ACTA ARITHMETICA
LXXIV.3 (1996)

Sums of squares of integral linear forms

by

María Inés Icaza (Santiago)

1. Introduction. The purpose of this paper is to estimate the following function associated with a commutative ring A for the case when A is the ring of integers of a number field. For any integer $n \geq 1$ define

$$g_A(n) = \inf\{r \mid \Sigma_1^\infty(A,n) \subseteq \Sigma_1^r(A,n)\}$$

where $\Sigma_1^r(A,n)$ denotes the set of all sums of r squares of n-ary linear forms over A, and $\Sigma_1^\infty(A,n) = \bigcup_{r=1}^\infty \Sigma_1^r(A,n)$. If A is a field this function was studied in [BLOP], where for example it is shown, for any local or global field A, that $g_A(n) = n+3$ for all $n \geq 3$. If the ring A is $\mathbb{Z}$, i.e. the ring of rational integers, the estimate of $g_{\mathbb{Z}}(n)$ through an explicit function of n was unknown. We will find in Section 3 an explicit function $f(n)$ with $g_{\mathbb{Z}}(n) \leq f(n)$ for all n.

Actually, this question was raised by Mordell. He ($[\mathrm{Mo}]_1$) and later himself and Ko (see $[\mathrm{Mo}]_2$, [Ko]) proved that for $n \leq 5$, every positive definite classical integral quadratic form of rank n is a sum of $n+3$ squares of integral linear forms.

Since the positive definite form $g(X_1,\ldots,X_6) = \sum_{i=1}^6 X_i^2 + (\sum_{i=1}^6 X_i)^2 - 2X_1X_2 - 2X_2X_6$ is never a sum of squares of integral linear forms ($[\mathrm{Mo}]_3$), this forces to formulate the problem in terms of the g-function, and not in terms of expressing positive definite integral quadratic forms as sums of integral linear forms.

In Section 4 we extend the method used in Section 3 to the general case and we estimate $g_{O_K}(n)$ for O_K the ring of integers of a totally real number field. The idea behind all this is to estimate explicitly a certain constant appearing in the representation Theorem 1 of [HKK]. If K is not real, using the theory of indefinite forms one easily shows that $g_{O_K}(n) = n+3$ for all n. In Section 2 we will briefly consider the case of a local ring A. The classification theory of local lattices developed by O'Meara and Riehm (see

Supported by Fondecyt 3940002.

1991 *Mathematics Subject Classification*: Primary 11E, 11H; Secondary 11R, 15A.

[O'M]$_2$, [R]) leads in this case easily to the fact that $g_A(n) = n+3, n \geq 3$. These local results will be used in Sections 3 and 4.

All definitions and basic facts about quadratic forms will be taken from O'Meara's book [O'M]$_1$.

The author thanks J. S. Hsia for helpful comments during the preparation of this work and also the referee for the suggestions made, particularly concerning the proof of Proposition 2.

The main fact relating the function $g_A(n)$ to the representation of forms by forms is the following result (see [BLOP] for the case in which the ring A is a field):

PROPOSITION 1. *Let A be an integral domain with $2 \neq 0$. For $a_{ij} = a_{ji} \in A$ let $\phi(X_1, \ldots, X_n) = \sum_{1 \leq i,j \leq n} a_{ij} X_i X_j$ be a quadratic form defined over A. If $L_i(X_1, \ldots, X_n), 1 \leq i \leq r$, are r linear forms over A in $X_1, \ldots, X_n$, then*

$$\phi(X_1, \ldots, X_n) = \sum_{i=1}^{r} L_i(X_1, \ldots, X_n)^2$$

if and only if the form ϕ is represented over A by the form $I_r = Y_1^2 + \ldots + Y_r^2$.

