THESE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITE DE TOULOUSE

en mathématiques

Présentée et soutenue le 5 Mai 2010 par

Tony Mack Robert EZOME MINTSA

Intitulée

Courbes elliptiques, cyclotomie et primalité

JURY

Karim Belabas	Université de Bordeaux	Examinateur
Jean-Marc Couveignes	Université de Toulouse	Directeur
Pierrick Gaudry	LORIA, Nancy	Rapporteur
Reynald Lercier	IRMAR, Rennes	Examinateur
Christian Maire	Université de Franche-Comté	Rapporteur
Marc Reversat	Université de Toulouse	Examinateur

Institut de mathématiques de Toulouse, UMR 5219
Université Paul Sabatier, Toulouse III
31062 Toulouse, Cedex 9

Une parabole : Représentation graphique d'un trinôme du second degré, ou récit allégorique représentant le message chiffré d'une leçon de vie.

Remerciements

Je tiens à remercier à travers ces quelques lignes toutes les personnes qui ont rendu possible la réalisation de ces travaux.

En premier lieu, Jean marc Couveignes a su, pendant ces quatre années, surveiller mes progrès de manière très attentive, et ce me laissant au départ me familiariser avec les objets de base. Sa disponibilté et son implication ont établi des conditions on ne peut plus favorables au déroulement de cette thèse. Je suis très heureux et très fier d'avoir découvert la recherche mathématique à ses côtés.

Je remercie très sincèrement Pierrick Gaudry et Christian Maire d'avoir accepter de rapporter ce mémoire. Reynald Lercier, Marc Reversat et Karim Belabas ont accepté d'être membres du jury. Je les en remercie.

Guy Martial Nkiet et Jean-Marc Schlenker ont joué un rôle fondamental dans la réalisation de cette thèse. Alors que je validais ma maîtrise de mathématiques à l'Université des Sciences et Techniques de Masuku (USTM) à Franceville au Gabon, Guy Martial Nkiet m'a conseillé de continuer en troisième cycle. J'ai donc candidaté au master 2 de mathématiques fondamentales de l'Université Paul Sabatier. Après la validation du master 2 s'est posé le problème de trouver un directeur de thèse. Je me suis rapprocher, pour cela, de Jean-Marc Schlenker président du diplôme de master 2 mathématiques fondamentales du moment. Et il m'a mis en contact avec Jean-Marc Couveignes.

Je veux dire un grand merci également aux doctorants du laboratoire Emile Picard de l'époque, devenu équipe Emile Picard de l'Institut de mathématiques de Toulouse, qui m'ont accueilli et aidé à prendre mes marques. Je remercie tout particulièrement Anne Granier, Landry Salle, Alain Couvreur et Julien Roques. Je pense aussi à l'ensemble des doctorants de l'institut que j'ai rencontrés. Merci à tous, pour les moments de détente et les coups de pouces et astuces : commandes sur linux, commandes et packages sur latex, combines pour imprimer et travailler sur le reseau même en cas de mauvais fonctionnement, et ...

Beaucoup d'autres personnes ont joué un rôle important dans le contexte plus général dans lequel s'est déroulée cette thèse : les membres de l'ancienne équipe Grimm, les ensei-

gnants et personnels de l'Institut de mathématiques. Tous ces éléments forment un tableau dont je tiens à souligner la richesse humaine.

Table des matières

1 Généralités sur les variétés algébriques **11**

1.1 Variétés algébriques 11

1.1.1 Variétés affines 11

1.1.2 Variétés projectives 14

1.1.3 Diviseurs et formes différentielles 19

1.1.4 Théorème de Riemann-Roch 21

1.2 Courbes elliptiques 22

1.2.1 Définition et loi de groupe 22

1.2.2 Isogénies 24

1.2.3 Formules explicites pour la loi de groupe 25

1.2.4 Exemples 27

2 Réduction des courbes elliptiques **29**

2.1 Courbes elliptiques sur $\mathbf{C}$ 29

2.1.1 Tores complexes et fonctions doublement périodiques 29

2.1.2 Construction des fonctions elliptiques 30

2.1.3 L'uniformisation des courbes elliptiques sur $\mathbf{C}$ 32

2.2 Courbes elliptiques sur un anneau fini 37

2.2.1 L'anneau est un corps fini $\mathbb{F}_q$ 37

2.2.2 Courbes elliptiques sur $\mathbb{Z}/N\mathbb{Z}$ 39

2.3 Multiplication complexe et applications 40

2.3.1 Courbes elliptiques sur $\overline{\mathbf{Q}}$ 41

2.3.2 Réduction des courbes elliptiques définies sur un corps local 42

2.3.3 Réduction des courbes elliptiques CM 44

2.3.4 Exemples 47

3 Le test de primalité ECPP **55**

3.1 Le test ECPP 55

3.1.1 Le critère 55

3.1.2 L'algorithme 56

3.1.3 Commentaires 56

3.1.4 Théorie de la complexité . . . 58
3.1.5 Un exemple . . . 60
3.2 Améliorations et exemple . . . 63
3.2.1 L'algorithme fastECPP . . . 63
3.2.2 Exemple . . . 63

4 Le test de primalité AKS et ses variantes 69
4.1 Le test AKS . . . 69
4.1.1 Le critère . . . 69
4.1.2 L'algorithme . . . 72
4.1.3 Commentaires . . . 72
4.1.4 Exemple . . . 74
4.2 Améliorations . . . 74
4.2.1 La variante de Lenstra et Pomerance . . . 74
4.2.2 L'idée de Berrizbeitia améliorée par Bernstein . . . 75
4.2.3 Exemple . . . 78

5 Le critère de primalité AKS étendu 81
5.1 Quelques propriétés des anneaux artiniens . . . 81
5.2 Les extensions entières d'anneaux . . . 83
5.2.1 Relèvement des idéaux premiers . . . 83
5.2.2 Action d'un groupe sur un anneau : groupe de décomposition et groupe d'inertie . . . 88
5.3 Schémas et algèbres étales . . . 89
5.3.1 Morphismes étales de schémas . . . 89
5.3.2 Algèbres étales . . . 95
5.3.3 Exemples . . . 97
5.4 Extensions d'anneaux et preuve de primalité . . . 101

6 Une version du critère de primalité AKS utilisant les courbes elliptiques 105
6.1 Bases elliptiques et courbes définies sur un corps . . . 105
6.1.1 Préliminaires . . . 105
6.1.2 Base elliptique . . . 106
6.2 Courbes elliptiques sur un anneau . . . 108
6.2.1 Schémas projectifs . . . 109
6.2.2 Courbes elliptiques de Weierstrass universelles . . . 110
6.2.3 Construction d'un anneau des périodes elliptiques . . . 113
6.2.4 Loi de multiplication dans l'anneau **S** . . . 114
6.3 Le cas des courbes modulo n . . . 115
6.3.1 Un critère de primalité . . . 115
6.3.2 Commentaires . . . 116
6.3.3 Exemple . . . 116

Introduction

Dans cette thèse, on s'intéresse aux critères de primalité. Un tel critère affirme que l'entier $n \geq 2$ est premier si un certain anneau (schéma) sur $\mathbf{Z}/n\mathbf{Z}$ satisfait des propriétés plus ou moins faciles à vérifier.

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurer confidentialité, authenticité et intégrité) en s'aidant de secrets ou clés. Imaginons un canal, auquel ont accès plusieurs personnes parmi lesquelles Alice, Bob et Oscar. La cryptographie décrit comment Bob peut avoir une communication privée avec Alice via ce canal sans que les autres utilisateurs (Oscar par exemple) qui voient passer les messages ne puissent les lire, ni interférer dans la conversation. L'autre branche de la cryptologie est la cryptanalyse, qui met à l'épreuve les protocoles cyptographiques.
Le chiffrement d'un message confidentiel laisse deux choix principaux. On peut utiliser des algorithmes à clé secrète, et dans ce cas on parle de cryptographie symétrique. Le codage peut aussi se faire via des algorithmes à clé publique et clé privée, c'est la cryptographie asymétrique. L'existence de fonctions trappes (*i.e* faciles à calculer dans un sens mais difficiles à inverser sans la clé privée) est la base de sécurité de la cryptographie asymétrique. La conjecture

il n'existe pas d'algorithme polynomial qui donne les facteurs premiers d'un entier quelconque

est le fondement de plusieurs cryptosystèmes en cryptographie asymétrique. C'est le cas, par exemple, du cryptosystème RSA utilisé dans les protocoles de commerce en ligne. Il est donc très utile de pouvoir déterminer la primalité de grands entiers afin de construire des entiers difficilement factorisables qui pourront servir en cryptographie asymétrique. Pour ce faire on a recours aux tests de primalité. Les tests de primalités probabilistes tels que le test de Miller-Rabin marchent bien. En effet, si à la sortie d'un de ces tests on conclut que l'entier testé est probablement premier, il y a une forte probabilité que cela soit vrai. Seulement il n'existe pas de preuve mathématique rigoureuse qui étaie cette quasi-certitude. Pour des applications hautement sécurisées, un certificat indubitable de primalité est donc préférable. L'algorithme AKS basé sur la cyclotomie et l'algorithme ECPP basé sur les courbes elliptiques résolvent le problème.

Dans le premier chapitre de ce mémoire, nous reprenons les éléments fondamentaux de la géométrie algébrique des courbes afin de bien définir les courbes elliptiques et d'examiner les propriétés de ces dernières, importantes pour nos applications.
Au chapitre 2, nous étudions les courbes elliptiques définies sur le corps des nombres complexes. L'accent est mis sur l'anneau des endomorphismes de ces courbes. Le chapitre s'achève sur un exemple de réduction d'une courbe elliptique à multiplication complexe.
Le chapitre 3 est consacré à la présentation du test de primalité ECPP et de sa variante fastECPP selon [3], [29] et [14]. Pour chacun de ces algorithmes, nous donnons une illustration.
Dans le chapitre 4, nous présentons le test AKS en suivant [29]. Ensuite nous précisons les améliorations apportées par Lenstra et Pomerance dans [23] d'une part et celles apportées par Berrizbeitia et Bernstein selon [5] d'autre part. Ces méthodes sont ensuite illustrées sur des exemples simples.

Dans l'algorithme AKS, on passe beaucoup de temps à vérifier de nombreuses congruences dans une "grosse" algèbre libre S de dimension finie sur $\mathbf{Z}/n\mathbf{Z}$. Pour pallier ce problème, Lenstra et Pomerance commencent par réduire la taille de cette algèbre (réduire sa dimension). Puis Berrizbeitia et alii considèrent un automorphisme de S qui permutte les congruences à vérifier.
Dans le chapitre 5, on généralise le critère de primalité AKS en utilisant des extensions libres étales S de $\mathbf{Z}/n\mathbf{Z}$ munies d'un automorphisme.

Et dans le chapitre 6, nous énonçons un critère de primalité de type AKS qui repose sur un *anneau des périodes elliptiques*. Un tel anneau est obtenu comme anneau résiduel le long d'une section de torsion d'une courbe elliptique définie sur $\mathbf{Z}/n\mathbf{Z}$. Cette section joue le rôle dévolu à la racine de l'unité dans le test AKS d'origine. Nous montrons comment construire des extensions libres étales S de $\mathbf{Z}/n\mathbf{Z}$, munies d'un automorphisme, à partir d'isogénies entre courbes elliptiques modulo n.

Chapitre 1

Généralités sur les variétés algébriques

Nous rappelons quelques notions de géométrie algébrique en suivant le chapitre 1 de [17] pour les définitions et propriétés générales, les chapitres 1 et 2 de [30] et le chapitre 2 de [18] pour ce qui regarde les courbes algébriques, et plus particulièrement les courbes elliptiques.

1.1 Variétés algébriques

1.1.1 Variétés affines

Afin d'introduire les variétés algébriques affines, nous définissons d'abord l'espace affine. On appelle espace affine de dimension 2 (ou plan affine) sur un corps $\mathbf{K}$, l'ensemble $\mathbb{A}^2 = \mathbb{A}^2(\overline{\mathbf{K}}) = \{P = (x, y) \in \overline{\mathbf{K}} \times \overline{\mathbf{K}}\}$ où $\overline{\mathbf{K}}$ est une clôture algébrique de $\mathbf{K}$ fixée. De même, on appelle espace affine de dimension n sur un corps $\mathbf{K}$, l'ensemble $\mathbb{A}^n = \{P = (x_1, \ldots, x_n) \in \overline{\mathbf{K}} \times \cdots \times \overline{\mathbf{K}}\}$.

Si $\mathbf{L} \subset \overline{\mathbf{K}}$ est une extension du corps $\mathbf{K}$, on note $\mathbb{A}^n(\mathbf{L})$ l'ensemble des points $\mathbf{L}$-rationnels

$$\mathbb{A}^n(\mathbf{L}) = \{P = (x_1, \ldots, x_n) \in \mathbf{L} \times \cdots \times \mathbf{L}\}.$$

La *topologie de Zariski* sur l'espace affine de dimension n est celle dont les fermés V sont les lieux de zéros de familles de polynômes de $\overline{\mathbf{K}}[x_1, \ldots, x_n]$:

$$V = \{(x_1, \ldots, x_n) \in \mathbb{A}^n : f(x_1, \ldots, x_n) = 0 \text{ pour tout } f \in \mathfrak{a}\},$$

où $\mathfrak{a}$ est un idéal de $\overline{\mathbf{K}}[x_1, \ldots, x_n]$. Les fermés V de la topologie de Zariski sont aussi dits *ensembles algébriques affines*. À un ensemble algébrique affine V, on associe l'idéal

$$I(V) = \{P \in \overline{\mathbf{K}}[x_1, \ldots, x_n] : P(x_1, \ldots, x_n) = 0 \text{ pour tout } (x_1, \ldots, x_n) \in V\}$$

de tous les polynômes s'annulant en tous les points de V.

Les courbes planes affines sont des cas particuliers de variétés algébriques affines.

Définition 1.1.1. *Une courbe plane affine C est un ensemble de points $P = (x, y)$ de $\mathbb{A}^2$ dont les coordonnées vérifient une équation de la forme*

$$f(x, y) = 0,$$

où f est un polynôme non constant de $\overline{\mathbf{K}}[x, y]$; on note $C = V(f)$ et le degré de C est le degré de f. Si C est une courbe affine, l'idéal de C est donné par

$$I(C) = \{g \in \overline{\mathbf{K}}[x, y] : g(P) = 0 \text{ pour tout } P \in C\}.$$

La courbe $C = V(f)$ est définie sur $\mathbf{K}$ si $I(C)$ est engendré par des polynômes à coefficients dans $\mathbf{K}$, et dans ce cas on note $C/\mathbf{K}$. Si C est définie sur $\mathbf{K}$, l'ensemble des points $\mathbf{K}$-rationnels de C est

$$C(\mathbf{K}) = C \cap \mathbb{A}^2(\mathbf{K}).$$

Et pour toute extention $\mathbf{L}$ de $\mathbf{K}$ contenue dans $\overline{\mathbf{K}}$, l'ensemble des points $\mathbf{L}$-rationnels de C est

$$C(\mathbf{L}) = C \cap \mathbb{A}^2(\mathbf{L}).$$

À toute courbe plane affine $C/\mathbf{K}$, on associe les idéaux $I(C/\mathbf{K}) \subset \mathbf{K}[x, y]$ et $I(C) \subset \overline{\mathbf{K}}[x, y]$. Ils vérifient

$$I(C/\mathbf{K}) = \{g \in \mathbf{K}[x, y] : g(P) = 0 \text{ pour tout } P \in C\} = I(C) \cap \mathbf{K}[x, y],$$

et la courbe C est définie sur $\mathbf{K}$ si et seulement si

$$I(C) = I(C/\mathbf{K})\overline{\mathbf{K}}[x, y].$$

Une courbe plane affine $C/\mathbf{K} = V(f)$ est dite *irréductible* sur $\mathbf{K}$ lorsque son idéal $I(C/\mathbf{K}) \subset \mathbf{K}[x, y]$ est premier. Lorsque C est irréductible sur $\overline{\mathbf{K}}$, on dit qu'elle est absolument irréductible. Et plus généralement, on appelle *variéte affine*, un ensemble algébrique affine V dont l'idéal associé $I(V) \subset \overline{\mathbf{K}}[x_1, \ldots, x_n]$ est premier.

Une courbe plane affine $C = V(f)$ est dite *non-singulière* en $P = (x_P, y_P) \in C$ si les dérivées partielles $\frac{\partial f}{\partial x}(x_P, y_P)$, $\frac{\partial f}{\partial y}(x_P, y_P)$ ne sont pas simultanément nulles. On dit qu'une courbe est *lisse* si elle est non-singulière en chacun de ses points.

Soit $C/\mathbf{K}$ une courbe plane affine irréductible sur $\mathbf{K}$. Alors l'anneau des *fonctions* $\mathbf{K}$-*régulières* sur C est défini par

$$\mathbf{K}[C] = \frac{\mathbf{K}[x, y]}{I(C/\mathbf{K})},$$

il s'agit de l'ensemble des restrictions des polynômes de $\mathbf{K}[x, y]$ à C. C'est un anneau intègre, et son corps des fractions $\mathbf{K}(C)$ est le corps des *fonctions* $\mathbf{K}$-*rationnelles* sur C. Lorsque

la courbe C est absolument irréductible, on définit l'anneau des fonctions régulières ($\overline{\mathbf{K}}$-régulières) sur C noté $\overline{\mathbf{K}}[C] = \frac{\overline{\mathbf{K}}[x,y]}{I(C)}$ et le corps des fonctions rationnelles sur C noté $\overline{\mathbf{K}}(C) = \mathrm{Frac}(\overline{\mathbf{K}}[C])$ exactement de la même manière, en remplaçant $\mathbf{K}$ par $\overline{\mathbf{K}}$.

Soit P un point d'une courbe plane affine C, on définit l'idéal M_P de $\overline{\mathbf{K}}[C]$ par

$$M_P = \{g \in \overline{\mathbf{K}}[C] : g(P) = 0\}. \tag{1.1}$$

L'idéal M_P est maximal puisque l'application

$$\begin{array}{ccc} \overline{\mathbf{K}}[C]/M_P & \to & \overline{\mathbf{K}} \\ g & \mapsto & g(P) \end{array}$$

est un isomorphisme.

Soit $C/\overline{\mathbf{K}}$ une courbe plane affine absolument irréductible. L'anneau local de C en un point $P \in C$, noté $\overline{\mathbf{K}}[C]_P$, est la localisation de $\overline{\mathbf{K}}[C]$ en M_P. En d'autres termes

$$\overline{\mathbf{K}}[C]_P = \{g \in \overline{\mathbf{K}}(C) : g = g_1/g_2 \text{ pour } g_1, g_2 \in \overline{\mathbf{K}}[C] \text{ avec } g_2(P) \neq 0\}.$$

On dit que $\overline{\mathbf{K}}[C]_P$ est l'*anneau des fonctions sur C régulières en P*.

Soit $C = V(f)$ une courbe plane affine absolument irréductible, l'anneau $\overline{\mathbf{K}}[C]$ s'identifie à l'anneau $\bigcap_{P\in C} \overline{\mathbf{K}}[C]_P$ des fonctions régulières en tout point de C. En effet, toute fonction régulière $g = g/1 \in \overline{\mathbf{K}}[C]$ est une fonction de $\bigcap_{P\in C} \overline{\mathbf{K}}[C]_P$. D'autre part, si $g \in \bigcap_{P\in C} \overline{\mathbf{K}}[C]_P$ alors pour tout $P = (x_P, y_P) \in C$ il existe deux fonctions régulières $h_P, j_P \in \overline{\mathbf{K}}[C]$ telles que $g = h_P/j_P$ et $j_P(x_P, y_P) \neq 0$. Considérons l'idéal $D(g) = \{h \in \overline{\mathbf{K}}[C] : gh \in \overline{\mathbf{K}}[C]\}$ de $\overline{\mathbf{K}}[C]$. Les idéaux maximaux de $\overline{\mathbf{K}}[C]$ sont les idéaux maximaux de $\overline{\mathbf{K}}[x, y]$ contenant $I(C)$, c'est-à-dire les M_P pour tout $P \in C$. Donc $D(g)$ n'est contenu dans aucun idéal maximal, et par conséquent $D(g) = \overline{\mathbf{K}}[x, y]$. Ainsi $1 \in D(g)$, c'est-à-dire $g \in \overline{\mathbf{K}}[C]$.

Définition 1.1.2. *Soient $V_1/\mathbf{K} \subset \mathbb{A}^n$ et $V_2/\mathbf{K} \subset \mathbb{A}^m$ deux variétés affines irréductibles. Une application $\varphi : V_1 \to V_2$ est un $\mathbf{K}$-morphisme s'il existe m polynômes $\varphi_1, \ldots, \varphi_m \in \mathbf{K}[V_1]$ tels que pour tout $(x_1, \ldots, x_n) \in V_1(\overline{\mathbf{K}})$ on a*

$$\varphi(x_1, \ldots, x_n) = (\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n)) \in V_2(\overline{\mathbf{K}}).$$

Lorsque $\mathbf{K}$ est un corps algébriquement clos (ou s'il n'y a pas de confusion possible), on parle simplement de morphismes de variétés.

On dit que $\varphi : V_1 \to V_2$ un isomorphisme s'il existe un morphisme $\psi : V_2 \to V_1$ tel que $\psi \circ \varphi = \mathrm{Id}_{V_1}$ et $\varphi \circ \psi = \mathrm{Id}_{V_2}$.

Un $\mathbf{K}$-morphisme $\varphi : V_1 \to V_2$ de variétés algébriques affines définit un morphismes de $\mathbf{K}$-algèbres

$$\begin{array}{rccc} \varphi^* : & \mathbf{K}[V_2] & \to & \mathbf{K}[V_1] \\ & P(X_1, \ldots, X_m) & \mapsto & P \circ \varphi(X_1, \ldots, X_n) = P(\varphi_1(X_1, \ldots, X_n), \ldots, \varphi_m(X_1, \ldots, X_n)). \end{array}$$

Si $\psi : V_2 \to V_3$ est un autre $\mathbf{K}$-morphisme alors on a : $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$ et $(Id_{V_1})^* = Id_{\mathbf{K}[V_1]}$. L'application $\varphi \mapsto \varphi^*$ est une bijection de l'ensemble $\mathrm{Hom}_{\mathbf{K}}(X, Y)$ des $\mathbf{K}$-morphismes de X vers Y sur l'ensemble $\mathrm{Hom}_{\mathbf{K}-alg}(\mathbf{K}[Y], \mathbf{K}[X])$ des morphismes de $\mathbf{K}$-algèbres de $\mathbf{K}[Y]$ vers $\mathbf{K}[X]$. Pour qu'un $\mathbf{K}$-morphisme $\varphi : V_1 \to V_2$ soit un $\mathbf{K}$-isomorphisme il faut et il suffit que φ^* soit un isomorphisme de $\mathbf{K}$-algèbres.

1.1.2 Variétés projectives

Soit $\mathbf{K}$ un corps, le plan projectif (sur $\mathbf{K}$) est l'ensemble $\mathbb{P}^2 = \mathbb{P}^2(\overline{\mathbf{K}})$ de tous les triplets $(X, Y, Z) \in \mathbb{A}^3 - (0, 0, 0)$ modulo la relation d'équivalence définie par

$$(X, Y, Z) \sim (X', Y', Z') \Leftrightarrow \text{ il existe } \lambda \in \overline{\mathbf{K}}^* \text{ tel que } X' = \lambda X,\ Y' = \lambda Y \text{ et } Z' = \lambda Z.$$

On définit $\mathbb{P}^n$, l'espace projectif de dimension n, de la même manière à partir de $\mathbb{A}^{n+1} - (0, \ldots, 0)$. La classe d'équivalence d'un point $(X_0, \ldots, X_n) \in \mathbb{A}^{n+1} - (0, \ldots, 0)$ sera notée $(X_0 : \ldots : X_n)$ dans la suite. L'ensemble des points $\mathbf{K}$-rationnels de $\mathbb{P}^n$ est l'ensemble

$$\mathbb{P}^n(\mathbf{K}) = \{(X_0 : \ldots : X_n) \in \mathbb{P}^n : X_0, \ldots, X_n \in \mathbf{K}\}.$$

Avant de continuer donnons la définition d'un anneau gradué.

Définition 1.1.3. *Un anneau A est dit gradué par $\mathbb{Z}$, s'il existe une famille de sous-groupes additifs $(A_d)_{d\in\mathbb{Z}}$ telle que :*

1. *$A = \oplus_{d\in\mathbb{Z}} A_d$, c'est-à-dire que tout x dans A s'écrit de manière unique en $x = \sum_{d\in\mathbb{Z}} x_d$ avec $x_d \in A_d$; et pour tout $d \in \mathbb{Z}$ on a $x_d = 0$ sauf pour un nombre fini de d.*
2. *Si $x \in A_d$ et $y \in A_{d'}$ alors $xy \in A_{d+d'}$.*
3. *$1 \in A_0$.*

On dit que A_d est le sous-groupe des éléments homogènes de degré d et x_d est la composante de degré d.

L'anneau $A[X_0, X_1, \ldots, X_n]$ des polynômes en $n+1$ indéterminés à coefficients dans un anneau A est un anneau gradué (les éléments homogènes de degré d sont les combinaisons A-linéaires des monômes $X_0^{d_0} X_1^{d_1} \ldots X_n^{d_n}$ de même degré total $d = d_0 + d_1 + \cdots + d_n$).

La *topologie de Zariski* sur $\mathbb{P}^n$ est celle dont les fermés V sont les lieux de zéros de familles de polynômes homogènes de $\overline{\mathbf{K}}[X_0, \ldots, X_n]$

$$V = \{P \in \mathbb{P}^n : F(P) = 0 \text{ pour tout } F \in \mathfrak{a}\},$$

où $\mathfrak{a}$ est un idéal homogène de $\overline{\mathbf{K}}[X_0, \ldots, X_n]$ (i.e engendré par des polynômes homogènes). Les fermés V de la topologie de Zariski sont aussi dits *ensembles algébriques projectifs*. À un ensemble algébrique projectif V, on associe l'idéal homogène $I(V)$ égal à

$$\{F \in \overline{\mathbf{K}}[X_0, \ldots, X_n] : F \text{ est homogène et } F(P) = 0 \text{ pour tout } P \in V\}$$

Les courbes planes projectives sont des cas particuliers de variétés algébriques projectives.

Définition 1.1.4. *Une courbe plane projective C est un ensemble de points $P = (X : Y : Z)$ de $\mathbb{P}^2$ dont les coordonnées homogènes vérifient une équation de la forme*

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

où F est un polynôme homogène non constant de $\overline{\mathbf{K}}[x, y, z]$; on note $C = V(F)$. Si C est une courbe plane projective, l'idéal (homogène) de C est l'ensemble

$$I(C) = \{g \text{ polynôme homogène de } \overline{\mathbf{K}}[x, y, z] \text{ tel que pour tout } P = (x_P : y_P : z_P) \in C, \text{ on a : } g(x_P, y_P, z_P) = 0\}.$$

L'idéal d'une courbe plane projective $C = V(F)$ est principal. La courbe est définie sur $\mathbf{K}$ si son idéal $I(C)$ est engendré par un polynôme homogène de $\mathbf{K}[x, y, z]$, et dans ce cas on note $C/\mathbf{K}$. Si C est définie sur $\mathbf{K}$, l'ensemble des points $\mathbf{K}$-rationnels de C est

$$C(\mathbf{K}) = C \cap \mathbb{P}^2(\mathbf{K}).$$

Une courbe plane projective C est dite irréductible si son idéal homogène $I(C)$ est premier ou de façon équivalente si le générateur F de cet idéal est irréductible. Plus généralement, on appelle *variétes projectives*, les ensembles algébriques projectifs V tels que les idéaux homogènes associés $I(V) \subset \overline{\mathbf{K}}[X_0, \ldots, X_n]$ sont premiers.

Si $F \in \mathbf{K}[x_1, x_2, x_3]$ est un polynôme homogène de degré 1, alors l'hyperplan

$$F(x_1, x_2, x_3) = 0$$

est une droite. En particulier on note H_i la droite définie par $\{X_i = 0\}$, c'est la droite à l'infini de l'ouvert $U_i = \mathbb{P}^2 - H_i$ pour $i = 1, 2, 3$. Le plan projectif $\mathbb{P}^2$ est recouvert par les trois ouverts U_1, U_2 et U_3, et toute sous-variété $V \subset \mathbb{P}^2$ est recouverte par les trois ouverts $V \cap U_i$ avec $i = 1, 2, 3$. On définit l'application

$$\begin{array}{rccc} \varphi_1 : & U_1 & \to & \mathbb{A}^2 \\ & (x_1 : x_2 : x_3) & \mapsto & (\frac{x_2}{x_1}, \frac{x_3}{x_1}); \end{array}$$

et de la même façon on définit les applications φ_2 et φ_3. Les φ_i sont bien définies (car les quotients x_i/x_j ne dépendent pas du choix des coordonnées homogènes), elles établissent des homéomorphismes entre U_i muni de la topologie induite et $\mathbb{A}^2$ muni de sa topologie de Zariski. Le fait que les φ_i sont des homéomorphismes est lié aux notions *d'homogénéisation* et de *déshomogénéisation* que nous définissons maintenant.

Soit C une courbe projective irréductible d'idéal homogène $I(C) \subset \overline{\mathbf{K}}[x,y,z]$ telle que $C \cap U_3 \neq \emptyset$. Alors l'ensemble $\varphi_3(C \cap U_3) \subset \mathbb{A}^2$ est une courbe affine, son idéal $I(\varphi_3(C \cap U_3)) \subset \overline{\mathbf{K}}[x,y]$ est donné par

$$I(\varphi_3(C \cap U_3)) = \{g_*(x,y) = g(x,y,1) : g(x,y,z) \in I(C)\}.$$

On dit que g_* est la *déshomogénéisation* de g.

Par ailleurs, à tout polynôme non nul $f(x,y) \in \overline{\mathbf{K}}[x,y]$, on associe le polynôme homogène f^* défini par

$$f^*(x,y,z) = z^d f(\frac{x}{z}, \frac{y}{z}),$$

où $d = deg(f)$. Le polynôme f^* est l'*homogénéisation* de f par rapport à z.

Définition 1.1.5. *Soit C_a une courbe plane affine d'idéal $I(C_a) = (f)$. On considère C_a comme un sous-ensemble de $\mathbb{P}^2$ via l'application*

$$C_a \subset \mathbb{A}^2 \xrightarrow{\varphi_3^{-1}} \mathbb{P}^2. \tag{1.2}$$

L'adhérence de Zariski de C_a, notée $\overline{C_a}$, est l'ensemble algébrique projectif dont l'idéal homogène est engendré par le polynôme f^*.

Considérons à nouveau la courbe plane projective irréductible C d'idéal homogène $I(C) \subset \overline{\mathbf{K}}[x,y,z]$ telle que $C \cap U_3 \neq \emptyset$ et supposons que C est définie sur $\mathbf{K}$. Alors le corps $\mathbf{K}(C)$ des fonctions rationnelles sur C à coefficients dans $\mathbf{K}$ est le corps des fonctions rationnelles sur $C \cap U_3$ à coefficients dans $\mathbf{K}$; on définit $\overline{\mathbf{K}}[C]$ de la même façon. (Notons que quelle que soit la copie U_i de $\mathbb{A}^2$ dans $\mathbb{P}^2$ considérée, les différents $\mathbf{K}(C)$ sont canoniquement isomorphes et par conséquent on les identifie.)

Soient $C = V(F)$ une courbe plane projective irréductible et $P = (a : b : c)$ un point de C. Alors C est non-singulière en P si les dérivées partielles $\frac{\partial F}{\partial X}(a,b,c)$, $\frac{\partial F}{\partial Y}(a,b,c)$, $\frac{\partial F}{\partial Z}(a,b,c)$ ne sont pas simultanément nulles. Le point P appartient nécessairement à au moins l'un des trois ouverts U_i, nous supposons que $P \in U_3$. Dans ce cas C est non-singulière en P si $C \cap U_3$ est non-singulière en P et l'anneau des fonctions régulières en $P \in C$, noté $\overline{\mathbf{K}}[C]_P$, est le localisé de $\overline{\mathbf{K}}[C \cap U_3]$ en P.

Remarque 1.1.6. *1. Le corps des fonctions de $\mathbb{P}^n$ peut être vu comme le sous-corps de $\overline{\mathbf{K}}(X_0, \ldots, X_n)$ formé (du polynôme identiquement nul et) des fonctions $F(X_0, \ldots, X_n) = G_1(X_0, \ldots, X_n)/G_2(X_0, \ldots, X_n)$ telles que G_1 et G_2 sont des polynômes homogènes de même degré et $G_2 \neq 0$. Une telle expression donne une fonction bien définie en tout point P de $\mathbb{P}^n$ où $G_2(P) \neq 0$. De la même façon, le corps des fonctions d'une variété projective irréductible V est l'ensemble formé (du polynôme*

identiquement nul et) des fonctions rationnelles
$F(X_0, \ldots, X_n) = G_1(X_0, \ldots, X_n)/G_2(X_0, \ldots, X_n)$ *telles que*

(i) les polynômes G_1 *et* G_2 *sont homogènes de même degré ;*
(ii) $G_2 \notin I(V)$ *;*
(iii) Deux fonctions G_1/G_2 *et* H_1/H_2 *sont identifiées si* $G_1H_2 - G_2H_1 \in I(V)$.

2. *Une courbe projective lisse* C*, définie par* $F(x, y, z) = 0$*, est nécessairement irréductible. En effet si la courbe etait réductible, notant* F_1 *et* F_2 *deux facteurs irréductibles distincts de* F*, l'intersection* $V(F_1) \cap V(F_2)$ *serait non vide d'après le théorème de Bezout [[18], chapitre* 2*, théorème* 2.4*, P.* 27*]. Tout point de cette intersection serait un point singulier de la courbe. Contradiction.*

Avant de poursuivre, définissons la dimension d'une variété.

Définition 1.1.7. *Soit* V *une variété (affine ou projective). La dimension de* V*, notée* $\dim(V)$*, est le degré de transcendence de* $\overline{\mathbf{K}}(V)$ *sur* $\overline{\mathbf{K}}$.

Une courbe affine (resp. projective) est une variété affine (resp. projective) de dimension 1.

Si P est un point non-singulier d'une courbe plane projective C, alors $\overline{\mathbf{K}}[C]_P$ est un anneau de valuation discrete[[30], chapitre 2, proposition 1.1]. Son unique idéal maximal est l'idéal engendré par M_P (équation (1.1)) que nous notons encore M_P. L'application

$$\begin{array}{rccc} \mathrm{ord}_P : & \overline{\mathbf{K}}[C]_P & \to & \{0, 1, 2, \ldots\} \cup \{\infty\} \\ & f & \mapsto & \mathrm{ord}_P(f) = \mathrm{Sup}\{d : f \in M_P^d\} \end{array}$$

est une *valuation discrète* sur $\overline{\mathbf{K}}[C]_P$. En utilisant $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, on étend ord_P à $\overline{\mathbf{K}}(C)$. Une *uniformisante* de C en P est une fonction $t \in \overline{\mathbf{K}}(C)$ telle que $\mathrm{ord}_P(t) = 1$. Pour tout $f \in \overline{\mathbf{K}}(C)$, l'ordre de f en P est $\mathrm{ord}_P(f)$. Si $\mathrm{ord}_P(f) > 0$ alors P est un zéro de f. Si $\mathrm{ord}_P(f) < 0$ alors P est un pôle de f.

Proposition 1.1.8. *[[30],P. 22] Soient* C *une courbe projective lisse et* $f \in \overline{\mathbf{K}}(C)^*$*. Alors* f *n'a qu'un nombre fini de zéros et de pôles. De plus si* f *n'a pas de pôles alors* $f \in \overline{\mathbf{K}}^*$.

Maintenant nous définissons les morphismes de courbes projectives.

Définition 1.1.9. *Soient* $C_1/\mathbf{K}$ *et* $C_2/\mathbf{K}$ *deux courbes projectives absolument irréductibles. On dit que* $\phi : C_1 \to C_2$ *est une application rationnelle s'il existe trois fonctions rationnelles* $F_1, F_2, F_3 \in \overline{\mathbf{K}}(C_1)$ *non toutes nulles telles que* $\phi = (F_1 : F_2 : F_3)$ *et pour tout* $P \in C_1$*, en lequel ces trois fonctions sont définies, on a*

$$\phi(P) = (F_1(P) : F_2(P) : F_3(P)) \in C_2.$$

On dit que ϕ *est un application* $\mathbf{K}$*-rationnelle s'il existe* $F \in \overline{\mathbf{K}}(C)$ *telles que* $FF_1, FF_2, FF_3 \in \mathbf{K}(C_1)$*. Elle est régulière (définie) en* $P \in C_1$ *s'il existe une fonction* $G \in \overline{\mathbf{K}}(C_1)$ *telle que*

1. *chaque GF_i est régulière en P ;*
2. *Pour au moins un i, on a $GF_i(P) \neq 0$.*

Une application rationnelle (resp. $\mathbf{K}$-rationnelle) de C_1 vers C_2, qui est régulière en tout point de C_1, est un morphisme (resp. un $\mathbf{K}$-morphisme).
Un $\mathbf{K}$-morphisme ϕ de C_1 vers C_2 est un $\mathbf{K}$-isomorphisme s'il existe un $\mathbf{K}$-morphisme $\psi : C_1 \to C_2$ tel que $\psi \circ \phi$ et $\phi \circ \psi$ sont les applications identités sur C_1 et C_2.

Soient $\phi = (F_1 : \ldots : F_m) : C_1 \to V \subset \mathbb{P}^m$ une application rationnelle et $P \in C_1$ un point non-singulier de C_1. Alors notant t une uniformisante de C_1 en P et $n = min\{\mathrm{ord}_P(F_i)\}$, la fonction $t^{-n}F_i$ est régulière en P pour $i = 1, \ldots, m$ et il existe i tel que $t^{-n}F_i \neq 0$. Donc ϕ est régulière en P. Nous avons établi la

Proposition 1.1.10. *[[30],P. 23] Toute application rationnelle $\phi : C_1 \to V$, d'une courbe projective lisse vers une variété projective, est régulière.*

Énonçons un autre résultat intéréssant :

Théorème 1.1.11. *[[30],P. 24] Toute application régulière $\phi : C_1 \to C_2$ entre courbes projectives est constante ou surjective.*

Donc si $\phi : C_1 \to C_2$ est une application rationnelle non-constante entre courbes projectives, la composition avec ϕ induit une injection de corps de fonctions fixant $\mathbf{K}$:

$$\begin{array}{rccc} \phi^* : & \mathbf{K}(C_2) & \to & \mathbf{K}(C_1) \\ & f & \mapsto & f \circ \phi. \end{array}$$

Le corps $\mathbf{K}(C_1)$ est une extension de degré fini de $\mathbf{K}(C_2)$ [[30], chapitre 2, théorème 2.4]. On dit que ϕ est fini et on définit son degré par

$$\deg\phi = [\mathbf{K}(C_1) : \phi^*\mathbf{K}(C_2)]. \tag{1.3}$$

Si ϕ est constante, elle est de degré 0. On dit que ϕ est séparable (resp. inséparable ou purement inséparable) si l'extension $\mathbf{K}(C_1)/\mathbf{K}(C_2)$ est séparable (resp. inséparable ou purement inséparable).

Et si $\varphi : C_1 \to C_2$ est une application rationnelle non-constante entre courbes projectives lisses, P un point de C_1. On appelle *indice de ramification* de φ en P, et on note e_φ, l'entier

$$e_\varphi = \mathrm{ord}_P(\varphi^* t_{\varphi(P)}),$$

où $t_{\varphi(P)} \in \mathbf{K}(C_2)$ est une uniformisante en $\varphi(P)$. Notons que $e_\varphi(P) \geq 1$. On dit que φ est non ramifiée en P si $e_\varphi(P) = 1$; et φ est non ramifiée si elle est non ramifiée en tout point de C_1.

Proposition 1.1.12 ([30], Page 28)**.** *Une application rationnelle $\varphi : C_1 \to C_2$ est non-ramifiée si et seulement si $\#\varphi^{-1}(Q) = \deg(\varphi)$ pour tout $Q \in C_2$.*

1.1.3 Diviseurs et formes différentielles

Soit C une courbe projective. Un diviseur de C est une combinaison linéaire formelle de points de C, à coefficients entiers relatifs. Autrement dit, le groupe $\mathrm{Div}(C)$ des diviseurs est le groupe libre commutatif engendré par les points dans $C(\overline{\mathbf{K}})$. Un diviseur $D \in \mathrm{Div}(C)$ est donc une somme formelle

$$D = \sum_{P \in C} n_P [P]$$

où $n_P \in \mathbf{Z}$ et $n_P = 0$ sauf pour un nombre fini de points $P \in C$. Le degré de D est défini par

$$\deg(D) = \sum_{P \in C} n_P.$$

L'ensemble des diviseurs de degré 0 forment un sous-groupe de $\mathrm{Div}(C)$ que l'on note $\mathrm{Div}^0(C)$.

Soit C une courbe projective lisse et $f \in \overline{\mathbf{K}}(C)^*$, on associe à f le diviseur $\mathrm{div}(f)$ défini par

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)[P].$$

L'application

$$\mathrm{div} : \overline{\mathbf{K}}(C)^* \to \mathrm{Div}(C)$$

est un homomorphisme de groupes abéliens.

