Université de Limoges

Jacobiennes et cryptographie

THÈSE

présentée et soutenue le 16 mai 2003

pour l'obtention du

Doctorat de l'Université de Limoges

(Spécialité Mathématique)

par

Jean-Yves Enjalbert

sous la direction du professeur

Iwan Duursma

Composition du jury

Président :	Francois Laubie
Rapporteurs :	Jean-Pierre Cherdieu Jean-Marc Couveignes
Examinateurs :	Thierry Berger Abdelkader Necer

Laboratoire d'Arithmétique de Calcul formel et d'Optimisation — UMR 6090

Mis en page avec la classe thloria.

Remerciements

Ma motivation initiale pour entreprendre cette “aventure” était de découvrir les jacobiennes généralisées et d’essayer de les exploiter à des fins cryptographiques. Le professeur Iwan Duursma a accepté de me diriger pour cette thèse, son aide fut considérable ; il a toujours su recadrer et relancer nos recherches. Cependant une thèse ne se fait pas de manière isolée, elle n’aurait pu voir le jour sans l’apport de nombreuses autres personnes.

Je remercie avant tout les professeurs ayant accepté de faire partie de mon jury de thèse : Thierry Berger, qui m’a accueilli dans l’école doctorale de Limoges ; Jean-Pierre Cherdieu et Jean-Marc Couveignes pour leur minutieux travail en tant que rapporteurs ; François Laubie et Abdelkader Necer représentant l’université de Limoges.

Les professeurs de cette université m’ont particulièrement aidé tout au cours de ma thèse. François Laubie et Alain Salinier m’ont donné des éclairages sur les notions de cohomologie. Philippe Gaborit m’a conseillé sur mes exposés effectués dans le cadre du séminaire crypto. François Arnault, spécialiste du logarithme discret, m’a aider à affiner le premier chapitre. Enfin, Abdelkader Necer a été spécialement à mon écoute et de précieux conseils pour la mise en forme du manuscrit.

Ce travail est aussi le fruit de rencontres et séjours hors laboratoire d’origine. Je me dois de remercier Pascale Charpin, qui m’a permis l’accès aux moyens informatiques de l’INRIA durant un an. Mes deux séjours à l’université d’Urbana-Champaign dans l’Illinois ont été déterminants à l’avancement de ma thèse. Le directeur Nigel Boston m’a permis ainsi de suivre les intéressants séminaires de protection de l’information et d’arithmétique. J’y ai rencontré les professeurs Randy McCarthey, qui m’a fourni des exemples illustrant le calcul des entiers de certaines extensions quadratiques, et Andreas Stein avec lequel nous avons formé un groupe de travail auxquels participaient deux étudiants Eric Landquist et Jonathan Webster sur le logarithme discret quadratique. C’est suite à ces rencontres qu’ils

ont développé le programme résolvant les exemples cités en troisième chapitre. Certaines rencontrent lors de colloques, de durée donc plus courte, ont pourtant été très riches. Mikhail Tsfasman et surtout Peter Stevenhagen m'ont initié à la théorie des corps de rayon. Thierry Hennocq a toujours manifesté à mon travail un intérêt remotivant.

Tous ces voyages ont été facilités par le travail de Yolande Vieceli. Mentionnons aussi, pour leurs travails de secrétaires, Nadine Tchefranoff et Martine Guerletin. Elles trois m'ont permis au cours de ces années de me concentrer sur ma tâche sans soucis.

Il ne faut pas cependant négliger les échanges entre thésards. Ceux avec lesquels j'ai partagé mon espace de travail ont donc joué un rôle particulier dans l'élaboration de la thèse : citons Carmen Nedeloaia, et, pour leur efficacité en informatique, Ayoub Otmani et Philippe Segalat.

Pour finir, je remercie mes parents pour leur soutien tout au long de ces années.

Table des matières

Introduction

La cryptographie est l'activité qui consiste à transformer un message de manière à ce que son contenu ne soit compris que par des personnes déterminées. L'utilisation initiale de cet art, déjà en cours durant l'antiquité, consistait en des communications secrètes (à usages militaires ou diplomatiques). L'émetteur et le récepteur se devaient d'être les seuls à connaître le procédé pour écrire un message (pour "coder" au sens de ces anciens, pour chiffrer en langage actuel). Ils convenaient à l'avance du chiffrement utilisé (on dirait maintenant de la clé) comme par exemple affecter à chaque lettre de l'alphabet utilisé un sigle particulier (pour donner une idée simpliste, A était chiffré en 1, B en 2, C en 3, ..) et effectuer des permutations sur les messages obtenus. De tels systèmes (maintenant plus sophistiqués) sont appelés *à clé secrète.*

En 1976, W. Diffie et M. Hellman [DH76] proposent de nouveaux procédés de cryptage : les systèmes cryptographiques *à clés publiques.* L'algorithme de chiffrement –qui s'effectue à l'aide d'une "clé publique"– est maintenant divulgué librement et permet à tout le monde d'écrire des messages lisibles par un lecteur averti (i.e. connaissant la clé privée) uniquement. Seul ce dernier connaît en effet la clé de déchiffrage, qui doit être introuvable à partir de la clé de chiffrement.

Cette cryptographie (dite asymétrique) s'impose de plus en plus pour les besoins engendrés par les technologies informatiques tels le courrier électronique, la signature électronique de contrat, la carte à puce ... Leurs nombreux utilisateurs demandent aujourd'hui non seulement d'assurer la confidentialité, mais aussi l'intégrité, l'authenticité et la signature des communications. On peut construire de tels procédés (ou *cryptosystèmes*) à partir d'un problème mathématique facile à implanter mais difficile à résoudre. C'est le cas du *problème du logarithme discret* (PLD), qui a donné naissance à divers cryptosystèmes : citons par exemple les systèmes El Gamal [EG85] ou de Cramer-Shoup [CS98]. Ce problème s'énonce de la façon suivante :

PLD : Soient G un groupe fini noté multiplicativement, g un élément de G et h un élément du sous-groupe engendré par g. Trouver un entier x tel que $h = g^x$.

Le plus petit entier positif solution sera appelé le logarithme discret de h (en base g).

Un exemple usuel et couramment utilisé de ce problème est le cas où l'on prend pour groupe G le groupe multiplicatif $\mathbf{F}_p^\times$ des éléments inversibles du corps fini $\mathbf{F}_p$, l'entier naturel p étant un nombre premier. Par exemple, pour $p = 113$, travaillons avec l'élément $h = 53$ de $\mathbf{F}_{113}$ situé dans le sous-groupe engendré par $g = 2$. Le problème du logarithme discret équivaut ici à trouver un entier x tel que $53 \equiv 2^x \pmod{113}$. L'entier $x = 23$ est solution.

S'il est évident que le logarithme discret de h en base g existe – car h a été choisi dans $\langle g \rangle$ –, sa détermination lorsque g a un grand ordre est à priori difficile. Nous présentons dans le premier chapitre, après avoir donné des précisions sur le problème du logarithme discret, les différents algorithmes développés pour le résoudre. Il existe des algorithmes donnant une solution en $O(\sqrt{n})$, en notant n le cardinal du groupe G ([Pol78], [Sha71a]). Shoup [Sho01] a montré que l'on ne peut construire une attaque générique de complexité plus basse ; par attaque générique on entend une attaque sans utiliser des propriétés particulières du groupe G (comme la propriété de factorisation si $G = \mathbf{Z}$ ou $G = \mathbf{F}_q^\times$ [Adl83], le couplage de Tate [FR94] ou les classes d'automorphismes [DGM99] pour le groupe des diviseurs d'une courbe ...). On peut toutefois baisser le coefficient multiplicateur de n à l'aide d'une programmation en parallèle [vOW99] par un algorithme de recherche de cycles. L'échec de nos tentatives pour améliorer ce coefficient par d'autres méthodes en parallèle laisse penser qu'une bonne façon d'aborder ce problème est d'utiliser ce type d'algorithme de recherche avec fonction itérative.

Une activité majeure de la cryptographie moderne consiste à trouver un groupe G dans lequel on pourrait montrer que le meilleur algorithme possible pour résoudre le problème du logarithme discret a une complexité en $O(\sqrt{n})$ ([Fre]).

Parmi les groupes utilisés pour le logarithme discret, il a été proposé de travailler avec le groupe de points d'une courbe elliptique (voir [Mil86] ou [Kob87]), qui est la jacobienne de la courbe en question. L'idée initiale de cette thèse est de regarder plus généralement ce que donne un logarithme discret sur les jacobiennes généralisées d'une courbe C projective, irréductible et non singulière, définie sur un corps $\mathbf{K}$. On débute le deuxième chapitre par des rappels sur des objets mathématiques définis à partir d'une courbe C : ses diviseurs, sa jacobienne J, ses modules $\mathfrak{m}$ et leurs jacobiennes généralisées associées $J_{\mathfrak{m}}$, tous construits en tra-

vaillant sur une clôture algébrique $\overline{\mathbf{K}}$ de $\mathbf{K}$. On construit ensuite la suite exacte

$$0 \longrightarrow L_{\mathfrak{m}} \longrightarrow J_{\mathfrak{m}} \xrightarrow{\psi_{\mathfrak{m}}} J \longrightarrow 0,$$

et on calcule le noyau $L_{\mathfrak{m}}$ (tous ces rappels s'inspirent de [Ser59]). Pour le logarithme discret, il est plus approprié de travailler avec des objets "définis" sur $\mathbf{K}$: nous définissons les jacobiennes $J_{\mathbf{K}}$ "définies" sur $\mathbf{K}$, et notons $J_{\mathfrak{m}}^{\mathbf{K}}$ les jacobiennes généralisées "définies" sur $\mathbf{K}$ lorsque le module $\mathfrak{m}$ est rationnel. Nous montrons ensuite que cette suite reste exacte si l'on considère ces objets sur $\mathbf{K}$. On connaît ainsi, si $\mathbf{K}$ est fini, la taille de $J_{\mathfrak{m}}^{\mathbf{K}}$ en fonction de celle de $J_{\mathbf{K}}$.

Mais notre intérêt à comparer J et $J_{\mathfrak{m}}$ était de représenter les classes en fonction des éléments de la jacobienne pour pouvoir calculer dans les jacobiennes généralisées. Malheureusement, on n'a pas de relèvement de $\psi_{\mathfrak{m}}$, ce qui ruine nos espoirs de représentation. De plus, on peut par la suite exacte reporter le problème du logarithme discret de la jacobienne généralisée sur J et $L_{\mathfrak{m}}$. La complexité du logarithme discret dans $J_{\mathfrak{m}}$ découle ainsi de celles dans J et $L_{\mathfrak{m}}$ [Cou01]. Les jacobiennes généralisées en tant que groupe ne sont donc pas de meilleurs candidats pour le logarithme discret. On pourrait toutefois profiter du module pour masquer des informations et donc construire des cryptosystèmes, il faut cependant trouver une représentation "calculable" des classes.

On finit ce chapitre en limitant l'étude aux *courbes hyperelliptiques* (i.e. d'équation affine $y^2 = f(x)$, f étant un polynôme). On peut alors mettre en lien les jacobiennes généralisées et les groupes de classes des *ordres* du corps de fonctions. Ces groupes de classes sont connus lorsque $\mathbf{K} = \mathbf{Q}$, on peut dans ce cas y trouver des représentants et calculer la multiplication des classes. On va regarder si l'on peut généraliser l'algorithme de multiplication pour d'autres types de corps $\mathbf{K}$. Cela nous permettrait de transposer nos projets cryptographiques sur les jacobiennes généralisées aux groupes de classes d'un ordre.

Nous examinons donc dans le troisième chapitre ces groupes de classes, pour les courbes hyperelliptiques seulement. L'introduction de ce type de courbes en cryptographie est dû à Koblitz [Kob89]. S'intéresser aux groupes de diviseurs de ces courbes pour la cryptographie n'est pas saugrenu : rappelons que, du fait de la complexité de la loi de groupe, casser le logarithme discret sur une courbe elliptique a nécessité l'équivalent de 500 ans de travail pour un PC à 450MHz (pour ECC2K-108 (ECC2-97) proposé par Certicom [ECC]), soit 25 fois plus que RSA-155. Travailler avec ces courbes revient à regarder les ordres et leurs groupes de classes dans une extension de degré 2 de $\mathbf{K}$.

Nous avons signalé une situation d'extension de degré 2 où l'on connaît les ordres de façon explicite : les extensions quadratiques de $\mathbf{Q}$ (voir par exemple [Cox89], [Coh95] ou encore [Bue89]). Des cryptosystèmes y ont même déjà été proposés ([BW88] ou [HJPT01] ; on masque dans ce dernier le conducteur de l'ordre pour accroître la sécurité du cryptosystème El Gamal. Cela correspond au projet précédemment cité de construire un cryptosystème en masquant le module de la jacobienne généralisée.

Nous généralisons ici ces études avec un anneau factoriel A de caractéristique différente de 2 en se plaçant dans une extension M de degré 2 de son corps de fractions L. Nous calculons tout d'abord dans ce chapitre l'anneau des entiers A_M dans un grand nombres de situations où A est factoriel 3.2.3. Cela nous permet de généraliser, sous quelques hypothèses très largement vérifiées (notamment par les situations de 3.2.3), la théorie développée sur les extensions quadratiques de $\mathbf{Q}$: nous donnons une expression explicite des ordres, définissons le groupe des classes et trouvons un représentant explicite "remarquable" pour chaque classe. Nous construisons un algorithme donnant, à partir de deux représentants remarquables correspondant à deux classes, le représentant remarquable de la classe produit. Nous donnons ensuite un procédé explicite pour associer à chaque élément de la jacobienne un représentant remarquable (donc une classe), et nous vérifions que cela définit en fait un isomorphisme de groupe.

On a donc fixé un "bon cadre" pour généraliser les divers cryptosystèmes, attaques et signatures quadratiques. Regardons par exemple le problème du logarithme discret sur le groupe de classes d'une extension quadratique imaginaire de $\mathbf{Q}$. Gaudry [Gau00] propose une attaque par recherche de collision par une marche itérative puis par un traitement d'algèbre linéaire adapté. On peut adapter cette attaque à un groupe de classes d'un ordre : il suffit de changer le discriminant, tout fonctionne alors de manière complètement identique (même opérations utilisées pour le cryptosystème, même opérations pour l'attaque).

Afin de tester l'attaque de Gaudry, nous avons besoin de groupe de classe de 'grosse' taille avec des éléments connus de 'grand' ordre (que l'on utilisera comme générateur g). Cette condition ne pose pas problème lorsque le cardinal du groupe se décompose qu'en produit de grand nombres premiers. Il est délicat de trouver des extensions quadratiques où le cardinal h du groupe de classe de l'anneau des entiers se décompose de cette manière. Par contre on peut construire facilement de 'gros' groupes de classes de ce type. Nous avons proposé à Eric Landquist et Jonathan Webster, qui avaient programmé une attaque du logarithme discret sur le groupe des classes de l'anneau des entiers inspirée de [Gau00], plusieurs exemples à casser. Le programme de l'époque a réussi à résoudre le pro-

blème pour le discriminant $d = -1000860187773469590847 9$ mais a échoué pour un discriminant $d_f = -10000000000000000000000000001443 * 2000423^2$ (taille $h_f = 2 * 1000211 * 103902575992349$ qui a peu de facteurs premiers, et tous de puissance 1). Le plus grand exemple lors de ce premier test par ce programme est $d_f = -400169257549669493186 39 = -10000000991 * 2000423^2$, la taille du groupe étant $175571037674 = 2*87767*1000211$. On mentionne en section 3.6.2 les améliorations faites depuis grâce aux tests des groupes de classes d'ordres.

Notre intérêt pour les jacobiennes généralisées nous a amenés naturellement à regarder les "angles de Frobenius". Dans le chapitre quatre de cette thèse, nous établissons de nouveaux résultats à ce sujets. Soit X une courbe *algébrique* (i.e. projective, non singulière et absolument irréductible) définie sur un corps fini $\mathbf{F}_q$ et de genre g. Le nombre de points rationnels de X sur le corps $\mathbf{F}_{q^m}$ vérifie

$$N_m = q^m + 1 - \sum_{j=1}^{2g} \omega_j^m, \tag{1}$$

où les ω_j sont les valeur propres de l'endomorphisme de Frobenius de X [Wei49]. Par le théorème de Weil [Wei49], ces valeurs sont de la forme $\omega_j = \sqrt{q}e^{i\theta_j}$. Les réels $\{\theta_j\}_{1\leq j\leq 2g}$ sont appelés *angles de Frobenius* de X. Ils sont définis modulo 2π, et les valeurs propres sont conjuguées deux à deux ; il suffit de connaître les g premiers que l'on peut supposer dans $[0\,,\,\pi]$. Nous verrons comment utiliser l'égalité (1) pour affiner sur certains corps l'égalité de Hasse-Weil. Grâce aux travaux de Tsfasman et Vlăduţ [TV97] d'une part, de Serre [Ser97] d'autre part, nous démontrons que toute famille de courbes algébriques dont les angles de Frobenius ne sont pas denses est finie. Ces remarques nous ont conduit à poser les problèmes suivants [DE02].

Problème 1 Étant donné un ensemble discret Γ de $[0, \pi]$, trouver les valeurs maximales possibles de N et g pour une courbe dont les angles de Frobenius sont dans Γ.

Les courbes elliptiques définies sur $\mathbf{F}_2$ ont leurs angles de Frobenius θ vérifiant $2\sqrt{2}\cos(\theta) \in \{-2, -1, 0, 1, 2\}$. La résolution de ce problème pour ce cas nous permet de montrer que toute courbe sur $\mathbf{F}_2$ à jacobienne complètement décomposable vérifie $N \leq 6$ (sous-section 4.2.5) et $g \leq 26$ (sous-section 4.2.6), ce qui améliore l'estimation de Serre $g \leq 145$ dans [Ser97]).

De la même façon, toute famille de courbes qui n'a pas d'angle de Frobenius dans un intervalle donné est finie. Il existe donc un nombre de points maximum et un genre maximum pour de telles familles.

Problème 2 Étant donné un intervalle $I \subset [0, \pi]$, trouver les valeurs maximales de N et g pour toute courbe sur $\mathbf{F}_q$ dont les angles de Frobenius sont hors de I.

Nous consacrons toute la suite de ce chapitre à répondre à ce problème. Nous y établirons pour une multitude d'intervalles les conditions demandées. Elles sont "raisonnables" dans la mesure où il existe des courbes vérifiant chacune de ces conditions. Il nous a semblé intéressant de chercher des conditions sur des intervalles formant une "partition" (aux frontières près) de $[0,\ \pi]$: nous donnons par exemple les conditions optimum pour les intervalles $]0, \frac{\pi}{3}[$ (sous-section 4.2.9 avec $n = 3$), $]\frac{\pi}{3}, \frac{3\pi}{4}[$ (sous-section 4.2.8) et $]\frac{3\pi}{4}, \pi[$ (sous-section 4.2.4). Certains de ces résultats nous ont amenés à la généralisation suivante :

Tout courbe sur $\mathbf{F}_q$, dont le nombre de points rationnels vérifie $N > q^{n/2} + 1$, a un angle de Frobenius dans l'intervalle $]\frac{\pi}{n}, \frac{3\pi}{n}[$, ce pour tout entier n.

Nous finissons ce chapitre par la démonstration de ce cas asymptotique dans 4.2.9, et en mentionnant d'autres problèmes encore ouverts [DE02].

Nous avons ajouter des annexes en fin de cette thèse.

Nous rappelons dans l'annexe A le théorème des valeurs absolues et sa démonstration [Cas]. Celle-ci donne une construction explicite d'un élément vérifiant certaines congruence. Nous nous servons, au cours du deuxième chapitre, de l'existence d'un tel procédé de construction pour justifier la possible programmation de l'isomorphisme déterminant le noyau L .

Dans l'annexe B, nous démontrons que toutes familles infinies de courbes dont le genre tend vers l'infini admet une sous-suite asymptotiquement exacte. Ce résultat permet de justifier la recherche de conditions sur le genre et le nombre de points rationnels pour localiser les angles de Frobenius.

Chapitre 1

Problème du logarithme discret et ses attaques

Un des buts de cette thèse était d'utiliser les jacobiennes généralisées à des fin cryptographiques, en utilisant le problème du logarithme discret. Le problème du logarithme discret permet de construire divers cryptosystèmes (le système El Gamal [EG85] ou de Cramer-Shoup [CS98]), qui, construits avec le groupe des points des jacobiennes, sont actuellement très performants. Nous rappelons donc tout d'abord dans ce chapitre ce problème et ses diverses variantes. On arrive cependant à résoudre ce problème moyennant un temps de calcul plus ou moins long selon les procédés utilisés, de tels procédés sont appelés attaques du logarithme discret. Pour connaître les limites d'un cryptosystème basé sur le logarithme discret, il est nécessaire d'avoir à l'esprit ces attaques. Nous faisons donc dans ce chapitre un état de l'art à ce sujet. Notons que l'échec de nos tentatives d'améliorations des attaques en parallèle montre l'intérêt de l'approche avec fonction itérative pour ce type d'attaque.

1.1 Rappel du problème du logarithme discret

Soient G un groupe cyclique (de loi notée sous forme multiplicative), et g un générateur de G. Pour tout élément h de G, il existe alors un entier naturel x tel que $h = g^x$. Le problème du logarithme discret consiste à trouver, pour g et h donnés, le plus petit entier naturel x tel que $h = g^x$. Pour deux réels positifs a et b, il existe un unique réel y tel que $a = b^y$, il est donné par la fonction logarithme (à base b) : $y = log_b(a)$. De façon analogue, on note $log_g(h)$ le plus petit x tel que

$h = g^x$ (d'où le nom du problème).

Il existe plusieurs variantes du problème du logarithme discret. Le problème décisionnel du logarithme discret consiste, pour deux éléments g et h d'un groupe $(G, .)$ (plus nécessairement cyclique), de décider s'il existe un entier x tel que $h = g^x$, et de donner x s'il existe. On peut aussi imposer de trouver x (tel que $h = g^x$) dans un intervalle réel donné $[a, b]$, cela devient le problème du logarithme discret sur l'intervalle $[a, b]$, ou imposer à x de vérifier une relation de congruence, ou encore lui imposer un poids de Hamming maximum (pour les calculs informatiques). Toutes ces variantes (ainsi que des variantes avec répartition probabiliste) sont décrites dans [Tes01].

Les calculs de complexité s'expriment en fonction de la taille de l'entrée. Dans ce chapitre, l'entrée est le groupe G d'ordre $p = \#G$, mais du fait que le processeur fonctionne en binaire, on considérera la taille de l'entrée en $\log_2(p)$. Aussi une complexité polynômiale est en $O(\ln^r p)$, r réel, et une complexité exponentielle est en $O(p^r) = O(e^{r \ln p})$. On définit naturellement une complexité sous-exponentielle comme étant de la forme $O(e^{c \ln^{\alpha+o(1)} p})$ où $\alpha < 1$ et $c \in \mathbf{R}$.

Le problème du logarithme discret est, en général, un problème difficile, c'est à dire non résoluble en temps polynomial. On a donc construit des cryptosystèmes basés sur ce problème (comme les protocoles El Gammal, de Cramer-Shoup ou de Diffie-Hellman ; voir [EG85], [CS98] ou [DH76] respectivement). Voilà pourquoi on parle d'attaque du logarithme discret plutôt que de résolution du problème du logarithme discret. Les cryptosystèmes cités sont en fait définis sur un groupe pas forcément cyclique, mais utilisent un élément g et un élément h du sous-groupe $\langle g \rangle$ engendré par g. Ces éléments sont publics (i.e. accessibles à tous) et l'entier x tel que $h = g^x$ est gardé secret. On peut en fait travailler dans $\langle g \rangle$ connu et cyclique, ce qui fait que les groupes utiles pour la cryptographie sont essentiellement cycliques (même si ils peuvent apparaître comme sous-groupes cycliques d'un groupe non cyclique).

Pour donner une idée de la difficulté de ce problème, mentionnons les derniers records de résolution. En 2001, Joux et Lercier ont calculé un logarithme discret dans $\mathbf{F}_p$, p étant un nombre premier à 120 chiffres (voir en [Ler] leurs divers travaux dans ce domaine), Thomé l'a fait dans $\mathbf{F}_{2^{607}}$ [Tho01] en février 2002. La plus grande clef cassée pour les courbes elliptiques est de 109 bits (en 2000, voir la page net du recordman actuel R. Harley [Har]), contre 512 pour le système RSA (voir [RSA], août 1999).

1.2 Attaque de Shanks

Soit G un groupe cyclique fini d'ordre l'entier naturel p (de loi notée multiplicativement), muni d'une relation d'ordre totale. On considère un générateur g de G, et un élément h de G. Rappelons qu'on cherche un entier naturel x tel que $h = g^x$. On suppose choisi un entier $m > \sqrt{p} - 1$. Voici les quatre étapes de ce premier algorithme dû à Shanks (voir [Sha71a]) :

On fabrique une liste $L1$ formée des paires (j, g^{mj}) avec $0 \leq j \leq m-1$, en classant ces paires selon l'ordre de la deuxième coordonnée.

On fabrique une deuxième liste $L2$ formée des paires (i, hg^{-i}), avec $0 \leq i \leq m-1$, paires classées selon l'ordre de la deuxième coordonnée.

On trouve une paire (j, y) de la première liste et une paire (i, y) de la deuxième liste (y est identique pour les deux paires) grâce à la boucle :

Collision dans les listes
Entrée : les listes $L1$ et $L2$ définies ci-dessus.
Sortie : les entiers i et j, $y \in G$ tels que $(j, y) \in L1$ et $(i, y) \in L2$.
Programme :
$h := 1$; $k := 1$;
Tant que $L1[h][2] > L2[k][2]$ faire $k := k + 1$; fin tant que ;
Tant que $L1[h][2] \neq L2[k][2]$ faire
  $h := h + 1$;
  tant que $L1[h][2] > L2[k][2]$ faire $k := k + 1$; fin tant que ;
  fin tant que ;
$(j, y) := L1[h]$; $(i, y) := L2[k]$;
fin.

On a alors trouvé $h = g^{mj+i}$.

En effet, si (j, g^{mj}) et (i, hg^{-i}) ont une seconde coordonnée identique, $h = g^{mj+i}$. D'autre part, x s'écrit $x = mj + i$ avec $(i, j) \in \{0, 1, \ldots, m-1\}^2$ (division euclidienne par m de $x \leq p-1$) . On peut donc bien trouver deux paires de la forme désirée (j, y) et (i, y) (avec $y = g^{mj} = hg^{-i}$).

Dans la première liste on effectue à chaque pas une multiplication par g^m ('taille géant'), et dans la deuxième, pour chaque étape, une multiplication par g^{-1} ('taille bébé'). Ce qui a donné à cet algorithme son surnom 'pas de bébé, pas de géant'.

La construction des listes nécessite $O(m)$ opérations dans le groupe et $O(m \ln m)$ comparaisons. L'algorithme n'effectue que $O(m \ln m)$ comparaisons et additions

dans **N**. Aussi, dès que le coût d'une opération dans G est supérieur à $\ln m$, la complexité est en $O(m)$ opérations dans G. Dans le cas contraire, elle est en $O(m \ln m) = O((\sqrt{m})^{1+\varepsilon})$ opérations élémentaires. La première liste peut être pré-implantée (G et g sont préalablement connus, l'algorithme sort x à la rentrée de h), ce qui abaisse le facteur multiplicatif de la complexité.

En particulier, pour $m = \lfloor \sqrt{p} \rfloor$ (où $\lfloor x \rfloor$ est la partie entière de x, on a donc pris la valeur minimale pour m), la complexité est de $O(\sqrt{p}\ \ln p)$. Dans tout groupe cyclique, on peut donc résoudre le logarithme discret en $O(\sqrt{p}\ \ln p) = O(\sqrt{p}^{1+\varepsilon})$ opérations. Dès que le coût de calcul dans le groupe est important (i.e. nécessite au moins $\sqrt{p} \ln p$ opérations élémentaires), la complexité est en $O(\sqrt{p})$ opérations dans le groupe. D'autre part, pour un groupe fini G quelconque, Shoup [Sho01] a montré qu'un algorithme générique utilisant uniquement des simples opérations de loi de groupe (et non des propriétés particulières du groupe), doit effectuer au moins $O(\sqrt{p})$ telles opérations, où p est le plus grand nombre premier divisant l'ordre du groupe. Une part importante de l'activité de la cryptographie actuelle est donc la recherche de groupes pour lesquels on posséderait une preuve que le meilleur algorithme de résolution du logarithme discret est en $O(\sqrt{p})$ opérations dans G. Un tel groupe serait appelé groupe de Nechaev.

On a vu que l'algorithme de Shanks est en $O(\sqrt{p}^{1+\epsilon})$, cependant il convient de calculer une autre donnée qui peut gêner l'implantation (de la liste pré-calculée) ou les calculs : la taille utilisée en mémoire. Elle est en $O(\sqrt{p})$ (c'est la taille des tableaux pour $m = \lfloor \sqrt{p} \rfloor$ bien sûr). Nous allons maintenant présenter un algorithme qui a lui aussi une complexité en $O(\sqrt{p})$ opérations mais qui nécessite une taille mémoire de l'ordre de $O(1)$.

1.3 Attaque de Pollard

On travaille toujours dans un groupe cyclique fini G, d'ordre p, admettant g comme générateur, et avec un élément quelconque h de G. On cherche un entier x tel que $h = g^x$.

Pour réaliser l'attaque de Shanks, on a cherché à exhiber une égalité entre deux éléments de la forme $g^{a_k} h^{b_k}$, où $a_1 - a_2 \not\equiv 0 \pmod{p-1}$, et
$b_1 - b_2 \not\equiv 0 \pmod{p-1}$. On va ici chercher le même type d'égalité, mais au lieu de le faire de façon systématique (avec construction de tableau et comparaison), on va chercher une collision dans un parcours aléatoire constitué d'éléments de la forme $g^{a_k} h^{b_k}$.

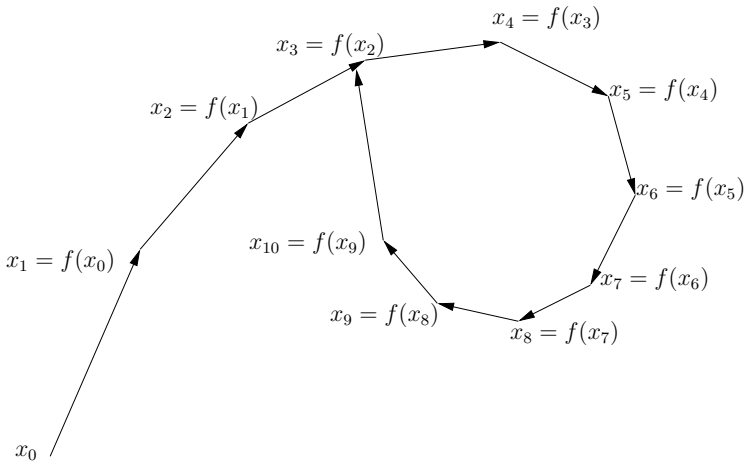

FIG. 1.1 – Chemin de $\{x_k\}_{k\in\mathbf{N}}$.

1.3.1 Complexité d'un algorithme de recherche de cycle

Le but de cette partie est de calculer le nombre d'opérations nécessaire pour trouver un cycle dans une suite donnée par $x_{n+1} = f(x_n)$.

Considérons un ensemble fini S de cardinal n, une permutation f de S, un élément x_0 de S. Construisons la suite $\{x_k\}_{k\in\mathbf{N}}$ définie par récurrence par $x_{k+1} = f(x_k)$. On dira qu'on a une collision si $x_k = x_l$ avec $l \neq k$.

On peut représenter le chemin décrit par les points de la suite comme sur la figure 1.1. Une collision apparaît pour cet exemple entre x_3 et x_{11}.

Dans notre cas on recherche une collision sur $x_n = hg$ du type $f(x_{k+1}) = x_k = x_l = f(x_{l-1})$, avec $x_{k-1} \neq x_{l-1}$ afin de pouvoir utiliser la relation correspondante $h^{c_k - c_l} = g^{d_l - d_k}$. C'est le cas de la première collision : c'est donc elle que nous allons chercher en remontant le chemin point par point. Calculons le coût d'un tel procédé.

Soit X la variable aléatoire donnée par $(X = k)$ ='La première collision apparaît avec x_k' (i.e. il n'y a pas de collision du type $x_i = x_j$, $1 \leq i, j \leq k-1$ et il y a une collision du type $x_k = x_i$, $i \in \{1, \ldots, k-1\}$). La probabilité qu'il n'y ait aucune collision avant k est

$$\begin{aligned} P(X \geq k) &= (1 - \frac{1}{n})(1 - \frac{2}{n}) \cdots (1 - \frac{k-1}{n}) \\ &= \prod_{i=1}^{k-1} (1 - \frac{i}{n}). \end{aligned} \tag{1.1}$$

Or, si $k \in O(\sqrt{n}\,)$,

$$\begin{aligned}\log \prod_{j=1}^{k}(1-\frac{j}{n}) &= \sum_{j=1}^{k}\log(1-\frac{j}{n}) \\ &= -\sum_{j=1}^{k}\frac{j}{n} - \frac{1}{2}\sum_{j=1}^{k}\frac{j^2}{n^2} - \frac{1}{3}\sum_{j=1}^{k}\frac{j^3}{n^3} - \cdots \\ &= -\frac{k(k+1)}{2n} - \frac{k(k+1)(2k+1)}{12n^2} - \frac{k^2(k+1)^2}{18n^3} - \cdots \\ &= -\frac{k^2}{2n} + O(\frac{1}{\sqrt{n}}).\end{aligned} \tag{1.2}$$

On arrive ainsi à estimer, toujours pour $k \in O(\sqrt{n}\,)$, la probabilité qu'il n'y ait aucune collision avant k :

$$\begin{aligned}P(X \geq k) &= e^{-\frac{k^2}{2n}+O(\frac{1}{\sqrt{n}})} \\ &= e^{-\frac{k^2}{2n}}\big(1+O(\frac{1}{\sqrt{n}})\big).\end{aligned} \tag{1.3}$$

On peut alors calculer le nombre moyen d'itérations nécessaires pour obtenir une collision :

$$\begin{aligned}E(X) &= \sum_{k=1}^{\infty} kP(X=k) \\ &= \sum_{k=1}^{\infty} P(X \geq k) \\ &= \big(\sum_{k=1}^{\infty} e^{-\frac{k^2}{2n}}\big)\big(1+O(\frac{1}{\sqrt{n}})\big) + O(1) \\ &= \big(\int_0^{\infty} e^{-\frac{x^2}{2n}}dx - O(1)\big)\big(1+O(\frac{1}{\sqrt{n}})\big) + O(1) \\ &= \sqrt{\frac{\pi n}{2}} + O(1).\end{aligned} \tag{1.4}$$

En effet, de $\forall x \in [k, k+1], e^{-\frac{(k+1)^2}{2n}} \leq e^{-\frac{x^2}{2n}} \leq e^{-\frac{k^2}{2n}}$, on déduit par intégration que la somme et l'intégrale différent d'au plus 1, d'où l'approximation (1.4).

