right)}dt = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{f^{*'}(e^{2i\pi(t+iR)})}{2i\pi e^{2i\pi(t+iR)} f^*(e^{2i\pi(t+iR)})}dt \\ &= -\int_{\mathcal{C}(0,e^{-2\pi R})} \frac{f^{*'}(z)}{f^*(z)}dz\end{aligned}$$

$\mathcal{C}(0, e^{-2\pi R})$ étant le cercle de centre 0 et de rayon $e^{-2\pi R}$ parcouru dans le sens trigonométrique. Pour R assez grand, la formule des résidus donne que ceci est égal à $-2i\pi \mathrm{res}_0\left(\frac{f^{*'}}{f^*}\right) = -2i\pi \mathrm{ord}_0(f^*) = -2i\pi \mathrm{ord}_\infty(f)$, l'avant dernière égalité ayant déjà été vue au cours de la preuve de la proposition 4.1.5.

Il reste à traiter les termes de l'arc de cercle inférieur. Comme $f(z) = f(S \cdot z) = f\left(-\frac{1}{z}\right)$, on a :

$$f'(z) = -\frac{1}{z^2} f'\left(-\frac{1}{z}\right)$$

Donc pour $k \in \{0, \cdots, n\}$, on a en notant $\theta(b)_k$ et $\theta(b)_{k+1}$ les arguments principaux des nombres complexes b_k et a_{k+1} respectivement :

$$\begin{aligned}\int_{[b_k,a_{k+1}]} \frac{f'(z)}{f(z)}dz &= -\int_{[b_k,a_{k+1}]} \frac{f'(S\cdot z)}{z^2 f(S\cdot z)}dz = \int_{\theta(a)_{k+1}}^{\theta(b)_k} \frac{ie^{it} f'(e^{-it+i\pi})}{e^{2it} f(e^{-it+i\pi})}dt \\ &= \int_{\theta(a)_{k+1}}^{\theta(b)_k} \frac{-ie^{-it+i\pi} f'(e^{-it+i\pi})}{f(e^{-it+i\pi})}dt = \int_{\theta(a')_{k+1}}^{\theta(b')_k} \frac{ie^{it} f'(e^{it})}{f(e^{it})}dt = -\int_{[a'_{k+1},b'_k]} \frac{f'(z)}{f(z)}dz\end{aligned}$$

Il reste à traiter les termes $\int_{\widehat{a_{k+1}b_{k+1}}} \frac{f'(z)}{f(z)}dz$ et $\int_{\widehat{b'_{k+1}a'_{k+1}}} \frac{f'(z)}{f(z)}dz$. Or, autour de p_{k+1}, on a (d'après un calcul mené dans la preuve de la proposition 4.1.5) :

$$\frac{f'(z)}{f(z)} = \frac{\mathrm{ord}_{p_{k+1}}(f)}{z - p_{k+1}} + g(z - p_{k+1})$$

avec g holomorphe définie au voisinage de 0. Donc :

$$\int_{\widehat{a_{k+1}b_{k+1}}} \frac{f'(z)}{f(z)}dz = \int_{\widehat{a_{k+1}b_{k+1}}} \frac{\mathrm{ord}_{p_{k+1}}(f)}{z - p_{k+1}}dz + \int_{\widehat{a_{k+1}b_{k+1}}} g(z)dz$$

avec :

$$\left| \int_{\widehat{a_{k+1}b_{k+1}}} g(z)dz \right| \leq |b_{k+1} - a_{k+1}| \sup_{z\in[a_{k+1},b_{k+1}]} |g(z)|$$

Ce terme tend donc vers 0 lorsque le rayon r de l'arc de cercle $\widehat{a_{k+1}b_{k+1}}$ tend vers 0. En outre, on obtient en notant $\phi(a)_{k+1}$ et $\phi(b)_{k+1}$ les arguments principaux respectifs de $a_{k+1} - p_{k+1}$ et de $b_{k+1} - p_{k+1}$:

$$\int_{\widehat{a_{k+1}b_{k+1}}} \frac{dz}{z - p_{k+1}} = \int_{\pi(a)_{k+1}}^{\pi(b)_{k+1}} \frac{ie^{it}dt}{e^{it}} = i(\pi(b)_{k+1} - \pi(a)_{k+1}) \underset{r\to 0}{\longrightarrow} i\pi$$

Donc :

$$\int_{\overset{\frown}{a_{k+1}b_{k+1}}} \frac{f'(z)}{f(z)}dz \underset{r\to 0}{\longrightarrow} i\pi \mathrm{ord}_{p_{k+1}}(f)$$

Et d'après les mêmes calculs :

$$\int_{\overset{\frown}{b'_0a_0}} \frac{f'(z)}{f(z)}dz \underset{r\to 0}{\longrightarrow} i\pi \mathrm{ord}_{i}(f)$$

$$\int_{\overset{\frown}{a_{n+1}b_{n+1}}} \frac{f'(z)}{f(z)}dz \underset{r\to 0}{\longrightarrow} i\frac{\pi}{3} \mathrm{ord}_{\rho+1}(f)$$

$$\int_{\overset{\frown}{b'_{n+1}a'_{n+1}}} \frac{f'(z)}{f(z)}dz \underset{r\to 0}{\longrightarrow} i\frac{\pi}{3} \mathrm{ord}_{\rho}(f)$$

Comme $\mathrm{ord}_{\rho+1}(f) = \mathrm{ord}_{\rho}(f)$ par invariance de f par S, on obtient le résultat voulu en faisant tendre la partie imaginaire R de e vers l'infini et le rayon commun r des arcs de cercles autour des pôles vers 0 dans l'égalité $(\star)$. □

Lemme F.4.3. *(lemme 4.4.6)*

(i). *Pour tout $k \in \mathbb{N}^*$ la fonction donnée pour tout $\tau \in \mathbb{H}$ par :*

$$s_{2k}(\tau) := s_{2k}(\mathbb{Z} + \tau\mathbb{Z}) = \sum_{n,m\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(n+\tau m)^{2k}}$$

introduite dans la proposition 4.2.3 admet le développement de Fourier suivant sur $\mathbb{H}$ tout entier :

$$s_{2k}(\tau) = 2\zeta(2k) + \frac{2(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{+\infty}\left(\sum_{d|n} d^{2k-1}\right)e^{2in\pi\tau}$$

(ii). *j est méromorphe à l'infini, de développement de Fourier à l'infini donné par :*

$$j^*(z) = \frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n$$

où $(c_n)_{n\in\mathbb{N}}$ est une suite d'entiers.

Démonstration. **(i).** On part du développement classique suivant que l'on admettra [17] :

$$\pi\mathrm{cotan}(\pi\tau) = \sum_{n=-\infty}^{+\infty} \frac{1}{\tau+n}$$

pour tout $\tau \in \mathbb{C}\setminus\mathbb{Z}$. Or, pour tout $\tau \in \mathbb{H}$, puisque $\mathrm{Im}(\tau) > 0$, on a $|e^{2i\pi\tau}| < 1$ donc on a le développement suivant :

$$\pi\mathrm{cotan}(\pi\tau) = i\pi\frac{e^{i\pi\tau}+e^{-i\pi\tau}}{e^{i\pi\tau}-e^{-i\pi\tau}} = i\pi\frac{e^{2i\pi\tau}+1}{e^{2i\pi\tau}-1} = i\pi + \frac{2i\pi}{e^{2i\pi\tau}-1} = i\pi - 2i\pi\sum_{n=0}^{+\infty} e^{2in\pi\tau}$$

Ainsi pour tout $\tau \in \mathbb{H}$:

$$\frac{1}{\tau} + \sum_{n=0}^{+\infty}\left(\frac{1}{\tau-n}+\frac{1}{\tau+n}\right) = i\pi - 2i\pi\sum_{n=0}^{+\infty} e^{2in\pi\tau}$$

On dérive alors cette expression terme à terme $2k-1$ fois (un argument de convergence normale locale permet de justifier que l'on peut faire cela) :

$$(-1)^{2k-1}(2k-1)!\sum_{n=-\infty}^{+\infty}\frac{1}{(\tau+n)^{2k}} = -2i\pi\sum_{n=1}^{+\infty}(2in\pi)^{2k-1}e^{2in\pi\tau}$$

17. C'est un exrecice classique de classes préparatoires qui consiste à montrer que le membre de droite et le membre de gauche vérifient des propriétés analogues de parité, de périodicité et une équation fonctionnelle commune. On étudie alors leur différence comme une fonction réelle que l'on peut étendre à $\mathbb{R}$ par continuité. Cette fonction périodique admet un maximum et on peut montrer à l'aide de l'équation fonctionnelle que ce maximum est nul. De même pour le minimum. On conclut alors avec le théorème du prolongement analytique.

Ainsi :

$$\begin{aligned}
s_{2k}(\tau) &= \sum_{n,m\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(n+\tau m)^{2k}} = 2\zeta(2k) + \sum_{m\in\mathbb{Z}^*}\sum_{n=-\infty}^{+\infty} \frac{1}{(n+\tau m)^{2k}} \\
&= 2\zeta(2k) + \sum_{m=1}^{+\infty}\left(\sum_{n=-\infty}^{+\infty} \frac{1}{(n+\tau m)^{2k}} + \sum_{n=-\infty}^{+\infty} \frac{1}{(n-\tau m)^{2k}}\right) \\
&= 2\zeta(2k) + \sum_{m=1}^{+\infty}\left(\sum_{n=-\infty}^{+\infty} \frac{1}{(n+\tau m)^{2k}} + \sum_{n=-\infty}^{+\infty} \frac{1}{(-n-\tau m)^{2k}}\right) \\
&= 2\zeta(2k) + 2\sum_{m=1}^{+\infty}\sum_{n=-\infty}^{+\infty} \frac{1}{(n+\tau m)^{2k}} = 2\zeta(2k) + \frac{2(2i\pi)^{2k}}{(2k-1)!}\sum_{m=1}^{+\infty}\sum_{l=1}^{+\infty} l^{2k-1}e^{2ilm\pi\tau} \\
&= 2\zeta(2k) + \frac{2(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{+\infty}\left(\sum_{d|n} d^{2k-1}\right)e^{2in\pi\tau}
\end{aligned}$$

La dernière inégalité venant du fait que $(l^{2k-1}e^{2ilm\pi\tau})_{(m,l)\in(\mathbb{N}^*)^2}$ est sommable puisque $|e^{2i\pi\tau}| < 1$ et du fait que $(m,l) \in (\mathbb{N}^*)^2 \longmapsto (ml, l)$ est une bijection de $(\mathbb{N}^*)^2$ dans :

$$\{(n,d) \in (\mathbb{N}^*)^2 \mid d|n\}$$

C'est en fait exactement le résultat voulu.

(ii). Rappelons que :

$$j(\tau) = 1728\frac{g_4(\tau)^3}{\Delta(\tau)}$$

avec $\Delta(\tau) = g_4(\tau)^3 - 27g_6(\tau)^2$. Avec d'après la proposition 4.2.3 et le point précédent :

$$g_4(\tau) = 60s_4(\tau) = 60\left(2\frac{\pi^4}{90} + \frac{2(2\pi)^4}{6}h_4(\tau)\right) = \frac{(2\pi)^4}{12}\left(1 + 240h_4(\tau)\right)$$

$$g_6(\tau) = 140s_6(\tau) = 140\left(2\frac{\pi^6}{945} - \frac{2(2\pi)^6}{120}h_6(\tau)\right) = \frac{(2\pi)^6}{72}\left(1 - 504\sum_{n=1}^{+\infty}\left(\sum_{d|n} d^5\right)e^{2in\pi\tau}\right)$$

Avec :

$$h_4(\tau) = \sum_{n=1}^{+\infty}\left(\sum_{d|n} d^3\right)e^{2in\pi\tau} \quad \text{et} \quad h_6(\tau) = \sum_{n=1}^{+\infty}\left(\sum_{d|n} d^5\right)e^{2in\pi\tau}$$

D'où :

$$\Delta(\tau) = \frac{(2\pi)^{12}}{1728}\left(\left(1 + 240h_4(\tau)\right)^3 - \left(1 - 504h_6(\tau)\right)^2\right)$$

Montrons qu'en fait tous les coefficients du développement de $\left(1 + 240h_4(\tau)\right)^3 - \left(1 - 504h_6(\tau)\right)^2$ sont congrus à 0 modulo 1728. Commençons par remarquer que :

$$\left(1 + 240h_4(\tau)\right)^3 - \left(1 - 504h_6(\tau)\right)^2 \equiv 144(5h_4(\tau) + 7h_6(\tau))\,[1728]$$

Il reste donc à montrer que $5h_4(\tau) + 7h_6(\tau) \equiv 0[12]$, ce qui revient à montrer que cette expression est congrue à 0 modulo 3 et modulo 4 d'après le théorème des restes chinois. Or, on a $d^5 - d^3 = d^3(d-1)(d+1)$ qui est congru à 0 modulo 3 et 4 pour tout $d \in \mathbb{N}^*$ (ce qui s'obtient en discutant sur la parité de d et le reste de d modulo 3). Donc :

$$\sum_{d|n} d^3 \equiv \sum_{d|n} d^5\,[3] \quad \text{et} \quad \sum_{d|n} d^3 \equiv \sum_{d|n} d^5\,[4]$$

pour tout $n \in \mathbb{N}$, ce qui prouve le résultat annoncé. Ainsi, Δ admet un développement de Fourier à coefficients entiers. En outre, en regardant le coefficient hdevant $e^{2i\pi\tau}$, on voit que ce coefficient vaut $(2\pi)^{12}$:

$$\Delta(\tau) = (2\pi)^{12}e^{2i\pi\tau}\left(1 + \sum_{n=1}^{+\infty} a_n e^{2in\pi\tau}\right)$$

avec $(a_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}^{\mathbb{N}^*}$. En outre, on obtient par développement de g_4 que :

$$g_4(\tau)^3 = \frac{(2\pi)^{12}}{1728}\left(1 + \sum_{n=1}^{+\infty} b_n e^{2in\pi\tau}\right)$$

avec $(b_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}^{\mathbb{N}^*}$. Donc :

$$j(\tau) = 1728\frac{g_4(\tau)^3}{\Delta} = \frac{1 + \sum_{n=1}^{+\infty} b_n e^{2in\pi\tau}}{e^{2i\pi\tau}\left(1 + \sum_{n=1}^{+\infty} a_n e^{2in\pi\tau}\right)} = \frac{1}{e^{2i\pi\tau}} + \sum_{n=0}^{+\infty} c_n e^{2in\pi\tau}$$

avec $(c_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$. Donc pour tout $z \in D^*$:

$$j^*(z) = \frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n$$

□

Théorème F.4.4. *(théorème 4.4.7)*

(i). *La fonction j induit une surjection entre $\mathcal{F}$, le domaine fondammental du groupe modulaire dans $\mathbb{H}$ et $\mathbb{C}$. Deux éléments $\mathcal{F}$ ont la même image par j si et seulement si ils sont dans le bord de $\mathcal{F}$.*

(ii). *Toute courbe elliptique sur $\mathbb{C}$ peut ainsi être représentée par un groupe de la forme $\mathbb{C}/\Lambda$, où Λ est un réseau de $\mathbb{C}$.*

Démonstration. **(i).** D'après le lemme précédent, j est holomorphe à l'infini et que $\mathrm{ord}_\infty(j) = -1$. Si $c \in \mathbb{C}$ est fixé, il en est de même de $j - c$. Comme $j - c$ est invariante sous l'action du groupe modulaire, on peut appliquer la proposition précédente pour obtenir :

$$\frac{1}{3}\mathrm{ord}_\rho(f) + \frac{1}{2}\mathrm{ord}_i(j-c) + \frac{1}{2}\sum_{\omega\in\partial\mathcal{F}\setminus\{\rho,i,\rho+1\}} \mathrm{ord}_\omega(j-c) + \sum_{\omega\in\mathring{\mathcal{F}}} \mathrm{ord}_\omega(j-c) = 1$$

ce qui n'est possible que si $j - c$ admet au moins un zéro dans $\mathcal{F}$. j n'ayant pas de pôle dans $\mathcal{F}$, elle admet au plus 2 zéros (lorsque ces zéros sont dans le bord de $\mathcal{F}$) et un seul zéro sinon.

(ii). Soit maintenant E une courbe elliptique sur $\mathbb{C}$. A isomorphisme près, son équation de Weierstrass s'écrit :

$$y^2 = 4x^3 - Ax - B$$

avec $A, B \in \mathbb{C}$. On dispose alors de $\tau \in \mathcal{F}$ tel que $j(\tau) = j(E)$. On a alors :

$$\frac{g_4(\Lambda_\tau)^3}{g_4(\Lambda_\tau)^3 - 27g_6(\Lambda_\tau)^2} = \frac{A^3}{A^3 - 27B^2} \quad (\star)$$

avec $\Lambda_\tau := \mathbb{Z} + \tau\mathbb{Z}$. Distinguons deux cas :

Premier cas : Si $j(E) = 0$ alors $A = g_4(\Lambda_\tau) = 0$ et $B, g_6(\Lambda_\tau) \neq 0$ (puisque E est une courbe elliptique donc de discriminant non nul et que $\Delta(\Lambda_\tau) \neq 0$ d'après le théorème 4.3.1). On considère alors $\alpha \in \mathbb{C}^*$ une racine 6-ième de $\frac{g_6(\Lambda_\tau)}{B}$. On sait qu'alors $g_6(\alpha\Lambda_\tau) = \frac{g_6(\Lambda_\tau)}{\alpha^6} = B$ et que $g_4(\alpha\Lambda_\tau) = \frac{g_4(\Lambda_\tau)}{\alpha^4} = 0 = A$. Donc $\mathbb{C}/\alpha\Lambda_\tau \approx E$ d'après le théorème 4.3.1.

Deuxième cas : Si $j(E) \neq 0$ alors $A \neq 0$ et $g_4(\Lambda_\tau) \neq 0$ on considère $\beta \in \mathbb{C}^*$ une racine 4-ième de $\frac{g_4(\Lambda_\tau)}{A}$. On a alors $g_4(\beta\Lambda_\tau) = A$ et donc par $(\star)$:

$$g_6(\beta\Lambda_\tau)^2 = \frac{1}{27}\left(g_4(\Lambda_\tau)^2 - \frac{g_4(\Lambda_\tau)^2(A^3 - 27B^2)}{A^3}\right) = B^2$$

Donc $g_6(\beta\Lambda_\tau) = \pm B$. Quitte à changer β en $i\beta$, ce qui ne change pas $g_4(\beta\Lambda_\tau) = \frac{g_4(\Lambda_\tau)}{\beta^4}$, on peut supposer que $g_6(\beta\Lambda_\tau) = B$. Donc $\mathbb{C}/\beta\Lambda_\tau \approx E$ d'après le théorème 4.3.1.

□

F.5 Courbes elliptiques, réseaux de $\mathbb{C}$ et isogénies.

Théorème F.5.1. **(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 f sur $\mathbb{C}$, s'annulant en 0 et vérifiant :*

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

(ii). *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 dans le théorème 4.3.1, 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 bien définie et c'est une bijection.

Démonstration. **(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 $f(0) = 0$ et :

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

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

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

Donc f' est une fonction holomorphe et elliptique donc constante d'après la proposition 4.1.4. On dispose donc de $\alpha \in \mathbb{C}$ tels que $f(z) = \alpha z + f(0) = \alpha z = \phi_\alpha(z)$ pour tout $z \in \mathbb{C}$.

