Expérimentations avec le calcul du groupe des classes de corps de nombres de grand degré

B. Allombert

Université Montpellier 2 LIRMM/I3M
(avec Karim Belabas, Université Bordeaux 1)

21/01/2010

Lignes directrices

Introduction

Algorithme pour le calcul du groupe de classes et du groupe des unités d'un corps de nombres.

- Inventé il y a 20 ans par J.Buchmann
- Généralisation de l'algorithme de Haffner et McCurley pour les corps quadratiques imaginaires.
- Implanté par Cohen-Diaz-Olivier dans PARI/GP
- Algorithme "Las Vegas", sous GRH, heuristiquement en temps sous-exponentiel en la taille du discriminant, si le degré est fixé.
- Autre implantation complète connue : Magma/KANT.

Lignes directrices

Notations

Soit K un corps de nombres on note :

- n le degré de K.
- (r_1, r_2) la signature de K.
- $(\sigma_1, \ldots, \sigma_n)$ les plongements complexes de K.
- $\mathcal{O}(K)$ l'anneau des entiers de K.
- $\mathrm{d}(K)$ le discriminant de $\mathcal{O}(K)$.
- $\mu(K)$ le groupe des racines de l'unité dans K.
- $U(K)$ la partie libre de $\mathcal{O}(K)^\times$.
- $R(K)$ le régulateur de K.
- $\mathcal{C}\ell(K)$ le groupe de classes de $\mathcal{O}(K)$.
- $h(K)$ le nombre de classes de $\mathcal{O}(K)$.

Lignes directrices

Structure des groupes

Théorème (P.Dirichlet)

$\mathcal{O}(K)^\times = \mu(K)U(K)$ *et* $U(K) \cong \mathbb{Z}^{r_1+r_2-1}$.

Théorème (E.Bach, sous GRH)

Soit C le plus petit nombre réel tel que l'ensemble des idéaux premiers de norme au plus $C\log(d(K))^2$ *engendre* $\mathcal{C}\ell(K)$*, alors* $C \leq 12$.

Conséquence :

- Les générateurs du groupe de classes sont connus, mais pas les relations.
- Les relations du groupe des unités sont connues mais pas les générateurs.

Lignes directrices

Fonction zeta

Théorème (R.Dedekind)

Soit

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}}$$

la fonction ζ du corps K, alors

$$\mathrm{Res}_1(\zeta_K) = 2^{r_1}(2\pi)^{r_2} \frac{h(K)R(K)}{|\mu(K)|\sqrt{|d(K)|}}$$

Remarque

$$\mathrm{Res}_1(\zeta_K) = \lim_{s=1} \zeta_K(s)/\zeta(s) = \prod_p \frac{1-p^{-1}}{\prod_{\mathfrak{p}|p}\left(1-\mathcal{N}(\mathfrak{p})^{-1}\right)}$$

Théorème (sous GRH)

Soit

$$z = 2^{-r_1}(2\pi)^{-r_2}|\mu(K)|\sqrt{|d(K)|}\prod_{p\leq M} \frac{1-p^{-1}}{\prod_{\mathfrak{p}|p,\mathcal{N}(\mathfrak{p})\leq M}\left(1-\mathcal{N}(\mathfrak{p})^{-1}\right)}$$

alors il existe $M = O(\log(|d(K)|)^2)$ *tel que* $z/\sqrt{2} < h(K)R(K) < z\sqrt{2}$.

Lignes directrices

Principe heuristique

Soit I un idéal entier de $\mathcal{O}_K$ supposé principal.

- L'élément α engendre I si et seulement si $|\mathcal{N}(\alpha)| = \mathcal{N}(I)$.
- Il s'agit donc de minimiser la fonction $\mathcal{N}$ sur I.
- Or on ne sait pas minimiser directement $\mathcal{N}$.
- On majore $\mathcal{N}$ par une forme quadratique définie positive.

$$|\mathcal{N}(x)| = |\prod_{i=1}^{n} \sigma_i(x)| \leq q(x)^{\frac{n}{2}}$$

(par exemple, $q(x) = \sum_{i=1}^{n} |\sigma_i(\alpha)|^2$).

- L'algorithme LLL nous donne un élément $\alpha \in I$ tel que $q(\alpha) \leq 2^{n-1} \min_I(q)$.
- On espère que $\mathcal{N}(\alpha)$ est proche de $\mathcal{N}(I)$.

Relations aléatoires

Soit

$$\mathcal{P} = \{\mathfrak{p}; \mathcal{N}(\mathfrak{p}) \leq C \log(\mathrm{d}(K))^2\}$$

la "base de facteur".

