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

B. Allombert

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

10/06/2009

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 quadratique imaginaire.
- 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 connu : 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.
- $\mathrm{d}(K)$ l'anneau des entiers de K.
- $\mathcal{O}(K)$ l'anneau des entiers de 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 regulateur 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 connus 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

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 $(a_\mathfrak{p})_{\mathfrak{p}\in\mathcal{P}}$ et 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.

Remarque

Si α' est le plus petit élément non nul de I pour q, alors nous avons $q(\alpha) \leq 2^{n-1} q(\alpha')$. Plus n est grand, plus $q(\alpha)$ peut être loin de $q(\alpha')$.

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 $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}$.
7. Calcul des relations dû 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 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 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 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 dû aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas ou 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 dû aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas ou 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 dû aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas ou 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 dû aux éléments de petites normes. Amélioration de l'implantation de l'algorithme de Fincke-Pohst pour éviter les cas ou 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 un relation.

Principe (2)

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

On choisit un ensemble fini S de petit idéaux premier. Pour chaque $\mathfrak{p}$ qui appartient à aucune relations, 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	Degré	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
$\mathbb{Q}(\zeta_{156})$	48	36.4	156	3.81112901 E17	5min
$\mathbb{Q}(\zeta_{109})^+$	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

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

Lignes directrices

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

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

Théorème (sous GRH+PARI)

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

Améliorations possibles

1. Implantation de la variante "single large prime".
2. Parallélisation du calcul des relations
3. Amélioration de l'implantation de l'algorithme de calcul de la HNF.