P. Feit
Nagoya Math. J.
Vol. 113 (1989), 37–87

EXPLICIT FORMULAS FOR LOCAL FACTORS IN THE EULER PRODUCTS FOR EISENSTEIN SERIES[1)]

PAUL FEIT

Introduction

Our objective is to prove that certain Dirichlet series (in our variable q^{-s}), which are defined by infinite sums, can be expressed as a product of an explicit rational function in q^{-s} times an unknown polynomial M in q^{-s}. Moreover we show that $M(q^{-s})$ is 1 if a simple condition is met. The Dirichlet series appear in the Euler products of Fourier coefficients for Eisenstein series. The series discussed below generalize the functions $\alpha_0(N, q^{-s})$ used by Shimura in [12], and the theorem is an extension of Kitaoka's result [5].

The paper is formulated in the language of formal Dirichlet series and local algebras, although the motivation comes from the study of Eisenstein series. The author has been studying automorphic forms on a "unitary" group G defined with respect to a totally real field F, a finite dimensional division F-algebra Δ, and an involution ρ of Δ such that F is the fixed field of ρ restricted to the center of Δ. The two seminal cases studied by Shimura in [12] are

(1.a) *Sp* Case: $\Delta = F$, $\rho = 1_F$, $G = Sp(m, F)$,

(1.b) *SU* Case: Δ/F is a totally imaginary extension field, ρ is Galois involution, $G = SU(m, m; \Delta)$.

Euler products naturally arise which are indexed by P, the set of primes of F. Moreover, the factor for $\mathfrak{p} \in P$ is an integral over the additive group of hermitian matrices in $\Delta_\mathfrak{p} = \Delta \otimes_F F_\mathfrak{p}$. When $\mathfrak{p}$ is finite, the integral can be naturally rewritten as a formal Dirichlet series in $N\mathfrak{p}^{-s}$. The series appearing in the cases (1.a, b) have been studied Shimura [12],

Received March 30, 1987.
Revised October 5, 1987.
[1)] The work on this paper was partially supported by NSF Grant DMS 8601130.

Kitaoka [5], and the present author [3]; if

(2.a) $\mathfrak{p} \nmid 2$ *Sp* Case,

(2.b) $\mathfrak{p}$ is unramified in Δ/F *SU* Case,

then the series is characterized as an explicit rational function in $N\mathfrak{p}^{-s}$ times a polynomial in $N\mathfrak{p}^{-s}$ which generalizes the classical σ-functions. Kitaoka also proves the same result in the *Sp* Case when $p = 2$ and $F = \boldsymbol{Q}$. For more general Δ, the existing theory easily extends to the cases when $\Delta_\mathfrak{p}$ is a matrix algebra over $F_\mathfrak{p}$, over $F_\mathfrak{p} \oplus F_\mathfrak{p}$, or over an unramified extension field of $F_\mathfrak{p}$. Our present objective is to prove the same sort of characterization for every finite prime. It suffices to handle the cases where $\Delta_\mathfrak{p}$ is a division algebra or is a sum of two division algebras. An immediate consequence of the present work is

THEOREM A. *Statements* [3; *Theorem* 9.1] *and* [3; *Theorem* 9.2] *are true when the level* $\mathfrak{b}$ *is* any *proper ideal.*

The statements in [3] involve many definitions and are omitted. In a later paper, we will give an analogous theorem at level 1 ($\mathfrak{b} = R$).

Part I looks at a class of formal Dirichlet series which includes the series arising when $\Delta_\mathfrak{p} = \Delta_0 \oplus \Delta_1$ is a sum of two algebras. In this case, the space of hermitian matrices is naturally identified with matrices over Δ_0. We consider constructions based on spaces of (possibly non-square) matrices over a local division algebra.

Part II deals with the much more interesting situation when $\Delta (\equiv \Delta_\mathfrak{p})$ is a division algebra. The main theorems are stated in Section 5. Siegel computed Fourier coefficients of Eisenstein series of large weight k for groups $Sp(m, \boldsymbol{Q})$ by relating certain infinite sums to a counting problem. The Fourier expansion of an automorphic form on $Sp(m, \boldsymbol{Q})$ is naturally indexed by the set L of half-integral symmetric matrices; for $h \in L$, the corresponding coefficient of an Eisenstein series is a limit as $n \mapsto \infty$ of quantities involving the number of solutions to the equation $TH_{2k}^{\mathbf{1}}{}^tT \equiv h \bmod (n)$ where H_{2k} is a hyperbolic half-integral matrix. When working adelically, we encounter local Dirichlet series instead of sums over integral matrices; however, the local series are also understood by relating them to a counting problem involving hermitian matrices over Δ. For $m \in \boldsymbol{Z}^+$, the group of additive character on $m \times m$ "(ρ, ε^ρ)-hermitian" matrices (defined below) which are 1 on "integral" matrices is identified

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

with an additive subgroup $\Sigma(m, S)^\sharp$ of $m \times m$ "(ρ, ε)-hermitian" matrices. (The group appears as a dual group of characters for a lattice $\Sigma(m, S)$.) The space $\Sigma(m, S)^\sharp$ plays the same role as the lattice of half-integral matrices in the classical theory; in fact, $\Sigma(m, S)^\sharp$ is the set of all hermitian matrices whose off-diagonal entries lie in one additive group $\mathscr{D}$ and whose diagonal entries lie in another group $\Sigma(1, S)^\sharp$. A critical technical fact is that $\Sigma(1, S)^\sharp = \{x + \varepsilon x^\rho : x \in \mathscr{D}\}$, which is proved as Corollary 9.2.1.

The structure of Part II is as follows: Section 6 develops a theory of "hermitian lattices" which closely parallels the classical theory of Z-lattices with inner products. "Modular" and "hyperbolic" hermitian lattices are defined, and a Witt Cancellation Theorem is proved for such lattices. Section 7 discusses the problem of counting the number of ways by which one hermitian lattice can be represented by another "mod $(\mathfrak{p}^n)$"-part of the problem is to give a usable definition of congruence modulo $\mathfrak{p}^n$. Much of this section could be simplified if Corollary 9.2.1 could be proved by a new argument; in our present work, we use the generalized theory to prove the corollary. Section 7 reduces the counting problem to the computation of certain numbers $|P(L, M)|$, which are studied in detail in Section 8. These technical quantities play the same role as that of the orders of the orthogonal groups of quadratic spaces over finite fields in Kitaoka's work [5, 6]. In Section 8, all modular lattices are classified up to form-preserving isomorphism. Section 9 combines the theory of hermitian lattices with some formal power series manipulation to prove the desired theorems.

The arguments in Part II are very general—they do not depend on whether Δ is commutative or not, whether ρ is of the first or second kind, whether hermitian or anti-hermitian matrices are considered, etc.. Unfortunately, the general formulation requires a deluge of notation. Occasionally, the same variable is used for different quantities in Part I and Part II; however, as neither Part depends upon the other, there should be no confusion. At the end of this introduction is a list of terms with the locations of their respective definitions.

Our formulation is purely local. We are primarily interested in local fields of characteristic 0, but the arguments apply to finite characteristics as well.

NOTATIONS.

$[x]$	§0.A	(ρ, ε)-hermitian	§0.B Definition 6.1
χ	non-trivial additive character–see after (1.7)	hyperbolic	
		$I_{r,k}$	(2.1)
		$\iota(C)$	(7.5)
$A(M, N; m)$	(7.10)	$j(T)$	(1.5, 6, 7)
$\alpha(N, t)$	(5.10)	$j_n(T)$	(9.2)
$b(E, s)$	(2.2)	l	logarithmic valuation of Δ–see start of §5
$B(E, s)$	(2.2)		
c.i.r.	§0.A		
$\mathscr{D}$	(5.5)	lattice	§0.C
$\mathscr{D}_n$	(9.1)	$\Lambda_{n,k}$	(8.6)
Δ	finite dimensional division F-algebra	$\mathfrak{m}$	maximal ideal of S
		$M'_{r,k+r}$	(3.1)
$\Delta(m)$	(5.5)	M'_k	$M'_{k,2k}$
$\Delta(\delta, r)$	after (7.2)	$M'_{r,k+r;pr}$	(3.1)
$\Delta_\iota, \Delta_\iota^m$	(5.7)	$M'_{k;pr}$	$M'_{k,2k;pr}$
ε	central S-unit for which $\varepsilon\varepsilon^\rho = 1$	$M_{r,k}(\Delta/S)$	(3.1)
		$M_k(\Delta/S)$	$M_{k,k}(\Delta/S)$
$E(r)$	(7.2)	mod (n)	modulo p^n–see before (1.8)
F	local field		
Φ_m	(2.3)	modular	Definition 6.2

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

η	Theorem 8.5.D or Definition 5.1	σ_2	(5.9), *except* in §8, where it is given by (8.5)
$\nu(T)$	(1.2), (1.7)		
$\nu_1(C)$	Definition 7.1	$\sigma_3, \sigma_4, \sigma_5$	(5.9)
$\mathfrak{p}$	maximal ideal of R	$\Sigma(m, \varepsilon), \Sigma(m, S)$	(5.3)
π	generator of $\mathfrak{m}$	$\Sigma(m, S)^\#$	(5.3)
π_0	generator of $\mathfrak{p}$	$\Sigma(r; n), \Sigma(r; n)^\#$	(9.1)
$P(M, N; m)$	(7.10)	t	σ/σ_3 in §8, indeterminate in §9
primitive	§0.A		
q	$\lvert R/\mathfrak{p}\rvert$	$\tau(T)$	(1.5)
q_0	$\lvert S/\mathfrak{m}\rvert$	tr	§0.D
R	integer ring of F	Type I~IV	Definition 8.2
$R(D)$	(5.6)	U_m	(2.3)
$s(L)$	scale (6.5)	Ω_k	(8.19)
S	maximal order of Δ	$\Omega(D)$	(5.6)
$S(\varepsilon)$	(5.5)	X	In §3 and §4, function defined after (3.2)
σ	determined by $q_0 = q^\sigma$		
σ_1	(5.8)		

§ 0. Notation and conventions

§ 0.A. Basics

Let $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, and $\boldsymbol{C}$ denote the ring of integers and the rational, real, and complex number fields, respectively. Let $\boldsymbol{R}^+$ be the set of positive real numbers and put $\boldsymbol{Z}^+ = \boldsymbol{Z} \cap \boldsymbol{R}^+$. We use the symbols $\sum$ and $\prod$ with the convention that for $n \in \boldsymbol{Z}$, any sum indexed by $\sum_n^{n-1}$ is 0 and any product $\prod_n^{n-1}$ is 1. (In Section 9, we actually have formulas which can specialize to products $\prod_n^{n-2}$, but these will *not* be interpreted as being 1.)

Our arguments involve counting over quotient spaces. Let X be a set and let $\sim$ be an equivalence relation on X. We say that W is a c.i.r. set for $X/\sim$ (or $\sim\backslash X$) if $W \subseteq X$ is a complete set of irredundant representatives for $X/\sim$ (or $\sim\backslash X$). If $x \in X$, the class of x is denoted by $[x]$. We sometimes write "$x \in X/\sim$" to mean that x varies over a c.i.r. set for $X/\sim$.

Let S be a (possibly non-commutative) ring. For $r, k \in \boldsymbol{Z}^+$, let $M_{r,k}(S)$ denote the space of $r \times k$ matrices of S, $M_k(S) = M_{k,k}(S)$, and $GL_k(S)$ denote the invertible $k \times k$ matrices. For $r, k \in \boldsymbol{Z}^+$ and $T \in M_{r,k}(S)$, and

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

we say that T is primitive if

(0.1.a) $k = r$ and T is invertible,

(0.1.b) $k > r$ and there exists $U \in M_{k-r,k}(S)$ such that $\begin{pmatrix} U \\ T \end{pmatrix}$ is invertible,

(0.1.c) $k < r$ and there exists $U \in M_{r,r-k}(S)$ such that (UT) is invertible.

we say that an element e_1 of a (left) S-module M is primitive if there exist $e_2, \cdots, e_m \in M$ such that $e_1, \cdots, e_m$ form an S-basis of M.

By module, we mean left module. Each ring S which we study has the property that if $m, n \in Z^+$ and $S^m \approx S^n$ as left S-modules, then $m = n$. Thus, if an S-module M is isomorphic to S^m for some $m \in Z^+$, we say m is $\mathrm{rk}_S(M)$ the rank of M with respect to S. If $f: M \to N$ is a homomorphism of free S-modules of finite rank, then we say f is primitive if its matrix representation over any choice of bases is primitive.

§ 0.B. Involutions and hermitian spaces

Let S be a (possibly non-commutative) ring. An involution on S is an anti-isomorphism $\rho: S \to S$ such that $\rho^2 = 1_S$. If T is a matrix, we let T^ρ denote the matrix generated by applying ρ to each entry of T; we also define the image of $a \in S$ under ρ by a^ρ. For a fixed involution, we use the notation

$$T^* = ({}^tT)^\rho = {}^t(T^\rho)\,, \tag{0.2}$$

where ${}^tT$ is the transpose of T. If T is invertible, we put $T^{-*} = (T^*)^{-1} = (T^{-1})^*$.

Our arguments require a variation of the usual hermitian space. Let Δ be a ring, S a subring, ρ an involution on Δ which maps S bijectively to S, and ε an element in the center of S such that $\varepsilon\varepsilon^\rho = 1$. We define a (ρ, ε)-hermitian module with respect to Δ/S to be a left S-module M with a biadditive function $(,): M \times M \to \Delta$ such that

(0.3.a) $\forall\, a, b \in S,\ \forall\, x, y \in M,\ (ax, by) = a(x, y)b^\rho$,

(0.3.b) $\forall\, x, y \in M,\ (x, y) = \varepsilon(y, x)^\rho$.

The map $(,)$ is also called the form of M. We usually work with a fixed choice of ρ, ε, S and Δ, when the context is clear, we refer to any such module as a hermitian module (or hermitian lattice–see below). Note that the classical "anti" hermitian case occurs when $\varepsilon = -1$.

If u is another member of the center of S for which $uu^\rho = 1$, we say u and ε are equivalent if there is a central S-unit such that $u = (\varepsilon c)/c^\rho$.

Clearly we may replace ε with any equivalent element without affecting the theory of hermitian modules.

If M is a (ρ, ε)-hermitian module defined with respect to Δ/S and $N \subseteq M$, define the orthogonal complement by

$$N^{\perp} = \{x \in M;\ (x, N) = \{0\}\}\,. \tag{0.4}$$

We say M is trivial if $M^{\perp} = M$.

§ 0.C. Orders and lattices

Let R be a Dedekind domain, F the field of fractions of R, and Δ a finite dimensional semisimple F-algebra. An order of Δ is a subring S such that S is a finitely generated R-module and $FS = \Delta$. A maximal order is an order which is not properly contained in another order. For S an order, an S-lattice is a finitely generated S-module with no R-torsion; if V is a Δ-module, then an S-lattice of V is an S-submodule $M \subseteq V$ which is an S-lattice and satisfies $FM = V$. When dealing with hermitian modules in this context, we define a hermitian lattice to be a hermitian module whose underlying module is an S-lattice.

Basic properties of matrices over a maximal order of a local semi-simple algebra are listed in [3; Section 2].

§ 0.D. Reduced trace

Let Δ be a finite dimensional semi-simple algebra over a field F. Express $\Delta = \oplus_{j=1}^{t} \Delta_j$ where each Δ_j is simple, and let K_j be the center of Δ_j. Define the reduced trace of $a = \oplus a_j \in \Delta$ to be $\mathrm{tr}(a) = \sum_j \mathrm{tr}_j(a_j)$ where tr_j is the composition of the reduced trace of $\Delta_j \to K_j$ with the field-theoretic trace $K_j \to F$.

§ 1. The standing hypothesis

For the rest of this paper, we let F be a local field (of any characteristic), R the integer ring of F, $\mathfrak{p}$ the maximal ideal of R, Δ a finite dimensional division algebra over F, S the maximal order of Δ, and $\mathfrak{m}$ the maximal ideal of S. (By "local", we mean local and non-archimedian; we do *not* include $F \in \{\boldsymbol{R}, \boldsymbol{C}\}$.) Put

$$q = |R/\mathfrak{p}| \quad \text{and} \quad q_0 = |S/\mathfrak{m}|\,. \tag{1.1}$$

In Part I, we require that F be the center of Δ; however, in Part II,

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

there are important situations in which F can *not* be the center of Δ.

