ÉCOLE NORMALE SUPÉRIEURE DE CACHAN
ANTENNE DE BRETAGNE
-
UNIVERSITÉ DE RENNES 1

RAPPORT DE STAGE

Stage de fin de 2e année de Magistère de Mathématiques
Du 13 mai au 5 juillet 2013

IMPLÉMENTATION D'ALGORITHMES POUR LA RÉSOLUTION DU PROBLÈME DU LOGARITHME DISCRET SUR LES COURBES ELLIPTIQUES SUR DES CORPS FINIS

Salim ROSTAM

Sous la direction de Claus DIEM
Universität Leipzig (Allemagne)
Mathematisches Institut – Abteilung Algebra

Table des matières

Remerciements

Je remercie M. Claus Diem de m'avoir proposé ce stage passionnant dans cette université flambant neuve de Leipzig.

Merci également à ses deux doctorants, Sebastian et Matthias, avec qui j'ai partagé leur bureau pendant ces deux mois. Je tiens également à remercier les autres doctorants du 5^{e} étage pour ces nombreuses parties de beach-volley ! Encore une fois merci à Sebastian, qui a passé une partie de son temps à m'expliquer tant de choses.

Je termine en remerciant Hagen, qui m'a hébergé durant tout ce temps !

Introduction

La sécurité des données est aujourd'hui un problème essentiel : lorsque l'on réalise un achat en ligne par carte bancaire ou par exemple lorsque l'on tient une conversation téléphonique, on n'a pas envie que les données échangées soient accessibles par une tierce personne. C'est pourquoi il est important de savoir crypter les données, en particulier de savoir les décrypter.

De nombreuses méthodes ont été inventées pour garantir un certain niveau de sécurité lors d'un échange d'information. Dans tous les cas, l'expéditeur (respectivement le destinataire) a besoin d'une *clé*, d'une méthode pour pouvoir crypter (resp. décrypter) le message ; on peut distinguer deux types de clés.

- Les clés *privées* (ou *symétriques*) : celui qui a crypté le message doit transmettre sa propre clé au destinataire qui l'utilise alors pour décrypter le message. Des exemples célèbres sont le « chiffre de César », le rouleau assyrien, ou plus simplement un banal mot de passe.
- Les clés *publiques* (ou *assymétriques*) : chaque personne possède deux clés, l'une qu'il garde pour lui seul (la clé privée) et l'autre à la vue de tous (la clé publique). Si A veut envoyer un message à B, A utilise la clé publique de B pour crypter son message et B utilise sa propre clé privée pour le décrypter. L'exemple d'un cadenas ouvert que B envoie et dont B seul possède la clé illustre parfaitement ce fait.

Remarquons que l'on peut transmettre une clé privée par l'intermédiaire d'un cryptage à clé publique : si l'on reprend l'exemple de B qui envoie un cadenas ouvert à A dont B seul possède la clé, il suffit à A de mettre une clé C, dont il est le seul à posséder le double, dans une boîte (scellée par le cadenas) qu'il renvoie à B ; ainsi A et B sont les seuls à posséder la clé C. Un cas particulier d'un tel échange de clé est le procédé de *Diffie–Hellman*, qui repose sur l'hypothèse que le problème du logarithme discret est très difficile à résoudre : voici comment il fonctionne.

- A et B se mettent d'accord sur un groupe G et un élément $g \in G$ d'ordre n (fini) ; ils peuvent faire cet échange de manière non cryptée ;
- A choisit un entier $0 < a < n$ et envoie g^a à B ;
- B choisit un entier $0 < b < n$ et envoie g^b à A ;
- A utilise l'entier a et l'élément g^b qu'il a reçu pour calculer g^{ba} ;
- B utilise l'entier b et l'élément g^a qu'il a reçu pour calculer $g^{ab} = g^{ba}$.

Ainsi, la clé (secrète) qu'ils ont en commun est g^{ab}. Si un espion surveille leurs échanges, alors cet espion a accès à G, g, g^a, g^b : le problème du logarithme discret étant très difficile à résoudre, il lui est très difficile d'obtenir a, b à partir de g^a, g^b. Savoir résoudre efficacement le problème du logarithme discret est donc essentiel pour garantir la sécurité de tels échanges.

Parmi les algorithmes permettant de résoudre le problème du logarithme discret, certains sont applicables dans n'importe quel groupe : on parle d'algorithme *générique*. Les algorithmes non génériques sont donc écrits (ou optimisés) pour certains groupes uniquement, l'intérêt étant que la complexité est alors meilleure que celle des algorithmes génériques. C'est en particulier le cas pour les algorithmes de résolution du problème du logarithme discret dans le groupe des points rationnels d'une courbe elliptique, ou dans le groupe des classes d'un corps de fonctions (on explicitera tout cela bien sûr dans la suite).

Dans ce rapport, on s'intéresse à un morphisme qui transfère le problème du logarithme discret d'un certain groupe dans un autre, dans l'optique de savoir le résoudre plus efficacement dans le groupe d'arrivée ; l'article de base est [4]. Avant de pouvoir présenter ce morphisme, on va tout d'abord présenter la théorie des *corps de fonctions algébriques en une variable* puis définir la notion de *diviseur*. On va ensuite définir la *conorme* puis la *norme* d'un diviseur : on sera à ce stade prêt à

présenter le morphisme qui nous intéresse. Précisons que dans ce rapport, l'accent a été mis sur les outils mathématiques nécessaires et non pas sur le problème du logarithme discret en lui-même.

Le but de ce stage étant d'implémenter ce morphisme en MAGMA (note [1]), pour les besoins de la programmation on va définir en outre les idéaux *fractionnaires* qui vont servir à établir une autre représentation des diviseurs. Finalement, on présentera quelques points du programme que j'ai entièrement réalisé (son intégralité se trouvant en annexe) en vérifiant les hypothèses mathématiques nécessaires à son bon fonctionnement.

Bien que les questions de complexité des programmes soient essentielles à la cryptographie, cet aspect n'a été que peu abordé durant ce stage pour se concentrer sur la compréhension des objets mathématiques et sur la programmation.

1 Le problème du logarithme discret

1.1 Le problème

Soit G un groupe et soit $x \in G$ un élément d'ordre fini. Si $y \in G$ est dans $\langle x \rangle$ on peut écrire (en notation additive) $y = mx$ pour un $m \in \mathbb{Z}$. L'entier m est donc le logarithme de y en base x : on parle de *logarithme discret*.

Concrètement, voici comment le problème se présente : on dispose d'un groupe fini G et de deux éléments $x, y \in G$; on sait que $y \in \langle x \rangle$ et l'on désire trouver un $m \in \mathbb{Z}$ tel que $y = mx$. On va présenter trois algorithmes génériques de résolution.

1.2 Algorithme naïf de résolution

On peut bien sûr considérer la suite $0, x, 2x, 3x, \ldots$; étant donné que G est fini et que $y \in \langle x \rangle$ on va inéluctablement tomber sur y. Cette méthode a une complexité temporelle au pire en $\mathcal{O}(\#G)$ et une complexité spatiale en $\mathcal{O}(1)$.

1.3 Algorithme « baby-step giant-step » de Shanks

L'algorithme repose sur la proposition suivante.

Proposition 1.1. *Soit G un groupe fini et $x, y \in G$. Alors :*

$$y \in \langle x \rangle \iff \exists a, b \in \{0, \ldots, n-1\}, y - bx = anx$$

où $n := \lceil \sqrt{\#G} \rceil$.

Démonstration. Tout d'abord, la condition suffisante est trivialement vérifiée. Écrivons $y = mx$ avec $m \in \{0, \ldots, \#G - 1\}$. On écrit à présent la division euclidienne de m par n : $m = an + b, 0 \leqslant b < n$. Étant donné que $m < \#G \leqslant n^2$, on a $a < n$. On a $y = mx = (an + b)x$ donc $y - bx = anx$. □

On procède alors ainsi ; soit $y \in \langle x \rangle$.

1. On calcule d'abord les « *baby steps* », donnés par $\{(b, y - bx)\}_{0 \leqslant b < n}$; on remarque que l'on peut s'arrêter si l'on trouve un $(b, 0)$.
2. On calcule ensuite les « *giant steps* », donnés par $\{(a, anx)\}_{0 \leqslant a < n}$.
3. On recherche un élément en commun dans les deuxièmes coordonnées des deux ensembles précédents : on est sûr qu'il en existe un par la proposition précédente. Un logarithme que l'on cherche est donc $an + b$.

1. `http://magma.maths.usyd.edu.au/magma/`

La complexité des deux premières étapes est bien sûr en $\mathcal{O}(n)$. Pour ce qui est de la recherche d'un élément dans l'intersection, pour peu que l'on sache trier le premier ensemble (en $\mathcal{O}(n \log n)$ opérations par exemple), la recherche d'un élément dans ce premier ensemble prend $\mathcal{O}(\log n)$ opérations : la recherche d'un élément dans l'intersection nécessite donc $\mathcal{O}(n \log n) + n\mathcal{O}(\log n) = \mathcal{O}(n \log n)$. La complexité de l'algorithme est $\mathcal{O}(n \log n)$, ce que l'on écrit $\widetilde{\mathcal{O}}(n)$ (cela signifie que l'on oublie les facteurs logarithmiques).

Finalement, on obtient un algorithme de complexité temporelle et spatiale en $\widetilde{\mathcal{O}}(\sqrt{\#G})$.

Remarque. On a vu qu'il est nécessaire d'avoir une relation d'ordre (totale) sur G ; si l'on ne dispose pas d'une telle relation, l'algorithme reste en $\widetilde{\mathcal{O}}(\sqrt{\#G})$ mais il nécessite au préalable que l'on établisse (une fois pour toutes) un ordre total, par exemple avec une bijection $G \simeq \{1, \ldots, \#G\}$.

1.4 Algorithme ρ de Pollard

Cet algorithme est décrit en [10, algorithme XI.5.3] : il a l'avantage d'avoir également une complexité temporelle en $\widetilde{\mathcal{O}}(\sqrt{\#G})$, mais cette fois la complexité spatiale est réduite à du $\mathcal{O}(1)$.

Remarque. Les deux algorithmes précédents font (pour l'instant) partie des meilleurs algorithmes génériques connus [2].

1.5 Ce qui va suivre

On va considérer le problème du logarithme discret dans des groupes particuliers (les algorithmes de résolution ne seront donc pas génériques) : dans les cas de groupes de classes de diviseurs de degré 0. On va d'abord définir ces groupes puis présenter la *méthode de calcul d'index*[3], qui débouche sur des algorithmes plus efficaces dans certains cas que ceux présentés ci-avant. Puis, je vais présenter le morphisme qui transfert le problème du logarithme discret sur une courbe (hyper)elliptique vers ce même problème mais dans un groupe de classes de diviseurs de degré 0.

2 Théorie des corps de fonctions algébriques en une variable

À partir de maintenant et jusqu'à la fin de cet exposé, si rien n'est précisé k désigne un corps parfait [4].

2.1 Notions de base

2.1.1 Premières définitions

Définition 2.1. On dit que $F|k$ est un *corps de fonctions algébrique en une variable sur* k si F est une extension de corps de k telle qu'il existe $x \in F$ transcendant sur k avec $F/k(x)$ finie.

Remarque. On dira simplement « corps de fonctions » ; durant tout cet exposé, on essaiera de se tenir à la convention suivante : étant donné deux corps F et F', la notation $F'|F$ signifie que F' est un corps de fonctions sur F alors que F'/F signifie simplement que F' est une extension de corps de F.

Exemple. Le corps des fractions rationnelles $k(X)$ est un corps de fonctions sur k.

Dans la suite de cette section, $F|k$ désigne un corps de fonctions.

Définition 2.2. On dit que $F|k$ est *rationnel* s'il existe $x \in F|k$ (transcendant) tel que $F = k(x)$.

2. En pratique, étant donné un groupe G on n'applique pas directement ces méthodes : on procède d'abord à l'algorithme de *Pohlig–Hellman* qui va diviser le problème dans plusieurs sous-groupes de G bien choisis.

3. La terminologie est héritée de C.F. Gauss, qui dans ses *Disquisitiones Arithmeticae* parlait d'« index » pour ce qui est aujourd'hui le calcul du logarithme discret dans le groupe multiplicatif des corps finis.

4. Voir [11, A.9] pour des rappels.

Propriété 2.3. *$y \in F|k$ est transcendant* ssi *$F/k(y)$ est finie.*

Démonstration. $F|k$ est un corps de fonctions donc on sait qu'il existe $x \in F|k$ transcendant tel que $F/k(x)$ est finie. Soit maintenant $y \in F$.

$\Leftarrow$. On suppose que $F/k(y)$ est finie. Si y est algébrique sur k, alors l'extension $k(y)/k$ est finie. En considérant la tour de corps $k \subseteq k(y) \subseteq F$ on en déduit donc que F/k est finie ce qui est absurde puisque $x \in F$ est transcendant sur k.

$\Rightarrow$. On suppose que y est transcendant sur k. Comme $F/k(x)$ est finie, y est algébrique sur $k(x)$. Ainsi, on peut trouver un entier $n \in \mathbb{N}^*$, des polynômes $p_0, \ldots, p_n \in k[x], p_n \neq 0$ tels que :

$$p_n(x)y^n + p_{n-1}(x)y^{n-1} + \cdots + p_0(x) = 0. \tag{1}$$

On écrit $p_j(x) = \sum_{i=0}^{d_j} p_{ij}x^i$ avec $d_j \in \mathbb{N}$ (et $d_j = -1$ si $p_j = 0$), $p_{ij} \in k$ et $p_{d_j,j} \neq 0$ si $p_j \neq 0$. Comme y est transcendant sur k, il existe un $j_0 \in \{0, \ldots, n\}$ tel que p_{j_0} n'est pas constant, *i.e.* l'entier $d := \max_{0 \leqslant j \leqslant n}(d_j)$ est supérieur ou égal à 1 ; pour $i > d_j$ on pose $p_{ij} := 0$. L'égalité (1) devient alors $\sum_{j=0}^{n}\sum_{i=0}^{d} p_{ij}x^iy^j = 0$ d'où en permutant les sommes :

$$\sum_{i=0}^{d}\left(\sum_{j=0}^{n} p_{ij}y^j\right)x^i = 0,$$

égalité qui devient $\sum_{i=0}^{d} q_i(y)x^i = 0$ avec $q_i(y) := \sum_{j=0}^{n} p_{ij}y^j \in k[y]$. Comme y est transcendant sur k, on a l'identification $k[y] \simeq k[X]$; ainsi, comme $p_{d_{j_0},j_0} \neq 0$ on a $q_{d_{j_0}} \neq 0$. Par choix de j_0 on a $d_{j_0} \geqslant 1$ donc :

$$x \text{ est algébrique sur } k(y).$$

Finalement, comme $k(x) \subseteq k(x,y) \subseteq F$ et que $F/k(x)$ est finie on a $F/k(x,y)$ finie ; de plus, on vient de montrer que $k(x,y)/k(y)$ est finie. En considérant la tour de corps $k(y) \subseteq k(x,y) \subseteq F$ on en déduit donc que $F/k(y)$ est finie. □

Remarque. Si $x \in F|k$ est transcendant, on dit que x est un élément *séparant* si l'extension $F/k(x)$ est séparable [5]. En particulier, si $x \in F|k$ transcendant est séparant, alors l'extension $F/k(x)$ est finie et séparable donc on peut lui appliquer le théorème de l'élément primitif (cf. [11, A.10]) : on peut donc trouver $y \in F$ (algébrique sur $k(x)$) tel que $F = k(x)[y] = k(x,y)$. On peut voir dans [11, proposition 3.10.2.(a)] que de tels éléments existent toujours ; remarquons que l'on a besoin de l'hypothèse k parfait. On peut donc sans perdre en généralité faire l'hypothèse suivante dans toute la suite : quand on choisit un élément $x \in F|k$ transcendant, on suppose qu'il existe un $y \in F$ (algébrique sur $k(x)$) tel que $F = k(x)[y]$. (On pourrait parler d'élément « monogénéisant ».)

Définition 2.4. On dit que $F|k$ est *régulier* si k est algébriquement clos dans F, *i.e.* tout élément de F algébrique sur k est dans k.

La condition de régularité est en particulier vérifiée si k est algébriquement clos ; outre ce cas qui ne concerne pas les corps finis, on verra plus tard que les corps de fonctions (hyper)elliptiques sont réguliers.

Définition 2.5. Un *anneau de valuation* de $F|k$ est un anneau $\mathcal{O}$ qui vérifie les deux conditions suivantes :

- $k \subsetneq \mathcal{O} \subsetneq F$;
- $\forall f \in F^*, f \in \mathcal{O}$ ou $f^{-1} \in \mathcal{O}$.

5. On rappelle qu'une extension de corps L/K est dite séparable si elle est algébrique et si tout élément de L/K est séparable (voir aussi [11, A.7]). Dans notre cas, l'extension est bien algébrique car elle est finie par la propriété précédente.

Lemme 2.6. *Soit $x \in F|k$ un élément transcendant. Alors $k(x)$ n'est contenu dans aucun anneau de valuation de $F|k$.*

Démonstration. D'après l'hypothèse que l'on a faite au début de cette section, il existe $y \in F$ (algébrique sur $k(x)$) tel que $F = k(x)[y]$. Si $y = 0$ alors $F|k$ est régulier ; si $\mathcal{O}$ est un anneau de valuation de $F|k$ alors on a par définition $\mathcal{O} \subsetneq F = k(x)$ ce qui démontre le lemme. On suppose donc maintenant $y \neq 0$; remarquons alors que l'on a également $F = k(x)[y^{-1}]$: en effet, la famille $(y^{-i})_{0 \leqslant i < [F:k(x)]}$ est $k(x)$-libre. Soit $\mathcal{O}$ un anneau de valuation de $F|k$; on suppose que $k(x) \subseteq \mathcal{O}$. Comme $\mathcal{O}$ est un anneau de valuation, on a $y \in \mathcal{O}$ ou $y^{-1} \in \mathcal{O}$; ainsi, $k(x)[y]$ ou $k(x)[y^{-1}]$ est inclus dans $\mathcal{O}$ ce qui contredit le fait que $\mathcal{O} \subsetneq F$. □

Propriété 2.7. *Un anneau de valuation $\mathcal{O}$ de $F|k$ est un anneau local, c'est-à-dire qu'il possède un unique idéal maximal.*

Démonstration. Il suffit de montrer que $P := \mathcal{O} \setminus \mathcal{O}^\times$ est un idéal de $\mathcal{O}$.

- Soient $x \in P, z \in \mathcal{O}$. On a $xz \in \mathcal{O}$ et si $xz \in \mathcal{O}^\times$ alors $x \in \mathcal{O}^\times$ ce qui est absurde. Donc $xz \in P$.
- Soient $x, y \in P$. Si x ou y est nul alors $x - y \in P$. Sinon, comme $\mathcal{O}$ est un anneau de valuation on peut supposer $\frac{y}{x} \in \mathcal{O}$. Ainsi, $1 - \frac{y}{x} \in \mathcal{O}$ donc par ce qui précède comme $x \in P$ on a $x - y \in P$.

□

Définition 2.8. On appelle l'unique idéal maximal d'un anneau de valuation une *place*. On note $\mathbb{P}_F$ l'ensemble des places de $F|k$.

Remarque. On dira parfois « place de $\mathbb{P}_F$ » pour désigner un élément de $\mathbb{P}_F$.

Propriété 2.9. *Soit $P \in \mathbb{P}_F$. Il existe un unique anneau de valuation pour lequel P est l'idéal maximal, et cet anneau est donné par $\mathcal{O}_P := \{f \in F^* : f^{-1} \notin P\} \cup \{0\}$.*

Démonstration. Soit $\mathcal{O}$ un anneau de valuation tel que P soit son unique idéal maximal. Montrons tout d'abord la proposition suivante : $\forall f \in F^*, (f \in P \iff f^{-1} \notin \mathcal{O})$.

- Si $f \in P$, alors $f \in \mathcal{O}$ et $f \notin \mathcal{O}^\times$ donc $f \in \mathcal{O}$ et $f^{-1} \notin \mathcal{O}$ donc $f^{-1} \notin \mathcal{O}$.
- Si $f^{-1} \notin \mathcal{O}$ alors comme $\mathcal{O}$ est un anneau de valuation on a $f^{-1} \notin \mathcal{O}$ et $f \in \mathcal{O}$ donc $f \in P$.

On a donc $\forall f \in F^*, (f^{-1} \in P \iff f \notin \mathcal{O})$ et finalement $\forall f \in F^*, (f^{-1} \notin P \iff f \in \mathcal{O})$. $\mathcal{O}$ est donc entièrement déterminé par P et par conséquent est unique ! □

Définition 2.10. Le *degré* d'une place $P \in \mathbb{P}_F$ est défini de la façon suivante :

$$\deg P := \left[\frac{\mathcal{O}_P}{P} : k\right] \in \mathbb{N}^*$$

Cette définition a bien un sens : $\mathcal{O}_P/P$ est bien un corps puisque P est un idéal maximal de $\mathcal{O}_P$. De plus, ce corps est bien une extension de k ; démontrons cela. $\mathcal{O}_P$ étant un anneau de valuation, on a l'injection $k \hookrightarrow \mathcal{O}_P$; le noyau de l'application $k \to \mathcal{O}_P/P$ est alors exactement $k \cap P$. Comme P est un idéal propre de $\mathcal{O} \supseteq k$, P ne contient aucun inversible de $\mathcal{O}$ donc $k \cap P = \{0\}$ et donc $k \to \mathcal{O}_P/P$ est injective. Finalement, [11, proposition 1.1.15] montre que le degré d'une place est fini.

Propriété 2.11. *Si k est algébriquement clos, alors toutes les places de $F|k$ sont de degré* 1.

Démonstration. En effet, $\mathcal{O}_P/P$ est une extension finie donc algébrique de k ; k étant algébriquement clos cette extension est triviale. □

2.1.2 Ordre en une place

$F|k$ désigne toujours un corps de fonctions.

Théorème 2.12. *Soit $\mathcal{O}$ un anneau de valuation de $F|k$, P son unique idéal maximal. Alors P est principal, et si π est un élément qui engendre P on a :*

$$\forall f \in \mathcal{O} \setminus \{0\}, \exists!(u,n) \in \mathcal{O}^\times \times \mathbb{N}, f = u\pi^n.$$

De plus, l'entier n ne dépend pas de l'élément π choisi.

Démonstration. [11, théorème 1.1.6]. Il est clair que n ne dépend pas du générateur choisi car si $\langle\pi\rangle = \langle\rho\rangle$ alors π et ρ sont associés. □

Définition 2.13. Soit $P \in \mathbb{P}_F$, f un élément de $\mathcal{O}_P$. L'entier n de la proposition précédente est appelé *ordre de f en P* et on le note $\mathrm{ord}_P(f)$.

Définition 2.14. Soit $P \in \mathbb{P}_F$. Un élément $\pi \in F$ tel que $P = \langle\pi\rangle$ est appelé un élément *premier* de P.

Propriété 2.15. *Soit $P \in \mathbb{P}_F$. Un élément $\pi \in \mathcal{O}_P$ est un premier de P* ssi $\mathrm{ord}_P(\pi) = 1$.

