(QUELQUES) ASPECTS ALGORITHMIQUES DE LA THÉORIE ALGÉBRIQUE DES NOMBRES

K. BELABAS

Résumé. Dans ce cours, nous examinons une partie de la théorie algébrique des nombres élémentaire d'un point de vue algorithmique, en se restreignant au cas des corps de nombres. On définit d'abord les ordres, en particulier l'ordre $\mathcal{O}_T$ associé par Dedekind à une équation du corps, puis le procédé « Round 2 » de normalisation de Zassenhaus. Dans le cas où l'ordre $\mathcal{O}_T$ est p-maximal, un théorème de Kummer détermine la décomposition du nombre premier p à partir de la factorisation de T modulo p. Le critère de Dedekind, conséquence de celui de Zassenhaus, permet de déterminer si ce résultat s'applique ; d'après Hensel, la seule obstruction est un nombre insuffisant de polynômes irréductibles de degré convenable dans $\mathbb{F}_p[X]$. La décomposition d'un p général se ramène aussi à un problème de factorisation, via la décomposition d'une $\mathbb{F}_p$-algèbre séparable, en utilisant le p-radical d'un ordre p-maximal quelconque.

On donne ensuite une application aux corps cubiques, en retrouvant le théorème de Davenport-Heilbronn qui paramètre les ordres cubiques maximaux. Finalement, on explique comment calculer groupes de classes et unités par la méthode du calcul d'indice, ainsi qu'une façon de résoudre le problème du logarithme discret associé à $\mathrm{Cl}(\mathcal{O}_K)$. L'omission la plus flagrante est la théorie de Galois effective.

Table des matières

Date: 1 Septembre 2003.

1. Introduction

1.1. **Motivations.** Un premier cours de théorie algébrique des nombres commence généralement par la théorie des corps (corps finis, théorie de Galois), puis introduit l'arithmétique : anneaux de Dedekind, finitude du groupe des classes, structure des unités. On passe ensuite aux sujets plus avancés : corps de classe, théorie d'Iwasawa, structures galoisiennes, cohomologie, K-théorie algébrique...

On s'intéresse dans ce cours (largement inspiré par Lenstra [3] et les livres d'Henri Cohen [1, 2]) à l'approche algorithmique de ces problèmes. À partir de données explicites, quelles quantités sont effectivement calculables ? Comment et sous quelle forme ? En quel temps ?

De ce point de vue, l'essentiel des difficultés se situe au niveau des points « élémentaires », qui sont pour l'essentiel mal résolus, et dont même la calculabilité n'est pas complètement triviale. Par exemple le théorème d'existence de Takagi qui couronne la plupart des cours de théorie du corps de classe a une traduction algorithmique simpliste, sans aucun rapport avec la difficulté de sa démonstration : une fois que l'on *sait* qu'une extension existe, on la cherche dans une liste finie obtenue par théorie de Kummer, en adjoignant au besoin les racines de l'unité manquantes au corps de base. La vraie difficulté pratique se situe au niveau du calcul d'un groupe de classes. (Il reste un énorme travail à faire pour rendre cette description simpliste praticable !)

Quelques motivations pour une telle approche :

- beauté/intérêt intrinsèque des algorithmes.
- intérêt pédagogique, exemples, expérimentation.
- vérification, démonstration automatisée d'un ensemble fini de cas.
- étape pour la résolution d'autres problèmes particuliers (équations diophantiennes, factorisation d'entiers par NFS...).
- meilleure compréhension des outils informatiques disponibles, par exemple Magma ou Pari/gp en théorie algébrique des nombres.

1.2. **Complexité.** On ne définira pas *algorithme*, *temps de calcul*. Informellement, un algorithme est *bon* s'il s'exécute en un temps polynomial en la taille des données. Pour un algorithme probabiliste, qui fait des choix aléatoires, on veut

que l'espérance du temps de calcul soit polynomiale. Un problème est *facile* si on connaît un bon algorithme (déterministe ou probabiliste) pour le résoudre, et *difficile* sinon.

Ce n'est pas une définition très raisonnable : la classe des problèmes « difficiles » a tendance à se résorber ; à l'inverse, une modification anodine [1] d'un problème facile peut le rendre difficile. Donc sans spécification du modèle de calcul, on bâtit sur du sable. Mais on peut déjà dire des choses intéressantes à partir de cette approche naïve. Il est aussi utile de distinguer plus finement entre bons, ou moins bons, algorithmes. Dans ce survol, on ne s'en préoccupera pas, ou à peine.

Exemples :

- Facile : primalité sur $\mathbb{Z}$ (AKS, 2002), factorisation sur $\mathbb{Q}[X]$ (LLL, 1982) ou sur $\mathbb{F}_q[X]$, construction d'un corps fini $\mathbb{F}_{p^n}$.
- Difficile : factorisation sur $\mathbb{Z}$, groupe de Galois d'une équation.

Si on rejette les algorithmes probabilistes, alors la factorisation sur $\mathbb{F}_q[X]$ et la construction d'un corps fini deviennent difficiles (l'irréductibilité reste facile). Même le calcul d'une racine carrée ou la construction d'un corps quadratique $\mathbb{F}_{p^2}$ sont difficiles dans ce cadre. *Si* l'Hypothèse de Riemann Généralisée (GRH) est vraie, construire $\mathbb{F}_{p^n}$ redevient facile ; plus précisément, on dispose d'un bon algorithme qui pour chaque valeur de (n, p) fixée, soit construit un polynôme irréductible de degré n sur $\mathbb{F}_p$, soit prouve que GRH est fausse.

1.3. **Exemple.** soit p un nombre premier et $G = (\mathbb{Z}/p\mathbb{Z})^*$ le groupe multiplicatif du corps fini associé. Quelques descriptions possibles :

- théorique : $G \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ est cyclique.
- pseudo-effective : $G = \mathbb{Z}/(p-1)\mathbb{Z} \cdot g$, où on fixe un générateur g pour fixer un isomorphisme.

  Calculabilité : la recherche de g se fait en temps fini en calculant l'ordre des éléments successifs de G.

  Complexité : En supposant que la factorisation de $p-1$ est connue, on a un bon algorithme pour calculer cet ordre. Sous GRH (pour les caractères mod p), il existe un générateur de représentant $O(\log^2 p)$. On a donc un bon algorithme en testant $2, 3, \ldots$ Seul le caractère polynomial est conditionnel.
- effective : comme la précédente mais, pour que l'isomorphisme soit effectif, il faut savoir résoudre le problème du logarithme discret dans G : étant donné $a \in G$, trouver l'unique $x := \log_g a \in \mathbb{Z}/(p-1)\mathbb{Z}$ tel que $g^x = a$.

Plus généralement pour décrire un groupe abélien de type fini, on le représente sous la forme

$$G = \oplus_{i=1}^{g} (\mathbb{Z}/d_i\mathbb{Z})g_i, \quad \text{où } d_1 \mid \cdots \mid d_g$$

[1] Par exemple exiger un algorithme déterministe, ou demander un bon comportement sur des données creuses (on mesure alors la taille en fonction du nombre de coefficients non nuls d'un polynôme, par exemple, et non plus en fonction de son degré).

Le problème du logarithme discret correspondant est le plus souvent difficile.