On obtient ainsi

Lemme 1.3.1 *Soient f une permutation d'un ensemble S de cardinal $n = \#S$, $\{x_k\}_{k\in\mathbf{N}}$ une suite vérifiant $x_{n+1} = f(x_n)$ pour tout $n \in \mathbf{N}$.*

Le nombre moyen d'itération nécessaire pour obtenir une collision est

$$E(X) = \sqrt{\frac{\pi n}{2}} + O(1).$$

1.3.2 Principe de l'attaque

Rappelons que nous cherchons à résoudre un problème de logarithme discret dans un groupe fini G de cardinal p avec l'élément h dans le sous-groupe $\langle g\rangle$ engendré par g.

Nous allons construire un chemin dans le groupe G étudié pour y trouver une collision. On choisit trois sous-ensembles S_1, S_2, S_3 formant une partition de G (i.e. disjoints deux à deux et de réunion G) tous de taille approximativement identique. On recherchera un cycle sur une suite $\{x_k\}_{k\in\mathbf{N}}$ vérifiant la relation de récurrence donnée par :

si $x_k \in S_1$, $x_{k+1} = hx_k$.
si $x_k \in S_2$, $x_{k+1} = {x_k}^2$.
si $x_k \in S_3$, $x_{k+1} = gx_k$.

La fonction f sous-jacente est donnée par $f(x) = hx$ sur S_1, $f(x) = x^2$ sur S_2, $f(x) = gx$ sur S_3.

Historiquement, Pollard –le premier à proposer ce type d'attaque [Pol78]– a établi son algorithme dans le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ des éléments inversibles de $\mathbf{Z}/p\mathbf{Z}$, p étant un nombre premier. Il a pris comme partition $S_1 = [1, \frac{p}{3}]\bigcap\mathbf{N}$, $S_2 =]\frac{p}{3}, \frac{2p}{3}]\bigcap\mathbf{N}$ et $S_3 =]\frac{2p}{3}, p-1]\bigcap\mathbf{N}$, avec l'initialisation $x_0 = 1$. Cette paternité et la forme en rho grec d'un chemin "idéal" lors d'un cycle (comme sur la figure 1.1) a donné à cette méthode le nom de Pollard-Rho.

Pour un groupe G fini cyclique, on débute le chemin (créé par la suite) avec un élément choisi au hasard parmi les éléments de la forme $x_0 = h^{c_0}g^{d_0}$. Par construction, on peut trouver pour tout entier naturel k un couple (c_k, d_k) d'entiers naturels tels que $x_k = h^{c_k}g^{d_k}$. Dans un groupe fini, on ne peut éviter une collision : on peut trouver $(l,\, k) \in \mathbf{N}^2$ tel que $x_l = x_k$ et $l \neq k$. On réécrit alors l'égalité sous la forme $h^{c_l - c_k} = g^{d_k - d_l}$. Si $pgcd(c_l - c_k,\, p-1) = 1$, on a trouvé $x \equiv (d_k - d_l)/(c_l - c_k) \pmod{p-1}$ tel que $h = g^x$. Sinon, cette collision n'est pas utilisable et on crée un nouveau chemin à partir d'un nouvel élément de départ (toujours tiré au hasard parmi ceux de forme souhaitée).

En considérant que le parcours est aléatoire, la collision a une probabilité d'être utilisable de $\phi(p-1)/(p-1)$ (lorsque $p-1$ n'a que de grands facteurs premiers, cet événement est quasi-sûr). En appliquant le lemme 1.3.1 avec pour ensemble S le groupe fini G de cardinal $p = \#G$ et pour fonction f celle exprimée plus haut, la première collision est attendue "en moyenne" au bout de $\sqrt{\pi p/2} \simeq 1.25\sqrt{p}$ itérations. Essentiellement, ce procédé nécessite donc $1.25\sqrt{p}$ évaluations de f.

1.3.3 Solution au problème de stockage

Un inconvénient de cette méthode est qu'à priori, pour trouver la première collision, on doit stocker toutes les valeurs déjà calculées $x_0,\ x_1, \ldots,\ x_k$ puis comparer la nouvelle itération x_{k+1} avec ces valeurs. On utilise dans ce cas une taille importante de stockage (en $O(\sqrt{p})$), alors que notre objectif était de baisser la taille mémoire trop élevée de l'algorithme de Shanks. On utilise en fait les algorithmes suivants pour trouver les cycles.

Algorithme de Floyd
Entrée : la valeur initiale x_0, la fonction itérative f.
Sortie : un entier j tel que $x_j = x_{2j}$.
Programme :
$x := x_0;\ w := x_0;\ j = 0;$
tant que $(x \neq w)$ faire
  $j := j + 1;$
  $x := f(x);$
  $w := f(w);\ w := f(w);$
  fin tant que ;
retourner j ;
fin.

A chaque pas on calcule x_j et x_{2j}, on les compare et on recommence au rang suivant tant qu'ils sont différents. On a ainsi bien trouvé une collision ($x_j = x_{2j}$) en n'utilisant que trois variables de stockage (x, w et j), la taille de stockage est en $O(1)$.

Remarquons qu'à chaque itération, on évalue trois fois f. Si f est choisie au hasard dans G^G sous une loi uniforme, on montre que le nombre moyen d'itérations nécessaire pour obtenir une collision par l'algorithme de Floyd est environ $1.0308\sqrt{p}$. En première estimation, on évalue en moyenne $3\sqrt{p}$ fois la fonction f

(à comparer avec les $1.25\sqrt{p}$ itérations du programme initial). La présentation de cet algorithme se trouve dans [Knu81].

Brent [Bre80] propose un algorithme abaissant le nombre d'évaluations de f par itération. Il procède en comparant la séquence $x_{k+1} = f(x_k)$ avec la variable stockée w (réactualisée de temps en temps) comme suit.

Algorithme de Brent
Entrée : la valeur initiale x_0, la fonction d'itérative f.
Sortie : des entiers j et k tels que $x_j = x_k$.
Programme :
$x := x_0;\ r := 1;\ k := 0; test := \text{`}faux'$;
tant que (non test) faire
  $w := x;\ j := k$;
  $r := 2r$;
  tant que ((test) ou ($k \leq r$)) faire
    $k := k + 1;\ x := f(x)$;
    $test := (w = x)$;
    fin tant que ;
  fin tant que ;
retourner j, k ;
fin.

Le programme débute avec $w = x_0$. Il compare w avec tous les x_k jusqu'à ce que k soit une puissance de 2. Il attribue alors à w la valeur x_k puis recommence la série de comparaisons décrites dans la phrase précédente. Il s'arrête évidemment dès qu'il trouve une égalité $w = x_k$.

1.3.4 Comparaison des algorithmes de Floyd et de Brent

Précisons un peu la forme du parcours aléatoire construit, afin de comparer le nombre d'évaluations des deux algorithmes présentés. On peut trouver deux entiers μ et λ tels que les premières valeurs

$$x_0, x_1, \ldots, x_\mu, \ldots, x_{\mu+\lambda-1}$$

soient deux à deux distinctes et tels que les suivantes forment une boucle

$$\forall k \geq \mu,\ x_k = x_{k+\lambda}.$$

L'entier λ est appelé la période de la suite $\{x_n\}_{n\in\mathbf{N}}$, et l'entier μ, qui correspond à la longueur du segment non-périodique du cycle, est nommé prépériode de la suite $\{x_n\}_{n\in\mathbf{N}}$. Posons μ_r le reste de la division euclidienne de μ par λ. Revenons maintenant à l'algorithme de Floyd. Lorsque cet algorithme se termine, il renvoie la valeur

$$j = \begin{cases} \mu \quad \text{si } \lambda|\mu \text{ et } \mu > 0 \\ \text{ou} \\ \mu + \lambda - \mu_r \quad \text{sinon} \end{cases} \tag{1.5}$$

On en déduit que $j \geq max\{\mu, \lambda\}$. Le nombre total d'évaluations de la fonction f dans l'algorithme de Floyd est de $W_F = 3j$ (il suffit de se souvenir que chaque itération de l'algorithme de Floyd utilise trois évaluations de f et augmente j d'une unité en partant de 1). D'où,

$$W_F \geq 3\, max\{\mu, \lambda\}.$$

Étudions à présent ce qui se passe pour l'algorithme de Brent. Notons s le nombre d'itérations nécessaires. A la fin de l'algorithme, on récupère les entiers

$$k = \lambda \text{ et } j = \begin{cases} 0 \quad \text{si } s = 1, \\ \text{ou} \\ 2^{s-1} \quad \text{si } s > 1. \end{cases} \tag{1.6}$$

Le nombre total d'évaluations de la fonction f est cette fois $W_B = j + k = j + \lambda$. Posons

$$\sigma = \max\{s \in \mathbf{N} / \; 2^{s-1} \leq \max\{\mu, \lambda\} \; \}.$$

Alors,

$$2^\sigma - 2^{\sigma-1} = 2^{\sigma-1} \leq \lambda,$$

et,

$$j \leq 2^{\sigma-1} \leq 2 \max\{\mu, \lambda\}.$$

On en déduit l'inégalité

$$W_B \leq \lambda + 2 \max\{\mu, \lambda\} \leq W_F.$$

L'algorithme de Brent a donc une complexité plus basse. Pour donner une idée, sous l'hypothèse que la fonction est choisie au hasard de façon uniforme dans G^G, on trouve avec cet algorithme une collision au bout d'environ $1.97\sqrt{p}$ itérations [Tes01]. Pour adopter cet algorithme, il faut cependant vérifier qu'il

utilise lui aussi peu de mémoire. On stocke les variables j, k, w et r (la variable test est juste introduite pour la lisibilité du programme), la taille mémoire utilisée est donc toujours en $O(1)$. Des modifications de l'algorithme de Brent ont été proposées baissant un peu le facteur multiplicatif pour le nombre d'itérations mais nécessitant plus de stockage ([SL84] et [Tes98a]).

1.3.5 Autres améliorations possibles

On peut mieux approcher un parcours aléatoire en utilisant une partition plus fine de $S = G$. On considère un entier naturel r dans $\{1, \ldots, 300\}$, et l'on effectue une partition de S en r ensembles $S_1, S_2, \ldots, S_r$ de taille approximativement identique. On peut par exemple les construire grâce à une fonction de hachage $v : G \to [1, r] \bigcap \mathbf{N}$ et définir $S_k = \{y \in G / v(y) = k\}$ — Une fonction de hachage n'est rien d'autre qu'une fonction du type $h : E \to F$, où F est un ensemble de taille déterminée. L'ensemble de départ E est souvent composé de messages quelconques. Bien choisies (i.e. lorsque le calcul de $h(m)$ est facile, trouver un antécédent par h est difficile et trouver des collisions ($h(m) = h(m')$, $m \neq m'$) est difficile), les fonctions de hachage sont utilisées comme ajout à la signature digitale —. On construit la marche à l'aide de la fonction $f : y \mapsto yM_{v(y)}$, où M_s est un multiplicateur de la forme $g^{m_s}h^{n_s}$ dont les coefficients m_s et n_s sont choisis au hasard. On cherche alors une collision avec une suite définie par $y_{n+1} = f(y_n)$, et on résout le logarithme discret de la même manière.

La première marche de ce type fut proposée par Sattler et Schnorr [SS85] avec $r = 8$. L'exemple le plus populaire de cette famille est la marche avec $r = 20$ de Teske [Tes98b] qui aboutit en moyenne au bout de $1.26\sqrt{p}$ itérations.

1.4 Accélération avec ordinateurs en parallèle

Afin d'accélérer l'obtention d'une collision, on va chercher à faire travailler en parallèle m ordinateurs. L'idée première est de demander à chaque ordinateur de trouver un cycle comme décrit ci-dessus indépendamment des calculs effectués par les autres processeurs. Aussi, si chaque ordinateur applique l'algorithme de la section précédente, la probabilité qu'il n'y ait aucune collision avant k est, avec

$k = O(\sqrt{n})$,

$$\begin{aligned} P(X \geq k) &= \big((1 - \frac{1}{n})(1 - \frac{2}{n}) \cdots (1 - \frac{k-1}{n})\big)^m \\ &= e^{-\frac{mk^2}{2n}} + O(\frac{1}{\sqrt{n}}). \end{aligned} \tag{1.7}$$

On trouve de la même manière que le nombre moyen de pas nécessaire pour obtenir une collision effectués par chaque ordinateur est de $\sqrt{(\pi n)/(2m)}$. L'utilisation de m ordinateurs avec cette méthode directe n'accélère que d'un facteur $\sqrt{m}$, ce qui est peu efficace.

Van Oorschot et Wiener [vOW99] ont proposé l'algorithme suivant de recherche des collisions en parallèle bien plus rapide. On suppose que l'on peut facilement tester dans $S = G$ si un point a une propriété remarquable fixée (par exemple : les r premiers bits codant le point sont nuls, r étant un petit entier fixe). On utilise toujours la partition de G en S_1, S_2, S_3, et la fonction f donnée par $f(x) = hx$ sur S_1, $f(x) = x^2$ sur S_2, $f(x) = gx$ sur S_3. Chaque processeur commence la construction d'un chemin constitué de points $x_k = f(x_{k-1})$ à partir d'un point origine choisi au hasard x_0 de la forme $h^{c_0}g^{d_0}$. Notons que les éléments de la suite s'écrivent donc encore sous la forme $x_k = h^{c_k}g^{d_k}$. Le processeur s'arrête dès qu'il rencontre un point remarquable. Il rajoute alors sur une liste commune à tous les processeurs un triplet constitué du point remarquable x_d trouvé, du point de départ x_0 et de la longueur d de la marche. Les processeurs construisent ainsi des marches aléatoires s'arrêtant à un point remarquable jusqu'à ce que un même point remarquable apparaisse dans deux triplets de la liste commune ayant des points origines différents. On trouve alors une collision entre deux chemins comme le montre l'exemple de la figure 1.2.

Les points communs y sont représentés en noir. Les marches s'arrêtent aux points remarquables (point 'blanc'). Les marches 3 et 4 finissent au même point remarquable $x_5 = y_4$. En remontant les chemins on trouve la collision
$f(x_2) = f(y_1)$. Par construction, on peut écrire les termes des suites sous la forme $x_k = h^{c_k}g^{d_k}$ et $y_k = h^{c'_k}g^{d'_k}$ pour tout k. La collision fournit l'égalité
$h^{c_k}g^{d_k} = h^{c'_l}g^{d'_l}$; avec, dans l'exemple de la figure 1.2, $k = 3$ et $l = 2$. On en tire alors une solution pour le logarithme discret comme on l'a fait pour une collision dans un cycle.

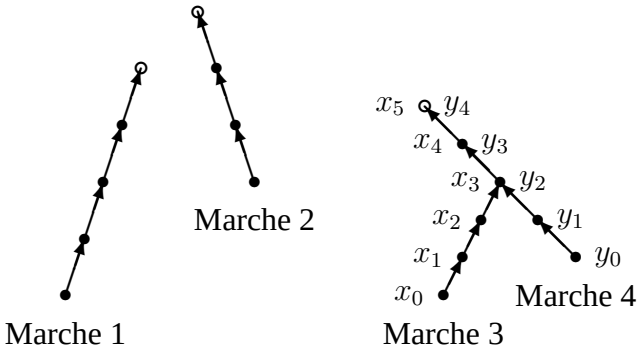

FIG. 1.2 – Marches aléatoires.

Cependant dans le cas où la collision se produit sur un point dit de "Robin Hood", c'est à dire si l'une des deux marches rejoint l'autre à son point de départ (par exemple $x_3 = y_0$), aucune collision n'est trouvée, et il faut continuer à générer des marches.

Notons θ la proportion de points vérifiant la propriété remarquable. Supposons que leur répartition est uniforme. Les marches ont alors pour longueur moyenne $1/\theta$. En pratique, il y a peu de points remarquables, les marches sont donc assez longues et les "Robin Hood" sont rares.

Examinons maintenant la complexité de cette méthode. Rappelons que l'on cherche une collision entre des chemins tracés dans le groupe G de cardinal p (pour résoudre un problème du logarithme discret) à l'aide de m ordinateurs travaillant en parallèle. Afin de comparer avec les résultats précédents, on supposera ici aussi que les collisions ne donnant pas la solution (i.e. lorsque $d_k - d_l \equiv c_l - c_k \pmod{(p-1)}$) sont négligeables (le calcul tenant compte des collisions se trouve dans [vOW99], la contribution en m dans la complexité alors obtenue est identique).

Le calcul fait à la sous-section 1.3.1 montre qu'il faut en moyenne calculer $\sqrt{p\pi/2}$ points pour qu'un chemin en rencontre un autre. Ce travail demande à chaque processeur de calculer $\frac{\sqrt{p\pi/2}}{m}$ points. Il faut ensuite recalculer les points

des chemins qui se rencontrent jusqu'à la collision, afin de connaître les puissances de g et de h dans x_k et y_l. Les chemins étant de longueur moyenne $1/\theta$, cela nécessite moins de $2/\theta$ évaluations de f supplémentaires (c'est en $O(1)$). L'ordre de grandeur du nombre de pas nécessaire pour une collision effectué par chaque ordinateur est donc en $O(\sqrt{p}/m)$: le gain devient maintenant significatif.

1.5 Accélération par classes d'équivalence d'un automorphisme

On cherche comme précédemment, connaissant un générateur g d'un groupe G cyclique d'ordre p et un élément h de G, à exprimer h comme puissance de g : $h = g^x$, $x \in \mathbf{Z}$. On suppose de plus que le groupe G possède une relation d'équivalence $\sim$ partitionnant G en $\lfloor p/m \rfloor$ classes d'équivalence. Supposons que l'on puisse transposer le problème aux classes $\overline{h} = \overline{g}^x$. Sa résolution aurait pour complexité $\sqrt{p/m}$, on abaisse la complexité par une division par $\sqrt{m}$. Ce facteur est ici intéressant car 'gratuit' contrairement au chapitre précédent qui coûtait l'utilisation de m ordinateurs

La réalisation de cette idée pose cependant quelques problèmes.

Tout d'abord, il peut être délicat de construire un parcours aléatoire sur les classes du type $\overline{x_{n+1}} = f(\overline{x_n})$. On ne peut pas forcément faire des calculs sur $G/\sim$, ou souvent difficilement ; on doit alors stocker l'image de chaque point pour la retrouver à chaque pas.

En général, on préfère plutôt boucler l'algorithme de Brent par

$$x = f(x) \text{ tant que } \overline{x} \neq \overline{w},$$

la fonction f étant choisie de manière à ce qu'elle induise une permutation sur les classes. Ainsi, les calculs nécessaires pour l'itération s'effectuent dans G.

Une fois trouvé le logarithme discret sur les classes, on ne peut pas en déduire directement le logarithme discret dans G : si $G = \left(\mathbf{Z}/9\mathbf{Z}\right)^\times = \{2, 4, 8, 7, 5, 1\}$, $g = 2$, $h = 5$, et si $\sim$ est la relation 'sont congrus modulo 3', la résolution dans les classes donne $\overline{2}^1 = \overline{5}$. Il n'y a que deux classes d'équivalence, on en déduit donc $h = g^x$ dans G avec $x \equiv 1 \pmod 2$. Mais on est ensuite obligé de calculer toutes les puissances de ce type (g, g^3, g^5) et les comparer avec h pour obtenir $h = g^5$.

On a résolu le logarithme discret avec une complexité en $O(n/2)$ ce qui est sans intérêt.

Cet exemple est évidemment extrême (bien que commun), on va chercher à construire des relations d'équivalence où la résolution dans $G/\sim$ donne rapidement le logarithme discret dans G.

Examinons un cas classique où la résolution dans $G/\sim$ est exploitable. Soit C une courbe dont la jacobienne $Jac(C)$ est cyclique d'ordre p, admettant D_1 comme générateur. Considérons un automorphisme σ de C, on peut l'étendre par linéarité au groupe $Jac(C)$. L'élément D_1 étant générateur de $Jac(C)$, on peut trouver un entier γ tel que $\sigma(D_1) = \gamma D_1$. Par linéarité, on obtient que σ est une homothétie de rapport γ.

Définissons la relation $\sim$ sur le groupe $Jac(C)$ par

$$D \sim D' \Longleftrightarrow \exists i \in \mathbf{N}/\ D = \sigma^i(D').$$

Cette relation est manifestement une relation d'équivalence. Remémorons-nous que l'on veut résoudre le logarithme discret dans $Jac(C)$: $D_2 = kD_1$, k étant un entier. Supposons qu'on ait pu le résoudre sur $G/\sim$: on connaît un entier ρ tel que $\overline{D_2} = \rho\overline{D_1}$. On peut donc trouver i tel que $D_2 = \rho\ \sigma^i(D_1) = \rho\ \gamma^i\ D_1$. On a donc résolu le logarithme discret : $k = \rho\ \gamma^i$. Regardons maintenant la complexité de ce procédé. On a supposé que la relation $\sim$ partitionne $Jac(C)$ en $\lfloor p/m \rfloor$ classes d'équivalence, où p est l'ordre du groupe $Jac(C)$. On doit d'abord chercher le logarithme discret dans l'ensemble quotient, ce qui est fait en $O(\sqrt{p/m})$ opérations de ce groupe (à noter que ces opérations sur les classes sont plus coûteuses que celles dans $Jac(C)$ même). Ensuite, on procède en calculant les $\rho\ \sigma^i(D_1)$, cela coûte m exponentiations dans le groupe, soit $O(m\log(p))$ opérations. Restent les multiplications dans les entiers avec réduction modulo l'ordre du groupe, effectuées en $O(1)$. Si m est assez petit, on trouve bien une complexité en $O(\sqrt{p/m})$. On peut trouver une recherche assez systématique d'exemples d'automorphismes et leurs courbes correspondantes dans [DGM99]. Notez dans ces exemples qu'en général les automorphismes se calculent rapidement ; aussi, pour vérifier que $\overline{D_2} = \rho\overline{D_1}$ on calcule directement les $\sigma^i(\rho D_1)$; on a au plus m applications de l'automorphisme à effectuer.

1.6 Attaque d'Adleman

Soient p un nombre premier "assez grand" de manière à ce qu'il soit intéressant d'utiliser le logarithme discret au groupe fini $G = \mathbf{F}_p$, g un générateur de G et h un élément de G. On suppose l'existence d'un sous-ensemble $S = \{q_1, q_2, \ldots, q_t\}$ de G, de cardinal $t << p-1$, tel que "une proportion significatives" d'éléments de G peut s'exprimer comme produit d'éléments de S (nous préciserons plus loin la condition sur cette proportion que nous noterons θ). On cherche toujours un entier x tel que $h = g^x$.

Pour un entier b compris entre 1 et $p-2$ au sens large tel que g^b est décomposable sous la forme

$$g^b = \prod_{i=1}^{t} {q_i}^{a_i},$$

on peut dire

$$b \equiv \sum_i a_i log_g(q_i) \pmod{p-1}.$$

Lorsque l'on fait varier b (parmi ceux tels que g^b se décompose sous S), on obtient un système d'équations linéaires d'inconnus les $log_g(q_i)$. On se pose ici le problème du logarithme discret pour p très grand (sinon une attaque en calculant tous les termes suffirait), de plus le cardinal t de l'ensemble S est demandé de taille "raisonnable" (pour faciliter ainsi la mise en service sur ordinateur) : on travaille donc avec t nettement plus petit que p. Le nombre de valeurs prises par g^b lorsque b décrit $\mathbf{N}$ est $(p-1)$. Le nombre de ces éléments décomposable sous S est $\theta(p-1)$. Avec une proportion θ d'éléments décomposables sous S importante, on espère ainsi très raisonnablement trouver t équations indépendantes lorsque b varie dans $\{1, \ldots, p-1\}$. On résout alors ce système, ce qui donne les valeurs des $log_g(q_i)$.

De même, de

$$hg^b = \prod_{q_i \leq M} {q_i}^{\alpha_i},$$

on tire

$$x + b \equiv \sum_i \alpha_i log_g(q_i) \pmod{p-1}.$$

En faisant varier b on a alors un système d'équations linéaires en les α_i et x : sa résolution conduit à trouver x.

Ce procédé fut introduit par L. Adleman en 1979 sur les groupes $\mathbf{F}_p^{\times}$, p étant premier [Adl79]. Certains le nomment aussi 'index calculus method'. Le calcul de

sa complexité donne un coût en $O(L(q))$, avec $L(q) = \exp\sqrt{\log(q)\log(\log(q))}$. C'est une attaque sous-exponentielle (avec $a = 1/2$ et $c = 1$ dans la notation en 1.1) du problème du logarithme discret. Cependant, la condition sur l'existence de S est restrictive : on peut appliquer cette attaque sur les groupes multiplicatifs des corps finis $\mathbf{F}_q^*$ (q étant une puissance d'un nombre premier), mais elle ne s'adapte pas au logarithme discret sur les courbes elliptiques (voir [Sil98]). Pour ces dernières, on peut pourtant se ramener à une attaque d'Adleman grâce à des techniques du type couplage de Tate décrit dans la section suivante.

1.7 Attaque de Frey-Rück

Soit C une courbe projective, lisse, irréductible de genre g sur un corps fini $\mathbf{k} = \mathbf{F}_q$, q étant une puissance d'un nombre premier p (Nous rappellerons la définition de ce type de courbe au début du prochain chapitre). Choisissons un entier l premier à p, et considérons un entier k tel que le corps $\mathbf{F}_{q^k}$ contienne les racines l-ième de l'unité (i.e. $l|q^k - 1$). Nous travaillerons sur le corps $\mathbf{K} = \mathbf{F}_{q^k}$; nous désignerons par C l'ensemble les points à coordonnées dans $\mathbf{K}$ vérifiant l'équation de C.

Notons $Div^0_{\mathbf{K}}(C)$ le groupe des diviseurs de degré zéro de C, $P_{\mathbf{K}}(C)$ le sous-groupe des diviseurs principaux, et $G = Div^0_{\mathbf{K}}(C)/P_{\mathbf{K}}(C)$ la "jacobienne" de C. Pour tout diviseur $D = \sum_{P\in C} n_P P$ de C, on définit son support par

$$Supp\, D = \{P \in C / \, n_P \neq 0\}.$$

Pour tout entier l, on définit le groupe de $l-$torsion par

$$G[l] = \{\overline{D} \in G / \, l\overline{D} = 0\}.$$

Pour toute fonction $f \in \mathbf{K}[C]$, et pour tout diviseur

$$E = \sum_{P\in C} n_P P$$

avec $\overline{E} \in G[l]$ tel que $Supp\,(f) \bigcap Supp\, E = \emptyset$, on définit

$$f(E) = \prod_{P\in Supp\, E} f(P)^{n_P} \in \mathbf{K}^\times.$$

On vérifie alors facilement le lemme suivant :

Lemme 1.7.1 *Soit l un entier premier à q. Pour $\overline{D} \in G[l]$, on peut trouver $f \in \mathbf{K}(C)$ tel que $(f) = lD$.*
Soit $\overline{E} \in G$ tel que $Supp\, D \bigcap Supp\, E = \emptyset$.
Alors,

(i) *La valeur $f(E) \pmod{\mathbf{K}^{\times l}}$ ne dépend pas du choix des représentants D et E dans $\overline{D}$ et $\overline{E}$ respectivement, ni du choix de f.*

(ii) *Si $\overline{E} \in lG$, alors $f(E) \in \mathbf{K}^{\times l}$.*

Nous pouvons désormais présenter le couplage de Tate.

Définition 1.7.2 *Avec les mêmes notations, le couplage de Tate est défini par :*
$$\begin{aligned}\langle -,- \rangle_l \ : G[l] \times G/lG &\longrightarrow \mathbf{K}^{\times}/\mathbf{K}^{\times l} \\ (\overline{D}, \tilde{E}) &\longmapsto \langle \overline{D}, \tilde{E} \rangle_l = f(E).\end{aligned}$$

Le couplage de Tate vérifie les propriétés remarquables décrites dans le théorème suivant.

Théorème 1.7.3 *Soit $\mathbf{K}$ un corps fini contenant les racines $l-$ème de l'unité. Le couplage de Tate satisfait les propriétés suivantes :*

(i) *Le couplage de Tate est bien défini.*

(ii) *Le couplage de Tate est non-dégénéré :*
pour tout $\overline{D} \in G[l] - \{0\}$, il existe $\overline{E} \in G$ tel que $\langle \overline{D}, \tilde{E} \rangle_l \neq \mathbf{K}^{\times l}$.

(iii) *Le couplage de Tate est "bilinéaire au sens suivant" :*
pour tout entier n, $\langle n\overline{D}, \tilde{E} \rangle_l = \langle \overline{D}, n\tilde{E} \rangle_l = \langle \overline{D}, \tilde{E} \rangle_l^{\,n}$.

Démonstration
Le (i) n'est rien d'autre que le lemme 1.7.1. La non-dégénérence du (ii) est due à l'hypothèse que $\mathbf{K}$ contient les racines l-ièmes de l'unité (voir [FR94]). Le (iii) est immédiat vu le caractère multiplicatif apparaissant dans la définition de $f(E)$. □

La programmation du couplage de Tate est facile. Dans le cas des courbes elliptiques ([FMR99]), le couplage de Weil est similaire mais a un temps d'exécution environ deux fois plus long. Il est de plus nécessaire de travailler sur une extension $\mathbf{K}_1$ de $\mathbf{K}$ telle que $G[l] \subset Div^0_{\mathbf{K}_1}(C)$.

Exemple sur $\mathbf{F}_5$
Soit C la courbe sur $\mathbf{k} = \mathbf{F}_5$ donnée par l'équation affine $y^2 = x^3 + x + 2$. Prenons $l = 4$. Dans cet exemple $q = 5$, l et q sont donc premiers entre eux. De plus $l|(q^1 - 1) = 4$: nous travaillerons avec $k = 1$ ($\mathbf{K} = \mathbf{k} = \mathbf{F}_5$).
L'ensemble des points de la courbe C est $\{(1, 2),\ (1, 3),\ (4, 0),\ \theta\}$, θ étant le point à l'infini. Par conséquent, $G[4] = G$ et $4G = \{\theta\}$. Remarquons de plus que $\mathbf{K}^{\times 4} = \{1\}$. Le couplage de Tate considéré ici est donc défini sur :

$$\langle -, - \rangle_4 \ : \ G \times G \longrightarrow \mathbf{F}_5^{\times}.$$

Soient le diviseur $D = (1,\ 2) - \theta$, f la fonction de $\mathbf{K}(C)$ donnée par $f(x, y) = y - (3 * x^2 + 4)$. D'où, $(f) = 4(2,\ 1) - 4\theta = 4D$. Soit maintenant le diviseur $E = (1,\ 3) - (4,\ 0)$, remarquons que $Supp\, D \bigcap Supp\, E = \emptyset$: on peut calculer le couplage de Tate.

$$\begin{aligned} \langle \overline{D},\ \tilde{E} \rangle_4 &= f(E) \\ &= \frac{f(1,\ 3)}{f(4,\ 0)} \\ &= \frac{3 - (3 * 1^2 + 4)}{0 - (3 * 4^2 + 4)} \\ &= 2. \end{aligned} \tag{1.8}$$

Par cette technique et en utilisant la "bilinéarité" du couplage de Tate, on construit le tableau des valeurs prises par $\langle \overline{D},\ \tilde{E} \rangle_4$:

$\overline{D} \setminus \overline{E}$	$(4,0) - (4,0)$	$(1,3) - (4,0)$	$\theta - (4,0)$	$(1,2) - (4,0)$
$\theta - \theta$	1	1	1	1
$(1,2) - \theta$	1	2	4	3
$(4,0) - \theta$	1	4	1	4
$(1,3) - \theta$	1	3	4	2

Regardons maintenant l'attaque de Frey-Rück présentée dans [FR94]. L'idée initiale provient en fait de A. Menezes, S. Vanstone et P. van Oorschot [MOV95]. Mentionnons aussi sur ce sujet l'article de Galbraith [Gal01] (pour les courbes de grand genre).

On se limite ici au problème du logarithme discret dans la courbe $G[l]$: étant donné $(\overline{D_1}, \overline{D_2}) \in G[l]^2$, résolvons $\overline{D_2} = \lambda \overline{D_1}$. Soit l l'ordre de D_1, et k le plus petit entier tel que $l|(q^k - 1)$.

Le programme de l'attaque de Frey-Rück est :

1. Choisir au hasard un diviseur $Q \in G$ jusqu'à ce que $\langle \overline{D_1}, \tilde{Q} \rangle_l \notin \mathbf{K}^{\times l}$.
2. Calculer $\zeta_i = \langle \overline{D_i}, \tilde{Q} \rangle_l \in \mathbf{F}_{q^k}^{\times}$, pour $i \in \{1, 2\}$.
3. Élever ζ_i à la puissance $(q^k - 1)/l$ (cette étape est optionnelle depuis que l'algèbre linéaire de l'attaque d'Adleman est performante modulo l).
4. Résoudre le problème du logarithme discret $\zeta_2 = {\zeta_1}^{\lambda}$ dans le corps fini $\mathbf{F}_{q^k}^{\times}$ à l'aide de l'attaque d'Adleman.