Définition 1.1.13. *Un diviseur $D \in \mathrm{Div}(C)$ est principal si l'on peut l'écrire sous la forme $D = \mathrm{div}(f)$ avec $f \in \overline{\mathbf{K}}(C)^*$. Deux diviseurs D_1, D_2 sont linéairement équivalents si $D_1 - D_2$ est principal. Le groupe des classes de diviseurs (ou groupe de Picard) de C, noté $\mathrm{Pic}(C)$, est le quotient de $\mathrm{Div}(C)$ par le sous-groupe des diviseurs principaux.*

Un diviseur principal $D = \mathrm{div}(f)$ d'une courbe projective lisse C est nul si et seulement si $f \in \overline{\mathbf{K}}^*$ [[30], chapitre 2, proposition 3.1(a)]. De plus le degré $\deg(\mathrm{div}(f))$ d'un diviseur principal d'une courbe projective lisse est toujours nul [[30], chapitre 2, proposition 3.1(b)]. Donc le sous-groupe des diviseurs principaux est contenu dans $\mathrm{Div}^0(C)$. Par conséquent on peut définir le degré d'une classe de diviseurs dans $\mathrm{Pic}(C)$. Les classes de $\mathrm{Pic}(C)$ de degré 0 forment un sous-groupe noté $\mathrm{Pic}^0(C)$, c'est le quotient de $\mathrm{Div}^0(C)$ par le sous-groupe des diviseurs principaux. La suite

$$1 \longrightarrow \overline{\mathbf{K}}^* \longrightarrow \overline{\mathbf{K}}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0$$

est exacte.

Maintenant nous allons introduire la notion de forme différentielle sur une courbe projective.

Définition 1.1.14. *Soit C une courbe projective. L'espace des formes différentielles méromorphes sur C, noté Ω_C, est le $\overline{\mathbf{K}}(C)$-espace vectoriel engendré par les symboles de la forme dx pour $x \in \overline{\mathbf{K}}(C)$, vérifiant les relations usuelles :*
(i) $d(x+y) = dx + dy$ pour tous $x, y \in \overline{\mathbf{K}}(C)$;
(ii) $d(xy) = xdy + ydx$ pour tous $x, y \in \overline{\mathbf{K}}(C)$;
(iii) $da = 0$ pour tout $a \in \overline{\mathbf{K}}$.

L'espace Ω_C est un $\overline{\mathbf{K}}(C)$-espace vectoriel de dimension 1 [[30], chapitre 2, proposition 4.2(a)]. Si $x \in \overline{\mathbf{K}}(C)$ alors la forme différentielle dx est une $\overline{\mathbf{K}}(C)$-base de Ω_C si et seulement si $\overline{\mathbf{K}}(C)/\overline{\mathbf{K}}(x)$ est une extension séparable [[30], chapitre 2, proposition 4.2(b)].

Proposition-Définition 1.1.15 ([30], Page 35)**.** *Soient P un point régulier sur une courbe projective C et $t \in \overline{\mathbf{K}}(C)$ une uniformisante en P.*
(a) Pour toute forme différentielle ω, il existe une unique fonction $g \in \overline{\mathbf{K}}(C)$, qui ne dépend que de ω et t, telle que

$$\omega = gdt.$$

La fonction g se note ω/dt.
(b) Soit $f \in \overline{\mathbf{K}}(C)$ une fonction régulière en P. Alors df/dt est aussi une fonction régulière en P.
(c) La quantité

$$\mathrm{ord}_P(\omega/dt)$$

ne dépend que de ω et P, elle est indépendante du choix de l'uniformisante t. Cette valeur s'appelle l'ordre en P de la forme différentielle ω et on la note $\mathrm{ord}_P(\omega)$.
(d) Soient $x, f \in \overline{\mathbf{K}}(C)$ deux fonctions sur C telles que $x(P) = 0$, on note $q = \mathrm{Char}(\mathbf{K})$. Alors

$$\mathrm{ord}_P(fdx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1, \ \textit{si } q = 0 \textit{ ou } q \nmid \mathrm{ord}_P(x),$$
$$\mathrm{ord}_P(fdx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x), \ \textit{si } q > 0 \textit{ et } q \mid \mathrm{ord}_P(x).$$

(e) Pour tout $P \in \overline{\mathbf{K}}(C)$ on a

$$\mathrm{ord}_P(\omega) = 0,$$

sauf peut-être pour un nombre fini d'entre eux.

Soit $\omega \in \Omega_C$. Le diviseur associé à ω est

$$div(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)[P] \in \mathrm{Div}(C).$$

Une différentielle $\omega \in \Omega_C$ est régulière (ou holomorphe) si

$$\mathrm{ord}_P(\omega) \geq 0 \text{ pour tout } P \in C.$$

La différentielle est sans zéros si

$$\mathrm{ord}_P(\omega) \leq 0 \text{ pour tout } P \in C.$$

Remarque 1.1.16. *Si $\omega_1, \omega_2 \in \Omega_C$ sont des différentielles non nulles, alors il existe $f \in \overline{\mathbf{K}}(C)^*$ telle que $\omega_1 = f\omega_2$ car Ω_C est de dimension 1. Ainsi*

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2),$$

cela donne un sens à la définition suivante.

Définition 1.1.17. *La classe des diviseurs canoniques sur C est l'image dans* $\mathrm{Pic}(C)$*, par l'application* div*, de toute différentielle non-identiquement nulle $\omega \in \Omega_C$.*

1.1.4 Théorème de Riemann-Roch

Soit C est une courbe plane projective. Un diviseur $D = \sum n_P[P] \in \mathrm{Div}(C)$ est dit positif (ou effectif), on note $D \geq 0$, si $n_P \geq 0$ pour tout $P \in C$. De même, si $D_1, D_2 \in \mathrm{Div}(C)$, alors $D_1 \geq D_2$ signifie que $D_1 - D_2$ est positif. Soit $D \in \mathrm{Div}(C)$. On associe à D l'ensemble des fonctions

$$\mathcal{L}(D) = \{f \in \overline{\mathbf{K}}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

C'est un $\overline{\mathbf{K}}$-espace vectoriel de dimension finie [[30], chapitre 2, proposition 5.2(b)], on note $l(D)$ sa dimension.

Enonçons un résultat fondamental en géométrie algébrique des courbes.

Théorème 1.1.18. *(Riemann-Roch). Soient C une courbe lisse et K_C un diviseur canonique sur C. Il existe un entier $g \geq 0$, appelé le genre de C, telle que pour tout diviseur $D \in \mathrm{Div}(C)$,*

$$l(D) - l(K_C - D) = \mathrm{deg}D - g + 1.$$

Corollaire 1.1.19 ([30], Page 39)**.** *(a)* $l(K_C) = g$.
(b) $\mathrm{deg}K_C = 2g - 2$.

(c) Si $\deg D > 2g-2$*, alors*

$$l(D) = \deg D - g + 1.$$

Nous allons, sur un exemple, calculer le genre g d'une courbe plane projective.

Exemple 1.1.20. *Soient* $\mathbf{K}$ *un corps de caractéristique* $\mathrm{Char}(\mathbf{K}) \notin \{2,3\}$ *et* $e_1, e_2, e_3 \in \overline{\mathbf{K}}$ *des éléments deux à deux distincts. Considérons la cubique projective* C *d'équation affine*

$$y^2 = (x-e_1)(x-e_2)(x-e_3).$$

On vérifie facilement que C *est lisse et qu'elle a un unique point* $P_\infty = (0:1:0)$ *à l'infini. Pour* $i = 1,2,3$ *on pose* $P_i = (e_i, 0) \in C$*. Alors les diviseurs des fonctions* $y, x-e_1, x-e_2$ *et* $x-e_3$ *sont donnés par*

$$\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty),$$

et

$$\mathrm{div}(x-e_i) = 2(P_i) - 2(P_\infty),$$

car $(x-e_i, y)$ *est l'idéal maximal du localisé* $\mathcal{O}_{C,P_i}$ *de* $\overline{\mathbf{K}}[C]$ *en* P_i *et pour* $j \neq i$*, la fonction* $x - e_j \in \mathcal{O}_{C,P_i}$ *est inversible (notons que les diviseurs principaux de courbes projectives lisses sont de degré* 0 *[[30], proposition* 3.1 *page 32]). Le diviseur associé à la différentielle* dx *est*

$$\mathrm{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

Pour évaluer $\mathrm{ord}_{P_i}(dx)$ *on écrit* $dx = d(x-e_i)$ *pour* $i = 1,2,3$*.*
Pour évaluer $\mathrm{ord}_{P_\infty}(dx)$ *on écrit* $dx = -(x-e_i)^2 d(1/(x-e_i))$*.*
Donc

$$\mathrm{div}(dx/y) = 0.$$

Par conséquent la différentielle dx/y *est holomorphe et même sans zero. Ainsi la classe des diviseurs canoniques sur* C *est triviale (définition* 1.1.17*). Donc le genre* g *de* C *est*

$$g = l(0) = 1.$$

1.2 Courbes elliptiques

1.2.1 Définition et loi de groupe

Soit $\mathbf{K}$ un corps. Une *cubique plane projective* est par définition une courbe plane projective $C \subset \mathbb{P}^2(\overline{\mathbf{K}})$ de degré 3 dans $\mathbb{P}^2$. La courbe C rencontre au moins l'un des trois ouverts U_i recouvrant $\mathbb{P}^2$. Supposons que $C \cap U_3 \neq \emptyset$ et que la courbe C est absolument irréductible. Alors C est la réunion de la courbe affine $C \cap U_3$ et d'un nombre fini de points à l'infini.

Définition 1.2.1. *Une courbe elliptique $E/\mathbf{K}$ sur $\mathbf{K}$ est une cubique plane projective lisse munie d'un point sur $\mathbf{K}$ (un point $\mathbf{K}$-rationnel).*
On dit qu'une telle cubique est une courbe elliptique de Weierstrass sur $\mathbf{K}$ si les conditions :

- *La cubique passe par le point $O = (0 : 1 : 0)$,*
- *La tangente en O à la cubique est la droite à l'infini $\{z = 0\}$,*
- *Le point O est un point d'inflexion (la multiplicité d'intersection de la cubique avec le plan à l'infini est ≥ 3, ici elle vaut exactement 3)*

sont vérifiées. Dans ce cas la courbe E a pour équation homogène

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{1.4}$$

Une courbe elliptique de Weierstrass E est la réunion d'un unique point à l'infini $O = (0 : 1 : 0)$ et d'une courbe plane affine E_{aff} d'équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.5}$$

On dit que E_{aff} est la partie affine de E.

Proposition 1.2.2 ([30], page 63)**.** *Soit E une courbe elliptique définie sur le corps $\mathbf{K}$.*
(a) Il existe des fonctions $x, y \in \mathbf{K}(E)$ telles que l'application

$$\phi : E \to \mathbb{P}^2(\overline{\mathbf{K}})$$
$$\phi = (x : y : 1)$$

définit un isomorphisme de $E/\mathbf{K}$ sur une courbe donnée par une équation de Weierstrass

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

à coefficients $a_1, \ldots, a_6 \in \mathbf{K}$, et tel que $\phi(O) = (0 : 1 : 0)$. On dit que x, y sont les fonctions coordonnées de Weierstrass sur E.
(b) Deux équations de Weierstrass de E comme dans (a) sont liées par un changement de variables de la forme

$$X = u^2X' + r$$
$$Y = u^3Y' + su^2X' + t$$

avec $u, r, s, t \in \mathbf{K}$ et $u \neq 0$.
(c) Réciproquement, toute cubique lisse donnée par une équation de Weierstrass comme dans (a) est une courbe elliptique définie sur $\mathbf{K}$ ayant pour origine $O = (0 : 1 : 0)$

Soit $L \subset \mathbb{P}^2$ une droite. D'après le théorème de Bezout [[18], chapitre 2, théorème 2.4, P. 27], la droite L recoupe la courbe E exactement en 3 points P, Q, R. On définit une loi de composition $\oplus$ sur $E(\overline{\mathbf{K}})$ de la façon suivante.

Loi de composition 1.2.3 ([30], P. 55)**.** *Soient P, Q deux points de E, L la droite passant par P et Q (i.e la tangente à E si $P = Q$), et R le troisième point d'intersection de L avec E. Soit L' la droite passant par R et O. Alors $P \oplus Q$ est le troisième point d'intersection de L' avec E.*

L'ensemble $E(\overline{\mathbf{K}})$ des points (dans $\mathbb{P}^2$) d'une courbe elliptique de Weierstrass a une structure de groupe abélien pour la loi $\oplus$ [[30], chapitre 3, §2, proposition 2.2], dont l'élément neutre est $O = (0 : 1 : 0)$. Et si E est définie sur $\mathbf{K}$, l'ensemble $E(\mathbf{K})$ des points $\mathbf{K}$-rationnels est un sous-groupe de $E(\overline{\mathbf{K}})$.

1.2.2 Isogénies

Si $E/\mathbf{K}$ est une courbe elliptique de Weierstrass sur $\mathbf{K}$, le point O est l'élément neutre du groupe $E(\overline{\mathbf{K}})$. Il peut être intéressant de regarder les morphismes, de E vers une courbe elliptique de Weierstrass $E'/\mathbf{K}$, qui fixent O.

Définition 1.2.4. *Soient E_1 et E_2 deux courbes elliptiques de Weierstrass. Une application $\varphi : E_1 \to E_2$ est un morphisme de courbes elliptiques de Weierstrass si φ est un morphisme pour les structures de courbes projectives et vérifie $\varphi(O) = O$. Dans ce cas on dit que φ est une isogénie.*

D'après le théorème 1.1.11, une isogénie ϕ vérifie $\phi(E_1) = \{O\}$ ou $\phi(E_1) = E_2$. Donc excepté l'isogénie identiquement nulle définie par $[0](P) = 0$ pour tout $P \in E_1$, toute autre isogénie est une application surjective entre courbes projectives.

Théorème 1.2.5 ([30], page 75)**.** *Une isogénie respecte les lois de groupe :*

$$\textit{Pour tous } P, Q \in E_1 \textit{ on a : } \varphi(P \oplus Q) = \varphi(P) \oplus \varphi(Q).$$

On suppose que le corps $\mathbf{K}$ est de caractéristique $\mathrm{Char}(\mathbf{K}) \notin \{2, 3\}$. Soit $E/\mathbf{K}$ une courbe elliptique de Weierstrass d'équation affine

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

Les applications $\varphi : (x, y) \mapsto (x, \frac{1}{2}(y - a_1x - a_3))$ et $\psi : (x, y) \mapsto ((x - 3(a_1^2 + 4a_2))/36, y/108)$ sont des isomorphismes de courbes elliptiques de Weierstrass. La composée $\psi \circ \varphi$ envoie E sur la courbe E' d'équation affine

$$y^2 = x^3 + ax^2 + b, \tag{1.6}$$

où a et b sont des polynômes en a_1, a_2, a_3, a_4, a_6 à coefficients dans $\mathbf{K}$. On dit que E' est une courbe elliptique de Weierstrass *réduite*.

Définition 1.2.6. *Soient $\mathbf{K}$ un corps de caractéristique $\mathrm{Char}(\mathbf{K}) \notin \{2, 3\}$ et E une courbe elliptique de Weierstrass réduite. On associe à E un discriminant $\Delta_E = -16(4a^3 + 27b^2)$ et un invariant modulaire $j(E) = -1728\frac{(4a)^3}{\Delta_E}$.*

Dans toute la suite, sauf mention contraire explicite, une courbe elliptique $E/\mathbf{K}$ sur un corps $\mathbf{K}$ désignera une courbe elliptique de Weierstrass réduite d'équation affine donnée par (1.6).

Nous clôturons la section par l'énoncé suivant.

Théorème-Définition 1.2.7 ([30], Page 84)**.** *Soit $\phi : E_1 \to E_2$ une isogénie non-constante de degré m. Alors il existe une unique isogénie*

$$\widehat{\phi} : E_2 \to E_1$$

appelée isogénie duale et vérifiant $\widehat{\phi} \circ \phi = [m]$.

1.2.3 Formules explicites pour la loi de groupe

Nous avons vu, à la section 1.2.1, que l'ensemble des points d'une courbe elliptique dans $\mathbb{P}^2$ forme un groupe. Nous donnons ici les formules donnant les coordonnées de "la somme" de deux points sur une courbe elliptique $E/\mathbf{K}$.

Soient $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ deux points de $E/\mathbf{K}$, on note $(x_{P\oplus Q}, y_{P\oplus Q})$ les coordonnées du point $P \oplus Q \in E$.

Algorithme 1.2.8. [1er cas :] *Si $x_P \neq x_Q$. On pose $s = (y_P - y_Q)/(x_P - x_Q)$ et $t = (y_P x_Q - y_Q x_P)/(x_P - x_Q)$. La droite qui passe par les points P et Q a pour équation $y = sx + t$. Elle recoupe la courbe E en un troisième point R de coordonnées $x_R = s^2 - x_P - x_Q, y_R = sx_R + t$. Finalement, le point $P \oplus Q$ (qui est le symétrique de R par rapport à l'axe des abscisses) a pour coordonnées :*

$$x_{P\oplus Q} = x_R = s^2 - x_P - x_Q, \tag{1.7}$$
$$y_{P\oplus Q} = -y_R = -s(s^2 - x_P - x_Q) - t. \tag{1.8}$$

[2eme cas :] *Si $x_P = x_Q$ et $y_P \neq y_Q$. On a nécessairement $y_P = -y_Q$ à cause de l'équation de la courbe. La droite sécante qui joint les deux points est verticale, donc le troisième point d'intersection de cette sécante avec la courbe est le point à l'infini : $P \oplus Q = O_E$.*

[3eme cas :] *Si $x_P = x_Q$ et $y_P = y_Q \neq 0$, autrement dit $P = Q$ et ce point n'est pas sur l'axe des abscisses. L'équation de la tangente à la courbe en P est $y = sx + t$, avec $s = (3{x_P}^2 + a)/(2y_P)$ et $t = y_P - (3{x_P}^2 + a)x_P/(2y_P)$. Le point $P \oplus Q = 2P$ a pour coordonnées :*

$$x_{2P} = s^2 - 2x_P, \tag{1.9}$$
$$y_{2P} = -y_P + s(x_P - x_{2P}). \tag{1.10}$$

[4eme cas :] *Si $x_P = x_Q$ et $y_P = y_Q = 0$. Le point $P = Q$ se trouve sur l'axe des abscisses, la tangente à la courbe en P est verticale, donc le troisième point d'intersection est le point à l'infini. Donc $P \oplus Q = 2P = O_E$.*

Avant d'énoncer un résultat fondamental concernant la loi de groupe sur une courbe elliptique, nous précisons que les coordonnées de l'opposé $-P$ d'un point $P = (x_P, y_P) \in E$ sont $x_{-P} = x_P$ et $y_{-P} = -y_P$.

Théorème 1.2.9 ([30], page 68)**.** *Soit $E/\mathbf{K}$ une courbe elliptique. Alors les équations de l'algorithme* 1.2.8*, explicitant la loi de groupe, définissent des morphismes de variétés*

$$\begin{array}{rccc} \oplus : & E \times E & \to & E \\ & (P_1, P_2) & \mapsto & P_1 \oplus P_2 \end{array} \quad et \quad \begin{array}{rccc} \ominus : & E & \to & E \\ & P & \mapsto & -P \end{array}$$

Soit

$$\mathrm{Hom}(E_1, E_2) = \{ \text{ isogénies } \phi : E_1 \to E_2 \}.$$

D'après le théorème 1.2.9, $\mathrm{Hom}(E_1, E_2)$ est un groupe, l'isogénie "somme" est définie par

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

Et si $E_1 = E_2$, on peut composer ces isogénies.

Soit $E/\mathbf{K}$ une courbe elliptique. On note

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

l'anneau des endomorphismes de E, la loi d'addition est celle définie ci-dessus et la multiplication est donnée par

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

L'ensemble $\mathrm{End}(E)$ des isogénies de E dans E n'est pas un anneau tout à fait quelconque, il a des propriétés particulières qui ne sont vérifiées que par une certaine classe d'anneaux. Le théorème 1.2.11 va nous éclairer dans ce sens, mais avant nous fixons une petite définition.

Définition 1.2.10. *Soit $\mathbf{K}$ une algèbre (non nécessairement commutative) de type fini sur $\mathbf{Q}$. Un ordre $\mathcal{R}$ de $\mathbf{K}$ est un sous-anneau de $\mathbf{K}$ qui est un $\mathbf{Z}$-module de type fini vérifiant $\mathcal{R} \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{K}$.*

Dans le cas où $\mathbf{K}$ est un corps de nombres, un ordre de $\mathbf{K}$ est un sous-anneau et un $\mathbf{Z}$-module libre de rang $[\mathbf{K} : \mathbf{Q}]$.

Théorème 1.2.11 ([30], corollaire 9.4., P. 102)**.** *L'anneau des endomorphismes* $\mathrm{End}(E)$ *d'une courbe elliptique E est soit $\mathbf{Z}$, soit un ordre quadratique imaginaire, ou un ordre d'une algèbre de quaternions.*

1.2.4 Exemples

Soit $E/\mathbf{K}$ une courbe elliptique. Pour chaque $m \in \mathbf{Z}$, on peut définir une isogénie

$$[m] : E \to E$$

de la façon suivante. Pour $m > 0$, on a

$$[m](P) = P \oplus P \oplus \cdots \oplus P(m \text{ termes }).$$

Si $m < 0$ alors $[m](P) = [-m](-P)$; l'isogénie identiquement nulle a déjà été définie.

Soit $E/\mathbf{K}$ une courbe ellipique et $m \in \mathbf{Z}$ un entier tel que $m \neq 0$. Le sous-groupe de m-torsion de $E(\overline{\mathbf{K}})$, noté $E[m]$, est l'ensemble des points de $E(\overline{\mathbf{K}})$ d'ordre divisant m

$$E[m] = \{P \in E : [m]P = O\}.$$

Si $E/\mathbf{K}$ est une courbe elliptique sur un corps $\mathbf{K}$ de caractéristique différente de 2 et 3, et $P = (X : Y : 1)$ un point de E alors il existe des polynômes $\phi_m(X,Y)$, $\psi_m(X,Y)$ et $\omega_m(X,Y)$ tels que

$$[m]P = \underbrace{P + \cdots + P}_{m \ fois} = (\phi_m(X,Y)\psi_m(X,Y) : \omega_m(X,Y) : \psi_m^3(X,Y)). \tag{1.11}$$

Les polynômes ϕ_m, ψ_m et ω_m sont dits *polynômes de division*. On a le théorème suivant :

Théorème 1.2.12. *Soient $\overline{\mathbf{K}}$ la clôture algébrique du corps $\mathbf{K}$ et m un entier.*
Si $P = (x : y : 1) \in E(\overline{\mathbf{K}})$ est tel que $P \neq 0_E$, alors P est un point de m-torsion si et seulement si $\psi_m(x,y) = 0$.

Supposons que $\mathrm{Char}(\mathbf{K}) = p > 0$ et fixons $q = p^r$. À toute courbe elliptique $C/\mathbf{K}$ d'équation affine

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

on associe la courbe elliptique $C^{(q)}/\mathbf{K}$ d'équation affine

$$y^2 = x^3 + a^q x + b^q$$

Il existe une application naturelle de C vers $C^{(q)}$ appelée *morphisme de Frobenuis* et donnée par

$$\mathrm{Frob}_q : C \to C^{(q)}$$
$$\mathrm{Frob}_q((x_0 : x_1 : x_2)) = (x_0^q : x_1^q : x_2^q).$$

L'application Frob_q est une isogénie.

Chapitre 2

Réduction des courbes elliptiques

Dans ce chapitre nous exposons la théorie algorithmique de la multiplication complexe des courbes elliptiques. Nous développons plus particulièrement les aspects algorithmiques des théorèmes de réduction et de relèvement de Deuring. Les méthodes de calcul introduites ici seront utiles dans la suite de notre travail.

2.1 Courbes elliptiques sur C

L'ensemble des points d'une courbe elliptique sur $\mathbf{C}$ est analytiquement isomorphe à un tore complexe. La construction de cet isomorphisme, à partir des fonctions elliptiques, est détaillée dans plusieurs ouvrages parmi lesquels [30]. Nous reprenons ici cette construction.

2.1.1 Tores complexes et fonctions doublement périodiques

Proposition 2.1.1. *Soit n un entier positif. Tout sous-groupe discret non nul Γ de $\mathbf{R}^n$ est de la forme*

$$\Gamma = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \ldots + \mathbf{Z}\omega_r$$

où r est un entier positif et $(\omega_1, \omega_2, \ldots, \omega_r)$ une partie libre du $\mathbf{R}$-espace vectoriel $\mathbf{R}^n$.

Un tel groupe Γ est appelé réseau de $\mathbf{R}^n$ et l'entier r est le rang de Γ.

En particulier les sous-groupes discrets de $\mathbf{C}$ non nuls et non isomorphes à $\mathbf{Z}$ sont de la forme

$$\mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$$

avec $\omega_1, \omega_2 \in \mathbf{C}$ et $\omega_2/\omega_1 \notin \mathbf{R}$.

Définition 2.1.2. *On appelle tore le quotient $T = \mathbf{C}/\Gamma$ du groupe $(\mathbf{C}, +)$ par un reseau $\Gamma = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ de rang 2. On note $\rho : \mathbf{C} \to T$ l'application quotient.*

Une fonction elliptique de périodes Γ *est une fonction meromorphe* f *sur* $\mathbf{C}$ *telle que* $f(z+\omega) = f(z)$ *pour tout* $\omega \in \Gamma$.

À toute fonction elliptique f on associe la fonction $\bar{f} : T \to \mathbf{C} \cup \infty$ telle que $f = \bar{f} \circ \rho$.

Une fonction elliptique de périodes Γ peut donc être vue comme une fonction méromorphe du tore.

Observons qu'une fonction elliptique sans pôle est constante car une telle fonction est holomorphe et bornée sur $\mathbf{C}$ (on conclut grâce au théorème de Liouville).

Proposition 2.1.3. *Soit* f *une fonction elliptique de périodes* Γ *et soit* (ω_1, ω_2) *une base du* $\mathbf{Z}$*-module* Γ. *Il existe un* $a \in \mathbf{C}$ *tel que le bord du parallélogramme* $\mathcal{P} = a + [0,1]\omega_1 + [0,1]\omega_2$ *ne rencontre pas l'ensemble des pôles de* f. *On a alors*

$$\sum_{z \in \mathcal{P}} Res_z(f) = 0.$$

Autrement dit, la somme des résidus de f *dans un parallélogramme fondamental de* Γ *est nulle.*

On en déduit qu'une fonction méromorphe non constante sur un tore a au moins deux pôles en comptant les multiplicités.

Proposition 2.1.4. *Soit* f *une fonction elliptique de périodes* Γ *et soit* (ω_1, ω_2) *une base du* $\mathbf{Z}$*-module* Γ. *Il existe un* $a \in \mathbf{C}$ *tel que le bord du parallélogramme* $\mathcal{P} = a + [0,1]\omega_1 + [0,1]\omega_2$ *ne rencontre pas l'ensemble des zéros et des pôles de* f. *On a alors*

$$\sum_{z \in \mathcal{P}} ord_z(f) = 0 \tag{2.1}$$

$$\sum_{z \in \mathcal{P}} z.ord_z(f) \in \Gamma. \tag{2.2}$$

Où $ord_z(f)$ *est l'ordre du zéro ou du pôle de* f *en* z.

L'ensemble des fonctions elliptiques de périodes Γ forment un corps que l'on note M_Γ. C'est le corps des fonctions méromorphes du tore T.

2.1.2 Construction des fonctions elliptiques

La construction de ce corps passe par l'étude de la fonction $\wp$ de Weierstrass. On utilise le

Lemme 2.1.5. *Si* $s \in \mathbf{R}$ *et* $s > 2$ *alors*

$$\sum_{\omega \in \Gamma - \{0\}} \frac{1}{\omega^s}$$

converge absolument.

En effet, il existe une constante positive ϵ telle que $|n_1\omega_1 + n_2\omega_2| > \epsilon(|n_1| + |n_2|)$ pour tout $(n_1, n_2) \in \mathbf{Z} \times \mathbf{Z} - \{(0,0)\}$. Comme, pour tout entier naturel non nul $n \in \mathbb{N}^*$, il existe $4n$ paires $(n_1, n_2) \in \mathbf{Z} \times \mathbf{Z} - \{(0,0)\}$ telles que $|n_1| + |n_2| = n$, on conclut aisément.

Il est alors naturel d'introduire la série

$$\sum_{\omega \in \Gamma} \frac{1}{(z-\omega)^3}.$$

On vérifie que cette série est absolument uniformément convergente dans tout compact disjoint de Γ et qu'elle définit une fonction elliptique impaire qui admet un pôle triple en tout point de Γ.

On définit une intégrale de cette dernière fonction en posant

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Gamma - \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

La fonction $\wp(z)$ est holomorphe sur $\mathbf{C} - \Gamma$ et méromorphe paire sur $\mathbf{C}$ avec des pôles doubles en tous points de Γ.

On a

$$\wp'(z) = -2 \sum_{\omega \in \Gamma} \frac{1}{(z-\omega)^3}$$

qui est elliptique.

Comme $\wp'$ est elliptique, on a pour tout $\omega \in \Gamma$

$$\wp(z + \omega) = \wp(z) + \nu$$

et ν ne dépend que de ω.

Remplaçant z par $-\omega/2$ dans l'équation précédente, on voit que $\nu = 0$ car $\wp$ est paire. Donc $\wp$ est elliptique.

Posant

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \in \Gamma - \{0\}} \frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2},$$

on obtient une fonction méromorphe de $\mathbf{C}$ munie d'un pôle simple en tout point de Γ et $\zeta' = -\wp$. Cependant ζ n'est pas elliptique car elle a un seul pôle. Pour toute période $\omega \in \Gamma$ on pose

$$\eta(\omega) = \zeta(z + \omega) - \zeta(z).$$

On montre que le corps M_Γ des fonctions elliptiques de périodes Γ n'est autre que $\mathbf{C}(\wp, \wp')$.

Pour cela on introduit la

Définition 2.1.6. *Un diviseur du tore T est une combinaison linéaire formelle finie de points de T, à coefficients entiers relatifs, c'est à dire un élément du groupe*

$$\mathrm{Div}(T) = \mathbf{Z} < T > .$$

La définition est la même que dans le cas d'une courbe plane projective. Un diviseur $D = \sum_{P \in T} e_P[P]$ sera dit *pair* si $e_P = e_{-P}$ pour tout $P \in T$ *et* $e_P \in 2\mathbf{Z}$ si P est un point de 2 torsion de T i.e. $2P = 0$.

Le degré du diviseur $D = \sum_{P \in T} e_P[P]$ est par définition $\deg(D) = \sum e_P$. L'ensemble $\mathrm{Div}^0(T)$ des diviseurs de degré nul est un sous-groupe de $\mathrm{Div}(T)$.

À toute fonction méromorphe $\bar{f}$ de T on associe le diviseur de ses zéros et pôles noté $(\bar{f}) \in \mathrm{Div}^0(T)$.

On voit sans peine que le diviseur d'une fonction paire est pair.

En particulier, pour tout $a \in \mathbf{C}$ le diviseur de $\bar{\wp}(z) - \bar{\wp}(a)$ est $[a] + [-a] - 2[0]$.

Soit alors f une fonction elliptique paire et non constante et soit $D = (\bar{f})$ le diviseur de T associé à $\bar{f}$. On peut écrire

$$D = e_0[0] + \sum_{1 \leq i \leq I} e_i([P_i] + [-P_i])$$

avec I entier positif et $P_i \neq 0$.

Soient alors z_i des complexes tels que $\rho(z_i) = P_i$. On a

$$f(z) = K \prod_{1 \leq i \leq I} (\wp(z) - \wp(z_i))^{e_i}$$

avec $K \in \mathbf{C}$, car le quotient de ces deux fonctions est elliptique et sans pôles.

On en déduit que l'ensemble des fonctions elliptiques paires est $\mathbf{C}(\wp)$.

Comme toute fonction elliptique f s'écrit

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

on a

$$M_\Gamma = \mathbf{C}(\wp, \wp').$$

2.1.3 L'uniformisation des courbes elliptiques sur C

Le carré $\wp'^2$ de la dérivée de la fonction $\wp$ de Weierstrass est paire, donc appartient à $\mathbf{C}(\wp)$. Pour l'exprimer comme une fraction rationnelle en $\wp$ on étudie son développement limité en 0.

On note que pour $|z| < |\omega|$

$$\frac{1}{z-\omega} = -\frac{1}{\omega}\sum_{n\geq 0}\left(\frac{z}{\omega}\right)^n.$$

On pose

$$G_k = \sum_{\omega\in\Gamma-\{0\}} \omega^{-2k} \tag{2.3}$$

et on trouve que si $|z| < |\omega|$ pour tout $\omega \in \Gamma - \{0\}$

$$\begin{aligned}
\zeta(z) &= \frac{1}{z} - \sum_{k\geq 2} G_k z^{2k-1} && (2.4)\\
\wp(z) &= \frac{1}{z^2} + \sum_{k\geq 2}(2k-1)G_k z^{2k-2} && (2.5)\\
\wp'(z) &= \frac{-1}{z^3} + \sum_{k\geq 2}(2k-1)(2k-2)z^{2k-3} && (2.6)
\end{aligned}$$

L'étude des premiers termes donne

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_2 z^2 + 5G_3 z^4 + ... && (2.7)\\
\wp'(z) &= \frac{-2}{z^3} + 6G_2 z + 20G_3 z^3 + ... && (2.8)\\
\wp'^2(z) &= \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 + ... && (2.9)\\
\wp^3(z) &= \frac{1}{z^6} + \frac{9G_2}{z^2} + 15G_3 + ... && (2.10)\\
\wp'^2(z) - 4\wp^3(z) + 60G_2\wp(z) &= -140G_3 + ... && (2.11)
\end{aligned}$$

Si bien que la fonction $\wp'^2(z) - 4\wp^3(z) + 60G_2\wp(z) + 140G_3$ est elliptique, sans pôle et nulle en zéro donc elle est identiquement nulle. On obtient donc

$$\wp'^2 = 4\wp^3 - 60G_2\wp - 140G_3.$$

Soit Γ un réseau de $\mathbf{C}$, alors le tore $\mathbf{C}/\Gamma$ muni de la loi d'addition naturelle est un groupe de Lie complexe. Et si $E/\mathbf{C}$ est une courbe elliptique, puisque l'addition $\oplus$ et l'inversion $\ominus$ sont données par des fonctions rationnelles définies localement en tout point de $E(\mathbf{C})\times E(\mathbf{C})$ et $E(\mathbf{C})$ respectivement (algorithme 1.2.8 et théorème 1.2.9 du chapitre 1), la variété $E = E(\mathbf{C})$ est aussi un groupe de Lie complexe.

Proposition 2.1.7 ([30],P. 158). *(a) Le polynôme*

$$f(x) = 4x^3 - 60G_2x - 140G_3.$$

n'a que des racines distinctes, et son discriminant

$$\Delta_\Gamma = (60G_2)^3 - (140G_3)^2$$

est non nul.
(b) Soit $E/\mathbf{C}$ la courbe plane projective d'équation affine

$$E : y^2 = 4x^3 - 60G_2x - 140G_3,$$

(qui est lisse d'après (a)). Alors l'application

$$\begin{array}{rccc} \phi : & \mathbf{C}/\Gamma & \to & E \subset \mathbb{P}^2(\mathbf{C}) \\ & z & \mapsto & (\wp(z) : \wp'(z) : 1) \end{array}$$

est un isomorphisme analytique complexe de groupes de Lie complexes.

Les applications analytiques complexes entre tores complexes ont une forme particulièrement simple ; de plus en les composant avec l'isomorphisme analytique de la proposition 2.1.7 on obtient des isogénies. En effet, soient Γ_1 et Γ_2 deux réseaux de $\mathbf{C}$. Si $\alpha \in \mathbf{C}$ vérifie $\alpha\Gamma_1 \subset \Gamma_2$, alors la multiplication par α

$$\begin{array}{rccc} \phi_\alpha : & \mathbf{C}/\Gamma_1 & \to & \mathbf{C}/\Gamma_2 \\ & z & \mapsto & \phi_\alpha(z) = \alpha z \end{array}$$

est un morphisme de groupes de Lie complexes. On a le

Théorème 2.1.8 ([30],P. 159). *1. L'application*

$$\begin{array}{ccc} \{\alpha \in \mathbf{C} : \alpha\Gamma_1 \subset \Gamma_2\} & \to & \{ \begin{array}{c} \textit{applications holomorphes} \\ \phi : \mathbf{C}/\Gamma_1 \to \mathbf{C}/\Gamma_2 \textit{ avec } \phi(0) = 0 \end{array} \} \\ \alpha & \mapsto & \phi_\alpha \end{array}$$

est une bijection.

2. *Soient E_1 et E_2 deux courbes elliptiques associées aux réseaux Γ_1 et Γ_2 (donc aux tores $\mathbf{C}/\Gamma_1$ et $\mathbf{C}/\Gamma_2$). Alors l'inclusion naturelle*

$$\{ \textit{ isogénies } \phi : E_1 \to E_2\} \to \{ \begin{array}{c} \textit{applications holomorphes} \\ \phi : \mathbf{C}/\Gamma_1 \to \mathbf{C}/\Gamma_2 \textit{ avec } \phi(0) = 0 \end{array} \}$$

est une bijection.

Donc les courbes elliptiques $E_1 = \mathbf{C}/\Gamma_1$ et $E_2 = \mathbf{C}/\Gamma_2$ sont isomorphes si et seulement si Γ_1 et Γ_2 sont homothétiques (*i.e* $\Gamma_1 = \alpha\Gamma_2$ pour $\alpha \in \mathbf{C}^*$).

Nous allons maintenant énoncer le théorème d'uniformisation.

Théorème 2.1.9 (Théorème d'uniformisation, [30],P. 158)**.** *Soient $A, B \in \mathbf{C}$ deux nombres complexes vérifiant $A^3 - 27B^2 \neq 0$. Alors il existe un unique réseau $\Gamma \subset \mathbf{C}$ tel que $60G_1(\Gamma) = A$ et $140G_3(\Gamma) = B$*

Corollaire 2.1.10. *Soit $E/\mathbf{C}$ une courbe elliptique. Alors il existe un réseau $\Gamma \subset \mathbf{C}$, unique à homothétie près, et un isomorphisme analytique complexe*

$$\phi : \mathbf{C}/\Gamma \to E(\mathbf{C}) \quad \phi(z) = (\wp(z,\Gamma) : \wp'(z,\Gamma) : 1)$$

de groupes de Lie.

Démonstration. L'existence vient du théorème 2.1.9 et de la proposition 2.1.7 . L'unicité vient du théorème 2.1.8 . □

Ainsi à toute courbe elliptique $E/\mathbf{C}$, on associe un réseau Γ de $\mathbf{C}$ unique à homothétie près de sorte que E s'identifie à $\mathbf{C}/\Gamma$. L'anneau des endomorphismes de E est isomorphe à l'ensemble des $\alpha \in \mathbf{C}$ tels que $\alpha\Gamma \subset \Gamma$. Si $\Gamma = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, on note $\tau = \omega_2/\omega_1$ un *quotient de base* de Γ associé à (ω_1, ω_2). Le réseau Γ est homothétique à $\mathbf{Z} + \tau\mathbf{Z}$.
Dans la suite, nous ne considérerons que des réseaux de la forme $\Gamma = \mathbf{Z} + \tau\mathbf{Z}$.

Un nombre complexe α vérifie $\alpha\Gamma \subset \Gamma$ si et seulement s'il existe quatre entiers a, b, c et d tels que

$$\alpha = a + b\tau \tag{2.12}$$
$$\tag{2.13}$$

$$\alpha\tau = c + d\tau \tag{2.14}$$

On en déduit que $\mathrm{End}(E) = \mathbf{Z}$ sauf si τ est solution d'une équation de degré deux. Dans ce dernier cas, on note $\mathbf{K} = \mathbf{Q}(\tau)$ le corps quadratique imaginaire engendré par τ et Δ son discriminant. Les équations (2.12) et (2.14) montrent que

$$\alpha^2 - (a+d)\alpha + da - bc = 0, \tag{2.15}$$

c'est-à-dire que $\alpha \in \mathbf{K}$ est entier sur $\mathbf{Z}$. Donc l'anneau $\mathrm{End}(E)$ est isomorphe à un ordre O (voir définition 1.2.10) de $\mathbf{K}$. Dans ce cas on dit que E est à multiplication complexe par O, ou CM par O. Rappelons que Δ est le discriminant de $\mathbf{K}$ (chapitre 5 du présent mémoire,

exemple 5.3.18). L'anneau $\mathbf{O_K}$ des entiers de $\mathbf{K}$ est un $\mathbf{Z}$-module libre de rang 2 [[27], P. 48] donné par

$$\mathbf{O_K} = \mathbf{Z}[u] = \mathbf{Z} + u\mathbf{Z} \tag{2.16}$$

avec $u = \frac{\Delta+\sqrt{\Delta}}{2}$ ([8], P. 224).

On en déduit ([19], chap 8, théorème 3) que l'ordre O est de la forme

$$O = \mathbf{Z} + f\mathbf{O_K} = \mathbf{Z} + fu\mathbf{Z} \tag{2.17}$$

où f est un entier appelé le *conducteur* de O.

