SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

RENÉ SMADJA

Calcul de groupes de classes

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. n° 3, p. 1-9

<http://www.numdam.org/item?id=STNG_1973-1974__3__A3_0>

21 mars 1974
Grenoble

CALCUL DE GROUPES DE CLASSES

par René SMADJA

1. POSITION DU PROBLEME.

Soit $K = \mathbb{Q}(\theta_o)$ un corps de nombres algébriques, donné par le polynôme minimal $F_o(X) = X^n + \ldots$ de l'élément primitif entier θ_o. On veut déterminer une base d'entiers, le discriminant, le groupe des classes d'idéaux de K.

Pour simplifier l'exposé, les résultats seront énoncés pour les corps cubiques uniquement. L'étude du cas général s'en déduit aisément, la seule différence est que l'on obtient en plus pour les corps cubiques une base fondamentale d'unités.

2. BASE D'ENTIERS - BASES D'IDEAUX.

On peut déterminer, au moyen d'un nombre fini d'opérations, un élément primitif $\theta = \frac{\theta_o + A_o}{B_o}$ de polynôme fondamental $F(X) = X^3 - sX^2 + tX + u$ et des entiers naturels A, B, C tels que $(\frac{\theta^2 + A\theta + C}{B}, \theta, 1)$ soit une base d'entiers de K. Si D est le discriminant de F, le discriminant de K est alors $\Delta = D/B^2$.

Un idéal $\mathfrak{J}$ est dit primitif si $\mathfrak{J} \subset \mathbb{Z}[\theta]$ et $\forall \ell \geq 2$, $\frac{1}{\ell}\mathfrak{J} \not\subset \mathbb{Z}[\theta]$. Tout idéal s'écrit $\mathfrak{a} = \frac{r}{s}\mathfrak{J}$ où $\mathfrak{J}$ est un idéal primitif, r et s des entiers

naturels. Tout idéal primitif a une $\mathbb{Z}$-base de la forme $(\theta^2+a\theta+b, m(\theta-c), mn)$ $a,b,c,m,n \in \mathbb{N}$; cette base est déterminée de façon unique par les conditions $0 \leq c < n$, $0 \leq a < m$, $0 \leq b < mn$. En particulier, un idéal premier du premier degré a une $\mathbb{Z}$-base de la forme suivante :

si $B = 1$, $\mathfrak{p} = (\theta^2+b, \theta-c, p)$ avec $F(c) \equiv 0 \pmod p$

$$b \equiv -c^2 \pmod p$$

si $B \neq 1$, $\mathfrak{p} = \frac{1}{B}(\theta^2+A\theta+b, B(\theta-c), Bp)$ avec $F(c) \equiv 0 \pmod p$

$$b \equiv -c(A+c) \pmod p$$

$$b(s+A-c)+c(A^2+As+t)+u \equiv 0 \pmod{Bp}$$

$$b(b+s^2+2As+A^2-t)+su+2Au+cF(A+s) \equiv 0 \pmod{B^2p} .$$

3. IDEAUX REDUITS.

On plonge le corps K et ses conjugués K' et K'' dans $\mathbb{R}$ ou $\mathbb{C}$.

(1) DEFINITION. Un idéal primitif $\mathfrak{J} = (\theta^2+a\theta+b, m(\theta-c), mn)$ est réduit si

$$\forall \xi \in \mathfrak{J}-\{0\} \ , \ \sup(|\xi|, |\xi'|, |\xi''|) \geq mn .$$

Il n'y a qu'un nombre fini d'idéaux réduits.

(2) IDEAL REDUIT EQUIVALENT A UN IDEAL PRIMITIF. Soit $\mathfrak{J} = (\theta^2+a\theta+b, m(\theta-c), mn)$ un idéal primitif.

Il est possible de déterminer, au moyen d'un nombre fini d'opérations, si $\mathfrak{J}$ est réduit et, s'il ne l'est pas, de lui trouver un idéal réduit équivalent.

