Proc. Indian Acad. Sci. (Math. Sci.), Vol. 104, No. 1, February 1994, pp. 31–48.

Multiplicative arithmetic of finite quadratic forms over Dedekind rings

ANATOLI ANDRIANOV*

Sonderforschungsbereich 170, "Geometrie und Analysis", Mathematisches Institut der Universität, Bunsenstr. 3–5, D-3400 Göttingen, Germany

*Permanent address: St. Petersburg Branch of the Steklov Mathematical Institute, Fontanka 27, 191011 St. Petersburg, Russia

Dedicated to the memory of Professor K G Ramanathan

Abstract. Let $q(X)$ be a quadratic form in an even number m of variables with coefficients in a Dedekind ring K. Let us assume that the sets

$$R(q,a)=\{N\in K^m;\, q(N)=a\}$$

of representations of elements a of K by the form q are finite. Then certain multiplicative relations are obtained by elementary means between the sets $R(q,a)$ and $R(q,ab)$, where b is a product of prime elements ρ of K with finite coefficients $K/\rho K$. The relations imply similar multiplicative relations between the numbers of elements of the sets $R(q,a)$, which formerly could be obtained only in some special cases like the case when $K=\mathbb{Z}$ is the ring of rational integers and only by means of the theory of Hecke operators on the spaces of theta-series. As an application, an almost elementary proof of the Siegel theorem on the mean number of representations of integers by integral positive quadratic forms of determinant 1 is given.

Keywords. Quadratic forms; multiplicative properties; rings of automorphs; Siegel theorem.

1. Introduction

We consider quadratic forms

$$q(X)=\sum_{1\leqslant i\leqslant j\leqslant m} q_{ij}x_ix_j,\quad \text{where}\quad X=\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}, \tag{1.1}$$

with coefficients q_{ij} in a Dedekind ring K and we shall be interested in relations between the sets

$$R(q,a)=R_K(q,a)=\{N\in K^m;\, q(N)=a\} \tag{1.2}$$

of the representations (over K) of various elements a of K by the form q. It turns out that under certain conditions on the form q and a principal prime ideal ρK of K each representation $N\in R(q,\rho a)$ can be factorized in the form

$$N=DN',$$

where $m \times m$-matrices D over K satisfy

$$q(DX) = \rho q'(X)$$

with suitable quadratic forms q' over K, and where N' belongs to $R(q', a)$. The explicit form of the factorization is given by Theorem 4.3. Consecutive application of the theorem to various principal prime ideals and their degrees reveals certain multiplicative properties of the sets $R(q, a)$, given by Corollaries 4.4 and 4.5. As to the quadratic forms under consideration, we assume that they are non-degenerate forms in an even number of variables. Those are the sufficient conditions to apply our main technical tool, the lifting theorem 2.1. We make also a natural assumption on finiteness of class number of the forms (see (2.20)). In addition, we assume in this paper that the forms are *finite*, i.e. each of the sets of representations $R(q, a)$ is finite. This will allow us to simplify the formulas and their proofs. The multiplicative relations between the sets $R(q, a)$ for finite forms imply similar relations between the numbers of their elements

$$r(q, a) = |R(q, a)|,$$

which are given by Theorem 5.1 and formulas (5.3). Formerly, similar general relations could be obtained only for certain specific rings like the ring $\mathbb{Z}$ of rational integers, using the theory of Hecke operators on corresponding spaces of modular forms. Finally, by specializing the relations to the case of positive definite quadratic forms of determinant 1 over the ring $\mathbb{Z}$ we obtain an "almost" elementary proof of the Siegel theorem on mean numbers of representations for these forms.

Notation. If $\mathbf{A}$ is a set, then $\mathbf{A}_n^m$ denotes the set of all $m \times n$-matrices with entries in $\mathbf{A}$, $\mathbf{A}^m = \mathbf{A}_1^m$. If M is a matrix, then ${}^tM$ is the transposed matrix. 1_n will denote the unit matrix of order n over the considered ring.

The letters $\mathbb{Z}$ and $\mathbb{C}$ are reserved for the ring of rational integers and the field of complex numbers respectively. The ground ring K is usually supposed to be a *Dedekind ring*, i.e. a commutative integral domain, where each ideal is a product of prime ideals.

2. Lifting of solutions of quadratic congruences

We associate to each quadratic form (1.1) over a ring K the *matrix* of the form given by

$$Q = Q(q) = (q_{ij}) + {}^t(q_{ij}). \tag{2.1}$$

This is a symmetric $m \times m$-matrix over K whose diagonal entries belong to $2K$. For brevity, such a matrix will be called an *even* matrix of order m over K and the set of all even matrices of order m over K will be denoted by

$$\mathbb{E}_m = \mathbb{E}_m(K). \tag{2.2}$$

It is clear that each matrix $Q \in \mathbb{E}_m$ is the matrix of a quadratic form q in m variables over K, which satisfies

$$2q(X) = {}^tXQX. \tag{2.3}$$

The element

$$d(q) = \det Q, \tag{2.4}$$

where Q is the matrix of a form q, is called *the determinant of* q. If q is a quadratic form in m variables and $M \in K_n^m$ with some $n = 1, 2, \ldots$, we set

$$q|M = (q|M)(X) = q(MX), \tag{2.5}$$

which is clearly a quadratic form in n variables over K. In this case, we say that M is a *representation* of the form $q' = q|M$ by the form q (over K), and we denote by

$$R(q, q') = R_K(q, q') = \{M \in K_n^m; q|M = q'\} \tag{2.6}$$

the set of all representations of q' by q, where equality of quadratic forms is understood coefficient-wise with respect to the "triangular" form (1.1). If $n = 1$, so that $q'(x) = ax^2$, it follows from the definitions that the set (2.6) coincides with the set (1.2) of representations of element a by q:

$$R(q, ax^2) = R(q, a). \tag{2.7}$$

It is clear that the matrix Q' of the form $q' = q|M$ is given by

$$Q' = Q(q|M) = {}^tMQM \tag{2.8}$$

where Q is the matrix of q. It follows that

$$R(q, q') = R(Q, Q') = \{M \in K_n^m; {}^tMQM = Q'\}$$

provided that characteristic of K is not 2.