Nous retenons de cette section que si $E/\mathbf{C}$ est une courbe elliptique sur le corps des nombres complexes, alors il existe un réseau $\Gamma = \mathbf{Z} + \mathbf{Z}\tau$ unique à homothétie près et un isomorphisme analytique complexe qui envoie E sur $\mathbf{C}/\Gamma$ (corollaire 2.1.10). On peut donc considérer que E est la courbe elliptique $E_\Gamma/\mathbf{C}$ d'équation affine

$$y^2 = 4x^3 - 60G_2(\Gamma)x - 140G_3(\Gamma). \tag{2.18}$$

Son anneau d'endomorphismes est soit $\mathbf{Z}$ soit un ordre de $\mathbf{Q}(\tau)$.

On a

$$\Delta(E_\Gamma) = \frac{1}{4}(20(G_2(\Gamma))^3 - 49(G_3(\Gamma))^2) \neq 0 \tag{2.19}$$

$$\text{et } j(E_\Gamma) = j(\Gamma) = 12^3\frac{G_2(\Gamma)^3}{G_2(\Gamma)^3 - 27G_3(\Gamma)^2}\ ; \tag{2.20}$$

où $G_k(\Gamma)$ (pour $k \in \{2,3\}$) est un nombre complexe qui dépend de Γ.

Si α est un nombre complexe non nul et Γ un réseau de $\mathbf{C}$, alors $G_k(\alpha\Gamma) = \alpha^{-2k}G_k(\Gamma)$. Donc $j(E_\Gamma) = j(E_{\alpha\Gamma})$, et par conséquent deux courbes elliptiques sur $\mathbf{C}$ qui ont le même invariant modulaire sont isomorphes .

Notons que si $j \notin \{0, 1728\}$, alors toute courbe elliptique sur $\mathbf{C}$ d'invariant modulaire j est isomorphe à une courbe elliptique d'équation affine

$$y^2 = 4x^3 - 27\frac{j}{j-1728}x - 27\frac{j}{j-1728}. \tag{2.21}$$

Si $j = 1728$, cette courbe est isomorphe à la courbe d'équation affine

$$y^2 = x^3 - x. \tag{2.22}$$

Si $j = 0$, cette courbe est isomorphe à la courbe d'équation affine

$$y^2 = x^3 - 1. \tag{2.23}$$

Exemple 2.1.11. *Considérons la courbe E d'équation*

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

L'application

$$\begin{array}{rccc} I: & E & \to & E \\ & (x,y) & \mapsto & (-x, iy) \end{array}$$

où $i^2 = -1 \in \mathbf{C}$, est un automorphisme de E. L'anneau $\mathrm{End}(E)$ *des endomorphismes de E contient donc $\mathbf{Z}[I]$ qui est isomorphe à $\mathbf{Z}[i]$ (l'isomorphisme envoie $a + bI$ sur $a + bi$). On a vu que l'anneau des endomorphismes d'une courbe elliptique sur $\mathbf{C}$ est soit $\mathbf{Z}$, soit un ordre quadratique imaginaire. Donc il existe un corps quadratique imaginaire $\mathbf{K}$ tel que $\mathbf{Z}[i] \subset \mathrm{End}(E) \subset \mathbf{K}$. Par conséquent $\mathbf{K} = \mathbf{Q}(i)$. Puisque tout élément de* $\mathrm{End}(E)$ *est entier sur $\mathbf{Z}$ (équation* (2.15)*) et que $\mathbf{Z}[i]$ est intégralement clos, on a* $\mathrm{End}(E) = \mathbf{Z}[I]$.

2.2 Courbes elliptiques sur un anneau fini

Les courbes elliptiques sur un anneau fini sont utiles pour les tests de primalité, la factorisation et pour la cryptographie en général. Nous présentons, dans cette section, les aspects intéressants de ces courbes.

2.2.1 L'anneau est un corps fini $\mathbb{F}_q$

Au chapitre 1, nous avons introduit les courbes elliptiques sur un corps quelconque et défini les principales notions liées à ces variétés. Si $E/\mathbf{K}$ est une courbe elliptique, nous avons vu que l'ensemble des isogénies de E vers E est un anneau : l'anneau $\mathrm{End}(E)$ des endomorphismes de E. Dans cette partie nous regardons de près l'endomorphisme de Frobenius d'une courbe elliptique sur un corps fini.

Soit $E/\mathbf{F}_q$ une courbe elliptique sur un corps fini $\mathbf{F}_q$ (q est une puissance d'un certain nombre premier p). Le morphisme de Frobenius $\mathrm{Frob}_q : E \to E^{(q)}$ est un élément de $\mathrm{End}(E)$. En effet, les courbes E et $E^{(q)}$ coincident dans ce cas. De plus un point $P = (x, y)$ est $\mathbf{F}_q$-rationnel si et seulement si $\mathrm{Frob}_q(x, y) = (x, y)$.

L'anneau $\mathrm{End}(E)$ est entier sur $\mathbf{Z}$. Il convient donc, étant donné un endomorphisme $\phi \in \mathrm{End}(E)$, de regarder le polynôme minimal de ϕ.

Théorème 2.2.1 ([32],P.95)**.** *Soit $E/\mathbf{F}_q$ une courbe elliptique définie sur le corps à q éléments et t un entier tel que*

$$t = q + 1 - \#E(\mathbf{F}_q).$$

Alors

$$\mathrm{Frob}_q^2 - t\mathrm{Frob}_q + q = 0,$$

et t est l'unique entier k vérifiant

$$\mathrm{Frob}_q^2 - k\mathrm{Frob}_q + q = 0.$$

En d'autre termes, si $(x, y) \in E(\overline{\mathbf{F}_q})$, alors

$$(x^{q^2}, y^{q^2}) \ominus [t](x^q, y^q) \oplus [q](x, y) = O,$$

et t est l'unique entier tel que la relation reste vraie pour tout $(x, y) \in E(\overline{\mathbf{F}_q})$.

Le polynôme $X^2 - tX + q$, souvent appelé polynôme caractéristique de l'endomorphisme de Frobenius Frob_q, est pratique pour estimer la cardinalité de $E(\mathbf{F}_q)$.

Il existe plusieurs méthodes pour compter les points $\mathbf{F}_q$-rationnels d'une courbe elliptique E définie sur $\mathbf{F}_q$. On peut par exemple utiliser la méthode naïve. Elle consciste à examiner tous les $x \in \mathbf{F}_q$ de façon à identifier ceux qui génèrent un point de $E(\mathbf{F}_q)$, puis déterminer l'effectif de ces derniers. Cette méthode n'est pas très intéressante en terme de complexité (aller à la sous-section 3.1.4 du chapitre 3 pour des précisions sur la notion de complexité). Supposons que $y^2 = x^3 + ax + b$ est l'équation affine de la courbe E. L'algorithme naïf consiste donc à considérer tous les éléments x de $\mathbf{F}_q$ et évaluer le nombre r de ceux pour lesquels x^3+ax+b est un carré dans $\mathbf{F}_q$. On conclut en donnant la cardinalité $\#E(\mathbf{F}_q) = 2r-1$.

L'algorithme de Schoof est une très bonne alternative à la méthode naïve, il est bien plus efficace du point de vue de la rapidité. D'après le raisonnement utilisé dans l'algorithme naïf pour compter les points de $E(\mathbf{F}_q)$, on voit qu'une borne supérieure évidente de $\#E(\mathbf{F}_q)$ est $2q - 1$. Mais nous avons un résultat plus fin, conjecturé par E. Artin et démontré par Hasse dans les années 30.

Théorème 2.2.2 (Hasse, [32],P. 91)**.** *Soit $E/\mathbf{F}_q$ une courbe elliptique. Alors*

$$|q + 1 - \#E(\mathbf{F}_q)| \leq 2\sqrt{q}.$$

L'idée dans l'algorithme de Schoof est de combiner le théorème 2.2.2 de Hasse, le théorème 1.2.12 concernant les polynômes de division et le théorème des restes chinois. On définit un entier $t = q+1-\#E(\mathbf{F}_q)$, puis on choisit un système $S = \{l_1, \ldots, l_r\}$ de nombres premiers distincts de sorte que le produit $N = \prod_{1 \leq i \leq r} l_i$ est strictement plus grand que $4\sqrt{q}$. Ensuite,

en utilisant le théorème de Hasse et les polynômes de division, on détermine $t \bmod l_i$ pour $i = 1, \ldots, r$. On conclut en déterminant $t \bmod N$ à l'aide du théorème des restes chinois. Grâce au théorème de Hasse on est sûr que $t \bmod N$ est la "vraie valeur" de t car $N > 4\sqrt{q}$. On en déduit $\#E(\mathbf{F}_q)$.

Le théorème suivant établit un lien entre les nombres $\#E(\mathbf{F}_q)$ et $\#E(\mathbf{F}_{q^n})$.

Théorème 2.2.3 ([32], P. 97)**.** *Soit $\#E(\mathbf{F}_q) = q + 1 - t$. On écrit $X^2 - tX + q = (X - \alpha)(X - \beta)$. Alors*

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

pour tout n.

Démonstration. La preuve de ce théorème repose sur l'affirmation suivante :

Affirmation : Soit $s_n = \alpha^n + \beta^n$. Alors $s_0 = 2$, $s_1 = t$, et $s_{n+1} = ts_n - qs_{n-1}$ pour tout $n \geq 1$.

D'après l'affirmation, $\alpha^n + \beta^n$ est un entier pour tout $n \geq 0$. Posons

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Alors $X^2 - tX + q = (X - \alpha)(X - \beta)$ divise $f(X)$. Donc

$$f(\mathrm{Frob}_q) = (\mathrm{Frob}_q^n)^2 - (\alpha^n + \beta^n)\mathrm{Frob}_q^n + q^n = 0,$$

d'après le théorème 2.2.1. On note que $\mathrm{Frob}_q^n = \mathrm{Frob}_{q^n}$. D'après le théorème 2.2.1, il existe un unique entier k tel que $(\mathrm{Frob}_q^n)^2 - k\mathrm{Frob}_q^n + q^n = 0$, et cet entier est donné par $k = q^n + 1 - \#E(\mathbf{F}_{q^n})$ □

2.2.2 Courbes elliptiques sur $\mathbb{Z}/N\mathbb{Z}$

Hendrick W. Lenstra a consacré toute la section 3 de [22] à l'étude des courbes elliptiques sur un anneau. Dans cette sous-section nous donnons les définitions et propriétés importantes (du moins celles qui nous seront utiles) des courbes elliptiques sur un anneau $\mathbf{Z}/N\mathbf{Z}$.

Définition 2.2.4. *Soit $N \in \mathbf{Z}$ un entier composé premier à 6.*
Un triplet $(X, Y, Z) \in (\mathbf{Z}/N\mathbf{Z})^3$ est dit primitif si $pgcd(X, Y, Z, N) = 1$.

Le plan projectif $\mathbb{P}^2(\mathbf{Z}/N\mathbf{Z})$ est l'ensemble des triplets primitifs $(X, Y, Z) \in (\mathbf{Z}/N\mathbf{Z})^3$ modulo la relation d'équivalence : $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ si et seulement s'il existe une unité $\lambda \in (\mathbf{Z}/N\mathbf{Z})^\times$ tel que $(X_2, Y_2, Z_2) = (\lambda X_1, \lambda Y_1, \lambda Z_1)$.

Nous considérerons qu'une courbe elliptique modulo N est l'ensemble des éléments de $\mathbb{P}^2(\mathbf{Z}/N\mathbf{Z})$ vérifiant l'équation

$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{2.24}$$

L'ensemble des points $E(\mathbf{Z}/N\mathbf{Z}) \subset \mathbb{P}^2(\mathbf{Z}/N\mathbf{Z})$ de la courbe elliptique E modulo N forme un groupe commutatif [[22], section 3] dont l'élément neutre est le point à l'infini $O = (0 : 1 : 0)$. L'obtention de formules explicites pour la loi de groupe n'est pas aussi aisée que dans le cas d'une courbe sur un corps. Les éléments non inversibles de $\mathbf{Z}/N\mathbf{Z}$ rendent la tâche plus ardue. Mais pour un test de primalité, cette situation est particulièrement intéressante. En fait l'utilisation sur $E(\mathbf{Z}/N\mathbf{Z})$ des formules requises pour la loi de groupe sur l'ensemble des points d'une courbe elliptique définie sur un corps peut engendrer des situations dégénérées dûes à la présence d'éléments non inversibles dans l'anneau. On peut obtenir des diviseurs de N de cette façon.

Soit N un nombre entier composé et k un diviseur de N. L'application canonique

$$\begin{array}{rccc} \varphi : & \mathbf{Z}/N\mathbf{Z} & \to & \mathbf{Z}/k\mathbf{Z} \\ & x \bmod N & \mapsto & x \bmod k \end{array}$$

est un morphisme surjectif d'anneaux.

Nous appellerons réduction modulaire, l'application

$$\begin{array}{rccc} \psi : & \mathbb{P}^2(\mathbf{Z}/N\mathbf{Z}) & \to & \mathbb{P}^2(\mathbf{Z}/k\mathbf{Z}) \\ & (X \bmod N : Y \bmod N : Z \bmod N) & \mapsto & (X \bmod k : Y \bmod k : Z \bmod k) \end{array}$$

induite par φ sur les plans projectifs.

La réduction modulaire conserve les droites des plans projectifs, c'est-à-dire envoie une droite passant par deux points donnés sur la droite passant par les deux points réduits. De plus, la loi d'addition sur l'ensemble des points d'une courbe elliptique est définie par des droites (voir loi de composition 1.2.3 au chapitre 1). Donc la surjection canonique φ (resp. l'isomorphisme des restes chinois) s'étend en un morphisme (resp. un isomorphisme) de groupes.

2.3 Multiplication complexe et applications

Soit $\mathbf{K}$ un corps quadratique imaginaire. Une courbe elliptique CM par un ordre O (voir définition 1.2.10) de $\mathbf{K}$ est une courbe elliptique $E/\mathbf{C}$ dont l'anneau des endomorphismes est isomorphe à O. Dans cette section, nous donnons quelques précisions au sujet des courbes elliptiques à multiplication complexe et nous explicitons la réduction de ces dernières.

2.3.1 Courbes elliptiques sur $\overline{\mathbf{Q}}$

Soit $\mathbf{K}$ un corps quadratique imaginaire. On note $\mathbf{O_K}$ l'anneau des entiers de $\mathbf{K}$ et O un ordre (voir définition 1.2.10) de $\mathbf{K}$. Nous considérons dans la suite le corps $\mathbf{K}$ comme un sous-corps de $\mathbf{C}$.

Il s'agit d'étudier les courbes elliptiques CM par O. Pour cela il suffit de considérer une classe particulère d'idéaux de O : les idéaux propres. Définissons cette notion.

Définition 2.3.1. *On dit qu'un idéal $\mathfrak{l}$ de O est propre si $\mathfrak{l} \subset O$ et si*

$$O = \{\lambda \in \mathbf{K} : \lambda\mathfrak{l} \subset \mathfrak{l}\}.$$

Un idéal $\mathfrak{l}$ de O est dit premier avec le conducteur f de O, si $\mathfrak{l} + fO = O$.

Un idéal de O premier avec f est nécessairement propre ([19], chap 8, théorème 4). Donc si $\mathfrak{l}$ est un idéal propre de O, alors le théorème 2.1.8 nous permet d'affirmer que le tore $\mathbf{C}/\mathfrak{l}$ est une courbe elliptique CM par O.

Définition 2.3.2. *On appelle discriminant quadratique le discriminant d'un ordre d'une extension de degré 2 du corps des nombres rationnels.*
Un entier rationnel $D \neq 1$ est dit discriminant fondamental lorsque D est le discriminant d'un corps quadratique, c'est-à-dire D n'est pas divisible par le carré d'un nombre premier impair, et de plus $D \equiv 1 \bmod 4$ ou bien $D = 4m$ avec $m \equiv 2, 3 \bmod 4$.
Soit $D = f^2\Delta < 0$ un discriminant quadratique avec $f \geq 1$ maximal tel que $\Delta \equiv 1$ ou $0 \bmod 4$. Alors Δ est un discriminant fondamental et f le conducteur associé à D. Notons $\mathbf{K} = \mathbf{Q}(\sqrt{\Delta})$. L'anneau des entiers du corps quadadratique $\mathbf{K}$ de discriminant Δ est $\mathbf{O}_\Delta = \mathbf{Z}[\omega]$ et l'ordre de $\mathbf{K}$ de discriminant D est $\mathbf{O}_D = \mathbf{Z}[f\omega]$ avec $\omega = \frac{\Delta+\sqrt{\Delta}}{2}$. Le groupe de classe Cl_D de $\mathbf{O}_D$ est le groupe abélien fini des idéaux inversibles de $\mathbf{O}_D$ modulo les idéaux principaux. Le groupe Cl_D est isomorphe ([19], chap 8, page 94) au groupe des idéaux fractionnaires de $\mathbf{O}_\Delta$ premiers avec f modulo les idéaux principaux $\alpha\mathbf{O}_\Delta$ tels que

$$\alpha \equiv a \bmod f\mathbf{O}_\Delta$$

pour $a \in \mathbf{Z}$ avec $pgcd(a, f) = 1$. Le cardinal du groupe de classes Cl_D est le nombre de classes h_D.

Le *corps de classes de Hilbert* $\mathbf{H}$ d'un corps de nombres $\mathbf{K}$ est son extension abélienne maximale non ramifiée ; le groupe de Galois $\mathrm{Gal}(\mathbf{H}/\mathbf{K})$ est isomorphe au groupe de classes de $\mathbf{K}$. Pour un ordre $\mathbf{O}$ de $\mathbf{K}$, le *corps de classes d'anneaux* associé à $\mathbf{O}$ est une extension abélienne de $\mathbf{K}$ dont le groupe de Galois est isomorphe au groupe de classes de $\mathbf{O}$ ([9]).

Heinrich Weber a établi le résultat suivant, qui peut être considéré comme le premier théorème principal de la multiplication complexe.

Théorème 2.3.3. *Soit $\mathbf{O}_D$ l'ordre de discriminant D dans un corps quadratique imaginaire $\mathbf{K}$. Soit $\mathfrak{l}_1, \cdots, \mathfrak{l}_{h_D}$ un système de représentants du groupe de classes Cl_D, et $\tau_1, \ldots, \tau_{h_D}$ des quotients de bases. Alors tout $j(\mathfrak{l}_i) = j(\tau_i)$ engendre, au-dessus de $\mathbf{K}$, le corps de classes d'anneaux $\mathbf{H}_D$ associé à $\mathbf{O}_D$. Le polynôme minimal de $j(\tau_i)$ est le polynôme de classes*

$$H_D(X) = \Pi_{i=1}^{h_D}(X - j(\mathfrak{l}_i)) = \Pi_{i=1}^{h_D}(X - j(\tau_i)) \ ,$$

qui est irréductible sur $\mathbf{K}$ et à coefficients dans $\mathbf{Z}$. Plus précisement, si $\mathfrak{l}_i$ est d'ordre 2 alors $j(\mathfrak{l}_i)$ est réel, sinon $j(\mathfrak{l}_i)$ et $j(\mathfrak{l}_i^{-1})$ sont conjugués complexes.

Le groupe de galois $\mathrm{Gal}(\mathbf{H}_D/\mathbf{K})$ agit sur les racines $j(\tau_i)$ de $H_D(X)$. Notons

$$\sigma : \mathrm{Cl}(\mathbf{O}_D) \to \mathrm{Gal}(\mathbf{H}_D/\mathbf{K})$$

l'isomorphisme entre le groupe de classes de $\mathbf{O}_D$ et le groupe de Galois de $\mathbf{H}_D/\mathbf{K}$ ainsi défini : si $\mathfrak{l}_i$ et $\mathfrak{l}_j$ sont deux idéaux propres de $\mathbf{O}_D$, alors l'image de $j(\mathfrak{l}_j)$ par $\sigma(\mathfrak{l}_i)$ est $j(\mathfrak{l}_i^{-1}\mathfrak{l}_j)$.

Par définition de $G_k(\mathfrak{l}_i)$ et $j(\mathfrak{l}_i)$ (équations (2.3) et (2.20)) on a $\overline{j(\mathfrak{l}_i)} = j(\overline{\mathfrak{l}_i})$. D'autre part si $\mathfrak{l} = \mathbf{Z} + \mathbf{Z}\tau$ est un idéal propre d'un ordre quadratique O, alors l'inverse de la classe de $\mathfrak{l}$ dans le groupe de classes de O est la classe de $\overline{\mathfrak{l}} = \mathbf{Z} + \mathbf{Z}\overline{\tau}$ [[19], page 90]. Ainsi la conjugaison complexe agit sur les racines de $H_D(X)$ par

$$\overline{j(\mathfrak{l}_i)} = j(\mathfrak{l}_i^{-1}).$$

La dernière phrase du théorème 2.3.3 se trouve donc justifiée : $j(\mathfrak{l}_i)$ et $j(\mathfrak{l}_i^{-1})$ sont conjugués complexes, et si $\mathfrak{l}_i$ est d'ordre 2 alors $\overline{j(\mathfrak{l}_i)} = j(\mathfrak{l}_i)$.

2.3.2 Réduction des courbes elliptiques définies sur un corps local

Nous allons décrire, dans cette section, comment se fait la réduction d'une courbe elliptique définie sur un corps local. Cette description nous prépare à la reduction des courbes elliptiques définies sur $\mathbf{C}$ à multiplication complexe par un ordre quadratique, une des six étapes du test de primalité ECPP. Sauf mention contraire explicite, nous utiliserons les notations suivantes.

$\mathbf{K}$	un corps local complet pour une valuation discrète v
$\mathbf{R}$	l'anneau des entiers de $\mathbf{K}$ égal à $\{x \in \mathbf{K} : v(x) \geq 0\}$
$\mathbf{R}^*$	le groupe des unités de $\mathbf{R}$ égal à $\{x \in \mathbf{K} : v(x) = 0\}$
$\mathfrak{m}$	l'idéal maximal de $\mathbf{R}$ égal à $\{x \in \mathbf{K} : v(x) > 0\}$
π	une uniformisante de $\mathbf{R}$ (c'est-à-dire $\mathfrak{m} = \pi\mathbf{R}$)
k	le corps résiduel de $\mathbf{R}$ égal à $\mathbf{R}/\mathfrak{m}$.

Soit E une courbe elliptique sur $\mathbf{K}$ d'équation affine

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.25}$$

L'application $(x, y) \to (u^{-2}x, u^{-3}y)$ est un isomorphisme de courbes elliptiques. En appliquant cet isomorphisme à l'équation (2.25), on obtient une équation affine de E à coefficients dans $\mathbf{R}$ (il suffit pour cela que u soit un multiple d'une grande puissance de π). Donc le discriminant Δ_E vérifie $v(\Delta_E) \geq 0$, et puisque $v_{\mathfrak{p}}$ est une valuation discrète on peut chercher une équation de E avec $v(\Delta_E)$ aussi petite que possible.

Définition 2.3.4. *Une équation de Weierstrass*

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

d'une courbe elliptique $E/\mathbf{K}$ est dite équation minimale (de Weierstrass) pour E en v si $v(\Delta_E)$ est minimale et si les coefficients $a_1, \ldots, a_6$ sont dans $\mathbf{R}$. Cette valeur $v(\Delta_E)$ est la valuation du discrimiant minimal de E en v.

Proposition 2.3.5 ([30],P. 172)**.** *(a) Toute courbe elliptique $E/\mathbf{K}$ admet une équation minimale de Weierstrass.*

(b) Une équation minimale de Weierstrass est unique au changement de coordonnées

$$x = u^2x' + r \qquad y = u^3y' + u^2sx' + t$$

près, avec $u \in \mathbf{R}^*$ et $r, s, t \in \mathbf{R}$.

(c) Réciproquement, si on a une équation de Weierstrass à coefficients dans $\mathbf{R}$, alors il existe un changement de coordonnées

$$x = u^2x' + r \qquad y = u^3y' + u^2sx' + t$$

permettant de passer à une équation minimale de Weierstrass avec $u, r, s, t \in \mathbf{R}$.

Maintenant nous allons décrire l'opération de réduction modulo π.

Étant donnée une équation de Weierstrass minimale d'une courbe elliptique E

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

nous pouvons réduire ses coefficients modulo π et obtenir une courbe (éventuellement singulière) sur k

$$\widetilde{E} : y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}.$$

La courbe $\widetilde{E}$ est la *réduction* (on dit aussi la *réduite*) de E modulo π. Les propositions 1.2.2(b) et 2.3.5(b) nous permettent de dire que l'équation de $\widetilde{E}$ est unique modulo un changement de coordonnées d'équations de Weierstrass sur k.

Définition 2.3.6. *Soient $E/\mathbf{K}$ une courbe elliptique, et $\widetilde{E}$ sa réduite pour une équation de Weierstrass minimale.*

(a) On dit que E a bonne réduction (ou une réduction stable) sur $\mathbf{K}$ si $\widetilde{E}$ est lisse.
(b) On dit que E a potentielle bonne réduction sur $\mathbf{K}$ s'il existe une extension finie $\mathbf{K}'/\mathbf{K}$ telle que E a bonne réduction sur $\mathbf{K}'$.

Proposition 2.3.7 ([30], page 181)**.** *Soit $E/\mathbf{K}$ une courbe elliptique. Alors E a potentielle bonne réduction si et seulement si son invariant modulaire $j(E) \in \mathbf{R}$.*

2.3.3 Réduction des courbes elliptiques CM

Ayant décrit de façon générale, dans la section précédente, la réduction des courbes elliptiques, nous pouvons maintenant spécifier le cas des courbes elliptiques définies sur $\mathbf{C}$ à multiplication par un ordre quadratique.

Soit $E/\mathbf{C}$ une courbe elliptique sur le corps des nombres complexes, CM par un ordre O du corps quadratique $\mathbf{K}$. Elle correspond à un tore complexe $\mathbf{C}/\Gamma$ où Γ est un réseau de $\mathbf{C}$, et l'anneau des endomorphismes $\mathrm{End}(E) = \{\alpha \in \mathbf{C} : \alpha\Gamma \subset \Gamma\}$ est égal à O. L'invariant modulaire $j(E) = j(\Gamma)$ de E est donné par l'équation (2.20) et on a vu que si $j(E) \notin \{0, 1728\}$ alors E est isomorphe à une courbe elliptique définie sur $\overline{\mathbf{Q}}$ par

$$y^2 = 4x^3 - 27\frac{j(E)}{j(E) - 1728}x - 27\frac{j(E)}{j(E) - 1728}.$$

Dans le cas où $j(E) \in \{0, 1728\}$ la courbe elliptique E est isomorphe à une courbe d'équation affine (2.22) ou (2.23). Dans tous les cas E est isomorphe à une courbe elliptique définie sur le corps $\mathbf{Q}(j(E))$ d'après le théorème 2.3.3.

On suppose que l'entier p est un nombre premier et que p est complètement décomposé dans le corps de classes d'anneau $\mathbf{H}$ de $\mathbf{K}$ associé à O. Notons h le nombre de classe de O. Puisque l'anneau des entiers $O_{\mathbf{H}}$ de $\mathbf{H}$ est de Dedekind [[27], chapitre 3, théorème 1], l'idéal engendré par p se décompose en

$$(p) = \prod_{1 \leq i \leq 2h} \mathfrak{p}_i.$$

On considère, pour $\mathfrak{p} \in \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{2h}\}$, la valution discrète $v_{\mathfrak{p}}$ de $\mathbf{H}$ associée à $\mathfrak{p}$.

On note $\mathbf{H}_{v_{\mathfrak{p}}}$ le *complété* (*la complétion*) de $\mathbf{H}$ pour la valuation $v_{\mathfrak{p}}$. L'anneau $\mathcal{O} = \{x \in \mathbf{H}_{v_{\mathfrak{p}}} : v_{\mathfrak{p}}(x) \geq 0\}$ des entiers de $\mathbf{H}_{v_{\mathfrak{p}}}$ est un anneau local principal d'idéal maximal $\mathfrak{P} = \{x \in \mathbf{H}_{v_{\mathfrak{p}}} : v_{\mathfrak{p}}(x) > 0\}$[[26], chapitre 2,§3, proposition 3.8]. Le quotient $\mathcal{O}/\mathfrak{P} \cong \mathbf{Z}/p\mathbf{Z}$ est le corps résiduel de $\mathcal{O}$ et p est une uniformisante de $\mathcal{O}$. Par ailleurs, $\mathcal{O}$ est la completion de $O_{\mathbf{H}}$, donc $j(E) \in \mathcal{O}$.

La courbe $E/\mathbf{C}$ est donc définie sur $\mathbf{H}_{v_{\mathfrak{p}}}$ et son équation affine est

$$y^2 = 4x^3 - 27\frac{j(E)}{j(E)-1728}x - 27\frac{j(E)}{j(E)-1728},$$

on remplacera cette équation par l'une des équations (2.22) ou (2.23) selon que $j(E) = 0$ ou $j(E) = 1728$.

D'après le théorème 2.3.3 l'invariant modulaire $j(E) \in O_{\mathbf{H}}$. Donc (proposition 2.3.7) notre courbe $E/\mathbf{C}$ a potentielle bonne réduction sur $\mathbf{Q}_p$. On peut donc associer à E une courbe $\overline{E}$ sur $\mathbf{Z}/p\mathbf{Z}$ d'invariant modulaire $j(\overline{E}) = j(E) \bmod \mathfrak{p}$.

Plus généralement, Max Deuring a établi la relation suivante entre les courbes elliptiques, définies sur le corps de classes d'anneau $\mathbf{H}$ d'un corps quadratique $\mathbf{K}$ associé à un ordre $O \subset \mathbf{K}$, et leurs réduites.

Théorème 2.3.8 (Théorème de réduction et de relèvement de Deuring)**.** *Soient E une courbe elliptique à multiplication complexe par $\mathbf{O}_D \subset \mathbf{K} = \mathbf{Q}(\sqrt{D})$, définie sur le corps de classes d'anneau $\mathbf{H}_D$ associé à $\mathbf{O}_D$, et $\mathfrak{P}$ un idéal premier de $\mathbf{H}_D$. Alors la réduction de E modulo $\mathfrak{P}$ est une courbe elliptique $\overline{E}$ avec $\mathbf{O}_D \subset \mathrm{End}(\overline{E})$.*
Soit $p\mathbf{Z} = \mathfrak{P} \cap \mathbf{Z}$. Si p est scindé dans $\mathbf{K} = \mathbf{Q}(\sqrt{D})$, soit D' le discriminant obtenu de D en enlevant les facteurs de p du conducteur ; alors $\mathrm{End}(\overline{E}) = \mathbf{O}_{D'}$. Si p est ramifié ou inerte dans $\mathbf{K}$, alors $\overline{E}$ est supersingulière.
Inversement, toute courbe définie sur un corps fini s'obtient de cette manière.

Corollaire 2.3.9. *Soient $\mathbf{F}_q = \mathbf{F}_{p^m}$ un corps fini de caractéristique p et $\mathbf{O}_D$ l'ordre quadratique imaginaire de discriminant D. Des courbes elliptiques à multiplication complexe par $\mathbf{O}_D$ définies sur $\mathbf{F}_q$ existent si et seulement si $p = \mathfrak{p}\overline{\mathfrak{p}}$ est scindé dans $\mathbf{K} = \mathbf{Q}(\sqrt{D})$, l'entier p ne divise pas le conducteur de $\mathbf{O}_D$ et l'ordre de $\mathfrak{p}$ dans Cl_D divise m. Dans ce cas, ces courbes sont au nombre de h_D, et s'obtiennent comme réduction des courbes à multiplication complexe par $\mathbf{O}_D$ définies sur $\mathbf{H}_D$ modulo un idéal premier de $\mathbf{H}_D$ au-dessus de $\mathfrak{p}$.*

Dans la suite nous allons expliquer en détail comment construire une courbe elliptique sur un corps fini avec un cardinal connu à l'avance.

Soient $\mathbf{K} = \mathbf{Q}(\sqrt{\Delta})$ un corps quadratique imaginaire de discriminant Δ, $\mathbf{O_K}$ son anneau d'entiers, $\mathbf{H}$ le corps de classes de Hilbert de $\mathbf{K}$, et p un nombre premier tel que $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ dans $\mathbf{O_K}$ et $\mathfrak{p}$ est complètement décomposé dans $\mathbf{H}$. On considère un idéal premier $\mathfrak{P}$ de $\mathbf{H}$ au dessus de $\mathfrak{p}$ ainsi que la valuation $v_{\mathfrak{P}}$ associée. Tout idéal $\mathfrak{l}$ de $\mathbf{O_K}$ induit une courbe elliptique $E_{\mathfrak{l}}/\mathbf{C} \cong \mathbf{C}/\mathfrak{l}$ à multiplication complexe par $\mathbf{O_K}$. Une telle courbe elliptique se réduit modulo $\mathfrak{P}$ en une courbe elliptique $\overline{E_{\mathfrak{l}}}/\mathbf{F}_p$ à multiplication complexe par $\mathbf{O_K}$. Il convient ici de regarder un élément particulier de $\mathbf{O_K}$: l'endomorphisme de Frobenius

$$\begin{array}{rccc} \mathrm{Frob}_p & : & \overline{E_{\mathfrak{l}}} & \to & \overline{E_{\mathfrak{l}}} \\ & & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

D'après le théorème 2.2.1, l'endomorphisme Frob_p est un entier $\pi \in \mathbf{O_K} = \mathrm{End}(\overline{E_\mathfrak{l}})$ tel que $N_{\mathbf{K/Q}}(\pi) = p$ (c'est-à-dire $p = \pi\overline{\pi}$). De plus, le nombre de points m de $\overline{E}(\mathbf{F}_p)$ est :

$$m = N_{\mathbf{K/Q}}(\pi - 1) = (\pi - 1)(\overline{\pi} - 1) = p + 1 - \mathrm{Tr}_{\mathbf{K/Q}}(\pi).$$

La condition $N_{\mathbf{K/Q}}(\pi) = p$ détermine π à une unité près dans $\mathbf{O_K}$. En général l'anneau $\mathbf{O_K}$ n'a que 2 unités (1 et -1) sauf dans les cas :

- $\Delta = -4$ il y a 4 uniés,
- $\Delta = -3$ il y en a 6.

Si l'on excepte ces deux cas, le cardinal de $\overline{E_\mathfrak{l}}(\mathbf{F}_p)$ appartient donc à l'ensemble

$$\{p + 1 - t,\ p + 1 + t\} \text{ où } t = \mathrm{Tr}_{\mathbf{K/Q}}(\pi).$$

Nous donnons une définition qui va nous aider à conclure quant à la procédure d'obtention d'une courbe elliptique $E/\mathbf{F}_p$ avec un cardinal fixé.

Définition 2.3.10. *Soit $\overline{E}/\mathbf{F}_p$ une courbe elliptique sur $\mathbf{F}_p$ donnée par l'équation affine*

$$\overline{E} : y^2 = x^3 + ax + b.$$

Une tordue quadratique de $\overline{E}$ est une courbe elliptique $\widetilde{E}/\mathbf{F}_p$ donnée par

$$\widetilde{E} : \gamma y^2 = x^3 + ax + b,\ \gamma \in \mathbf{F}_p^*,\ \gamma \textit{ non-résidu quadratique modulo } p\ ,$$

ou bien

$$\widetilde{E} : y^2 = x^3 + a\gamma^{-2}x + b\gamma^{-3},\ \gamma \textit{ non-résidu quadratique modulo } p\ .$$

On conserve les notations de la définition 2.3.10. L'application

$$\begin{array}{rccc} \overline{E}/\mathbf{F}_p(\gamma^{1/2}) : & \to & \widetilde{E}/\mathbf{F}_p(\gamma^{1/2}) \\ (x, y) & \mapsto & (x, \gamma^{1/2}y) \end{array}$$

est un isomorphisme de courbes elliptiques sur $\mathbf{F}_p(\gamma^{1/2})$.
Puisque $\mathrm{End}(\overline{E}) = \mathbf{O_K}$, la courbe $\widetilde{E}$ est elle aussi CM par $\mathbf{O_K}$.

On vérifie sans peine que si $\overline{E}$ a $p + 1 - t$ points $\mathbf{F}_p$-rationnels alors $\widetilde{E}$ en a $p + 1 + t$, et réciproquement.

2.3.4 Exemples

Les notations dans cette sous-section sont les mêmes qu'à la fin de la section précédente.

Nous allons, à l'aide du même corps quadratique imaginaire $\mathbf{K} = \mathbf{Q}(\sqrt{-404})$ et selon deux méthodes différentes, construire des courbes elliptiques $E/\mathbf{F}_{1009}$ à multiplication complexe par l'anneau des entiers $\mathbf{O_K}$ de $\mathbf{K}$ avec le logiciel PARI / GP. Grâce à l'équation (2.21), on peut se contenter de donner, j mod 1009, la réduction du j-invariant de la courbe $\mathbf{C}/\mathbf{O_K}$ modulo un idéal premier $\mathfrak{P}$ du corps de classes de Hilbert de $\mathbf{K}$ au-dessus de 1009.

Première méthode : l'approche standard

Nous commençons par l'approche standard. Elle consiste à réduire le polynôme de classes H_D modulo 1009 et calculer une racine j mod 1009.

Le polynôme de classes H_D est intéressant car il fait le lien direct entre le corps de classes et les courbes elliptiques mais il s'avère difficile à calculer à cause de la taille de ses coefficients. Classiquement, le polynôme de classes s'obtient à partir d'approximations complexes de ses racines. Si la précisions de calcul est suffisamment grande, on peut arrondir les coefficients ainsi calculés vers des entiers. Malheureusement les coefficients de H_D croissent très vite avec le discriminant. La parade est de négocier avec des générateurs des corps de classes ayant des polynômes minimaux plus petits.

Considérons le discriminant fondamental $-D = -404$. L'anneau $\mathbf{O_K}$ des entiers de $\mathbf{K} = \mathbf{Q}(\sqrt{-404})$ est $\mathbf{Z}[\rho/2]$ avec $\rho = \sqrt{-404}$.
L'idéal $3 \in \mathbf{Z}$ est décomposé dans $\mathbf{O}$. Plus précisément $3 = \mathfrak{p}\overline{\mathfrak{p}}$ où $\mathfrak{p}$ désigne l'idéal premier engendré par 3 et $1 + \rho$.
Le groupe des classes $\mathrm{Cl}(-404)$ est de cardinal 14 et il est engendré par la classe de $\mathfrak{p}$.
C'est ce que nous apprend la séquence d'instructions suivante :

```
K=bnfinit(x^2+404);
K.no
%2 =14
K.zk
%3=[1, 1/2*x]
idealprimedec(K,3)
%4=[[3,[2,2]~,1,1,[1,-1]~,[3,[4,2]~,1,1,[-1,-1]~]]
p=idealprimedec(K,3)[1];
idealhnf(K,p)
%6=
[3 1]
```

```
[0 1]
```

On calcule maintenant une base des idéaux $\mathfrak{p}^k$ pour $0 \leq k \leq 13$.

```
for (k=0,K.no-1,print(idealhnf(K,idealpow(K,p,k))))
[1, 0; 0, 1]
[3, 1; 0, 1]
[9, 4; 0, 1]
[27, 13; 0, 1]
[81, 40; 0, 1]
[243, 40; 0, 1]
[729, 283; 0, 1]
[2187, 1741; 0, 1]
[6561, 1741; 0, 1]
[19683, 1741; 0, 1]
[59049, 21424; 0, 1]
[177147, 21424; 0, 1]
[531441, 375718; 0, 1]
[1594323, 1438600; 0, 1]
```

On a donc $\mathfrak{p}^k = (a_k, b_k + \rho)$ où $k = 0, 1, 2, \ldots, 13$, on note $\tau_k = \frac{b_k+\rho}{a_k}$ le quotient de base de $\mathfrak{p}^k$ et on calcule $j_k = j(\tau_k)$

```
Ideaux=vector(K.no,k,0);

for(k=0,K.no-1,Ideaux[1+k]=idealhnf(K,idealpow(K,p,k)))

\p 1000

rac=polroots(x^2+404)[1];
z= subst(K.zk[2],x,rac);

mestau=vector(14,k,0);

{for(k=1,K.no,matr=Ideaux[k];
resu=(matr[1,2]+z*matr[2,2])/(matr[1,1]+z*matr[2,1]);
if(imag(resu)<0,resu=1/resu,);mestau[k]=resu;)}

mesj=vector(K.no,k,ellj(mestau[k]));
```

On calcule

$$H_{-404}(X) = \Pi_{1\leq k\leq 14}(X - j_k)$$

à l'aide des instructions suivantes

```
H=prod(k=1,K.no,X-mesj[k]);
Hr=round(real(H))

%12=X^14 - 26523162922592872254376679 68*X^13 -
13659966873012807294779259158094190148403 2*X^12 -
18914753547800938220605525785297549126598228285849 6*X^11 -
26181691797967322135414182137360796150916199553840777999155 2*X^10 -
11938851150588269566222488021842096539844729124873940665420165939 2*X^9 -
19970076081487858762907119018999559036025406760107290495924627270795264*X^8 +
70524492551600286857708450126047595357088538427268967051429368624924170649 6*X^7 -
33872799529198964844915900102578375435327831844475016592225474796536885894184960*X^6
28964740677799848606869471095560110578849599906939259716546639301246667627522162688*X
22566820068513462879102848318500041903056887054402436772792424652098200 98
759090340102144*X^4 -20029857140725594241374103253519991803846628029288114898 83
63030841251201350298522427064320*X^3 +47260057763554643848267927603680487900953
99865685681356244989969038745364404937703103177687 04*X^2 +13093856356049558753
67012999470271658586864508328051014508458343390877415208257790347777711311104*X
-15943210057537075528292972435295450404008134844001700638256476034219735166547 2
136478486380891078656
```

Pour continuer cet exemple, on a besoin d'un entier premier complètement décomposé dans le corps de classes de Hilbert $\mathbf{H}$ de $\mathbf{K}$. Un nombre premier p est décomposé dans $\mathbf{K} = \mathbf{Q}(\sqrt{-404})$ si et seulement si -404 est résidu quadratique modulo p. Un idéal premier de $\mathbf{O_K}$ est complètement décomposé dans $\mathbf{H}$ si cet idéal est principal.

