Enumération d'extensions cubiques de corps de nombres

Anna Morra

October 9, 2007

1 Rappels

Soit R un anneau de Dedekind.
Soit $K = \mathrm{Frac}(R)$.

Théorème 1 *Soit M un module de type fini sur R.*

1. *M est sans torsion $\Longleftrightarrow$ M est un module projectif.*
2. *Il existe un sous-module N de M sans torsion tel que*
$$M = M_{\mathrm{tors}} \oplus N \quad N \simeq M/M_{\mathrm{tors}}.$$
3. *Si M sans torsion et $V = K \otimes_R M$, alors il existe des idéaux fractionnaires $\mathfrak{A}_i$ et des éléments $\omega_i \in V$ tels que*
$$M = \mathfrak{A}_i\omega_i \oplus \cdots \oplus \mathfrak{A}_n\omega_n.$$
La classe de l'idéal $\mathfrak{A} := \mathfrak{A}_1 \cdots \mathfrak{A}_n$ dans $Cl(R)$ dépend seulement du module M et est appelée la classe de Steinitz de M.
4. *Le module M est un R-module libre $\Longleftrightarrow$ sa classe de Steinitz est égale à la classe triviale $\Longleftrightarrow$ $\mathfrak{A}$ est un idéal principal.*
5. *Si M est un module de torsion, il existe des uniques idéaux entiers non nuls ∂_i de R et (non uniques) éléments $\omega_i \in V$ tels que*
$$M = (R/\partial_1)\omega_1 \oplus \cdots \oplus (R/\partial_n)\omega_n$$
et $\partial_{i-1} \subset \partial_i$ pour tout $2 \leq i \leq n$.

Définition 1 (pseudo-objets) *Soit M un R-module de type fini sans torsion, $V = K \otimes_R M$.*

1. *Un pseudo-élément de V est un sous R-module de V de la forme $\mathfrak{A}\omega$ avec $\omega \in V$, $\mathfrak{A}$ idéal fractionnaire de R.*
2. *Le pseudo-élément $\mathfrak{A}\omega$ est dit entier si $\mathfrak{A}\omega \subset M$.*
3. *Soient $\mathfrak{A}_i$ des idéaux fractionnaires de R, $\omega_i \in V$. $(\omega_i, \mathfrak{A}_i)_{1\leq i\leq n}$ est un pseudo-ensemble générateur pour M si*

$$M = \mathfrak{A}_1\omega_1 + \cdots + \mathfrak{A}_n\omega_n.$$

4. *$(\omega_i, \mathfrak{A}_i)_{1\leq i\leq n}$ est une pseudo-base si*

$$M = \mathfrak{A}_1\omega_1 \oplus \cdots \oplus \mathfrak{A}_n\omega_n.$$

Soit L/K une extension de corps de nombres $[L : K] = n < \infty$. $\mathbb{Z}_L$ (l'anneau des entiers de L) est un $\mathbb{Z}_K$-module de type fini.
$\mathbb{Z}_K$ n'est pas forcément principal, donc $\mathbb{Z}_L$ n'est pas forcément libre. Donc, en général, on ne pourra pas parler de base de $\mathbb{Z}_L$, par contre on pourra parler de pseudo-base.

Définition 2 (Discriminants) *Soit $(\mathfrak{A}_i, \omega_i)_{1\leq i\leq n}$ une pseudo-base de $\mathbb{Z}_L$ sur $\mathbb{Z}_K$.*
On définit:

- $\mathrm{disc}(\omega_1, \cdots, \omega_n) = \det(\sigma_i(\omega_j))^2 = \det(\mathrm{Tr}_{L/K}(\omega_i, \omega_j))$.
  (où les σ_i sont les K-plongements de L dans $\mathbb{C}$)
- $\partial(L/K) = \mathrm{disc}(\omega_1, \cdots, \omega_n)(\mathfrak{A}_1 \cdots \mathfrak{A}_n)^2$, *l'idéal discriminant relatif.*
- $\overline{d(L/K)} = \overline{\mathrm{disc}(\omega_1, \cdots, \omega_n)} \in K^*/(K^*)^2$.
- $\mathrm{disc}(L/K) = (\partial(L/K), \overline{d(L/K)})$ *le discriminant relatif.*