To study the multiplicative dependence of representations $N \in R(q, \rho a)$ on ρ and a, we consider them as solutions of quadratic congruences

$$q(N) \equiv 0 \pmod{\rho}, \tag{2.9}$$

which, according to (2.7), can be written in the form

$$q|N \equiv 0 \pmod{\rho}, \tag{2.10}$$

and ask in how many ways it is possible to "lift" a solution $N \in K^m$, that is to find a matrix $D \in K_m^m$ which satisfies the congruence

$$q|D \equiv 0 \pmod{\rho} \tag{2.11}$$

and divides N in the sense that $N \in DK^m$, where congruences for quadratic forms are understood coefficient-wise. The answer is essentially given by the following lifting theorem.

Theorem 2.1. *Let $q(X)$ be a quadratic form in an even number $m = 2k$ of variables over a Dedekind ring K and let ρK be a non-trivial principal prime ideal of K with finite residue class ring $K/\rho K$ of $n(\rho)$ elements. Let us assume that*

$$d = \det q \neq 0 \text{ and } \rho \text{ does not divide } d.$$

Then, for each column $N \in K^m$ *satisfying the congruence* (2.9), *the number of matrices*

$$D \in \Lambda d_k(\rho)\Lambda/\Lambda, \quad \text{where} \quad \Lambda = \Lambda^m = GL_m(K) \quad \text{and} \quad d_k(\rho) \equiv \begin{pmatrix} 1_k & 0 \\ 0 & \rho 1_k \end{pmatrix}$$

satisfying the congruence (2.11) *and dividing N depends only on whether N is congruent to zero modulo* ρ *or not, and can be given by the following formula*

$$\sum_{\substack{D \in \Lambda d_k(\rho)\Lambda/\Lambda, \\ q[D \equiv 0 (\mathrm{mod}\, \rho),\, D|N}} 1 = c_\rho(q)(1 + \delta(N/\rho)\varepsilon_\rho(q)n(\rho)^{k-1}), \tag{2.12}$$

where

$$c_\rho(q) = \begin{cases} \prod_{i=0}^{k-2} (1 + \varepsilon_\rho(q)n(\rho)^i), & \text{if } m = 2k > 2 \\ 1, & \text{if } m = 2, \end{cases} \tag{2.13}$$

$\varepsilon_\rho(q) = \pm 1$ *is the sign of the form q modulo* ρ, *i.e. the sign of the non-degenerate quadratic space* $((K/\rho K)^m, q \bmod \rho)$ *defined by the form q modulo* ρ *over the finite field* $K/\rho K$; *in particular, if the characteristic of the field is not* 2, *then*

$$\varepsilon_\rho(q) = \begin{cases} 1, \text{if } (-1)^k \det q \text{ is a square modulo } \rho \\ -1, \text{otherwise,} \end{cases}$$

and where, for a matrix M over the quotient field of K, we set

$$\delta(M) = \begin{cases} 1 \text{ if all the entries of } M \text{ belong to } K \\ 0 \text{ otherwise.} \end{cases}$$

Proof. The theorem is just a specialization of the Theorem 5.1 [1] to the case when $m = 2k$, $r = k$ and $n = 1$. □

Note that the factor $c_\rho(q)$ in (2.12) satisfies

$$c_\rho(q) \neq 0 \text{ if and only if } m = 2 \text{ or } m > 2 \text{ and } \varepsilon_\rho(q) = 1. \tag{2.14}$$

Now we are going to transform the formula (2.12) for further use, but first we introduce some definitions and notations. For an element $a \in K$ we shall call the number (finite or infinite)

$$n(a) = |K/aK|$$

the *norm* of a. An element $\rho \in K$ will be called prime, if the ideal ρK is non-trivial and prime. By

$$P = P(q) \tag{2.15}$$

will be denoted a set of representatives modulo invertible elements (units) of K of all prime elements $\rho \in K$ of finite norm which do not divide the determinant $d = \det q$ and satisfy the condition (2.14).

For each $\rho \subset P$ and each $N \in K^m$ satisfying (2.9) or (2.10), we can write the formula

(2.12). Each matrix D appearing in the formula defines a quadratic form q' over K satisfying the relation

$$q|D = \rho q'. \tag{2.16}$$

If Q and Q' are the matrices of q and q' respectively and d and d' are their determinants, it follows from (2.8) and (2.16) that

$$^tDQD = \rho Q' \tag{2.17}$$

and so

$$(\det D)^2 d = \rho^m d'.$$

Since $D \in \Lambda d_k(\rho)\Lambda$, it follows that $\det D = \rho^k \eta$ and so $d' = \eta^2 d$, where η is invertible in K. Further, the replacement of D by another representative DU with $U \in \Lambda$ in the same coset $D\Lambda$ replaces the form q' by another form $q'|U$ in the same *class*

$$\{q'\} = \{q'|U; U \in \Lambda\} \tag{2.18}$$

of equivalent quadratic forms in m variables over K, and each form of the class can be obtained in this way. Note that the determinants of all quadratic forms of the same class belong to the same coset modulo the group of squares of invertible elements of K. The coset is called the *determinant of the class*. The above considerations show that each quadratic form q' associated to a matrix D in (2.12) by the relation (2.16) belongs to a class of determinant $d = \det q$ and can be replaced by an arbitrary representative of the class by replacing D in $D\Lambda$. Because $n(\rho) < \infty$, it follows that the set $\Lambda d_k(\rho)\Lambda/\Lambda$ is finite (see, for example, [1], § 2), and so the forms q' related to various D in (2.12) belong to a finite set of the classes. But to apply the formulas, a stronger *finiteness condition* will be required. We shall assume that the form q satisfies the following finiteness condition: The set $S(q)$ of all quadratic forms q' in m variables over K belonging to classes of the same determinant as that of $\{q\}$ and satisfying a condition of the form

$$q|D = \mu q' \tag{2.19}$$

with $D \in K_m^m$ and a non-zero $\mu \in K$ is a finite union of different classes (2.18):

$$S(q) = \bigcup_{i=1}^{h} \{q_i\}. \tag{2.20}$$

We shall denote by

$$\langle q \rangle = (q_1, \ldots, q_h) \tag{2.21}$$

a system of representatives of the classes. Without loss of generality, one can assume that

