Comptage asymptotique et algorithmique d'extensions cubiques relatives

Anna Morra

Université Bordeaux 1

Soutenance de thèse, 7 décembre 2009

Introduction

- K un corps de nombres
- G un groupe de permutations transitif sur n éléments

Introduction

- K un corps de nombres
- G un groupe de permutations transitif sur n éléments

$$\mathcal{F}_{K,n}(G) = \{\text{extensions } L/K, [L:K] = n, \text{la clôture galoisienne } N \text{ de } L/K \text{ a } \mathrm{Gal}(N/K) \simeq G\}/\simeq$$

Introduction

- K un corps de nombres
- G un groupe de permutations transitif sur n éléments

$$\mathcal{F}_{K,n}(G) = \{\text{extensions } L/K, [L:K] = n, \text{la clôture galoisienne } N \text{ de } L/K \text{ a } \mathrm{Gal}(N/K) \simeq G\}/\simeq$$

$$N_{K,n}(G,X) = |\{L \in \mathcal{F}_{K,n}(G), |\mathcal{N}\mathfrak{d}(L/K)| \leq X\}|.$$

Plusieurs questions :

- Formule asymptotique pour $N_{K,n}(G, X)$ avec (K, n, G) fixés et X qui tend vers l'infini.

Plusieurs questions :

- Formule asymptotique pour $N_{K,n}(G, X)$ avec (K, n, G) fixés et X qui tend vers l'infini.
- Valeur exacte de $N_{K,n}(G, X)$ pour (K, n, G, X) fixés.

Plusieurs questions :

- Formule asymptotique pour $N_{K,n}(G, X)$ avec (K, n, G) fixés et X qui tend vers l'infini.
- Valeur exacte de $N_{K,n}(G, X)$ pour (K, n, G, X) fixés.
- Tables des corps de nombres dans $\mathcal{F}_{K,n}(G)$ jusqu'à une certaine borne X sur le discriminant relatif.

Résultats principaux

- Une formule asymptotique pour les extensions cubiques (relatives) avec résolvante quadratique fixée. (avec H. Cohen)

Résultats principaux

- Une formule asymptotique pour les extensions cubiques (relatives) avec résolvante quadratique fixée. (avec H. Cohen)
- Un algorithme pour énumerer les extensions cubiques de K jusqu'à une borne X sur la norme du discriminant relatif, où K est un corps quadratique imaginaire de nombre de classes 1.

Résultats principaux

- Une formule asymptotique pour les extensions cubiques (relatives) avec résolvante quadratique fixée. (avec H. Cohen)
- Un algorithme pour énumerer les extensions cubiques de K jusqu'à une borne X sur la norme du discriminant relatif, où K est un corps quadratique imaginaire de nombre de classes 1.
- Des calculs explicites des constantes asymptotiques, et des tables d'extensions cubiques de K (comme ci-dessus).

Comptage d'extensions cubiques avec résolvante quadratique fixée

(avec H. Cohen)

Asymptotiques

Conjecture 1 (Malle)

$$N_{K,n}(G,X) \sim c_{K,G} X^{a_G} (\log X)^{b_{K,G}-1}$$

avec $a_G \in \mathbb{Q}$, $0 < a_G \leq 1$ $b_{K,G} \in \mathbb{Z}$, $b_{K,G} \geq 1$, $c_{K,G} > 0$.

Asymptotiques

Conjecture 1 (Malle)

$$N_{K,n}(G,X) \sim c_{K,G} X^{a_G} (\log X)^{b_{K,G}-1}$$

avec $a_G \in \mathbb{Q}$, $0 < a_G \leq 1$ $b_{K,G} \in \mathbb{Z}$, $b_{K,G} \geq 1$, $c_{K,G} > 0$.

La conjecture est vraie pour

- tous les groupes abéliens G (Cohn, Mäki, Wright).
- $n = 3$ et $G = S_3$ (Davenport-Heilbronn, Datskovsky-Wright).
- $n = 4$ et $G = D_4$ (Cohen-Diaz y Diaz-Olivier).
- $n = 4$ et 5, $G = S_n$ et $K = \mathbb{Q}$ (Bhargava).

Asymptotiques

Conjecture 1 (Malle)

$$N_{K,n}(G,X) \sim c_{K,G} X^{a_G} (\log X)^{b_{K,G}-1}$$

avec $a_G \in \mathbb{Q}$, $0 < a_G \leq 1$ $b_{K,G} \in \mathbb{Z}$, $b_{K,G} \geq 1$, $c_{K,G} > 0$.

