JOURNAL OF NUMBER THEORY **24**, 272–283 (1986)

Integral Points on Norm-Form Varieties

B. Z. MOROZ

Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, D-5300 Bonn-3, West Germany

Communicated by D. Zagler

Received March 8, 1985; revised March 20, 1985

We study the distribution of integral points on the varieties of the form $f_1(x_1) = \cdots = f_r(x_r)$, where f_j, $1 \leqslant j \leqslant r$, is a norm-form associated to an ideal class in a totally complex finite extension of $\mathbb{Q}$. © 1986 Academic Press, Inc.

1

Let $f_j(x_j)$, $1 \leqslant j \leqslant r$, be a form of degree d_j with integral rational coefficients depending on n_j variables

$$x_j = (x_{j1}, ..., x_{jn_j}).$$

Consider an algebraic variety V defined over $\mathbb{Q}$[1] by a system of equations

$$f_1(x_1) = f_2(x_2) = \cdots = f_r(x_r), \qquad r \geqslant 2. \tag{1}$$

Suppose that f_j is nonnegative definite over $\mathbb{R}$ for each j, that is, $f_j(a_j) \geqslant 0$ when $a_j \in \mathbb{R}^{n_j}$, and consider an algebraic variety

$$V_j : f_j(x_j) = 1, \qquad 1 \leqslant j \leqslant r,$$

and a subvariety

$$V_0 = V_1 \times \cdots \times V_r : f_1(x_1) = \cdots = f_r(x_r) = 1$$

of V. Let $U_j \subseteq V_j|_{\mathbb{R}}$ and let $U = U_1 \times \cdots \times U_r$, so that U_j and U are certain subsets of the manifolds of real points in V_j and V_0, respectively. We write

$$\|a_j\| = f_j(a_j)^{\delta_j}, \qquad 1 \leqslant j \leqslant r, \qquad a_j \in \mathbb{R}^{n_j}, \qquad \delta_j =: \frac{1}{d_j}$$

[1] As usual, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}$ denote the field of rational numbers, the field of real numbers, the field of complex numbers, and the ring of rational integers, respectively.

0022-314X/86 $3.00

and define a projection

$$\pi\colon V|_{\mathbb{R}} \to V_0|_{\mathbb{R}} \cup \{0\}$$

by the relations

$$\pi = \pi_1 \times \cdots \times \pi_r, \qquad \pi_j(a_j) = \begin{cases} 0 & \text{when } f_j(a_j) = 0 \\ \dfrac{a_j}{\|a_j\|} & \text{otherwise} \end{cases}, \qquad 1 \leqslant j \leqslant r.$$

Choose $X > 0$ and denote by $\mathcal{N}(U, X)$ the cardinality of the set

$$v(U, X) = \{a \mid a \in \mathbb{Z}^n, f_1(a_1) = \cdots = f_r(a_r) < X, \pi(a) \in U\},$$

where $n = \sum_{j=1}^{r} n_j$, $a = (a_1, ..., a_r)$, $a_j \in \mathbb{Z}^{n_j}$ for each j.

It is a classical problem in analytic number theory to estimate asymptotically the number $\mathcal{N}(U, X)$ of the lattice points as $X \to \infty$. The simplest non-trivial case of two positive definite binary quadratic forms allows for elementary treatment (cf. [6]). Several authors (see, e.g., [1, 10, 12] and references therein) have considered the case of an arbitrary number of binary quadratic forms. If, in particular, the discriminant of any of these forms is equal to the discriminant of the corresponding quadratic field and if these quadratic fields are arithmetically independent in the sense of the definition given in Section 4, then one can obtain [8] (cf. also [9, Chap. II, Sect. 5]) an asymptotic formula for $\mathcal{N}(U, X)$ as $X \to \infty$.

In [7] we considered this problem for two quadratic forms of several variables. If the number of variables n is large compared to the degrees of the forms and to the number of equations, then one can approach the problem by analytic methods (cf. [11] and references therein). The goal of this paper is to treat full norm-forms corresponding to ideal classes of the maximal order in a totally complex algebraic number field. We achieve it by reducing the problem to an estimate for the number of integral ideals having equal norms that lie in fixed ideal classes and whose image under a natural map to the Minkowski manifold associated with these fields is confined to smooth subsets of the manifold. Such an estimate has been obtained recently (cf. [8, 9], loc. cit.). Combining it with simple algebraic considerations we prove that, under certain natural conditions, integral points are equidistributed over V. It is interesting to compare our estimates (19), (23) with results of other authors on representation of integers by decomposable forms (see, for instance, [2, 10] and references therein).