- On choisit au hasard des entiers positifs $(a_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$.
- On calcule $I = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{a_\mathfrak{p}}$.
- On choisit des entiers v_i et l'on munit I de la forme quadratique $q(\alpha) = \sum_{i=1}^{n} e^{v_i} |\sigma_i(\alpha)|^2$.
- LLL permet de trouver un élément $\alpha \in I$ petit pour q.
- On espère que $\mathcal{N}(\alpha)$ est petit.

On essaie de factoriser $\alpha\mathcal{O}_K$ dans la base $\mathcal{P}$. En cas de succès on obtient la factorisation de $J = I/\alpha$. On écrit $J = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{b_\mathfrak{p}}$ et l'on a la relation

$$\prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{b_\mathfrak{p}-a_\mathfrak{p}} = \alpha\mathcal{O}_K \ .$$

Dans le groupe de classe nous avons :

$$\prod_{\mathfrak{p}\in\mathcal{P}} \mathcal{C}\ell(\mathfrak{p})^{b_\mathfrak{p}-a_\mathfrak{p}} = 1$$

De plus si, en combinant des relations, nous trouvons une relation

$$\prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{0} = \beta\mathcal{O}_K$$

alors β est une unité.

Critère d'arrêt

Supposons que l'on ait trouvé un ensemble de relations et un ensemble d'unités. Soit $\widetilde{U}$ le sous-groupe de $U(K)$ engendré, et $\widetilde{\mathcal{C}\ell}$ le quotient obtenu, alors on peut calculer une valeur $\widetilde{h}$ et $\widetilde{R}$. On a

$$\widetilde{h}\widetilde{R} = [U(K) : \widetilde{U}][\widetilde{\mathcal{C}\ell} : \mathcal{C}\ell(K)]h(K)R(K)$$

donc si

$$z/\sqrt{2} < \widetilde{h}\widetilde{R} < \sqrt{2}z$$

alors $U(K) = U$ et $\widetilde{\mathcal{C}\ell} = \mathcal{C}\ell(K)$.

Lignes directrices

Résumé de l'algorithme

1. Calcul de $\mathrm{d}(K)$ et d'une base d'entiers de $\mathcal{O}(K)$.
2. Calcul de $\mu(K)$.
3. Calcul de $B = C \log(\mathrm{d}(K))^2$.
4. Calcul de tout les idéaux premiers de norme au plus B.
5. Calcul de z tel que $z/\sqrt{2} < h(K)R(K) < z\sqrt{2}$.
6. Calcul des relations triviales $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p}}$.
7. Calcul des relations dues aux éléments de petites normes.
8. Calcul de relations aléatoires.
9. Calcul de $\widetilde{h}$ et $\widetilde{R}$.
10. Si $z/\sqrt{2} < \widetilde{h}\widetilde{R} < z\sqrt{2}$, terminer l'algorithme, sinon recommencer en 8

Progrès

1. Calcul de $\mathrm{d}(K)$ et d'une base d'entiers de $\mathcal{O}(K)$. Implantation de l'algorithme Round4 de H.Zassenhaus/D.Ford par X.Roblot et S.Pauli.
2. Calcul de $\mu(K)$. Implantation d'un algorithme en temps polynomial (P.Molin)
3. Calcul de $B = C\log(\mathrm{d}(K))^2$. L'algorithme de K.Belabas/F.Diaz Y Diaz/E.Friedmann permet de trouver une constante C adapté à un corps donné (souvent $C \leq \frac{2}{3}$).

Progrès

1. Calcul de $\mathrm{d}(K)$ et d'une base d'entiers de $\mathcal{O}(K)$. Implantation de l'algorithme Round4 de H.Zassenhaus/D.Ford par X.Roblot et S.Pauli.
2. Calcul de $\mu(K)$. Implantation d'un algorithme en temps polynomial (P.Molin)
3. Calcul de $B = C \log(\mathrm{d}(K))^2$. L'algorithme de K.Belabas/F.Diaz Y Diaz/E.Friedmann permet de trouver une constante C adapté à un corps donné (souvent $C \leq \frac{2}{3}$).

Progrès

1. Calcul de $\mathrm{d}(K)$ et d'une base d'entiers de $\mathcal{O}(K)$. Implantation de l'algorithme Round4 de H.Zassenhaus/D.Ford par X.Roblot et S.Pauli.
2. Calcul de $\mu(K)$. Implantation d'un algorithme en temps polynomial (P.Molin)
3. Calcul de $B = C \log(\mathrm{d}(K))^2$. L'algorithme de K.Belabas/F.Diaz Y Diaz/E.Friedmann permet de trouver une constante C adapté à un corps donné (souvent $C \leq \frac{2}{3}$).