(ii). Pour prouver que l'application F est bien définie, il s'agit de voir que $\Phi_2^{-1} \circ \varphi \circ \Phi_1$ est holomorphe pour toute isogénie $\varphi \in \mathrm{Hom}(E_1, E_2)$. Il suffit pour cela de vérifier que Φ_2^{-1} est suffisamment régulière, plus précisément différentiable au sens complexe. Pour cela, il s'agit de voir que E_2 est une surface de Riemann (c'est à dire une variété différentielle complexe de dimension 1) et que Φ_2^{-1} est un difféomorphisme au sens complexe entre E_2 et $\mathbb{C}/\Lambda_2$ en appliquant le théorème d'inversion globale [18]. Nous ne présentons ici que des arguments heuristiques, vrais dans le cas réel en admettant que tout se généralise bien dans le cas complexe. Considérons :

$$P_2 := Y^2 - 4X^3 - A_2X - B_2$$

le polynôme de Weierstrass associé à E_2. E_2 est la courbe d'équation $P_2(x, y) = 0$ et le gradient de P_2 s'écrit :

$$\nabla P_2(X, Y) = (-12X^2 - A_2, 2Y)$$

qui ne s'annule en aucun point de E_2 puisque sinon $4X^3 + A_2X + B_2$ et sa dérivée $12X^2 + A_2$ aurait un zéro commun, et donc le discriminant de la courbe serait nul. Ceci justifie le fait que E_2 soit une variété complexe de dimension 1. En outre :

$$\mathcal{P}'^2_{\Lambda_2} = 4\mathcal{P}^3_{\Lambda_2} + A_2\mathcal{P}_{\Lambda_2} + B_2$$

Donc en dérivant cette relation, il vient :

$$2\mathcal{P}'_{\Lambda_2}\mathcal{P}''_{\Lambda_2} = 12\mathcal{P}'_{\Lambda_2}\mathcal{P}^2_{\Lambda_2} + A_2\mathcal{P}'_{\Lambda_2}$$

Donc en simplifiant par $\mathcal{P}'_{\Lambda_2}$ en dehors des zéros de cette fonction et en appliquant le théorème du prolongement analytique pour étendre cette égalité aux zéros de $\mathcal{P}'_{\Lambda_2}$, on obtient que :

$$2\mathcal{P}''_{\Lambda_2} = 12\mathcal{P}^2_{\Lambda_2} + A_2$$

Donc si $\Phi_2'(z) = (\mathcal{P}'_{\Lambda_2}(z), \mathcal{P}''_{\Lambda_2}(z)) = 0$ alors $(\mathcal{P}_{\Lambda_2}(z), \mathcal{P}'_{\Lambda_2}(z))$ est un point de E_2 en lequel ∇P_2 s'annule, ce qui est impossible. Donc la différentielle de Φ_2 est en tout point un isomorphisme $\mathbb{C}$-linéaire entre $\mathbb{C}$ et l'espace tangent en ce point de E_2 et de plus Φ_2 est bijective donc on peut

18. Il semble que les résultats et le formalisme des variétés différentielles réelles qui font l'objet du cours de période 1 se généralise en complexe. Toutefois nous n'introduirons pas la théorie des surfaces de Riemann ici car ce n'est pas le coeur du sujet.

appliquer le théorème d'inversion globale pour obtenir que Φ_2 est un difféomorphisme au sens complexe. D'où la bonne définition de F.
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 est clair que $F \circ G = G \circ F = \mathrm{id}_{\mathrm{Hol}_0(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)}$. 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 :

$$\Phi_2 \circ f \circ \Phi_1^{-1}(P) = (\mathcal{P}_{\Lambda_2}(f(z)), \mathcal{P}'_{\Lambda_1}(f(z))) = (\mathcal{P}_{\Lambda_2}(\alpha z), \mathcal{P}'_{\Lambda_2}(\alpha z))$$

Or, comme $\alpha\Lambda_1 \subset \Lambda_2$, $z \longmapsto \mathcal{P}_{\Lambda_2}(\alpha z)$ et $z \longmapsto \mathcal{P}'_{\Lambda_2}(\alpha z)$ sont Λ_1-périodiques et méromorphes donc elliptiques par rapport à Λ_1. On en déduit grâce à la proposition 4.2.2 que ce sont des fractions rationnelles en $\mathcal{P}_{\Lambda_1}$ et $\mathcal{P}'_{\Lambda_1}$. En outre, il est clair que $\Phi_2 \circ f \circ \Phi_1^{-1}$ envoie $\mathcal{O}$ sur $\mathcal{O}$, ce qui achève de montrer que $\Phi_2 \circ f \circ \Phi_1^{-1}$ est une isogénie. D'où la bonne définition de G et la bijectivité de F. □

F.6 Polynômes modulaires.

F.6.1 Matrices primitives et isogénies.

Proposition F.6.1. *(proposition 4.6.3) 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 Γ par multiplication à gauche.

Démonstration. Soit $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in P_n$. Soient $g := \frac{c}{\mathrm{pgcd}(a,c)}$ et $h := -\frac{a}{\mathrm{pgcd}(a,c)}$, 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 :

$$Q := \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \Gamma$$

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 Γ.

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 Γ. Alors on dispose de $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ telles 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 Γ). 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 Γ. □

Proposition F.6.2. *(proposition 4.6.4) Le groupe $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ est cyclique d'ordre n si et seulement si $P \in P_n$.*

Démonstration. On ne traite que le cas où n est un nombre premier p, plus simple d'un point de vue arithmétique. En fait, c'est le seul cas qui nous servira en pratique.

$\Longrightarrow$ Supposons $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ cyclique d'ordre p et écrivons $P := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a alors :

$$\omega_1 = a\omega_3 + b\omega_4 \quad \text{et} \quad \omega_2 = c\omega_3 + d\omega_4$$

Donc pour $k, l \in \mathbb{Z}$ fixés, $k\omega_3 + l\omega_4 \equiv 0 \bmod \Lambda_1$ si et seulement si il existe $m, q \in \mathbb{Z}$ tels que $k\omega_3 + l\omega_4 = m\omega_1 + q\omega_2$ i.e. tels que :

$$k = am + cq \quad \text{et} \quad l = bm + dq \quad (\star)$$

Or, comme $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ est d'ordre p, $p(\omega_3 + \omega_4) = 0$, donc il existe $m, q \in \mathbb{Z}$ tels que :

$$p = am + cq \quad \text{et} \quad p = bm + dq$$

Donc $\text{pgcd}(a, c)|p$ et $\text{pgcd}(b, d)|p$. Donc ces nombres valent 1 ou p. Si par l'absurde ces deux nombres valent p alors par $(\star)$, les seuls $k, l \in \mathbb{Z}$ tels que $k\omega_3 + l\omega_4 \equiv 0 \bmod \Lambda_1$ sont des multiples de p et il s'ensuit alors que $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ est d'ordre au moins p^2 ce qui n'est pas le cas. Il s'ensuit que $\text{pgcd}(a, c) = 1$ ou $\text{pgcd}(b, d) = 1$, donc que P est une matrice primitive.

Comme toute $\mathbb{R}$-base de $\mathbb{C}$ dont la matrice de passage à partir de (ω_1, ω_2) est dans Γ reste une base de Λ_1, on peut supposer, quitte à changer de base que $P \in R_n$ (avec $n = \det(P)$). On a donc $c = 0$ et $0 \leq b < a$. Dans ce cas, il est aisé de voir que les $l\omega_4$ pour $l \in \{0, \cdots, d-1\}$ et $k\omega_3 + l\omega_4$ pour $k \in \{1, \cdots, a-1\}$ et $l \in \{0, \cdots, d-1\}$ ont des classes d'équivalences distinctes modulo Λ_1 et qu'il n'y en a pas d'autres. Il s'ensuit que $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ contient au $ad = \det(P)$ éléments distincts donc $\det(P) = p$ et $P \in R_p$.

$\Longleftarrow$ Si $P \in P_p$ alors quitte à changer de base, on peut supposer comme précédemment que $P \in R_p$. Donc $P = \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}$ avec $i \in \{0, \cdots, p-1\}$ ou $P = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Dans le premier cas $\frac{1}{\alpha}\Lambda_2/\Lambda_1$ est cyclique d'ordre p engendré par ω_3 et dans le deuxième cas il en est de même mais il faut prendre ω_4 comme générateur. □

F.6.2 Le polynôme modulaire.

Proposition F.6.3. *Φ_n est à coefficients dans $\mathbb{Z}[j]$.*

Démonstration. On ne prouve le résultat que dans le cas où n est un nombre premier, noté p.

Les coefficients de Φ_p sont des polynômes symétriques en $j \circ P$ pour $P \in R_p$. En outre, si $P \in R_n$ et $Q \in \Gamma$ alors $PQ \in P_n$ et donc on dispose de $P' \in R_p$ et de $Q' \in \Gamma$ tellles que $Q'P' = PQ$, de sorte que $j \circ P \circ Q = j \circ Q' \circ P' = j \circ P'$. Puis, si $P_2 \in R_p$ vérifie $Q_2'P' = P_2Q_2$ avec $Q_2, Q_2' \in \Gamma$ alors P_2 et P sont dans la même orbite sous l'action de Γ et donc $P = P_2$ d'après la proposition 4.6.3. 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 Γ.

En outre, on a vu dans le lemme 4.4.6 que pour tout $\tau \in \mathbb{H}$:

$$j(\tau) = \frac{1}{e^{2i\pi\tau}} + \sum_{k=0}^{+\infty} c_k e^{2ik\pi\tau}$$

Donc si $P := \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in R_p$ alors :

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

avec $\zeta_d := e^{\frac{2i\pi}{d}}$. Donc :

$$(j \circ P)^*(z) = \sum_{k=-1}^{+\infty} c_k z^{\frac{ak}{d}}\zeta_d^{kb} \quad (\star)$$

en couvenant que $c_{-1} = 1$. Or, $\Phi_p(X) = \prod_{P \in R_p}(X - j \circ P)$ donc les coefficients de Φ_p sont des fonctions méromorphes à l'infini (de pôle à l'infini d'ordre au plus $|R_p|$) développables en puissances de $z^{\frac{1}{p}}$ et dont les coefficients sont dans $\mathbb{Z}[\zeta_p]$.

Ecrivons explicitement le développement de ces fonctions. Pour cela, on énumère R_p :

$$R_p := \left\{ M_k := \begin{pmatrix} a_k & b_k \\ 0 & d_k \end{pmatrix} \mid k \in \{0, \cdots, p\} \right\}$$

avec $a_k = 1$, $b_k = k$ et $d_k = p$ pour $k \in \{0, \cdots, p-1\}$ et $a_k = p$, $b_k = 0$ et $d_k = 1$ pour $k = p$. Ainsi, pour tout $k \in \{0, \cdots, p+1\}$, le développement à l'infini coefficient devant X^k de Φ_n s'écrit pour $z \in D*$:

$$\begin{aligned}
f_k^*(z) &= (-1)^{p+1-k} \sum_{1 \le m_1 < \cdots < m_k \le p+1} \prod_{s=1}^{k} (j \circ M_{m_s})^*(z) \\
&= (-1)^{p+1-k} \sum_{1 \le m_1 < \cdots < m_k \le p+1} \prod_{s=1}^{k} \left(\sum_{l=-1}^{+\infty} c_l z^{\frac{a_{m_s} l}{d_{m_s}}} \zeta_{d_{m_s}}^{l b_{m_s}} \right) \\
&= (-1)^{p+1-k} \sum_{1 \le m_1 < \cdots < m_k \le p+1} \sum_{l_1, \cdots, l_k \ge -1} \prod_{s=1}^{k} c_{l_s} z^{\frac{a_{m_s} l}{d_{m_s}}} \zeta_{d_{m_s}}^{l_s b_{m_s}} \\
&= (-1)^{p+1-k} \sum_{l_1, \cdots, l_k \ge -1} \sum_{1 \le m_1 < \cdots < m_k \le p+1} \prod_{s=1}^{k} c_{l_s} z^{\frac{a_{m_s} l_s}{d_{m_s}}} \zeta_{d_{m_s}}^{l_s b_{m_s}} \\
&= (-1)^{p+1-k} \sum_{l_1, \cdots, l_k \ge -1} \prod_{s=1}^{k} \left(\sum_{m=1}^{p+1} c_{l_s} z^{\frac{a_m l_s}{d_m}} \zeta_{d_m}^{l_s b_m} \right) \\
&= (-1)^{p+1-k} \sum_{l_1, \cdots, l_k \ge -1} \prod_{s=1}^{k} \left(c_{l_s} z^{p l_s} + c_{l_s} z^{\frac{l_s}{p}} \sum_{b=0}^{p-1} \zeta_p^{l_s b} \right)
\end{aligned}$$

Les développements et interversions de sommes étant légales en vertu d'un argument de sommabilité qui s'appuie sur les calculs précédents en remplaçant z par son module. Comme :

$$\sum_{b=0}^{p-1} \zeta_p^{lb} = \begin{cases} p & \text{si } p | l \\ 0 & \text{sinon} \end{cases}$$

on en déduit que seules les puissances entières de z interviennent dans le développement de f_k^* [19] et que les coefficients sont entiers. Comme les f_k sont invariantes sous l'action de Γ, on déduit de la proposition 4.6.5 que f_k est un polynôme en j à coefficients entiers. Ceci donne le résultat voulu. □

Proposition F.6.4 (relation de Kronecker)**.** *On a pour tout nombre premier p :*

$$\Phi_p(X, Y) \equiv (X - Y^p)(X^p - Y) \, [p]$$

Démonstration. Soit p un nombre premier. On sait alors que :

$$R_p = \left\{ M_k := \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix} \mid k \in \{0, \cdots, p-1\} \right\} \cup \left\{ M_p := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Donc d'après le développement de Fourier de j établi dans le lemme 4.4.6, on a pour tout $k \in \{0, \cdots, p-1\}$:

$$j \circ M_k(\tau) = j\left(\frac{\tau + k}{p}\right) = \frac{1}{e^{\frac{2i\pi\tau}{p}} e^{\frac{2ik\pi}{p}}} + \sum_{n=0}^{+\infty} c_n \left(e^{\frac{2i\pi\tau}{p}} e^{\frac{2ik\pi}{p}} \right)^n$$

Donc pour $k \in \{0, \cdots, p-1\}$ fixé, $j \circ M_k$ admet un développement à l'infini qui s'écrit (pour $z = \frac{1}{2i\pi} \ln(\tau) \to 0$) :

$$(j \circ M_k)^*(z) = \frac{1}{z^{\frac{1}{p}} \zeta_p^k} + \sum_{n=0}^{+\infty} c_n z^{\frac{n}{p}} \zeta_p^{kn} = \frac{\zeta_p^{p-k}}{z^{\frac{1}{p}}} + \sum_{n=0}^{+\infty} c_n z^{\frac{n}{p}} \zeta_p^{kn}$$

avec $\zeta_p := e^{\frac{2i\pi}{p}}$. Adoptons la notation $f^*(z) \equiv g^*(z) \, [1 - \zeta_p]$ lorsque le développement de f^* et g^* en puissances de $\frac{1}{z^{\frac{1}{p}}}$ est à coefficients dans $\mathbb{Z}[\zeta_p]$ et que tous ces coefficients sont congrus modulo $1 - \zeta_p$ (et de même modulo p). Comme $\zeta_p \equiv 1 \, [1 - \zeta_p]$, on a :

$$(j \circ M_k)^*(z) \equiv \frac{1}{z^{\frac{1}{p}}} + \sum_{n=0}^{+\infty} c_n z^{\frac{n}{p}} \, [1 - \zeta_p]$$

19. Ce résultat devient faux lorsque n n'est plus un nombre premier. Nous ne savons pas si [5] utilise ce fait de façon générale mais il se débarasse des puissances fractionnaires de z au cours de sa preuve page 55 de façon assez mystérieuse, l'action du groupe de Galois de $\mathbb{Q}[\zeta_p]/\mathbb{Q}$ ne semblant pas suffisante pour éliminer ces termes, mais seulement pour prouver que les coefficients qui se trouvent devant sont entiers. Pour plus de clarté nous nous sommes donc restreint au cas où n est premier car c'est le seul cas intéressant en pratique pour l'implémentation de l'algorithme de Satoh.

Puis, pour $z \in D^*$ au voisinage de 0 :

$$(j \circ M_p)^*(z) = j^*(z^p) = \frac{1}{z^p} + \sum_{n=0}^{+\infty} c_n z^{np} \equiv \frac{1}{z^p} + \sum_{n=0}^{+\infty} c_n^p z^{np} \equiv \left(\frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n\right)^p \ [p]$$

Or, en réécrivant l'équation $\zeta_p^p - 1 = 0$ en $(1-(1-\zeta_p))^p - 1 = 0$ et en développant avec la formule du binôme de Newton, on obtient que :

$$(1-\zeta_p)\sum_{k=2}^{p}(-1)^{k-1}\binom{p}{k}(1-\zeta_p)^k = p$$

donc que $1-\zeta|p$. Il s'ensuit que ce sui est congru modulo p, est congru modulo $1-\zeta_p$. D'où, pour $z \in D^*$ au voisinage de 0 :

$$\begin{aligned}\Phi_p(X, j^*(z)) = \prod_{i=0}^{p}(X - (j\circ M_i)^*(z)) &\equiv \left(X - \left(\frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n\right)^p\right)\left(X - \frac{1}{z^{\frac{1}{p}}} - \sum_{n=0}^{+\infty} c_n z^{\frac{n}{p}}\right)^p \\ &\equiv \left(X - \left(\frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n\right)^p\right)\left(X^p - \left(\frac{1}{z} + \sum_{n=0}^{+\infty} c_n z^n\right)\right) \equiv (X - j^*(z)^p)(X^p - j^*(z))\,[1-\zeta_p]\end{aligned}$$

En invoquant le théorème du prolongment analytique, on obtient que cette égalité s'étend à D^* tout entier. On a donc :

$$\Phi_p(X, j) = (X - j^p)(X^p - j) + \sum_{k=0}^{p+1} f_k X^k$$

f_k étant une fonction méromorphe à l'infini (car son pôle à l'infini est d'ordre au plus 2) telle que f_k^* s'exprime comme série en $\frac{1}{z^{\frac{1}{p}}}$ à coefficients dans $(1-\zeta_p)\mathbb{Z}[\zeta_p]$ pour tout $k \in \{0, \cdots, p+1\}$. La proposition 4.6.5 assure alors que les f_k sont des polynômes en j à coefficients dans $(1-\zeta_p)\mathbb{Z}[\zeta_p]$. Mais les coefficients de $\Phi_p(X, j) - (X - j^p)(X^p - j)$, donc les f_k sont dans $\mathbb{Z}[j]$ d'après la proposition 4.6.7. Donc les coefficients des f_k dans $\mathbb{Z}[j]$ sont dans $(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}$ (puisque $1-\zeta_p|p$), et donc tous divisibles par p. Ainsi :

$$\Phi_p(X, j) \equiv (X - j^p)(X^p - j)\,[p]$$

On remplace alors j par l'indéterminée Y dans cette équation. D'où le résultat. □

G Preuves et compléments de la section 5.

G.1 Généralités sur les groupes formels.

Proposition G.1.1. *Soit F un groupe formel sur $\mathbb{A}$. F vérifie de plus les deux proporiétés suivantes :*

1. *$F(X,Y) = X + Y +$ (termes de degré $\geqslant 1$)*
2. *Il existe $i(X) \in \mathbb{A}[\![X]\!]$ telle que $F(X, i(X)) = F(i(X), X) = 0$*

Démonstration. Le fait que $F(X,0) = X$ et $F(X,Y) = F(Y,X)$ prouve le premier point. Pour le second point en notant

$$F(X,Y) = \sum_{i+j\geq 1} a_{i,j} X^i Y^j$$

il suffit de considérer

$$i(X) = \sum_{n\geq 1} b_n X^n$$

avec $b_1 = -1$ et pour $n \in \mathbb{N}$

$$b_n = -\sum_{i=1}^{n} \sum_{j\geq 0} \sum_{k_1+\cdots+k_j=n-i} a_{ij} b_{k_1} \cdots b_{k_j}$$

□

Lemme G.1.2. *(lemme 5.1.3) Soit $F \in \mathbb{A}[\![X,Y]\!]$ sans terme constant. Posons pour $f, g \in X\mathbb{A}[\![X]\!]$, $f \oplus g = F(f,g)$. Si $\oplus$ est associative, commutative et admet 0 comme élément neutre, alors F est un groupe formel.*

Démonstration. Si 0 est neutre pour $\oplus$, on a bien $F(X,0) = X$. Montrons $F(X,Y) = F(Y,X)$. Posons

$$G(X,Y) = F(X,Y) - F(Y,X) = \sum_{i+j\geq 0} g_{ij} X^i Y^j$$

On a pour tous $a, b \geq 1$, $G(X^a, X^b) = 0$ car $\oplus$ commutative. Donc pour tout $n \in \mathbb{N}$, $\sum_{ia+jb=n} g_{ij} = 0$. Supposons par l'absurde $G \neq 0$ et considérons les couples (i,j) avec $g_{ij} \neq 0$ tels que $i + j$ est minimal. Soit (i_0, j_0) le plus petit de ces coefficients pour l'ordre lexicographique. Posons :

$$N_1 = i_0 + j_0, N_2 = i_0$$

et soient $M_2 \geq 1$ et $M_1 > M_2 N_2$. Prenons enfin $a = M_1 + M_2$, $b = M_1$ et $N = N_1 M_1 + N_2 M_2$. On a $\sum_{ia+jb=N} g_{ij} = 0$. Soit (i,j) tel que $g_{ij} \neq 0$ et $ia + jb = N$. On peut réécrire cette dernière égalité

$$(i+j)M_1 + iM_2 = N_1 M_1 + N_2 M_2$$

Par minimalité de $i_0 + j_0$ on a $i + j \geq N_1$. De plus si l'inégalité est stricte on a

$$N_1 M_1 + N_2 M_2 \geq (N_1 + 1)M_1 + iM_2 > N_1 M_1 + N_2 M_2 + iM_2$$

puis $iM_2 < 0$ (absurde). Donc $i+j = N_1$, puis par minimalité de N_2 on a $i = N_2 = i_0$ donc $(i,j) = (i_0, j_0)$. Ceci contredit le fait que $\sum_{ia+jb=N} g_{ij} = 0$ (absurde). On en déduit $G = 0$ et $F(X,Y) = F(Y,X)$. L'associativité de F se prouve de façon analogue (voir [12]). □

G.2 Morphismes de groupes formels.