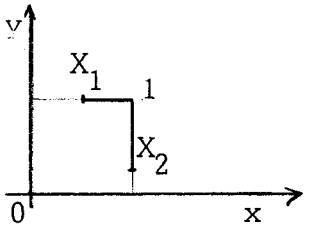
Il suffit de chercher les éléments ξ de $\mathfrak{J}$ tels que $|\xi| < mn$, $|\xi'| < mn$, $|\xi''| < mn$. Il n'y en a qu'un nombre fini. S'il n'y en a pas, $\mathfrak{J}$ est réduit. Sinon, soit α un tel élément pour lequel $\|\alpha\| = \sup(|\alpha|, |\alpha'|, |\alpha''|)$ est minimum ; considérons l'idéal $\alpha'\alpha''\mathfrak{J}$ et associons-lui un idéal primitif $\mathfrak{J}_{\text{Réd}} = \frac{\alpha'\alpha''}{t}\mathfrak{J}$ en le divisant par le p.g.c.d. des coordonnées de ses éléments sur $(\theta^2, \theta, 1)$, qui est un entier naturel t . $\mathfrak{J}_{\text{Réd}}$ est un idéal réduit équivalent à $\mathfrak{J}$.

(3) IDEAUX REDUITS EQUIVALENTS A UN IDEAL REDUIT.

a. Cubiques imaginaires (abréviation signifiant qu'un conjugué de K n'est pas réel). A tout point $X = (x,y)$ de la frontière $\mathcal{F}$ du carré unité de $\mathbb{R}_+^2$, on associe une norme sur $\mathbb{R}\times\mathbb{C}$ donc sur $K\times K'$: $\|\xi\|_X = \sup(x|\xi|, y|\xi'|)$.

DOMAINE DE REDUCTION de l'idéal réduit $\mathcal{J} = \{X\in\mathcal{F} \mid \forall \xi \in \mathcal{J}-\{0\}, \|\xi\|_X \geq mn\}$

$$\|\xi\|_X \leq mn \Leftrightarrow \begin{cases} x|\xi| \leq mn \\ \\ y|\xi'| \leq mn \end{cases} \Leftrightarrow \begin{cases} x \leq \dfrac{mn}{|\xi|} \\ \\ y \leq \dfrac{mn}{|\xi'|} \end{cases} \Leftrightarrow \begin{cases} x \leq \inf(\dfrac{mn}{|\xi|}, 1) \\ \\ y \leq \inf(\dfrac{mn}{|\xi'|}, 1) \end{cases}$$



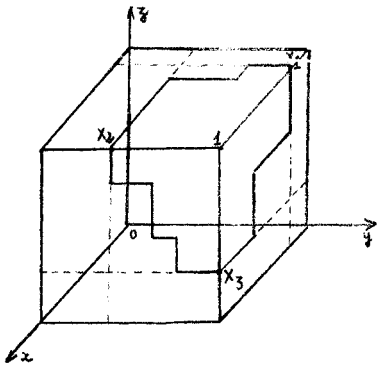
A tout élément ξ de $\mathcal{J}$ dont un des conjugués est inférieur à mn , on associe un point P_ξ de $\mathcal{F}$ dont les coordonnées sont $(\inf(\frac{mn}{|\xi|},1), \inf(\frac{mn}{|\xi'|},1))$. Les extrémités du domaine de réduction sont, parmi ces points, ceux qui correspondent à des extremums.

En particulier $X_1 = P_\alpha$ avec $|\alpha'| < mn < |\alpha| = \dfrac{mn}{x_1}$, x_1 maximum, c'est-à-dire $|\alpha|$ minimum. On cherche donc un élément $\omega = i(\theta^2+a\theta+b) + jm(\theta-c) + kmn$ de $\mathcal{J}$ tel que $|\omega'| < mn$, en faisant croître i dans $\mathbb{N}$, j et k étant bornés par les conditions $|\mathrm{Re}\,\omega'| < mn$ et $|\mathrm{Im}\,\omega'| < mn$; ensuite, on énumère tous les éléments ξ de $\mathcal{J}$ tels que $|\xi| \leq |\omega|$, $|\xi'| < mn$ et on note α celui pour lequel $|\xi|$ est minimum.