La conjecture est vraie pour

- tous les groupes abéliens G (Cohn, Mäki, Wright).
- $n = 3$ et $G = S_3$ (Davenport-Heilbronn, Datskovsky-Wright).
- $n = 4$ et $G = D_4$ (Cohen-Diaz y Diaz-Olivier).
- $n = 4$ et 5, $G = S_n$ et $K = \mathbb{Q}$ (Bhargava).
- contre-exemple : Klüners (2005)

Asymptotiques

Conjecture 1 (Malle)

$$N_{K,n}(G,X) \sim c_{K,G} X^{a_G} (\log X)^{b_{K,G}-1}$$

avec $a_G \in \mathbb{Q}$, $0 < a_G \leq 1$ $b_{K,G} \in \mathbb{Z}$, $b_{K,G} \geq 1$, $c_{K,G} > 0$.

La conjecture est vraie pour

- tous les groupes abéliens G (Cohn, Mäki, Wright).
- $n = 3$ et $G = S_3$ (Davenport-Heilbronn, Datskovsky-Wright).
- $n = 4$ et $G = D_4$ (Cohen-Diaz y Diaz-Olivier).
- $n = 4$ et 5, $G = S_n$ et $K = \mathbb{Q}$ (Bhargava).
- contre-exemple : Klüners (2005)
- Türkelli : propose une modification à la conjecture pour éviter ce type de contre-exemples.

Motivation

- On connait des formules asymptotiques (qui prouvent la conjecture de Malle) pour extensions C_2, C_3, S_3, C_4, V_4, D_4, S_4, S_5, ...

Motivation

- On connait des formules asymptotiques (qui prouvent la conjecture de Malle) pour extensions C_2, C_3, S_3, C_4, V_4, D_4, S_4, S_5, ...
- mais on n'a pas un résultat complet pour A_4.

Motivation

- On connait des formules asymptotiques (qui prouvent la conjecture de Malle) pour extensions C_2, C_3, S_3, C_4, V_4, D_4, S_4, S_5, ...
- mais on n'a pas un résultat complet pour A_4.
- Résultat partiel : $N_{A_4,K}(X, C_3)$ i.e. on fixe une résolvante cubique. (Cohen)

Motivation

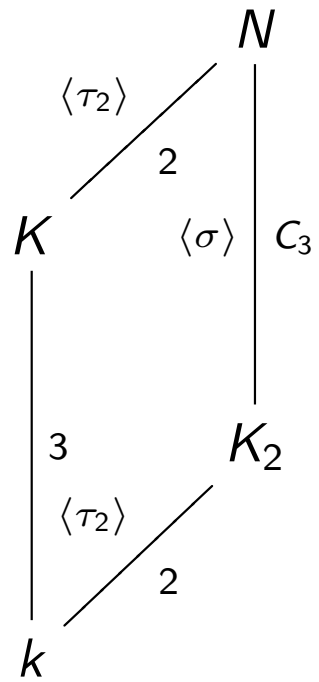
- On connait des formules asymptotiques (qui prouvent la conjecture de Malle) pour extensions C_2, C_3, S_3, C_4, V_4, D_4, S_4, S_5, ...
- mais on n'a pas un résultat complet pour A_4.
- Résultat partiel : $N_{A_4,K}(X, C_3)$ i.e. on fixe une résolvante cubique. (Cohen)
- On veut trouver un résultat analogue pour les extensions cubiques, ce qui nous permet aussi de donner une formule plus précise.

Le problème

Soit k un corps de nombres, on fixe K_2 une extension quadratique de k.

On définit $\mathcal{F}(K_2)$ l'ensemble des extensions cubiques K de k (mod $\sim$) dont la clôture galoisienne N contient K_2.

Si on accepte $[K_2 : k] = 1$ on peut aussi décrire les extensions cubiques cycliques.



Notre but

On cherche une formule asymptotique pour

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{d}(K/k) \leq X\}| \ .$$

Notre but

On cherche une formule asymptotique pour

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{d}(K/k) \leq X\}|\ .$$

Mais

$$\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}, \quad \text{et} \quad \mathfrak{d}(K/k) = \mathfrak{d}(K_2/k)\mathfrak{f}(K/k)^2,$$

Notre but

On cherche une formule asymptotique pour

$$N(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{d}(K/k) \leq X\}|\ .$$

Mais

$$\mathfrak{f}(N/K_2) = \mathfrak{f}(K/k)\mathbb{Z}_{K_2}, \quad \text{et} \quad \mathfrak{d}(K/k) = \mathfrak{d}(K_2/k)\mathfrak{f}(K/k)^2,$$