2

We use the following notations: k is a finite extension of $\mathbb{Q}$ of degree $2n=[k:\mathbb{Q}]$ assumed to be totally complex; $\mathfrak{o}$ is its ring of integers; H is the group of ideal classes of k; $I_0(k)$ is the monoid of integral ideas of k; $I(k)$ is the group of its fractional ideas; Y is a direct sum of n copies of $\mathbb{C}$ regarded as a $(2n)$-dimensional algebra over $\mathbb{R}$; given a ring B we denote by B^* the multiplicative group of invertible elements in B; $\mathbb{R}_+$ is the multiplicative group of positive real numbers; $\bar{k}$ is a fixed algebraic closure of k. Let

$$\{\sigma_j \mid 1 \leqslant j \leqslant 2n\}$$

be the set of all the embeddings of k into $\mathbb{C}$ indexed so that $\sigma_{j+n}(\gamma)=\overline{\sigma_j(\gamma)}$ for $\gamma \in k$, $j \leqslant n$; we extend σ_j to an isomorphism of $\bar{k}$ into $\mathbb{C}$ denoted by the same symbol

$$\sigma_j\colon \bar{k} \to \mathbb{C}, \qquad 1 \leqslant j \leqslant n,$$

and let $\sigma_{j+n}(\gamma)=\overline{\sigma_j(\gamma)}$ for $j \leqslant n$, $\gamma \in \bar{k}$. Choose a basis $\{e_j \mid 1 \leqslant j \leqslant n\}$ of Y over $\mathbb{C}$ for which

$$e_i e_j = 0 \qquad \text{when } i \neq j,\ e_i^2 = e_i,\ 1 \leqslant i, j \leqslant n,$$

and define a homomorphism

$$N\colon Y^* \to \mathbb{R}_+, \qquad N\colon \sum_{j=1}^{n} y_j e_j \mapsto \prod_{j=1}^{n} |y_j|^2, \qquad y_j \in \mathbb{C}.$$

Obviously,

$$Y^* \cong \mathbb{R}_+ \times W,$$

where

$$W =\colon \{y \mid y \in Y^*, Ny = 1\}$$

is a $(2n-1)$-dimensional subgroup of Y^*. Let

$$\sigma\colon \bar{k} \to Y, \qquad \sigma(\gamma) = \sum_{j=1}^{n} e_j \sigma_j(\gamma), \qquad \gamma \in \bar{k}$$

be the componentwise embedding of $\bar{k}$ into Y. Since $N(\sigma(\gamma)) = N_{k/\mathbb{Q}}\gamma$ for any γ in k, the group W contains a discrete subgroup

$$\sigma(\mathfrak{o}^*) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}^{n-1},$$

where m denotes the order of the maximal finite subgroup of k^*, and we get an exact sequence of groups

$$1 \longrightarrow \mathfrak{v}^* \xrightarrow{\sigma} W \xrightarrow{\tau} \mathscr{T} \longrightarrow 1,$$

where $\mathscr{T}$ is a $(2n-1)$-dimensional torus

$$\mathscr{T} = \{(z_1,..., z_{2n-1}) \mid z_j \in \mathbb{C}^*, |z_j| = 1, 1 \leqslant j \leqslant 2n-1\}. \tag{2}$$

Let μ_0 be the Haar measure on $\mathscr{T}$ normalized by the condition $\mu_0(\mathscr{T}) = 1$ and let $\bar{\mu}$ be the positive Borel measure on W uniquely defined by the conditions:

(1) $\bar{\mu}(\sigma(\varepsilon)\, U) = \bar{\mu}(U)$ for $U \subseteq W$, $\varepsilon \in \mathfrak{v}^*$, so that $\bar{\mu}$ is $\mathfrak{v}^*$-invariant, and

(2) $\bar{\mu}(U) = \mu_0(\tau(U))$ when τ separates points on U, that is $\tau(a) \neq \tau(a')$ for $a \neq a'$, $a \in U$, $a' \in U$.

