Lenstra Constant and Extreme Forms in Algebraic Number Fields

R. Coulangeon* & M. I. Icaza† & M. ORyan‡

Abstract

In this paper we compute $\gamma_{K,2}$ for $K = \mathbb{Q}(\rho)$ where $\rho^3 - \rho + 1 = 0$. We refine some techniques introduced in [BCIO] to construct all possible sets of minimal vectors for perfect forms. This construction gives rise (see Section 2) to results that can be applied in several other cases.

1 Introduction

Let $K/\mathbb{Q}$ be a number field of degree $m = r + 2s$, let d_K be its discriminant and $\mathcal{O}_K$ be its ring of integers. Let $\{\sigma_1, \dots, \sigma_r\}$ (respectively $\{\sigma_{r+1}, \dots, \sigma_m\}$ with $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$) be its real (respectively complex) embeddings. A tuple $S = (S_1, \dots, S_{r+s})$ where $S_1, \dots, S_r$ are real symmetric n-dimensional positive definite matrices and $S_{r+1} \dots, S_{r+s}$ are n-dimensional positive definite Hermitian matrices is called an n dimensional positive definite Humbert form. We refer to such forms as Humbert forms
With all the notations as before we may define (see [I])

$$\mu(S) = \min_{x \in \mathcal{O}_K^n - \{0\}} \{\prod_{i=1}^{r} S_i[x^{\sigma_i}](\prod_{i=r+s}^{s} S_i[x^{\sigma_i}])^2\},$$

*Partially supported by Proyecto FONDECYT 7020959

†Partially supported by Proyecto FONDECYT 7020959, and Partially supported by Programa Formas Cuadraticas Universidad de Talca, Chile. MSC(2000) 11H50 11H55

‡Partially supported by Proyecto FONDECYT 1040670, and Partially supported by Programa Formas Cuadraticas Universidad de Talca, Chile. MSC(2000) 11H50 11H55

where for $x = (x_1 \ldots, x_n)$, $x^{\sigma_i} = (\sigma_i(x_1), \ldots, \sigma_i(x_n))$ for each embedding σ_i of $K$and $S_i[x_i^\sigma] := (x_i^\sigma)^t S_i(x_i^\sigma)$. We say that a vector $v \in \mathcal{O}_K^n - \{0\}$ is a *Minimal vector of* S if $S[v] = \mu(S)$. For each Humbert form, the set of minimal vectors is finite up to multiplicaction by units. Throughout this paper we denote by $M(S)$ a finite set of representatives of the minimal vectors of S and we call it the set of minimal vectors of S.
We also need to define

$$d(S) = \prod_{i=1}^{r} \det S_i \prod_{i=r+1}^{r+s} (\det S_i)^2.$$

The n-dimensional Hermite-Humbert constant of K is then given by (see [I])

$$\gamma_{K,n} = \sup_S \frac{\mu(S)}{d(S)^{1/n}},$$

where S runs over all n-dimensional positive definite Humbert forms. A form S with $\gamma_{K,n} = \gamma(S) = \frac{\mu(S)}{\det(S)^{1/n}}$ is called an *Extreme Form.*

Two n- dimensional Humbert forms S and T are called *equivalent* if there exists $U \in GL(n, \mathcal{O}_K)$ such that $T = S[U]$, where for $S = (S_1, \ldots, S_{r+s})$, $S[U] = (S_1[\sigma_1(U)], \ldots, S_{r+s}[\sigma_{r+s}(U)])$. Then $\gamma(S)$ is class invariant.
In a previous work by Baeza, Coulangeon, Icaza and O'Ryan (see [BCIO]), the actual values for $\gamma_{K,2}$ were obtained for $K = \mathbb{Q}(\sqrt{5})$, $K = \mathbb{Q}(\sqrt{3})$ and $K = \mathbb{Q}(\sqrt{2})$. Also lately (see Pohst) $\gamma_{K,2}$ has been computed for $K = \mathbb{Q}(\sqrt{13})$.
In all those cases, the main computational tool was provided by the work of Coulangeon (see [Co]) which generalizes a result due to Voronoi. Namely the characterization of *Extreme Forms* for the classical Hermite constant as forms which are Perfect and Eutactic. In his work Coulangeon obtains the same characterization for *Extreme Forms* for Hermite-Humbert constant introducing suitable definitions for Perfection and Eutaxy. Considering this characterization, the procedure for finding perfect forms is based on the construction of their posible sets of minimal vectors (see [BCIO]). Such construction turns out to be not easy and it becomes more complicated as the degree of the field or else the dimension of the forms to be considered increase. As we already mentioned, the same strategy was used to provide all known examples so far.

In Section 1 we show how this construction can be related to the so called Lenstra Constant of a number field K. This constant, associated to any number filed K, denoted by $M(K)$, is defined to be the maximum length m of sequences $\omega_1, \ldots, \omega_m$ in $\mathcal{O}_K$, for which all possible mutual differences $\omega_i - \omega_j$ are units (see [Le]). Following [L-M], a sequence of the form $0 = \omega_1, 1 = \omega_2, \omega_3 \ldots, \omega_n$ with $\omega_n \in K$ with $\omega_i - \omega_j$ units is called *Exceptional Sequence*. In Section 2 we obtain $\gamma_{K,2}$ for the cubic field $K = \mathbb{Q}(\rho)$ where $\rho^3 - \rho + 1 = 0$. Finnally in Section 3 we give a list of other number fields in which the value of Lenstra constant makes them suitable for applying the same techniques to obtain their binary Hermite-Humbert constant. We also provide in this last section some further remarks.