On étudie

$$M(K_2/k, X) = |\{K \in \mathcal{F}(K_2),\ \mathcal{N}_{k/\mathbb{Q}}\mathfrak{f}(K/k) \leq X\}|$$

Théorème 1 (Cohen, Morra)

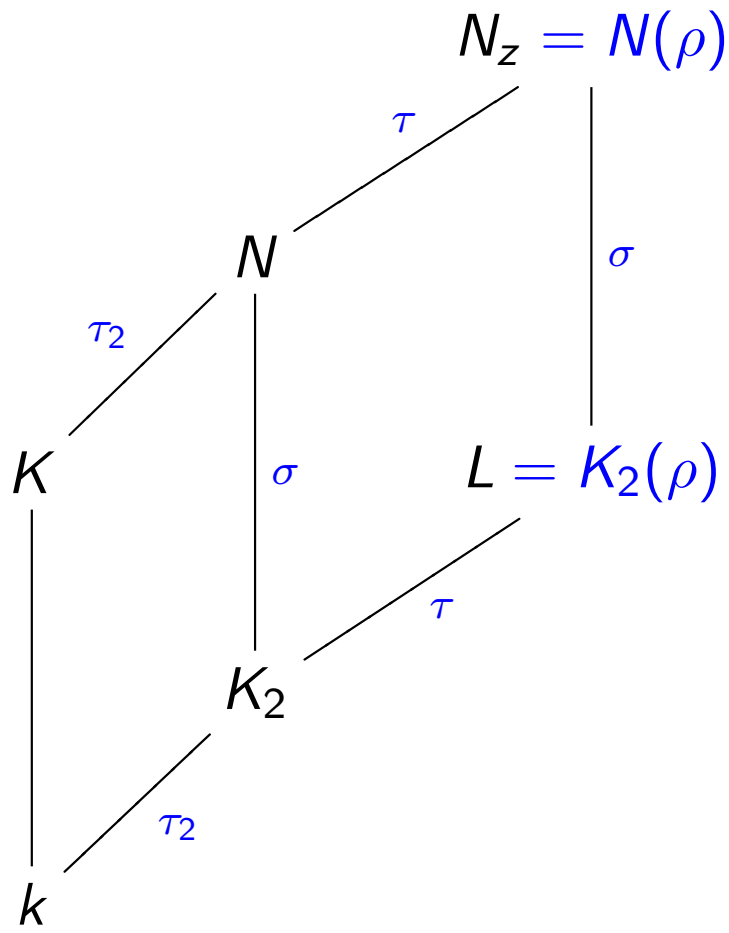
Soit k un corps de nombres quelconque, K_2 une extension de k, $[K_2 : k] \leq 2$.
Alors, on a une des deux formules asymptotiques suivantes:

$$M(K_2/k, X) = C \cdot X + O(X^{\alpha+\varepsilon}), \ ou$$

$$M(K_2/k, X) = C \cdot X(\log(X) + D - 1) + O(X^{\alpha+\varepsilon})$$

où $C > 0, D \in \mathbb{R}$ et $\alpha < 1$ sont des constantes explicites dépendant que de k et K_2.

Cas général



ρ racine cubique primitive de l'unité, $k \neq K_2 \neq L$.

Première bijection

Proposition 1

Il existe une bijection entre :

- *Éléments de* $\mathcal{F}(K_2)$ *(classes d'isomorphisme d'extensions* K/k *ayant résolvante quadratique isomorphe à* K_2*)* , *et*
- *éléments* $\overline{\alpha} \in \mathcal{L} = (L^*/L^{*3})[\tau + 1, \tau_2 + 1]$, $\overline{\alpha} \neq \overline{1}$, $\alpha \sim \alpha^{-1}$.

Première bijection

Proposition 1

Il existe une bijection entre :

- *Éléments de* $\mathcal{F}(K_2)$ *(classes d'isomorphisme d'extensions* K/k *ayant résolvante quadratique isomorphe à* K_2*)* , *et*
- *éléments* $\overline{\alpha} \in \mathcal{L} = (L^*/L^{*3})[\tau+1, \tau_2+1]$, $\overline{\alpha} \neq \overline{1}$, $\alpha \sim \alpha^{-1}$.

$$\overline{\alpha} \in \mathcal{L} \Leftrightarrow \begin{cases} \alpha \in L^* \\ \alpha\tau(\alpha) = \gamma^3, \quad \gamma \in L^* \\ \alpha\tau_2(\alpha) = \gamma'^3, \quad \gamma' \in L^* \end{cases}$$