Write $z_j = \exp(2\pi i \varphi_j)$, $0 \leqslant \varphi_j < 1$, in parametrization (2), and define *smooth sets* on $\mathscr{T}$ as in [8] (see also [9, p. 49–50]).[2] A subset U of W is called *toroidal* if $\tau(U)$ is smooth and τ separates points on U. To define the "ideal numbers" introduced by Hecke [3], we decompose H in a direct sum of its cyclic subgroups, say

$$H \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_q\mathbb{Z}, \qquad m_j \in \mathbb{Z}, m_j > 1, 1 \leqslant j \leqslant q.$$

Choose a generator A_j of $\mathbb{Z}/m_j\mathbb{Z}$ and an integral ideal $\mathscr{B}_j$ in the class A_j^{-1}. Let β_j in $\bar{k}^*$ be chosen in such a way that $\beta_j^{m_j} \in k$ and the principal ideal $(\beta_j^{m_j})$ coincides with $\mathscr{B}_j^{m_j}$. For $A \in H$ we write $A = \sum_{j=1}^{q} l_j A_j$, $0 \leqslant l_j \leqslant m_j - 1$, $1 \leqslant j \leqslant q$, and let $\mathscr{B}(A) = \prod_{j=1}^{q} \mathscr{B}_j^{l_j}$, $\beta(A) = \prod_{j=1}^{q} \beta_j^{l_j}$. Let $\{\omega_j(A) \mid 1 \leqslant j \leqslant 2n\}$ be an integral basis of the ideal $\mathscr{B}(A)$ and let

$$w_j(A) = \omega_j(A)\, \beta(A)^{-1}, \qquad 1 \leqslant j \leqslant 2n.$$

We define a nonsingular linear map

$$g_A : \mathbb{R}^{2n} \to Y, \qquad g_A : a \mapsto \sum_{j=1}^{2n} a_j \sigma(w_j) \qquad \text{for} \quad a = (a_1,..., a_{2n}), a_j \in \mathbb{R} \tag{3}$$

of $\mathbb{R}^{2n}$ on Y and a norm-form

$$f_A(x) = N_{k(x)/\mathbb{Q}(x)} \left(\sum_{j=1}^{2n} x_j \omega_j(A) \right) N_{k/\mathbb{Q}}\, \mathscr{B}(A)^{-1} \tag{4}$$

[2] A subset of $\mathscr{T}$ is smooth if it is (E, μ_0)-smooth in the sense of Section 3 when one takes as elementary the rectangular subsets of $\mathscr{T}$.

associated to A. By construction, $f_A(x)$ is a homogeneous polynomial of $2n$ variables $x=(x_1,..., x_{2n})$ and of degree $2n$ with integral rational coefficients. Up to a unimodular transformation the form $f_A(x)$ is determined by the ideal class A and depends neither on the choice of $\mathscr{B}(A)$ in A^{-1} nor on the choice of the basis $\{\omega_j(A) \mid 1 \leqslant j \leqslant 2n\}$ of $\mathscr{B}(A)$. Since

$$N_{k/\mathbb{Q}}\mathscr{B}(A)=N(\sigma(\beta(A))),$$

we have

$$f_A(a)=N(g_A(a)) \qquad \text{for} \quad a \in \mathbb{R}^{2n}.$$

We define a map

$$\psi: I(k) \to \mathscr{T}$$

letting for $\mathscr{A} \in A$ (here A varies over the elements of H)

$$\psi(\mathscr{A})=\tau\left(\frac{\sigma(\alpha\beta(A)^{-1})}{N_{k/\mathbb{Q}}\mathscr{A}^{\delta}}\right), \qquad \delta=:\frac{1}{2n}, \tag{5}$$

where $(\alpha)=\mathscr{A}\mathscr{B}(A)$. Since $\tau(\sigma(\varepsilon))=1$ for $\varepsilon \in \mathfrak{v}^*$, the right-hand side of (5) depends, in fact, only on $\mathscr{A}$ but not on the choice of α. For each A in H let the map

$$\lambda_A: \mathbb{Q}^{2n} \to A \cup \{0\}$$

be given by

$$\lambda_A(0)=0, \qquad \lambda_A(a)=(\alpha)\,\mathscr{B}(A)^{-1} \quad \text{when} \quad a \neq 0,$$

$$a=(a_1,..., a_{2n}), \qquad \alpha=\sum_{j=1}^{2n} a_j\omega_j(A),$$

where $a_j \in \mathbb{Q}$, $1 \leqslant j \leqslant 2n$, so that $\alpha \in k^*$. We summarize the properties of these maps in the following statements.