L'idéal réduit $\mathcal{J}' = \dfrac{\alpha'\alpha''}{t}\mathcal{J}$ est appelé suivant de $\mathcal{J}$. On effectue pour lui la même opération que pour $\mathcal{J}$ et ainsi de suite. On démontre que l'on obtient ainsi tous les idéaux réduits équivalents à $\mathcal{J}$, ordonnés suivant un cycle.

b. <u>Cubiques réels</u>. A tout point $X = (x,y,z)$ de la frontière $\mathcal{F}$ du cube unité de $\mathbb{R}_+^3$, on associe une norme sur $\mathbb{R}^3$ donc sur $K\times K'\times K''$: $\|\xi\|_X = \sup(x|\xi|, y|\xi'|, z|\xi''|)$. Le domaine de réduction et les points P_ξ sont définis comme précédemment. Le domaine de réduction est un polygone

tracé sur $\mathcal{F}$, dont les côtés sont parallèles aux axes et dont les sommets sont ceux des points P_ξ qui correspondent à des extremums.



On cherche tout d'abord ω_1 , ω_2 , $\omega_3 \in \mathcal{J}$ tels que

$$\begin{cases} |\omega_1'| < mn & |\omega_1''| < mn \\ |\omega_2| < mn & |\omega_2''| < mn \\ |\omega_3| < mn & |\omega_3'| < mn \end{cases} .$$

On énumère alors tous les éléments ξ de $\mathcal{J}$ tels que $|\xi| \leq |\omega_1|$, $|\xi'| \leq |\omega_2|$, $|\xi''| \leq |\omega_3|$ et dont un des conjugués au moins est inférieur à mn ; on en déduit tous les sommets du domaine de réduction.

Chaque sommet fournit un idéal réduit équivalent à $\mathcal{J}$; pour chacun d'eux, on recherche de même les idéaux réduits voisins et on obtient ainsi, par itération de ce procédé, tous les idéaux réduits de la classe de $\mathcal{J}$.

4. CALCUL DU GROUPE DES CLASSES.

L'idéal $[B] = (\theta^2 + A\theta + C \ , \ B\theta \ , \ B)$ est réduit. La méthode précédente permet alors d'obtenir tous les idéaux réduits principaux.

Toute classe contient un produit d'idéaux premiers du premier degré de norme inférieure à $C = \sqrt{\frac{\Delta}{49}}$ si le corps cubique K est réel, $C = \sqrt{\frac{\Delta}{-23}}$ s'il est imaginaire.

Pour chaque nombre premier p inférieur à C , on cherche des idéaux de norme p (au plus deux pour chaque p car la classe du troisième est engendrée par celle des deux premiers). A chaque fois que l'on trouve un tel idéal $\mathfrak{p}$ (ou plutôt l'idéal primitif associé $\mathfrak{P}$), on calcule $\mathfrak{P}_{Réd}$. Si $\mathfrak{P}_{Réd}$ est principal, on cherche l'idéal suivant (correspondant au même nombre premier p ou au nombre premier suivant). Si $\mathfrak{P}_{Réd}$ n'est pas principal, on le multiplie par chacun des idéaux représentant les classes non

principales trouvées jusque là, on réduit et on cherche si l'un des produits est principal ; si aucun ne l'est, $\mathfrak{p}$ représente une classe non encore obtenue. On calcule $\mathfrak{p}^2$ et on itère ces opérations. On aboutit ainsi au groupe de classes, donné par une suite de composition à quotients cycliques.

Si l'on connaît h a-priori, il suffit de s'arrêter lorsque l'on a obtenu h classes au lieu d'examiner tous les idéaux de norme p inférieure à C .

5. UNITES FONDAMENTALES DES CORPS CUBIQUES.

Pour les corps cubiques imaginaires, les idéaux d'une classe se répartissent en un cycle : on obtient l'unité fondamentale en faisant le produit des facteurs $\frac{\alpha'\alpha''}{t}$ d'un cycle, par exemple le cycle principal.

Pour les corps cubiques réels, on applique le résultat suivant :

Soient ε , η , ζ les unités de norme 1 de K déterminées par les conditions

$$|\varepsilon| > 1 \quad |\varepsilon'| < 1 \quad |\varepsilon''| < 1 \quad |\varepsilon| \text{ minimum}$$

$$|\eta| < 1 \quad |\eta'| > 1 \quad |\eta''| < 1 \quad |\eta'| \text{ minimum}$$

$$|\zeta| < 1 \quad |\zeta'| < 1 \quad |\zeta''| > 1 \quad |\zeta''| \text{ minimum .}$$

Alors, deux quelconques des trois éléments ε, η, ζ forment une base fondamentale d'unités de K . Si K est abélien, ces unités sont conjuguées (unités de Minkowski).