Démonstration. Soit ρ un premier de P ; on va se servir de cet élément pour calculer ord_P. L'élément π est un premier de P ssi $P = \langle\pi\rangle$ ssi $\exists u \in \mathcal{O}_P^\times, \pi = u\rho$ ssi $\mathrm{ord}_P(\pi) = 1$. □

Propriété 2.16. *Soient $P \in \mathbb{P}_F, f \in \mathcal{O}_P \setminus \{0\}$. Alors $\forall n \in \mathbb{N}, n \leqslant \mathrm{ord}_P(f) \iff f \in P^n$.*

Démonstration. Soit π un élément premier de P et soit $n \in \mathbb{N}$; remarquons que $P^n = \langle\pi\rangle^n = \langle\pi^n\rangle$. Si $n \leqslant \mathrm{ord}_P(f)$, alors on a $f = u\pi^{\mathrm{ord}_P(f)} = u\pi^{\mathrm{ord}_P(f)-n} \cdot \pi^n \in \langle\pi^n\rangle$. Réciproquement, on suppose que $f \in \langle\pi^n\rangle$: on peut donc écrire $f = g\pi^n$ avec $g \in \mathcal{O}_P$. On a $g = u\pi^{\mathrm{ord}_P(g)}$ avec $u \in \mathcal{O}_P^\times$ donc $f = u\pi^{n+\mathrm{ord}_P(g)}$. Par unicité de la décomposition dans le théorème 2.12 on a donc $\mathrm{ord}_P(f) = n + \mathrm{ord}_P(g)$: comme $\mathrm{ord}_P(g) \geqslant 0$ on a $n \leqslant \mathrm{ord}_P(f)$. □

Propriété 2.17. *Soit $f \in k^*$. Alors $\mathrm{ord}_P(f) = 0$ $\forall P \in \mathbb{P}_F$.*

Démonstration. Par définition d'un anneau de valuation, on a $k \subseteq \mathcal{O}_P$ donc $f \in \mathcal{O}^\times$. En écrivant $f = f\pi^0$ on a donc $\mathrm{ord}_P(f) = 0$. □

Soient $P \in \mathbb{P}_F$ et $f \in F \setminus \mathcal{O}_P$; par définition d'un anneau de valuation, on a $f^{-1} \in \mathcal{O}_P$. On définit alors $\mathrm{ord}_P(f) := -\mathrm{ord}_P(f^{-1})$. On obtient ainsi un morphisme $\mathrm{ord}_P : F^* \to \mathbb{Z}$; on notera $\mathrm{ord}_P(0) := \infty$.

Remarque. Si $f \in F^*$ est tel que f et f^{-1} sont dans $\mathcal{O}_P$ alors on a *a priori* deux valeurs pour $\mathrm{ord}_P(f)$. Or, d'après les hypothèses sur f on a $f \in \mathcal{O}_P^\times$ d'où $\mathrm{ord}_P(f) = 0$ donc on n'a bien qu'une seule valeur pour $\mathrm{ord}_P(f)$.

Propriété 2.18. *On a les trois égalités suivantes :*
- $\mathcal{O}_P = \{f \in F : \mathrm{ord}_P(f) \geqslant 0\}$;
- $\mathcal{O}_P^\times = \{f \in F : \mathrm{ord}_P(f) = 0\}$;
- $P = \{f \in F : \mathrm{ord}_P(f) > 0\}$.

Démonstration. Se voit directement avec la définition du prolongement de ord_P à F et en écrivant $f = u\pi^{\mathrm{ord}_P(f)}$. □

Définition 2.19. Soient $f \in F^*$ et $P \in \mathbb{P}_F$.
- Si $\mathrm{ord}_P(f) > 0$ on dit que P est un *zéro* de f ;

– Si $\mathrm{ord}_P(f) < 0$ on dit que P est un *pôle* de f.

Remarque. D'après la propriété 2.17, les éléments de k^* n'ont ni zéro ni pôle.

Proposition 2.20. *Les éléments de F transcendants sur k ont au moins un zéro et un pôle.*

Démonstration. [11, corollaire 1.1.20]. □

Corollaire 2.21. $\mathbb{P}_F \neq \emptyset$.

Démonstration. Par définition d'un corps de fonctions algébrique, il existe $x \in F$ transcendant sur k ; il ne reste plus qu'à appliquer la proposition. □

Après ces résultats d'existence, on peut énoncer un résultat de finitude.

Théorème 2.22. *Un élément $f \in F^*$ ne possède qu'un nombre* fini *de zéros et de pôles.*

Démonstration. [11, corollaire 1.3.4]. □

On conclut cette section par deux résultats dont on se servira plus tard.

Théorème 2.23 (Théorème d'approximation, version faible)**.** *Soit $r \in \mathbb{N}^*$; soient $P_1, \ldots, P_r \in \mathbb{P}_F$ des places deux à deux distinctes, $x_1, \ldots, x_r \in F$ et $n_1, \ldots, n_r \in \mathbb{Z}$. Alors il existe un élément $x \in F$ tel que :*

$$\mathrm{ord}_{P_i}(x - x_i) = n_i \quad \forall i \in \{1, \ldots, r\}.$$

Démonstration. [11, théorème 1.3.1] (preuve technique). □

Corollaire 2.24. *Si $F|k$ est régulier alors $\mathbb{P}_F$ est infini.*

Démonstration. On suppose que $\mathbb{P}_F = \{P_1, \ldots, P_r\}$ (remarque : on a vu que $\mathbb{P}_F \neq \emptyset$). On peut utiliser le théorème pour trouver un élément $x \in F$ tel que $\mathrm{ord}_{P_i}(x) \in \mathbb{N}^*$ $\forall i$. Ainsi, x n'a pas de pôle donc d'après la proposition 2.20 l'élément x est algébrique sur k ; comme $F|k$ est régulier, x est en fait dans k. Par la propriété 2.17 on a donc $\mathrm{ord}_{P_i}(x) = 0$ $\forall i$ ce qui est absurde ! □

Théorème 2.25 (Théorème d'approximation, version forte)**.** *Soient $S \subsetneq \mathbb{P}_F$ et $r \in \mathbb{N}$; soient $P_1, \ldots, P_r \in S$ des places deux à deux distinctes, $x_1, \ldots, x_r \in F$ et $n_1, \ldots, n_r \in \mathbb{Z}$. Alors il existe un élément $x \in F$ tel que les deux conditions suivantes soient réunies :*

$$\mathrm{ord}_{P_i}(x - x_i) = n_i \quad \forall i \in \{1, \ldots, r\}$$
$$\mathrm{ord}_P(x) \geqslant 0 \quad \forall P \in S \setminus \{P_1, \ldots, P_r\}$$

Démonstration. [11, théorème 1.6.5] (la démonstration utilise des objets non introduits ici). □

Remarque. Le fait que $\mathbb{P}_F$ soit infini si $F|k$ est régulier ne fonctionne plus avec cette version du théorème !

2.1.3 Diviseurs

À partir de maintenant $F|k$ désigne un corps de fonctions régulier.

Définition 2.26. Le *groupe des diviseurs* $\mathrm{Div}(F)$ du corps de fonctions $F|k$ est le groupe libre abélien engendré par les éléments de $\mathbb{P}_F$. On appelle les éléments de ce groupe des *diviseurs* ; ils s'expriment comme des sommes formelles $\sum_{P\in\mathbb{P}_F} n_P P$ où les entiers n_P sont presque tous nuls (i.e. tous nuls sauf un nombre fini). Le *support* de D est défini par $\mathrm{Supp}(D) := \{P \in \mathbb{P}_F : n_P \neq 0\}$.

Remarque. Si $P \in \mathbb{P}_F$ est une place, on peut donc aussi considérer P comme un élément de $\mathrm{Div}(F)$; les diviseurs de cette forme s'appellent des diviseurs *premiers*.

Définition 2.27. Le *degré* d'un diviseur $D := \sum_{P\in\mathbb{P}_F} n_P P$ est $\deg D := \sum_{P\in\mathbb{P}_F} n_P \deg P$. En particulier, on note $\mathrm{Div}^0(F)$ le sous-groupe de $\mathrm{Div}(F)$ constitué des diviseurs de degré 0.

Définition 2.28. On dit qu'un diviseur $D := \sum_{P\in\mathbb{P}_F} n_P P \in \mathrm{Div}(F)$ est *positif* ou encore *effectif* si $n_P \geqslant 0\ \forall P$. Si $D' \in \mathrm{Div}(F)$ est un autre diviseur, on écrit $D \leqslant D'$ si $D' - D$ est positif.

Le théorème 2.22 permet d'énoncer la définition suivante.

Définition 2.29. Soit $f \in F^*$. On définit le *diviseur principal associé à* f comme étant le diviseur de $\mathrm{Div}(F)$ suivant :

$$\mathrm{div}_F(f) := \sum_{P\in\mathbb{P}_F} \mathrm{ord}_P(f)\, P$$

(On écrira simplement $\mathrm{div}(f)$ quand il n'y a pas de confusion possible.) On dit qu'un diviseur de $\mathrm{Div}(F)$ est *principal* s'il est de la forme $\mathrm{div}(f)$ avec $f \in F^*$; on note $\mathrm{Princ}(F)$ l'ensemble des diviseurs principaux.

Remarque. L'application div hérite de la propriété de morphisme des fonctions ord_P.

Proposition 2.30. $\forall f \in F^*,\ \mathrm{div}(f) = 0 \iff f \in k^*$.

Démonstration. Soit $f \in F^*$. Si $f \in k^*$ alors d'après la propriété 2.17 on a $\mathrm{div}(f) = 0$. Réciproquement, si $\mathrm{div}(f) = 0$ alors par la proposition 2.20 f n'est pas transcendant sur k ; f est donc algébrique sur k, et comme k est algébriquement clos dans F on a $f \in k$ (c'est en fait la réciproque de la propriété 2.17). □

Théorème 2.31. *Tout diviseur principal est de degré nul. Autrement dit :*

$$\forall f \in F^*, \deg \mathrm{div}(f) = 0.$$

Démonstration. [11, théorème 1.4.11]. □

Définition 2.32. Le groupe des *classes de diviseurs de degré* 0 est défini de la façon suivante :

$$\mathrm{Cl}^0(F) := \frac{\mathrm{Div}^0(F)}{\mathrm{Princ}(F)}.$$

Remarque. On va voir que c'est un groupe *fini* si k est fini.

2.1.4 Genre

On considère de nouveau un corps de fonctions régulier $F|k$ avec k un corps parfait, pas forcément fini. Cette section a pour but de définir la notion de *genre*, qui très importante dans la théorie des corps de fonctions.

Définition 2.33. La dimension d'un diviseur $D \in \mathrm{Div}(F)$ est définie par $\ell(D) := \dim \mathcal{L}(D)$ où $\mathcal{L}(D) := \{f \in F^* : \mathrm{div}(f) \geqslant -D\} \cup \{0\}$.

Remarque. L'ensemble $\mathcal{L}(D)$ est un k-espace vectoriel, de dimension finie ([11, proposition 1.4.9]) : c'est l'*espace de Riemann-Roch* associé à D. En particulier, c'est sa dimension en tant que k-espace vectoriel que l'on considère.

Définition 2.34. Le *genre* du corps de fonctions $F|k$ est défini par :

$$g(F) := \max\{\deg D - \ell(D) + 1 : D \in \mathrm{Div}(F)\}.$$

Théorème 2.35. *Le genre d'un corps de fonctions est un entier naturel.*

Démonstration. [11, corollaire 1.4.16]. □

2.1.5 Nombre de classes

Comme on l'a mentionné dans l'introduction, on va plus tard s'intéresser au problème du logarithme discret dans $\mathrm{Cl}^0(F)$ où $F|\mathbb{F}_q$ est un corps de fonctions. Il est ainsi utile de connaître le cardinal de ce groupe $\mathrm{Cl}^0(F)$: c'est ce que l'on a appelé le *nombre de classes*, noté h_F. En accord avec la remarque qui suit la définition des groupes Cl^0, on va montrer dans cette section que $h_F < \infty$ et on va même donner un équivalent asymptotique (quand $q \to +\infty$). On fixe dans la suite un corps de fonctions $F|\mathbb{F}_q$ où q est une puissance d'un nombre premier.

Définition 2.36. On définit le L-polynôme de $F|\mathbb{F}_q$ par :

$$L_F(t) := (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n \in \mathbb{Z}[[t]]$$

où les A_n sont donnés par $A_n := \#\{A \in \mathrm{Div}(F) : A \geqslant 0 \text{ et } \deg A = n\}$.

Remarque. Les A_n sont finis par [11, lemme 5.1.1] ; la série entière $\sum_{n=0}^{\infty} A_n t^n$ a un rayon de convergence non nul ([11, proposition 5.1.6]) et on l'appelle la *fonction Zêta* de $F|\mathbb{F}_q$.

Proposition 2.37. *L_F est un polynôme et de degré $2g$ et $L_F(1) = h_F$.*

Démonstration. On déduit de [11, corollaire 5.1.12] que L_F est un polynôme ; les points (a) et (c) de [11, théorème 5.1.15] concluent. □

La proposition permet de factoriser L_F dans $\mathbb{C}[t]$ sous la forme suivante :

$$L_F(t) = \prod_{n=1}^{2g}(1-\alpha_n t)$$

où $\alpha_n \in \mathbb{C}$; on a bien $L_F(0) = 1$ car $A_0 = 1$ (seul 0 est un diviseur positif de degré 0).

Théorème 2.38 (Hasse–Weil)**.** *Les élément α_n précédents vérifient $|\alpha_n| = \sqrt{q}$ $\forall n \in \{1, \ldots, 2g\}$.*

Remarque. Ce théorème est aussi appelé « hypothèse de Riemann pour les corps de fonctions » ; voir [11, remarque 5.2.2] pour plus de détails.

Démonstration. [11, théorème 5.2.1]. □

Corollaire 2.39. $(\sqrt{q}-1)^{2g} \leqslant h_F \leqslant (\sqrt{q}+1)^{2g}$.

Démonstration. Par la proposition précédente on a $h_F = L_F(1)$; ainsi, $h_F = \prod_{n=1}^{2g}(1-\alpha_n) = \left|\prod_{n=1}^{2g}(1-\alpha_n)\right| = \prod_{n=1}^{2g}|1-\alpha_n|$ et on conclut en utilisant les deux inégalités triangulaires et le théorème. □

Ainsi, à g fixé on a $\#\mathrm{Cl}^0(F|\mathbb{F}_q) \sim q^g$; les méthodes présentées dans la section 1 pour la résolution du problème du logarithme discret dans $\#\mathrm{Cl}^0(F|\mathbb{F}_q)$ ont donc une complexité en $\widetilde{\mathcal{O}}(q^{g/2})$.

2.2 Extensions de corps de fonctions algébriques

Dans cette section, tous les corps de fonctions algébriques considérés sont supposés réguliers.

2.2.1 Définitions de base

Définition 2.40. On dit que $F'|k'$ est une extension *algébrique* (respectivement *finie*) de $F|k$ si :
- $k' \supseteq k$;
- F'/F est une extension algébrique (resp. finie) de corps.

Quand rien n'est précisé, $F'|k'$ désigne une extension algébrique de $F|k$, P' une place de $F'|k'$ et P une place de $F|k$.

Propriété 2.41. *L'extension k'/k est algébrique ; ainsi k' est également parfait. De plus, F'/F est finie* ssi *k'/k est finie.*

Démonstration. Soit $x \in F|k$ transcendant ; comme $F/k(x)$ est finie et que F'/F est algébrique, l'extension $F'/k(x)$ est algébrique. Si $x \in k'$, alors $k(x) \subseteq k'$ donc l'extension $F'/k(x)$ serait transcendante ; c'est absurde donc $x \notin k'$. Comme $x \in F'$ et que F'/k' est régulier, on en déduit que x est transcendant sur k'.

Soit maintenant $f \in k'$; f est dans F' donc par ce qui précède f est algébrique sur $k(x)$. On peut donc écrire

$$p_n(x)f^n + \cdots + p_0(x) = 0$$

avec $n \in \mathbb{N}^*, p_i \in k[x], p_n \neq 0$. On a $p_i \in k'[x]$; on vient de voir que x est transcendant sur k' donc on peut identifier $k'[x]$ avec $k'[X]$. Autrement dit, chaque terme (en les puissances de x) de l'égalité précédente est nul ; en considérant le terme en $x^{\deg p_n}$ on obtient que f est algébrique sur k. (Remarquons que l'on a également la réciproque : si k'/k est algébrique alors $k'(x)/k(x)$ donc $F'/k(x)$ et finalement F'/F sont algébriques.)

L'équivalence qui traite du caractère fini est démontré dans [11, lemme 3.1.2.(*b*)]. □

Définition 2.42. On dit que P' est une *extension* de (ou *divise*) P et on écrit $P'|P$ si $P' \supseteq P$.

Proposition 2.43. *On a :*

$$P'|P \text{ ssi } \mathcal{O}_{P'} \supseteq \mathcal{O}_P \text{ ssi } \exists e \in \mathbb{N}^*, \forall x \in F, \mathrm{ord}_{P'}(x) = e \cdot \mathrm{ord}_P(x).$$

De plus, si $P'|P$ alors $P = P' \cap F$ et $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$.

Démonstration. [11, proposition 3.1.4]. □

Définition 2.44. On suppose que $P'|P$; l'entier (unique) e de la proposition précédente est l'*indice de ramification* de P' sur P et on le note $e_{P'|P}$.

Proposition 2.45. *On suppose que $P'|P$; alors pour $e \in \mathbb{N}^*$ on a :*

$$e \leqslant e_{P'|P} \iff P \subseteq P'^e \iff P = P'^e \cap F.$$

En particulier, $e_{P'|P} = \max\{e \in \mathbb{N}^* : P \subseteq P'^e\} = \max\{e \in \mathbb{N}^* : P = P'^e \cap F\}$.

Démonstration. Tout d'abord, une fois les équivalences démontrées les deux égalités sont immédiates. La deuxième équivalence est évidente : on a clairement $\Leftarrow$ et l'autre sens se démontre en disant que si $P \subseteq P'^e$ alors d'une part $P \subseteq P'^e \cap F$ et d'autre part $P \subseteq P'$ donc par la proposition 2.43 $P = P' \cap F \supseteq P'^e \cap F$.

Reste donc à montrer la première équivalence. Soit π un élément premier de P et soit π' un élément premier de P'. Remarquons que $\mathrm{ord}_{P'}(\pi) = e_{P'|P} \,\mathrm{ord}_P(\pi) = e_{P'|P}$. Par la propriété 2.16 on a donc $e \leqslant e_{P'|P}$ ssi $\pi \in P'^e$ ssi $P \subseteq P'^e$. □

Proposition 2.46. *Si $P'|P$ alors $\mathcal{O}_{P'}/P'$ est une extension de corps de $\mathcal{O}_P/P$.*

Démonstration. On suppose que $P'|P$; le noyau de l'application $\mathcal{O}_P \to \mathcal{O}_{P'}/P'$ est $\mathcal{O}_P \cap P' = (\mathcal{O}_P \cap F) \cap P' = \mathcal{O}_P \cap (F \cap P')$ qui est égal par la proposition 2.43 à $\mathcal{O}_P \cap P = P$. □

Définition 2.47. On suppose que $P'|P$; le *degré relatif* (ou *degré d'inertie*) de P' sur P est défini par $f_{P'|P} := [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$.

Proposition 2.48. *On suppose que $P'|P$. Alors $f_{P'|P} < \infty \iff [F' : F] < \infty$.*

Démonstration. [11, proposition 3.1.6.(a)]. □

Remarque. On va en réalité ne considérer que des cas où k et k' sont finis : les degrés d'inertie seront donc toujours finis (cf. propriété 2.41).

Voici une proposition très importante pour la suite.

Proposition 2.49.
- *Chaque place $P' \in \mathbb{P}_{F'}$ divise exactement une place $P \in \mathbb{P}_F$ et cette place est donnée par $P = P' \cap F$.*
- *Chaque place de $F|k$ possède possède un nombre* fini *et non nul d'extensions dans $F'|k'$.*

Démonstration. [11, proposition 3.1.7]. □

Remarque. On n'a pas supposé que l'extension F'/F est finie.

Enfin, mentionnons un théorème qui va nous être utile.

Théorème 2.50 (Égalité fondamentale)**.** *On suppose que l'extension F'/F est finie ; soit $P \in \mathbb{P}_F$. Alors on a la relation suivante :*

$$\sum_{P'|P} e_{P'|P} f_{P'|P} = [F' : F]$$

où P' parcourt $\mathbb{P}_{F'}$.

Remarque. La somme possède un nombre fini de termes par le deuxième point de la proposition 2.49 et chaque terme est fini par la proposition 2.48.

Démonstration. [11, théorème 3.1.11]. □

2.2.2 Conorme, norme (I)

$F'|k'$ désigne toujours une extension algébrique de $F|k$.

Définition 2.51. Si P est une place de $F|k$, on définit sa conorme par :

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e_{P'|P} P' \in \mathrm{Div}(F')$$

où P' parcourt $\mathbb{P}_{F'}$. On prolonge l'application $\mathrm{Con}_{F'/F}$ par linéarité au groupe des diviseurs de $F|k$.

La définition du morphisme de conorme peut sembler pour l'instant un peu mystérieuse ; on va voir d'où il vient dans la section 6.2. Avant cela, on peut quand même voir que ce morphisme « étend » un diviseur de F en un diviseur de F'.

On suppose maintenant que l'extension F'/F est finie.

Proposition 2.52. *L'application* $\mathrm{Con}_{F'/F} : \mathrm{Div}(F) \to \mathrm{Div}(F')$ *envoie les diviseurs de degré* 0 *sur des diviseurs de degré* 0. *Plus encore, elle envoie les diviseurs principaux sur des diviseurs principaux. Finalement, on obtient un morphisme* $\mathrm{Con}_{F'/F} : \mathrm{Cl}^0(F) \to \mathrm{Cl}^0(F')$.

Démonstration. Conséquence de [11, corollaire 3.1.14] pour la première partie et [11, proposition 3.1.9] pour la deuxième. La fin est alors évidente. □

Après avoir vu comment « étendre » un diviseur de F en un diviseur de F', on va voir comment associer un diviseur de F à un diviseur de F' : c'est le rôle du morphisme de norme.

Définition 2.53. On définit la *norme* d'une place $P' \in \mathbb{P}_{F'}$ de la façon suivante :

$$\mathrm{N}_{F'/F}(P') := f_{P'|P} P \in \mathrm{Div}(F)$$

où $P := P' \cap F$ est l'unique place de F que divise P'. On prolonge l'application $\mathrm{N}_{F'/F}$ par linéarité au groupe des diviseurs de $F'|k'$.

Remarque. Le degré relatif $f_{P'|P}$ est fini par la proposition 2.48.

On peut se demander ce que vient faire le degré relatif dans la définition ; c'est essentiellement pour obtenir le théorème qui va suivre. On suppose que F'/F est *galoisienne* ; soit $G := \mathrm{Gal}(F'/F)$ le groupe des automorphismes de F' laissant fixe chaque élément de F.

Lemme 2.54. *Soit* $P' \in \mathbb{P}_{F'}$ *une place qui divise* $P \in \mathbb{P}_F$ *et soit* $\sigma \in G$. *Alors* $\sigma(P') \in \mathbb{P}_{F'}$ *et* $\sigma(P')|P$.

Démonstration. [11, lemme 3.5.2]. □

Lemme 2.55. *Si* $P'_1, P'_2 \in \mathbb{P}_{F'}$ *sont deux places qui divisent une même place* $P \in \mathbb{P}_F$, *alors :*
- $e_{P'_1|P} = e_{P'_2|P} =: e_P$;
- $f_{P'_1|P} = f_{P'_2|P} =: f_P$;
- $\#\{\sigma \in G : \sigma(P'_1) = P'_2\} = e_{P'_1|P} f_{P'_2|P}$.

Démonstration. Les deux premiers points résultent de [11, corollaire 3.7.2.(a)]. Pour le troisième, posons $G_Z^1 := \{\sigma \in G : \sigma(P'_1) = P'_1\}$ et $G_Z^{12} := \{\sigma \in G : \sigma(P'_1) = P'_2\}$. Par [11, théorème 3.7.1], comme F'/F est galoisienne il existe $\rho \in G$ tel que $\rho(P'_1) = P'_2$; ainsi $G_Z^{12} = \rho \circ G_Z^1$. On conclut alors par [11, théorème 3.8.2.(a)] et par le deuxième point. □

Théorème 2.56. *Si* $f \in F'^*$ *alors :*

$$\mathrm{N}_{F'/F}(\mathrm{div}_{F'}(f)) = \mathrm{div}_F(\mathrm{N}_{F'/F}(f)).$$

Remarque. $\mathrm{N}_{F'/F}(f)$ désigne la norme de f en tant qu'élément de l'extension galoisienne F'/F (cf. [11, A.14.(7)]). Ainsi, il est légitime de considérer $\mathrm{div}_F(\mathrm{N}_{F'/F}(f))$ car $\mathrm{N}_{F'/F}(f) \in F$.
Remarque. Le théorème reste valable quand F'/F n'est pas galoisienne, voir [1, p. 108, ch. IV §34].