Proof. For $1 \leq j \leq r$, let $L_j = b_{j1}X_1 + \ldots + b_{jn}X_n$ with $b_{ij} \in A$ for $1 \leq i \leq n$. Assume that

$$\phi(X_1, \ldots, X_n) = \sum_{j=1}^{r} [L_j(X_1, \ldots, X_n)]^2.$$

Comparing coefficients we obtain

$$a_{ii} = \sum_{j=1}^{r} b_{ji}^2 \quad \text{for } 1 \leq i \leq n, \tag{1}$$

and since $2 \neq 0$,

$$a_{il} = \sum_{j=1}^{r} b_{ji} b_{jl} \quad \text{for } 1 \leq i \leq n,\ 1 \leq l \leq n. \tag{2}$$

Let $M_\phi = Ae_1 \oplus \ldots \oplus Ae_n$ be the A-lattice associated with ϕ. For the form I_r we also denote by I_r its associated A-lattice. Consider in I_r the vectors $b_i = (b_{1i}, \ldots, b_{ri})$, $1 \leq i \leq n$, and define

$$\sigma : M_\phi \to I_r \quad \text{by} \quad \sigma(e_i) = b_i.$$

Equations (1) and (2) then imply that σ is an isometry. Conversely, any representation $\sigma : M_\phi \to I_r$ defines vectors $b_i = (b_{1i}, \ldots, b_{ri}) \in I_r$ through $\sigma(e_i) = b_i$. By setting $L_j(X_1, \ldots, X_n) = b_{j1}X_1 + \ldots + b_{jn}X_n$, we get $\phi(X_1, \ldots, X_n) = \sum_{j=1}^{r} L_j^2$.

2. The g-function of local rings. Let us fix in this section a local ring A, i.e. the ring of integers of a local field K, which we assume to be of characteristic 0.

THEOREM 1. *For any $n \geq 1$,*

$$g_A(n) \leq n+3.$$

If $A = \mathbb{Z}_p$ is the ring of p-adic integers, then

$$g_{\mathbb{Z}_p}(n) = n+3 \quad \textit{for all } n \geq 1.$$

Proof. If $2 \in A^*$ is a unit, the result follows from Proposition 1 and the fact that the form $I_{n+3} = X_1^2 + \ldots + X_{n+3}^2$ is associated with a maximal unimodular lattice over A (see [Ki]) and hence I_{n+3} represents any integral lattice of rank $\leq n$ by Lemma (1.1) of [HKK], which is valid for any local ring as above. Let us assume that 2 is not a unit in A. Let L be any integral lattice over A of rank n. Then we have to check the representation conditions of Riehm's Third Main Theorem in [R] to prove that L is represented by I_{n+3} over A, i.e. $S(L) \subseteq S(I_{n+3})$ and $g(L) \subseteq g(I_{n+3})$, where S denotes the scale group and g the norm group (see *loc. cit.*). Since L is integral, the conditions are obviously satisfied. This shows $g_A(n) \leq n+3$. In the case when $A = \mathbb{Z}_p$ is the ring of p-adic integers, we have to show that $g_{\mathbb{Z}_p}(n) \geq n+3$ for all $n \geq 1$. This follows from the following general fact.

PROPOSITION 2. *Let A be a domain and $K = \mathrm{Quot}(R)$ be its quotient field. Then*

$$g_K(n) \leq g_A(n) \quad \textit{for all } n.$$

Proof. Let $\phi = a_1X_1^2 + \ldots + a_nX_n^2$ be an n-dimensional quadratic form over K, which is a sum of squares of n-ary linear forms over K. Scaling we may assume that for certain $d \in A$, $d^2\phi$ is a sum of squares of linear forms in A. Hence $d^2\phi$ is a sum of at most $g_A(n)$ squares of integral linear forms in A. Thus ϕ is a sum of the same number of squares of linear forms with coefficients in the field K.

3. The g-function of $\mathbb{Z}$. In this section we will find an explicit function $f(n)$ with $g_{\mathbb{Z}}(n) \leq f(n)$ for all n. The fact that $g_{\mathbb{Z}}(n) = n+3$ for $n \leq 5$ (see $[\mathrm{Mo}]_1$, $[\mathrm{Mo}]_2$, [Ko]) follows easily from the existence of only one class in the genus of I_m for $m \leq 8$ (see [BI]). Although this is not true for $m \geq 9$, one could still hope that $g_{\mathbb{Z}}(n) = n+3$ for all n. But we are far from getting such a bound for $g_{\mathbb{Z}}(n)$.

The proof of the finiteness of $g_{\mathbb{Z}}(n)$ (see [I], [BI]) given here leads to the following estimate of $g_{\mathbb{Z}}(n)$ in terms of the constant $c(I_m)$ of the form $I_m = X_1^2 + \ldots + X_m^2$ appearing in the representation Theorem 1 of [HKK].