For convenience, we make our next definitions for a family of rings. Let A be a finitely dimensional semi-simple F-algebra, and let B be a maximal order of A. For $n \in Z^+$, we denote $M_{1,n}(B)$ and $M_{n,1}(B)$ by B^n when context makes clear which is meant. Define a function $\nu(T)$ for $T \in M_n(B)$ by the property that

$$q^{\nu(T)} = [B^n\colon TB^n] = [B^n\colon B^nT]\,, \tag{1.2}$$

with the convention that $\nu(T) = \infty$ if $T \notin GL_n(A)$. The restriction of ν to $GL_n(\Delta) \cap M_n(S)$ has a unique extension to a group homomorphism $GL_n(\Delta) \to Z$, and we denote this extension by ν as well. The ν function plays the role of logarithmic determinant or reduced norm; its basic properties are stated in [3; Section 2].

For $r, k \in Z^+$, define

$$\begin{aligned} G_{r,k} &= GL_{k+r}(A), \\ P_{r,k} &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G_{r,k}\colon\ a \in M_k(A)\ \ d \in M_r(A),\ \ b \in M_{k,r}(A) \right\}, \\ C_{r,k} &= GL_{k+r}(B), \\ \eta_{r,k} &= \begin{bmatrix} 0 & 1_r \\ 1_k & 0 \end{bmatrix}. \end{aligned} \tag{1.3}$$

We signify the analogous constructions defined with respect to the opposite ring of A by the superscript "0". The standard Iwasawa decomposition for $G_{r,k}$ implies that

$$G_{r,k} = P_{r,k} \cdot C_{r,k}\,. \tag{1.4}$$

If $T \in M_{r,k}(A)$, define $\tau(T)$ and $j(T)$ by the properties that

$$\begin{aligned} &\tau(T) = \begin{bmatrix} 1_k & 0 \\ T & 1_r \end{bmatrix} \in G_{r,k}, \\ &j(T) = \nu(d) \qquad \text{if } \tau(T) = y\omega \text{ where } y \in P_{r,k},\ \omega \in C_{r,k}, \\ &\qquad\qquad \text{and } \omega = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \text{ for } d \in M_r(B). \end{aligned} \tag{1.5}$$

If y, ω, c and d are as in (1.5), then $(c\ d)$ is primitive and

$$B^r = cB^k + dB^r \tag{1.6}$$

$$\Longrightarrow \qquad j(T) = [B^r\colon dB^r] = [cB^k + dB^r\colon dB^r] = [TB^k + B^r\colon B^r].$$

The function $g \mapsto \eta^0_{r,k}({}^t g^0)^{-1}(\eta^0_{r,k})^{-1}$ is a group isomorphism $G_{r,k} \to G^0_{r,k}$ which

sends $C_{r,k} \to C^0_{r,k}$, $\tau(T) \mapsto \tau(-{}^tT^0)$, and $P_{r,k} \to P^0_{k,r}$. It follows that

LEMMA 1.1. *Let A and B be as above. Let $r, k \in Z^+$ and $T \in M_{r,k}(A)$.*
(A) *$j(\alpha T\beta) = j(T)$ for $\alpha \in GL_r(B)$ and $\beta \in GL_k(B)$,*
(B) *$j({}^tT^0) = j(T)$,*
(C) *$j(T)$ factors to a function on $M_{r,k}(A)/M_{r,k}(B)$ (where the quotient refers to the additive structure of $M_{r,k}(A)$).*

We denote the factored map of Lemma 1.1.C by j as well. We write $\nu[A, B]$ and $j[A, B]$ to emphasize the ring and order.

(1.7) CONVENTION. $j = j[\Delta, S]$ and $\nu = \nu[\Delta, s]$ unless explicitly stated otherwise.

Let χ be a fixed non-trivial character of the additive group of F. For $n \in Z^+$, extend χ to $T \in M_n(\Delta)$ by $\chi(T) = \chi(\mathrm{tr}(T))$ where $\mathrm{tr}: M_n(\Delta) \to F$ is the reduced trace function. Our objective is to find the Fourier expansion of the function $T \mapsto q^{j(T)s}$ (where s is a formal complex variable) restricted to certain additive subgroups of $M_{r,k}(\Delta)/M_{r,k}(S)$. Using χ, we can identify the group of additive characters of such an additive subgroup D with an R-submodule of $M_n(\Delta)$. Our main interest is in the case where this "dual" submodule is *not* contained in $M_n(S)$.

We use a non-standard version of Hensel's Lemma, which we now state.

If L is an R-lattice and $n \in Z^+$, we let "$\mathrm{mod}(n)$" denote equivalence up to $\mathfrak{p}^nL$. We also refer to the class of $v \in L$ modulo $\mathfrak{p}^nL$ by "$v \mathrm{mod}(n)$". We use this notation even when L is an S-lattice. Fix π a generator of $\mathfrak{p}$.

Let L and M be R-lattices. A function $\theta: L \to M$ said to be polynomial if there are polynomials $p_1, \cdots, p_k \in R[X_1, \cdots, X_r]$ such that

$$\theta(x_1, \cdots, x_r) = (p_1(x_1, \cdots, x_r), \cdots, p_k(x_1, \cdots, x_r)) \tag{1.8}$$

with respect to the coordinates determined by a choice of basis $a_1, \cdots, a_r$ of L and $b_1, \cdots, b_k$ of M. For $T \in L$, let $d\theta_T \in \mathrm{Hom}_R(L, M)$ denote the linear part of θ with respect to a system of affine coordinates centered at T. In terms of the representation of θ using coordinates as in (1.8), the d-th coordinate of $\theta_T(x_1, \cdots, x_r)$ is $\sum_{i=1}^r (\partial p_d/\partial x_i|_{x=T} \cdot x_i$. Let $d\theta$ denote the construction $T \to d\theta_T$ from $L \to \mathrm{Hom}_R(L, M)$, and then the map $d\theta$ is also polynomial.

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Fix a polynomial function $\theta\colon L \to M$. Put

$$o(T) = \{n \in \mathbf{Z}\colon \mathfrak{p}^n M \subseteq d\theta_T(L)\} \qquad \text{for } T \in L, \tag{1.9}$$
$$L(n, T) = d\theta_T^{-1}(\mathfrak{p}^n M) \qquad \text{for } T \in L \text{ and } n \in o(T).$$

Suppose that $T \in L$ and $n \in o(T)$. Note that if $o(T) \neq \varnothing$, then $\operatorname{rk} L \leq \operatorname{rk} M$. If $m > n$ and $U \in T + \mathfrak{p}^m L$, then $d\theta_U \in d\theta_T + \mathfrak{p}^m \operatorname{Hom}_R(L, M)$, and consequently

$$n \in o(U) \quad \text{and} \quad L(n, T) = L(n, U). \tag{1.10}$$

It follows that for $m \in \mathbf{Z}^+$ and $T_0 \in L/\mathfrak{p}^m L$, there is a set $o(T_0)$ and an indexed family of lattices $\{L(n, T_0)\colon n \in o(T_0)\}$ with the property that

$$o(T_0) = \{n \in o(T)\colon n < m\}, \quad \forall\, n \in o(T_0), \quad L(n, T_0) = L(n, T) \tag{1.11}$$

for each $T \in L$ such that $T_0 = T + \mathfrak{p}^m L$.

Let $T \in L$ and $n \in o(T)$. For $m \geq 2n + 1$, we have

$$\mathfrak{p}^m L \subseteq \mathfrak{p}^{m-n} L(n, T) \subseteq \mathfrak{p}^{n+1} L. \tag{1.12}$$

Suppose $U \in L$ so that $U \equiv T \bmod (n + 1)$. For $v \in L$,

$$\theta(U + \pi^{m-n} v) = \theta(U) + \pi^{m-n} d\theta_U(v) + \pi^{2m-2n} E(U, v) \tag{1.13}$$

for a polynomial E,

$$\Longrightarrow \qquad \theta(U + \pi^{m-n} v) \equiv \theta(U) + \pi^{m-n} d\theta_U(v) \bmod (m).$$

If $\theta(U) \equiv C \bmod (m)$, then $\theta(U') \equiv C \bmod (m)$ for every $U' \equiv U \bmod (\mathfrak{p}^{m-n} \cdot L(n, T))$. Hence, θ factors to $L/\mathfrak{p}^{m-n} L(n, T) \to M/\mathfrak{p}^m M$, and we also denote the factored map by θ.

The standard proof for Hensel's Lemma can be adjusted to yield

THEOREM 1.2. *Let L and M be R-lattices and let $\theta\colon L \to M$ be a polynomial function, $T \in L$ and $n \in o(T)$. For $m \geq 2n + 1$, define*

$$W(n, T; m) \tag{1.14}$$
$$= \{U \in L/\mathfrak{p}^{m-n} L(n, T)\colon U \equiv T \bmod (n + 1) \text{ and } \theta(U) \equiv 0 \bmod (m)\}.$$

Let $m \geq 2n + 1$, and suppose that $U_0 \in W(n, T; m)$. Then there is $U \in L$ such that $\theta(U) = 0$ and $U \equiv U_0 \bmod (\mathfrak{p}^{m-n} L(n, T))$. Moreover, for $a \in \mathbf{Z}^+$

$$|\{U_1 \in W(n, T; m + a)\colon U_1 \equiv U_0 \bmod (\mathfrak{p}^{m-n} L(n, T))\}| = q^{a(\operatorname{rk}(L) - \operatorname{rk}(M))}. \tag{1.15}$$

(where rk *means* rk_R*).* □

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

An easy consequence is the weaker

COROLLARY 1.2.1. *Let L and M be R-lattices and let $\theta\colon L \to M$ be a polynomial function. Let $D_0 \subseteq L/\mathfrak{p}L$ and $D_1 = \{T \in L\colon T \bmod (1) \in D_0\}$. For $m \geq 1$, put*

$$P(\theta, m) = \{T \in L/\mathfrak{p}^m L\colon \theta(T) \equiv 0 \bmod (m) \text{ and } T \in D_1\}. \tag{1.16}$$

Suppose that $n \in \boldsymbol{Z}^+$ such that $\mathfrak{p}^n M \subseteq d\theta_T(L)$ for each $T \in D_1$. Then for $m \geq 2n+1$ and $a \in \boldsymbol{Z}^+$,

$$|P(\theta,\ m+a)| = q^{a(\mathrm{rk}(L)-\mathrm{rk}(M))}|P(\theta, m)|, \tag{1.17}$$

where rk *means* rk_R. *Also, if $T_0 \in P(\theta, m)$ then there is $T \in D_1$ such that $\theta(T) = 0$ and $T \equiv T_0 \bmod (m-n)$.*

Proof. Trivial. □

PART I

In Part, I, we make the standing assumption that F is the center of Δ.

§ 2. Statement of theorems for Part I

For $r, k \in \boldsymbol{Z}^+$, put

$$I_{r,k} = \{E \in M_{k,r}(\Delta)\colon \chi(M_{r,k}(S)E) = \{1\}\}. \tag{2.1}$$

Fix $\delta \in \Delta^*$ such that δ^{-1} is a generator of the fractional S-ideal $I_{1,1}$. Then $I_{r,k} = \delta^{-1}M_{k,r}(S)$ is an S-lattice, and $E \mapsto (\theta\colon T \mapsto \chi(TE))$ is an isomorphism from $I_{r,k}$ to the group of additive characters of $M_{r,k}(\Delta)/M_{r,k}(S)$.

We consider the Dirichlet series

$$b(E, s) = \sum_{T \in M_{r,k}(\Delta)/M_{r,k}(S)} q^{-j(T)s}\chi(ET) \tag{2.2}$$

where $E \in \delta^{-1}M_{k,r}(S)$ and s is a (formal) complex variable. The series corresponds to a Fourier coefficient of the function $q^{-j(T)s}$ on $M_{r,k}(\Delta)/M_{r,k}(S)$. We regard $b(E, s)$ and all subsequent series as formal power series, and we do not consider questions of convergence. (We remark in Section 3 that the summation properly defines a formal series.)

It is convenient to make

DEFINITION 2.1. For $m \in \boldsymbol{Z}^+$, put

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$$U_m = GL_m(S), \qquad \Phi_m = GL_m(\Delta) \cap M_m(S). \tag{2.3}$$

Let U_m act on Φ_m by left multiplication. For $E \in \Phi_m$, define a polynomial in $Z[t]$ by

$$p(E, t) = \sum_{\{D \in \cup_m \backslash \Phi_m : E D^{-1} \in \Phi_m\}} t^{\nu(D)}. \tag{2.4}$$

The indexing set is clearly finite.

THEOREM 2.1. *Let F be a local (non-archimedian) field of any characteristic and let Δ be a finite dimensional central division F-algebra. Let $\sigma \in Z^+$ so that $q_0 = q^\sigma$; all other parameters are as in* §0, §1 *and* §2 *above.*

(A) If $r, k \in Z^+$ and $E \in \delta^{-1} M_{k,r}(S)$, then $b({}^tE^0, s) = b(E, s)$ (where $b({}^tE^0, s)$ is defined with respect to the opposite algebra of Δ).

(B) Let $r, k \in Z^+$ so that $k \geq r$, and let $0_{r,k}$ denote the $k \times r$ zero matrix. Then

$$b(0_{r,k}, s) = \frac{\prod_{j=1}^{r} (1 - q^{\sigma(j-1-s)})}{\prod_{j=1}^{r} (1 - q^{\sigma(k+j-1-s)})}. \tag{2.5}$$

(C) Suppose $m, r, k \in Z^+$ such that $k \geq r \geq m$, and suppose $E' \in \delta^{-1} \cdot M_{k,r}(S)$ so that $\beta E' \alpha$ has the form $\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$ for some $\alpha \in GL_r(S)$, $\beta \in GL_k(S)$, and $E \in GL_m(\Delta) \cap \delta^{-1} M_m(S)$. Then

$$b(E', s) = \frac{\prod_{j=1}^{r} (1 - q^{\sigma(j-1-s)})}{\prod_{j=1}^{r-m} (1 - q^{\sigma(k+j-1-s)})} p(\delta E, q^{k+r-m-s}). \tag{2.6}$$

If the reduced norm of δE is an R-unit, then $p(\delta E, t) = 1$.

The remainder of Part I consist of the proof of Theorem 2.1. Lemma 1.1 already implies that $b(E, s) = b({}^tE^0, s)$ and that $b(E, s) = b(\beta E \alpha, s)$ for $\beta \in GL_k(S)$ and $\alpha \in GL_r(S)$.

An easy consequence of Theorem 2.1 is

COROLLARY 2.1.1. *Let F and Δ be as in Theorem* 2.1. *Let $A = A_1 \times A_2$ be a product of finite-dimensional F-algebras, B a maximal order of A, and ρ an involution of A which induces a bijection $A_1 \times \{0\} \to \{0\} \times A_2$. Suppose γ: $A_1 \to M_n(\Delta)$ is an isomorphism of F-algebras for some $n \in Z^+$, and that $\gamma(B \cap A_1) = M_n(S)$. In general, we let γ denote the morphism $M_m(A) \to M_{mn}(\Delta)$ which expands the (i, j)-entry to the image under projections $A \to A_1 \to M_n(\Delta)$.*

Let ε and u be a central B-units such that $\varepsilon\varepsilon^\rho = 1$, $uu^\rho = 1$ and $\varepsilon u \neq$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

-1. *Put* $j = j[A, B]$. *For* $m \in \boldsymbol{Z}^+$, *put* $\chi_0 = \chi \circ tr$ *on* $M_m(A)$, *and define*

$$\begin{aligned} \Sigma(m, \varepsilon) &= \{T \in M_m(A)\colon\ T = \varepsilon^t T^\rho\}\,, \\ \Sigma(m, u) &= \{T \in M_m(A)\colon\ T = u_t T^\rho\}\,, \\ \Sigma(m, B) &= \Sigma(m, \varepsilon) \cap M_m(B)\,, \\ \Sigma(m, B)^\# &= \{E \in \Sigma(m, u)\colon\ \chi_0(E \cdot \Sigma(m, B)) = \{1\}\}\,. \end{aligned} \tag{2.7}$$

Then for each $E \in \Sigma(m, B)^\#$ *and* s *a formal variable,*

$$\sum_{\Sigma(m,\varepsilon)/\Sigma(m,B)} \chi_0(ET) q^{-j(T)s} = b(\gamma((1 + \varepsilon u)^{-1}E),\ 2ns)\,, \tag{2.8}$$

where the quotient $\Sigma(m)/\Sigma(m, B)$ *is taken with respect to addition.*

§ 3. Auxiliary series

Fix $r, k \in \boldsymbol{Z}^+$, $k \geq r$. When we express $T = (C\ D)$ and $T = (C_1\ C_2\ D)$ for $T \in M_{r,k+r}(\Delta)$, we assume that C, D, C_1 and C_2 are the corresponding submatrix blocks of size $r \times k$, $r \times r$, $r \times r$ and $r \times (k - r)$, respectively. Put

$$\begin{aligned} M'_{r,k+r} &= \{(C\ D) \in M_{r,k+r}(S)\colon\ \nu(D) < \infty\}\,, \\ M'_{r,k+r;pr} &= \{T \in M'_{r,k}\colon\ T \text{ is primitive over } S\}\,, \\ M_{r,k}(\Delta/S) &= M_{r,k}(\Delta)/M_{r,k}(S)\,. \end{aligned} \tag{3.1}$$

The multiplicative group U_r acts on $M'_{r,k+r}$ by left multiplication, and the additive group $M_{r,k}(S)$ acts on the right of $M'_{r,k+r}$ by

$$\forall\, a \in M_{r,k}(S), \quad \forall\, T \in M'_{r,k+r}, \quad T \cdot a = T \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}. \tag{3.2}$$

Let "$\sim$" denote equivalence up to left U_r-action *and* right $M_{r,k}(S)$ action. The actions preserve the subset $M'_{r,k+r;pr}$. Denote the class of $(C\ D) \in M'_{r,k+r}$ by $[C\ D]$. Let $X\colon\ U_r \backslash M'_{r,k+r} / M_{r,k}(S) \to M_{r,k}(\Delta/S)$ be the function $X([C\ D]) = [D^{-1}C]$.

