ON A RECIPROCITY THEOREM OF GAUSS

Lynne H. Walling

25 May, 2008

Abstract. Gauss proved a reciprocity theorem, showing the number of times a ternary positive definite $\mathbb{Z}$-lattice L primitively represents a positive integer d is equal to the number of times the dual of L primitively represents binary quadratic forms of discriminant $d/\operatorname{disc}L$. In this note we extend this theorem to lattices of arbitrary rank over the ring of integers $\mathcal{O}$ of a number field $\mathbb{K}$, equipped with either a positive definite or an indefinite quadratic form.

1. Introduction

In Arts. 278-292 [5], Gauss proved a reciprocity between the number of times a positive definite ternary quadratic form with matrix Q primitively represents an integer d and the number of times Q^{-1} primitively represents a binary quadratic form of discriminant $d/\det Q$. In 1949, Jones [7] and Pall [9] independently published articles using matrix arguments to examine primitive representations of arbitrary quadratic forms over $\mathbb{Z}$; among other things, they recover Gauss' result. In 1987, Arenas [2] gave a new proof of Gauss' result using exterior algebras. (See also [11], where the author discusses reducing the number of variables in an equation describing primitive representations of one quadratic form by another.)

The purpose of this note is to provide an elementary proof of Gauss' theorem and its generalisation to arbitrary rank lattices, over $\mathbb{Z}$ and over the ring of integers of a number field, allowing both positive definite and indefinite quadratic forms. Our argument utilises dual bases, which we believe makes transparent the duality of Gauss' theorem.

It should be noted that this result can surely be derived from Siegel's deep and beautiful results that give average representation numbers (or, in the indefinite case, measures of representations) as products of local densities [10].

What we prove herein is as follows (precise definitions and a precise statement of the theorem are given below). Let L be a rank m lattice over the ring of integers of a number field, equipped with a non-degenerate quadratic form Q. When the number field is $\mathbb{Q}$ and Q is positive definite, we show that the number of times L

2000 *Mathematics Subject Classification.* 11F41.

Key words and phrases. Quadratic forms, Reciprocity, Siegel Modular Forms, Theta Series.

primitively represents rank n sublattices of discriminant d is the number of times the dual of L primitively represents rank $m-n$ sublattices of discriminant $d/\ \mathrm{disc}L$ ($n < m$). When Q is indefinite, we prove the analogous result for "measures" of the representations. For an arbitrary number field, the same results hold with the discriminant of a lattice replaced by its volume. As an application, we show that with L, K two rank $2k$ positive definite $\mathbb{Z}$-lattices with $\mathrm{disc}L = \mathrm{disc}K$, the degree n Koecher-Maass series for L and K are equal if and only if the degree $2k-n$ Koecher-Maass series for the duals of L and K are equal ($n < 2k$).

The reader is referred to [8] for basic theory of quadratic forms, and to [1] and [4] for basic theory of Siegel modular forms.

The author thanks Trevor Wooley for the heuristic used to count primitive representations by L "in a box" in the case that Q is indefinite.

2. Definitions and statements of results

Let $\mathbb{K}$ be a number field with ring of integers $\mathcal{O}$, and let L be a lattice on a dimension m quadratic space V with quadratic form Q. The discriminant of $V = \mathbb{K}v_v + \cdots + \mathbb{K}v_m$ equipped with a quadratic form Q is

$$\mathrm{disc}(v_1, \ldots, v_m) = \det(B(v_i, v_j))$$

where B is the symmetric bilinear form associated to Q so that $B(x,x) = Q(x)$ (so $\mathrm{disc}V$ is well-defined up to squares of non-zero elements of $\mathbb{K}$). The discriminant of a rank m free lattice $\mathcal{O}v_1 + \cdots + \mathcal{O}v_m$ is $\mathrm{disc}(v_1, \ldots, v_m)$ (so it is well-defined up to squares of units of $\mathcal{O}$). In general, our lattices may not be free over $\mathcal{O}$, but a lattice L does have a decomposition $L = \mathcal{A}_1 v_1 \oplus \cdots \oplus \mathcal{A}_m v_m$ for some fractional ideals $\mathcal{A}_i$ and vectors v_i so that $(v_1, \ldots, v_m)$ is a basis for V; we define the volume of L to be $\mathrm{vol}L = (\mathcal{A}_1 \cdots \mathcal{A}_m)^2\ \mathrm{disc}(v_1, \ldots, v_m)$. We consider here only regular lattices L, meaning that $\mathrm{vol}L \neq 0$, or equivalently, $\mathrm{disc}V \neq 0$, and we define $L^{\#} = \{v \in V :\ B(v, L) \subseteq \mathcal{O}\ \}$.