$$\det q_1 = \cdots = \det q_h = \det q. \tag{2.22}$$

Let us return to the formula (2.12). If for $D \in K_m^m$ and $D' = DU$ with $U \in \Lambda$ we have

$$q|D = \rho q_j = q|D' = q|DU = \rho q_j|U,$$

then $q_j|U = q_j$, which means that U belongs to *the group of units*

$$E_j = E(q_j) = R(q_j, q_j) \cap \Lambda \tag{2.23}$$

of the quadratic form q_j. Noticing that the condition $q|D = \rho q_j$ for a matrix $D \in K_m^m$ means exactly that $D \in R(q, \rho q_j)$, we finally can write the formula (2.12) for each prime $\rho \in P$ in the form

$$\sum_{j=1}^{h} \sum_{\substack{D \in R^*(q, \rho q_j)/E_j, \\ D|N}} 1 = c_\rho(q)(1 + \delta(N/\rho)\varepsilon_\rho(q)n(\rho)^{k-1}), \tag{2.24}$$

where

$$R^*(q, \rho q') = R(q, \rho q') \cap \Lambda d_k(\rho)\Lambda. \tag{2.25}$$

Remark 2.2. For many Dedekind rings, for example, for rings of integers of finite extensions of the field of rational numbers or fields of p-adic numbers, there are only finitely many classes of quadratic forms in a given number of variables with a given non-zero determinant (see, for example, [2], Ch. 8–10). For such a ring, the condition (2.20) is automatically fulfilled.

Remark 2.3. If K is a principal ideal domain, it easily follows from the theory of elementary divisors for matrices over K that

$$R^*(q, \rho q') = R(q, \rho q')$$

for every two quadratic forms q and q' in $m = 2k$ variables over K with the same determinant $d \neq 0$ and for each prime element ρ not dividing d.

3. Rings of automorphs and their action on representations

In order to understand the multiplicative meaning of the lifting formulas (2.24), we introduce here the ring of automorphs of the system of representatives (2.21) and define its action on representations of elements of K by forms of the system.

First, for an arbitrary set S and a commutative ring $\mathbf{A}$, we let $L_{\mathbf{A}}(S)$ be the $\mathbf{A}$-*linearization* of S, i.e. the free $\mathbf{A}$-module consisting of all formal finite linear combinations

$$t = \sum_\alpha a_\alpha \{s_\alpha\} \quad a_\alpha \in \mathbf{A}, \quad s_\alpha \in S$$

with coefficients in $\mathbf{A}$ of the symbols $\{s\}$ corresponding in a one–one way to elements of S. Further, if we have a *pairing* of two sets S and X into a set Z, i.e. a mapping

$$(S, X) \to S \cdot X \subset Z,$$

then by setting

$$\left(\sum_\alpha a_\alpha \{s_\alpha\}\right) \cdot \left(\sum_\beta b_\beta \{x_\beta\}\right) = \sum_{\alpha,\beta} a_\alpha b_\beta \{s_\alpha . x_\beta\}, \tag{3.1}$$

where a_α, $b_\beta \in \mathbf{A}$, $s_\alpha \in S$, $x_\beta \in X$, and the sums on the left are finite, we obtain a bilinear pairing

$$(L_{\mathbf{A}}(S), L_{\mathbf{A}}(X)) \to L_{\mathbf{A}}(S) \cdot L_{\mathbf{A}}(X) \subset L_{\mathbf{A}}(Z) \tag{3.2}$$

of their linearizations into $L_{\mathbf{A}}(Z)$. The mapping

$$L_{\mathbf{A}}(S) \supset t = \sum_\alpha a_\alpha \{s_\alpha\} \to c(t) = \sum_\alpha a_\alpha \in \mathbf{A} \tag{3.3}$$

defines clearly a homomorphism of $\mathbf{A}$-modules

$$c: L_{\mathbf{A}}(S) \to \mathbf{A}$$

which will be called *the coefficient mapping*. The coefficient mappings are compatible with the pairing (3.1), since, by the definition,

$$\begin{aligned} c\left(\left(\sum_\alpha a_\alpha \{s_\alpha\}\right) \cdot \left(\sum_\beta b_\beta \{x_\beta\}\right)\right) &= c\left(\sum_{\alpha,\beta} a_\alpha b_\beta \{s_\alpha \cdot x_\beta\}\right) \\ = \sum_{\alpha,\beta} a_\alpha b_\beta = \left(\sum_\alpha a_\alpha\right)\left(\sum_\beta b_\beta\right) &= c\left(\sum_\alpha a_\alpha \{s_\alpha\}\right) \cdot c\left(\sum_\beta b_\beta \{x_\beta\}\right). \end{aligned} \tag{3.4}$$

In what follows, the ring $\mathbf{A}$ will be of no importance. So we shall take $\mathbf{A}$ to be the field $\mathbb{C}$ of complex numbers.

Coming back to a system of representatives of the form (2.21), we consider the $\mathbb{C}$-linearizations

$$L_{ij} = L_{\mathbb{C}}(A_{ij}) \quad (i,j = 1, \ldots, h)$$

of the sets

$$A_{ij} = \bigcup_{\mu \in K, \mu \neq 0} R(q_i, \mu q_j)$$

of *automorphs* of the form q_i to q_j with non-zero multipliers μ, and $\mathbb{C}$-linearizations

$$L_j = L_{\mathbb{C}}(R_j) \quad (j = 1, \ldots, h)$$

of the sets

$$R_j = \bigcup_{a \in K} R(q_j, a) = K^m$$

of representations of elements of K by the form q_j. It follows from obvious inclusions

$$R(q_i, \mu q_j) \cdot R(q_j, \nu q_r) \subset R(q_i, \mu \nu q_r)$$

and

$$R(q_i, \mu q_j) \cdot R(q_j, a) \subset R(q_i, \mu a)$$

that

$$A_{ij} A_{jr} \subset A_{ir} \text{ and } A_{ij} \cdot R_j \subset R_i.$$

Then, by (3.1) and (3.2), we get bilinear pairings

$$(L_{ij}, L_{jr}) \to L_{ij} \cdot L_{jr} \subset L_{ir} \tag{3.5}$$

and

$$(L_{ij}, L_j) \to L_{ij} \cdot L_j \subset L_i. \tag{3.6}$$

The pairings (3.5) enable us to define the structure of an associative $\mathbb{C}$-algebra on the set