Démonstration. Soit $f \in F'^*$. On rappelle que les sommes sur P sont indexées par $\mathbb{P}_F$, celles sur P' indexées par $\mathbb{P}_{F'}$; les sommes sur σ sont indexées par G. On a :

$$\mathrm{div}_F(\mathrm{N}_{F'/F}(f)) = \sum_P \mathrm{ord}_P(\mathrm{N}_{F'/F}(f))P = \sum_P \mathrm{ord}_P\left(\prod_\sigma \sigma(f)\right)P\,;$$

pour utiliser la propriété de morphisme de ord_P, il faudrait que $\sigma(f) \in F\ \forall\sigma$. Cela n'étant vérifié que si $f \in F$, on va passer par une fonction $\mathrm{ord}_{P'_0}$ pour une place $P'_0 \in \mathbb{P}_{F'}$ divisant P. On obtient donc :

$$\mathrm{div}_F(\mathrm{N}_{F'/F}(f)) = \sum_P \frac{1}{e_{P'_0|P}} \mathrm{ord}_{P'_0}\left(\prod_\sigma \sigma(f)\right)P = \sum_P \frac{1}{e_{P'_0|P}} \sum_\sigma \mathrm{ord}_{P'_0}(\sigma(f))P$$

d'où en faisant le changement d'indice $\sigma \leftarrow \sigma^{-1}$ et en utilisant [11, lemme 3.5.2.(a)] :

$$\mathrm{div}_F(\mathrm{N}_{F'/F}(f)) = \sum_P \frac{1}{e_{P'_0|P}} \sum_\sigma \mathrm{ord}_{\sigma(P'_0)}(f)P = \sum_P \frac{1}{e_{P'_0|P}} \sum_{P'|P} \sum_{\sigma(P'_0)=P'} \mathrm{ord}_{P'}(f)P.$$

Ainsi, par le lemme précédent :

$$\mathrm{div}_F(\mathrm{N}_{F'/F}(f)) = \sum_P \frac{1}{e_{P'_0|P}} \sum_{P'|P} e_{P'_0|P} f_{P'|P} \,\mathrm{ord}_{P'}(f)P = \sum_P \sum_{P'|P} \mathrm{ord}_{P'}(f)\,\mathrm{N}_{F'|F}(P')$$

et finalement :

$$\mathrm{div}_F(\mathrm{N}_{F'/F}(f)) = \sum_{P'} \mathrm{ord}_{P'}(f)\,\mathrm{N}_{F'|F}(P') = \mathrm{N}_{F'/F}(\mathrm{div}_{F'}(f))$$

par linéarité. □

Remarque. On peut faire la démonstration autrement, en utilisant $\widetilde{\mathrm{N}}_{F'/F}(P') := \sum_{\sigma\in G} \sigma(P') \in \mathrm{Div}(F')$ pour $P' \in \mathbb{P}_{F'}$; remarquons que c'est exactement la même définition pour la trace d'un élément $z \in F'$ (note [6]). On a alors les égalités successives :

$$\forall f \in F'^*, \widetilde{\mathrm{N}}_{F'/F}(\mathrm{div}_{F'}(f)) = \mathrm{div}_{F'}(\mathrm{N}_{F'/F}(f))$$
$$\forall P' \in \mathbb{P}_{F'}, \widetilde{\mathrm{N}}_{F'/F}(P') = f_{P'|P}\,\mathrm{Con}_{F'/F}(P)$$
$$\mathrm{Con}_{F'/F} \circ \mathrm{N}_{F'/F} = \widetilde{\mathrm{N}}_{F'/F}$$

et on se sert de $\mathrm{Con}_{F'/F}(\mathrm{div}_F(f)) = \mathrm{div}_{F'}(f)$ pour $f \in F^*$ (voir [11, proposition 3.1.9]) et de l'injectivité de la conorme pour conclure. On voit donc de manière plus naturelle le degré d'inertie apparaître dans la définition de la norme.

Proposition 2.57. *L'application* $\mathrm{N}_{F'/F} : \mathrm{Div}(F') \to \mathrm{Div}(F)$ *envoie les diviseurs de degré* 0 *sur des diviseurs de degré* 0. *Plus encore, elle envoie les diviseurs principaux sur des diviseurs principaux. Finalement, on obtient un morphisme* $\mathrm{N}_{F'/F} : \mathrm{Cl}^0(F') \to \mathrm{Cl}^0(F)$.

Démonstration. Le deuxième point résulte simplement du théorème précédent. Pour démontrer le premier point, on va en fait démontrer la formule suivante :

$$\forall D' \in \mathrm{Div}(F'), \deg \mathrm{N}_{F'/F}(D') = [k' : k] \deg D'.$$

Par linéarité, il suffit de le démontrer pour les places de F' ; soit $P' \in \mathbb{P}_{F'}$ et soit P l'unique place de F qu'elle divise. On a $\deg \mathrm{N}_{F'/F}(P') = f_{P'|P} \deg P = [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P][\mathcal{O}_P/P : k]$ donc par la formule de multiplicativité des degrés on a $\deg \mathrm{N}_{F'/F}(P') = [\mathcal{O}_{P'}/P' : k'][k' : k] = [k' : k] \deg P'$. □

6. On voit donc que le terme de « trace » serait plus adapté pour les places ; le terme de « norme » provient en fait de la théorie des idéaux, comme on le verra dans la section 6.2.

3 Ellipticité et hyperellipticité

Dans cette section k désigne un corps (parfait) de caractéristique différente de 2 et $\overline{k}$ désigne une clôture algébrique de k. De plus, on désigne toujours par $F|k$ un corps de fonctions. Commençons par introduire une notation et par énoncer un petit lemme.

Définition 3.1. Soit V un sous-ensemble de $\mathbb{P}^2(\overline{k})$ et soit k' un sous-corps de $\overline{k}$. L'ensemble des *points rationnels de V sur k'* est défini par $V(k') := V \cap \mathbb{P}^2(k') = \{\xi \in V : \exists (x, y, z) \in {k'}^3 \setminus \{(0, 0, 0)\}, \xi = (x : y : z)\}$.

Lemme 3.2. *Toute extension de degré 2 d'un corps de caractéristique impaire est séparable.*

Démonstration. Soit K'/K une telle extension. Soit x un élément de K', P son polynôme minimal sur K. Comme $[K' : K] = 2$, P est de degré 1 ou 2. Si $\deg P = 1$ alors x est séparable ; supposons que $\deg P = 2$. Si P possède une racine multiple (dans $\overline{K}$) alors comme $\deg P = 2$ on a $P = (X + a)^2$ pour un $a \in \overline{K}$. On a donc $P = X^2 + 2aX + a^2$; ainsi, $2a \in K$ et comme la caractéristique de K est différente de 2 on a $a \in K$. Ainsi, P n'est pas irréductible sur K ce qui est absurde ; P ne possède donc pas de racine multiple donc x est séparable. Finalement, K'/K est séparable. □

Si $F|k$ est régulier, alors $F|k$ est rationnel ssi [$g(F) = 0$ et il existe un diviseur de $F|k$ de degré 1] ([11, proposition 1.6.3]). En particulier, si k est fini ou algébriquement clos, la condition du diviseur est automatiquement réalisée ([11, remarque 1.6.4]). Ainsi, si l'on veut sortir du cadre du corps des fractions rationnelles, on doit considérer les corps de fonctions de genre au moins 1.

3.1 Ellipticité

3.1.1 Définitions

Définition 3.3. On dit que $F|k$ est *elliptique* si :
- $F|k$ est régulier ;
- $g(F) = 1$;
- il existe un diviseur de $F|k$ de degré 1.

Théorème 3.4. *$F|k$ est elliptique si et seulement si la condition suivante est réalisée :*

$$\exists x, y \in F, \exists f \in k[x] \text{ de degré 3 sans facteur carré}, F = k(x)[y] \text{ avec } y^2 = f(x).$$

Démonstration. [11, proposition 6.1.2.(a)] pour la condition nécessaire et [11, proposition 6.1.3.(a).(1)] pour la condition suffisante. □

Remarque. Si $F|k$ est elliptique, alors avec l'élément x du théorème on a automatiquement le fait que $F/k(x)$ est monogène. On suppose par la suite que lorsque l'on fixe un élément transcendant d'un corps de fonctions elliptique, c'est un élément x comme dans le théorème.

Définition 3.5. Une *courbe elliptique E sur k*, notée E/k, est un sous-ensemble de $\mathbb{P}^2(\overline{k})$ du type suivant :

$$\{(x : y : 1) \in \mathbb{P}^2(\overline{k}) : y^2 = f(x)\} \cup \{(0 : 1 : 0)\}$$

où f est un polynôme à coefficients dans k de degré 3 et sans facteur carré ; on dit que $y^2 = f(x)$ est l'*équation* de E/k. Le *corps de fonctions* de E/k est défini par $k(E) := k(X)[Y]/\langle Y^2 - f(X)\rangle$.

Remarque. Le corps de fonctions d'une courbe elliptique est un corps de fonctions algébrique en une variable elliptique.

3.1.2 Loi de groupe

Soit $F|k$ un corps de fonctions elliptique ; on fixe une place P_0 de degré 1 (c'est possible par [11, proposition 6.1.6.(a)]). On va énoncer un théorème fondamental.

Théorème 3.6. *On a une bijection :*

$$\{P \in \mathbb{P}_F : \deg P = 1\} \simeq \mathrm{Cl}^0(F)$$

et l'application $P \mapsto [P - P_0]$ réalise cette bijection.

Démonstration. [11, proposition 6.1.6 (b)]. □

Corollaire 3.7. *L'ensemble $\{P \in \mathbb{P}_F : \deg P = 1\}$ peut être muni d'une loi de groupe abélien d'élément neutre P_0.*

Démonstration. En notant Φ la bijection du théorème, la loi de groupe est simplement donnée par un transport de structure : $P \oplus Q := \Phi^{-1}(\Phi(P) + \Phi(Q))$. □

Soit E/k une courbe elliptique. On peut associer à chaque point de E l'*anneau des fonctions régulières en P* ([10, proposition II.1.1]) ; on obtient ainsi toutes les places de $\overline{k}(E)$ ([6, théorème 7.5.2]). Par la propriété 2.11 et par le corollaire ci-dessus, on dispose d'une loi sur les places de $\overline{k}(E)$: elle se transmet donc naturellement sur les points de E. De plus, $E(k)$ est stable pour cette loi ([6, théorème 7.9.8]) ; on a en fait $E(k) \simeq \mathrm{Cl}^0(k(E))$. Une illustration de la loi de groupe est donnée dans l'annexe A.

3.1.3 Forme de Legendre

Soit E/k une courbe elliptique ; par définition, E/k a pour équation $y^2 = f(x)$ où $f \in k[x]$ est un polynôme de degré 3 sans facteur carré. La forme de Legendre de E/k est une équation $y^2 = g(x)$ où g a une forme « simple » et où la courbe elliptique associée à cette équation est « équivalente » à la courbe elliptique E/k.

Définition 3.8. On dit que deux courbes elliptiques sur k sont *isomorphes* si leur corps de fonctions sont k-isomorphes en tant que k-algèbres.

Proposition 3.9. *Soit E/k une courbe elliptique, d'équation $y^2 = f(x)$. Il existe une courbe elliptique E'/k' d'équation $y^2 = x(x-1)(x-\lambda)$ où :*
- *k' est un corps de décomposition de f ;*
- *$\lambda \in k' \setminus \{0, 1\}$;*

telle que E/k' et E'/k' soient isomorphes.

Démonstration. On peut écrire $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ dans un corps de décomposition k' de f. Étant donné que f est de degré 3, on a $[k' : k] \leqslant 3! = 6$. De plus, f est sans facteur carré donc α, β et γ sont deux à deux distincts. On considère alors l'application de $\mathbb{P}^1(k')$ dans lui-même définie par $\phi(x) := (x-\alpha)/(\beta-\alpha)$. L'application envoie bien sûr α sur 0, β sur 1 et l'infini sur l'infini [7] ; on pose $\lambda := \phi(\gamma)$. La courbe elliptique d'équation $y^2 = x'(x'-1)(x'-\lambda)$ est alors isomorphe à E/k'. □

Remarque. Le λ n'est pas unique ; on voit en effet qu'il dépend de l'ordre que l'on a choisi pour les racines de f. Cependant, on obtient facilement que les seules autres valeurs de λ possibles sont dans $\{\frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}$.

7. On note $\phi =: [\alpha, \beta, \infty, \cdot]$: c'est ce qui s'appelle le *birapport*.

3.2 Hyperellipticité

Définition 3.10. On dit que $F|k$ est *hyperelliptique* si :
- $F|k$ est régulier ;
- $g(F) \geqslant 2$;
- il existe $x \in F$ tel que $[F : k(x)] = 2$.

Théorème 3.11. *$F|k$ est hyperelliptique si et seulement si la condition suivante est réalisée :*

$$\exists x, y \in F, \exists f \in k[x] \text{ de degré} \geqslant 5 \text{ sans facteur carré}, F = k(x)[y] \text{ avec } y^2 = f(x).$$

Démonstration. [11, proposition 6.2.3]. □

Remarque. Plus précisément, si un tel polynôme f est de degré m alors le genre de $F|k$ est $\lfloor (m-1)/2 \rfloor$. En outre, on a automatiquement le fait que $F/k(x)$ est monogène. On suppose par la suite que lorsque l'on fixe un élément transcendant d'un corps de fonction hyperelliptique, c'est un élément x comme dans le théorème.

Définition 3.12. Une *courbe hyperelliptique E sur k*, notée E/k, est un sous-ensemble de $\mathbb{P}^2(\overline{k})$ du type suivant :

$$\{(x : y : 1) \in \mathbb{P}^2(\overline{k}) : y^2 = f(x)\} \cup \{(0 : 1 : 0)\}$$

où f est un polynôme à coefficients dans k de degré au moins 5 et sans facteur carré. Le *corps de fonctions* de E/k est défini par $k(E) := k(X)[Y]/\langle Y^2 - f(X)\rangle$.

Remarque. Le corps de fonctions d'une courbe hyperelliptique est un corps de fonctions algébrique en une variable hyperelliptique.

4 La méthode du calcul d'index

4.1 Quelques théorèmes

Ce procédé de calcul de logarithme discret est la base des résultats suivants, dûs à C. Diem. Tous proviennent de [3], sauf le théorème 4.2 qui est issu de [2].

Théorème 4.1. *Soient $g \geqslant 2$ un entier fixé et q une puissance d'un nombre premier. Alors si $H/\mathbb{F}_q$ est une courbe hyperelliptique de genre g, on peut résoudre le problème du logarithme discret dans* $\mathrm{Cl}^0(\mathbb{F}_q(H))$ *en un temps* $\widetilde{\mathcal{O}}(q^{2-\frac{2}{g}})$.

Remarque. On a vu dans la section 2.1.5 que les méthodes de la section 1 nécessitent un temps de calcul en $\widetilde{\mathcal{O}}(q^{\frac{g}{2}})$. La complexité donnée dans le théorème est donc bien meilleure dès que $g \geqslant 3$.

Remarque. Ce résultat s'étend en fait aux corps de fonctions.

Théorème 4.2. *Soient $g \geqslant 3$ un entier fixé et q une puissance d'un nombre premier. Alors si $F|\mathbb{F}_q$ est un corps de fonctions* non *hyperelliptique de genre g, on peut résoudre le problème du logarithme discret dans* $\mathrm{Cl}^0(F|\mathbb{F}_q)$ *« presque toujours » en* $\widetilde{\mathcal{O}}(q^{2-\frac{2}{g-1}})$.

Remarque. Voir [2] pour le « presque toujours » ; en particulier, on peut résoudre le problème du logarithme discret dans le groupe des classes de diviseurs de degré 0 d'un corps de fonctions non hyperelliptique de genre 3 en un temps $\widetilde{\mathcal{O}}(q)$, contre $\widetilde{\mathcal{O}}(q^{\frac{3}{2}})$ pour les algorithmes génériques de la section 1.

Théorème 4.3. *Soient $n \geqslant 2$ un entier fixé et q une puissance d'un nombre premier. Alors si $E/\mathbb{F}_{q^n}$ est une courbe elliptique, on peut résoudre le problème du logarithme discret dans $E(\mathbb{F}_{q^n})$ en un temps* $\widetilde{\mathcal{O}}(q^{2-\frac{2}{n}})$.

Remarque. C'est beaucoup mieux que les méthodes de la section 1 dès que $n \geqslant 3$ car elles nécessitent un temps de calcul en $\widetilde{\mathcal{O}}(q^{\frac{n}{2}})$!

Théorème 4.4. *Il existe une suite de corps finis $(k_n)_n$ strictement croissante (en cardinalité) telle que si E/k_n est une courbe elliptique, on peut résoudre le problème du logarithme discret dans $E(k_n)$ en un temps* $\exp(\mathcal{O}(\log(\#k_n)^{\frac{2}{3}}))$.

Remarque. La complexité est cette fois sous-exponentielle en $\log(\#k_n)$. Remarquons que c'est un résultat d'existence, et qu'il ne concerne donc pas tous les corps finis.

4.2 Description

On va illustrer la méthode de calcul d'index pour une courbe elliptique sur un corps k algébriquement clos. Soit E/k une courbe elliptique d'élément neutre O et soient A et B dans E. On a vu que si C est un point de E on peut lui associer une place de $k(E)$, que l'on renote C ; on peut finalement considérer sa classe $[C-O]$ dans $\mathrm{Cl}^0(k(E))$ (le « $-$ » étant bien sûr dans $\mathrm{Div}(k(E))$).

On considère alors la liste $\mathcal{F} := [[A-O],[B-O]]$; $\mathcal{F}$ va devenir ce que l'on appelle une *base de facteurs*.

On procède de la façon suivante.

1. On choisit deux droites f et g, qui vont couper E en 3 points distincts (si ce n'est pas le cas on change f ou g).
2. On note P_i les points d'intersection de f avec E et Q_i ceux de g. On a alors $\mathrm{div}(\frac{f}{g}) = \sum P_i - \sum Q_j$ donc en passant au quotient on obtient $\sum[P_i-O] - \sum[Q_j-O] = 0$; on appelle cela une *relation* entre les points P_i et Q_i (à noter que nos deux premières relations sont $[A-O]=[A-O]$ et $[B-O]=[B-O]$).
3. On ajoute ensuite les éléments $[P_i-O],[Q_i-O]$ à la fin de $\mathcal{F}$ s'ils n'y sont pas déjà présents.
4. On recommence la première étape jusqu'à ce que $\mathcal{F}$ soit « assez grande » (cf. étape suivante).
5. On considère l'égalité matricielle $M\mathcal{F} = ([A-O],[B-O],0,\ldots,0)^T$ où l'on voit $\mathcal{F}$ comme un vecteur colonne et où M est la matrice des relations que l'on a trouvées. Bien entendu, M est une matrice creuse : il y a au plus six coefficients par ligne qui sont non nuls (et qui valent de surcroît ± 1) ! On trouve alors un vecteur (à coefficients dans $\mathbb{Z}$) dans le noyau à gauche de M.
6. Ce vecteur dans le noyau va directement nous donner une relation $a[A-O]+b[B-O]=0$. Si a est inversible dans k, alors $-\frac{b}{a}$ est un logarithme discret de A en base B ; sinon, on recommence avec un autre vecteur du noyau ou avec une autre base de facteurs (on rajoute des points à $\mathcal{F}$ ou bien on recommence tout) [8].

Pour finir, on voit que si l'on sait résoudre le problème du logarithme discret dans $\mathrm{Cl}^0(k(E))$ alors on sait le résoudre dans E ; c'est pour cela que l'on s'intéresse au problème du logarithme discret dans ces groupes de classes.

5 L'attaque GHS

Tout qui va suivre est détaillé et démontré dans [4]. De plus, dans toute la suite et jusqu'à la fin de cet exposé, q désigne une puissance d'un nombre premier impair.

8. Cela peut paraître un peu bancal, mais l'on peut prouver que si les éléments de la base de facteurs sont choisis de façon aléatoire cela va fonctionner.

5.1 Idée

On part d'une courbe (hyper)elliptique $H/\mathbb{F}_{q^n}$: on désire transférer le problème du logarithme discret dans $\mathrm{Cl}^0(\mathbb{F}_{q^n}(H))$ vers le même problème mais dans $\mathrm{Cl}^0(F)$ où $F|\mathbb{F}_q$ est un corps de fonctions bien choisi. On s'attend à ce que $F|\mathbb{F}_q$ soit d'un genre plus élevé que $\mathbb{F}_{q^n}(H)$, mais on espère qu'il ne soit quand même pas trop élevé (on rappelle que $\#\mathrm{Cl}^0(F|\mathbb{F}_q) \simeq q^{g(F)}$). En fait, on aura la borne $g(F) \leqslant 2^{n-1}([g(\mathbb{F}_{q^n}(H)) + 1]n - 2) + 1$ (cf. [4, théorème 1]). Si $F|\mathbb{F}_q$ n'est pas hyperelliptique et que son genre est assez élevé, on pourra tirer profit du théorème 4.2.

5.2 Le morphisme de conorme–norme

Soit $H/\mathbb{F}_{q^n}$ une courbe (hyper)elliptique. Pour réaliser l'opération précédente, on va utiliser les morphismes de norme et de conorme dont on a parlé précédemment. Tout d'abord, on doit bien sûr construire le corps de fonctions $F|\mathbb{F}_q$ en question. En réalité, F est défini comme sous-corps de F' comme étant le corps fixe d'un certain automorphisme (cf. [4, avant la proposition 3]), où F' est lui-même défini comme étant la clôture galoisienne de $\mathbb{F}_{q^n}(H)/\mathbb{F}_{q^n}(x)$ où x est un élément transcendant de $\mathbb{F}_{q^n}(H)|\mathbb{F}_{q^n}$ que l'on fixe jusqu'à la fin de cet exposé. (On rappelle que la clôture galoisienne d'une extension finie séparable de corps L/K est une plus petite extension L'/K galoisienne[9] avec $L' \supseteq L$; voir aussi [11, A.11].) Remarquons que $\mathbb{F}_{q^n}(H)/\mathbb{F}_{q^n}(x)$ est finie (par définition d'un corps de fonctions (hyper)elliptique) et comme q est impair elle est aussi séparable par le lemme 3.2 donc on peut considérer sa clôture galoisienne.

On envoie $\mathrm{Cl}^0(\mathbb{F}_{q^n}(H))$ sur $\mathrm{Cl}^0(F)$ de la façon suivante :

$$\mathrm{Cl}^0(\mathbb{F}_{q^n}(H)|\mathbb{F}_{q^n}) \xrightarrow{\mathrm{Con}_{F'/\mathbb{F}_{q^n}(H)}} \mathrm{Cl}^0(F'|\mathbb{F}_{q^n}) \xrightarrow{\mathrm{N}_{F'/F}} \mathrm{Cl}^0(F|\mathbb{F}_q).$$

Remarque. Il est montré dans [4] que le problème du logarithme discret pour deux éléments dans le groupe de départ et pour l'image de ces deux éléments dans le groupe d'arrivée sont équivalents.

On ne va pas en fait programmer directement avec des diviseurs ; on va utiliser une représentation par idéaux des diviseurs, que l'on va présenter dans les deux prochaines sections.