PROPOSITION 1. (1) $\lambda_A(a) \in I_0(k)$ *if and only if* $a \neq 0$ *and* $a \in \mathbb{Z}^{2n}$;

(2) $f_A(a)=N_{k/\mathbb{Q}}(\lambda_A(a))$ *for* $a \in \mathbb{Q}^{2n}$;

(3) $\lambda_A(a)=\lambda_A(a')$ *if and only if* $g_A(a)=\sigma(\varepsilon)\, g_A(a')$ *for some* ε *in* $\mathfrak{v}^*$.

Assertions 1–3 follow easily from the definitions. Let

$$V^{(A)}=\{a \mid a \in \mathbb{R}^{2n}, f_A(a)=1\}$$

and let (with $\delta=1/2n$)

$$\pi_A: \mathbb{R}^{2n} \to V^{(A)} \cup \{0\}, \qquad \pi_A(a)=\begin{cases} 0 & \text{when} \quad f_A(a)=0 \\ af_A(a)^{-\delta} & \text{when} \quad f_A(a) \neq 0 \end{cases}$$

For $U \subseteq V^{(A)}$ let

$$c_A(U) = \pi_A^{-1}(U) \cap \mathbb{Q}^{2n}$$

be the rational cone supported on U, and let

$$c'_A(U) = \{\mathscr{A} \mid \mathscr{A} \in A, \psi(\mathscr{A}) \in \tau(g_A(U))\}$$

be a subset of A associated to U. Since

$$g_A(V^{(A)}) = W,$$

the function $\tau \circ g_A$ is well defined on subsets of $V^{(A)}$. A subset U of $V^{(A)}$ is called *toroidal* whenever $g_A(U)$ is toroidal.

PROPOSITION 2. (1) *The map ψ is a homomorphism of $I(k)$ into $\mathscr{T}$;*

(2) $\psi(\lambda_A(a)) = (\tau \circ g_A)(\pi_A(a))$ *for* $a \neq 0$;

(3) *if U is a toroidal subset of $V^{(A)}$, then λ_A separates points on $c_A(U)$, that is $\lambda_A(a) \neq \lambda_A(a')$ when $a \neq a'$, $a \in c_A(U)$, $a' \in c_A(U)$.*

(4) $\lambda_A(c_A(U)) = c'_A(U)$ *whenever* $U \subseteq V^{(A)}$.

Proof. Let $\mathscr{A}$ and $\mathscr{A}'$ be two fractional ideals. We have to prove that

$$\psi(\mathscr{A}\mathscr{A}') = \psi(\mathscr{A})\,\psi(\mathscr{A}'). \tag{6}$$

Let $\mathscr{A} \in A$, $\mathscr{A}' \in A'$ for some A, A' in H; write $A = \sum_{j=1}^{q} l_j A_j$, $A' = \sum_{j=1}^{q} l'_j A_j$ with $0 \leqslant l_j, l'_j \leqslant m_j - 1$ for each j. We have $AA' = \sum_{j=1}^{q} l''_j A_j$ with $l''_j = l_j + l'_j - \kappa_j m_j$, where $\kappa_j = 0$ when $l_j + l'_j < m_j$ and $\kappa_j = 1$ when $l_j + l'_j \geqslant m_j$. Choose α and α' satisfying the conditions

$$\mathscr{A}\mathscr{B}(A) = (\alpha), \qquad \mathscr{A}'\mathscr{B}(A') = (\alpha')$$

and let $\beta_0(A_j) = \beta(A_j)^{m_j}$ for each j. It follows that

$$\beta(A)\,\beta(A') = \beta(AA') \prod_{j=1}^{q} \beta_0(A_j)^{\kappa_j} \tag{7}$$

and that

$$\mathscr{B}(A)\,\mathscr{B}(A') = \mathscr{B}(AA')(\alpha''), \qquad \text{where} \quad \alpha'' := \prod_{j=1}^{q} \beta_0(A_j)^{\kappa_j}.$$

Therefore

$$(\mathscr{A}\mathscr{A}')\,\mathscr{B}(AA') = (\alpha\alpha'\alpha''^{-1}). \tag{8}$$