Le groupe de Selmer

On définit le groupe des 3-**unités virtuelles**

$$V_3(L) = \{u \in L^* \mid u\mathbb{Z}_L = \mathfrak{q}^3, \exists \text{ un idéal } \mathfrak{q} \subset L\}$$

Le groupe de Selmer

On définit le groupe des 3-**unités virtuelles**

$$V_3(L) = \{u \in L^* \mid u\mathbb{Z}_L = \mathfrak{q}^3, \exists \text{ un idéal } \mathfrak{q} \subset L\}$$

et le 3-**groupe de Selmer**

$$S_3(L) = V_3(L)/L^{*3}$$

Bijection fondamentale

Proposition 2

Il existe une bijection entre $\mathcal{F}(K_2)$ *et les classes d'équivalence de triplets* $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$ *tels que*

1. *Les* $\mathfrak{a}_i$ *sont idéaux entiers de* L*, sans facteur carré, premiers entre eux, tels que* $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ *et* $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[\tau+1, \tau_2+1]$*, où* I *est le groupe des idéaux fractionnaires de* L*.*
   On appellera J *l'ensemble des paires* $(\mathfrak{a}_0, \mathfrak{a}_1)$
2. $\overline{u} \in \mathcal{S} = S_3(L)[\tau+1, \tau_2+1]$*, et* $\overline{u} \neq 1$ *quand* $\mathfrak{a}_0 = \mathfrak{a}_1 = \mathbb{Z}_L$*.*

modulo la relation d'équivalence $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u}) \sim (\mathfrak{a}_1, \mathfrak{a}_0, 1/\overline{u})$

La série de Dirichlet

Définition 3

On définit la série de Dirichlet

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} \cdot$$

La série de Dirichlet

Définition 3

On définit la série de Dirichlet

$$\Phi(s) = \frac{1}{2} + \sum_{K \in \mathcal{F}(K_2)} \frac{1}{\mathcal{N}(\mathfrak{f}(K/k))^s} \cdot$$

Par la bijection fondamentale

$$\Phi(s) = \frac{1}{2} \sum_{(\mathfrak{a}_0, \mathfrak{a}_1) \in J} \sum_{\overline{u} \in \mathcal{S}} \frac{1}{\mathcal{N}(\mathfrak{f}(N/K_2))^s} ,$$

Forme finale de la série de Dirichlet

Théorème 2 (Cohen, Morra)

On a

$$\Phi(s) = \frac{|(U(L)/U(L)^3)[\tau+1,\tau_2+1]|}{2\cdot 3^{(3/2)[k:\mathbb{Q}]s}\prod_{\substack{p|3\mathbb{Z}_k,\\ e(\mathfrak{p}/3)\,impair}} \mathcal{N}(p)^{s/2}} \cdot$$
$$\cdot \sum_{\mathfrak{b}\in\mathcal{B}} \left(\frac{\lceil\mathcal{N}\rceil(\mathfrak{b})}{\mathcal{N}(\mathfrak{r}^e(\mathfrak{b}))}\right)^s \frac{P_{\mathfrak{b}}(s)}{|(Z_{\mathfrak{b}}/Z_{\mathfrak{b}}^3)[\tau+1,\tau_2+1]|} \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} F(\mathfrak{b},\chi,s)\,.$$

Les autres cas

Cas	type extension	ρ	τ, τ_2	T
1	cyclique	$\rho \in k$	$\tau = \tau_2 = 1$	$\emptyset$
2	cyclique	$\rho \notin k$	$\tau_2 = 1$ $\tau(\rho) = \rho^{-1}$	$T = \{\tau + 1\}$
3	non cyclique	$\rho \in k$	$\tau = 1$ $\tau_2(\rho) = \rho$	$T = \{\tau_2 + 1\}$
4	non cyclique	$\rho \in K_2 \setminus k$	$\tau = 1$ $\tau_2(\rho) = \rho^{-1}$	$T = \{\tau_2 - 1\}$
5	non cyclique	$\rho \notin K_2$	$\tau, \tau_2 \neq 1$ $\tau(\rho) = \rho^{-1}$ $\tau_2(\rho) = \rho$	$T = \{\tau + 1,$ $\tau_2 + 1\}$

- Dans les cas 2,3 et 5 on développe $\Phi(s)$ autour du pôle $s = 1$

$$\Phi(s) = \frac{C}{(s-1)} + O(1),$$

et grâce à un théorème tauberien

$$M(K_2/k, X) \sim C \cdot X$$

- Dans les cas 2,3 et 5 on développe $\Phi(s)$ autour du pôle $s = 1$

$$\Phi(s) = \frac{C}{(s-1)} + O(1),$$

et grâce à un théorème tauberien

$$M(K_2/k, X) \sim C \cdot X$$

- Dans les cas 1 et 4 de manière similaire on obtient

$$\Phi(s) = \frac{C}{(s-1)^2} + \frac{C \cdot D}{(s-1)} + O(1), \text{ et donc}$$

$$M(K_2/k, X) \sim C \cdot X(\log(X) + D - 1)$$

Le terme d'erreur

- On peut prouver que le terme d'erreur dans les formules asymptotiques du théorème est $O(X^{\alpha+\varepsilon})$, $\alpha < 1$, pour tout $\varepsilon > 0$.