Voici quelques nombres premiers complètement décomposés dans $\mathbf{H}$:

```
{forprime(N=1000,2000,dec=idealprimedec(K,N);
if(length(dec)==2,
if(bnfisprincipal(K,dec[1])[1]==0,print(N))))}
1009
1493
1693
1697
1933
```

On choisit $N = 1009$.

Maintenant, on recherche, grâce à l'algorithme de Cornacchia [[28],théorème 4.1], un vecteur minimal φ dans un idéal premier $\mathfrak{P}$ au-dessus de N. Ce vecteur minimal est de norme N si et seulement si $\mathfrak{P}$ est principal.

On peut aussi commencer par examiner si $-D = -404$ est un carré modulo N et calculer les racines carrées le cas échéant :

```
N=1009;
if (issquare(Mod(-404,N)),z=lift(polrootsmod(X^2+404,N)[1]);print(z))
343
```

L'idéal $\mathfrak{P} = (1009, 343 - \sqrt{-404})$ apparaît dans la décomposition de 1009 en idéaux premiers dans $\mathbf{O_K}$. C'est un idéal principal, l'instruction suivante nous le confirme.

```
bnfisprincipal(K,idealadd(K,N,343-x))
%16=[[0]~, [10, -3]~]
```

Pour trouver un générateur de $\mathfrak{P}$ on a recours à un algorithme de réduction de réseaux pour déterminer un plus court vecteur φ. Si ce vecteur minimal est de norme N, on sait que $\mathfrak{P} = (\varphi)$.

Recentrons-nous sur notre objectif : la construction d'une courbe elliptique sur $\mathbf{F}_{1009}$ à multiplication complexe par $\mathbf{O_K}$.

L'approche standard consiste à factoriser $H_{-404}(X)$ modulo $N = 1009$. La commande **polrootsmod** nous donne les racines du polynôme de classes modulo 1009.

```
Jinv=polrootsmod(Hr,N)
%17=[Mod(205, 1009), Mod(393, 1009), Mod(394, 1009), Mod(397, 1009),
 Mod(456, 1009), Mod(490, 1009), Mod(502, 1009), Mod(540, 1009),
 Mod(586, 1009), Mod(613, 1009), Mod(700, 1009), Mod(741, 1009),
 Mod(778, 1009), Mod(996, 1009)]~
```

Il s'agit des j-invariants de courbes elliptiques sur $\mathbf{F}_{1009}$ à multiplication complexe par $\mathbf{O_K}$.

Deuxième méthode : la méthode galoisienne

Maintenant nous allons calculer une des racines j mod N de $H_{-404}(X)$ précédentes par la méthode galoisienne, proposée par Enge, Hanrot et Morain dans [12] et [16]. Ces derniers

proposent d'utiliser les sous-corps du corps de classes de Hilbert $\mathbf{H}$ de $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$. Le groupe de Galois de cette extension est $\mathrm{Gal}(\mathbf{H}/\mathbf{K}) \cong \mathrm{Cl}(-D)$. Supposons que ce groupe ait une cardinalité friable. On peut décomposer l'extension $\mathbf{H}/\mathbf{K}$ en tours d'extensions de petits degrés $d_1, d_2, \ldots, d_I$ tels que $\Pi d_i = h_{-D}$. Le calcul de $j \mod N$ se ramène alors à une séquence de I factorisations de polynômes de degrés d_i.

Dans le cas général, le groupe de classes $\mathrm{Cl}(-D)$ est commutatif et fini. Donc tous ses sous-groupes sont distingués et on peut l'écrire comme produit direct de sous-groupes cycliques.

Comme nous l'avons vu à la première partie de cet exemple (première méthode), le groupe $\mathrm{Cl}(-404)$, qui nous intéresse, est cyclique engendré par la classe de $\mathfrak{p} = (3, 1+\rho)$. Soit γ l'élément du groupe de Galois $\mathrm{Gal}(\mathbf{H}_{-404}/\mathbf{K}) \cong \mathrm{Cl}(-D)$ associé à la classe de $\mathfrak{p}$. On considère les deux sous-groupes maximaux $C_2 =< \gamma^7 >$ et $C_7 =< \gamma^2 >$ de $\mathrm{Cl}(-D)$. Le groupe $\mathrm{Gal}(\mathbf{H}_{-404}/\mathbf{K})$ est égal au produit direct $C_2 C_7$.

Le corps $\mathbf{H}_{-404}$ est une extension galoisiènne de $\mathbf{Q}$ de groupe de Galois égal au groupe diédral $\mathrm{Gal}(\mathbf{H}_{-404}/\mathbf{K}) \rtimes C = (C_2 C_7) \rtimes C$, où $C =< \sigma >$ est le groupe de Galois de $\mathbf{K}/\mathbf{Q}$ et σ la conjugaison complexe. Le groupe C normalise les sous-groupes C_2 et C_7 de $\mathrm{Gal}(\mathbf{H}_{-404}/\mathbf{K})$. Donc le sous-groupe $< C_i, C >$ est égal au produit semi-direct $C_i \rtimes C$, pour $i = 2, 7$. Nous avons vu à la section précédente que le groupe $\mathrm{Gal}(\mathbf{H}_{404}/\mathbf{Q})$ agit sur les j-invariants. Le stabilisateur $\mathrm{Stab}(j_0)$, de j_0, est isomorphe à C. Nous allons abusivement confondre ces deux groupes pour alléger les notations : $\mathrm{Stab}(j_0) = C$. On note $\mathbf{Q}(j_0)$ le corps fixé par $\mathrm{Stab}(j_0)$ et $\mathbf{H}_{-404}^{C_i \rtimes C}$ le corps fixé par $C_i \rtimes C$.

La somme $s = j_0 + j_2 + j_4 + j_6 + j_8 + j_{10} + j_{12} = j_0 + \gamma^2(j_0) + \cdots + \gamma^{12}(j_0)$ est dans $\mathbf{H}_{-404}^{C_7 \rtimes C}$ et $\gamma(s)$ aussi. On calcule le polynôme minimal de s

$$A(X) = (X - s)(X - \gamma(s)) = X^2 - (s + \gamma(s))X + s\gamma(s) \in \mathbf{Z}[X]$$

à l'aide des instructions

```
Jinv=polrootsmod(Hr,N)
[Mod(205, 1009), Mod(393, 1009), Mod(394, 1009), Mod(397, 1009), Mod(456, 1009),
Mod(490, 1009), Mod(502, 1009),Mod(540, 1009), Mod(586, 1009), Mod(613, 1009),
Mod(700, 1009), Mod(741, 1009), Mod(778, 1009), Mod(996, 1009)]~
s0=sum(X=0,6,mesj[2*X+1]);
s1=sum(X=1,7,mesj[2*X]);
A=round((X-s0)*(X-s1))
%20=X^2 - 265231629225928722543766796 8*X
 - 136599667524090789976555995770706082361344
```

Le corps $\mathbf{H}_{-404}^{C_7 \rtimes C} = \mathbf{Q}(s)$ est une extension de $\mathbf{Q}$ de degré 2.

La somme $t = j_0 + j_7 = j_0 + \gamma^7(t)$ est dans $\mathbf{H}_{-404}^{C_2 \rtimes C}$, de même que $\gamma(t), \gamma^2(t), \ldots, \gamma^6(t)$.

On calcule le polynôme minimal de t

$$B(X) = (X - t)(X - \gamma(t))(X - \gamma^2(t)) \ldots (X - \gamma^6(t)) \in \mathbf{Z}[X]$$

à l'aide des instructions

```
mest=vector(7,k,mesj[k]+mesj[k+7]);
B=round(prod(k=1,7,(X-mest[k])))
%22=X^7 - 265231629225928722543766796 8*X^6
 -367262306763485522191287580838597427 2*X^5
 - 508403597616245335775642835254277838233980108 8*X^4
 - 251499550115331285629044666462320246286785957173657 6*X^3
 - 478494704301611127223475246681354532196844840012564398080*X^2
 - 162116502962524168048996084888545378341999300308002033945804 8*X
 - 291129875966157849392517545280722393238466615769441321965752156 16.
```

Le corps $\mathbf{H}_{-404}^{C_2 \rtimes C} = \mathbf{Q}(t)$ est une extension de $\mathbf{Q}$ de degré 7.
Notons que $(1, s)$ est une base de $\mathbf{Q}(s)$ sur $\mathbf{Q}$ et $(1, t, t^2, \ldots, t^6)$ une base de $\mathbf{Q}(t)$ sur $\mathbf{Q}$. Donc $(1, t, t^2, st, \ldots, st^6)$ est une base de $\mathbf{Q}(s, t) = \mathbf{Q}(j_0)$ sur $\mathbf{Q}$. On cherche les coordonnées de j_0 dans cette base. Il s'agit des rationnels $(m_{\alpha,\beta})_{0 \le \alpha \le 1, 0 \le \beta \le 6}$ tels que

$$j_0 = \sum_{0 \le \alpha \le 1} \sum_{0 \le \beta \le 6} m_{\alpha,\beta} s^\alpha t^\beta.$$

En faisant agir le groupe $< \gamma >$ sur cette équation, on obtient 14 équations qui suffisent à calculer tous les coefficients $m_{\alpha,\beta}$. En fait, il est préférable de faire agir préalablement l'un de ses sous groupes C_i et de compléter ensuite par l'action du générateur γ. On se ramène ainsi à des systèmes de plus petite taille. Faisons par exemple agir C_2. On obtient deux équations :

$$j_0 = \sum_{0 \le \alpha \le 1} s^\alpha \sum_{0 \le \beta \le 6} m_{\alpha,\beta} t^\beta$$

et

$$\gamma^7(j_0) = j_7 = \sum_{0 \le \alpha \le 1} \sigma^7(s^\alpha) \sum_{0 \le \beta \le 6} m_{\alpha,\beta} t^\beta$$

D'où le système

$$\begin{pmatrix} 1 & s \\ 1 & \gamma^7(s) \end{pmatrix} \begin{pmatrix} \sum_{0 \le \beta \le 6} m_{0,\beta} t^\beta \\ \sum_{0 \le \beta \le 6} m_{1,\beta} t^\beta \end{pmatrix} = \begin{pmatrix} j_0 \\ j_7 \end{pmatrix}$$

qui permet de calculer $\sum_{0\leq\beta\leq 6} m_{0,\beta}t^\beta$ et $\sum_{0\leq\beta\leq 6} m_{1,\beta}t^\beta$.

On fait agir γ sur les expressions donnant $\sum_{0\leq\beta\leq 6} m_{0,\beta}t^\beta$ et $\sum_{0\leq\beta\leq 6} m_{1,\beta}t^\beta$. Deux systèmes 7×7 permettent alors de trouver les $m_{0,\beta}$ puis les $m_{1,\beta}$.

Au total on résout 7 systèmes 2×2 puis 2 systèmes 7×7.

On en déduit des approximations numériques des $m_{\alpha,\beta}$ puis leurs valeurs exactes.

```
V3=vector(4,k,[1,s0;1,s1]^(-1)*[mesj[2*k-1],mesj[2*k+6]]~);
V4=vector(3,k,[1,s1;1,s0]^(-1)*[mesj[2*k],mesj[2*k+7]]~);
V0=matrix(7,2,k);
for(k=1,4,V0[2*k-1,1]=V3[k][1];V0[2*k-1,2]=V3[k][2]);
for(k=1,3,V0[2*k,1]=V4[k][1];V0[2*k,2]=V4[k][2])

M0=matrix(7,7,k);
for(j=1,7,for(k=1,7,M0[j,k]=mest[j]^(k-1)));

M=M0^(-1)*V0;

ratio(r,v)=if(1, v=algdep(r,1);-polcoeff(v,0)/polcoeff(v,1),);
M=real(M);

for(b=1,7,M[b,1]=ratio(M[b,1]));
for(b=1,7,M[b,2]=ratio(M[b,2]));
```

Revenons à notre entier premier $N = 1009$.
On factorise $A(X)$ modulo N. On trouve deux racines 796 et 941 modulo N.
On choisit $s = 796$
On factorise ensuite $B(X)$ modulo N. On trouve sept racines $88, 234, 355, 477$, $818, 850$, et 933 modulo N. On choisit $t = 88 \bmod N$.
On calcule alors

$$j = \sum_{0\leq\alpha\leq 1}\sum_{0\leq\beta\leq 6} m_{\alpha,\beta}s^\alpha t^\beta = 397 \bmod N$$

à l'aide de la séquence de commandes

```
N=1009
s=polrootsmod(real(A),N)[1];
t=polrootsmod(real(B),N)[1];
j=sum(k=0,6,t^k*(M[k+1,1]+s*M[k+1,2]))
%42=Mod(397,1009)
```

Donc en combinant judicieusement les racines du polynôme de classes $H_{-404}(X)$, on remplace la factorisation d'un polynome de degré 14 par la factorisation d'un polynôme de degré 2 et celle d'un polynôme de degré 7.

La variété algébrique $C \subset \mathbb{P}^2(\overline{\mathbf{F}_{1009}})$ d'équation affine

$$y^2 = 4x^3 - 27\frac{397}{397-1728}x - 27\frac{397}{397-1728}$$

est une courbe elliptique sur $\mathbf{F}_{1009}$ à multiplication complexe par $\mathbf{O_K}$.

Chapitre 3

Le test de primalité ECPP

Le test de primalité ECPP (Elliptic Curves Primality Proving) a été proposé par A.O.L Atkin en 1988. Voir [3], [25] et [29]. C'est l'un des tests de primalité les plus puissants utilisés en pratique. On prouve qu'un entier $N = N_0$ est premier en construisant une suite de nombres $N_1, N_2, \ldots, N_k$ tels que la primalité de N_i implique celle de N_{i-1}. La suite (N_i) décroit, elle est de taille $k = O(\log N)$ et $N_k = O(1)$.

Dans ce chapitre, nous présentons l'algorithme ECPP et ses principales variantes. Nous illustrons à cette occasion quelques unes des propriétés algorithmiques des courbes elliptiques qui nous seront utiles dans la suite de notre travail.

3.1 Le test ECPP

3.1.1 Le critère

Nous allons énoncer la proposition sur laquelle repose l'algorithme :

Proposition 3.1.1. *Soient N un entier naturel et E une courbe elliptique modulo N. On suppose qu'il existe un point $P \in E(\mathbf{Z}/N\mathbf{Z})$ et un entier $s > 0$ pour lequel*

$$sP = 0, \text{ dans } E(\mathbf{Z}/N\mathbf{Z}); \tag{3.1}$$

$$\frac{s}{q}P \neq 0 \text{ dans } E(\mathbf{Z}/p\mathbf{Z}), \tag{3.2}$$

pour tout nombres premiers p, q divisant respectivement N, s. Alors tout nombre premier p divisant N vérifie $\#E(\mathbf{Z}/p\mathbf{Z}) \equiv 0 \bmod s$. En particulier, si $s > (\sqrt[4]{N} + 1)^2$, alors N est premier.

Démonstration. En effet, les conditions du théorème impliquent que pour tout diviseur premier p de N, l'ordre de $P \in E(\mathbf{Z}/p\mathbf{Z})$ est égal à s. Donc $\#E(\mathbf{Z}/p\mathbf{Z}) \equiv 0 \bmod s$. D'après le théorème 2.2.2 (borne de Hasse) le cardinal de $E(\mathbf{Z}/p\mathbf{Z})$ vérifie

$$\#E(\mathbf{Z}/p\mathbf{Z}) \leq (\sqrt{p}+1)^2.$$

Puisque $s > (\sqrt[4]{N}+1)^2$, on a

$$(\sqrt{p}+1)^2 \geq \#E(\mathbf{Z}/p\mathbf{Z}) \geq s > (\sqrt[4]{N}+1)^2.$$

Par conséquent tout diviseur p de N vérifie $p > \sqrt{N}$. Cela est contraire au fait que tout entier composé n admet un diviseur premier $p \leq \sqrt{n}$. Donc N est un nombre premier. □

3.1.2 L'algorithme

Les étapes de l'algorithme sont les suivantes :

Algorithme 3.1.2. *Soit N un entier naturel dont on veut tester la primalité.*

[Etape 1.] *Répéter l'instruction suivante : Trouver un corps quadratique imaginaire $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$ de discriminant $-D, D > 0$, tel que N est la norme d'un entier φ dans $\mathbf{K}$. Si on trouve un bon discriminant $-D$, on note $\mathcal{S} = \{\zeta\varphi\}$ où ζ parcourt l'ensemble des racines de l'unité de $\mathbf{K}$.*
[Etape 2.] *Pour tout $\varphi \in \mathcal{S}$, calculer $m = N + 1 - \mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\varphi)$. Si un de ces nombres se décompose en $m = cN'$ où $c > 1$ est un entier B-friable et N' un nombre probablement premier tel que $N' > (\sqrt[4]{N}+1)^2$, aller à l'étape 3. Sinon revenir à l'étape 1.*

[Etape 3.] *Construire une courbe elliptique E sur $\overline{\mathbf{Q}}$ à multiplication complexe par l'anneau des entiers de $\mathbf{K}$.*

[Etape 4.] *On suppose que N est premier. D'après la condition imposée à l'étape 1, l'entier N est complètement décomposé dans $\mathbf{K}_H$. Réduire E modulo un idéal premier au-dessus de N dans $\mathbf{K}_H$, pour obtenir une courbe $\overline{E}$ modulo N.*

[Etape 5.] *Trouver un point $P = (x_P : y_P : 1)$ sur $\overline{E}$ tel que $[N']P = O_{\overline{E}}$. La proposition 3.1.1 implique alors que N est premier pour peu que N' le soit.*

[Etape 6.] *Poser $N = N'$ et aller à l'étape 1.*

3.1.3 Commentaires

Nous allons, pour achevez notre présentation de l'algorithme ECPP, faire une brève analyse de chacune de ses étapes.

Étape 1 : Si N est un nombre premier, il s'agit dans cette étape de trouver, pour $-D$ parcourant l'ensemble des discriminants fondamentaux, un corps quadratique imaginaire

$\mathbf{K} = \mathbf{Q}(\sqrt{-D})$ tel que que N est complètement décomposé dans le corps de classes se Hilbert $\mathbf{H}_{-D}$ de $\mathbf{K}$. La probabilité qu'une telle situation se présente est égale à $1/2h$, où h est le nombre de classes de $\mathbf{K}$. C'est pourquoi en pratique, on considère d'abord les corps quadratiques imaginaires $\mathbf{K}$ dont le nombre de classes est $h_{\mathbf{K}} = 1$, puis ceux avec $h_{\mathbf{K}} = 2$ et ainsi de suite. On commence par vérifier que N se décompose dans $\mathbf{K}$. Si N est premier, il se décompose dans $\mathbf{K}$ si et seulement si le discriminant $-D$ de $\mathbf{K}$ est un carré non nul modulo N.

Si N est décomposé dans $\mathbf{K}$, on vérifie que c'est le produit de deux idéaux premiers principaux. Pour le faire, on extrait une racine carrée modulo N de $-D$ notée z. L'idéal $\mathfrak{p} = (N, z - \sqrt{-D})$ divise (N) dans $O_{\mathbf{K}}$. On utilise un algorithme de réduction de réseau (par exemple la réduction de Gauss ou l'algorithme "LLL") pour déterminer un vecteur minimal φ de $\mathfrak{p}$. L'idéal $\mathfrak{p}$ est principal si et seulement si $N_{\mathbf{K}/\mathbf{Q}}(\varphi) = N$. Si la norme du vecteur minimal n'est pas égale à N, l'idéal $\mathfrak{p}$ n'est pas principal et il n'existe aucun élément $\varphi \in O_{\mathbf{K}}$ de norme $N(\varphi) = N$. Dans ce cas, on ne peut pas utiliser de courbes elliptiques à multiplication complexe par $O_{\mathbf{K}}$, il faut repartir au début de l'étape 1. On peut directement utiliser l'algorithme de Cornacchia [[28] théorème 4.1 ou [8], page 34] pour déterminer un éventuel générateur d'un idéal au-dessus d'un nombre premier p tel que le discriminant $-D$ est un carré modulo p.

Étape 2 : Dès qu'on a trouvé un discriminant $-D$ et un élément $\varphi \in \mathbf{K}$ entier sur $\mathbf{Z}$, on peut calculer d'autres éléments $\zeta\varphi \in \mathbf{K}$ de norme N et construire l'ensemble
$\mathcal{S} = \{\zeta\varphi : \zeta \in \mathbf{O_K} \text{ est une racine de l'unité }\}$.

Pour chaque $\varphi \in \mathcal{S}$, on calcule $m = N + 1 - \mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\varphi)$ et on vérifie que

$$m = cN'. \tag{3.3}$$

Le nombre $c > 1$ est un produit de nombres premiers inférieurs à un certain entier B et N' un entier tel que $N' > (\sqrt[4]{N}+1)^2$ et probablement premier, en ce sens qu'il a passé un test de primalité probabiliste (Miller-Rabin par exemple). Si ce n'est pas le cas on revient à l'étape 1.

Les étapes 3 et 4 ont été complètement détaillées dans le chapitre 2. Nous rappellons ici l'essentiel de ces étapes.

Étape 3 : Ici il faut construire une courbe elliptique $E/\overline{\mathbf{Q}}$. Toute courbe elliptique sur $\mathbf{C}$ à multiplication complexe par un ordre quadratique convient. Soit $O_{\mathbf{K}}$ l'anneau des entiers d'un corps quadratique $\mathbf{K}$, tout idéal $\mathfrak{i}$ de $O_{\mathbf{K}}$ est un réseau de $\mathbf{C}$ (de même que l'anneau $O_{\mathbf{K}}$ lui-même). Donc les tores $\mathbf{C}/\mathfrak{i}$ ou $\mathbf{C}/O_{\mathbf{K}}$ suffisent. La donnée de $j(\mathbf{C}/\mathfrak{i})$ détermine la courbe $\mathbf{C}/\mathfrak{i}$. Pour calculer les $j(\mathbf{C}/\mathfrak{i})$, il suffit d'une base (ω_1, ω_2) du réseau $\mathfrak{i}$ positivement orientée. On pose $\tau = \omega_2/\omega_1$ et $q = exp(2i\pi\tau)$, puis on injecte q dans le développement de Fourier de j (avec le logiciel PARI/GP, on fait le calcul grâce à la commande **ellj**).

Étape 4 : On veut réduire E modulo un idéal de $\mathbf{H}_{-D}$ au-dessus de N. La solution standard consiste à réduire le polynôme de classes $H_D(X)$ modulo N. On construit $\overline{E}$ modulo N à partir d'une racine j mod N de $H_D(X)$ modulo N. Cependant le polynôme de classes est difficile à calculer à cause de la taille de ses coefficients. Enge, Morain et Hanrot ont proposé une solution alternative. Il s'agit de décomposer l'extension $\mathbf{H}_{-D}/\mathbf{K}$ en une tour d'extensions de petits degrés.

Étape 5 : Trouver un point $Q \in \overline{E}(\mathbf{Z}/N\mathbf{Z})$ peut se faire par un algorithme qui cherche les x tels que $x^3 + ax + b$ est un carré modulo N. Le cas échéant, on extrait une racine carrée y de x modulo N en utilisant par exemple l'algorithme de Tonelli-Shanks [[8], page 32]. Une fois qu'un point $Q(x, y) \in \overline{E}(\mathbf{Z}/N\mathbf{Z})$ est choisi, on calcule $P = [c]Q = \underbrace{Q \oplus Q \oplus \cdots \oplus Q}_{c-fois}$. Ce calcul peut se faire rapidement en adaptant la méthode de l'exponentiation rapide (on se sert de la décomposition de c en base 2). Alors le calcul de $P = [c]Q$ a une complexité de l'ordre de $\log c$ additions pour la loi $\oplus$, quand la méthode naïve (faire les sommes successives $P \oplus P \oplus \cdots \oplus P$) nécessite c additions.

On s'assure que le point $P \in \overline{E}(\mathbf{Z}/N\mathbf{Z})$ est de la forme $(x_P : y_P : 1)$ et qu'il vérifie $[N']P = O_{\overline{E}}$. Dans le cas où N' est premier, le point P est alors d'ordre N' dans $\overline{E}(\mathbf{Z}/p\mathbf{Z})$ pour tout p divisant N. Et puisque nous nous sommes assurés à l'étape 2 que N' vérifie $N' > (\sqrt[4]{N} + 1)^2$, la proposition 3.1.1 nous permet de conclure que N est premier si N' est premier.

3.1.4 Théorie de la complexité

Dans cette section nous donnons quelques éléments de la théorie de la complexité tirés de [15], dans le but de classer le test de primalité ECPP.

Le but de la théorie de la complexité est de définir des modèles formels des processeurs et des algorithmes que nous utilisons sur nos ordinateurs et de fournir une classification des algorithmes selon le *temps de calcul* et la *quantité (l'espace) de mémoire* nécessaires.

Tous les calculs effectués par un ordinateur peuvent être simulés par un automate qui a une très simple structure mathématique : une *machine de Turing*. Une machine de Turing est définie par un ensemble fini d'états : un état initial, un ensemble fini de symboles et une *fonction de transition*. Une machine de Turing procède étape par étape en suivant les règles imposées par la fonction de transition et peut écrire des symboles sur une *bande mémoire*. Il est alors facile de définir le temps de calcul d'un algorithme comme le nombre d'étapes entre le début et la fin du calcul et la quantité de mémoire comme la longueur de la bande mémoire nécessaire. Nous allons utiliser le modèle de calcul appelé *Random access machine*. Dans ce modèle la détermination du temps de calcul d'un algorithme revient à compter le nombre d'opérations élémentaires en langage machine nécessaires à son exécution.

Un *problème de décision* $X \subset I$ est un sous-ensemble d'un ensemble de cas possibles I.

Par exemple l'ensemble $X = \{x \in \mathbb{N} : x \text{ est un nombre premier } \} \subset I = \mathbb{N}$. Par ailleurs une machine de Turing associé au problème de décision "l'entier $n \in \mathbb{N}$ est-il premier ?" est une "boîte" qui prend en entrées les entiers naturels n et renvoie les réponses "oui" ou "non" adaptées.

La *classe de complexité* $\mathcal{P}$ (*"temps polynômial"*) est la classe des X pour lesquels il existe une machine de Turing qui accepte (si $x \in X$) et rejette (si $x \notin X$) correctement tout x en un nombre d'étapes qui est polynômial en la taille des entrées $\lambda(x)$ (par exemple $\lambda(x) = 1 + \lfloor \log_2 x \rfloor$ pour la représentation binaire d'un entier $x \in \mathbb{N}$). Une machine associée à la classe $\mathcal{P}$ est dite *machine de Turing polynômiale*. Par exemple le problème "l'entier $a \in \mathbb{N}$ est-il le produit des entiers b et c" est dans la classe polynômiale $\mathcal{P}$.

La *classe de complexité aléatoire* $\mathcal{BPP}$ ("bounded-error probabilistic polynômial time") est la classe des problèmes de décision X pour lesquelles il existe une machine de Turing polynômiale qui accepte les $x \in X$ avec une probabilité au moins égale à $2/3$ et rejette les $x \notin X$ de même avec une probabilité au moins égale à $2/3$. Une telle machine est appelée *machine de Turing two-side Monte Carlo*. On remarquera que $X \in \mathcal{BPP}$ si et seulement son complémentaire $I \setminus X \in \mathcal{BPP}$.

La *classe de complexité* $\mathcal{RP}$ ("random polynômial time") est la classe des problèmes de décision X pour lesquelles il existe une machine de Turing polynômiale qui accepte les $x \in X$ avec une probabilité au moins égale à $1/2$ et rejette à chaque fois les $x \notin X$. Une telle machine est appelée *machine de Turing one-side Monte Carlo*. Une utilisation standard consiste à rentrer k-fois la même entrée et à accepter si et seulement si la machine accepte. Par ailleurs, on définit la classe de complexité co-$\mathcal{RP}$ comme étant celle des X dont les complémentaires $I \setminus X \in \mathcal{RP}$. Par exemple, le test de primalité Miller-Rabin fait du problème "l'entier N est-il premier ?" un problème de la classe co-$\mathcal{RP}$. Donc le problème "l'entier N est-il composé ?" est de la classe de complexité One-side Monte Carlo en utilisant le test de Miller-Rabin.

La *classe de complexité* $\mathcal{ZPP} = \mathcal{RP} \cap$ co-$\mathcal{RP}$ ("zero-error probabilistic polynomial time") est la classe des problèmes de décision X pour lesquelles il existe une machine de Turing polynômiale probabiliste qui donne toujours la bonne réponse. Une telle machine est appelée *machine de Turing de Las Vegas*.

L'algorithme ECPP, et surtout sa variante dûe à Huang et Adleman, fait de la preuve de primalité un problème de la classe de complexité Las Vegas. C'est un test de primalité très efficace en pratique, mais son temps de calcul n'est pas rigoureusement établi. On ne dispose que d'une analyse heuristique en $\widetilde{O}((\log n)^{5+\mu})$, ou $\widetilde{O}((\log n)^5)$ asymptotiquement [25]. Si un entier N est donné en entrée, ECPP donne à la sortie l'une de ces trois réponses : "*N est premier*", "*N est composé*", "*je ne sais pas*". Nous rappellons que le test ECPP est envisagé généralement après avoir effectué un test de primalité probabiliste Monte Carlo. On se doute donc que l'entier à tester est premier parce qu'il a passé plusieurs fois le test de Miller-Rabin par exemple. Mais on veut en être sûr, et avoir une preuve. Il est donc question de confirmer qu'un entier probablement premier l'est réellement. Les réponses "*N est premier*" et "*N est composé*" renvoyées à la sortie d'une machine de Turing ECPP sont

correctes avec une preuve vérifiable en temps polynômiale. La difficulté consiste à montrer que la troisième éventualité arrive avec une probabilité bornée.

En pratique, les programmes implémentant ECPP ou fastECPP (nous définirons cette variante du test ECPP dans la suite) suivent cette philosophie et donnent toujours des réponses correctes. La réponse "*je ne sais pas*" est renvoyée à la sortie de l'algorithme lorsque la procédure imposée par l'algorithme ECPP (resp. fastECPP) pour tester un entier N est complexe et nécessite beaucoup trop de temps (en l'occurence le calcul des racines carrées modulo N de discriminants $-D$ tels que N est la norme d'un entier de $\mathbf{Q}(\sqrt{-D})$ ou bien le calcul des polynômes de classes et ou des racines de ces polynômes). Les programmeurs peuvent remédier à ces défauts, puis relancer le test. On n'a pas de rapport sur des nombres entiers probablement premiers ayant indéfiniment résisté au test (fast)ECPP mais on n'a pas non plus, à l'heure où ces notes sont écrites, la preuve qu'il n'en existe pas.

3.1.5 Un exemple

Nous allons montrer que l'entier $N = 392593$ est un nombre premier.

Nous précisons que dans l'algorithme ECPP, les calculs préliminaires se font comme si N était premier.

Nous cherchons les discriminants fondamentaux $-D$ qui sont résidus quadratiques modulo N. On commence par les 9 corps quadratiques dont l'anneau des entiers est principal. Voyons ce qui se passe pour $\mathbf{K} = \mathbf{Q}(\sqrt{-1}) = \mathbf{Q}(i)$.

```
N=392593;
D=-nfdisc(X^2+1)
%2=4
if(issquare(Mod(-D,N)),z=lift(polrootsmod(X^2+D,N)[1]));
print(z)
181814
```

Donc le discriminant $-D = -4$ (de $\mathbf{Q}(i)$) est un résidu quadratique modulo N et on a $-D = 181814^2 \bmod N$.

Rappelons qu'en théorie de la multiplication complexe (cette théorie est utilisée tout au long de l'algorithme), on dit qu'une courbe elliptique sur $\mathbf{C}$ est à multiplication complexe par O (ou CM par O) lorsque son anneau d'endomorphisme $\mathrm{End}(E) = O$ est un ordre quadratique imaginaire. Et le nombre de courbes elliptiques sur $\mathbf{C}$, à isomorphisme près, CM par l'anneau des entiers d'un corps quadratique est égal au nombre de classes du corps quadratique.

Puisque le groupe de classes de $\mathbf{K} = \mathbf{Q}(i)$ est trivial, toute courbe elliptique définie sur le corps des nombres complexes $\mathbf{C}$ et CM par l'anneau $\mathbf{O_K}$ des entiers de Gauss est isomorphe à la courbe elliptique $E/\mathbf{C}$ d'équation affine

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

L'invariant modulaire de cette classe de courbes est $j(E) = 1728$.

Si $N = 392593$ est premier, il est complètement décomposé dans le corps de classes de Hilbert de $\mathbf{K}$, car nous avons choisi $\mathbf{K}$ tel que son discriminant $-D = -4$ est un carré modulo N. La courbe $E/\mathbf{C}$ se réduit en une courbe $\overline{E}/\mathbf{F}_N$, CM par $\mathbf{O_K}$, d'équation

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

Tout idéal de $\mathbf{O_K}$ est principal. Grâce à l'algorithme de Cornacchia [[28],théorème 4.1 ou [8], page 34] on détermine un vecteur minimal φ générateur d'un idéal premier $\mathfrak{P} = (N, \frac{181814+\sqrt{-D}}{2}) \in \mathrm{Spec}\mathbf{O_K}$, au-dessus de N.

```
z=181814;

x=2*N;y=181814;u=x%y;n=2*sqrt(N);

while(u >n,x=y;y=u;u=x%y);

print(u)
976

v=sqrt((u^2-4*N)/(-D))
393.00000000000000000000000000
```

Le vecteur $\varphi = \frac{976+393\times 2\times i}{2} \in \mathbf{O_K}$ engendre $\mathfrak{P}$ (ou son conjugué $\overline{\mathfrak{P}}$) [[28],théorème 4.1] et sa norme $\varphi\ \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\varphi)$ est égale à 392593.

Si on note ϕ l'endomorphisme de Frobenius de $\overline{E}$, la norme de ϕ est $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\phi) = N$ et $\#\overline{E}(\mathbf{F}_N) = N + 1 - \mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\phi)$.

Puisque le générateur de $\mathfrak{P}$ et ϕ ont la même norme, il existe une racine de l'unité $\zeta \in \mathbf{O_K}$ telle que $\phi = \zeta\frac{976+393\times 2\times i}{2}$. Le groupe des racines de l'unité contenues dans $\mathbf{O_K}$ est $\mu_4 = \{1, -1, i, -i\}$, donc on a

- soit $\phi = \frac{976+393\times 2\times i}{2}$;
- soit $\phi = -\frac{976+393\times 2\times i}{2}$;
- soit $\phi = \frac{-393\times 2+976\times i}{2}$;
- soit $\phi = \frac{393\times 2-976\times i}{2}$.

Le point $P = (603 : 58669 : 1)$ appartient à $\overline{E}(\mathbf{Z}/N\mathbf{Z})$ et $\#\overline{E}(\mathbf{Z}/N\mathbf{Z}) = N + 1 - 2 \times 393 = 391808$ (donc $\phi = \frac{393 \times 2 - 976 \times i}{2}$). Les instructions suivantes le confirment.

```
 E=ellinit([0,0,0,Mod(-1,392593),0]);

issquare(Mod(603^3-603,392593))
1

z=polrootsmod(y^2-(603^3-603),392593)[1]
Mod(58669,392593)

ellisoncurve(E,[603,58669])
1

ellpow(E,[603,58669],392593+1-u)
[Mod(299996, 392593), Mod(300967, 392593)]

ellpow(E,[603,58669],392593+1+u)
[Mod(192962, 392593), Mod(247850, 392593)]

ellpow(E,[603,58669],392593+1-2*v)
[0]

ellpow(E,[603,58669],392593+1+2*v)
[Mod(326629, 392593), Mod(373006, 392593)]
```

Pour finir, vérifions que la trace $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\phi) = 2 \times v$ est telle que l'entier $m = N + 1 - 2 \times v$ est le produit de petits nombres premiers par un nombre probablement premier.

```
m=N+1-2*v
391808

m1=m;
forprime(q=1,100,if(m1%q==0,print(q);while(!(m1%q), m1=m1/q);print(m1, ";" m/m1)))
2
3061 ; 128
```

Donc $m = 2^7 \times 3061$.

L'entier 3061 est un nombre premier. On vérifie que $3061P = O_{\overline{E}}$.

```
ellpow(E,[603,58669],3061)
[0]
```

On a même mieux : le point $P = (603 : 58669 : 1)$ est d'ordre exact 3061.
Par ailleurs, $((N)^{1/4} + 1)^2 = 677.635279360427133333796454$, donc

$$3061 > ((N)^{(1/4)} + 1)^2.$$

D'après la proposition 3.1.1, l'entier 392593 est premier.

3.2 Améliorations et exemple

Les références pour cette section sont [25] et [14].

3.2.1 L'algorithme fastECPP

Lorsqu'il s'agit de prouver la primalité d'entiers très grands, l'algorithme ECPP prend beaucoup de temps pour trouver les discriminants $-D$. Cela suppose un nombre important de racines carrées modulo N à calculer. Un moyen de réduire ces calculs consiste à accumuler de petits nombres premiers q tels que $(\frac{q^*}{N}) = 1$ avec $q^* = (-1)^{\frac{q-1}{2}} q$ (on inclut les nombres $q^* = -4, -8, 8$ lorsqu'ils vérifient la condition $(\frac{q^*}{N}) = 1$).
Ensuite on calcule une racine carrée modulo N de chacun des q^*. Ainsi pour toute combinaison multiplicative des q^*, on dispose d'une racine carrée de ce produit modulo N par simple multiplication des racines déjà calculées. On peut donc remplacer l'Etape 1 de l'algorithme ECPP par une Etape 1'. Le résultat de cette substitution est l'algorithme fastECPP.

[Etape 1'.]

1.1 Trouver tous les $r = O(\log N)$ plus petits nombres premiers q^* tels que $(\frac{q^*}{N}) = 1$, et former l'ensemble $\mathfrak{Q} = \{q_1^*, q_2^*, \ldots, q_r^*\}$.

1.2 Calculer toutes les racines carrées $\sqrt{q^*}$ mod N pour $q^* \in \mathfrak{Q}$.

1.3 Essayer tous les sous-ensembles d'éléments distincts $\mathcal{S} = \{q_{i_1}^*, q_{i_2}^*, \ldots, q_{i_s}^*\}$ de $\mathfrak{Q}$ jusqu'à obtenir un produit $-D = \Pi_{q^* \in \mathcal{S}}\ q^* < 0$ tel qu'il existe un élément φ de l'anneau des entiers de $\mathbf{Q}(\sqrt{-D})$ de norme $\mathrm{N}_{\mathbf{Q}(\sqrt{-D})/\mathbf{Q}}(\varphi) = N$.

3.2.2 Exemple

Dans cet exemple nous illustrons les différentes phases de l'étape 1' de l'algorithme fastECPP, pour l'entier $N = 777977$.

De façon générale, il faut fixer la taille maximale des r plus petits nombres premiers q en fonction de la taille maximale des discriminants envisagés. Pour notre exemple, nous allons considérer les nombres premiers $1 \leq q \leq 50$.

On rappelle que d'après le théorème des nombres premiers, le nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à un nombre réel positif x est tel que

$$\pi(x) \sim \frac{x}{\log x}$$

quand x tend vers l'infini.