We analyze the series (2.2), which is indexed by $M_{r,k}(\Delta/S)$, by re-indexing it in terms of the double coset space.

Lemma 3.1. *In the present notation.*

(A) *X restricts to a bijection* $U_r \backslash M'_{r,k+r;pr} / M_{r,k}(S) \rightleftarrows M_{r,k}(\Delta/S)$.

(B) *If* $(c\ d) \in M'_{r,k+r;pr}$, *then* $j(X[c\ d])) = \nu(d)$.

(C) *Let W be a c.i.r. set for* $U_r \backslash \Phi_r$, *and let* $(c\ d) \in M'_{r,k+r;pr}$. *Then* $\{(\alpha c\ \alpha d)\colon\ \alpha \in W\}$ *is a c.i.r. set for the* $X^{-1}([d^{-1}c])$.

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Proof. As noted in (1.5), for $T \in L$ there is at least one $(c\ d) \in M'_{r,k+r;pr}$ such that $X([c\ d]) = T$ and $j(T) = \nu(d)$; surjectivity in (A) and statement (B) follows immediately.

We prove injectivity in (A) and statement (C) together. Fix W a c.i.r. set for $U_r \backslash \Phi_r$, and $(c\ d) \in M'_{r,k+r;pr}$. Put $T = d^{-1}c$. For $\alpha \in W$, $(\alpha c\ \alpha d) \in M'_{r,k+r}$ and $X([\alpha c\ \alpha d]) = [T]$. Suppose first that $\alpha, \beta \in W$ so that $[\alpha c\ \alpha d] = [\beta c\ \beta d]$. There exist $u \in U_r$ and $t \in M_{r,k}(S)$ such that $u(\alpha c\ \alpha d)\tau(t) = (\beta c\ \beta d)$. Then $d \in GL_r(\Delta)$ and $u\alpha d = \beta d$. But then $u\alpha = \beta$, and the hypothesis on W implies that $\alpha = \beta$.

Suppose that $(C\ D) \in M'_{r,k+r}$ and $X([C\ D]) = [T]$. Let $t = T - D^{-1}C \in M_{r,k}(S)$. There exist matrices A, B over Δ and a, b over S for which $N = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_{k+r}(\Delta)$ and $\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_{k+r}(S)$. Express $N = yw$ where $y \in P_{r,k}$ and $w \in GL_{k+r}(S)$. The bottom r rows of $w\tau(t)$ and ω each have the form $z(T\ 1)$ for some $z \in GL_r(\Delta)$; hence, the bottom r rows of $w\tau(t)\omega^{-1}$ must have the form $(0\ v)$ for $v \in GL_r(\Delta)$. Since $w\tau(t)\omega^{-1} \in GL_{k+r}(S)$, we conclude that $v \in U_r$. Express $y = \begin{pmatrix} * & * \\ 0 & g \end{pmatrix}$ where $g \in GL_r(\Delta)$. Now $y = Nw^{-1}$ where the last r rows of N have entries in S; thus, $g \in \Phi_r$. We have shown that

$$g^{-1}(C\ D) = v(c\ d)\tau(-t)\,. \tag{3.3}$$

Hence $[C\ D] = [\alpha c\ \alpha d]$ where α represents the U_r-coset of $gv \in \Phi_r$. The proof of statement (C) is now complete.

In the above paragraph, $(\alpha c\ \alpha d)$ is primitive if and only if $\alpha \in U_r$. There is exactly one $\alpha \in W \cap U_r$, which shows that X sends a unique coset of $U_r \backslash M'_{r,k+r;pr}/M_{r,k}(S)$ to $[T]$. Thus, the restriction in (A) is injective. □

We assume the standard fact that

$$\sum_{D \in U_r \backslash \Phi_r} q^{-\nu(D)s} = \prod_{j=1}^{r} (1 - q_0^{j-1-s})^{-1}\,. \tag{3.4}$$

For $M \in \boldsymbol{Z}^+$, the number of double cosets $[C\ D]$ in $U_r \backslash M'_{r,k+r}/M_{r,k}(S)$ such that $\nu(D) \leq M$ is finite. Hence, we are justified in defining

DEFINITION 3.1. Let $r, k \in \boldsymbol{Z}^+$ and $E \in \delta^{-1}M_{k,r}(S)$. The summations

$$\begin{aligned} B(E, s) &= \sum_{(C\ D) \in U_r \backslash M'_{r,k+r}/M_{r,k}(S)} q^{-\nu(D)s}\chi(D^{-1}CE)\,, \\ b(E, s) &= \sum_{T \in M_{r,k}(\Delta/S)} q^{-j(T)s}\chi(TE)\,, \end{aligned} \tag{3.5}$$

determine formal Dirichlet series, and

$$B(E, s) = \prod_{j=1}^{r} (1 - q_0^{j-1-s})^{-1} b(E, s) . \tag{3.6}$$

Equation (3.6) follows by identifying $M_{r,k}(\Delta/S)$ with $U_r \backslash M'_{r,k+r;pr}/M_{r,k}(S)$ under X. Fix c.i.r. sets W and Z for $U_r \backslash \Phi_r$ and $U_r \backslash M'_{r,k+r;pr}/M_{r,k}(S)$ respectively, and identify $W \times Z$ with $U_r \backslash M'_{r,k+r}/M_{r,k}(S)$ under the map $(\tau, (c\ d)) \mapsto (\tau c\ \tau d)$. Note that this indexing of $U_r \backslash M'_{r,k+r}/M_{r,k}(S)$ depends on the choice of representatives in Z.

The series $B(E, s)$ is surprisingly easy to manipulate. We have an immediate reduction of the problem to the square matrix case.

THEOREM 3.2 (Reduction I). *Let $r, k \in \boldsymbol{Z}^+$ and assume $k > r$. Let $E \in \delta^{-1} M_r(S)$. Then*

$$B\left(\begin{pmatrix} E \\ 0 \end{pmatrix}, s\right) = B(E, s + r - k) , \tag{3.7}$$

where 0 is the $(k - r) \times r$ zero matrix.

Proof. For $D \in \Phi_r$, put

$$V(D) = M_{r,k-r}(S)/DM_{r,k-r}(S) . \tag{3.8}$$

Let W be a c.i.r. set for $U_r \backslash M'_{r,2r}/M_r(S)$, and to each $(C_1\ D) \in W$ assign an c.i.r. set $J(D)$ for $V(D)$. Then $\{(C_1 C_2 D)\colon (C_1\ D) \in W, C_2 \in J(D)\}$ is a c.i.r. set for $U_r \backslash M'_{r,k+r}/M_{r,k}(S)$ Now

$$|V(D)| = [S^r\colon DS^r]^{k-r} = q^{\nu(D)(k-r)} . \tag{3.9}$$

Hence,

$$\begin{aligned} B\left(\begin{pmatrix} E \\ 0 \end{pmatrix}, s\right) &= \sum_{(C_1 D) \in W} \sum_{C_2 \in J(D)} q^{-\nu(D)s} \chi(D^{-1} C_1 E) \\ &= \sum_{(C_1 D) \in W} q^{\nu(D)(k-r-s)} \chi(D^{-1} C_1 E) . \end{aligned} \tag{3.10}$$

□

§ 4. Square matrices

We consider the summation indexed by square matrices. For $k \in \boldsymbol{Z}^+$, put $M'_k = M'_{k,2k}$ and $M'_{k;pr} = M'_{k,2k:pr}$. We now prove

THEOREM 4.1 (Reduction II). *Let $k, m \in \boldsymbol{Z}^+$ so that $k > m$, For $E \in \delta^{-1} M_m(S)$,*

$$B\left(\begin{bmatrix} E & 0 \\ 0 & 0 \end{bmatrix}, s\right) = \left\{ \prod_{j=1}^{k-m} (1 - q_0^{k+j-1-s}) \right\}^{-1} B(E, s + 2m - 2k) \tag{4.1}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

where $\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$ *is a* $k \times k$ *matrix.*

Proof. When we express $T \in M_k(\Delta)$ as $T\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we mean that the submatrices a, b, c, and d have size $m \times m$, $m \times (k-m)$, $(k-m) \times m$ and $(k-m) \times (k-m)$, respectively.

Each coset of $U_k \backslash M_k' / M_k(S)$ can be represented by $(C\ D)$ where

$$C = \begin{bmatrix} C_1 & C_2 \\ C_3 & C_4 \end{bmatrix}, \qquad D = \begin{bmatrix} D_1 & 0 \\ D_3 & D_4 \end{bmatrix}. \tag{4.2}$$

Straightforward algebra shows that the cosets of $U_k \backslash M_k' / M_k(S)$ are indexed by letting submatrices vary over c.i.r. sets for the following spaces,

$$\begin{aligned} (C_1 D_1) &\in U_m \backslash M_m' / M_m(S)\,, \\ D_4 &\in U_{k-m} \backslash \Phi_{k-m}\,, \\ D_3 &\in M_{k-m,m}(S) / M_{k-m,m}(S) D_1\,, \\ C_2 &\in M_{m,k-m}(S) / D_1 M_{m,k-m}(S)\,, \\ C_3 &\in M_{k-m,m}(S) / D_4 M_{k-m,m}(S)\,, \\ C_4 &\in M_{k-m}(S) / D_4 M_{k-m}(S)\,, \end{aligned} \tag{4.3}$$

Note that the indexing process has a definite order—that is, certain variables must be fixed before others can be chosen. Counting as in (3.9), we find

$$\begin{aligned} B\left(\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}, s\right) &= \sum_{D_4 \in U_{k-m} \backslash \Phi_{k-m}} \sum_{(C_1 D_1) \in U_m \backslash B t_m / A_m} q^{2\nu(D_1)(k-m) + \nu(D_4)k - \nu(D)s} \chi(D_1^{-1} C_1 E) \\ &= \Big\{ \sum_{D_4 \in U_{k-m} \backslash \Phi_{k-m}} q^{\nu(D_4)(k-s)} \Big\} B(E, s + 2m - 2k)\,. \end{aligned} \tag{4.4}$$

□

Direct computation shows that

$$B(0_{1,1}, s) = \sum_{n=0}^{\infty} q_0^n q_0^{-ns} = (1 - q_0^{1-s})^{-1}\,. \tag{4.5}$$

The proof of Theorem 2.1 follows by calculation once we have

LEMMA 4.2 (Reduction III). *Let* $k \in Z^+$ *and* $E \in \delta^{-1} M_k(S) \cap GL_k(\Delta)$. *Then* $B(E, s) = p(\delta E, q^{k-s})$.

Proof, For $D \in \Phi_k$, put

$$V(D) = M_k(S) / D \cdot M_k(S)\,. \tag{4.6}$$

The summation $B(E, s)$ may be indexed by letting D vary over $U_k \backslash \Phi_k$ and,

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

for each D, letting C vary over $V(D)$. For a fixed D, the function $\chi(D^{-1}CE) = \chi(CED^{-1})$ factors to an additive character on $C \in V(D)$. The character is trivial if and only if $ED^{-1} \in \delta^{-1}M_k(S)$. Thus

$$\sum_{C \in V(D)} \chi(D^{-1}CE) = \begin{cases} |V(D)| = q^{k\nu(D)} & \text{if } ED^{-1} \in \delta^{-1}M_k(S), \\ 0 & \text{if } ED^{-1} \notin \delta^{-1}M_k(S). \end{cases} \tag{4.7}$$

Now $ED^{-1} \in \delta^{-1}M_k(S)$ if and only if $(\delta E)D^{-1} \in M_k(S)$. Thus, $B(E, s)$ equals a finite sum over classes in $D \in U_k \backslash \Phi_k$ of $q^{k\nu(D)}q^{-\nu(D)s}$. Comparing this sum with (2.4), we deduce the theorem. □

Part II

§ 5. Statement of theorems for Part II

In Part II, we add the following conventions to our standing hypothesis. Let π be a fixed generator of $\mathfrak{m}$. The valuation on F has a canonical extension to a multiplicative norm on Δ. Let l be the logarithmic valuation on Δ with the normalization that $l(\pi) = 1$ and the convention $l(0) = \infty$. If $N \subseteq \Delta$, put

$$l(N) = \min\{l(x): x \in N\}. \tag{5.1}$$

We permit the values $l(N) = -\infty$ and $l(N) = \infty$. Let ρ be an involution of Δ and fix ε a central S-unit such that $\varepsilon\varepsilon^\rho = 1$. We make

(5.2) *Standing hypothesis for Part* II:

(a) $\mathrm{char}(F) \neq 2$,

(b) F is the fixed field of ρ restricted to the center of Δ.

We permit ρ to be of either the first or second kind.

For $m \in \boldsymbol{Z}^+$, put

$$\begin{aligned} \Sigma(m, \varepsilon^\rho) &= \{T \in M_m(\Delta): T = \varepsilon^\rho({}^tT^\tau)\}, \\ \Sigma(m, \varepsilon) &= \{N \in M_m(\Delta): T = \varepsilon({}^tT^\tau)\}, \\ \Sigma(m, S) &= \Sigma(m, \varepsilon^\rho) \cap M_m(S), \\ \Sigma(m, S)^\sharp &= \{T \in \Sigma(m, \varepsilon): \chi(T \cdot \Sigma(m, S)) = \{1\}\}. \end{aligned} \tag{5.3}$$

Assumption (5.2) implies that $T \mapsto T + \varepsilon T^*$ is a surjection $M_m(\Delta) \to \Sigma(m, \varepsilon)$. If L is a hermitian S-lattice and $\theta: L \xrightarrow{\sim} M_{1,m}(S)$ is an S-isomorphism, then $(\,,\,)$ is uniquely determined by $T \in M_m(\Delta)$ such that

$$(x, y) = \theta(x)T\theta(y)^*, \tag{5.4}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

and each $T \in \Sigma(m, \varepsilon)$ determines an isomorphism class of hermitian lattice in this way. Note that $\Sigma(m, S)^\sharp$ is an R-lattice of $\Sigma(m, \varepsilon)$. We also put

$$\begin{aligned} \Delta(\varepsilon) &= \Sigma(1, \varepsilon^\rho) = \{t \in \Delta\colon\ t = (\varepsilon t)^\rho\}\,, \\ S(\varepsilon) &= \Sigma(1, S) = \{t \in S;\ t = (\varepsilon t)^\rho\}\,, \\ \mathscr{D} &= \{d \in \Delta\colon\ \forall b \in S,\ \chi(bd + b^\rho d^\rho) = 1\}\,. \end{aligned} \tag{5.5}$$

Then $T \in \Sigma(m, S)^\sharp$ if and only if $T_{ij} \in \mathscr{D}$ and $T_{jj} \in \Sigma(1, S)^\sharp$ for each pair of indices (i, j).