Progrès

4. Calcul de $\mathcal{P} = \{\mathfrak{p}; \mathcal{N}(\mathfrak{p}) \leq B\}$.
5. Calcul de z tel que $z/\sqrt{2} < h(K)R(K) < z\sqrt{2}$.
6. Calcul des relations triviales $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}$.
7. Calcul des relations dues aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas où il y a un nombre exponentiel de vecteurs minimaux.
8. Calcul de relations aléatoires. Implantation de LLL^2 de P-Q.Nguyen et D.Stelhé pour la réduction de réseau. Amélioration de la stratégie pour le choix des $(a_\mathfrak{p})$.
9. Calcul de $\widetilde{h}$ et $\widetilde{R}$. Amélioration de la stabilité numérique du calcul de $\widetilde{R}$.

Progrès

4. Calcul de $\mathcal{P} = \{\mathfrak{p}; \mathcal{N}(\mathfrak{p}) \leq B\}$.
5. Calcul de z tel que $z/\sqrt{2} < h(K)R(K) < z\sqrt{2}$.
6. Calcul des relations triviales $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}$.
7. Calcul des relations dues aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas où il y a un nombre exponentiel de vecteurs minimaux.
8. Calcul de relations aléatoires. Implantation de LLL^2 de P-Q.Nguyen et D.Stelhé pour la réduction de réseau. Amélioration de la stratégie pour le choix des $(a_\mathfrak{p})$.
9. Calcul de $\widetilde{h}$ et $\widetilde{R}$. Amélioration de la stabilité numérique du calcul de $\widetilde{R}$.

Progrès

4. Calcul de $\mathcal{P} = \{\mathfrak{p}; \mathcal{N}(\mathfrak{p}) \leq B\}$.
5. Calcul de z tel que $z/\sqrt{2} < h(K)R(K) < z\sqrt{2}$.
6. Calcul des relations triviales $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}$.
7. Calcul des relations dues aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas où il y a un nombre exponentiel de vecteurs minimaux.
8. Calcul de relations aléatoires. Implantation de LLL^2 de P-Q.Nguyen et D.Stelhé pour la réduction de réseau. Amélioration de la stratégie pour le choix des $(a_{\mathfrak{p}})$.
9. Calcul de $\widetilde{h}$ et $\widetilde{R}$. Amélioration de la stabilité numérique du calcul de $\widetilde{R}$.

Progrès

4. Calcul de $\mathcal{P} = \{\mathfrak{p}; \mathcal{N}(\mathfrak{p}) \leq B\}$.
5. Calcul de z tel que $z/\sqrt{2} < h(K)R(K) < z\sqrt{2}$.
6. Calcul des relations triviales $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}$.
7. Calcul des relations dues aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas où il y a un nombre exponentiel de vecteurs minimaux.
8. Calcul de relations aléatoires. Implantation de LLL^2 de P-Q.Nguyen et D.Stelhé pour la réduction de réseau. Amélioration de la stratégie pour le choix des $(a_\mathfrak{p})$.
9. Calcul de $\widetilde{h}$ et $\widetilde{R}$. Amélioration de la stabilité numérique du calcul de $\widetilde{R}$.

Une nouvelle stratégie pour les relations

Principe (1)

Pour que la matrice des relations soit de rang maximal, il faut au moins que chaque idéal de la base appartienne à au moins une relation.

Principe (2)

Pour trouver des relations relativement vite, il faut que I soit relativement petit.

- On choisit un ensemble fini $S \subset \mathcal{P}$ de petits idéaux premiers.
- On réduit la matrice des relations par HNF.
- Pour chaque $\mathfrak{p}$ qui n'est pas "éliminé", on essaie un vecteur (a) avec $a_{\mathfrak{p}} = 1$ et $a_{\mathfrak{p}'} = 0$ si $\mathfrak{p}' \notin S \cup \{\mathfrak{p}\}$.
- Si l'on ne fait pas de progrès, on change S et l'on recommence.