We say that a sublattice J is a primitive sublattice of L, or that L primitively represents J, if $\mathbb{K}J \cap L = J$ (or equivalently, if J is a direct summand of L).

Say Q is positive definite; when $\mathbb{K} = \mathbb{Q}$, we let

$$r_n^*(L, d) = \#\left\{\text{primitive sublattices } J \text{ of } L :\ \mathrm{rank}J = n,\ \ \mathrm{disc}J = d\ \right\}.$$

More generally, for any number field $\mathbb{K}$ and $\mathcal{I}$ a fractional ideal, let

$$r_n^*(L, \mathcal{I}) = \#\left\{\text{primitive sublattices } J \text{ of } L :\ \mathrm{rank}J = n,\ \mathrm{vol}J = \mathcal{I}\ \right\}.$$

When Q is indefinite and $\mathbb{K} = \mathbb{Q}$, we set

$$r_n^*(L, d; t) = \#\Big\{\text{primitive sublattices } J \text{ of } L :\ \mathrm{rank}J = n,\\ \mathrm{disc}_Q J = d,\ \ \mathrm{disc}_R J \leq t\sqrt{\ \mathrm{disc}_R L}\ \Big\}$$

where R is a majorant of Q, $t > 0$. (So R is a positive definite quadratic form so that, associating R and Q to matrices relative to a basis for V, $R^{-1}QR^{-1} = Q^{-1}$.) Then we set

$$r_n^*(L,d) = \lim_{t\to\infty} t^{1-m/2} r_n^*(L,d;t).$$

More generally, for any number field $\mathbb{K}$ and fractional ideal $\mathcal{I}$, we set

$$r_n^*(L,\mathcal{I};t) = \#\big\{\text{primitive sublattices } J \text{ of } L:\ \mathrm{rank}J = n,\\ \mathrm{vol}_Q J = \mathcal{I},\ N(\mathrm{vol}_R J) \le t\sqrt{N(\mathrm{vol}_R L)}\ \big\}$$

where N denotes the norm from $\mathbb{K}$ to $\mathbb{Q}$, and we set

$$r_n^*(L,\mathcal{I}) = \lim_{t\to\infty} t^{1-m/2} r_n^*(L,\mathcal{I};t).$$

Theorem. *Let L be a rank m lattice on V with quadratic form Q so that $\mathrm{disc}V \neq 0$. When $\mathbb{K} = \mathbb{Q}$ and $d \in \mathbb{Q}$, $d \neq 0$,*

$$r_n^*(L,d) = r_{m-n}^*(L^\#, d/\ \mathrm{disc}L)$$

for any n with $0 < n < m$. More generally, for $\mathbb{K}$ any number field and $\mathcal{I}$ a fractional ideal,

$$r_n^*(L,\mathcal{I}) = r_{m-n}^*(L^\#, \mathcal{I}/\mathrm{vol}L).$$

This implies the following.

Corollary. *Let L, K be positive definite $\mathbb{Z}$-lattices with the same discriminant and even rank $2k$. Then for $1 \le n < 2k$,*

$$\zeta_n(L,s) = \zeta_n(K,s) \iff \zeta_{2k-n}(L^\#,s) = \zeta_{2k-n}(K^\#,s).$$

If L, K are unimodular, this says $\zeta_n(L,s) = \zeta_n(K,s)$ for all $n < 2k$ if $\zeta_n(L,s) = \zeta_n(K,s)$ for all $n \le k$.

Remarks.

(1) For general $\mathbb{K}$, we can replace volumes by ideles of local discriminants in the above theorem.

(2) In our definition of $r_n^*(L,\mathcal{I};t)$ we bound $N(\mathrm{vol}_R J)$ by $t\sqrt{N(\mathrm{vol}_R L)}$ rather than by t to reflect the number of lattice points of L in a box of a given size. For example, if $\mathbb{K} = \mathbb{Q}$ and K is a sublattice of L with index d, then a fundamental parallelopiped of K contains d fundamental parallelopipeds of L, and $\mathrm{disc}K = d^2 \cdot \mathrm{disc}L$.