Proposition G.2.1. *(proposition 5.2.2)*

(i). *$[m](X)$ est un homomorphisme sur F*

(ii). *$[m](X) = mX + O(X^2)$*

(iii). *Si $m \in \mathcal{U}(\mathbb{A})$, alors $[m](X)$ est un isomorphisme.*

Démonstration. **(i).** On prouve le résultat par récurrence sur $m \in \mathbb{N}$. L'initialisation est triviale puisque $F(0,0) = 0$. Soit $m \in \mathbb{N}$. Supposons le résultat au rang m. Alors $[m](F(X,Y)) = F([m](X), [m](Y))$ et donc :

$$\begin{aligned}
[m+1](F(X,Y)) &= F([m](F(X,Y)), F(X,Y)) = F(F([m](X), [m](Y)), F(X,Y)) \\
&= F([m](X), F([m](Y), F(X,Y))) = F([m](X), F([m](Y), F(Y,X))) \\
&= F([m](X), F(F([m](Y), Y), X)) = F([m](X), F(X, F([m](Y), Y))) \\
&= F(F([m](X), X), F([m](Y), Y)) = F([m+1](X), [m+1](Y))
\end{aligned}$$

D'où l'itération.

Puis, on généralise cela à $\mathbb{Z}$ par récurrence descendante.

(ii). C'est une récurrence immédiate sur m.

(iii). Pour prouver ce point plus difficile, on commence par établir le lemme suivant :

Lemme G.2.2. *Soit $f \in \mathbb{A}[\![X]\!]$ tel que $f(X) = \sum_{n=1}^{+\infty} a_n X^n$ avec $a_1 \in \mathcal{U}(\mathbb{A})$. Alors il existe $g \in \mathbb{A}[\![X]\!]$ tel que $f(g(X)) = g(f(X)) = X$.*

Démonstration. On construit une suite de polynômes $(g_n)_{n\in\mathbb{N}^*}$ telle que pour tout $n \in \mathbb{N}^*$:

$$f(g_n(X)) = X + O(X^{n+1}) \quad \text{et} \quad g_n(X) = g_{n+1}(X) + O(X^{n+1})$$

On prend $g_1 := \frac{1}{a_1}X$, qui convient. Soit maintenant $n \in \mathbb{N}^*$. Supposons construits $g_1, \cdots, g_n$. Alors pour $b \in \mathbb{A}$ fixé, on a :

$$\begin{aligned} f(g_n(X) + bX^{n+1}) &= \sum_{k=1}^{+\infty} a_k (g_n(X) + bX^{n+1})^k = \sum_{k=1}^{+\infty} a_k \sum_{l=0}^{k} \binom{k}{l} g_n(X)^l (bX^{n+1})^{k-l} \\ &= \sum_{k=1}^{+\infty} a_k g_n(X)^k + a_1 bX^{n+1} + O(X^{n+2}) = f(g_n(X)) + a_1 bX^{n+1} + O(X^{n+2}) \end{aligned}$$

Mais $f(g_n(X)) = X + cX^{n+1} + O(X^{n+2})$ avec $c \in \mathbb{A}$ par hypothèse de récurrence. Donc, en prenant $b = -\frac{c}{a_1} \in \mathbb{A}$, on obtient que :

$$f(g_n(X) + bX^{n+1}) = X + O(X^{n+2})$$

Posons donc $g_{n+1}(X) := g_n(X) + bX^{n+1}$, qui convient.

Comme $\mathbb{A}[\![X]\!]$ est un anneau de valuation discrète complet pour la valuation donnée par plus petit degré des monômes intervenant dans l'écriture de la série formelle considérée, et que $(g_n)_{n\in\mathbb{N}^*}$ est de Cauchy pour cette valuation, on obtient que $g := \lim_{n\to} g_n$ existe dans $\mathbb{A}[\![X]\!]$ et vérifie $f(g(X)) = X$ par construction.

Comme $\frac{1}{a_1}X$ est le premier terme de g et que $\frac{1}{a_1} \in \mathcal{U}(\mathbb{A})$, on peut appliquer le résultat que nous venons de montrer à g, pour obtenir l'existence de $h \in \mathbb{A}[\![X]\!]$ telle que $g(h(X)) = X$. On a alors :

$$g(f(X)) = g(f(g(h(X)))) = g(h(X)) = X$$

D'où le résultat. □

Supposons que $m \in \mathcal{U}(\mathbb{A})$. Alors par (ii)., on dispose de $g \in \mathbb{A}[\![X]\!]$ telle que $[m](g(X)) = g([m](X)) = X$ et on a alors :

$$g(F(X,Y)) = g(F([m](g(X)), [m](g(Y)))) = g([m]F(g(X), g(Y))) = F(g(X), g(Y))$$

Donc g est bien un homomorphisme de F vers F. Ainsi, f est bien un isomorphisme.

□

G.3 Groupe formel d'une courbe elliptique.

Pour pouvoir considérer le point $\mathcal{O}$ aisément, on représente les points de E sous la forme (τ, σ), avec $\tau = -X/Y$ et $\sigma = -1/Y$. Le polynôme de Weierstrass s'écrit alors

$$\mathcal{W}(T,S) = -S + T^3 + a_1 TS + a_2 T^2 S + a_3 S^2 + a_4 TS^2 + a_6 S^3$$

On souhaite associer à $f \in T\mathbb{K}[\![T]\!]$ un point $(f,g) \in E(\mathbb{K}((T)))$. On aurait alors $\mathcal{W}(f,g) = 0$. La proposition suivante va nous permettre de le faire.

Proposition G.3.1. *Soit $f \in T\mathbb{K}[\![T]\!]$. Il existe un unique $g \in T\mathbb{K}[\![T]\!]$ tel que $\mathcal{W}(f,g) = 0$. De plus $g \in T^2\mathbb{K}[\![T]\!]$.*

Démonstration. Considérons le polynôme $A = \mathcal{W}(f,S) \in \mathbb{K}((T))[S]$. On va lui appliquer le lemme de Hensel (théorème 2.2.1) avec $\mathbb{K} = \mathbb{K}((T)), P = A, x = 0$. Notons v la valuation de $\mathbb{K}((T))$. On a $A(0) = T^3$ donc $v(A(0)) = 3$ et $A'(0) = a_1 T + a_2 T^2$ donc $v(A'(0)) = 1$ puis $2v(A'(0)) = 2 < v(A(0))$ donc (lemme de Hensel) on dispose d'une unique racine g de A telle que $v(g) > v(A'(0)) = 1$, donc $g \in T\mathbb{K}[\![T]\!]$ (et c'est l'unique racine de A dans $T^2\mathbb{K}[\![T]\!]$. Montrons que g est l'unique racine de A dans $T\mathbb{K}[\![T]\!]$. Soit h une autre racine de A dans $T\mathbb{K}[\![T]\!]$. On a alors

$$0 = A(g) - A(h) = (g-h)(-1 + a_1 f + a_2 f^2 + a_3(g+h) + a_4 f(g+h) + a_6(g^2 + gh + h^2))$$

Donc comme $-1 + a_1 f + a_2 f^2 + a_3(g+h) + a_4 f(g+h) + a_6(g^2+gh+h^2)$ est inversible, $h = g$. □

Soit s l'unique série formelle de $T\mathbb{K}[\![T]\!]$ telle que $\mathcal{W}(T,s)=0$. On a pour $f \in T\mathbb{K}[\![T]\!]$, $\mathcal{W}(T,s)$ évalué en f est nul donc $s(f)$ est l'unique série formelle de $T\mathbb{K}[\![T]\!]$ telle que $\mathcal{W}(f,s(f))=0$.

On dispose donc d'une injection de $T\mathbb{K}[\![T]\!]$ dans $E(\mathbb{K}((T)))$ en posant $\boxed{Q(f)=(f,s(f))}$.

Remarque. On a $\mathcal{W}(T,s(T))=0$, donc on a

$$s = T^3 + a_1Ts + a_2T^2s + a_3s^2 + a_4Ts^2 + a_6s^3$$

En remplaçant s par sa propre expression dans l'égalité ci-dessus, on peut obtenir s à n'importe quelle précision.

Remarque. Notons $X, Y \in \mathbb{K}(E)$ les paramètres usuels de la courbe E ainsi que $\tau = -X/Y$ un paramètre local en $\mathcal{O}$ et $\sigma = -1/Y$. Reprenons l'homomorphisme isométrique Φ de $\mathbb{K}(E)$ vers $\mathbb{K}((T))$ de la proposition 5.3.1 tel que $\Phi(\tau)=T$. On a $\mathcal{W}(\Phi(\tau),\Phi(\sigma))=0$ car $\mathcal{W}(\tau,\sigma)=0$ et que Φ isométrique. De plus $ord_{\mathcal{O}}(\sigma) \geq 1$ donc $\Phi(\sigma) \in T\mathbb{K}[\![T]\!]$ puis $\Phi(\sigma)=s(\Phi(\tau))=s(T)$. Comme Φ homomorphisme on peut calculer $\Phi(X)=T/s(T)$ et $\Phi(Y)=-1/s(T)$. On a en particulier

$$\begin{aligned}\Phi(X) =& T^{-2} - a_1T^{-1} - a_2 - a_3T - (a_1a_3+a_4)T^2 - (a_2a_3+a_1^2a_3+a_1a_4)T^3 \\ & - (a_1^2a_4+a_1^3a_3+a_2a_4+2a_1a_2a_3+a_3^2+a_6)T^4 + O(T^5)\end{aligned}$$

et $\Phi(Y)=T^{-1}\Phi(X)$

Construisons à présent $F \in \mathbb{K}[\![T,S]\!]$ telle que pour $f,g \in T\mathbb{K}[\![T]\!]$,

$$Q(f)+Q(g)=Q(F(f,g))$$

L'application des formules d'addition (faite en détail dans [12]) montre qu'il existe des séries formelles α et β de $\mathbb{K}[\![T,S]\!]$ sans terme constant telles que pour $f,g \in T\mathbb{K}[\![T]\!]$,

$$Q(f)+Q(g)=(\alpha(f,g),\beta(f,g))$$

On a alors $(\alpha(f,g),\beta(f,g)) \in E(\mathbb{K}((T)))$ donc $\mathcal{W}(\alpha(f,g),\beta(f,g))=0$ donc d'après la proposition G.3.1 $\beta(f,g)=s(\alpha(f,g))$. En posant $F=\alpha$, on a bien F sans terme constant donc $F(f,g) \in T\mathbb{K}[\![T]\!]$ et

$$Q(f)+Q(g)=(F(f,g),s(F(f,g)))=Q(F(f,g))$$

Comme de plus $Q(0)=(0,0)$, on peut appliquer la proposition 5.1.4, dont on déduit que F est un groupe formel sur $\mathbb{K}$.

Définition G.3.2. *Le groupe formel F défini ci-dessus est appelé groupe formel de la courbe elliptique E.*

G.4 Formules de Vélu

Notons le polynôme de Weierstrass de E :

$$W(X,Y)=Y^2-X^3+a_1XY-a_2X^2+a_3Y-a_4X-a_6$$

Soient de plus $f_0, g_0 \in \mathbb{K}(E)$ avec pour $P \in E$

$$f_0(P)=\sum_{Q\in G} X(P+Q) - \sum_{Q\in G\setminus\{\mathcal{O}\}} X(Q)$$

et

$$g_0(P)=\sum_{Q\in G} Y(P+Q) - \sum_{Q\in G\setminus\{\mathcal{O}\}} Y(Q)$$

On va montrer que f_0 et g_0 annulent un polynôme de Weierstrass, qui sera celui de E/G, et que (f_0,g_0) est une isogénie de noyau G.

Posons :

$$
\begin{aligned}
G_2 &= \{\text{Points d'ordre 2 de G}\}\\
R &\subset G\backslash\{\mathcal{O}\}\backslash G_2 \text{ tel que } G\backslash\{\mathcal{O}\}\backslash G_2 = R \cup -R \text{ et } R \cap -R = \emptyset\\
S &= G_2 \cup R\\
b_2 &= a_1^2 + 4a_2\\
b_4 &= a_1a_3 + 2a_4\\
b_6 &= a_3^2 + 4a_6\\
t_P &= 3X(P)^2 + 2a_2X(P) + a_4 - a_1Y(P) \text{ Pour } P \in G_2\\
t_P &= 6X(P)^2 + b_2X(P) + b_4 \text{ Pour } P \in G\backslash G_2\\
u_P &= 4X(P)^3 + b_2X(P)^2 + 2b_4X(P) + b_6 \text{ Pour } P \in G\\
t &= \sum_{P\in S} t_P\\
w &= \sum_{P\in S} (u_P + X(P)t_P)
\end{aligned}
$$

L'application des formules d'addition, ainsi que le calcul, effectué ci-dessus, de $\Phi(X)$ et $\Phi(Y)$ (où Φ est l'homomorphisme isométrique de $\mathbb{K}(E)$ muni de la valuation en $\mathcal{O}$ vers $\mathbb{K}((T))$) nous permettent d'obtenir $\Phi(f_0)$ et $\phi(g_0)$ dont voici les premiers termes :

$$
\begin{aligned}
\Phi(f_0) =& T^-2 - a_1T^{-1} - a_2 - a_3T + (-a_3a_1 + (t - a_4))T^2 + (-a_3a_1^2 + (t - a_4)a_1 - a_2a_3)T^3\\
&+ (-a_3a_1^3 + (t - a_4)a_1^2 - 2a_2a_3a_1 + (-a_3^2 + (a_2t + (-a_4a_2 + (w - a_6)))))T^4 + O(T^5)\\
\Phi(g_0) =& - T^{-3} + a_1T^{-2} + a_2T^{-1} + a_3 + (a_3a_1 + (-5t + a_4))T + (a_3a_1^2 + (-5t + a_4)a_1 + a_2a_3)T^2\\
&+ (a_3a_1^3 + (-6t + a_4)a_1^2 + 2a_2a_3a_1 + (a_3^2 + (-9a_2t + (a_4a_2 + (-7w + a_6)))))) * T^3 + O(T^4)
\end{aligned}
$$

Considérons le polynôme de Weierstrass

$$W'(X, Y) = Y^2 - X^3 + A_1XY - A_2X^2 + A_3Y - A_4X - A_6$$

avec :

$$
\begin{aligned}
A_1 &= a_1\\
A_2 &= a_2\\
A_3 &= a_3\\
A_4 &= a_4 - 5t\\
A_6 &= a_6 - b_2t - 7w
\end{aligned}
$$

On a $W'(f_0, g_0) \in \mathbb{K}(E)$ et on vérifie

$$\Phi(W'(f_0, g_0)) = O(T)$$

donc comme Φ est une isométrie, on a $ord_{\mathcal{O}}(W'(f_0, g_0)) \geq 1$ puis $W'(f_0, g_0)(\mathcal{O}) = 0$.

De plus pour $Q \in G$, $f_0(Q + .) = f_0$ et $g_0(Q + .) = g_0$ donc $W'(f_0, g_0)(Q) = 0$ De plus on voit que si $P \notin G$, P n'est pas un pôle de $W'(f_0, g_0)$. Par conséquent $W'(f_0, g_0)$ a plus de zéros que de pôles puis d'après la proposition 3.1.12, on a $W'(f_0, g_0) = 0$. On en déduit que l'application $(f_0, g_0) : Q \in E \mapsto (f_0(Q), g_0(Q)) \in \mathbb{P}^3(\mathbb{K})$ est un morphisme de E vers la courbe E' de polynôme de Weierstrass W'. De plus $\mathcal{O}$ est un pôle de f_0 donc $(f_0, g_0)(\mathcal{O}) = \mathcal{O}$ puis (f_0, g_0) est une isogénie. Les pôles de f_0 et g_0 sont exactement les éléments de G donc (f_0, g_0) est l'isogénie de noyau G cherchée et $E' = E/G$.

G.5 Groupe formel et isogénies.

Théorème G.5.1 (isogénies et groupe formel)**.** *(théorème 5.5.1)*

(i). *L'application Ψ précédente est à valeurs dans $Hom(F_1, F_2)$, l'ensemble des morphismes de groupes formels entre F_1 et F_2 et c'est un morphisme injectif de groupes.*

(ii). *Si E_3 est une courbe elliptique de paramètre local en $\mathcal{O}$ τ_3 et si $\varphi \in Hom(E_1, E_2)$ et $\psi \in Hom(E_2, E_3)$ alors on a la formule :*

$$\tau_3 \circ (\psi \circ \varphi) = (\tau_3 \circ \psi) \circ (\tau_2 \circ \varphi)$$

où la composition du milieu à droite est la composition des séries formelles, tandis que celle de gauche est la composition de l'isogénie $\psi \circ \varphi$ par la fonction τ_3.

Démonstration. **(i).** Pour montrer que Ψ est à valeurs dans $\mathrm{Hom}(F_1, F_2)$, il s'agit de vérifier que pour des indéterminées ξ, η indépendantes données, on a :

$$\forall \varphi \in \mathrm{Hom}(E_1, E_2), \quad (\tau_2 \circ \varphi)(F_1(\xi, \eta)) = F_2(\tau_2 \circ \varphi(\xi), \tau_2 \circ \varphi(\eta))$$

Considérons les points $P(\xi) := \left(\frac{\xi}{s_1(\xi)}, -\frac{1}{s_1(\xi)}\right) \in E(\mathbb{K}(\xi))$ et $Q(\eta) := \left(\frac{\eta}{s_1(\eta)}, -\frac{1}{s_1(\eta)}\right) \in E(\mathbb{K}(\eta))$ où $s_1 \in \mathbb{K}((T))$ est la série associée à la fonction $-\frac{1}{Y}$ de E_1. Alors pour tout $\varphi \in \mathrm{Hom}(E_1, E_2)$:

$$\begin{aligned}(\tau_2 \circ \varphi)(F_1(\xi, \eta)) &= \tau_2(\varphi(P(\xi) + Q(\eta))) = \tau_2(\varphi(P(\xi)) + \varphi(Q(\eta))) = F_2(\varphi(P(\xi)), \varphi(Q(\eta))) \\ &= F_2(\tau_2 \circ \varphi(\xi), \tau_2 \circ \varphi(\eta))\end{aligned}$$

Considérons maintenant $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$. Alors, comme l'addition des morphismes suit la même loi que l'addition des points (en termes algébriques) :

$$\Psi(\varphi + \psi) = \tau_2 \circ (\varphi + \psi) = F_2(\tau_2(\varphi), \tau_2(\psi)) = \Psi(\varphi) \oplus_{F_2} \Psi(\psi)$$

Donc Ψ est un morphisme de groupes.

Enfin, on a pour tout $\varphi \in \mathrm{Hom}(E_1, E_2)$:

$$\varphi = \left(\frac{\Phi(\varphi)}{s_2(\Phi(\varphi))}, -\frac{1}{w_2(\Phi(\varphi))}\right)$$

où $s_2 \in \mathbb{K}((T))$ est la série associée à la fonction $-\frac{1}{Y}$ de E_2. Ceci donne immédiatement l'injectivité de Φ. D'où (i).

(ii). On a :

$$\varphi = \left(\frac{\tau_2 \circ \varphi}{s_2(\tau_2 \circ \varphi)}, -\frac{1}{s_2(\tau_2 \circ \varphi)}\right) \quad \text{et} \quad \psi = \left(\frac{\tau_3 \circ \psi}{s_3(\tau_3 \circ \psi)}, -\frac{1}{s_3(\tau_3 \circ \psi)}\right)$$

où s_3 est l'analogue de s_2 pour E_3. Donc :

$$\psi \circ \varphi = \left(\frac{(\tau_3 \circ \psi) \circ (\tau_2 \circ \varphi)}{s_3((\tau_3 \circ \psi) \circ (\tau_2 \circ \varphi))}, -\frac{1}{s_3((\tau_3 \circ \psi) \circ (\tau_2 \circ \varphi))}\right)$$

Ainsi, en composant par τ_3, on voit immédiatement que :

$$\tau_3 \circ (\psi \circ \varphi) = (\tau_3 \circ \psi) \circ (\tau_2 \circ \varphi)$$

□

H Preuves de la section 6.

Lemme H.0.1. *Soient $x, y \in M_{\overline{\mathbb{Q}_q}}$. Alors $F_{\tilde{E}}(x, y)$ est bien défini et c'est un élément de $M_{\overline{\mathbb{Q}_q}}$.*

Démonstration. Nous avons vu que $F_{\tilde{E}}$ peut s'écrire :

$$F_E(X, Y) = X + Y + \sum_{\substack{n,m\in\mathbb{N} \\ n+m\geq 2}} a_{n,m} X^n Y^m$$

$a_{n,m} \in \mathbb{Z}_q$ pour tous $n, m \in \mathbb{N}$ tels que $n + m \geq 2$. Soient $x, y \in M_{\overline{\mathbb{Q}_q}}$. Considérons la suite de terme général :

$$z_N := x + y + \sum_{\substack{n,m\in\mathbb{N} \\ 2\leq n+m\leq N}} a_{n,m} x^n y^m$$

pour $N \geq 2$. On a pour tous $M \geq N \geq 2$:

$$v_p(z_M - z_N) = v_p\left(\sum_{\substack{n,m\in\mathbb{N} \\ N\leq n+m\leq M}} a_{n,m} x^n y^m\right) \geq N \min(v_p(x), v_p(y)) \underset{N\to+\infty}{\longrightarrow} +\infty$$

Donc $(z_N)_{N\geq 2}$ est de Cauchy. Mais tous les nombres de $\overline{\mathbb{Q}_q}$ sont algébriques donc $\mathbb{Q}_q[x, y]$ est une extension finie de $\mathbb{Q}_q$, donc est complête puisque $\mathbb{Q}_q$ est complet. Comme $(z_N)_{N\geq 2}$ est à valeurs dans $\mathbb{Q}_q[x, y]$, elle est donc convergente. Donc $F_{\tilde{E}}(x, y) = \lim_{N\to+\infty} z_N$ existe.