$$\mathbb{L} = L(q_1, \ldots, q_h) = \{T = (t_{ij}); t_{ij} \in L_{ij}, i, j = 1, \ldots, h\} \tag{3.7}$$

of all $h \times h$-matrices with entries in L_{ij} with respect to the standard matrix operations. Whereas the pairings (3.6) allow us to define a natural linear representation

$$(\mathbb{L}, \mathbb{R}) \to \mathbb{L} \cdot \mathbb{R} \subset \mathbb{R} \tag{3.8}$$

of the algebra $\mathbb{L}$ on the space

$$\mathbb{R} = R(q_1, \ldots, q_h) = \left\{ X = \begin{pmatrix} x_1 \\ \vdots \\ x_h \end{pmatrix}; \quad x_j \in L_j, j = 1, \ldots, h \right\} \tag{3.9}$$

of all h-columns with entries in L_j, given by standard multiplication of a matrix by columns. The algebra (3.7) and the space (3.9) will be called respectively the *automorph ring* and the *representation space* of the system $(q_1, \ldots, q_h)$.

It follows from (3.4) that the coefficient mappings (3.3) define a homomorphism of $\mathbb{C}$-algebras

$$c: \mathbb{L} = L(q_1, \ldots, q_h) \to \mathbb{C}_h^h \tag{3.10}$$

and a $\mathbb{C}$-linear mapping

$$c: \mathbb{R} = R(q_1, \ldots, q_h) \to \mathbb{C}^h, \tag{3.11}$$

which are compatible with the representation (3.8) of $\mathbb{L}$ on $\mathbb{R}$ in the sense that

$$c(T \cdot X) = c(T) \cdot c(X) \quad (T \in \mathbb{L}, X \in \mathbb{R}). \tag{3.12}$$

4. Finite quadratic forms and their multiplicative properties

Here we shall apply the lifting formula (2.24) to study multiplicative properties of an important class of quadratic forms, the finite quadratic forms. A quadratic form q over a commutative ring $\mathbf{A}$ is said to be *finite* if the set of representations

$$R(q, a) = R_{\mathbf{A}}(q, a) = \{N \in \mathbf{A}^m; q(N) = a\},$$

where m is the number of variables of q, is finite for each $a \in K$. An example of finite forms is given by positive definite forms over rings of integers of totally real finite extensions of the field of rational numbers.

Lemma 4.1. *If q is a finite quadratic form in m variables over an integral domain* **A** *and q' is a quadratic form satisfying*

$$q|D = aq' \tag{4.1}$$

for a non-singular matrix $D \in \mathbf{A}_m^m$ and $a \in \mathbf{A}$, then the form q' is also finite.

Proof. If a column $N \in \mathbf{A}^m$ satisfies $q'|N = b$, then it follows from (4.1) that $q|DN = ab$, that is

$$DR(q', b) \subset R(q, ab).$$

Since the last set is finite and the mapping $N \to DN$ is an imbedding of $\mathbf{A}^m$ into itself, it follows that the set $R(q', b)$ is finite. □

Lemma 4.2. *Let q be a finite quadratic form over a ring* **A**. *Then the set of representations $R_{\mathbf{A}}(q, q')$ is finite for each quadratic form q' over* **A**.

Proof. Let $q'_{11}, \ldots, q'_{nn}$ be the diagonal coefficients of the form q'. If a matrix V with columns $V_1, \ldots, V_n$ belongs to $R(q, q')$, it follows from $q|M = q'$ that

$$q|V_1 = q'_{11}, \ldots, q|V_n = q'_{nn},$$

which implies that the columns $V_1, \ldots, V_n$ belong to finite sets $R(q, q'_{11}), \ldots, R(q, q'_{nn})$ respectively. □

Let us return to a system of representatives of the form (2.21), assuming now that q is a finite form over a Dedekind ring K. Since the form q is finite, it follows from (2.19) and Lemma 4.1 that each of the representatives q_i in (2.21) is finite too. Then, from Lemma 4.2 we conclude that each of the sets $R(q_i, \mu q_j)$ with $\mu \in K$ is finite. In particular, the sets $R^*(q_i, \rho q_j) \subset R(q_i, \rho q_j)$ given by (2.25) and the groups of units (2.23) are finite. This allows us to define elements of the automorph ring (3.7) of the form

$$T^*(\rho) = (T^*_{ij}(\rho)) \in L(q_1, \ldots, q_h) \text{ with } T^*_{ij}(\rho) = e_i^{-1} \sum_{D \in R^*(q_i, \rho q_j)} \{D\} \in L_{ij}, \tag{4.2}$$

where

$$e_i = |E_i|$$

is the number of units of q_i. As to the space of representations (3.9), we introduce the elements of the form

$$R(a) = \begin{pmatrix} R_1(a) \\ \vdots \\ R_h(a) \end{pmatrix} \in R(q_1, \ldots, q_h) \text{ with } R_j(a) = e_j^{-1} \sum_{N \in R(q_j, a)} \{N\}. \tag{4.3}$$

The elements we have just introduced have a clear arithmetical meaning since their entries are just *averaged sums* of all representations belonging to corresponding sets.