(3) When Q is indefinite, we expect $r_n^*(L,\mathcal{I};t) \asymp t^{m/2-1}$ (meaning $r_n^*(L,\mathcal{I};t) \ll t^{m/2-1}$ and $r_n^*(L,\mathcal{I};t) \gg t^{m/2-1}$) based on the following heuristic (due to Trevor Wooley): Say $\mathbb{K} = \mathbb{Q}$, and let R be a majorant for Q. Then with $C = (x_{ij})$ an $m \times n$ matrix of indeterminates, $\det({}^tCRC)$ is a positive definite

polynomial in mn variables of degree $2n$ (each term in the $n \times n$ determinant is quadratic). Then if

$$\det({}^tCRC) \le t,$$

one expects that the variables are each typically of size $\asymp t^{1/(2n)}$, and are otherwise unrestricted.

The polynomial $\det({}^tCQC) - d$ has degree $2n$ and has mn variables, each typically of size $\asymp t^{1/(2n)}$. Provided that this equation $\det({}^tCQC) - d$ is not highly singular, one expects by Birch's work on the circle method [3] that the number of solutions will be

$$\asymp c(t^{1/(2n)})^{mn-2n}$$

where c is given by a product of local densities. (Here we note that Birch's theorem becomes applicable once the codimension of the singular locus exceeds $n2^{2n+1}$, which in present circumstances would demand that $m > 2^{2n+1}$. However, the conclusion is expected to hold true under much milder conditions on m.) Then if the equation possesses non-singular real and p-adic solutions for each prime p, the number of solutions of the system is expected to be

$$\asymp t^{m/2-1}.$$

Notice that there may be an average of divisor functions hidden in this argument, and this has the potential to generate a power of $\log t$ in the heuristic formula.

(4) Conjecturally, the measure $r_n^*(L, \mathcal{I})$ is independent of the choice of majorant R. Proposition 4.3 of [6] shows that when $n = 1$ and $\mathbb{K} = \mathbb{Q}$,

$$r(L, d) = \lim_{t\to\infty} t^{1-m/2} \cdot \#\{x \in L : \ Q(x) = d, \ R(x) \le t \ \}$$

is independent of the choice of majorant, and hence $r_1^*(L, d)$ is as well; the proof involves having explicit knowledge of Fourier coefficients of nonholomorphic Eisenstein series.

3. Proofs

Proof of Theorem. Suppose J is a rank n sublattice of L so that $\mathrm{vol}J \neq 0$ and $\mathbb{K}J \cap L = J$. Let $v_1, \dots, v_n$ be a basis for $\mathbb{K}J$; extend this to a basis $v_1, \dots, v_m$ for $V = \mathbb{K}L$. By 81:3 of [8], there are $x_i \in \mathbb{K}v_1 + \cdots + \mathbb{K}v_i$, and fractional ideals $\mathcal{A}_i$ so that $L = \mathcal{A}_1x_1 + \cdots + \mathcal{A}_mx_m$. Note that $\mathcal{A}_1x_1 + \cdots + \mathcal{A}_nx_n = \mathbb{K}J \cap L = J$ (since $\mathbb{K}x_1 + \cdots + \mathbb{K}x_n = \mathbb{K}J$). Let $y_1, \dots, y_m$ be the basis dual to $x_1, \dots, x_m$. So $B(x_i, y_j) = \delta_{ij}$, and

$$L^{\#} = \mathcal{A}_1^{-1}y_1 + \cdots + \mathcal{A}_m^{-1}y_m.$$

Set $M = \mathcal{A}_{n+1}^{-1}y_{n+1} + \cdots + \mathcal{A}_m^{-1}y_m$ and $K = J + M$. Since $\mathrm{vol}J \neq 0$ and $M = \mathbb{K}J^{\perp} \cap L^{\#}$, we have $K = J \perp M$ and so $\mathrm{vol}K = \mathrm{vol}J \cdot \mathrm{vol}M$.