C'est bien un élément de $p\overline{Q_q}$ car $v_p(z_N) \geq \min(v_p(x), v_p(y)) \geq 1$ pour tout $N \geq 2$, de sorte que $v_p(F_{\tilde{E}}(x, y)) \geq 1$. □

Proposition H.0.2.

$$\tau : ker(\pi) \longmapsto M_{\overline{\mathbb{Q}_q}}$$

est un isomorphisme de groupes.

Démonstration. On commpence par vérifier que l'application τ est bien à valeurs dans $M_{\overline{\mathbb{Q}_q}}$. Soit $P \in \ker(\pi)$. Si $P = \mathcal{O}$ alors $\tau(P) = 0 \in p\overline{\mathbb{Q}_q}$. Sinon, on écrit $P := (x, y)$. Comme nous l'avons vu au paragraphe précédent, il existe $k \in \mathbb{N}^*$ tel que $v_p(x) = -2k$ et $v_p(y) = -3k$. On a alors $v_p(\tau(P)) = v_p(x) - v_p(x) = k > 0$ donc $\tau(P) \in M_{\overline{\mathbb{Q}_q}}$.

On sait en outre par définition de $F_{\tilde{E}}$ que $\tau(P + Q) = F_{\tilde{E}}(\tau(P), \tau(Q)) = \tau(P) \oplus_{F_{\tilde{E}}} \tau(Q)$ pour tous $P, Q \in \tilde{E}$. Donc τ induit bien un morphisme de groupes entre $\ker(\pi)$ et $p\overline{\mathbb{Q}_q}$.

On a vu au paragraphe 5.3 que la fonction de $\mathbb{Q}_q(\tilde{E})$ définie par $w = -\frac{1}{Y}$, s'exprime comme série formelle en τ de valuation 3. Autrement dit, il existe $s \in \mathbb{Z}_q[\![T]\!]$ dont le premier terme est T^3 et telle que $w(P) = s(\tau(P))$ pour tout $P \in \tilde{E}$. On sait qu'alors :

$$\forall P \in \tilde{E} \setminus \{\mathcal{O}\}, \quad P = \left(-\frac{\tau(P)}{s(\tau(P))}, -\frac{1}{s(\tau(P))}\right)$$

donc $P = Q$ dès que $\tau(P) = \tau(Q)$. Ce qui prouve l'injectivité de τ.

Pour la surjectivité, on considère un élément $\alpha \in M_{\overline{\mathbb{Q}_q}} \setminus \{\mathcal{O}\}$. En vertu d'un raisonnement analogue à celui du lemme précédent $s(\alpha)$ existe dans $M_{\overline{\mathbb{Q}_q}}$ et comme s a pour premier terme T^3, on a $v_p(\tilde{w}(\alpha)) = 3v_p(\alpha)$. On peut donc poser :

$$P := \left(-\frac{\alpha}{s(\alpha)}, -\frac{1}{s(\alpha)}\right)$$

Comme $W\left(-\frac{X}{\tilde{w}(X)}, -\frac{1}{\tilde{w}(X)}\right) = 0$ d'après ce qui a été vu lors de l'étude du groupe formel, on en déduit que $P \in \tilde{E}$. En outre :

$$v_p(x(P)) = v_p(\alpha) - v_p(\tilde{w}(\alpha)) = -2v_p(\alpha) < 0$$

donc $P \in \ker(\pi)$. Ceci montre la surjectivité de τ. D'où le résultat. □

I Preuves et compléments de la section 7.

I.1 Prérequis technique : relèvement en temps court d'un facteur polynomial de $\mathbb{F}_q[X]$.

Pour établir les résultats de complexité, nous nous réfèrerons au lemme suivant que nous admettrons.

Lemme I.1.1. **(i).** *La division euclidienne de A par B dans un anneau $\mathbb{A}[X]$ tels que $deg(B) \leq deg(A)$ coûte $O(deg(A) - deg(B) + 1)$ opérations sur élémentaires sur $\mathbb{A}$.*

(ii). *L'algorithme d'Euclide étendu appliqué à $A, B \in \mathbb{F}_q[X]$ non constants peut être effectué en $O(deg(A)deg(B))$ opérations élémentaires sur $\mathbb{F}_q$. Le couple de Bézout $(U, V) \in \mathbb{F}_q[X]^2$ trouvé (ie le couple tel que $AU + BV = 1$) vérifie alors $deg(U) < deg(B)$, $deg(B) < deg(A)$.*

Rappelons que le lemme C.2.2 nous autorise à appliquer la formule de Taylor-Young pour les polynômes dans $\mathbb{Z}_q[X]$ sans se poser de question et que v_G désigne la valuation de Gauss, définie en 2.2.3. Rappelons aussi un résultat évoqué en C.2 :

Lemme I.1.2. *Soient $P, Q \in \mathbb{Z}_q[X]$. Supposons que $\overline{P}$ et $\overline{Q}$, les réduites de P et Q modulo p soient premières entre elles. Alors P et Q sont premiers entre eux.*

Démonstration. Notons $n := \deg(P)$ et $m := \deg(Q)$. Alors d'après la proposition C.2.4 :

$$\overline{\mathrm{Res}_{m,n}(P, Q)} = \mathrm{Res}_{m,n}(\overline{P}, \overline{Q}) \neq 0$$

De sorte que P et Q soient premiers entre eux. □

Lemme I.1.3. *Soient $U, P \in \mathbb{Z}_q[X]$. Posons $t := v_G(U')$. Supposons que P vérifie les conditions suivantes :*

(i). *P est unitaire.*

(ii). *La réduction $\overline{P}$ de P modulo p est sans facteurs carré est première avec $\overline{p^{-t}U'}$.*

(iii). *Il existe $Q_0 \in \mathbb{Z}_q[X]$ et $u \in \mathbb{N}^*$ tels que $v_G(U - PQ_0) \geq u + t$.*

Posons $v := 2u + \min(t, u)$. Alors les résultats suivants sont vérifiés :

(i). *Si $R, Q_1 \in \mathbb{Z}_q[X]$ vérifient $R \equiv P\,[p]$ et $v_G(U - RQ_1) \geq v$, alors pour $S \in \mathbb{Z}_q[X]$ tel que $S \equiv R\,[p^{2u}]$, il existe $Q_2 \in \mathbb{Z}_q[X]$ tel que $v_G(U - SQ_2) \geq v$.*

(ii). *Il existe $Q_3 \in \mathbb{Z}_q[X]$ et $Q \in \mathbb{Z}_q[X]$ unitaire tels que $v_G(U - QQ_3) \geq v$ et $Q \equiv P\,[p^u]$. Q peut être construit avec $O\left((deg(P) + deg(U))^2\right)$ opérations sur l'anneau $\mathbb{Z}_q/p^{2u}\mathbb{Z}_q$.*

Démonstration. **(i).** On suppose qu'il existe $R, Q_1 \in \mathbb{Z}_q[X]$ vérifiant $R \equiv P\,[p]$ et $v_G(U - RQ_1) \geq v$. Soit $S \in \mathbb{Z}_q[X]$ tel que $S \equiv R\,[p^{2u}]$. Alors on pose $D := p^{-2u}(S - R)$ (1), qui est dans $\mathbb{Z}_q[X]$ par hypothèse. Comme $R \equiv P\,[p^{2u}]$, on a $\overline{R} = \overline{P}$ modulo p donc $\overline{R}$ est aussi unitaire et sans facteur carré, donc premier avec sa dérivée. Le lemme I.1.2 assure l'existence de $A, B \in \mathbb{Z}_q[X]$ tels que $AR + BR' \equiv 1\,[p^v]$, ce qui donne en multipliant par D :

$$A_1R + B_1R' \equiv D\,[p^{v-2u}] \quad (2)$$

avec $A_1 := DA$ et $B_1 := DB$. Par hypothèse, $U \equiv RQ_1\,[p^v]$ donc en évaluant cette relation en $X + p^{2u}A_1(X)$, on obtient :

$$U(X + p^{2u}A_1(X)) \equiv R(X + p^{2u}A_1(X))Q_1(X + p^{2u}A_1(X))\,[p^v]$$

Or, comme $v_G(U') = t \geq v - 2u$, la formule de Taylor-Young (que l'on peut appliquer grâce au lemme C.2.2) assure que :

$$U(X + p^{2u}A_1(X)) = U(X) + \sum_{k=1}^{+\infty} \frac{p^{2uk}A_1^k}{k!}U^{(k)}(X) \equiv U(X)\,[p^v] \quad (3)$$

En outre, comme $v \leq 3u$, on a $(1 + p^{2u}B_1)(1 - p^{2u}B_1) \equiv 1\,[p^v]$ et donc modulo p^v :

$$\begin{aligned}
R(X + p^{2u}A_1(X))Q_1(X + p^{2u}A_1(X)) &= \left(\sum_{k=0}^{+\infty} \frac{p^{2uk}A_1^k}{k!}R^{(k)}\right) Q_1(X + p^{2u}A_1(X)) \\
&\equiv (R(X) + p^{2u}[A_1R'](X))[(1 + p^{2u}B_1)(1 - p^{2u}B_1)](X)Q_1(X + p^{2u}A_1(X)) \\
&\equiv (R(X) + p^{2u}[A_1R' + B_1R](X))(1 - p^{2u}B_1(X))Q_1(X + p^{2u}A_1(X)) \\
&\equiv (R(X) + p^{2u}D(X))(1 - p^{2u}B_1(X))Q_1(X + p^{2u}A_1(X)) \quad \text{par (2)} \\
&\equiv S(X)(1 - p^{2u}B_1(X))Q_1(X + p^{2u}A_1(X)) \quad \text{par (1)}
\end{aligned}$$

Donc d'après (3), $Q_2 := (1 - p^{2u}B_1(X))Q_1(X + p^{2u}A_1(X))$ convient.

(ii). On pose $R_0 := p^{-u-t}(U - PQ_O)$ et $R_1 := p^{-t}U'$, qui sont des polynômes de $\mathbb{Z}_q[X]$ vu que $v_G(U') = t$ et d'après l'hypothèse (iii). Quitte à remplacer Q_0 par le quotient de la division euclidienne de U par P (que l'on peut effectuer dans $\mathbb{Z}_q[X]$ car P est unitaire), on peut supposer que $\deg(R_0) < \deg(P)$.

Soit Y une idéterminée algébriquement indépendante de X. Alors d'après la formule de Taylor-Young :

$$U(X + p^u Y) = U(X) + p^u Y U'(X) + \sum_{k=2}^{+\infty} p^{ku} Y^k \frac{U^{(k)}(X)}{k!}$$

Mais, d'après le lemme C.2.2 pour tout $k \geq 3$, $\frac{U^{(k)}(X)}{k!} \in \mathbb{Z}_q[X]$ donc $p^{ku}Y^k \frac{U^{(k)}(X)}{k!} \equiv 0\,[p^v]$. En outre, on voit immédiatement en dérivant que $v_G(U''(X)) \geq v_G(U'(X))$. Ainsi, comme $p \neq 2$, $v_G\left(p^{2u}\frac{U''(X)}{2}\right) = v(p^{2u})v_G(U''(X)) \geq 2u + t = v$, de sorte que :

$$U(X + p^u Y) \equiv U(X) + p^u Y U'(X) \equiv P(X)Q_0(X) + p^{u+t}(R_0(X) + Y R_1(X))\,[p^v]$$

D'après l'hypothèse (ii). et le lemme I.1.2, on dispose alors de $A, B \in \mathbb{Z}_q[X]$ tels que $AP + BR_1 \equiv 1\,[p^v]$. On obtient alors en multipliant cela par R_0 que :

$$A_1 P + B_1 R_1 \equiv R_0\,[p^v]$$

avec $A_1 := AR_0$ et $B_1 := BR_0$. Ainsi :

$$U(X + p^u Y) \equiv P(X)Q_0(X) + p^{u+t}(A_1(X)P(X) + B_1(X)R_1(X) + Y R_1(X))\,[p^v]$$

Et donc en substituant $X + p^u B_1(X)$ à X et $-B(X)$ à Y, on obtient :

$$U(X) \equiv P(X + p^u B_1(X))Q_4(X)\,[p^v] \quad (3)$$

avec $Q_4(X) := Q_0(X + p^u B_1(X)) + p^{u+t}A_1(X + p^u B_1(X))$. Mais la formule de Taylor-Young donne :

$$P(X + p^u B_1(X)) \equiv P(X) + p^u B_1(X)P'(X) + p^{2u}B_1(X)^2\frac{P''(X)}{2}\,[p^v]$$

les termes d'ordre ≥ 3 s'annulant vu que $v \leq 3u$ et d'après le lemme C.2.2. Ainsi, $P(X) \equiv P(X + p^u B_1(X))\,[p]$, et $P(X + p^u B_1(X)) \equiv P(X) + p^u B_1(X)P'(X)\,[p^{2u}]$, donc d'après (3), on peut appliquer le point (i). prouvé ci-dessus pour obtenir l'existence de $Q_5 \in \mathbb{Z}_q[X]$ tel que :

$$U(X) \equiv (P(X) + p^u B_1(X)P'(X))Q_5(X)\,[p^v] \quad (4)$$

Soient $Q_6, R_2 \in \mathbb{Z}_q[X]$ le quotient et le reste de la divison euclidienne de B_1P' par P (Q_6 et R_2 sont bien dans $\mathbb{Z}_q[X]$ car P est unitaire). Alors on a :

$$(1 - p^u Q_6 + p^{2u}Q_6^2)(1 + p^u Q_6) \equiv 1\,[p^v] \quad (5)$$

Donc, modulo p^v, (4) et (5) donnent :

$$\begin{aligned} U(X) &\equiv (1 - p^u Q_6(X) + p^{2u}Q_6(X)^2)(1 + p^u Q_6(X))(P(X) + p^u B_1(X)P'(X))Q_5(X) \\ &= (1 - p^u Q_6(X) + p^{2u}Q_6(X)^2)(P(X) + p^u[PQ_6 + R_2](X))(1 + p^u Q_6(X))Q_5(X) \\ &\equiv (P(X) + p^u R_2(X) - p^{2u}Q_6(X)R_2(X))Q_7(X) \quad (6) \end{aligned}$$

Avec $Q_7(X) := (1 + p^u Q_6(X))Q_5(X)$. Posons $R := P + p^u R_2$. Alors, comme $R(X) \equiv P(X)\,[p]$ et $P(X) + p^u R_2(X) - p^{2u}Q_6(X)R_2(X) \equiv R(X)\,[p^{2u}]$, l'équation (6) et le point (i). prouvé ci-dessus assurent l'existence de $Q_3 \in \mathbb{Z}_q[X]$ tel que $v_G(U - RQ_3) \geq v$.

Pour prouver le résultat voulu, il ne reste donc plus qu'à établir la complexité de l'algorithme décrit dans la preuve. Tous les polynômes utilisés sont de degré en $O(\deg(P) + \deg(Q))$ et les seules opérations effectuées sont des sommes, des produits, des divisions euclidiennes et l'application de l'algorithme d'Euclide étendu. Le lemme I.1.1 assure alors que toutes ces opérations coûtent $O((\deg(P) + \deg(Q))^2)$ opérations élémentaires sur $\mathbb{Z}_q/p^{2u}\mathbb{Z}_q$. D'où la complexité totale.

□

Le lemme suivant prouve que l'algorithme prédédemment décrit converge vers un facteur polynomial de U à racines dans $\mathbb{Q}_q^{nr}$.

Lemme I.1.4. *Soient $P \in \mathbb{Z}_q[X]$, $(a_n)_{n\in\mathbb{N}}$ une suite d'entiers naturels non nuls strictement croissante et $(Q_n)_{n\in\mathbb{N}} \in \mathbb{Z}_q[X]^{\mathbb{N}}$ une suite de polynômes unitaires vérifiant :*

(i). $\forall n \in \mathbb{N}$, $v_G(Q_{n+1} - Q_n) \geq a_n$

(ii). *Pour tout $n \in \mathbb{N}$, il existe $R_n \in \mathbb{Z}_q[X]$ tel que $v_G(P - Q_n R_n) \geq a_n$.*

(iii). *$\overline{Q_0}$ est sans facteur carré.*

Alors $(Q_n)_{n\in\mathbb{N}}$ converge dans $\mathbb{Z}_q[X]$ (pour la norme associée à v_G définie au paragraphe 2.2 après la définition 2.2.4) vers un facteur de $Q \in \mathbb{Z}_q[X]$ de P dont toutes les racines sont dans $\mathbb{Q}_q^{nr}$.

Démonstration. Comme les Q_n sont tous unitaires, (i). assure que tous les Q_n ont même degré d. Comme $\mathbb{Q}_q$ est complet (comme extension finie de $\mathbb{Q}_p$), et que $(\mathbb{Q}_q)_d[X]$ est un $\mathbb{Q}_q$-espace vectoriel de dimension finie, cet espace est aussi complet pour la norme associée à v_G. Or, $(Q_n)_{n\in\mathbb{N}}$ est de Cauchy dans $(\mathbb{Q}_q)_d[X]$ car d'après (i)., on a pour tous entiers naturels $n < m$:

$$v_G(Q_m - Q_n) \geq \sum_{k=n}^{m-1} v_G(Q_{k+1} - Q_k) \geq \sum_{k=n}^{m-1} a_k \geq a_n \underset{n\to+\infty}{\longrightarrow} +\infty$$

Donc $(Q_n)_{n\in\mathbb{N}}$ converge vers $Q \in (\mathbb{Q}_q)_d[X]$. Le passage à la limite dans (i). assure alors que Q est unitaire de degré d et à coefficients dans $\mathbb{Z}_q$.

Soit $x \in \overline{\mathbb{Q}_q}$ une racine de Q. Comme $\overline{Q} = \overline{Q_0}$ d'après (i). et que $\overline{Q_0}$ est sans facteur carré d'après (iii)., le lemme 2.3.12 assure que $x \in \mathbb{Z}_q^{nr}$. En outre, on a pour tout $n \in \mathbb{N}$:

$$P = (P - Q_n R_n) + (Q_n - Q)R_n + QR_n$$

De sorte que par (ii). et (iii). :

$$v(P(x)) \geq \min(v(P(x)-Q_n(x)R_n(x)), v(Q_n(x)-Q(x))+v(R_n(x)), v(Q(x))+v(R_n(x))) \geq \min(a_n, a_n, +\infty) = a_n$$

Donc, comme $a_n \underset{n\to+\infty}{\longrightarrow} +\infty$, on a $v(P(x)) = +\infty$ i.e. $P(x) = 0$. Ceci étant vrai pour toute racine de Q, Q est un facteur de P. □

I.2 Quelques propriétés techniques des polynômes de division.

Nous prouvons ici quelques résultats techniques utilisés par Satoh (notamment en 7.2.1 et 7.2.3) et prouvés par Cassels dans [11]. Nous rappelons les relations de récurrence qui lient les polynômes de division (proposition E.5.5) :

$$\Psi_1 := 1, \quad \Psi_2 := 2Y, \quad \Psi_3 := 3X^4 - 6AX^2 - 12BX - A^2, \quad \Psi_4 := 4Y(X^6 - 5AX^4 - 20BX^3 - 4ABX + A^3 - 8B^2)$$

Et :

$$\Psi_{2n+1} := \Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3 \quad \text{pour } n \geq 2$$

$$\Psi_{2n} := \frac{\Psi_n(\Psi_{n-1}^2\Psi_{n+2} - \Psi_{n-2}\Psi_{n+1}^2)}{2Y} \quad \text{pour } n \geq 3$$

On note aussi pour tout $n \geq 2$:

$$\phi_n := X\Psi_n^2 - \Phi_{n-1}\Phi_{n+1} \quad \text{et} \quad \Omega_n := \frac{\Psi_{n-1}^2\Psi_{n+2} - \Psi_{n-2}\Psi_{n+1}^2}{4Y}$$

$\phi_1 := 1$, $\Omega_1 := Y$ avec la convention $\Psi_0 := 0$ pour le calcul de Ω_n.

Tous ces polynômes sont a priori dans $\mathbb{Z}[X, Y, A, B]$ mais la substitution $Y^2 = X^3 + AX + B$ permet de voir Ψ_n^2, ϕ_n et Ω_{2n} comme des polynômes de $\mathbb{Z}[X, A, B]$. Par convention, X sera la variable "principale", c'est à dire que l'on se réfèrera à X pour parler de degré, de coefficient dominant...etc. On peut obtenir le résultat suivant par récurrence :

Lemme I.2.1. *Si n est impair, alors Ψ_n est un polynôme de degré $\frac{n^2-1}{2}$ et de coefficient dominant n et si n est pair, $\frac{\Psi_n}{Y}$ est un polynôme en X de degré $\frac{n^2-4}{2}$ et de coefficient dominant n. ϕ_n est unitaire de degré n^2. En outre, $\Psi_{2n+1}(0, A, 0) = (-1)^n A^{n(n+1)}$.*

Lemme I.2.2. *ϕ_n (et Ψ_n si n est impair) n'ont aucun facteur non trivial dans $\mathbb{Z}[A, B]$. Si n est pair, les seuls diviseurs non triviaux de Ψ_n dans $\mathbb{Z}[A, B]$ sont les 2^k pour $k \in \{1, \cdots, v_2(n)\}$.*

Démonstration. Le résultat est trivial pour ϕ_n puisque ce polynôme est unitaire. Si n est impair on écrit $n = 2m + 1$. Si $f \in \mathbb{Z}[A, B]$ divise Ψ_n il divise donc son coefficient dominant $2m + 1$ et son coefficient constant, de terme dominant en A égal à $(-1)^n A^{n(n+1)}$ (d'après le lemme I.2.1) donc $f = 1$.