6. EXEMPLES NUMERIQUES.

Soit $\xi = i(\theta^2 + a\theta + b) + jm(\theta - c) + kmn$, $i \geq 0$.

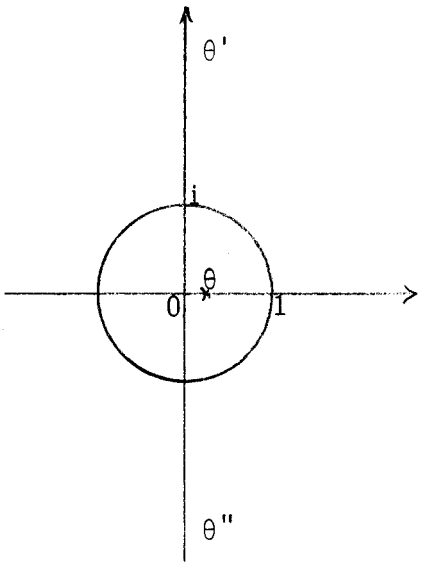
Les inégalités $\begin{cases} |\xi| < R_1 \\ |\xi'| < R_2 \\ |\xi''| < R_3 \end{cases}$ impliquent $\begin{cases} i < \dfrac{R_1|\theta'-\theta''| + R_2|\theta''-\theta| + R_3|\theta-\theta'|}{\sqrt{|D|}} \\ |j| < \dfrac{R_1|\theta'^2-\theta''^2| + R_2|\theta''^2-\theta^2| + R_3|\theta^2-\theta'^2|}{\sqrt{|D|}} + \dfrac{a}{m} i \end{cases}$

i et j étant fixés, il est facile de borner k .

(1) Corps cubique de discriminant -283 . Ce corps est le premier cubique imaginaire non principal.

$F(X) = X^3 + 4X - 1$ Discriminant de F : $D = -283$.

D n'a pas de facteur carré donc $(\theta^2, \theta, 1)$ est base d'entiers et le discriminant de K est $\Delta = -283$.



$\theta = 0,246$ $\qquad \left.\begin{matrix}\theta' \\ \theta''\end{matrix}\right\} = -0,123 \pm 2,011\, i$

$\dfrac{|\theta'-\theta''|}{\sqrt{|D|}} = 0,239$ $\qquad \dfrac{2|\theta-\theta'|}{\sqrt{|D|}} = 0,243$

$\dfrac{|\theta'^2-\theta''^2|}{\sqrt{|D|}} = 0,059$ $\qquad \dfrac{2|\theta^2-\theta'^2|}{\sqrt{|D|}} = 0,490$.

a. Détermination du cycle principal.

On cherche $\omega \in (\theta^2, \theta, 1)$ tel que $|\omega| < 1 < |\omega'|$: $\omega = \theta$ convient.

On cherche alors $\theta = i\theta^2 + j\theta + k$ tel que $|\xi| < 1$, $|\xi'| < |\theta'| = 2,\ldots$ $|\xi'|$ minimum. $0 \le i < 0,239+2,\ldots \times 0,243 < 1 \Rightarrow i = 0$. Il suffit donc de prendre j positif ou nul. $0 \le j < 0,059+2,\ldots \times 0,490 \Rightarrow$ $j = 0$ ou 1 . 0 est exclu car $k < 1 < k' = k$ ne convient pas. Donc $\xi = \theta - k$. Il est clair (voir figure) que $|\xi'|$ est minimum pour $k = 0$: l'extrémité X_2 du domaine de réduction correspond à θ .

Effectuons les calculs comme le fait l'ordinateur, sans remarquer que θ est une unité, en utilisant les formules $\theta^3 = -4\theta + 1$, $\theta^4 = -4\theta^2 + \theta$, $\theta'\theta'' = \dfrac{\theta^3+4\theta}{\theta} = \theta^2+4$. $(\theta^2+4)(\theta^2, \theta, 1) = (\theta^4+4\theta^2, \theta^3+4\theta, \theta^2+4) = (\theta, 1, \theta^2+4) = (\theta^2, \theta, 1)$. Le cycle principal se réduit à l'idéal unité. Les unités fondamentales sont $\begin{cases} \epsilon = \theta \\ \epsilon^{-1} = \theta^2 + 4 \end{cases}$.

b. Calcul du groupe des classes.

$c = \sqrt{\dfrac{283}{23}} = \sqrt{12,\ldots} = 3,\ldots$: il faut étudier les classes des idéaux de norme 2 et 3 .