2 Introduction

Soit L/K une extension de corps de nombres. On définit:

$$N_{K,n}(X) = \sharp\{L \mid [L:K] = n, \mathcal{N}_{K/\mathbb{Q}}\partial(L/K) \leq X\}/\sim$$

On s'intéresse à cette valeur pour deux problèmes différents:

1. On étudie la valeur asymptotique de $N_{K,n}(X)$ pour $X \to \infty$ (K, n fixés):
   - asymptotiques pour les extensions quadratiques: Wright, Cohen-Diaz y Diaz-Olivier;
   - asymptotiques pour les extensions cubiques: Davenport-Heilbronn ($K = \mathbb{Q}$), Datskovsky-Wright (K arbitraire);
   - asymptotiques pour $n = 4, 5$ et $K = \mathbb{Q}$: Bhargava.
2. On s'intéresse à l'algorithmique, et en particulier, non seulement au calcul de $N_{K,n}$, mais aussi à construire des tables d'extensions de K de degré n avec discriminant borné par X:
   - On a des algorithmes pour les extensions quadratiques (sur $K \neq \mathbb{Q}$, vu que sur les rationnels le problème est trivial);
   - on a un algorithme efficace, dû a Belabas, pour calculer une liste de corps cubiques (sur $\mathbb{Q}$) de discriminant borné.

A ce point de la recherche, il reste donc des problèmes ouverts. En particulier il manque:

- Un algorithme pour les extensions cubiques de K arbitraire,
- un algorithme pour les extensions de degré $4, 5$ de $\mathbb{Q}$.

On va dorénavant s'intéresser aux extensions cubiques.
On va tout d'abord décrire le cas $K = \mathbb{Q}$, pour après passer au cas général, K arbitraire, où on va décrire notre résultat:

Théorème 2 *Soit K un corps de nombres.*

- *Il existe un algorithme pour énumérer toutes les extensions cubiques de K avec discriminant borné.*
- *Si K est un corps quadratique imaginaire, cet algorithme marche en temps polynomial dans la taille des résultats.*

On décrira enfin une implémentation pour K quadratique imaginaire avec nombre de classes 1.

3 Extensions cubiques sur $\mathbb{Q}$

Théorème 3 (Levi, Delone-Faddeev, Davenport-Heilbronn, Belabas, Bhargava) *Il existe une bijection entre les extensions cubiques de $\mathbb{Q}$ (modulo isomorphisme) est les classes de formes cubiques binaires irréductibles*

$$ax^3 + bx^2y + cxy^2 + dy^3, \quad a, b, c, d \in \mathbb{Z},$$

modulo $\mathrm{GL}_2(\mathbb{Z})$*, telles que* $\langle 1, ax, ax^2 + bx \rangle_{\mathbb{Z}}$ *est un anneau maximal de* $\mathbb{Q}[x]/(ax^3 + bx^2 + cx + d)$.

Pour vérifier cette dernière condition, on va utiliser le critère de Dedekind:

Théorème 4 (Critère de Dedekind) *Soit L/K une extension de corps de nombres, $L = K(\theta)$, θ entier algébrique dont le polynôme minimal dans $\mathbb{Z}_K[x]$est $T(x)$.*
Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_K$.
Soit β une uniformisante de $\mathfrak{p}^{-1}$, i.e. $\beta \in \mathfrak{p}^{-1} \setminus \mathbb{Z}_K$.
Soit $\overline{T(x)} = \prod_{1 \leq i \leq k} \overline{T_i(x)}^{e_i}$ la factorisation de $\overline{T(x)} \in (\mathbb{Z}_{\mathbb{K}}/\mathfrak{p})[x]$ (avec les $\overline{T_i}$ unitaires).
Soient

$$g(x) = \prod_{1 \leq i \leq k} T_i(x), \quad h(x) = \prod_{1 \leq i \leq k} T_i(x)^{e_i - 1},$$

alors $g(x)h(x) - T(x) \in \mathfrak{p}[x]$.
Soit $f(x) = \beta(g(x)h(x) - T(x)) \in \mathbb{Z}_K[x]$.
Alors $\mathcal{O} = \mathbb{Z}_K[\theta]$ est $\mathfrak{p}$-maximal si et seulement si $(\overline{f}, \overline{g}, \overline{h}) = 1$ dans $(\mathbb{Z}_{\mathbb{K}}/\mathfrak{p})[x]$.