Sinon, on écrit $n = 2^k m$ avec $k \in \mathbb{N}^*$ et $m \in \mathbb{N}$ impair et on prouve le résultat par récurrence sur k.

Initialisation : Pour $k = 1$, on utilise l'égalité :

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

Si $f \in \mathbb{Z}[A, B]$ divise Ψ_n, il divise donc $\frac{\Psi_{m-1}^2\Psi_{m+2}-\Psi_{m-2}\Psi_{m+1}^2}{2Y}$, puisque Ψ_m n'a aucun diviseur non trivial dans $\mathbb{Z}[A, B]$. Or, d'après le lemme I.2.1, le terme dominant de $\Psi_{m-1}^2\Psi_{m+2} - \Psi_{m-2}\Psi_{m+1}^2$ vaut :

$$(m+2)(m-1)^2Y^2X^{\frac{(m+2)^2-1}{2}+(m-1)^2-4} - (m-2)(m+1)^2Y^2X^{\frac{(m-2)^2-1}{2}+(m+1)^2-4} = 4Y^2X^{\frac{3(m^2-1)}{2}}$$

Donc $f|2$. D'où le résultat pour $k = 1$.

Hérédité : Soit $k \in \mathbb{N}^*$. Supposons le résultat vrai au rang k. On utilise alors l'égalité :

$$\Psi_{2^{k+1}m} := \frac{\Psi_{2^km}(\Psi_{2^km-1}^2\Psi_{2^km+2} - \Psi_{2^km-2}\Psi_{2^km+1}^2)}{2Y}$$

Si $f \in \mathbb{Z}[A, B]$ divise $\Psi_{2^{k+1}m}$, on écrit donc $f = gh$ avec g divisant Ψ_{2^km}, donc $g|2^k$, d'après l'hypothèse de récurrence, et h divisant $\frac{\Psi_{2^km-1}^2\Psi_{2^km+2}-\Psi_{2^km-2}\Psi_{2^km+1}^2}{2Y}$. D'après le lemme I.2.1, le terme dominant de $\Psi_{2^km-1}^2\Psi_{2^km+2} - \Psi_{2^km-2}\Psi_{2^km+1}^2$ vaut :

$$(2^km-1)^2(2^km+2)X^{(2^km-1)^2-1+\frac{(2^km+2)^2-4}{2}}Y - (2^km+1)^2(2^km-2)X^{(2^km+1)^2-1+\frac{(2^km-2)^2-4}{2}}Y$$
$$= 4YX^{3m^2 2^{2k-1}}$$

Donc $h|2$. Donc $f|2^{k+1}$. D'où l'itération et le résultat.

□

Pour prouver le lemme qui suit, on voit les polynômes de division comme des polynômes associés à une courbe elliptique effective définie sur un corps de caractéristique nulle qui se plonge dans $\mathbb{C}$ (par exemple la courbe $\tilde{E}$ définie sur $\mathbb{Q}_q$). On note E cette courbe elliptique (à ne pas confondre avec la courbe E définie sur $\mathbb{F}_q$) et on conserve les coefficients A et B pour définir son polynôme de Weierstrass $Y^2 - X^3 - AX - B$. On sait qu'alors (voir théorèmes 4.3.1 et) $A = -g_4(\Lambda)$ et $B = -g_6(\Lambda)$ pour un certain réseau Λ de $\mathbb{C}$ et que :

$$\Phi : z \in \mathbb{C}/\Lambda \longmapsto \left(\mathcal{P}_\Lambda(z), \frac{1}{2}\mathcal{P}'_\Lambda(z)\right) \in E$$

est un automorphisme de groupes. Pour tout $P := (x, y) \in E$, on a donc $x = \mathcal{P}_\Lambda(z)$, $y = \frac{1}{2}\mathcal{P}'_\Lambda(z)$ pour un unique $z \in \mathbb{C}$, de sorte que :

$$[n]P = [n]\Phi(z) = \Phi(nz) \quad \text{i.e.} \quad \mathcal{P}_\Lambda(nz) = \frac{\Phi_n(x)}{\Psi_n(x)^2} \quad \text{et} \quad \mathcal{P}'_\Lambda(nz) = \frac{2\Omega_n(x, y)}{\Psi_n(x)^3} \quad (\star)$$

d'après le corollaire E.5.6.

Lemme I.2.3.

$$\Phi_{2n}(X) = \Psi_n^8(X)\Phi_2\left(\frac{\Phi_n(X)}{\Psi_n^2(X)}\right) \quad \textit{et} \quad \Psi_{2n}^2(X) = \Psi_n^8(X)\Psi_2^2\left(\frac{\Phi_n(X)}{\Psi_n^2(X)}\right)$$

Démonstration. On a $\Phi(2nz) = [2]\Phi(nz)$ donc par $(\star)$:

$$\frac{\Phi_{2n}(x)}{\Psi_{2n}^2(x)} = \mathcal{P}_\Lambda(2nz) = \frac{\Phi_2(\mathcal{P}_\Lambda(nz))}{\Psi_2^2(\mathcal{P}_\Lambda(nz))} = \frac{\Phi_2\left(\frac{\Phi_n(x)}{\Psi_n^2(x)}\right)}{\Psi_2^2\left(\frac{\Phi_n(x)}{\Psi_n^2(x)}\right)}$$

En outre, en regardant les zéros, les pôles et les coefficients dominants de $\Psi_{2n}^2(X)$ et de $\Psi_n^8(X)\Psi_2^2\left(\frac{\Phi_n(X)}{\Psi_n^2(X)}\right)$, on voit que ces deux fonctions rationnelles de E sont égales. On en déduit alors que :

$$\Phi_{2n}(X) = \Psi_n^8(X)\Phi_2\left(\frac{\Phi_n(X)}{\Psi_n^2(X)}\right)$$

en combinant les deux égalités obtenues précédemment. □

Proposition I.2.4. *$\overline{\phi}_n$ et $\overline{\Psi}_n^2$, les réductions modulo p de ϕ_n et Ψ_n^2 n'ont pas de facteur commun non trivial dans $\mathbb{F}_p[X,A,B]$ (pour $p \geq 3$).*

Démonstration. On raisonne par l'absurde. Soit $f \in \mathbb{F}_p[X,A,B]$ un polynôme irréductible divisant $\overline{\phi}_n$ et $\overline{\Psi}_n^2$. Supposons de plus que que n soit l'indice minimal vérifiant cette propriété. On distingue alors deux cas :

Premier cas : Supposons n pair et écrivons $n := 2m$, pour $m \in \mathbb{N}^*$. Le lemme précédent et les formules donnant Φ_2 et Ψ_2 assurent alors que :

$$\begin{cases} \overline{\phi}_n = \overline{\phi}_{2m} = \overline{\phi}_m^4 - 2A\overline{\phi}_m^2\overline{\Psi}_m^4 - 8B\overline{\Phi}_m\overline{\Psi}_m^6 + A^2\overline{\Psi}_m^8 \equiv 0\,[f] \\ \overline{\Psi}_n^2 = \overline{\Psi}_{2m}^2 = 4(\overline{\phi}_m^3\overline{\Psi}_m^2 + A\overline{\phi}_m\overline{\Psi}_m^6 + B\overline{\Psi}_m^8) \equiv 0\,[f] \end{cases} \qquad (S)$$

Donc en combinant ces équations pour éliminer les puissances de ϕ_n :

$$(4A^3 - 27B^2)\overline{\phi}_m\overline{\Psi}_m^{10} \equiv 0\,[f]$$

Or, comme Φ_n est unitaire, f ne peut être dans $\mathbb{F}_p[A,B]$. Ainsi, $f|\overline{\phi}_m\overline{\Psi}_m^{10}$ donc $f|\overline{\phi}_m$ ou $f|\overline{\Psi}_m^2$ (comme f est irréductible). Les équations de (S) assurent qu'en fait les deux cas sont simultanément réalisés. Comme $m < n$, ceci contredit la minimalité de n.

Deuxième cas : Supposons n impair. Alors $\Psi_n \in \mathbb{F}_p[X,A;B]$ et donc $f|\Psi_n$. On utilise alors la définition de ϕ_n :

$$\phi_n = X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}$$

pour obtenir que $f|\overline{\Psi}_{n-1}\overline{\Psi}_{n+1}$ donc $f|\overline{\Psi}_{n-1}^2\overline{\Psi}_{n+1}^2$ et donc que $f|\overline{\Psi}_{n\pm1}^2$ par irréductibilité de f. Puis :

$$\overline{\Phi}_{n\pm1} = X\overline{\Psi}_{n\pm1}^2 - \overline{\Psi}_n\overline{\Psi}_{n\pm2} \equiv 0\,[f]$$

puisque $f|\overline{\Psi}_n$. Donc on peut se ramener au premier cas en partant de $n \pm 1$, qui est pair.

□

Proposition I.2.5. *Soit $k \in \mathbb{N}^*$. Si $p^k|n$ alors $\phi_n' \equiv (\Psi_n^2)' \equiv 0\,[p^k]$ (pour $p \geq 3$).*

Démonstration. D'après $(\star)$, on a :

$$\begin{aligned} \frac{\Psi_n^2(x)\phi_n'(x) - (\Psi_n^2)'(x)\phi_n(x)}{\Phi_n^4(x)} &= \frac{d}{dx}\left(\frac{\phi_n(x)}{\Psi_n(x)^2}\right) = \frac{d\mathcal{P}_\Lambda(nz)}{dx} = \frac{dz}{dx}\frac{d\mathcal{P}_\Lambda(nz)}{dz} \\ &= \left(\frac{d\mathcal{P}_\Lambda(z)}{dz}\right)^{-1} n\mathcal{P}_\Lambda'(nz) = \frac{n\mathcal{P}_\Lambda'(nz)}{2y} = \frac{n\Omega_n(x,y)}{y\phi_n(x)^3} \end{aligned}$$

Donc $\Psi_n^2(X)\phi_n'(X) - (\Psi_n^2)'(X)\phi_n(X) = n\phi_n(X)\frac{\Omega_n(X,Y)}{Y} \equiv 0\,[p^k]$. Soient p^{l_1}, p^{l_2} les plus grandes puissances de p divisant respectivement ϕ_n' et $(\Psi_n^2)'$. Il s'agit de montrer que $\min(l_1,l_2) \geq k$. Supposons par l'absurde que le contraire soit vrai. Comme p ne divise ni Φ_n ni Ψ_n^2 d'après le lemme I.2.2, il est nécessaire que $l_1 = l_2$ (vu que $\Psi_n^2(X)\phi_n'(X) - (\Psi_n^2)'(X)\phi_n(X) \equiv 0\,[p^k]$ et que $\min(l_1,l_2) < k$). Posons donc $l := l_1 = l_2$. On a alors :

$$\Psi_n^2(X)(p^{-l}\phi_n'(X)) \equiv (p^{-l}\Psi_n^2)'(X)\phi_n(X)\,[p^{k-l}]$$

avec aucun des ces quatre facteurs divisible par p. Comme $l < k$, cette égalité est en fait une égalité dans $\mathbb{F}_p[X,A,B]$ avec aucun des quatres polynômes nul dans $\mathbb{F}_p[X,A,B]$. Ainsi, $\overline{\Psi}_n^2$ et $\overline{\phi}_n$ étant premiers entre eux dans $\mathbb{F}_p[X,A,B]$ d'après la proposition précédente, on obtient que $\overline{\Psi}_n^2|\overline{p^{-l}\Psi_n^2}'$, ce qui est absurde pour raison de degré. D'où le résultat. □

Proposition I.2.6. *Soit E une corbe elliptique définie sur $\mathbb{F}_q$ ($q = p^N$) de polynôme de Weierstrass :*

$$W(X,Y) = Y^2 - X^3 - AX - B$$

Et $\tilde{E}$ un relèvement p-adique de E à précision ≥ 2 (c'est à dire dont les coeffcients $\tilde{A}$ et $\tilde{B}$ sont égaux à ceux de E modulo p^2). Soit $f \in \mathbb{F}_q[X]$ le polynôme donné par :

$$f(X) = \sum_{k=0}^{\frac{p-1}{2}} \frac{u_k}{u_{\frac{p-1}{2}}} X^k$$

où pour tout $k \in [\![0, \frac{p-1}{2}]\!]$, u_k est le coefficient devant X^{pk} de $\Psi_p(X, A^{p^{N-1}}, B^{p^{N-1}})$. Alors :

$$\Psi_p(X,\tilde{A},\tilde{B}) \equiv f(X)Q(X)\,[p^2]$$

avec $Q(X) \in \mathbb{Z}_q/p^2\mathbb{Z}_q[X]$ et f est sans facteur carré.

Démonstration. On obtient par la proposition précédente que $(\Psi_p(X,\tilde{A},\tilde{B})^2)' = 2\Psi_p(X,\tilde{A},\tilde{B})\Psi'_p(X,\tilde{A},\tilde{B})$ est divisible par p mais que p ne divise pas $\Psi_p(X,\tilde{A},\tilde{B})$ avec le lemme I.2.2 (ici le $'$ est la dérivée selon X). Ainsi, $p|\Psi'_p(X,\tilde{A},\tilde{B})$. On peut donc écrire $\overline{\Psi}_p(X,\tilde{A},\tilde{B})$ sous la forme :

$$\overline{\Psi}_p(X,\tilde{A},\tilde{B}) = \Psi_p(X,A,B) = \lambda g(X^p) = \lambda f(X)^p$$

avec $\lambda \in \mathbb{F}_p^*$ et $f, g \in \mathbb{F}_p[X]$ unitaire (f étant obtenu en prenanant la puissance p^{N-1}-ième des coefficients de g). On obtient de la même manière que :

$$\Psi_p(X, A^{p^{N-1}}, B^{p^{N-1}}) = h(X^p)$$

avec $h \in \mathbb{F}_q[X]$. Or, par propriété de morphisme du Frobénius (en caractéristique p), on obtient que les coefficients de $\Psi_p(X, A^{p^{N-1}}, B^{p^{N-1}})$ sont égaux à ceux de $\Psi_p(X,A,B)$ élevés à la puissance p^{N-1}, de sorte que :

$$f(X) = \sum_{k=0}^{\frac{p-1}{2}} \frac{u_k}{u_{\frac{p-1}{2}}} X^k$$

où pour tout $k \in [\![0, \frac{p-1}{2}]\!]$, u_k est le coefficient devant X^k de h, c'est à dire le coefficient devant X^{pk} de $\Psi_p(X, A^{p^{N-1}}, B^{p^{N-1}})$. On a donc :

$$\Psi_p(X,\tilde{A},\tilde{B}) \equiv f(X)Q(X)\,[p^2]$$

avec $Q(X) \in \mathbb{F}_q[X]$. Cette relation modulo p est en fait valable modulo p^2 mais nous n'avons rien trouvé dans la littérature pour justifier ce résultat.

Les racines de $\overline{\Psi}_p(X,\tilde{A},\tilde{B})$ sont les abscisses des points non nuls de $\pi(\tilde{E}[p]) = E[p]$ donc les racines de f sont les $\frac{p-1}{2}$ abscisses des points non nuls de $E[p]$, ce qui montre que f est sans facteur carré. □

I.3 Relèvement des j-invariants à l'aide du polynôme modulaire.

Proposition I.3.1. *(proposition 7.1.1) Soient $m \in \mathbb{N}^*$ et $z_0, \cdots, z_{N-1} \in \mathbb{Z}_q$ vérifiant pour tout $i \in \{0, \cdots, N-1\}$:*

(i). $z_i \equiv z_{i+1}^p\,[p]$.

(ii). $\overline{z_i}^{p^2} \neq \overline{z_i}$.

(iii). $\Phi_p(z_i, z_{i+1}) \equiv 0\,[p^m]$.

en convenant que $z_N := z_0$. Alors il existe $\zeta_0, \cdots, \zeta_{N-1} \in \mathbb{Z}_q$ dont les coefficients sont déterminés de façon unique modulo p^{2m}, vérifiant pour tout $i \in \{0, \cdots, N-1\}$:

(i). $\zeta_i \equiv z_i\,[p^m]$.

(ii). $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0\,[p^{2m}]$.

en convenant de nouveau que $\zeta_N := \zeta_0$.

De plus, connaissant le résidu modulo p^{2m} de Φ_p, on peut calculer les $\zeta_i\,[p^{2m}]$ en $O(N)$ opérations sur $\mathbb{Z}_q/p^{2m}\mathbb{Z}_q$.

Démonstration. Considérons l'appication :

$$F : (x_0, \cdots, x_{N-1}) \in \mathbb{Z}_q^N \longmapsto (\Phi_p(x_0,x_1), \Phi_p(x_1,x_2), \cdots, \Phi_p(x_{N-1},x_0)) \in \mathbb{Z}_q^N$$

Posons $z := (z_0, \cdots, z_{N-1})$. En écrivant le développement en série de Taylor de chaque composante de F, on trouve que pour tout $\delta \in \mathbb{Z}_q$:

$$F(z + p^m\delta) \equiv F(z) + p^m \mathrm{Jac}_z(F)\,{}^t\delta\,[p^{2m}] \quad (\star)$$

Avec :

$$\mathrm{Jac}_z(F) = \left(\frac{\partial F_i}{\partial x_j}(z)\right)_{1\leq i,j\leq N} = \begin{pmatrix} \frac{\partial \Phi_p}{\partial X}(z_0,z_1) & \frac{\partial \Phi_p}{\partial Y}(z_0,z_1) & 0 & \cdots & 0 \\ 0 & \frac{\partial \Phi_p}{\partial X}(z_1,z_2) & \frac{\partial \Phi_p}{\partial Y}(z_1,z_2) & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ \frac{\partial \Phi_p}{\partial Y}(z_{N-1},z_0) & 0 & \cdots & 0 & \frac{\partial \Phi_p}{\partial X}(z_{N-1},z_0) \end{pmatrix}$$

Or, d'après la relation de Kronecker, qui fait l'objet de la proposition 4.6.8 :

$$\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p)\,[p]$$

Donc :

$$\frac{\partial \Phi_p}{\partial X}(X,Y) \equiv X^p - Y\,[p] \quad \text{et} \quad \frac{\partial \Phi_p}{\partial Y}(X,Y) \equiv Y^p - X\,[p]$$

Donc d'après l'hypothèse (i). $\frac{\partial \Phi_p}{\partial X}(z_i, z_{i+1}) \equiv z_i^p - z_{i+1} \equiv z_{i+1}^{p^2} - z_{i+1}\,[p]$ et $\frac{\partial \Phi_p}{\partial Y}(z_i, z_{i+1}) \equiv z_{i+1}^p - z_i \equiv 0\,[p]$ pour tout $i \in \{0, \cdots, N-1\}$. Donc la réduction modulo p de $\mathrm{Jac}_z(F)$ est la matrice diagonale :

$$\mathrm{Diag}\left(\overline{z_1}^{p^2} - \overline{z_1}, \overline{z_2}^{p^2} - \overline{z_2}, \cdots, \overline{z_0}^{p^2} - \overline{z_0}\right)$$

de déterminant $\prod_{i=0}^{N-1}(\overline{z_i}^{p^2} - \overline{z_i}) \neq \overline{0}$ d'après l'hypothèse (ii).. Ainsi, $v_p\left(\det(\mathrm{Jac}_z(F))\right) = 0$ et donc $\det(\mathrm{Jac}_z(F))$ est dans le groupe des inversibles de $\mathbb{Z}_q$, ce qui assure que $\mathrm{Jac}_z(F)$ est inversible dans $\mathbb{Z}_q$. On peut donc considérer $\delta := -\frac{1}{p^m}\mathrm{Jac}_z(F)^{-1}F(z)$, qui est à priori dans $\mathbb{Q}_q$, mais qui est en fait dans $\mathbb{Z}_q$ d'après l'hypothèse (iii).. Ainsi, en prenant $\zeta := z + p^m\delta$, on obtient par $(\star)$ que les coordonnées ζ_i de ζ vérifient les propriétés (i). et (ii). que l'on devait montrer.

Ayant montré l'existence de ζ, prouvons maintenant l'unicité modulo p^{2m}. Soit $\zeta' \in \mathbb{Z}_q$, une autre solution convenable. Alors en posant $\zeta' := z + p^m\delta'$, on obtient par $(\star)$ que $\mathrm{Jac}_z(F)\,{}^t(\delta - \delta') \equiv 0[p^m]$, et donc $\delta \equiv \delta'[p^m]$ par inversibilité de $\mathrm{Jac}_z(F)$ modulo p^m. Ainsi, $\zeta \equiv \zeta'\,[p^{2m}]$.