Le terme d'erreur

- On peut prouver que le terme d'erreur dans les formules asymptotiques du théorème est $O(X^{\alpha+\varepsilon})$, $\alpha < 1$, pour tout $\varepsilon > 0$.
- En particulier pour $k = \mathbb{Q}$ on peut montrer $\alpha = 2/3$.

Le terme d'erreur

- On peut prouver que le terme d'erreur dans les formules asymptotiques du théorème est $O(X^{\alpha+\varepsilon})$, $\alpha < 1$, pour tout $\varepsilon > 0$.
- En particulier pour $k = \mathbb{Q}$ on peut montrer $\alpha = 2/3$.
- Si on suppose l'hypothèse de Lindelöf (généralisée) on a $\alpha = 1/2$ pour tout k, K_2.

Le terme d'erreur

- On peut prouver que le terme d'erreur dans les formules asymptotiques du théorème est $O(X^{\alpha+\varepsilon})$, $\alpha < 1$, pour tout $\varepsilon > 0$.
- En particulier pour $k = \mathbb{Q}$ on peut montrer $\alpha = 2/3$.
- Si on suppose l'hypothèse de Lindelöf (généralisée) on a $\alpha = 1/2$ pour tout k, K_2.
- **Remarque :** GRH $\Longrightarrow$ Lindelof.

Exemples

Extensions cubiques cycliques $\mathbb{Q}$

$$\sum_{K/\mathbb{Q} \text{ cubiques cycliques}} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{p \equiv 1 \pmod 3} \left(1 + \frac{2}{p^s}\right),$$

donc

$$M(\mathbb{Q}, X) = C \cdot X + O(X^{2/3+\varepsilon}),$$

avec

$$C = \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{2}{p(p+1)}\right)$$
$$= 0.158528258396142060283507820357 5\ldots$$

Corps cubiques purs sur $\mathbb{Q}$

Cas (4) : $K_2 = \mathbb{Q}(\rho)$ et $L = K_2$, donc $K/\mathbb{Q}$ est un *corps cubique pur* i. e. $K = \mathbb{Q}(\sqrt[3]{m})$. On obtient

$$\sum_{K/\mathbb{Q} \text{ cubiques purs}} \frac{1}{f(K)^s} = -\frac{1}{2} + \frac{1}{6}\left(1 + \frac{2}{3^s} + \frac{6}{3^{2s}}\right) \prod_{p \neq 3} \left(1 + \frac{2}{p^s}\right)$$
$$+ \frac{1}{3} \prod_{p \equiv \pm 1 \pmod 9} \left(1 + \frac{2}{p^s}\right) \prod_{p \not\equiv \pm 1 \pmod 9} \left(1 - \frac{1}{p^s}\right).$$

et donc

$$M(\mathbb{Q}(\sqrt{-3}), X) = C \cdot X \cdot (\log(X) + D - 1) + O(X^{2/3+\varepsilon}),$$

où

$$C = C(\mathbb{Q}(\sqrt{-3})) = \frac{7}{30} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right)$$
$$= 0.066907733301378371291841632984295\ldots$$
$$D = D(\mathbb{Q}(\sqrt{-3})) = 2\gamma - \frac{16}{35}\log(3) + 6\sum_p \frac{\log(p)}{p^2 + p - 2}$$
$$= 3.450222797830591962790711919671110\ldots,$$

et γ est la constante d'Euler.

Cas (5) : $K_2 = \mathbb{Q}(\sqrt{D})$ **avec** $D \neq -3$

Il existe une fonction $\phi_D(s)$ holomorphe pour $\mathrm{Re}(s) > 1/2$ telle que

$$\sum_{K \in \mathcal{F}(K_2)} \frac{1}{f(K)^s} = \phi_D(s) + \frac{3^{r_2(D)}}{6} L_3(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{2}{p^s}\right),$$

où

$$L_3(s) = \begin{cases} 1 + 2/3^{2s} & \text{si } 3 \nmid D, \\ 1 + 2/3^s & \text{si } D \equiv 3 \pmod 9, \\ 1 + 2/3^s + 6/3^{2s} & \text{si } D \equiv 6 \pmod 9. \end{cases}$$

$r_2(D) = 1$ pour $D < 0$, $r_2(D) = 0$ sinon.