1.4. **Notations.** Dans la suite, on fixe $K/\mathbb{Q}$ un corps de nombres, c'est-à-dire une extension finie de $\mathbb{Q}$, $n := \dim_{\mathbb{Q}} K < \infty$. On supposera[2] que K est donné par le polynôme minimal T d'un élément primitif. En d'autres termes $K = \mathbb{Q}[X]/(T)$; on note $\theta = X \pmod T$, soit $K = \mathbb{Q}(\theta)$. On supposera que $T \in \mathbb{Z}[X]$.

Dans une première partie, on s'intéressera aux ordres de K et en particulier à son anneau d'entiers $\mathcal{O}_K$. Dans une deuxième, on parlera de groupes de classes et d'unités.

2. Ordres

Il y a d'intéressantes généralisations de ces notions dans le cadre de l'algèbre effective (anneaux noethériens de dimension 1, éventuellement intègres), qui permettent en particulier de traiter parallèlement corps de nombres et corps de fonctions d'une variable. Ici, nous adoptons un point de vue terre à terre, centré sur le cas des corps de nombres, en admettant un minimum d'algèbre commutative élémentaire.

Pour de nombreuses applications, on n'a pas besoin de connaître $\mathcal{O}_K$, mais seulement un sous-anneau qui en est une approximation raisonnable. On peut citer la décomposition des nombres premiers, la factorisation dans $K[X]$ donc les problèmes d'isomorphisme ou du sous-corps (a-t-on $L \subset K$?), la détermination de l'ensemble des sous-corps, du groupe de Galois de $K/\mathbb{Q}$...

2.1. **Définitions.** Un *ordre*[3] de K est un sous-anneau (donc contenant 1) qui est un $\mathbb{Z}$-module de rang n (*autre* : de type fini, de corps de fractions K ; *autre* : sous-anneau de $\mathcal{O}_K$ de rang maximal ; *autre* : si $\mathcal{O}$ est un anneau intègre libre de type fini comme $\mathbb{Z}$-module, alors $\mathcal{O}$ est un ordre de $\operatorname{Frac}\mathcal{O}$). Les ordres de K sont partiellement ordonnés par inclusion.

Proposition 2.1. *L'anneau $\mathcal{O}_K$ des entiers algébriques de K est son ordre maximal.*

Preuve. $\mathcal{O}_K$ est un ordre. Soit $\mathcal{O}$ un ordre de K et $\alpha \in \mathcal{O}$, alors $\mathbb{Z}[\alpha] \subset \mathcal{O}$ est de type fini donc α est entier. □

Un $\mathcal{O}$-idéal fractionnaire[4] $\mathfrak{a}$ est un sous $\mathcal{O}$-module de type fini de K. En particulier, $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de type fini et il existe $d \in \mathbb{N}_{>0}$ tel que $d\mathfrak{a}$ soit un idéal de $\mathcal{O}$.

[2]Il y a de très nombreux autres points de vue possibles, qui ont tous leur intérêt, par exemple $K \xhookrightarrow{\sigma} \mathbb{C}$ (on fixe un plongement explicite), K corps de décomposition ou donné par une tour d'extensions, K compositum de sous-corps, corps fixe donné par théorie de Galois, extension donnée par théorie du corps de classe...

[3]Introduit par Dedekind (*Ordnung*) comme anneau de stabilisateurs $(A : A)$ d'un $\mathbb{Z}$-module de type fini A. Généralise la notion introduite par Gauss pour les formes quadratiques binaires de discriminant fixé (*ordo,-inis* = rangée, file).

[4]*ganz/gebrochen* (=entier/cassé) chez Dedekind.

Les ordres non maximaux sont de braves anneaux intègres (noethériens, de dimension 1…) de corps de fraction K, mais ils gardent des comportement pathologiques par rapport à l'anneau de Dedekind $\mathcal{O}_K$. Par exemple, la norme $N\mathfrak{a} := \mathcal{O}/\mathfrak{a}$ d'un idéal non nul est bien définie mais n'est plus multiplicative, il existe des idéaux non inversibles, $\mathfrak{a} \subset \mathfrak{b}$ n'implique pas $\mathfrak{b} \mid \mathfrak{a}$ (il existe un $\mathcal{O}$-idéal fractionnaire $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$), etc. Par contre il est très facile d'en construire :

Exemple : Supposons que $T \in \mathbb{Z}[X]$ est *unitaire*. Alors

$$\mathcal{O}_T := \left\langle 1, \theta, \dots, \theta^{n-1} \right\rangle_{\mathbb{Z}} = \mathbb{Z}[\theta]$$

est un ordre.

Exemple : (Dedekind) Dans le cas général, soit $T(X) = a_0 X^n + \cdots + a_n$; on définit une suite (T_i) de polynômes de degré $i < n$:

$$T_0 := a_0 \quad \text{et} \quad T_{i+1} := XT_i + a_{i+1}, \text{ pour } 0 \leqslant i < n.$$

En particulier $T_n = T$: on a écrit un schéma d'évaluation de Horner pour T. Alors $\mathcal{O}_T := \langle 1, T_1(\theta), \dots, T_{n-1}(\theta) \rangle_{\mathbb{Z}}$ est un ordre. Si $a_0 = \pm 1$, on retrouve l'exemple précédent.

Preuve. Posons $t_i := T_i(\theta)$ pour $0 \leqslant i \leqslant n$. Pour $1 \leqslant i \leqslant j < n$, on a

$$t_i t_j = (\theta t_{i-1} + a_i) t_j = a_i t_j + t_{i-1}(t_{j+1} - a_{j+1}) \equiv t_{i-1} t_{j+1} \mod \mathcal{O}.$$

En itérant, on se ramène au cas de $t_i t_n$ ou $t_0 t_j$; le premier est nul, le deuxième égal à $a_0 t_j \in \mathcal{O}$. Donc ce $\mathbb{Z}$-module de rang au plus n est un anneau. Il contient $a_0\theta$, donc on a bien $\operatorname{Frac} \mathcal{O} = K$. *Autre* : il est de rang n car sa base est échelonnée. □

Plus généralement, les ordres apparaissent comme « anneaux de stabilisateurs ». Si A et B sont deux sous-$\mathbb{Z}$-modules de K, on note

$$(A : B) := \{\alpha \in K, \alpha B \subset A\},$$

souvent appelé transporteur de B dans A, ou « A divisé par B ». C'est un $\mathbb{Z}$-module.

Proposition 2.2. *Si* $\operatorname{rg}_{\mathbb{Z}} A = n$, *alors* $\mathcal{O} = (A : A)$ *est un ordre.*

Preuve. C'est évidemment un anneau. Tout $\alpha \in \mathcal{O}$ est entier (en effet $M := A$ est un $\mathbb{Z}$-module de type fini tel que $\alpha M \subset M$), donc $\mathcal{O} \subset \mathcal{O}_K$ est de type fini. Comme A est de type fini et $A \otimes_{\mathbb{Z}} \mathbb{Q} = K$, il existe $d \in \mathbb{N}_{>0}$ tel que $d\mathcal{O}_K A \subset A$, donc $\mathcal{O} \supset d\mathcal{O}_K$ est de rang n. □

Exemple : on pose $A := \langle 1, \theta, \dots, \theta^{n-1} \rangle_{\mathbb{Z}}$ ($\neq \mathbb{Z}[\theta]$ en général !). Si $T \in \mathbb{Z}[X]$ est de contenu 1, qu'il soit unitaire ou non, on obtient $\mathcal{O}_T = (A : A)$.