On parvient de cette manière à obtenir une complexité sous-exponentielle. Notons cependant qu'il faut envoyer G dans un corps $\mathbf{F}_{q^k}$ contenant les racines l-ième de l'unité (l étant l'ordre du diviseur générateur D_1 considéré). Si l'on ne peut trouver de tel corps que pour des grandes valeurs de k, l'attaque se révèle en fait peu intéressante. On appelle indice de sécurité de D_1 le plus petit entier naturel k tel que $\mathbf{F}_{q^k}$ contienne les racines l-ième de l'unité, c'est à dire tel que k soit l'ordre de q dans $\mathbf{F}_l^*$. Il mesure la sécurité du système face à l'attaque de Frey-Rück : plus il est grand, plus le système est sûr.

Chapitre 2

Sur les jacobiennes généralisées

Parmi les groupes sur lesquels le logarithme discret a été proposé, on trouve les jacobiennes de courbes. Ces objets, construits ici à partir de groupes de diviseurs, s'avèrent intéressantes pour le logarithme discret. Il existe des groupes construits en généralisant la jacobienne : les jacobiennes généralisées. Il paraît de ce fait intéressant de chercher à les utiliser à des fins cryptographiques. Pour fabriquer un logarithme discret, seuls les groupes des jacobiennes généralisées nous serons utiles : on considérera donc **abusivement** ces jacobiennes comme des groupes quotients de groupes de diviseurs. Nous décrivons dans ce chapitre nos tentatives pour trouver une "bonne" représentation des classes formées par ces quotients susceptible d'être utilisée pour des algorithmes de calcul. Nous examinons tout d'abord le lien entre la jacobienne généralisée et la jacobienne usuelle. Après la donnée des définitions nécessaires, nous construirons la suite exacte

$$0 \longrightarrow L_{\mathfrak{m}} \longrightarrow J_{\mathfrak{m}} \longrightarrow J \longrightarrow 0,$$

où J est la jacobienne, $J_{\mathfrak{m}}$ est la jacobienne généralisée de module $\mathfrak{m}$, et calculerons le noyau $L_{\mathfrak{m}}$ [Ser59]. Malheureusement, on ne dispose pas d'un relèvement de cette suite exacte : on ne peut pas représenter ainsi les éléments des jacobiennes généralisées par ceux de la jacobienne. Notons de plus que la suite exacte permet le transfert du problème du logarithme discret de la jacobienne généralisée $J_{\mathfrak{m}}$ à la jacobienne J et à $L_{\mathfrak{m}}$. La complexité de ce problème dans $J_{\mathfrak{m}}$ dépend donc de celle dans J et $L_{\mathfrak{m}}$ [Cou01]. Nous en déduisons les limites de l'intérêt des jacobiennes généralisées pour le logarithme discret.

Nous verrons cependant dans le chapitre suivant d'autres applications cryptographiques possibles pour les jacobiennes généralisées. Pour préparer ce troisième

chapitre, et afin de pouvoir calculer dans $J_{\mathfrak{m}}$, nous traiterons dans la dernière partie de ce chapitre du lien entre les jacobiennes généralisées et les ordres, dans lesquels il paraît plus simple de programmer des calculs.

2.1 Quelques rappels

Rappelons tout d'abord les outils standards avec lesquels nous travaillerons. Dans toute cette section, on travaillera sur un corps $\mathbf{K}$.

Définition 2.1.1 *Soit $S \subset \mathbf{K}[X_0, X_1, \ldots, X_n]$ un ensemble de polynômes homogènes.*

On dit que l'ensemble $V(S) = \{x \in \mathbf{P}^n_{\mathbf{K}} / \forall P \in S,\ P(x) = 0\}$ est l'ensemble algébrique projectif défini par S.

Pour un ensemble algébrique projectif X, nous poserons $I(X)$ l'ensemble des polynômes homogènes de $\mathbf{K}[X_0, X_1, \cdots, X_n]$ nuls sur X. L'anneau $\mathbf{K}[X_0, X_1, \cdots, X_n]$ étant noethérien, on peut trouver un nombre fini de générateurs de $I(X)$.

On munit $\mathbf{P}^n_{\mathbf{K}}$ de la *topologie de Zariski* dont les ouverts sont les complémentaires des ensembles algébriques projectifs. Soit V un ensemble algébrique projectif, muni de la topologie induite. Pour tout polynôme homogène $P \in \mathbf{K}[X_0, X_1, \ldots, X_n]$, on note $D(P) = \{x \in V / P(x) \neq 0\}$: c'est un ouvert de V. De plus, tout ouvert de V est réunion fini d'ouverts de la forme $D(P)$.

Définition 2.1.2 *Un espace topologique X est dit irréductible si pour tous fermés F et G tels que $X = F \bigcup G$, on a $F = X$ ou $G = X$.*

Cette définition n'a d'intérêt que pour un espace topologique non séparé (tout espace séparé ayant plus d'un point n'est pas irréductible). En particulier, elle est utile pour les ensembles algébriques (projectifs mais aussi affines) munie de la topologie de Zariski. Par exemple l'ensemble affine $XY = 0$, réunion des fermés $X = 0$ et $Y = 0$, n'est pas irréductible. On peut le décomposer en réunion de deux ensembles irréductibles ($X = 0$ et $Y = 0$), et étudier chaque composante. On procède en général, comme pour cet exemple, en ramenant l'étude aux composantes irréductibles. Cela explique l'intérêt particulier porté aux espaces irréductibles. Rappelons qu'un ensemble algébrique est irréductible si et seulement si $I(X)$ est un idéal premier (sur l'irréductibilité en géométrie algébrique, voir [Per93]).

Définition 2.1.3 *On appelle variété projective tout espace annelé isomorphe à un espace annelé de type* $(V, \mathcal{O}_V)$ *où* V *est variété projective, et* $\mathcal{O}_V$ *le faisceau de fonctions qui à* $D(P)$ *associe l'ensemble des fonctions de la forme* G/P^r*,* G *et* P *étant des polynômes homogènes tels que* $degG = r\, degP$*.*

Pour plus précisions sur les espaces annelés et les faisceaux de fonctions consulter [Per93]. Il y est vérifié notamment qu'on peut se contenter de définir un faisceau sur une base d'ouverts, ici constituée des ouverts $D(F)$.

Pour toute variété projective X, on note $\mathbf{K}(X)$ le corps des *fonctions rationnelles* composé des fonctions du type f/g lorsque f et g sont des polynômes homogènes de $\mathbf{K}[X_0, \ldots, X_n]/I(X)$ de même degré avec $g \notin I(X)$, quotientées par la relation d'équivalence

$$f/g \sim f'/g' \Longleftrightarrow fg' - f'g \in I(X).$$

On nomme *courbe projective* toute variété projective de dimension 1

Pour éviter les points de rebroussement ou non réguliers, on définit :

Définition 2.1.4 *Soit* C *une courbe projective irréductible de* $\mathbf{P}^n$ *définie sur un corps* $\mathbf{K}$*. Soient* $P_1, \ldots, P_n$ *un système de générateurs de* $I(C)$*.*

On dit que C *est non singulière au point* $x \in C$ *si la matrice*

$$\left(\partial P_i/\partial X_j\,(x)\right)_{1\leq i\leq n,\, 0\leq j\leq n}$$

a pour rang $(n-1)$*.*

Une courbe est dite non singulière si elle l'est en tout point.

Seules de "bonnes" courbes nous intéressent ici. Aussi, afin de faciliter la lecture, on utilisera le raccourci suivant.

Convention 1 *Dans ce chapitre, la courbe* C *désigne une variété projective* C *définie sur un corps* $\mathbf{K}$ *, irréductible, non singulière et de dimension* 1*.*

On notera $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$. Pour tout corps $\mathbf{K}' \subset \overline{\mathbf{K}}$, $C(\mathbf{K}')$ désignera l'ensemble des points à coordonnées dans $\mathbf{K}'$ satisfaisant aux équations de C.

Soit P un point de la courbe de C. Posons $\mathcal{M}_P = \{f \in \mathbf{K}(C)/\ f(P) = 0\}$ et notons $\mathbf{K}[C]_P$ l'ensemble des fonctions rationnelles $F = f/g$ avec f et g homogènes de même degré, et $g \notin \mathcal{M}_P$. Les fonctions de $\mathbf{K}[C]_P$ sont dites *régulières* en P.

Définition 2.1.5 *La valuation v_P en P est l'application qui à toute fonction régulière en P associe $v_P(f) = \max\{d \in \mathbf{N} \bigcup \{\infty\} / \ f \in \mathcal{M}_P^d\}$.*

On prolonge v_P sur $K(C)$ en écrivant toute fonction rationnelle F comme le quotient f/g de deux fonctions régulières en P et en posant $v_P(F) = v_P(f) - v_P(g)$.

Définition 2.1.6 *On appelle uniformisante de C en P toute fonction $t \in \mathbf{K}(C)$ telle que $v_P(t) = 1$.*

Pour tout point $P \in C$, les corps $\mathbf{K}[C]_P/\mathcal{M}_P$ et $\mathbf{K}$ sont isomorphes par $f \mapsto f(P)$. Les uniformisantes de C en P sont donc les générateurs de $\mathcal{M}_P$. De plus, si t est une telle uniformisante, on peut développer toute fonction régulière en P en une série formelle du type $\sum_{i=0}^{\infty} a_i t^i$, les a_i étant des éléments de $\mathbf{K}$.

Pour pouvoir additionner les points d'une courbes, introduisons les diviseurs.

Définition 2.1.7 *On appelle diviseur sur la courbe C toute somme formelle*

$$\sum_{n_P \in C(\overline{\mathbf{K}})} n_P P,$$

la famille $\{n_P\}_P$ étant composée d'entiers rationnels presque tous nuls.

Le *degré* du diviseur D est l'entier $deg(D) = \sum_{P \in C(\overline{\mathbf{K}})} n_P$, son *support* est l'ensemble $Supp(D) = \{P \in C(\overline{\mathbf{K}}) / \ n_P \neq 0\}$. L'ensemble $Div(C)$ des diviseurs sur C forme un groupe (pour l'addition), admettant l'ensemble $Div^0(C)$ des diviseurs de degré 0 comme sous-groupe.

Définition 2.1.8 *On appelle diviseur principal tout diviseur de la forme*

$$(f) = \sum_{P \in C} v_P(f) P,$$

où v_P est la valuation en P et f est élément de l'ensemble $\overline{\mathbf{K}}(C)^{\times}$ des fonctions rationnelles non nulles de C.

L'ensemble $\mathcal{P}_C$ des diviseurs principaux forment un sous-groupe de $Div^0(C)$. Pour nos visées cryptographiques, seul le groupe des points nous intéresse. Aussi, nous assimilerons (abusivement) *la jacobienne* J de C au groupe quotient $Div^0(C)/\mathcal{P}_C$, et gardons cette appellation au cours de ce travail (en fait, la jacobienne d'une courbe est une variété).

On a défini les diviseurs sur $\overline{\mathbf{K}}$, regardons ce qu'il en est sur un corps quelconque.

Définition 2.1.9 *Un diviseur D est défini sur $\mathbf{K}' \subset \overline{\mathbf{K}}$ si $D^\sigma = D$ pour tout $\sigma \in Gal(\overline{\mathbf{K}}/\mathbf{K}')$.*

On note $Div_{\mathbf{K}'}(C)$ le groupe des diviseurs définis sur $\mathbf{K}'$, $Div^0_{\mathbf{K}'}(C)$ le sous-groupe des diviseurs de degré 0 définie sur $\mathbf{K}'$. La jacobienne $J_{\mathbf{K}'}$ de C sur $\mathbf{K}'$ sera ici, toujours abusivement, le sous-groupe des classes de J fixe par l'action de $Gal(\overline{\mathbf{K}}/\mathbf{K}')$.

Pour ces rappels sur les diviseurs, on peut consulter [Sil85], [Sam81] ou [Har77].

2.2 Jacobiennes généralisées, premières propriétés

Précisons avant tout la signification du terme *diviseurs étrangers à S* ; ce sont des diviseurs dont le support ne contient pas certains points choisis de la courbe C.

Définition 2.2.1 *Soit S un ensemble fini de points de la courbe C.*
Un diviseur D de $Div(C)$ est dit étranger à S s'il s'écrit

$$D = \sum_{P \in C \setminus S} n_P P \, ,$$

où la famille $\{n_P\}_{P \in C(\overline{\mathbf{K}}) \setminus S}$ est une famille presque nulle d'entiers rationnels.

Si S est un ensemble fini de points de la courbe C sur $\overline{\mathbf{K}}$, on notera respectivement $Div_S(C)$ et $Div^0_S(C)$ l'ensemble des diviseurs étrangers à S et l'ensemble des diviseurs de degré 0 étrangers à S : ils sont manifestement des sous-groupes additifs de $Div(C)$.

Définition 2.2.2 *Soit $S \subset C(\overline{\mathbf{K}})$ un ensemble fini de points de la courbe C.*
On appelle $\mathfrak{m}$ module de support S, la donnée, pour tout point P de S, d'un entier n_P strictement positif.

On peut considérer un module $\mathfrak{m}$ de support S comme un diviseur positif $\sum_{P \in S} n_P P$ de support S. On peut comparer les modules comme les diviseurs correspondants.

Définition 2.2.3 *Soient S et S' deux sous-ensembles finis de points de la courbe C, $\mathfrak{m}$ un module de support S, $\mathfrak{m}'$ un module de support S'.*

On note $\mathfrak{m}' \geq \mathfrak{m}$ si $S \subset S'$ et $n'_P \geq n_P$ pour tout point P de S.

La relation $\geq$ ainsi définie sur les modules de C est une relation d'ordre.

Définition 2.2.4 *Soient φ une fonction rationnelle sur C, et $\mathfrak{m}$ un module de support S. On note $\varphi \equiv 1 \pmod{\mathfrak{m}}$ si $\forall P \in S, v_P(1-\varphi) \geq n_P$.*

Nous noterons $\Gamma_{\mathfrak{m}}$ l'ensemble des diviseurs correspondant à ces fonctions :

Notation 1 *Pour tout module $\mathfrak{m}$ de support $S \subset C$, on pose*

$$\Gamma_{\mathfrak{m}} = \{(\varphi) : \varphi \in \overline{\mathbf{K}}(C) \text{ et } \varphi \equiv 1 \pmod{\mathfrak{m}}\}.$$

Constatons que si $\varphi \equiv 1 \pmod{\mathfrak{m}}$, le diviseur (φ) est étranger à S. L'ensemble $\Gamma_{\mathfrak{m}}$ apparaît donc comme un sous-groupe de $Div_S^0(C)$; on va pouvoir examiner le groupe quotient.

Définition 2.2.5 *Soit $\mathfrak{m}$ un module de support S. On appelle jacobienne généralisée associée à $\mathfrak{m}$ le groupe quotient $J_{\mathfrak{m}} = Div_S^0(C)/\Gamma_{\mathfrak{m}}$.*

Attention, cette définition ne peut être dissociée de la remarque suivante.

Remarque Il faut faire très attention avec la terminologie utilisée ici. N'ayant que des préoccupations cryptographiques, nous nous permettons cette approximation sur la terminologie des jacobiennes généralisées. Les "vraies" jacobiennes généralisées sont construites de manière à vérifier la propriété "universelle" suivante.

Proposition 2.2.6 *Pour tout module $\mathfrak{m}$, il existe un groupe algébrique T et une application rationnelle $f_{\mathfrak{m}} : C \longrightarrow T$ tels que :*

pour tout groupe commutatif G et toute fonction $f : C \longrightarrow G$ rationnelle, nulle sur $\Gamma_{\mathfrak{m}}$, il existe une unique factorisation rationnelle de T vers G du type :

$$\begin{array}{ccc} C & \xrightarrow{f} & G \\ f_{\mathfrak{m}} \downarrow & \nearrow & \\ T & & \end{array}$$

De plus $T \simeq J_{\mathfrak{m}}$.

Notons qu'ici les jacobiennes généralisées sont considérées en tant que groupe algébrique, c'est leur véritable nature. On montre alors qu'elles sont isomorphes en tant que groupe aux groupes quotients $Div_S^0/\Gamma_{\mathfrak{m}}$ [Ser59], d'où l'abus de langage utilisé au cours de cette thèse. Nous avons signaler que les jacobiennes généralisées peuvent être définies par la proposition 2.2.6. C'est le point de vue développé par Serre dans [Ser59]. Pour les propriétés "universelles" des jacobiennes on confère donc à [Ser59] mais aussi à [Ros54].

Les jacobiennes généralisées de même support apparaîssent comme quotient les unes des autres comme le décrit la proposition suivante.

Proposition 2.2.7 *Soient $\mathfrak{m}$ et $\mathfrak{m}'$ des modules de même support S tels que $\mathfrak{m}' \geq \mathfrak{m}$.*
On a alors la suite exacte :

$$0 \longrightarrow \Gamma_{\mathfrak{m}}/\Gamma_{\mathfrak{m}'} \longrightarrow J_{\mathfrak{m}'} \longrightarrow J_{\mathfrak{m}} \longrightarrow 0.$$

Ainsi, la connaissance des jacobiennes généralisées de module suffisamment grand suffit à déterminer toutes les jacobiennes généralisées. La démonstration de cette proposition est triviale dans la mesure où l'on ne considère les jacobiennes qu'en terme de quotient de groupes de diviseurs.

On a travailler jusqu'ici en travaillant sur $\overline{\mathbf{K}}$. Pour travailler sur $\mathbf{K}$, on utilise les diviseurs définis sur $\mathbf{K}$. Pour les modules –assimilables à des diviseurs positifs–, on utilisera la notion suivante.

Définition 2.2.8 *Soit $\mathbf{K}$ un corps parfait, admettant $\overline{\mathbf{K}}$ comme clôture algébrique. Notons $G = Gal(\overline{\mathbf{K}}/\mathbf{K})$ le groupe de Galois de $\overline{\mathbf{K}}$ sur $\mathbf{K}$.*

Un module $\mathfrak{m}$ est dit rationnel sur $\mathbf{K}$ si les coordonnées des points de son support sont algébriques sur $\mathbf{K}$ et si $m^\sigma = m$ pour tout $\sigma \in G$.

2.3 Structure des jacobiennes généralisées

Nous allons dans cette section construire une application d'une jacobienne généralisée dans la jacobienne de la courbe C. Elle s'avère être surjective, nous calculerons son noyau. Ce calcul se trouve dans [Ser59].

2.3.1 Construction de la suite $J_{\mathfrak{m}} \longrightarrow J \longrightarrow 0$

Afin d'harmoniser les notations, nous écrirons $\Gamma = \{(\varphi)/\varphi \in \overline{\mathbf{K}}(C)\}$ le groupe $\mathcal{P}_C$ des diviseurs principaux.

Considérons un module $\mathfrak{m}$ de support S. Le groupe $Div_S^0(C)$ s'envoie dans $Div^0(C)$ (par l'inclusion) puis dans J par passage au quotient. On peut ainsi construire la suite exacte

$$0 \longrightarrow \Gamma_S \longrightarrow Div_S^0(C) \longrightarrow J,$$

où le noyau Γ_S est le groupe des diviseurs principaux étrangers à S.

Pour toute classe de J, on peut considérer un représentant $D = \sum_P n_P P$ élément du groupe $Div^0(C)$. On peut trouver (par exemple en utilisant le théorème d'approximation des valeurs absolues décrit dans l'annexe A) $\varphi \in K(C)$ telle que

$$\forall P \in S, v_P(\varphi) = n_P.$$

Alors, $D-(\varphi)$ est élément de $Div_s^0(C)$ et appartient à la classe de D : l'application $Div_S^0(C) \longrightarrow J$ est surjective.

On obtient ainsi $Div_S^0(C)/\Gamma_S \simeq J$.

De $\Gamma_{\mathfrak{m}} \subset \Gamma_S$, on déduit la surjectivité de l'application

$$J_{\mathfrak{m}} = Div_S^0(C)/\Gamma_{\mathfrak{m}} \longrightarrow Div_S^0(C)/\Gamma_S \simeq J.$$

Notons $\psi_{\mathfrak{m}}$ la surjection de $J_{\mathfrak{m}}$ dans J exhibée ci-dessus.

La jacobienne J apparaît comme un groupe quotient de $J_{\mathfrak{m}}$; $J_{\mathfrak{m}}$ possède donc plus d'éléments que J. Cela laisse espérer que l'on peut trouver dans $J_{\mathfrak{m}}$ des éléments d'ordre plus grand que ceux de J, avec lesquels le logarithme discret serait intéressant. On va donc chercher à préciser la structure de $J_{\mathfrak{m}}$.

2.3.2 Description du noyau

Soit S un sous-ensemble fini de la courbe C. On veut examiner la structure d'une jacobienne généralisée $J_{\mathfrak{m}}$ associée au module $\mathfrak{m}$ de support S. Il s'agit en fait, par ce qui précède, d'étudier la suite exacte :

$$0 \longrightarrow L_{\mathfrak{m}} \longrightarrow J_{\mathfrak{m}} \xrightarrow{\psi_{\mathfrak{m}}} J \longrightarrow 0.$$

Par construction, $L_{\mathfrak{m}}$ est le noyau de l'application

$$Div_S^0(C)/\Gamma_{\mathfrak{m}} \longrightarrow Div_S^0(C)/\Gamma_S.$$

Donc $L_{\mathfrak{m}} = \Gamma_S/\Gamma_{\mathfrak{m}}$. Rappelons l'expression des ensembles en question

$$\begin{aligned} \Gamma_S &= \{(\varphi)/\varphi \in \overline{\mathbf{K}}(C)\ et\ \forall P \in S, v_P(\varphi) = 0\} \text{ et} \\ \Gamma_{\mathfrak{m}} &= \{(\varphi)/\ \varphi \in \overline{\mathbf{K}}(C)\ et\ \forall P \in S,\ v_P(1-\varphi) \geq n_P\}. \end{aligned} \tag{2.1}$$

Ils apparaîssent comme les ensembles des diviseurs principaux des fonctions des ensembles respectifs

$$\begin{aligned} U_S &= \{\varphi \in \overline{\mathbf{K}}/\ \forall P \in C,\ v_P(\varphi) = 0\} \text{ et} \\ U_{\mathfrak{m}} &= \{\varphi \in \overline{\mathbf{K}}(C)/\ \forall P \in S,\ v_P(1-\varphi) \geq n_P\}. \end{aligned} \tag{2.2}$$

On va chercher à ramener l'étude de $L_{\mathfrak{m}}$ sur les ensembles de fonctions. Pour comparer les points de vue, on considère la surjection $U_S \longrightarrow \Gamma_S$ qui a φ associe (φ). Elle induit une surjection $\Phi\ :\ U_S \longrightarrow \Gamma_S/\Gamma_{\mathfrak{m}} = L_{\mathfrak{m}}$ par passage au quotient.

Une fonction φ de U_S est dans le noyau de Φ si $(\varphi) \in \Gamma_{\mathfrak{m}}$, c'est à dire s'il existe $f \in U_{\mathfrak{m}}$ telle que $(\varphi) = (f)$ autrement dit si $\varphi = \lambda f$, où $\lambda \in \overline{\mathbf{K}}^{\times}$ et $f \in U_{\mathfrak{m}}$ (car $(g) = (f) \Leftrightarrow \forall P \in C, v_p(\frac{g}{f}) = 0$).

Au final, on obtient $L_{\mathfrak{m}} = U_S/\ (\overline{\mathbf{K}}^{\times} \times U_{\mathfrak{m}}\ )$. Il ne nous reste plus qu'à étudier les ensembles de fonctions U_S et $U_{\mathfrak{m}}$.

2.3.3 Étude avec les fonctions

Soit S un sous-ensemble fini de la courbe C, $\mathfrak{m}$ un module de support S. On va chercher à ramener l'étude du quotient $U_S/U_{\mathfrak{m}}$ à des études locales plus faciles à effectuer grâce au développement en série entière en l'uniformisante.

Pour tout $P \in S$, posons

$$U_P = \{\varphi \in \overline{\mathbf{K}}(C)/v_P(\varphi) = 0\}$$

l'ensemble des fonctions régulières en P et, si n_P est un entier naturel, posons

$$U_P^{(n_P)} = \{\varphi \in \overline{\mathbf{K}}(C)/v_P(1-\varphi) \geq n_P\}.$$

Si t est une uniformisante en P, une fonction de $U_P^{(n_P)}$ a donc, dans $\overline{\mathbf{K}}(C)_P$, un développement en série formelle du type

$$1 + at^{n_P} + bt^{n_P+1} + ct^{n_P+2} \dots\ ,$$

avec a, b, c, ... éléments de $\overline{\mathbf{K}}$.

Considérons un module $\mathfrak{m}$ de support S. L'ensemble $U_S = \bigcap_{P\in S} U_P$ des fonctions inversibles en tout point de S s'envoie sur $\prod_{P\in S}\left(U_P/U_P^{(n_P)}\right)$ diagonalement par $\Delta\ :\ x \mapsto (x, x, \ldots, x)$, le noyau étant $U_{\mathfrak{m}} = \bigcap_{P\in S} U_P^{(n_P)}$.

De plus, si $\{g_P\}_{P\in S} \in \prod_{P\in S} U_P$, par le théorème d'approximation des valeurs absolues, $\Delta(U_S) \bigcap \prod_{P\in S}\left(g_P + U_P^{(n_P)}\right) \neq \emptyset$: l'application diagonale de U_S dans $\prod_{P\in S}\left(U_P/U_P^{(n_P)}\right)$ est surjective.

On a obtenu la suite exacte :

$$1 \longrightarrow U_{\mathfrak{m}} \longrightarrow U_S \longrightarrow \prod\nolimits_{P\in S}\left(U_P/U_P^{(n_P)}\right) \longrightarrow 1.$$

On a atteint donc notre but : on n'a en effet plus qu'à étudier maintenant les quotients "locaux" $U_P^{(n_P)}$.

2.3.4 Étude de $U_P/U_P^{(n)}$

Soit P un point de la courbe C, n un entier strictement positif. Considérons une uniformisante t de C en P. Le groupe quotient $U_P/U_P^{(n)}$ admet comme système de représentants :

$$\sum_{i=0}^{n-1} a_i t^i \text{ avec } a_0 \in \overline{\mathbf{K}}^{\times} \text{ et } \forall i,\ a_i \in \overline{\mathbf{K}},$$

soit,

$$a_0(1 + \sum_{i=1}^{n-1} b_i t^i) \text{ où } b_i = a_i/a_0 \in \overline{\mathbf{K}} \text{ et } a_0 \in \overline{\mathbf{K}}^{\times}.$$

Remarquons au passage que $U_P/U_P^{(n)}$ est isomorphe au groupe $(\overline{\mathbf{K}}[[T]]^{\times} \pmod{T^n})$.

Notons $V_{(n)}$ le groupe multiplicatif composé des éléments $1 + \sum_{i=1}^{n-1} b_i t^i$ où les b_i sont des éléments de $\overline{\mathbf{K}}$, muni de la multiplication suivante :

$$(1 + \sum_{i=1}^{n-1} b_i t^i)(1 + \sum_{i=1}^{n-1} c_i t^i) = 1 + \sum\nolimits_{i=1}^{n-1} d_i t^i$$

avec $d_i = b_i + \sum_{j=1}^{i-1} b_{i-j} c_j + c_i$

On a donc $U_P/U_P^{(n)} \simeq \overline{\mathbf{K}}^{\times} \times V_{(n)}$.

2.3.5 Caractéristique 0

Il nous faut donc maintenant étudier le groupe multiplicatif $V_{(n)}$ composé des éléments de la forme $1 + \sum_{i=1}^{n-1} b_i X^i$. Pour cette section, nous suivrons encore le point de vue de [Ser59] (section V15 page 101). Nous travaillons dans le cas où $\mathbf{K}$ est de caractéristique 0. Dans ce cas, on peut définir la série formelle $\exp(X) = \sum_{k=0}^{\infty} \frac{X^k}{k!}$, et utiliser le lemme suivant.

Lemme 2.3.1 *Supposons que le corps* $\mathbf{k}$ *a pour caractéristique* 0*. Soient* n *un entier strictement positif,* $g(X)$ *un polynôme de* $\mathbf{k}[X]$ *de la forme* $1 + \sum_{i=1}^{n-1} b_i X^i$*.*

Il existe alors un unique $(n-1)$*-uplet* $(c_1, \ldots, c_{n-1})$ *de* $\mathbf{k}^{n-1}$ *tel que :*

$$g(X) \equiv \prod_{i=1}^{n-1} \exp(c_i X^i) \pmod{X^n}.$$

Démonstration
Cette proposition est évidente : en développant le produit d'exponentielle en série entière, on obtient pour X^i un coefficient du type $c_i + Q_i(c_1, \ldots, c_{i-1})$, $1 \leq i \leq n-1$, avec $Q_i \in \mathbf{k}[X]$, on peut ainsi calculer les c_i en remontant à partir de c_0 sous forme polynômiale des b_i. □

En appliquant le lemme avec $\mathbf{k} = \overline{\mathbf{K}}$, on arrive à exprimer $V_{(n)}$.

Proposition 2.3.2 *Supposons que le corps* $\mathbf{K}$ *ait pour caractéristique* 0*. Soit* n_P *un nombre entier strictement positif.*

L'application Φ *qui tout à un élément* g_P *du groupe* $(V_{(n_P)}; \times)$ *associe le* $(n_P - 1)$*-uplet* $(c_i)_{1 \leq i \leq n_P - 1}$ *du groupe* $(V_{(n_P)}; \times)$ *donné par le lemme 2.3.1 est un isomorphisme birégulier de groupe.*

Cette application est bien évidemment un morphisme de groupe car $\exp(c + c') = \exp(c)\exp(c')$. Elle est trivialement surjective, birégulière (les b_i s'expriment comme polynômes en les c_i et réciproquement), et injective (par le lemme).

Le groupe $U_S/U_{\mathfrak{m}}$ est donc isomorphe au groupe algébrique

$$\prod_{P \in S} \left(K^{n_P - 1} \times \overline{\mathbf{K}}^{\times} \right)$$

muni de la loi $\prod_{P \in S}(+; \times)$. Le sens

$$\begin{array}{ll} \prod_{P\in S}\left(\overline{\mathbf{K}}^{n_P-1}\times\overline{\mathbf{K}}^{\times}\right) & \longrightarrow \prod_{P\in S}\left(U_P/U_P^{(n_P)}\right) \longrightarrow U_S/U_{\mathfrak{m}} \\ \left((c_{P;i})_{1\le i\le n_P-1};d_P\right)_{P\in S} & \longmapsto \prod_{P\in S}\left(d_P\exp(c_{P;i}t_P^i \pmod{t_P^n})\right) \longmapsto g \end{array}$$

est ainsi explicite et programmable.

De même, pour tout $P \in S$, on peut trouver les d_P puis les $c_{P;i}$ tels que $g \in d_P \exp(c_{P;i}t_P^i)+U_P^{(n_P)}$ à l'aide d'un calcul formel. On peut donc programmer aussi le sens :

$$\begin{array}{rl} U_S \,/\, U_{\mathfrak{m}} & \longrightarrow \prod_{P\in S}(\overline{\mathbf{K}}^{n_P-1} \times \overline{\mathbf{K}}^{\times}) \\ g & \longmapsto ((c_{P;1}, c_{P;2}, \ldots, c_{P;n_P-1}; b)) \,. \end{array}$$

2.3.6 Caractéristique p

Supposons maintenant que le corps $\mathbf{K}$ est de caractéristique un nombre premier p. On ne peut plus travailler avec la fonction $\exp$ car $1/n!$ n'est pas défini si $n \geq p$. On va introduire une fonction E qui pourra jouer le même rôle, pour cela commençons par quelques rappels.

La fonction de Moebius μ est définie sur $\mathbf{N}$ par :

$$\begin{array}{rcl} \mu(n) & = & 0 \quad \text{si } \exists q \in \mathbf{N}\setminus\{0,1\}/\ q^2 \mid n, \\ \mu(\prod_{i=1}^k p_i) & = & (-1)^k \quad \text{si les } p_i \text{ sont des entiers premiers distincts,} \\ \mu(1) & = & 1. \end{array}$$

Rappelons aussi que si $n > 1$, $\sum_{d|n}\mu(d) = 0$.

Nous allons donc chercher à remplacer la fonction $\exp$. Pour cela on utilise la série formelle $\exp\left(-\sum_{i=0}^{\infty}\frac{X^{p^i}}{p^i}\right)$. Évidemment, on ne peut définir cette série que sur un corps de caractéristique nulle. On va donc se placer dans un tel corps et chercher à en trouver une autre expression.

Lemme 2.3.3 *Soit S la série formelle définie sur un corps de caractéristique 0 par $S(X) = \exp\left(-\sum_{i=0}^{\infty}\frac{X^{p^i}}{p^i}\right)$.*

Alors, $S(X) = \prod_{(n,p)=1}(1-X^n)^{\frac{\mu(n)}{n}}$.

