Structure galoisienne des S-unités

Isabelle Dubois

Partons de l'équation diophantienne suivante, appelée équation de Pell :

$$a^2 - b^2 d = \pm 1 \qquad (*)$$

où $a, b \in \mathbb{Z}$, et d est un entier ≥ 2 sans facteurs carrés congru à 2 ou 3 modulo 4.

Pour comprendre la structure des solutions de $(*)$, il est naturel d'introduire le corps de nombres quadratique $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d}, x, y \in \mathbb{Q}\}$. C'est un sous-corps de $\mathbb{R}$ et une extension algébrique galoisienne de $\mathbb{Q}$ de degré 2. Son groupe de Galois est composé de deux éléments, l'identité et σ, l'automorphisme de $\mathbb{Q}(\sqrt{d})$ défini par $\sigma(x + y\sqrt{d}) = x - y\sqrt{d}$. C'est ainsi que l'ensemble des solutions de $(*)$ est exactement l'ensemble $E_{\mathbb{Q}(\sqrt{d})} = \{\varepsilon \in \mathbb{Z}[\sqrt{d}], \varepsilon \times \sigma(\varepsilon) = \pm 1\}$, avec $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d}, x, y \in \mathbb{Z}\}$ qui est un sous-anneau de $\mathbb{Q}(\sqrt{d})$ (appelé anneau d'entiers). Le groupe multiplicatif de l'anneau $\mathbb{Z}[\sqrt{d}]$ n'est rien d'autre que $E_{\mathbb{Q}(\sqrt{d})}$, et est appelé groupe des unités. La structure de ce groupe est connue : il est isomorphe à $\{\pm 1\} \times \mathbb{Z}$ (voir [6], chap. 4.6, p 76). Ainsi, on obtient l'existence d'une unique unité $\varepsilon_1 = a_1 + b_1\sqrt{d} > 1$ telle que toute solution $(a,\ b)$ de $(*)$ vérifie $a + b\sqrt{d} = \pm\varepsilon_1^n, n \in \mathbb{Z}$. Par exemple, si $d = 94$ alors $\varepsilon_1 = 2143295 + 2221064\sqrt{94}$.

Nous allons maintenant considérer un problème plus général consistant en l'étude de la structure du groupe des S-unités dans une extension galoisienne quelconque de corps de nombres. On consultera [6] et [4] pour la définition des objets qui suivent.

Soit K/k une extension finie de corps de nombres, galoisienne de groupe $G = Gal(K/k)$. Pour S un ensemble de places (i.e. un ensemble de classes d'équivalence de valeurs absolues) de K contenant l'ensemble S_∞ des places infinies (archimédiennes) de K, et stable par l'action naturelle de G sur les places de K, nous pouvons considérer E_S le groupe des S-unités de K, défini par :

$$E_S = \{x \in K^*, \forall \mathfrak{P} \notin S, v_{\mathfrak{P}}(x) = 0\}$$

($v_{\mathcal{B}}(x)$ est la valuation associée à une place $\mathfrak{P}$).

La structure de E_S en tant que groupe abélien est bien connue par le théorème de Dirichlet (voir [4], chap. V.1, p 104) : $E_S \simeq \mu_K \times \mathbb{Z}^{\#S-1}$. Ici, μ_K désigne le groupe des racines de l'unité appartenant à K.

Mais, par choix de S, E_S est aussi un module galoisien, c'est-à-dire un module sur l'anneau de groupe $\mathbb{Z}[G]$; l'action d'un élément $\sum_{g\in G} a_g g \in \mathbb{Z}[G]$ sur une

S-unité x est donnée par :

$$\left(\sum_{g\in G} a_g g\right)\cdot x = \prod_{g\in G} g(x)^{a_g}$$

On cherche alors à déterminer la structure du module E_S et à relier celle-ci avec l'arithmétique de l'extension.