Now we are in a position to rewrite the formula (2.24) for a finite form q in terms of the actions of automorph rings on representation spaces. Since clearly $S(q_i) \subset S(q)$ for each $i = 1, \ldots, h$, the formula (2.24) is true with q_i in place of q. Let us multiply

two sides of the formula with $q = q_i$ by the symbol $e_i^{-1}\{N\}$ and sum up over all N of $R(q_i, \rho a)$ for a given $a \in K$. For each $i = 1, \ldots, h$ and each $a \in K$, we get the relation

$$\sum_{j=1}^{h} \sum_{N \in R(q_i, \rho a)} e_i^{-1}\{N\} \sum_{\substack{D \in R^*(q_i, \rho q_j)/E_j, \\ D|N}} 1$$

$$= c_\rho(q)\left(\sum_{N \in R(q_i, \rho a)} e_i^{-1}\{N\} + \varepsilon_\rho(q) n(\rho)^{k-1} \sum_{N \in R(q_i, \rho a) \cap \rho K^m} e_i^{-1}\{N\} \right) \tag{4.4}$$

(Note that $c_\rho(q_i) = c_\rho(q)$ and $\varepsilon_\rho(q_i) = \varepsilon_\rho(q)$ for each $i = 1, \ldots, h$). Now, if $q_i|N = \rho a$ and $N = DN'$ with $D \in R(q_i, \rho q_j)$ and $N' \in K^m$, then it follows that $q_i|N = q_i|DN' = \rho q_j|N' = \rho a$ from which $N' \in R(q_j, a)$. Conversely, if $N' \in R(q_j, a)$ and $D \in R(q_i, \rho q_j)$, it follows that $N = DN'$ belongs to $R(q_i, \rho a)$. Therefore the left side of (4.4) can be written in the form

$$\sum_{j=1}^{h} \sum_{N \in R(q_i, \rho a)} e_i^{-1}\{N\} \sum_{\substack{D \in R^*(q_i, \rho q_j)/E_j \\ N' \in R(q_j, a),\ DN' = N}} 1$$

$$= \sum_{j=1}^{h} \sum_{\substack{D \in R^*(q_i, \rho q_j)/E_j, \\ N' \in R(q_j, a)}} e_i^{-1}\{DN'\}$$

$$= \sum_{j=1}^{h} e_i^{-1} e_j^{-1} \sum_{\substack{D \in R^*(q_i, \rho q_j), \\ N' \in R(q_j, a)}} \{DN'\},$$

because, clearly, $UR(q_j, a) = R(q_j, a)$ for each $U \in E_j$. Using the notation (4.2) and (4.3) and the multiplication (3.1), the last expression can be written in the form

$$= \sum_{j=1}^{h} e_i^{-1} \sum_{D \in R^*(q_i, \rho q_j)} \{D\} \cdot e_j^{-1} \sum_{N' \in R(q_j, a)} \{N'\}$$

$$= \sum_{j=1}^{h} T_{ij}^*(\rho) R_j(a). \tag{4.5}$$

The right side of (4.4) in the same notation is clearly equal to

$$c_\rho(q)\left(R_i(\rho a) + \varepsilon_\rho(q) n(\rho)^{k-1} \sum_{\rho N' \in R(q_i, \rho a)} e_i^{-1}\{\rho N'\} \right)$$

$$= c_\rho(q)\left(R_i(\rho a) + \varepsilon_\rho(q) n(\rho)^{k-1} \{\rho 1_m\} R_i(a/\rho) \right),$$

where $R_i(a/\rho) = 0$ if ρ does not divide a. The above considerations show that the relation (4.4) can be written in the form

$$\sum_{j=1}^{h} T_{ij}^*(\rho) R_j(a) = c_\rho(q)(R_i(\rho a) + \varepsilon_\rho(q) n(\rho)^{k-1} \{\rho 1_m\} R_i(a/\rho)) \tag{4.6}$$

valid for $i = 1, \ldots, h$ and for each $a \in K$. With the matrix notation (4.2) and (4.3) these relations give us a single matrix relation for each $a \in K$ and each prime ρ of P:

$$T^*(\rho) R(a) = c_\rho(q)(R(\rho a) + \varepsilon_\rho(q) n(\rho)^{k-1} [\rho] R(a/\rho)), \tag{4.7}$$

where

$$[b] = \operatorname{diag}(\{b1_m\},\ldots,\{b1_m\}) \in L(q_1,\ldots,q_h), \quad (b \in K), \tag{4.8}$$

and

$$R(a/\rho) = 0 \text{ if } a/\rho \notin K. \tag{4.9}$$

The formula (4.7) is the main goal of our consideration. Let us now join together for convenience of references all of the assumptions made to prove the formula.

Theorem 4.3. *Let $q(X)$ be a quadratic form in an even number $m = 2k$ of variables with a non-zero determinant d over a Dedekind ring K. Suppose that q satisfies the finiteness of class number condition* (2.20) *and let $q_1,\ldots,q_h$ be a system of representatives* (2.21). *Then the formula* (4.7) *is true for each prime element $\rho \in K$ of finite norm $n(\rho)$ which does not divide d and satisfies the condition* (2.14) *and each $a \in K$, where $T^*(\rho) \in L(q_1,\ldots,q_h)$ is the matrix* (4.2), *$R \in R(q_1,\ldots,q_h)$ are the columns* (4.3) *and*

$$c_\rho(q) \neq 0 \text{ and } \varepsilon_\rho(q) = \pm 1$$

are as defined in Theorem 2.1.

COROLLARY 4.4.

With the notation and assumptions of Theorem 4.3, *each formal power series of the form*

$$\varphi(t) = \sum_{n=0}^{\infty} R(a\rho^n)t^n$$

with a of K not divisible by ρ can be formally summed in the form.

$$\varphi(t) = ([1] - c_\rho(q)^{-1} T^*(\rho)t + \varepsilon_\rho(q)n(\rho)^{k-1}[\rho]t^2)^{-1} \cdot R(a), \tag{4.10}$$

where $[1] = [1_K]$ and $[\rho]$ are the elements of the form (4.8) *and the inverse on the right is understood in the ring of formal power series in one variable over the ring $L(q_1,\ldots,q_h)$.*

Proof. Multiplying the series $\varphi(t)$ by the matrix $c_\rho(q)^{-1} T^*(\rho)$ coefficient-wise from the left and using the formula (4.7) with $a\rho^n$ in place of a, we obtain

$$\begin{aligned} &c_\rho(q)^{-1} T^*(\rho)\varphi(t) \\ &\quad = \sum_{n=0}^{\infty} (R(a\rho^{n+1}) + \varepsilon_\rho(q)n(\rho)^{k-1}[\rho]R(a\rho^{n-1}))t^n \\ &\quad = (\varphi(t) - R(a))t^{-1} + \varepsilon_\rho(q)n(\rho)^{k-1}[\rho]\varphi(t)t, \end{aligned}$$

since $R(a\rho^{-1}) = 0$ by (4.9). It follows that

$$\begin{aligned} R(a) &= \varphi(t) - c_\rho(q)^{-1} T^*(\rho)t\varphi(t) + \varepsilon_\rho(q)n(\rho)^{k-1}[\rho]t^2\varphi(t) \\ &= ([1] - c_\rho(q)^{-1} T^*(\rho)t + \varepsilon_\rho(q)n(\rho)^{k-1}[\rho]t^2) \cdot \varphi(t). \end{aligned} \tag{4.11}$$