Remark 5.1. The various factors of "ε" and "ε^ρ" may be confusing. The present calculation arises when computing Fourier coefficients of a function on the local points of an additive group of hermitian matrices defined over a number field. The character group of the space of local (ρ, ε)-hermitian matrices is the space of local (ρ, ε^ρ)-hermitian matrices. For a matrix N representing a character, we will describe the corresponding Fourier coefficient in terms of the hermitian form given by N. The theory of hermitian spaces used here is ultimately applied to matrices representing characters. For this reason, we define our sums—which are just integrals over local spaces—to be over (ρ, ε^ρ)-hermitian matrices so that all of the characters are (ρ, ε)-hermitian,

Let U_m and Φ_m be as in Definition 1.1. For $D \in \Phi_m$, we need to consider

$$\begin{aligned} \Omega(D) &= \{C \in M_m(S)\colon\ CD^* = \varepsilon^\rho DC^*\}\,, \\ R(D) &= |\Omega(D)/(D \cdot \Sigma(m,\ S))|\,. \end{aligned} \tag{5.6}$$

Note that if $D \in \Phi_m$ and $b \in R - \{0\}$ so that $l(b) \geq \nu(D)$, then there is a matrix D_1 such that $DD_1 = b1_m$, and it follows easily that $b\Omega(D) \subseteq D \cdot \Sigma(m, S)$. Thus, $\Omega(D)/(D \cdot \Sigma(m, S))$ is a finitely generated R-module annihilated by b, and $R(D)$ is a finite value.

For $t \in Z$, put

$$\begin{aligned} \Delta_t &= \{d \in \Delta\colon\ l(d) \geq t\}\,. \\ \Delta_t^m &= \{T \in M_{1,m}(\Delta)\colon\ l(T_{1j}) \geq t\}\,, \\ A_t &= \{b + \varepsilon b^\rho\colon\ b \in \Delta_t\}\,. \end{aligned} \tag{5.7}$$

We also let $\Delta_t^m = \{T \in M_{m,1}(\Delta)\colon\ l(T_{j1}) \geq t\}$ when context makes clear which is meant. For $U \in M_m(\Delta)$, note that $S^m U = \Delta_t^m$ if and only if $U \in GL_m(S)\pi^t$.

We need a list of fundamental constants. Put

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$$\sigma = \operatorname{rank}_F \Delta\,, \tag{5.8}$$
$$\sigma_1 = \operatorname{rank}_F \Delta(\varepsilon)\,.$$

Take $\delta = l(\mathscr{D})$. Let θ be the R-linear function $b \mapsto b + \varepsilon b^\rho$ factored to $\Delta_{\delta+1}/\mathfrak{p}\Delta_\delta \to A_\delta/\mathfrak{p}A_\delta$. Define constants by the equations

$$q^{\sigma_2} = |\ker(\theta)|, \tag{5.9}$$
$$q^{\sigma_3} = q_0 = |S/\mathfrak{m}|,$$
$$q^{\sigma_4} = R(\pi),$$
$$q^{\sigma_5} = [S(\varepsilon):\ \pi S(\varepsilon)\pi^\rho].$$

The values σ, σ_1, σ_3, σ_4 and σ_5 remain unchanged throughout the rest of this paper; however, we consider values for σ_2 corresponding to "scales" other than δ in Section 8. We shall prove in Section 9 that

LEMMA 5.1. *The parameters defined in* (5.8) *and* (5.9) *satisfy* $\sigma_1 + \sigma_2 + \sigma_3 = \sigma_4 + \sigma$.

For $m \in \boldsymbol{Z}^+$ and $N \in \Sigma(m, S)^*$, define a formal power series in t by

$$\alpha(N, t) \sum_{x \in \Sigma(r, \varepsilon\rho)/\Sigma(r, S)} \chi(Nx) t^{j(x)}\,. \tag{5.10}$$

Clearly if $u \in GL_m(S)$, then $\alpha(N, t) = \alpha(uNu^*, t)$. We cite

THEOREM 5.2. *Let* $r, m \in \boldsymbol{Z}^+$ *so that* $m \geq r \geq 0$. *For* $m \in \boldsymbol{Z}^+$ *and* $N \in \Sigma(m, S)^\sharp$, *the summation* (5.10) *properly defines a formal power series. Let* $r, m \in \boldsymbol{Z}^+$ *so that* $m \geq r \geq 0$. *Then there is a formal Dirichlet series* $F(s)$ *with the property that if* $N \in \Sigma(r, S)^\sharp$ *and* $N_0 = \begin{pmatrix} N & 0 \\ 0 & 0 \end{pmatrix} \in (m, S)^\sharp$, *then*

$$\alpha(N_0, q^{-s}) = F(s)\alpha(N, q^{m-r-s})\,. \tag{5.11}$$

Proof. This is Theorem 4.1 of [3]. Although the statement appears in a section under the standing hypothesis that F has characteristic 0 and $\varepsilon \in \{1, -1\}$, the proof is valid in the present, more general, context. The proof is *not* effective—that is, the factor $F(s)$ is not given in a usable form. □

Suppose $N_0 \in \Sigma(m, S)^\sharp$ is non-zero, and regard N_0 as defining a hermitian structure on $M = S^m$. Then $M/M^\perp$ has no R-torsion, and so there is a complementary S-submodule L such that $M = L \perp M^\perp$. Representing the form on M with respect to a basis which respects the flag

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$0 \subseteq L \subseteq M$ yields a matrix of the type $\begin{pmatrix} N & 0 \\ 0 & 0 \end{pmatrix}$ where $N \in GL_r(\Delta)$. Thus, there is $u \in GL_m(S)$ such that $uN_0u^* = \begin{pmatrix} N & 0 \\ 0 & 0 \end{pmatrix}$. We can compute $\alpha(N, t)$ in general once we know $\alpha(N, t)$ when $N = 0_m$ for any m (this yields the $F(s)$ factor) and when $N \in \Sigma(m, S)^\# \cap GL_m(\Delta)$. The latter series can be characterized by using hermitian lattices.

We now state the main results of Part II.

DEFINITION 5.1. Let $m \in Z^+$. First, let $N \in \Sigma(m, S)^\# \cap GL_m(\Delta)$. If m is odd, define $\eta(N) = 1$. If m is even, define

(5.12.a) $\eta(N) = 0$ if for each $C \in \Phi_m$, either $C^{-1}NC^{-*} \notin \Sigma(m, S)^\#$ *or* $C^{-1}NC^{-*}\pi^{-l(\mathscr{D})} \notin GL_m(S)$,

(5.12.b) $\eta(N) = 1$ if there exists $d \in \Delta$ and $C \in \Phi_m$ such that $l(d) = l(\mathscr{D})$ and

$$C^{-1}NC^{-*} = \begin{bmatrix} 0 & dI_{m/2} \\ \varepsilon d^\rho I_{m/2} & 0 \end{bmatrix},$$

(5.12.c) $\eta(N) = -1$ if neither (5.12.a) nor (5.12.b) hold. In general, for $N \in \Sigma(m, S)^\#$, put $\eta(N) = 1$ if $N = 0$ and $\eta(N) = \eta(N_0)$ if $N_0 \in \Sigma(r, S)^\# \cap GL_r(\Delta)$ for $m > r \geq 1$ such that $uNu^* = \begin{pmatrix} N_0 & 0 \\ 0 & 0 \end{pmatrix}$ for some $u \in GL_m(S)$. Corollary 8.5.2. will imply that the quantity $\eta(N)$ is well-defined.

THEOREM 5.3 (Context and Notation of Sections 1 and 5). *Assume F is contained in the center of Δ and that* (5.2) *holds. Let $m \in Z^+$ and $N \in \Sigma(m, S)^\#$. Let $r = \operatorname{rank}_\Delta(N\Delta^m)$ and $\eta = (N)$. Express $r = 2g + \lambda$ where $g \in Z$ and $\lambda \in \{0, 1\}$. Then $\alpha(N, t)$ is a polynomial in $Z[t]$ times*

(5.13)
$$\frac{\prod_{b=0}^{m-g-\lambda-2}(1 + q^{b\sigma_3+\sigma_4}t^{\sigma_3})\prod_{b=0}^{m-g-1}(1 - q^{b\sigma_3}t^{\sigma_3})}{\prod_{j=0}^{m-r-1}(1 - q^{(m-1+j)\sigma_3+\sigma_5}t^{2\sigma_3})}(1 + \eta q^{(m-g-\lambda-1)\sigma_3+\sigma_4}t^{\sigma_3})$$

if $g \neq 0$ and $\eta \neq 0$,

$$\frac{\prod_{b=0}^{m-g-\lambda-1}(1 + q^{b\sigma_3+\sigma_4}t^{\sigma_3})\prod_{b=0}^{m-g-\lambda}(1 - q^{b\sigma_3}t^{\sigma_3})}{\prod_{j=0}^{m-r-1}(1 - q^{(m-1+j)\sigma_3+\sigma_5}t^{\sigma_3})}$$

if $\eta = 0$,

$$\frac{\prod_{b=0}^{m-\lambda-1}(1 + q^{b\sigma_3+\sigma_4}t^{2\sigma_3})\prod_{b=0}^{m-1}(1 - q^{b\sigma_3}t^{\sigma_3})}{\prod_{j=0}^{m-r-1}(1 - q^{(m-1+j)\sigma_3+\sigma_5}t^{2\sigma_3})}$$

if $q = 0$.

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Moreover, if $N = 0$ *or there exists* $r \in Z^+$, $u \in GL_r(S)$ *and* $N_0 \in \Sigma(r, S)^\sharp \cap GL_r(S)\pi^{l(\varrho)}$ *such that* $uNu^* = \begin{pmatrix} N_0 & 0 \\ 0 & 0 \end{pmatrix}$, *then* $\alpha(N, t)$ *is exactly the factor in* (5.13).

Remark 5.2. Expression (5.13) generalizes the formulas of [12], [5] and [3]. Under the assumption $\Delta = F$ (the *Sp* Case of [3]) or Δ/F an unramified quadratic extension (the *SU* Case of [3]), the quantities σ, σ_1, σ_2, σ_3, σ_4 are determined and all of the numerator terms of the form $1 + q^a t^b$ are cancelled by denominator terms $1 - q^{2a}t^{2b}$ to produce the formulas already in the literature.

We conclude this section by stating a version of Theorem 5.3 for matrix algebras over a division ring. The proof is elementary, and is omitted.

COROLLARY 5.3.1. *Let* F, Δ, R, S, *and* q *be as in Section* 1, ρ *an involution on* Δ *and* ε *a central* S*-unit such that* $\varepsilon\varepsilon^\rho = 1$. *Assume that* (5.2) *holds. Let* $n \in Z^+$, *put* $A = M_n(\Delta)$ *and* $B = M_n(S)$, *and let* j *denote* $j[A, B]$ *as defined in* (1.5) *and* (1.6). *For* $m \in Z^+$, *we let* $\gamma\colon M_n(A) \to M_{mn}(\Delta)$ *be canonical function. Let* $v \in GL_n(S)$ *for which* $u = v({}^t v^{-\rho})$ *is a central* S*-unit, and define an involution on* A *by* $\tau\colon x \mapsto v({}^t x^\rho)v^{-1}$.

For $m \in Z^+$, *put*

$$
\begin{aligned}
\Sigma(m, \varepsilon^\rho) &= \{T \in M_m(A)\colon T = \varepsilon^\rho({}^t T^\tau)\}, \\
\Sigma(m, \varepsilon) &= \{T \in M_m(A)\colon T = \varepsilon({}^t T^\tau)\}, \\
\Sigma(m, B) &= \Sigma(m, \varepsilon^\rho) \cap M_m(B), \\
\Sigma(m, B)^\sharp &= \{N \in \Sigma(m, \varepsilon)\colon \chi(N \cdot \Sigma(m, B)) = \{1\}\}, \\
\hat{v}_m &= \operatorname{diag}\{v, \cdots, v\} \in M_m(A)).
\end{aligned} \tag{5.14}
$$

Then for $m \in Z^+$ *and* $N \in \Sigma(m, B)^\sharp$, *we have an equality of Dirichlet series in the formal complex parameters* s

$$
\sum_{x \in \Sigma(m, \varepsilon^\rho)/\Sigma(m, B)} \chi(Nx) q^{-j(x)s} = \alpha(\gamma(\hat{v}_m^{-1}N), q^{-ns}), \tag{5.15}
$$

where α *is defined by* (5.10) *with respect to the algebra* Δ, *the involution* ρ, *and the central unit* εu^ρ.

§ 6. A Witt Theorem for hermitian lattices

Suppose $a \in \Delta^*$ and $b, c \in \Delta$ such that $l(b) > l(a)$ and $l(c) > l(a)$. Let

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$T = \begin{pmatrix} b & a \\ \varepsilon a^\rho & c \end{pmatrix}$. Now

$$\begin{bmatrix} 1 & -\varepsilon^\rho b a^{-\rho} \\ 0 & 1 \end{bmatrix} T = \begin{bmatrix} 0 & a - \varepsilon^\rho b a^{-\rho} c \\ \varepsilon a^\rho & c \end{bmatrix} \tag{6.1}$$

and $l(a - \varepsilon^\rho b a^{-\rho} c) = l(a)$. It follows that the matrix T is invertible. Let

$$L = \{(x\ y) \in M_{1,2}(\Delta) \colon l(x), l(y) \geq l(a)\} = \Delta^2_{l(a)}. \tag{6.2}$$

We claim

$$S^2 T = L, \quad T S^2 = L^*, \quad S^2 = L T^{-1} \quad \text{and} \quad S^2 = T^{-1} L^*. \tag{6.3}$$

Since T is invertible and hermitian, it suffices to show that $S^2 T = L$. Clearly $S^2 T \subseteq L$. Suppose $(x\ y) \in \Delta^2 - S^2$. If $l(x) \geq l(y)$, then

$$l(xb) > l(\varepsilon y a^\rho) \Longrightarrow l(xb + \varepsilon y a^\rho) = l(y a^\rho) < l(a)\,, \tag{6.4}$$

and $(x\ y)T \notin L$. If $l(x) < l(y)$, then $l(xa + yc) = l(xa) \notin L$.

We say that a hermitian lattice is fundamental if it is of rank 1 or it can be represented by a matrix $T = \begin{pmatrix} b & a \\ \varepsilon a^\rho & c \end{pmatrix}$ where $a \neq 0$, $b = \varepsilon b^\rho$, $c = \varepsilon c^\rho$, and $l(b) > l(a)$ and $l(c) \geq l(a)$.

If L is a hermitian lattice, define the scale of L to be

$$s(L) = l((L, L))\,. \tag{6.5}$$

LEMMA 6.1 (Existence of Jordan Splittings). *Let L be a hermitian lattice.*

(A) *If $L^\perp = \{0\}$, then L is the orthogonal sum of fundamental lattices.*

(B) *Suppose $M \subseteq L$ is a sublattice such that*

(B.1.a) *M is fundamental,*

(B.1.b) *$s(M) = s(L)$.*

Then $L = M \perp M^\perp$.

Proof. The proof of (B) is contained in our proof of (A). We must show that if L is a lattice non-trivial radical, then $L = M \perp M^\perp$ for some fundamental lattice M.

Put $\delta = s(L)$. Suppose that $x \in L$ so that $l((x, x)) = \delta$. Put $M = Sx$ and $N = M^\perp$. If $y \in L$, take $\lambda \in S$ so that $\lambda(x, x) = (y, x)$, and then $y - \lambda x \in N$. Thus, $L = M + N$. Since $L^\perp = \{0\}$, $M \cap N = \{0\}$ and $L = M \perp N$.

Suppose that $l((x, x)) > s(L)$ for every $x \in L$. Take $x, y \in L$ so that $l((x, y)) = \delta$. Then x and y are linearly independent over Δ, and the form

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

restricted to $M = Sx + Sy$ is given by a fundamental matrix $T = \begin{pmatrix} b & a \\ \varepsilon a^{\rho} & c \end{pmatrix}$. Suppose $z \in L$, and let

$$(\lambda\ \mu) = ((z, x)\,(z, y))T^{-1}\,. \tag{6.6}$$

Now $\lambda, \mu \in S$ by (6.3). By construction, $(z - \lambda x - \mu y, M) = \{0\}$. Thus, $L = M \perp N$ where $N = M^{\perp}$. □

Remark 6.1. From the argument it is clear that we can write any lattice L as a sum of $L^{\perp}$ and fundamental lattices where each 2×2 component can be represented by $\begin{pmatrix} b & a \\ \varepsilon a^{\rho} & c \end{pmatrix}$ for $l(b) > l(a)$ and $l(c) > l(a)$. This observation is useful in Section 9.