Démonstration

De $\mu(1) = 1$ et, pour $n \geq 2$, $\sum_{d|n} \mu(d) = 0$, on peut déduire

$$\begin{aligned} -X &= \sum_{n=1}^{\infty} \frac{-X^n}{n} \sum_{d|n} \mu(d) \\ &= \sum_{d=1}^{\infty} \frac{\mu(d)}{d} \sum_{m=1}^{\infty} \frac{-X^{dm}}{m} \\ &= \sum_{d=1}^{\infty} \frac{\mu(d)}{d} \log(1 - X^d). \end{aligned} \tag{2.3}$$

L'image de cette égalité par $\exp$ donne

$$\exp(-X) = \prod_{n \in \mathbf{N}} (1 - X^n)^{\frac{\mu(n)}{n}}.$$

Par $(p^2|n \Rightarrow \mu(n) = 0)$, on peut écrire le produit sous la forme

$$\exp(-X) = \Big(\prod_{(n,p)=1} (1 - X^n)^{\frac{\mu(n)}{n}} \Big) \Big(\prod_{(m,p)=1} (1 - X^{pm})^{\frac{\mu(pm)}{pm}} \Big).$$

Définissons maintenant la série formelle $F(X) = \prod_{(n,p)=1} (1 - X^n)^{\frac{\mu(n)}{n}}$. De $((p, m) = 1 \Rightarrow \mu(pm) = -\mu(m))$, on obtient finalement

$$\exp(-X) = F(X)/F(X^p)^{\frac{1}{p}}.$$

Pour tout $N \in \mathbf{N}$,

$$\prod_{(n,p)=1 \text{et } n \leq N} (1 - X^{p^k n})^{\frac{\mu(n)}{n}}$$

a une série formelle du type

$$1 - X^{p^k}/p^k + \dots.$$

La série

$$F(X^{p^k})^{1/p^k} = \prod_{(n,p)=1} (1 - X^{p^k n})^{\frac{\mu(n)}{np^k}}$$

a donc un développement du type

$$1 - X^{p^k}/p^k + \sum_{i>p^k} a_i X^i \,,$$

les a_i étant des coefficients. Or, de l'équation (2.3.6), on déduit pour tout entier k

$$\begin{aligned} F(X) &= \exp(-X)F(X^p)^{1/p} \\ &= \exp(-X - \frac{X^p}{p})F(X^{p^2})^{1/p^2} \\ &= \dots \\ &= \exp(-\sum_{i=0}^{k} \frac{X^i}{p^i})F(X^{p^k})^{1/p^k}. \end{aligned} \tag{2.4}$$

Pour tout k, les p^k premiers termes des développements de $F(X)$ et $S(X)$ sont donc identiques ; par suite, $F(X) = S(X)$. □

Pour travailler avec $\exp\big(-\sum_{i=0}^{\infty} \frac{X^{p^i}}{p^i}\big)$ en caractéristique p, on utilisera $F(X) = \prod_{(n,p)=1} (1 - X^n)^{\frac{\mu(n)}{n}}$, qui est bien définie sur $\mathbf{K}$, au lieu de S.

De façon à transposer la propriété de morphisme de groupes de l'exponentielle, on va utiliser les vecteurs de Witt. Ils apparaissent pour la première fois dans un écrit de Witt [Wit36]. On peut les retrouver dans [AH28] et [Die57]. Nous suivons ici plutôt le point de vue de Demazure [Dem72], notamment pour la notation de la fonction suivante (cette notation n'est aucunement universelle).

Définition 2.3.4 *Soit R un anneau commutatif unitaire. Soit, pour n élément de $\mathbf{N}$, la fonction ϕ_n de R^{n+1} dans R^{n+1} définie par*

$$\phi_n\left((x_i)_{0\le i\le n}\right) = \sum_{i=0}^{n} p^i {x_i}^{p^{n-i}}$$

pour tout $(x_i)_{0\le i\le n} \in R^{n+1}$.

On peut alors définir la loi $\uplus$ qui, elle aussi, n'est nullement fixée sous cette notation.

Définition 2.3.5 *On appelle groupe des vecteurs de Witt relatif à p, de longueur infinie, pour un anneau R le groupe noté $W(R) = R^{\mathbf{N}}$ muni de la loi $\uplus$ suivante :*

Si $(a_i)_{i\in\mathbf{N}}$ et $(b_i)_{i\in\mathbf{N}}$ sont des éléments de $R^{\mathbf{N}}$, $(a_i)_{0\leq i\leq n} \uplus (b_i)_{0\leq i\leq n}$ est l'unique élément $(c_i)_{0\leq i\leq n}$ de $R^{\mathbf{N}}$ tel que :

$$\forall n \in \mathbf{N},\ \phi_n\left((a_i)_{0\leq i\leq n}\right) + \phi_n\left((b_i)_{0\leq i\leq n}\right) = \phi_n\left((c_i)_{0\leq i\leq n}\right). \tag{2.5}$$

L'élément somme est bien défini car la partie droite de l'équation (2.5) de rang n s'écrit $c_n + pc_{n-1}^p + p^2 c_{n-2}^{p^2} + \ldots + p^n c_0^{p^n}$. On peut donc calculer de proche en proche $\{c_n\}_{n\in\mathbf{N}}$.

Définition 2.3.6 *On appelle vecteur de Witt relatif à p, de longueur n, pour un anneau R commutatif unitaire, un vecteur de Witt défini précédemment tronqué aux $(n+1)$ premières coordonnées.*

En gardant le cadre de travail et les hypothèses de 2.3.5, on définit l'exponentielle de Artin-Hasse comme suit.

Définition 2.3.7 *On nomme exponentielle de Artin-Hasse la fonction qui à un vecteur de Witt x et un scalaire t associe*

$$E(x;t) = \prod_{n=0}^{\infty} F(x_n t^{p^n}),$$

où

$$F(X) = \prod_{(n,p)=1} (1 - X^n)^{\frac{\mu(n)}{n}}.$$

A l'image de l'exponentielle réelle – qui est un morphisme du groupe $(\mathbf{R};\ +)$ dans le groupe $(\mathbf{R}_+^*;\ \times)$ –, l'exponentielle de Artin-Hasse est un morphisme de monoïde de $(W(R);\ \uplus)$ dans $(R;\ \times)$, comme le dit la proposition suivante.

Proposition 2.3.8 *Soit R un corps commutatif. Alors,*

$$\forall (x;y) \in W(R), \forall t \in R,\ E(x \uplus y;t) = E(x;t)E(y;t).$$

Démonstration
Supposons tout d'abord que R est de caractéristique nulle. On a vu que dans ce cas $F(X) = \exp\big(-\sum_{i=0}^{\infty} \frac{X^{p^i}}{p^i}\big)$. Par la propriété de l'exponentielle, on peut donc écrire E sous la forme

$$E(X;t) = \exp\left(-\sum_{n=0}^{\infty} \frac{t^{p^n}\phi_n(X)}{p^n}\right).$$

Si x et y sont des vecteurs de Witt de $W(R)$, on déduit de cette expression et de la définition des vecteurs de Witt l'égalité $E(x;t)E(y;t) = E(x \uplus y;t)$.
Mais en fait $F(X) = \prod_{(n,p)=1} (1-t^n)^{\frac{\mu(n)}{n}}$. Par le principe de prolongement des identités, l'égalité trouvée $E(x;t)E(x;t) = E(x \uplus y;t)$ peut donc se regarder aussi dans un corps de caractéristique p, d'où le résultat. □

Les vecteurs de Witt permettent de travailler "comme en caractéristique 0", notamment E peut jouer le rôle de la fonction $\exp$. Ceci va nous permettre, comme en caractéristique 0, d'analyser $V_{(n)}$.

Théorème 2.3.9 *Supposons que* $\mathbf{K}$ *ait pour caractéristique le nombre premier* p*. Pour tout entier naturel* i *inférieur ou égal à* $n-1$ *et premier à* p*, on note* r_i *le plus petit entier* r *vérifiant* $ip^r \geq n$*.*

Si g *est élément de* $V_{(n)}$*, il existe une unique famille* $(x_i)_{(i,p)=1 \ et \ 1\leq i\leq n-1}$ *de vecteurs de Witt de longueur respectivement* r_i *pour* x_i *telle que :*

$$g(t) = \prod_{\substack{i=1 \\ (i,p)=1}}^{n-1} E(x_i;t^i).$$

La démonstration est similaire au cas vu en caractéristique 0, voir [Ser59] pour plus de détails.

On peut maintenant décrire $V_{(n)}$.

Proposition 2.3.10 *L'application de* $V_{(n)}$ *dans* $\prod_{i=1}^{n-1} W_{r_i}$ *qui à tout élément* g *de* $V_{(n)}$ *associe l'uplet* $(x_i)_{(i,p)=1 \ et \ 1\leq i\leq n-1}$ *déterminé par le théorème 2.3.9 est un ismorphisme de groupe birégulier.*

Conclusion En caractéristique p, le groupe $U_S/U_{\mathfrak{m}}$ est isomorphe au groupe algébrique :

$$G = \prod_{P \in S} \left(K^\times \times \prod_{\substack{i=1 \\ (i,p)=1}}^{n-1} W_{r_i} \right).$$

Comme dans le cas de la caractéristique 0, on peut programmer l'application inverse

$$U_S/U_{\mathfrak{m}} \longrightarrow G\ ,$$

ce sens inverse est donc lui aussi explicite et programmable.

2.3.7 Autre représentation de $U_S/U_{\mathfrak{m}}$

Nous avons précédemment cherché à exprimer $U_S/U_{\mathfrak{m}}$ sous forme de produit de groupes : une addition s'effectue alors rapidement composantes par composantes mais le passage à $U_S/U_{\mathfrak{m}}$ est délicat. D'où l'intêret de la proposition suivante.

Proposition 2.3.11 *Soient P un point de la courbe C, n un entier strictement positif, et t une uniformisante de C en P.*

Pour tout élément g de U_P, il existe une unique famille $(a_i)_{1\leq i\leq n-1}$ d'éléments de $\overline{\mathbf{K}}$ telle que :

$$g(t) \equiv \prod_{i=1}^{n-1}(1 + a_i t^i) \pmod{U_P^{(n)}}.$$

Remarques
1. On déduit trivialement les a_i de g par itération sur l'ordre des t^i, d'où l'existence et l'unicité demandées par la proposition. Il est très dur de les exprimer explicitement mais on peut programmer leurs constructions.
2. Cette fois, l'application $g \longrightarrow (a_i)_{1\leq i\leq n-1}$ n'est plus un morphisme de groupes, l'addition devient plus délicate.

Proposition 2.3.12 *Soient P un point de la courbe C, n un entier strictement positif, et t une uniformisante de C en P. Pour $(a_1,\, a_2,\, \ldots,\, a_{n-1}) \in \overline{\mathbf{K}}^{n-1}$, on pose*

$$M(a_1,\, a_2,\, \ldots,\, a_{n-1}) = \begin{pmatrix} 1 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ 0 & 1 & a_1 & \cdots & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & 0 & 1 & a_1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

L'application

$$g \longrightarrow \prod_{i=1}^{n-1}(1 + a_i t^i) \longrightarrow M(a_1,\, a_2,\, \ldots,\, a_{n-1})$$

est un isomorphisme du groupe $U_P/U_P^{(n)}$ sur le groupe multiplicatif

$$T_S^n = \{M(a_1,\, a_2,\, \ldots,\, a_{n-1}) \in \mathcal{M}_n(\overline{\mathbf{K}})/\ (a_1,\, a_2,\, \ldots,\, a_{n-1}) \in \overline{\mathbf{K}}^{n-1}\}.$$

La démonstration est évidente [Ser59] ; la proposition donne un isomorphisme de $U_S/U_{\mathfrak{m}}$ dans $\prod_{P\in S}\left(\overline{\mathbf{K}}^{\times} \times T_S^{n_P}\right)$: le passage de $U_S/U_{\mathfrak{m}}$ dans $\prod_{P\in S}\left(\overline{\mathbf{K}}^{\times} \times T_S^{n_P}\right)$ est plus facile (d'après ce qui précède) mais l'addition (dans le deuxième groupe) est un peu plus complexe. Cependant, ce n'est qu'un calcul matriciel (chose déjà bien implantée) : cette décomposition semble plus performante.

2.3.8 Bilan

Nous avons effectué une étude "sur les fonctions" du quotient $U_S/U_{\mathfrak{m}}$, mais notre objectif concernait les diviseurs, plus exactement le noyau $L_{\mathfrak{m}}$ de $J_{\mathfrak{m}} \longrightarrow J$. On a vu que $L_{\mathfrak{m}} \simeq U_S/\left(\overline{\mathbf{K}}^{\times} \times U_{\mathfrak{m}}\right)$.

On choisit un point $P \in S$.

On obtient finalement, $L_{\mathfrak{m}} \simeq V_{(n_P)} \times \prod_{Q\in S\setminus P}\left(\overline{\mathbf{K}}^{\times} \times V_{(n_Q)}\right)$ avec

$$(V_n, \times) \simeq \begin{cases} (\overline{\mathbf{K}}^{n-1}; +) \text{ en caractéristique } 0 \\ \text{ ou bien} \\ (\prod_{i=1}^{n-1} W_{r_i}, \uplus) \text{ en caractéristique } p \end{cases} \tag{2.6}$$

Nous avons étudier la suite exacte

$$0 \longrightarrow L_{\mathfrak{m}} \longrightarrow J_{\mathfrak{m}} \longrightarrow J \longrightarrow 0,$$

mais nous ne sommes pas en mesure d'en donner un relèvement. Nous ne pouvons donc pas représenter les classes de $J_{\mathfrak{m}}$ par des éléments de la jacobienne et du noyau. Nous chercherons donc un autre moyen pour les représenter.

Auparavant, nous allons regarder ce qui se passe sur le corps de base $\mathbf{K}$. Nous avons défini les jacobiennes généralisées avec les diviseurs construits sur la clôture algébrique $\overline{\mathbf{K}}$. Examinons ce qui se passe si l'on se limite aux diviseurs définis sur le corps de départ $\mathbf{K}$.

2.3.9 Descente sur le corps de base

Le but de cette sous-section est "d'abaisser" l'étude faites sur les jacobiennes généralisées définies sur la clôture $\overline{\mathbf{K}}$ au corps $\mathbf{K}$. Nous commencerons par des rappels d'algèbre homologique.

Tout d'abord, si G est un groupe, nous appellerons G module tout module sur l'anneau $\mathbf{Z}(G)$; un homomorphisme de G module sera un homomorphisme de $\mathbf{Z}(G)$ module. Pour tout ensemble A sur lequel G agit, on pose A^G l'ensemble des éléments de A fixe par G (i.e. $\sigma(x) = x$ pour tout $\sigma \in G$).

Définition 2.3.13 *Soit G un groupe.*

Un complexe de G module est une suite $\mathcal{C}$

$$\cdots \longrightarrow C_{p+1} \xrightarrow{\partial_{p+1}} C_p \xrightarrow{\partial_p} C_{p-1} \longrightarrow \cdots$$

de G modules C_p, indexée sur $\mathbf{N}$ ou sur $\mathbf{Z}$ avec des homomorphismes vérifiant pour tout p : $\partial_p \circ \partial_{p+1} = 0$, soit $Im\,\partial_{p+1} \subset Ker\,\partial_p$.

On ne demande pas à la suite d'être exacte, groupe quotient

$$H_p(\mathcal{C}) = Ker\,\partial_p / Im\,\partial_{p+1}$$

est à priori non nul. On l'appelle p-ème groupe d'homologie du complexe $\mathcal{C}$.

Un complexe de G module est dit libre si les G modules C_p sont tous libres.

Pour tous modules A, B, B', et tout homomorphisme $\beta : B \to B'$, on note $\beta^\sharp$ l'homomorphisme

$$\begin{array}{rccc} \beta^\sharp : & Hom_G(B', A) & \longrightarrow & Hom_G(B, A) \\ & f & \longmapsto & f \circ \beta. \end{array}$$

Proposition/Définition 2.3.14 *Soit G un groupe et $\mathcal{C}$ un complexe de G module.*
Pour tout G module A, la suite

$$\cdots \longrightarrow Hom_G(C_{p-1}, A) \xrightarrow{\partial_p^\sharp} Hom_G(C_p, A) \xrightarrow{\partial_{p+1}^\sharp} Hom_G(C_{p+1}, A) \longrightarrow \cdots$$

vérifie pour tout p : $\partial_{p+1}^\sharp \circ \partial_p^\sharp = 0$, soit $Im\,\partial_p^\sharp \subset Ker\,\partial_{p+1}^\sharp$.
On appelle $p$ème groupe de cohomologie de G avec A pour $\mathcal{C}$ le groupe quotient

$$Ker\,\partial_{p+1}^\sharp / Im\,\partial_p^\sharp.$$

Attention, la proposition n'affirme pas que la suite définie par les $\partial_p^\sharp$ est exacte, le quotient considéré est donc, ici aussi, à priori non nul.

Définition 2.3.15 *Soit G un groupe.*
On appelle complexe standard de G module tout complexe libre $\mathcal{C}$ de G module indexé sur $\mathbf{N}$ couplé avec un homomorphisme de G module

$$\varepsilon \ : \ C_0 \longrightarrow \mathbf{Z}$$

tel que

$$C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\varepsilon} \mathbf{Z} \longrightarrow 0$$

soit une suite exacte.

Pour les complexes standards, on montre la proposition suivante [Iya75].

Proposition 2.3.16 *Soient G un groupe, $\mathcal{C}$ et $\mathcal{C}'$ deux complexes standards de G module.*
Pour tout G module A, il existe une suite $\{\varphi_p\}_{p\in\mathbf{Z}}$ d'isomorphismes telle que le diagramme

$$\begin{array}{ccccccc}
\cdots \longrightarrow Hom_G(C_{p-1}, A) & \xrightarrow{\partial_p^\sharp} & Hom_G(C_p, A) & \xrightarrow{\partial_{p+1}^\sharp} & Hom_G(C_{p+1}, A) & \longrightarrow \cdots \\
\varphi_{p-1} \ \big| \wr & & \varphi_p \ \big| \wr & & \varphi_{p+1} \ \big| \wr & \\
\cdots \longrightarrow Hom_G(C'_{p-1}, A) & \xrightarrow{\partial'^\sharp_p} & Hom_G(C'_p, A) & \xrightarrow{\partial'^\sharp_{p+1}} & Hom_G(C'_{p+1}, A) & \longrightarrow \cdots
\end{array}$$

soit commutatif.

Il découle de ce diagramme commutatif que φ_p induit un isomorphisme entre $Im\,\partial_p^\sharp$ et $Im\,\partial'^\sharp_p$ d'une part, et entre $Ker\,\partial_{p+1}^\sharp$ et $Ker\,\partial'^\sharp_{p+1}$ d'autre part. Les groupes de cohomologie de G avec A sont donc identiques à isomorphisme près pour tout complexe standard, la définition suivante a donc un sens.

Définition 2.3.17 *Soit G un groupe, et A un G module.*

On appelle p-ème groupe de cohomologie de G avec A le groupe quotient noté $H^p(G,\ A)$ donné par

$$H^p(G,\ A) = Ker\,\partial^\sharp_{p+1}/\ Im\,\partial^\sharp_p\,,$$

pour un complexe (quelconque) $\mathcal{C}$ standard de G module.

Soit G un groupe. L'objectif de ce paragraphe est de construire, à partir d'un homomorphisme $\alpha\ :\ A \longrightarrow A'$ de G module, un homomorphisme de G module entre $H^p(G, A)$ et $H^p(G, A')$. Soit donc α un homomorphisme du G module A dans le G module A'. Pour tout G module C_p, on peut définir l'application

$$\begin{array}{rcl}\alpha_p : Hom(C_p, A) & \longrightarrow & Hom(C_p, A') \\ u & \longmapsto & \alpha \circ u,\end{array}$$

Alors, par construction, si $\mathcal{C}$ est un complexe de G module, le diagramme

$$\begin{array}{ccccccc}\cdots \longrightarrow Hom_G(C_{p-1}, A) & \xrightarrow{\partial^\sharp_p} & Hom_G(C_p, A) & \xrightarrow{\partial^\sharp_{p+1}} & Hom_G(C_{p+1}, A) & \longrightarrow \cdots \\ \alpha_{p-1}\ \downarrow & & \alpha_p\ \downarrow & & \alpha_{p+1}\ \downarrow & \\ \cdots \longrightarrow Hom_G(C_{p-1}, A') & \xrightarrow{\partial^\sharp_p} & Hom_G(C_p, A') & \xrightarrow{\partial^\sharp_{p+1}} & Hom_G(C_{p+1}, A') & \longrightarrow \cdots\end{array}$$

est commutatif. Par suite, α induit pour tout entier p un homomorphisme

$$\overline{\alpha_p}\ :\ H^p(G, A) \longrightarrow H^p(G, A').$$

Fort de cette construction, on peut décrire maintenant le passage d'une suite exacte de G module à leurs groupes cohomologiques. On peut montrer ce résultat en appliquant aux groupes $H^p(G,\ A)$ le "résultat cohomologique fondamentale" décrit dans [Per93], ou regarder la démonstration de [Iya75] (vue générale avec application au cas décrit ici).

Théorème 2.3.18 *Soit G un groupe. Considérons trois G module A, b, et C vérifiant la suite exacte d'homomorphismes de G module*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0.$$

Il existe alors des homomorphismes $\{\delta_p\}_{p\in\mathbf{N}}$ dit de connexion tels que l'on ait une suite exacte longue

$$\cdots \to H^p(G,\ A) \xrightarrow{\overline{f_p}} H^p(G,\ B) \xrightarrow{\overline{g_p}} H^p(G,\ C) \xrightarrow{\delta_p} H^{p+1}(G,\ A) \xrightarrow{\overline{f_{p+1}}} H^{p+1}(G,\ B) \to \cdots$$

Revenons à la définition 2.3.17 des groupes de cohomologie de G module. Nous allons chercher à déterminer ces groupes pour les petits degrés.

Soient pour cela un groupe G, un G module A, et un complexe standard de G module $\mathcal{C}$. On peut écrire par définition la suite exacte

$$C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\varepsilon} \mathbf{Z} \longrightarrow 0.$$

On en déduit la suite exacte

$$0 \longrightarrow Hom_G(\mathbf{Z},\, A) \xrightarrow{\varepsilon^\sharp} Hom_G(C_0,\, A) \xrightarrow{\partial_1^\sharp} Hom_G(C_1,\, A).$$

Par suite,

$$H^0(G,\, A) = Ker\, \partial_1^\sharp \simeq Hom_G(\mathbf{Z},\, A).$$

Nous supposerons désormais que le groupe G agit trivialement sur $\mathbf{Z}$. Rappelons que l'application $\Psi \;:\; u \mapsto u(1)$ est une injection de $Hom_G(\mathbf{Z},\, A)$ dans A (cela quelque soit l'action de G sur $\mathbf{Z}$). Mais, pour tout $u \in Hom_G(\mathbf{Z},\, A)$, $\sigma\, u(1) = u(\sigma\, 1) = u(1)$ pour tout élément σ de G. L'application Ψ est donc à valeurs dans A^G. Réciproquement, pour tout $a \in A^G$, l'application $n \mapsto na$ est élément de $Hom_G(\mathbf{Z},\, A)$. Ainsi, $Hom_G(\mathbf{Z},\, A) \simeq A^G$, et l'on connaît 0-ème groupe de cohomologie.

Proposition 2.3.19 *Soit G un groupe qui agit trivialement sur $\mathbf{Z}$, et soit A un G module.*

Le groupe de cohomologie de G de degré 0 est

$$H^0(G, A) = \{x \in A / \forall \sigma \in G,\, \sigma(x) = x\}.$$

Revenons à nos préoccupations principales. Nous avons étudier la suite exacte issue de $J_{\mathfrak{m}} \to J$, ces objet étant définis sur la clôture algébrique $\overline{\mathbf{K}}$ d'un corps $\mathbf{K}$. Pour proposer un logarithme discret, il est préférable de travailler avec un groupe fini (de toute façon il nous faut un élément g d'ordre fini). Il paraît donc plus approprié de travailler avec le sous-groupe $J_{\mathfrak{m}}^G$ des éléments de $J_{\mathfrak{m}}$ fixe par le groupe de Galois G de $\overline{\mathbf{K}}$ sur $\mathbf{K}$. Nous allons profiter des précédentes remarques sur la cohomologie pour déduire de la suite exacte sur $J_{\mathfrak{m}}$ la structure de $J_{\mathfrak{m}}^G$.

Dans cette sous-section nous travaillerons avec un corps $\mathbf{K}$ parfait, admettant le corps $\overline{\mathbf{K}}$ pour clôture algébrique. Notons $G = Gal(\overline{\mathbf{K}}/\, \mathbf{K})$ le groupe de Galois de $\overline{\mathbf{K}}$ sur $\mathbf{K}$. Nous utiliserons le théorème suivant décrit par Serre dans [Ser64]

Théorème 2.3.20 *Soient* $\mathbf{K}$ *un corps parfait,* $\overline{\mathbf{K}}$ *sa clôture algébrique et* $G = Gal(\overline{\mathbf{K}}/\,\mathbf{K})$ *le groupe de Galois de* $\overline{\mathbf{K}}$ *sur* $\mathbf{K}$.

Alors, pour tout groupe algébrique connexe L*,*

$$H^1(G, L) = 0.$$

Outre [Ser64], on peut trouver une démonstration de ce théorème dans [Lan56]. Notons que lorsque l'on travaille avec la topologie de Zariski, tout ensemble est connexe car cette topologie est séparée.

Nous travaillerons dans cette sous-section avec un module $\mathfrak{m}$ rationnel. Rappelons la suite exacte sur $\overline{\mathbf{K}}$

$$0 \longrightarrow L_{\mathfrak{m}} \longrightarrow J_{\mathfrak{m}} \longrightarrow J \longrightarrow 0.$$

Grâce au théorème 2.3.18, on en déduit

$$0 \to H^0(G,\, L_{\mathfrak{m}}) \to H^0(G,\, J_{\mathfrak{m}},) \to H^0(G,\, J) \to H^1(G,\, L_{\mathfrak{m}}) \to H^1(G,\, J_{\mathfrak{m}}) \to \cdots$$

Or, par 2.3.19,

$$\begin{aligned} H^0(G,\, L_{\mathfrak{m}}) &= L_{\mathfrak{m}}^G \\ H^0(G,\, J_{\mathfrak{m}}) &= J_{\mathfrak{m}}^G \\ H^0(G,\, J) &= J^G = J_{\mathbf{K}}. \end{aligned} \tag{2.7}$$

D'autre part, à l'aide du théorème 2.3.20, on sait que

$$\begin{aligned} H^1(G,\, L_{\mathfrak{m}}) &= 0 \\ H^1(G,\, J_{\mathfrak{m}}) &= 0 \\ H^1(G,\, J) &= 0. \end{aligned} \tag{2.8}$$

En reportant ces résultats dans (2.3.9), on déduit la proposition suivante.

Proposition 2.3.21 *Soit* $\mathbf{K}$ *un corps parfait, admettant* $\overline{\mathbf{K}}$ *pour clôture algébrique. Notons* $G = Gal(\overline{\mathbf{K}}/\,\mathbf{K})$ *le groupe de Galois de* $\overline{\mathbf{K}}$ *sur* $\mathbf{K}$.

Pour tout module rationnelle $\mathfrak{m}$*, la suite*

$$0 \longrightarrow L_{\mathfrak{m}}^G \longrightarrow J_{\mathfrak{m}}^G \longrightarrow J_{\mathbf{K}} \longrightarrow 0$$

est exacte.

Pour $\mathbf{K} = \mathbf{F}_q$ un corps fini, cette suite permet de connaître le cardinal de "la jacobienne généralisée fixe sous G" : $|J^G_{\mathfrak{m}}| = |L^G_{\mathfrak{m}}|\,|J_{\mathbf{k}}|$. Malheureusement, elle ne fournit toujours pas de relèvement et ne permet pas de représenter les éléments de $J^G_{\mathfrak{m}}$.

Nous voulions proposer un logarithme discret sur $J^G_{\mathfrak{m}}$. Or l'existence de cette suite exacte permet de transposer le logarithme discret aux groupes $L^G_{\mathfrak{m}}$ et $J_{\mathbf{K}}$, la complexité du problème du logarithme discret dans $J^G_{\mathfrak{m}}$ équivaut à celle de ces deux groupes [Cou01]. Bien que non optimal pour le logarithme discret, nous allons chercher à utiliser les jacobiennes généralisées pour d'autres applications cryptographiques. Il nous faut toujours trouver à les représenter pour pouvoir les manipuler. Pour cela, nous allons les traduire en terme d'idèle.

2.4 Traduction en termes d'idèles

Introduisons tout d'abord le vocabulaire utile.

Définition 2.4.1 *Un corps est dit corps global s'il est une extension finie de* $\mathbf{Q}$ *ou de* $\mathbf{k}(T)$*,* $\mathbf{k}$ *étant une extension finie d'un corps fini* $\mathbf{F}_q$*.*

Cela couvre les corps qui nous intéresse ; en effet les extensions quadratiques de $\mathbf{Q}$ et les corps de fonctions d'une courbe sur $\mathbf{F}_q$ sont des corps globaux. En fait, on peut considérer un corps global comme un corps de fonctions d'une variété sur $\mathbf{Q}$ ou sur $\mathbf{k}$.

Sur un corps algébriquement clos, un diviseur d'une courbe est une série formelle presque nulle de points de C. Lorsque le corps $\mathbf{K}$ sur lequel on considère C n'est pas algébriquement clos, on remplace la notion de point par celle de place. *Une place* v de C est une classe de conjugaison des points définis sur une clôture algébrique $\overline{\mathbf{K}}$ du corps $\mathbf{K}$ satisfaisant l'équation de C par le groupe de Galois $Gal(\overline{\mathbf{K}}/\,\mathbf{K})$. Un diviseur (v) associé à une place v est la somme de ses points. Pour tout $\sigma \in Gal(\overline{\mathbf{K}}/\,\mathbf{K})$, $(v)^\sigma = (v)$: le diviseur v est donc défini sur $\mathbf{K}$. Réciproquement, remarquons que tout diviseur défini sur $\mathbf{K}$ peut s'écrire sous la forme d'une somme presque nulle de places $\sum n_v(v)$. Ainsi, le degré $\deg(v)$ d'une place v est son cardinal.

De même, les entiers des modules rationnels vérifiant $n_p = n_P^\sigma$ pour tout $\sigma \in Gal(\overline{\mathbf{K}}/\,\mathbf{K})$, on peut définir ces modules en donnant les entiers n_v indexé sur les places.

Pour toute place v, on notera O_v le complété de $\mathbf{K}[C]_P$ par v_P où P est un point élément de v (le choix de P dans v est indifférent à isomorphisme près pour le résultat O_v de la complétion). C'est un anneau de valuation discrète (anneau principal ayant un unique idéal premier non nul). On notera indifféremment v la valuation associée (v prolonge v_P), et $\mathbf{K}_v$ le corps de fraction de O_v.

Définition 2.4.2 *Soit C une courbe définie sur un corps $\mathbf{K}$. Notons $\mathcal{V}$ l'ensemble de ses places.*

L'anneau $\mathbf{A_F}$ des adèles du corps $\mathbf{F} = \mathbf{K}(C)$ est le produit restreint $\prod'_{v\in V} \mathbf{K}_v$ de $\{\mathbf{K}_v\}_{v\in\mathcal{V}}$ par rapport à $\{O_v\}_{v\in\mathcal{V}}$, c'est à dire

$$\mathbf{A_F} = \{\{x_v\}_{v\in\mathcal{V}} \in \prod_{v\in\mathcal{V}} \mathbf{F}^v \,/\, x_v \in O_v \text{ pour presque tout } v\}.$$

Les composantes x_v d'une adèle vérifient donc $v(x_v) \geq 0$ pour presque tout v.

Proposition/Définition 2.4.3 *Soit C une courbe définie sur un corps $\mathbf{K}$, $\mathcal{V}$ l'ensemble de ses places, et $\mathbf{F} = \mathbf{K}(C)$ le corps de ses fonctions rationnelles.*

On appelle idèle toute adèle inversible. L'ensemble des idèles est un groupe, c'est le produit restreint de $\{\mathbf{F}_v\}_{v\in\mathcal{V}}$ par rapport à $\{O_v^\times\}_{v\in\mathcal{V}}$:

$$\mathbf{I_F} = \{\{x_v\}_{v\in\mathcal{V}} \in \prod_{v\in\mathcal{V}} \mathbf{F}^v \,/\, v(x_v) = 0 \text{ pour presque tout } v\}.$$

Nous travaillerons désormais avec $\mathbf{F}$ un corps global extension fini d'un corps $\mathbf{K}$ (qui est du type $\mathbf{Q}$ ou de $\mathbf{k}(T)$). Les idèles sont de valuation nulle presque partout, on peut associer à une idèle $\{x_P\}_P$ le diviseur $\sum_P v_P(x_P)P$. Notons U le noyau de ce morphisme de groupe. D'autre part, le groupe $\mathbf{F}^\times$ des inversibles de $\mathbf{F}$ s'envoie dans $\mathbf{I_F}$ par plongement diagonal. Notons $C_\mathbf{F}$ le groupe quotient $\mathbf{I_F} \,/\, \mathbf{F}^\times$, il s'appelle groupe de classe des idèles de F. Le groupe $\mathbf{K}^\times$ s'envoie aussi dans le groupe $\mathcal{P}_C$ des diviseurs principaux de C. Le groupe $C_\mathbf{F}$ s'envoie donc dans $Pic(C)$, notons Q le noyau de ce morphisme. Résumons par le diagramme commutatif suivant.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbf{K}^\times & \longrightarrow & \mathbf{F}^\times & \longrightarrow & \mathcal{P}_C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U & \longrightarrow & \mathbf{I_F} & \longrightarrow & Div(C) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & &
\end{array}$$

$$\begin{array}{ccccccc} 0 & \longrightarrow & Q & \longrightarrow & C_{\mathbf{F}} & \longrightarrow & Pic(C) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

Soit $\mathfrak{m}$ un module de support S. Associons lui le sous-groupe de U suivant

$$U_m = \{(x_v) \in U \,/\, \forall P \in S,\, v_P(1 - x_{v_p}) \geq n_P\}.$$

C'est aussi un sous-groupe de $C_{\mathbf{F}}$, le quotient $C_{\mathbf{F}} \,/\, U_m$ est nommé groupe de classe de rayon m. On a vu qu'il est isomorphe à la jacobienne généralisée J_m.