Equation (6) follows from (5), (7), and (8). This proves Assertion 1. Assertion 2 follows from the definitions of g_A and λ_A. To prove Assertion 3 suppose that $a \neq 0$ and $\lambda_A(a) = \lambda_A(a')$. Then by Assertion 3 of Proposition 1,

$$(\tau \circ g_A)(\pi_A(a)) = (\tau \circ g_A)(\pi_A(a')). \tag{9}$$

If $a \in c_A(U)$, $a' \in c_A(U)$, and $g_A(U)$ is toroidal, it follows from (9) that $\pi_A(a) = \pi_A(a')$. By Assertion 2 of Proposition 1, we have also $f_A(a) = f_A(a')$; therefore $a = a'$. Let us prove Assertion 4. If $a \in c_A(U)$, then $\pi_A(a) \in U$ and therefore $\psi(\lambda_A(a)) = (\tau g_A)(\pi_A(a)) \in (\tau g_A)(U)$; thus $\lambda_A(c_A(U)) \subseteq c'_A(U)$. Conversely, let $\mathscr{A} \in c'_A(U)$, so that

$$\psi(\mathscr{A}) \in \tau(g_A(U)). \tag{10}$$

Let $\mathscr{A}\mathscr{B}(A) = (\alpha)$, then it follows from (10) that

$$N_{k/\mathbb{Q}}\mathscr{A}^{-\delta}\, \sigma(\alpha\beta(A)^{-1}\varepsilon) \in g_A(U) \qquad \text{for some } \varepsilon \text{ in } v^*,$$

and therefore

$$\sigma(\alpha\beta(A)^{-1}\varepsilon) = N_{k/\mathbb{Q}}\,\mathscr{A}^{\delta}\, g_A(b), \qquad b = (b_1, ..., b_{2n})$$

for some b in U. Let $a = (a_1, ..., a_{2n})$, $a_j = b_j N_{k/\mathbb{Q}}\,\mathscr{A}^{\delta}$, so that

$$\sigma(\alpha\beta(A)^{-1}\varepsilon) = \sum_{j=1}^{2n} a_j \sigma(w_j(A)). \tag{11}$$

It follows from (11) that $a \in \mathbb{Q}^{2n}$ and $\mathscr{A} = \lambda_A(a)$; moreover, by construction, $\pi_A(a) = b \in U$, so that $a \in c_A(U)$, and we deduce the inclusion $c'_A(U) \subseteq \lambda_A(c_A(U))$. This completes the proof of Proposition 2.

3

Let M be a differentiable manifold of dimension n and let μ be a positive Borel measure on M; let E be a system of μ-measurable subsets, the elements of E being called *elementary* sets. A subset U of M is said to be (E, μ)-*smooth*, if there exists a positive number $C(U)$ such that for every Δ in the interval $0 < \Delta < 1$ one can find a finite system

$$E_0(\Delta) = \{\rho_j \mid 1 \leqslant j \leqslant N\}$$

of elementary sets satisfying the following conditions:

(A_1) $U \subseteq \bigcup_{j=1}^{N} \rho_j$,

(A_2) $N \leqslant \Delta^{-n}$,

(A_3) $\rho_i \cap \rho_j = \emptyset$ when $i \neq j$,

(A_4) there is N_1 such that $\rho_i \subseteq U$ for $i < N_1$ and

$$\mu\Bigl(\bigcup_{N_1 \leqslant j \leqslant N} \rho_j\Bigr) < C(U)\,\Delta.$$

Suppose we are given a set S and two maps:

$$\pi\colon S \to M, \qquad N\colon S \to \mathbb{R}_+.$$

The triple (S, π, N) is said to be *(E, μ)-equidistributed*, if the cardinality $\mathcal{N}(\rho, t)$ of the set

$$u(\rho, t) = \{s \mid s \in S, \pi(s) \in \rho, Ns < t\}$$

satisfies the relation

$$\mathcal{N}(\rho, t) = b\mu(\rho)\, t + O(t^{1-\gamma}) \qquad \text{as} \quad t \to \infty \tag{12}$$

for each ρ in E, with positive b and γ that do not depend on ρ and t.

PROPOSITION 3. *Suppose that (S, π, N) is (E, μ)-equidistributed and let U be an (E, μ)-smooth subset of M. We have then*

$$\mathcal{N}(U, t) = b\mu(U)\, t + O(C(U)\, t^{1-\gamma_1}) \tag{13}$$

with $\gamma_1 = \gamma/(n+1)$ and an O-constant independent of U and t.