Let V be a hermitian Δ-module. We say that $\{x, y\} \in V$ is a hyperbolic pair if

$$(x, x) = (y, y) = 0 \quad \text{and} \quad (x, y) \in \Delta^{*}\,. \tag{6.7}$$

We can define two types of form-preserving transformations which do not rely on specifying a choice of basis of V. First, suppose $v \in V$ so that $(v, v) \neq 0$ and $\lambda \in \Delta^{*}$ so that $(v, v) = \lambda + \varepsilon\lambda^{\rho}$. Define

$$\sigma_{v,\lambda}(x) = x - (x, v)\lambda^{-1}v\,. \tag{6.8}$$

Direct computation shows that $(\sigma_{v,\lambda}(x), \sigma_{v,\lambda}(y)) = (x, y)$ for all $x, y \in V$. Next, let $\{w, v\}$ be a hyperbolic pair in V and put $a = (w, v)$. Suppose that $u \in \langle w, v\rangle^{\perp}$ and $b \in \Delta$ so that $(u, u) = ba + \varepsilon(ba)^{\rho}$. Define $\xi = \xi_{\{w,v\},b,u}$ by

$$\begin{aligned} &\xi(w) = w\,, \\ &\xi(v) = v - bw + u\,, \\ &\xi(z) = z - (z, u)a^{-1}w \qquad \text{for } z \in \langle w, v\rangle^{\perp}\,. \end{aligned} \tag{6.9}$$

Tedius calculation shows that ξ preserves the form. Moreover, it is easily checked that for parameters v, w, u, t, λ, b

$$\sigma_{v,\varepsilon\lambda^{\rho}} = (\sigma_{v,\lambda})^{-1} \tag{6.10.a}$$

$$\xi_{\{w,v\},bu} \circ \xi_{\{w,v\},c,t} = \xi_{\{w,v\},b+c+(t,u)a^{-1},u+t}\,, \tag{6.10.b}$$

$$\xi_{\{w,v\},(u,u)a^{-1}-b,-u} = (\xi_{\{w,v\},b,u})^{-1}\,. \tag{6.10.c}$$

Our next step is to interpret these constructions in terms of lattices.

Let L be a non-trivial hermitian lattice and put $\delta = s(L)$. First, sup-

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

pose $v \in L$ and $\lambda \in \Delta^*$ so that $l(\lambda) = \delta$ and $(v, v) = \lambda + \varepsilon\lambda^\rho$. Then $\sigma_{v,\lambda}(L) = L$. In particular, if $v, w \in L$ so that

(6.11.a) $$(v, v) = (w, w)\,,$$

(6.11.b) $$l((w, w - v)) = \delta\,,$$

then $\tau = \sigma_{w-v,(w,(w-v))}$ satisfies

(6.12.a) $$\tau(L) = L\,,$$

(6.12.b) $$\tau(w) = v\,.$$

Next, suppose that $\{x, y\}$ is a hyperbolic pair of elements in L such that $l((x, y)) = s(L)$. Suppose that $y' \in L$ so that $(y', y') = 0$ and $(x, y) = (x, y')$. Then there exist $u \in L$ and $b \in S$ such that $\tau = \xi_{\{x,y\},b,u}$ satisfies

(6.13.a) $$\tau(L) = L\,,$$

(6.13.b) $$\tau(y) = y'\,.$$

We can now prove

THEOREM 6.2 (Witt's Theorem for hyperbolic pairs). *Let L be non-trivial hermitian lattice. Suppose that $\{x, y\}$, $\{x', y'\}$ are hyperbolic pairs of elements in L such that*

(6.14.a) $$(x, y) = (x', y')\,,$$

(6.14.b) $$l((x, y)) = s(L)\,.$$

Then there is a form-preserving S-automorphism $\tau\colon L \simeq L$ such that $\tau(x) = x'$ and $\tau(y) = y'$.

Proof. In the following argument, we write "morphism" to mean "form-preserving S-automorphism". Let $\delta = s(L)$, $H = Sx + Sy$ and $N = H^\perp$. Then $L = H \perp N$ by Lemma 6.1.B. If $x = x'$ or $y = y'$, we are done by the remark in (6.13).

Put $a = (x, y)$. For c an S-unit, the S-homomorphisms of H given by

(6.15.a) $$x \longmapsto cy\,, \qquad y \longmapsto \varepsilon a^\rho c^{-\rho} a^{-1} x\,,$$

(6.15.b) $$x \longmapsto cx\,, \qquad y \longmapsto a^\rho c^{-\rho} a^{-\rho} y\,,$$

are morphisms of H. Hence, the conclusion follows if either x' or y' is a multiple of x or y by an S-unit.

Express $x' = cx + dy + u$ where $c, d \in S$ and $u \in N$. If c is an S-unit, then $\tau = \sigma_{y-x',(y,y-x')}$ determines a morphism of L which sends y to x'. There is an analogous symmetry if d is an S-unit, or if the projection of y' to H is primitive. Thus, we are reduced to the case

$$\begin{aligned} x' &= \alpha + u \qquad \alpha \in H \quad \text{and} \quad u \in N, \\ y' &= \beta + v \qquad \beta \in H \quad \text{and} \quad v \in N, \\ &\text{and} \quad \alpha, \beta \text{ are not primitive.} \end{aligned} \tag{6.16}$$

Using the assumption that α and β are not primitive, we conclude that $l((u, v)) = l((x', y'))$. It is simple to construct $\alpha' \in H$ which is primitive such that $(\alpha, \alpha) = (\alpha', \alpha')$. Put $x'' = \alpha' + u$. Then $(x'', x'') = 0$ and $l((y', y' - x'')) = \delta$. Thus, $\tau = \sigma_{y'-x'',(y',y'-x'')}$ determines a morphism of L which sends y' to x''. The projection of x'' to H is primitive, so we are done by a previous remark. □

DEFINITION 6.1. If L is a hermitian lattice and $s(L) = \delta \neq \infty$, a hyperbolic pair of L is a pair $\{x, y\} \subseteq L$ such that $l((x, y)) = s(L)$. A hermitian lattice H is called hyperbolic of denominator $-\delta$ if H is the orthogonal union of lattices of rank 2 over S each of which has a hyperbolic pair $\{x, y\}$ with $l((x, y)) = \delta$ as basis. A lattice of rank 2 over S with a hyperbolic pair as basis is called a hyperbolic plane.

Witt's Theorem extends to a few other lattices. Let $a \in \Delta^*$ and $b \in \Delta$ and $\lambda \in S$ so that $b = a\lambda + \varepsilon\lambda^\rho a^\rho$, then

$$\begin{bmatrix} 1 & -\lambda^\rho \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b & a \\ \varepsilon a^\rho & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\lambda & 1 \end{bmatrix} = \begin{bmatrix} 0 & a \\ \varepsilon a^\rho & 0 \end{bmatrix}. \tag{6.17}$$

Thus, the matrix $\begin{pmatrix} b & a \\ \varepsilon a^\rho & 0 \end{pmatrix}$ determines a hyperbolic plane.

Let $a \in \Delta^*$, $b, c \in \Delta$ so that $b = \varepsilon b^\rho$, $c = \varepsilon c^\rho$, $l(b) > l(a)$ and $l(c) \geq l(a)$. Let L be a lattice of rank 4, e_1, e_2, e_3, e_4 a basis of L, and suppose that the matrix of the form with respect to the basis is

$$\begin{bmatrix} b & a & 0 & 0 \\ \varepsilon a^\rho & c & 0 & 0 \\ 0 & 0 & -b & -a \\ 0 & 0 & -\varepsilon a^\rho & -c \end{bmatrix}. \tag{6.18}$$

The elements

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$$e_1 + e_3,\ e_2,\ e_3 - \varepsilon^\rho b a^{-\rho} c a^{-1}(e_1 + e_3) + \varepsilon^\rho b v^{-\rho} e_2$$

and

$$-(1 - ca^{-1}b^\rho a^{-1\rho})^{-1}\{e_4 - ca^{-1}(e_1 + e_3) + e_2\}$$

also form a basis. The matrix with respect to this basis is

$$\begin{bmatrix} 0 & a & 0 & 0 \\ \varepsilon a^\rho & c & 0 & 0 \\ 0 & 0 & \varepsilon^\rho b a^{-\rho} c a^{-1} b - b & a \\ 0 & 0 & \varepsilon a^\rho & 0 \end{bmatrix} \tag{6.19}$$

If b and c can each be expressed as $a\lambda + \varepsilon(a\lambda)^\rho$ for $\lambda \in S$, then the matrix in (6.19) determines the orthogonal product of two hyperbolic planes.

Finally, suppose that $a \in \Delta^*$ and $\lambda \in S$ such that $a = \lambda a + \varepsilon(\lambda a)^\rho$. The hermitian lattice given by $\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ is hyperbolic with respect to basis $e_1 + e_2,\ e_1 - \lambda^\rho(e_1 + e_2)$.

DEFINITION 6.2. Let $\delta \in Z$. We say that a lattice is δ-modular if $l((v, L)) = \delta$ for each primitive $v \in L$ and $(v, v) \in A_\delta$ (as defined in (5.7)) for each $v \in L$.

"δ-modular" hermitian lattices should be regarded as a generalization of O'Meara's [8]" α-modular" lattices, *not* of "unimodular" lattices.

For L a hermitian lattice, we let $-L$ denote the module of L with the form $-(\ ,\ )$. We have found a variety of hermitian lattices L such that $L \perp (-L)$ is hyperbolic. If L and M have this property, then so does $L \perp M$. Suppose L is of one of the above types, and put $\delta = s(L)$. Let M and N be hermitian lattices such that $s(M), s(N) \geq \delta$ and $L \perp M \approx L \perp N$ (that is, isomorphic as hermitian lattices). Then $((-L \perp L) \perp M \approx ((-L) \perp L) \perp N$. By Theorem 6.2, it follows that $M \approx N$.

Mimicking classical arguments from the theory of quadratic forms, we can summarize with

THEOREM 6.3 (First structure theorem of modular lattices). *Let $\delta \in Z$ and L be a δ-modular lattices.*

(A) *If $x \in L$ is primitive and $(x, x) = 0$, then there is $y \in L$ so that $\{x, y\}$ is a hyperbolic pair of L.*

(B) *$L \perp (-L)$ is a hyperbolic space of denominator $-\delta$.*

(C) *If M is a lattice which contains L such that $s(M) = \delta$, then $M = L \perp L^\perp$.*

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

(D) *Let M and N be hermitian lattices for which $s(M), s(N) \geq \delta$. If $L \perp M \approx L \perp N$, then $M \approx N$ (where "$\approx$" means isomorphic as hermitian lattices).*

§ 7. Counting representations mod (n)

For this section, we fix $\delta \in \boldsymbol{Z}$, π a generator of $\mathfrak{m}$, and π_0 a generator of $\mathfrak{p}$.

Fix E an R-submodule of $\Delta(\varepsilon)$ such that

$$A_\delta \subseteq E \subseteq \Delta_\delta\,, \tag{7.1.a}$$

$$\forall\, u \in S, \quad \forall\, x \in E, \quad uxu^* \in E\,. \tag{7.1.b}$$

For $r \in \boldsymbol{Z}^+$, define $E(r)$ to be the R-module of $r \times r$ matrices such that

$$\begin{aligned} N_{ij} &\in \Delta_\delta \qquad \text{for } i \neq j, \quad \text{and} \\ N_{jj} &\in E \qquad \text{for each index } j\,. \end{aligned} \tag{7.2}$$

Note that $E = A_\delta$ satisfies our conditions, and for this choice we denote $E(r)$ by $\Delta(\delta, r)$. For convenience, we also define

$$\sigma(r) = \dim_F \Sigma(r, \varepsilon) = r(r-1)\sigma/2 + r\sigma_1\,. \tag{7.3}$$

Each $N \in E(r)$ determines a hermitian lattice. If $U \in GL_r(S)\pi^\delta$, then $NU^{-1} \in M_r(S)$ for $N \in E(r)$.

For $C \in \Phi_r$ and $N \in E(r)$, put $N[C] = C^- NC^{-*}$. We remark

LEMMA 7.1. *If $N \in E(r) \cap GL_r(\Delta)$, then the set $\{C \in \Phi_r\colon N[C] \in E(r)\}$ is a finite union of right U_r-cosets.*

Proof. Let $N \in E(r) \cap GL_r(\Delta)$ and let $U \in GL_r(S)\pi^\delta$. For $C \in \Phi_r$,

$$\nu(N[C]U^{-1}) = \nu(U^{-1}) + \nu(C^{-1}) + \nu(N) + \nu(C^{-*}) = \nu(NU^{-1}) - 2\nu(C)\,. \tag{7.4}$$

If $N[C] \in E(r)$, then NU^{-1} and $N[C]U^{-1}$ have entries in S, and so $\nu(NU^{-1}) \geq 2\nu(C) \geq 0$. □

For $C \in \Phi_r$, put

$$\iota(C) = [C^{-1}E(r)C^{-*}\colon E(r)] = [E(r)\colon CE(r)C^*]\,. \tag{7.5}$$

If $C, D \in \Phi_r$, then $\iota(CD) = \iota(C)\iota(D)$. If $C \in U_r$, then $\iota(C) = 1$.

For $C \in \Phi_r$, there exist $\alpha, \beta \in U_r$ so that $\alpha C \beta = \operatorname{diag}\{c_1, \cdots, c_r\}$ where $c_j \in S - \{0\}$ for each j. In terms of the matrix coordinates, we see

$$\iota(C) = \left(\prod_{i<j} [\Delta_\delta\colon c_i \Delta_\delta c_j^*]\right) \times \left(\prod_j [E\colon c_j E c_j^*]\right). \tag{7.6}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

If $i \neq j$, then

$$[\Delta_\delta\colon c_i\Delta_\delta c_j^*] = [\Delta_\delta\colon c_i\Delta_\delta]\,[c_i\Delta_\delta\colon c_i\Delta_\delta c_j^*] = q^{\nu(c_i)+\nu(c_j)}\,. \tag{7.7}$$

We are led to

DEFINITION 7.1. For $c \in S - \{0\}$, put $\nu_1(c) = [E\colon cEc^*]$. For $r \in Z^+$ and $C \in \Phi_r$, define $\nu_1(C)$ to be the integer determined by

$$\iota(C) = q^{\nu_1(C)+(r-1)\nu(C)}\,. \tag{7.8}$$

If $\alpha, \beta \in U_r$ so that $\alpha C\beta = \operatorname{diag}\{c_1, \cdots, c_r\}$, then

$$\nu_1(C) = \textstyle\sum_j \nu_1(c_j)\,. \tag{7.9}$$

Fix $k, r \in Z^+$ and $M \in E(k) \cap GL_k(\Delta)$. For $N \in E(r)$ and $m \in Z^+$, define

$$\begin{aligned} A(M, N; m) &= \{T \in M_{r\times k}(S/\mathfrak{p}^m S)\colon TMT^* \equiv N \bmod (m)\}\,, \\ P(M, N; m) &= \{T \in A(M, N; m)\colon T \text{ is primitive}\}\,, \end{aligned} \tag{7.10}$$

where $\bmod(m)$ refers to the R-lattice $E(r)$. If $T \in M_{r\times k}(S)$, we abuse notation and write $T \in A(M, N; m)$ ($T \in P(M, N; m)$, respectively) if $T \bmod (m) \in A(M, N; m)$ (if $T \bmod (m) \in P(M, N; m)$, respectively).

Suppose $k \geq r$. Let $\theta\colon M_{r\times k}(S) \to E(r)$ be the function $T \mapsto TMT^* - N$. With respect to any choice of R-basis for S and $E(r)$, the map θ is polynomial with coefficients in R. For $T \in M_{r\times k}(S)$, the differential of θ at T is

$$d\theta_T\colon v \longmapsto vMT^* + TMv^* = vMT^* + \varepsilon(vMT^*)^*\,. \tag{7.11}$$

Let $n_1 \in Z^+ \cup \{0\}$ so that $\mathfrak{p}^{n_1}\Delta_\delta^k \subseteq S^k M$. We claim that if T is primitive, then $\mathfrak{p}^{n_1}\Delta(\delta, r) \subseteq d\theta_T(M_{r\times k}(S))$. First, suppose that $r = k$ and T is invertible. Since Δ_δ is an S-ideal, $\Delta_\delta^k T^* \subseteq \Delta_\delta^k$ and $\Delta_\delta^k T^{-*} \subseteq \Delta_\delta^k$, Thus, $\mathfrak{p}^{n_1}M_k(\Delta_\delta) \subseteq M_k(S)MT^*$. The map $d\theta_T$ has image $\{\alpha + \varepsilon\alpha^*\colon \alpha \in M_k(S)MT^*\}$, which contains the set of $\mathfrak{p}^{n_1}\Delta(\delta, r)$. Now suppose $k > r$, and take a matrix U so that $\begin{pmatrix} U \\ T \end{pmatrix} \in GL_k(S)$. For $u \in M_{(k-r)\times k}(S)$ and $v \in M_{r\times k}(S)$,

$$\begin{bmatrix} u \\ v \end{bmatrix} M \begin{bmatrix} U \\ T \end{bmatrix}^* = \begin{bmatrix} * & * \\ * & vMT^* \end{bmatrix} \tag{7.12}$$

and we are finished by the first case.