Remarque 2.3. Si A est un $\mathcal{O}$-idéal fractionnaire inversible[5], alors $A^{-1} = (\mathcal{O} : A)$. En particulier si $\mathcal{O} = \mathcal{O}_K$ est de Dedekind, on a $(A : B) = AB^{-1}$ pour tous idéaux fractionnaires A, B ($B \neq 0$).

[5]Il existe un $\mathcal{O}$-idéal fractionnaire noté A^{-1} tel que $AA^{-1} = \mathcal{O}$.

En un certain sens, la notion d'ordre est duale de celle de localisé : un ordre est un sous-anneau de $\mathcal{O}_K$ de type fini comme $\mathbb{Z}$-module, mais non intégralement clos (si $\mathcal{O} \neq \mathcal{O}_K$). Un localisé $S^{-1}\mathcal{O}_K$ est un sur-anneau intégralement clos, non de type fini (si $S^{-1}\mathcal{O}_K \neq \mathcal{O}_K$). Géométriquement elle correspond à la notion de courbe singulière : sur la courbe $(\operatorname{spec}\mathcal{O}, \mathcal{O})$, un nombre fini de localisés $\mathcal{O}_{\mathfrak{p}}$ ne sont pas des anneaux de valuation discrètes.

2.2. **Représentation et dénominateurs.** L'écriture $K = \mathbb{Q}[X]/(T)$ donne une représentation canonique pour les éléments de K (polynôme représentant de degré minimal, obtenu par division euclidienne), et de bons algorithmes pour les opérations de corps (Euclide étendu pour l'inverse).

Si $\mathcal{O}$ est un ordre fixé[6], on peut représenter ses sous-$\mathbb{Z}$-modules par une $\mathbb{Z}$-base. Un des principes de l'algorithmique arithmétique est de transformer presque tous les problèmes arithmétiques en algèbre linéaire. On utilisera intensivement le fait suivant : l'algèbre linéaire sur un corps fini ou sur $\mathbb{Z}$ est facile. Par là nous entendons plus précisément le calcul de noyaux, images, conoyaux, polynômes caractéristiques. Sur un corps fini cela suit du pivot de Gauss, sur $\mathbb{Z}$ de la forme normale d'Hermite[7]. En particulier, il est facile de transformer un système fini de $\mathbb{Z}$-générateurs en une $\mathbb{Z}$-base. On en déduit de bons algorithmes pour le calcul de $A \cap B$, $A + B$, AB, $(A : B)\ldots$

Pour manipuler un sous $\mathbb{Z}$-module de type fini M de K, par exemple un idéal fractionnaire, on choisit un entier $d \in \mathbb{N}_{>0}$, unique si on l'impose minimal, tel que $dM \subset \mathcal{O}$, et on est ramené au cas précédent. Si $\mathcal{O} = \mathcal{O}_K$, les dénominateurs d, et plus généralement les coûts de manipulation dans la représentation choisie, sont aussi petits que possible. Dans le cas général, un élément $\alpha \in \mathcal{O}_K$ a un dénominateur divisant l'exposant du groupe additif $\mathcal{O}_K/\mathcal{O}$.

2.3. **Discriminant.**

Définition 2.4. Si $\mathcal{O} = \langle w_1, \ldots, w_n\rangle_{\mathbb{Z}}$ est un ordre de K, on appelle *discriminant* de $\mathcal{O}$ la quantité

$$\operatorname{disc}\mathcal{O} := \det(\operatorname{Tr}(w_i w_j))_{1\leqslant i,j\leqslant n},$$

où $\operatorname{Tr} : K \to \mathbb{Q}$ est la trace absolue. Il ne dépend pas de la $\mathbb{Z}$-base choisie.

Lemme 2.5. *Si $\sigma_1, \ldots, \sigma_n$ sont les n plongements complexes[8] de K dans $\mathbb{C}$, et $\mathcal{O} = \langle w_1, \ldots, w_n\rangle$, on a*

$$\operatorname{disc}\mathcal{O} = (\det(\sigma_i(w_j)))^2.$$

[6]Pour être correct dans les estimations de complexité, il faut le supposer donné par une base (w_i) et la table de multiplication correspondante $w_i w_j = \sum a_{i,j,k} w_k$, où $a_{i,j,k} \in \mathbb{Z}$.

[7]C'est non trivial : contrairement au cas des corps finis, $O(n^3)$ opérations dans $\mathbb{Z}$ ne garantissent pas contre l'explosion des coefficients. Il faut une méthode modulaire élaborée, due à Hafner et McCurley (1991).

[8]donnés par $x \mapsto x_i$ si $(x_1, \ldots, x_n)$ sont les racines complexes de T.

Définition 2.6. Si $T \in \mathbb{Q}[X]$ est un polynôme de degré n, de coefficient dominant a_0, on pose

$$\operatorname{disc}(T) := (-1)^{n(n-1)/2} \frac{\operatorname{Res}(T, T')}{a_0}.$$

Exemple : Dans l'exemple du §2.1, on a $\operatorname{disc} \mathcal{O}_T = \operatorname{disc}(T)$.

Preuve. Avec le calcul d'un déterminant de Vandermonde, on obtient

$$\operatorname{disc} \mathcal{O}_T = (a_0^{n-1} \det(T_j(\sigma_i(\theta))/a_0))^2 = a_0^{2n-2} \prod_{i<j} (\sigma_j(\theta) - \sigma_i(\theta))^2.$$

De même, on a

$$\operatorname{Res}(T, T')/a_0 = a_0^{2n-2} \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta)).$$

□

Proposition 2.7. *Si $\mathcal{O} \subset \mathcal{O}_K$ est un ordre, alors* $\operatorname{disc} \mathcal{O} = [\mathcal{O}_K : \mathcal{O}]^2 \operatorname{disc} \mathcal{O}_K$.

Preuve. diviseurs élémentaires. □

3. Normalisation

Le calcul de $\mathcal{O}_K$ est un problème local : à partir d'un ordre $\mathcal{O}$ quelconque, par exemple $\mathcal{O} = \mathcal{O}_T$, il suffit de calculer la clôture intégrale des localisés $\mathcal{O}_{\mathfrak{p}}$ pour chaque $\mathfrak{p} \mid p$, où $p^2 \mid \operatorname{disc} \mathcal{O}$. Mais d'un point de vue algorithmique, la vraie obstruction est globale :

Théorème 3.1 (Chistov)**.** *Les deux problèmes suivants sont de même difficulté :*

- *étant donné un corps de nombre K, trouver $\mathcal{O}_K$,*
- *étant donné un entier D, trouver le plus grand entier $d \mid D$ qui soit sans facteur carré.*

Pour les mêmes raisons, tester si un ordre donné est maximal est difficile : il faut décider si un entier est sans facteur carré. Pour s'en convaincre, considérer $\mathbb{Z}[\sqrt{D}] \subset \mathbb{Q}(\sqrt{D})$.

On va maintenant examiner le problème local pour donner une idée de la méthode.

3.1. L'algorithme Round 2.

Définition 3.2. Soit m un entier. Un ordre $\mathcal{O} \subset \mathcal{O}_K$ est dit *m-maximal* si $\operatorname{pgcd}(m, [\mathcal{O}_K : \mathcal{O}]) = 1$.