PROPOSITION 3. *For all $n \geq 1$,*

$$g_{\mathbb{Z}}(n) \leq 8 + \sum_{i=6}^{n} c(I_{2i+6}).$$

Proof. Let N be a positive definite integral lattice with associated quadratic form Q of rank n. Assume that N is represented by I_r for some r. Let $\mu(N) = \min\{Q(x) \mid x \in N,\ x \neq 0\}$ be the minimum of the lattice N. Let us consider the following two cases:

(i) $\mu(N) \geq c(I_{2n+6})$. Then Section 2 and Theorem 1 in [HKK] imply that N is represented by I_{2n+6}.

(ii) $\mu(N) < c(I_{2n+6})$. In this case we assume that the form $Q = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ is reduced in the sense of Minkowski. Since N is represented by I_r we have

$$Q(X_1, \ldots, X_n) = \sum_{j=1}^{r} [L_j(X_1, \ldots, X_n)]^2,$$

where each $L_j(X_1, \ldots, X_n) = b_{1j}X_1 + \ldots + b_{nj}X_n$ is a linear form with integral coefficients. Comparing coefficients we get

$$a_{11} = \sum_{j=1}^{r} b_{1j}^2.$$

By assumption $a_{11} < c(I_{2n+6})$. Therefore at most $[c(I_{2n+6})]$ of the integral coefficients b_{1j} can be non-zero (here $[x]$ denotes the integral part of x). Hence

$$Q(X_1, \ldots, X_n) = \sum_{j=1}^{[c(I_{2n+6})]} [L_j(X_1, \ldots, X_n)]^2 + \sum_{j=[c(I_{2n+6})]+1}^{r} [L_j(X_2, \ldots, X_n)]^2,$$

where the summation in the second term involves linear forms in $n-1$ variables. Hence

$$g_{\mathbb{Z}}(n) \leq c(I_{2n+6}) + g_{\mathbb{Z}}(n-1).$$

Since $g_{\mathbb{Z}}(5) = 8$ we obtain the desired result.

In order to obtain an explicit bound for $g_{\mathbb{Z}}(n)$ we must estimate $c(I_m)$. For the sake of completeness we mention below some results from [HKK] which will be needed. The following result is (1.2) in [HKK].

LEMMA 1. *Let L be a positive $\mathbb{Z}$-lattice of rank $l \geq 3$. Let q be a prime such that $L_q = L \otimes \mathbb{Z}_q$ is isotropic and assume that the genus of L coincides with its spinor genus. Then there is an integer $s \geq 1$ such that L represents every $\mathbb{Z}$-lattice N satisfying*

$$q^s L_p \text{ represents } N_p \text{ for every prime } p.$$

The integer s in the above lemma can be determined using the following construction from $[\mathrm{BeH}]_1$. Let L be a positive $\mathbb{Z}$-lattice with quadratic form Q. For a prime p we write $d(L_p)$ for the usual discriminant of L_p if $l = \dim L$ is even, and half the discriminant of L_p if l is odd. The lattice L is called *good* at p if $Q(L_p) \subseteq \mathbb{Z}_p$ and $d(L_p) \in \mathbb{Z}_p^*$. If L is good at p one can associate (see *loc. cit.*) with (L, p) a graph $(L : p)$ whose vertices are those lattices K in $\mathrm{gen}(L)$ with $K_q = L_q$ for all primes $q \neq p$. The distance function on the vertices is defined by $\mathrm{dis}(L, K, p) = r$ if and only if $[L_p : L_p \cap K_p] = p^r$. We call L, K *neighbors* if $r = 1$, and in this case L and K are connected by one edge. This graph contains representative classes from at most two spinor genera, and if a spinor genus is represented in the graph, then every class in its spinor genus is represented (see $[\mathrm{BeH}]_2$). With these remarks one easily gets

PROPOSITION 4. *Let L be as in Lemma 1. If L is good at the prime q, then the integer s can be taken as $s = h(L) - 1$, where $h(L)$ is the class number of L. If the lattice L is unimodular*, $\dim L \geq 5$ *and $q = 2$, then s can be taken as $s = h(L) - 1$.*

P r o o f. Since L is good at q we can consider its graph $(L : q)$ which contains representatives of each class in the spinor genus of L. Then noticing that for neighboring lattices L, K we have $qK \subseteq L$ and that isomorphic lattices have isomorphic sets of neighbors, we obtain the first statement. The second one follows directly from $[\mathrm{O'M}]_1$, (106:B).