Apply Corollary 1.2.1 to get

LEMMA 7.2. *Let $k, r \in Z^+$ so that $k \geq r$, $M \in E(k) \cap GL_k(\Delta)$ and $N \in E(r)$. Let $n_1, n_2 \in Z^+ \cup \{0\}$ so that $\mathfrak{p}^{n_1}\Delta_\delta^k \subseteq MS^k$ and $\mathfrak{p}^{n_2}E \subseteq A_\delta$, and put*

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$n = n_1 + n_2$. *Let* $m \in \boldsymbol{Z}$ *so that* $m \geq 2n + 1$.

(A) *If* $T_0 \in P(M, N; m)$, *then there is* $T \in M_{r\times k}$ *such that* $TMT^* = N$ *and* $T \equiv T_0 \bmod (m - n)$.

(B) *If* $a \in \boldsymbol{Z}^+$, *then*

$$|P(M, N; m + a)| = q^{a(kr\sigma - \sigma(r))}|P(M, N; m)|. \tag{7.13}$$

Let $k, r \in \boldsymbol{Z}^+$ so that $k \geq r$, $M \in E(k) \cap GL_k(\Delta)$ and $N \in E(r) \cap GL_r(\Delta)$. As above, take $n_1, n_2 \in \boldsymbol{Z}^+ \cup \{0\}$ so that $\mathfrak{p}^{n_1}\Delta_\delta^k \subseteq MS^k$ and $\mathfrak{p}^{n_2}E \subseteq A_\delta$, and put $n = n_1 + n_2$. In this case, we can reduce the computation of $|A(M, N; m)|$ to the computation of values $|P(M, N'; 2n + 1)|$. Fix $U \in GL_r(S)\pi^\delta$. We restrict attention to values $m \in \boldsymbol{Z}^+$ for which $m > \nu(NU^{-1}) + 2n$.

If $T \in M_{r\times k}(S)$ so that $T \in A(M, N; m)$, then $(TMT^* - N)U^{-1} \in \mathfrak{p}^m M_r(S)$. By the properties of the function ν, it follows that $\nu(TMT^*U^{-1}) = \nu(NU^{-1})$, and consequently TMT^* is invertible over Δ. If $wT = 0$ for $w \in \Delta^r$, then $wTMT^* = 0$, and consequently $w = 0$. By [3; Corollary 2.3], there is $C \in \Phi_r$ and a primitive matrix $T_0 \in M_{r\times k}(S)$ so that $T = CT_0$. By that same theorem, if $C_1 \in \Phi_r$ and T_1 is a primitive $r \times k$ matrix such that $T = C_1T_1$, then there is $\alpha \in U_r$ such that $C_1 = C\alpha$ and $T_1 = \alpha^{-1}T_0$. Thus, the right U_r-coset of C is uniquely determined by T.

Let $C \in \Phi_r$ and $T \in M_{r\times k}(S)$ so that $CTMT^*C^* \equiv N \bmod (m)$. Since $\nu(CTMT^*C^*U^{-1}) = \nu(NU^{-1})$, and $TMT^*U^{-1} \in M_r(S)$,

$$m > \nu(NU^{-1}) \geq 2\nu(C) \geq 0. \tag{7.14}$$

There is $C_0 \in M_r(S)$ so that $CC_0 = \pi_0^{\nu(C)}1_r$. Let $D = \pi_0^{-m}(TMT^* - N) \in E(r)$. Then

$$TMT^* - C^{-1}NC^{-*} = C_0\pi_0^{m-2\nu(C)}DC_0^*. \tag{7.15}$$

Thus $N[C] \in E(r)$. Conversely, suppose $C \in \Phi_r$ so that $N[C] \in E(r)$. As before, it follows that $\nu(NU^{-1}) \geq 2\nu(C)$. Let $D_1, \cdots, D_a$ be a complete irredundant list of coset representatives for $C^{-1}\pi_0^m E(r)C^{-*}/\pi_0^m E(r)$. Then $a = \iota(C)$ and $D_j \equiv 0 \bmod (2n + 1)$ for each j. Now for $T \in M_{r\times k}(S/\mathfrak{p}^m S)$, it follows that

$$CTMT^*C^* \equiv N \bmod (m) \Longleftrightarrow \exists\, j\colon\ TMT^* \equiv N[C] + D_j \bmod (m). \tag{7.16}$$

Finally, C divides $\pi_0^{m-1}1_r$ in $M_r(S)$. Hence, if $T \in M_{r,k}(S)$ and $C^{-1}T$ is primitive (with respect to S), then $C^{-1}T'$ is primitive if $T' \in M_{r,k}(S)$ and $T' \equiv T \bmod (m)$.

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Let $C \in \Phi_r$ so that $N[C] \in E(r)$. Let $W(M, N, C; m)$ be the set of elements $T \in A(M, N; m)$ for which $C^{-1}T$ is primitive. Then map $T \mapsto CT$ is an additive endomorphism of $M_{r,k}(S/\mathfrak{p}^m S)$ whose kernel has order

$$(7.17) \qquad [C^{-1}\pi_0^m M_{r,k}(S);\ \pi_0^m M_{r,k}(S)] = [M_{r,k}(S):\ FM_{r,k}(S)] = [S^r:\ CS^r]^k = q^{k\nu(C)}.$$

The inverse image of $W(M, N, C; m)$ is the union of the sets $P(M, N[C] + D_j; m)$. Thus

$$(7.18) \qquad |W(M, N, C; m)| = q^{-k\nu(C)} \sum_{j=1}^{\iota(C)} |P(M, N[C] + D_j; m)|$$
$$= q^{-k\nu(C)} \sum_{j=1}^{\iota(C)} q^{(m-2n-1)(kr\sigma - \sigma(r))} |P(M, N[C] + D_j; 2n+1)|$$
$$= q^{-k\nu(C) + (m-2n-1)(kr\sigma - (r))\nu(C)} |P(M, N[C];\ 2n+1)|.$$

Putting everything together, we first get

THEOREM 7.3. *Let $k, r \in \boldsymbol{Z}^+$ so that $k \geq r$, $M \in E(k) \cap GL_k(\Delta)$ and $N \in E(r) \cap GL_r(\Delta)$. Let $n_1, n_2 \in \boldsymbol{Z}^+ \cup \{0\}$ so that $\mathfrak{p}^{n_1}\Delta_\delta^k \subseteq MS^k$ and $\mathfrak{p}^{n_2}E \subseteq A_\delta$, and put $n = n_1 + n_2$. Then there is a number $b \in \boldsymbol{Z}^+$ which depends only on N with the property that if $m \in \boldsymbol{Z}^+$ and $m \geq b + 2n$, then*

$$(7.19) \qquad |A(M, N; m)| = \sum_C q^{(m-2n-1)\{kr\sigma - r(r-1)\sigma/2 - r\sigma_1\} + (r-1-k)\nu(C) + \nu_1(C)} |P(M, N[C];\ 2n+1)|,$$

where the summation is taken over a complete irredundant set of representatives of the finite set $\{C \in \Phi_r:\ N[C] \in E(r)\}/U_r$. □

Remark 7.1. A choice for b is $\nu(NU^{-1}) + 1$ where $U \in GL_r(S)\pi^\delta$. Put $b' = b + 2n$. For $m \geq b'$, we have

$$(7.20) \qquad q^{m(\sigma(r) - kr\sigma)} |A(M, N; m)| = q^{b'(\sigma(r) - kr\sigma)} |A(M, N; b')|.$$

§ 8. Classification of δ-modular lattices and counting arguments

Our objective is to compute value $|P(M, N; 1)|$ as defined in Section 7 when M defines an "modular" lattice; in order to do this, we work with a rather bizarre category.

In this section we fix $\delta \in \boldsymbol{Z}$. Terms such as "lattice", "rank" and "primitive" are used with respect to S-module structure, unless explicitly stated otherwise. Define a category $\mathscr{C}$ as follows. An object is a (ρ, ε)-hermitian lattice L such that for $s(L) \geq \delta$ and $(v, v) \in A_\delta$ every $v \in L$. We

say $L \in \mathscr{C}$ is hyperbolic if L is hyperbolic of denominator $-\delta$, and we say L is modular if it is δ-modular. A morphism $L \to M$ is a primitives $S/\mathfrak{p}S$-homomorphism θ: $L/\mathfrak{p}L \to M/\mathfrak{p}M$ such that if $v_1, v_2 \in L$ and $w_1, w_2 \in M$, where $\theta(v_i) \equiv w_1 \bmod (1)$ for $i = 1\,2$, then

$$(v_1, v_2) - (w_1, w_2) \in \mathfrak{p}\Delta_\delta\,, \tag{8.1.a}$$

$$(v_i, v_i) - (w_i, w_i) \in \mathfrak{p}A_\delta\,. \tag{8.1.b}$$

Define categorical composition to be the usual composition. Denote the set of morphisms $L \to M$ by $P(L, M)$.

For a lattice, L, let $\varphi = \varphi_L$: $L \to L/\mathfrak{p}L$. If $\theta \in P(L, M)$, then a lift of θ is a form-preserving S-homomorphism θ_0: $L \to M$ for which $\varphi \circ \theta_0 = \theta \circ \varphi$. By Lemma 7.1, if $\theta \in P(L, M)$ and M is modular, then θ has a lifting. We let "$\equiv$" refer to congruence module $\mathfrak{p}L$, $\mathfrak{p}\Delta_\delta$, $\mathfrak{p}A_\delta$, etc.. For $z \in L$, put $\bar{z} = z + \mathfrak{p}L$. Also let $Q = Q_L$ denote the map $Q(z) = (z, z)$. We regard Q as mapping into the R-module, A_δ, so equations "$Q(z) \equiv b$" refer to congruence mod $\mathfrak{p}A_\delta$. Note that the l function factors to $(\Delta_\delta - \mathfrak{p}\Delta_\delta)/\mathfrak{p}\Delta_\delta$, and we adopt the convention that l of the 0-coset is $l(\mathfrak{p}) + \delta$. Using Lemma 7.1 and Theorem 6.3.A, it is simple to show that if M is modular lattice and $x \to M$ such that $Q(x) \equiv 0$, then there is $x' \in M$ such that $x' \equiv x$ and $Q(x) = 0$.

LEMMA 8.1. *Let $L, M, N \in \mathscr{C}$ and suppose that L and M are modular. Then*

$$|P(L \perp N, L \perp M)| = |P(L, L \perp M)||P(N, M)|\,. \tag{8.2}$$

Proof. Each $\theta \in P(L \perp N, L \perp M)$ is determined by $\theta_1 = \theta_{|L/\mathfrak{p}L}$ and $\theta_{2|M/\mathfrak{p}M}$. We must show that for each $\theta_1 \in P(L, L \perp M)$ there are exactly $|P(N, M)|$ choices for θ_2.

Let θ_1 be a lift of an element in $P(L, L \perp M)$. Then $L \perp M = \theta_1(L) \perp \theta_1(L)^\perp$ where $M \approx \theta_1(L)^\perp$ by Theorem 6.3. If $w \in \theta_1(L)$ is primitive and $\gamma \in S$, then $l((\gamma w, \theta_1(L)) = l(\gamma) + \delta$. Consquently, for $w \in \theta_1(L)$

$$(w, \theta_1(L)) \subseteq \mathfrak{p}\Delta_\delta \Longrightarrow w \in \mathfrak{p}\theta_1(L) + \theta_1(L)^\perp\,. \tag{8.3}$$

If $\theta_1 \oplus \theta_2 \in P(L \perp N, L \perp M)$, then

$$\theta_2(N/\mathfrak{p}N) \subseteq \theta_1(L)^\perp/\mathfrak{p}\theta_1(L)^\perp\,. \tag{8.4}$$

It follows that $\theta_1 \oplus \theta_2 \in P(L \perp N, L \perp M)$ if and only if $\theta_2 \in P(N, \theta_1(L)^\perp)$. □

LEMMA 8.2. *If $L, M \in \mathscr{C}$, then $|P(L, M)| = |P(-L, -M)|$.*

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Proof. Trivial. □

Let M be a modular lattice and let L be a lattice such that $P(L, M) \neq \emptyset$. Express $L = L_0 \perp L_1$ where L_0 is modular and $s(L_1) > \delta$. By Lemma 8.1, there is M' modular such that $|P(L, M)| = |P(L_0, M)||P(L_1, M')|$. We proceed by first classifying the isomorphism classes of modular lattices, computing $|P(L, M)|$ for L and M modular, and then by computing $|P(L, M)|$ in the case when $l((L, L)) > \delta$. For $k \in \boldsymbol{Z}^+$, let H_k denote a hyperbolic lattice of rank $2k$.

Consider the factoring θ: $\Delta_\delta/\mathfrak{p}\Delta_\delta \to A_\delta/\mathfrak{p}A_\delta$ of the R-homomorphism $a \mapsto a + \varepsilon a^\rho$. The map is surjective, so the kernel has order $q^{\sigma - \sigma_1}$. In this section, we define σ_2 by

$$q^{\sigma_2} = |\ker(\theta|_{\Delta_{\delta+1}/\mathfrak{p}\Delta_\delta})| \tag{8.5}$$

and then $\sigma - \sigma_1 \geq \sigma_2$. For convenience, we also put $t = \sigma/\sigma_3$.

DEFINITION 8.1. A modular lattice M is called anisotropic if $P(H_1, M) = \emptyset$. Equivalently, a modular lattice M is anisotropic if and only if there does not exist a primitive $x \in M$ such that $Q(x) \equiv 0$.

We regard the zero lattice $\{0\}$ as an anisotropic space. It follows that every modular lattice is the orthogonal sum of a hyperbolic space and an anisotropic space.

We begin with a technical refinement of Lemma 7.1. For $n \in \boldsymbol{Z}$ and $k \in \boldsymbol{Z}^+$, let $\Lambda_{n,k}$ be the additive group of matrices N in $\Sigma(k, \varepsilon)$ such that

$$\begin{aligned} &N_{ij} \in \Delta_n \quad \text{for each pair } i, j \text{ and} \\ &N_{jj} \in A_n \quad \text{for each } j. \end{aligned} \tag{8.6}$$

Equivalently,

$$\Lambda_{n,k} = \{T + \varepsilon T^* : T \in M_k(\Delta_n)\}. \tag{8.7}$$

Suppose $n_0, r, k \in \boldsymbol{Z}^+$ so that $k \geq r$, $M \in \Lambda_{n,k} \cap GL_k(S)\pi^\delta$, $N \in \Lambda_{n,r}$ and $T \in M_{r,k}(S)$ is a primitive matrix for which $TMT^* - N \in \Lambda_{n+n_0,r}$. Let G be the set of cosets $[U] \in M_{r,k}(S)/\mathfrak{m}^{n_0+1}M_{r,k}(S)$ such that

$$U \equiv 0 \bmod (\mathfrak{m}^{n_0}), \qquad (T + U)M(T + U)^* - N \in \Lambda_{n+n_0+1,r}, \tag{8.8}$$

for every representative U in the coset. The number of such cosets is non-zero and depends only on $n + n_0$. Thus, for $n_1 \in \boldsymbol{Z}^+$, the number of $\mathfrak{m}^{n_1}M_{r,k}(S)$ cosets of primitive matrices T which satisfy the condition

$TMT^* - N \in \Lambda_{n+n_1,r}$ is the product of a non-zero constant that depends only on n and n_1 with the number of solutions when $n_1 = 1$.

Observe that

$$p\Lambda_{n,k} = \Lambda_{n+l(p),k}\,. \tag{8.9}$$

In terms of lattices, the above remarks imply

LEMMA 8.3. *Let M, N and N' be objects in $\mathscr{C}$ of ranks k, r and r respectively, where $k \geq r$. Suppose that M is modular and that there is an S-isomorphism $\varphi\colon N \to N'$ such that for all $x, y \in N$,*

$$Q(\varphi(x)) - Q(x) \in A_{\delta+1}\,, \tag{8.10.a}$$

$$(\varphi(x), \varphi(y)) - (x, y) \in \Delta_{\delta+1}\,. \tag{8.10.b}$$

Then $|P(N, M)| = |P(N', M)|$.

COROLLARY 8.3.1. *Let M be an anisotropic space. If $v \in M$ is primitive, then $Q(v) \in A_\delta - A_{\delta+1}$.*

Proof. Apply Lemma 8.3 to the choices $N = (0)$ and $N' = (Q(v))$. □

We begin our counting arguments.