Soit $\mathcal{O}$ un ordre et p un nombre premier. On désire calculer l'ordre p-maximal R, $\mathcal{O} \subset R \subset \mathcal{O}_K$, tel que $[R : \mathcal{O}]$ soit une puissance de p. Explicitement

$$R := \{x \in \mathcal{O}_K,\ p^n x \in \mathcal{O} \text{ pour } n \gg 1\}.$$

On note $I_p := \mathrm{rad}(p\mathcal{O})$ l'idéal radical de $p\mathcal{O}$: par définition $I_p/p\mathcal{O}$ est le nilradical (l'idéal des nilpotents) de $\mathcal{O}/p\mathcal{O}$ et I_p en est le relèvement dans $\mathcal{O}$. C'est aussi l'intersection des idéaux premiers de $\mathcal{O}$ contenant p,

$$I_p := \bigcap_{\mathfrak{p}:\, p\in\mathfrak{p}} \mathfrak{p} = \prod_{\mathfrak{p}:\, p\in\mathfrak{p}} \mathfrak{p}$$

Ces idéaux premiers sont en nombre fini et ils sont maximaux.

Il est facile de calculer I_p : si t est un entier tel que $p^t \geqslant n = \dim_{\mathbb{Q}} K$, alors $\mathcal{O}/p\mathcal{O}$ est un $\mathbb{F}_p$-ev de dimension n et $I_p/p\mathcal{O}$ est le noyau de l'application $\mathbb{F}_p$-linéaire $x \mapsto x^{p^t}$. Si $p > n$, c'est aussi le noyau de

$$\begin{array}{rcl} \mathcal{O}/p\mathcal{O} & \to & \mathrm{Hom}(\mathcal{O}/p\mathcal{O}, \mathbb{F}_p) \\ x & \mapsto & (y \mapsto \mathrm{Tr}(xy)) \end{array}$$

Preuve. Soit u un endomorphisme d'un $\mathbb{F}_p$-ev de dimension finie $n < p$; si $\mathrm{Tr}(u^k) = 0$ pour tout k, alors u est nilpotent (formules de Newton + Cayley-Hamilton par exemple). Donc un élément du noyau appartient à I_p (en choisissant $y = 1, x, x^2, \dots$). Réciproquement, tout nilpotent est de trace nulle. □

La deuxième description est préférable quand p est grand : la première requiert $O(n \log p^t)$ multiplications dans $\mathcal{O}/p\mathcal{O}$; dans la deuxième ce nombre ne dépend pas de p (mais le coût des opérations dans $\mathcal{O}/p\mathcal{O}$, si).

L'algorithme Round 2 de Zassenhaus est un bijou, issu du théorème suivant :

Théorème 3.3 (Zassenhaus)**.** *Soit $\mathcal{O}' := (I_p : I_p)$. L'ordre $\mathcal{O}$ est p-maximal si et seulement si $\mathcal{O} = \mathcal{O}'$.*

Idée : on veut vérifier que les maximaux contenant p sont inversibles ; il suffit de vérifier que leur produit l'est.

Preuve. $\mathcal{O}'$ est un ordre contenant $\mathcal{O}$ (car I_p est un $\mathcal{O}$-idéal) ; comme $p \in I_p \subset \mathcal{O}$, on obtient $p\mathcal{O}' \subset \mathcal{O}$ donc $[\mathcal{O}' : \mathcal{O}] \mid p^n$. D'où $\mathcal{O} = \mathcal{O}'$ si $\mathcal{O}$ est p-maximal.

Réciproquement, si $\mathcal{O} = \mathcal{O}'$, soit R l'ordre p-maximal contenant $\mathcal{O}$ du début de la section. Par l'absurde, supposons qu'il existe $m \geqslant 0$ tel que $RI_p^m \not\subset \mathcal{O}$ et choisissons m maximal, puis $\alpha \in RI_p^m \setminus \mathcal{O}$. Alors $\alpha I_p \subset \mathcal{O}$ et donc $\alpha I_p \subset I_p$ (comme I_p est de type fini, il existe k tel que $I_p^k \subset p\mathcal{O}$), soit $\alpha \in (I_p : I_p) = \mathcal{O}$. Absurde. □

L'algorithme de normalisation est immédiat : on part de $\mathcal{O} = \mathcal{O}_T$; on calcule $I_p/p\mathcal{O}$ et on remplace $\mathcal{O}$ par $\mathcal{O}' := (I_p : I_p)$ tant que $\mathcal{O} \neq \mathcal{O}'$. C'est un bon algorithme, qu'il suffit d'appliquer à tous les p premiers tels que $p^2 \mid \mathrm{disc}\,\mathcal{O}$. À condition de les connaître !

Cet algorithme a ceci de remarquable qu'on peut remplacer p par un entier m sans facteurs carrés arbitraire (Buchmann-Lenstra). Soit l'algorithme rencontre une impossibilité qui exhibe un facteur de m (un élément non nul mais non inversible de $\mathbb{Z}/m\mathbb{Z}$), soit il produit un ordre m-maximal. La philosophie générale

du calcul modulaire indique cependant que c'est une mauvaise idée de commencer par multiplier tous les p pour exécuter une seule fois l'algorithme de normalisation.

Cet algorithme nécessite quand même la manipulation de matrices $n \times n^2$. En pratique, on utilise un autre algorithme de normalisation locale lié à la factorisation sur $\mathbb{Z}_p$ (Round 4), d'autant plus efficace que n ou $v_p([\mathcal{O}_K : \mathcal{O}])$ est grand, mais de description moins attrayante. Je ne sais pas si l'on peut obtenir les même garanties pour Round 4 que pour l'algorithme Round 2 modifié par Buchmann et Lenstra (où p est remplacé par m sans facteur carrés). C'est probable.

3.2. **Le cas particulier de $\mathcal{O}_T$.** Pour chaque premier p, la première étape de l'algorithme Round 2 se traduit plus efficacement par :

Théorème 3.4 (Dedekind)**.** *On suppose que $p \nmid a_0$, le coefficient dominant de T, et que*

$$\overline{T} = \overline{a_0} \prod_i \overline{P_i}^{e_i},$$

où les $\overline{P_i}$ sont irréductibles unitaires 2 à 2 distincts. On choisit des relèvements unitaires P_i des $\overline{P_i}$ et on note

- *f un relèvement dans $\mathbb{Z}$ de $\prod_i \overline{P_i}$,*
- *g un relèvement dans $\mathbb{Z}$ de $\overline{T}/\overline{f}$,*
- *$h := (T - fg)/p \in \mathbb{Z}[X]$.*

Soit $\delta := \operatorname{pgcd}(\overline{f}, \overline{g}, \overline{h})$ dans $\mathbb{F}_p[X]$, et U un relèvement de $\overline{T}/\delta$, alors

$$\mathcal{O}' = \mathcal{O}_T + \frac{a_0^{\deg U} U(\theta)}{p} \mathcal{O}_T.$$

En particulier, $\mathcal{O}_T$ est p-maximal ssi $\delta = 1$.