$\mathfrak{p}_p = (\theta^2-c^2, \theta-c, p)$, $F(c) \equiv 0 \pmod p$, $p = 2 \Rightarrow c = 1$; $p = 3 \Rightarrow c = 2$.
$\mathfrak{p}_2 = (\theta^2+1, \theta-1, 2)$.

Idéal réduit équivalent à $\mathfrak{p}_2$. $0 \le i < 2.(0,239+0,243) = 0,964 \Rightarrow i = 0$; $0 \le j < 2.(0,059+0,490) = 1,098 \Rightarrow j = 0$ ou 1 . $\xi = \theta - 1 + k$ est, pour tout k , tel que $|\xi'| > 2$ (voir figure). Donc $\mathfrak{p}_2$ est réduit. $\mathfrak{p}_2$ représente ainsi une classe non principale.

Calcul de $\mathfrak{p}_2^2$ et $(\mathfrak{p}_2^2)_{\text{Réd}}$.

$$\begin{aligned}(\theta^2+1, \theta-1, 2)(\theta^2+1, \theta-1, 2) &= (\theta^4+2\theta^2+1, \theta^3-\theta^2+\theta-1, 2\theta^2+2, \theta^2-2\theta+1, 2\theta-2, 4)\\ &= (-2\theta^2+\theta+1, -\theta^2-3\theta, 2\theta^2+2, \theta^2-2\theta+1, 2\theta-2, 4)\\ &= (\theta^2+3\theta, 7\theta+1, -6\theta+2, -5\theta+1, 2\theta-2, 4)\\ &= (\theta^2+3\theta, \theta+3, -20, 20, 16, 4, 4)\\ &= (\theta^2+3\theta, \theta+3, 4)\\ &= (\theta^2+3, \theta-1, 4) \quad .\end{aligned}$$

En énumérant les éléments $\xi = i(\theta^2+3)+j(\theta-1)+4k$ tels que $|\xi| < 4$ et $|\xi'| < 4$, on trouve que celui qui est de norme minimum est $\alpha = \theta-1$.

Le polynôme minimal de α est $(\alpha+1)^3+4(\alpha+1)-1 = \alpha^3+3\alpha^2+7\alpha+4$, donc $\alpha'\alpha'' = \dfrac{-4}{\alpha} = \alpha^2+3\alpha+7 = (\theta-1)^2 + 3(\theta-1) + 7 = \theta^2+\theta+5$.

$$\begin{aligned}(\theta^2+\theta+5)(\theta^2+3, \theta-1, 4) &= (\theta^4+\theta^3+8\theta^2+3\theta+15, \theta^3+4\theta-5, 4\theta^2+4\theta+20)\\ &= (4\theta^2+16, -4, 4(\theta^2+\theta+5))\\ &= 4(\theta^2+4, \theta+1, 1)\\ &= 4(\theta^2, \theta, 1) \quad .\end{aligned}$$

Donc $(\mathfrak{p}_2^2)_{\text{Réd}} = [4]$ est principal : la classe de $\mathfrak{p}_2$ est d'ordre 2 .
$\mathfrak{p}_3 = (\theta^2+2, \theta-2, 3)$.

Idéal réduit équivalent à $\mathfrak{p}_3$. L'élément de norme minimum est $\beta = \theta+1$, dont le polynôme minimal est $(\beta-1)^3+4(\beta-1)-1 = \beta^3-3\beta^2+7\beta-6$. Donc $\beta'\beta'' = \dfrac{6}{\beta} = \beta^2 - 3\beta + 7 = (\theta+1)^2 - 3(\theta+1) + 7 = \theta^2-\theta+5$.

$$(\theta^2-\theta+5)(\theta^2+2,\theta-2,3) = (\theta^4-\theta^3+7\theta^2-2\theta+10,\theta^3-3\theta^2+7\theta-10,3(\theta^2-\theta+5))$$
$$= (3\theta^2+3\theta+9,-3\theta^2+3\theta-9,3(\theta^2-\theta+5))$$
$$= 3(\theta^2+\theta+3,\theta^2-\theta+3,\theta^2-\theta+5)$$
$$= 3(\theta^2+\theta+3,2\theta,-2\theta+2)$$
$$= 3(\theta^2+\theta+3,2\theta,2) \quad .$$

$(\mathfrak{p}_3)_{\text{Réd}} = (\theta^2+\theta+1,2\theta,2)$. $\mathfrak{p}_3$ n'est pas principal.