D'un autre coté, on peut associer à une idèle $\{x_v\}_{v \in calV}$ l'idéal $\prod_{v \in V} P_v^{v(x_v)}$ (toujours car $v(x_v) = 0$ presque partout). On peut donc chercher à quel groupe d'idéaux correspond un groupe de classe de rayon, c'est à dire une jacobienne généralisée. Introduisons pour cela la définition suivante [Cox89].

Proposition/Définition 2.4.4 *Soient* $\mathbf{F}$ *une extension finie de* $\mathbf{Q}$ *et* $f \in \mathbf{N}$. *Notons* $A_{\mathbf{F}}$ *l'anneau des entiers de* $\mathbf{F}$ *sur* $\mathbf{Z}$.

Il existe une extension abélienne maximale de $\mathbf{F}$ *telle que tout idéal principal de* $A_{\mathbf{F}}$ *engendré par* $\pi \equiv 1 \mod (fA_{\mathbf{F}})$ *se décompose complètement, elle est unique à isomorphisme près. Cette extension est appelé le corps de classe de rayon* f *de* $\mathbf{F}$.

Si $\mathbf{F}$ est une extension finie de $\mathbf{Q}$, et si f est un entier, on peut décomposer $fA_{\mathbf{F}}$ sous la forme

$$fA_{\mathbf{F}} = \prod_P \mathcal{M}_P^{n_P},$$

les n_P étant des entiers positifs presque tous nuls. On notera $\mathfrak{m}_f$ le module donné par ces n_P.

Comme on le verra dans le prochain chapitre, un ordre de F est un sous-anneau de l'anneau des entiers $A_{\mathbf{F}}$ engendrant F. Il est d'indice fini dans $A_{\mathbf{F}}$, cet indice est nommé le conducteur de l'ordre.

Pour déterminer les groupes de classes de rayon, on utilise la théorie du corps des classes qui construit un morphisme des idèles sur le groupe de Galois de l'extension [Iya75] (en associant à un idéal non ramifié le Frobenius de l'extension résiduelle). Dans le cas d'une extension quadratique imaginaire de $\mathbf{Q}$, on en déduit ce qui suit [Cox89].

Théorème 2.4.5 *Soient* $\mathbf{F}$ *une extension quadratique imaginaire de* $\mathbf{Q}$, $A_{\mathbf{F}}$ *l'anneau des entiers de* $\mathbf{F}$ *sur* $\mathbf{Z}$, A_f *un ordre de conducteur* f.

Le corps de classe H_f de rayon f a pour groupe de Galois le groupe de classe de rayon $\mathfrak{m}_f$. Il contient une sous-extension R_f telle que
$Gal(H_f/R_f) = (\mathbf{Z}/f\mathbf{Z})^\times / \mathbf{Z}^\times$ *et* $Gal(R_f/F)$ *est le groupe de classe de l'ordre* A_f.

Les jacobiennes généralisées apparaîssent donc comme le produit du groupe de classe d'un ordre et du groupe $(\mathbf{Z}/f\mathbf{Z})^\times / \mathbf{Z}^\times$. Pour le logarithme discret, on utilise le sous-goupe engendré par un élément. Plutôt que de travailler avec les jacobiennes généralisées, on doit donc se contenter de travailler avec le groupe de classe de l'ordre.

Chapitre 3

Sur les extensions quadratiques

Nous regardons dans ce chapitre les possibilités cryptographiques du groupe de classes d'un ordre d'une extension quadratique. Notre premier objectif est donc d'établir un algorithme de multiplication pour ce groupe. On se place pour cela dans une extension M/L de degré 2, où K est le corps des fractions d'un anneau factoriel A. Nous expliciterons quelques généralisations des corps quadratiques $\mathbf{Q}$: nous calculons l'anneau des entiers de L sur A, donnons une expression explicite des ordres de L, et exhibons un représentant "remarquable" d'une classe. Nous présentons alors un algorithme de multiplication des classes en utilisant ces représentants. Nous construisons de plus un procédé associant à chaque élément de la jacobienne de la courbe de corps de fonctions M un des ces éléments remarquables. Cette construction définit un isomorphisme de groupes. Nous finissons par des applications cryptographiques des groupes de classes d'un ordre.

3.1 Rappels d'algèbre et d'arithmétique

Nous avons besoin dans ce chapitre de quelques notions usuelles d'algèbre et d'arithmétique. Cette section sera consacrée à ces rappels élémentaires. On peut en trouver une description dans tout ouvrage traitant d'arithmétique élémentaire, mentionnons par exemple [Per81] et [Sam67].

Nous allons travailler avec un type d'anneau précis. Aussi,

Convention 2 *Nous désignerons désormais dans tout ce chapitre par le terme anneau un anneau commutatif unitaire.*

L'existence d'une unité pour la loi multiplicative permet de travailler avec les éléments inversibles ; avec la commutativité, l'ensemble de ces éléments inversibles forment un groupe commutatif. Ne pas oublier donc ce raccourci de vocabulaire pour toute application des propositions de ce chapitre.

Si A est un tel anneau, on notera $A^\times$ le groupe des éléments inversibles de A.

Définition 3.1.1 *Soient B un anneau, A un sous-anneau de B.*

Un élément de B est dit entier sur A s'il est racine d'un polynôme unitaire à coefficients dans A.

L'ensemble des éléments de B entier sur A forme un sous-anneau de A_B contenant A (lire par exemple [Sam67] section 2.1). Nous l'appellerons l'anneau des entiers de B sur A (nommé aussi fermeture intégrale de A dans B).

Définition 3.1.2 *Soit A un anneau.*

On dit que A est intégralement clos s'il est intègre et si l'ensemble des éléments du corps des fractions de A entiers sur A est A.

On peut définir la primalité sur un anneau comme suit.

Définition 3.1.3 *Soient A un anneau, $a \in A \setminus \{0\}$ et $b \in A$.*

On dit que a divise b et on note $a|b$ s'il existe un élément u dans A tel que $au = b$.

On dit que a et b sont premiers entre eux si

$$\forall c \in A \setminus \{0\}, \big((c|a \text{ et } c|b) \Longrightarrow c \in A^\times\big).$$

Deux éléments a et b de A vérifiant la relation de Bézout $ua + vb = 1$ où u et v sont des éléments de A sont premiers entre eux (car tout diviseur commun e avec $a = ec$ et $b = ed$ est inversible : $e(uc + vd) = 1$).

Rappelons comment généraliser la décomposition en nombres premiers dans **Z**.

Définition 3.1.4 *Soit A un anneau.*

Un élément p non nul de cet anneau est dit irréductible si

$$p \notin A^\times \text{ et } \big(p = ab \Longrightarrow (a \in A^\times \text{ ou } b \in A^\times)\big).$$

Remarquons que la relation $\mathcal{R}$ définie sur les éléments irréductibles par

$$p\mathcal{R}q \Longleftrightarrow \exists a \in A^{\times} / \, p = aq$$

est une relation d'équivalence. Elle partitionne l'ensemble des éléments irréductibles par des classes du type $A^{\times}p$, où p est un élément irréductible de A.

Définition 3.1.5 *L'anneau A est dit factoriel s'il est intègre et si tout élément non nul de A s'écrit de manière unique (à permutation près) comme produit d'un élément inversible et d'éléments irréductibles.*

Notons qu'un anneau principal (anneau intègre et dont tout idéal est engendré par un élément) est factoriel. Dans le cas d'un anneau factoriel A admettant 2 comme élément irréductible, nous dirons par commodité qu'un élément de A est pair si 2 intervient dans sa décomposition en éléments irréductibles, qu'il est impair dans le cas contraire.

Dans tout anneau factoriel A, on peut définir le $pgcd$ comme suit. On choisit un représentant dans chaque classe de $\mathcal{R}$. Soit $\mathcal{S}$ l'ensemble de ces représentants. Soient n un entier naturel et $\{a_i\}_{1\leq i\leq n}$ des éléments de A. Écrivons leurs décompositions en éléments irréductibles de $\mathcal{S}$: $a_i = u_i \prod_{j\in J_i} {p_j}^{n_{i,j}}$, avec $u_i \in A^{\times}$, $J_i \subset \mathcal{S}$ pour tout $i \in \{1, \ldots, n\}$. Leur $pgcd$ est alors :

$$pgcd(\{a_i\}_{1\leq i\leq n}) = \prod_{j\in \bigcup_{1\leq i\leq n} J_i} {p_j}^{inf\{n_{i,j}, 1\leq i\leq n\}}.$$

Comme sur les entiers, les $pgcd$ servent à l'étude de la primalité entre éléments.

Proposition 3.1.6 *Deux éléments sont premiers entre eux si et seulement si leur $pgcd$ est inversible.*

Présentons un type d'anneau qui nous sera utile.

Définition 3.1.7 *Un anneau A est dit euclidien s'il est intègre et muni d'un stathme euclidien c'est à dire d'une application $v : A \setminus \{0\} \longrightarrow \mathbf{N}$ telle que :*

$$\forall (a, b) \in (A \setminus \{0\})^2, \exists (q, r) \in A^2 / a = bq + r \text{ et } (r = 0 \text{ ou } v(r) < v(b)\,).$$

L'anneau $\mathbf{Z}$ est un anneau euclidien avec la valeur absolue $x \longmapsto |x|$ pour application v. C'est aussi le cas avec $\mathbf{K}[X]$, où $\mathbf{K}$ est un corps, muni de l'application $P \longmapsto \deg(P)$. On peut adapter l'algorithme d'Euclide sur $\mathbf{Z}$ à un anneau euclidien quelconque en donnant le rôle joué par la valeur absolue à l'application v ; ainsi, sur tout anneau euclidien, on est en possession d'un algorithme permettant de trouver le $pgcd$ de deux éléments (et donc de plusieurs).

Afin d'introduire les discriminants, donnons ces quelques rappels sur les modules.

Pour tout ensemble $\mathcal{A}$ et I, on note $\mathcal{A}^{(I)}$ l'ensemble des familles $\{a_i\}_{i\in I}$, indexées sur I, d'éléments de $\mathcal{A}$ presque tous nuls. Un module B est libre sur A s'il existe un ensemble I et une famille $\{e_i\}_{i\in I}$ d'éléments de B telle que l'application

$$\begin{array}{rl} \Phi \ : \ A^{(I)} & \longrightarrow B \\ \{a_i\}_{i\in I} & \longmapsto \sum_{i\in I} a_i e_i \end{array}$$

soit bijective. Une telle famille est alors appelée une base de B sur A. Le module B est de type fini sur A s'il existe une famille finie $\{e_i\}_{i\in I}$ d'éléments de B telle que l'application Φ définie ci-dessus soit surjective. Lorsque le module B est libre de type fini, toutes les familles finies rendant Φ surjective ont même cardinal $[B : A]$ nommé indice de B sur A. Si u est endomorphisme d'un module B libre et de type fini sur A, d'indice n, admettant $\{e_i\}_{1\leq i\leq n}$ comme base, il existe une unique famille $\{u_{i,j}\}_{i\in I}$ d'éléments de B telle que $u(e_j) = \sum_{1\leq i\leq n} u_{i,j}e_i$. La somme $\sum_{1\leq i\leq n} u_{i,i}$ ne dépend pas du choix de la base (même vérification que pour un corps), on la nomme la trace de l'endomorphisme u.

Définition 3.1.8 *Soient B un anneau, A un sous-anneau de B tel que B soit un module libre de type fini sur A, et soit x un élément de B.*

On appelle trace de x relativement à B et A, que l'on note $Tr_{B/A}(x)$, la trace de l'endomorphisme m_x multiplication par x.

Cette définition a bien un sens car $m_x \in End_A(B)$. Nous avons introduit la notion de trace pour définir la notion de discriminant.

Définition 3.1.9 *Soient B un anneau, A un sous-anneau de B tel que B soit un module libre de rang fini n sur A. Soit $(x_1, \ldots, x_n)$ un élément de B^n.*

On appelle discriminant du n-uplet $(x_1, \ldots, x_n)$ l'élément de A défini par $D(x_1, \ldots, x_n) = det\big(Tr_{B/A}(x_i x_j)\big)_{1\leq i,j\leq n}$.

Nous travaillerons avec un anneau A intègre, de corps de fraction L, et avec M une extension du corps L. Nous utiliserons des discriminants lorsque B est l'anneau des entiers de M sur A. On peut dans ce cas exprimer le discriminant sous la forme suivante.

Proposition 3.1.10 *Soient A un anneau intègre de corps des fractions L, M une extension finie de L, $B = A_M$ l'anneau des entiers de M sur A. Soit $n = [M : L]$ le degré de l'extension de M/L. Supposons l'existence de n isomorphismes distincts $\sigma_1, \ldots, \sigma_n$ de M dans une clôture algébrique L^{alg} de L ($\sigma_j \in Hom_L(M, L^{alg})$ pour tout j). Soit enfin $(x_1, \ldots, x_n)$ un élément de B^n.*

Alors, $D(x_1, \ldots, x_n) = det^2\big(\sigma_i(x_j)\big)_{1\leq i,j\leq n}$.

On trouve cette égalité grâce au fait qu'avec ces hypothèses, $Tr_{B/A}(y) = \sum_{i=1}^{n} \sigma_i(y)$ pour tout $y \in B$. Rappelons que l'hypothèse d'existence des isomorphismes est vérifiée si l'extension M/L est séparable.

Définition 3.1.11 *Soient A un anneau intègre de corps des fractions L, M une extension de L, $B = A_M$ l'anneau des entiers de M sur A. Supposons que B soit un module de type fini sur A.*

On appelle discriminant de B sur A l'idéal engendré par les discriminants des bases de M sur L contenues dans B.

Si $\{e_i\}_{1\leq i\leq n}$ et $\{f_i\}_{1\leq i\leq n}$ sont deux bases de M sur L contenues dans B (avec les notations de la définition précédente), de matrice de passage $(a_{i,j})$, les matrices $\big(Tr_{B/A}(f_p f_q)\big)$ et $\big(a_{p,i}\big)\big(Tr_{B/A}(e_i e_j)\big)^t\big(a_{q,j}\big)$ sont égales. On en déduit $D(f_1, \ldots, f_n) = det^2\big(a_{i,j}\big)\ D(e_1, \ldots, e_n)$. La matrice de passage est une matrice inversible, son déterminant est donc élément de $A^\times$. Le discriminant de B sur A est donc un idéal principal, engendré par n'importe quel discriminant d'une base de M sur L contenue dans B. Par abus de langage, on appellera discriminant de B sur A le discriminant d'une telle base.

De telles bases de M sur L contenues dans L existent, la démonstration de ce lemme montre comment en construire à partir d'une base quelconque de M sur L lorsque M/L est une extension finie.

Lemme 3.1.12 *Soient A un anneau intègre de corps des fractions L, M une extension finie de L, $B = A_M$ l'anneau des entiers de M sur A.*

Il existe une base de M sur L formée d'éléments de B.

Démonstration
Soit n la dimension de M sur L. Si f est un élément de M, la famille $(1,\ f,\ f^2,\ \ldots,\ f^n)$ est liée sur L, en multipliant par les dénominateurs on obtient une relation à coefficient dans A : $a_q f^q + a_{q-1} f^{q-1} + \ldots + a_0 = 0$, avec $a_q \neq 0$. L'élément ${a_q}^q f$ est racine du polymôme $X^q + a_{q-1}a_q X^{q-1} + \ldots + a_0 {a_q}^q \in A[X]$, il est donc élément de B. Soit $(f_1,\ \ldots,\ f_n)$ une base de M sur L. Pour tout i, on trouve comme précédemment un élément α_i non nul de A tel que $\alpha_i f_i \in B$. La famille $(\alpha_1 f_1,\ \ldots,\ \alpha_n f_n)$ est une base de M sur L incluse dans B. □

Finissons enfin par quelques rappels sur les idéaux.

Définition 3.1.13 *Soit A un anneau et soient I et J deux idéaux de A.*
On appelle produit de I et J, noté $I.J$, l'ensemble des éléments de la forme $\sum_{k\in E} a_k b_k$, avec E un ensemble fini et $(a_k, b_k) \in I \times J$ pour tout k dans E. C'est un idéal de A.
L'idéal I est dit inversible si il existe un idéal H de A tel que $I.H = A$.

Définition 3.1.14 *Soit A un anneau intègre, et K son corps des fractions.*
On appelle idéal fractionnaire de A tout ensemble de la forme αI, où α est un élément de K et I un idéal de A.

3.2 Entiers dans les extensions de degré deux

Nous voulons travailler sur les ordres d'une extension quadratique M/L, L étant donné comme le corps des fractions d'un anneau A. Nous aurons besoin de l'expression de l'ordre maximal c'est à dire de l'anneau des entiers A_M de M sur A. L'objectif de cette section est de donner la forme de cet anneau dans le cas où A euclidien.

3.2.1 Première caractérisation

Soient A un anneau intégralement clos, L son corps de fractions (noté aussi $frac(A)$), M une extension de degré 2 de L de la forme $M = L(\sqrt{\alpha})$, où α est un élément de L, et $\sqrt{\alpha}$ un élément de $M \supset L$ dont le carré est α. Notons que si L n'est pas de caractéristique 2, toute extension de degré 2 de L a la forme souhaitée. Soit A_M l'anneau des éléments de M entiers sur A. On peut résumer la situation par le diagramme d'inclusion :

$$\begin{array}{ccc} M = L(\sqrt{\alpha}\,) & \hookleftarrow & A_M \\ | \, 2 & & | \\ L = Frac(A) & \hookleftarrow & A \end{array}$$

La famille $(1\,,\sqrt{\alpha})$ est une famille libre (car $\sqrt{\alpha} \notin L$) donc est une base de M sur L. On peut donc définir σ l'automorphisme 'conjugué' de $Aut_L(M)$ par $\sigma(a+b\sqrt{\alpha}\,) = a - b\sqrt{\alpha}$, pour tout $(a,b) \in L^2$.

Considérons un élément x de A_M. Comme élément de M, on peut le mettre sous la forme $a+b\sqrt{\alpha}$, avec $(a,b) \in L^2$. Il est entier sur A, donc $\sigma(x)$ est entier sur A ainsi que $x+\sigma(x)$. Mais $x+\sigma(x) = 2a \in L$, donc, A étant intégralement clos, $2a \in A$. De même, $x\sigma(x)$ est entier (A_M est un anneau) sur A, et $x\sigma(x) = a^2 - \alpha b^2 \in L$, d'où $a^2 - \alpha b^2 \in A$. Réciproquement, si a et b sont des éléments de L tels que $2a \in A$ et $a^2 - \alpha b^2 \in A$, montrons que $y = a + b\sqrt{\alpha}$ est élément de A_M. Posons $P(X) = X^2 - 2aX + (a^2 - \alpha b^2)$, il est élément de $A[X]$ par hypothèse. Or $P(y) = (a+b\sqrt{\alpha}\,)^2 - 2a(a+b\sqrt{\alpha}\,) + (a^2 - \alpha b^2) = 0$, donc y est élément de A_M.

On en déduit le lemme suivant.

Lemme 3.2.1 *Soit A un anneau intégralement clos, L son corps de fractions, $M = L(\sqrt{\alpha}\,)$ une extension quadratique de L.*

L'anneau des éléments entiers de M sur A est l'ensemble

$$A_M = \{a + b\sqrt{\alpha}, (a,b) \in L^2 / \; 2a \in A \text{ et } a^2 - \alpha b^2 \in A\}.$$

Notons que ce résultat est valable avec pour seule hypothèse A intégralement clos (et commutatif, unitaire par convention), mais pour préciser A_M nous allons nous restreindre à des cas assez usuels.

3.2.2 Généralités pour un anneau factoriel en caractéristique différente de 2

On suppose ici que A est un anneau factoriel de caractéristique différente de 2. Soit $\mathcal{P}$ un ensemble contenant un représentant irréductible de chaque classe de $\mathcal{R}$ (définie sur les irréductibles de A).

Rappelons que l'on avait exprimé M sous la forme $L(\sqrt{d})$, $d \in L$. Mais $d = g/h$, avec $(g,h) \in A \times A^*$, et $M = L(\sqrt{d}) = L(\sqrt{gh}/h) = L(\sqrt{gh}\,)$. On peut décomposer gh dans A en $r^2\alpha$, $r \in A$ et α est un élément de A sans facteur carré.

On écrit ainsi M sous la forme $M = L(\sqrt{\alpha}\,)$, où $\sqrt{\alpha}$ est un élément dont le carré est $\alpha \in A$, α sans facteur carré. Remarquons qu'alors $\sqrt{\alpha}$ est zéro de $X^2 - \alpha \in A[X]$, aussi $\sqrt{\alpha} \in A_M$, et par suite $A[\sqrt{\alpha}\,] \subset A_M$.

Tout élément y de L s'écrit comme un quotient d'éléments de A que l'on peut décomposer en irréductibles de $\mathcal{P}$; aussi y s'écrit sous forme unique en $w \prod_{p\in\mathcal{P}} p^{n_p}$, $n_p \in \mathbf{Z}$, w étant un inversible de A. On pose usuellement $v_p(y) = n_p$. On appelle $v_p(y)$ la valuation de y en p.

Soit x un élément de A_M ; il s'écrit par le lemme précédent $a + b\sqrt{\alpha}$, $(a, b) \in L^2$, $2a \in A$ et $a^2 - \alpha b^2 \in A$ (car A factoriel implique A intégralement clos). Posons $u = 2a \in A$. Alors, $u^2 - \alpha(2b)^2 \in A$, et, $\alpha(2b)^2 \in A$. L'élément $2b$ étant élément de L, on peut considérer les valuations en tout irréductible :

$$\forall p \in \mathcal{P},\ v_p(\alpha) + 2v_p(2b) \geq 0. \tag{3.1}$$

Or α est sans facteur carré donc $\forall p \in \mathcal{P},\ v_p(\alpha) \in \{0, 1\}$. D'autre part $v_p(2b) \in \mathbf{Z}$, donc la condition (3.1) n'est possible que si $v_p(2b) \geq 0$ pour tout $p \in \mathcal{P}$. On en déduit que $2b \in A$. Posons $v = 2b \in A$. En réécrivant la condition $a^2 - \alpha b^2 \in A$, on arrive au lemme suivant.

Lemme 3.2.2 *Soit A un anneau factoriel de caractéristique différente de 2 . Soient L son corps des fractions, et M une extension quadratique de L. Soit $\alpha \in A$ sans facteur carré tel que $M = L(\sqrt{\alpha}\,)$.*

Tout élément de M entier sur A s'écrit $\frac{u}{2} + \frac{v}{2}\sqrt{\alpha}$ avec $(u, v) \in A^2$ tels que :

$$u^2 - \alpha v^2 \in 4A. \tag{3.2}$$

Sous ces condition, tout élément vérifiant (3.2) est racine du polynôme $X^2 - uX + (u^2 - \alpha v^2)/4$ donc en fait

$$A_M = \{\frac{u}{2} + \frac{v}{2}\sqrt{\alpha}, \forall (u, v) \in A^2 / \, u^2 - \alpha v^2 \in 4A\}.$$

3.2.3 Cas particuliers

Nous donnons maintenant une expression de l'anneau A_M des entiers sous diverses hypothèses.

On travaille encore dans le cas où A est un anneau factoriel en caractéristique différente de 2. Soient L le corps des fractions de A, et $M = L(\sqrt{\alpha}\,)$ une extension quadratique où α est un élément de A sans facteur carré ; A_M désigne l'anneau des entiers de M sur A.

Rappelons que $A[\sqrt{\alpha}\,] \subset A_M$. Nous utiliserons comme précédemment pour tout $x \in A_M$ ses écritures en $a+b\sqrt{\alpha}$ ou en $\frac{u}{2}+\frac{v}{2}\sqrt{\alpha}$ avec les conditions trouvées. Examinons plus en détails quelques cas.

- On suppose que 2 admet un inverse dans A.
  La condition (3.2) est alors triviale. Surtout, $a = u/2$ et $b = v/2$ sont éléments de A, donc $A_M \subset A[\sqrt{\alpha}\,]$. On arrive ainsi à énoncer :

  Si 2 admet un inverse dans A, l'anneau des entiers A_M est $A[\sqrt{\alpha}\,]$.

  C'est le cas pour tous les anneaux de polynôme $k[X]$, k étant un corps de caractéristique différente de deux.

- Supposons 2 irréductible dans A, et $\alpha \in 2A$.
  La condition (3.2) implique alors $u^2 \in 2A$. 2 étant irréductible, on en déduit $u \in 2A$. On tire maintenant de la condition (3.2) le fait $\alpha v^2 \in 4A$. Or $\alpha \in 2A$ (par hypothèse) est sans facteur carré donc $v_2(\alpha) = 1$ et par suite $v_2(v^2) \geq 1$. D'où $v \in 2A$ (2 irréductible), et $x \in A[\sqrt{\alpha}\,]$. Sachant $A[\sqrt{\alpha}\,] \subset A_M$, on conclut :

  Si 2 est irréductible, et si $\alpha \in 2A$, $A_M = A[\sqrt{\alpha}\,]$.

  Par exemple, pour $A = \mathbf{Z}[X]$, $\alpha = 2X$, on trouve que les éléments du corps $\mathbf{Q}(X,Y)/(Y^2 - 2X)$ entiers sur $\mathbf{Z}[X]$ sont les éléments de $\mathbf{Z}[X,Y]/(Y^2-2X)$. Ce type de corps apparaissent en géométrie algébrique comme corps des fonctions rationnelles d'une courbe (ici de la courbe d'équation $Y^2 - 2X = 0$).

- De façon plus générale, supposons juste 2 irréductible.
  Si $u \in 2A$, $\alpha v^2 \in 4A$ (par (3.2)) avec encore $v_2(\alpha) \leq 1$ (α sans facteur carré). Donc $v \in 2A$ (2 irréductible).
  Sinon, $v_2(u) = 0$, et la condition (3.2) implique $v_2(\alpha v^2) = 0$, avec $v_2(\alpha) \in \{0, 1\}$ et $v_2(v) \geq 0$. Donc $v_2(v) = 0$ et $v_2(\alpha) = 0$.
  Ce qui nous permet d'affirmer :

  Si 2 est irréductible, u et v sont de même parité. De plus, si A_M possède un élément du type $\frac{u}{2} + \frac{v}{2}\sqrt{\alpha}$, u et v étant non divisibles par 2, α n'est pas divisible 2.

  On retrouve par une autre voie avec la deuxième partie de cette assertion nulle autre chose que la contraposée du résultat précédent.

- Supposons maintenant $A = \mathbf{Z}$.
  Si u est impair, on a vu que v l'était aussi (car 2 est irréductible dans $\mathbf{Z}$). Alors $u^2 \equiv v^2 \equiv 1 \pmod 4$. La condition (3.2) amène donc

$\alpha \equiv 1 \pmod 4$. Notons qu'alors $x = \frac{u}{2} + \frac{v}{2}\sqrt{\alpha} = \frac{u-v}{2} + v\frac{1+\sqrt{\alpha}}{2} \in A[\frac{1+\sqrt{\alpha}}{2}]$ car u et v ont même parité. Réciproquement, si $\alpha \equiv 1 \pmod 4$, tout élément $x = \frac{u}{2} + \frac{v}{2}\sqrt{\alpha}$ avec u et v de même parité vérifie $x^2 - ux + \frac{u^2 - v^2\alpha}{4} = 0$ (tous les coefficients sont dans A) donc $x \in A_M$. En particulier pour $u = v = 1$, on trouve $[\frac{1+\sqrt{\alpha}}{2}] \in A_M$, donc $A_M = A[\frac{1+\sqrt{\alpha}}{2}]$.
Par contraposée, on obtient aussi que si $\alpha \not\equiv 1 \pmod 4$, u est pair, puis v est pair par ce qui précède, donc $A_M = A[\sqrt{\alpha}\,]$.
D'où le résultat :

Pour $A = \mathbf{Z}$, A_M est égale à $\mathbf{Z}[\frac{1+\sqrt{\alpha}}{2}]$ si $\alpha \equiv 1 \pmod 4$, et vaut $\mathbf{Z}[\sqrt{\alpha}\,]$ sinon.

Ce résultat est très classique. On peut le retrouver par exemple dans [Sam67].

- Soit maintenant A un anneau tel que $A/4A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \simeq \mathbf{Z}/4\mathbf{Z}$.
Si la classe de u modulo $4A$ est $\overline{1}$ ou $\overline{3}$, alors $u^2 \equiv 1 \pmod{4A}$ et la condition (3.2) implique v^2 est dans la classe $1 + 4A$ (car les carrés modulo $4A$ sont donc 0 ou 1). Par suite α est aussi dans $1 + 4A$.
Donc, si $\alpha \not\equiv 1 \pmod{4A}$, $u \in 2A$. Or α est sans facteur carré, donc $\alpha \notin 4A$, et $v^2 \in 2A$ (par (3.2)). Si de plus 2 est irréductible, on conclut comme précédemment :

Si A est tel que $A/4A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \simeq \mathbf{Z}/4\mathbf{Z}$ et si $\alpha \not\equiv 1 \pmod{4A}$, $A_M \subset A + A\sqrt{\alpha}/2$. Si de plus 2 est irréductible, $A_M = A[\sqrt{\alpha}\,]$.

Bien sûr, pour $A = \mathbf{Z}$, on retrouve la partie $\alpha \not\equiv 1 \pmod 4$ du cas précédent. L'anneau $\mathbf{Z}_2$ des entiers 2-adique vérifie les hypothèses demandées à A, et $3 \not\equiv 1 \pmod{4\mathbf{Z}_2}$. Ainsi l'anneau des entiers de $\mathbf{Q}_2(\sqrt{3})$ sur $\mathbf{Z}_2$ est $\mathbf{Z}_2[\sqrt{3}]$. Ce critère peut se généraliser comme suit.

- Soit $\mathcal{A}$ un anneau tel que $\mathcal{A}/4\mathcal{A} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \simeq \mathbf{Z}/4\mathbf{Z}$, posons $A = \mathcal{A}[X]$.
Soit α un polynôme de $A = \mathcal{A}[X]$ tel que son coefficient de plus haut degré non divisible par 4 ne soit congru pas à 1 modulo 4. Cela revient à demander que réduit modulo 4, $\overline{\alpha} \in (\mathcal{A}/4\mathcal{A})[X]$ ne soit pas unitaire.
On a vu qu'un élément entier de $L(\sqrt{\alpha}\,)$ est de la forme $\frac{u}{2} + \frac{v}{2}\sqrt{\alpha}$, avec u et v dans A c'est à dire des polynômes de $\mathcal{A}[X]$. Il vérifie de plus
$u^2 - \alpha v^2 \in 4A = 4\mathcal{A}[X]$. Réduisons modulo 4, dans $(\mathcal{A}/4\mathcal{A})[X]$:

$$\overline{u}^2 - \overline{\alpha}\,\overline{v}^2 \equiv 0 \tag{3.3}$$

Or, $\overline{u}$ s'écrit

$$\sum_{k=0}^{d} \overline{u_k} X^k,$$

les $\overline{u_k}$ étant éléments de $\mathcal{A}/4\mathcal{A}$. Mais

$$\overline{u}^2 = \sum_{k=0}^{d} \overline{u_k}^2 X^{2k} + \sum_{0 \le i < j \le d} 2\overline{u_i}\,\overline{u_j} X^{i+j}.$$

Si $\overline{u_d}$ est dans la classe $2 + 4\mathcal{A}$, $\overline{u_d}^2 \equiv 0$ et $2\overline{u_d}\,\overline{u_i} \equiv 0$. Le terme de plus haut degré de $\overline{u}^2$ dans $(\mathcal{A}/4\mathcal{A})[X]$ est donc $\overline{u_n}^2 X^{2n}$, où n est le plus grand entier k tel que $\overline{u_k} \in \{1+\mathcal{A}, 3+\mathcal{A}\}$. De même, le terme de plus haut degré de $\overline{v}^2$ dans $(\mathcal{A}/4\mathcal{A})[X]$ est $\overline{v_m}^2 X^{2m}$, où m est le plus grand entier k tel que $\overline{v_k} \in \{1+\mathcal{A}, 3+\mathcal{A}\}$. Notons enfin $\overline{\alpha_r} X^r$ le terme de plus haut degré non nul de $\overline{\alpha}$, par hypothèse $\alpha_r \not\equiv 1 \pmod{4\mathcal{A}}$.
Reprenons l'équation (3.3), et examinons le terme de plus haut degré de $\overline{u}^2 - \overline{\alpha}\,\overline{v}^2$.
Si $2n > r + 2m$, ce terme est $\overline{u_n}^2 X^{2n}$. Par (3.3), ${u_n}^2$ doit appartenir à $4\mathcal{A}$, ce qui est faux car $\overline{u_k} \in \{1+\mathcal{A}, 3+\mathcal{A}\}$.
Si $2n < r+2m$, ce terme est $\overline{\alpha_r}\,\overline{v_m}^2 X^{2m+r}$. Par (3.3), $\alpha_r {v_m}^2$ doit appartenir à $4\mathcal{A}$. Or $\overline{v_m} \in \{1+\mathcal{A}, 3+\mathcal{A}\}$, d'où $\overline{v_m}^2 \equiv 1 \pmod{4\mathcal{A}}$, $\alpha_r {v_m}^2 \in 4\mathcal{A}$ implique donc $\alpha_r \in 4\mathcal{A}$, ce qui impossible par définition de r.
Donc $2n = r - 2m$, le terme de plus haut degré est $(\overline{u_n}^2 - \overline{\alpha_r}\,\overline{v_m}^2)X^{2n}$. L'équation (3.3) implique ici $\overline{u_n}^2 - \overline{\alpha_r}\,\overline{v_m}^2 \equiv 0$, mais on a vu que $\overline{v_m}^2 \equiv 1 \pmod{4\mathcal{A}}$ et de même, $\overline{u_n}^2 \equiv 1 \pmod{4\mathcal{A}}$. On aboutit à $1 - \overline{\alpha_r} \equiv 0 \pmod{4\mathcal{A}}$, ce qui contredit l'hypothèse sur α.
Par suite, tous les coefficients de u et v sont dans $2 + 4\mathcal{A}$ ou $4\mathcal{A}$, c'est à dire que u et v sont divisibles par 2. Donc $A_M = A[\sqrt{\alpha}\,]$.