Proof. Choose Δ in the interval $0 < \Delta < 1$ and let $E_0(\Delta)$ satisfy conditions A_1–A_4. Let U_1 be the union of those ρ in $E_0(\Delta)$ for which $\rho \cap U \neq \emptyset$ and let U_2 be the union of those ρ in $E_0(\Delta)$ for which $\rho \subseteq U$. By A_4, we have

$$\mu(U_1 \backslash U_2) < C(U)\,\Delta. \tag{14}$$

Obviously,

$$\mathcal{N}(U_1, t) \geqslant \mathcal{N}(U, t) \geqslant \mathcal{N}(U_2, t) \tag{15}$$

and

$$\mu(U_1) \geqslant \mu(U) \geqslant (U_2). \tag{16}$$

It follows from $A_1 - A_3$ and (12) that

$$\mathcal{N}(U_j, t) = b\mu(U_j)\, t + O(\Delta^{-n} t^{1-\gamma}), \qquad j = 1, 2. \tag{17}$$

By (14)–(17), one obtains

$$\mathcal{N}(U, t) = b\mu(U)\, t + O(\Delta^{-n} t^{1-\gamma}) + O(C(U)\, \Delta t). \tag{18}$$

Taking $\Delta = t^{-\gamma_1}$, $\gamma_1 = \gamma/(n+1)$ we deduce (13) from (18).

4

Let k_j, $1 \leqslant j \leqslant r$, be r finite Galois extensions of $\mathbb{Q}$. We say that the fields $k_1, \ldots, k_r$ are *arithmetically independent* (cf. [5; 8; 9, p. 120–121]) if for every rational prime p its ramification indices $e_j(p)$ in k_j and $e_i(p)$ in k_i are coprime whenever $1 \leqslant i < j \leqslant r$. Suppose that k_j, $1 \leqslant j \leqslant r$, is totally complex and fix an ideal class A_j in k_j. Let f_j and g_j be the norm-form and the map associated to A_j respectively by (4) and (3); let $d_j = [k_j : \mathbb{Q}]$ and let $d = \sum_{j=1}^{r} d_j$. Consider the real manifolds

$$V_j(h) = \{a \mid f_j(a) = h,\ a \in \mathbb{R}^{d_j}\}, \qquad 1 \leqslant j \leqslant r,\ h \geqslant 0,$$

and let

$$V_0(h) = V_1(h) \times \cdots \times V_r(h);$$

let

$$V = \{(a_1, \ldots, a_r) \mid f_1(a_1) = \cdots = f_r(a_r);\ a_j \in \mathbb{R}^{d_j},\ 1 \leqslant j \leqslant r\}$$

be the manifold of real points on the variety defined by the system of equations (1). Let

$$\pi_j : \mathbb{R}^{d_j} \to V_j(1) \cup \{0\} \qquad \text{and} \qquad \pi : V \to V_0(1)$$

be defined as in Section 1, so that $\pi = \pi_1 \times \cdots \times \pi_r$ on $V_0(h)$ and

$$\pi_j(a) = \begin{cases} 0 & \text{when } h = 0 \\ h^{-\delta_j} a & \text{when } h > 0 \end{cases} \quad \text{for} \quad a \in V_j(h),\ 1 \leqslant j \leqslant r,$$

where we set, for brevity, $\delta_j = 1/d_j$. We define a positive Borel measure μ_j on $V_j(1)$ by

$$\mu_j(U) = \bar{\mu}_j(g_j(U)) \qquad \text{for} \quad U \subseteq V_j(1),$$

where $\bar{\mu}_j$ denotes the measure on the manifold $W_j = g_j(V_j(1))$ defined in Section 2; let $\mu = \mu_1 \times \cdots \times \mu_r$ be the product measure on $V_0(1)$. Let us define a system E of subsets of $V_0(1)$ by the condition: $\rho \in E$ if and only if $\rho = \rho_1 \times \cdots \times \rho_r$ and ρ_j is a toroidal subset of $V_j(1)$ for each j.