Preuve. On trouve $I_p = p\mathcal{O}_T + a_0^{\deg g} g(x)\mathcal{O}_T$, et on explicite le calcul de $(I_p : I_p)$. (On peut supposer que $a_0 = 1$, par changement de variable.) □

Corollaire 3.5. *Si T est d'Eisenstein, alors $\mathcal{O}_T$ est p-maximal.*

Preuve. $f = X$, $g = X^{n-1}$, $h(0) = a_n/p$. □

3.3. **Diviseurs inessentiels.** En changeant au besoin T, on peut espérer obtenir un ordre $\mathcal{O}_T$ qui soit p-maximal. Hélas, dès que $n \geqslant 3$, il peut exister des *diviseurs inessentiels p du discriminant*[9] tels que $p \mid [\mathcal{O}_K : \mathcal{O}_T]$ pour tout T tel que $p \nmid a_0$ (ou, de façon équivalente, pour T unitaire) :

Théorème 3.6 (Hensel)**.** *Soit p un nombre premier fixé. On note*

- *$r(f)$ le nombre de $\mathfrak{p} \mid p$ de degré résiduel f.*
- *$i(f)$ le nombre de $P \in \mathbb{F}_p[X]$ irréductibles unitaires de degré f.*

Alors p est diviseur inessentiel ssi il existe f tel que $r(f) > i(f)$.

[9]Dedekind écrit *ausserwesentlich* (= d'essence extérieure), Bourbaki (mal inspiré) « facteurs extraordinaires » dans ses notes historiques. La littérature se partage entre diviseurs essentiels ou inessentiels... pour la même notion.

On en déduit que si p diviseur inessentiel, alors $p < n = \dim_{\mathbb{Q}} K$.

Exemple : (Dedekind) : dans un corps cubique, seul 2 peut être diviseur inessentiel. En fait, il l'est ssi il est totalement décomposé.

La condition de Hensel est trivialement suffisante d'après le critère de Kummer, la réciproque exige un calcul local assez précis (une dizaine de lignes, c'est un bon exercice). Pour mémoire :

Théorème 3.7 (Kummer)**.** *Si $\mathcal{O}_T$ est p-maximal et p ne divise pas le coefficient dominant a_0 de T, alors « la factorisation de T mod p reflète celle de $p\mathcal{O}_K$ ». Plus précisément, supposons*

$$\overline{T} = \overline{a_0} \prod_i \overline{P_i}^{e_i}$$

dans $\mathbb{F}_p[X]$ où les $\overline{P_i}$ sont irréductibles unitaires 2 à 2 distincts. Alors

$$p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$$

où les $\mathfrak{p}_i := p\mathcal{O}_K + a_0^{\deg P_i} P_i(\theta)\mathcal{O}_K$ sont maximaux, 2 à 2 distincts et de degré résiduel $\deg \overline{P_i}$.

3.4. **Une application quand $n = 3$.** Par commodité dans cette section, on remplace T par le polynôme homogène en 2 variables associé ($T \to Y^n T(X/Y)$). Soit donc T un polynôme irréductible de degré 3. L'ordre $\mathcal{O}_T$ a même discriminant, mais il est muni d'une base spécifique par l'application $T \mapsto \mathcal{O}_T$. Faire agir $\mathrm{GL}(2,\mathbb{Z})$ sur T par changement de variable revient à changer cette base. En construisant explicitement l'application réciproque (qui est aussi classique : c'est la forme indice), on en déduit :

Théorème 3.8 (Delone-Faddeev)**.** *L'application de Dedekind $T \mapsto \mathcal{O}_T$ induit une bijection préservant le discriminant entre*

- *classes modulo $\mathrm{GL}(2,\mathbb{Z})$ de formes cubiques irréductibles, binaires, à coefficients dans $\mathbb{Z}$.*
- *classes d'isomorphismes d'ordres de rang 3.*

La bijection s'étend aux (classes de) formes cubiques binaires entières, et l'image devient l'ensemble des (classes d'isomorphismes d') anneaux commutatifs qui sont libres de rang 3 comme $\mathbb{Z}$-modules, comme $\mathbb{Z}[X]/(X^3)$ par exemple. Dans cette généralisation, les ordres sont les anneaux intègres correspondant à T irréductible, les anneaux réduits correspondent à T sans facteurs carrés, etc. En appliquant le critère de Dedekind à l'ordre $\mathcal{O}_T$, on obtient

Théorème 3.9 (Davenport-Heilbronn)**.** *L'application de Dedekind $T \mapsto \mathcal{O}_T$ induit une bijection préservant le discriminant entre*

- *classes d'isomorphismes d'ordres cubiques maximaux*
- *classes modulo $\mathrm{GL}(2,\mathbb{Z})$ de formes cubiques irréductibles, binaires, à coefficients dans $\mathbb{Z}$, qui sont de surcroît primitives et qui ne contiennent pas de forme du type $(a, b, pc, p^2 d)$, où p est premier.*

Preuve. Si $p \mid T$, alors $\mathcal{O}_T \subsetneq \mathcal{O}_{T/p}$ n'est pas maximal. Si p ne divise pas $\operatorname{disc} \mathcal{O}_T = \operatorname{disc}(T)$ il n'y a pas de problème, sinon utiliser l'action de $\mathrm{GL}(2,\mathbb{Z})$ pour placer la racine double en 0 et s'assurer qu'il n'y a pas de racine à l'infini, et appliquer Dedekind. □

Proposition 3.10. *Si $T(X,Y)$ est associé comme ci-dessus à un ordre maximal $\mathcal{O}_T$, la factorisation de $T(X,Y)$ dans $\mathbb{F}_p[X,Y]$ reflète celle de p dans* $\operatorname{Frac} \mathcal{O}_T$.

Preuve. on peut appliquer Kummer sauf si p est diviseur inessentiel, i.e $p = 2$ totalement décomposé. Ceci se traduit par le fait que $T \mod 2$ a une racine en 0 et en ∞ (sinon on pourrait appliquer Kummer) et ces racines sont simples puisque $\operatorname{disc}(T) = \operatorname{disc} \mathcal{O}_K$ n'est pas divisible par 2 (non ramifié dans K). T est donc bien totalement décomposé modulo 2. □

On dispose de domaines fondamentaux simples pour l'action de $\mathrm{GL}(2,\mathbb{Z})$ sur les formes cubiques binaires. On peut donc décrire les extensions cubiques de $\mathbb{Q}$ de discriminant borné par les points entiers d'un semi-algébrique explicite. Il y a de nombreuses applications analytiques, comme

Théorème 3.11 (Davenport-Heilbronn)**.** *On a*

$$\sum_{\substack{K \text{ cubique} \\ |\operatorname{disc} \mathcal{O}_K| \leqslant X}} 1 \sim \frac{X}{3\zeta(3)},$$

où les corps K sont comptés à isomorphisme près.

Manjul Bhargava a généralisé ce type de construction, y compris les critères de maximalité, aux anneaux de rang inférieur ou égal à 5. De nombreux résultats de densité devraient s'ensuivre (il reste quelques problèmes analytiques pour maîtriser les domaines fondamentaux associés).