The last result which we need is Lemma (1.7) from [HKK]:

LEMMA 2. *For a positive lattice N let $\mu(N)$ be its minimum. Then there is a constant $b_n > 0$ such that for any Minkowski-reduced basis $(v_i)_{i=1}^n$ of the lattice N, the matrix $(B(v_i, v_j)) - b_n \mu(N) I_n$ is positive definite (here I_n is the unit matrix and B is the bilinear form associated with Q).*

LEMMA 3. *With the same notations as in Lemma 2*

$$b_n = n^{-(n-1)} \left(\frac{4}{5}\right)^{-(n-3)(n-4)/2} \left(\frac{\pi}{4}\right)^n \left[\Gamma\left(\frac{n}{2} + 1\right)\right]^{-2}$$

if $n \geq 5$.

P r o o f. Let us introduce some notation. For two symmetric matrices A, B of the same size we write $A > B$ (resp. $A \geq B$) if $A - B$ is positive definite (resp. positive semi-definite). Set $N_0 = \mathrm{diag}(B(v_1, v_1), \ldots, B(v_n, v_n)) = \mathrm{diag}(Q(v_1), \ldots, Q(v_n))$ for the diagonal matrix with entries $Q(v_1), \ldots, Q(v_n)$. Using Minkowski's reduction theory (see [vdW] or [Ki]) and Lemmas (1.3.2), (1.3.3) in [Ki] we conclude

$$(B(v_i, v_i)) - b_n N_0 > 0.$$

But since $N_0 - \mu(N)I_n \geq 0$, we conclude

$$(B(v_i, v_i)) - b_n\mu(N)I_n > 0.$$

With these preliminary results we are able to estimate the constants $c(I_{2n+6})$, $n \geq 1$, appearing in Proposition 1.

Proposition 5. *For any* $n \geq 1$,

$$c(I_{2n+6}) \leq \frac{1}{b_n} n^2\, 2^{4(h(I_{n+3})-1)}$$

($h(I_m) =$ *class number of* I_m).

Proof. We will effectively construct the proof of (1.3) in [HKK]. Let $N = \sum_{i=1}^n \mathbb{Z}v_i$ be a positive definite lattice with $\{v_i\}_{i=1}^n$ a Minkowski-reduced basis. Let $L = K = I_{n+3}$ be two copies of I_{n+3}. Choose vectors $(v_i^h, \ldots, v_n^h)$, $v_i^h \in K$, $1 \leq h \leq t$, such that for any set $(x_{i,2}) \in K_2^n$ there is some h with

$$(*) \qquad v_i^h \equiv x_{i,2} \pmod{2^{2s}K_2},$$

where $s = h(L)-1$. Let $K = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_{n+3}$ with $\{e_i\}$ being the standard basis. Then $v_i^h = \sum_{j=1}^{n+3} a_{ij}e_j$ and

$$(B(v_i^h, v_j^h)) = (a_{ij})^t(a_{ij}) \leq \operatorname{Tr}((a_{ij})^t(a_{ij}))I_n.$$

From $(*)$ it follows that we may assume $0 \leq a_{ij} < 2^{2s}$. Hence

$$\operatorname{Tr}((a_{ij})^t(a_{ij})) < n^2 2^{4s}.$$

Put $c' = c'(K, 2^sL) = n^2 2^{4s}$. Then $c'I_n - (B(v_i^h, v_j^h))$ is positive definite for all $1 \leq h \leq t$. Assume now $\mu(N) > (1/b_n)c'$. Then by the previous lemma

$$(B(v_i, v_j)) - \mu(N)b_nI_n > 0.$$

From the local representation theory (see Section 2) we can find $x_{i,2} \in K_2$ for all i with

$$B(v_i, v_j) = B(x_{i,2}, x_{j,2})$$

(i.e. N is represented by I_{n+3} over $\mathbb{Z}_2$). Thus from $(*)$ we have $x_{i,2} = v_i^h + 2^{2s}z_{i,2}$, $z_{i,2} \in K_2$, for $1 \leq i \leq n$. Then

$$\begin{aligned} A := {} & (B(v_i, v_j) - B(v_i^h, v_j^h)) \\ = {} & 2^{2s}(B(v_i^h, z_{i,2}) + B(z_{i,2}, z_{j,2}) + 2^{2s}B(z_{i,2}, z_{j,2})). \end{aligned}$$

