Journal de Théorie des Nombres
de Bordeaux **14** (2002), 325–343

Weber's class invariants revisited

par Reinhard SCHERTZ

Résumé. Soit K un corps quadratique imaginaire de discriminant d et $\mathfrak{O}_t$ l'ordre à conducteur $t \in \mathbb{N}$ dans K. L'invariant modulaire $j(\mathfrak{O}_t)$ est un nombre algébrique qui génère sur K le corps de classes d'anneau modulo t. Les coefficients du polynôme minimal de $j(\mathfrak{O}_t)$ étant assez large, Weber considère dans [We] les fonctions $f, f_1, f_2, \gamma_2, \gamma_3$ définies plus bas, par lesquelles il construit des générateurs plus simples pour les corps de classes d'anneau.

Plus tard les valeurs singulières de ces fonctions ont joué un rôle central dans la solution de Heegner [He] du célèbre problème de déterminer tous les corps quadratiques imaginaires dont le nombre de classes est égal à 1 [He,Me2,St]. Actuellement on s'en sert en cryptographie pour trouver des courbes elliptiques sur des corps finis avec certaines jolies propriétés.

Le but de cet article est i) d'énoncer certains résultats déjà connus de [We,Bi,Me2,Sch1] cf. Théorèmes 1,2 et 3, concernant les valeurs singulières des fonctions $f, f_1, f_2, \gamma_2, \gamma_3$, et ii) de développer une preuve courte de ces résultats.

Cette méthode s'applique aussi à d'autres fonctions cf. Théorème 4 et le tableau précédent celui-ci. Les preuves des théorèmes 1 à 4 sont données en fin d'article.

Ces démonstrations résultent de la loi de réciprocité de Shimura (cf. théorème 5, ainsi que théorèmes 6 et 7), du calcul de la racine 24-ième de l'unité de $\eta = \sqrt[24]{\Delta}$ lors des transformations unimodulaires (cf. proposition 2, tirée de [Me1] formules (4.21) à (4.23) p.162), et donnent aussi via la proposition 3 des formules explicites pour les conjugués des valeurs singulières, qui sont très utiles pour des calculs numériques.

Certains de ceux-ci sont donnés comme exemples juste avant la Bibliograpie.

Abstract. Let K be a quadratic imaginary number field of discriminant d. For $t \in \mathbb{N}$ let $\mathfrak{O}_t$ denote the order of conductor t in K and $j(\mathfrak{O}_t)$ its modular invariant which is known to generate the ring class field modulo t over K. The coefficients of the minimal equation of $j(\mathfrak{O}_t)$ being quite large Weber considered in [We]

Manuscrit reçu le 20 juillet 2000.

the functions $f, f_1, f_2, \gamma_2, \gamma_3$ defined below and thereby obtained simpler generators of the ring class fields.

Later on the singular values of these functions played a crucial role in Heegner's solution [He] of the class number one problem for quadratic imaginary number fields [He,Me2,St]. Actually these numbers are used in cryptography to find elliptic curves over finite fields with nice properties.

It is the aim of this paper i) to enunciate some known results of [We,Bi,Me2,Sch1] cf. Theorem 1, 2 and 3, concerning singular values of the functions $f, f_1, f_2, \gamma_2, \gamma_3$, and ii) to give a short and easy proof of these results.

That method also applies to other functions, such as those in the table preceding Theorem 4. The proofs of Theorems 1 to 4 are given at the end of our article.

Our proofs rely on the reciprocity law of Shimura (cf. Theorem 5, and also Theorem 6 and 7), and on the knowledge of the 24-th root of unity that acquires $\eta = \sqrt[24]{\Delta}$ by unimodular substitution (cf. Proposition 2, and [Me1] p.162); they also give via Proposition 3 explicit formulas for the conjugates of the singular values (of the above functions), that are quite useful for numerical calculations.

Examples of such calculations are to be found immediately before the References.

Reinhard SCHERTZ
Institut für Mathematik der Universität Augsburg
Universitätsstraße 8
86159 Augsburg, Germany
E-mail : Reinhard.Schertz@Math.Uni-Augsburg.DE