On pose $D' = -3D$ si $3 \nmid D$ et $D' = -D/3$ si $3 \mid D$, et on note $\chi_{D'}$ le caractère $\left(\frac{D'}{\cdot}\right)$. Alors si $D \neq -3$ est un discriminant fondamental, pour tout $\varepsilon > 0$ on a

$$M(\mathbb{Q}(\sqrt{D}), X) = C \cdot X + O(X^{2/3+\varepsilon}),$$

avec

$$C = \frac{3^{r_2(D)} \ell_3 L(\chi_{D'}, 1)}{\pi^2} \prod_{p \mid D'} \left(1 - \frac{1}{p+1}\right) \cdot \prod_{\left(\frac{D'}{p}\right)=1} \left(1 - \frac{2}{p(p+1)}\right), \quad \text{où}$$

$$\ell_3 = \begin{cases} 11/9 & \text{si } 3 \nmid D, \\ 5/3 & \text{si } D \equiv 3 \pmod 9, \\ 7/5 & \text{si } D \equiv 6 \pmod 9. \end{cases}$$

Un algorithme pour énumerer les extensions cubiques relatives

Résultat principal

Théorème 3

Soit K un des 9 corps quadratiques imaginaires de nombre de classes 1.

Résultat principal

Théorème 3

Soit K un des 9 corps quadratiques imaginaires de nombre de classes 1.

- *Il existe un algorithme pour énumerer toutes les extensions cubiques de K $(\mathrm{mod}\ \sim)$ jusqu'à une borne X sur la norme du discriminant relatif.*

Résultat principal

Théorème 3

Soit K un des 9 corps quadratiques imaginaires de nombre de classes 1.

- *Il existe un algorithme pour énumerer toutes les extensions cubiques de K (mod $\sim$) jusqu'à une borne X sur la norme du discriminant relatif.*
- *Cet algorithme marche en temps $O_\varepsilon(X^{1+\varepsilon})$, pour tout $\varepsilon > 0$.*

Résultat principal

Théorème 3

Soit K un des 9 corps quadratiques imaginaires de nombre de classes 1.

- *Il existe un algorithme pour énumerer toutes les extensions cubiques de K (mod $\sim$) jusqu'à une borne X sur la norme du discriminant relatif.*
- *Cet algorithme marche en temps $O_\varepsilon(X^{1+\varepsilon})$, pour tout $\varepsilon > 0$.*

On a programmé une version explicite en PARI/GP pour le cas $K = \mathbb{Q}(i)$ qui peut être facilement adaptée pour tout corps quadratique imaginaire de nombre de classes 1.

L'algorithme sur $\mathbb{Q}$

Théorème 4 (Levi, Delone-Faddeev, Davenport-Heilbronn, Belabas, Bhargava)

Il existe une bijection entre les corps cubiques sur $\mathbb{Q}$ (modulo isomorphisme) et les classes de formes quadratiques 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* $\mathbb{Q}[x]/(ax^3 + bx^2 + cx + d)$.

L'algorithme sur $\mathbb{Q}$

Théorème 4 (Levi, Delone-Faddeev, Davenport-Heilbronn, Belabas, Bhargava)

Il existe une bijection entre les corps cubiques sur $\mathbb{Q}$ (modulo isomorphisme) et les classes de formes quadratiques 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* $\mathbb{Q}[x]/(ax^3 + bx^2 + cx + d)$.

L'algorithme de Belabas : utilise le critère de Dedekind + des méthodes de crible $\Longrightarrow$ on peut énumerer les $O(X)$ corps de discriminant borné par X en utilisant $O(X)$ opérations sur entiers $\leq X$.

Le théorème de Taniguchi (1)

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

Le théorème de Taniguchi (1)

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

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

Le théorème de Taniguchi (1)

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

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

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

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

.

Le théorème de Taniguchi (1)

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

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

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

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

.