Soit $\mathcal{A}$ un anneau tel que $\mathcal{A}/4\mathcal{A} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \simeq \mathbf{Z}/4\mathbf{Z}$. Posons $A = \mathcal{A}[X]$. Soit α un polynôme de $A = \mathcal{A}[X]$ tel que son coefficient de plus haut degré non divisible par 4 ne soit pas congru à 1 modulo 4. Notons $M = \mathrm{frac}(A)(\sqrt{\alpha}\,)$.
Alors, l'anneau des entiers de M sur A est $A_M = A[\sqrt{\alpha}\,]$.

Notons qu'on peut appliquer ce critère pour $A = \mathbf{Z}[X]$, ou pour l'anneau $\mathbf{Z}_2[X]$ des polynômes dont les coefficients sont des entiers 2-adiques.

3.2.4 Expression à l'aide du discriminant

Soient A un anneau factoriel, L le corps de fractions de A, et $M = L(\sqrt{\alpha}\,)$ une extension quadratique de L où α est un élément de A sans facteur carré.

On va calculer le discriminant Δ de A_M sur A. On exprimera ensuite M et A_M à l'aide de Δ et A uniquement.

L'isomorphisme identité $Id : x \mapsto x$ et l'isomorphisme conjugué σ défini par $\sigma(1) = 1$ et $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$ donnent deux isomorphismes distincts de $Aut_L(M)$. On peut donc calculer le discriminant de A_M sur A dès que l'on connait une base de M sur K contenue dans A_M.

Dans les cas où $A_M = A[\sqrt{\alpha}]$, le discriminant de A_M sur A est $\Delta = 4\alpha$.

Dans le cas où $A = \mathbf{Z}$ et $\alpha \equiv 1 \pmod 4$, le discriminant de A_M est $\Delta = \alpha$.

Remarquons que dans tous ces cas décrits dans la sous-section 3.2.3, on peut exprimer donc M et A_M sous la forme

$$M = L(\sqrt{\Delta}) \text{ et } A_M = A + (\frac{\Delta + \sqrt{\Delta}}{2})A. \tag{3.4}$$

3.3 Précisions sur les ordres

Pour cette section, A est un anneau intègre de caractéristique différente de 2, de corps des fractions L, M est une extension finie de L, A_M est l'anneau des éléments de M entiers sur A.

Nous définissons dans une première sous-section un ordre et calculons son expression. Lors de la sous-section suivante, nous donnons une construction de son groupe de classes et trouvons une représentation remarquable de ce groupe grâce aux idéaux primitifs.

3.3.1 Définition et expression d'un ordre

Définition 3.3.1 *Soit M un corps contenant le corps des fractions L d'un anneau A.*

On appellera ordre de M sur A tout sous-anneau unitaire de M contenant une base de M sur le corps $L = frac(A)$ et qui est un A-module de type fini.

Dans la suite, nous nous limiterons à examiner des ordres sur l'anneau A, aussi nous écrirons ordre de M pour ordre de M sur A. Nous nous contentons de plus d'examiner les ordres dans les extensions de degré deux. Les ordres des extensions quadratiques de $\mathbf{Q}$ sont connus de façon explicite ([Can87] ou [Coh95]). Nous allons essayer de calculer explicitement leurs expressions pour toute extension de degré deux.

Proposition/Définition 3.3.2 *Soit M une extension de degré 2 du corps L des fractions d'un anneau A de caractéristique différente de 2.*

Tout ordre de M est inclus dans A_M ; il y est d'indice fini f. Il s'écrit $A+fA_M$. L'entier naturel f est appelé le conducteur de l'ordre en question.

Soit Θ un ordre de M sur A. Un élément de Θ avec torsion sur A est un élément de M avec torsion. Mais le corps M est intègre donc n'a pas d'élément avec torsion. L'ordre Θ est donc un A module libre. Si l'extension M sur L est quadratique, l'ordre Θ a au moins pour rang 2 car il contient une base de M sur L, et son rang est en fait 2 car de toute famille d'au moins trois éléments, la décomposition de ces éléments dans la base de M sur L permet, en multipliant par un dénominateur convenable, d'écrire une combinaison linéaire nulle sur A ; une telle famille ne peut être libre.

L'ordre Θ s'écrit donc $A\alpha+A\beta$, $(\alpha,\beta)\in M^2$ étant libre sur A. L'appartenance de 1 et α^2 à Θ permet de trouver $(n,m,n',m')\in A^4$ tels que :

$$\begin{aligned} 1 &= n\alpha + m\beta \text{ et} \\ \alpha^2 &= n'\alpha + m'\beta. \end{aligned} \tag{3.5}$$

En multipliant la première relation par α, la seconde par n, avec une "réorganisation" des termes, on obtient :

$$\begin{aligned} \alpha - m\alpha\beta &= n\alpha^2 \\ &= nn'\alpha + nm'\beta. \end{aligned} \tag{3.6}$$

De plus $\alpha\beta\in\Theta$ donc on peut trouver $(r;t)\in A^2$ tels que $\alpha\beta = r\alpha + t\beta$. D'où,

$$\begin{aligned} (1-nn')\alpha - nm'\beta &= m\alpha\beta \qquad \text{(en ordonnant (3.6))} \\ &= mr\alpha + mt\beta. \end{aligned} \tag{3.7}$$

La famille (α,β) étant libre sur A,

$$\begin{aligned} mr + nn' &= 1 \qquad & m \text{ est premier avec } n, \\ mt + nm' &= 0 \qquad & m \text{ divise donc } m'. \end{aligned} \tag{3.8}$$

On reprend les décompositions initiales de 1 et α^2 dans (α,β) :

$$\begin{aligned} m\alpha^2 &= mn'\alpha + m'm\beta \\ &= (mn'-m'n)\alpha + m' \qquad \text{en utilisant l'équation (3.5).} \end{aligned} \tag{3.9}$$

On en tire donc $\alpha^2 = (n' - n\frac{m'}{m})\alpha + \frac{m'}{m}$ où $\frac{m'}{m} \in A$: α est entier.

Un raisonnement symétrique donne β entier : $\Theta = A\alpha + A\beta$ est donc inclus dans l'anneau des entiers.

On sait que A_M et Θ sont des A modules libres de rang 2 avec $\Theta \subset A_M$, donc Θ est d'indice fini f dans A_M ($f = |A_M/\Theta|$ par définition). Alors, $A + fA_M$ est un A module libre de rang 2 contenant A, inclus dans l'ordre Θ et d'indice f dans A_M donc c'est Θ.

Pour peu que l'on connaisse une expression de A_M, on peut préciser la forme de l'ordre, comme dans le cas ci-dessous.

Corollaire 3.3.3 *Soit M une extension de degré 2 du corps des fractions L d'un anneau A de caractéristique différente de 2. Notons A_M l'anneau des éléments entiers de M sur A.*

Si A_M/A a Δ pour discriminant et vérifie (3.4),
l'unique ordre de conducteur f est

$$A_{\Delta_f} = A + \frac{\Delta_f + \sqrt{\Delta_f}}{2} A$$

avec $\Delta_f = f^2\Delta$. L'élément Δ_f est alors appelé le discriminant de l'ordre A_{Δ_f}.

Dans ce cas, $A + fA_M = A + f(A + \frac{\Delta+\sqrt{\Delta}}{2}A) = A + \frac{f\Delta+f\sqrt{\Delta_f}}{2}A$. Or f étant un entier naturel, $f^2\Delta \equiv f\Delta \pmod{2A}$ (séparer les cas f pair et f impair). Le résultat est alors immédiat.

3.3.2 Groupe de classes d'un ordre

Regardons à présent des sous-ensembles intéressants des ordres : les idéaux. Dans un anneau de Dedekind, les idéaux fractionnaires sont inversibles et forment ainsi un groupe. En général, on utilise plutôt le groupe quotient des idéaux fractionnaires par les idéaux principaux. Ce groupe quotient est appelé groupe de classes de l'anneau en question. Un ordre n'est pas forcément de Dedekind, mais en se limitant à des idéaux bien choisis, on peut aussi construire un groupe des classes.

Définition 3.3.4 *Soit M un corps contenant le corps des fractions L d'un anneau intègre A, et soit Θ un ordre de M.*

Un idéal I de l'ordre Θ est dit propre si

$$\forall \beta \in M,\ \beta I \subset I \Longrightarrow \beta \in \Theta.$$

Une démonstration élémentaire montre que tout idéal inversible d'un ordre est propre, quelque soit la forme de l'extension M/L : si $\beta \in M$ est tel que $\beta\mathfrak{a} \subset \mathfrak{a}$ et si $\mathfrak{b}$ est l'inverse de $\mathfrak{a}$, alors $\beta\Theta = \beta\,\mathfrak{ab} = (\beta a)\,\mathfrak{b} \subset \mathfrak{ab} \subset \Theta$, $\mathfrak{a}$ est bien propre.

On suppose dorénavant que A est factoriel, que M/L est de degré 2 et vérifie (3.4). On désigne par Δ le discriminant de A_M/A. On se limitera ici à l'étude des ordres dont le conducteur f vérifie

$$\forall b \in A,\ b^2 \equiv f^2\Delta \pmod{4A} \Longrightarrow b \equiv f\Delta \pmod{2A}. \tag{3.10}$$

Remarquons que cette condition est automatiquement vérifiée si f est pair, et qu'elle l'est pour tous les ordres des anneaux, où, parmi les exemples de 3.2, on a pu donner une expression explicite de A_M.

Nous utiliserons pour cela la notation $\langle \alpha, \beta \rangle$ pour désigner l'idéal $\alpha A + \beta A$.

Lemme 3.3.5 *Soient A un anneau factoriel de caractéristique différente de 2 de corps des fractions L et M une extension de degré 2 de L. Notons Δ le discriminant de A_M/A.*

Soit $g(X) = aX^2+bX+c$ une forme quadratique où les coefficients a, b, c sont dans A et premiers entre eux, telle que son discriminant $D = b^2 - 4ac$ n'admette pas de racine carrée dans A. Alors, si $\tau \in M$ est un zéro de $g(X)$,

(i) *L'ensemble $\langle a, a\tau \rangle$ est un idéal propre de l'ordre $\langle 1, a\tau \rangle$.*

(ii) *si M/L vérifie (3.4), lorsque l'on choisit la forme quadratique g telle que son discriminant s'écrit $D = f^2\Delta$ avec f entier naturel vérifiant (3.10), l'ordre $\langle 1, a\tau \rangle$ a pour conducteur f.*

Démonstration

(i) L'anneau $\langle 1, a\tau \rangle$ est manifestement un ordre de M sur A contenant l'idéal $\langle a, a\tau \rangle$. De plus, pour tout élément $\beta \in M$,

$$\begin{aligned} \beta \langle\, a\ ,\ a\tau \,\rangle \subset \langle\, a\ ,\ a\tau \,\rangle &\Longleftrightarrow \exists (n,m) \in A^2 / \begin{cases} \beta = m + n\tau \\ \beta\tau = m\tau + n\tau^2 \end{cases} \\ &\Longleftrightarrow \exists (n,m) \in A^2 / \begin{cases} \beta = m + n\tau \\ \beta\tau = -\frac{cn}{a} + (\frac{bn}{a} + m)\tau. \end{cases} \end{aligned} \tag{3.11}$$

Or les éléments a, b et c sont premiers entre eux et $\tau \notin A$, donc,

$$\beta\tau \subset \langle\ 1\ ,\ \tau\ \rangle \Longleftrightarrow \exists (n,m) \in A^2 / \begin{cases} \beta = m + n\tau \\ a \mid n. \end{cases}$$

D' où,

$$\forall \beta \in K, \quad \beta\langle\ a\ ,\ a\tau\ \rangle \subset \langle\ a\ ,\ a\tau\ \rangle \Longleftrightarrow \beta \in \langle\ 1\ ,\ a\tau\ \rangle.$$

(ii) Rappelons que

$$\begin{aligned} a\tau &= \frac{-b + f\sqrt{\Delta}}{2} \\ &= -\frac{b + f\Delta}{2} + f\frac{\Delta + \sqrt{\Delta}}{2}. \end{aligned} \tag{3.12}$$

Or f vérifie (3.10) et $f(fd_K) = b^2 - 4ac$, donc $b \equiv f\Delta \pmod{2A}$.
Par conséquent,

$$-\frac{b + f\sqrt{\Delta}}{2} \in A$$

et,

$$\langle\ 1\ ,\ a\tau\ \rangle\ =\ \langle\ 1\ , f\frac{\Delta + \sqrt{\Delta}}{2}\ \rangle.$$

Puisque M/L vérifie (3.4), cet ensemble n'est autre que l'ordre de conducteur f de A_M sur A. □

Proposition 3.3.6 *Soient A un anneau factoriel de caractéristique différente de 2 de corps des fractions L et M une extension de degré 2 de L vérifiant la condition (3.4). Notons Δ le discriminant de A_M/A. Soient Θ un ordre dont le conducteur f vérifie (3.10) et $\mathfrak{a}$ un idéal fractionnaire de Θ.*

L'idéal $\mathfrak{a}$ est propre si et seulement si il est inversible dans le monoïde des idéaux fractionnaires.

Démonstration
On sait déjà qu'un idéal inversible est propre. Soit $\mathfrak{a}$ un idéal propre de Θ. On peut écrire $\mathfrak{a}$ sous la forme $\alpha\langle 1, \tau\rangle$, avec $\alpha \in M^\times$, et τ ayant $aX^2 + bX + c$ pour

polynôme minimum sur A avec a, b, c premiers entre eux tels que $b^2 - 4ac = \Delta_f$. On a vu qu'alors $\Theta = \langle 1, a\tau \rangle$. Pour tout élément x, notons $\overline{x}$ le conjugué de x.

$$\begin{aligned} a a\overline{a} &= a\alpha\overline{\alpha}\,\langle\, 1\,;\,\tau\,\rangle\langle\, 1\,;\,\overline{\tau}\,\rangle \\ &= N(\alpha)\langle\, a\,;\, a\tau\,;\, a\overline{\tau}\,;\, a\tau\overline{\tau}\,\rangle \\ &= N(\alpha)\langle\, a\,;\, a\tau\,;\, -b\,;\, -c\,\rangle \\ &= N(\alpha)\langle\, 1\,;\, a\tau\,\rangle \qquad \text{car } (a, b, c) \text{ sont premiers entre eux.} \end{aligned} \tag{3.13}$$

L'idéal $\mathfrak{a}$ est inversible. □

Sous ces hypothèses, l'ensemble des idéaux fractionnaires propres de l'ordre A_{Δ_f} forme un groupe. Il admet l'ensemble des idéaux principaux comme sous-groupe distingué. On peut ainsi travailler avec le quotient du groupe des idéaux fractionnaires par le sous-groupe des idéaux principaux, que l'on nomme groupe des classes de l'ordre A_{Δ_f}, noté $C(A_{\Delta_f})$. Si I est un idéal fractionnaire propre de l'ordre A_{Δ_f}, nous noterons $Cl(I)$ sa classe dans $C(A_{\Delta_f})$. Dans chacune de ces classes on peut trouver un représentant remarquable que l'on va décrire.

Proposition/Définition 3.3.7 *Toute classe de $C(A_{\Delta_f})$ contient des idéaux de la forme $\langle a, \frac{-b+\sqrt{\Delta_f}}{2}\rangle$ avec $(a, b) \in A^2$ et $b^2 = \Delta_f - 4ac$ où $c \in A$ est tel que $pgcd(a, b, c) = 1$. Un tel idéal est nommé idéal primitif de A_{Δ_f}.*

Démonstration
Il suffit de se souvenir que l'on peut écrire tout idéal propre sous la forme $\alpha\langle 1, \tau\rangle$, avec $\alpha \in M^\times$, et τ ayant $aX^2 + bX + c$ pour polynôme minimum sur A avec a, b, c premiers entre eux tels que $b^2 - 4ac = \Delta_f$. Quitte à utiliser le conjugué de τ et en multipliant par l'idéal principal engendré par a/α, on obtient la proposition. □

3.4 Multiplication dans le groupe des classes

Nous allons décrire un algorithme de multiplication d'idéaux bien choisis du groupe de classes avec un anneau de départ A euclidien, de caractéristique différente de 2, et avec une extension M/L de degré 2 et vérifiant (3.4). On considère A_{Δ_f} ordre de A_M sur A de conducteur f vérifiant (3.10).

On sait que si α, β sont des éléments de A tels que $\beta^2 \equiv \Delta_f \pmod{4\alpha\Theta}$, l'idéal $\langle \alpha, \frac{-\beta+\sqrt{\Delta_f}}{2}\rangle$ est un idéal propre de A_{Δ_f}, et que toute classe admet un

représentant de cette forme. On dira plus simplement qu'elle est représentée par α, β ou par $\alpha, \beta, \frac{\beta^2-\Delta_f}{2\alpha}$ si on a besoin de plus de précision. Cette classe est alors

$$(\alpha A + \frac{-\beta+\sqrt{\Delta}_f}{2}A)/\{e\big(A + \frac{\Delta_f+\sqrt{\Delta_f}}{2}A\big); e \in M^\times\}.$$

Examinons maintenant les différentes étapes de l'algorithme de multiplication des classes.

1. On prend deux classes représentées par a_1, b_1, c_1 et a_2, b_2, c_2. Ces derniers sont des éléments de A vérifiant bien sûr :

   $$\forall i \in \{1,2\},\ {b_i}^2 - 4a_ic_i = \Delta_f.$$

   Remarquons que par (3.10), $b_i \equiv f\Delta \pmod{2A}$ pour $i \in \{1,2\}$. La somme $(b_1+b_2)/2$ est donc un élément de A (congru à $f\Delta$ modulo A).
2. On trouve par l'algorithme d'Euclide le pgcd d de $a_1,\ a_2$ et $\frac{b_1+b_2}{2}$ dans A ainsi que son écriture dans A sous la forme :

   $$d = h_1a_1 + h_2a_2 + h_3\frac{b_1+b_2}{2}$$

3. On pose $a = a_1a_2/d^2$. L'élément a appartient manifestement à A.
4. On calcule

   $$b' = \frac{h_1a_1b_2 + h_2a_2b_1 + h_3\frac{b_1b_2+\Delta_f}{2}}{d}$$

   et on pose b reste de la division euclidienne de b' par a.

   Remarquons que b est l'unique élément de A tel que :

   $$\begin{cases} b \equiv \frac{h_1a_1b_2+h_2a_2b_1+h_3\frac{b_1b_2+\Delta_f}{2}}{d} \pmod{aA} \\ v(b) < v(a). \end{cases} \tag{3.14}$$

L'idéal $\langle a, b\rangle$ va évidemment être un postulant à représenter le produit $\langle a_1, b_1\rangle.\langle a_2, b_2\rangle$ modulo les idéaux principaux. Pour s'en rendre compte, calculons tout d'abord diverses congruences.

Sachant ${b_1}^2 = \Delta_f + aa_1c_1$, on déduit :

$$\begin{aligned} b &\equiv \frac{h_1a_1b_1 + h_2a_2b_1 + h_3b_1\frac{b_1+b_2}{2}}{d} \pmod{\frac{2a_1}{d}A} \\ &\equiv b_1 \pmod{\frac{2a_1}{d}A}. \end{aligned}$$

De même, (3.15)

$$\begin{aligned} b &\equiv \frac{h_1a_1b_2 + h_2a_2b_2 + h_3b_2\frac{b_1+b_2}{2}}{d} \pmod{\frac{2a_2}{d}A} \\ &\equiv b_2 \pmod{\frac{2a_2}{d}A}. \end{aligned}$$

D'autre part, pour la même raison,

$$\begin{aligned} a_1b_2\frac{b_1+b_2}{2} &\equiv a_1\frac{b_1b_2+\Delta_f}{2} \pmod{2a_1a_2A} \text{ et,} \\ a_2b_1\frac{b_1+b_2}{2} &\equiv a_2\frac{b_1b_2+\Delta_f}{2} \pmod{2a_1a_2A}. \end{aligned} \tag{3.16}$$

En additionnant ces deux dernières relations multipliées par h_1 et h_2 respectivement avec la relation

$$a_2b_1\frac{b_1+b_2}{2} = a_2\frac{b_1b_2+\Delta_f}{2} \tag{3.17}$$

multipliée par h_3, on trouve, avec la définition de b,

$$\frac{b_1+b_2}{2}b \equiv \frac{b_1b_2+\Delta_f}{2} \pmod{\frac{a_1a_2}{d}A}.$$

Or,

$$\big(a_1A + \frac{-b_1+\sqrt{\Delta_f}}{2}A\big).\big(a_2A + \frac{-b_2+\sqrt{\Delta_f}}{2}A\big)$$

n'est autre que :

$$a_1a_2A + a_1\frac{-b_2+\sqrt{\Delta_f}}{2}A + a_2\frac{-b_1+\sqrt{\Delta_f}}{2}A + \frac{b_1b_2+\Delta_f-(b_1+b_2)\sqrt{\Delta_f}}{4}A.$$

On déduit donc, à l'aide des congruences précédentes,

$$d^2\big(aA+\frac{-b+\sqrt{\Delta_f}}{2}A\big) \subset \big(a_1A+\frac{-b_1+\sqrt{\Delta_f}}{2}A\big).\big(a_2A+\frac{-b_2+\sqrt{\Delta_f}}{2}A\big) \subset \frac{1}{2}\big(aA+\frac{b+\sqrt{\Delta_f}}{2}A\big).$$

Notons que pour tout élément $\alpha \in A$,

$$\alpha\big(aA + \frac{b+\sqrt{\Delta_f}}{2}A\big) = \big(\alpha\big(A + \frac{\Delta_f+\sqrt{\Delta_f}}{2}A\big)\big).\big(aA + \frac{b+\sqrt{\Delta_f}}{2}A\big).$$

On obtient donc le résultat suivant :

Proposition 3.4.1 *Si a_1, b_1 et a_2, b_2 permettent de représenter deux idéaux primitifs de l'ordre A_{Δ_f}, alors*

$$Cl\big(\langle a_1, \frac{-b_1+\sqrt{\Delta_f}}{2}\rangle\big)\, Cl\big(\langle a_2, \frac{-b_2+\sqrt{\Delta_f}}{2}\rangle\big) = Cl\big(\langle a, \frac{-b+\sqrt{\Delta_f}}{2}\rangle\big).$$

où a et b sont les éléments de A tels que :

$$a = \frac{a_1 a_2}{d^2}, \quad \begin{cases} b \equiv \frac{h_1 a_1 b_2 + h_2 a_2 b_1 + h_3 \frac{b_1 b_2 + \Delta_f}{2}}{d} \pmod{aA} \\ v(b) < v(a). \end{cases} \tag{3.18}$$

On obtient ainsi un algorithme pour effectuer la multiplication des idéaux primitifs de A_{Δ_f}. Ces calculs ont déjà été effectués lorsque $A = \mathbf{Z}$ par une comparaison avec les formes quadratiques de déterminant Δ_f. La multiplication correspond en effet à la décomposition de Gauss des formes quadratiques. (Voir le rapport formes quadratiques idéaux primitifs avec $A = \mathbf{Z}$ chez [Cox89], [Bue89], [Coh95].) On voit ici que l'on peut généraliser cet algorithme sans problème à des anneaux euclidiens avec les hypothèses (3.4) et (3.10).

3.5 Rapport avec les diviseurs

3.5.1 Lien entre jacobienne et groupe de classe pour une courbe hyperelliptique

On s'intéresse aux diviseurs d'une courbe projective C définie sur un corps $\mathbf{k}$ de caractéristique autre que 2, lisse, de genre g, et d'équation affine $y^2 = F(x)$, F étant un polynôme à coefficients dans $\mathbf{k}$ qui ne soit pas un carré. Ce cadre de travail correspond à celui de Cantor dans [Can87] (il étudie le cas où F est de degré impair). Cantor y représente un diviseur par un couple de polynômes afin d'effectuer l'addition de deux diviseurs. Nous allons présenter cette association sous une forme correspondant aux sections précédentes.

On cherche à appliquer le travail précédent à l'anneau $A = \mathbf{k}[X]$. Cet anneau est euclidien (voir [Per81]). Notons L son corps des fractions, M une extension de degré 2 de L engendrée par une racine carrée de $F(X)$, A_M l'anneau des éléments de M entiers sur A. Le diagramme d'inclusion s'écrit dans ce cas :

$$\begin{array}{ccccc} M = L[Y]/(Y^2 - F(X)) & \hookleftarrow & A_M \\ | \, 2 & & | \\ L & = & \mathbf{k}(X) & \hookleftarrow & A = \mathbf{k}[X] \end{array}$$

Les discriminants de A_M/A valent F modulo le carré d'un inversible. Travaillons avec le discriminant $\Delta = F$. Nous noterons $\mathcal{P}_C$ le groupe des diviseurs principaux de C.

Si P de coordonnées affine (x, y) est un point de C avec y, P' de coordonnées de $(x, -y)$ est aussi un point de C, ce sont les seuls points "affines" d'abscisse x de C. Le diviseur principal $(X - x)$ s'écrit donc $P + P' - 2\infty$, le symbole ∞ représentant le point à l'infini de la courbe ; aussi $-P' \equiv P - 2\infty \pmod{\mathcal{P}_C}$. De ce fait, toute classe de la jacobienne de C admet un unique représentant de forme réduite $D = \sum_{i=1}^{r'} k_i P_i - r\infty$, où les P_i sont des points de la courbe C distincts deux à deux et de coordonnées affines notées (x_i, y_i) (apparaîssant avec la multiplicité $k_i \in \mathbf{N}$), avec $r = \sum_{i=0}^{r'} k_i \leq g$ et la condition : si $P_i(x_i, y_i)$ apparaît dans la somme, aucun P_j, $j \neq i$ n'a pour coordonnées $(x_i, -y_i)$. Cantor associe alors à ce représentant D les polynômes a et b de $A = \mathbf{k}[X]$ suivants

$a(X) = \prod_{i=1}^{r'} (X - x_i)^{k_i}$ et

$b(X)$ est l'unique polynôme de degré strictement inférieur à $\deg(a)$ vérifiant :

$$\forall i \in \{1, \ldots, r'\}, \ (X - x_i)^{k_i} | \big(b(X) - y_i\big)$$

où k_i est la multiplicité de P_i dans D.

Cette deuxième condition signifie que a divise $(b^2 - F)$. On peut alors considérer c dans A tel que $4ac = b^2 - F$. Nous associerons à D l'idéal de A_M définie par

$$A_D = a\, A + \frac{-b + Y}{2}\, A.$$

En définissant $pgcd(\sum_{i \in I} n_i P_i, \sum_{j \in J} m_j P_j)$ par $\sum_{r \in I \bigcup J} min(n_r, m_r) P_r$, remarquons qu'alors $D = pgcd((a), (b - y))$. Le diviseur D correspond donc ainsi à un unique idéal $\langle a \, , \, (-b + Y)/2 \rangle$ tel que $b^2 - F \equiv 0 \pmod{4aA}$.

Observons aussi que si X ne divise pas a, ou si $v_X(F) \leq 1$, alors a, b et $c = (b^2 - F)/(4a)$ sont premiers entre eux : l'idéal associé est un idéal primitif de A_M. Or, $v_X(F) > 1$ implique que C n'est pas régulière en $(0, 0)$: A_D est donc primitif.

3.5.2 Traduction de l'addition dans la jacobienne

On suppose toujours pour cette section que C est une courbe lisse d'équation affine $y^2 = F(X)$ sur un corps $\mathbf{k}$ est de caractéristique différente de 2. Considérons deux classes de la jacobienne de C dont les représentants de forme réduite sont les diviseurs D_1 et D_2 respectivement. Associons alors, par le procédé décrit en 3.5.1, aux diviseurs D_1 et D_2, les polynômes $a_1,\ b_1$ et $a_2,\ b_2$ respectivement. L'algorithme décrit en 3.4.1 donne les polynômes a et b tels que la classe $Cl(\langle a,\ (-b + F)/2\rangle)$ soit le produit des classes $Cl(\langle a_1,\ (-b_1 + F)/2\rangle)$ et de $Cl(\langle a_2,\ (-b_2 + F)/2\rangle)$. La somme des diviseurs correspond à la multiplication des classes comme le décrit la proposition suivante :

Proposition 3.5.1 *Sous ces hypothèses, la classe du diviseur $D_1 + D_2$ correspond, au sens développé à la section 3.5.1, à la classe de l'idéal $aA + (-b + F)/2A$.*

On peut reprendre la démonstration faite dans [Can87] qui compte la multiplicité de a et b en chaque point et la compare à celle de D (Cantor travaille avec F de degré impair, mais cette démonstration n'utilise pas cette hypothèse). L'algorithme de multiplication des classes permet ainsi de construire un algorithme d'addition des diviseurs, dû d'ailleurs à David Cantor [Can87]. Constatons que sa complexité est de $g\big(\ln(g)\big)^2$ opérations.

3.6 Lien avec la cryptographie

3.6.1 Cryptosystème quadratique

On va décrire un cryptosystème de type El Gammal construit sur un groupe de classes d'un ordre d'une extension quadratique de $\mathbf{Q}$. Ce système a été proposé par Hunlein, Jacobson, Paulus, et Takagi en 1998 [HJPT01].

Bob veut construire un cryptosytème à clé publique, afin de recevoir des messages confidentiels (notamment d'Alice) lisible par lui uniquement. Bob choisit pour cela un nombre naturel p et note Δ le discriminant de $\mathbf{Q}[\sqrt{-p}\,]/\mathbf{Q}$. La situation se résume ici par

$$\begin{array}{ccccc} M = \mathbf{Q}[\sqrt{\Delta}] & \hookleftarrow & A_M \\ | \, 2 & & | \\ L = \mathbf{Q} & \hookleftarrow & A = \mathbf{Z} \end{array}$$

Bob choisit ensuite un nombre premier q pour travailler dans l'ordre de discriminant Δ_q. Il y choisit un idéal $\mathfrak{g} = \langle g, \frac{b_g + \sqrt{\Delta_q}}{2} \rangle$. Enfin, Bob choisit un entier a et un idéal équivalent à $\mathfrak{g}^a$ qu'elle nomme $\mathfrak{a}$.

Il rend publique :

le discriminant Δ_q,
les idéaux $\mathfrak{a}$ et $\mathfrak{g}$ dans Θ_{Δ_q}.

Il garde secret :

le conducteur q,
la clé secrète a vérifiant $\mathfrak{a} \sim \mathfrak{g}^a$.

Alice veut envoyer son message sous forme d'un idéal $\mathfrak{m}$ de Θ_{Δ_q}. Elle choisit k et transmet au récepteur Bob les idéaux $\mathfrak{r} = \mathfrak{g}^k$ et $\mathfrak{p} = \mathfrak{m}\ \mathfrak{a}^k$. On reconnait un cryptosystème El Gammal. Remarquons toutefois que l'on doit effectuer une multiplication d'idéaux ; en fait on sait multiplier les classes correspondantes. Pour retomber sur le message, on peut introduire la notion d'idéal réduit.

Proposition/Définition 3.6.1 *Un idéal de A_{Δ_q} du type $\langle a, \frac{-b+\sqrt{\Delta_q}}{2} \rangle$ avec $b^2 = \Delta_q - 4ac$ est dit réduit si $|b| \leq a \leq c$ avec de plus $b \geq 0$ dès que $|b| = a$ ou $a = c$.*

Tout idéal $\langle a, \frac{-b+\sqrt{\Delta_q}}{2} \rangle$ avec $b^2 = \Delta_q - 4ac$ de norme inférieure à $\frac{\sqrt{-\Delta_q}}{4}$ est réduit.

Il existe un unique idéal réduit dans chaque classe de $C(A_{\Delta_q})$.

Ce qui se passe pour les extensions quadratiques de $\mathbf{Q}$ est déjà bien connu : on peut trouver une démonstration de ce résultat par exemple dans [Cox89] ou dans [Coh95].

On impose donc initialement au message à envoyer $\mathfrak{m}$ la condition $N(\mathfrak{m}) < \sqrt{-\Delta_q}/4$, de façon à être sûr qu'il soit réduit. En suivant le décodage du El Gammal, Bob peut récupérer la classe de $\mathfrak{m}$; puis il cherche l'unique idéal réduit dans cette classe : c'est le message envoyé. Voir [Enj99] ou [HJPT01] pour l'aspect pratique de ces opérations.

L'avantage de ce système est de proposer une 'double sécurité', au sens qui est montré dans [HJPT01] :

Proposition 3.6.2 *Supposons connue une attaque du cryptosystème El Gammal dans $C(\Theta_\Delta)$.*

Alors, casser le cryptosystème revient à pouvoir trouver la décomposition de Δ_q en $q^2\Delta$.

On peut construire l'analogue de ce cryptosystème sur les courbes en partant de $A = \mathbf{F}_q[X]$, avec $q = p^r$, et p un nombre premier différent de 2. On considère une extension quadratique du corps des fractions de A :

$$\begin{array}{ccccc} M = L[Y]/(Y^2 - F(X)) & \hookleftarrow & A_M \\ | \, 2 & & | \\ L & = & \mathbf{k}(X) & \hookleftarrow & A = \mathbf{k}[X] \end{array}$$

Nous pouvons reprendre la construction du cryptosystème présenté sur $\mathbf{Z}$ avec les mêmes formules sur A : par ce qui précède, toutes les opérations y sont algébriquement identiques. Malheureusement, le discriminant de l'ordre $\Delta_q = q^2\Delta$ se décompose en produit des polynômes $q \in \mathbf{F}_q[X]$ et $\Delta \in \mathbf{F}_q[X]$. Or, s'il est difficile de factoriser des entiers, il existe des algorithmes de complexité polynômiale pour factoriser les polynômes de $\mathbf{F}_q[X]$. La version "courbe" de l'algorithme de Hunlein, Jacobson, Paulus et Takagi est donc inintéressante dans la mesure où elle n'apporte aucune sécurité supplémentaire,

3.6.2 Avantage de travailler avec un ordre

L'étude des ordres dans le cas d'une extension quadratique de $\mathbf{Q}$ est un domaine connu, rappelons en particulier ce théorème [Cox89].