On sait que l'anneau engendré par $\{1, ax, ax^2 + bx\}$ est maximal si et seulement si il satisfait le critère de Dedekind pour tous les idéaux premiers $\mathfrak{p}$ qui divisent le discriminant de la forme cubique $ax^3 + bx^2 + cx + d$.
Le seul problème est qu'on a besoin de factoriser le discriminant, et la complexité des meilleurs algorithmes de factorisation n'est que sous-exponentielle. Belabas a résolu ce problème en utilisant des méthodes de crible, qui nous permettent d'avoir un algorithme en $\widetilde{\mathcal{O}}(X)$ (les méthodes de crible requièrent en contrepartie de l'espace, mais cela ne nous pose aucun probleme vu qu'on veut une liste de $\mathcal{O}(X)$ corps).
A ce point il ne nous manque que de choisir un unique représentant pour toute classe modulo $\mathrm{GL}_2(\mathbb{Z})$.
Pour cela on va utiliser un covariant, c'est-à-dire on associe à chaque forme F une forme H_F telle que

$$H_{\gamma \cdot F} = \gamma \cdot H_F \quad \forall \gamma \in \mathrm{GL}_2(\mathbb{Z})$$

Dans ce cas particulier, où $K = \mathbb{Q}$, ce covariant est donné par:

$$H_F = -\frac{1}{4}\begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2,$$

où $P = b^2 - 3ac, Q = bc - 9ad, R = c^2 - 3bd$.
Or, on a une théorie de la réduction pour les formes quadratiques binaires (en particulier pour celles définies) qui remonte à Gauss.
Donc on définit F réduite $\iff H_F$ réduite.
On a donc des bornes sur P, Q, R en fonction du discriminant D de F, et on obtient successivement des bornes sur a, b, c, d en fonction de D (cela marche particulièrement bien grâce au fait que P, Q, R sont des polynômes en a, b, c, d).
Grâce aux bornes de Belabas (et Davenport précédemment), il est possible d'énumérer toutes les extensions cubiques de $\mathbb{Q}$ (modulo $\sim$) avec discriminant borné par X en temps $\widetilde{\mathcal{O}}(X)$.

4 Extensions cubiques sur K arbitraire

Pour généraliser l'algorithme de Belabas, on va utiliser un théorème de Taniguchi. Pour l'énoncer on aura besoin de quelques définitions supplementaires.

Définition 3 *Soit $\mathcal{O}$ un anneau de Dedekind.*
Soit $V = (\mathrm{Sym}^3 \mathcal{O}^2)^*$.
On peut voir un élément de V comme une forme cubique binaire:

$$F = ax^3 + bx^2y + cxy^2 + dy^3, \quad a, b, c, d \in \mathcal{O}.$$

- *Soit $\mathcal{C}(\mathcal{O})$ l'ensemble des classes d'isomorphisme des $\mathcal{O}$-algèbres qui sont projectives de rang 3 comme $\mathcal{O}$-modules. On les appellera les algèbres cubiques.*

- *Pour tout idéal fractionnaire $\mathfrak{a}$, on définit*

$$\mathcal{C}(\mathcal{O}, \mathfrak{a}) = \{R \in \mathcal{C}(\mathcal{O}) \mid \mathrm{St}(R) = \mathfrak{a}\}.$$

On définit:

- $$G_{\mathfrak{a}} = \left\{ \begin{pmatrix} \alpha \in \mathcal{O} & \beta \in \mathfrak{a}^{-1} \\ \gamma \in \mathfrak{a} & \delta \in \mathcal{O} \end{pmatrix} \;\middle|\; \alpha\delta - \beta\gamma \in \mathcal{O}^\times \right\}$$

- $$V_{\mathfrak{a}} = \{F = (a, b, c, d) \mid a \in \mathfrak{a}, b \in \mathcal{O}, c \in \mathfrak{a}^{-1}, d \in \mathfrak{a}^{-2}\}$$

On peut maintenant énoncer le théorème de Taniguchi:

Théorème 5 (Taniguchi) *Il existe une bijection canonique entre $\mathcal{C}(\mathcal{O}, \mathfrak{a})$ et $V_{\mathfrak{a}}/G_{\mathfrak{a}}$ qui rend commutatif le diagramme suivant:*

$$\begin{array}{ccc} V_{\mathfrak{a}}/G_{\mathfrak{a}} & \longrightarrow & \mathcal{C}(\mathcal{O}, \mathfrak{a}) \\ {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle \mathfrak{d}} \\ \mathfrak{a}^{-2}/(\mathcal{O}^\times)^2 & \xrightarrow{\times \mathfrak{a}^2} & \{ \textit{ idéaux entiers de } \mathcal{O}\} \end{array}$$

Exemple
Soit K un corps quadratique imaginaire de nombre de classes 1. Soit $\mathcal{O}$ son anneau des entiers.
Alors, vu que il n'y a qu'une classe de Steinitz, on n'a qu'à considérer les orbites de

$$V = \{(a,b,c,d) | a,b,c,d \in \mathcal{O}\}$$

modulo l'action de $\mathrm{GL}_2(\mathcal{O})$.

□

Plus généralement, soit $\mathcal{O}$ un ordre imaginaire quadratique maximal.
Soit $F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$.
On a:

$$F(x,1) = a(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \in \mathbb{C}[x].$$

Grâce au travail de G. Julia, J. Cremona et M. Stoll, on sait qu'un covariant pour l'action de $\mathrm{GL}_2(\mathcal{O})$ est la forme binaire hermitienne:

$$H_F = t_1^2|x-\alpha_1 y|^2 + t_2^2|x-\alpha_2 y|^2 + t_3^2|x-\alpha_3 y|^2,$$

où $t_i^2 = |a|^2|\alpha_j - \alpha_k|^2$; $\quad i,j,k$ distincts deux à deux.
On peut écrire

$$H_F = P|x|^2 + Qx\overline{y} + \overline{Q}\overline{x}y + R|y|^2,$$

où

$$\begin{cases} P = t_1^2 + t_2^2 + t_3^2 \in \mathbb{R} \\ Q = \alpha_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2 \in \mathbb{C} \\ R = |\alpha_1|^2 t_1^2 + |\alpha_2|^2 t_2^2 + |\alpha_3|^2 t_3^2 \in \mathbb{R}. \end{cases}$$

On sait que H_F est un covariant pour l'action du groupe $\mathrm{GL}_2(\mathcal{O})$, et donc on peut imposer

$$F \text{ réduite } \iff H_F \text{ réduite.}$$

On connait une théorie de la réduction pour les formes binaires hermitiennes modulo $\mathrm{SL}_2(\mathbb{Z})$, donc on relaxe pour le moment nos conditions de réduction à $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{GL}_2(\mathcal{O})$.
On obtient les conditions suivantes sur P, Q, R :

$$\begin{cases} P \leq R \\ -P/2 \leq \mathrm{Re}(Q) \leq P/2 \\ 0 \leq \mathrm{Im}(Q) \leq P/2. \end{cases}$$

et par conséquent

$$P \leq \sqrt{2\Delta} \text{ and } R \leq 2\Delta/P,$$

où Δ est le discriminant de la forme hermitienne. Grâce à ces bornes, on obtient des bornes pour les α_i et pour a, b, c, d:

$$|\alpha_i| \leq \mathcal{C}\frac{|D|^{1/4}}{|a|}, \quad \mathcal{C} = (27/2)^{1/4},$$