Comparaison de la classe de $\mathfrak{p}_3$ avec les classes non principales précédemment trouvées.

$$\mathfrak{p}_2.(\mathfrak{p}_3)_{\text{Réd}} = (\theta^2+1,\theta-1,2)(\theta^2+\theta+1,2\theta,2)$$
$$= (\theta^4+\theta^3+2\theta^2+\theta+1,\theta^3-1,2\theta^2+2\theta+2,2\theta^3+2\theta,2\theta^2-2\theta,4\theta,2\theta^2+2,2\theta-2,4)$$
$$= (-2\theta^2-2\theta+2,-4\theta,2\theta^2+2\theta+2,-6\theta+2,2\theta^2-2\theta,4\theta,2\theta^2+2,2\theta-2,4)$$
$$= 2(\theta^2+1,\theta-1,1)$$
$$= 2(\theta^2,\theta,1) \quad .$$

Donc $\mathfrak{p}_3$ est dans la classe inverse de celle de $\mathfrak{p}_2$.

Conclusion.

Le groupe des classes est d'ordre 2, engendré par $\mathfrak{p}_2 = (\theta^2+1,\theta-1,2)$.

(2) Un corps cubique abélien.

Considérons le polynôme $F(X) = X^3-X^2-1374X+18019$. Le discriminant de F est $D = (7.11.19.31)^2$; $F(X+s) = X^3+2X^2-1373X+16645$.

Les congruences $\begin{cases} F(A+s) \equiv 0 \pmod{p^2} \\ F'(A+s) \equiv 0 \pmod{p} \end{cases}$ ont une solution commune $(A = 2)$ pour $p = 11$, mais pas pour $p = 7,19$ ou 31. Donc le dénominateur du terme de degré 2 de la base d'entiers est $B = 11$, les coefficients A et C valent respectivement 2 et $A^2+As+t \equiv 7 \pmod{11}$:

$(\frac{\theta^2+2\theta+7}{11},\theta,1)$ est une base d'entiers ; le discriminant de K est

$\Delta = (7.19.31)^2 = (4123)^2$.

On affecte tout d'abord le numéro 1 à l'idéal primitif associé à l'idéal unité $(\theta^2+2\theta+7, 11\theta, 11)$. La recherche de son domaine de réduction fournit 15 sommets donc 15 idéaux réduits voisins, que l'on désigne par des numéros (les idéaux $3n$ et $3n+1$ étant les conjugués de $3n-1$) ; on obtient ainsi dans l'ordre (à partir de X_1 vers X_2, X_3, X_1 , les positions correspondant à X_1, X_2, X_3 étant soulignées) les idéaux
$\underline{1}\ 1\ 3\ 6\ 2\ \underline{1}\ 1\ 4\ 7\ 3\ \underline{1}\ 1\ 2\ 5\ 4$. Il faut alors étudier les idéaux 2 à 7 mais, puisqu'ils sont conjugués trois à trois, il suffit d'en étudier deux :

l'idéal 4 : $(\theta^2+651\theta+953, 1375\theta, 1375)$ a pour idéaux voisins $\underline{1}\,\underline{1}\,5\,\underline{2}\,3\,7$
l'idéal 7 : $(\theta^2+640\theta+3032, 6149\theta, 6149)$ a pour idéaux voisins $\underline{1}\,\underline{4}\,\underline{3}$.

On n'obtient pas de nouvel idéal donc la classe principale contient 7 idéaux réduits.

On trouve que $\mathfrak{p}_5$, $\mathfrak{p}_5'$, $\mathfrak{p}_7$ représentent des classes non principales, indépendantes, d'ordre 3 . Si l'on sait (tables de M.N. Gras) que le nombre de classes est 27, il est inutile d'étudier tous les idéaux premiers de norme inférieure à $\frac{4123}{7} = 589$ pour conclure que le groupe des classes est engendré par $\mathfrak{p}_5$, $\mathfrak{p}_5'$, $\mathfrak{p}_7$ et isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

BIBLIOGRAPHIE

R. SMADJA - Sur le groupe des classes des corps de nombres. C.R.A.S. A 276 (1973) pp. 1639-1641.

-o-o-