6 Idéaux

On désire associer à chaque diviseur un unique couple d'idéaux. Ainsi, dans la représentation par idéaux que l'on va présenter dans la prochaine section, F. Heß a développé un algorithme efficace pour générer une base de l'espace de Riemann-Roch associé à un diviseur ; dans le cas qui nous intéresse, les calculs de conorme et de norme se voient facilités.

Soit $F|k$ un corps de fonctions algébrique en une variable ; l'idée de la représentation par idéaux est la suivante. Soit $D := \sum n_P P$ un diviseur positif ; chaque P étant un idéal de $\mathcal{O}_P$, on peut penser qu'il est possible d'associer au diviseur D un idéal d'un certain anneau $\mathcal{O}$.

- On peut considérer $\mathcal{O}$ comme un anneau contenant une réunion de $\mathcal{O}_P$; on aura un problème car les $\mathcal{O}_P$ sont sous-anneaux maximaux de F ([11, théorème 1.1.13.(d)]).
- On peut considérer $\mathcal{O}$ comme une intersection de $\mathcal{O}_P$; on va voir que c'est cette idée qui va fonctionner.

Bien entendu, l'anneau $\mathcal{O}$ que l'on choisit doit être indépendant du support du diviseur D. Une fois que l'on a notre application Φ qui transforme les places en des idéaux (premiers) de $\mathcal{O}$, l'idée est de considérer l'idéal $\prod \Phi(P)^{n_P} \subseteq \mathcal{O}$. Il y a encore un problème : on ne sait pas faire quand D n'est pas positif, *i.e.* quand il existe des $n_P < 0$. On va résoudre cela en définissant un nouveau type d'idéal

9. On ne considère ici que des extensions galoisiennes finies.

où chaque idéal de ce type aura un inverse qui sera encore un idéal ; c'est ce à quoi cette section est consacrée.

Dans toute la suite de cette section, F désigne un corps quelconque.

6.1 Idéaux fractionnaires

Définition 6.1. Soient $A \subseteq B$ deux anneaux commutatifs unitaires intègres. La *fermeture intégrale* de A dans B est l'ensemble des éléments de B qui sont entiers sur A. Si A est égal à sa propre clôture intégrale dans B, on dit que A est *intégralement clos dans* B. En particulier, si $B = \mathrm{Frac}(A)$ on dit que A est *intégralement clos*.

Définition 6.2. On dit qu'un sous-anneau de F est un *anneau de Dedekind* s'il est noethérien, intégralement clos et si tout idéal premier non nul est maximal.

Exemple. Un sous-anneau principal est un anneau de Dedekind (il est intégralement clos car factoriel).

Soit $\mathcal{O} \subseteq F$ un anneau de Dedekind.

Théorème 6.3. *Tout idéal propre non nul de $\mathcal{O}$ se décompose de façon unique en un produit fini d'idéaux premiers (non nuls), à l'ordre des facteurs près.*

Démonstration. [9, théorème I.3.3]. □

Corollaire 6.4. *Tout idéal propre non nul de $\mathcal{O}$ s'écrit de façon unique $\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$ où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers non nuls de $\mathcal{O}$ et où les $\nu_\mathfrak{p} \in \mathbb{N}$ sont presque tous nuls.*

Définition 6.5. Soit I un idéal propre non nul de $\mathcal{O}$ et soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$. On dit que $\mathfrak{p}$ *divise* I et on écrit $\mathfrak{p}|I$ si $\mathfrak{p}$ intervient dans la décomposition de I en un produit fini d'idéaux premiers du théorème précédent.

Remarque. Avec les notations du corollaire, $\mathfrak{p}|I \iff \nu_\mathfrak{p} > 0$.

En voyant la décomposition du corollaire sous forme additive, on voit que l'on obtient l'analogue de diviseurs positifs. Pour retrouver le groupe des diviseurs, on a besoin d'introduire de « nouveaux » idéaux : les idéaux *fractionnaires*.

On suppose maintenant que $\mathcal{O}$ a pour corps des fractions F.

Définition 6.6. Un *idéal fractionnaire* de $\mathcal{O}$ est un sous-$\mathcal{O}$-module de type fini non nul de F.

Remarque. $\mathcal{O}$ étant noethérien, ses idéaux sont les sous-$\mathcal{O}$-modules de type fini de $\mathcal{O}$; ainsi, les idéaux non nuls de $\mathcal{O}$ sont des idéaux fractionnaires de $\mathcal{O}$.

Définition 6.7. Des *générateurs* d'un idéal fractionnaire de $\mathcal{O}$ sont des générateurs en tant que $\mathcal{O}$-module.

Propriété 6.8. *Un sous-$\mathcal{O}$-module non nul I de F est un idéal fractionnaire de $\mathcal{O}$ si et seulement si $\exists d \in \mathcal{O} \setminus \{0\}, dI \subseteq \mathcal{O}$. De plus, dans ce cas dI est un idéal de $\mathcal{O}$.*

Démonstration. Le sens direct résulte du fait que $F = \mathrm{Frac}(\mathcal{O})$, l'autre du fait que $\mathcal{O}$ est noethérien. La fin est triviale. □

Définition 6.9. Un élément d de la propriété précédente est appelé un *dénominateur* de I.

Théorème 6.10. *Les idéaux fractionnaires de $\mathcal{O}$ forment un groupe abélien, que l'on note $\mathfrak{J}_\mathcal{O}$. L'élément neutre est $\mathcal{O}$ et l'inverse d'un élément I est $I^{-1} := \{z \in F : zI \subseteq \mathcal{O}\}$.*

Démonstration. [9, proposition I.3.8]. □

Voilà alors ce que l'on attendait.

Corollaire 6.11. *Tout idéal fractionnaire propre de $\mathcal{O}$ s'écrit de façon unique $\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$ où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers non nuls de $\mathcal{O}$ et où les $\nu_\mathfrak{p} \in \mathbb{Z}$ sont presque tous nuls.*

Démonstration. Par abus de langage, on appellera encore cela une décomposition en produit d'idéaux premiers. □

Démonstration. Soit I un idéal fractionnaire propre et soit d un dénominateur ; montrons que $I = (d\mathcal{O})^{-1}(dI)$.

- Si $a \in I$, alors $a = \frac{1}{d}(da) \in (d\mathcal{O})^{-1}(dI)$.
- Si $a \in (d\mathcal{O})^{-1}(dI)$ alors on peut écrire a comme une somme finie $\sum b_i c_i$ avec $b_i \in (d\mathcal{O})^{-1}$ et $c_i \in dI$; on écrit $c_i := dc_i'$ avec $c_i' \in I$. Comme $b_i \in (d\mathcal{O})^{-1}$ on a $b_i(d\mathcal{O}) \subseteq \mathcal{O}$ donc $b_i d \in \mathcal{O}$. Ainsi, $b_i c_i = (b_i d)c_i' \in I$ car I est un $\mathcal{O}$-module ; cette même propriété de module permet de conclure que $a \in I$.

Finalement, on conclut avec le fait que $d\mathcal{O}$ et dI sont des idéaux propres non nuls de $\mathcal{O}$ donc on sait déjà les décomposer de la sorte par le corollaire 6.4. □

6.2 Conorme, norme (II)

Soit F'/F une extension finie et soit $\mathcal{O}$ un anneau de Dedekind de corps de fractions F.

Proposition 6.12. *La fermeture intégrale $\mathcal{O}'$ de $\mathcal{O}$ dans F' est un anneau de Dedekind de corps de fractions F'.*

Démonstration. [9, proposition I.12.8] montre que $\mathcal{O}'$ est un anneau de Dedekind ; montrons que $\mathrm{Frac}(\mathcal{O}') = F'$. Soit $z \in F'$; comme F'/F est finie, z est algébrique sur F donc il existe $n \in \mathbb{N}^*$ et $a_0, \dots, a_{n-1} \in F$ tels que $z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0$. Considérons les a_i comme des éléments de $\mathrm{Frac}(\mathcal{O})$ (on a le droit car cet ensemble est précisément F tout entier) ; soit $a \in \mathcal{O}\backslash\{0\}$ un dénominateur commun. En multipliant l'égalité précédente par a^n il vient $(az)^n + a_{n-1}a(az)^{n-1} + \cdots + a_0 a^n = 0$. Par définition de a on a $a_i a \in \mathcal{O}$ donc $a_i a^{n-i} \in \mathcal{O}$ $\forall i \in \{0, \dots, n-1\}$ car $a \in \mathcal{O}$. Ainsi, $az \in F'$ est entier sur $\mathcal{O}$ donc $az \in \mathcal{O}'$ par définition de $\mathcal{O}'$. Comme $a \neq 0$ et que $\mathcal{O} \subseteq \mathcal{O}'$ on en déduit que $z \in \mathrm{Frac}(\mathcal{O}')$. Ainsi on a $F' \subseteq \mathrm{Frac}(\mathcal{O}')$ et l'autre inclusion étant triviale on a bien l'égalité. □

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$; étant donné que $\mathcal{O}'$ est un anneau de Dedekind, l'idéal de $\mathcal{O}'$ engendré par les éléments de $\mathfrak{p}$ (que l'on note $\langle\mathfrak{p}\rangle_{\mathcal{O}'}$ ou encore $\langle\mathfrak{p}\rangle$ quand il n'y a pas de confusion possible) se décompose en un produit d'idéaux premiers non nuls. On a toutefois besoin du lemme suivant.

Lemme 6.13. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$. Alors $\langle\mathfrak{p}\rangle_{\mathcal{O}'}$ est un idéal propre de $\mathcal{O}'$.*

Démonstration. [9, juste après la preuve de la proposition I.8.1]. □

Remarque. Si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}$, alors $\mathfrak{p} = \sum_{i=1}^n a_i\mathcal{O}$ avec $a_i \in \mathcal{O}$ (déjà vu) ; on a $\langle\mathfrak{p}\rangle_{\mathcal{O}'} = \sum_{i=1}^n a_i\mathcal{O}'$. Ainsi, si $I := \sum_{i=1}^n a_i\mathcal{O}$ avec $a_i \in F$ est un idéal fractionnaire de $\mathcal{O}$ on pose $\langle I\rangle_{\mathcal{O}'} := \sum_{i=1}^n a_i\mathcal{O}'$.

Définition 6.14. On définit la *conorme* d'un idéal premier non nul $\mathfrak{p}$ de $\mathcal{O}$ par $\mathrm{Con}_{F'/F}(\mathfrak{p}) := \langle\mathfrak{p}\rangle_{\mathcal{O}'}$.

On remarque que contrairement au cas des places, c'est une définition intuitive.

Proposition 6.15. *L'application $\mathrm{Con}_{F'/F}$ se prolonge en un morphisme $\mathfrak{J}_\mathcal{O} \to \mathfrak{J}_{\mathcal{O}'}$.*

Démonstration. On prolonge simplement par multiplicativité en utilisant la décomposition en produits d'idéaux premiers (corollaire 6.11). C'est bien le bon ensemble d'arrivée d'après le lemme 6.13. □

Proposition 6.16. *Si $I \in \mathfrak{J}_{\mathcal{O}}$ alors* $\mathrm{Con}_{F'/F}(I) = \langle I \rangle_{\mathcal{O}'}$.

Démonstration. Il suffit de démontrer le fait suivant : si I et J sont deux idéaux fractionnaires de $\mathcal{O}$ alors $\langle IJ \rangle_{\mathcal{O}'} = \langle I \rangle_{\mathcal{O}'} \langle J \rangle_{\mathcal{O}'}$. Cela découle directement du fait que $I = \sum_{i=1}^{n} a_i \mathcal{O}$ et $\langle I \rangle_{\mathcal{O}'} = \sum a_i \mathcal{O}'$ avec $a_i \in F$ pour un idéal fractionnaire I de $\mathcal{O}$ quelconque. □

Si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}$, écrivons la décomposition de sa conorme en produits d'idéaux premiers de $\mathcal{O}'$ (corollaire 6.4) de la façon suivante : $\mathrm{Con}_{F'/F}(\mathfrak{p}) = \prod \mathfrak{p}'^{\nu_{\mathfrak{p}'}}$.

Définition 6.17. Soit $\mathfrak{p}'$ un idéal premier non nul de $\mathcal{O}'$; on dit que $\mathfrak{p}'$ *divise* $\mathfrak{p}$ et on écrit $\mathfrak{p}' | \mathfrak{p}$ si $\mathfrak{p}'$ divise $\mathrm{Con}_{F'/F}(\mathfrak{p}) = \langle \mathfrak{p} \rangle_{\mathcal{O}'}$. Si $\mathfrak{p}' | \mathfrak{p}$, l'entier $\nu_{\mathfrak{p}'}$ défini comme précédemment s'appelle l'*indice de ramification* de $\mathfrak{p}'$ sur $\mathfrak{p}$ et on le note $e_{\mathfrak{p}'|\mathfrak{p}}$. De plus, le *degré relatif* (ou *degré d'inertie*) de $\mathfrak{p}'$ par rapport à $\mathfrak{p}$ est défini par $f_{\mathfrak{p}'|\mathfrak{p}} := [\mathcal{O}'/\mathfrak{p}' : \mathcal{O}/\mathfrak{p}]$.

Remarque. Les quotients $\mathcal{O}'/\mathfrak{p}'$ et $\mathcal{O}/\mathfrak{p}$ sont bien des corps puisque dans un anneau de Dedekind les idéaux premiers non nuls sont maximaux. De plus, le noyau de l'application $\mathcal{O} \to \mathcal{O}'/\mathfrak{p}'$ est $\mathcal{O} \cap \mathfrak{p}' = \mathfrak{p}$ (cf. propriété 6.20) donc on a bien l'injection canonique $\mathcal{O}/\mathfrak{p} \hookrightarrow \mathcal{O}'/\mathfrak{p}'$.

Au delà du vocabulaire dans l'analogie avec les places, on retrouve encore le théorème suivant.

Théorème 6.18 (Égalité fondamentale)**.** *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$. Si F'/F est séparable, on a l'égalité suivante :*

$$\sum_{\mathfrak{p}'|\mathfrak{p}} e_{\mathfrak{p}'|\mathfrak{p}} f_{\mathfrak{p}'|\mathfrak{p}} = [F' : F]$$

où $\mathfrak{p}'$ parcourt les idéaux premiers non nuls de $\mathcal{O}'$.

Démonstration. [9, théorème I.8.2]. □

Remarque. Ainsi les degrés relatifs sont finis.

Notre but est maintenant de définir le morphisme de norme.

Proposition 6.19. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$ et soit $\mathfrak{p}'$ un idéal premier non nul de $\mathcal{O}'$. Alors $\mathfrak{p}' | \mathfrak{p}$ ssi $\mathfrak{p} \subseteq \mathfrak{p}'$.*

Démonstration. Tout d'abord, il est clair que si $\mathfrak{p}' | \mathfrak{p}$ alors $\mathfrak{p} \subseteq \mathfrak{p}'$ car $\mathfrak{p} \subseteq \mathrm{Con}_{F'/F}(\mathfrak{p})$ (rappelons que si I, J sont deux idéaux alors $I \cdot J \subseteq I$).

Pour démontrer l'autre implication, on va raisonner de manière générale. Soit $\Sigma := \{I$ idéal non nul de $\mathcal{O}' : \exists \mathfrak{q}$ idéal premier de $\mathcal{O}', \mathfrak{q} \supseteq I$ et $\mathfrak{q}$ ne divise pas $I\}$ et supposons que $\Sigma \neq \emptyset$. Comme $\mathcal{O}'$ est noethérien, Σ possède un élément maximal, que l'on note I. Étant donné que $I \in \Sigma, \exists \mathfrak{q}$ idéal premier de $\mathcal{O}'$ tel que $I \subseteq \mathfrak{q}$ et $\mathfrak{q}$ ne divise pas I. D'après le théorème 6.3, comme I est propre (car $I \subseteq \mathfrak{q} \subsetneq \mathcal{O}'$) et non nul (par construction de Σ) on peut décomposer I en un produit fini d'idéaux premiers non nuls de $\mathcal{O}'$; on obtient alors $I = \prod_{i=1}^{n} \mathfrak{p}_i \subseteq \mathfrak{q}$. En utilisant un théorème classique d'algèbre commutative, on en déduit que $\exists i, \mathfrak{p}_i \subseteq \mathfrak{q}$. Comme $\mathfrak{p}_i$ est un idéal premier non nul de $\mathcal{O}'$ qui est un anneau de Dedekind, $\mathfrak{p}_i$ est un idéal maximal donc $\mathfrak{p}_i = \mathfrak{q}$. Cela contredit le fait que $\mathfrak{q}$ ne divise pas I ; on a donc $\Sigma = \emptyset$.

Ainsi, reprenons notre idéal $\mathfrak{p}$ de l'énoncé et supposons que $\mathfrak{p} \subseteq \mathfrak{p}'$; par définition de la conorme on a $\langle 0 \rangle \subsetneq \mathrm{Con}_{F'/F}(\mathfrak{p}) \subseteq \mathfrak{p}'$. Si $\mathfrak{p}'$ ne divise pas $\mathfrak{p}$, alors comme $\mathfrak{p}'$ est premier on a $\mathrm{Con}_{F'/F}(\mathfrak{p}) \in \Sigma$ ce qui est absurde puisque $\Sigma = \emptyset$; on en déduit que $\mathfrak{p}'$ divise $\mathfrak{p}$. □

Propriété 6.20. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$ et soit $\mathfrak{p}'$ un idéal premier non nul de $\mathcal{O}'$ qui divise $\mathfrak{p}$. Pour $1 \leqslant e \leqslant e_{\mathfrak{p}'|\mathfrak{p}}$ on a $\mathfrak{p} = \mathfrak{p}'^{e} \cap \mathcal{O}$.*

Démonstration. On a $\mathfrak{p} \subseteq \mathrm{Con}_{F'/F}(\mathfrak{p}) \subseteq \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}} \subseteq \mathfrak{p}'^{e}$ donc $\mathfrak{p} \subseteq \mathfrak{p}'^{e} \cap \mathcal{O}$. Étant donné que $\mathcal{O}$ est un anneau de Dedekind, $\mathfrak{p}$ est un idéal maximal donc pour conclure que l'inclusion précédente est une égalité il suffit de montrer que $\mathfrak{p}'^{e} \cap \mathcal{O}$ est un idéal propre de $\mathcal{O}$; c'est trivialement un idéal de $\mathcal{O}$ et c'est un idéal propre car il ne contient par 1. □

Proposition 6.21. *Soit $\mathfrak{p}'$ un idéal premier non nul de $\mathcal{O}'$. Alors $\mathfrak{p} := \mathfrak{p}' \cap \mathcal{O}$ est un idéal premier non nul de $\mathcal{O}$, et c'est l'unique idéal premier non nul de $\mathcal{O}$ que divise $\mathfrak{p}'$.*

Démonstration. (On s'inspire de [11, proposition 3.1.7.(a)].) On vérifie trivialement que $\mathfrak{p}$ est un idéal premier de $\mathcal{O}$. Pour montrer que $\mathfrak{p}$ est un idéal non nul, considérons un élément $z \in \mathfrak{p}' \setminus \{0\}$. On a $\mathfrak{p}' \subseteq \mathcal{O}'$ donc par construction de $\mathcal{O}'$, z est entier sur $\mathcal{O}$: il existe $n \in \mathbb{N}^*, a_0, \dots a_{n-1} \in \mathcal{O}$ tels que

$$z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0.$$

Quitte à diviser plusieurs fois par z, on peut supposer $a_0 \neq 0$. Comme $a_i \in \mathcal{O} \subseteq \mathcal{O}'$ et que $z \in \mathfrak{p}'$, on obtient $a_0 \in \mathfrak{p}'$. Ainsi, a_0 est un élément non nul de $\mathcal{O}$ qui est dans $\mathfrak{p}'$ donc $\mathfrak{p} \neq \langle 0 \rangle$.

Finalement, par la proposition 6.19, on a $\mathfrak{p}'|\mathfrak{p}$; l'unicité est garantie par la propriété 6.20. □

On est maintenant prêt pour donner la définition de la norme d'un idéal fractionnaire.

Définition 6.22. On définit la *norme* d'un idéal premier non nul $\mathfrak{p}'$ de $\mathcal{O}'$ par :

$$\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}}$$

où $\mathfrak{p} := \mathfrak{p}' \cap \mathcal{O}$ est l'unique idéal premier non nul de $\mathcal{O}$ que divise $\mathfrak{p}'$. On prolonge l'application en un morphisme $\mathfrak{J}_{\mathcal{O}} \to \mathfrak{J}_{\mathcal{O}'}$.

Pour sentir d'où vient le degré relatif dans la définition, on peut soit faire une analogie avec ce que l'on a fait pour les places des corps de fonctions, soit on peut aller faire un tour du côté des corps de nombres. Soit $F := \mathbb{Q}$ et F'/F une extension finie de corps. Soit $\mathcal{O} := \mathbb{Z}$ et soit $\mathcal{O}'$ la fermeture intégrale de $\mathcal{O}$ dans F'. Si $\mathfrak{p}'$ est un idéal premier non nul de $\mathcal{O}'$, alors $\mathcal{O}'/\mathfrak{p}'$ est *fini* (voir [9, proposition I.2.12]) ; on peut définir la *norme* de $\mathfrak{p}'$ par $\mathrm{N}_{F'/F}(\mathfrak{p}') := \#(\mathcal{O}'/\mathfrak{p}')$. L'anneau $\mathcal{O}'/\mathfrak{p}'$ étant intègre et fini, c'est un corps (fini) de caractéristique $p > 0$, où l'entier p vérifie (par définition de la caractéristique) $\mathfrak{p}' \cap \mathcal{O} = \mathfrak{p}$ avec $\mathfrak{p} := p\mathcal{O}$. En posant $f_{\mathfrak{p}'|\mathfrak{p}} := [\mathcal{O}'/\mathfrak{p}' : \mathcal{O}/\mathfrak{p}]$ $(= \dim_{\mathbb{F}_p}(\mathcal{O}'/\mathfrak{p}'))$ on obtient donc $\mathrm{N}_{F'/F}(\mathfrak{p}') = p^{f_{\mathfrak{p}'|\mathfrak{p}}}$.

Dans le cas qui nous intéresse, on a juste à remplacer F par un corps quelconque et $\mathcal{O}$ par un anneau de Dedekind de corps de fractions F ; on veut obtenir un idéal donc on pose cette fois $\mathrm{N}_{F'/F}(\mathfrak{p}') := \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}}$.

Remarque. Contrairement à la conorme, la définition de la norme ne permet par d'avoir d'expression de la norme d'un idéal fractionnaire sans passer par sa décomposition en produits d'idéaux premiers.

7 Représentation par idéaux des diviseurs

Dans toute cette section, $F|k$ désigne un corps de fonctions.

7.1 Ordres maximaux

Définition 7.1. Soit A un anneau commutatif unitaire, $\mathfrak{p}$ un idéal premier de A. On note $A_{\mathfrak{p}}$ le localisé de A par rapport à la partie multiplicative $A \setminus \mathfrak{p}$.

Dans la suite, on fixe un élément $x \in F|k$ transcendant.

Définition 7.2. On définit les deux anneaux suivants :
- l'*ordre fini maximal* $\mathcal{O}_F$ comme étant la fermeture intégrale de $k[x]$ dans F ;
- l'*ordre infini maximal* $\mathcal{O}_F^{\infty}$ comme étant la fermeture intégrale de $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$ dans F.

Remarque. On peut continuer le rapprochement avec les corps de nombres ; si $K/\mathbb{Q}$ est un corps de nombres, alors l'anneau $\mathcal{O}_K$ des entiers de K est défini comme étant la fermeture intégrale de $\mathbb{Z}$ dans K. C'est bien la même notion que $\mathcal{O}_F$ car $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) \leftrightarrow k(x) = \mathrm{Frac}(k[x])$ et $K/\mathbb{Q}$ est finie $\leftrightarrow F/k(x)$ est finie.