et

$$|a| \leq \left(\frac{2}{3}\right)^{3/4} |D|^{1/4}; \quad |b| \leq 3\mathcal{C}|D|^{1/4}$$

$$|ad| \leq 2\sqrt{2}|D|^{1/2}; \quad |bc| \leq 9|D|^{1/2}.$$

donc on peut faire une boucle sur les (a, b, c, d) qui nous intéressent en $\widetilde{\mathcal{O}}(X)$. Après on ne choisira que les algèbres maximales, grâce au critère de Dedekind, comme dans l'algorithme de Belabas, et on aura donc un algorithme qui marche en $\widetilde{\mathcal{O}}(X)$.
En pratique, pour implémenter cet algorithme on a quelques soucis techniques:

- On a un domaine fondamental $\mathcal{D}$ pour les formes hermitiennes, mais sur les bords de ce domaine fondamental on n'est pas sûr de trouver un seul représentant de chaque orbite;
- les formes hermitiennes peuvent avoir des automorphismes : $\sigma \in \mathrm{GL}_2(\mathcal{O})$ telles que $F_1 = \sigma \cdot F_2$ avec F_1, F_2 réduites et $H_{F_1} = H_{F_2}$.
- on peut aussi avoir des automorphismes sur les bords, c'est-à-dire les deux problèmes précedents en même temps.

En outre, pour l'instant on n'a réduit que modulo $\mathrm{SL}_2(\mathbb{Z})$. Quand on passe à $\mathrm{GL}_2(\mathcal{O})$, le risque c'est d'avoir des orbites plus grandes qui contiennent plusieurs éléments réduits modulo $SL_2(\mathbb{Z})$.
J'ai prouvé que en effet dans chaque orbite modulo $\mathrm{GL}_2(\mathbb{Z}[i])$ il y a exactement deux formes réduites modulo $\mathrm{SL}_2(\mathbb{Z})$ et on peut chosir l'une des deux (par exemple, si on n'est pas sur le bord, il suffit d'imposer $\mathrm{Re}(Q) > 0$).

5 Résultats

J'ai programmé cet algorithme en PARI/GP dans le cas $K = \mathbb{Q}(i)$, et j'ai comparé mes résultats et les temps d'éxécution avec un autre algorithme (H. Cohen, "Advanced Topics in Computational Number Theory", Algorithmes 9.2.5 et 9.2.7), qui utilise la théorie du corps des classes.
Voici une table des résultats, où le temps est évalué sur une machine 4-processeur Opteron dual-core 2,4 GHz (avec 32 Go RAM).

X	$\sharp\{L\}$	t_1	t_2
2500	56	13 s	12 s
10000	276	1 mn 13 s	1 mn, 18 s
22500	702	2 mn, 49 s	4 mn, 6 s
40000	1339	5 mn, 6 ms	9 mn 19, s
62500	2135	9 mn, 1 s	17 mn, 25 s
90000	3305	15 mn, 6 s	29 mn, 23 s
10^6	42692	$\sim$8h	$\sim$ 20h

6 Conclusions

Même si j'ai programmé l'algorithme seulement dans le cas $K = \mathbb{Q}(i)$, il va marcher pour tout corps K quadratique imaginaire:

- si $h(K) = 1$, alors tout va se passer de la même manière, il ne manque qu'à décrire explicitement les automorphismes et les morphismes du bord.
- si $h(K) \neq 1$ il faudra parcourir les classes de Steinitz, mais dans ce cas là il existe aussi une théorie de la réduction, grâce à l'action de $GL_2(\mathcal{O})$ sur $\mathcal{H}_3$.

Pour le travail futur:

- On voudrait généraliser l'algorithme au cas des corps de fonctions globaux ($\mathbb{F}_q(T)$);
- on voudrait essayer de trouver un algorithme pour les extensions de degré 4 et 5 de $\mathbb{Q}$ (il y a des résultats théoriques de Bhargava, mais aucun algorithme).