Il ne reste plus qu'à vérifier le calcul de complexité. Calculer les N composantes de $F(z)$ et les $2N$ coordonnées non nulles de $\mathrm{Jac}_z(F)$ est fait avec $O(N)$ opérations arithmétiques élémentaires sur $\mathbb{Z}_q/p^{2m}\mathbb{Z}_q$. Pour calculer $\mathrm{Jac}_z(F)^{-1}F(z)$, on résout $\mathrm{Jac}_z(F)X = F(z)$ par la méthode du pivot de Gauss sur les matrices creuses (connaissant la structure de la matrice à l'avance) :

1. On commence par éliminer les termes supra-diagonaux par $N-1$ opérations sur les colonnes successives du type $C_2 \longleftarrow C_2 - a_1C_1$, puis $C_3 \longleftarrow C_3 - a_2C_2$, ..., $C_N \longleftarrow C_N - a_{N-1}C_{N-1}$.
2. Ceci fait apparaître des coefficients potentiellement non nuls sur la dernière ligne que l'on élimine avec $N-1$ opérations sur les ligne du type $L_N \longleftarrow L_N - b_1L_1$, $L_N \longleftarrow L_N - b_2L_2$, ..., $L_N \longleftarrow L_N - b_{N_1}L_{N-1}$.
3. On inverse le système diagonal obenu en N opérations.

Il faut donc $3N-2 = O(N)$ opérations pour calculer $\mathrm{Jac}_z(F)^{-1}F(z)$. Il reste à faire une soustraction dans $\left(\mathbb{Z}_q/p^{2m}\mathbb{Z}_q\right)^N$ pour obtenir $\zeta := z - \mathrm{Jac}_z(F)^{-1}F(z)$, ce qui se fait en temps $O(N)$. D'où la complexité attendue. □

Proposition I.3.2. *(proposition 7.1.2) Supposons que $j(E) \neq j(E)^{p^2}$. Soient $(a_n)_{n\in\mathbb{N}}$ une suite strictement croissante d'entiers naturels non nuls et $(z_{0,n})_{n\in\mathbb{N}}, \cdots, (z_{N-1,n})_{n\in\mathbb{N}}$, N suites d'éléments de $\mathbb{Z}_q$ telles que pour tout $i \in \{0, \cdots, N-1\}$:*

(i). $\overline{z_{i,0}} = j(E_i)$.

(ii). $z_{i,n+1} \equiv z_{i,n}\,[p^{a_n}]$.

(iii). $\Phi_p(z_{i,n}, z_{i+1,n}) \equiv 0\,[p^{a_n}]$.

En convenant toujours que $(z_{N,n})_{n\in\mathbb{N}} = (z_{0,n})_{n\in\mathbb{N}}$. Alors pour tout $i \in \{0, \cdots, N-1\}$, $z_{i,n} \underset{n\to+\infty}{\longrightarrow} j(E_i^{\uparrow})$ et pour tout $n \in \mathbb{N}$, $z_{i,n} \equiv j(E_i^{\uparrow})\,[p^{a_n}]$.

Démonstration. L'isogénie de Frobenius étant de noyau cyclique d'ordre p, le théorème 4.6.9 assure que :

$$\forall 0 \leq i \leq N-1, \quad \Phi_p(j(E_i^{\uparrow}), j(E_{i+1}^{\uparrow})) = 0 \quad (S)$$

Appliquons maintenant la proposition précédente au vecteur $(j(E_i^{\uparrow}))_{0\leq i\leq N-1}$ pour tout $m \in \mathbb{N}^*$. Ceci est possible puisque les hypothèses (ii). et (iii). de cette proposition sont trivialement vérifiées et que l'hypothèse (i). l'est aussi car pour tout $i \in \{0, \cdots, N-1\}$:

$$j(E_{i+1}^{\uparrow}) \equiv j(E_{i+1}) = \frac{1728 * 4\left(A^{p^{i+1}}\right)^3}{4\left(A^{p^{i+1}}\right)^3 + 27\left(B^{p^{i+1}}\right)^2} = \left(\frac{1728 * 4\left(A^{p^i}\right)^3}{4\left(B^{p^i}\right)^3 + 27\left(A^{p^i}\right)^2}\right)^p = j(E_i)^p \equiv j(E_{i+1}^{\uparrow})^p\,[p]$$

On obtient alors que $(j(E_i^{\uparrow}))_{0\leq i\leq N-1}$ est l'unique solution de ce système d'équations modulo p^{2m} pour tout $m \in \mathbb{N}^*$, donc l'unique solution. Par ailleurs, pour tout $i \in \{0, \cdots, N-1\}$, $(z_{i,n})_{n\in\mathbb{N}}$ est de Cauchy d'après l'hypothèse (ii). et par stricte croissance de $(a_n)_{n\in\mathbb{N}}$, donc convergente dans $\mathbb{Q}_q$, qui est complet. La continuité de la valuation p-adique assure qu'en fait la limite z_i de $(z_{i,n})_{n\in\mathbb{N}}$ est dans $\mathbb{Z}_q$. De plus, il est clair que $z_i \equiv z_{i,n}\,[p^{a_n}]$ pour tout $n \in \mathbb{N}$ vu que $(z_{i,m}\,[p^{a_n}])_{m\geq n}$ est stationnaire. L'hypothèse (iii). assure qu'en fait pour tous $i \in \{0, \cdots, N-1\}$ et $n \in \mathbb{N}$:

$$\Phi_p(z_i, z_{i+1}) \equiv \Phi_p(z_{i,n}, z_{i+1,n}) \equiv 0\,[p^{a_n}]$$

donc que $\Phi_p(z_i, z_{i+1}) = 0$ puisque $a_n \underset{n\to+\infty}{\longrightarrow} +\infty$. Comme $(j(E_i^{\uparrow}))_{0\leq i\leq N-1}$ est l'unique solution de (S), on a $z_i = j(E_i)$ pour tout $i \in \{0, \cdots, N-1\}$. □

I.4 Algorithme de calcul du cycle de relèvements p-adiques.

Soit $\tilde{E}$ un relèvement p-adique quelconque de E, de polynôme de Weierstrass $Y^2 - X^3 - \tilde{A}X - \tilde{B}$. Notons pour toute partie S de $\overline{\mathbb{Q}_q}$, $\tilde{E}(S)$ l'ensemble des points de $\tilde{E}$ à coordonnées dans S ($\mathcal{O}$ inclus).

La question est de savoir à quelle précision $\tilde{E}$ doit-elle approcher $E^\uparrow$ pour que $\tilde{E}[p]$ se réduise sur $E[p]$. Pourquoi ceci est-il important ? Parce qu'en fait, $\ker(V_p) = E[p]$. Ainsi, comme $V_p^\uparrow$ est séparable et de même degré que V_p, la proposition 6.1.2 nous donne que $\ker(V_p^\uparrow)$ est l'ensemble des points de $E^\uparrow[p]$ dont les coordonnées sont de valuation positive. On connait alors la réduction de ces points [20] donc en les relevant, on peut en théorie avoir accès à$\ker(V_p^\uparrow)$

Comme $\ker(V_p^\uparrow)$ est un groupe cyclique d'ordre p, il suffit en fait que $\tilde{E}[p] \cap \tilde{E}[\mathbb{Z}_q^{nr}] \neq \{\mathcal{O}\}$ pour que $\tilde{E}[p]$ se réduise sur $E[p]$. Le théorème suivant nous dit quand cela se produit.

Théorème I.4.1. *(théorème 7.2.1) Les assertions suivantes sont équivalents :*

(i). $\tilde{E}[p] \cap \tilde{E}[\mathbb{Z}_q^{nr}] \neq \{\mathcal{O}\}$.

(ii). *Il existe* $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ *tel que* $\tau(pP) \in p^2\mathbb{Z}_q^{nr}$.

(iii). *Il existe* $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ *tel que* $\Psi_p(x(P), \tilde{A}, \tilde{B}) \equiv 0\,[p^2]$.

(iv). $j(\tilde{E}) \equiv j(E^\uparrow)\,[p^2]$.

Démonstration. $(i). \Longrightarrow (ii).$ Si $P \in \tilde{E}[p] \cap E[\mathbb{Z}_q^{nr}] \setminus \{\mathcal{O}\}$ alors $pP = \mathcal{O}$ donc $\tau(pP) = 0 \in p^2\mathbb{Z}_q^{nr}$.

$(i). \Longrightarrow (iii).$ Si $P \in \tilde{E}[p] \cap E[\mathbb{Z}_q^{nr}] \setminus \{\mathcal{O}\}$ alors $\Psi_p(\tilde{A}, \tilde{B}, x(P)) = 0 \equiv 0\,[p^2]$ par définition.

$(i). \Longrightarrow (iv).$ Cette implication est difficile. Satoh utilise notamment un résultat non trivial de Nakamura (voir [13]) pour en donner la preuve. Nous allons donc l'admettre.

$(ii). \Longrightarrow (i).$ Soit $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ tel que $\tau([p]P) \in p^2\mathbb{Z}_q^{nr}$. D'après la proposition H.0.2 (et la remarque qui suit), on dispose de $Q \in \tilde{E}(\mathbb{Z}_q^{nr}) \cap \ker(\pi)$ tel que $\tau(Q) = \tau(pP)$.

On voudrait alors montrer l'existence de $\alpha \in p\mathbb{Z}_q^{nr}$ tel que $[p]\alpha = \tau(Q)$, $[p]$ étant la multiplication par p dans le groupe $p\mathbb{Z}_q^{nr}$ muni de $\oplus_{F_E}$, où F_E est le groupe formel associé à E. On serait tenté d'appliquer la proposition 6.2.3, corollaire de la 5.2.2 mais $p \notin \mathcal{U}(\mathbb{Z}_q^{nr})$. Toutefois, en reprenant la preuve de la proposition 5.2.2, on peut montrer l'existence d'un "inverse" g de $[p]$ dans $\frac{1}{p}\mathbb{Z}_p[\![X]\!]$, comme $\tau(Q) \in p^2\mathbb{Z}_q^{nr}$, on peut poser $\alpha := g(\tau(Q))$, qui est bien dans $p\mathbb{Z}_q^{nr}$ et qui vérifie $[p]\alpha = \tau(Q)$. En posant $Q' := \tau^{-1}(\alpha) \in \tilde{E}(\mathbb{Q}_q^{nr}) \cap \ker(\pi)$ (qui existe d'après la proposition H.0.2 et la remarque qui suit), on obtient que :

$$\tau([p]Q') = [p]\tau(Q') = [p]\alpha = \tau([p]P)$$

Mais :

$$[p]P = \left(-\frac{\tau(P)}{s(\tau(P))}, -\frac{1}{s(\tau(P))}\right)$$

où $s(T)$ est une série formelle définie au paragraphe G.3, dont le premier terme est T^3. On a donc :

$$v_p(x([p]P)) = v_p(\tau(P)) - v_p(\tilde{w}(\tau(P))) = v_p(\tau(P)) - 3v_p(\tau(P)) = -2v_p(\tau(P)) \leq -4$$

donc $[p]P \in \ker(\pi) \cap \tilde{E}(\mathbb{Q}_q^{nr})$. De même, $[p]Q' \in \ker(\pi) \cap \tilde{E}(\mathbb{Q}_q^{nr})$ puisque $Q' \in \ker(\pi) \cap \tilde{E}(\mathbb{Q}_q^{nr})$. Donc $[p]P = [p]Q'$ i.e. $P - Q' \in \tilde{E}[p]$ par injectivité de τ sur $\ker(\pi) \cap \tilde{E}(\mathbb{Q}_q^{nr})$. Puis, comme $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ et $Q' \in \ker(\pi)$, on a $\pi(P - Q') = \pi(P) \neq \mathcal{O}$ donc $P - Q' \in E(\mathbb{Z}_q^{nr})$. D'où (i).

$(iii). \Longrightarrow (ii).$ Soit $P \in E(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ tel que $\Psi_p(\tilde{A}, \tilde{B}, x(P)) \equiv 0\,[p^2]$. Si $pP = \mathcal{O}$ il n'y a rien à prouver. Supposons donc que $pP = \mathcal{O}$. Commençons par remarquer que $\Phi_p(\tilde{A}, \tilde{B}, x(P)) \not\equiv 0[p]$ car sinon $\Phi_p(A, B, X)$ et $\Psi_p(A, B, X)$ ne seraient pas premiers entre eux dans $\mathbb{F}_q[X]$, ce qui contredirait la proposition I.2.4. Ainsi $v_p(\Phi_p(x(P), \tilde{A}, \tilde{B})) = 0$ et donc :

$$v_p(x(pP)) = v_p(\Phi_p(x(P), \tilde{A}, \tilde{B})) - 2v_p(\Psi_p(x(P), \tilde{A}, \tilde{B})) \leq -4$$

En outre :

$$y(pP)^2 = x(pP)^3 + \tilde{A}x(pP) + \tilde{B}$$

avec $v_p(\tilde{A}), v_p(\tilde{B}) = 0$ car $AB \neq 0$ et $v_p(x(pP)) < 0$ donc d'après le point (i). du lemme 2.1.4 :

$$2v_p(y(pP)) = v_p(x(pP)^3 + \tilde{A}x(pP) + \tilde{B}) = 3v_p(x(pP))$$

20. C'est justement parce que le Frobenius est inséparable que nous perdons cette connaissance si l'on remplace V_p par Fr_p. D'où l'intérêt de considérer V_p dans l'algorithme de Satoh.

Donc :

$$v_p(\tau(pP)) = v_p(x(pP)) - v_p(y(pP)) = -\frac{1}{2}v_p(x(pP)) \geq 2$$

Et ainsi $\tau(pP) \in p^2\mathbb{Z}_q^{nr}$. D'où (ii).

$(iv). \Longrightarrow (iii)$. On commence par montrer que $E^\uparrow$ vérifie (iii). On sait que $\pi(\ker(V_p^\uparrow)) = \ker(V_p)$, V_p étant l'isogénie de Verschiebung définie comme l'isogénie duale du p-ième Frobenius. Comme E est supposée ordinaire, $\ker(V_p) = E[p]$. Or, $V_p^\uparrow$ est séparable car toute isogénie est séparable en caractéristique nulle donc $|\ker(V_p^\uparrow)| = \deg(V_p^\uparrow) = \deg(V_p) = p$.

Considérons le polynôme d'annulation de $V_p^\uparrow$:

$$f_{V_p^\uparrow} = \prod_{i=1}^{p}(X - x_i)$$

où les x_i sont les $\frac{p-1}{2}$ abscisses distinctes des éléments de $\ker(V_p^\uparrow)\setminus\{\mathcal{O}\}$. Il est dans $\mathbb{Q}_q[X]$ car V_p est définie sur $\mathbb{Q}_q$. En outre, les x_i se réduisent modulo p en les $\frac{p-1}{2}$ abscisses distinctes des éléments de l'ensemble $\pi(\ker(V_p^\uparrow)) = \ker(V_p) = E[p]$ privé de l'origine. Ceci montre que $f_{V_p^\uparrow}$ est en fait à coefficients dans $\mathbb{Z}_q$ (tous les x_i étant de valuation positive, car sinon le point associé se réduirait sur $\mathcal{O}$) et que la réduction modulo p de $f_{V_p^\uparrow}$ est sans facteur carré. Ainsi, le lemme 2.3.12, les x_i sont tous dans $\mathbb{Z}_q^{nr}$. Ceci montre que si $P \in \ker(V_p^\uparrow) \setminus \{\mathcal{O}\}$, alors $x(P) \in \mathbb{Z}_q^{nr}$. Mais alors $y(P)^2 \in \mathbb{Z}_q^{nr}$ (d'après l'équation de Weierstrass). Ainsi, $y(P)^2 \in \mathbb{K}$ où $\mathbb{K}$ est une extension finie non-ramifiée de $\mathbb{Q}_q$, qui est donc complète ; et $v_p(y(P)^2) = v_p(\tilde{B}) = 0$ d'après l'équation de Weierstrass (puisque $v_p(x(P)) \geq 0$). Donc $X^2 - y(P)^2$ est un polynôme à coefficients dans $\mathbb{K}$ dont la réduction modulo p est sans facteur carré et le lemme 2.3.12 assure alors que $y(P) \in \mathbb{K}^{nr} \subset \mathbb{Z}_q^{nr}$. Donc $P \in E^\uparrow(\mathbb{Z}_q^{nr})$. Comme $\ker(V_p^\uparrow) \subset E^\uparrow[p]$ puisque $\deg(V_p^\uparrow) = p$, on en déduit que $E^\uparrow[p] \cap E^\uparrow(\mathbb{Z}_q^{nr}) \neq \{mO\}$. Comme $(i). \Longrightarrow (iii).$, on en déduit que $E^\uparrow$ vérifie (iii).

Soit $Y^2 - X^3 - A^\uparrow X - B^\uparrow$ un polynôme de Weierstrass associé à $E^\uparrow$. Supposons que $j(\tilde{E}) \equiv j(E^\uparrow)\,[p^2]$. Alors on dispose de $s \in \mathbb{Z}_q$ tel que $j(\tilde{E}) = j(E^\uparrow) + p^2 s$ ie :

$$\frac{1728 * 4\tilde{A}^3}{4\tilde{A}^3 + 27\tilde{B}^2} = \frac{1728 * 4(A^\uparrow)^3}{4(A^\uparrow)^3 + 27(B^\uparrow)^2} + p^2 s \quad (\star)$$

Donc en posant $t := \frac{s}{27\times 1728}$, qui est toujours dans $\mathbb{Z}_q$, puisque p ne divise pas $27 = 3^4$ et $1728 = 2^6\times 3^3$ ($p \geq 5$), on obtient en multipliant l'équation précédente par $\frac{1}{27}(4\tilde{A}^3+27\tilde{B}^2)(4(A^\uparrow)^3+27(B^\uparrow)^2)$:

$$\tilde{A}^3(B^\uparrow)^2 = (A^\uparrow)^3\tilde{B}^2 + p^2 t$$

Donc $\tilde{A} = u^2 A^\uparrow + p^2\frac{t}{\tilde{A}^2(B^\uparrow)^2}$ avec $u := \frac{A^\uparrow\tilde{B}}{\tilde{A}B^\uparrow}$, avec $\frac{t}{\tilde{A}^2(B^\uparrow)^2}, u \in \mathcal{U}(\mathbb{Z}_q)$ puisque $A^\uparrow, B^\uparrow, \tilde{A}, \tilde{B} \in \mathcal{U}(\mathbb{Z}_q)$. Ainsi, $\tilde{A} \equiv u^2 A^\uparrow\,[p^2]$ et en réinjectant ceci dans $(\star)$, on obtient que $\tilde{B} \equiv u^3 B^\uparrow\,[p^2]$.

Comme $u \in \mathcal{U}(\mathbb{Z}_q)$, la réduction modulo p de $X^2 - u$ est scindée à racines simples donc le lemme 2.3.12 assure l'existence de $v \in \mathcal{U}(\mathbb{Z}_q)$ tel que $v^2 = u$. Comme $E^\uparrow$ vérifie $(iii).$, on dispose de $P^\uparrow := (x, y) \in E^\uparrow(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ tel que $\Psi_p(x, A^\uparrow, B^\uparrow) \equiv 0\,[p^2]$. On sait qu'alors, d'après le lemme E.5.7 :

$$\Psi_p(ux, \tilde{A}, \tilde{B}) \equiv \Psi_p(ux, u^2A^\uparrow, u^3B^\uparrow) = u^{\frac{p^2-1}{2}}\Psi_p(x, A^\uparrow, B^\uparrow) \equiv 0\,[p^2]$$

tandis que $y^2 = x^3 + A^\uparrow x + B^\uparrow$, de sorte que $(v^3y)^2 = (ux)^3 + u^2A^\uparrow(ux) + u^3B^\uparrow$ et donc :

$$(vy)^2 - ((ux)^3 + \tilde{A}(ux) + \tilde{B}) \equiv 0\,[p^2]$$

Appliquons le lemme de Hensel (théorème 2.2.1) au polynôme $Q := X^2 - ((ux)^3 + \tilde{A}(ux) + \tilde{B})$, en nous plaçons dans une extension finie non-ramifiée de $\mathbb{Q}_q$ contenant t, que nous noterons $\mathbb{K}$. On sait que $v_p(P(vy)) \geq 2$ et $v_p(Q'(vy)) = v_p(2vy) = 0$ et que $\mathbb{K}$ est complet comme extension finie de $\mathbb{Q}_q$. Le lemme de Hensel assure alors l'existence de $\zeta \in \mathbb{K}$ tel que $Q(\zeta) = 0$ et $v_p(\zeta - vy) \geq 2$. Ainsi, en prenant $P := (x, \zeta)$, on obtient que $P \in \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$ vérifie (iii). Donc $\tilde{E}$ vérifie (iii).

□

Lemme I.4.2. *(lemme 7.2.2) Supposons que $\tilde{E}$ satisfasse l'une des conditions du théorème précédent. Alors pour tout $P \in \tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{nr}) \setminus \{\mathcal{O}\}$:*

$$v_p\left(\frac{\partial\Psi_p}{\partial X}(x(P), \tilde{A}, \tilde{B})\right) = 1$$

Démonstration. $\tilde{E}[p] \cap \ker(\pi)$ est un sous-groupe non trivial de $\tilde{E}[p]$ puisque $\pi : \tilde{E}[p] \longrightarrow E[p]$ n'est pas injective (car $|\tilde{E}[p]| = p^2$ tandis que $|E[p]| = p$). En outre, nous avons vu dans la preuve de la proposition précédente (implication $(iv). \Longrightarrow (iii).$), que π est surjective (puisque $\pi(\ker(V_p^{\uparrow})) = \ker(V_p) = E[p]$ et que $\ker(V_p^{\uparrow}) \subset \tilde{E}[p]$). Ainsi, $\tilde{E}[p] \cap \ker(\pi) \subsetneq \tilde{E}[p]$ et donc ce groupe est cyclique d'ordre p d'après le théorème de Lagrange. En outre, π induit une bijection entre $\tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{nr})$ et $E[p]$ qui préserve la structure de groupe (puisque π est un morphisme de groupes). Donc $\tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{nr})$ est aussi un sous-groupe d'ordre p de $\tilde{E}[p]$.