Théorème 3.6.3 *Soient M une extension quadratique de $\mathbf{Q}$ de discriminant Δ, A_M l'anneau des entiers de M, A_f un ordre de conducteur f de M. Notons $h = \#C(A_M)$ le cardinal du groupe de classes de A_M.*

Le cardinal du groupe des classes de A_F est donné par

$$h_f = \frac{f\,h}{[A_M^\times : A_f^\times]} \prod_{p|f} (1 - (\frac{\Delta}{p})\frac{1}{p}).$$

Le terme $\left(\frac{\Delta}{p}\right)$ représente le symbole de Legendre, qui vaut 1 si Δ est un carré modulo p, -1 sinon. On peut trouver une démonstration de ce théorème dans

[Cox89], [Coh95] ou [Enj99]. On va appliquer ce théorème lorsque l'extension $M/\mathbf{Q}$ est quadratique imaginaire, dans ce cas $[A_M^\times : A_f^\times] = 1$.

Il apparaît alors bien plus facile de calculer l'ordre d'un groupe de classes d'un ordre qu'un groupe de classes de même grandeur. Ce fait rend le cryptosystème quadratique d'autant plus intéressant.

Un autre intérêt de la facilité de contrôler l'ordre des classes des ordres est de pouvoir construire des groupes tests. On a vu, dans le cas d'une courbe hyperelliptique, que la jacobienne s'exprime comme un groupe de classe. La cryptographie s'est particulièrement développée en utilisant cet isomorphisme (avec des cryptosystèmes basés sur le logarithme discret, voir 1). Les attaques de ce genre de système utilisent donc les opérations du groupe de classes, identiques à celle du groupe de classes d'un ordre. L'une des plus aboutie (car parmi les plus récentes) est celle de Gaudry [Gau00], utilisant une recherche de collision par une marche itérative puis un traitement d'algèbre linéaire optimisé. Deux chercheurs de l'université d'Urbana-Champaign, Eric Landquist et Jonathan Webster, ont amélioré et programmé l'algorithme de Gaudry. Ce programme fonctionnait (en mars 2002) pour les groupes de classes qu'ils pouvaient calculer mais qui restaient d'ordre petit. La constatation que l'attaque est identique pour les ordres (il suffit juste de changer le discriminant Δ par $f^2\Delta$) nous a permis de leur proposer des gros groupes à casser. Le programme a réussi à résoudre le problème pour le discriminant -10008601877734695908479 mais a échoué pour un discriminant $d_f = -10000000000000000000000000001443 * 2000423^2$. Cet exemple est intéressant car la taille h_f du groupe de classes de l'ordre de discriminant d_f cité est $h_f = 2 * 1000211 * 103902575992349$ qui a peu de facteurs premiers, et tous de puissance 1 : on peut donc y trouver des éléments de grand ordre, ce qu'il nous faut pour un bon logarithme discret. L'exemple résolu le plus grand par ce programme était $d_f = -40016925754966949318639 = -10000000991 * 2000423^2$, la taille du groupe des classes étant $h_f = 175571037674 = 2 * 87767 * 1000211$ (bonne décomposition). Eric Landquist et Jonathan Webster ont alors réfléchi de nouveau sur leur programme : ils pouvaient tester maintenant leurs nouvelles améliorations à l'aide d'exemples issus des ordres. Ils ont ainsi, en autres, annoncé la résolution par leur programme du logarithme discret

– le 29 août, en travaillant avec l'ordre de discriminant

$$\begin{aligned} d_f &= -10000000000000000000000000001443 * 2000423^2 \\ &= -40016921789290000000000000057744418141945 47 \end{aligned}$$

dont la taille de groupe des classes est

$$\begin{aligned} h_f &= 103902575992349 * 2 * 1000211 \\ &= 207848998871766771278 \end{aligned}$$

et avec

$g = [23; 19]$ et
$h = [221620891566838614101; -170818227905445527653]$

en 947 secondes. Ils trouvent $x = 39895106467666494903$.

– le 7 octobre, en travaillant avec l'ordre de discriminant

$$\begin{aligned} d_f &= -10000000000000000000000001443 * 10000000993^2 \\ &= -10000001986000098604900000014430002865798142286870 7 \end{aligned}$$

dont la taille de groupe des classes est

$$h_f = 1039025863202650536394906$$

et avec

$g = [23; -17]$ et
$h = [48013790078683574846440 09; -30098049887381082758865 47]$

en 5943 secondes. Ils trouvent $x = 729556922614964277230474$.

– le 15 octobre, en travaillant avec l'ordre de discriminant

$$\begin{aligned} d_f &= -10000000000000000000000001443 * 10000000993^2 \\ &= -10000001986000098604900000014430002865798142286870 7 \end{aligned}$$

dont la taille de groupe des classes est

$$h_f = 1039025863202650536394906$$

et avec

$g = [23; -17]$ et
$h = [366047529346934227897348 7; 32450835673500545076534 73]$

en 2272.91 secondes. Ils trouvent $x = 725748555769821823169543$.

– le 29 octobre, en travaillant avec l'ordre de discriminant

$$d_f = -10000001986000098604900000014430002$$

dont la taille de groupe des classes est

$$h_f = 1039025863202650536394906$$

et avec

$g = [23; -17]$ et
$h = [1328147294067310596642667; 3338927209934598803]$

en 1797.9 secondes. Ils trouvent $x = 248529387001287896877585$.
Pour tous ces exemples, on entend par la notation $[a, b]$ l'idéal

$$\langle a; (-b + \sqrt{d_f})/2 \rangle.$$

Chapitre 4

Répartition des angles de Frobenius

4.1 Introduction

Pour une courbe X lisse sur un corps fini $\mathbf{K}$, on définit la fonction zéta par $Z(X,T) = \exp\left(\sum_{n\geq 1} N_n T^n/n\right)$, où N_n désigne le nombre de points de X sur une extension de degré n de $\mathbf{K}$. Son étude est donc importante car elle nous donne des informations sur les nombres N_n. Weil a montré la rationalité de la fonction zéta. Le but de ce chapitre est d'étudier la distribution de ses zéros. On rappelle tout d'abord dans la section 4.1 des outils mathématiques nécessaires pour notre étude. Après avoir précisé notre motivation en 4.2.1, on expose "la formule explicite" et les travaux déjà effectués sur ce sujet (Serre, Tsfasman, Lachaud) dans les sections 4.2.2 et 4.2.3. Les sections suivantes prolongent ces études, on y trouve entre autres les résultats annoncés dans l'introduction.

4.1.1 Exemples de courbes

On appelle *courbe* toute variété projective de dimension 1. Avant toute étude examinons quelques exemples classiques de courbes. Pour une telle courbe X définie sur un corps fini $\mathbf{K}$, on notera N le nombre de points de X sur $\mathbf{K}$ et g le genre de X (on trouve dans [Per93] la définition du genre arithmétique d'une courbe irréductible).

Proposition 4.1.1 *La droite projective est une courbe sur $\mathbf{F}_q$ de nombre de points $N = q+1$. Son genre g est nul.*

Silverman calcule ce genre dans [Sil85] en constatant qu'il n'existe pas de différentielle holomorphe sur $\mathbf{P}^1$.

Proposition/Définition 4.1.2 *On appelle courbe hermitienne toute courbe définie par*

$$X/\mathbf{F}_{r^2} \ : \ Y^r Z + Y Z^r = X^{r+1}.$$

Ces courbes ont pour nombre de points rationnels $N = r^3 + 1$ *et pour genre* $g = \frac{r(r-1)}{2}$.

On verra qu'elles réalisent le nombre maximal de points pour un genre donné.

Proposition/Définition 4.1.3 *La courbe de Klein est définie par*

$$X^3Y + Y^3Z + Z^3X = 0.$$

Sur $\mathbf{F}_{2^v}$*, son nombre de points est*

$$N = \begin{cases} 2^v + 1 \text{ si } v \not\equiv 0 \pmod 3, \\ 2^v + 1 - s_v \text{ si } v \equiv 0 \pmod 3 \end{cases}$$

où $\{s_{3n}\}_{n\in\mathbf{N}}$ *est définie par la relation de récurrence*

$$s_{3(n+2)} + 5s_{3(n+1)} + 8s_{3n} = 0$$

et les valeurs initiales $s_0 = 6$ *et* $s_3 = -15$.

Pour l'étude du nombre de points de la courbe de Klein voir par exemple [Ste]. Klein a trouvé l'équation de cette courbe comme modèle pour l'équation modulaire $X(7)$ (voir chez [Ogg69] ou [Mor97] la définition des courbes modulaires).

Proposition/Définition 4.1.4 *Soit* n *un entier naturel. Posons* $q_0 = 2^n$ *et* $q = 2q_0^2 = 2^{2n+1}$.

La courbe définie sur $\mathbf{F}_q$ *d'équation affine*

$$y^q + y = x^{q_0}(x^q + x)$$

a pour genre $g = q_0(q-1)$ *et pour nombre de points rationnels* $N = q^2 + 1$. *Elle admet le groupe simple de Suzuki* $S_{\mathbf{Z}}(q)$ *pour groupe d'automorphismes, nous la nommerons donc courbe de Suzuki.*

Cette courbe atteint le nombre maximum de points rationnels possible pour ce genre (voir pour cela [HS90]).

Proposition/Définition 4.1.5 *Soit s un entier naturel. Posons $q_0 = 3^s$ et $q = 3q_0^2 = 3^{2s+1}$.*

La courbe de $\mathbf{P}^3$ d'équation affine sur $\mathbf{F}_q(x, y_1, y_2)$

$$\begin{cases} y_1^q - y_1 = x^{q_0}(x^q - x) \\ y_2^q - y_2 = x^{2q_0}(x^q - x) \end{cases} \tag{4.1}$$

a pour nombre de points rationnels $N = q^3 + 1$ et pour genre

$$g = \frac{3}{2} q_0 (q-1)(q + q_0 + 1).$$

Son groupe d'automorphismes est un groupe de Ree d'ordre $q^3(q-1)(q^3+1)$, nous nommerons cette courbe courbe de Ree.

Cette courbe atteint aussi le nombre de points rationnels maximum pour le genre correspondant (voir [HP93]).

4.1.2 Rappels sur la conjecture de Weil

Définition 4.1.6 *Soit V une variété projective sur un corps fini $\mathbf{K}$. Pour toute extension $\mathbf{K}_n$ de degré n de $\mathbf{K}$, on pose N_n le nombre de points de la variété regardée sur $\mathbf{K}_n$ (i.e. de points à coordonnées dans $\mathbf{K}_n$ vérifiant les équations définissant V). On appelle fonction zéta la fonction*

$$Z(V/K, T) = \exp\big(\sum_{n \geq 1} N_n \frac{T^n}{n}\big). \tag{4.2}$$

On montre que pour les variétés lisses (i.e. non singulières) la fonction zéta est rationnelle ; Weil a conjecturé la forme de la fonction zeta en 1949 [Wei49], et l'a démontrée pour les courbes et variétés abéliennes. On peut regarder dans [Sil85] (ou dans [Har77]) un énoncé de cette conjecture ainsi qu'un résumé des divers travaux faits depuis à ce sujet. Nous allons juste donner l'écriture rationnelle de Z dans le cas d'une courbe sur $\mathbf{F}_q$, q étant une puissance d'un nombre premier.

Théorème 4.1.7 *Considérons une courbe irréductible X lisse de genre g définie sur le corps fini $\mathbf{F}_q$. La fonction zéta s'écrit alors*

$$Z(X,T) = \frac{P(T)}{(1-T)(1-qT)} \tag{4.3}$$

avec $P(T)$ un polynôme de la forme : $P(T) = 1 + \sum_{j=1}^{2g-1} c_j T^j + q^g T^{2g}$, où les c_j sont des éléments de $\mathbf{Z}$.

Dans le corps $\mathbf{C}$ des nombres complexes, on peut donc écrire le polynôme numérateur sous la forme

$$P(T) = \prod_{i=1}^{2g} (1 - \omega_i T).$$

En comparant les deux écritures du polynôme $P(X,t)$, on déduit que

$$\prod_{j=1}^{2g} \omega_j = q^g.$$

En fait, la contribution en module de chaque ω_j au produit est uniforme [Wei49] :

Théorème 4.1.8 *Considérons une courbe irréductible X lisse de genre g définie sur le corps fini $\mathbf{F}_q$. Notons $1/\omega_j$, où $1 \leq j \leq 2g$, les racines dans $\mathbf{C}$ du polynôme numérateur de la fonction zéta de X.*

Les nombres complexes ω_j sont conjugués deux à deux et de module $\sqrt{q}$.

En développant en série entière $\ln Z(X,t)$, on obtient

Proposition 4.1.9 *Soit X une courbe irréductible lisse de genre g définie sur le corps $\mathbf{F}_q$. Notons $1/\omega_j$, où $1 \leq j \leq 2g$, les racines dans $\mathbf{C}$ du polynôme numérateur de la fonction zéta de X. Le nombre de points de X sur une extension de degré n du corps $\mathbf{K}$ est donné par*

$$N_n = q^n + 1 - \sum_{j=1}^{2g} {\omega_j}^n. \tag{4.4}$$

Toute information sur les ω_j permet donc de mieux connaître le nombre de points de la courbe. On va appeler leurs arguments angles de Frobenius.

4.1.3 Lien avec le Frobenius, cas des courbes elliptiques, terminologie générale

Dans la première partie de cette section, on donne une esquisse de la démonstration de la proposition 4.1.9, en concluant de façon plus précise pour les courbes elliptiques. Cela permet d'appréhender la terminologie fixée dans la proposition 4.1.11, avec laquelle nous travaillerons tout au cours de ce chapitre.

Nous travaillons toujours sur un corps fini $\mathbf{K} = \mathbf{F}_q$, avec $q = p^r$, p étant un nombre premier et r un entier naturel. Notons $\overline{\mathbf{K}}$ une clôture algébrique de $\mathbf{K}$, et $\mathbf{P}^m$ l'espace projectif sur $\overline{\mathbf{K}}$ de dimension m.

Définition 4.1.10 *Pour tout entier naturel n on appelle q^n-ième puissance de Frobenius l'application*

$$\begin{aligned}\Phi_n : \mathbf{P}^m &\longrightarrow \mathbf{P}^m \\ (x_0, x_1, \cdots, x_m) &\longmapsto (x_0{}^{q^n}, x_1{}^{q^n}, \cdots, x_m{}^{q^n}).\end{aligned}$$

$\overline{\mathbf{K}}$ étant de caractéristique p, Φ_n est manifestement un morphisme.

Nous considérons maintenant une courbe donnée par les équations $F_i(x_0, x_1, \cdots, x_m) = 0$, $1 \leq i \leq m-1$, les F_i étant des polynômes homogènes de $\mathbf{K}[X_0, X_1, \cdots, X_m]$. Pour tout corps $\mathbf{k} \subset \overline{\mathbf{K}}$, nous poserons $E(\mathbf{k})$ l'ensemble des points $(x_0, x_1, \cdots, x_m) \in \mathbf{P}^m \bigcap \mathbf{k}^{m+1}$ zéros de tous les F_i. Remarquons que, pour tout $i \in \{1, \ldots, m-1\}$,

$$\forall (x_0, x_1, \cdots, x_m) \in \mathbf{P}^m, F(\Phi_n(x_0, x_1, \cdots, x_m)) = \big(F(x_0, x_1, \cdots, x_m)\big)^q.$$

La restriction de Φ_n à $E(\overline{\mathbf{K}})$ est donc à valeurs dans $E(\overline{\mathbf{K}})$. De plus, si $\mathbf{K}_n$ désigne une extension de degré n de $\mathbf{K}$, l'extension $\overline{\mathbf{K}}/\mathbf{K}_n$ est galoisienne, de groupe de Galois engendré par Φ_n, donc

$$P \in E(\mathbf{K}_n) \Longleftrightarrow \Phi_n(P) = P$$

On en déduit donc $E(\mathbf{K}_n) = (Id - \Phi_n)^{-1}(0)$.

Prenons maintenant X une courbe sur un corps $\mathbf{K} = \mathbf{F}_q$ fixé. On appelle alors la restriction de la q-ième puissance de Frobenius à X *endomorphisme de Frobenius de X*. Notons que c'est la puissance qui correspond au corps de travail fixé $\mathbf{K}$. Nous notons maintenant Φ l'endomorphisme de Frobenius de X. L'endomorphisme Φ^n est alors la q^n-ième puissance de Frobenius. On obtient donc que N_n est le cardinal de $(Id - \Phi^n)^{-1}(0)$.

On suppose en plus pour ce paragraphe que la courbe X est elliptique (i.e. de genre 1). L'endomorphisme Φ induit sur le module de Tate de X un endomorphisme Φ_l. On montre que Φ_l a deux valeurs propres distinctes complexes conjuguées ω_1 et ω_2 de produit q, et que le cardinal de $(Id - \Phi^n)^{-1}(0)$ vaut $det(T\ Id - {\Phi_l}^n)(1)$ pour tout entier naturel n. On en déduit, si X est elliptique,

$$N_n = 1 + q^n - (\omega^n + \overline{\omega}^n), \text{ avec } \omega = \sqrt{q}\mathrm{e}^{i\Theta}.$$

Θ est l'angle d'une valeur propre de l'endomorphisme induit de l'endomorphisme de Frobenius, on l'appelle *angle de Frobenius* de X. On peut trouver les détails des faits annoncés ici dans [Sil85].

La forme particulière des N_n trouvée dans le cas des courbes elliptiques se généralise pour une courbe irréductible comme suit.

Proposition/Définition 4.1.11 *Soit X une courbe lisse, absolument irréductible, de genre g sur $\mathbf{K} = \mathbf{F}_q$. Alors, pour tout $n \in \mathbf{N}^*$,*

$$N_n = q^n + 1 - \sum_{j=1}^{g} ({\omega_j}^n + \overline{\omega_j}^n) \tag{4.5}$$

avec $\forall j \in \{1, \cdots, g\},\ \omega_j = \sqrt{q}\mathbf{e}^{i\theta_j}$.

On appelle les nombres réel $\theta_j \in [\,0,\ \pi\,]$ angles de Frobenius de X.

On utilise alors plutôt (4.5) sous la forme :

$$N_n = q^n + 1 - 2\sqrt{q^n} \sum_{j=1}^{g} \big(\cos(n\theta_j)\big). \tag{4.6}$$

4.2 Étude

Nous travaillerons dans toute cette fin de chapitre avec une courbe projective X lisse, absolument irréductible (une courbe réalisant ces trois exigence est dite algébrique), de genre g, définie sur le corps $\mathbf{K} = \mathbf{F}_q$.

4.2.1 Motivation

Nous cherchons des informations sur les nombres de points N_r sur les différentes extensions de $\mathbf{K}$, mais bien sûr plus particulièrement sur $N = N_1$ le nombre de points sur $\mathbf{K}$. Notons que la borne de Hasse-Weil nous donne déjà $|N - (q+1)| \leq 2g\sqrt{q}$ pour toute courbe sur $\mathbf{K} = \mathbf{F}_q$. Rappelons qu'asymptotiquement, par la borne de Drinfeld-Vladuts [VD83], $\limsup_{g\to\infty} N/g \leq \sqrt{q} - 1$ pour toute famille infinie de courbes dont le genre tend vers l'infini. La borne de Hasse-Weil semble donc trop large pour g tendant vers l'infini. Nous donnons tout d'abord des majorations du type $N \leq ag + b$ plus fines moyennant des hypothèses sur X ou $\mathbf{K}$ en section 4.2.3.

On s'intéresse ensuite aux familles infinies de courbes dont le genre tend vers l'infini. Nous démontrons dans l'annexe B qu'on peut extraire d'une famille de ce type une sous-famille dont tous les quotients N_r/g admettent une limite lorsque g croit vers l'infini. De telles familles (dont les quotients N_r/g convergent) sont appelées *familles asymptotiquement exactes* [Tsf92]. Tsfasman et Vlăduţ montrent que pour une famille asymptotiquement exacte, la répartition des angles de Frobenius admet une distribution limite donnée par une mesure continue sur $[0, \pi]$ [TV97]. Il en découle que les angles de Frobenius d'une famille asymptotiquement exacte sont denses dans $[0, \pi]$. Une famille infinie de courbes dont le genre tend vers l'infini comprenant une sous-famille asymptotiquement exacte, on en déduit que toute famille de courbes dont les angles ne sont pas denses est finie. Concrètement, si Θ contient un ouvert non vide, toute famille de courbes sans angles de Frobenius dans Θ est finie. Nous cherchons dans ce chapitre à connaître les valeurs maximales du nombres de point rationnel et du genre de ces familles avec angles hors de Θ.

On peut trouver les renseignements sur la répartition des angles de Frobenius pour des familles aux genres non bornés dans les études de Tsfasman et Vladuts [TV97] et de Serre [Ser97]. Duursma et Enjalbert proposent des problèmes ouverts sur ce sujet dans [DE02].

4.2.2 Étude théorique

Nous reprenons ici le travail fait dans [Ser83].
Rappelons (4.6) :

$$\forall n \in \mathbf{N}^*,\ N_n = q^n + 1 - q^{n/2} \sum_{i=1}^{g} 2\cos(n\Theta_i)$$

où $\{\theta_i\}_{1\leq i\leq g}$ est l'ensemble des angles de Frobenius de la courbe X de genre g.

Nous poserons pour toute la suite $r = \sqrt{q}$. On peut alors réécrire (4.6) sous la forme

$$N_1 r^{-n} + (N_n - N_1)r^{-n} = r^n + r^{-n} - 2\sum_{i=1}^{g} \cos(n\theta_i) \tag{4.7}$$

On peut généraliser en $n = 0$ par

$$0 = 2g - 2\sum_{i=1}^{g} 1.$$

Introduisons maintenant une suite de nombres réels $\{u_n\}_{n\in\mathbf{N}}$ et définissons les fonctions

$$\begin{aligned} f : \mathbf{R} &\longrightarrow \mathbf{R} \\ \Theta &\longmapsto u_0 + \textstyle\sum_{n\geq 1} u_n \cos(n\Theta) \end{aligned}$$

et,

$$\begin{aligned} \psi : \mathbf{R} &\longrightarrow \mathbf{R} \\ x &\longmapsto \textstyle\sum_{n\geq 1} u_n x^n. \end{aligned}$$

Pour chaque n, multiplions u_n avec l'équation (4.7) correspondante, la somme sur n du résultat donne

$$N_1\psi(r^{-1}) + \sum_{n\geq 1} u_n(N_n - N_1)r^{-n} = 2u_0 g + \psi(r) + \psi(r^{-1}) - 2\sum_{j=1}^{g} f(\theta_j). \tag{4.8}$$

4.2.3 Application : majorant du nombre de points rationnels

Reprenons le choix de $\{u_n\}_{n\in\mathbf{N}}$ fait dans [Ser83].

(a) $u_0 = 1$,

(b) $\forall n \geq 1, u_n \geq 0$

(c) $f(\theta) \geq 0$, pour tout $\theta \in [0, \pi]$.

Appliqué à (4.8), ce choix amène à :

$$N\psi(r^{-1}) \leq 2g + \psi(r^{-1}) + \psi(r).$$

Pour illustrer ce cas, considérons la fonction f donnée par :

$$\begin{aligned} f(\theta) &= \cos^2(\theta)\big(1 - \frac{\cos(\theta)}{\cos(2\pi/3)}\big)^2 \\ &= 1 + \sqrt{3}\cos(\theta) + \frac{7}{6}\cos(2\theta) + \frac{\sqrt{3}}{3}\cos(3\theta) + \frac{1}{6}\cos(4\theta). \end{aligned} \tag{4.9}$$

L'égalité (4.8) conduit alors à, pour $q = 3$ (i.e. pour les courbes définies sur $\mathbf{F}_3$),

$$N \leq \frac{54}{41}(g - 15) + 28 < 1,317g + 8,244.$$

Cette inégalité est donc meilleure que celle de Hasse-Weil [Iha81]. Elle est atteinte si $N_1 = N_2 = N_3 = N_4$ et si les angles de Frobenius sont dans $\{\pi/2, 2\pi/3\}$. C'est le cas pour la courbe de Deligne-Lusztig associé à ${}^2G_2(3)$ [HP93]. Cette courbe est de genre $g = 15$ et a pour nombre de points $N = 28$. Le polynôme numérateur de sa fonction zéta est $P(T) = (1 + 3T^2)^7(1 + 3T + 3T^2)^8$.

4.2.4 Premier choix : $u_0 = 1$

Remarquons la généralisation possible du choix de Serre [Ser83] ; si on peut trouver un ensemble Θ tel que $\{u_n\}_{n\in\mathbf{N}}$ vérifie

(a) $u_0 = 1$,

(b) $\forall n \geq 2, u_n \geq 0$

(c) $f(\theta) \geq 0$, pour tout $\theta \subset \Theta \in [0, \pi]$.

On déduit alors de (4.8) :

$$N\psi(r^{-1}) \leq 2g + \psi(r^{-1}) + \psi(r) - 2\sum_{\theta\,\in\Theta} f(\theta).$$

Par suite, toute courbe telle que

$$N\psi(r^{-1}) > 2g + \psi(r^{-1}) + \psi(r)$$

doit avoir une somme $\sum_{\theta\,\in\Theta} f(\theta)$ négative, elle a donc un de ses angles de Frobenius dans $[0, \pi] \setminus \Theta$.

Pour tout élément $\alpha \in [0, \frac{\pi}{2}[$, choisissons la suite $u_0 = 1$, $u_1 = -\frac{1}{\cos(\alpha)}$ et les termes suivants nuls. On obtient la fonction

$$f \;:\; \Theta \longmapsto 1 - \frac{\cos(\Theta)}{\cos(\alpha)}.$$

Elle est positive sur $[\alpha, \pi]$, strictement négative sur $[0, \alpha[$. En appliquant ce qui précède, on déduit que toute courbe sur $\mathbf{F}_q$ telle que $N + 2\sqrt{q}\cos(\alpha)\ g < q + 1$ a un angle de Frobenius dans $[0, \alpha[$.

Utilisons maintenant la fonction

$$f \ : \theta \longmapsto 1 + 3\sqrt{2}\cos(\theta) + 2\sqrt{2}\cos(3\theta).$$

Elle correspond à une suite $\{u_n\}_{n\in\mathbf{N}}$ vérifiant les conditions du choix. Elle se factorise sous la forme $f(\theta) = (1 + \sqrt{2}\cos(\theta))\big(1 - 2\sqrt{2}\cos(\theta)\big)^2$. On obtient ainsi que toute courbe sur $\mathbf{F}_2$ avec $N > \frac{g}{2} + \frac{9}{2}$ a un angle de Frobenius dans $]\frac{3\pi}{4}, \pi[$. On peut trouver dans [vdGvdV00] des exemples de courbes satisfaisant la condition. Toutes les vérifications d'existence de courbes vérifiant les conditions trouvées dans les prochains chapitres viendront aussi de [vdGvdV00].

4.2.5 Deuxième choix : $u_0 = 0$

On suppose maintenant que :

(a) $u_0 = 0$,

(b) $\forall n \geq 2, u_n \geq 0$

(c) $f(\theta) \geq 0$, pour tout $\theta \in \Theta \subset [0, \pi]$.

On déduit alors de la formule (4.8) :

$$N\psi(r^{-1}) \leq \psi(r^{-1}) + \psi(r) - 2\sum_{\theta\ \in\Theta} f(\theta).$$

Donc, toute courbe vérifiant l'inégalité

$$N\psi(r^{-1}) > \psi(r^{-1}) + \psi(r)$$

doit avoir une somme $\sum_{\theta\ \in\Theta} f(\theta)$ négative, elle a donc un de ses angles de Frobenius dans $[0, \pi] \setminus \Theta$.

Si de plus la suite $\{u_n\}_{n\in\mathbf{N}}$ vérifie

(d) $\exists m \in \mathbf{N}/ \begin{cases} \forall n > m,\ u_n = 0. \\ \forall n \in \{1, \cdots, m\},\ u_n = u_{m+1-n}. \end{cases}$

alors, la condition suffisante pour avoir un angle dans $[0,\pi]\setminus\Theta$ devient

$$N > r^{m+1}+1.$$

En effet , dans le cas (d), $\frac{\psi(r)}{\psi(r^{-1})} = \frac{\sum_{n=0}^{m} u_n r^n}{\sum_{n=0}^{m} r^{n-m}} = r^m$.

On peut appliquer cela à la suite issue de la fonction $f\ :\ \theta \longmapsto \cos(\theta)$. On trouve alors que toute courbe dont le nombre de points vérifie $N > r^2+1$ a un angle de Frobenius dans $]\pi/2, 3\pi/2[$. La droite projective a un nombre de points $N = r^2+1$ et n'a aucun angle dans $]\pi/2, 3\pi/2[$, la condition trouvée est donc optimum.

La fonction $f\ :\ \theta \longmapsto \cos(\theta)+\cos(2\theta)$ donne une suite $\{u_n\}_{n\in\mathbf{N}}$ vérifiant les points $(a),\ (b),\ (c)\ et\ (d)$. Elle est strictement négative uniquement sur $]\pi/3, \pi[$. On obtient donc que toute courbe telle que $N > r^3+1$ a un angle de Frobenius dans l'intervalle ouvert $]\pi/3, \pi[$. On ne peut améliorer l'inégalité : la courbe hermitienne sur $\mathbf{F}_{r^2}$ n'a aucun angle dans $]\pi/3, \pi[$ bien que son nombre de points soit $N = r^3+1$ [RS94].

La fonction

$$\begin{aligned} f(\theta) &= \frac{\sqrt{2}}{5}\cos(\theta)\big(1-2\cos^2(\theta)\big)\big(1-8\cos^2(\theta)\big) \\ &= \frac{7}{10}\sqrt{2}\cos(\theta) + \frac{1}{2}\sqrt{2}\cos(3\,\theta) + \frac{1}{5}\sqrt{2}\cos(5\,\theta) \end{aligned}$$

s'annule aux angles de Frobenius des cinq courbes elliptiques sur $\mathbf{F}_2$. La suite $\{u_n\}_{n\in\mathbf{N}}$ associée vérifie les quatre conditions requises. On en déduit que toute courbe sur $\mathbf{F}_2$ à jacobienne complètement décomposable a son nombre de points borné par $N \le 6$. Cette borne est atteinte par la courbe

$$y^2+y = \frac{x^2+x}{(x^2+x+1)^3}.$$

4.2.6 Troisième choix : $u_0 = -1$

On suppose ici que :

(a) $u_0 = -1$,

(b) $\forall n \ge 2, u_n \ge 0$

(c) $f(\theta) \geq 0$, for all $\theta \in \Theta \subset [0, \pi]$.
On déduit alors de la formule (4.8) :

$$N\psi(r^{-1}) \leq -2g + \psi(r^{-1}) + \psi(r) - 2\sum_{\theta\ \in\Theta} f(\theta).$$

Donc, toute courbe vérifiant l'inégalité :

$$N\psi(r^{-1}) > -2g + \psi(r^{-1}) + \psi(r)$$

doit avoir une somme $\sum_{\theta\ \in\Theta} f(\theta)$ négative, elle a donc un de ses angles de Frobenius dans $[0, \pi] \setminus \Theta$.

Si de plus la suite $\{u_n\}_{n\in\mathbf{N}}$ vérifie la condition supplémentaire
(d) $\psi(r^{-1}) = 0$,
toute courbe dont les angles de Frobenius sont dans l'ensemble Θ a un genre borné par

$$g \leq \frac{\psi(r)}{2}.$$

La fonction construite de manière à s'annuler aux angles de Frobenius des trois courbes elliptiques considérées sur $\mathbf{F}_4$ et définies sur $\mathbf{F}_2$ et de degré minimum a la forme suivante

$$f(\theta) = -1 - \frac{4}{3}\cos(\theta) + \frac{7}{9}\cos(2\theta) + \frac{26}{9}\cos(3\theta) + \frac{16}{9}\cos(4\theta).$$

La suite associée vérifie les quatre conditions. Il s'ensuit que toute courbe sur $\mathbf{F}_2$ à jacobienne complètement décomposable a un genre inférieur à 26, améliorant la borne donnée par Serre ($g \leq 145$ dans [Ser97]). Cette méthode est d'autant plus intéressante que la courbe modulaire $X(11)$ atteint cette nouvelle borne [Lig77].

4.2.7 Étude du degré deux

On cherche toujours à trouver des conditions pour l'existence d'un angle de Frobenius dans l'intervalle ouvert $]\alpha, \beta[$. La première idée est de considérer une fonction f de degré 2 en $\cos(\theta)$. Quitte à diviser par un scalaire pour pouvoir appliquer les cas précédents (division qui ne change rien au raisonnement), il est plus intéressant de prendre f sous la forme :

$$x \mapsto \big(\cos(x) - \cos(\alpha)\big) \cdot \big(\cos(x) - \cos(\beta)\big).$$

On obtient $f(x) = \frac{1}{2}\cos(2x) - \big(\cos(\alpha)+\cos(\beta)\big)\cos(x) + \big(\frac{1}{2}+\cos(\alpha)\cos(\beta)\big)$.

Remarquons que $u_0 = \frac{1}{2} + \cos(\alpha)\cos(\beta)$.