Proposition 7.3. *Les anneaux $\mathcal{O}_F$ et $\mathcal{O}_F^\infty$ sont des anneaux de Dedekind.*

Démonstration. L'anneau $k[x]$ est principal donc est un anneau de Dedekind ; de plus, F est une extension finie de $k(x) = \mathrm{Frac}(k[x])$. Le fait que $\mathcal{O}_F$ soit un anneau de Dedekind découle alors directement de [9, proposition I.12.8]. On applique le même raisonnement pour $\mathcal{O}_F^\infty$ en remarquant toutefois deux choses : $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$ est principal en tant que localisé d'un anneau principal et $k[\frac{1}{x}] \subseteq k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle} \subseteq k(x)$ donc $\mathrm{Frac}(k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}) = k(x)$. □

Théorème 7.4. *Si $F|k$ est régulier, on a les égalités suivantes :*

$$\mathcal{O}_F = \bigcap_{\mathrm{ord}_P(x) \geqslant 0} \mathcal{O}_P$$
$$\mathcal{O}_F^\infty = \bigcap_{\mathrm{ord}_P(x) < 0} \mathcal{O}_P$$

où les intersections sont prises sur $P \in \mathbb{P}_F$. De plus, F est le corps des fractions de $\mathcal{O}_F$ et de $\mathcal{O}_F^\infty$.

Démonstration. On utilise [11, théorème 3.2.6.(b)] avec $R := k[x]$ pour la première égalité puis $R := k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$ pour la deuxième. Reste à montrer les deux équivalences suivantes :

$$k[x] \subseteq \mathcal{O}_P \iff \mathrm{ord}_P(x) \geqslant 0 \tag{2}$$
$$k\left[\frac{1}{x}\right]_{\langle \frac{1}{x} \rangle} \subseteq \mathcal{O}_P \iff \mathrm{ord}_P(x) < 0 \tag{3}$$

Avant de commencer, mentionnons que l'on va utiliser la propriété 2.18 à plusieurs reprises. Démontrons maintenant (2).

- Si $k[x] \subseteq \mathcal{O}_P$, alors $x \in \mathcal{O}_P$ donc $\mathrm{ord}_P(x) \geqslant 0$;
- si $\mathrm{ord}_P(x) \geqslant 0$, alors $x \in \mathcal{O}_P$; par définition d'un anneau de valuation, $k \subseteq \mathcal{O}_P$ donc on a $k[x] \subseteq \mathcal{O}_P$.

Démontrons maintenant (3) ; pour plus de lisibilité on pose $y := \frac{1}{x}$.

- Si $k[y]_{\langle y \rangle} \subseteq \mathcal{O}_P$ alors $y \in \mathcal{O}_P$; supposons que $y \notin P$. Tous les éléments de $k[y] \setminus \langle y \rangle$ sont inversibles dans $k[y]_{\langle y \rangle}$ donc sont également inversibles dans $\mathcal{O}_P$. De plus, $y \in \mathcal{O}_P \setminus P$ donc y est également inversible dans $\mathcal{O}_P$. Finalement, pour $f \in k[y]$ on peut écrire $f = y^n g$ avec $n \in \mathbb{N}$ et $g \in k[y] \setminus \langle y \rangle$; ces deux éléments y^n et g sont dans $\mathcal{O}_P^\times$ donc f l'est également. Tous les éléments de $k[y]$ sont ainsi inversibles dans $\mathcal{O}_P$ donc $\mathrm{Frac}(k[y]) = k(x) \subseteq \mathcal{O}_P$. Ce résultat contredit le lemme 2.6 ; on a finalement $y \in P$ donc $\mathrm{ord}_P(y) > 0$ *i.e.* $\mathrm{ord}_P(x) < 0$.
- Si $\mathrm{ord}_P(x) < 0$, alors $\mathrm{ord}_P(y) > 0$ donc comme précédemment on obtient $k[y] \subseteq \mathcal{O}_P$. Soit $f \in k[y] \setminus \langle y \rangle$ et montrons que f est inversible dans $\mathcal{O}_P$; pour cela, écrivons $f = a + yg$ avec $a \in k^*$ et $g \in k[y]$. On a $\mathrm{ord}_P(y) > 0$ donc $y \in P$; comme $g \in k[y] \subseteq \mathcal{O}_P$ on a $yg \in P$. Or, $a \notin P$ donc $f \notin P$; comme $f \in k[y] \subseteq \mathcal{O}_P$ on a donc $f \in \mathcal{O}_P^\times$. Ainsi, les éléments de $k[y] \setminus \langle y \rangle$ sont inversibles dans $\mathcal{O}_P$ donc $k[y]_{\langle y \rangle} \subseteq \mathcal{O}_P$.

Cela achève la démonstration. □

Dans toute la suite, le symbole $*$ signifie que l'on considère l'ordre fini ou bien l'ordre infini ; bien sûr on doit faire la même référence tout au long d'un énoncé. Ainsi, l'énoncé suivant :

$$\forall P \in \mathbb{P}_F^*, \mathcal{O}_F^* \subseteq \mathcal{O}_P$$

doit s'interpréter de cette façon :

– pour les places $P \in \mathbb{P}_F$ avec $\mathrm{ord}_P(x) \geqslant 0$ on a $\mathcal{O}_F \subseteq \mathcal{O}_P$;
– pour les places $P \in \mathbb{P}_F$ avec $\mathrm{ord}_P(x) < 0$ on a $\mathcal{O}_F^\infty \subseteq \mathcal{O}_P$.

On ne va pas utiliser l'astérisque pour désigner un anneau privé de 0 donc il n'y a pas de confusion possible.

7.2 Quelques résultats

On regroupe dans cette section quelques résultats relatifs aux places, aux idéaux et aux ordres maximaux.

Lemme 7.5. *On suppose que $F|k$ est régulier. Toute place de $\mathbb{P}_F^*$ admet un élément premier dans $\mathcal{O}_F^*$, i.e. :*

$$\forall P \in \mathbb{P}_F^*, \exists \pi \in P \cap \mathcal{O}_F^*, P = \langle \pi \rangle.$$

Démonstration. Soit $P \in \mathbb{P}_F$.

– On suppose que $\mathrm{ord}_P(x) < 0$. Par le théorème 2.22, on sait que x n'a qu'un nombre fini de pôles ce qui signifie que l'ensemble $S := \{Q \in \mathbb{P}_F : \mathrm{ord}_Q(x) < 0\}$ est fini. Par le théorème 2.23, on peut donc trouver $x \in F$ tel que $\mathrm{ord}_P(x) = 1$ et $\mathrm{ord}_Q(x) \geqslant 0 \ \forall Q \in S \setminus \{P\}$. Ainsi, d'une part x est un élément premier de P (propriété 2.15) et d'autre part on a $x \in \cap_{Q \in S} \mathcal{O}_Q = \mathcal{O}_F^\infty$ par le théorème 7.4.
– On suppose que $\mathrm{ord}_P(x) \geqslant 0$. Par la proposition 2.20, on sait que x possède au moins un pôle ce qui signifie que l'ensemble $S := \{Q \in \mathbb{P}_F : \mathrm{ord}_Q(x) \geqslant 0\}$ est strictement inclus dans $\mathbb{P}_F$. Par le théorème 2.25, on peut donc trouver $x \in F$ tel que $\mathrm{ord}_P(x) = 1$ et $\mathrm{ord}_Q(x) \geqslant 0 \ \forall Q \in S \setminus \{P\}$. Ainsi, d'une part x est un élément premier de P et d'autre part on a $x \in \cap_{Q \in S} \mathcal{O}_Q = \mathcal{O}_F$ par le théorème 7.4.

□

Soit maintenant $x \in F|k$ un élément transcendant.

Proposition 7.6. *Si $F/k(x)$ est séparable, alors tout idéal fractionnaire de $\mathcal{O}_F$ (respectivement $\mathcal{O}_F^\infty$) est un $k[x]$-module libre (resp. $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$-module libre) de rang $[F : k(x)]$.*

Démonstration. Cela résulte de [9, proposition I.2.10] ; remarquons encore une fois que $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$ est principal en tant que localisé d'un anneau principal. □

Définition 7.7. Si I est un idéal fractionnaire de $\mathcal{O}_F$ (resp. $\mathcal{O}_F^\infty$), une *base* de I désigne une base de I en tant que $k[x]$-module libre (resp. $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$-module libre).

Remarque. Une base d'un idéal fractionnaire de $\mathcal{O}_F^*$ est également un système de générateurs.

Finalement, soit $F'|k$ un corps de fonctions tel que $F'|F$ soit une extension finie. On suppose de plus que c'est aussi l'élément x qui a servi à définir les ordres maximaux de $F'|k$.

Propriété 7.8. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F^*$. Alors $\mathcal{O}_F^*/\mathfrak{p}$ est une extension finie de k.*

Démonstration. (On s'inspire de [11, proposition 1.1.15].) Comme $k \subseteq \mathcal{O}_P \ \forall P \in \mathbb{P}_F$ on a $k \subseteq \mathcal{O}_F^*$; l'application $k \to \mathcal{O}_F^*/\mathfrak{p}$ reste injective car $k \cap \mathfrak{p} = \{0\}$ ($\mathfrak{p}$ ne contient aucun élément inversible dans $\mathcal{O}_F^*$). Montrons maintenant que $\mathcal{O}_F^*/\mathfrak{p}$ est une extension finie de k.

On fixe un $y \in \mathfrak{p} \setminus \{0\}$; comme dans la démonstration de la proposition 6.21, on montre que si y est algébrique sur k alors $\exists a \in k^*, a \in \mathfrak{p}$ ce qui est absurde puisque a est alors inversible dans $\mathcal{O}_F^*$ (on vient de voir que $k \subseteq \mathcal{O}_F^*$). Ainsi, y est transcendant sur k donc par la propriété 2.3, $[F : k(y)] < \infty$; on va montrer que $[\mathcal{O}_F^*/\mathfrak{p} : k] \leqslant [F : k(y)]$.

Pour cela, soit $([z_1], \ldots, [z_n])$ une famille k-libre de $\mathcal{O}_F^*/\mathfrak{p}$, $z_i \in \mathcal{O}_F^*$. Montrons que $(z_1, \ldots, z_n)$ est une famille $k(y)$-libre de F ; on suppose qu'il existe $\lambda_1, \ldots, \lambda_n \in k(y)$ non tous nuls tels que

$\sum_{i=1}^n \lambda_i z_i = 0$; quitte à multiplier par un dénominateur commun, on peut supposer $\lambda_i \in k[y]$ $\forall i$. De plus, quitte à diviser par y plusieurs fois on peut supposer qu'il existe un λ_{i_0} qui n'est pas divisible par y. En écrivant $\lambda_i = \lambda_i^0 + y\mu_i$ avec $\lambda_i^0 \in k, \mu_i \in k[y]$, comme $k[y] \subseteq \mathcal{O}_F^*$ et que $y \in \mathfrak{p}$ on a $[\lambda_i] = [\lambda_i^0]$. Ainsi, la relation $\sum_{i=1}^n \lambda_i z_i = 0$ devient dans $\mathcal{O}_F^*/\mathfrak{p}$:

$$\sum_{i=1}^n [\lambda_i^0][z_i] = 0.$$

Comme $\lambda_i^0 \in k$ et que $([z_i])$ est une famille k-libre, on a $\lambda_i^0 \in \mathfrak{p}$ $\forall i$ donc comme $\lambda_i^0 \in k$ on a $\lambda_i^0 = 0$ $\forall i$: cela contredit le fait que $\lambda_{i_0}^0 \neq 0$. Ainsi, une telle famille (λ_i) n'existe pas ce qui signifie que $(z_1, \ldots, z_n)$ est libre sur $k(y)$.

Finalement, il existe s'il existe une famille k-libre dans $\mathcal{O}_F^*/\mathfrak{p}$ de cardinal n alors $n \leqslant [F : k(y)] < \infty$ (on rappelle que y a été fixé) ce qui conclut la démonstration. □

Définition 7.9. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F^*$. On définit le *degré* de $\mathfrak{p}$ de la façon suivante :

$$\deg \mathfrak{p} := \left[\frac{\mathcal{O}_F^*}{\mathfrak{p}} : k\right] \in \mathbb{N}^*.$$

Propriété 7.10. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_F^*$ et soit $\mathfrak{p}'$ un idéal premier non nul de $\mathcal{O}_{F'}^*$ qui divise $\mathfrak{p}$. Alors on a l'égalité suivante :*

$$f_{\mathfrak{p}'|\mathfrak{p}} = \frac{\deg \mathfrak{p}'}{\deg \mathfrak{p}}.$$

Démonstration. Cela résulte simplement de la formule de multiplicativité des degrés : $\deg \mathfrak{p}' = [\mathcal{O}_{F'}^*/\mathfrak{p}' : k] = [\mathcal{O}_{F'}^*/\mathfrak{p}' : \mathcal{O}_F^*/\mathfrak{p}] \cdot [\mathcal{O}_F^*/\mathfrak{p} : k] = f_{\mathfrak{p}'|\mathfrak{p}} \deg \mathfrak{p}$. □

7.3 Idéaux fractionnaires correspondant à un diviseur

On suppose ici que $F|k$ est régulier. Le théorème 7.4 permet de considérer les inclusions $\iota_P^* : \mathcal{O}_F^* \to \mathcal{O}_P$. En particulier si $P \in \mathbb{P}_F^*$ est une place, comme P est un idéal maximal de $\mathcal{O}_P$ c'est un idéal premier donc $(\iota_P^*)^{-1}(P) = P \cap \mathcal{O}_F^*$ est un idéal premier de $\mathcal{O}_F^*$ (non nul par le lemme 7.5).

Définition 7.11. On dit que $\mathfrak{p}$ idéal premier non nul de $\mathcal{O}_F^*$ et $P \in \mathbb{P}_F^*$ sont *associés* si $\mathfrak{p} = (\iota_P^*)^{-1}(P)$.

On a vu que toute place de F possède un idéal premier non nul de $\mathcal{O}_F^*$ associé. La proposition suivante affirme que tous les idéaux premiers non nuls de $\mathcal{O}_F^*$ sont associés à une place de F.

Proposition 7.12. *Il y a une correspondance bijective entre l'ensemble des idéaux premiers non nuls de $\mathcal{O}_F^*$ et l'ensemble des places $P \in \mathbb{P}_F^*$, et cette bijection est donnée par $P \mapsto (\iota_P^*)^{-1}(P) = P \cap \mathcal{O}_F^*$.*

Démonstration. La proposition 7.3 nous assure que les idéaux premiers non nuls de $\mathcal{O}_F^*$ sont exactement ses idéaux maximaux. On conclut alors avec la première partie de [11, proposition 3.2.9]. □

Profitons-en pour énoncer un lemme qui nous sera utile plus tard.

Lemme 7.13. *Soit $P \in \mathbb{P}_F^*$ et soit I un idéal propre de $\mathcal{O}_P$ tel que $P \cap \mathcal{O}_F^* \subseteq I \cap \mathcal{O}_F^*$. Alors $P = I$.*

Démonstration. Par le lemme 7.5, on peut trouver $\pi \in P \cap \mathcal{O}_F^*$ tel que $P = \langle \pi \rangle$. Ainsi, $\pi \in I$ donc $P \subseteq I$; comme P est maximal et que I est propre on en déduit que $P = I$. □

Voici maintenant la définition de la correspondance entre idéaux fractionnaires et diviseurs.

Définition 7.14. Soit $D := \sum n_P P \in \mathrm{Div}(F)$. On définit la *partie finie* de D par :

$$D_0 := \prod_{\mathrm{ord}_P(x) \geqslant 0} [\iota_P^{-1}(P)]^{n_P} \in \mathfrak{J}_{\mathcal{O}_F}$$

ainsi que la *partie infinie* de D par :

$$D_\infty := \prod_{\mathrm{ord}_P(x) < 0} [(\iota_P^\infty)^{-1}(P)]^{n_P} \in \mathfrak{J}_{\mathcal{O}_F^\infty}$$

les produits portant sur les places du support de D.

Remarque. Les notations $\mathfrak{J}_{\mathcal{O}_F}$ et $\mathfrak{J}_{\mathcal{O}_F^\infty}$ sont justifiées par la proposition 7.3.

Théorème 7.15 (Correspondance entre diviseurs et idéaux)**.** *L'application de* $\mathrm{Div}(F)$ *dans le produit direct* $\mathfrak{J}_{\mathcal{O}_F} \times \mathfrak{J}_{\mathcal{O}_F^\infty}$ *qui à un diviseur* D *associe le couple* (D_0, D_∞) *est un isomorphisme.*

Remarque. On fait un abus de langage car on devrait dire « correspondance entre diviseurs et idéaux *fractionnaires* ».

Démonstration. C'est bien un morphisme ; l'injectivité découle de l'unicité de la décomposition du corollaire 6.11 ; la surjectivité est assurée par la proposition 7.12 et par le fait que les ensembles $\{P \in \mathbb{P}_F : \mathrm{ord}_P(x) \geqslant 0\}$ et $\{P \in \mathbb{P}_F : \mathrm{ord}_P(x) < 0\}$ sont disjoints. □

Définition 7.16. On note $\mathfrak{D}_F$ l'inverse de l'application qui réalise la correspondance $\mathrm{Div}(F) \to \mathfrak{J}_{\mathcal{O}_F} \times \mathfrak{J}_{\mathcal{O}_F^\infty}$.

7.4 Conorme, norme (III)

On suppose encore que $F|k$ est régulier. Soit $F'|k'$ un corps de fonctions régulier qui est une extension finie de $F|k$; rappelons que l'on a alors k'/k finie. On suppose que c'est le même élément transcendant x qui a été choisi pour définir les ordres maximaux de F et de F' ; on suppose également que k'/k est galoisienne.

Proposition 7.17. *$\mathcal{O}_{F'}^*$ est la fermeture intégrale de $\mathcal{O}_F^*$ dans F'.*

Démonstration. On se place tout d'abord dans le cas des places qui ne sont pas des pôles de x. La propriété résulte du fait que $k'[x]$ est entier (*i.e.* tous les éléments sont entiers) sur $k[x]$. En effet, comme k'/k est finie, k' est entier sur k donc sur $k[x]$; x est trivialement entier sur $k[x]$ donc comme les éléments entiers forment un anneau [10] on a $k'[x]$ entier sur $k[x]$. Ainsi pour $z \in F', z$ entier sur $\mathcal{O}_F$ ssi z entier sur $k[x]$ (note [11]) ssi z entier sur $k'[x]$ ssi $z \in \mathcal{O}_{F'}$.

Dans le cas des ordres infinis maximaux, il suffit juste de montrer que l'inclusion $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle} \subseteq k'[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$ est entière. Pour plus de clarté, posons $y := \frac{1}{x}$; on doit donc montrer que l'inclusion $k[y]_{k[y]\setminus\langle y \rangle} \subseteq k'[y]_{k'[y]\setminus\langle y \rangle}$ est entière. Étant donné que $k[y] \setminus \langle y \rangle_{k[y]} = k[y] \setminus \langle y \rangle_{k'[y]}$, on peut simplement écrire $k[y] \setminus \langle y \rangle$; en outre, $k'[y] \setminus \langle y \rangle$ signifie $k'[y] \setminus \langle y \rangle_{k'[y]}$. Par ce qui précède, $k'[y]$ est entier sur $k[y]$ donc on a trivialement le fait que $k[y]_{k[y]\setminus\langle y \rangle} \subseteq k'[y]_{k[y]\setminus\langle y \rangle}$ est entière. Reste à montrer que $k'[y]_{k[y]\setminus\langle y \rangle} \subseteq k'[y]_{k'[y]\setminus\langle y \rangle}$ est entière. En fait, on va montrer l'égalité.

Soit $R \in k'[y]_{k'[y]\setminus\langle y \rangle}$: montrons que $R \in k'[y]_{k[y]\setminus\langle y \rangle}$. On peut écrire $R = P/(1 + yQ)$ avec $P, Q \in k'[y]$; il suffit de trouver $S \in k'[y] \setminus \langle y \rangle$ tel que $(1 + yQ)S \in k[y] \setminus \langle y \rangle$ (remarquons que $(1 + yQ)S \in k'[y] \setminus \langle y \rangle$) ; en effet, on aura alors $R = P/(1 + yQ) = PS/((1 + yQ)S) \in k'[y]_{k[y]\setminus\langle y \rangle}$.

Pour cela, on va montrer que l'extension $k'(y)/k(y)$ est galoisienne ; on pourra ainsi utiliser la *norme* de $1 + yQ$. Il suffit de montrer que $\#\mathrm{Gal}(k'(y)/k(y)) = [k'(y) : k(y)]$.

10. C'est un résultat classique d'algèbre commutative ; voir par exemple [9, juste avant la proposition I.2.4].
11. C'est également un résultat classique d'algèbre commutative, voir [9, proposition I.2.4].

– On a un isomorphisme canonique $\mathrm{Gal}(k'/k) \simeq \mathrm{Gal}(k'(y)/k(y))$: pour $\sigma \in \mathrm{Gal}(k'/k)$ il suffit de poser $\sigma(y) := y$ et si $\sigma \in \mathrm{Gal}(k'(y)/k(y))$ il suffit de remarquer que $\sigma(k') = k'$ car $\deg \sigma(P) = \deg T \ \forall T \in k'[y]$. Ainsi $\#\mathrm{Gal}(k'(y)/k(y)) = \#\mathrm{Gal}(k'/k)$.
– D'après [11, lemme 3.1.10] on a $[k'(y) : k(y)] = [k' : k]$ (remarquons que k est parfait et que k'/k est finie).

Ainsi, comme k'/k est galoisienne (par hypothèse) on a $\#\mathrm{Gal}(k'/k) = [k' : k]$ donc par ce qui précède on a $\#\mathrm{Gal}(k'(y)/k(y)) = [k'(y) : k(y)]$ *i.e.* $k'(y)/k(y)$ est galoisienne.

Pour $\sigma \in \mathrm{Gal}(k'(y)/k(y))$ on a $\sigma(1 + yQ) = 1 + y\,\sigma(Q) \in k'[y] \setminus \langle y \rangle$; en effet, $\sigma(k'[y]) = k'[y]$ (toujours car $\deg \sigma(T) = \deg T \ \forall T \in k'[y]$). Ainsi, si l'on pose $S := \prod_{\sigma \neq \mathrm{id}} \sigma(1 + yQ)$ (où σ parcourt $\mathrm{Gal}(k'(y)/k(y))$), comme $\langle y \rangle_{k'[y]}$ est premier on obtient $(1 + yQ)S \in k'[y] \setminus \langle y \rangle$. Or, $(1 + yQ)S$ est également la norme relative à l'extension de corps $k'(x)/k(x)$ de l'élément $1 + yQ$: on a donc $(1 + yQ)S \in k(x)$. Finalement, on a $(1 + yQ)S \in k[y] \setminus \langle y \rangle$ ce qui termine la démonstration. □

Remarque. On a en fait également démontré que $\mathcal{O}_{F'}$ est la fermeture intégrale de $k[x]$ dans F' et que $\mathcal{O}_{F'}^{\infty}$ est la fermeture intégrale de $k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$ dans F'.

Théorème 7.18. *Les deux morphismes de norme sont compatibles avec la correspondance entre diviseurs et idéaux, plus précisément :*

$$\forall D' \in \mathrm{Div}(F'), \mathrm{N}_{F'/F}(D') = \mathfrak{D}_F(\mathrm{N}_{F'/F}(D'_0), \mathrm{N}_{F'/F}(D'_\infty)).$$

La démonstration du théorème repose sur le lemme suivant.

Lemme 7.19. *Soit $P \in \mathbb{P}_F^*$ une place et $P' \in \mathbb{P}_{F'}^*$ une place qui divise P ; on note $\mathfrak{p}$ et $\mathfrak{p}'$ leur idéal associé respectif. Alors $f_{\mathfrak{p}'|\mathfrak{p}} = f_{P'|P}$.*

Démonstration. Remarquons tout d'abord que l'on a bien $\mathfrak{p}'|\mathfrak{p}$: en effet, on a $\mathfrak{p} = P \cap \mathcal{O}_F^* \subseteq P' \cap \mathcal{O}_{F'}^* = \mathfrak{p}'$ donc on conclut par la proposition 6.19.