On commence par déterminer les nombres q^* (et leurs racines carrées modulo N) obtenus à partir des nombres premiers entre 3 et 50.

```
N=777977;
V1=vector(truncate(50/log(50)),k);
n=0;



forprime( p=3,50,
q=(-1)^((p-1)/2)*p;

if(!(Mod((q)^((N-1)/2),N)-1),z=lift(polrootsmod(X^2-q,N)[1]);

print(q,";",z);n=n+1;V1[n]=q ));

-7 ; 88128
-23 ; 159740
29 ; 367004
-31 ; 281840
41 ; 266856
-43 ; 115364

print(n)
6
```

Ensuite on traite le cas de $q^* \in \{-4, \pm 8\}$.

```
if(!(Mod((-4)^((N-1)/2),N)-1),z=lift(polrootsmod(X^2+4,N)[1]));
print(z)
```

```
242454

if(!(Mod((-8)^((N-1)/2),N)-1),z=lift(polrootsmod(X^2+8,N)[1]));
print(z)
254809

if(!(Mod((8)^((N-1)/2),N)-1),z=lift(polrootsmod(X^2-8,N)[1]));
print(z)
153858

V1[7]=-4;V1[8]=-8;V1[9]=8;
```

On calcule tous les produits de deux éléments $-D = q_1^* \times q_2^* < 0$ avec $q_i^* \in \mathfrak{Q}$ tels que la valeur absule $|q_1^* \times q_2^*| < 41 \times 43$. Puis on repère les produits $-D$ qui sont des discriminants fondamentaux.

```
n=0;
V2=V1;
V3=vector(8*(1+8)/2,n);
for(k=1,9, for(l=k+1,9,q=V1[k]*V2[l];
if(41*43 > abs(q),
if(q<0,n=n+1;V3[n]=q;
if(isfundamental(V3[n]),print(V3[n],":",k,",",l))))));

-203 : 1 , 3

-287 : 1 , 5

-56 : 1 , 9

-667 : 2 , 3

-943 : 2 , 5

-184 : 2 , 9

-899: 3 , 4

-1247 : 3 , 6

-116 : 3 , 7
```

```
-232 : 3 , 8

-1271 : 4 , 5

-248 : 4 , 9

-164 : 5 , 7

-328 : 5 , 8

-344 : 6 , 9

print(n)
17
```

Les nombres $-D \in \{-203, -287, -56, -667, -943, -184, -899, -1247, -116, -232, -1271, -248, -164, -328, -344\}$ sont des discriminants fondamentaux et des carrés modulo N. Le calcul des racines carrées de $-D$ modulo N ne coûte quasiment rien (une multiplication d'entiers), il correspond au produit des racines carrées des q^* (déjà connues) qui composent $-D$. Par exemple $-667 = (-23) \times 29$ et $-23 = 159740^2 \bmod 777977$ puis $29 = 367004^2 \bmod 777977$, donc $-667 = (159740 \times 367004)^2 = 762125 \bmod 777977$.

Ensuite il faut trouver les "bons" discriminants, c'est-à-dire les $-D$ pour lesquels N est complètement décomposé dans le corps de classes de Hilbert de $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$. Grâce à l'algorithme de Cornacchia [[28],théorème 4.1], on pourra déterminer un vecteur minimal φ dans un idéal premier $\mathfrak{P}$ au-dessus de N. Ce vecteur minimal est de norme N si et seulement si $\mathfrak{P}$ est principal.

Le nombre -667 est un bon candidat, la sequence de commandes suivante le confirme.

```
D=667;
x=2*N;y=762125;u=x%y;

while(sign(u-2*sqrt(N))+1,x=y;y=u;u=x%y);
print(u)
1229

sqrt((u^2-4*N)/(-D))
49.000000000000000000000000
```

L'élélement $\varphi = \frac{1229+49\times\sqrt{667}\times i}{2} \in \mathbf{O}_{\mathbf{Q}(\sqrt{-D})}$ est de norme 777977 et φ engendre un idéal $\mathfrak{P}$ au-dessus de N (ou son conjugué $\overline{\mathfrak{P}}$) [[28],théorème 4.1].

La détermination d'un vecteur minimal de norme N marque la fin de l'étape 1'. Les étapes suivantes sont exactement les mêmes que celles de l'algorithme ECPP ordinaire.

Chapitre 4

Le test de primalité AKS et ses variantes

Le test de primalité AKS est un algorithme déterministe de preuve de primalité qui a été publié en Août 2002 par Agrawal, Kayal et Saxena dans [1]. La preuve de l'algorithme est inconditionnelle (par opposition par exemple au test de Miller qui repose sur l'hypothèse de Riemann). On peut donc décider si un nombre est premier ou composé en temps déterministe polynomial. Dans ce chapitre nous introduisons et nous illustrons le test AKS ainsi que ses principales variantes. Ce faisant, nous préparons la voie au test AKS étendu et au test de primalité elliptique qui feront l'objet du prochain chapitre.

4.1 Le test AKS

4.1.1 Le critère

Cette section reprend l'analyse de l'algorithme AKS faite par René Schoof dans [29].

Pour tout nombre premier r, on note $\Phi_r(X) = X^{r-1} + \cdots + X + 1$ le r-ième polynôme cyclotomique. Si ζ_r est une racine de Φ_r, l'extension $\mathbf{Q}(\zeta_r)$ de $\mathbf{Q}$ est le r-ième corps cyclotomique, son anneau d'entiers est $\mathbf{Z}[\zeta_r]$. Pour tout $n \in \mathbf{Z}$, on note $\mathbf{Z}[\zeta_r]/(n)$ l'anneau des résidus de $\mathbf{Z}[\zeta_r]$ modulo l'idéal (n). Si $n \neq 0$, c'est un anneau fini.

Théorème 4.1.1. *Soient $n \geq 3$ un entier positif impair et r un nombre premier. Supposons que :*

1. *n n'est divisible par aucun des nombres premiers q tels que $q \leq r$;*
2. *l'ordre de $n \bmod r$ est strictement supérieur à $(\log n / \log 2)^2$;*
3. *Pour tout $0 \leq j < r$ on a $(\zeta_r + j)^n = \zeta_r^n + j$ dans $\mathbf{Z}[\zeta_r]/(n)$.*

Alors n est une puissance d'un nombre premier.

Preuve : D'après la condition 2 du théorème on a $n \not\equiv 1 \bmod r$, donc il existe un diviseur premier p de n non congru à 1 modulo r. On note A la $\mathbf{F}_p$-algèbre $\mathbf{Z}[\zeta_r]/(p) \cong \mathbf{F}_p[X]/\Phi_r(X)$.

Posons $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_r)/\mathbf{Q})$. Pour tout entier k premier à r on note σ_r l'élément de Δ qui envoie ζ_r sur ζ_r^k. L'application

$$\begin{array}{ccc} (\mathbf{Z}/r\mathbf{Z})^\times & \to & \Delta \\ k & \mapsto & \sigma_k \end{array} \tag{4.1}$$

est un isomorphisme de groupes. Tout $\sigma \in \Delta$ induit un automorphisme $\overline{\sigma}$ de A. En effet, pour tout $\sigma \in \Delta$ on a $\sigma(\mathbf{Z}[\zeta_r]) = \mathbf{Z}[\zeta_r]$ et $\sigma(p\mathbf{Z}[\zeta_r]) = p\mathbf{Z}[\zeta_r]$.

Notons que n est premier à r d'après la condition 1. Ainsi, σ_n est l'élément de Δ tel que $\sigma_n(\zeta_r) = \zeta_r^n$. L'application σ_p est l'automorphisme de Frobenius en p et on note Γ le sous-groupe de Δ engendré par σ_n et σ_p.
Intéressons nous aux idéaux de A. Soit $\mathfrak{p}$ un idéal premier de $\mathbf{Z}[\zeta_r]$ au dessus de (p). On observe que (p) est non-ramifié dans $\mathbf{Z}[\zeta_r]$, car r est premier à n d'après la condition 1 (le seul nombre premier qui se ramifie dans $\mathbf{Q}(\zeta_r)$ est r).

Soit $D(\mathfrak{p}) \subset \Delta$ le groupe de décomposition de $\mathfrak{p}$. Le degré résiduel de $\mathfrak{p}$ est $f = \#D(\mathfrak{p})$. Le groupe $D(\mathfrak{p})$ est le sous-groupe de Δ engendré par le Frobenius σ_p. Donc f est l'ordre de p dans $(\mathbf{Z}/r\mathbf{Z})^*$. Notons $d = [\Delta : D(\mathfrak{p})] = (r-1)/f$.

Soit $(\iota_1, \iota_2, \ldots, \iota_d)$ un système de représentants des classes de $(\mathbf{Z}/r\mathbf{Z})^*$ modulo le sous groupe $< p >$ engendré par p. Alors, $(\sigma_{\iota_1}, \ldots, \sigma_{\iota_d})$ est un système de représentants des classes de Δ modulo $D(\mathfrak{p})$. Les idéaux premiers de $\mathbf{Z}[\zeta_r]$ au-dessus de (p) sont les $\sigma_{\iota_i}(\mathfrak{p})$ pour $1 \leq i \leq d$.

Les idéaux maximaux de $A = \mathbf{Z}[\zeta_r]/(p)$ sont les images par la réduction modulo (p) des facteurs premiers de (p) dans $\mathbf{Z}[\zeta_r]$. Donc $\mathfrak{m} = \mathfrak{p}/(p) \subset A$ est un idéal maximal de A. On note $\mathbf{K} = A/\mathfrak{m}$. Le corps $\mathbf{K}$ est une extension de degré f de $\mathbf{F}_p$.

On appelle G le sous-groupe du groupe multiplicatif $A^\times$ égal au noyau de l'endomorphisme $\sigma_n - n \in \mathbf{Z}[\Delta]$:

$$G = \{a \in A^\times ; \sigma_n(a) = a^n\}.$$

Soit $H = \pi(G) \subset \mathbf{K}^*$ où π est la surjection canonique $\pi : A \to \mathbf{K}$; le groupe H est cyclique et on note s son ordre. On a le diagramme commutatif suivant :

$$\begin{array}{ccc} G & \hookrightarrow & A^\times \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ H & \hookrightarrow & \mathbf{K}^* \end{array}$$

Puisque Δ est abélien, il agit sur G. Les éléments σ_n et σ_p agissent sur G en élevant à la puissance n et p respectivement. Donc tout $\sigma_m \in \Gamma$ agit sur G en élevant à une certaine puisance e_m qui est première à $\#G$ du fait qu'il s'agit d'automorphismes de G. Ainsi l'application $\Gamma \to (\mathbf{Z}/\exp(G)\mathbf{Z})^\times$, définie par $\sigma_m \mapsto e_m$, est un morphisme de groupes bien défini. Puisque H est un quotient cyclique de G, son ordre s divise $\#G$. L'application $\sigma_m \mapsto e_m \bmod s$ induit un morphisme g qui fait commuter le diagramme suivant :

$$\begin{array}{ccc} \Gamma & \longrightarrow & \mathbf{Z}/(\#G)\mathbf{Z})^\times \\ & \searrow^{g} & \downarrow \\ & & (\mathbf{Z}/s\mathbf{Z})^\times \end{array} \tag{4.2}$$

Si $m \equiv p^i n^j \bmod r$, alors $g(\sigma_m) \equiv p^i n^j \bmod s$.
L'idée dans cette preuve est de montrer que si H est gros, c'est-à-dire $s > n^{\lfloor\sqrt{\#\Gamma}\rfloor}$, alors n est une puissance d'un nombre premier.
Regardons ce qui se passe quand n est premier. Dans ce cas $n = p$ et σ_n est l'automorphisme de Frobenius σ_p. Le groupe G est égal à $A^\times$ tout entier et donc H est égal à $\mathbf{K}^*$. Comme f est l'ordre de p modulo r, le groupe $\Gamma =< \sigma_p >$ est d'ordre f, le groupe $H = \mathbf{K}^*$ est d'ordre $s = p^f - 1 = n^{\#\Gamma} - 1$ et son groupe d'automorphismes $Aut(H)$ est isomorphe à $(\mathbf{Z}/s\mathbf{Z})^\times$.

Revenons aux cas général. Sous les hypothèses du théorème 4.1.1, et sans supposer n premier, on peut montrer que s est assez gros.
Affirmation. On a

$$s > n^{\lfloor\sqrt{\#\Gamma}\rfloor}. \tag{4.3}$$

La preuve de cette affirmation repose essentiellement sur des arguments de combinatoire. Expliquons d'abord comment cette inégalité permet de conclure. Considérons l'homomorphisme g construit précédemment, et soit $q = n/p$. On s'intéresse aux produits $\sigma_p^i \sigma_q^j$ pour $0 \leq i, j \leq \lfloor\sqrt{\#\Gamma}\rfloor$. Puisque $(1+\lfloor\sqrt{\#\Gamma}\rfloor)^2 > \#\Gamma$, il existe deux couples $(i, j) \neq (i', j')$ tels que $\sigma_p^i \sigma_q^j = \sigma_p^{i'} \sigma_q^{j'}$ dans Γ. Il s'ensuit que leurs images par g sont égales dans $(\mathbf{Z}/s\mathbf{Z})^\times$. Puisque $g(\sigma_q) = q \bmod s$, cela signifie que $p^i q^j = p^{i'} q^{j'} \bmod s$. Les entiers $p^i q^j$ et $p^{i'} q^{j'}$ sont inférieurs à $n^{max(i,i',j,j')}$. Or $n^{max(i,j)} \leq n^{\lfloor\sqrt{\#\Gamma}\rfloor} < s$, donc $p^i q^j = p^{i'} q^{j'}$ dans $\mathbf{Z}$. Puisque $(i, j) \neq (i', j')$, q est une puissance de p et il en est de même pour n □

Preuve de l'Affirmation. Nous donnons les grandes idées de la preuve.
Soit C un ensemble de représentants des classes modulo Γ dans Δ. On considère le morphisme

$$\begin{array}{ccc} G & \to & \Pi_{\sigma \in C} \mathbf{K}^* \\ a & \mapsto & (\sigma(a) \bmod \mathfrak{m})_{\sigma \in C} \end{array}$$

Cette application est injective, donc

$$s > \#G^{1/[\Delta:\Gamma]}. \tag{4.4}$$

Les éléments $\zeta_r + j$ sont des unités de A car ils n'appartiennent à aucun idéal maximal de A. D'après la condition 3 du théorème, pour chaque sous-ensemble $J \subset \{0, 1, \ldots, r-2\}$ l'élément

$$\Pi_{j \in J}(\zeta_r + j)$$

est contenu dans G.
De plus ces éléments sont distincts. En effet, si $\prod_{j\in J_1}(\zeta_r+j) = \prod_{j\in J_2}(\zeta_r+j)$ alors la différence $\prod_{j\in J_1}(\zeta_r+j) - \prod_{j\in J_2}(\zeta_r+j)$ est nulle dans A. Le degré de ϕ_r impose que cela n'est possible que si $J_1 = J_2$.

Puisqu'il y a 2^{r-1} sous-ensembles $J \subset \{0, 1, \ldots, r-2\}$, on conclut que

$$\#G \geq 2^{r-1}. \tag{4.5}$$

En combinant les inégalités (4.4) et (4.5) on a

$$s \geq \#G^{1/[\Delta:\Gamma]} \geq 2^{(r-1)/[\Delta:\Gamma]} = 2^{\#\Gamma}. \tag{4.6}$$

Mais nous sommes sous les conditions du théorème 4.1.1, en particulier l'ordre de n modulo r est strictement supérieur à $(\log n/\log 2)^2$. Donc $\#\Gamma > (\log n/\log 2)^2$, ainsi

$$2^{\#\Gamma} > n^{\sqrt{\#\Gamma}} \geq n^{\lfloor\sqrt{\#\Gamma}\rfloor}. \tag{4.7}$$

L'inégalité (4.3) en découle.

4.1.2 L'algorithme

Le théorème 4.1.1 mène au test de primalité suivant :

Algorithme 4.1.2. *Soit $n > 1$ un entier impair donné.*

1. *Vérifier que n n'est pas une puissance propre d'un entier.*
2. *a. En essayant successivement avec $2, 3, 5, \ldots$, déterminer le plus petit nombre premier r ne divisant pas n ni aucun des nombres $n^i - 1$ pour $0 \leq i \leq (\log n/\log 2)^2$;*
   b. Puis vérifier que n n'est divible par aucun des nombres premiers $q, q \leq r$.
3. *Pour $0 \leq j \leq r-1$ vérifier que $(\zeta_r + j)^n = \zeta_r^n + j$ dans $\mathbf{Z}[\zeta_r]/(n)$.*

Si le nombre n ne passe pas les tests, il est composé. Et s'il les passe tous, il est premier.

4.1.3 Commentaires

Pour commencer, estimons la taille maximale de r en fonction de n. Par définition de r, tout nombre premier $q < r$ divise le produit $n\Pi_{1\leq i\leq(\frac{\log n}{\log 2})^2}(n^i - 1)$. Donc

$$\sum_{\substack{q<r \\ q \text{ premier}}} \log q \leq \log n + \log n \sum_{1\leq i\leq(\frac{\log n}{\log 2})^2} i = O((\log n)^5).$$

Une version faible du théorème des nombres premiers nous permet d'affirmer qu'il existe une constante $c > 0$ telle que pour tout nombre réel r, $\sum_{q<r} \log q \geq cr$. Donc la valeur

maximale de r est $O((\log n)^5)$.

Maintenant nous allons faire une analyse de la complexité de chaque test de l'algorithme. Le premier test se fait en vérifiant que $n^{\frac{1}{m}} \notin \mathbf{Z}$ pour tout entier m tel que $2 \leq m \leq \log_2 n$. Cela peut se faire en utilisant par exemple l'algorithme de detection de puissance parfaite que Daniel J. Bernstein décrit dans [4]. La complexité du test 1 est $O((\log n)^(1+o(1)))$ ([4]).

Dans le second test, il s'agit , pour $r = 2, 3, 5, \ldots$ de considérer la classe de n dans $\mathbf{Z}/r\mathbf{Z}$, donc un nombre à $O(\log r)$ bits. Puis de calculer $n^i - 1$ pour $1 \leq i \leq (\log_2 n)^2$ dans chaque $\mathbf{Z}/r\mathbf{Z}$. Cela revient à faire $r \times (\log_2 n)^2$ multiplications de nombres à $O(\log r)$ chiffres binaires. Le second test prend $O(r((\log_2 n)(\log r))^2))$ opérations élémentaires.

Le troisième nécessite $r \times O(\log n)$ multiplications dans l'anneau $A = \mathbf{Z}[\zeta_r]/(n) \cong \mathbf{Z}[X]/(n, \Phi_r(X))$. Un élément $\alpha \in A$ est de la forme $\alpha = P(\zeta_r)$ où P est un polynôme de degré au plus égal à $r-1$ à coefficients dans $\mathbf{Z}/n\mathbf{Z}$. Donc multiplier deux éléments de A revient au maximum à multiplier deux nombres de taille $O(r \log n)$, c'est-à-dire $O((r \log n)^{1+\epsilon})$ ($\epsilon = 1$ lorsqu'on utilise l'algorithme de multiplication standard ; pour des techniques de multiplication rapide on a : $0 < \epsilon < 1$). Puisque $r = O((\log n)^5)$, le temps de calcul nécessaire au troisième test est $O((\log n)^{6(2+\epsilon)})$. Donc le test 3. est le plus couteux.

Pour finir établissons l'authenticité de l'algorithme, c'est-à-dire montrons qu'il répond clairement et sans erreur à la question "l'entier N est-il premier ?"
Si $N = p$ est un nombre premier, il passe le premier test. On peut toujours trouver en temps $O((\log(p))^5)$ un nombre premier r qui vérifie la condition 2.a et la 2.b est immédiatement vérifiée. Et puisque p est premier, pour toute racine primitive r-ième de l'unité ζ_r et pour tout j, $0 \leq j \leq r-2$ on a :

$$(\zeta_r + j)^p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) \zeta_r^{p-k} j^k \equiv \zeta_r^n + j \bmod p.$$

Donc la condition 3 du test est satisfaite.

Réciproquement, supposons qu'un entier n vérifie tous les tests de l'algorithme. Nous allons montrer à l'aide du théorème 4.1.1 que n est premier. Le test 2.b de l'algorithme implique la condition 1 du théorème. Puisque r ne divise aucun des nombres $n^i - 1$ pour $0 \leq i \leq (\log n / \log 2)^2$ (condition 2.a de l'algorithme), l'ordre de n mod r est plus grand que $(\log n / \log 2)^2$ (condition 2 du théorème). La condition 3 de l'algorithme étant vérifiée, la condition 3 du théorème est vérifiée (il s'agit de la même condition à chaque fois). D'après le théorème, l'entier n est une puissance d'un nombre premier. Puisque n n'est pas une puissance propre d'un entier (test 1 de l'algorithme), l'entier n est premier.

4.1.4 Exemple

Prouvons que 30000001 est un nombre premier.

On vérifie que 30000001 n'est pas une puissance propre d'un entier avec la séquence d'instructions suivantes :

```
N=30000001;
ispower(N)
0
```

Donc l'entier 30000001 n'est pas une puissance propre. Ensuite on cherche r :

```
{forprime(p=1, log(N)^4,
X=Mod(N,p);
Y=X*prod(k=1, floor((log(N)/log(2))^2), (X^k-Mod(1, p)));
if(Y,r=p;print(r);break))}
647
```

Puis on vérifie que 30000001 n'est divisible par aucun des nombres premiers $q, q \leq r = 647$:

```
forprime(q=1,r,Y=gcd(N,q);if((Y-1),print("error", ":","N n'est pas premier")))
```

Et enfin on vérifie que pour $N = 30000001$ la relation de la condition 3 est vérifiée :

```
P(x)=sum(k=0,r-1,x^k);
PN(x)=P(x)*Mod(1,N)
X=Mod(x,PN(x));Z=X^N;
for(k=1,r-1,
if((X + Mod(k,N))^N - (Z + Mod(k,N)),
print("error", ":","N n'est pas premier")))
```

On conclut que 30000001 est premier.

4.2 Améliorations

4.2.1 La variante de Lenstra et Pomerance

On a vu, au niveau de l'analyse de l'algorithme AKS, que ce dernier passe le plus gros du temps sur le troisième test. Pour améliorer cela, Lenstra et Pomerance observent dans [23] que l'on peut remplacer l'anneau $A = \mathbf{Z}[\zeta_r]/(n) = (\mathbf{Z}/n\mathbf{Z})[X]/\Phi_r(X)$ par un quotient plus

général $(\mathbf{Z}/n\mathbf{Z})[X]/f(X)$ où $f(X) \in \mathbf{Z}[X]$ est un polynôme unitaire de degré $d > (\log_2 n)^2$. De plus on n'a que $\sqrt{d}\log_2 n$ congruences dans A à vérifier. On suppose que

$$f(X^n) = 0 \bmod (n, f(X))$$

et

$$X^{n^d} = X \bmod (n, f(X)).$$

On suppose aussi que pour tout premier l divisant d, la classe de $X^{n^{\frac{d}{l}}} - X$ dans A est inversible.

Donc il existe un automorphisme $\sigma : A \to A$ d'ordre d. Le test AKS s'adapte à ce contexte plus général. Quel est l'avantage ?

Dans l'algorithme AKS, on choisit un nombre premier r tel que l'ordre de n dans $(\mathbf{Z}/r\mathbf{Z})^*$ soit plus grand que $(log_2 n)^2$. Mais il se pourrait que cet ordre soit petit par rapport à $\varphi(r)$. Donc le polynôme $\Phi_r(X)$ se décompose en beaucoup de polynômes modulo n. On travaille alors modulo $\Phi_r(X)$ alors qu'un seul facteur suffirait. La variante de Lenstra et Pomerance permet d'avoir un degré de $f(X)$ plus proche du minimum $(\log_2 n)^2$ et de limiter ainsi les multiplicités inutiles.

Naturellement, il n'est pas question de factoriser $\Phi_r(X)$ modulo n. Ce serait plus coûteux que de prouver la primalité. Et ce ne serait pas déterministe. Au lieu de cela, on remplace le polynôme $\Phi_r(X)$ par le polynôme minimal d'un générateur d'une sous-extension de $\mathbf{Q}(\zeta_r)/\mathbf{Q}$ de degré d. Donc on cherche un nombre premier r tel que $\varphi(r) = r - 1$ ait un facteur d de degré proche de $(\log_2 n)^2$. On peut même considérer le compositum de telles extensions.

Autrement dit, la plus grande variété de polynômes disponibles permet d'ajuster au mieux le degré d à la borne $(\log_2 n)^2$.

La complexité de l'algorithme de Lenstra et Pomerance est $\widetilde{O}((\log n)^6)$.

4.2.2 L'idée de Berrizbeitia améliorée par Bernstein

D'une certaine façon, l'observation de Berrizbeitia-Bernstein est un cas particulier de la variante de Lenstra et Pomerance. Pour le voir, revenons sur le test AKS.

Nous avons vu, en examinant chacune des étapes de l'algorithme AKS, qu'il est fastidieux de vérifier les r relations de congruences

$$(X + j)^n = X^n + j \bmod (n, \Phi_r(X))$$

pour $0 \leq j < r$. En effet, chacune de ces vérifications requiert le calcul d'une exponentiation dans un très gros anneau.

Dans l'algorithme de Lenstra et Pomerance, on aura à vérifier $O((\log_2 n)^2)$ congruences de la forme

$$(X+j)^n = X^n + j \bmod (n, f(X))$$

où $f(X)$ est un polynôme de degré $O((\log_2 n)^2)$.

Déjà, il y a moins de congruences à calculer et l'anneau $\mathbf{S} = \mathbf{Z}[X]/(n, f(X))$ est un peu plus petit.

Pour gagner encore un peu de temps, on essaye d'appliquer un automorphisme de $\mathbf{S}$ à une congruence déjà vérifiée, dans l'espoir de faire apparaître une autre congruence intéressante. Soit donc $\sigma : \mathbf{S} \to \mathbf{S}$ un automorphisme de $\mathbf{S}$ et supposons que la congruence

$$(\alpha + j)^n = \alpha^n + j \in \mathbf{S}$$

est vérifiée où $\alpha = X \bmod (n, f(X)) \in \mathbf{S}$. Alors

$$(\sigma(\alpha) + j)^n = \sigma(\alpha)^n + j \bmod (n, f(X)).$$

Cette congruence n'a pas grand chose à voir avec celles qui nous intéressent *sauf si* $\sigma(\alpha)$ *est une expression affine en* α.

Supposons que $\mathbf{K}$ est un corps commutatif contenant les racines n-ièmes de l'unité, où n est un nombre entier premier à la caractéristique de $\mathbf{K}$ lorsqu'elle est positive. Par définition, une extension $\mathbf{L}/\mathbf{K}$ est de Kummer si le corps $\mathbf{L}$ est $\mathbf{K}$-engendré par une racine d'un polynôme $X^n - a$ à coefficients dans $\mathbf{K}$. Si $\mathbf{K}$ ne contient aucune racine m-ième de a, pour m divisant n, le corps $\mathbf{L}$ est une extension cyclique de degré n. Sans hypothèse sur les racines de a dans $\mathbf{K}$, l'extension est cyclique de degré divisant n.

Bernstein énonce dans [5] un théorème qui tient lieu de critère de la version améliorée de l'algorithme AKS que nous étudions. Nous reprenons ce théorème en l'adaptant à notre contexte (cas particulier $d = 1$ et $e = d$ pour les notations du théorème 2.1 de [5]).

Théorème 4.2.1 (Critère de Berrizbeitia-Bernstein,[5], théorème 2.1)**.** *Soient n et d des entiers positifs tels que $2^d - 1 \geq n^{2\lfloor\sqrt{d}\rfloor}$ et d divise $n-1$. Soit $r \in \mathbf{Z}/n\mathbf{Z}$ tel que $r^{n-1} = 1$ dans $\mathbf{Z}/n\mathbf{Z}$, $r^{\frac{n-1}{q}} - 1$ est une unité de $\mathbf{Z}/n\mathbf{Z}$ pour tout nombre premier q divisant d, et $r-1$ est une unité de $\mathbf{Z}/n\mathbf{Z}$.*
Si $(X-1)^n = r^{\frac{n-1}{d}} X - 1$ dans $\mathbf{S} = (\mathbf{Z}/n\mathbf{Z})[X]/(X^d - r)$ alors n est une puissance d'un nombre premier.

Démonstration. Voir corollaire 5.4.2 du chapitre 5. □

- On choisit donc un polynôme $f(X) = X^d - r$ de type Kummer. Soit p un nombre premier qui divise n, et $\pi : \mathbf{Z}/n\mathbf{Z} \to (\mathbf{Z}/n\mathbf{Z})/(p\mathbf{Z}/n\mathbf{Z}) \cong \mathbf{F}_p$ la surjection canonique. Soit $\zeta = \pi(r^{\frac{n-1}{d}}) \in \mathbf{F}_p$, alors ζ est une racine primitive d-ième de l'unité. Le corps $\mathbf{K} =$

$\mathbf{F}_p[X]/(X^d - r) \cong \mathbf{F}_{p^d}$ est une extension de Kummer de $\mathbf{F}_p$.

- On gagne un facteur r sur la complexité puisqu'il n'y a plus qu'une congruence à vérifier pour en déduire toutes les autres. Pour le voir, notons σ un générateur de $\mathrm{Gal}(\mathbf{K}/\mathbf{F}_p)$. Si $(X+1)^n = X^n + 1$ est une congruence déjà vérifiée dans $\mathbf{K}$, alors $\sigma((X+1)^n) = \sigma(X^n + 1)$. Donc $(\zeta X + 1)^n = \zeta^n X^n + 1$, ainsi $(X + \zeta^{-1})^n = X^n + \zeta^{-1}$. On obtient toutes les autres congruences de cette façon.

Ces observations mènent à l'algorithme suivant :

Algorithme 4.2.2. *Soit $n > 1$ un entier impair donné.*

1. *Vérifier que n n'est pas une puissance propre d'un entier.*
2. *Trouver un entier d divisant $n - 1$ tel que $2^d - 1 \geq n^{2\lfloor\sqrt{d}\rfloor}$.*
3. *Trouver un résidu r modulo n tel que $\zeta = r^{\frac{n-1}{d}}$ est une racine primitive d-ième de l'unité modulo n.*
4. *Vérifier que $(X-1)^n = \zeta X - 1$ dans $\mathbf{S} = (\mathbf{Z}/n\mathbf{Z})[X]/(X^d - r)$.*

Si le nombre n passe les tests, il est premier.

Il ne s'agit plus d'un algorithme déterministe, comme l'est l'algorithme AKS. Regardons de près chacune des étapes :

Étape 1 : Cette étape est exactement la même que la première étape de l'algorithme AKS.

Étape 2 : On veut que $n - 1$ soit divisible par un entier d tel que $2^d - 1 \geq n^{2\lfloor\sqrt{d}\rfloor}$. Cela découle du fait que si n est premier, l'extension $\mathbf{Z}[X]/(n, X^d - r)$ n'est de Kummer que lorsque $\mathbf{Z}/n\mathbf{Z}$ contient au moins une racine primitive d-ième de l'unité.

Étape 3 : Il faut calculer une racine primitive d-ième dans $(\mathbf{Z}/n\mathbf{Z})^*$. C'est très facile : il suffit de choisir un résidu au hasard modulo n et de l'élever à la puissance $(n-1)/d$. Mais ce *n'est pas déterministe.*

Étape 4 : En notant α la classe de X dans $\mathbf{S}$, il s'agit ici de vérifier que $(\alpha - 1)^n - \zeta\alpha + 1$ est nul.

Au total, on obtient un algorithme probabiliste (une étape sur quatre est probabiliste) pour tester la primalité de n. Quelques complications surviennent du fait que $n - 1$ n'a pas toujours de facteur d de la taille escomptée. Par exemple on ne peut pas prouver à l'aide de l'algorithme 4.2.2 que 97 est un nombre premier. On se heurte au fait que 96 ne possède pas de diviseur d tel que $2^d - 1 \geq 96^{2\lfloor\sqrt{d}\rfloor}$.

4.2.3 Exemple

Prouvons à l'aide l'algorithme 4.2.2 que $n = 809$ est un nombre premier.

On vérifie que 809 n'est pas une puissance propre d'un entier avec la séquence d'instructions suivantes :

```
n=809;
for(k=2,floor(log (n)/log (2)),q=n^(1/k);print(q))
28.442925306655783572931236 87
9.317859848626759599594648074
5.333190912264043784981001422
3.815836029337661065910768208
3.052516969424864573195782645
2.602682652279448562928520112
2.309370241486636067235999937
2.104289030709356968225812388
```

Donc l'entier 809 n'est pas une puissance propre. Ensuite on cherche d :

```
for(k=1,n-1,if((n-1)%k==0,if(2^k-1>n^(2*floor(sqrt(k))),print(k), ), ))
404
808
```

On choisit $d = 404$ puis on cherche r.
Le groupe $(\mathbf{Z}/809\mathbf{Z})^\times$ est cyclique, il est engendré par un élément $r \in (\mathbf{Z}/809\mathbf{Z})^\times$ si $r^m \neq 1$ pour m parcourant l'ensemble des diviseurs maximaux de $\#(\mathbf{Z}/809\mathbf{Z})^\times$.

```
d=404;
factor(d)
[2  2]

[101  1]

for(k=2,20,
if( Mod(k^(808/2)-1,809) * Mod(k^(808/101)-1,809),
print(k), ))

3
6
11
12
15
17
```

On pose $r = 3 \bmod 809$, donc $\zeta = 3^2 = 9 \bmod 809$. On vérifie la condition 4 de l'algorithme :

```
r=3;
z=9;
P=x^d-r;
Pn=P*Mod(1,n)
X=Mod(x,Pn);
Y=(X-Mod(1,n))^n -z*X+Mod(1,n);
print(Y)
0
```

Les conditions du théorème 4.2.1 étant vérifiées, l'entier 809 est une puissance d'un nombre premier. Mais nous nous sommes assurés que 809 n'est pas une puissance propre, donc 809 est un nombre premier.

Chapitre 5

Le critère de primalité AKS étendu

L'objectif de ce chapitre est d'énoncer un nouveau critère de primalité qui utilise à la fois les idées de la cyclotomie et la théorie des courbes elliptiques. Dans la section 5.1 nous rappelons les propriétés des anneaux artiniens qui nous seront utiles dans la suite. La section 5.2 présente les principales propriétés des extensions entières d'anneaux, en particulier celles obtenues en quotientant par l'action d'un groupe fini. La section 5.3 est consacrée aux morphismes étales de schémas. Nous énonçons dans la section 5.4 un critère général de primalité qui repose sur l'existence et les propriétés d'une algèbre libre étale et galoisienne sur l'anneau $\mathbf{Z}/n\mathbf{Z}$ où n est le nombre dont on veut prouver la primalité.

Dans ce chapitre, tous les anneaux sont supposés commutatifs et unitaires.

5.1 Quelques propriétés des anneaux artiniens

Soit Σ un ensemble partiellement ordonné par la relation $\leq$, on a :

Proposition-Définition 5.1.1. *Les conditions suivantes dans Σ sont équivalentes :*

(i) Toute suite croissante $x_1 \leq x_2 \leq \dots$ d'éléments de Σ est stationnaire (i.e., il existe n tel que $x_n = x_{n+1} = \dots$).

(ii) Tout sous-ensemble non vide de Σ admet un élément maximal.

Si Σ est l'ensemble des sous-modules d'un module M, ordonné par la relation $\supset$ (contient). Alors la condition (i) est dite condition de chaine descendante (ou d.c.c pour l'abréviation anglaise descending chain condition) et (ii) est la condition minimale. Un module M vérifiant l'une de ces conditions est dit artinien.
Si Σ est ordonné par $\subset$, alors (i) est la condition de chaine ascendante (a.c.c) et (ii) est la condition maximale. Un module M vérifiant l'une de ces condition est dit noethérien.

On dit qu'un anneau A est artinien ou que A est un anneau d'Artin (resp. noethérien) si A est un A-module artinien (resp. noethérien).

Dans un certain sens, les anneaux d'Artin sont les anneaux les plus simples (après les corps bien entendu), leurs idéaux ont des propriétés agréables. Donnons un premier énoncé :

Proposition 5.1.2. *Dans un anneau d'Artin tout idéal premier est maximal.*

On appelle chaine d'idéaux premiers d'un anneau A, une suite strictement croissante d'idéaux premiers $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_r$; la longueur de la chaine est r. La *dimension* n de A est la borne supérieure de l'ensemble des longueurs de toutes les chaines d'idéaux premiers de A : on a $n \in \mathbb{N} \cup \{\infty\}$.
La proposition 5.1.2 dit que tout anneau d'Artin est de dimension nulle.

De façon générale, le *radical de Jacobson* (ou simplement le radical) d'un anneau est l'intersection de tous ses idéaux maximaux.
Étant donné un anneau A et I un idéal de A distinct de A, le radical $\sqrt{I}$ de I est l'idéal formé de tous les $x \in A$ pour lesquels il existe un entier non nul n tel que $x^n \in I$. Le *nilradical* de l'anneau A est l'idéal $\sqrt{(0)}$ formé des éléments nilpotents de A. On peut aussi définir $\sqrt{(0)}$ comme l'intersection de tous les idéaux premiers de A.
Donc pour tout anneau de dimension 0, le nilradical est égal au radical de Jacobson.

Énonçons deux autres propositions concernant les idéaux d'un anneau d'Artin.

Proposition 5.1.3. *Un anneau d'Artin n'a qu'un nombre fini d'idéaux maximaux.*

Proposition 5.1.4. *Dans un anneau d'Artin A le nilradical $nil(A)$ est nilpotent.*

La symmétrie apparente entre anneaux d'Artin et anneaux noethérien est fausse en réalité. Le théorème suivant précise les choses.

Théorème 5.1.5. *Un anneau A est artinien si et seulement si A est noethérien et* $\dim A = 0$.

Si A est un anneau d'Artin local d'idéal maximal $\mathfrak{m}$, alors $\mathfrak{m}$ est l'unique idéal premier de A et par conséquent $\mathfrak{m}$ est le nilradical de A. Donc tous les éléments de $\mathfrak{m}$ sont nilpotents, et $\mathfrak{m}$ est lui-même nilpotent. Par conséquent un élément de A est soit nilpotent, soit une unité.

Proposition 5.1.6. *Soient A un anneau noethérien local et $\mathfrak{m}$ son idéal maximal. Alors exactement un (à la fois) des énoncés suivants est vrai :*
- $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ *pour tout n ;*
- $\mathfrak{m}^n = 0$ *pour un certain n, et dans ce cas A est un anneau d'Artin local.*

Cette section s'achève avec le théorème de structure des anneaux d'Artin suivant.

Théorème 5.1.7 (Théorème de structure des anneaux d'Artin, [2] page 90)**.** *Un anneau d'Artin A s'écrit de façon unique (à isomorphisme près) comme un produit direct fini d'anneaux d'Artin locaux.*

Démonstration. Nous ne donnons qu'une partie de la preuve, celle qui concerne l'existence. L'unicité n'est pas justifiée ici. Ce théorème est entièment démontré dans [2].

Soient $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ les idéaux maximaux de A. Alors le nilradical $nil(A) = \bigcap_{i=1}^{n} \mathfrak{m}_i$ de A est nilpotent. Notons $k > 0$ son degré de nilpotence. On a $\mathfrak{m}_i^k + \mathfrak{m}_j^k = A$ pour $i \neq j$, donc

$$\bigcap_{i=1}^{n} \mathfrak{m}_i^k = \prod_{i=1}^{n} \mathfrak{m}_i^k.$$

Par conséquent A est isomorphe au produit $\prod_{i=1}^{n} A/\mathfrak{m}_i^k$. Chaque $A/\mathfrak{m}_i^k$ est un anneau artinien local. □

5.2 Les extensions entières d'anneaux

Cette section traite des extensions entières d'anneaux. Nous n'exposons ici que le principales propriétés qui nous seront utiles. Pour une étude plus approfondie, les ouvrages [20], [7] et [27] sont de très bonnes références.

5.2.1 Relèvement des idéaux premiers

Soit **A** un anneau. Si **B** est un sous-anneau de **A**, alors on dit aussi que **A** est une extension d'anneau de **B**.
Un élément $x \in \mathbf{A}$ est entier sur **B** si l'une des conditions équivalentes suivantes est satisfaite :

1. Il existe un entier positif n et des éléments $b_0, \ldots, b_{n-1} \in \mathbf{B}$ tels que

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 + b_0 = 0. \tag{5.1}$$

2. L'anneau $\mathbf{B}[x]$ est un **B**-module de type fini.
3. Il existe un sous-anneau **R** de **A**, contenant **B** et x, et qui est un **B**-module de type fini.

L'anneau A est dit entier sur B si tout élément de A est entier sur B.

Exemple 5.2.1. *Considérons* **K** *un corps de nombres (i.e le corps* **K** *est une extension de* **Q** *et un* **Q***-espace vectoriel de dimension finie), A son anneau d'entiers (A est l'ensemble des éléments de* **K** *entiers sur* **Z***),* **L** *une extension de degré fini de* **K** *et B l'anneau des entiers de* **L***. L'anneau B est une extension de A et entier sur A (i.e tout $x \in B$ est entier sur A). Soit* $\mathfrak{p}$ *un idéal premier de A. Puisque B est un anneau de Dedekind on a*

$$\mathfrak{p}B = \Pi\mathfrak{P}_i^{e_i} \text{ une décomposition unique en produit d'idéaux premiers.}$$

Pour tout i, les $\mathfrak{P}_i$ *figurant dans la décomposition de* $\mathfrak{p}B$ *sont dits idéaux au-dessus de* $\mathfrak{p}$*.*

On veut étudier plus généralement les liens entre l'arithmétique de A et celle de B.

Définition 5.2.2. *Soient A, A' deux anneaux , $h : A \to A'$ un homorphisme d'anneaux. L'ensemble $h(A)$ est un sous-anneau de A' et l'anneau A' est muni d'une structure de A-module.*
Pour tout idéal $\mathfrak{a}$ de A, on note $\mathfrak{a}A'$ l'idéal de A' engendré par $h(\mathfrak{a})$.
On dit qu'un idéal $\mathfrak{a}'$ de A' est au-dessus d'un idéal $\mathfrak{a}$ si $\mathfrak{a} = h^{-1}(\mathfrak{a}')$.