Lignes directrices

Résultats expérimentaux

Corps	Deg.	Root	$\mathcal{C}\ell$	R	temps
$\mathbb{Q}(\zeta_{23})^H$	66	19.9	1	1.98138718 E17	3h, 51min
$\mathbb{Q}(\zeta_{120})^h$	64	23.2	2	1.147710183 E19	3h, 11min
$\mathbb{Q}(\zeta_{29})^h$	56	25.7	2x2	3.29663170 E17	3h, 21min
$\mathbb{Q}(\zeta_{39})^H$	48	18.2	1	1.19342320 E12	9min
$\mathbb{Q}(\zeta_{109})^+$	54	99.9	1	9.79264019 E36	1h, 17min
$\mathbb{Q}(\zeta_{113})^+$	56	103.9	1	9.43984600 E38	2h, 12min
$\mathbb{Q}(\alpha_{59})$	59	59.0	1	5.60503440 E28	7h, 48min
$\mathbb{Q}(\alpha_{61})$	61	61.0	1	6.45543747 E29	56h, 11min
$\mathbb{Q}(\sqrt[53]{2})$	53	104.6	1	5.74645573 E32	30h, 43min
$\mathbb{Q}(\sqrt[54]{2})$	54	106.6	1	2.84366591 E33	80h, 23min
$\mathbb{Q}(\zeta_{36}, \sqrt[6]{2})$	72	29.8	3	7.395320 E24	327h
$\mathbb{Q}(\zeta_{16}, \sqrt[16]{2})$	64	34.1	1	2.75018677 E24	6h, 47min
$\mathbb{Q}(\zeta_9, \sqrt[9]{2})$	54	21.7	1	1.41057940 E15	6min

$(\alpha_p)^p = \alpha_p + 1$

Lignes directrices

Conclusion heuristique

Il semble que la présence de racines de l'unité dans le corps de nombres rende le calcul plus facile. Nous proposons plusieurs justifications heuristiques :

- Les corps cyclotomiques ont un root-discriminant relativement petits.
- Les racines de l'unités implique l'existence d'unités cyclotomiques, facile à calculer.
- Les réseaux contenant les racines de l'unités semblent être plus faciles à traiter par LLL qui retourne souvent le plus petit vecteur.

Lignes directrices

Extensions ramifiées en un seul premier

Théorème (D.Harbater (1994), théorème 2.6 in «Galois groups with prescribed ramification»)

1. *Si* $p < 23$ *est premier, alors* $\pi_1^t(\mathrm{Spec}(\mathbb{Z}[\frac{1}{p}])) \cong \mathbb{Z}/(p-1)\mathbb{Z}$
2. *Le groupe* $\pi_1^t(\mathrm{Spec}(\mathbb{Z}[\frac{1}{23}]))$ *n'est pas cyclique.*

Théorème (sous GRH+PARI)

$$\pi_1^t(\mathrm{Spec}(\mathbb{Z}[\frac{1}{23}]))^{\mathrm{solv}} \cong \mathbb{Z}/11\mathbb{Z} \times \mathrm{D}_6$$

Lignes directrices

Construction explicite de corps de classes.

Soit K un corps de nombre, un conducteur $\mathfrak{f}$ et un sous-groupe C de $\mathcal{C}\ell_{\mathfrak{f}}(K)$ d'indice ℓ premier. Il s'agit de calculer le sous-corps L du corps de classe de rayon $\mathfrak{f}$ de K correspondant à C ($[L : K] = \ell$).
Les algorithmes algébriques de constructions explicites de corps de classes basés sur la théorie de Kummer requièrent le calcul du groupe de classe et du groupe des unités du corps $K(\zeta_\ell)$, mais ont une complexité polynomial en le conducteur.

Kronecker Jugendraum

Les algorithmes basés sur une version effective du "Jugendraum" de Kronecker ont une complexité exponentielle dans le conducteur et ne sont connus que pour certaines classes de corps de bases.

Réalisation explicite de groupe de Galois.

En utilisant des constructions explicite de corps de classes, nous avons pu calculer des polynômes réalisant explicitement certains groupe de Galois comme extensions totalement réelles et totalement complexes sur $\mathbb{Q}$.

Groupe	sign.	$[K:\mathbb{Q}]$	ℓ	$[K(\zeta_\ell):\mathbb{Q}]$	$[L:\mathbb{Q}]$	cond.
$C_{13} \rtimes C_8$	cplx	4	13	48	52	499
$C_{13} \rtimes C_8$	réel	4	13	48	52	155
$C_{25} \rtimes C_4$	cplx	20	5	20	100	14
$C_{25} \rtimes C_4$	réel	20	5	40	100	107
$C_{31} \rtimes C_3$	réel	3	31	31	93	155
$C_{17} \rtimes C_4$	réel	4	17	17	68	137