4. Décomposition des nombres premiers

4.1. **Décomposition.** Soit p un nombre premier. Comment se décompose p dans K quand $\mathcal{O}_T$ n'est pas p-maximal ? C'est là encore un problème facile. Soient $\mathcal{O}$ un ordre p-maximal et I_p comme précédemment. Alors $A_p = \mathcal{O}/I_p$ est une $\mathbb{F}_p$-algèbre finie réduite donc séparable. Deux bonnes approches sont possibles, toutes deux probabilistes :

- trouver un élément primitif α de $A_p \simeq \prod_{\mathfrak{p}|p} A_p/(\mathfrak{p}/I_p)$, en tirant α au hasard jusqu'à ce que son polynôme minimal m_α sur $\mathbb{F}_p$ soit de degré $\dim_{\mathbb{F}_p} A_p$. Factoriser
$$m_\alpha = \prod_i \overline{P_i},$$
qui est sans facteurs carrés (A_p est réduite), puis poser $\mathfrak{p} = p\mathcal{O} + P_i(\theta)\mathcal{O}$.
- utiliser Berlekamp pour décomposer une $\mathbb{F}_p$-algèbre séparable de la forme $A = A_p/I$ (initialement $I = (0)$). L'idée est la suivante : soit ϕ l'endomorphisme de A donné par $a \mapsto a^p - a$ et $V := \operatorname{Ker} \phi$. Alors $\dim_{\mathbb{F}_p} V$ est

le nombre de facteurs simples de A. S'il vaut 1, A est un corps et I est un idéal maximal contenant p. Sinon, soit $\alpha \in V \setminus \mathbb{F}_p$ et m_α son polynôme minimal. m_α est produit de r facteurs linéaires 2 à 2 premiers entre eux ; $r \geqslant 2$ puisque $\alpha \notin \mathbb{F}_p$. Le lemme des noyaux décompose A en r facteurs, et on peut recommencer.

Explicitement, on écrit pour simplifier une factorisation non triviale en produit de deux facteurs : $m_\alpha = m_1 m_2$ et $U_1 m_1 + U_2 m_2 = 1$ une relation de Bezout. Alors $\varepsilon_i := (U_i m_i)(\alpha)$ sont des idempotents orthogonaux non triviaux de

$$A = \varepsilon_1 A \oplus \varepsilon_2 A = A_p/I_2 \oplus A_p/I_1,$$

avec $I_i := I + \varepsilon_i \mathcal{O}$. (On écrit $\varepsilon_1(A_p/I) = A_p/(I + \varepsilon_2 A_p)$ pour garder une trace explicite des idéaux par lesquels on quotiente.)

On en déduit récursivement une factorisation de A_p en produit de corps finis de la forme $A_p/(\mathfrak{p}/I_p)$. Les $\mathfrak{p}/I_p$ sont donnés comme sous-$\mathbb{F}_p$-ev de A_p, d'où on déduit $\mathfrak{p}/p\mathcal{O} \subset \mathcal{O}/p\mathcal{O}$ puis $\mathfrak{p} \subset \mathcal{O}$ comme $\mathbb{Z}$-modules.

Remarque 4.1. La deuxième approche est probabiliste à cause de la factorisation de m_α. Berlekamp ramène la décomposition d'une $\mathbb{F}_p$-algèbre réduite finie au calcul des racines d'un polynôme scindé, et ce dernier problème est difficile pour un algorithme déterministe. L'algorithme de Berlekamp est souvent associé à la factorisation de $P \in \mathbb{F}_p[X]$ sans facteur carré, problème équivalent à la décomposition de l'algèbre réduite $\mathbb{F}_p[X]/(P)$.

Exercice 4.2– La proportion d'éléments primitifs dans A_p est

$$\prod_{\mathfrak{p}|p} \sum_{d|f(\mathfrak{p})} \frac{\mu(d)}{p^{f(\mathfrak{p})(1-1/d)}}$$

où $f(\mathfrak{p})$ désigne le degré résiduel de l'idéal premier $\mathfrak{p}$.

Exercice 4.3 (Racines d'un polynôme scindé)– Soit p un premier impair et $P \in \mathbb{F}_p[X]$ scindé à racines simples de degré $r \geqslant 2$. Montrer que, si $\alpha \in \mathbb{F}_p[X]/(P)$ est tiré uniformément au hasard, $\gcd(\alpha^{(p-1)/2} - 1, P)$ est trivial ($= 1$ ou P) avec probabilité

$$((p-1)/2p)^r + ((p+1)/2p)^r \leqslant 5/9.$$

En déduire qu'il est facile de calculer les racines de P (le cas $p = 2$ est trivial).

4.2. **Uniformisante.** Avec Berlekamp, on n'obtient pas directement $\mathfrak{p}$ sous la forme $\mathfrak{p} = p\mathcal{O} + \pi\mathcal{O}$. Là aussi au moins deux stratégies possibles, la première probabiliste :

- tester $\pi \in \mathfrak{p}/p\mathcal{O}$ jusqu'à trouver une uniformisante : π est une uniformisante si et seulement si $pN\mathfrak{p} \nmid N\pi$, où $N\mathfrak{p} = p^f(\mathfrak{p})$, avec

$$f(\mathfrak{p}) = \dim_{\mathbb{F}_p} \mathcal{O}/\mathfrak{p} = \dim_{\mathbb{F}_p}(\mathcal{O}/I_p) - \dim_{\mathbb{F}_p}(\mathfrak{p}/I_p).$$

Dans le cas le pire, $p = 2$ est totalement décomposé ; la probabilité de succès est $1/2^n$, donc l'espérance du temps de calcul est exponentielle dans ce cas.

- utiliser un argument d'approximation : écrire $I_p = \mathfrak{p}J$, où $J := \prod_{\mathfrak{q}|p,\ \mathfrak{q}\neq\mathfrak{p}} \mathfrak{q}$ (calculé comme relèvement de J/I_p vu comme intersection des $\mathbb{F}_p$-ev $\mathfrak{q}/I_p$). Comme $\mathfrak{p} + J = \mathcal{O}$, écrire une relation de Bezout $i + j = 1$, où $i \in \mathfrak{p}$ et $j \in J$. Si $\mathfrak{p}/p$ est non ramifié, $\pi := i$ est uniformisante ; sinon tester les $\pi := j\tau + i$ où τ parcourt la $\mathbb{F}_p$-base de $\mathfrak{p}/I_p$: c'est une uniformisante ssi $\tau \in \mathfrak{p} \setminus \mathfrak{p}^2$. C'est un bon algorithme.

Remarquons que l'algorithme Round 4 évoqué au §3.1 trivialise ces problèmes : il fournit simultanément la factorisation de T dans $\mathbb{Q}_p[X]$, un ordre p-maximal $\mathcal{O}$ de $\mathbb{Q}[X]/(T)$, et la décomposition de $p\mathcal{O}$ en produit d'idéaux maximaux donnés sous la forme $\mathfrak{p} = p\mathcal{O} + \pi\mathcal{O}$.

Exercice 4.4– La proportion d'uniformisantes dans $\mathfrak{p}/p\mathcal{O}$ est

$$\prod_{\mathfrak{p}|p}(1 - 1/N\mathfrak{p})$$

Proposition 4.5. *Si $x \in K^*$, il est facile de calculer $v = v_\mathfrak{p}(x)$.*

Preuve. Appliquer la définition : pour $x \in \mathcal{O}$ p-maximal, $v = \max\{w : x \in \mathfrak{p}^w\}$. Plus efficace dès que $\mathfrak{p} = p\mathcal{O}+\pi\mathcal{O}$: on calcule τ une $\{\mathfrak{p}\}$-unité tel que $v_\mathfrak{p}(\tau) = -1$ et $v_\mathfrak{q}(\tau) = 0$ pour tout $\mathfrak{q} \mid p$, $\mathfrak{q} \neq \mathfrak{p}$. Par exemple $\tau := \tau_0/p$, où $\tau_0\pi = 0 \mod p\mathcal{O}$, τ_0 non trivial que l'on obtient comme élément du noyau de la multiplication par π dans le $\mathbb{F}_p$-ev $\mathcal{O}/p\mathcal{O}$. Alors $v = \max\{w, \tau^w x \in \mathcal{O}\}$. □

5. Groupe de classes et unités

À partir de cette section, on suppose connu l'ordre maximal $\mathcal{O}_K$ et on note $\Delta_K := |\mathrm{disc}\,\mathcal{O}_K|$. Étudier directement $\mathrm{Cl}(\mathcal{O})$ et $\mathcal{O}^*$ pour un ordre quelconque rajouterait des difficultés techniques sans éclaircir le problème initial. Pour montrer que $\mathrm{Cl}(\mathcal{O}_K)$ est calculable en principe, il ne suffit pas d'invoquer la borne de Minkowski :

Théorème 5.1 (Minkowski)**.** *Toute classe d'idéaux contient un idéal de norme inférieure à $(n!/n^n)(4/\pi)^{r_2}\Delta_K^{1/2}$, où r_2 est le nombre de places complexes de K.*

Il manque une procédure effective pour décider si deux idéaux sont équivalents ! « Factoriser suffisamment d'idéaux principaux » n'est pas recevable...