D'après [11, proposition 3.2.9], l'injection canonique $\mathcal{O}_F^* \hookrightarrow \mathcal{O}_P/P$ induit un isomorphisme de corps $\mathcal{O}_F^*/\mathfrak{p} \simeq \mathcal{O}_P/P$; de plus, cet isomorphisme laisse k invariant. Ces deux corps étant des k-espaces vectoriels, cet isomorphisme est k-linéaire donc les espaces étant de dimension finie ils ont la même dimension sur k. Ainsi, on obtient l'égalité suivante :

$$\left[\frac{\mathcal{O}_F^*}{\mathfrak{p}} : k\right] = \left[\frac{\mathcal{O}_P}{P} : k\right]$$

(*i.e.* $\deg \mathfrak{p} = \deg P$) ; on a évidemment de la même façon $\deg \mathfrak{p}' = \deg P'$. Ainsi, par la formule de multiplicativité des degrés :

$$\left[\frac{\mathcal{O}_{F'}^*}{\mathfrak{p}'} : k\right] = \left[\frac{\mathcal{O}_{F'}^*}{\mathfrak{p}'} : k'\right][k' : k] = \left[\frac{\mathcal{O}_{P'}}{P'} : k'\right][k' : k] = \left[\frac{\mathcal{O}_{P'}}{P'} : k\right].$$

Or, on a également :

$$\left[\frac{\mathcal{O}_{F'}^*}{\mathfrak{p}'} : k\right] = \left[\frac{\mathcal{O}_{F'}^*}{\mathfrak{p}'} : \frac{\mathcal{O}_F^*}{\mathfrak{p}}\right]\left[\frac{\mathcal{O}_F^*}{\mathfrak{p}} : k\right]$$
$$\left[\frac{\mathcal{O}_F}{P'} : k\right] = \left[\frac{\mathcal{O}_{P'}}{P'} : \frac{\mathcal{O}_P}{P}\right]\left[\frac{\mathcal{O}_P}{P} : k\right]$$

donc par ce qui précède on obtient :

$$\left[\frac{\mathcal{O}_{F'}^*}{\mathfrak{p}'} : \frac{\mathcal{O}_F^*}{\mathfrak{p}}\right] = \left[\frac{\mathcal{O}_{P'}}{P'} : \frac{\mathcal{O}_P}{P}\right]$$

et c'est exactement ce que l'on voulait démontrer. □

Démonstration du théorème. Étant donné que $\mathrm{N}_{F'/F}$ et $\mathfrak{D}_F$ sont des morphismes, il suffit de vérifier l'égalité pour les places de $\mathbb{P}_{F'}$; soit $P' \in \mathbb{P}_{F'}$. On va faire la démonstration dans la cas où $\mathrm{ord}_P(x) < 0$, l'autre cas étant totalement similaire. Soit $P \in \mathbb{P}_F$ l'unique place de F que divise P' ; soient $\mathfrak{p}$ et $\mathfrak{p}'$ les idéaux associés à P et P' respectivement. Autrement dit, on a $\mathfrak{D}_F(\mathcal{O}_F, \mathfrak{p}) = P$ et $P'_0 = \mathcal{O}_{F'}, P'_\infty = \mathfrak{p}'$. On a $\mathfrak{D}_F(\mathrm{N}_{F'/F}(P'_0), \mathrm{N}_{F'/F}(P'_\infty)) = \mathfrak{D}_F(\mathrm{N}_{F'/F}(\mathcal{O}_{F'}), \mathrm{N}_{F'/F}(\mathfrak{p}')) = \mathfrak{D}_F(\mathcal{O}_F, \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}})$. Or, $(\mathcal{O}_F, \mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}}) = (\mathcal{O}_F, \mathfrak{p})^{f_{\mathfrak{p}'|\mathfrak{p}}}$ donc comme $\mathfrak{D}_F$ est un morphisme on a $\mathfrak{D}_F(\mathrm{N}_{F'/F}(P'_0), \mathrm{N}_{F'/F}(P'_\infty)) = f_{\mathfrak{p}'|\mathfrak{p}}\mathfrak{D}_F(\mathcal{O}_F, \mathfrak{p}) = f_{\mathfrak{p}'|\mathfrak{p}}P$. Par le lemme, cette quantité est donc exactement égale à $f_{P'|P}P$ qui n'est autre que $N_{F'/F}(P)$ par définition. □

Une autre façon de voir le théorème est de dire que le diagramme de la figure 1 est commutatif.

$$\begin{array}{ccc} \mathrm{Div}(F') & \xrightarrow{(\mathfrak{D}_{F'})^{-1}} & \mathfrak{J}_{\mathcal{O}_{F'}} \times \mathfrak{J}_{\mathcal{O}_{F'}^\infty} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F} \times \mathrm{N}_{F'/F}} \\ \mathrm{Div}(F) & \xleftarrow[\mathfrak{D}_F]{} & \mathfrak{J}_{\mathcal{O}_F} \times \mathfrak{J}_{\mathcal{O}_F^\infty} \end{array}$$

FIGURE 1 – Illustration du théorème 7.18.

Théorème 7.20. *Si F'/F est séparable, alors les deux morphismes de conorme sont compatibles avec la correspondance entre diviseurs et idéaux, plus précisément :*

$$\forall D \in \mathrm{Div}(F), \mathrm{Con}_{F'/F}(D) = \mathfrak{D}_{F'}(\mathrm{Con}_{F'/F}(D_0), \mathrm{Con}_{F'/F}(D_\infty)).$$

La démonstration du théorème repose sur le lemme suivant.

Lemme 7.21. *Soit $P \in \mathbb{P}_F^*$ une place et $P' \in \mathbb{P}_{F'}^*$ une place qui divise P ; on note $\mathfrak{p}$ et $\mathfrak{p}'$ leur idéal associé respectif. Si F'/F est séparable alors $e_{\mathfrak{p}'|\mathfrak{p}} = e_{P'|P}$.*

Démonstration. Rappelons que par le lemme précédent on a $f_{\mathfrak{p}'|\mathfrak{p}} = f_{P'|P}$. Pour montrer l'égalité des indices de ramification, on va en fait montrer une inégalité puis utiliser les deux égalités fondamentales que l'on a présentées, *i.e.* les résultats des théorèmes 2.50 et 6.18.

Soit $e \in \mathbb{N}^*$ tel que $\mathfrak{p} \subseteq \mathfrak{p}'^e$. On a donc $P \cap \mathcal{O}_F^* \subseteq (P' \cap \mathcal{O}_{F'}^*)^e \subseteq P'^e \cap \mathcal{O}_{F'}^*$ donc $P \cap \mathcal{O}_F^* \subseteq P'^e \cap \mathcal{O}_F^*$. Comme $\mathcal{O}_F^* \subseteq F$ on a $\mathcal{O}_F^* = \mathcal{O}_F^* \cap F$; on a donc $P \cap \mathcal{O}_F^* \subseteq (P'^e \cap F) \cap \mathcal{O}_F^*$. Or, $P'^e \cap F$ est un idéal propre de $\mathcal{O}_P$: en effet, $P'^e \cap F \subseteq P' \cap F = P$. On déduit alors du lemme 7.13 que $P = P'^e \cap F$. D'après la proposition 2.45 on a donc $e \leqslant e_{P'|P}$. En prenant $e = e_{\mathfrak{p}'|\mathfrak{p}}$ on a donc $e_{\mathfrak{p}'|\mathfrak{p}} \leqslant e_{P'|P}$.

Par le théorème 2.50 on a $\sum_{P'|P} e_{P'|P} f_{P'|P} = [F' : F]$ où l'on somme sur $P' \in \mathbb{P}_{F'}$; de plus, comme F'/F est séparable on a également par le théorème 6.18 l'égalité $\sum_{\mathfrak{p}'|\mathfrak{p}} e_{\mathfrak{p}'|\mathfrak{p}} f_{\mathfrak{p}'|\mathfrak{p}} = [F' : F]$ où l'on somme sur les idéaux premiers non nuls $\mathfrak{p}'$ de $\mathcal{O}_F^*$. On a donc $\sum_{P'|P} e_{P'|P} f_{P'|P} = \sum_{\mathfrak{p}'|\mathfrak{p}} e_{\mathfrak{p}'|\mathfrak{p}} f_{\mathfrak{p}'|\mathfrak{p}}$ avec $e_{\mathfrak{p}'|\mathfrak{p}} \leqslant e_{P'|P}$ et $f_{\mathfrak{p}'|\mathfrak{p}} = f_{P'|P}$ $\forall P', \mathfrak{p}' := (\iota_{P'}^*)^{-1}(P')$ donc $e_{\mathfrak{p}'|\mathfrak{p}} = e_{P'|P}$ $\forall P', \mathfrak{p}'$ associés.

□

Remarque. En prenant $e = 1$ dans la démonstration, on démontre que si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers non nuls tels que $\mathfrak{p}'|\mathfrak{p}$, alors en considérant leur place $P \in \mathbb{P}_F$ et $P' \in \mathbb{P}_{F'}$ respective alors on a $P = P' \cap F$ *i.e.* $P'|P$. On peut donc dans les deux lemmes précédents considérer d'abord les idéaux $\mathfrak{p}$ et $\mathfrak{p}'$ puis leur place associée respective P et P'.

Proposition 7.22. *Soient $P \in \mathbb{P}_F^*, P' \in \mathbb{P}_{F'}^*$ et soient $\mathfrak{p}, \mathfrak{p}'$ des idéaux premiers non nuls de $\mathcal{O}_F^*, \mathcal{O}_{F'}^*$ respectivement. On suppose que P et $\mathfrak{p}$ sont associés ainsi que P' et $\mathfrak{p}'$. Alors $P'|P$ ssi $\mathfrak{p}'|\mathfrak{p}$.*

Démonstration. Sens direct : début de la démonstration du lemme 7.19. Sens indirect : remarque ci-avant. □

Démonstration du théorème. Encore une fois, il suffit de démontrer l'égalité pour les places de F. Soit $P \in \mathbb{P}_F$ telle que $\mathrm{ord}_P(x) < 0$ (encore une fois, l'autre cas est totalement similaire) et soit $\mathfrak{p}$ l'idéal associé ; P' parcourt $\mathbb{P}_{F'}$ et $\mathfrak{p}'$ parcourt les idéaux premiers non nuls de $\mathcal{O}_{F'}^{\infty}$. Quand les lettres P' et $\mathfrak{p}'$ sont utilisées en même temps, cela signifie que P' et $\mathfrak{p}'$ sont associés.

On a :

$$\begin{aligned}\mathfrak{D}_{F'}(\mathrm{Con}_{F'/F}(P_0), \mathrm{Con}_{F'/F}(P_\infty)) &= \mathfrak{D}_{F'}(\mathrm{Con}_{F'/F}(\mathcal{O}_F), \mathrm{Con}_{F'/F}(\mathfrak{p})) \\ &= \mathfrak{D}_{F'}(\mathcal{O}_{F'}, \prod_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{p}'^{e_{\mathfrak{p}'|\mathfrak{p}}}) = \sum_{\mathfrak{p}'|\mathfrak{p}} e_{\mathfrak{p}'|\mathfrak{p}} \mathfrak{D}_{F'}(\mathcal{O}_{F'}, \mathfrak{p}') = \sum_{\mathfrak{p}'|\mathfrak{p}} e_{\mathfrak{p}'|\mathfrak{p}} P'.\end{aligned}$$

donc par la proposition précédente cette quantité est égale à $\sum_{P'|P} e_{\mathfrak{p}'|\mathfrak{p}} P'$. En utilisant le lemme, on obtient alors $\sum_{P'|P} e_{P'|P} P'$ ce qui est par définition $\mathrm{Con}_{F'/F}(P)$. □

Une autre façon de voir le théorème est de dire que le diagramme de la figure 2 est commutatif.

$$\begin{array}{ccc} \mathrm{Div}(F') & \xleftarrow{\mathfrak{D}_{F'}} & \mathfrak{J}_{\mathcal{O}_{F'}} \times \mathfrak{J}_{\mathcal{O}_{F'}^{\infty}} \\ \uparrow{\scriptstyle \mathrm{Con}_{F'/F}} & & \uparrow{\scriptstyle \mathrm{Con}_{F'/F} \times \mathrm{Con}_{F'/F}} \\ \mathrm{Div}(F) & \xrightarrow[(\mathfrak{D}_F)^{-1}]{} & \mathfrak{J}_{\mathcal{O}_F} \times \mathfrak{J}_{\mathcal{O}_F^{\infty}} \end{array}$$

FIGURE 2 – Illustration du théorème 7.20.

8 Avant d'écrire le programme

On rappelle que l'on utilise le logiciel MAGMA. Le morphisme de conorme–norme va être implémenté avec la représentation par idéaux des diviseurs. Remarquons que les isomorphismes entre diviseurs et idéaux fractionnaires $\mathfrak{D}$ et $\mathfrak{D}^{-1}$ sont implémentés en MAGMA.

MAGMA a beau être un logiciel capable de beaucoup de choses, il ne dispose par exemple pas de fonction pour construire les clôtures galoisiennes. Ainsi, cette section a pour but d'une part de présenter sur quelles bases l'on va programmer les objets en MAGMA et d'autre part de vérifier les hypothèses dont on a besoin, en particulier en vue d'utiliser les théorèmes 7.18 et 7.20 sur la correspondance entre diviseurs et idéaux. À partir de maintenant on se place dans le cadre de ce que j'ai réalisé durant mon stage : $n = 3$ et $E/\mathbb{F}_{q^3} := H/\mathbb{F}_{q^n}$ est une courbe elliptique. En particulier, q et n sont impairs et n est premier ce qui nous place dans le cadre de [4].

8.1 La courbe elliptique initiale

Soit σ un générateur de $\mathrm{Gal}(\mathbb{F}_{q^3}/\mathbb{F}_q)$, par exemple $\sigma : \alpha \mapsto \alpha^q$ (cf. [11, A.15]). L'automorphisme σ s'étend de façon unique en un automorphisme de $\mathbb{F}_{q^3}(x)$ qui laisse x invariant, où x est un élément transcendant sur $\mathbb{F}_{q^3}$; on renote σ cet automorphisme. On suppose que la courbe elliptique $E/\mathbb{F}_{q^3}$ est donnée par le polynôme $y^2 - g\,\sigma(g)$ où $g \in \mathbb{F}_{q^3}[x]$ est un polynôme unitaire de degré 2 tel que $f := g\,\sigma(g)$ ne soit pas un carré dans $\mathbb{F}_{q^3}[x]$; on explique dans l'annexe B comment trouver le polynôme g à partir d'une forme de Legendre de $E/\mathbb{F}_{q^3}$. En décomposant g dans $\mathbb{F}_{q^6}[x]$ il est facile de voir que

la condition sur f est équivalente à :

$$g \text{ n'est pas un carré dans } \mathbb{F}_{q^3}[x] \text{ et } g \neq \sigma(g)$$
$$\textit{i.e. } g \text{ n'est pas un carré dans } \mathbb{F}_{q^3}[x] \text{ et } g \notin \mathbb{F}_q[x].$$

Vérifions finalement sur $\mathbb{F}_{q^3}(E)|\mathbb{F}_{q^3}$ les hypothèses que l'on a imposées sur les corps de fonctions :
- $\mathbb{F}_{q^3}$ est parfait (car fini, voir par exemple [11, A.15]) ;
- $\mathbb{F}_{q^3}$ est de caractéristique différente de 2 (car q est impair ; nécessaire pour notre définition des corps de fonctions elliptiques) ;
- $\mathbb{F}_{q^3}(E)/\mathbb{F}_{q^3}(x)$ est monogène (engendrée par y).

8.2 Le corps de fonctions $F'|\mathbb{F}_{q^3}$

Par définition, $F'/\mathbb{F}_{q^3}(x)$ est défini comme étant la clôture galoisienne de $\mathbb{F}_{q^3}(E)/\mathbb{F}_{q^3}(x)$. Ainsi, c'est une extension finie donc $F'|\mathbb{F}_{q^3}$ est bien un corps de fonctions. Vérifions sur $F'|\mathbb{F}_{q^3}$ les hypothèses que l'on a imposées sur les corps de fonctions :
- $\mathbb{F}_{q^3}$ est parfait ;
- $F'/\mathbb{F}_{q^3}(x)$ est monogène (car finie séparable car galoisienne : on peut appliquer le théorème de l'élément primitif).

On peut voir dans [11, A.11] que l'on a en fait l'égalité suivante :

$$F' = \mathbb{F}_{q^3}(E)\,\widehat{\sigma}(\mathbb{F}_{q^3}(E))\,\widehat{\sigma}^2(\mathbb{F}_{q^3}(E))$$

où $\widehat{\sigma}$ est un prolongement de $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^3}(x)/\mathbb{F}_q(x))$ en un automorphisme de F' (on a le droit car $F'/\mathbb{F}_{q^3}(x)$ est normale). Chaque $\widehat{\sigma}^i(\mathbb{F}_{q^3}(E))$ est en fait défini par $\widehat{\sigma}^i(\mathbb{F}_{q^3}(E)) = \mathbb{F}_{q^3}(x, y_i) = \mathbb{F}_{q^3}(x)[y_i]$ avec $y_i^2 = \sigma^i(f)(x)$; ainsi, on a $F' = \mathbb{F}_{q^3}(x)[y_0, y_1, y_2]$. Remarquons que comme f n'est pas un carré dans $\mathbb{F}_{q^3}(x)$, chaque $\mathbb{F}_{q^3}(x)[y_i]$ est une extension non triviale de $\mathbb{F}_{q^3}(x)$.

On observe le fait suivant :

$$y_2^2 = \sigma^2(f)(x) = [\sigma^2(g)\,\sigma^3(g)](x) = [\sigma^2(g)\,g](x) = y_1^2 y_2^2/[\sigma(g)(x)]^2.$$

Ainsi, $y_2 = y_0 y_1/\sigma(g)(x)$: étant donné que $\sigma(g) \in \mathbb{F}_{q^3}(x)$, le fait de rajouter la racine y_2 à $\mathbb{F}_{q^3}(x)[y_0, y_1]$ ne change rien. On a donc :

$$F' = \mathbb{F}_{q^3}(x)[y_0, y_1].$$

Remarque. En vertu des polynômes minimaux de y_0 et de y_1 (qui sont distincts car $f = \sigma(f) \iff g = \sigma^2(g) \iff \sigma(g) = g$ et on a vu que l'on excluait cette hypothèse), les éléments de $\mathrm{Gal}(F'/\mathbb{F}_{q^3}(x))$ sont exactement les automorphismes de $F'/\mathbb{F}_{q^3}(x)$ qui envoient y_i sur $\pm y_i, i = 1, 2$.

Posons $z := y_0 + y_1 + y_2$; z est un élément primitif de $F'/\mathbb{F}_{q^3}(x)$. En effet, les conjugués de z sous l'action de $\mathrm{Gal}(F'/\mathbb{F}_{q^3}(x))$ sont les $z_j := (-1)^{j_0} y_0 + (-1)^{j_1} y_1 + (-1)^{j_0+j_1} y_2$ pour $j \in \mathbb{F}_2^2$; on montre sans difficulté (il y a juste à utiliser $g \neq \sigma(g)$) que $\#\{z_j\}_{j\in\mathbb{F}_2^2} = 4$ qui est donc le degré du polynôme minimal h de z sur $\mathbb{F}_{q^3}(x)$ et donc également la dimension de $\mathbb{F}_{q^3}(x)[z]/\mathbb{F}_{q^3}(x)$. Or, comme $F' = \mathbb{F}_{q^3}(x)[y_0, y_1]$ on a $[F' : \mathbb{F}_{q^3}(x)] \leqslant 4$ donc finalement :

$$F' = \mathbb{F}_{q^3}(x)[z]$$

et $(1, z, z^2, z^3)$ est une $\mathbb{F}_{q^3}(x)$-base de F'.

Remarque. Chaque y_i^2 est dans $\mathbb{F}_{q^3}[x]$ donc chaque y_i est dans la fermeture intégrale de $\mathbb{F}_{q^3}[x]$ dans F' : ainsi, z est également dans cette fermeture intégrale ce qui signifie que h est à coefficients dans $\mathbb{F}_{q^3}[x]$ (note [12]).

12. C'est un résultat classique de théorie des nombres : voir par exemple [9, avant la définition I.2.5] ($\mathbb{F}_{q^3}[x]$ est bien intégralement clos).

8.3 Conorme

Pour pouvoir utiliser le théorème 7.20, on doit vérifier les hypothèses suivantes :
- $\mathbb{F}_{q^3}(E)|\mathbb{F}_{q^3}$ est régulier (c'est un corps de fonctions elliptique) ;
- $F'|\mathbb{F}_{q^3}$ est régulier (car f est unitaire, cf. [4, proposition 14]) ;
- $F'/\mathbb{F}_{q^3}(E)$ est séparable finie (car $F'/\mathbb{F}_{q^3}(x)$ l'est par définition de F') ;
- $\mathbb{F}_{q^3}(E)/\mathbb{F}_{q^3}(x)$ et $F'/\mathbb{F}_{q^3}(x)$ sont monogènes (déjà vu ; c'est pour pouvoir définir les ordres maximaux à partir du même élément transcendant x) ;
- $\mathbb{F}_{q^3}/\mathbb{F}_{q^3}$ est galoisienne (!).

Finalement, on arrive bien dans $\mathrm{Cl}^0(F'|\mathbb{F}_{q^3})$ car $F'/\mathbb{F}_{q^3}(E)$ est finie (cf. proposition 2.52).

8.4 Le corps de fonctions $F'|\mathbb{F}_q$

Tout d'abord, vérifions que c'est bien un corps de fonctions en une variable. D'après [11, lemme 3.1.10] l'extension $\mathbb{F}_{q^3}(x)/\mathbb{F}_q(x)$ est finie (car $\mathbb{F}_q$ est parfait et $\mathbb{F}_{q^3}/\mathbb{F}_q$ est finie) donc en considérant la tour de corps $\mathbb{F}_q(x) \subseteq \mathbb{F}_{q^3}(x) \subseteq F'$ on obtient que $F'/\mathbb{F}_q(x)$ est finie. Vérifions maintenant sur $F'|\mathbb{F}_q$ les hypothèses que l'on a imposées sur les corps de fonctions :
- $\mathbb{F}_q$ est parfait (car fini) ;
- $F'/\mathbb{F}_q(x)$ est monogène : on a déjà vu qu'elle est finie, et elle est séparable car les deux extensions $F'/\mathbb{F}_{q^3}(x)$ et $\mathbb{F}_{q^3}(x)/\mathbb{F}_q(x)$ le sont [13].

On va maintenant expliciter une base du $\mathbb{F}_q(x)$-espace vectoriel F'. Soit $(1, \alpha, \alpha^2)$ une base du $\mathbb{F}_q$-espace vectoriel $\mathbb{F}_{q^3}$.

Lemme 8.1. *La famille $(1, \alpha, \alpha^2)$ est également une base du $\mathbb{F}_q(x)$-espace vectoriel $\mathbb{F}_{q^3}(x)$.*

Démonstration. D'après [11, lemme 3.1.10] on a déjà $[\mathbb{F}_{q^3}(x) : \mathbb{F}_q(x)] = 3$. Ainsi, il suffit de montrer que la famille $(1, \alpha, \alpha^2)$ est $\mathbb{F}_q(x)$-libre. C'est le cas car d'après la démonstration de [11, lemme 3.1.10] le polynôme minimal de α sur $\mathbb{F}_q(x)$ est de degré 3 (c'est en fait le même que celui sur $\mathbb{F}_q$). □

On a vu que la famille $(1, z, z^2, z^3)$ est une $\mathbb{F}_{q^3}(x)$-base de F' ; par le lemme des bases téléscopiques, la famille $(z^i\alpha^j)_{\substack{0\leqslant i\leqslant 3\\ 0\leqslant j\leqslant 2}}$ est une $\mathbb{F}_q(x)$-base de F'.