En général, nous ne disposons que de peu de résultats explicites, et on s'intéresse soit au groupe des unités (i.e. le groupe E_{S_∞}), soit au groupe des S-unités pour un ensemble S "assez grand". En ce qui concerne les unités, citons par exemple l'article [3] de A. Frohlich dans lequel est étudiée la structure galoisienne locale et globale du groupe des unités de certaines classes d'extensions abéliennes de corps de nombres. D'autre part, lorsque S est "assez grand", structure des S-unités et valeurs de fonctions L sont étroitement liées via la conjecture de Chinburg (voir par exemple l'article de J. Ritter et A. Weiss [5]).

Nous allons présenter ici les résultats que nous avons obtenus pour tout ensemble S dans le cas d'un corps de nombres cyclique de degré premier (on consultera [2] pour les démonstrations).

Pour toute la suite, nous utiliserons les notations suivantes : soit $k=\mathbb{Q}$, et K un corps de nombres cyclique de degré $[K:\mathbb{Q}]=l$ un nombre premier impair. Ainsi, G est isomorphe à $\mathbb{Z}/l\mathbb{Z}$, et on en choisit un générateur σ.

1 Une première décomposition

Nous allons tout d'abord nous débarrasser du sous-module de torsion de E_S, qui est égal à $\{\pm 1\}$.

Posons $U_S=\{x\in E_S, N_{K/\mathbb{Q}}(x)>0\}$. Nous avons alors la décomposition de E_S en sous-$\mathbb{Z}[G]$-modules stables :

$$E_S=\{\pm 1\}\oplus U_S.$$

Dans ce qui suit, nous allons donc étudier le module U_S qui est un $\mathbb{Z}$-module libre de dimension $\#S-1$.

2 Un théorème de structure

Nous allons introduire un résultat classifiant les $\mathbb{Z}[G]$-modules lorsque G est cyclique d'ordre premier, et qui nous permettra de décrire la structure galoisienne de U_S. Il existe trois types de $\mathbb{Z}[G]$-modules $\mathbb{Z}$-libres indécomposables de type fini. Ce sont :

- *Type I :* $\mathbb{Z}$ avec action triviale de G.

- *Type II :* tout idéal fractionnaire $\mathfrak{A}$ du l-ième anneau cyclotomique $\mathbb{Z}[l]$; pour $a \in \mathfrak{A}$, l'action de G est donnée par : $\sigma \cdot a = \zeta a$, où ζ est une racine primitive l-ième de 1.
- *Type III :* tout module de type $(\mathfrak{A}, a_0)$ qui est somme d'un idéal $\mathfrak{A}$. (type II) et de $\mathbb{Z}$ (type I), et où a_0 est un élément de $\mathfrak{A}$; l'action de G sur un élément $(a, k) \in (\mathfrak{A}, a_0)(a \in \mathfrak{A}$, et $k \in \mathbb{Z})$ est donnée par : $\sigma \cdot (a, k) = (\zeta a + k a_0, k)$.

En particulier, $\mathbb{Z}[G]$ est de type III, car $\mathbb{Z}[G] = (\mathbb{Z}[l], 1)$.

Nous avons alors le théorème (voir [1], Chap. XI, § 74)

Théorème 1. *(Diederischen-Reiner)*

Soit M un $\mathbb{Z}[G]$-module de type fini et sans $\mathbb{Z}$-torsion. Alors, il existe r_1, r_2, r_3 des éléments de $\mathbb{N}$, $\mathfrak{A}$ un idéal de $\mathbb{Z}[l]$, a_0 un élément de $\mathfrak{A} \backslash (\zeta - 1)\mathfrak{A}$, tels que

$$M \simeq \mathbb{Z}[G]^{r_3} \oplus \mathbb{Z}[l]^{r_2 - 1} \oplus \mathfrak{A} \oplus \mathbb{Z}^{r_1}$$

ou bien, si $r_2 = 0$,

$$M \simeq \mathbb{Z}[G]^{r_3 - 1} \oplus (\mathfrak{A}, a_0) \oplus \mathbb{Z}^{r_1}.$$

De plus, la classe d'isomorphisme de M est déterminée par les entiers r_1, r_2, r_3, et la classe (M) de l'idéal $\mathfrak{A}$ dans $Cl(\mathbb{Z}[l])$, le groupe de classes de $\mathbb{Z}[l]$.