Now write $x_i = \sum_j a_{ij}y_j$. Let A be the $n \times n$ matrix with i, j-entry a_{ij}; so

$$(x_1 \cdots x_n \ y_{n+1} \cdots y_m) = (y_1 \cdots y_m) \begin{pmatrix} A & 0 \\ * & I \end{pmatrix}.$$

The matrix $(B(x_i, x_j))$ takes $(y_1 \dots y_m)$ to $(x_1 \dots x_m)$; so A is the upper left $n \times n$ block of this matrix and hence $\det A = \text{ disc}(x_1, \dots, x_n)$. Also,

$$\begin{aligned} \text{vol}K &= (\mathcal{A}_1 \cdots \mathcal{A}_n \mathcal{A}_{n+1}^{-1} \cdots \mathcal{A}_m^{-1})^2 \cdot \text{ disc}(x_1, \dots, x_n, y_{n+1}, \dots, y_m) \\ &= (\mathcal{A}_1 \cdots \mathcal{A}_n \mathcal{A}_{n+1}^{-1} \cdots \mathcal{A}_m^{-1})^2 \cdot (\det A)^2 \cdot \text{ disc}(y_1, \dots, y_m) \\ &= (\mathcal{A}_1 \dots \mathcal{A}_n)^4 \cdot (\det A)^2 \cdot \text{vol}L^{\#}. \end{aligned}$$

We have $\text{vol}J = (\mathcal{A}_1 \cdots \mathcal{A}_n)^2 \cdot \det A$, so $\text{vol}K = (\text{vol}J)^2 \text{vol}L^{\#}$ and hence

$$\text{vol}M = \text{vol}J \cdot \text{vol}L^{\#} = \text{vol}J/\text{vol}L.$$

Observe that the primitive rank n sublattices J of L with $\text{vol}J = \mathcal{I}$ are in one-to-one correspondence with the primitive rank $m-n$ sublattices M of $L^{\#}$ with $\text{vol}M = \mathcal{I}/\text{vol}L$ via the relation $M = \mathbb{K}J^{\perp} \cap L^{\#}$, $J = \mathbb{K}M^{\perp} \cap L$.

When Q is positive definite, we know the representation numbers attached to isometry classes are finite, and the number of isometry classes of a given volume is finite; this proves the theorem in this case.

So say Q is indefinite; take R a majorant for Q (so R is positive definite, and associating Q and R with matrices relative to $x_1, \dots, x_m$, $RQ^{-1}R = Q$). Let $y_1', \dots, y_m'$ be a basis dual to $x_1, \dots, x_m$ relative to R. So $(y_1', \dots, y_m') = (x_1, \dots, x_m)R$; thus as above, with $M' = \mathcal{A}_{n+1}^{-1} y_{n+1}' + \cdots + \mathcal{A}_m^{-1} y_m'$, $\text{vol}_R M' = \text{vol}_R J/\text{vol}_R L$. On the other hand, $(B(y_i, y_j)) = Q^{-1}RQ^{-1} = R^{-1} = (B(y_i', y_j'))$. In particular, this means $\text{ disc}(y_{n+1}', \dots, y_m') = \text{ disc}(y_{n+1}, \dots, y_m)$ and so $\text{vol}_R M = \text{vol}_R M' = \text{vol}_R J/\text{vol}_R L$. Consequently $r_n^*(L, \mathcal{I}; t) = r_{m-n}^*(L^{\#}, \mathcal{I}/\text{vol}_Q L; t)$ for all $t > 0$, and thus $r_n^*(L, \mathcal{I}) = r_{m-n}^*(L^{\#}, \mathcal{I}/\text{vol}_Q L)$.

The same argument holds with volumes replaced by (ideles of local) discriminants. □

Proof of Corollary. The theta series of degree n attached to L is

$$\theta_n(L; \tau) = \sum_{C \in \mathbb{Z}^{2k,n}} \exp(\pi i Tr(\ {}^t CDC\tau))$$

where $D = (B(x_i, x_j))$ is a matrix for Q on L, and τ is in the degree n Siegel upper half-plane. Thus

$$\theta_n(L; \tau) = \sum_T r(D, T) \exp(\pi i Tr(T\tau)),$$

T varying over $n \times n$ positive semi-definite symmetric matrices and

$$r(D, T) = \#\{C \in \mathbb{Z}^{2k,n} : \ {}^t CDC = T\ \}.$$

Particularly when $Q(L) \subseteq 2\mathbb{Z}$, this theta series is one of the prototypical examples of a degree n Siegel modular form of weight $m/2$ and some level N and character χ. The Koecher-Maass series for $\theta_n(L; \tau)$ is