Remarque. Contrairement à $F'|\mathbb{F}_{q^3}$, le corps de fonctions $F'|\mathbb{F}_q$ n'est pas régulier : il suffit de considérer un élément de $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$.

8.5 Isomorphisme entre les « deux » F'

On veut faire un « changement de coordonnées » sur les éléments de $F'|\mathbb{F}_{q^3}$. Étant donné que l'on va construire F' en Magma par $F' = \mathbb{F}_{q^3}(x)[y_0, y_1]$, la base par défaut qu'il va considérer est $(1, y_0, y_1, y_0y_1)$. Si l'on trouve la matrice de changement de base entre cette base et la base $(1, z, z^2, z^3)$, alors c'est gagné. En effet, si on écrit $x \in F'$ comme $\sum \lambda_i z^i$ avec $\lambda_i \in \mathbb{F}_{q^3}$, il ne reste plus qu'à décomposer les λ_i dans la base des (α^j) pour obtenir les coordonnées de x dans la $\mathbb{F}_q(x)$-base $(z^i\alpha^j)$ de F'.

8.6 Le corps de fonctions $F|\mathbb{F}_q$

On peut se demander pourquoi on veut écrire un élément $x \in F'$ dans la $\mathbb{F}_q(x)$-base $(z^i\alpha^j)$. En fait, c'est parce que F est exactement le sous-$\mathbb{F}_q(x)$-espace vectoriel de F' engendré par les puissances de z : cela est pratique pour le calcul de la norme (cf. prochaine section). On reprend les notations de [4, 7.2] :

13. Elles sont séparables car galoisiennes : la première par définition de F' et la deuxième par la preuve de la proposition 7.17. Le résultat découle alors de la fin de [11, A.7].

– $[F' : \mathbb{F}_{q^3}(x)] = 2^2$ donc $m = 2$;
– f est unitaire donc $\overline{m} = m$ (cf. après la démonstration de [4, lemme 23]) ;
– $\phi_2(3) = 2$.

Il existe donc un élément $\widehat{\sigma}$ de $\mathrm{Gal}(F'|\mathbb{F}_q(x))$, extension de σ, qui opère suivant $y_0 \mapsto y_1, y_1 \mapsto y_2$ (cf. [4, lemme 21 et après la démonstration du lemme 23]) ; F est alors par définition exactement l'ensemble des vecteurs laissés fixes par cet automorphisme ([4, après le lemme 2]). Vérifions sur $F|\mathbb{F}_q$ les hypothèses que l'on a imposées sur les corps de fonctions :

– $\mathbb{F}_q$ est parfait ;
– $F/\mathbb{F}_q(x)$ est monogène : elle est finie et séparable en tant que sous-extension de l'extension finie et séparable $F'/\mathbb{F}_q(x)$ donc on peut appliquer le théorème de l'élément primitif.

On va maintenant montrer que z est un élément primitif de $F/\mathbb{F}_q(x)$. Remarquons que $\widehat{\sigma}(y_2) = y_1y_2/\sigma^2(g)(x) = y_1(y_0y_1)/[\sigma(g)(x)\,\sigma^2(g)(x)] = y_0$; ainsi, $\widehat{\sigma}(z) = z$ donc $z \in F$. D'après [4, lemme 22], pour montrer que z est un élément primitif de $F/\mathbb{F}_q(x)$ on a juste à vérifier que $z \notin \mathbb{F}_q(x)$. Si $z \in \mathbb{F}_q(x)$ alors z est laissé fixe par l'élément de $\mathrm{Gal}(F'/\mathbb{F}_{q^3}(x))$ déterminé par $y_0 \mapsto -y_0, y_1 \mapsto y_1$. L'élément y_2 est alors envoyé sur $-y_2$ et on obtient donc $y_0 + y_1 + y_2 = -y_0 + y_1 - y_2$ donc $y_0 = -y_2$ (remarquons que l'on est en caractéristique différente de 2) ce qui est absurde. On a donc bien :

$$F = \mathbb{F}_q(x)[z].$$

D'après [4, après le lemme 2], on a $[F' : F] = n = 3$ donc par le lemme des bases télescopiques on a $[F : \mathbb{F}_q(x)] = 4$. Ainsi, $(1, z, z^2, z^3)$ est une $\mathbb{F}_q(x)$-base de F et h est également le polynôme minimal de z sur $\mathbb{F}_q(x)$ (on rappelle que h est le polynôme minimal de z sur $\mathbb{F}_{q^3}(x)$).

Remarque. On a donc h à coefficients dans $\mathbb{F}_q(x)$; on a déjà vu que h est à coefficients dans $\mathbb{F}_{q^3}[x]$ donc h est finalement à coefficients dans $\mathbb{F}_q[x]$.

8.7 Norme

Rappelons que l'on ne sait calculer la norme d'un idéal fractionnaire qu'en la calculant pour les facteurs premiers qui interviennent dans sa décomposition en un produit d'idéaux premiers non nuls ; soit $\mathfrak{p}'$ un idéal premier non nul de $\mathcal{O}^*_{F'|\mathbb{F}_{q^3}}$. Par définition, la norme de $\mathfrak{p}'$ est exactement $\mathfrak{p}^{f_{\mathfrak{p}'|\mathfrak{p}}}$ où $\mathfrak{p} := \mathfrak{p}' \cap F$.

8.7.1 Calcul de l'intersection

On va passer par le corps de fonctions $F'|\mathbb{F}_q$. Remarquons que par la proposition 7.17 on a $\mathcal{O}^*_{F'|\mathbb{F}_{q^3}} = \mathcal{O}^*_{F'|\mathbb{F}_q}$: en effet, la proposition dit que $\mathcal{O}^*_{F'|\mathbb{F}_{q^3}}$ est la fermeture intégrale de $\mathcal{O}^*_{F'|\mathbb{F}_q}$ dans F'. Or, $\mathcal{O}^*_{F'|\mathbb{F}_q}$ est un anneau de Dedekind donc il est par définition intégralement clos dans $\mathrm{Frac}(\mathcal{O}^*_{F'|\mathbb{F}_q}) = F'$ donc on a bien l'égalité annoncée. Remarquons que c'est une « vraie » égalité : ce sont les mêmes sous-anneaux de F'.

Ainsi, $\mathfrak{p}'$ est un idéal premier non nul de $\mathcal{O}^*_{F'|\mathbb{F}_q}$; pour clarifier les choses, on note $\mathfrak{p}'_q$ l'idéal $\mathfrak{p}'$ quand on le considère en tant qu'idéal de $\mathcal{O}^*_{F'|\mathbb{F}_q}$.

Soit M la matrice d'une base de $\mathfrak{p}'_q$ dans la $\mathbb{F}_q(x)$-base $\mathcal{B} := (z^i\alpha^j)_{\substack{0\leqslant i\leqslant 3\\ 0\leqslant j\leqslant 2}} = (1, z, z^2, z^3, \alpha, \alpha z, \dots)$ de F'. Remarquons que c'est une matrice carrée d'après la proposition 7.6 : on doit quand même dire que l'extension $F'/\mathbb{F}_q(x)$ est séparable (déjà vu).

On peut trouver une matrice H qui représente $\mathfrak{p}'_q$ dans cette même base $\mathcal{B}$ qui est triangulaire supérieure avec des coefficients non nuls sur la diagonale. Il suffit par exemple de faire une élimination de Gauss sur M (qui est à coefficients dans F'), les coefficients diagonaux étant non nuls car M est inversible. Notons que Magma considère automatiquement la *forme normale d'Hermite*, qui est en particulier de la forme recherchée.

Il se trouve que cette forme est particulièrement adaptée au calcul de l'intersection car on a vu que F est le sous-$\mathbb{F}_q(x)$-espace vectoriel de F' engendré par $1, z, z^2$ et z^3 : autrement dit, F est le sous-$\mathbb{F}_q(x)$-espace vectoriel de F' engendré par les quatre premiers vecteurs de la base $\mathcal{B}$. Ainsi, il est clair que si $x \in F'$ et si $X = \chi_{\mathcal{B}}(x)$ est le vecteur des coordonnées de x dans la base $\mathcal{B}$, $x \in F$ ssi les seules entrées éventuellement non nulles de X sont les quatre premières. Étant donné que la matrice H est triangulaire supérieure à coefficients diagonaux non nuls, une matrice qui représente l'idéal $\mathfrak{p}$ de $\mathcal{O}_F^*$ dans la $\mathbb{F}_q(x)$-base $(1, z, z^2, z^3)$ de F est la sous-matrice 4×4 supérieure gauche de H.

8.7.2 Calcul du degré d'inertie

On a vu que $\mathcal{O}^*_{F'|\mathbb{F}_{q^3}} = \mathcal{O}^*_{F'|\mathbb{F}_q}$ et que $\mathfrak{p}' = \mathfrak{p}'_q$: on a donc $\mathcal{O}^*_{\mathbb{F}_{q^3}}/\mathfrak{p}' = \mathcal{O}^*_{\mathbb{F}_q}/\mathfrak{p}'_q$. Ainsi, $f_{\mathfrak{p}'|\mathfrak{p}} = [\mathcal{O}^*_{\mathbb{F}_{q^3}}/\mathfrak{p}' : \mathcal{O}^*_{\mathbb{F}_q}/\mathfrak{p}] = [\mathcal{O}^*_{\mathbb{F}_q}/\mathfrak{p}'_q : \mathcal{O}^*_{\mathbb{F}_q}/\mathfrak{p}]$. Or, comme $\mathfrak{p}'|\mathfrak{p}$ on a $\mathfrak{p}' \supseteq \mathfrak{p}$ donc $\mathfrak{p}'_q \supseteq \mathfrak{p}$ (puisque $\mathfrak{p}' = \mathfrak{p}'_q$) donc $\mathfrak{p}'_q|\mathfrak{p}$ par la proposition 6.19. Finalement, on a $f_{\mathfrak{p}'|\mathfrak{p}} = [\mathcal{O}^*_{\mathbb{F}_q}/\mathfrak{p}'_q : \mathcal{O}^*_{\mathbb{F}_q}/\mathfrak{p}] = f_{\mathfrak{p}'_q|\mathfrak{p}}$; on peut maintenant utiliser la propriété 7.10 pour calculer ce degré d'inertie, et c'est très facile car Magma possède justement une fonction qui calcule le degré d'un idéal premier.

8.8 Retour aux diviseurs

Pour pouvoir utiliser le théorème 7.18, on doit vérifier les hypothèses suivantes :
- $F'|\mathbb{F}_{q^3}$ est régulier (déjà vu) ;
- $F|\mathbb{F}_q$ est régulier (car f est unitaire, cf. [4, proposition 14]) ;
- F'/F est finie (déjà vu : $[F' : F] = n = 3$) ;
- $F'/\mathbb{F}_{q^3}(x)$ et $F/\mathbb{F}_q(x)$ sont monogènes (déjà vu ; c'est pour pouvoir définir les ordres maximaux à partir du même élément transcendant x) ;
- $\mathbb{F}_{q^3}/\mathbb{F}_q$ est galoisienne (voir par exemple [11, A.15]).

Finalement, on retombe bien dans $\mathrm{Cl}^0(F)$ car F'/F est galoisienne (cf. propriété 2.57). En effet, $\mathrm{Gal}(F'/F) \simeq \mathrm{Gal}(\mathbb{F}_{q^3}(x)/\mathbb{F}_q(x))$ (par [4, démonstration de proposition 3]) donc $\#\mathrm{Gal}(F'/F) = 3 = [F' : F]$ (on a déjà vu que $\mathrm{Gal}(\mathbb{F}_{q^3}(x)/\mathbb{F}_q(x)) \simeq \mathrm{Gal}(\mathbb{F}_{q^3}/\mathbb{F}_q)$, par exemple lors de la démonstration de la proposition 7.17).

9 Le programme

Étant donné une fonction $g \in \mathbb{F}_{q^3}[X]$ qui n'est pas un carré et qui n'est pas dans $\mathbb{F}_q[X]$, le programme renvoie l'application (instruction `map`) de conorme–norme décrite ci-avant entre les groupes $\mathrm{Div}(\mathbb{F}_{q^3}(E)|\mathbb{F}_{q^3})$ et $\mathrm{Div}(F|\mathbb{F}_q)$; remarquons que ce n'est pas internement un morphisme (instruction `hom`).

L'intégralité du programme est donnée dans l'annexe C ; on détaillera ici seulement les points délicats ou alors on mentionnera les noms de certaines fonctions. Les détails des fonctions déjà implémentées en Magma sont consultables dans le manuel que l'on peut trouver à l'adresse suivante :

`http://magma.maths.usyd.edu.au/magma/handbook/`.

9.1 Importance des structures en Magma

Magma possède une multitude de fonctions pour implémenter des objets qui sont mathématiquement identiques (isomorphes) mais différents en Magma. Par exemple, si $f := X + Y \in \mathbb{Q}[X, Y]$ est implémenté en Magma comme un polynôme en deux indéterminées, il n'est pas si facile en Magma de considérer f comme un élément de $\mathbb{Q}[X][Y]$.

9.2 Définition des objets

9.2.1 Noms des objets en Magma

Pour pouvoir comprendre ce qui va suivre, voici le tableau de correspondance entre les noms que l'on a donné ici et les noms en Magma.

$\mathbb{F}_q$	$\mathbb{F}_{q^3}$	$\mathbb{F}_q(x)$	$\mathbb{F}_{q^3}(x)$	$\mathbb{F}_{q^3}(E)$	$F'\|\mathbb{F}_{q^3}$	$F'\|\mathbb{F}_q$
`k`	`K`	`kx`	`Kx`	`FFp`	`Fp`	`Fp2`

9.2.2 Les corps $\mathbb{F}_q$ et $\mathbb{F}_{q^3}$

Étant donné les hypothèses sur g, il est facile en s'aidant de la fonction `BaseRing` de récupérer l'entier q ; en réalité, on s'arrange plutôt pour récupérer un couple (p, ν) tel que $q = p^\nu$ où p est un nombre premier. Il est alors facile de définir le corps $\mathbb{F}_q$ par `k := GF(p, puiss_p)` (note [14]).

Vient alors la première subtilité : la définition du corps $\mathbb{F}_{q^3}$. Souvenons nous que l'on a besoin d'avoir une $\mathbb{F}_q$-base de $\mathbb{F}_{q^3}$; si l'on écrit `K<alph> := ext<k | 3>`, alors en utilisant l'instruction `Basis` on obtient une base de `K` constituée des puissances de `alph` en tant que $\mathbb{F}_p$-espace vectoriel. Pour éviter cela et avoir le résultat escompté, on utilise `K<alph> := ext<k | IrreduciblePolynomial(k, 3)>`. Plus encore, cette définition de `K` permettra d'utiliser pour σ la fonction `Frobenius` qui sera alors définie de la bonne façon (dans le premier cas, cela aurait été la fonction $x \mapsto x^p$).

9.2.3 Le corps $\mathbb{F}_{q^3}(E)$

On définit tout d'abord $\mathbb{F}_{q^3}(x)$ par `Kx<x> := RationalFunctionField(K)`. Vient ensuite l'instruction `FFp<Y0> := FunctionField(KxX ! [-f, 0, 1]);` où `KxX := PolynomialRing(Kx)` et où `f` est un élément de `Kx` (en fait de `PolynomialRing(K)` mais il y a une coercition automatique). On remarque que cela correspond exactement à $\mathbb{F}_{q^3}(E) := \frac{\mathbb{F}_{q^3}(x)[Y]}{\langle Y^2 - f \rangle}$.

9.2.4 Les corps F'

On construit $F'|\mathbb{F}_{q^3}$ par l'instruction suivante :

```
Fp<y0, y1> := FunctionField([KxX ! [-f, 0, 1], KxX ! [-sigma(f), 0, 1]]);
```

Cela permet de définir facilement une injection de `FFp` dans `Fp` en précisant que l'image de `Y0` doit être `y0`.

Remarque. Si l'on essaie de rajouter `KxX ! [-(sigma^2)(f), 0, 1]` alors on obtient un message d'erreur comme quoi le polynôme n'est pas irréductible (comme on l'a montré).

La construction de $F'|\mathbb{F}_q$, n'est pas plus difficile : on utilise h et le polynôme qui a servi à construire `K`.

9.2.5 Isomorphisme entre les deux F'

C'est l'étape délicate, mais en faite elle est très facile vu les fonctions qu'offre Magma. Tout d'abord, remarquons (on l'a en fait déjà dit) que Magma considère automatiquement pour F' la $\mathbb{F}_{q^3}(x)$-base $(1, y_0, y_1, y_0 y_1)$; il suffit en fait de déterminer la matrice de changement de base entre cette base et la base $(1, z, z^2, z^3)$. Pour cela, on utilise la fonction `ElementToSequence` qui donne les coordonnées d'un vecteur dans la base de l'espace ambiant : étant donné un élément, on peut donc connaître ses coordonnées dans la base $(1, z, z^2, z^3)$.

La famille $(1, z, z^2, z^3, \alpha, \alpha z, \dots)$ est comme on l'a vu une $\mathbb{F}_q(x)$-base de F' ; pour déterminer les coordonnées dans $F'|\mathbb{F}_q$ d'un élément de $F'|\mathbb{F}_{q^3}$, il reste quand même à associer à un élément de

14. `GF` signifie « Galois Field » qui est une autre appellation pour les corps finis.

$\mathbb{F}_{q^3}$ un élément de $\mathbb{F}_q$: on utilise encore une fois la fonction `ElementToSequence`, qui grâce à notre définition de `K` va bien retourner les coordonnées d'un élément de $\mathbb{F}_{q^3}$ dans la $\mathbb{F}_q$-base $(1, \alpha, \alpha^2)$.

Remarque. On construit seulement une injection $F'|\mathbb{F}_{q^3} \hookrightarrow F'|\mathbb{F}_q$.

9.2.6 Construction de F

On pourrait bien sûr construire F comme le sous-corps de $F'|\mathbb{F}_q$ engendré par l'élément z avec `F := sub<Fp2 | z>`, mais le problème est que ce n'est pas la « bonne » base que Magma considère (on veut exactement $(1, z, z^2, z^3)$ comme $\mathbb{F}_q(x)$-base). On procède donc de la sorte :

```
F<zF> := ext<kx | h>;
surj_Fp2_F := hom<Fp2 -> F | zF, 0>;
```

La deuxième ligne se base sur le fait que les générateurs de $F'|\mathbb{F}_q$ sont (z, α) (on le sait d'après l'ordre des équations lors de la définition de `Fp2`) : ainsi, si un élément de F' est (mathématiquement) dans F, après lui avoir appliqué la fonction `surj_Fp2_F` il est considéré par Magma comme un élément de F.

9.2.7 À propos des idéaux fractionnaires

Les ordres maximaux sont déjà implémentés et accessibles par les fonctions `MaximalOrderFinite` et `MaximalOrderInfinite`. On accède aux générateurs d'un idéal fractionnaire avec `Generators` et on accède à une base avec l'instruction `Basis`. On construit un idéal avec `ideal<O | G>` où `O` est l'ordre voulu et `G` une famille de générateurs.

9.3 Le morphisme de conorme–norme

Le plus dur était en fait de construire les différents objets de façon adéquate. L'implémentation du morphisme de conorme–norme est maintenant assez facile.

Étant donné un diviseur, la fonction `Ideals` permet de récupérer les deux idéaux fractionnaires associés. Étant donné un idéal fractionnaire I de $\mathbb{F}_{q^3}(E)$, on calcule la norme des idéaux premier intervenant dans la décomposition en produits d'idéaux premiers non nuls de l'image de I dans $F'|\mathbb{F}_q$ (pour calculer cette image, on a juste à trouver l'image des générateurs) ; on obtient cette factorisation avec `Factorization`. Le degré d'un idéal premier s'obtient avec `Degree` ; finalement, la fonction $\mathfrak{D}$ s'obtient avec `Divisor`.

9.4 Exemple et vérification

Voici un exemple de ce que fait le programme ; on vérifie au passage quelques propriétés que doit avoir le morphisme de conorme–norme (en particulier que c'est un morphisme).

```
load "cnh.m";
p := NextPrime(10^8);
puiss_p := 2;
// q := p^puiss_p;
k := GF(p, puiss_p);
K := GF(p, puiss_p * 3);
kx := PolynomialRing(k);
_<X> := PolynomialRing(K);
g := kx ! 0;
while (Coefficient(g, 1) in k) and (Coefficient(g, 0) in k) do
    g := X^2 + Random(K) * X + Random(K);
end while;
```

```
// La fonction g vérifie maintenant les bonnes hypothèses.

cnh := renvoie_CNH(g);
FFp := FunctionField(Domain(cnh));
F := FunctionField(Codomain(cnh));
```

La fonction `renvoie_CNH` nécessite environ 10 secondes pour être exécutée. On obtient alors les résultats suivants :

```
> Genus(F);
3
> Degree(F);
4
> DefiningPolynomial(F);
T^4 + (100000001*x^4 + (69292378*k.1 + 50008019)*x^3 + (50499796*k.1 +
    50075612)*x^2 + (97588278*k.1 + 61714221)*x + (45725444*k.1 + 85897509))*T^2
    + (99999999*x^6 + (38584749*k.1 + 16031)*x^5 + (29385049*k.1 + 47413279)*x^4
    + (96898357*k.1 + 67565843)*x^3 + (54054255*k.1 + 58240953)*x^2 +
    (2523994*k.1 + 62353109)*x + (7585275*k.1 + 88831699))*T + 100000004*x^8 +
    (69292378*k.1 + 50008019)*x^7 + (78885260*k.1 + 97337674)*x^6 + (2582712*k.1
    + 66206112)*x^5 + (21070345*k.1 + 53455530)*x^4 + (91377098*k.1 +
    32789418)*x^3 + (56765857*k.1 + 70385510)*x^2 + (79401993*k.1 + 52713220)*x
    + 23769949*k.1 + 69628312
```

(`k.1` est un générateur de $k = \mathbb{F}_{p^2}$ en tant que $\mathbb{F}_p$-algèbre.) On retrouve bien le fait que h est à coefficients dans $k[x]$. De plus, $g(F) = 3 = n$ donc pour peu que $F|\mathbb{F}_q$ ne soit pas hyperelliptique le problème du logarithme discret se résout plus rapidement dans $\mathrm{Cl}^0(F|\mathbb{F}_q)$ que dans $E(\mathbb{F}_{q^3})$ d'après les théorèmes 4.2 et 4.3.

On peut également vérifier la compatibilité du passage au quotient.

```
> time IsPrincipal(cnh(Divisor(Random(FFp, 1))));
true
Time: 133.730
> time Degree(cnh(RandomPlace(FFp, 2)
              - RandomPlace(FFp, 1) - RandomPlace(FFp, 1)));
0
Time: 113.130
> P := RandomPlace(FFp, 1);
> Q := RandomPlace(FFp, 1);
> time IsPrincipal(cnh(P + Q + Divisor(Random(FFp, 1))) - (cnh(P) + cnh(Q)));
true
Time: 241.030
```

(`Divisor(Random(FFp, 1))` renvoie un élément de `FFp` (le `1` est un paramètre), `RandomPlace(FFp, 1)` renvoie une place de degré 1 de `FFp` ; les temps renvoyés sont en secondes.)

Remarque. On pourrait tester si le logarithme est conservé, mais c'est beaucoup plus long : par exemple, si l'on regarde ce que cela donne avec nP où n est grand et P est une place, on fera beaucoup de produits d'idéaux et j'imagine que c'est cela qui prend du temps. Même avec une petite valeur de p, le calcul est long dès que n est grand.