The choices made above imply that A is positive definite. From [O'M]$_2$, Theorem 3, we see that A is represented by 2^sL_2 over $\mathbb{Z}_2$, and from Section 2 we conclude that A is represented by 2^sL_p for all $p \neq 2$. Since $s = h(L) - 1$ satisfies the conditions of Lemma 1 (see Lemma 1.2 of [HKK]), we see that A is represented by L. Hence we have

$$B(v_i, v_j) = B(v_i^h + W_i, v_j^h + W_j)$$

with $W_i \in L, 1 < i < n$. This shows that N is represented by $L \perp K = I_{2n+6}$, and therefore we can take $c(I_{2n+6}) = (1/b_n)n^2 2^{4s}$.

Inserting this result in Proposition 1 we get

THEOREM 2. *For every $n \geq 6$,*

$$g_{\mathbb{Z}}(n) \leq 8 + \frac{2^{4(h(I_{n+3})-1)}}{b_n}\left[\frac{n(n+1)(2n+1)}{6} - 55\right].$$

4. The g-function of global rings. The purpose of this section is to extend Theorem 2 of Section 3 to the ring of integers of a totally real number field. Let $K/\mathbb{Q}$ be a totally real number field of degree $[K : \mathbb{Q}] = l$. Since the ideas are similar to those in the previous section, we will only sketch the proofs. The main point is to replace Minkowski's reduction theory by Humbert's reduction theory of forms defined over K (see $[\mathrm{H}]_1$, $[\mathrm{H}]_2$) and also the representation Theorem 1 of [HKK] by its generalization to K, i.e. Theorem 3 of [HKK]. The proof of the finiteness of $g_{\mathbb{Z}}(n)$ (see [I], [BI]) follows almost identically for $g_{O_K}(n)$ and one gets in particular the following analogue of Proposition 1, where $c(M)$ now denotes the constant associated with any positive definite O_K-lattice M in Theorem 3 of [HKK].

PROPOSITION 6. *For any totally real number field K,*

$$g_{O_K}(n) \leq \sum_{i=2}^{n} c(I_{2i+6}) + 5.$$

Proof. For any positive definite O_K-lattice N of rank n, we denote by $\mu(N) = \min\{\mathrm{Tr}_{K/\mathbb{Q}}(Q(x)) \mid 0 \neq x \in N\}$ its minimum. We consider again two separate cases:

(i) $\mu(N) \geq c(I_{2n+6})$. Then Theorem 1 in Section 2 and Theorem 3 in [HKK] imply that N is represented by I_{2n+6}.

(ii) $\mu(N) < c(I_{2n+6})$. Then we assume that the form $Q = \sum_{i,j=1}^{n} a_{ij}X_iX_j$ is reduced in the sense of Humbert. Hence if

$$Q(X_1, \ldots, X_n) = \sum_{j=1}^{r} [L_j(X_1, \ldots, X_n)]^2,$$

where the linear forms $L_j(X_1, \ldots, X_n) = b_{1j}X_1 + \ldots + b_{nj}X_n$ have coefficients in O_K, we obtain

$$a_{11} = \sum_{j=1}^{r} b_{1j}^2.$$

Hence $\mu(N) = \mathrm{Tr}_{K/\mathbb{Q}}(a_{11}) = \sum_{j=1}^{r} \mathrm{Tr}_{K/\mathbb{Q}}(b_{1j}^2)$. Since the field K is totally real we deduce as before that at most $[c(I_{2n+6})]$ of the b_{1j} are non-zero.

By the same argument as for the case of $g_{\mathbb{Z}}(n)$ and using the fact that $g_{O_K}(1) \le 5$, we obtain the stated result.