THEOREM. *Suppose that k_j is a Galois extension of $\mathbb{Q}$, $1 \leqslant j \leqslant r$, and that the fields $k_1, ..., k_r$ are arithmetically independent. There exist two positive numbers b and γ depending only on the fields k_j, $1 \leqslant j \leqslant r$, such that*

$$\mathscr{N}(U, X) = b\mu(U)\, X + O(C(U)\, X^{1-\gamma}), \qquad \text{as} \quad X \to \infty, \tag{19}$$

for any (E, μ)-smooth subset U of $V_0(1)$, with an O-constant independent of U and X.

Proof. In view of Proposition 3, it is enough to prove that (19) holds for any ρ in E. But for $\rho = \rho_1 \times \cdots \times \rho_r$ with toroidal ρ_j, $1 \leqslant j \leqslant r$, it follows from Propositions 1and 2 that $\mathscr{N}(\rho, t)$ coincides with the cardinality of the set

$$v_0(\rho, t) = \{\mathscr{A} \mid N_{k_1/\mathbb{Q}} \mathscr{A}_1 = \cdots = N_{k_r/\mathbb{Q}} \mathscr{A}_r < t;\, \mathscr{A}_j \in A_j;\, \psi_j(\mathscr{A}_j) \in \bar{\rho}_j\},$$

where $\mathscr{A}$ varies over r-tuples $(\mathscr{A}_1, ..., \mathscr{A}_r)$, $\mathscr{A}_j \in I_0(k_j)$ of integral ideals; $\psi_j \colon I(k_j) \to \mathscr{T}_j$ is the homomorphism (5) of the group of fractional ideals of k_j into the basic $(d_j - 1)$-dimensional torus $\mathscr{T}_j$ assigned to k_j by (2), and $\bar{\rho}_j = (\tau_j \circ g_j)(\pi_j(\rho_j))$ is the projection of ρ_j on the torus $\mathscr{T}_j$ with $\tau_j \colon W_j \to \mathscr{T}_j$ as defined in Section 2; the index j varies over the interval $1 \leqslant j \leqslant r$. By a theorem on equidistribution of ideals having equal norms (see [8, Theorem 2 and remarks in n° 4] or [9, p. 120, Theorem 3]), the cardinality $\mathscr{N}_0(\rho, t)$ of $v_0(\rho, t)$ can be estimated as

$$\mathscr{N}_0(\rho, t) = b\mu_0(\bar{\rho})\, t + O(t^{1-\gamma}), \qquad b > 0, \gamma > 0, \tag{20}$$

where $\bar{\rho} = \bar{\rho}_1 \times \cdots \times \bar{\rho}_r$, and μ_0 is the Haar measure on $\mathscr{T} = \mathscr{T}_1 \times \cdots \times \mathscr{T}_r$ normalized by the condition $\mu_0(\mathscr{T}) = 1$; the constants b and γ depend only on the fields k_j, $1 \leqslant j \leqslant r$. Since by definition of a toroidal set and by construction of the measure μ we have

$$\mu_0(\bar{\rho}) = \mu(\rho),$$

estimate (20) coincides with (12), and (19) follows.

Remark 1. The constant b in (19) is given explicitly by Theorem 2 in [8]. It is a matter of formal considerations to deduce from the asymptotic formula (19) for the number of integral points in a cone supported on a smooth subset U of $V_0(1)$ an estimate for the number of integral points in a more general subset of V. We notice that

$$V = V_0(0) \cup (V_0(1) \times \mathbb{R}_+)$$

and that $V_0(0)$ contains no rational points except the origin. Let λ denote the restriction of the Lebesgue measure on $\mathbb{R}$ to $\mathbb{R}_+$; we define a positive

Borel measure μ' on V by the conditions $\mu'(V_0(0))=0$, $\mu'=\mu\times\lambda$ on $V_0(1)\times\mathbb{R}_+$. Let E_1 be a system of subsets of V of the form

$$U_1 = U \times I,$$

where U is an (E, μ)-smooth subset of $V_0(1)$ and $I=\{t \mid t_1 < t \leqslant t_2\}$ is a subinterval of $\mathbb{R}_+$ (so that $0 \leqslant t_1 < t_2$), and let $\mathcal{N}_1(u)$ denote the number of integral points in a subset u of V. Suppose $k_1,\dots, k_r$ are Galois extensions of $\mathbb{Q}$ which are arithmetically independent; then it follows from (19) that

$$\mathcal{N}_1(U_1) = b\mu'(U_1) + O(C(\pi(U_1))\, t(U_1)^{1-\gamma}) \qquad \text{for } U_1 \text{ in } E_1, \tag{21}$$

where

$$t(u) =: \sup\{h \mid V_0(h) \cap u \neq \varnothing\} \qquad \text{when} \quad u \subseteq V.$$