Conclusion

Le but de ce stage était avant tout d'écrire un programme qui fonctionne, ce qui est chose faite. Cependant, il nécessite en entrée cette fonction g telle que la courbe elliptique initiale soit de la forme $y^2 = [g\,\sigma(g)](x)$. On pourrait donc chercher plus précisément quand est-ce qu'une telle fonction g existe (voir section B.2).

De plus, le programme n'a été écrit que pour les courbes elliptiques sur $\mathbb{F}_{q^3}$ alors que dans [4] on s'intéresse à des courbes (hyper)elliptiques sur $\mathbb{F}_{q^n}$ avec n impair (voire premier). Si la courbe est elliptique on peut encore utiliser la méthode de l'annexe B ; si la courbe est hyperelliptique alors rien ne dit que l'on peut encore écrire une équation du type $y^2 = g\,\sigma(g)$: l'algorithme de recherche de la fonction g ne fonctionne plus puisqu'il n'y a plus de forme de Legendre (cf. section B).

Références

[1] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*. Springer, 1973.

[2] C. Diem, *An Index Calculus Algorithm for Plane Curves of Small Degree*. Algorithmic Number Theory, ANTS VII, Springer LNTS 4076, 543–557, 2006.

[3] C. Diem, *On arithmetic and the discrete logarithm problem in class groups of curves*. Thèse d'habilitation à Universität Leipzig, 2008.

[4] C. Diem, *The GHS Attack in odd Characteristic*. J. Ramanujan Math. Soc. 18, No.1, 1–32, 2003.

[5] O. Forster, *Lectures on Riemann Surfaces*. Springer, 1981.

[6] S. Galbraith, *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.

[7] R. Hartshorne, *Algebraic Geometry*. Springer, 1977.

[8] F. Momose et J. Chao, *Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristics*. IACR Cryptology ePrint Archive 2009 : 236, 2009.

[9] J. Neukirch, *Algebraic Number Theory*. Springer, 1999.

[10] J.H. Silverman, *The Arithmetic of Elliptic Curves* (second edition). Springer, 2009.

[11] H. Stichtenoth, *Algebraic Function Fields and Codes* (second edition). Springer, 2009.

[12] M. Wagner, *Über Korrespondenzen zwischen algebraischen Funktionenkörpern*. Thèse de doctorat à Technische Universität Berlin, 2009.

A Illustration géométrique de la loi de groupe sur une courbe elliptique

Soit $E/\mathbb{C}$ une courbe elliptique sur $\mathbb{C}$, soit $O \in E(\mathbb{R})$: on va décrire la loi qui fait de $E(\mathbb{R})$ un groupe abélien de neutre O. Soient A, B deux points de $E(\mathbb{R})$. Soit f la droite de $\mathbb{P}^2(\mathbb{C})$ qui joint A et B ; f coupe E en un autre point R (note [15]). Soit g la droite de $\mathbb{P}^2(\mathbb{C})$ qui joint O et R ; g coupe E en un autre point S. On a bien $\frac{f}{g} \in \mathbb{C}(E)$ et on a $[\mathrm{div}(\frac{f}{g})] = [0]$; c'est une égalité dans le groupe des classes $\mathrm{Cl}^0(\mathbb{C}(E))$.

On identifie un point avec sa place associée ; on a $\mathrm{div}(\frac{f}{g}) = A + B + R - O - R - S$ donc on obtient $[A + B - O - S] = [0]$. Ainsi $[A - O] + [B - O] = [S - O]$ *i.e.* $\Phi(A) + \Phi(B) = \Phi(S)$ où Φ est l'application de la proposition.

On a donc $S = \Phi^{-1}(\Phi(A) + \Phi(B))$ ce qui signifie que $S = A \oplus B$. On peut voir une illustration dans la figure 3.

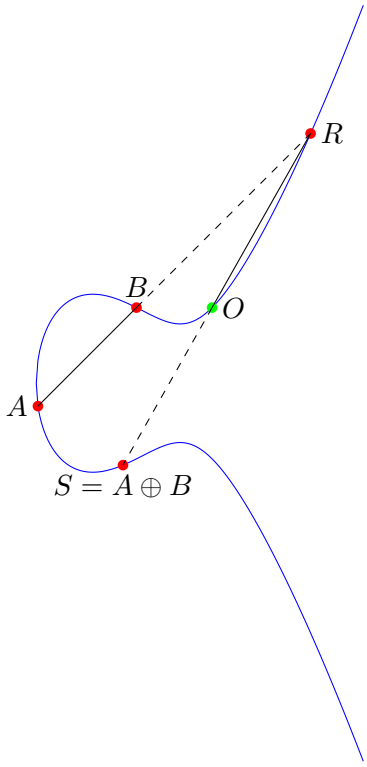

FIGURE 3 – Loi de groupe sur $E : y^2 = x^3 - x + 1$ avec neutre $O(1, 1)$.

B Une autre équation pour les courbes elliptiques

B.1 Le problème

Étant donné une courbe elliptique, on veut l'écrire sous la forme $y^2 = f(x)$ avec $f \in \mathbb{F}_{q^3}[x]$ telle que $f = g\,\sigma(g)$ avec $g \in \mathbb{F}_{q^3}[x] \setminus \mathbb{F}_q[x]$ unitaire qui n'est pas un carré où $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^3}/\mathbb{F}_q)$ est donnée par $\alpha \mapsto \alpha^q$. Tout d'abord, remarquons qu'il n'est pas choquant de voir une courbe elliptique définie par une équation $y^2 = f(x)$ avec f de degré 4 ; étant donné un polynôme de degré 3, il suffit de faire un changement de variable homographique (comme pour trouver la forme de Legendre) qui ramène l'infini dans le plan.

15. Si $A = B$ cela signifie géométriquement que f est tangente à E en A.

Ainsi, posons $g = (x-\alpha)(x-\beta) \in \mathbb{F}_{q^3}[x]$ et supposons que $\#\{\alpha, \beta, \alpha^q, \beta^q\} = 4$ (*i.e.* $f := g\,\sigma(g)$ est sans facteur carré). Pour trouver le λ de la forme de Legendre correspondant à la courbe définie par $y^2 = g\,\sigma(g)$, on peut encore utiliser le birapport ; un λ possible est donc le suivant :

$$\lambda = [\alpha, \beta, \alpha^q, \beta^q] = \frac{\beta^q - \alpha}{\beta^q - \alpha^q} \Big/ \frac{\beta - \alpha}{\beta - \alpha^q} = \frac{(\beta^q - \alpha)(\beta - \alpha^q)}{(\beta^q - \alpha^q)(\beta - \alpha)} \tag{4}$$

Arrêtons-nous maintenant sur les ensembles d'appartenance de α, β. Tout d'abord, il est clair que $\alpha, \beta \in \mathbb{F}_{q^6}$ car ils sont racine d'un polynôme de degré 2 sur $\mathbb{F}_{q^3}$; la terminologie qui suit est issue de [8].

(Type 1) Si $\alpha \in \mathbb{F}_{q^3}$, alors $\beta \in \mathbb{F}_{q^3}$ donc par la condition $\#\{\alpha, \beta, \alpha^q, \beta^q\} = 4$ on obtient en particulier $\alpha, \beta \notin \mathbb{F}_q$.

(Type 2) Si $\alpha \notin \mathbb{F}_{q^3}$, alors β est l'unique conjugué de α par $\mathrm{Gal}(\mathbb{F}_{q^6}/\mathbb{F}_{q^3}) = \langle \gamma \mapsto \gamma^{q^3} \rangle$ donc $\beta = \alpha^{q^3}$. Si $\alpha \in \mathbb{F}_{q^2}$ alors $\beta = \alpha^{q^3} = \alpha^q$ ce qui contredit la condition $\#\{\alpha, \beta, \alpha^q, \beta^q\} = 4$ donc on a $\alpha \notin \mathbb{F}_{q^2}$; de même, $\beta \notin \mathbb{F}_{q^2}$.

Remarque. Dans [8, lemme 9], dans le cas $\alpha \in \mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^3} \cup \mathbb{F}_{q^2}), \beta = \alpha^{q^3}$ le λ est obtenu avec $[\alpha, \beta^q, \beta, \alpha^q]$.

La stratégie est alors la suivante : on dispose d'un polynôme $f \in \mathbb{F}_{q^3}[x]$ de degré 3, on calcule un λ associé. On cherche alors α, β tels que l'égalité (4) soit vérifiée ; on cherche dans un premier temps avec $\alpha, \beta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ puis si on ne trouve pas de solution on cherche avec $\alpha \in \mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^3} \cup \mathbb{F}_{q^2}), \beta = \alpha^{q^3}$. Si l'on trouve un couple (α, β) solution alors on a notre fonction g et donc $y^2 = g\,\sigma(g)$ définit la même courbe elliptique (à isomorphisme près) que la courbe elliptique initiale !

Remarque. Dans tous les exemples de fonctions f non irréductibles sur $\mathbb{F}_{q^3}$ que j'ai considérés j'ai toujours trouvé une solution (α, β) ; en outre, quand f est irréductible sur $\mathbb{F}_{q^3}$ alors on a *a priori* $\lambda \in \mathbb{F}_{q^9}$ (note [16]). L'ensemble exact des courbes pour lesquelles il y a une solution est donné dans [8, théorème 1].

B.2 Résolution

On se place dans le cadre du type 1. Bien sûr, on pourrait résoudre l'équation (4) à la force brutale en essayant toutes les valeurs de α, β possibles : on a besoin au pire de q^6 itérations (on remarquera que c'est la même valeur pour le type 2).

On va en fait procéder autrement, en remarquant que $\mathbb{F}_{q^3}$ est un $\mathbb{F}_q$-espace vectoriel de dimension 3 dans lequel l'application $\sigma : \alpha \mapsto \alpha^q$ est une application linéaire. En réécrivant (4) sous la forme

$$\lambda(\beta^q - \alpha^q)(\beta - \alpha) = (\beta^q - \alpha)(\beta - \alpha^q)$$

il ne reste donc plus qu'à résoudre un système (S) d'équations quadratiques sur $\mathbb{F}_{q^3}^2$ homogène (*i.e.* $\{q_i(x) = 0\}$ où les q_i sont des formes quadratiques). Si l'on considère une $\mathbb{F}_q$-base $(1, \zeta, \zeta^2)$ de $\mathbb{F}_{q^3}$, on remarque que l'on peut supposer que la première coordonnée de α dans cette base est nulle : si $\alpha := \alpha_0 + \alpha_1\zeta + \alpha_2\zeta^2, \beta := \beta_0 + \beta_1\zeta + \beta_2\zeta^2, \alpha_i, \beta_i \in \mathbb{F}_q$ vérifient (4) alors $\widetilde{\alpha} := \alpha_1\zeta + \alpha_2\zeta^2, \widetilde{\beta} := \beta_0 - \alpha_0) + \beta_1\zeta + \beta_2\zeta^2$ vérifient également (4) (car σ est $\mathbb{F}_q$-linéaire) et de plus α (respectivement β) $\in \mathbb{F}_q$ ssi $\widetilde{\alpha}$ (resp. $\widetilde{\beta}$) $\in \mathbb{F}_q$. Il reste donc au pire q^5 itérations.

Reste donc encore la question de savoir comment on va résoudre le système d'équation (S). Pour essayer de faire le moins d'itérations possible, on va calculer une base de Gröbner de (S) pour un ordre *lexicographique* : on obtient ainsi un système (G) équivalent à (S) dans lequel on trouve une équation minimale en nombre d'inconnues, et qui dit moins d'inconnues dit moins d'itérations ! On peut alors résoudre le système avec une méthode de retour sur trace (*backtracking*) ; plus précisément, si $(G) = (f_i = 0)_{1 \leqslant i \leqslant n}$ (rangé par ordre lexicographique décroissant selon les f_i), on résout à partir de $i = n$ puis on décrémente i. Bien sûr, il ne faut pas oublier la condition d'arrêt $\#\{\alpha, \beta, \alpha^q, \beta^q\} = 4$.

16. Le corps de rupture de f est déjà un corps de décomposition car on travaille avec des corps finis.

B.3 Programme

Voici le programme pour déterminer si une courbe elliptique peut être ramenée au type 1. En entrée, on trouve le corps $k := \mathbb{F}_q$ et un $\lambda \in \mathbb{F}_{q^6}$ tel que λ soit « atteignable » par une équation de Legendre d'une courbe elliptique sur $\mathbb{F}_{q^3}$, *i.e.* il existe une courbe elliptique sur $\mathbb{F}_{q^3}$ dont une équation de Legendre est $y^2 = x(x-1)(x-\lambda)$.

Remarque. Tous les $\lambda \in \mathbb{F}_{q^6}$ ne sont *a priori* pas atteignables par une équation de Legendre d'une courbe elliptique sur $\mathbb{F}_{q^3}$. En outre, l'ensemble des λ que fourni l'ensemble des courbes elliptiques $y^2 = f(x)$ avec $f \in \mathbb{F}_{q^3}[x]$ non irréductible de degré 3 est de cardinal $\sim 4q^3$ (note [17]).

On suppose que l'on dispose d'une fonction `resout` telle que `resout(k, G, mon_ev, test)` retourne une solution (si elle existe) du système d'équation `G` à coefficients dans le corps `k` qui vérifie le prédicat `test` et qui étend le vecteur `mon_ev` (note [18]). Dans notre cas, le prédicat `test` est la fonction `retourne_sol`, non présentée ici mais qui essentiellement vérifie $\#\{\alpha, \beta, \alpha^q, \beta^q\} = 4$ (il faut en plus considérer les cas où il reste des indéterminées).

Le programme est assez tordu car il y a de nombreuses coercitions (les `!`) ; peut-être y a t-il un moyen plus simple d'y arriver.

```
trouve_T1 := function(k, lambda)
n := 3;
q := #k;
P := IrreduciblePolynomial(k, n);

ktemp := PolynomialRing(k, 2 * n + 1);
/* 2n pour les coordonnées,
   le dernier pour la variable pour la base de l'ev. */

Coord<xi, a0, a1, a2, b0, b1, b2> := quo< ktemp |
        MultivariatePolynomial(ktemp, P, 1)>;
// C'est GF(q^n)[a0,..., b2].

calc<XI> := quo<PolynomialRing(k) | P>;
// Pour faire des calculs (inverse, évaluation...).

calcc := ext<k | P>;
// Bien sûr calc et calcc sont identiques du point de vue mathématique.

Embed(sub<Parent(lambda) | lambda>, calcc);
// Pour pouvoir considérer lambda comme un élément de calcc
k_res := GF(q^n); // préférer GF(p, n * puiss_p);
Embed(calcc, k_res);
/* On a bien sûr un isomorphisme ;
  c'est juste pour avoir une belle impression. */
ll := calc ! ElementToSequence(calcc ! lambda);

complete := function (s)
        while #s ne n do
```

17. C'est un calcul bête de cardinalité ; on se ramène au cas où $\lambda = \frac{\zeta+\alpha}{\zeta-\alpha}$ avec $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}[\zeta]$ et $\alpha \in \mathbb{F}_{q^3}$, sans oublier les 5 autres valeurs associées à un même λ qui donnent la même courbe.

18. Le vecteur `mon_ev` est constitué d'éléments de `k` et d'indéterminées ; si on appelle la fonction avec (par exemple) `mon_ev := [1, X]`, la fonction retournera une solution de la forme `[1, x]` avec $x \in k$.

```
        // Dangereux mais normalement ok.
                Append(~s, 0);
        end while;
        return s;
end function;

Lk := Matrix(k, n, n,
        [complete(Coefficients((xi^i)^q, 1))
                : i in [0..n - 1]]);
// Transposée de la matrice de alpha :-> alpha^q.

L := Matrix(Coord, Lk);
aa := Matrix(Coord, 1, n, [a0, a1, a2]);
bb := Matrix(Coord, 1, n, [b0, b1, b2]);

convert := function (vect)
        return &+ [vect[1, i] * xi^(i - 1) : i in [1..n]];
end function;

fois := function(v1, v2)
        return convert(v1) * convert(v2);
end function;

/**** RÉSOLUTION DU SYSTÈME D'ÉQUATIONS QUADRATIQUES ****/
d := 2 * n - 1;
_<A1, A2, B0, B1, B2> := PolynomialRing(k, d);

construit := function(ld)
        pol := ld * fois(bb - aa, (bb - aa) * L)
                - fois(bb * L - aa, bb - aa * L);
        return [Evaluate(i, [0, 0, A1, A2, B0, B1, B2])
                : i in Coefficients(pol, 1)];
end function;
// Construit le système d'équations.

Ld := [ll, 1 / ll, 1 - ll, 1 / (1 - ll), ll / (ll - 1), (ll - 1) / ll];
for ld_courant in Ld do
        ld := Evaluate(ld_courant, xi);
        bool, sol := resout(k, GroebnerBasis(construit(ld)),
                [A1, A2, B0, B1, B2], retourne_sol);
        if bool then
                sol := [k ! i : i in Insert(sol, 1, 0)];
                return true, k_res ! calcc ! sol[1..3], k_res ! calcc ! sol[4..6];
        end if;
end for;
return false, _;
// La valeur de lambda ne peut pas être associée à une courbe de type 1.

end function;
```

C Le programme de conorme–norme

```
/**** Fonction préliminaire : appliquer une fonction à une liste. ****/
mapl := function(f, l)
        return [f(i) : i in l];
end function;

/* Morphisme CN */
function renvoie_CNH(g)

/**** 1. Récupération des informations de g ****/
Rg := BaseRing(g);
p := Characteristic(Rg);
puiss_p := ExactQuotient(Ilog(p, #Rg), 3);
q := p^puiss_p;

/**** 2. Construction des structures de base ****/
k := GF(p, puiss_p);
Pol_def := IrreduciblePolynomial(k, 3);
K<alph> := ext<k | Pol_def>;

/* D'après la documentation sur les corps finis sur la fonction F.1, alph
   est l'image de l'indéterminée de Pol_def et alph = K.1 = Generator(K)
   = Generator(K, k) (car k est le corps de base de K car on a défini K
   avec un polynôme). Ainsi, Pol_def est le polynôme minimal de alph sur k. */

Kx<x> := RationalFunctionField(K);
KxP<xP> := PolynomialRing(K);

sigma := hom<KxP -> KxP | map<K -> K | x :-> Frobenius(x)>, xP>;
// Frobenius a beaucoup de signatures, c'est pourquoi ça ne marche pas directement.

Embed(Rg, K);
// Permet la coercition automatique.
f := g * sigma(g);

KxX := PolynomialRing(Kx);
FFp<Y0> := FunctionField(KxX ! [-f, 0, 1]);
// Corps des fonctions de la courbe y^2 = f(x)

/**** 3. Construction des deux F', respectivement Fp et Fp2 ****/
Fp<y0, y1> := FunctionField([KxX ! [-f, 0, 1], KxX ! [-sigma(f), 0, 1]]);

inj_FFp_Fp := hom<FFp -> Fp | y0>;
/* Injection de FFp dans Fp ; on aurait pu définir directement FFp comme
   sub<Fp | y0> mais alors le générateur de FFp retourné par Magma
   n'est pas y0 (pas le même polynôme minimal). */

y2 := y0 * y1 / sigma(g);
y := [y0, y1, y2];
```

```
z := &+ y;
/* On se rend compte que z est primitif par exemple avec
   Fp eq sub<Fp | z>. */

_<T> := PolynomialRing(Fp);
h := &* [
        T - (&+ [(-1)^(Integers() ! j[i]) * y[i] : i in [1..3]])
        : j in {jj : jj in CartesianPower(GF(2), 3) | jj[1] + jj[2] eq jj[3]}];
// C'est le polynôme minimal de z sur k(x).

kx<x> := RationalFunctionField(k);
kxX := PolynomialRing(kx);

Fp2<zFp2, aFp2> := FunctionField([kxX ! Coefficients(h),
                                  kxX ! Coefficients(Pol_def)]);
// Plus prudent que ! P car P est à coeffs dans k.

/**** 4. Construction de l'injection de Fp dans Fp2. ****/
// On injecte d'abord K dans Fp2.
plonge_K := map<K -> Fp2 | a :-> &+ [seq[i + 1] * aFp2^i : i in [0..2]]
        where seq := ElementToSequence(a)>;
/* D'après la documentation sur les corps finis sur la fonction ElementToSequence,
   la décomposition est bien celle sur la base (1, alph, alph^2). */

// On injecte maintenant K(x) dans Fp2.
plonge := hom<Kx -> Fp2 | plonge_K, x>;

// Et finalement Fp.
P := Matrix(Kx, [ElementToSequence(z^i) : i in [0..3]]);
/* P est la transposée de la matrice dans la base B := [1, y0, y1, y0*y1]
   des vecteurs de la base des z^i. */
P := P^(-1);
// P est la transposée de la matrice dans la base des z^i des vecteurs de B

isom_Fp_Fp2 := map<Fp -> Fp2 | x :-> &+ [plonge(nvell_coord[1, i + 1]) * zFp2^i :
        i in [0..3]]
        where nvell_coord := Matrix(Kx, [ElementToSequence(Fp ! x)]) * P>;

/**** 5. Construction de F et de la restriction de Fp2 dans F. ****/
F<zF> := ext<kx | h>;

surj_Fp2_F := hom<Fp2 -> F | zF, 0>;
// Même corps de base kx ; les générateurs de Fp2 sont [zFp2, aFp2].

/**** 6. Construction de l'homomorphisme conorme-norme. ****/
// Intersection avec F (fondement de la norme).
MOF_Fp2 := MaximalOrderFinite(Fp2);
MOInf_Fp2 := MaximalOrderInfinite(Fp2);
MOF_F := MaximalOrderFinite(F);
```

```
MOInf_F := MaximalOrderInfinite(F);

meet_f := map<
              Parent(ideal<MOF_Fp2 | 1 >) -> Parent(ideal<MOF_F | 1>) |
              I :-> ideal<MOF_F | mapl(surj_Fp2_F, Basis(I)[1..4])>
             >;

meet_inf := map<
                Parent(ideal<MOInf_Fp2 | 1 >) -> Parent(ideal<MOInf_F | 1>) |
                J :-> ideal<MOInf_F | mapl(surj_Fp2_F, Basis(J)[1..4])>
               >;

// Morphisme conorme-isomorphisme-factorisation-norme pour les idéaux.
cifnh_f := function(I)
// Idéal de FFp pour l'ordre fini maximal.
    if IsOne(I) then
        return ideal<MOF_F | 1>;
    end if;
    gen := Generators(I);
    ciI := ideal<MOF_Fp2 | mapl(inj_FFp_Fp * isom_Fp_Fp2, gen)>;
    // Conorme + isomorphisme appliqué à I ; attention, gof se code f * g.
/**** Le mapl se fait très rapidement, mais
      la création de l'idéal est très lente. ****/

    FI := Factorization(ciI);
    // Ça aussi ça prend du temps !
    return &* [prem^(FI[i, 2] *
               ExactQuotient(Degree(FI[i, 1]), Degree(prem)))
               where prem := meet_f(FI[i, 1])
               : i in [1..#FI]];
end function;

cifnh_inf := function(J)
// Idéal J de FFp pour l'ordre infini maximal.
    if IsOne(J) then
        return ideal<MOInf_F | 1>;
    end if;
    gen := Generators(J);
    ciJ := ideal<MOInf_Fp2 | mapl(inj_FFp_Fp * isom_Fp_Fp2, gen)>;

    FJ := Factorization(ciJ);
    return &* [prem^(FJ[j, 2] *
               ExactQuotient(Degree(FJ[j, 1]), Degree(prem)))
               where prem := meet_inf(FJ[j, 1])
               : j in [1..#FJ]];
end function;

// Pareil, mais pour les diviseurs.
CNH := map<DivisorGroup(FFp) -> DivisorGroup(F) |
```

```
            D :-> Divisor(cifnh_f(I), cifnh_inf(J))
            where I, J := Ideals(D)>;

/**** On termine la rédaction de la fonction retourne_CNH. ****/
return CNH;
end function;
```