- $G_{\mathfrak{a}} = \left\{ \begin{pmatrix} \alpha\in\mathcal{O} & \beta\in\mathfrak{a}^{-1} \\ \gamma\in\mathfrak{a} & \delta\in\mathcal{O} \end{pmatrix} \middle| \alpha\delta-\beta\gamma\in\mathcal{O}^{\times} \right\}$
- $V_{\mathfrak{a}} = \{F = (a,b,c,d) \mid a\in\mathfrak{a}, b\in\mathcal{O}, c\in\mathfrak{a}^{-1}, d\in\mathfrak{a}^{-2}\}$

Le théorème de Taniguchi (2)

Théorème 5 (Taniguchi)

Il existe une bijection canonique entre $\mathcal{C}(\mathcal{O}, \mathfrak{a})$ et $V_{\mathfrak{a}}/G_{\mathfrak{a}}$ qui rend ce diagramme commutatif :

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

Le covariant

Soit $\mathcal{O}$ un ordre *quadratique imaginaire* maximal.

Soit $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Le covariant

Soit $\mathcal{O}$ un ordre *quadratique imaginaire* maximal.

Soit $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

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

Le covariant

Soit $\mathcal{O}$ un ordre *quadratique imaginaire* maximal.

Soit $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

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

grâce au travail de G. Julia, on sait que un covariant pour l'action de $\mathrm{GL}_2(\mathcal{O})$ est la forme hermitienne binaire:

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

où $t_i^2 = |a|^2|\alpha_j - \alpha_k|^2 \quad i \neq j \neq k \neq i.$

On peut écrire

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

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 peut écrire

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

où

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

Soit

$$\Delta := PR - |Q|^2 = 3|D(F)|$$

Le 3-espace hyperbolique

$$\begin{aligned}\mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}_+^*\} \\ &= \{h = z + tj \mid t > 0, h \in \mathbb{H} \text{ de } k - \text{composante } 0\},\end{aligned}$$

où $\mathbb{H}$ est l'anneau des quaternions.

Le 3-espace hyperbolique

$$\begin{aligned}\mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}_+^*\} \\ &= \{h = z + tj \mid t > 0, h \in \mathbb{H} \text{ de } k - \text{composante } 0\},\end{aligned}$$

où $\mathbb{H}$ est l'anneau des quaternions.

L'action de $\mathrm{SL}_2(\mathbb{C})$ sur $\mathcal{H}_3$ (notation des quaternions)

$$M \cdot h = (Ah + B)(Ch + D)^{-1},$$

pour tout $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}), h \in \mathcal{H}_3.$

Le 3-espace hyperbolique

$$\begin{aligned}\mathcal{H}_3 &= \{z + tj \mid z \in \mathbb{C}, t \in \mathbb{R}_+^*\} \\ &= \{h = z + tj \mid t > 0, h \in \mathbb{H} \text{ de } k - \text{composante } 0\},\end{aligned}$$

où $\mathbb{H}$ est l'anneau des quaternions.

L'action de $\mathrm{SL}_2(\mathbb{C})$ sur $\mathcal{H}_3$ (notation des quaternions)

$$M \cdot h = (Ah + B)(Ch + D)^{-1},$$

pour tout $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}), h \in \mathcal{H}_3$.

Soit $\mathscr{P} =$
$\{$ formes hermitiennes binaires, définies positives dans $\mathbb{C}\}$
et soit $\widetilde{\mathscr{P}} = \mathscr{P}/\mathbb{R}^+$ où $\mathbb{R}^+$ agit sur $\mathscr{P}$ par multiplication.

$\Phi : \mathscr{P} \longrightarrow \mathcal{H}_3$ défini par:

$$\Phi\left(\begin{pmatrix} P & Q \\ Q & R \end{pmatrix}\right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j.$$

$\Phi : \mathscr{P} \to \mathcal{H}_3$ défini par:

$$\Phi\left(\begin{pmatrix} P & Q \\ Q & R \end{pmatrix}\right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j.$$

Φ induit une bijection $\widetilde{\Phi} : \widetilde{\mathscr{P}} \to \mathcal{H}_3$,
qui commute avec l'action de $\mathrm{SL}_2(\mathcal{O})$.

$\Phi : \mathscr{P} \to \mathcal{H}_3$ défini par:

$$\Phi\left(\begin{pmatrix} P & Q \\ Q & R \end{pmatrix}\right) = -\frac{Q}{P} + \frac{\sqrt{\Delta}}{P} j.$$

Φ induit une bijection $\widetilde{\Phi} : \widetilde{\mathscr{P}} \to \mathcal{H}_3$,
qui commute avec l'action de $\mathrm{SL}_2(\mathcal{O})$.

Les domaines fondamentaux de $\mathcal{H}_3$ modulo $SL_2(\mathcal{O})$ sont bien connus (Swan).