3 Structure de U_S

Nous allons déterminer la structure de U_S selon le théorème 1. Ainsi, il nous faut trouver les 3 invariants entiers et l'invariant classe de ce module.

3.1 Invariants entiers

Les invariants entiers vont dépendre des conditions arithmétiques suivantes :
i) la nature des places finies de S.

Posons rd le nombre de places finies de $\mathbb{Q}$ qui sont totalement décomposées dans S, et r_{nd} les places finies de $\mathbb{Q}$ non décomposées dans S.
ii) la dimension de certains sous-espaces vectoriels de Cl_K, le groupe de classes de K.

Soit t le nombre de places ramifiées dans K, et $Cl_K(Ram)$ le groupe de classes engendré par les classes d'idéaux premiers ramifiés. Alors $Cl_K(Ram)$ est un $\mathbb{Z}/l\mathbb{Z}$-espace vectoriel de dimension $t - 1$. On considère ensuite deux sous-espaces de $Cl_K(Ram)$ engendrés par les classes de certains idéaux à support dans S, de dimension s et *s'*. Finalement, on pose $\delta = s - s'$, qui est un entier tel que $0 \leq \delta \leq t - 1$.

iii) les relations vérifiées par les places ramifiées de S. Posons $\epsilon = 1 (resp. \epsilon = 0)$ lorsque les idéaux premiers ramifiés à support dans S vérifient une relation (resp. ne vérifient pas de relation) de dépendance non triviale dans Cl_K.

Nous obtenons alors la valeur des invariants entiers en fonction des entiers $r_d, r_{nd}, \delta,$ et ϵ :

Théorème 2. *Les invariants entiers r_{i,U_S} déterminant la structure de U_S sont égaux à :*

$$\begin{cases} r_{1,U_S} = r_{nd} + \delta - \epsilon \\ r_{2,U_S} = \delta + 1 - \epsilon \\ r_{3,U_S} = r_d - \delta + \epsilon \end{cases}$$

3.2 Invariant classe

L'invariant classe (U_S) (qui un élément de $Cl(\mathbb{Z}[l])$) dépend de la structure galoisienne du S-groupe de classes de K. Ce dernier, noté $Cl_{K,S}$, est défini comme étant le quotient du groupe de classes de Kpar le sous-groupe engendré par les classes d'idéaux à support dans S. C'est un $\mathbb{Z}[G]$-module fini, dont la structure détermine une classe $(Cl_{K,S})$ dans $Cl(\mathbb{Z}[l])$.

Nous avons alors l'égalité suivante :

Théorème 3. *Dans $Cl(\mathbb{Z}[l])$,*

$$(U_S) = (Cl_{K,S}).$$

Bibliographie

[1] C. W. Curtis et I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers (1962).

[2] I. Dubois, *S-unités et S-groupe de classes d'un corps de nombres cyclique de degré premier*, Prépublication **88** (mai 1998), Université Bordeaux I.

[3] A. Frohlich, *Units in real abelian fields*, J. reine angew. Math., **429** (1992), 191-217.

[4] S. Lang, *Algebraic number theory*, Addison-Wesley.

[5] J. Ritter et A. Weiss, *On the local Galois structure of S-units*, in Algebra and Number Theory, eds G. Frey, J. Ritter, de Gruyter, Berlin (1994), 229-245.

[6] P. Samuel, *Théorie algébrique des nombres*, Hermann.

Université Bordeaux I
Laboratoire de Mathématiques Pures
351, Cours de la Libération 33405 Talence FRANCE
dubois@math.u-bordeaux.fr