Journal de Théorie des Nombres
de Bordeaux **18** (2006), 265–283

Sur la paramétrisation des solutions des équations quadratiques

par Denis SIMON

Résumé. L'objectif de cet article est de proposer un lien entre plusieurs aspects classiques de la théorie des formes quadratiques entières. Dans un premier temps, on étudie en détail les propriétés des formes quadratiques binaires qui paramétrisent les solutions des équations quadratiques ternaires. En particulier, on donne un moyen simple de construire une paramétrisation à partir d'une solution particulière, dont les invariants ne dépendent que de l'équation de départ. Cette paramétrisation permet de simplifier l'algorithme de la 2-descente sur les courbes elliptiques.

Dans un deuxième temps, on considère $Q(X,Y)$ une forme quadratique entière primitive de discriminant Δ non carré. Certains auteurs (dans [1] et [2]) dressent un lien entre une solution rationnelle particulière de $Q(X,Y)=1$ dans $\mathbb{Q}^2$ et une solution de $[R]^2=[Q]$ dans le groupe de classes $Cl(\Delta)$. Nous montrons que ce lien est bien plus direct que celui décrit dans [1] et [2]. En effet, lorsque l'équation $Q(X,Y)=1$ admet une solution, il est possible de paramétrer toutes les solutions sous la forme $X=\dfrac{q_1(s,t)}{q_3(s,t)}$ et $Y=\dfrac{q_2(s,t)}{q_3(s,t)}$ où q_1,q_2 et q_3 sont trois formes quadratiques entières avec $\operatorname{Disc} q_3=\Delta$. Nous montrons que la forme quadratique q_3 est exactement (au signe près) la solution R de l'équation $[R]^2=[Q]$ dans $Cl(\Delta)$. Nous comparons alors notre algorithme d'extraction de racine carrée de forme quadratique, avec celui de Gauss.

Abstract. Our goal in this paper is to give a link between different classical aspects of the theory of integral quadratic forms. First, we investigate the properties of the binary quadratic forms involved in the parametrization of the solutions of ternary quadratic equations. In particular, we exhibit a simple rule to obtain a parametrization from a particular solution, such that its invariants only depend on the original equation. Used in the context

Manuscrit reçu le 29 mars 2004.
Mots clefs. Formes quadratiques binaires et ternaires, paramétrisation, groupe de classes.

of elliptic curves, this parametrization simplifies the algorithm of 2-descent.

Secondly, we consider a primitive quadratic form $Q(X,Y)$, with nonsquare discriminant. Some authors (in [1] and [2]) make a link between a particular rational solution of $Q(X,Y) = 1$ over $\mathbb{Q}^2$ and a solution of $[R]^2 = [Q]$ in the class group $Cl(\Delta)$. We explain why this link is much more direct than this. Indeed, when the equation $Q(X,Y) = 1$ has a solution, it is possible to parametrize them all by $X = \dfrac{q_1(s,t)}{q_3(s,t)}$ and $Y = \dfrac{q_2(s,t)}{q_3(s,t)}$ where q_1,q_2 and q_3 are three integral quadratic forms with $\operatorname{Disc} q_3 = \Delta$. We show that the quadratic form q_3 is exactly (up to sign) the solution R of $[R]^2 = [Q]$ in $Cl(\Delta)$. We end by a comparison between our algorithm for extracting square roots of quadratic forms and the algorithm of Gauss.

Bibliographie

[1] W. Bosma, P. Stevenhagen, *On the computation of quadratic 2-class groups*. J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313.

[2] K. Hardy, K. Williams, *The squareroot of an ambiguous form in the principal genus*. Proc. Edinburgh Math. Soc. (2) **36** (1993), no. 1, 145–150.

Denis Simon
LMNO - UMR 6139
Université de Caen – France
Campus II – Boulevard Mal Juin
BP 5186 – 14032 Caen Cedex, France
E-mail : simon@math.unicaen.fr