- Quand $h_K = 1$, à partir de la description du domaine fondamental de $\mathcal{H}_3$ modulo $SL_2(\mathcal{O})$ on obtient une borne inférieure $t \geq t_K > 0$ qui ne dépend que du discriminant du corps de nombres K, pour $z + it \in \mathcal{H}_3$ dans le domaine fondamental.
  Cela nous permet de borner P, Q, R, et donc a, b, c, d.

- Quand $h_K = 1$, à partir de la description du domaine fondamental de $\mathcal{H}_3$ modulo $SL_2(\mathcal{O})$ on obtient une borne inférieure $t \geq t_K > 0$ qui ne dépend que du discriminant du corps de nombres K, pour $z + it \in \mathcal{H}_3$ dans le domaine fondamental.
  Cela nous permet de borner P, Q, R, et donc a, b, c, d.

- (Question ouverte) Quand $h_K > 1$, il y a des points du domaine fondamental tels que $t = 0$ (pointes), donc on a besoin d'une action de groupe supplémentaire pour envoyer ces autres pointes sur la pointe à infini. Une fois trouvée cette action, il devrait être possible de borner P, Q, R et obtenir un algorithme explicite aussi dans le cas $h_K \neq 1$.

Quand $h_K = 1$

$$\{\text{extensions cubiques } L/K, \text{ avec } \mathfrak{d}(L/K) \leq X\}/\sim$$

Quand $h_K = 1$

$$\{\text{extensions cubiques } L/K, \text{ avec } \mathfrak{d}(L/K) \leq X\}/\sim$$
$$\updownarrow$$
$$\{\text{formes cubiques binaires modulo } GL_2(\mathcal{O})\}$$

Quand $h_K = 1$

$$\{\text{extensions cubiques } L/K, \text{ avec } \mathfrak{d}(L/K) \leq X\}/\sim$$
$$\updownarrow$$
$$\{\text{formes cubiques binaires modulo } GL_2(\mathcal{O})\}$$
$$\downarrow$$
$$\{\text{(covariant) formes hermitiennes binaires définies positives}\}$$

Quand $h_K = 1$

$$\{\text{extensions cubiques } L/K, \text{ avec } \mathfrak{d}(L/K) \leq X\}/\sim$$
$$\updownarrow$$
$$\{\text{formes cubiques binaires modulo } GL_2(\mathcal{O})\}$$
$$\downarrow$$
$$\{\text{(covariant) formes hermitiennes binaires définies positives}\}$$
$$\updownarrow$$
$$\{\text{points de } \mathcal{H}_3 \text{ modulo } GL_2(\mathcal{O})\}.$$

Théorème 6

Soit $F = (a, b, c, d)$ une forme cubique binaire réduite, avec coefficients dans $\mathcal{O}$, dont la norme du discriminant relatif est bornée par X. Alors

$$|a| \ll X^{1/8}; \quad |b| \ll X^{1/8}$$

$$|ad| \ll X^{1/4}; \quad |bc| \ll X^{1/4}.$$

et donc on peut parcourir les telles formes F en temps $O(X)$.

Implémentation

- Automorphismes et morphismes du bord (algorithme pour parcourir toutes les matrices).

Implémentation

- Automorphismes et morphismes du bord (algorithme pour parcourir toutes les matrices).
- Calculs flottants et vérification d'identités algébriques.

Implémentation

- Automorphismes et morphismes du bord (algorithme pour parcourir toutes les matrices).
- Calculs flottants et vérification d'identités algébriques.
- Étude de la précision nécessaire.

Implémentation

- Automorphismes et morphismes du bord (algorithme pour parcourir toutes les matrices).
- Calculs flottants et vérification d'identités algébriques.
- Étude de la précision nécessaire.
- Une autre réduction pour parcourir plus rapidement les (a, b, c, d).

Implémentation

- Automorphismes et morphismes du bord (algorithme pour parcourir toutes les matrices).
- Calculs flottants et vérification d'identités algébriques.
- Étude de la précision nécessaire.
- Une autre réduction pour parcourir plus rapidement les (a, b, c, d).
- Comparaison avec l'algorithme classique (corps de classes de rayon).

Résultats

$K = \mathbb{Q}(i)$

X	$N(X)$	t	t'
10^4	276	5s	16s
$4 \cdot 10^4$	1339	19s	1mn 18s
$9 \cdot 10^4$	3305	56s	3mn 45s
10^6	42692	24mn 1s	2h 52mn 9s
$4 \cdot 10^6$	181944	2h 49mn	34h 24mn 8s
$9 \cdot 10^6$	421559	9h 37 mn	$>$ 134h
10^8	4990974	359h 25mn	$>$ 2720 h

(Intel Xeon 5160 dual core, 3.0 GHz)

Merci