THEOREM 8.4. *Let $r, k \in \boldsymbol{Z}^+$.*

(A) *If $N \in \mathscr{C}$ is an anisotropic space of rank r over S, then the order of $P(H_1, H_k \perp N)$ is*

$$q^{(r+2k-1)\sigma-\sigma_1}(q^{k\sigma} - q^{k\sigma-k\sigma_3})\,(q^{(r+k)\sigma-\sigma_1} + q^{(r+k-1)(\sigma-\sigma_3)+\sigma_2})\,. \tag{8.11}$$

(B) *The order of $P(H_r, H_k)$ is*

$$q^{r\{(2k-r)(2\sigma-\sigma_3)+\sigma_2-\sigma_1\}} \prod_{j=0}^{r-1} \{(q^{(k-j-1)\sigma_3+\sigma-\sigma_1-\sigma_2} + 1)(q^{(k-j)\sigma_3} - 1)\}\,. \tag{8.12}$$

Proof. (B) is an tedious consequence of an induction based on Lemma 8.1 and (A).

Fix $a \in \Delta$ so that $l(a) = \delta$. Express $H_k = M_1 \oplus M_2$ where $(M_1, M_1) = (M_2, M_2) = \{0\}$ and put $M = H_k \perp N$. Let us first classify the classes of primitive elements $z \in M/\mathfrak{p}M$ such that $Q(z) \equiv 0$. First, suppose that $v \in H_k$ and $w \in N$ so that $Q(v + w) \equiv 0$. If w is primitive then $(w, w) = -(v, v)$, and Corollary 8.3.1 implies that v must be primitive. Thus, we need only consider elements whose projection to H_k is primitive.

For the next step, fix $v_1 \in M_1$ be primitive and choose $v_2 \in M_2$ such

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

that $(v_1, v_2) = a$. Decompose $M_2 = \Delta v_2 \oplus Y$ where $Y = \{u \in M_2 : (v_1, u) = \{0\}\}$. Put

$$D = \{w \in (M_2 + N)/\mathfrak{p}(M_2 + N) : Q(v_1 + w) \equiv 0\}. \tag{8.13}$$

For each $w_0 \in Y + N$, there are exactly $q^{\sigma - \sigma_1}$ values $b \in \Delta$ such that $bv_2 + w_0 \in D$. Thus

$$|D| = q^{(rk(Y+N))\sigma + \sigma - \sigma_1} = q^{(r+k)\sigma - \sigma_1}. \tag{8.14}$$

If $y \in Y + N$ is not primitive, then $Q(y) \in A_{\sigma+2}$ and there is at least one $\alpha \in \mathfrak{m}$ such that $Q(v_1 + \alpha v_2 + y) \equiv 0$. It is now easy to check such that

$$|\{w \in D : w \text{ not primitive}\}| = q^{(r+k-1)\sigma_3(t-1)+\sigma_2} = q^{(r+k-1)\sigma - (r+k-1)\sigma_3 + \sigma_2}. \tag{8.15}$$

A similar argument also holds for fixed $v_2 \in M_2$. The number of primitive $x \in M/\mathfrak{p}M$ such that $Q(x) \equiv 0$ is computed as

$$\begin{aligned} &2(q^{k\sigma} - q^{k\sigma - k\sigma_3})q^{(r+k)\sigma - \sigma_1} - (q^{k\sigma} - q^{k\sigma - k\sigma_3})(q^{(r+k)\sigma - \sigma_1} - q^{(r+k-1)\sigma - (r+k-1)\sigma_3 + \sigma_2}) \\ &\quad = (q^{k\sigma} - q^{k\sigma - k\sigma_3})(q^{(r+k)\sigma - \sigma_1} + q^{(r+k-1)\sigma - (r+k-1)\sigma_3 + \sigma_2}). \end{aligned} \tag{8.16}$$

Next fix $x \in M$ so $Q(x) \equiv 0$. Without changing $\mathfrak{p}M$ coset, we may assume that $Q(x) = 0$. There exists $y \in M$ such that $(x, y) = a$ and $Q(y) = 0$. For $w \in M$, $(x, w) \equiv a$ and $Q(w) \equiv 0$ if and only if

$$\begin{aligned} &w = bx + cy + u \quad \text{where } b, c \in S,\ u \in \langle x, y\rangle^{\perp},\ c \equiv 1 \\ &\qquad \text{and } ba + \varepsilon(ba)^{\rho} \equiv -Q(u). \end{aligned} \tag{8.17}$$

Thus, the number of hyperbolic pairs in $M/\mathfrak{p}M$ is

$$q^{(r+2k-1)\sigma - \sigma_1}(q^{k\sigma} - q^{k\sigma - k\sigma_3})(q^{(r+k)\sigma - \sigma_1} + q^{(r+k-1)\sigma - (r+k-1)\sigma_3 + \sigma_2}). \tag{8.18}$$

□

DEFINITION 8.2. For $k \in \mathbf{Z}^+$, put

$$\Omega_k = \Lambda_{\delta,k} \cap GL_k(S)\pi^{\delta}. \tag{8.19}$$

The group $GL_k(S)$ acts on Ω_k by $u \cdot M = uMu^*$.

We divide tuples $(\Delta, \rho; \delta, \varepsilon)$ into types.

Type I: $l(A_\delta) = \delta$ and $\sigma > \sigma_1 + \sigma_2$,
Type II: $l(A_\delta) = \delta$ and $\sigma = \sigma_1 + \sigma_2$,
Type III: $l(A_\delta) \neq \delta$ and $\sigma > \sigma_1 + \sigma_2$,
Type IV: $l(A_\delta) \neq \delta$ and $\sigma = \sigma_1 + \sigma_2$.

THEOREM 8.5 (Quantitative structure theorem of modular lattices). *We work in the category $\mathscr{C}$ as defined above. Let σ, σ_1, and σ_3 be the*

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

quantities defined in (5.8) *and* (5.9), *and let* σ_2 *be as defined in* (8.5). *By "rank", we mean rank as an S-lattice.*

(A) *There does not exist an anisotropic lattice of rank greater than* 2.

(B) *If* M *and* N *are modular lattices and* $\mathrm{rk}(N) < \mathrm{rk}(M)$, *then* $P(N, M) \neq \emptyset$.

(C) *The isomorphism classes of modular lattices are classified as follows.*

Type I: *For* $r \in \boldsymbol{Z}^+$, *there exists a modular lattice of rank* r. *Any two modular lattices of the same rank are isomorphic. A modular lattice is an orthogonal sum of rank* 1 *lattices.*

There are anisotropic lattices of ranks 0 *and* 1.

Type II: *Let* $r \in \boldsymbol{Z}^+$. *There exists a modular lattice of rank* r, *There are two distinct isomorphism classes of modular lattices of rank* r. *If* L *and* M *are modular lattices of rank* r, *then* $L \perp L \approx M \perp M$.

A modular lattice is an orthogonal sum of rank 1 *lattices.*

There are anisotropic lattices of ranks 0, 1 *and* 2.

Type III: *A lattice is modular if and only if it is hyperbolic.*

Type IV: *There exists a modular lattice of rank* $r \in \boldsymbol{Z}^+$ *if and only if* r *is even. If* r *is even, there are two isomorphism classes of modular lattices of rank* r.

There is an anisotropic lattice of rank 2.

(D) *Let* M *be a modular lattice. Express* $\mathrm{rk}(M) = 2g + \lambda$ *where* $g \in \boldsymbol{Z}^+ \cup \{0\}$ *and* $\lambda \in \{0, 1\}$. *Put* $\eta(M) = 1$ *unless* g *is even and* M *is not hyperbolic; in this case, put* $\eta(M) = -1$. *Then* $|P(M, M)|$ *is*

$$q^{g\{(g+\lambda)(2\sigma-\sigma_3)-\sigma_1\}+(g+\lambda)\sigma_2}\left\{(q^{g\sigma_3}-\eta(M))\prod_{\alpha=1}^{g-1}(q^{\alpha\sigma_3}-1)\right\}\prod_{b=0}^{g+\lambda-1}(q^{b\sigma_3+\sigma-\sigma_1-\sigma_2}+1), \tag{8.20}$$

with the convention that $\{(q^{g\sigma_3}-\eta(M))\prod_{\alpha=1}^{g-1}(q^{\alpha\sigma_3}-1)\}$ *is* 1 *if* $g = 0$.

COROLLARY 8.5.1 (Context of Theorem 8.5). *For* $k \in \boldsymbol{Z}^+$, Ω_k *is non-empty if* k *is* $(\Delta, \rho; \delta, \varepsilon)$ *is of Type* I *or* II, *or* k *is even. If* $\Omega_k \neq \emptyset$, *then the number of orbits under conjugation by* $GL_k(S)$ *is* 1 *if* $(\Delta, \rho; \delta, \varepsilon)$ *is of Type* I *or* III *and* 2 *if* $(\Delta, \rho; \delta, \varepsilon)$ *is of Type* II *or* IV. *If* $(\Delta, \rho; \delta, \varepsilon)$ *is of Type* I or II, *then each orbit contains a diagonal matrix.*

COROLLARY 8.5.2 (Context of Theorem 8.5). *Let* M *and* N *be modular lattices. If* $M \otimes_R F$ *and* $N \otimes_R F$ *are isomorphic as hermitian spaces over* Δ, *then* M *and* N *are isomorphic as lattices over* S.

Proof. The corollaries are simple consequences of Theorem 8.5. Their

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

verifications are left to the reader.

For $k \in \boldsymbol{Z}^+$, define $\sim$ on Ω_k by

$$M \sim N \Longleftrightarrow M \equiv N \bmod (\mathfrak{p}M_k(\Delta_\delta)) \quad \text{and} \quad M_{jj} \equiv N_{jj} \bmod (\mathfrak{p}A_\delta) \quad \text{for each } j\,. \tag{8.21}$$

Put $\Omega_k' = \Omega_k/\sim$. If $M \sim N$, then M and N lie in the same $GL_k(S)$-orbit by Lemma 7.2. Thus, the action by $GL_k(S)$ on Ω_k factors to an action by $G = GL_k(S/\mathfrak{p}S)$ on Ω_k'.

We must classify the modular spaces of $(\Delta, \rho; \delta, \varepsilon)$. We do so by giving a laborious analysis of anisotropic spaces when $k = 1, 2$, and then deducing all other results from these two cases. In particular, Theorem 8.4 determines the order of the $|P(N, N)|$ in general once we give formulas for anisotropic lattices. The number of isomorphism classes of modular lattices of rank k is the number of G-orbits of Ω_k'.

Case 1: $l(A_\delta) = \delta$

First, put $\Omega = \Omega_1$. Let H be a hyperbolic plane and let $\{e_1, e_2\}$ be a hyperbolic pair of H. Let $a \in \Omega$. If $v \in H$ and $Q(v) \equiv a$, then v is primitive—in fact, if $v = \lambda e_1 + \mu e_2$, then λ and μ must be S-units. For each S-unit λ, there exists $\mu \in S$ such that $Q(\lambda e_1 + \mu e_2) \equiv a$, and the number of such values mod $(\mathfrak{p})$ is $q^{\sigma - \sigma_1}$. Hence,

$$|P((a), H)| = q^{\sigma-\sigma_1}(q^\sigma - q^{\sigma-\sigma_3})\,. \tag{8.22}$$

Now $H \approx (a) \perp (-a)$, and so

$$|P((a), (a))| = |P((-a), (-a))| = |P(H, H)|/|P((a), H)| = q^{\sigma-\sigma_1} + q^{\sigma_2}\,. \tag{8.23}$$

Note that $|P((a), (a))|$ does not depend on a.

Define $\tau \in \boldsymbol{Z}^+$ by

$$q^\tau = |\{b \in A_\delta\colon\ l(b) > \delta\}/\mathfrak{p}A_\delta|\,. \tag{8.24}$$

Each G-orbit of Ω' contains $|G|/(q^{\sigma-\sigma_1} + q^{\sigma_2})$ points. The number of orbits is

$$\begin{aligned}(q^{\sigma_1} - q^\tau)(q^{\sigma-\sigma_1} + q^{\sigma_2})/(q^\sigma - q^{\sigma-\sigma_3}) \\ = 1 + \{q^{\sigma_1+\sigma_2} + q^{\sigma-\sigma_3} - q^{\sigma+\tau-\sigma_1} - q^{\tau+\sigma_2}\}/(q^\sigma - q^{\sigma-\sigma_3})\,.\end{aligned} \tag{8.25}$$

First, suppose that the number of orbits is 1. Now if $d, e, f \in Z$ and $d > e, f$, then $q^d \geq q^e + q^f$. Hence either

$$\sigma_1 + \sigma_2 = \sigma + \tau - \sigma_1 \quad \text{and} \quad \sigma - \sigma_3 = \tau + \sigma_2\,, \quad \text{or} \tag{8.26.a}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

(8.26.b) $$\sigma_1 + \sigma_2 = \tau + \sigma_2 \quad \text{and} \quad \sigma - \sigma_3 = \sigma + \tau - \sigma_1 .$$

Since $\sigma_1 > \tau$, the latter equations do not hold. The conditions of (8.26.a) are equivalent to $\sigma_3 = 2(\sigma_1 - \tau)$ and $\sigma = \sigma_1 + \sigma_2 + (\sigma_3/2)$.

Next, suppose that the number of orbits is greater than 1. First, suppose that $\sigma_1 + \sigma_2 < \sigma$. Then we have

(8.27) $$q^{\sigma_1+\sigma_2} + q^{\sigma-\sigma_3} > q^{\sigma} - q^{\sigma-\sigma_3},$$
$$\Longrightarrow 3q^{\sigma-1} > q^{\sigma} \Longrightarrow q = 2 .$$

Substituting $q = 2$ into (8.25), we quickly see that $\sigma_3 = 1$. It follows that

(8.28) $$(2^{\sigma_1+\sigma_2} - 2^{\sigma+\tau-\sigma_1} - 2^{\tau+\sigma_2})/2^{\sigma-1} \in \boldsymbol{Z}^+ \cup \{0\} .$$

From $\sigma_1 + \sigma_2 \leq \sigma - 1$, we get

(8.29) $$2^{\sigma_1+\sigma_2} = 2^{\sigma+\tau-\sigma_1} + 2^{\tau+\sigma_2} = 2^{\tau+\sigma_2}(2^{\sigma-\sigma_1-\sigma_2+1}) .$$

But $\sigma - \sigma_1 - \sigma_2 \in \boldsymbol{Z}^+$, so the last equation is impossible.

Assume $\sigma = \sigma_1 + \sigma_2$. The number of orbits is

(8.30) $$2 + \{2q^{\sigma-\sigma_3} - 2q^{\tau+\sigma_2}\}/(q^{\sigma} - q^{\sigma-\sigma_3}) .$$

The righthand ratio is 0 if and only if $\sigma_3 = \sigma_1 - \tau$. Reasoning as above, we find that the ratio is a positive integer only if $q = 2$, $\sigma_3 = 1$ and $\tau = \sigma_1 - 2$. If (Δ, ρ) produces these parameters, then $\Delta = F$ or Δ is a ramified quadratic extension of F. But $\tau \geq 0$ and so $\sigma_1 = 2$, which is not true in either case. Hence, the number of orbits must be 2.

We need a special remark in the Type II case. Let b and c represent the distinct orbits of Ω. We claim that $(b) \perp (b) \approx (c) \perp (c)$. Suppose that $v \in (b) \perp (b)$ such that $Q(v) = c$. Then $(Sv)^{\perp} = Sw$ where $(c) \perp (Q(w)) \approx (b) \perp (b)$. Now $(Q(w))$ is not isomorphic to (b), and we are done. Suppose $c \notin \mathrm{Im}\,(Q_{(b)\perp(b)})$. Under this assumption,

(8.31) $$\mathrm{Im}\,(Q_{(b)}) = \mathrm{Im}\,(Q_{(b)\perp(b)}) .$$

But now a simple induction implies that $\mathrm{Im}\,(Q_{(b)}) = \mathrm{Im}\,(Q_N)$ where N is a finite orthogonal sum of spaces isomorphic to (b). The sum N_0 of q copies contains a primitive v' such that $Q(v') \equiv 0$, which implies that H imbeds into N_0. But then $v \in \mathrm{Im}\,(Q_{N_0})$, which leads to a contradiction.

Still assuming that $l(a) = \delta$, suppose that N is a modular space of rank $k > 1$. Then N contains a fundamental lattice of rank 1 or 2. In either case, it is easy to show that N must contain a primitive element

v such that $l(Q(v)) = \delta$. By induction, we see that N is an orthogonal sum of rank 1 lattices. In the Type I case, this implies that the isomorphism class of N is determined by its rank. In the Type II case, our special remark implies that there are two isomorphism classes for each rank. For either type, we can also conclude that if N and N' are two modular lattices and $\operatorname{rank}(N) < \operatorname{rank}(N')$, then $P(N, N') \neq \varnothing$.