Once again we want to estimate $c(I_{2i+6})$. We will need the following notation. Let $\sigma_1, \ldots, \sigma_l : K \to \mathbb{R}$ be the real embeddings of K. Then for any integral basis $\alpha = \{\alpha_1, \ldots, \alpha_l\}$ of K set

$$\beta_\alpha = \max\{|\sigma_i(\alpha_j)| \mid 1 \le i, j \le l\} \quad \text{and} \quad \beta = \min_\alpha \beta_\alpha,$$

where α runs over all integral bases of O_K. This number β can be estimated in terms of the discriminant d_K of K. Let us fix a basis $W = \{W_1, \ldots, W_l\}$ of O_K such that $\beta = |\sigma_t(W_s)|$ for some t, s. We have at once

Lemma 4. *Let p be a prime number. The set $R = \{\lambda = \sum_{i=1}^{l} a_i W_i \mid 0 \le a_i \le p^r - 1\}$ is a set of representatives for $O_K / \prod_{i=1}^{g} \mathcal{P}_i^r$, where $\mathcal{P}_i$ runs over all primes in O_K over (p). Moreover, for any $\lambda \in R$,*

$$|\sigma_i(\lambda)| \le (p^r - 1)\beta.$$

For any positive O_K-lattice N let $\mu(N)$ be its minimum. Then the analogue of Lemma 2 says now that if $\{v_i\}_{i=1}^n$ is a Humbert-reduced basis of N, the matrix $(B(v_i, v_j)) - b_n \mu(N) I_n$ is positive definite for some constant b_n depending only on n and K. The estimate of b_n can be done using the reduction constants c_1, c_2, c_3 appearing in Section 1 of $[\mathrm{H}]_2$, but we will omit the details. Now the main result of this section is

Proposition 7. *For any $n \ge 2$,*

$$c(I_{2n+6}) \le \frac{4}{b_n} \beta^2 n^2 3^{4(h(I_{n+3})-1)},$$

where $h(I_n)$ denotes the class number of the lattice I_n.

Proof. Let $S = \{\mathcal{P} \mid \mathcal{P} \text{ prime in } O_K,\ \mathcal{P} \cap \mathbb{Z} = (2)\} \cup \{\mathcal{Q} \mid \mathcal{Q} \text{ prime in } O_K,\ \mathcal{Q} \cap \mathbb{Z} = (3)\}$. For $\mathcal{P} \in S$, $\mathcal{P}$ dyadic, set $r_{\mathcal{P}} = 1$ and for non-dyadic $\mathcal{Q} \in S$ set $2s = r_{\mathcal{Q}} = 2(h(I_{n+3}) - 1)$. Fix $\mathcal{Q}_1 \in S$, $\mathcal{Q}_1$ non-dyadic. Let $M = L = I_{n+3}$ be two copies of I_{n+3} and set $c' = 4\beta^2 n^2 3^{2r}$. Suppose N is an n-dimensional positive definite O_K-lattice with $\{v_i\}$ a Humbert-reduced basis. Assume $\mu(N) > c'/b_n$. We will show that N is represented by I_{2n+6}, i.e. $c(I_{2n+6}) \le c'/b_n$. From the local results of Section 2 we know that N is represented by $(I_{2n+6})_{\mathcal{P}}$ for all primes $\mathcal{P}$ of K. Choose a finite set of n-tuples $(v_i^h, \ldots, v_n^h)$, $1 \le h \le t$, with $v_i^h \in M$ such that for any n-tuple $(x_{i,\mathcal{P}})$, $\mathcal{P} \in S$, $1 \le i \le n$, with $x_{i,\mathcal{P}} \in M_{\mathcal{P}}$ there is some h with

$$v_i^h \equiv x_{i,\mathcal{P}} \pmod{\mathcal{P}^{r_{\mathcal{P}}} M_{\mathcal{P}}}.$$