Proceeding as in the proof of Proposition 3 we deduce from (21) that under the above assumptions

$$\mathcal{N}_1(u) = b\mu'(u) + O(\Delta C(u)) + O(\Delta^{-d}\, t(u)^{1-\gamma}) \tag{22}$$

for any (E_1, μ')-smooth subset u of V and any Δ in the interval $0<\Delta<1$. If

$$\Delta = t(u)^{(1-\gamma)\delta}\, C(u)^{-\delta} < 1, \qquad \delta = \frac{1}{d+1},$$

it follows from (22) that

$$\mathcal{N}_1(u) = \mu_1(u) + O\left(\left(\frac{t(u)}{C(u)}\right)^{\delta} C(u)\, t(u)^{-\gamma\delta}\right), \tag{23}$$

where $\mu_1 = b\mu'$ is a positive Borel measure on V.

Remark 2. The estimate (23) is not trivial only for large enough $t(u)$. It is important to observe that (23) holds for a subset u of a rather general shape, not only for the conic sets considered in the theorem.

One can prove estimates (19) and (22) under a weaker condition on the fields assuming only that $k_1,\dots, k_r$ are linearly disjoint over $\mathbb{Q}$. In this case, however, the coefficient b may depend on the choice of the ideal classes A_j, $1 \leqslant j \leqslant r$, and for some sequences $A_1,\dots, A_r$ it can be equal to zero. If the fields are not assumed to be linearly disjoint Eq. (19) takes the form

$$\mathcal{N}(U, X) = \mu(U)\, X\, P(\log X) + O(C(U)\, X^{1-\gamma}) \tag{19'}$$

for some polynomial $P(t)$, as in the problem of equidistribution of integral ideals having equal norms (cf. [5; 8, Appendix; 9, Chap. 2]).

Acknowledgments

We are grateful to Professor O. Gabber, Professor W. Sinnott, and Professor D. Zagier for remarks and comments related to this work. This paper was written during the summer of 1984 at the Institut des Hautes Études Scientifiques (Bures-sur-Yvette, France) whose hospitality we gratefully acknowledge.

References

1. P. K. J. Draxl, Fonctions L et représentation simultanée d'un nombre premier par plusieurs formes quadratiques, Séminaire Delange–Pisot–Poitou, 12ème année 1970–71, Paris, n° 12.
2. K. Györy, A. Pethö, Über die Verteilung der Lösungen von Normformen Gleichungen, *Acta Arithmetica* **37** (1980), 143–165.
3. E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen (Zweite Mitteilung), *Math. Z.* **6** (1920), 11–51.
4. L. Kuipers and H. Niederreiter, "Uniform distribution of sequences," Wiley–Interscience, New York, 1974.
5. W.-Ch. W. Li and B. Z. Moroz, On ideal classes of number fields containing integral ideals of equal norms, *J. Number Theory* **21** (1985), 185–203.
6. B. Z. Moroz, Composition of binary quadratic forms and scalar product of Hecke series, *Proc. Steklov Inst. Math.* **80** (1965), 102–109.
7. B. Z. Moroz, Distribution of integral points on multidimensional hyperboloids and cones, *Zapiski LOMI*, **1** (1966), 84–113.
8. B. Z. Moroz, On the distribution of integral and prime divisors with equal norms, *Ann. Inst. Fourier (Grenoble)* **34** (1984), 1–17.
9. B. Z. Moroz, "Vistas in Analytic Number Theory," Bonner Mathematische Schriften No. 156, Bonn, 1984.
10. R. Odoni, Some global norm density results obtained from an extended Chebotarev density theorem *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), pp. 485–495, Academic Press, New York/London, 1977.
11. W. M. Schmidt, The density of integer points on homogeneous varieties *in* "Séminaire de Théorie des Nombres, Paris 1981–82," pp. 283–286, Birkhäuser, 1983.
12. A. I. Vinogradov, On the extension to the left half-plane of the scalar product of Hecke's L-series "mit Grössencharakteren," *Izv. Acad. Sci. USSR* **29** (1965), 485–492.