Considérons donc P et Q des points non nuls respectifs de $\tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{nr})$ et $\tilde{E}[p] \cap \ker(\pi)$. Il engendrent alors ces deux groupes. Comme l'intersection de ces groupes est réduite à $\mathcal{O}$, l'application $(i,j) \in [\![0, p-1]\!]^2 \longmapsto iP + jQ \in \tilde{E}[p]$ est injective donc surjective par égalité des cardinaux, de sorte que :

$$\tilde{E}[p] = \{iP + jQ \mid (i,j) \in [\![0, p-1]\!]^2\}$$

Ainsi, on obtient que l'ensemble des abscisses des points de $\tilde{E}[p]$ est égal à :

$$\left\{x(iP+jQ) \mid (i,j) \in \left[\!\left[1, \frac{p-1}{2}\right]\!\right] \times [\![1, p-1]\!]\right\} \cup \left\{x(iP) \mid i \in \left[\!\left[1, \frac{p-1}{2}\right]\!\right]\right\} \cup \left\{x(jQ) \mid j \in \left[\!\left[1, \frac{p-1}{2}\right]\!\right]\right\}$$

En effet, comme les points opposés, ont même abscisse et que $iP = -(p-i)P$ et $jQ = -(p-j)Q$ pour tous $i, j \in [\![0, p-1]\!]$, il est facile de vérifier que ceci décrit bien toutes les abscisses possibles. Comme il y a au plus $\frac{p^2-1}{2}$ éléments distincts dans cet ensemble, la description donnée est en fait bijective. Ainsi, le p-ième polynôme de division s'écrit :

$$\Psi_p(X, \tilde{A}, \tilde{B}) = p \prod_{\substack{1 \leq i \leq \frac{p-1}{2} \\ 1 \leq j \leq p-1}} (X - x(iP+jQ)) \prod_{i=1}^{\frac{p-1}{2}} (X - x(iP)) \prod_{j=1}^{\frac{p-1}{2}} (X - x(jQ))$$

Et ainsi :

$$\frac{\partial \Psi_p}{\partial X}(x(P), \tilde{A}, \tilde{B}) = p \prod_{\substack{1 \leq i \leq \frac{p-1}{2} \\ 1 \leq j \leq p-1}} (x(P) - x(iP+jQ)) \prod_{i=2}^{\frac{p-1}{2}} (x(P) - x(iP)) \prod_{j=1}^{\frac{p-1}{2}} (x(P) - x(jQ))$$

Posons pour tout $j \in [\![1, p-1]\!]$, $\tau_j := \tau(jQ)$. D'après les résultats du paragraphe 5.3, on a :

$$\forall j \in [\![1, p-1]\!], \quad x(jQ) = \tau_j^{-2} - \tilde{A}\tau_j^2 + O(\tau_j^3) \quad \text{et} \quad y(jQ) = \tau_j^{-3} + \tilde{A}\tau_j^2 + O(\tau_j^3)$$

Ainsi, avec les formules d'addition des points, on obtient que pour tous $(i,j) \in [\![1, p-1]\!]^2$:

$$x(iP+jQ) = \left(\frac{y(jQ) - y(iP)}{x(jQ) - x(iP)}\right)^2 - x(iP) - x(jQ) = x(iP) + 2y(iP)\tau_j + O(\tau_j^2)$$

Comme $iP \notin \ker(\pi)$ pour tout $i \in [\![1, p-1]\!]$, on obtient avec l'équation de Weierstrass que $v_p(y(iP)) = 0$. De plus, comme π induit une bijection entre $\tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{nr})$ et $E[p]$, on a $x(P) \not\equiv x(iP)\,[p]$ pour tout $i \in [\![2, p-1]\!]$. Comme $v_p(\tau_j) \geq 1$ puisque $jQ \in \ker(\pi)$, on en déduit que pour tout $j \in [\![1, p-1]\!]$:

$$v_p(x(P) - x(P+jQ)) = v_p(-2y(iP)\tau_j + O(\tau_j^2)) = v_p(\tau_j)$$

Et pour tous $i \in [\![2, p-1]\!]$ et $j \in [\![1, p-1]\!]$:

$$\begin{aligned} v_p(x(P) - x(iP+jQ)) &= v_p(x(P) - x(iP) + x(iP) - x(iP+jQ)) \\ &= \min(v_p(x(P) - x(iP)), v_p(x(iP) - x(iP+jQ))) = 0 \end{aligned}$$

Enfin, comme $P \notin \ker(\pi)$, $v_p(x(P)) \geq 0$ tandis que $v_p(x(jQ)) < 0$ puisque $jQ \in \ker(\pi)$ et donc :

$$v_p(x(P) - x(jQ)) = v_p(x(jQ)) = -2\tau_j$$

Pour tout $j \in [\![1, p-1]\!]$. D'où :

$$\begin{aligned} v_p\left(\frac{\partial \Psi_p}{\partial X}(\tilde{A}, \tilde{B}, x(P))\right) &= v_p(p) + \sum_{\substack{1 \leq i \leq \frac{p-1}{2} \\ 1 \leq j \leq p-1}} v_p(x(P) - x(iP+jQ)) + \sum_{i=2}^{\frac{p-1}{2}} v_p(x(P) - x(iP)) \\ &\quad + \sum_{j=1}^{\frac{p-1}{2}} v_p(x(P) - x(jQ)) = 1 + \sum_{j=1}^{p-1} v_p(\tau_j) - 2\sum_{j=1}^{\frac{p-1}{2}} v_p(\tau_j) = 1 \end{aligned}$$

où l'on a utilisé le fait que $jQ = -(p-j)Q$ et donc que $\tau_j = -\tau_{p-j}$ pour tout $j \in [\![1, p-1]\!]$. D'où le lemme. □

Théorème I.4.3. *(théorème 7.2.3) Soit $E : Y^2 = X^3 + AX + B$ une courbe elliptique sur $\mathbb{F}_q(q = p^N)$ telle que $j(E) \notin \mathbb{F}_{p^2}$, $E_i(0 \leq i \leq N-1)$ son image par Fr_p^i, $M \geq 2$ un entier. Alors on dispose d'un algorithme pour construire des courbes elliptiques $E^{((i))}$ sur $\mathbb{Z}_q$ et un polynôme $h^{((i))}$ à coefficients dans $\mathbb{Z}_q$ tels que :*

(i).

$$h^{((i))} \equiv \prod_{P \in \frac{G^{((i))} \setminus \{\mathcal{O}\}}{\{-1,1\}}} (X - x(P)) \text{ modulo } p^{M-1}$$

avec $G^{((i))} = E^{((i))}[p] \cap E^{((i))}(\mathbb{Z}_q^{nr})$

(ii). $j(\overline{E^{((i))}}) \equiv j(E^{(i)\uparrow})$ modulo p^M

(iii). $\overline{(A^{((i))})} = A^{p^i}$ et $\overline{(B^{((i))})} = B^{p^i}$

(iv). $G^{((i))}$ est un groupe d'ordre p dont la réduction modulo p est la p-torsion de E_i

Les polynômes $h^{((i))}$ et les coefficients $A^{((i))}$ et $B^{((i))}$ peuvent être calculés avec $O(N \ln(M))$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$.

Démonstration. Relevons tout d'abord les j-invariants. Soient $z_0^{(0)}, \ldots, z_0^{(N-1)}$ des éléments de $\mathbb{Z}_q$ tels que $\overline{z_0^{(i)}} = j(E_{N-i})$. Alors on a bien $z_0^{(i)} \equiv z_0^{(i+1)p}$ modulo p. De plus comme le Frobenius est de degré p, on a $\Phi_p(z_0^{(i)}, z_0^{(i+1)}) = 0$. Enfin, $z_0^{(0)} \notin \mathbb{F}_{p^2}$ donc comme le Frobenius est un morphisme de corps surjectif sur $\mathbb{F}_{p^2}$, $z_0^{(i)} \notin \mathbb{F}_{p^2}$ pour tout i. On peut donc appliquer la proposition 7.1.1 qui nous fournit une suite $(z_k^{(i)})_{k\in\mathbb{N}}$ de $\mathbb{Z}_q$ vérifiant pour tout k, $z_k^{(i)} \equiv z_k^{(i+1)p}$ modulo p, $z_k^{(i)} \equiv z_{k-1}^{(i)}$ modulo p^{2^k} et $\Phi_p\left(z_k^{(i)}, z_k^{(i+1)}\right) \equiv 0$ modulo p. Le corollaire 7.1.2 avec $a_k = 2^k$ montre que pour $0 \leq i \leq N-1$ et $k \in \mathbb{N}$, $z_k^{(i)} \equiv j(E_{N-i}^{\uparrow})$ modulo p^{2^k}. Pour $k_0 = \lceil log_2(M-1) \rceil$ on a $z_{k_0}^{(i)} \equiv j(E_{N-i})[p^{M-1}]$.

On veut maintenant trouver $A^{((i))}$ et $B^{((i))}$ dans $\mathbb{Z}_q$ tels que $j(A^{((i))}, B^{((i))}) = z_{k_0}^{(N-i)}$. c'est-à-dire

$$(4z_{k_0}^{(N-i)} - 1728)A^{((i))3} + 27z_{k_0}^{(N-i)}B^{((i))2} = 0$$

Soit $B^{((i))} \in \mathbb{Z}_q$ un relèvement de B_i et posons

$$P = (4z_{k_0}^{(N-i)} - 1728)X^3 + 27z_{k_0}^{(N-i)}B^{((i))3}$$

Alors $P \in \mathbb{Z}_q[X]$, et

$$\overline{P} = (4j(E_i) - 1728)X^3 + 27j(E_i)B^{(i)^3}$$

Donc $\overline{P}$ admet A_i pour racine simple. Donc d'après le lemme de Hensel on dispose de $A^{((i))}$ une racine de P dont la réduction modulo p vaut A_i et qui s'obtient en $O(\log(M))$ itérations de Newton. La courbe définie par $A^{((i))}$ et $B^{((i))}$ vérifie bien les conditions (ii) et (iii) du théorème.

Étudions le groupe $G^{((i))}$. D'une part, d'après la condition (ii), la courbe $E^{((i))}$ vérifie les conditions du théorème 7.2.1 donc $G^{((i))}$ n'est pas réduit à $\mathcal{O}$. Comme c'est un sous-groupe de $E^{((i))}[p]$ qui est d'ordre p^2, $G^{((i))}$ est d'ordre p ou p^2. D'autre part, la réduction modulo p π induit un morphisme de groupes de $G^{((i))}$ vers $E_i[p]$ dont le noyau est réduit à $\mathcal{O}$ d'après la proposition H.0.2. Comme $E_i[p]$ est d'ordre p, on en déduit que $G^{((i))}$ est d'ordre p et la réduction de $G^{((i))}$ modulo p est $E_i[p]$.

Relevons à présent le polynôme de division. $(E_i[p]\setminus\{\mathcal{O}\})/\{\pm 1\}$ a $\frac{p-1}{2}$ éléments d'abscisses deux à deux distinctes, toutes racines de $\overline{\Psi_p(X, A^{((i))}, B^{((i))})}$. Par ailleurs on dispose (voir proposition I.2.6) d'un polynôme unitaire $f \in \mathbb{Z}_q[X]$ tel que $\overline{f}$ est séparable vérifiant :

$$\Psi_p(X, A_{i-1}, B_{i-1}) = \overline{\Psi_p(X, A^{((i-1))}, B^{((i-1))})} = \lambda \overline{f}^p$$

Dont l'expression est donnée par :

$$\overline{f}(X) = \sum_{k=0}^{\frac{p-1}{2}} \frac{u_k}{u_{\frac{p-1}{2}}} X^k$$

où pour tout $k \in [\![0, \frac{p-1}{2}]\!]$, u_k est le coefficient devant X^{pk} de $\Psi_p(X, A_{i-1}, B_{i-1})$. Or on sait (proposition I.2.5) que p divise $\frac{\partial \Psi_p(X, A^{((i))}, B^{((i))})}{\partial X}$ et d'après le lemme 7.2.2 et ce qui précède, les racines de $\overline{f}$ ne sont pas racines de $p^{-1}\frac{\partial \Psi_p(X, A^{((i))}, B^{((i))})}{\partial X}$.

Comme on a de plus que f divise $\Psi_p(X, A^{((i))}, B^{((i))})$ modulo p^2, on peut appliquer plusieurs fois le lemme I.1.3 en initialisant à $u = 1$ et $t = 1$. On obtient alors une suite de polynômes unitaires de degré $\frac{p-1}{2}$ $f_k \in \mathbb{Z}_q[X](k \geq 1)$ avec $f_1 = f$. La suite $(f_k)_{k\geq 1}$ vérifie les hypothèses du lemme I.1.4 avec $a_k = 2^{2^k}$. La suite f_k converge donc vers un facteur h de $\Psi_p(X, A^{((i))}, B^{((i))})$ avec $\overline{h^{((i))}} = \overline{f}$ et h unitaire de degré $(p-1)/2$. On en déduit que h est séparable, donc ses racines sont exactement les abscisses d'éléments de $G^{((i))}$. On obtient alors $h^{((i))}$ vérifiant la propriété (i) avec $\lceil log(M-1) \rceil$ applications du lemme I.1.3. □

I.5 Calcul effectif de la trace du Frobenius et comptage de points.

Proposition I.5.1. *Soient $i \in \{1, \cdots, N\}$ et $\tau_i := -\frac{X}{Y}$ le paramètre local en $\mathcal{O}$ de $E_i^\uparrow$ et $c_{i,1} \in \mathbb{Z}_q$ le premier coefficient du développement du Verschiebung V_i :*

$$\tau_{i-1} \circ V_i = \sum_{n=1}^{\infty} c_{i,n} \tau_i^n$$

On suppose connus les coefficients $A_i^\uparrow$, $B_i^\uparrow$ et le polynôme unitaire et séparable $h_i^\uparrow(X)$ dont les racines sont les abscisses des points du groupe $G_i := E_i^\uparrow[p] \cap E_i^\uparrow(\mathbb{Z}_q^{nr})$ privé de $\mathcal{O}$. Alors on peut calculer $c_{i,1}^2$ avec $O(1)$ opérations sur $\mathbb{Z}_q$.

Démonstration. Le théorème E.9.5 (et la remarque qui suit) assurent l'existence d'une isogénie $v_i \in \mathrm{Hom}(E_i^\uparrow, E_i^\uparrow/G_i)$ (il s'agit de celle construite par Vélu dans [10] avec les formules présentées à la fin de la section 3). Or, on a vu que $G_i = \ker(V_i)$ (en effet, $\pi(G_i) = E_i[p] = \ker(V_p) = \pi(\ker(V_p^\uparrow))$ et $|\ker(V_p)| = \deg(V_p) = p = |G_i|$). Ainsi, la proposition E.9.3 assure l'existence d'une isogénie $\lambda \in \mathrm{Hom}(E_i^\uparrow/G_i, E_{i-1}^\uparrow)$ telle que $\lambda \circ v_i = V_i$. Comme $p = |\ker(V_i)| = |\ker(\lambda \circ v_i)| = |\ker(\lambda)||\ker(v_i)| = |\ker(\lambda)|p$, on a $\ker(\lambda) = \{\mathcal{O}\}$ et donc λ est un isomorphisme d'après la proposition E.9.4. On peut donc écrire, d'après la proposition 3.3.8 :

$$\lambda(X, Y) := (\gamma_i^2 X, \gamma_i^3 Y)$$

avec $\gamma_i^2 = \frac{\alpha_i B_{i-1}^\uparrow}{\beta_i A_{i-1}^\uparrow}$, α_i et β_i étant les coefficients de l'équation de Weierstrass $Y^2 = X^3 + \alpha_i X + \beta_i$ de $E_i^\uparrow/G_i$. Les formules de Vélu donnent α_i et β_i en fonction des coefficients s_j de $X^{\frac{p-1}{2}-j}$ de $h_i^\uparrow$:

$$\alpha_i := A_i^\uparrow - 5 \sum_{P \in G_i \setminus \{\mathcal{O}\}} (3x(P)^2 + A_i^\uparrow) = (6-5p)A_i^\uparrow - 30(s_1^2 - 2s_2)$$

$$\beta_i := B_i^\uparrow - 7 \sum_{P \in G_i \setminus \{\mathcal{O}\}} (5x(P)^3 + 3A_i^\uparrow x(P) + 2B_i^\uparrow) = (15-14p)B_i^\uparrow - 70(s_1^3 - 3s_1 s_2 + 3s_3) + 42A_i^\uparrow s_1$$

Connaissant $h_i^\uparrow$, ces nombres sont donc calculables en $O(1)$ opérations sur $\mathbb{Z}_q$.

Les formules de Vélu assurent aussi que le $\tilde{\tau}_i \circ v_i = \tau_i + O(\tau_i^2)$ ($\tilde{\tau}_i$ désignant le paramètre local en $\mathcal{O}$ de $E_i^\uparrow/G_i$). Et de plus $\tau_{i-1} \circ \lambda = \frac{\tau_i}{\gamma_i}$ donc :

$$\tau_{i-1} \circ V_i = \tau_{i-1} \circ (\lambda \circ v_i) = \frac{\tau_i}{\gamma_i} + O(\tau_i^2)$$

De sorte que $c_{1,i} = \frac{1}{\gamma_i}$, puis $c_{1,i}^2 = \frac{1}{\gamma_i^2} = \frac{\beta_i A_{i-1}^\uparrow}{\alpha_i B_{i-1}^\uparrow}$, ce qui s'obtient en $O(1)$ opérations sur $\mathbb{Z}_q$. □

Théorème I.5.2. *Soit E une courbe elliptique non supersingulière définie sur $\mathbb{F}_q$, avec $q := p^N$. Si $j(E)^{p^2} \neq j(E)$, alors on il existe un algorithme permettant de déterminer $|E(\mathbb{F}_q)|$ avec $O(N \ln(M))$ opérations dans $\mathbb{Z}_q/p^M\mathbb{Z}_q$ (pour $M := \lfloor \frac{N}{2} \rfloor + 3$) et $O(N^2)$ opérations dans $\mathbb{F}_q$.*

Démonstration. D'après la proposition 6.2.4 et les propriétés du relèvement p-adique des isogénies :

$$\mathrm{Tr}(\mathrm{Fr}_q) = \mathrm{Tr}(V_{N-1}^\uparrow \circ \cdots \circ V_0^\uparrow) = c + \frac{q}{c}$$

avec $c := \prod_{i=0}^{N-1} c_{i,1}$. Comme $|\mathrm{Tr}(\mathrm{Fr}_q)| \leq 2\sqrt{q}$ d'après le théorème de Hasse, il suffit de connaître c modulo p^M avec $M := \lfloor \frac{N}{2} \rfloor + 3$. D'après le théorème 7.2.3, on peut trouver pour tout $i \in \{0, \cdots, N-1\}$, $\tilde{A}_i = A_i^\uparrow[p^M]$, $\tilde{B}_i = B_i^\uparrow[p^M]$ et $\tilde{h}_i(X) \equiv h_i^\uparrow(X)[p^M]$ avec $O(N \ln(M))$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$ et $O(N^2)$ opérations sur $\mathbb{F}_q$. D'après la proposition précédente, on peut obtenir les $c_{i,1}^2$ modulo p^M en $O(1)$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$ donc c^2 en $O(N)$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$ (après avoir effectué le produit).

En notant A_{p^r} le coefficient devant $X^{\frac{p^r-1}{2}}$ de $(X^3 + AX + B)^{\frac{p^r-1}{2}}$ pour tout $r \in \mathbb{N}^*$, on obtient par le lemme E.11.3 que :

$$A_q \equiv \mathrm{Tr}(\mathrm{Fr}_q) = c + \frac{q}{c} \equiv c\,[p]$$

Et grâce à la relation de récurrence $A_{p^{r+1}} = A_p^{p^r} A_{p^r}$ on sait que l'on peut obtenir A_q en $O(N)$ opérations sur $\mathbb{F}_q$. Connaissant $c^2\,[p^M]$ et $c\,[p]$, on peut retrouver $c\,[p^M]$ en $O(\ln(M))$ opérations sur $\mathbb{Z}_q/p^M\mathbb{Z}_q$ avec la méthode de Newton (utilisée dans la preuve du lemme de Hensel). On en déduit alors $\mathrm{Tr}(\mathrm{Fr}_q) = c + \frac{q}{c}$ et donc $|E(\mathbb{F}_q)| = 1 + q - \mathrm{Tr}(\mathrm{Fr}_q)$ (d'après le théorème de Hasse) avec au total $O(N \ln(M))$ opérations dans $\mathbb{Z}_q/p^M\mathbb{Z}_q$ et $O(N^2)$ opérations dans $\mathbb{F}_q$. □

I.6 Cas $j(E) \in \mathbb{F}_{p^2}$.