Using the same arguments as in the proof of Proposition 5 we obtain

$$(\sigma(B(v_i^h, v_j^h))) < 4\beta^2 n^2 3^{2r} I_n$$

for any embedding σ of K in $\mathbb{R}$. Hence

$$c' I_n - (B(v_i^h, v_j^h)) > 0$$

is positive definite (over K). But since $\mu(N) > c'/b_n$ we conclude that $(B(v_i, v_j)) - c' I_n > 0$. Thus the matrix $A = (B(v_i, v_j)) - (B(v_i^h, v_j^h))$ is positive definite. The local results of Section 2 imply that A is represented by $\mathcal{Q}_1^s L_{\mathcal{P}}$ for all $\mathcal{P} \notin S$ and for $\mathcal{P} \in S, \mathcal{P} \neq \mathcal{Q}_1$. But Theorem 1 of [O'M]$_2$ says that A is also represented by $\mathcal{Q}_1^s L_{\mathcal{Q}_1}$. The general version of Lemma 1 (see Section 3 of [HKK]) implies that A is represented by $L = I_{n+3}$. Thus N is represented by I_{2n+6}, and hence $c(I_{2n+6}) \leq c'/b_n$.

We have thus shown

THEOREM 3. *With all notations as above*, *let* $r = 2(h(I_{n+3}) - 1)$. *Then for* $n \geq 2$,

$$g_{O_K}(n) \leq 5 + \frac{4}{b_n} \beta^2 n^2 3^{2r} \left[\frac{n(n+1)(2n+1)}{6} - 1 \right].$$

Remarks. (1) If $K/\mathbb{Q}$ is not real, then using the theory of spinor genus (see [O'M]$_1$) we easily show that

$$g_{O_K}(n) = n + 3 \quad \text{for } n \geq 1.$$

(2) The same arguments as in (1) can be used to show $g_{\mathbb{Z}[1/p]}(n) = n+3$, $n \geq 1$, for any prime p.

References

[BI] R. Baeza and M. I. Icaza, *Decomposition of positive definite integral quadratic forms as sums of positive definite quadratic forms*, in: Proc. Sympos. Pure Math., Amer. Math. Soc. 58 (1995), 63–72.

[BLOP] R. Baeza, D. Leep, M. O'Ryan and J. P. Prieto, *Sums of squares of linear forms*, Math. Z. 193 (1986), 297–306.

[BeH]$_1$ J. W. Benham and J. S. Hsia, *On spinor exceptional representations*, Nagoya Math. J. 87 (1982), 247–260.

[BeH]$_2$ —, —, *Spinor equivalence of quadratic forms*, J. Number Theory 17 (1983), 337–342.

[HKK] J. S. Hsia, Y. Kitaoka and M. Kneser, *Representations of positive definite quadratic forms*, J. Reine Angew. Math. 301 (1978), 132–141.

[H]$_1$ P. Humbert, *Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique fini*, Comment. Math. Helv. 12 (1939/40), 263–306.

[H]$_2$ —, *Réduction des formes quadratiques dans un corps algébrique fini*, ibid. 23 (1949), 50–63.

[I] M. I. Icaza, *Effectiveness in representations of positive definite quadratic forms*, Dissertation, The Ohio State University, 1992.

[Ki] Y. Kitaoka, *Siegel Modular Forms and Representation by Quadratic Forms*, Tata Inst. Fund. Res. Stud. Math. Bombay, Springer, 1986.

[Ko] C. Ko, *On the representation of a quadratic form as a sum of squares of linear forms*, Quart. J. Math. Oxford 8 (1937), 81–98.

[Mo]$_1$ L. J. Mordell, *A new Waring's problem with squares of linear forms*, ibid. 1 (1930), 276–288.

[Mo]$_2$ —, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z. 35 (1932), 1–15.

[Mo]$_3$ —, *The representation of a definite quadratic form as a sum of two other*, Ann. of Math. 38 (1937), 751–757.

[O'M]$_1$ O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren Math. Wiss. 117, Springer, 1973.

[O'M]$_2$ —, *The integral representation of quadratic forms over local rings*, Amer. J. Math. 80 (1958), 843–878.

[R] C. Riehm, *On the representation of quadratic forms over local fields*, ibid. 86 (1964), 25–62.

[VdW] B. L. van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. 96 (1956), 265–309.

DEPARTMENT OF MATHEMATICS
FACULTAD DE CIENCIAS
UNIVERSIDAD DE CHILE
CASILLA 653
SANTIAGO, CHILE
E-mail: ICAZAP@ABELLO.DIC.UCHILE.CL

Received on 10.2.1995
and in revised form on 16.6.1995 (2742)