Si le morphisme h est une injection et que l'on identifie les anneaux A et $h(A)$, alors les idéaux $\mathfrak{a}'$ de A' au-dessus d'un idéal $\mathfrak{a}$ de A sont ceux tels que $\mathfrak{a}' \cap A = \mathfrak{a}$ (ceux qui rencontrent A exactement en $\mathfrak{a}$).

On notera que pour qu'il existe un idéal de A' au-dessus de l'idéal (0) de A, il faut et il suffit que $h : A \to A'$ soit injective.

Soit $\mathfrak{a}$ un idéal de A ; par passage aux quotients, l'homomorphisme h donne un homomorphisme

$$\begin{array}{rccc} h_1 : & A/\mathfrak{a} & \to & A'/\mathfrak{a}A' = A'/h(\mathfrak{a})A' \\ & a \bmod \mathfrak{a} & \mapsto & h(a) \bmod \mathfrak{a}A'. \end{array}$$

Remarque 5.2.3. *Dire que $\mathfrak{a}'$ est un idéal de A' au-dessus de $\mathfrak{a}$ équivaut à dire que $\mathfrak{a}A' \subset \mathfrak{a}'$ et que $\mathfrak{a}'/\mathfrak{a}A'$ est un idéal de $A'/\mathfrak{a}A'$ au-dessus de (0). En effet :*

Supposons que $\mathfrak{a}'$ est un idéal de A' au-dessus de $\mathfrak{a}$. On a $h(\mathfrak{a}) = h(h^{-1}(\mathfrak{a}')) \subset \mathfrak{a}'$, donc $\mathfrak{a}A' \subset \mathfrak{a}'$. Soit $a \bmod \mathfrak{a}$ un élément du noyau de h_1, alors $h(a) \in \mathfrak{a}A'$. Donc $a \in h^{-1}(\mathfrak{a}A') \subset h^{-1}(\mathfrak{a}') = \mathfrak{a}$, et h_1 est injective.

Inversement si $\mathfrak{a}A' \subset \mathfrak{a}'$, alors $h(\mathfrak{a}) \subset \mathfrak{a}'$. Donc $\mathfrak{a} \subset h^{-1}(\mathfrak{a}')$. Supposons que l'idéal $\mathfrak{a}'/\mathfrak{a}A'$ de $A'/\mathfrak{a}A'$ est au-dessus de $(\overline{0})$. Cela équivaut à $(\overline{0}) = h_1^{-1}(\mathfrak{a}'/\mathfrak{a}A') = h^{-1}(\mathfrak{a}')/\mathfrak{a}$ dans $A/\mathfrak{a}$. Donc $h^{-1}(\mathfrak{a}') = \mathfrak{a}$.

Faisons un bref rappel sur les anneaux de fractions d'un anneau A par rapport à une partie multiplicative S.

Définition 5.2.4. *Soit A un anneau. On dit qu'un sous-ensemble $S \subset A - \{0\}$ est une partie multiplicative de A lorsque S contient 1 et que le produit de deux éléments de S est encore un élément de S.*
L'anneau des fractions de A par rapport à S (la localisation ou encore le localisé de A en S) est l'ensemble, noté $S^{-1}A = A_S$, quotient de $A \times S$ par la relation d'équivalence

$$(a, s)\mathcal{R}(a', s') \Leftrightarrow \text{ il existe } t \in S \text{ tel que } t(sa' - s'a) = 0.$$

La classe d'équivalence du couple (a, s) est notée a/s, l'application $i_A^S : a \mapsto a/1$ est le morphisme canonique de A dans $S^{-1}A$. Pour tout idéal $\mathfrak{a}$ de A, on note $S^{-1}\mathfrak{a}$ l'idéal de $S^{-1}A$ engendré par $i_A^S(\mathfrak{a})$.
Le localisé A_S de A en S est aussi défini par la propriété universelle suivante :

Pour tout morphisme d'anneaux $\psi : A \to B$ tel que $\psi(S) \subset B^\times$, il existe un unique morphisme $\widetilde{\psi} : A_S \to B$ tel que $\widetilde{\psi} \circ i_A^S = \psi$.
Lorsque l'anneau A est supposé intègre, et que la partie multiplicative S est l'ensemble $A^\times$ des éléments non nuls de A, l'anneau des fractions $S^{-1}A$ est le corps des fractions de A.

Lemme 5.2.5. *[[6] page 90 et [7] page 31] Soient $h : A \mapsto A'$ un homomorphisme d'anneaux et S une partie multiplicative de A. On note $S^{-1}A$ (resp. $S^{-1}A'$) la localisation de A (resp. A') en S et $i_A^S : a \mapsto a/1$ (resp. $i_{A'}^S : a' \mapsto a'/1$) le morphisme canonique. Soit $h_1 = S^{-1}h : S^{-1}A \mapsto S^{-1}A'$ le morphisme d'anneaux tel que le diagramme*

$$\begin{array}{ccc} A & \xrightarrow{h} & A' \\ {\scriptstyle i_A^S}\downarrow & & \downarrow{\scriptstyle i_{A'}^S} \\ S^{-1}A & \xrightarrow[h_1]{} & S^{-1}A' \end{array} \tag{5.2}$$

commute.

Alors :
i. L'application $\mathfrak{q} \mapsto (i_A^S)^{-1}(\mathfrak{q})$ est une bijection de l'ensemble des idéaux premiers de $S^{-1}A$ sur l'ensemble des idéaux premiers de A ne rencontrant pas S ; l'application réciproque est $\mathfrak{p} \mapsto \mathfrak{p}(S^{-1}A)$
ii. Soit $\mathfrak{p}$ un idéal premier de A tel que $\mathfrak{p} \cap S = \emptyset$. L'application $\mathfrak{p}' \mapsto S^{-1}\mathfrak{p}'$ est une bijection de l'ensemble des idéaux premiers de A' au-dessus de $\mathfrak{p}$ sur l'ensemble des idéaux premiers de $S^{-1}A'$ au-dessus de $S^{-1}\mathfrak{p}$.

La proposition suivante affine le relèvement des idéaux premiers.

Proposition 5.2.6. *Soient $h : A \to A'$ un homorphisme d'anneaux tel que A' est entier sur A, $\mathfrak{p}'$ un idéal premier de A', et $\mathfrak{p} = h^{-1}(\mathfrak{p}')$. Pour que $\mathfrak{p}$ soit maximal il faut et il suffit que $\mathfrak{p}'$ le soit.*

Démonstration. Posons $B = A/\mathfrak{p}, B' = A'/\mathfrak{p}'$ et soit $h_1 : B \to B'$ l'homomorphisme déduit de h par passage aux quotients. Les anneaux B et B' sont intègres et B' est entier sur B. Dire que $\mathfrak{p}$ (resp. $\mathfrak{p}'$) est maximal signifie que B (resp. B') est un corps. La proposition résulte donc du lemme suivant.

Lemme 5.2.7. *Soient B un anneau intègre, A un sous-anneau de B tel que B est entier sur A. Pour que B soit un corps, il faut et il suffit que A soit un corps.*

□

Corollaire 5.2.8. *Soient $h : A \to A'$ un morphisme d'anneaux tel que A' est entier sur A, $\mathfrak{p}$ un idéal premier de A, $\mathfrak{p}'$ et $\mathfrak{a}'$ deux idéaux de A' au-dessus de $\mathfrak{p}$ tels que $\mathfrak{p}' \subset \mathfrak{a}'$. Si $\mathfrak{p}'$ est premier, on a $\mathfrak{a}' = \mathfrak{p}'$.*

Nous allons maintenant énoncer un théorème d'existence.

Théorème 5.2.9. *Soient $h : A \to A'$ un homomorphisme injectif d'anneaux tel que A' est entier sur A, et $\mathfrak{p}$ un idéal premier de A. Il existe un idéal premier $\mathfrak{p}'$ de A' au-dessus de $\mathfrak{p}$.*

Démonstration. Traitons d'abord le cas particulier des anneaux locaux :
Supposons que A est un anneau local. Puisque l'anneau nul n'est pas local et que A' contient A, l'anneau A' n'est pas nul et par conséquent il admet au moins un idéal maximal. Soit $\mathfrak{p}$ l'unique idéal maximal de l'anneau local A. D'après la proposition 5.2.6, pour tout idéal maximal $\mathfrak{m}'$ de A' l'idéal $h^{-1}(\mathfrak{m}')$ est maximal, donc égal à $\mathfrak{p}$.

Maintenant, nos traitons le cas général :
Posons $S = A - \mathfrak{p}$. L'anneau des fractions $S^{-1}A$ est un anneau local et son idéal maximal est $S^{-1}\mathfrak{p}$. Le morphisme d'anneaux

$$\begin{array}{rccc} h_1 : & S^{-1}A & \to & S^{-1}A' \\ & a/s & \mapsto & h(a)/s \end{array}$$

est injectif, et $S^{-1}A'$ est entier sur $S^{-1}A$. D'après le cas particulier, il existe un idéal premier $\mathfrak{q}'$ de $S^{-1}A'$ au-dessus de $S^{-1}\mathfrak{p}$. Le (ii) du lemme 5.2.5 nous permet de conclure. □

Corollaire 5.2.10. *Avec les hypothèses et notations du théorème* 5.2.9*, on a : $h^{-1}(\mathfrak{p}A') = \mathfrak{p}$.*

Démonstration. D'une part on a $\mathfrak{p} \subset h^{-1}(h(\mathfrak{p})) \subset h^{-1}(h(\mathfrak{p})A') = h^{-1}(\mathfrak{p}A')$.
Par ailleurs la remarque 5.2.3 implique que $\mathfrak{p}A' \subset \mathfrak{p}'$. Donc $h^{-1}(\mathfrak{p}A') \subset h^{-1}(\mathfrak{p}') = \mathfrak{p}$. □

Nous clôturons cette section par le théorème suivant, qui est une conséquence du théorème de structure des anneaux d'Artin.

Théorème 5.2.11. *Soient A un anneau d'Artin, k un entier positif tel que $nil(A)^k$ est l'idéal nul et $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_d$ les idéaux maximaux de A. Alors pour tout $1 \leq i \leq d$ on a $A/\mathfrak{m}_i^k \cong A_{\mathfrak{m}_i}$ et A est isomorphe au produit direct $\prod_{i=1}^{d} A_{\mathfrak{m}_i}$.*

Démonstration. Commençons par montrer que pour tout i, le nilradical de $A_{\mathfrak{m}_i}$ vérifie

$$nil(A_{\mathfrak{m}_i})^k = 0.$$

En effet, pour tout $j \neq i$ il existe $m_j \in \mathfrak{m}_j$ tel que $m_j \notin \mathfrak{m}_i$. Et puisque $\mathfrak{m}_i$ est un idéal premier, on a $m_j^k \notin \mathfrak{m}_i$ pour tout $j \neq i$. Donc

$$b = \prod_{j \neq i} m_j^k \notin \mathfrak{m}_i, \tag{5.3}$$

mais $b \in \prod_{j \neq i} \mathfrak{m}_j^k$.

Tout élément $x \in nil(A_{\mathfrak{m}_i})^k = \mathfrak{m}_i^k A_{\mathfrak{m}_i}$ est de la forme $x = \frac{m_i}{s}$ avec $m_i \in \mathfrak{m}_i^k$ et $s \notin \mathfrak{m}_i$.

Donc pour tout $x = \frac{m_i}{s} \in nil(A_{\mathfrak{m}_i})^k$, on a $\frac{m_i}{s} = \frac{0}{1}$ car

$$b = \prod_{j \neq i} m_j^k \notin \mathfrak{m}_i \quad \text{et} \quad bm_i \in \prod_{i=1}^{m} \mathfrak{m}_i^k = nil(A)^k = (0).$$

Donc pour tout i, on a $nil(A_{\mathfrak{m}_i})^k = (0)$.

Montrons que $A/\mathfrak{m}_i^k \cong A_{\mathfrak{m}_i}$ pour tout i.
L'application canonique

$$\begin{array}{rccc} \rho_i : & A & \to & A/\mathfrak{m}_i^k \\ & a & \mapsto & a \bmod \mathfrak{m}_i^k \end{array}$$

est un épimorphisme d'anneaux. Tout $s \notin \mathfrak{m}_i$ est tel que son image $\rho_i(s)$ n'appartient pas à $\mathfrak{m}_i/\mathfrak{m}_i^k$ l'unique idéal maximal de $A/\mathfrak{m}_i^k$, c'est-à-dire que $\rho_i(s)$ est inversible dans $A/\mathfrak{m}_i^k$. D'après la propriété universelle définissant la localisation, il existe un unique morphisme d'anneaux $\widetilde{\rho_i}$ rendant le diagramme suivant commutatif

$$\begin{array}{ccc} A & \xrightarrow{\rho_i} & A/\mathfrak{m}_i^k \\ {\scriptstyle i_A^{\mathfrak{m}_i}}\downarrow & \nearrow_{\widetilde{\rho_i}} & \\ A_{\mathfrak{m}_i}. & & \end{array} \tag{5.4}$$

Le morphisme $\widetilde{\rho_i}$ est défini par

$$\widetilde{\rho_i}(\frac{a}{s}) = \rho_i(a) \times \rho_i(s)^{-1} = (a + \mathfrak{m}_i^k)(s + \mathfrak{m}_i^k)^{-1}. \tag{5.5}$$

Soit $s' \in A$ tel que $(s+\mathfrak{m}_i^k)^{-1} = s'+\mathfrak{m}_i^k$. Alors $\widetilde{\rho_i}(\frac{a}{s}) = (a+\mathfrak{m}_i^k)(s'+\mathfrak{m}_i^k)$ avec $(s+\mathfrak{m}_i^k)(s'+\mathfrak{m}_i^k) = 1 + \mathfrak{m}_i^k$.

Par construction $\widetilde{\rho_i}$ est surjectif.

Et si $\frac{a}{s} \in A_{\mathfrak{m}_i}$ est tel que $\widetilde{\rho_i}(\frac{a}{s}) = 0 \bmod \mathfrak{m}_i^k$ alors $(a + \mathfrak{m}_i^k)(s' + \mathfrak{m}_i^k) = \mathfrak{m}_i^k$ avec $(s + \mathfrak{m}_i^k)(s' + \mathfrak{m}_i^k) = 1 + \mathfrak{m}_i^k$.

Autrement dit : $as' + \mathfrak{m}_i^k = \mathfrak{m}_i^k$ et $ss' + \mathfrak{m}_i^k = 1 + \mathfrak{m}_i^k$.
Donc $as' \in \mathfrak{m}_i^k$ et il existe $b \in \mathfrak{m}_i^k$ tel que $1 = ss' + b$. Ainsi $a = ass' + ab \in \mathfrak{m}_i^k$, et $\frac{a}{s} \in \mathfrak{m}_i^k A_{\mathfrak{m}_i} = nil(A_{\mathfrak{m}_i})^k = (0)$.

Par conséquent $\widetilde{\rho_i}$ est injectif.

D'après le théorème 5.1.7 (théorème structure des anneax d'Artin), l'anneau A est isomorphe au produit direct $\prod_{i=1}^{d} A/\mathfrak{m}_i^k$ et puisque $\widetilde{\rho_i}$ est un isomorphisme, A est isomorphe à $\prod_{i=1}^{d} A_{\mathfrak{m}_i}$.

□

5.2.2 Action d'un groupe sur un anneau : groupe de décomposition et groupe d'inertie

Soient $\mathbf{K}$ un anneau, $\mathbf{A}$ une $\mathbf{K}$-algèbre et $\mathcal{G}$ un groupe opérant sur $\mathbf{A}$. On note $\mathbf{A}^{\mathcal{G}}$ l'ensemble des éléments de $\mathbf{A}$ invariants par $\mathcal{G}$; il est clair que c'est une sous-$\mathbf{K}$-algèbre de $\mathbf{A}$.
Nous dirons que $\mathcal{G}$ est un groupe d'opérateurs localement fini sur $\mathbf{A}$ si toute orbite de $\mathcal{G}$ dans $\mathbf{A}$ est finie.

Proposition 5.2.12. *[[7], page 29] Soit $\mathcal{G}$ un groupe d'opérateurs localement fini sur $\mathbf{A}$, alors $\mathbf{A}$ est entière sur la sous-algèbre $\mathbf{A}^{\mathcal{G}}$.*

Définition 5.2.13. *Si A' est un anneau et $\mathcal{G}$ un groupe opérant sur A'. Étant donné un idéal premier $\mathfrak{p}'$ de A', on appelle groupe de décomposition de $\mathfrak{p}'$ (par rapport à $\mathcal{G}$) et on note $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$, le sous-groupe des éléments $\sigma \in \mathcal{G}$ tels que $\sigma(\mathfrak{p}') = \mathfrak{p}'$.*
L'anneau $A^{\mathbf{Z}}(\mathfrak{p}')$, des éléments de A' invariants par $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$, est l'anneau de décomposition de $\mathfrak{p}'$.

Pour tout $\sigma \in \mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$, nous désignerons encore par $z \mapsto \sigma(z)$ l'endomorphisme de l'anneau $A'/\mathfrak{p}'$ déduit de l'endomorphisme $x \mapsto \sigma(x)$ de A' en passant aux quotients. Il est clair que le groupe $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$ opère sur l'anneau $A'/\mathfrak{p}'$.

Définition 5.2.14. *Avec les notations de la définition* 5.2.13*, le sous-groupe de $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$ formé des σ tels que l'endomorphisme $z \mapsto \sigma(z)$ de $A'/\mathfrak{p}'$ soit l'identité, est le groupe d'inertie de $\mathfrak{p}'$ (par rapport à $\mathcal{G}$) et se note $\mathcal{G}^{\mathbf{T}}(\mathfrak{p}')$.*
L'anneau $A^{\mathbf{T}}(\mathfrak{p}')$ des éléments de A' invariants par $\mathcal{G}^{\mathbf{T}}(\mathfrak{p}')$ est l'anneau de d'inertie de $\mathfrak{p}'$.

Si A est le sous-anneau de A' formé des invariants de $\mathcal{G}$, il est clair que l'on a

$$A \subset A^{\mathbf{Z}}(\mathfrak{p}') \subset A^{\mathbf{T}}(\mathfrak{p}') \subset A'.$$

Il résulte des définitions 5.2.13 et 5.2.14 que pour tout $\rho \in \mathcal{G}$, on a

$$\mathcal{G}^{\mathbf{Z}}(\rho(\mathfrak{p}')) = \rho\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')\rho^{-1}, \mathcal{G}^{\mathbf{T}}(\rho(\mathfrak{p}')) = \rho\mathcal{G}^{\mathbf{T}}(\mathfrak{p}')\rho^{-1}$$

Si, pour tout $\sigma \in \mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$, $\overline{\sigma}$ est l'automorphisme $z \mapsto \sigma(z)$ de $A'/\mathfrak{p}'$, alors $\sigma \mapsto \overline{\sigma}$ est un morphisme canonique de $\mathcal{G}^{\mathbf{Z}}$ dans le groupe Γ_0 des automorphismes de $A'/\mathfrak{p}'$ laisant invariants les éléments de $A^{\mathbf{Z}}/(\mathfrak{p}' \cap A^{\mathbf{Z}})$. Par définition $\mathcal{G}^{\mathbf{T}}(\mathfrak{p}')$ est le noyau de ce morphisme, il s'agit donc d'un sous-groupe distingué de $\mathcal{G}^{\mathbf{Z}}$. Si $\mathbf{K}'$ est le corps des fractions de $A'/\mathfrak{p}'$, tout automorphisme de $A'/\mathfrak{p}'$ se prolonge d'une seule manière en un automorphisme de $\mathbf{K}'$, si bien que l'on peut aussi considérer $\sigma \mapsto \overline{\sigma}$ comme un morphisme de $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$ dans le groupe des automorphismes de $\mathbf{K}'$. On notera enfin que $A^{\mathbf{T}}$ est stable pour $\mathcal{G}^{\mathbf{Z}}$, car $\mathcal{G}^{\mathbf{T}}$ est distingué dans $\mathcal{G}^{\mathbf{Z}}$.

Théorème 5.2.15 ([7] page 38)**.** *Soient A' un anneau, $\mathcal{G}$ un groupe fini opérant sur A' et A l'anneau des invariants de $\mathcal{G}$ de sorte que A' est entière sur A (proposition* 5.2.12*).*

(i) Étant donnés deux idéaux premiers $\mathfrak{p}'$ et $\mathfrak{q}'$ de A' au-dessus d'un même idéal premier $\mathfrak{p}$ de A, il existe $\sigma \in \mathcal{G}$ tel que $\mathfrak{q}' = \sigma(\mathfrak{p}')$. Autrement dit, le groupe $\mathcal{G}$ opère transitivement dans l'ensemble des idéaux premiers de A' au-dessus de $\mathfrak{p}$.

(ii) Soient $\mathfrak{p}'$ un idéal premier de A', $\mathfrak{p} = \mathfrak{p}' \cap A$, $\mathbf{K}$ (resp. $\mathbf{K}'$) le corps des fractions de $A/\mathfrak{p}$ (resp. $A'/\mathfrak{p}'$). Alors $\mathbf{K}'$ est une extension normale de $\mathbf{K}$, et le morphisme canonique $\sigma \mapsto \overline{\sigma}$ de $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')$ dans le groupe Γ des $\mathbf{K}$-automorphismes de $\mathbf{K}'$ définit , par passage au quotient, un isomorphisme de $\mathcal{G}^{\mathbf{Z}}(\mathfrak{p}')/\mathcal{G}^{\mathbf{T}}(\mathfrak{p}')$ sur Γ.

5.3 Schémas et algèbres étales

Nous allons faire un peu de théorie des schémas pour nous armer afin de bien définir ce qu'est une algèbre étale. Les définitions et propriétés énoncées ici sont reprises de [24].

5.3.1 Morphismes étales de schémas

Soit A un anneau (commutatif unitaire), le *spectre* de A, noté Spec A, est l'ensemble de tous les idéaux premiers de A. Par convention, l'anneau A lui-même n'est pas considéré comme un idéal premier. On a donc Spec $\{(0)\} = \emptyset$.

L'énoncé suivant est une version faible du théorème des zéros de Hilbert.

Théorème 5.3.1. *Soit $\mathbf{K}$ un corps algébriquement clos. Alors l'application $(a_1, \ldots, a_n) \mapsto (x_1 - a_1, \ldots, x_n - a_n)$ est une bijection de l'espace affine $\mathbb{A}^n$ de dimension n sur l'ensemble des idéaux maximaux de l'anneau $\mathbf{K}[x_1, \ldots, x_n]$.*

Les points de l'espace $\mathbb{A}^n$ correspondent donc aux idéaux maximaux de $\mathbf{K}[x_1, \ldots, x_n]$. Cela suggère une généralisation de la géométrie algébrique de $\mathbb{A}^n$ à l'ensemble $Max(A)$ des idéaux maximaux d'un anneau arbitraire A, où les idéaux maximaux sont assimilés aux points de notre espace. L'idée en théorie des schémas est d'élargir cette notion de point en incluant les idéaux premiers de A.

Si A est un anneau. La *topologie de Zariski sur* Spec A est celle dont les fermés sont les ensembles de la forme $V(I) = \{\mathfrak{p} \in \text{Spec } A : I \subset \mathfrak{p}\}$, où I est un idéal de A. Soit $f \in A$, on pose $D(f) = \text{Spec } A \setminus V(f)$. Un ensemble ouvert de la forme $D(f)$ est dit *ouvert principal* et son complémentaire $V(f)$ est appelé *fermé principal*.

Une façon de définir les schémas consiste à les considérer comme des espaces topologiques annelés identifiés localement aux schémas affines. Avant de donner les définitions des espaces topologiques annelés et des schémas affines, nous rappellons brièvement quelques points de la théorie des faisceaux.

Définition 5.3.2. *Soit X un espace topologique. Un préfaisceau $\mathcal{F}_X$ d'ensembles sur X est la donnée d'un ensemble $\mathcal{F}_X(U)$, pour chaque ouvert $U \subset X$, et d'une application $\rho_{UV} : \mathcal{F}_X(U) \to \mathcal{F}_X(V)$, pour tout couple d'ouverts (U, V) tels que $V \subset U$, vérifiant les conditions suivantes :*

1. *ρ_{UU} est l'application identité pour tout U ;*
2. *Étant donnés trois ouverts $W \subset V \subset U$, on a $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.*

Un élément $s \in \mathcal{F}_X(U)$ est une section de $\mathcal{F}$ sur U ; les applications ρ_{UV} sont appelées applications de restriction.

Si les ensembles $\mathcal{F}_X(U)$ ont une structure plus riche, par exemple s'il s'agit de groupes (resp. d'anneaux), on dit que $\mathcal{F}_X$ est un préfaisceau de groupes (resp. d'anneaux). Dans ce cas, on exige que les applications de restriction soient des morphismes de groupes (resp. d'anneaux). La condition 1 de la définiton 5.3.2 doit également être modifiée en $\mathcal{F}_X(\emptyset)$ est le groupe trivial (resp. l'anneau nul).

Définition 5.3.3. *Soit $\mathcal{F}_X$ un préfaisceau. On dit que $\mathcal{F}_X$ est un faisceau si les deux conditions suivantes (identité et recollement) sont satisfaites pour tout recouvrement $(U_\lambda)_{\lambda\in\Lambda}$ de l'ouvert*
$U = \bigcup_{\lambda\in\Lambda} U_\lambda$:
On pose $U_{\lambda\mu} = U_\lambda \cap U_\mu$, $\rho_\lambda = \rho_{UU_\lambda}$ et $\rho_{\lambda\mu} = \rho_{U_\lambda U_{\lambda\mu}}$.

1. *Identité : Pour tout $f, g \in \mathcal{F}_X(U)$, si $\rho_\lambda(f) = \rho_\lambda(g)$ pour tout $\lambda \in \Lambda$ alors $f = g$.*
2. *Recollement : étant données des sections $f_\lambda \in \mathcal{F}_X(U_\lambda)$ telles que $\rho_{\lambda\mu}(f_\lambda) = \rho_{\mu\lambda}(f_\mu)$ pour tout $\lambda, \mu \in \Lambda$, il existe $f \in \mathcal{F}_X(U)$ tel que $f_\lambda = \rho_\lambda(f)$ pour tout λ.*

La définition 5.3.3 précise qu'un préfaisceau $\mathcal{F}_X$ est un faisceau si et seulement si chaque $\mathcal{F}_X(U)$ peut être complètement reconstruit à partir des informations locales. En effet, cette définition revient à dire que pour tout recouvrement ouvert $U = \bigcup_{\lambda\in\Lambda} U_\lambda$, on a

$$\mathcal{F}_X(U) \cong \{\{f_\lambda\}_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} \mathcal{F}_{U_\lambda} : \rho_{\lambda\mu}(f_\lambda) = \rho_{\mu\lambda}(f_\mu) \text{ pour tout } \lambda, \mu \in \Lambda\}.$$

Remarque 5.3.4. *Soit $\mathcal{B}$ une base d'ouverts de l'espace topologique X (i.e $\mathcal{B}$ est un ensemble d'ouverts de X, tout ouvert de X est réunion d'éléments de $\mathcal{B}$ et $\mathcal{B}$ est stable par intersection finie). On peut définir les notions de $\mathcal{B}$-préfaisceau et de $\mathcal{B}$-faisceau en remplaçant les ouverts U de X par les ouverts de $\mathcal{B}$ dans les définitions précédentes. Ainsi tout $\mathcal{B}$-faisceau $\mathcal{F}_0$ sétend de manière unique (à isomorphisme près pour être précis) à un faisceau $\mathcal{F}_X$ sur X. En effet, tout ouvert U de X est la réunion d'une famille d'ouverts U_i de $\mathcal{B}$. Dans ce cas, $\mathcal{F}_X(U)$ est l'ensemble des éléments $(s_i)_i \in \prod_i \mathcal{F}_0(U_i)$ tel que $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$. En d'autres termes, un faisceau est complètement déterminé par ses sections sur une base d'ouverts.*

Nous avons défini à la sous-section précédente, définition 5.2.4, la localisation $S^{-1}A = A_S$ d'un anneau A par rapport à une partie multiplicative S. Les anneaux A_{S_i} où $S_1 = \{1, f, f^2, \ldots\}$ avec $f \in A \setminus \sqrt{(0)}$, et $S_2 = A \setminus \mathfrak{p}$ pour $\mathfrak{p} \in \text{Spec } A$ sont des exemples intéressants de localisation de l'anneau A. On pose $A_{S_1} = A_f$ et $A_{S_2} = A_{\mathfrak{p}}$.

Le morphisme canonique $\sigma : A \to A_S$ induit une application entre spectres :

$$\begin{array}{rccc} \sigma^* : & \text{Spec } A_S & \to & \text{Spec } A \\ & \mathfrak{p} & \mapsto & \sigma^{-1}(\mathfrak{p}). \end{array} \tag{5.6}$$

Le (i) du lemme 5.2.5 nous dit que σ^* est une bijection de Spec A_S sur $\{\mathfrak{p} \in \text{Spec } A : \mathfrak{p} \cap S = \emptyset\}$. Donc si $S = \{1, f, f^2, \ldots\}$, pour $f \in A \setminus \sqrt{(0)}$, alors σ^* induit une bijection de entre Spec A_f et $D(f) = (\text{Spec } A) \setminus V(f)$.

Remarque 5.3.5. *Soient $I \subset A$ un idéal de A et $\{f_\lambda\}_{\lambda \in \Lambda}$ un ensemble de générateurs de I. Soit $\mathfrak{p} \in$ Spec A. Alors $I \subset \mathfrak{p}$ si et seulement si $f_\lambda \in \mathfrak{p}$ pour tout $\lambda \in \Lambda$.*

On a Spec $A \setminus V(I) = \{\mathfrak{p} \in \text{Spec } A : I \nsubseteq \mathfrak{p}\} = \{\mathfrak{p} \in \text{Spec } A :$ *il existe* $\lambda \in \Lambda, f_\lambda \notin \mathfrak{p}\} = \bigcup_{\lambda \in \Lambda}(D(f_\lambda))$.

Ainsi l'ouvert Spec $A \setminus V(I)$ *est la réunion des ouverts $D(f_\lambda)$. Puisque l'idéal I est arbitraire, la famille $\{D(f) | f \in A\}$ des ouverts principaux est une base d'ouverts pour la topologie de Zariski sur* Spec A.

Nous donnons dans la suite une interprétation de la localisation en termes de limites inductives.

Définition 5.3.6. *Soient $\mathcal{R}$ une relation d'ordre partielle et Λ un ensemble partiellement ordonné (par $\mathcal{R}$) filtrant (à droite), autrement dit :*

$$\textit{Pour tout } \lambda, \mu \in \Lambda, \textit{ il existe } \nu \in \Lambda \textit{ tel que } \lambda \mathcal{R} \nu \textit{ et } \mu \mathcal{R} \nu.$$

Soit $\{A_\lambda\}_{\lambda \in \Lambda}$ une famille d'ensembles. Supposons que pour tout $\lambda, \mu \in \Lambda$ avec $\lambda \mathcal{R} \mu$, il existe une application $\Phi_{\lambda\mu} : A_\lambda \to A_\mu$ telle que $\Phi_{\lambda\lambda} = Id_{A_\lambda}$ pour tout $\lambda \in \Lambda$ et $\Phi_{\mu\nu} \circ \Phi_{\lambda\mu} = \Phi_{\lambda\nu}$ pour tous $\lambda, \mu, \nu \in \Lambda$ tel que $\lambda \mathcal{R} \mu$ et $\mu \mathcal{R} \nu$. Dans ce cas, on dit que la famille $\{A_\lambda\}_{\lambda \in \Lambda}$ est un système inductif (ou système direct).

La limite inductive $\lim_{\overrightarrow{\lambda \in \Lambda}} A_\lambda$ d'un système inductif $\{A_\lambda\}_{\lambda \in \Lambda}$ est définie par :
$$\lim_{\overrightarrow{\lambda \in \Lambda}} A_\lambda = \amalg_{\lambda \in \Lambda} A_\lambda / \sim,$$

où $\sim$ est la relation d'équivalence suivante :
Étant donné $(x_\lambda, x_\mu) \in A_\lambda \times A_\mu$, on dit que $x_\lambda \sim x_\mu$ s'il existe $\nu \in \Lambda$ tel que $\lambda \mathcal{R} \nu, \mu \mathcal{R} \nu$ et $\Phi_{\mu\nu}(x_\mu) = \Phi_{\lambda\nu}(x_\lambda)$.

La limite inductive A d'un système inductif $\{A_\lambda\}_{\lambda \in \Lambda}$ est caractŕeisée par la propriété universelle suivante.

Propriété universelle : *Il existe des applications $\Phi_\lambda : A_\lambda \to A$ compatibles avec tous les $\Phi_{\lambda\mu}$ de la définition précédente. De plus, si A' est un autre ensemble et $\Phi'_\lambda : A_\lambda \to A'$ une famille d'applications compatibles avec tous les $\Phi_{\lambda\mu}$ alors il existe une unique application $\Psi : A \to A'$, compatible avec tous les Φ_λ et Φ'_λ.*

Remarque 5.3.7. *En fait, on peut définir la limite inductive d'un système à partir de cette proporiété universelle. Pour cela on dit qu'une limite inductive du système $\{A_\lambda\}_{\lambda\in\Lambda}$ est un couple $(A', (\Phi'_\lambda)_{\lambda\in\Lambda})$ vérifiant la propriété universelle. Ensuite, on remarque que deux limites inductives $(A', (\Phi'_\lambda)_{\lambda\in\Lambda})$ et $(A'', (\Phi''_\lambda)_{\lambda\in\Lambda})$ (au sens qu'elles vérifient la propriété universelle) sont nécessairement telles que A' est en bijection avec A''. La limitee inductive du système $\{A_\lambda\}_{\lambda\in\Lambda}$ est l'un des couples vérifiant la propriété universelle : on dit que la limite inductive d'un système inductif est unique à isomorphiseme près.*
Si les ensembles A_λ sont munis d'une structure supplémentaire (s'il s'agit par exemple de groupes ou d'anneaux), cette structure s'étend, en général, de façon évidente à la limite inductive.

Regardons comment se traduisent les notions de système inductif et de limite inductive dans le cadre des systèmes inductifs d'anneaux de fractions.

Exemple 5.3.8. *Soient A un anneau et S un ensemble multiplicatif de A. On définit un ordre partiel sur S en disant que les éléments $f, g \in S$ sont tels que $f \leq g$ s'il existe $f_1 \in S$ tel que $g = ff_1$. Donc S est un ensemble filtrant, car pour $f, g \in A$ on a $f \leq fg$ et $g \leq fg$. Les localisés A_f, pour f parcourant S, forment un système inductif d'anneaux. En effet, si f et g sont dans S tels que $f \leq g$ alors il existe $f_1 \in S$ tel que $g = ff_1$. L'application*

$$\begin{array}{rccc} \Phi_{fg} : & A_f & \to & A_g \\ & \frac{a}{f^n} & \mapsto & \frac{af_1^n}{g^n} \end{array} \tag{5.7}$$

est un morphisme d'anneaux, et $\Phi_{ff} = Id_{A_f}$. Si f, g et h sont des éléments de S tels que $f \leq g \leq h$ alors $\Phi_{gh} \circ \Phi_{fg} = \Phi_{fh}$.

D'autre part, pour tout $f \in S$, les morphismes d'anneaux

$$\begin{array}{rccc} \Phi_f : & A_f & \to & A_S \\ & \frac{a}{f^n} & \mapsto & \frac{a}{f^n} \end{array} \tag{5.8}$$

sont compatibles avec tous les Φ_{fg}. Et si B est un anneau, puis $\varphi_f : A_f \to B$ une famille de morphismes d'anneaux compatibles avec tous les Φ_{fg}, alors l'application

$$\begin{array}{rccc} \Psi : & A_S & \to & B \\ & \frac{a_1}{s_1} & \mapsto & \varphi_{s_1}(\frac{a_1}{s_1}) \end{array} \tag{5.9}$$

est l'unique morphisme d'anneaux de A_S dans B compatible avec tous les Φ_f et φ_f pour $f \in S$. Donc A_S est la limite inductive du système $\{A_f\}_{f\in S}$ (remarque 5.3.7).

Plus généralement, soient X est un espace topologique, $\mathcal{F}_X$ un préfaisceau d'ensembles sur X et x un point de X. L'ensemble O_x des ouverts de X contenant x est filtrant pour la relation d'ordre partiel suivante :

Si $U, V \in O_x$ alors $U\mathcal{R}V$ si et seulement si U contient V.
Et la famille $\{\mathcal{F}_U\}_{U\in O_x}$ est un système inductif.

Définition 5.3.9. *La fibre $\mathcal{F}_{X,x}$ de $\mathcal{F}_X$ en x est donnée par*

$$\mathcal{F}_{X,x} = \varinjlim_{U\in O_x} \mathcal{F}_X(U).$$

Si U un ouvert de X contenant x et $f \in \mathcal{F}_X(U)$ une section de $\mathcal{F}_X$ sur U, alors l'image (par $\Phi_U : \mathcal{F}_X(U) \to \mathcal{F}_{X,x}$) de f, que nous noterons f_x dans la suite, est appelée le germe de f en x.

Si $\mathcal{F}_X$ et $\mathcal{G}_X$ sont deux préfaisceaux d'ensembles sur X. Un *morphisme de préfaisceaux* $\alpha : \mathcal{F}_X \to \mathcal{G}_X$ est la donnée d'une famille d'applications $\alpha(U) : \mathcal{F}_X(U) \to \mathcal{G}_X(U)$, pour tout ouvert U, compatibles avec les applications de restriction ρ_{UV}. Pour tout $x \in X$, α induit canoniquement une application $\alpha_x : \mathcal{F}_{X,x} \to \mathcal{G}_{X,x}$ telle que $(\alpha(U)(s))_x = \alpha_x(s_x)$ pour tout ouvert $U \in O_x$ et toute section $s \in \mathcal{F}_X(U)$.

Définition 5.3.10. *Un espace topologique annelé est un espace topologique X muni d'un faisceau d'anneaux $\mathcal{F}_X$ sur X tel que $\mathcal{F}_{X,x}$ est un anneau local pour tout $x \in X$. Si $\mathfrak{m}_x$ est l'idéal maximal de $\mathcal{F}_{X,x}$, le quotient $\mathcal{F}_{X,x}/\mathfrak{m}_x$ est le corps résiduel de X en x que l'on note $k(x)$.*

Un morphisme d'espaces topologiques annelés

$$(f, f^{\#}) : (X, \mathcal{F}_X) \to (Y, \mathcal{F}_Y)$$

consiste en une application continue $f : X \to Y$ et un morphisme de faisceaux d'anneaux $f^{\#} : \mathcal{F}_Y \to f_*\mathcal{F}_X$ tel que pour tout $x \in X$, la fibre $f_x^{\#} : \mathcal{F}_{Y,f(x)} \to \mathcal{F}_{X,x}$ est un morphisme local (i.e $f_x^{\#-1}(\mathfrak{m}_x) = \mathfrak{m}_{f(x)}$ ou alors $f_x^{\#}(\mathfrak{m}_{f(x)}) \subset \mathfrak{m}_x$).

Soit A un anneau. Considérons l'espace $X = \text{Spec } A$ muni de sa topologie Zariski. Nous allons construire un faisceau d'anneaux $\mathcal{F}_X$ sur X.

On a vu juste après la remarque 5.3.4 que $D(f) \cong \text{Spec } A_f$. On pose $\mathcal{F}_X(D(f)) = A_f$, cet anneau ne dépend pas du choix du générateur f de l'idéal $(f) \subset A$ [[24], sous-section 2.3.1]. On obtient ainsi un $\mathcal{B}$-préfaisceau (remarque 5.3.4), où $\mathcal{B}$ est la base d'ouverts de X formée des ouverts principaux $D(f)$ avec $f \in A$.

Proposition 5.3.11. *Soit A un anneau et $X = \text{Spec } A$. On a les propriétés suivantes.*

(a) $\mathcal{F}_X$ est un $\mathcal{B}$-faisceau d'anneaux. Il induit donc un faisceau d'anneaux sur X, que nous notons encore $\mathcal{F}_X$, et on a $\mathcal{F}_X(X) = A$.

(b) Pour tout $\mathfrak{p} \in X$, la fibre $\mathcal{F}_{X,\mathfrak{p}}$ est canoniquement isomorphe à $A_{\mathfrak{p}}$. En particulier $(X, \mathcal{F}_X)$ est un espace topologique annelé.

Le deuxième point de cette proposition est immédiat. En effet, la fibre de $\mathcal{F}_X$ en $\mathfrak{p}$ est donnée par

$$\mathcal{F}_{X,\mathfrak{p}} = \varinjlim_{U \in O_\mathfrak{p}} \mathcal{F}_X(U) = \varinjlim_{D(f) \in O_\mathfrak{p}} \mathcal{F}_X(D(f)) = \varinjlim_{f \notin \mathfrak{p}} A_f = A_\mathfrak{p}.$$

où $O_\mathfrak{p}$ est l'ensemble des ouverts de X contenant $\mathfrak{p}$.

Définition 5.3.12. *Un schéma affine est une paire* $(\text{Spec } A, \mathcal{F}_{\text{Spec } A})$ *où* A *est un anneau,* Spec A *est muni de sa topologie de Zariski et* $\mathcal{F}_{\text{Spec } A}$ *est le faisceau sur* Spec A *défini à la proposition* 5.3.11. *Par abus de notation, nous désignerons simplement le schéma affine* $(\text{Spec } A, \mathcal{F}_{\text{Spec } A})$ *par* Spec A.