Since $[1] = [1_K]$ is the identity element of the ring $\mathbb{L} = L(q_1,\ldots,q_h)$, it follows that the quadratic polynomial in parentheses on the right is invertible in the ring of

formal power series in t with coefficients in $\mathbb{L}$: one can take, for example,

$$([1]-c_\rho(q)^{-1}T^*(\rho)t+\varepsilon_\rho(q)n(\rho)^{k-1}[\rho]t^2)^{-1}$$
$$=[1]+\sum_{n=1}^{\infty}(c_\rho^{-1}(q)\,T^*(\rho)t-\varepsilon_\rho(q)n(\rho)^{k-1}[\rho]t^2)^n. \tag{4.12}$$

Therefore the relation (4.11) can be written in the form (4.10). □

Let us now join together the summation formulas (4.10) for all primes ρ of a countable (or finite) subset P' of P:

$$P'=(\rho_1,\rho_2,\ldots)\subset P(q).$$

To this end, we let $S(P')$ be the multiplicative semigroup generated by the unit element $1=1_K$ of K and all prime elements of P'. To each element $b=\rho_1^{n_1}\cdots\rho_r^{n_r}$ of $S(P')$ we associate the monomial

$$t(b)=t(\rho_1^{n_1}\cdots\rho_r^{n_r})=t_1^{n_1}\cdots t_r^{n_r}$$

where $t_1, t_2,\ldots$ are commuting independent variables.

COROLLARY 4.5.

With the above notation and assumptions, for each a of K which is not divisible by primes $\rho_1,\rho_2,\ldots$, the following identity for formal power series in $t_1,t_2,\ldots$ with coefficients in the space $R(q_1,\ldots,q_h)$ is valid:

$$\sum_{b\in S(P')}R(ab)t(b)=\left\{\prod_{i\geqslant 1}([1]-c_i^{-1}T^*(\rho_i)t_i+\varepsilon_i n_i^{k-1}[\rho_i]t_i^2)^{-1}\right\}\cdot R(a) \tag{4.13}$$

where

$$c_i=c_{\rho_i}(q),\quad \varepsilon_i=\varepsilon_{\rho_i}(q)\ \text{and}\ n_i=n(\rho_i).$$

Proof. For finite $P'=P_r=(\rho_1,\ldots,\rho_r)$ the relation follows from (4.10) by induction on r.

If P' is infinite, we write the relation for finite subsets of the form P_r and then take the formal coefficient-wise limit as $r\to\infty$. □

Remark 4.6. According to (4.12), each of the ρ_i-factors on the right can be written as a formal power series in t_i, say,

$$([1]-c_i^{-1}T^*(\rho_i)t_i+\varepsilon_i n_i^{k-1}[\rho_i]t_i^2)^{-1}$$
$$=\sum_{n\geqslant 0}T_i(\rho_i^n)t_i^n,$$

where the coefficients

$$T_i(\rho_i^0)=[1],\ T_i(\rho_i)=c_i^{-1}\,T^*(\rho_i),\ T_i(\rho_i^2),\ldots$$

belong to the ring $L(q_1,\dots,q_h)$, and so their product has the form

$$\sum_{b\in S(P')} T(b)t(b)$$

with

$$T(\rho_1^{n_1}\cdots\rho_r^{n_r}) = T_1(\rho_1^{n_1})\cdots T_r(\rho_r^{n_r})\in L(q_1,\dots,q_h).$$

Then the identity (4.13) means just that

$$R(ab) = T(b)\cdot R(a) \tag{4.14}$$

for each $a\in K$ not divisible by primes in P' and each $b\in S(P')$. This actually gives us an explicit expression for every one of the averaged sums $R_1(ab),\dots,R_h(ab)$ of representations of ab by the forms $q_1,\dots,q_h$ in terms of $R_1(a),\dots,R_h(a)$ and the averaged sums $T_{ij}^*(\rho)$ of automorphs of $R^*(q_i,\rho q_j)$ for $i,j=1,\dots,h$, where ρ runs over the prime divisors of b.

5. Numbers of representations by finite forms

The multiplicative properties of representations by finite quadratic forms obtained above imply similar properties of their numbers. For a finite quadratic form q and an arbitrary quadratic form q' over a ring K we shall denote by

$$r(q,q') = |R(q,q')|$$

the number of representations of q' by q over K. According to Lemma 4.2, each of the numbers is finite.

Theorem 5.1. *With the notation and assumptions of Theorem* 4.3, *for each* $\rho\in P$ *and each* $a\in K$ *the following formula holds*:

$$t^*(\rho)r(a) = c_\rho(q)(r(\rho a) + \varepsilon_\rho(q)n(\rho)^{k-1}r(a/\rho)), \tag{5.1}$$

where

$$t^*(\rho) = (e_i^{-1}r^*(q_i,\rho q_j))\in\mathbb{C}_h^h \text{ with } r^*(q_i,\rho q_j) = |R^*(q_i,\rho q_j)|$$

and

$$r(a) = \begin{pmatrix} e_1^{-1}\, r\,(q_1,a) \\ \vdots \\ e_h^{-1}\, r\,(q_h,a)\end{pmatrix}\in\mathbb{C}^h.$$