5.1. **Calculabilité.** Pour toute place $\mathfrak{p}$ de K, on note $|.|_\mathfrak{p}$ la valeur absolue normalisée associée. Soit S_∞ l'ensemble des places archimédiennes de K et $S \supset S_\infty$ un ensemble fini de places. On note

$$U_S(K) = \left\{x \in K : |x|_\mathfrak{p} = 1, \forall \mathfrak{p} \notin S\right\}$$

le groupe des S-unités de K. En particulier $U_\emptyset(K) := U(K) = \mathcal{O}_K^*$.

Définition 5.2. La *hauteur* naïve $H(\alpha)$ de $\alpha \in K$ est définie par

$$H(\alpha) := \prod_{\mathfrak{p}} \max\left\{1, |\alpha|_{\mathfrak{p}}\right\}$$

Théorème 5.3 (Lenstra)**.** *Soit* $d := (2/\pi)^{r_2}\Delta_K^{1/2}$, $S_0 := \{\mathfrak{p}, N\mathfrak{p} \leqslant d\}$ *et* $S := S_\infty \cup S_0$. *Alors le groupe* $U_S(K)$ *est engendré par* $\{\alpha \in U_S(K), H(\alpha) \leqslant d^2\}$, *et* $\mathrm{Cl}(\mathcal{O}_K)$ *est engendré par les classes des éléments de* S_0.

La calculabilité de $\mathcal{O}_K^*$ et $\mathrm{Cl}(\mathcal{O}_K)$ se déduit de la suite exacte :

$$0 \longrightarrow \mathcal{O}_K^* \longrightarrow U_S(K) \xrightarrow{f} \mathbb{Z}^{S_0} \xrightarrow{g} \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 0,$$

où $f : \alpha \mapsto (v_{\mathfrak{p}}(\alpha))_{\mathfrak{p}\in S_0}$ et $g : (e_{\mathfrak{p}}) \mapsto \prod_{\mathfrak{p}} cl(\mathfrak{p})^{e_{\mathfrak{p}}}$. L'exactitude provient du théorème et il suffit de calculer noyau et conoyau de f, en commençant par construire une $\mathbb{Z}$-base de $U_S(K)$ grâce au Théorème 5.3.

Ce théorème est un peu surprenant puisqu'on s'attend à ce que le *régulateur* de K soit souvent de la taille de $\Delta_K^{1/2}$ (Brauer-Siegel + h « fréquemment » petit). Et donc que certains plongements des unités fondamentales soient de l'ordre de $\exp(\Delta_K^{1/2}/n)$, quelle que soit la $\mathbb{Z}$-base choisie pour $\mathcal{O}_K^*$/torsion. Par exemple, il est bien connu que l'unité fondamentale d'un corps quadratique peut devenir gigantesque. L'astuce consiste à considérer un système non minimal de générateurs. La démonstration est élémentaire (théorème de Minkowski ; l'assertion sur les générateurs de $\mathrm{Cl}(\mathcal{O}_K)$ est triviale car plus faible que celle de Minkowski).

Ce n'est *pas* un bon algorithme, car $U_S(K)$ est beaucoup trop gros (dimension exponentielle en $\log \Delta_K$).

5.2. **Calcul d'indice.** Pour calculer $\mathrm{Cl}(\mathcal{O}_K)$ et $\mathcal{O}_K^*$ en un temps raisonnable (sous-exponentiel en $\log \Delta_K$), on admet GRH[10].

Théorème 5.4 (Bach)**.** *Soit* $\mathfrak{B} := \{\mathfrak{p}, N\mathfrak{p} \leqslant 12(\log \Delta_K)^2\}$. *Sous GRH, les classes des éléments de* $\mathfrak{B}$ *engendrent* $\mathrm{Cl}(\mathcal{O}_K)$.

Pour calculer un groupe abélien *fini* M par générateurs et relations, la méthode de calcul d'indice nécessite quatre ingrédients :

- Un $\mathbb{Z}$-module libre A_0 dont M est un quotient
$$0 \longrightarrow \Lambda_0 ? \longrightarrow A_0 \longrightarrow M \longrightarrow 0$$
(le noyau Λ_0 est inconnu).
- Un sous-groupe de type *fini* $A \subset A_0$, muni d'une $\mathbb{Z}$-base (de factorisation) $\mathfrak{B}$, dont M reste un quotient :
$$0 \longrightarrow \Lambda_0 \cap A =: \Lambda ? \longrightarrow A = \mathbb{Z}^{\mathfrak{B}} \longrightarrow M \longrightarrow 0$$
(le noyau Λ est inconnu).

[10]Même sous ces hypothèses, la complexité sous-exponentielle des algorithmes reste heuristique. Le résultat n'est rigoureusement démontré que pour K quadratique imaginaire. La variante décrite est très simplifiée donc inefficace.

- Un moyen de produire des éléments « bien répartis » dans Λ_0 et de les plonger dans $\mathbb{Z}^{\mathfrak{B}}$ s'ils appartiennent à Λ (factorisation des éléments friables).
- Une évaluation grossière H de $h := \#M = [A : \Lambda]$, telle que $H < 2h$.

L'algorithme probabiliste suivant détermine alors Λ : produire des éléments de Λ, engendrant un sous groupe $\widehat{\Lambda} \subset \Lambda$, jusqu'à ce que

$$\widehat{h} := [A : \widehat{\Lambda}] \leqslant H,$$

ce qui entraîne $\widehat{h} = h$ puisque $\widehat{h}$ est un multiple entier de h, et donc $\widehat{\Lambda} = \Lambda$. On en déduit la structure de

$$M = \oplus(\mathbb{Z}/d_i\mathbb{Z})g_i, \quad d_1 \mid d_2 \mid \ldots, \quad g_i \in A.$$

La solution du logarithme discret dans A, c'est-à-dire l'écriture d'un élément de M comme produit des g_i et d'un élément de Λ est une généralisation simple que l'on considérera ultérieurement.