Une variété affine sur un corps $\mathbf{K}$ (selon la définition classique donnée au chapitre 1) est un schéma affine associé à une algèbre de type fini sur $\mathbf{K}$.

Toutes les conditions sont désormais réunies pour définir la notion de schéma.

Définition 5.3.13. *Un schéma est un espace topologique annelé* $(X, \mathcal{F}_X)$ *admettant un recouvrement ouvert* $\{U_i\}_i$ *tel que* $(U_i, \mathcal{F}_X|_{U_i})$ *est un schéma affine pour tout* i. *Nous le noterons simplemennt* X *s'il n'y a pas de confusion. Si* U *est un ouvert de* X, *on dit que* $(U, \mathcal{F}_X|_U)$ *(ou plus simplement* U*) est un sous-schéma ouvert de* X. *On dit que* U *est un ouvert affine si* $(U, \mathcal{F}_X|_U)$ *est un schéma affine.*

Un schéma X *est dit noethérien si* X *est l'union finie d'ouverts affines* X_i *tels que* $\mathcal{F}_X(X_i)$ *est un anneau noethérien pour tout* i.
On dit qu'un schéma X *est localement noethérien si pour tout* $x \in X$ *il existe un ouvert affine* U *contenant* x *tel que* $\mathcal{F}_X(U)$ *est noethérien.*

Un morphisme de schémas $f : X \to Y$ *est un morphisme d'espaces topologiques annelés. Le morphisme* f *est dit fini (resp. de type fini) si* Y *peut être recouvert par des ouverts affines* Spec B_i *tels que la pré-image* $f^{-1}(\text{Spec } B_i)$ *est un ouvert affine (resp. recouverte par un nombre fini d'ouverts affines)* Spec A_i *et le morphisme (resp. chaque morphisme) canonique* $B_i \to A_i$ *définit sur* A_i *une structure de* B_i*-algèbre fini (resp. de type fini).*

Si S *est un shéma, on appelle* S*-schéma où schéma sur* S *la donnée d'un schéma* X *muni d'un morphisme de schémas* $\pi : X \to S$. *Lorsque* $S = \text{Spec}(A)$, *on dit que* X *est un* A*-schéma.*

Les morphismes de variétés affines sont de bons exemples de morphismes de schémas.

Soit A un anneau. Un A-module M est dit *plat* (sur A) si pour tout morphisme injectif de A-modules $f : N \to N'$, le morphisme

$$\begin{array}{ccc} N \otimes M & \to & N' \otimes M \\ \sum x \otimes y & \mapsto & \sum f(x) \otimes y \end{array}$$

est injectif. Une A-algèbre B est dite plate si B est plate sur A pour sa structure de A-module. Dans ce cas, on dit que le morphisme canonique $\rho : A \to B$ définissant la structure de A-module sur B est un morphisme plat.

Les deux propositions suivantes vont nous être très utiles.

Proposition 5.3.14 ([24],P. 7)**.** *Soit A un anneau. Alors*
(a) Tout A-module libre est plat.
(b) Le produit tensoriel de modules plats sur A est plat sur A.

Proposition 5.3.15 ([24],P. 11)**.** *Soit $\rho : A \to B$ un morphisme d'anneaux. Les propriétés suivantes sont équivalentes.*
(i) $\rho : A \to B$ est plat.
(ii) Pour tout idéal premier $\mathfrak{p} \in \text{Spec } B$, la $A_{\rho^{-1}(\mathfrak{p})}$-algèbre $B_{\mathfrak{p}}$ est plate sur $A_{\rho^{-1}(\mathfrak{p})}$.
(iii) Pour tout idéal maximal $\mathfrak{p} \in \text{Spec } B$, la $A_{\rho^{-1}(\mathfrak{p})}$-algèbre $B_{\mathfrak{p}}$ est plate sur $A_{\rho^{-1}(\mathfrak{p})}$.

Nous pouvons à présent définir la notion de morphismes étales de schémas.

Définition 5.3.16 ([24],P. 136 et P. 139)**.** *Soit $f : X \to Y$ un morphisme de schémas. On dit que f est plat en $x \in X$ si le morphisme $f_x^{\#} : \mathcal{F}_{Y,f(x)} \to \mathcal{F}_{X,x}$ est plat. On dit que f est plat si f est plat en tout point de X.*

Soit $f : X \to Y$ un morphisme de type fini de schémas localement noethériens. Soit $x \in X$ et
$y = f(x)$. On dit que f est non-ramifié en x si le morphisme $f_x^{\#} : \mathcal{F}_{Y,y} \to \mathcal{F}_{X,x}$ vérifie $f_x^{\#}(\mathfrak{m}_y)\mathcal{F}_{X,x} = \mathfrak{m}_x$ (en d'autres termes, $\mathcal{F}_{X,x}/f_x^{\#}(\mathfrak{m}_y)\mathcal{F}_{X,x} = k(x)$) et l'extension de corps résiduels $k(y) \to k(x)$ est séparable. On dit que f est étale en x si f est non-ramifié et plat en x.
On dit que f est non-ramifié (resp. étale) si f est non-ramifié (resp. étale) en tout point de X.

5.3.2 Algèbres étales

Nous voulons ici définir la notion d'algèbre étale à partir de ce qui a été dit précédemment au sujet des morphismes étales de schémas. Ensuite nous donnerons une condition nécessaire et suffisante pour qu'une algèbre B sur un anneau A soit étale.

Soient A un anneau et B une A-algèbre libre de rang fini d dont la structure de A-module est définie par le morphisme d'anneaux $\rho : A \to B$. Le morphisme ρ induit un morphisme de schémas

$$\begin{array}{rccc} \rho^* : & \text{Spec } B & \to & \text{Spec } A \\ & \mathfrak{p}_i & \mapsto & \rho^{-1}(\mathfrak{p}_i). \end{array}$$

On dit que B est une *algèbre étale* sur A si le morphisme ρ est étale.

Soit $b \in B$. La "*multiplication par* b", définie par

$$\begin{array}{rccc} m_b : & B & \to & B \\ & x & \mapsto & m_b(x) = bx \end{array}$$

est un endomorphisme A-linéaire.
Pour tout $b \in B$, la trace $\mathrm{Tr}_{B/A}(b)$ de b est égale à la trace $\mathrm{Tr}_{B/A}(m_b)$ de la matrice de m_b dans une A-base de B.

L'application

$$\begin{array}{rccc} \mathrm{Tr}_{B/A} : & B \times B & \to & A \\ & (x, y) & \mapsto & \mathrm{Tr}_{B/A}(xy) \end{array}$$

est une forme bilinéaire symmétrique. On associe à $\mathrm{Tr}_{B/A}$ une matrice M donnée par

$$M = (\mathrm{Tr}_{B/A}(\omega_i \omega_j))_{1 \leq i,j \leq d}$$

où $(\omega_i)_{1 \leq i \leq d}$ une base de B sur A.

Une grande partie du chapitre 2 concerne les discriminants des corps quadratiques imaginaires et les discriminants des ordres de ces corps. Nous donnons ici, et en toute généralité la définition de cette notion de discriminant.

Définition 5.3.17. *Soient B un anneau et A un sous-anneau de B tel que B est un A-module libre de rang fini n. On appelle discriminant de B sur A, et on note $D_{B/A}$, l'idéal de A engendré par le déterminant de la matrice de la forme $\mathrm{Tr}_{B/A}$ dans n'importe quelle base de B sur A.*

Remarque 5.3.18. *L'anneau des entiers d'un corps de nombres $\mathbf{K}$ est un $\mathbf{Z}$-module libre de rang $[\mathbf{K} : \mathbf{Q}]$ [[27], §7 page 48], et les discriminants des bases de cet anneau (pour sa structure de $\mathbf{Z}$-module) sont tous égaux : leur valeur commune est le discriminant de $\mathbf{K}$.*

Le A-module $\mathrm{Hom}_A(B, A)$ est de même dimension que B. On dit que la forme bilinéaire $\mathrm{Tr}_{B/A}$ est non-dégénérée si l'application linéaire

$$\begin{array}{rccc} \phi : & B & \to & \mathrm{Hom}_A(B, A) \\ & x & \mapsto & \phi(x) = (y \mapsto \mathrm{Tr}_{B/A}(xy) = x^t M y). \end{array}$$

est un isomorphisme ($i.e$ la matrice M est inversible).

Proposition 5.3.19 ([21] 1.4 et exercice 1.3, puis proposition 6.9)**.** *La A-algèbre B est étale si et seulement si la forme $\mathrm{Tr}_{B/A}$ est non dégénée.*

5.3.3 Exemples

Soient $\mathbf{K}$ un corps commutatif et $\mathbf{L}$ une $\mathbf{K}$-algèbre commutative de dimension finie $d \geq 1$ telle que $\mathbf{K} \subset \mathbf{L}$. Le corps $\mathbf{K}$ peut être considéré comme un sous-anneau de $\mathbf{L}$ et on a un morphisme injectif

$$\begin{array}{rccc} f: & \mathbf{K} & \to & \mathbf{L} \\ & k & \mapsto & k. \end{array}$$

D'après la proposition 5.3.14 le morphisme f est plat ($i.e$ $\mathbf{L}$ est plate sur $\mathbf{K}$).

On suppose de plus qu'il existe un $\mathbf{K}$-automorphisme σ de $\mathbf{L}$ et une $\mathbf{K}$-base $(\omega_i)_{i\in\mathbf{Z}/d\mathbf{Z}}$ de $\mathbf{L}$ telle que

$$\sigma(\omega_i) = \omega_{i+1}.$$

Donc $\mathbf{L}$ est un $\mathbf{K}[\mathcal{G}]$-module libre de rang 1 (engendré par exemple par ω_0), où $\mathcal{G} =< \sigma >$ est le groupe cyclique engendré par σ.

L'anneau $\mathbf{L}$ est noethérien car c'est un espace vectoriel de dimension finie sur le corps $\mathbf{K}$. Par ailleurs $\mathbf{K}$ est le sous-anneau $\mathbf{L}^{\mathcal{G}}$ des invariants de $\mathbf{L}$ par σ. D'après la proposition 5.2.12, $\mathbf{L}$ est algébrique sur $\mathbf{K}$. Soit $\mathfrak{p}$ un idéal premier de $\mathbf{L}$. L'intersection $\mathfrak{p} \cap \mathbf{K}$ est un idéal premier de $\mathbf{K}$, donc égal à l'idéal nul (0). Puisque (0) est maximal dans $\mathbf{K}$, la proposition 5.2.6 implique que l'idéal $\mathfrak{p}$ est maximal dans $\mathbf{L}$. Donc $\mathbf{L}$ est un anneau de dimension 0. Mais nous avons vu que $\mathbf{L}$ est noethérien, c'est donc un anneau artinien d'après le théorème 5.1.5.

Les propriétés des anneaux artiniens, de la section 5.1 du présent chapitre, nous permettent d'affirmer que $\mathbf{L}$ n'a qu'un nombre fini d'idéaux premiers : $\mathrm{Spec}\ \mathbf{L} = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\}$ et ils sont tous maximaux. Le nilradical $nil(\mathbf{L}) = \bigcap_{i=1}^m \mathfrak{p}_i = \prod_{i=1}^m \mathfrak{p}_i$ est nilpotent : il existe $k \in \mathbb{N}$ tel que

$$nil(\mathbf{L})^k = \prod_{i=1}^m \mathfrak{p}_i^k = (0). \tag{5.10}$$

Le morphisme f induit un morphisme de schémas $(f^*, f^\#) : \mathrm{Spec}\ \mathbf{L} \to \mathrm{Spec}\ \mathbf{K}$ donné par

$$\begin{array}{rccc} f^*: & \mathrm{Spec}\ \mathbf{L} & \to & \mathrm{Spec}\ \mathbf{K} = \{(0)\} \\ & \mathfrak{p}_i & \mapsto & f^{-1}(\mathfrak{p}_i), \end{array}$$

$$f^\# : \mathcal{F}_{\mathrm{Spec}\ \mathbf{K}} \to \mathcal{F}_{\mathrm{Spec}\ \mathbf{L}}$$

Et pour tout $i = 1, 2, \ldots, m$

$$\begin{array}{rccc} f^\#_{\mathfrak{p}_i}: & \mathbf{K} & \to & \mathbf{L}_{\mathfrak{p}_i} \\ & x & \mapsto & \frac{x}{1}. \end{array} \tag{5.11}$$

Le spectre de $\mathbf{K}$ est réduit à l'idéal nul (0), donc $\mathcal{F}_{\text{Spec }\mathbf{K}}((0)) = \mathbf{K}$, $(f^*)^{-1}(\text{Spec }\mathbf{K}) = \text{Spec }\mathbf{L}$ et $\mathcal{F}_{\text{Spec }\mathbf{L}}(\text{Spec }\mathbf{L}) = \mathbf{L}$. Pour tout $i = 1, 2, \ldots, m$ on a $f^{-1}(\mathfrak{p}_i) = (0)$ et la fibre $\mathcal{F}_{\text{Spec } L,\mathfrak{p}_i} = \mathbf{L}_{\mathfrak{p}_i}$. Le couple $(f^*, f^{\#})$ est un morphisme fini de schémas noethériens affines.

Afin de bien expliciter le morphisme d'anneaux $f^{\#}_{\mathfrak{p}_i}$ de l'équation (5.11), nous allons établir un lien entre les nilradicaux $nil(\mathbf{L})$ et $nil(\mathbf{L}_{\mathfrak{p}_i})$ pour tout i.

Mais avant on fixe une petite définition.

Définition 5.3.20. *Soit I un idéal nilpotent d'un anneau A. L'indice de nilpotence de I est le plus petit entier strictement positif n tel que I^n est l'idéal nul de A.*

Affirmation. Le nilradical $nil(\mathbf{L}_{\mathfrak{p}_i}) = \mathfrak{p}_i\mathbf{L}_{\mathfrak{p}_i}$ est nilpotent de même indice k que $nil(\mathbf{L})$.

En effet, d'après le théorème 5.2.15, le groupe $\mathcal{G} =< \sigma >$ agit transitivement sur $\text{Spec }\mathbf{L} = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m\}$. Donc si $\mathfrak{p}_1, \mathfrak{p}_i \in \text{Spec }\mathbf{L}$ sont deux idéaux premiers de $\mathbf{L}$, alors il existe $r \in \mathbb{N}$ tel que $\sigma^r(\mathfrak{p}_1) = \mathfrak{p}_i$. Le $\mathbf{K}$-automorphisme σ^r de $\mathbf{L}$ induit l'isomorphisme

$$\begin{array}{rccc} \overline{\sigma^r}: & \mathbf{L}/\mathfrak{p}_1^k & \to & \mathbf{L}/\mathfrak{p}_i^k \\ & x \bmod \mathfrak{p}_1^k & \mapsto & \sigma^r(x) \bmod \mathfrak{p}_i^k. \end{array}$$

Puisque pour tout $i \in \{1, 2, \ldots, m\}$ l'anneau $\mathbf{L}/\mathfrak{p}_i^k$ est isomorphe à $\mathbf{L}_{\mathfrak{p}_i}$ (voir preuve du théorème 5.2.11), les anneaux $\mathbf{L}_{\mathfrak{p}_1}$ et $\mathbf{L}_{\mathfrak{p}_i}$ sont isomorphes et leurs nilradicaux ont même indice de nilpotence que nous notons l.

On a vu que $l \leq k$ (preuve du théorème 5.2.11).

Réciproquement, notons

$$\begin{array}{rccc} \psi: & \mathbf{L} & \to & \prod_{i=1}^m \mathbf{L}_{\mathfrak{p}_i} \\ & x & \mapsto & (\widetilde{\rho}_1^{-1}(x \bmod \mathfrak{p}_1^k), \widetilde{\rho}_2^{-1}(x \bmod \mathfrak{p}_2^k), \ldots, \widetilde{\rho}_m^{-1}(x \bmod \mathfrak{p}_2^k)) \end{array}$$

l'isomorphisme donné par le théorème 5.2.11 ($\widetilde{\rho}_i$ est définie dans la preuve du théorème 5.2.11 par l'équation (5.5) et le diagramme commutatif (5.4)).

L'idéal $nil(\mathbf{L})^l$ est engendré par des éléments de la forme

$$x = x_1 x_2 \ldots x_l,$$

où $x_j \in nil(\mathbf{L}) = \bigcap_{i=1}^m \mathfrak{p}_i$ pour $j \in \{1, 2, \ldots, l\}$. Donc chacune des composantes de $\psi(x)$ est nulle car l'indice de nilpotence de chaque $nil(\mathbf{L}_{\mathfrak{p}_i})$ est l.

Donc $x = 0$, par conséquent $nil(\mathbf{L})^l = (0)$ et $k \leq l$.

On obtient finalement que les nilradicaux $nil(\mathbf{L}_{\mathfrak{p}_i})$ sont nilpotents de même indice k que $nil(\mathbf{L})$.

Ainsi pour tout i, la fibre $f^{\#}_{\mathfrak{p}_i} : \mathbf{K} \to \mathbf{L}_{\mathfrak{p}_i}$ est telle que

$$f^{\#}_{\mathfrak{p}_i}(0) = \mathfrak{p}_i^k \mathbf{L}_{\mathfrak{p}_i}. \tag{5.12}$$

D'après la proposition 5.3.15 (iii), la $\mathbf{K}$-algèbre $\mathbf{L}_{\mathfrak{p}_i}$ définie par $f^{\#}_{\mathfrak{p}_i} : \mathbf{K} \to \mathbf{L}_{\mathfrak{p}_i}$ est plate pour tout $i = 1, 2, \ldots, m$. Donc $\mathbf{L}$ est étale sur $\mathbf{K}$ si et seulement pour tout $i \in \{1, 2, \ldots, m\}$ le quotient $\mathbf{L}_{\mathfrak{p}_i}/f^{\#}_{\mathfrak{p}_i}(0) = \mathbf{L}_{\mathfrak{p}_i}/\mathfrak{p}_i^k \mathbf{L}_{\mathfrak{p}_i} \cong \mathbf{L}/(\mathfrak{p}_i)^k$ est un corps ($i.e$ $k = 1$, $\mathbf{L}$ est réduite) et $(\mathbf{L}_{\mathfrak{p}_i}/\mathfrak{p}_i \mathbf{L}_{\mathfrak{p}_i}) \cong \mathbf{L}/\mathfrak{p}_i$ est une extension séparable de $\mathbf{K}$.

Examinons l'action de $\mathcal{G} =< \sigma >$ sur $\mathbf{L}$.

Le groupe $\mathcal{G}$ des $\mathbf{K}$-automorphismes de $\mathbf{L}$ est abélien, donc les groupes de décomposition (resp. d'inertie) des $\mathfrak{p}_i \in \text{Spec } \mathbf{L}$ sont tous égaux. On note $\mathcal{G}^{\mathbf{Z}}$ (resp. $\mathcal{G}^{\mathbf{T}}$) le groupe de décomposition (resp. groupe d'inertie) commun à ces idéaux premiers. Soient $e \geq 1$ l'ordre du groupe d'inertie et f le cardinal du quotient $\mathcal{G}^{\mathbf{Z}}/\mathcal{G}^{\mathbf{T}}$. On a : $d = efm$ et $nil(\mathbf{L}) = \bigcap_{1 \leq i \leq m} \mathfrak{p}_i$. L'application canonique

$$\varphi : \mathbf{L} \to \prod_{1 \leq i \leq m} \mathbf{L}/\mathfrak{p}_i \tag{5.13}$$

est un morphisme surjectif d'anneaux et son noyau est égal au nilradical $nil(\mathbf{L})$. D'après le théorème 5.2.15, le quotient $\mathcal{G}^{\mathbf{Z}}/\mathcal{G}^{\mathbf{T}}$ est isomorphe au groupe des $\mathbf{K}$-automorphismes de $\mathbf{M}_i = \mathbf{L}/\mathfrak{p}_i$ pour tout i, les extensions $\mathbf{M}_i/\mathbf{K}$ sont normales et leur degré séparable est égal à f. Notons r leur degré inséparable. Alors la dimension du $\mathbf{K}$-espace vectoriel $\mathbf{M}_i$ est égal à rf. On en déduit que la dimension de $\prod_{1 \leq i \leq m} \mathbf{L}/\mathfrak{p}_i$ est rfm. Ainsi la dimension du radical $nil(\mathbf{L})$ est

$$dim(nil(\mathbf{L})) = d - rfm = (e - r)fm. \tag{5.14}$$

Proposition 5.3.21. *Une condition suffisante pour que* $\mathbf{L}$ *soit non-ramifée est la suivante : pour tout diviseur premier* l *de* d *il existe un élément* $a_l \in \mathbf{L}$ *tel que* $\sigma^{\frac{d}{l}}(a_l) - a_l$ *est une unité.*

Démonstration. Supposons que pour tout diviseur premier l de d il existe un élément $a_l \in \mathbf{L}$ tel que $\sigma^{\frac{d}{l}}(a_l) - a_l$ est une unité.

Le groupe $\mathcal{G}^{\mathbf{T}}$ est engendré par $\sigma^{\frac{d}{e}}$:

– Si $e = 1$, alors $\mathcal{G}^{\mathbf{T}}$ est trivial et d'après l'équation (5.14) on a $e = r = 1$. Par conséquent $\mathbf{L}$ est un anneau réduit et les extensions $\mathbf{M}_i/\mathbf{K}$ sont séparables. Donc $\mathbf{L}$ est une $\mathbf{K}$-algèbre étale.

– Mais si $e > 1$, en écrivant la décomposition en facteurs premiers

$$e = \prod q_1 \dots q_r, r \in \mathbb{N},$$

on voit que

$$\sigma^{\frac{d}{q_r}} = (\sigma^{\frac{d}{e}})^{\prod_{i=1}^{r-1} q_i} \in \mathcal{G}^{\mathbf{T}}, \tag{5.15}$$

c'est-à-dire que le nombre premier q_r (divisant d) est tel que pour tout $a \in \mathbf{L}$ on a $\sigma^{\frac{d}{q_r}}(a) - a \in nil(\mathbf{L})$. Mais cela est contraire à notre hypothèse. Donc on a nécessairement $e = 1$, et comme nous l'avons vu, dans ce cas $\mathbf{L}$ est une $\mathbf{K}$-algèbre étale.

□

Maintenant nous démontrons la proposition 5.3.19 dans le cas de la $\mathbf{K}$-algèbre $\mathbf{L}$. Il s'agit d'établir que :

Proposition 5.3.22. $\mathbf{L}$ *est étale si et seulement si la forme* $\mathrm{Tr}_{\mathbf{L/K}}$ *est non dégénée.*

En effet, supposons d'abord que $\mathbf{L}$ est étale sur $\mathbf{K}$. Dans ce cas $\mathbf{L}$ est réduite et les corps $\mathbf{M}_i = \mathbf{L}/\mathfrak{p}_i$ sont des extensions séparables de $\mathbf{K}$. Donc les formes bilinéaires $\mathrm{Tr}_{\mathbf{M}_i/\mathbf{K}}$ sont non-dégénérées [[27], chapitre 2, proposition 3]. De plus $\mathbf{L}$ est isomorphe au produit $\prod_{1 \leq i \leq m} \mathbf{L}/\mathfrak{p}_i$ (équation (5.13)). Donc la matrice de la forme $\mathrm{Tr}_{\mathbf{L/K}}$ est une matrice diagonale par bloc dont les blocs diagonaux sont les matrices des formes $\mathrm{Tr}_{\mathbf{M}_i/\mathbf{K}}$. Par conséquent la forme $\mathrm{Tr}_{\mathbf{L/K}}$ est non-dégńérée (parce que les formes $\mathrm{Tr}_{\mathbf{M}_i/\mathbf{K}}$ le sont).

Réciproquement, si $\mathrm{Tr}_{\mathbf{L/K}}$ est non-dégénérée alors $\mathbf{L}$ est réduit : $nil(\mathbf{L}) = (0)$.
En effet, soit $x \in nil(\mathbf{L})$. Pour tout $y \in \mathbf{L}$ on a $xy \in nil(\mathbf{L})$, car $nil(\mathbf{L})$ est un idéal de $\mathbf{L}$. Donc m_{xy} (la mulitiplication par xy) est un endomorphisme nilpotent.

La réduction de Jordan des matrices nilpotentes nous permet d'affirmer que la trace d'une matrice nilpotente est nulle. Donc $\mathrm{Tr}_{\mathbf{L/K}}(xy) = 0$ pour tout $y \in \mathbf{L}$. Par conséquent $x = 0$, car $\mathrm{Tr}_{\mathbf{L/K}}$ est non dégénérée.

Par ailleurs si $\tau \in \mathcal{G}^{\mathbf{T}}$ alors pour tout $l \in \mathbf{L}$ on a $\tau(l) - l \in \bigcap_{1 \leq i \leq m} \mathfrak{p}_i = nil(\mathbf{L}) = (0)$. Donc $\tau = \mathrm{Id}_{\mathbf{L}}$ et $\mathcal{G}^{\mathbf{T}}$ est trivial. Par conséquent $\mathbf{L}$ est étale sur $\mathbf{K}$ (on fait le même raisonnement que dans la preuve de la proposition 5.3.21).

Remarque 5.3.23. *Nous supposons, en plus des hypothèses faites au début de la présente sous-section, que le corps* $\mathbf{K} = \mathbf{F}_p$ *est fini et* $\mathbf{L}$ *est un anneau réduit (i.e étale). On rappelle que* Spec $\mathbf{L} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$.

L'automorphisme de Frobenius Φ_i *de* $\mathbf{M}_i = \mathbf{L}/\mathfrak{p}_i$ *est la réduction modulo* $\mathfrak{p}_i$ *d'un élément* σ^{z_i} *de* $\mathcal{G}^{\mathbf{Z}}$ *avec* $z_i \in \mathbb{N}$. *En particulier, pour tout* $a \in \mathbf{L}$, *on a*

$$\sigma^{z_1}(a) = a^p \bmod \mathfrak{p}_1. \tag{5.16}$$

Le groupe $\mathcal{G}$ agit transitivement sur Spec $\mathbf{L}$*, donc pour $j = 1, \ldots, m$ il existe $\tau_j \in \mathcal{G}$ tel que $\tau_j(\mathfrak{p}_1) = \mathfrak{p}_j$. En faisant agir les τ_j sur l'equation* 5.16*, on obtient que $z_1 = z_2 = \cdots = z_m$. Donc il existe un entier z tel que pout tout $a \in \mathbf{L}$ on a $\sigma^z(a) - a^p \in nil(\mathbf{L}) = (0)$, c'est-à-dire*

$$\sigma^z(a) = a^p \tag{5.17}$$

pour tout $a \in \mathbf{L}$.

On a $(\sigma^z)^f = \mathrm{Id}$, donc $d = efm$ divise zf et par conséquent z est un multiple de m.

5.4 Extensions d'anneaux et preuve de primalité

Dans cette section nous donnons un critère de primalité qui généralise le critère AKS [théorème 4.1.1 du chapitre 4].

Les principales étapes dans la preuve du critère de Berrizbeitia-Bernstein sont la construction d'une extension de Kummer $\mathbf{K} = \mathbf{F}_p[X]/(X^d - r)$, où p est un diviseur premier de l'entier n dont on veut prouver la primalité, et la formulation d'une hypothèse combinatoire supposant que le groupe $\mathbf{F}_p^*$ est assez gros (cette dernière hypothèse combinatoire est déjà présente dans la preuve du critère AKS d'origine).

Notons σ un générateur de $\mathrm{Gal}(\mathbf{K}/\mathbf{F}_p)$, $\omega_0 = 1 + X + X^2 + \cdots + X^{d-1} \bmod X^d - r$ et $\omega_i = \sigma^i(\omega_0)$ pour $0 \leq i \leq d-1$. Alors $(\omega_0, \omega_1, \ldots, \omega_{d-1})$ est une $\mathbf{F}_p$-base normale de $\mathbf{K}$. On le voit en calculant le déterminant (de Vandermonde) de la matrice de passage entre les bases $(\omega_i)_{0 \leq i \leq d-1}$ et $(X^i \bmod X^d - r)_{0 \leq i \leq d-1}$.

Au lieu de construire des extensions de Kummer, on peut de façon plus générale, regarder les algèbres $\mathbf{S}$ de dimension fini $d \geq 1$ sur un corps $\mathbf{L}$ telles que $\mathbf{S}$ est munie d'un $\mathbf{L}$-automorphisme σ et d'une $\mathbf{L}$-base normale $(\omega_i)_{i \in \mathbf{Z}/d\mathbf{Z}}$ avec $\omega_i = \sigma^i(\omega_0)$. Une telle algèbre $\mathbf{S}$ est étale sur $\mathbf{L}$ si et seulement si $\mathbf{S}$ est un anneau réduit.

Ces observations mènent au critère gènéral suivant :

Théorème 5.4.1. *Soient $n \geq 2$ un entier et $R = \mathbf{Z}/n\mathbf{Z}$. Soit $S \supset R$ une algèbre libre de rang d sur R. Soit σ un R-automorphisme de S. Soit $\mathcal{G}$ le groupe engendré par σ. On suppose que S est un $R[\mathcal{G}]$-module libre de rang 1 : il existe un élément ω dans S tel que $(\omega, \sigma(\omega), \ldots, \sigma^{d-1}(\omega))$ est une R-base de S. Soit θ une unité de S telle que $\theta^n = \sigma(\theta)$. Soit p un diviseur premier de n. On suppose que S/pS est un anneau réduit et que $\theta \bmod p$ engendre un sous groupe d'ordre au moins égal à $n^{\lfloor\sqrt{d}\rfloor}$ dans $(S/pS)^*$. Alors n est une puissance de p.*

Démonstration. Posons $\mathbf{L} = S/pS$ et $\mathbf{K} = R/pR = \mathbf{Z}/p\mathbf{Z}$. L'algèbre $\mathbf{L}$ est dimension d sur $\mathbf{K}$. Par hypothèse $\mathbf{L}$ est un anneau réduit, on peut donc utiliser les éléments de la remarque 5.3.23 (en l'occurence l'équation (5.17)).

Le R-automorphisme σ induit un $\mathbf{K}$-automorphisme de $\mathbf{L}$ que nous notons encore σ. Par hypothèse θ est une unité de S telle que

$$\sigma(\theta) = \theta^n. \tag{5.18}$$

En réduisant cette égalité modulo p et en posant $a = \theta \bmod pS$, on obtient

$$a^n = \sigma(a) \text{ et } a^{n^i} = \sigma^i(a) \text{ pour } i \in \mathbf{Z}/d\mathbf{Z}. \tag{5.19}$$

En utilisant les équations (5.17) et (5.19), on prouve qu'il existe un entier z tel que pour $k, l \in \mathbb{N}$, on a :

$$a^{n^k p^l} = \sigma^{k+zl}(a). \tag{5.20}$$

Soit $\mathfrak{p}$ un idéal premier de $\mathbf{L}$, on pose $\mathbf{M} = \mathbf{L}/\mathfrak{p}$ et

$$\pi : \mathbf{L} \to \mathbf{M}$$

le morphisme canonique de reduction modulo $\mathfrak{p}$. Soit $b = a \bmod \mathfrak{p}$. On note $G \subset \mathbf{L}^*$ le sous-groupe engendré par a et $H \subset \mathbf{M}^*$ le sous-groupe engendré par b. La restriction $\pi|_G : G \to H$ est une bijection. En effet, si k est un entier positif tel que $b^k = 1$ dans $\mathbf{M}$ alors $a^k = 1 \bmod \mathfrak{p}$. En élevant les deux membres de cette congruance à la puissance n, l'equation (5.19) nous donne $a^{kn^i} = (\sigma^i(a))^k = \sigma^i(a^k) = 1 \bmod \mathfrak{p}$. Donc $a^k = 1 \bmod (\sigma^i)^{-1}(\mathfrak{p})$. On rappele que $< \sigma >= \mathcal{G}$ agit transitivement sur Spec $\mathbf{L}$, donc $a^k - 1 \in \bigcap_{1 \le i \le m} \mathfrak{p}_i = nil(\mathbf{L})$. Puisque $\mathbf{L}$ est réduit, on en déduit que $a^k = 1$.

L'ordre h du sous-groupe $H \subset \mathbf{M}^*$ divise $p^f - 1$ où f est la dimension de $\mathbf{M}$ sur $\mathbf{K}$, donc p et $\#H$ sont premiers entre eux. En itérant d-fois (5.19) on a $a^{n^d} = a$. Donc n est inversible modulo $h = \#H = \#G$. Ainsi l'équation (5.20) garde tout son sens lorsque $n, p \in \mathbf{Z}/h\mathbf{Z}$ et $l, k \in \mathbf{Z}$.

On pose $q = n/p$, des équations (5.16) et (5.19) on déduit que $a^q = \sigma^{1-z}(a)$.

Rendu à ce niveau, la preuve devient une adaptation de la preuve du critère AKS (théorème 4.1.1 du chapitre 4). On constate que $(1 + \sqrt{d})^2 > d$. Donc il existe quatre entiers $i, i', j, j' \in \{0, 1, \ldots, \lfloor\sqrt{d}\rfloor\}$ tels que les couples (i, j) et (i', j') sont différents mais $i(1-z)+jz$ est congru à $i'(1 - z) + j'z$ modulo d. En posant, dans l'équation (5.20), pour commencer $k = i$ et $l = j - i$ et ensuite $k = i'$ et $l = j' - i'$, on montre que les exponentiations par $q^i p^j$ et $q^{i'} p^{j'}$ agissent de la même façon sur a. On en déduit que

$$q^i p^j = q^{i'} p^{j'} \bmod \#G.$$

Puisque $max(q^i p^i, q^{i'} p^{j'}) \leq n^{\lfloor\sqrt{d}\rfloor} \leq \#G$, on en déduit que l'égalité est vrai dans $\mathbf{Z}$. Donc n est une puissance de p. □

Le théorème 4.2.1 du chapitre 4, tiré de l'article de Bernstein, est une conséquence du théorème 5.4.1, nous donnons ici un énoncé reformulé de ce dernier.

Corollaire 5.4.2 (Critère de Berrizbeitia-Bernstein,[5], théorème 2.1)**.** *Soit $n \geq 3$ un entier, on pose $R = \mathbf{Z}/n\mathbf{Z}$. Soit $S = R[x]/(x^d - \alpha)$ où $d \geq 2$ divise $n-1$. On fixe $n-1 = dm$ et on suppose que $\zeta = \alpha^m$ est d'ordre exact d dans R^*. On suppose de plus que*

$$(x-1)^n = \zeta x - 1 \bmod (n, x^d - \alpha). \tag{5.21}$$

Si 2^d est plus grand que $n^{\lfloor\sqrt{d}\rfloor}$, alors n est une puissance d'un nombre premier.

Démonstration. Dire que ζ est d'odre exact d dans R revient à dire que $\zeta^d = 1$ et $\zeta^k - 1$ est une unité pour tout $1 \leq k < d$. On définit un R-automorphisme $\sigma : S \to S$ par $\sigma(x) = \zeta x$. On pose $\omega = (\alpha - 1)/(x - 1) = 1 + x + x^2 + \cdots + x^{d-1} \bmod x^d - \alpha$ et on vérifie que $(\omega, \sigma(\omega), \ldots, \sigma^{d-1}(\omega))$ est une R-base de S. En effet, $(1, x, x^2, \ldots, x^{d-1})$ est une base de S et la matrice de passage de $(x_i)_{i \in \mathbf{Z}/d\mathbf{Z}}$ à $(\sigma^i(\omega))_{i \in \mathbf{Z}/d\mathbf{Z}}$ est une matrice de Vandermonde $V(1, x, x^2, \ldots, x^{d-1})$ qui est inversible puisque ζ est d'ordre exact d. Donc S est un $R[\sigma]$-module libre de rang 1.

La classe $x \bmod x^d - \alpha$ est une unité de S car α est une unité de R. Par conséquent pour tout entier $1 \leq k < d$, la différence $\sigma^k(x) - x = (\zeta^k - 1)x$ est une unité de S car ζ est d'ordre exact d.

Soit p un nombre premier divisant n. On pose $\mathbf{K} = R/pR = \mathbf{Z}/p\mathbf{Z}$ et $\mathbf{L} = S/pS$. L'algèbre $\mathbf{L}$ est de dimension d sur $\mathbf{K}$ et σ induit un $\mathbf{K}$-automorphisme de $\mathbf{L}$ que nous notons encore σ. On fixe $X = x \bmod pS$, d'après ce qui précède $\sigma^k(X) - X$ est une unité de $\mathbf{L}$ pour $1 \leq k < d$. La condition suffisante de la proposition 5.3.21 nous permet d'affirmer que $\mathbf{L}$ est une $\mathbf{K}$-algèbre étale (*i.e* un anneau réduit).

On pose $\theta = x - 1 \bmod (n, x^d - \alpha)$, c'est une unité de S car $\alpha - 1$ est une unité de R. Par hypothèse, on a

$$(x-1)^n = \zeta x - 1 \bmod (n, x^d - \alpha). \tag{5.22}$$

Donc pour tout entier positif k, la classe $\zeta^k x - 1 \bmod (n, x^d - \alpha)$ est une puissance de θ.

Posons $a = \theta \bmod p = x - 1 \bmod (p, x^d - \alpha) \in \mathbf{L}$. Pour tout sous-ensemble $\mathcal{S}$ de $\{0, 1, \ldots, d-1\}$, on note $a_{\mathcal{S}}$ le produit

$$\prod_{k \in \mathcal{S}} (\zeta^k - 1) \bmod (p, x^d - a) = \prod_{k \in \mathcal{S}} \sigma^k(a).$$

C'est une puissance de a parce que $\sigma^k(a)$ est une.

À ce niveau, une fois de plus, nous utilisons une astuce de la preuve du critère de primalité AKS.

Deux sous-ensembles stricts et distincts $\mathcal{S}_1$ et $\mathcal{S}_2$ de $\{0, 1, \ldots, d-1\}$ induisent des classes $a_{\mathcal{S}_1}$ et $a_{\mathcal{S}_2}$ distinctes pour des raisons de degré (voir la preuve du critère AKS). Donc l'ordre de a dans $(S/pS)^*$ est au moins égal à $2^d - 1$. Mais par hypothèse $2^d > n^{\lfloor\sqrt{d}\rfloor}$. Donc le sous-groupe engendré par $a = \theta \bmod p$ est d'ordre au moins égal à $n^{\lfloor\sqrt{d}\rfloor}$. D'après le théorème 5.4.1, l'entier n est un puissance d'un nombre premier. □

Chapitre 6

Une version du critère de primalité AKS utilisant les courbes elliptiques

À la section 5.4 du chapitre 5, nous avons vu que l'existence d'un critère de primalité de type AKS passe par la construction d'une algèbre libre étale et la formulation d'une hypothèse combinatoire. Dans ce chapitre nous construisons des algèbres libres étales $\mathbf{S}$ de rang fini sur $\mathbf{Z}/n\mathbf{Z}$, munies d'un $\mathbf{Z}/n\mathbf{Z}$-automorphisme, à partir d'isogénies entre courbes elliptiques modulo n.

Nous tenons à préciser que tout au long du chapitre nous aurons recours à la technique dite du *"changement d'anneau de base"*. Il s'agit d'un outil important en théorie des schémas. Cette technique permet par exemple de considérer qu'une courbe elliptique $E/\mathbf{Q}$, sur le corps des rationnels, définit une courbe sur le corps des nombres complexes.

6.1 Bases elliptiques et courbes définies sur un corps

Dans cette section nous donnons un énoncé décrivant la construction d'une algèbre libre étale sur un corps $\mathbf{K}$ grâce à une isogénie entre courbes elliptiques définies sur $\mathbf{K}$.

6.1.1 Préliminaires

Soient $\mathbf{K}$ un corps de caractéristiques p et $E/\mathbf{K}$ une courbe elliptique d'équation de Weierstrass

$$\Lambda(a_1, a_2, a_3, a_4, a_6, X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

On pose

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

On note $O = (0 : 1 : 0)$ le point à l'infini de E. Si A est un point de $E(\overline{\mathbf{K}})$, on note

$$\begin{array}{rccc} \tau_A : & E & \to & E \\ & P & \mapsto & P \oplus A \end{array}$$

la translation par A. En suivant [10], on construit des fonctions sur E en posant

$$x = X/Z,\ y = Y/Z,\ x_A = x \circ \tau_{-A},\ y_A = y \circ \tau_{-A} \text{ et } u_{A,B} = \frac{y_A - y(A-B)}{x_A - x(A-B)} \tag{6.1}$$

où B est un point de E distinct de A.

Soient $d \geq 3$ un entier impair, $T \in E(\mathbf{K})$ un point d'ordre d et

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

l'équation affine de E. On pose $x_k = x_{kT}$, $y_k = y_{kT}$ et on définit

$$x' = x + \sum_{1 \leq k \leq d-1} [x_k - x(kT)] \text{ et } y' = y + \sum_{1 \leq k \leq d-1} [y_k - y(kT)]. \tag{6.2}$$

Vélu a établi, dans sa thèse [31], la relation suivante, qui rappelle bien l'équation affine d'une courbe elliptique :

$$(y')^2 + a_1'x'y' + a_3'y' = (x')^3 + a_2'(x')^2 + a_4'x' + a_6', \tag{6.3}$$

où $a_1', a_2', a_3', a_4', a_6' \in \mathbf{K}[a_1, a_2, a_3, a_4, a_6]$.