Proof. Applying the coefficient mapping (3.3) to both sides of (4.6) and using (3.4), we get the relations

$$\sum_{j=1}^{h} e_i^{-1}r^*(q_i,\rho q_j)e_j^{-1}r(q_j,a)$$

$$= c_\rho(q)(e_i^{-1}r(q_i,\rho a) + \varepsilon_\rho(q)n(\rho)^{k-1}e_i^{-1}r(q_i,a/\rho)) \tag{5.2}$$

for $i=1,\dots,h$. The relations imply (5.1). □

In the same way as we have proved the corollaries 4.4 and 4.5 or directly from the corollaries, using the mappings (3.11) and (3·10) coefficient-wise and the relations (3.12), we obtain the summation formula

$$\sum_{n\geqslant 0} r(a\rho^n)t^n = (1_h - c_\rho(q)^{-1}t^*(\rho)t + \varepsilon_\rho(q)n(\rho)^{k-1}t^2)^{-1}r(a)$$

for every $a\in K$ and ρ of P not dividing a, and the decomposition

$$\sum_{b\in S(P')} r(ab)t(b) = \left\{\prod_{i\geqslant 1}\left(1_h - c_i^{-1}t^*(\rho_i)t_i + \varepsilon_i n_i^{k-1}t_i^2\right)^{-1}\right\}r(a), \tag{5.3}$$

where notation and assumptions are the same as in (4.10) and (4.13). The last relation can be written in a form similar to (4.14), which shows that it actually gives us an explicit expression of numbers $r(q_1, ab),\ldots,r(q_h, ab)$ of representations of ab by the forms $q_1,\ldots,q_h$ in terms of $r(q_1,a),\ldots,r(q_h,a)$ and the numbers $r^*(q_i,\rho q_j)$ for $i,j=1,\ldots,h$ and ρ of P' dividing b. In the case of quadratic forms over the ring $\mathbb{Z}$ of rational integers, similar relations could be formerly obtained, only using the theory of Hecke operators on the spaces of theta-series of the quadratic forms (see [3] and [4]).

Let us consider now the following *mean numbers of representations*

$$\bar{r}(a) = \sum_{i=1}^{h} e_i^{-1}r(q_i,a)r(q_i,0) \tag{5.4}$$

of elements $a\in K$ by the forms of a system of representatives (2.21).

Theorem 5.2. *Let quadratic forms q and $q_1,\ldots,q_h$ be the same as in Theorem* 4.3, *and let $P=P(q)$ be the set* (2.15). *Denote by $S(P)$ the multiplicative semigroup generated by the unit element of the ground ring and by all prime elements of P and let*

$$\varepsilon: S(P)\to\{\pm 1\} \text{ and } n: S(P)\to\mathbb{Z}$$

be the multiplicative extensions of the mappings

$$\rho\to\varepsilon_\rho(q) \text{ and } \rho\to n(\rho) \quad (\rho\in P)$$

respectively. Then for each b of $S(P)$ and each a of K not divisible by prime factors of b the mean numbers of representations (5.4) *satisfy the following relation*

$$\bar{r}(ab) = \left(\sum_{\delta\in S(P),\,\delta|b}\varepsilon(\delta)n(\delta)^{k-1}\right)\bar{r}(a). \tag{5.5}$$

Proof. It is an easy consequence of definitions that the mapping $D\to\rho D^{-1}$ for a prime ρ of P defines a bijection of each set $R^*(q_i,\rho q_j)$ onto the set $R^*(q_j,\rho q_i)$. In particular, we have the relations

$$r^*(q_i,\rho q_j) = r^*(q_j,\rho q_i) \quad (i,j=1,\ldots,h). \tag{5.6}$$

If we multiply both sides of (5.2) by e_i, set $a = 0$ and use (5.6), we obtain the relation

$$\sum_{j=1}^{h} e_j^{-1} r^*(q_j, \rho q_i) r(q_j, 0)$$
$$= c_\rho(q)(1 + \varepsilon_\rho(q) n(\rho)^{k-1}) r(q_i, 0) \tag{5.7}$$

valid for $i = 1, \ldots, h$. Let us multiply now both sides of (5.2) by $r(q_i, 0)$ and sum up over $i = 1, \ldots, h$. We obtain the relation

$$\sum_{i,j=1}^{h} e_i^{-1} r^*(q_i, \rho q_j) e_j^{-1} r(q_j, a) r(q_i, 0)$$
$$= c_\rho(q)(\bar{r}(\rho a) + \varepsilon_\rho(q) n(\rho)^{k-1} \bar{r}(a/\rho)). \tag{5.8}$$

Using (5.7), we can write the left side of (5.8) in the form

$$\sum_{j=1}^{h} e_j^{-1} r(q_j, a) \sum_{i=1}^{h} e_i^{-1} r^*(q_i, \rho q_j) r(q_i, 0)$$
$$= c_\rho(q)(1 + \varepsilon_\rho(q) n(\rho)^{k-1}) \bar{r}(a).$$

By comparing the expressions and dividing both sides by $c_\rho(q)$ (note that $c_\rho(q) \neq 0$ for $\rho \in P$), we get the relation

$$(1 + \varepsilon_\rho(q) n(\rho)^{k-1}) \bar{r}(a) = \bar{r}(\rho a) + \varepsilon_\rho(q) n(\rho)^{k-1} \bar{r}(a/\rho).$$

Quite analogously to in the proof of Corollary 4.4, it follows from the last relation that for each $a \in K$ not divisible by ρ, the following summation formula

$$\sum_{n \geq 0} \bar{r}(a\rho^n) t^n = (1 - (1 + \varepsilon_\rho(q) n(\rho)^{k-1}) t + \varepsilon_\rho(q) n(\rho)^{k-1} t^2)^{-1} \bar{r}(a)$$

holds in the ring of formal power series in one variable over $\mathbb{C}$. Since the right side of the formula can be written in the form

$$(1 - t)^{-1} (1 - \varepsilon_\rho(q) n(\rho)^{k-1} t)^{-1} \bar{r}(a)$$
$$= \sum_{j \geq 0} \left(\sum_{i=0}^{j} \varepsilon_\rho(q)^i n(\rho)^{i(k-1)} \right) t^j \cdot \bar{r}(a),$$

the formula implies the relation

$$\bar{r}(a\rho^j) = \left(\sum_{i=0}^{j} \varepsilon_\rho(q)^i n(\rho)^{i(k-1)} \right) \bar{r}(a)$$

for every a not divisible by ρ and $j = 0, 1, 2, \ldots$. This proves the formula (5.5), if b is of the form $b = \rho^j$. The general case easily follows by induction on the number of different prime divisors of b. □