Regardons quelques cas particuliers :

- Pour $\alpha = \frac{\pi}{4}$ et $\beta = \frac{3\pi}{4}$, on trouve $u_0 = 0$ (deuxième choix), $f(x) = \cos(2x)$ est strictement négative uniquement sur $]\frac{\pi}{4}, \frac{3\pi}{4}[$. Nous trouvons ainsi que toute courbe dont le nombre de points rationnels vérifie $N > 1 + r^4$ a un angle de Frobenius dans $]\frac{\pi}{4}, \frac{3\pi}{4}[$.
- Pour $\alpha = \frac{\pi}{3}$ et $\beta = \frac{3\pi}{4}$, on trouve $u_0 = \frac{2-\sqrt{2}}{4}$, la fonction correspondante $f(x) = \frac{1}{2}\cos(2x) + \frac{\sqrt{2}-1}{2}\cdot\cos(x) + \frac{2-\sqrt{2}}{4}$ est strictement négative uniquement sur $]\frac{\pi}{3}, \frac{3\pi}{4}[$. La fonction f/u_0 a le même signe et vérifie les conditions du premier choix. Pour $q = 2$, si $N > \frac{8-2\sqrt{2}}{7}g + \frac{27+2\sqrt{2}}{2}$, la courbe possède donc un angle de Frobenius dans $]\frac{\pi}{3}, \frac{3\pi}{4}[$ (Le minorant s'applique pour un genre de 2 à 28).
- Pour $\alpha = \frac{\pi}{4}$ et $\beta = \pi$, on trouve $u_0 = -\frac{\sqrt{2}-1}{2}$ négatif. On applique le travail fait au troisième choix à la fonction $\frac{f(x)}{u_0} = -1 + \sqrt{2}\cos(x) + \frac{\cos(2x)}{\sqrt{2}-1}$, ce qui donne que toute courbe sur $\mathbf{F}_q$ telle que

$$N + \frac{2(\sqrt{2}-1)q}{(2-\sqrt{2})\sqrt{q}+1} > 1 + \frac{\sqrt{q}+2-\sqrt{2}}{(2-\sqrt{2})\sqrt{q}+1}q^{3/2}$$

  a un angle de Frobenius dans $]\frac{\pi}{4}, \pi[$. Numériquement, cette condition devient $N + 0.9061g > 4.0939$ sur $\mathbf{F}_2$, elle est $N + 1.2336g > 6.9783$ sur $\mathbf{F}_3$, elle donne $N + 1.5259g > 10.526$ sur $\mathbf{F}_4$ et elle s'approxime par $N + 1.7932g > 14.6586$ sur $\mathbf{F}_5$. Pour entier naturel g non nul, on peut trouver une courbe de genre g et vérifiant les inégalités obtenues sur $\mathbf{F}_2$, $\mathbf{F}_3$ et $\mathbf{F}_4$.

4.2.8 Exemple de construction en degré supérieur

On cherche ici à construire une fonction permettant par ce procédé de déterminer une condition pour qu'une courbe ait un angle dans l'intervalle $]\arccos(a), -\arccos(a+\epsilon)[$. On part d'une fonction de degré 2

$$\theta \longmapsto (\cos(\theta) - a)(\cos(\theta) + a + \epsilon)$$

donnant l'intervalle voulu. Cette fonction ne donnant pas de résultats intéressants, on passe au degré 3 avec

$$\theta \longmapsto (\cos(\theta) - a)(\cos(\theta) + a + \epsilon)(\cos(\theta) - b),$$

avec $b \in]-\infty, -1] \bigcup [1, \infty[$, de façon à contrôler l'intervalle des valeurs négatives, mais qui, même optimisé ($b = -1$), n'est pas plus probante. On construit alors une fonction de degré 4 du type

$$\theta \longmapsto (\cos(\theta) - a)(\cos(\theta) + a + \epsilon)(\cos(\theta) - b)^2$$

encore fabriquée de manière à contrôler le signe, puis même de degré 5 avec

$$f(\theta) = (\cos(\theta) - a)(\cos(\theta) + a + \epsilon)(\cos(\theta) - b)(\cos(\theta) - c)^2,$$

avec toujours $b \in]-\infty, -1] \bigcup [1, \infty[$. Cette dernière fonction s'avère plus efficace.

On développe $f(\theta) = \sum_{k=0}^{5} u_k \cos(k\theta)$. En cherchant à minimiser la condition sur N avec $r = \sqrt{2}$ (i.e. en travaillant sur $\mathbf{F}_2$) avec $u_k \geq 0$ pour $k > 1$, on trouve qu'il faut prendre $b = -1$, puis $u_4 = 0$, et enfin $u_3 = 0$. On travaille donc avec

$$f(\theta) = \big(\cos(\theta) - a\big)\big(\cos(\theta) + a + \epsilon\big)\big(\cos(\theta) + 1\big)\big(\cos(\theta) + \frac{a + \epsilon(a)}{2}\big)^2.$$

Pour avoir une condition optimum, il faut donc, pour chaque a, déterminer $\epsilon(a)$ par $u_3 = 0$. Toutes les autres conditions sont en effet satisfaites.

Sans chercher à optimiser, travaillons avec $a = \cos(\frac{\pi}{3})$ et ϵ_1 tel que

$$-a - \epsilon_1 = \cos(\frac{3\pi}{4}),$$

c'est à dire avec la fonction

$$\begin{aligned} f(\theta) &= \big(\cos(\theta) - \frac{1}{2}\big)\big(\cos(\theta) + \frac{\sqrt{2}}{2}\big)\big(\cos(\theta) + 1\big)\big(\cos(\theta) - \frac{1 + \sqrt{2}}{4}\big)^2 \\ &= \frac{3 - 2\sqrt{2}}{64} + \frac{3 - \sqrt{2}}{64}\cos(\theta) + \frac{7 + 2\sqrt{2}}{64}\cos(2\theta) + \frac{3 - 2\sqrt{2}}{64}\cos(3\theta) + \frac{1}{16}\cos(5\theta). \end{aligned}$$

On est dans les conditions du premier choix ; l'étude de ce cas nous donne que toute courbe X a un angle de Frobenius dans $]\frac{\pi}{3}, \frac{3\pi}{4}[$ dès que

$$X \text{ est définie sur } \mathbf{F}_2 \text{ avec } N > 0.0424g + 6.7044,$$
$$X \text{ est définie sur } \mathbf{F}_3 \text{ avec } N > 0.0609g + 18.0362,$$
$$X \text{ est définie sur } \mathbf{F}_4 \text{ avec } N > 0.0770g + 39.5582\ .$$

On trouve des courbes vérifiant (4.2.8) pour tout genre $g \geq 2$, vérifiant (4.2.8) pour tout genre $g \geq 10$, et vérifiant (4.2.8) pour tout genre $g \geq 17$.

Regardons la fonction obtenue avec $a = \cos(\frac{\pi}{4})$ et $-a - \epsilon_1 = -\cos(\frac{\pi}{4})$, soit $\epsilon_1 = 0$:

$$\begin{aligned} f(\theta) &= \big(\cos(\theta) - \frac{\sqrt{2}}{2}\big)\big(\cos(\theta) + \frac{\sqrt{2}}{2}\big)\big(\cos(\theta) + 1\big)\big(\cos(\theta) - \frac{1}{2}\big)^2 \\ &= \frac{1}{16}\cos(\theta) + \frac{1}{8}\cos(2\theta) + \frac{1}{16}\cos(5\theta). \end{aligned} \tag{4.10}$$

On reconnaît le deuxième choix. Toute courbe sur $\mathbf{F}_q$ telle que

$$N > 1 + \frac{q^2 + 2q^{1/2} + 1}{q^2 + 2q^{3/2} + 1} q^3$$

a un angle de Frobenius dans $]\frac{\pi}{4}, \frac{3\pi}{4}[$.

Numériquement, cette condition devient $N > 6.8768$ sur $\mathbf{F}_2$, et $N > 18.8269$ sur $\mathbf{F}_3$. On trouve des courbes candidates pour tout genre $g \geq 3$ sur $\mathbf{F}_2$, et pour tout genre $g \geq 9$ sur $\mathbf{F}_3$. Cependant ces inégalités sont plus mauvaises que celles obtenues en 4.2.7 pour le même intervalle $]\frac{\pi}{4}, \frac{3\pi}{4}[$: pour q proche de l'infini, elle s'approxime par $N > q^3$ au lieu de $N > q^2$, et même, une étude rapide montre que le terme de droite de (4.2.8) est supérieur à $q^2 + 1$ pour tout $q \geq 1$. Le degré était pourtant plus petit en 4.2.7, on va donc chercher à généraliser l'exemple de la section 4.2.7.

4.2.9 Exemple asymptotique

On a vu en 4.2.5 que toute courbe avec $N > r^2 + 1$ a un angle de Frobenius dans $]\pi/2, 3\pi/2[$, puis que toute courbe avec $N > r^3 + 1$ en avait un dans $]\pi/3, \pi[$. De plus, dans la section 4.2.7, on s'est aperçu que toute courbe avec $N > r^4 + 1$ a un tel angle dans $]\pi/4, 3\pi/4[$ (puis que c'était même une 'bonne' condition dans la section suivante). Essayons de trouver plus généralement une condition pour l'existence d'un angle dans $]\pi/n, 3\pi/n[$, n entier naturel quelconque.

Soit $n \geq 4$. La fonction f définie par

$$f(\theta) = 2^{n-3} \prod_{k=2}^{n-1} \big(\cos\theta - \cos(2k+1)\frac{\pi}{n} \big)$$

est négative uniquement sur $]\pi/n, 3\pi/n[$, elle nous permettra donc d'obtenir une condition pour cet intervalle pour peu qu'elle satisfasse à un des cas étudiés. Il s'agit donc maintenant de regarder son développement de Fourrier.

A l'aide par exemple d'une décomposition en éléments simples (ou de façon plus sophistiquée par une fonction génératrice d'un polynôme gaussien [And98]), on montre que

$$\frac{1}{(1-T)(1-yT)(1-y^2T)(1-y^3T)} = \sum_{i\geq 0} \left[\begin{array}{c} i+3 \\ 3 \end{array} \right] T^i$$

où

$$\left[\begin{array}{c} i+3 \\ 3 \end{array} \right] = \frac{(y^{i+3}-1)(y^{i+2}-1)(y^{i+1}-1)}{(y^3-1)(y^2-1)(y-1)}$$

Pour y avec $y^n = 1$, le membre de droite est périodique et, en réindexant avec $j = i+2$,

$$\frac{T^2(1-T^n)}{(1-T)(1-yT)(1-y^2T)(1-y^3T)} = \sum_{j=2}^{n-2} \frac{(y^{j+1}-1)(y^j-1)(y^{j-1}-1)}{(y^3-1)(y^2-1)(y-1)} T^j$$

Prenons $x = e^{i\alpha}$, tel que $x^n = -1$. Avec $y = x^2$ et $t = x^3T$, nous obtenons

$$\frac{(1+t^n)}{(t+t^{-1}-2\cos\alpha)(t+t^{-1}-2\cos 3\alpha)} = \sum_{j=2}^{n-2} \frac{\sin(j-1)\alpha \, \sin j\alpha \, \sin(j+1)\alpha}{\sin\alpha \sin 2\alpha \sin 3\alpha} \, t^j$$

En additionnant les équations trouvées avec $t = e^{i\theta}$ puis $t = e^{-i\theta}$, en divisant par 2, et en factorisant f, on trouve enfin

Lemme 4.2.1 *Tout $\theta \in \mathbf{R}$ vérifie l'égalité*

$$f(\theta) = \frac{1+\cos n\theta}{4(\cos\theta - \cos\frac{\pi}{n})(\cos\theta - \cos 3\frac{\pi}{n})} = \sum_{j=2}^{n-2} u_j \cos j\theta \tag{4.11}$$

avec

$$u_j = \frac{\sin(j-1)\frac{\pi}{n} \, \sin j\frac{\pi}{n} \, \sin(j+1)\frac{\pi}{n}}{\sin\frac{\pi}{n} \, \sin 2\frac{\pi}{n} \, \sin 3\frac{\pi}{n}}. \tag{4.12}$$

La suite $\{u_n\}_{n\in\mathbf{N}}$ vérifie les conditions du deuxième choix. En prenant en compte l'étude précédente des cas $n = 2$ et $n = 3$, on aboutit au résultat suivant :

Proposition 4.2.2 *[DE02] Soit n un entier tel que $n \geq 2$. Soit X une courbe lisse, absolument irréductible, définie sur $\mathbf{F}_q$. Posons $r = \sqrt{q}$, et soit N le nombre de points rationnels de X sur $\mathbf{F}_q$.*

Alors, $N > r^n + 1$ implique que X a un angle de Frobenius dans $]\pi/n, 3\pi/n[$.

On a vu que l'inégalité de la condition doit être stricte pour $n = 2$ et $n = 3$. C'est aussi le cas pour $n = 4$ et $n = 6$. La courbe de Suzuki sur $\mathbf{F}_8$ a $N = 65$ points mais aucun angle dans $]\pi/4, 3\pi/4[$. La courbe de Ree sur $\mathbf{F}_3$ a $N = 28$ points mais aucun angle dans $]\pi/6, 3\pi/6[$.

4.3 Conclusions

Grâce à une étude théorique utilisant les travaux de Tsfasman, Vlăduţ et Serre, nous avons pu poser les problèmes non triviaux suivants.

Problème 1 Étant donné un ensemble discret Γ de $[0, \pi]$, trouver les valeurs maximales possibles de N et g pour une courbe dont les angles de Frobenius sont dans Γ.

Problème 2 Étant donné un intervalle $I \subset [0, \pi]$, trouver les valeurs maximales de N et g pour toute courbe sur $\mathbf{F}_q$ dont les angles de Frobenius sont hors de I.

Nous les avons résolus que pour certains intervalles, mais il reste encore beaucoup à faire. L'objectif final serait de pouvoir construire une table donnant la localisation des angles de Frobenius en fonction du nombre de points rationnels et du genre d'une courbe.

Nous donnons comme autre problème un cas particulier du problème **1** .

Problème 3 Trouver les valeurs maximales de N et g des courbes sur $\mathbf{F}_q$ dont toutes les valeurs propres du Frobenius soient de degré au plus d fixé.

Résoudre le problème **3** avec $d = 2$ correspond aux courbes avec variété jacobienne complètement décomposable. Nous avons résolu le cas $d = 2$ sur $\mathbf{F}_2$, mais le problème reste ouvert pour d'autres corps et d'autres degrés.

L'idéal serait de pouvoir donner une localisation très fine des angles de Frobenius, d'où le dernier problème.

Problème 4 Étant donné $\delta \in \mathbf{R}_+^*$, trouver les maximums possibles de N et g pour une courbe sur $\mathbf{F}_q$ telle que $[0\,,\,\pi] \not\subset \bigcup_j]\theta_j - \delta, \theta_j + \delta[$.

La seule esquisse d'approche de ce problème est le cas asymptotique, il reste donc complètement ouvert.

Annexe A

Théorème d'approximation des valeurs absolues

Nous rappelons ici le théorème d'approximation des valeurs absolues. On peut le trouver dans [Cas]. Nous en donnons la démonstration car elle donne une construction de l'élément g vérifiant $v_p(g - g_i) \geq n_i$ pour tout i où les $(g_i,\, n_i) \in \mathbf{K} \times \mathbf{N}$ sont donnés et finis. Cela confirme l'affirmation du deuxième chapitre

Lemme A.1 *Soit* $\mathbf{K}$ *un corps, doté de* k *valeurs absolues* $|\ |_1, |\ |_2, \ldots, |\ |_k$ *non équivalentes.*

On peut alors construire a *tel que* $|a|_1 > 1$ *et* $|a|_j < 1$ *pour tout entier* j *compris entre* 2 *et* k*.*

Procédons par récurrence

Pour $k = 2$, $|\ |_1$ et $|\ |_2$ ne sont pas équivalentes, on peut donc trouver b et c dans $\mathbf{K}$ tels que

$$\begin{cases} |b|_1 < 1 \text{ et } |b|_2 \geq 1 \\ \text{et} \\ |c|_2 < 1 \text{ et } |c|_2 \geq 1. \end{cases} \tag{A.1}$$

L'élément $a = cb^{-1}$ convient.

Supposons l'énoncé du lemme vrai au rang $k-1$. Par l'hypothèse de récurrence, on peut construire $b \in \mathbf{K}$ tel que

$$|b|_1 > 1 \text{ et } \forall j \in \{2, \ldots, k-1\},\ |b|_j < 1.$$

En utilisant la démonstration au rang 2, on peut construire $c \in \mathbf{K}$ tel que

$$|c|_1 > 1 \text{ et } |b|_k < 1.$$

Si $|b|_k < 1$, $a = b$ convient.
Si $|b|_k = 1$, $a = b^n c$ convient pour n suffisamment grand.
Si $|b|_k > 1$, $a = \frac{b^n}{1+b^n} c = \frac{1}{1+b^{-n}} c$ convient pour n suffisamment grand.

Théorème A.2 *Soit* $\mathbf{K}$ *un corps, doté de* k *valeurs absolues* $|\ |_1, |\ |_2, \ldots, |\ |_k$ *non équivalentes.*

Fixons $g_1, g_2, \ldots, g_k$ k *éléments de* $\mathbf{K}$*. Alors,*

$$\forall \epsilon > 0,\ \exists g \in \mathbf{K} / \ \forall i \in \{1, \ldots, k\},\ v_i(g - g_i) \geq n_i\ .$$

Par le lemme, on peut construire un k-uplet $(c_1, \ldots, c_k) \in \mathbf{K}^k$ tel que pour tout entier $j \in \{1, \ldots, k\}$,

$$|c_j|_j > 1 \text{ et } \forall i \neq j,\ |c_j|_i < 1.$$

Alors,

$$g = \sum_{j=1}^{k} \frac{c_j}{1 + c_j} g_j$$

convient pour n suffisamment grand.

Annexe B

Familles infinies dont le genre tend vers l'infini

L'objectif de cette annexe est de trouver des familles asymptotiquement exactes, pour leurs appliquer les résultats de densité des angles de Frobenius mentionnés par Serre [Ser97]. Nous rappelons tout d'abord la définition d'asymptotiquement exacte, puis nous démontrons qu'une famille infini de courbe dont le genre tend vers l'infini admet une sous-famille vérifiant les condition de cette définition. Cela valide le raisonnement effectué dans la section 4.2.1.

Soit $\mathcal{F} = \{\mathcal{C}_{g_\lambda}\}_\lambda$ une famille de courbes algébriques dont le genre g_λ tend vers l'infini et définies sur un corps fini $\mathbf{K}$. On notera $\mathbf{K}_n$ une extension de degré $n \in \mathbf{N}$ de $\mathbf{K}$. Pour une courbe $\mathcal{C}_g \in \mathcal{F}$, on pose $N_n(\mathcal{C}_g)$ le nombre de points rationnels de $\mathcal{C}_g$ sur $\mathbf{K}_n$.

Rappelons la définition des familles asymptotiquement exactes.

Définition B.1 *Une famille $\mathcal{F} = \{\mathcal{C}_g\}$ de courbes définies sur $\mathbf{K}$ est dite asymptotiquement exacte si tous les quotients $N_r(\mathcal{C}_g)\,/g$ convergent lorsque le genre g tend vers l'infini.*

Cette définition a été introduite par Tsfasman [Tsf92].

L'inégalité de Hasse-Weil s'écrit, pour la courbe $\mathcal{C}_g$ considérée sur $\mathbf{K}_n$ [Wei71],

$$|N_n(\mathcal{C}_g) - (q^n + 1)| \leq 2g\sqrt{q^n}.$$

Ainsi, pour tout entier n,

$$0 \leq \frac{N_n(\mathcal{C}_g)}{g} \leq 2\sqrt{q^n} + \frac{q^n + 1}{g} \leq 4q^n. \tag{B.1}$$

Posons, pour tout $n \in \mathbf{N}$, $K_n = [0,\ 4q^n]$. On déduit des inégalités (B.1), pour tout n et g,

$$\frac{N_n(\mathcal{C}_g)}{g} \in K_n.$$

Ainsi, pour tout g_λ, l'uplet $(\frac{N_1(\mathcal{C}_{g_\lambda})}{g_\lambda}, \frac{N_2(\mathcal{C}_{g_\lambda})}{g_\lambda}, \frac{N_3(\mathcal{C}_{g_\lambda})}{g_\lambda}, \ldots, \frac{N_r(\mathcal{C}_{g_\lambda})}{g_\lambda}, \ldots)$ est élément de l'ensemble $K = \prod_{r\in\mathbf{N}} K_r$. Par le théorème Tychonoff, K est un compact [Bou71]. La suite $(\frac{N_r(\mathcal{C}_{g_\lambda})}{g_\lambda})_\lambda$ admet donc une valeur d'adhérence. On en déduit,

Proposition B.2 *Toute famille infinie de courbes algébriques dont le genre tend vers l'infini admet une sous-famille asymptotiquement exacte.*

Bibliographie

[Adl79] L. ADLEMAN – « A subexponential algorithm for the discrete logarithm problem with applications to cryptography », *Proc. IEEE 20th annual symposium on foundations of computer science* (1979), p. 55–60.

[Adl83] L. ADLEMAN – « On breaking the iterated merke-hellman public key cryptosystem », *Proceeding of the 15th ACM Symposium on the Theory of Computing* (1983), p. 402–412.

[AH28] E. ARTIN et H. HASSE – « Die beiden ergangungsatze zum reziprozitatsgeseitz der l^n-ten potenzrete in korper den l^n-ten », *Hamb Abl* **6** (1928), p. 146–162.

[And98] G. E. ANDREWS – *The theory of partitions*, Cambridge University Press, Cambridge, 1998, Reprint of the 1976 original.

[Bou71] N. BOURBAKI – *Topologie générale*, Hermann, Paris, 1971.

[Bre80] R. P. BRENT – « An improved monte carlo factorization algorithm », *BIT* **20** (1980), p. 176–184.

[Bue89] D. A. BUELL – *Binary quadratic forms*, Springer-Verlag, 1989.

[BW88] J. BUCHMANN et H. WILLIAMS – « A key-exchange system based on imaginary quadratic fields », *Journal of Cryptology* **1** (1988), p. 107–118.

[Can87] D. G. V. CANTOR – « Computing in the jacobian of a hyperelliptic curve », *Mathematics of Computation* **48** (1987), p. 95–101.

[Cas] J. CASSELS – *Local fields*, London Mathematical Society.

[Coh95] H. COHEN – *A course in computational algebraic number theory*, Springer, 1995.

[Cou01] J.-M. COUVEIGNES – « Algebraic groups and discrete logarithm », *Public-Key Cryptography and Computational Number Theory* **1** (2001), p. 17–27.

[Cox89] D. COX – *Primes of the form $x^2 + ny^2$*, John Wiley and Sons, 1989, New York.

[CS98] R. CRAMER et V. SHOUP – « A practical public key cryptosystem provably secure against adaptive chosen ciphertext attacks », *Crypto'98* **1462** (1998), p. 13–25.

[DE02] I. DUURSMA et J.-Y. ENJALBERT – « Bounds », *Finite Fields and Applications Fq6* (2002).

[Dem72] M. DEMAZURE – *Lectures on p-divisible groups,* Springer-Verlag, 1972.

[DGM99] I. DUURSMA, P. GAUDRY et F. MORAIN – « Speeding up the discret log computation on curves with automorphisms », *Advances in Cryptology - Asiacrypt'98* **1716** (1999), p. 103–121.

[DH76] W. DIFFIE et M. HELLMAN – « New directions in cryptography », *IEEE Transaction on Information Theory* **IT-22** (1976), p. 644–654.

[Die57] J. DIEUDONNÉ – « On the artin-hasse exponential series », *Proc. Amer. Math. Soc.* **8** (1957), p. 210–214.

[ECC] « http ://www.certicom.com/ressources/ecc-chall/challenge.htlm ».

[EG85] T. EL GAMAL – « A public key cryptosystem and a signature scheme based on discrete logarithms », *IEEE transactions on Information Theory* **31** (1985), p. 469–472.

[Enj99] J.-Y. ENJALBERT – « Mémoire dea », Université de Limoges, 1999.

[FMR99] G. FREY, M. MÜLLER et H. RÜCK – « The tate pairing and the discrete logarithm applied to elliptic cryptosystems », *IEEE Trans. Inform. Theory* **45** (1999), p. 1717–1719.

[FR94] G. FREY et H. RÜCK – « A remark concerning m-divisibility and the discrete logarithm in divisor class group of curves », *Mathematics of Computation* **62(206)** (1994), p. 865–874.

[Fre] G. FREY – « http ://www.iccip.cls.uiuc.edu ».

[Gal01] S. GALBRAITH – « Supersingular curves in cryptography », *Advances in Cryptology - Asiacrypt 2001* **2248** (2001), p. 495–513.

[Gau00] P. GAUDRY – « An algorithm for solving the discret log problem on hyperelliptic curves », *Advances in Cryptology* **LNCS 1807** (2000), p. 19–34.

[Han95] S. H. HANSEN – *Rational points on curves over finite fields*, Aarhus Universitet Matematisk Institut, Aarhus, 1995.

[Har] « http ://pauillac.inria.fr/ harley ».

[Har77] R. HARTSHORNE – *Algebraic geometry*, Springer, 1977.

[HJPT01] D. HUHLEIN, M. J. JACOBSON, S. PAULUS et T. TAKAGI – « A cryptosystem based on non-maximal imaginary quadratic orders with fast description », *Advances in Cryptology - Eurocrypt'98* (2001), p. 295–306.

[HP93] J. P. HANSEN et J. P. PEDERSEN – « Automorphism groups of Ree type, Deligne-Lusztig curves and function fields », *J. Reine Angew. Math.* **440** (1993), p. 99–109.

[HS90] J. P. HANSEN et H. STICHTENOTH – « Group codes on certain algebraic curves with many rational points », *Appl. Algebra Engrg. Comm. Comput.* **1** (1990), p. 67–77.

[Iha81] Y. IHARA – « Some remarks on the number of rational points of algebraic curves over finite fields », *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 3, p. 721–724 (1982).

[Iya75] S. IYANAGA – *The theory of numbers*, North-Holland Mathematical Library, 1975.

[Knu81] D. KNUTH – *The art of computer programming*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1981, Vol. 2, 2nd édition.

[Kob87] N. KOBLITZ – « Elliptic curve cryptosystems », *Math. Comp.* **48(177)** (1987), p. 203–209.

[Kob89] — , « Hyperelliptic cryptosystems », *Journal of Cryptology* **1** (1989), p. 139–150.

[Lan56] S. LANG – « Algebraic groups over finite fields », *American Journal of Mathematic* **78** (1956), p. 555–563.

[Lan58] — , *Introduction to algebraic geometry*, New-York, 1958, Interscience.

[Lan83] — , *Abelian varieties*, Springer-Verlag, 1983.

[Ler] « http ://www.medicis.polytechnique.fr/∼lercier/francais/dlog.htlm ».

[Lig77] G. LIGOZAT – « Courbes modulaires de niveau 11 », Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn,

Bonn, 1976), Springer, Berlin, 1977, p. 149–237. Lecture Notes in Math., Vol. 601.

[Mil86] V. MILLER – « Use of elliptic curves in cryptography », *Advances in Cryptology - CRYPTO'86* **263** (1986), p. 417–426.

[Mor97] F. MORAIN – « Courbes elliptiques, arithmétique et corps finis », Habilitation à diriger des recherches, Université Paris 6, 1997.

[MOV95] A. MENEZES, T. OKAMOTO et A. VANSTONE – « Reducing elliptic curves over finite fields : strategies and performances », *Advances in Cryptology - Eurocrypt'95* **921** (1995), p. 79–94.

[Ogg69] A. OGG – *Modular forms and dirichlet series*, W.A. Benjamin, 1969, New York.

[Per81] D. PERRIN – *Cours d'algèbre*, ENS, 1981.

[Per93] — , *Introduction à la géométrie algébrique*, Paris Onze Edition, 1993.

[Pol78] J. POLLARD – « Monte carlo methods for index computation $(\mathrm{mod}\ p)$ », *IEEE - Transactions on Information Theory* **24** (1978), p. 437–447.

[Ros54] M. ROSENLICHT – « Generalized jacobian varieties », *Ann. of Math.* **59** (1954), p. 505–530.

[RS94] H.-G. RÜCK et H. STICHTENOTH – « A characterization of Hermitian function fields over finite fields », *J. Reine Angew. Math.* **457** (1994), p. 185–188.

[RSA] « http ://www.lix.polytechnique.fr/labo/francois.morain/rsa155.htlm ».

[RSA78] M. RIVEST, A. SHAMIR et A. ADLEMAN – « A method for obtaining digital signatures and public-key cryptosystems », *ACM Communications* **21** (1978), p. 120–126.

[Sam67] P. SAMUEL – *Théorie algébrique des nombres*, Hermann, 1967.

[Sam81] — , *Méthode d'algèbre abstraite en géométrie algébrique*, Springer, 1981, Ergeb. der Math.

[Ser59] J.-P. SERRE – *Groupes algébriques et corps de classes*, Herman, 1959, Publications de l'institut de Mathématique de l'Université de Nancago.

[Ser64] — , *Cohomologie galoisienne*, Springer-Verlag, 1964, Lecture Notes in Mathematics.

[Ser83] — , « Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini », *C. R. Acad. Sci. Paris Sér. I Math.* **296** (1983), no. 9, p. 397–402.

[Ser97] — , « Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p », *J. Amer. Math. Soc.* **10** (1997), no. 1, p. 75–102.

[Sha71a] D. SHANKS – « Class number, a theory of factorization and genera », *Proc. Symp. Pure Math.* **20** (1971), p. 415–440.

[Sha71b] — , « A theory of factorization, and genera », *Proc. Sympos Pures Math* **20** (1971), p. 415–440.

[Sha77] I. SHAFAREVICH – *Basic algebraic geometry*, Springer-Verlag, 1977.

[Sho01] V. SHOUP – « Lower bounds for discrete logarithms and related problems », *Advances in Cryptology - Eurocrypt'97* **1233** (2001), p. 256–266.

[Sil85] J. H. SILVERMAN – *The arithmetic of elliptic curves*, Springer-Verlag, 1985.

[Sil98] — , « The xedni calculus and the elliptic curve discrete logarithm problem », *Brown university* (1998).

[SL84] C. SCHNORR et H. LENSTRA – « A monte carlo factorization algorithm with linear storage », *Mathematics of Computation* **43(167)** (1984), p. 289–311.

[SS85] J. SATTLER et C. SCHNORR – « Generating random walks in groups », *Ann.-Univ.-Sci.-Budapest.-Sect.-Comput.* **67** (1985), p. 65–79.

[Ste] S. A. STEPANOV – *Codes on algebraic curves*, Klumer academic, Plenum Publishers.

[Tes98a] E. TESKE – « A space efficient algorithm for group structure computation », *Mathematics of Computation* **67** (1998), p. 1637–1663.

[Tes98b] — , « Speeding up pollard's rho method for computing discrete logarithms », *Algorithmic Number Theory Seminar ANTS-III* **1423** (1998), p. 541–554.

[Tes01] — , « Square-root algorithms for the discrete logarithm problem », *Mathematics Subject Classification* (2001), p. 1–27.

[Tho01] E. THOMÉ – « Computation of discrete logarithms in $\mathbf{gf}(2^{607})$ », *Asiacrypt* **LNCS 2248** (2001), p. 107–124.

[Tsf92] M. A. TSFASMAN – « Some remarks on the asymptotic number of points », Coding theory and algebraic geometry (Luminy, 1991), Springer, Berlin, 1992, p. 178–192.

[TV97] M. A. TSFASMAN et S. G. VLĂDUŢ – « Asymptotic properties of zeta-functions », *J. Math. Sci. (New York)* **84** (1997), no. 5, p. 1445–1467, Algebraic geometry, 7.

[VD83] S. G. VLĂDUŢ et V. G. DRINFELḌ – « The number of points of an algebraic curve », *Funktsional. Anal. i Prilozhen.* **17** (1983), no. 1, p. 68–69.

[vdGvdV91] G. VAN DER GEER et M. VAN DER VLUGT – « Tables of curves with many points », *Mathematics Subjet Classification* (1991), p. 497–508.

[vdGvdV00] — , « Tables of curves with many points », *Math. Comp.* **69(230)** (2000), p. 797–810.

[vOW99] P. C. VAN OORSCHOT et J. M. WIENER – « Parallel collision search with cryptanalytic applications », *Journal of Cryptology* **12** (1999), p. 1–28.

[Wei49] A. WEIL – « Number of solutions of equations in finite fields », *Bull. AMS* **55** (1949), p. 497–508.

[Wei71] — , *Courbes algébriques et variétés abéliennes*, Hermann, Paris, 1971.

[Wit36] E. WITT – « Zyklische korper und algebren der charakteristik p vom grad p^n », *J. Reine Angez. Math.* **176** (1936), p. 126–140.

Résumé

L'objectif premier de cette thèse est d'étudier le problème du logarithme discret dans des groupes constitués de jacobiennes généralisées de courbes irréductibles non singulières. Nous donnons tout d'abord un état de l'art de ce problème et de ses diverses attaques connues. Nous étudions ensuite les jacobiennes généralisées et exhibons leurs liens avec des groupes de classes d'ordres. Nous reportons alors nos visées cryptographiques à ces groupes de classes : nous donnons des applications cryptographiques utilisant des corps quadratiques, et nous utilisons les groupes de classes pour construire des exemples permettant de tester les attaques connues. Nous finissons par l'étude des courbes utilisées. Nous donnons des majorations du genre et du nombre de points rationnels de certaines de ces courbes, ainsi que des conditions permettant de localiser leurs angles de Frobenius.

Mots-clés: cryptographie, logarithme discret, jacobiennes généralisées, extensions quadratiques, courbes sur les corps finis, angles de Frobenius

Abstract

In this thesis we study the discrete logarithm problem in the generalized Jacobians. Thus we begin with a description of the discret logarithm problem and the various known attacks. Thereafter we study generalized Jacobians and give the link with the class group of orders. We then relate our cryptographic goals to these class groups : we give some applications of cryptography using quadratic fields and we use the class group to construct examples on wich know attacks can be tested. We finish with the study of irreductible nonsingular curves, for them we construct the generalized Jacobians we need. We give bounds for genus and for numbers of rational points for some of these curves, and we derive conditions that can be used to locate the Frobenius angles.

Keywords: Cryptography, Discret Logarithm, Generalized Jacobians, Quadratic Extensions, Curves over Finite Fields, Frobenius Angles