Donc l'application $(x, y) \mapsto (x', y')$ définit une isogénie $I : E \to E'$ de degré d, où E' est la courbe elliptique d'équation affine donnée par la relation de Vélu (6.3) ; on note $I' : E' \to E$ son isogénie duale.

6.1.2 Base elliptique

Soient $\mathfrak{a}, \mathfrak{b} \in \mathbf{K}$ des scalaires tels que

$$u_k = \mathfrak{a}u_{kT,(k+1)T} + \mathfrak{b} \quad \text{et} \quad \sum_{k \in \mathbf{Z}/d\mathbf{Z}} u_k = 1. \tag{6.4}$$

Le système $(u_k)_{k \in \mathbf{Z}/d\mathbf{Z}}$ est une base de $\mathbf{K}(E)$ sur $\mathbf{K}(E')$. Plus précisement on a le lemme suivant, qui est une généralisation du lemme 5 de [10].

Lemme 6.1.1 (Ezome et Lercier, [13] section 2.1.3)**.** *Soit E une courbe elliptique définie sur un corps $\mathbf{K}$. Soient $T \in E(\mathbf{K})$ un point d'ordre $d \geq 3$ (un entier impair) et $I : E \to E'$ l'isogénie séparable de degré d définie à partir de T par les formules de Vélu. Soit $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ le système de fonctions de $\mathbf{K}(E)$ définies ci-dessus. Alors $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ est une $\mathbf{K}(E')$-base de $\mathbf{K}(E)$.*

Supposons en plus que $\mathbf{L}$ est une extension de $\mathbf{K}$, et $A \in E'(\mathbf{L})$ un point non nul pour lequel il existe un point $B \in E(\overline{\mathbf{L}})$ avec $I(B) = A$. Soit

$$I^{-1}(A) = [B] + [B+T] + [B+2T] + \ldots + [B+(d-1)T]$$

la fibre de I au-dessus de A. Alors les trois conditions suivantes sont équivalentes :

(i) L'image du sytème $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ dans l'anneau résiduel en $I^{-1}(A)$ en est une $\mathbf{L}$-base ;

(ii) La matrice $(u_k(B+lT))_{k,l\in\mathbf{Z}/d\mathbf{Z}}$ est inversible ;

(iii) Le point A n'est pas contenu dans le noyau de l'isogénie duale $I' : E' \to E$.

Démonstration. On fait un changement d'anneau de base préalable sur E et E' de $\mathbf{K}$ à $\mathbf{L}$. Le système $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ est $\mathbf{L}$-linéairement indépendant et constitue une base de l'espace vectoriel $\mathcal{L}(I^{-1}(O'))$ où O' est l'origine de E' et $I^{-1}(O') = [O] + [T] + [2T] + \ldots + [(d-1)T]$ le noyau de I. En effet, soient $(\lambda_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ des scalaires dans $\mathbf{L}$ tels que $f = \sum_{k\in\mathbf{Z}/d\mathbf{Z}} \lambda_k u_k$ est la fonction nulle. Les developpements de Taylor de f au pôles des u_k (voir [10], Section 2) montrent que tous les λ_k sont égaux. On en déduit que $\lambda_k = 0$ pour tout $k \in \mathbf{Z}/d\mathbf{Z}$, car la somme des u_k est égale à 1. Donc $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ est un système de fonctions $\mathbf{L}$-linéairement indépendantes. Ce système est une base de $\mathcal{L}(I^{-1}(O'))$ car $I^{-1}(O')$ est un diviseur de degré d (voir corollaire 1.1.19 du théorème de Riemann-Roch donné au chapitre 1).

Maintenant nous établissons la preuve de la seconde partie du lemme.

Pour montrer que (i) est équivalent à (ii), on remarque qu'un vecteur $(\lambda_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ est dans le noyau de la matrice $(u_k(B+lT))_{k,l\in\mathbf{Z}/d\mathbf{Z}}$ si et seulement si la somme $\sum_{k\in\mathbf{Z}/d\mathbf{Z}} \lambda_k u_k(B+lT)$ est nulle pour tout $l \in \mathbf{Z}/d\mathbf{Z}$. Cela est équivalent à dire que la fonction $\sum_{k\in\mathbf{Z}/d\mathbf{Z}} \lambda_k u_k$ est nulle sur la fibre $I^{-1}(A)$.

Pour montrer que (iii) entraine (i), considérons un système $(\lambda_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ de scalaires de $\mathbf{L}$ tels que $f = \sum_{k\in\mathbf{Z}/d\mathbf{Z}} \lambda_k u_k$ s'annule sur la fibre $I^{-1}(A)$. Si les λ_k ne sont pas tous nuls, alors f est une fonction non identiquement nulle, et son diviseur est $I^{-1}(A) - I^{-1}(O')$. On en déduit que $\sum_{k\in\mathbf{Z}/d\mathbf{Z}}[B+kT] - [kT]$ est un diviseur principal. Ainsi

$$\sum_{k\in\mathbf{Z}/d\mathbf{Z}} B + kT - kT = dB = I'(A) = O(\text{voir [30], corollaire 3.5page 67}),$$

où O désigne l'origine de E. Donc A est contenu dans le noyau de I'.

Réciproquement, si A est dans le noyau de I' alors le diviseur $\sum_{k\in\mathbf{Z}/d\mathbf{Z}}[B+kT] - [kT]$ est principal (voir [30], corollaire 3.5 page 67). Soit f une fonction sur E non identiquement nulle telle que $\mathrm{div}(f) = I^{-1}(A) - I^{-1}(O')$. Puisque $f \in \mathcal{L}(I^{-1}(O'))$, il existe un vecteur non

nul $(\lambda_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ de $\mathbf{L}^d$ tel que $f=\sum_{k\in\mathbf{Z}/d\mathbf{Z}}\lambda_k u_k$ car nous avons montré au début de la preuve que $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ est une base de $\mathcal{L}(I^{-1}(O'))$.
Mais f s'annule sur la fibre par construction. Donc on a une combinaison linéaire nulle $\sum_{k\in\mathbf{Z}/d\mathbf{Z}}\lambda_k u_k \bmod I^{-1}(A)=0$ où les λ_k ne sont pas tous nuls. Ainsi (i) implique (iii).

Pour établir la première partie du lemme, on applique la seconde partie que nous venons de démontrer au cas $\mathbf{L}=\mathbf{K}(E')$ et $A=G'=(x',y')$ le point générique de E'. L'anneau résiduel en $I^{-1}(G')$, dans ce cas, est $\mathbf{K}(E)$. Puisque G' n'est pas dans le noyau de I', la seconde partie du lemme nous dit que le système $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ est une base de $\mathbf{K}(E)$ sur $\mathbf{K}(E')$. □

Un système de fonctions $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ tel que celui du lemme 6.1.1 est appelé *base elliptique.*

On note $\mathbf{S}$ l'anneau résiduel en $I^{-1}(A)$ dans le lemme 6.1.1 ci-dessus.

Lemme 6.1.2 (Ezome et Lercier, [13] section 2.1.4.4)**.** *Les conditions* (i)*,* (ii) *et* (iii) *du lemme* 6.1.1 *sont équivalentes à :*
La matrice $(\mathrm{Tr}_{\mathbf{S}/\mathbf{L}}(u_k u_l \bmod I^{-1}(A)))_{k\in\mathbf{Z}/d\mathbf{Z}}$ *est inversible.*

Concernant la forme trace $\mathrm{Tr}_{\mathbf{K}(E)/\mathbf{K}(E')}$ de $\mathbf{K}(E)$ sur $\mathbf{K}(E')$, on a le résultat suivant.

Lemme 6.1.3 (Ezome et Lercier, [13] section 2.1.4.4)**.** *Le déterminant* D *de la matrice* $(\mathrm{Tr}_{\mathbf{K}(E)/\mathbf{K}(E')}(u_k u_l))_{k,l\in\mathbf{Z}/d\mathbf{Z}}$ *est un polynôme en* x' *de degré inférieur ou égal à* $d-1$*. Il vérifie l'égalité*

$$\psi_I^{2d}(x)D(x')=\mathfrak{a}^{2d-2}\psi_d^2(x),$$

où

$$\psi_I(x)=\prod_{1\le k\le (d-1)/2}(x-x(kT))$$

est le facteur de $\psi_d(x)$ *(voir la section "Exemples" du chapitre 1) correspondant aux points du noyau de* I*.*

6.2 Courbes elliptiques sur un anneau

Reconsidérons la seconde partie du lemme 6.1.1 de la section précédente. Si $A\in E'(\mathbf{K})$ est un point $\mathbf{K}$-rationnel qui ne rencontre pas le noyau de l'isogénie I', alors l'anneau résiduel $\mathbf{S}$ en $I^{-1}(A)$ est une $\mathbf{K}$-algèbre libre et $(u_k \bmod I^{-1}(A))_{k\in\mathbf{Z}/d\mathbf{Z}}$ en est une $\mathbf{K}$-base. Le lemme 6.1.2 affirme que, dans ce cas, la forme $\mathrm{Tr}_{\mathbf{S}/\mathbf{K}}$ est non dégénérée. D'aprés la proposition 5.3.19, l'anneau $\mathbf{S}$ est donc une $\mathbf{K}$ -algèbre libre étale de rang d.

Notre objectif dans cette section est construire des algèbres libres étales sur $\mathbf{Z}/n\mathbf{Z}$ à partir d'isogénies entre courbes elliptiques modulo n. Pour cela nous considérons le contexte plus général des courbes elliptiques définies sur un anneau commutatif unitaire $\mathbf{R}$ et nous utilisons la technique des courbes définies sur un corps que nous venons de décrire.

6.2.1 Schémas projectifs

Soient A un anneau et $B = \oplus_{d\geq 0} B_d$ une A-algèbre graduée (voir définition 1.1.3 et remplacer $\mathbf{Z}$-modules par A-modules). Un idéal I de B est dit homogène s'il est engendré par des éléments homogènes. Cela revient à dire que $I = \oplus_{d\geq 0}(I \bigcap B_d)$. Dans ce cas le quotient B/I a une graduation naturelle $(B/I)_d = B_d/(I \bigcap B_d)$. On note $\mathrm{Proj}(B)$ l'ensemble des idéaux premiers homogènes de B ne contenant pas l'idéal $B_+ := \oplus_{d>0} B_d$. Pour tout idéal homogène I de B, on note $V_+(I)$ l'ensemble des idéaux $\mathfrak{p} \in \mathrm{Proj}(B)$ contenant I. La *topologie de Zariski* sur $\mathrm{Proj}(B)$ est celle dont les fermés sont les ensembles de la forme $V_+(I)$.

Si $f \in B$ est un élément homogène, on pose $D_+(f) = \mathrm{Proj}(B) - V_+(fB)$ et on a le résultat suivant :

Proposition 6.2.1. *Soient A un anneau et B une algèbre gradué sur A. Alors on peut munir* $\mathrm{Proj}(B)$ *d'une structure de A-schéma telle que pour tout élément homogène $f \in B_+$, l'ouvert $D_+(f)$ est affine et isomorphe à* $\mathrm{Spec}(B_{(f)})$.

Maintenant nous définissons les notions d'immersions fermées et de sous-schémas fermés nécéssaires pour introduire les schémas projectifs.

Définition 6.2.2. *Un morphisme $(f, f^{\#}) : (X, \mathcal{F}_X) \to (Y, \mathcal{F}_Y)$ d'espaces topologiques annelés est une immersion ouverte (resp. immersion fermée) si X est homéomorphe à un sous-ensemble ouvert (resp. fermé) de Y et si $f_x^{\#}$ est un isomorphisme (resp. un morphisme surjectif) pour tout $x \in X$.*

Un sous-schéma fermé d'un schéma X est un sous-ensemble fermé Y de X muni d'une structure $(Y, \mathcal{F}_Y)$ de schéma et avec une immersion fermée $(j, j^{\#}) : (Y, \mathcal{F}_Y) \to (X, \mathcal{F}_X)$, où $j : Y \to X$ est l'injection canonique. La structure de sous-schéma sur un sous-ensemble fermé n'est pas unique.

L'espace projectif $\mathbb{P}^n$ (de dimension relative n) sur A est le schéma $\mathrm{Proj}(B)$ *où* $B = A[X_0, X_1, \ldots, X_n]$.

Un schéma projectif sur A est un A-schéma isomorphe à un sous-schéma fermé de $\mathbb{P}^n$ pour $n \geq 0$.

Comme premiers exemples de schémas projectifs nous pouvons citer les variétés projectives (application directe du lemme 3.41 page 53 de [24]). De plus les morphismes de variétés projectives sont des morphismes de schémas projectifs.

Soient $\mathbf{R}$ un anneau commutatif unitaire et a_1, a_2, a_3, a_4, a_6 des éléments de $\mathbf{R}$.
Une courbe elliptique sur $\mathbf{R}$ est un schéma projectif

$$E = \mathrm{Proj}(\mathbf{R}[X,Y,Z]/\Lambda(a_1,a_2,a_3,a_4,a_6,X,Y,Z)) \text{ tel que } \Delta(a_1,a_2,a_3,a_4,a_6) \in \mathbf{R}^\times.$$

Soient $x_0, y_0, z_0 \in \mathbf{R}$ trois éléments de $\mathbf{R}$ tels que l'idéal (x_0, y_0, z_0) qu'ils engendrent est égal à $\mathbf{R}$ tout entier. Alors l'application

$$\begin{array}{rccc} \rho: & \mathbf{C} = \mathbf{R}[X,Y,Z]/\Lambda(a_1,a_2,a_3,a_4,a_6,X,Y,Z) & \to & \mathbf{B} = \mathbf{R}[t] \\ & P(X,Y,Z) & \mapsto & P(x_0t, y_0t, z_0t) \end{array}.$$

est un morphisme surjectif d'anneaux gradués.

L'image par ρ de $\mathbf{C}_+$ est contenue dans $\mathbf{B}_+$. Donc ρ définit un morphisme de schémas [[24], lemme 3.40, Page 53]

$$\rho^*: \ \mathrm{Proj}(\mathbf{R}[t]) \ \to \ E = \mathrm{Proj}(\mathbf{R}[X,Y,Z]/\Lambda(a_1,a_2,a_3,a_4,a_6,X,Y,Z)).$$

L'inclusion naturelle

$$\begin{array}{rccc} s: & \mathbf{R} & \to & \mathbf{R}[X,Y,Z]/\Lambda(a_1,a_2,a_3,a_4,a_6,X,Y,Z) \\ & x & \mapsto & x \end{array}$$

induit aussi un morphisme de schémas s^* et on a le diagramme commutatif suivant

$$\begin{array}{ccc} & & E \\ & \overset{\rho^*}{\nearrow} & \downarrow{\scriptstyle s^*} \\ \mathrm{Proj}(\mathbf{R}[t]) & \xrightarrow{\psi} & \mathrm{Spec}(\mathbf{R}) \end{array} \tag{6.5}$$

L'application ψ est un isomorphisme de schémas, donc s^* admet une section que l'on peut définir à partir de ψ^{-1} et ρ^*.

Puisque ρ^* est bien définie par le triplet $(x_0, y_0, z_0) \in \mathbf{R}^3$, nous dirons que le $\mathbf{R}$-point $A = (x_0, y_0, z_0)$ de E est une section de s^*.

Remarque 6.2.3. *Toutes les sections du morphisme de schémas s^* ne se construisent pas nécessairement à partir d'un tel triplet de $\mathbf{R}$. C'est le cas cependant lorsque l'anneau R est principal.*

6.2.2 Courbes elliptiques de Weierstrass universelles

Soient A_1, A_2, A_3, A_4 et A_6 des indéterminées et

$$B_2 = A_1^2 + 4A_2, \ B_4 = 2A_4 + A_1A_3, \ B_6 = A_3^2 + 4A_6, \ B_8 = A_1^2A_6 + 4A_2A_6 - A_1A_3A_4 + A_2A_3^2 - A_4,$$
$$\text{et} \qquad \Delta(A_1,A_2,A_3,A_4,A_6) = -B_2^2B_8 - 8B_4^3 - 27B_6^2 + 9B_2B_4B_6.$$

On pose

$$\mathcal{A}_1 = \mathbf{Z}[A_1, A_2, A_3, A_4, A_6, \frac{1}{\Delta}].$$

Soient x et y deux indéterminées supplémentaires. On pose

$$\Lambda(A_1, A_2, A_3, A_4, A_6, x, y) = y^2 + A_1xy + A_3y - x^3 - A_2x^2 - A_4x - A_6 \in \mathcal{A}_1[x, y].$$

Soit E_{aff} la courbe plane lisse affine d'équation $\Lambda(A_1, A_2, A_3, A_4, A_6, x, y) = 0$. Soit E le schéma projectif sur $\mathcal{A}_1$ d'équation $\Lambda(A_1, A_2, A_3, A_4, A_6, X, Y, Z) = 0$. En notant O la section $(0 : 1 : 0)$, on a $E_{\text{aff}} = E - O$.

Nous revenons sur les polynômes de division introduits au chapitre 1.

Soit $k \in \mathbb{N}$ un entier naturel. On note $\psi_k(a_1, a_2, a_3, a_4, a_6, x, y)$ les fonctions définies récursivement par :

$$\begin{gathered}
\psi_0 = 0,\ \psi_1 = 1,\ \psi_2 = 2y + a_1x + a_3, \\
\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\
\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + \\
(b_2b_8 - b_4b_6)x + b_4b_8 - b_6^6), \\
\psi_{2k} = \frac{\psi_k}{\psi_2}(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2), \\
\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3.
\end{gathered}$$

Ces polynômes sont dans $\mathcal{A}_1[x, y]/\Lambda(a_1, a_2, a_3, a_4, a_6, x, y)$ mais on peut les voir comme des polynômes de $\mathcal{A}_1[x, y]$ de degré 0 ou 1 en y. Si k est impair, ψ_k appartient à $\mathcal{A}_1[x]$ et on a $\psi_k = kx^{\frac{k^2-1}{2}} + O(x^{\frac{k^2-3}{2}})$. Si k est pair , alors ψ_k/ψ_2 appartient à $\mathcal{A}_1[x]$.

L'anneau $\mathcal{A}_1[x, y]$ est intègre. En suivant [11], on définit les éléments suivants dans son corps de fractions :

$$\begin{gathered}
g_k = x - \frac{\psi_{k+1}\psi_{k-1}}{\psi_k^2}, \\
h_k = y + \frac{\psi_{k+2}\psi_{k-1}^2}{\psi_2\psi_k^3} + (3x^2 + 2A_2x + A_4 - A_1y)\frac{\psi_{k-1}\psi_{k+1}}{\psi_2\psi_k^2}.
\end{gathered}$$

La multiplication par k sur $E - E[k]$ est donnée par $(x, y) \to (g_k, h_k)$.

Soient $d \geq 3$ un entier impair et "$x(T)$" et "$y(T)$" deux autres indéterminées . Soit S le sous-ensemble multiplicatif de $\mathcal{A}_1[x, y]$ engendré par $\psi_k(x(T), y(T))$ pour $1 \leq k \leq d-1$. On pose

$$\mathcal{A}_d = \mathcal{A}_1[x(T), y(T), \frac{1}{S}, 1/d]/(\psi_d(x(T), \Lambda(A_1, A_2, A_3, A_4, A_6, x(T), y(T))).$$

L'anneau $\mathcal{A}_d$ est intègre, on note $\mathcal{K}_d$ son corps de fractions. Le point $T \in E/\mathcal{K}_d$ définit une section de E_{aff}. La courbe E, via un changement d'anneau de base de $\mathcal{A}_1$ à $\mathcal{A}_d$, peut être considérée comme une courbe elliptique de Weierstrass universelle munie d'un point d'ordre exact d sur un anneau dans lequel d est inversible.

Pour tout k tel que $1 \leq k \leq d-1$, le point kT définit une section de E sur $\mathcal{A}_d$. On note $x(kT)$ et $y(kT)$ ses coordonnées et on a :

$$\begin{array}{l} x(kT) = g_k(A_1, A_2, A_3, A_4, A_6, x(T), y(T)) \in \mathcal{A}_d, \\ y(kT) = h_k(A_1, A_2, A_3, A_4, A_6, x(T), y(T)) \in \mathcal{A}_d. \end{array} \tag{6.6}$$

Un changement d'anneau de base sur E de $\mathcal{A}_1$ à $\mathcal{K}_d$ E donne alors une courbe elliptique $E/\mathcal{K}_d$ définie sur un corps. Il est donc possible d'exploiter le lemme 6.1.1. On introduit alors tous les scalaires et fonctions de la section 6.1 : $x_k, y_k, u_k, x', x', \omega_4, \omega_6$. Les dénominateurs apparaissant dans la définition de ces scalaires et fonctions sont des unités de

$$\mathcal{A}_d[E - E[d]] = \mathcal{A}_d[\frac{1}{\psi_d(x)}, x, y]/(\Lambda(A_1, A_2, A_3, A_4, A_6, x, y)).$$

Tous ces scalaires (resp. fonctions) sont dans $\mathcal{A}_d$ (resp. $\mathcal{A}_d[E-E[d])$. On peut donc définir la courbe isogène E' grâce à l'équation 6.3 et aussi les isogénies I et I'.

L'ensemble ouvert $E' - \mathrm{Ker}I'$ est le spectre de l'anneau

$$\mathcal{A}_d[E' - \mathrm{Ker}I'] = \mathcal{A}_d[\frac{1}{D(x')}, x', y']/(\Lambda(A'_1, A'_2, A'_3, A'_4, A'_6, x', y'))$$

Les équations (6.1),(6.2) et (6.6) montrent que $\mathcal{A}_d[E'-\mathrm{Ker}I']$ est inclus dans $\mathcal{A}_d[E-E[d]$. En fait l'anneau $\mathcal{A}_d[E-E[d]]$ est un $\mathcal{A}_d[E'-\mathrm{Ker}I']$-module libre et $(u_k)_{k\in\mathbf{Z}/d\mathbf{Z}}$ en est une base. Et plus précisement, $\mathcal{A}_d[E - E[d]]$ est une $\mathcal{A}_d[E' - \mathrm{Ker}I']$-algèbre étale car le déterminant $D(x')$ de la forme trace est inversible dans $\mathcal{A}_d[E' - \mathrm{Ker}I']$.

Lemme 6.2.4 (Ezome et Lercier)**.** *L'anneau*

$$\mathcal{A}_d[E - E[d]] = \mathcal{A}_d[\frac{1}{\psi_d(x,y)}, x, y]/\Lambda(a_1, a_2, a_3, a_4, a_6, x, y)$$

est une algèbre libre étale de rang d sur

$$\mathcal{A}_d[E' - \mathrm{Ker}I'] = \mathcal{A}_d[\frac{1}{D(x')}, x', y']/\Lambda(a'_1, a'_2, a'_3, a'_4, a'_6, x', y')$$

et $(u_l)_{l\in\mathbf{Z}/d\mathbf{Z}}$ en est une base.

Pour tout $k \in \mathbf{Z}/d\mathbf{Z}$, on a $\sigma(u_k) = u_{k+1}$ où σ est le $\mathcal{A}_d[E' - \mathrm{Ker}I']$-automorphisme de $\mathcal{A}_d[E - E[d]]$ induit par la translation τ_{-T}.

6.2.3 Construction d'un anneau des périodes elliptiques

En faisant un changement d'anneau de base dans le lemme 6.2.4 ci-dessus, on a :

Théorème 6.2.5 (Ezome et Lercier)**.** *Soient $d \geq 3$ un entier impair et $\mathbf{R}$ un anneau commutatif unitaire dans lequel d est inversible. Soient $a_1, a_2, a_3, a_4, a_6, \mathfrak{r}$ et $\mathfrak{n}$ des éléments de $\mathbf{R}$ tels que*

- *$\Delta(a_1, a_2, a_3, a_4, a_6)$ est une unité de $\mathbf{R}$,*
- *$\psi_d(a_1, a_2, a_3, a_4, a_6, \mathfrak{r}, \mathfrak{n}) = 0$,*
- *$\psi_k(a_1, a_2, a_3, a_4, a_6, \mathfrak{r}, \mathfrak{n})$ est une unité de $\mathbf{R}$ pour tout $1 \leq k \leq d-1$.*

Alors $T = (\mathfrak{r}, \mathfrak{n})$ est un point d'ordre exact d sur la courbe elliptique de Weierstrass $E/\mathbf{R}$ d'équation

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

On fixe $\mathfrak{a} = 1$, $c_1 = \mathrm{Tr}(u_{O,T})$, $\mathfrak{b} = (1 - c_1)/d$ et $u_k = \mathfrak{a}u_{kT,(k+1)T} + \mathfrak{b}$. Alors l'anneau

$$\mathbf{R}[E - E[d]] = \mathbf{R}[\frac{1}{\psi_d(x,y)}, x, y]/\Lambda(a_1, a_2, a_3, a_4, a_6, x, y)$$

est une algèbre libre étale de rang d sur

$$\mathbf{R}[E' - \mathrm{Ker}I'] = \mathbf{R}[\frac{1}{D(x')}, x', y']/\Lambda(a'_1, a'_2, a'_3, a'_4, a'_6, x', y')$$

et $(u_l)_{l \in \mathbf{Z}/d\mathbf{Z}}$ en est une base.

Pour tout $k \in \mathbf{Z}/d\mathbf{Z}$, on a $\sigma(u_k) = u_{k+1}$ où σ est le $\mathbf{R}[E' - \mathrm{Ker}I']$-automorphisme de $\mathbf{R}[E - E[d]]$ induit par la translation τ_{-T}.

En réduisant modulo $I^{-1}(A)$ où A est une section de $E'(\mathbf{R})$ qui ne rencontre pas le noyau de l'isogénie duale $I' : E' \to E$, on obtient :

Théorème 6.2.6 (Ezome et Lercier)**.** *Soient $d \geq 3$ un entier impair et $\mathbf{R}$ un anneau commutatif unitaire dans lequel d est inversible. Soient $a_1, a_2, a_3, a_4, a_6, \mathfrak{r}$ et $\mathfrak{n}$ des éléments de $\mathbf{R}$ tels que $\Delta(a_1, a_2, a_3, a_4, a_6)$ est une unité de $\mathbf{R}$ et le point $T = (\mathfrak{r}, \mathfrak{n})$ est d'ordre exact d sur la courbe elliptique de Weierstrass $E/\mathbf{R}$ d'équation*

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

Soient $I : E \to E'$ l'isogénie de Vélu de noyau $< T >$ et $A = (x'(A), y'(A)) \in E'(\mathbf{R})$ une section qui ne rencontre pas le noyau de l'isogénie duale $I' : E' \to E$ (cela revient à dire que $D(x'(A))$ est une unité de $\mathbf{R}$). Soit $\mathfrak{F}_A = (x' - x'(A), y' - y'(A))$ l'idéal de

$$\mathbf{R}[E - [d]] = \mathbf{R}[\frac{1}{\psi_d(x,y)}, x, y]/\Lambda(a_1, a_2, a_3, a_4, a_6, x, y)$$

correspondant au point A. Soit

$$\mathbf{S} = \mathbf{R}[\frac{1}{\psi_d(x,y)}, x, y]/(\Lambda(a_1, a_2, a_3, a_4, a_6, x, y), \mathfrak{F}_A),$$

l'anneau résiduel de $I^{-1}(A)$. *Alors* $\mathbf{S}$ *est une* $\mathbf{R}$*-algèbre libre étale de rang* d. *Et si on note*

$$\begin{array}{rccc} \sigma : & \mathbf{S} & \to & \mathbf{S} \\ & f \bmod \mathfrak{F}_A & \mapsto & f \circ \tau_{-T} \bmod \mathfrak{F}_A \end{array} \tag{6.7}$$

le $\mathbf{R}$*-automorphisme induit sur* $\mathbf{S}$ *par la translation* τ_{-T}, *alors* $\mathbf{S}$ *est un* $\mathbf{R}[\sigma]$*-module libre de rang* 1.

Si de plus on fixe $\mathfrak{a} = 1$, $\mathfrak{b} = (1 - c_1)/d$, $u_k = \mathfrak{a}u_{kT,(k+1)T} + \mathfrak{b}$ *et* $\theta_k = u_k \bmod \mathfrak{F}_A$, *alors* $\sigma(\theta_k) = \theta_{k+1}$, *et* $\Theta = (\theta_k)_{k \in \mathbf{Z}/d\mathbf{Z}}$ *est une* $\mathbf{R}$*-base de* $\mathbf{S}$. *Si* $M = (x(M), y(M)) \in E(\mathbf{R})$ *est une section auxiliaire ne rencontrant pas* $E[d]$, *alors la loi de multiplication de l'anneau* $\mathbf{S}$ *est donnée par l'équation* (6.8) *ci-dessous.*

Un anneau $\mathbf{S}$ tel que celui du théorème 6.2.6 est dit *anneau des périodes elliptiques.*

Pour compléter l'énoncé de ce théorème, nous décrivons maintenant la loi de multiplication dans l'anneau résiduel $\mathbf{S}$.

6.2.4 Loi de multiplication dans l'anneau S

Nous explicitons ici la loi de multiplication dans $\mathbf{S}$. Soient $\alpha = \sum_{k \in \mathbf{Z}/d\mathbf{Z}} \alpha_k \theta_k$ et $\beta = \sum_{k \in \mathbf{Z}/d\mathbf{Z}} \beta_k \theta_k$ deux éléments de $\mathbf{S}$ de vecteurs coordonnées respectifs $\overrightarrow{\alpha} = (\alpha_k)_{k \in \mathbf{Z}/d\mathbf{Z}} \in \mathbf{R}^d$ et $\overrightarrow{\beta} = (\beta_k)_{k \in \mathbf{Z}/d\mathbf{Z}} \in \mathbf{R}^d$ dans la base Θ. Alors les veteurs coordonnées de $\sigma(\alpha)$ et $\sigma(\beta)$ sont $\sigma(\overrightarrow{\alpha}) = (\alpha_{k-1})_{k \in \mathbf{Z}/d\mathbf{Z}}$ et $\sigma(\overrightarrow{\beta}) = (\beta_{k-1})_{k \in \mathbf{Z}/d\mathbf{Z}}$. En notant $\mathcal{L} \subset \mathbf{R}[E - E[d]]$ le $\mathbf{R}$-module engendré par les u_k pour $k \in \mathbf{Z}/d\mathbf{Z}$. La réduction modulo $\mathfrak{F}_A$ définit un isomorphisme de $\mathbf{R}$-modules :

$$\begin{array}{rccc} \epsilon_A : & \mathcal{L} & \to & \mathbf{S} \\ & f & \mapsto & f \bmod \mathfrak{F}_A. \end{array}$$

Donc les éléments de $\mathbf{S}$ peuvent être représentés par ceux de $\mathcal{L}$.

On suppose que $M = (x(M), y(M)) \in E(\mathbf{R})$ est une section ne rencontrant pas $E[d]$, donc l'image $N = I(M)$ de M par I est telle que l'anneau résiduel en $I^{-1}(N)$ est un $\mathbf{R}$-module libre de rang d et l'application d'évaluation

$$\begin{array}{rccc} \epsilon_N : & \mathcal{L} & \to & \mathbf{R}^d \\ & f & \mapsto & (f(M + kT))_{k \in bZ/d\mathbf{Z}}. \end{array}$$

est une bijection. Le vecteur

$$\overrightarrow{u_N} = (u_0(M + kT))_{k \in \mathbf{Z}/d\mathbf{Z}}$$

est inversible pour le produit de convolution [[10] section 4.3] dans $\mathbf{R}^d$. On note $\overrightarrow{u_N}^{-1}$ son inverse. On pose

$$\overrightarrow{x_N} = \epsilon_N(x) = (x(M + kT))_{k \in \mathbf{Z}/d\mathbf{Z}}.$$

Et on note

$$\zeta_k = x_k \bmod \mathfrak{F}_A$$

pour tout $k \in \mathbf{Z}/d\mathbf{Z}$. Puisque $\mathbf{S}$ est libre sur $\mathbf{R}$ et que Θ en est une base, il existe un système de scalaires $(\hat{\imath}_k)_{k \in \mathbf{Z}/d\mathbf{Z}}$ de $\mathbf{R}$ tels que

$$\zeta_0 = \sum_{k \in \mathbf{Z}/d\mathbf{Z}} \hat{\imath}_k \theta_k.$$

La multiplication, dans la $\mathbf{R}$-base Θ, de $\overrightarrow{\alpha}, \overrightarrow{\beta} \in \mathbf{S}$ est donnée par

$$\overrightarrow{\alpha}\,\overrightarrow{\beta} = (\mathfrak{a}^2 \overrightarrow{\hat{\imath}}) \star \Big((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta})) \Big) +$$
$$\overrightarrow{u_N}^{-1} \star \Big((\overrightarrow{u_N} \star \overrightarrow{\alpha}) \diamond (\overrightarrow{u_N} \star \overrightarrow{\beta}) - (\mathfrak{a}^2 \overrightarrow{x_N} \star \Big((\overrightarrow{\alpha} - \sigma(\overrightarrow{\alpha})) \diamond (\overrightarrow{\beta} - \sigma(\overrightarrow{\beta})) \Big) \Big). \qquad (6.8)$$

Notation : Si $\overrightarrow{\alpha} = (\alpha_i)_{i \in \mathbf{Z}/d\mathbf{Z}}$ et $\overrightarrow{\beta} = (\beta_i)_{i \in \mathbf{Z}/d\mathbf{Z}}$ sont deux éléments de $\mathbf{S}$, on note $\overrightarrow{\alpha} \diamond \overrightarrow{\beta}$ le produit composante par composante . On note $\overrightarrow{\alpha} \star_j \overrightarrow{\beta} = \sum_i \alpha_i \beta_{j-i}$ la j-ième composante du produit de convolution, et enfin on note $\overrightarrow{\alpha} \star \overrightarrow{\beta} = (\overrightarrow{\alpha} \star_i \overrightarrow{\beta})_i$ le produit convolution.

6.3 Le cas des courbes modulo n

Maintenant que nous savons construire des algèbres libres étales $\mathbf{S}$ sur un anneau commutatif unitaire $\mathbf{R}$ (et donc en particulier sur $\mathbf{Z}/n\mathbf{Z}$), il ne reste plus qu'à inclure un argument combinatoire pour obtenir un critère de primalité de type AKS.

6.3.1 Un critère de primalité

Le théorème 5.4.1 appliqué à un anneau de périodes elliptiques conduit au critère de primalité suivant :

Corollaire 6.3.1 (Critère AKS elliptique, Ezome et Lercier)**.** *Soient $n \geq 2$ un entier et E une courbe elliptique de Weierstrass définie sur $\mathbf{R} = \mathbf{Z}/n\mathbf{Z}$. Soit $T \in E(\mathbf{R})$ une section d'ordre exact d où d est un entier premier avec $2n$. Soient $I : E \to E'$ l'isogénie de Vélu de noyau $< T >$ et $A \in E'(\mathbf{R})$ une section qui ne rencontre pas le noyau de l'isogénie duale $I' : E' \to E$ (i.e $D(x'(A))$ est une unité de $\mathbf{R}$).*

Supposons que l'égalité

$$(\theta_0)^n = \theta_1 \tag{6.9}$$

est vérifiée dans l'anneau des périodes elliptiques

$$\mathbf{S} = \mathbf{R}[x, y, 1/\psi_d(x, y)]/(x' - x'(A), y' - y'(A)).$$

Supposons de plus que

$$2^{\frac{d-1}{2}} \geq n^{\sqrt{d}}. \tag{6.10}$$

Alors n est une puissance d'un nombre premier.

6.3.2 Commentaires

Le corollaire 6.3.1 ci-dessus donne lieu à un algorithme probabiliste de preuve de primalité constitué de trois étapes principales :

1. La vérification de l'équation (6.10) (*i.e* le choix de d) ;
2. La construction d'un anneau des périodes elliptiques $\mathbf{S}$ (via la construction d'une courbe elliptique modulo n grâce à la théorie de la multiplication complexe) ;
3. La vérification de l'équation (6.9) ($O(\log n)$ multiplications dans $\mathbf{S}$).

L'algorithme obtenu est de complexité $O((\log n)^4(\log\log n)^{2+o(1)})$, l'étape 3 est la plus coûteuse (le $o(1)$ désigne une fonction de n qui tend vers 0 quand n tend vers l'infini).

On peut trouver un degré d de taille $O((\log n)^2)$.

6.3.3 Exemple

Nous voulous prouver que l'entier $n = 1009$ est premier en utilisant le critère AKS elliptique.

On commence par vérifier que n n'est pas une puissance propre d'un entier.

Ensuite on s'intéresse au choix du degré d. Une condition suffisante sur d est

$$d \geq d_{min} \text{ avec } d_{min} = \lfloor 4(\log_2 n)^2 + 2 \rfloor. \tag{6.11}$$

Pour cet exemple, on a $d_{min} = \lfloor 4(\log_2 n)^2 + 2 \rfloor = 401$.

Soit E la courbe elliptique d'équation

$$y^2 + xy = x^3 + 364x + 907$$

définie sur $\mathbf{Z}/1009\mathbf{Z}$. On vérifie que $T = (296, 432)$ est une section de E d'ordre exact $d = 479$.

Les formules de Vélu nous donnent la courbe elliptique quotient

$$E' = E/ < T >: y^2 + xy = x^3 + 130x + 233.$$

Le point $A = (383, 201) \in E'$ ne rencontre pas le noyau de l'isogénie duale I' de $I : E \to E'$ (A est d'ordre exact d, les propriétés de l'accouplement de Weil permettent de conclure).

En suivant le théorème 6.2.6, on définit :
– un anneau résiduel $\mathbf{S} = (\mathbf{Z}/1009\mathbf{Z})[E - E[d]]/\mathfrak{F}_A$;
– une $\mathbf{Z}/1009\mathbf{Z}$-base $\Theta = (\theta_k)_{k \in \mathbf{Z}/d\mathbf{Z}}$ de $\mathbf{S}$.

On vérifie que

$$\theta_0^{1009} = \theta_{91}.$$

Puisque 91 est premier à $d = 479$ et à 1009, le point $T' = 91T$ est d'ordre exact d et le système $\Theta' = (\theta'_k)_{k \in \mathbf{Z}/d\mathbf{Z}}$ obtenue en posant $\theta'_k = \theta_{91k}$ (pour tout $k \in \mathbf{Z}/d\mathbf{Z}$) est une base normale elliptique de $\mathbf{S}$.

On vérifie que

$$(\theta'_0)^{1009} = \theta'_1.$$

Le corollaire 6.3.1 nous permet donc de conclure que 1009 est premier.

Bibliographie

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2) :781–793, 2004.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[3] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203) :29–68, 1993.

[4] Daniel J. Bernstein. Detecting perfect powers in essentially linear time. *Math. Comp.*, 67(223) :1253–1283, 1998.

[5] Daniel J. Bernstein. Proving primality in essentially quartic random time. *Math. Comp.*, 76(257) :389–403 (electronic), 2007.

[6] N. Bourbaki. *Éléments de mathématique. Fascicule XXVII. Algèbre commutative. Chapitre 1 : Modules plats. Chapitre 2 : Localisation.* Actualités Scientifiques et Industrielles, No. 1290. Herman, Paris, 1961.

[7] N. Bourbaki. *Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5 : Entiers. Chapitre 6 : Valuations.* Actualités Scientifiques et Industrielles, No. 1308. Hermann, Paris, 1964.

[8] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics.* Springer-Verlag, Berlin, 1993.

[9] Harvey Cohn. Some examples of Weber-Hecke ring class field theory. *Math. Ann.*, 265(1) :83–100, 1983.

[10] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields Appl.*, 15(1) :1–22, 2009.

[11] Andreas Enge. *Elliptic curves and their applications to cryptography, an introduction.* Kluwer Academic Publishers, Boston, 1999.

[12] Andreas Enge and François Morain. Fast decomposition of polynomials with known Galois group. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 254–264. Springer, Berlin, 2003.

[13] Tony Ezome and Reynald Lercier. Elliptic periods and primality proving. *Soumis*, pages 1–26, 2009.

[14] J. Franke, T. KLeinjung, F. Morain, and T. Wirth. Proving primality of very large numbers with fastecpp. *Mathematish institut*, 2004.

[15] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, 2003.

[16] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 175–182 (electronic), New York, 2001. ACM.

[17] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[18] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[19] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[20] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[21] H. W. Lenstra, Jr. Galois theory for schemes. *http ://websites.math.leidenuniv.nl/algebra/GSchemes.pdf*, 1985.

[22] H. W. Lenstra, Jr. Elliptic curves and number-theoretic algorithms. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 99–120, Providence, RI, 1987. Amer. Math. Soc.

[23] H.W. Lenstra and C. Pomerance. Primality testing with gaussian periods. *http ://math.dartmouth.edu/ carlp/PDF/complexity12.pdf*, 2005.

[24] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[25] F. Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp.*, 76(257) :493–505 (electronic), 2007.

[26] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[27] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[28] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1) :219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[29] René Schoof. Four primality testing algorithms. In *Algorithmic number theory : lattices, number fields, curves and cryptography*, Math. Sci. Res. Inst. Publ., pages 101–126. Cambridge Univ. Press, Cambridge, 2008.

[30] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[31] Jacques Vélu. Courbes elliptiques munies d'un sous-groupe $\mathbf{Z}/n\mathbf{Z} \times \mu_n$. *Bull. Soc. Math. France Mém.*, (57) :5–152, 1978.

[32] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.