Finally let us have a look at the classical case of positive definite quadratic forms over the ring $\mathbb{Z}$ with determinant 1. In this case, there are only finitely many classes

of quadratic forms q in a given number m of variables and we can take $q_1, \ldots, q_h$ to be a system of representatives for the classes. Since in this case $m = 2k \equiv 0 \pmod 8$ (see, for example [5], Ch. 5), it implies that

$$\varepsilon_p(q) = \varepsilon_p(q_i) = 1$$

for each prime p, and so P is the set of all prime numbers and $S(P)$ is the multiplicative semigroup $\mathbb{N}$ of all natural numbers. The mean number (5.4) of representations of a natural number b by the forms $q_1, \ldots, q_h$ turns into

$$\bar{r}(b) = \sum_{i=1}^{h} e_i^{-1} r(q_i, b),$$

and the formula (5.5) for $a = 1$ turns into the relation

$$\bar{r}(b) = \left(\sum_{\delta \in \mathbb{N}, \delta | b} \delta^{k-1} \right) \bar{r}(1). \tag{5.9}$$

To get a complete picture, it would be nice to find also a formula for $\bar{r}(1)$. Unfortunately we can do it only using transcendental means. We shall give here a brief account of computations; for details see, for example, [5], Ch. 7 or [6], Ch. 4, 6. The theta-series

$$\Theta_j(z) = \sum_{n \geqslant 0} r(q_j, n) \exp(2\pi i n z) \quad (z = x + iy, y > 0)$$

of the forms $q_1, \ldots, q_h$ belong to the space $\mathcal{M}_k$ of holomorphic modular forms of weight $k = m/2$ relative to the modular group $SL_2(\mathbb{Z})$, and so does their linear combination

$$\bar{\Theta}(z) = \sum_{j=1}^{h} e_j^{-1} \Theta_j(z) = \sum_{n \geqslant 0} \bar{r}(n) \exp(2\pi i n z),$$

which according to (5·9) can be written in the form

$$\bar{\Theta}(z) = \bar{r}(0) + \bar{r}(1) \sum_{n \geqslant 1} \left(\sum_{\delta | n} \delta^{k-1} \right) \exp(2\pi i n z).$$

On the other hand, the space $\mathcal{M}_k$ contains also the so-called Eisenstein series $E_k(z)$ with the Fourier expansion of the form

$$E_k(z) = 1 + \gamma_k \sum_{n \geqslant 1} \left(\sum_{\delta | n} \delta^{k-1} \right) \exp(2\pi i n z)$$

where

$$\gamma_k = \frac{(2\pi)^k}{(k-1)! \zeta(k)} \text{ with } \zeta(k) = \sum_{n \geqslant 1} n^{-k},$$

and so the space contains also the linear combination

$$\gamma_k \bar{\Theta}(z) - \bar{r}(1) E_k(z) = \gamma_k \bar{r}(0) - \bar{r}(1),$$

which is a constant. But the space $\mathcal{M}_k$ contains no constants except zero and so

$$\tilde{r}(1) = \gamma_k \tilde{r}(0) = \frac{(2\pi)^k}{(k-1)!\zeta(k)} \sum_{j=1}^{h} e_j^{-1}.$$

Substituting it in (5.9), we finally obtain the formula

$$\left(\sum_{j=1}^{h} e_j^{-1}\right)^{-1} \sum_{j=1}^{h} e_j^{-1} r(q_j, b) = \frac{(2\pi)^k}{(k-1)!\zeta(k)} \sum_{\delta|b} \delta^{k-1}$$

valid for all natural numbers b, which is a finite form of the famous Siegel theorem [7] on mean numbers of representations for positive quadratic forms over $\mathbb{Z}$ with determinant 1.

6. Concluding remarks

The case when the sets of representations $R(q, q')$ are, in general, infinite can be considered in a similar way, provided that the sets $E(q)\backslash R(q, q')$ of cosets modulo the corresponding group of units $E(q) = R(q, q) \cap \Lambda$ are finite, which often happens. In this case, instead of linear combinations of representations D of $R(q, q')$, one should consider corresponding linear combinations of their cosets $E(q)D$ modulo the group of units. For more, see [1], § 5.

The technique of lifting of solutions of quadratic congruences modulo prime elements, unfortunately, does not work in the case of quadratic forms in an odd number of variables. Recently F A Andrianov (Jr.) has succeeded in considering multiplicative properties of positive definite quadratic forms in an odd number of variables over the ring $\mathbb{Z}$, using a technique of lifting of solutions of quadratic congruences modulo squares of prime numbers. A generalization to finite forms over Dedekind rings goes through without any problem. The corresponding papers by F A Andrianov are due to appear in *Zapisky Nauchn. Sem. St. Petersburg Otdel. Steklov Math. Inst.*, vol. 212 1993/94.

Acknowledgement

This research was carried out and written in the spring of 1993 during the author's stay at Sonderforschungsbereich 170 "Geometrie und Analysis" at Mathematical Institute of Göttingen University. The author would like to take this opportunity to thank the SFB-Board, and especially Professor Ulrich Christian, for their kind invitation, hospitality, and very stimulating research environment.

References

[1] Andrianov A N, Automorphic factorizations of solutions of quadratic congruences and their applications, *Algebra and Analysis* **5** (1993), No. 5 (Russ.); Engl. transl.: *St. Petersburg Math. J.* **5** 1–46 (1993)

[2] O'Meara O T, Introduction to quadratic forms (*Grundlehren Math. Wiss.* Band 117, Springer, Berlin–Heidelberg) (1963)

[3] Andrianov A N, Integral representations of quadratic forms by quadratic forms: multiplicative properties, In *Proc. Int. Cong. Math.* Warszawa, 1 1983, Vol. I, pp. 465–474
[4] Andrianov A N, Composition of solutions of quadratic Diophantine equations, *Russ. Math. Surv.* **46:2** (1991) 1–44
[5] Serre J P, *Cours d'Arithmétique*, (Press Universitaire de France, Paris) (1970)
[6] Ogg A, *Modular forms and Dirichlet series*, (Benjamin, New York – Amsterdam) (1969)
[7] Siegel C L, Über die analytische Theorie der quadratischen Formen, Teil I, *Ann. Math.* **36** (1935) 527–606