$$\zeta_n(L; s) = \sum_T \frac{r(D, \det T)}{o(T)} (\det T)^{-s}$$

where T varies over $GL_n(\mathbb{Z})$-inequivalent symmetric $n \times n$ matrices with nonzero determinant (the series is known to converge absolutely for $\Re s$ sufficiently large). Letting $r(L, J)$ be the number of distinct sublattices of L isometric to J, one easily verifies that $r(L, J) = r(D, T)/o(T)$ where T is a matrix representing the quadratic form on J, and $o(T) = o(J)$ is the order of the orthogonal group $O(T) = O(J)$. Thus

$$\zeta_n(L, s) = \sum_{\text{cls}J} r(L, J)\ \text{disc}J^{-s} = \sum_{d>0} r_n(L, d)d^{-s}$$

where

$$r_n(L, d) = \#\left\{\text{primitive sublattices } J \text{ of } L : \ \text{rank}J = n, \ \ \text{disc}J = d\ \right\}.$$

We claim that the $r_n(L, d)$ are determined by the $r_n^*(L, d')$, and vice-versa. To see this, first note that given a rank n sublattice J of L,

$$J' = \mathbb{K}J \cap L$$

is the unique primitive rank n sublattice of L containing J. Also, if $[J' : J] = \ell$ then $\text{disc}J = \ell^2 \cdot \ \text{disc}J'$. Thus

$$r_n(L, d) = \sum_{\ell^2 | d} \eta(\ell) r_n^*(L, d/\ell^2)$$

where $\eta(\ell)$ is the number of index ℓ sublattices J of a rank n lattice J'. Note that since $J'/\ell J'$ is finite, so is $\eta(\ell)$. (Also, η is multiplicative: Say J is a sublattice of J' with $[J' : J] = p^r\ell$, p prime with $p \nmid \ell$. Then $J'' = p^{-r}J \cap J'$ is the unique lattice such that $J' \subseteq J'' \subseteq J$ with $[J : J''] = \ell$, $[J'' : J'] = p^r$.)

This relation between r_n and r_n^* implies that

$$r_n(L, d) = r_n(K, d)\ \forall d > 0 \iff \ \ r_n^*(L, d) = r_n^*(K, d)\ \forall d > 0.$$

Thus, by the Theorem,

$$r_n(L, d) = r_n(K, d)\ \forall d > 0 \iff \ \ r_{m-n}(L^{\#}, d) = r_{m-n}(K^{\#}, d)\ \forall d > 0,$$

proving the Corollary. □

References

1. A.N. Andrianov, *Quadratic Forms and Hecke Operators*, Grundlehren Math. Wiss., Vol. 286, Springer-Verlag, 1987.
2. A. Arenas, *On integral representations by quadratic forms*, Linear and Multilinear Alg. **22** (1987), 149-160.
3. B.J. Birch, *Forms in many variables*, Proc. Roy. Soc. London, Series A **265** (1962), 245-263.
4. E. Freitag, *Siegelsche Modulfunktionen*, Grundlehren Math. Wiss., Vol. 254, Springer-Verlag, 1983.
5. K.F. Gauss, *Disquisitiones arithmeticae (translated by A. A. Clarke, S.J.)*, Yale Univ. Press, 1966.

6. J.L. Hafner and L.H. Walling, *Indefinite quadratic forms and Eisenstein series*, Forum Math. **11** (1999), 313-348.
7. B.W. Jones, *Representations by quadratic forms*, Annals of Math. **50 no. 4** (1949), 884-899.
8. O.T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren Math. Wiss., Vol. 117, Springer-Verlag, 1973.
9. G. Pall, *Representations by quadratic forms*, Canadian J. Math. **1** (1949), 344-364.
10. C.L. Siegel, *Indefinite quadratische Formen und Funktionentheorie. I.*, math. Ann. **124** (1951), 17-54.
10. V.G. Zhuravlev, *Deformations of quadratic Diophantine systems*, Izv. Ross. Akad. Nauk Ser. Mat. **65** (2001), 15-56.

L.H. Walling, Department of Mathematics, University of Bristol, Bristol BS8 1TW, England
E-mail address: l.walling@bristol.ac.uk