Supposons à présent que $j = j(E) \in \mathbb{F}_{p^2}$ (ie que $j(E) = j(E)^{p^2}$). Soit $m \in \{1, 2\}$ tel que $p^m = |\mathbb{F}p(j)|$. Ainsi $m = 1$ si $j \in \mathbb{F}p$ et $m = 2$ sinon. L'idée est de construire une courbe elliptique sur $\mathbb{F}_{p^m}$ isomorphe à E sur $\mathbb{F}_q$. On remarquera que **l'algorithme décrit ici ne fonctionne que pour $\frac{N}{m}$ impair.**

Proposition I.6.1. *Il existe une courbe elliptique E' sur $\mathbb{F}_{p^m}$ telle que $j(E') = j$.*

Démonstration. En effet, plaçons-nous momentanément dans le corps $\mathbb{F}_{p^m}$ et supposons $j \neq 0$ et $j \neq 1728$. Alors la courbe elliptique

$$(E') : y^2 + xy = x^3 - \frac{36}{(j-1728)^3}x - \frac{1}{j-1728}$$

définie sur $\mathbb{F}_{p^m}$ a pour j-invariant j. Sinon, les courbes

$$(E') : y^2 + y = x^3, j = 0$$

et

$$(E') : y^2 = x^3 + x, j = 1728$$

conviennent. □

Proposition I.6.2. *Soit N tel que $q = p^N$. Alors $m|N$.*

Démonstration. Supposons $m = 2$ (sinon $m = 1$ et c'est immédiat) et rappellons que $Fq = \{u \in \overline{\mathbb{F}_q} \mid u^q = u\}$. Soit alors la divisions euclidienne de N par 2 : $N = 2 * a + r$. $j \in \mathbb{F}_{p^2}$ donc $j^{p^2} = j$. En élevant a fois cette égalité à la puissance p^2, on obtient $j^{p^{2a}} = j$ puis $j^q = j^{p^r}$. Comme $j \in \mathbb{F}q$, $j^q = j$. Comme $m = 2$, $j^p \neq j$. Or $j^{p^r} = j$ donc $r = 0$. □

Soit E' une courbe elliptique sur $\mathbb{F}_{p^m}$ telle que $j(E') = j$. On met l'équation de Weierstrass sous forme canonique :

$$(E') : y'^2 = x'^3 + A'x' + B'$$

et on cherche un isomorphisme entre les courbes $E(\mathbb{F}q)$ et $E'(\mathbb{F}_q)$ sous la forme $(x, y) \mapsto (u^2x, u^3y)$ pour $u \in \mathbb{F}_q^*$. Si un tel isomorphisme existait, on aurait $u^4A = A'$ et $u^6B = B'$. Il s'agit donc de savoir s'il existe un élément $u = (\frac{B'}{B})^{1/6} = (\frac{A'}{A})^{1/4}$ dans $\mathbb{F}_q$.

Pour ce faire, on se place dans le cas particulier $AB \neq 0$. Alors $j \neq 0$ et $j \neq 1728$. On vérifie si $(\frac{AB'}{A'B})^{\frac{q-1}{2}} = 1$, auquel cas l'élément $u^2 = \frac{AB'}{A'B}$ possède une racine carrée dans $\mathbb{F}_q$. Alors $E_0 = E'$ est isomorphe à E sur $\mathbb{F}q$. Sinon, on s'intéresse à la courbe

$$(E_0) : y'^2 = x^3 + d^2A'x + d^3B'$$

où d est un élément de $\mathbb{F}_{p^m}$ qui ne possède pas de racine carrée dans $\mathbb{F}_q$. **Notons qu'un tel élément existe si et seulement si $\frac{N}{m}$ est impair.** On effectue alors un twist de la courbe E' qui n'est pas isomorphe à E' sur $\mathbb{F}_q$. En remarquant que E, E' et E_0 ont le même j-invariant, elles sont donc isomorphes sur $\overline{\mathbb{F}_p}$ comme expliqué plus haut (la question de l'appartenance de u à $\overline{\mathbb{F}p}$ ne se pose pas). Ainsi, comme ni E et E' ni E' et E_0 ne sont isomorphes sur $\mathbb{F}_q$ et qu'il n'y a que deux classes d'équivalence d'isomorphisme (selon que u est un carré ou non), on en déduit que E et E_0 sont isomorphes sur $\mathbb{F}_q$.

Proposition I.6.3. *Pour $i \in [\![0, \frac{N}{m}]\!]$, on définit $T_i = Tr(Fr_{p^m}^i)$ la trace du Frobenius p^m itéré i fois sur la courbe E_0. Alors*

$$T_{i+2} - T_1T_{i+1} + p^mT_i = 0$$

Démonstration. On se place dans le module de Tate $T_l(E_0)$ pour l premier différent de p. On considère le polynôme caractéristique de l'application $\mathbb{Z}_l$-linéaire induite par Fr_{p^m} sur $T_l(E_0)$:

$$\chi := X^2 - \mathrm{Tr}(\mathrm{Fr}_{p^m})X + \det(\mathrm{Fr}_{p^m}) = X^2 - T_1X + \deg(\mathrm{Fr}_{p^m}) = X^2 - T_1X + p^m$$

Le théorème de Cayley-Hamilton (vrai aussi pour les modules), donne alors que :

$$\mathrm{Fr}_{p^m}^2 - T_1\mathrm{Fr}_{p^m} + p^m\mathrm{id}_{T_l(E')} = 0$$

On obtient alors le résultat en composant par $\mathrm{Fr}_{p^m}^i$ à droite et en prenant la trace.

Sachant que $T_0 = 2$ et que $T_1 = 1 + p^m - |E_0(\mathbb{F}_{p^m})|$, on peut en déduire la valeur de $T_{\frac{N}{m}}$. **Finalement,** on peut en déduire $|E(\mathbb{F}q)| = |E_0(\mathbb{F}q)| = 1 + q - T_{\frac{N}{m}}$. □

On en déduit le :

Théorème I.6.4. *Lorsque $j(E) \in \mathbb{F}_{p^2}$ et que $\frac{N}{[\mathbb{F}_p(j(E)):\mathbb{F}_p]}$ est impair, il exixte un algorithme pour calculer $|E(\mathbb{F}_q)|$ en temps $O(N)$.*

Démonstration. On peut compter naïvement les points sur $E_0(\mathbb{F}_{p^m})$ en temps $O(p^m) = O(1)$ (p étant fixé et petit). Il suffit alors d'itérer $\frac{N}{m} - 2$ fois la suite $(T_i)_{i\in\mathbb{N}^*}$ de la proposition précédente pour trouver $\mathrm{Tr}(\mathrm{Fr}_q)$, et donc $|E(\mathbb{F}_q)| = q + 1 - \mathrm{Tr}(\mathrm{Fr}_q)$. □

I.7 Code de l'algorithme de Satoh.

Voici le code de l'algorithme de Satoh que nous avons utilisé lors de nos tests de temps. Nous avons utilisé le langage Sage créé notamment à partir de Python.

Nous avons constaté que la précision préconnisée par Satoh $M = \lfloor \frac{N}{2} \rfloor + 3$ n'est pas suffisante, notamment parce que la fonction lifth (qui trouve les facteurs $h^{((i))}$ du théorème 7.2.3) fait perdre en précision puisqu'elle mobilise beaucoup d'opérations de division. Pour N suffisament grand $M = N$ suffit mais pour $N < 20$, il faut en général prendre $M > N$. Régler la précision est en fait l'une des principales difficultés pratiques que nous avons rencontrées dans l'implémentation.

```
# donnees de base.

p = 5
N = 50
q = p^N

# precision
M = N

# Corps de base Q_q (q=p^N) de generateur a
# Attention : a reduit modulo p donne un generateur de Fq. Pour faire
    facilement des calculs dans Fq, on ne se preocupera que des termes
    modulo p, quitte a tronquer les autres termes sans perdre en precision a
     l'aide de la fonction liftto.
K.<a> = Qq(q, prec=M)

# Corps fini Fq de generateur g (dont le polynome minimal est la reduction
    modulo p du polynome minimal de a):
Fq.<g> = GF(q)

#anneau des polynomes a une variable Q_q[Z].
Ann1.<z> = K[]

#anneau des polynomes a deux variables Q_q[X, Y].
Ann2.<x, y> = K[]

# Attention, on prendra garde au fait que les polynomes a une variable s'
    ecrivent en z et que les polynomes a deux variables s'ecrivent en x et y
    .

#polynome modulaire (pour p=5, changer pour p different) donne par https://
    math.mit.edu/~drew/ClassicalModPolys.html
Phi = K(1413599471547213586977534746910713627510046720000)+K
    (5327433080342442545042016027335650915123200 0)*(x+y)+K
    (-2640734570766205962597157902479787829493 76)*x*y+K
    (6692500042627997708487149415015068467200)*(x^2+y^2)+K
    (3655473658394962929570647233265664000 0)*(x^2*y+x*y^2)+K
    (5110941777552418083110765199360000)*x^2*y^2+K
    (2802447778284395278043215652978688 00)*(x^3+y^3)+K
    (-1924579346189282996551082311680 00)*(x^3*y+x*y^3)+K
    (2689848885838073157741772800 0)*(x^3*y^2+x^2*y^3)+K
    (-4412069655129148352461 00)*x^3*y^3+K(1284733132841424456253440)*(x^4+y
    ^4)+K(1285417989068288163840 00)*(x^4*y+x*y^4)+K(3830836097798112153 75)*(
```

```
    x^4*y^2+x^2*y^4)+K(107878928185336800)*(x^4*y^3+x^3*y^4)+K
    (1665999364600)*x^4*y^4+K(1963211489280)*(x^5+y^5)+K(-246683410950)*(x
    ^5*y+x*y^5)+K(2028551200)*(x^5*y^2+x^2*y^5)+K(-4550940)*(x^5*y^3+x^3*y
    ^5)+K(3720)*(x^5*y^4+x^4*y^5)+K(-1)*x^5*y^5+K(1)*(x^6+y^6)

# Anneau des matrices N*N aux coefficients dans A
M_N = MatrixSpace(K,N,N, sparse=True)
M_N1 = MatrixSpace(K,N,1, sparse=True)

# Fonction de relevement (ou de reduction) a precision donnee
def liftto(b,n):
        prec = b.precision_absolute()
        liftb = O(p^n)
        bList = b.expansion()
        for i in range(min(prec,n)):
                for j in range(len(bList[i])):
                        liftb = liftb + bList[i][j]*a^j*5^i
        return liftb


# Fonction de reduction de Qq dans Fq.
def down(A):
        alpha = Fq(0)
        Aliste = A.expansion()
        for i in range(len(Aliste[0])):
                alpha += Aliste[0][i]*g^i
        return alpha

## Generation aleatoires d'elements dans le corps
def rd():
        s = K(0)
        for i in range(N):
                s += randint(0,p-1)*a^i
        return s

# Generation aleatoire de deux elements non nuls.
def ABz():
        A = rd()
        B = rd()
        while A == 0:
                A = rd()
        while B == 0:
                B = rd()
        return A,B

# AB() permet de generer aleatoirement A et B dans Fq
def AB():
        A,B = ABz()
        d = 4*A^3+27*B^2
        while d == 0:
                A,b = ABz()
                d = 4*A^3+27*B^2
        return A,B

# Fonction de relevement des j-invariants (j fourni)
def liftJ(j):
        Z = M_N1(0)
        Z[0,0] = j
        for i in range(1,N):
                Z[i,0] = Z[i-1,0]^p
        d = {(N-1,0):diff(Phi,y),(N-1,N-1):diff(Phi,x)}
```

```
        for i in range(N-1):
                d[(i,i)] = diff(Phi,x)
                d[(i,i+1)] = diff(Phi,y)
        stop = 1
        while stop < M:
                stop = 2*stop
                e = {(N-1,0):d[(N-1,0)](Z[N-1,0],Z[0,0]),(N-1,N-1):d[(N-1,N
                    -1)](Z[N-1,0],Z[0,0])}
                for i in range(N-1):
                        e[(i,i)] = d[(i,i)](Z[i,0],Z[i+1,0])
                        e[(i,i+1)] = d[(i,i+1)](Z[i,0],Z[i+1,0])
                Jac = M_N(e)
                F = M_N1(0)
                F[N-1,0] = Phi(Z[N-1,0],Z[0,0])
                for i in range(N-1):
                        F[i,0] = Phi(Z[i,0],Z[i+1,0])
                Z = Z-Jac^-1*F
        return Z

# Methode de Newton a une variable pour relever la racine xi d'un polynome
    P a precision M. Attention, les polynomes univaries portent la variable
    z.
def Newt(P,xi):
        Pprime = diff(P,z)
        zeta = xi
        stop = 1
        while stop < M:
                zeta = zeta-P(zeta)/Pprime(zeta)
                stop = stop*2
        return zeta

# relevement des A_i et B_i. Les B_i sont les memes, seuls les A_i sont
    releves.
def liftAB(A,B,j):
        Z = liftJ(j)
        relA = M_N1(0)
        relB = M_N1(0)
        relA[0] = A
        relB[0] = B
        for i in range(1,N):
                relA[i,0] = relA[i-1,0]^p
                relB[i,0] = relB[i-1,0]^p
        for i in range(N):
                relA[i,0] = Newt(4*(1728-Z[i,0])*z^3-27*Z[i,0]*relB[i,0]^2,
                    relA[i,0])
        return [relA,relB]

# Relevement d'un facteur polynomial a la precision M (traduction du
    travail de Gustave en Sage). Attention, les polynomes univaries sont
    selon la variable z.

def lift_P(P,U,t=1):
        Q = P
        u = 1
        R0 = p^(-t-u)*(U%Q)
        R1 = p^(-t)*diff(U,z)
        while u < M:
                B1 = xgcd(Q,R1)[2]*R0
                R2 = (diff(Q,z)*B1)%Q
                Q = Q+p^u*R2
                u = 2*u
```

```
                R0 = p^(-t-u)*(U%Q)
        return Q

# Calcul du p-ieme polynome de division pour p=5 (changer pour p different)
    .

def divpol(A,B):
        return 32*(z^3+A*z+B)^2*(z^6+5*A*z^4+20*B*z^3-5*A^2*z^2-4*A*B*z-A
            ^3-8*B^2)-(3*z^4+6*A*z^2+12*B*z-A^2)^3

## relevement du facteur h du p-ieme polynome de division

# Cette fonction extrait le facteur f a partir du polynome Psi_p(A^(i-1),B
    ^(i-1))

def extract(Psi):
        L = list(Psi)
        i = 0
        f = Ann1(0)
        l = liftto(liftto(L[p*(p-1)//2],1),M)
        while p*i <= len(L):
                f += liftto(liftto(L[p*i],1),M)/l*z^i
                i += 1
        return f

# Cette fonction calcule les h^(i) en prenant liftAB(A,B) en argument

def lifth(rel):
        relA,relB = rel[0],rel[1]
        Psi = []
        for i in range(N):
                Psi.append(divpol(relA[i][0],relB[i][0]))
        H = []
        for i in range(N):
                f = extract(Psi[i-1])
                H.append(lift_P(f,Psi[i]))
        return H

# Calcul de la trace modulo p (qui donne aussi un critere de
    supersingularite).

def trmod(A,B):
        P = (z^3+A*z+B)^((p-1)/2)
        t1 = list(P)[p-1]
        t = t1
        for i in range(1,N):
                t = t*t1^(p^i)
        return t

# Convertit un element de Qp en entier (utile pour calculer la trace).

def convtest(c,val):
        intc = 0
    prec = len(c)
        for i in range(min(prec,N//2+1)):
                if len(c[i])>0:
                        intc+=c[i][0]*p^(i+val)
        return intc

def toInt(c):
        if c == 0:
```

```
                return 0
        prec = c.precision_absolute()
    intC = 0
    cList = c.expansion()
    if prec <= N//2+1:
    # Pas de terme de rang N//2+1.
                val = valuation(c,p)
                for i in range(prec):
                        if len(cList[i]) > 0:
                                intC += cList[i][0]*p^(i+val)
                if N%2 == 0:
                        if intC > 2*p^(N//2):
                                return intC-p^prec
                        else:
                                return intC
                elif intC > 2*p^(N//2)*sqrt(float(p)):
                        return intC - p^prec
                else:
                        return intC
        if len(cList[N//2+1]) > 1:
    # Le terme de rang N//2+1 n'est pas fiable
                val = valuation(c,p)
                test = convtest(cList,val)
                if N%2 == 0:
                        if test > 2*p^(N//2):
                c = -c
                cList = c.expansion()
                                return -convtest(c,val)
                        else:
                                return test
        if len(cList[N//2+1]) > 0 and cList[N//2+1][0] == p-1:
                pos = 0
                exp = p^valuation(c,p)
                intC += (cList[pos][0]-5)*exp
                pos += 1
                exp *= p
                while pos < N//2+1:
                        if len(cList[pos]) == 0:
                                intC += (1-p)*exp
                        else:
                                intC += (1-p+cList[pos][0])*exp
                        pos += 1
                        exp *= p
        else:
                val = valuation(c,p)
                for i in range(N//2+1):
                        if len(cList[i]) > 0:
                                intC += cList[i][0]*5^(i+val)
        return intC

## Fonctions qui s'utilisent dans le cas j\in\mathbb{F}_{p^2}

# Cette fonction renvoit un element de \mathbb{F}_{p^m} qui n'est pas un
    carre dans \mathbb{F}_q.

def non_carre(p,m,j):
        d = j
        if m == 1:
                while d^((p-1)//2) != -1:
                        d += j
                return d
```

```
        for i in range(p):
                for k in range(p):
                        if d^((p^2-1)//2) == -1:
                                return d
                        d += 1
                d += j
        return null

# Cette fonction execute l'algorithme decrit dans la section precedente.

def Fp2(A,B):
        j = 1728*4*A^3/(4*A^3+27*B^2)
        m = 2
        if j^p == j:
                m = 1
        d = 1+1728/(j-1728)
        a1 = -27*d
        b1 = 54*d
        d = 1
        if (A*b1/(a1*B))^((q-1)//2) != 1:
                if (N//m)%2 == 0:
                        print("Cas non implemente")
                        return 0
                d = non_carre(p,m,j)
        a1 = a1*d^2
        b1 = d^3*b1
        c = 1
        if m == 1:
                for i in range(p):
                        x = Fq(i)
                        s = x^3 + a1*x + b1
                        if s == 0:
                                c+=1
                        elif s^p == s and s^((p-1)//2) == 1:
                                c += 2
        else:
                x = Fq(0)
                for i in range(p):
                        for k in range(p):
                                s = x^3+a1*x+b1
                                if s == 0:
                                        c += 1
                                elif s^(p^2) == s and s^(((p^2)-1)//2) ==
                                    1:
                                        c += 2
                                x = x + 1
                        x = x + j
        T1 = 1 + p^m - c
        c = 2
        d = T1
        for i in range(1, N/m):
                e = c
                c = d
                d = T1*d-p^m*e
        return 1+q-d

## Fonctions qui permettent de tester le cas particulier precedant.
def jp2():
                j = Fq(0)
                if N%2 == 1:
                        j = Fq(randint(1,p-1))
```

```
                else:
                        j = Fq(randint(0,p-1))*self.g^((q-1)//(p^2-1))
                        if j == 0:
                                j += Fq(randint(1,p-1))
                        else:
                                j += Fq(randint(0,p-1))
                return j

        def ABp2():
                j = jp2()
                while j == 1728:
                        j = jp2()
                d = 1+1728/(j-1728)
                a1 = -27*d
                b1 = 54*d
                return a1,b1

def testp2():
        A,B = ABp2()
    return Fp2(A,B) == EllipticCurve(Fq,[A,B]).cardinality()

## Cette fonction applique les formules de Velu pour calculer la trace. C'
    est le resultat final.

def Satoh(A,B):
        t = trmod(A,B)
        if t.residue(1)==0:
                print("La courbe est supersinguliere donc l'algorithme de
                    Satoh ne donne pas le bon resultat.")
                return 0
        j = 1728*4*A^3/(4*A^3+27*B^2)
        if (j+O(p))^(p^2) == j + O(p):
                return Fp2(down(A),down(B))
        rel = liftAB(A,B,j)
        relA, relB = rel[0], rel[1]
        H = lifth(rel)
        c2 = K(1)
        for i in range(N):
                L = list(H[i])
                s1 = L[(p-1)//2-1]
                s2 = L[(p-1)//2-2]
                s3 = K(0)# a changer pour p different de 5
                alpha = (6-5*p)*relA[i,0]-30*(s1^2-2*s2)
                beta = (15-14*p)*relB[i,0]-70*(-s1^3+3*s1*s2-3*s3)+42*relA[
                    i,0]*s1
                c2 = c2*relA[i-1][0]*beta/(relB[i-1][0]*alpha)
        c = Newt(z^2-c2,liftto(liftto(t,1),M))
        return q+1-toInt(c)

# Pour verifier le resultat
def testRes():
        A,B = AB()
    return Satoh(A,B) == EllipticCurve(Fq,[down(A),down(B)]).cardinality()

# Pour faire des tests de duree d'execution.
def testTemps():
        A,B = AB()
        t = cputime()
        Satoh(A,B)
        fin = cputime(t)
        return fin
```