5.3. **Adaptation au cas $M = \mathrm{Cl}(\mathcal{O}_K)$.** On étend l'idée précédente en calculant simultanément $\widehat{\Lambda}$ comme ci-dessus et un sous-groupe $\widehat{U}$ de $U := \mathcal{O}_K^*$. On désire calculer $M := \mathrm{Cl}(\mathcal{O}_K)$,

- A_0 est le groupe des idéaux fractionnaires non nuls de K,
- $\mathfrak{B}$ est l'ensemble d'idéaux premiers qui engendre $\mathrm{Cl}(\mathcal{O}_K)$ sous GRH (donné par Bach, qui remplace l'ensemble S_0 de Lenstra),
- on produit des élément de Λ en factorisant des éléments α de petite norme dans $\mathcal{O}_K$ (par divisions successives par les idéaux de $\mathfrak{B}$),
- la formule de Dirichlet

  $$\zeta_K(0) = -hR/w$$

  permet d'obtenir une approximation numérique du produit hR. On calcule en pratique un produit Eulérien tronqué convergeant vers le résidu en $s = 1$ de ζ_K :

  $$\prod_{p \leqslant Y} \frac{(1 - 1/p)}{\prod_{\mathfrak{p}|p}(1 - 1/N\mathfrak{p})} \longrightarrow \left(\frac{\zeta_K}{\zeta}\right)(1) = 2^{r_1}(2\pi)^{r_2}\frac{hR}{w\sqrt{\Delta_K}}$$

  On utilise de nouveau GRH pour garantir l'approximation avec $Y = O((\log \Delta_K)^2)$.

Les dépendances entre éléments de $\widehat{\Lambda}$, découvertes au moment du calcul de $[A : \widehat{\Lambda}]$, se traduisent par des identités entre idéaux principaux $(\alpha) = (\alpha')$. On en déduit des unités $u := \alpha/\alpha' \in U$; ces éléments u engendrent un sous-groupe $\widehat{U}$ de U. Soit $\widehat{R}$ le régulateur de $\widehat{U}$, qui est un multiple entier du régulateur R ; tout comme ci-dessus, lorsque $hR < 2\widehat{h}\widehat{R}$, alors $U = \widehat{U}$ et $\Lambda = \widehat{\Lambda}$, d'où on tire $\mathrm{Cl}(\mathcal{O}_K)$.

Pour obtenir des générateurs (g_i) explicites, il faut conserver les matrices de changement de base associées à toute cette algèbre linéaire. On obtient les g_i sous forme *factorisée* dans $\mathbb{Z}^{\mathfrak{B}}$, ce qui est une présentation compacte agréable. En développant, on obtient des idéaux de norme déraisonnable, fort loin de la

borne de Minkowski. Nous allons voir qu'il est facile d'extraire un « contenu » principal d'un idéal arbitraire, pour obtenir une « partie principale » de petite norme (partie principale s'entend ici au sens de $x/\mathrm{cont}(x)$, elle peut représenter un idéal principal ou non).

5.4. **Réduction LLL.**

Théorème 5.5 (Lenstra, Lenstra, Lovász)**.** *Soit $(\mathbb{R}^n, q)$ un espace euclidien et Λ un sous-réseau de $(\mathbb{Z}^n, q)$ donné par un ensemble fini de générateurs. Il existe un bon algorithme déterminant une base (b_i) de Λ, dite LLL-réduite, telle que pour toute suite de vecteurs* indépendants *$x_1, \dots, x_t$ de Λ, on ait*

$$q(b_j) \leqslant 2^{n-1} \max\{q(x_1), \dots, q(x_t)\}.$$

On peut remplacer la constante 2 par tout $\gamma > 4/3$.

En particulier le premier vecteur b_1 est essentiellement aussi court que possible (à un facteur 2^{n-1} près). Trouver un *plus court* vecteur est NP-dur, donc difficile.

Définition 5.6. On définit la forme quadratique définie positive $T_2 : K \to \mathbb{R}^+$ par

$$T_2(\alpha) := \sum_{\sigma : K \to \mathbb{C}} |\alpha|_\sigma^2 .$$

C'est la restriction de la forme euclidienne $\mathrm{Tr}_{E/\mathbb{R}}(x\overline{x})$ sur la $\mathbb{R}$-algèbre à involution $E := K \otimes_{\mathbb{Q}} \mathbb{R}$. Un sous-$\mathbb{Z}$-module de K muni de T_2 devient un réseau de E.

Soit $\mathfrak{A}$ un idéal fractionnaire non nul. Le premier vecteur d'une base LLL-réduite de $\mathfrak{A}$ est un $\alpha \in \mathfrak{A}$ de norme relativement petite. On récrit

$$\mathfrak{A} = (\alpha)(\mathfrak{A}/\alpha) = (a)(\alpha)\mathfrak{a},$$

où $\mathfrak{a}$ est entier et primitif, $\alpha \in \mathcal{O}_K$ et $a \in \mathbb{Q}^*$. Ces trois composantes dépendent de la variante de l'algorithme LLL utilisé mais

Lemme 5.7. *$N\mathfrak{a}$ est bornée par une constante ne dépendant que de K.*

Preuve. Minkowski + LLL □

En particulier, un produit quelconque d'idéaux se simplifie sous la forme $(\alpha)\mathfrak{a}$, où α est un produit d'éléments de K^*, que l'on peut développer si nécessaire, et $\mathfrak{a}$ est un *petit* idéal entier. Il est préférable de conserver α sous forme de produit *formel* : on écrit $\alpha = \prod x_i^{e_i} \in \mathbb{Z}[K^*]$. (Penser aux 30000 chiffres décimaux de la représentation développée de 2^{100000}, par exemple.) Dans l'essentiel des applications, on n'utilisera pas α mais sa projection sur un domaine où les calculs sont plus simples : $K \otimes \mathbb{R}$, $K \otimes \mathbb{Q}_p$, $(\mathcal{O}_K/\mathfrak{f})^*$, $K^*/(K^*)^\ell \dots$

5.5. **Logarithme discret.** Nous pouvons donc calculer

$$\mathrm{Cl}(\mathcal{O}_K) = \oplus(\mathbb{Z}/d_i\mathbb{Z})g_i,$$

où l'on sait exprimer les g_i comme produits d'éléments de $\mathfrak{B}$, où comme *petit* idéal, à un idéal principal explicite près. Réciproquement on peut exprimer un élément de $\mathfrak{B}$ en terme des g_i. Soit maintenant un idéal $I = (\alpha)\mathfrak{a}$, donné sous la forme précédente. On veut calculer son logarithme discret, c'est-à-dire $(e_i) \in \prod_i(\mathbb{Z}/d_i\mathbb{Z})$ et $\tau \in \mathbb{Z}[K^*]$, tels que $I = (\tau)\prod g_i^{e_i}$.

- Pour calculer les (e_i), multiplier $\mathfrak{a}$ par des produits aléatoires d'idéaux de $\mathfrak{B}$ et LLL-réduire le résultat, jusqu'à ce que la composante non-principale soit friable. À un idéal principal près, on sait alors exprimer $\mathfrak{a}$ comme produit d'éléments de $\mathfrak{B}$, donc des g_i.
- Calculer $\mathfrak{a}\prod g_i^{-e_i}$ sous la forme $(\beta)\mathfrak{B}$, $\beta \in \mathbb{Z}[K^*]$. Puis réaliser le *petit* idéal *principal* $\mathfrak{B}$ comme (γ), en utilisant la même méthode que ci-dessus, mais cette fois-ci en accumulant les idéaux principaux rencontrés. On peut poser $\tau := \alpha\beta\gamma \in \mathbb{Z}[K^*]$.

Références

[1] H. Cohen, *A course in computational algebraic number theory*, third ed., Springer-Verlag, 1996.

[2] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, 2000.

[3] H. W. Lenstra, Jr., Algorithms in algebraic number theory, *Bull. Amer. Math. Soc. (N.S.)* **26** (1992), no. 2, pp. 211–244.