Let N be an anisotropic rank 2 lattice in the Type II situation. Let $a \in \Omega$ and put $g = |P((a), (a))|$. Now $N = (a) \perp (b)$ for some $b \in \Omega$, and so

$$|P((a), N)| = |P(N, N)|/|P((b), (b))| = |P(N, N)|/g\,. \tag{8.32}$$

Now $\sum_{a \in \Omega'} |P((a), N)|$ is the number of primitive elements of $N/\mathfrak{p}N$. Thus,

$$\begin{aligned} &2(|G|/g)(|P(N, N)|/g) = q^{2\sigma} - q^{2\sigma - 2\sigma_3}\,, \\ \Longrightarrow\ &|P(N, N)| = 2q^{\sigma + 2\sigma_2 - \sigma_3}(q^{\sigma_3} + 1)\,. \end{aligned} \tag{8.33}$$

The remaining claims for the Types I and II situations follow easily.

Case 2: $l(A_\delta) > \delta$.

Let N be an anisotropic lattice with matrix $\begin{pmatrix} b & a \\ \varepsilon a^\rho & c \end{pmatrix}$ over a basis f_1, f_2. We compute $|P(N, N)|$ by studying $|P(N, H_2)|$.

Express $H_2 = M_1 \oplus M_2$ where $(M_1, M_1) = (M_2, M_2) = \{0\}$. If $v_1 \in M_1$ and $v_2 \in M_2$ so that $Q(v_1 + v_2) \equiv b$, then v_1 and v_2 must be primitive (because $b \notin A_{\delta+1}$). For $v_1 \in M_1$ primitive, there is $v_2 \in M_2$ such that $M_2 = \Delta v_2 \oplus ((\Delta v_1)^\perp \cap M_2)$. Thus, the number of $y \in M_2/\mathfrak{p}M_2$ such that $Q(v_1 + y) \equiv b$ is $q^{2\sigma - \sigma_1}$. Next, suppose $e_1 \in M$ so that $Q(e_1) \equiv b$, and put $b' = Q(e_1)$. There is $y \in H_2$ so that the matrix of the form with respect to $\{e_1, y\}$ is $\begin{pmatrix} b' & a \\ \varepsilon a^\rho & c' \end{pmatrix}$. Now $\langle e_1, y\rangle^\perp$ is isomorphic to $-\begin{pmatrix} b' & a \\ \varepsilon a^\rho & c' \end{pmatrix}$. Thus, we can choose $e_2 \in M$ so that the matrix with respect to $\{e_1, e_2\}$ is $\begin{pmatrix} b' & a \\ \varepsilon a^\rho & 0 \end{pmatrix}$. Hence, there are e_3, e_4 such that the matrix with respect to e_1, e_2, e_3, e_4 is

$$\begin{bmatrix} b' & a & 0 & 0 \\ \varepsilon a^\rho & 0 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & \varepsilon a^\rho & 0 \end{bmatrix}. \tag{8.34}$$

Let $y = \alpha e_1 + \beta e_2 + u$ where $u \in \langle e_3, e_4\rangle$. Then

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$$(8.35)\qquad (e_1, y) \equiv a \Longleftrightarrow \beta \equiv 1 - \varepsilon\alpha b' a^{-\rho}\,,$$
$$Q(y) \equiv c \Longleftrightarrow Q(u) \equiv c - \alpha b'\alpha^{\rho} - \alpha a\beta^{\rho} - \varepsilon(\alpha a\beta^{\rho})^{\rho}\,.$$

The two equations imply that $Q_{H_2}(u) \in Q_N(f_2 - \alpha f_1) + A_{\delta+1}$. If (α, u) solves the two equations, then $u = \lambda e_3 + \mu e_4$ where λ, μ are S-units. The number of solutions is $q^{2\sigma-\sigma_1}(q^{\sigma} - q^{\sigma-\sigma_3})$. Now $-N$ is also anisotropic and $N \perp -N \approx H_2$, so

$$(8.36)\qquad |P(N, H_2)| = q^{4\sigma-2\sigma_1}(q^{2\sigma} - q^{2\sigma-2\sigma_3})(q^{\sigma} - q^{\sigma-\sigma_3})\,,$$
$$|P(N, N)| = |P(H_2, H_2)|/|P(-N, H_2)|$$
$$= q^{\sigma+2\sigma_2-\sigma_3}(q^{\sigma_3+\sigma-\sigma_1-\sigma_2} + 1)(q^{\sigma-\sigma_1-\sigma_2} + 1)\,.$$

Put $\Omega' = \Omega'_2$. Inspection shows that

$$(8.37)\qquad |\Omega'| = q^{2\sigma_1}(q^{\sigma} - q^{\sigma-\sigma_3})\,.$$

The orbit of hyperbolic matrices in Ω' contains

$$(8.38)\qquad q^{2\sigma-2\sigma_3+\sigma_1-\sigma_2}(q^{2\sigma_3} - 1)/(q^{\sigma-\sigma_1-\sigma_2} + 1)$$

elements. Suppose that $\sigma_3 < \sigma - \sigma_1 - \sigma_2$. Then $\sigma - \sigma_1 - \sigma_2 \geq 1$, $q^{\sigma-\sigma_1-\sigma_2} + 1$ is prime to q, and (8.38) implies that $2\sigma_3 > \sigma - \sigma_1 - \sigma_2$. Moreover, $q^{\sigma-\sigma_1-\sigma_2} + 1$ divides

$$(8.39)\qquad q^{2\sigma_3} + q^{\sigma-\sigma_1-\sigma_2} = q^{\sigma-\sigma_1-\sigma_2}(q^{2\sigma_3-\sigma+\sigma_1+\sigma_2} + 1)\,.$$

But then $2\sigma_3 \geq 2(\sigma - \sigma_1 - \sigma_2)$, which is a contradiction.

If $\sigma_3 = \sigma - \sigma_1 - \sigma_2$, then (8.38) equals (8.37) and there is one orbit.

Suppose $\sigma_3 > \sigma - \sigma_1 - \sigma_2$. The number of anisotropic orbits is computed to be

$$(8.40)\qquad q^{-\sigma+\sigma_1+\sigma_2}(q^{\sigma_3-\sigma+\sigma_1+\sigma_2} - 1)(q^{\sigma_3+\sigma-\sigma_1-\sigma_2} + 1)/(q^{2\sigma_3} - 1)\,.$$

This is a q-adic integer only if $\sigma = \sigma_1 + \sigma_2$, and in this case there is only one anisotropic orbit.

Let N be an anisotropic lattice of rank 2. Then $-N \approx N$. If N' is another anisotropic lattice, then N is an orthogonal sum of anisotropic fundamental lattices. But the sum of two such lattices is isomorphic to $N \perp -N \approx H_2$, and so $N' \approx N$ or $N' = \{0\}$.

All claims concerning Types III and IV follow. □

We turn to the second problem—compute $|P(L, M)|$ when M is modular and $s(L) > \delta$. We write $N \sim N'$ if there is an S-isomorphism $\varphi\colon N \to N'$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

which fulfills the hypothesis of Lemma 8.3. For the moment, fix L a non-trivial hermitian lattice and consider $\mathscr{L}$ the class of lattices L_1 such that $L \sim L_1 \perp D$ for some trivial hermitian lattice D.

Let $L_1 \in \mathscr{L}$. First, suppose $v \in L_1$ such that $Q(v) \in A_{\delta+1}$, and $l((v, L_1)) = s(L_1)$. If $l((v, v)) = s(L_1)$, then $L_1 = (Sv) \perp L'$ for some L', and $L_1 \sim (0) \perp L'$. If $l((v, v)) > s(L_1)$, then there exists w so that $\{v, w\}$ is fundamental and $L_1 = \langle v, w\rangle \perp L'$. The matrix of the form with respect to $\{v, w\}$ is $\begin{pmatrix} b & a \\ \varepsilon a^\rho & c \end{pmatrix}$ and so $L_1 \sim \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} \perp L'$. Next, observe that if $L_1 = A \perp B$ where A is a rank 2 fundamental lattice given by $\begin{pmatrix} b & a \\ \varepsilon a^\rho & c \end{pmatrix}$, then $L_1 \sim \begin{pmatrix} b & 0 \\ 0 & c \end{pmatrix} \perp B$.

We conclude that there is an element $L_1 \in \mathscr{L}$ which is given by a diagonal matrix and with the property that $Q(v) \notin A_{\delta+1}$ for $v \in L_1$ primitive. Formally, we have

DEFINITION 8.3. Let

$$V = \{x \in A_\delta \colon l(x) > \delta\}/A_{\delta+1}\,. \tag{8.41}$$

Then V becomes an $S/\mathfrak{m}$-module under an action with the property that

$$\forall a \in S, \quad \forall x \in A_\delta, \quad \bar{a} \cdot \bar{x} = \overline{axa^\rho}\,, \tag{8.42}$$

where "$\bar{\ }$" denotes the equivalence class of an element in $A_\delta/A_{\delta+1}$ or $S/\mathfrak{m}$. If $L \in \mathscr{C}$ so that $s(L) > \delta$, then the function Q_L composed with ϕ: $A_\delta \to V$ is an S-homomorphism. Define the defect of L to be

$$\operatorname{def}(L) = \operatorname{rank}_{S/\mathfrak{m}} \operatorname{Im}(\phi \circ Q_L)\,. \tag{8.43}$$

LEMMA 8.6. *Let $L \in \mathscr{C}$ such that $s(L) > m$. Then there exists $L_1 \in \mathscr{C}$ (possibly of rank 0) such that $L \sim L_1 \perp D$ for a trivial lattice D, and $\phi \circ Q_{L_1}$ induces an injection on $L_1/\mathfrak{m}L_1$. Moreover* $\operatorname{rank}_S(L_1) = \operatorname{def}(L)$.

Let us compute $d = \dim_{S/\mathfrak{m}}(V)$ for each of the Types. The space $A_{\delta+1}/\mathfrak{p}A_\delta$ is the image of θ of (8.5) restricted to $\Delta_{\delta+1}/\mathfrak{p}\Delta_\delta$. Thus,

$$|A_{\delta+1}/\mathfrak{p}A_\delta| = q^{\sigma-\sigma_3-\sigma_2}\,, \tag{8.44}$$

and

$$q^{\sigma-\sigma_3-\sigma_2+d\sigma_3} = |A_\delta/\mathfrak{p}A_\delta| - |\Omega_1'|\,. \tag{8.45}$$

Hence,

$$d = 0 \text{ for Types I, II and III, and } d = 1 \text{ for Type IV}\,. \tag{8.46}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Let M be a modular lattice, $D \in \mathscr{C}$, and let S_0 denote the lattice S with the trivial form. The number of $v \in M/\mathfrak{p}M$ for which $Q(v) \equiv 0$ is computed in (8.16). If $v \in M$ so that $Q(v) = 0$, we may express $M = \langle v, w\rangle \perp M'$ where $\{v, w\}$ is a hyperbolic pair. An extension of $1 \mapsto v$ to a S-homomorphism $\varphi\colon S_0 \perp D \to M$ is determined by its projections $\varphi_1\colon D \to M'$ and $\varphi_2\colon D \to \langle v, w\rangle$. It follows that if N is anisotropic of rank r and $k \in \boldsymbol{Z}^+$, then

$$(8.47)\qquad \begin{aligned} |P(S_0 \perp D, H_k \perp N)| &= q^{(r+2k-1)(\sigma-\sigma_3)+\sigma_2+rk(D)\sigma}(q^{k\sigma_3}-1) \\ &\times (q^{(r+k-1)\sigma_3+\sigma-\sigma_1-\sigma_2}+1)|P(D, H_{k-1} \perp N)|\,. \end{aligned}$$

Next we make a special comment in the Type IV situation. Fix $b \in A_\delta - A_{\delta+1}$. Let $M \in \mathscr{C}$ be modular of rank $2k$. Now $\mathrm{rk}\, V = 1$, so if $c \in A_\delta - A^\sigma{}_{+1}$, there exists $u \in S - m$ such that $c \in ubu^\rho + A_{\delta+1}$. Consequently, $|P((c), M)| = |P((b, M)$. The number of primitive members of M is

$$(8.48)\qquad |(A_\delta - A_{\delta+1})/\mathfrak{p}A_\delta||P((b, M)| + |A_{\delta+1}/\mathfrak{p}A_\delta||P((0, M)|\,.$$

Thus,

$$(8.49)\qquad |P((b), M)| = q^{2k\sigma-\sigma_1-k\sigma_3}(q^{k\sigma_3}-\eta(M))\,.$$

Computation produces

THEOREM 8.7 (Context of Theorem 8.5). *Let $D, M \in \mathscr{C}$. Suppose M is modular lattice, $\mathrm{rk}\,(D) > 0$ and $s(D) > \delta$. Put $d = \mathrm{rk}\,(D)$, $\mu = \mathrm{def}\,(D)$, $\eta = \eta(M)$, and express $\mathrm{rk}\,(M) = 2g + \lambda$ for $g \in \boldsymbol{Z}$ and $\lambda \in \{0, 1\}$. Then $P(D, M) \neq \varnothing$ if and only if $d = \mu = 1$ or $P(H_{d-\mu}, M) \neq \varnothing$. If $P(D, M) \neq \varnothing$, then it has order*

$$(8.50)\qquad \begin{aligned} &q^{d\{(2g+\lambda-d)(\sigma-\sigma_3)+\sigma_2+(d-1)\sigma/2\}} \\ &\times \Big\{(q^{(g-d+\lambda)\sigma_3+\sigma-\sigma_1-\sigma_2}+(1-\mu)\eta)\prod_{\alpha=1}^{d-1}(q^{(g-\alpha+\lambda)\sigma_3+\sigma-\sigma_1-\sigma_2}+\eta) \\ &\times \prod_{\alpha=0}^{d-1}(q^{(g-\alpha)\sigma_3}-\eta)\,. \end{aligned}$$

with the convention that the second term $\{*\}$ is 1 if $d = 0$.

§ 9. Hermitian lattices and the power series

Fix $\delta = l(\mathscr{D})$ for this section. For $r \in \boldsymbol{Z}^+$ and $n \in \boldsymbol{Z}$, put

$$(9.1)\qquad \begin{aligned} \Sigma(r; n) &= \{T \in \Sigma(r, \varepsilon^\rho)\colon l(T_{ij}) \geq n \text{ for each pair of indices } (i, j)\}\,, \\ \Sigma(r; n)^* &= \{T \in \Sigma(r, \varepsilon)\colon \chi(T\cdot\Sigma(r; n)) = \{1\}\}\,, \\ \mathscr{D}_n &= \{d \in \Delta\colon \forall\, b \in \Delta,\ l(b) \geq n \Longrightarrow \chi(bd + b^\rho d^\rho) = 1\}\,. \end{aligned}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Clearly $\mathscr{D}_n = \Delta_{\delta-n}$. For $T \in M_r(\Delta)$, also let

$$j_n(T) = [TS^r + \Delta_n^r : \Delta_n^r]. \tag{9.2}$$

We begin with a Gauss Integral.

THEOREM 9.1. *Let $r, k \in Z^+$, $n \in Z$, and $N \in \Sigma(r, \varepsilon^\rho)$. Let H be a $2k \times 2k$ matrix which represents a hyperbolic lattice of type (ρ, ε) and denominator $n - \delta$, and let μ be the Haar measure on $M_{2k,r}(S)$ for which $\mu(M_{2k,r}(S)) = 1$. Then*

$$\int_{x \in M_{2k\times r}(S)} \chi(HxNx^*)d\mu(x) = q^{-j_n(N)k} \tag{9.3}$$

Proof. When we apply this lemma later, the "N" term here will correspond to a variable on $\Sigma(r, \varepsilon^\rho)$. For that reason, we have written the hypothesis so that N has type (ρ, ε^ρ) and H has type (ρ, ε). In this argument, however, we apply lemmas from previous sections to the matrix N regarded as a (ρ, ε^ρ)-hermitian lattice.

Clearly we are free to replace H by any matrix of the form uHu^* for $u \in GL_{2k}(S)$. Let $d \in \Delta$ so that $l(d) = \delta - n$, and put

$$H_k = \operatorname{diag}\left\{\begin{bmatrix} 0 & \varepsilon d^\rho \\ d & 0 \end{bmatrix}, \cdots, \begin{bmatrix} 0 & \varepsilon d^\rho \\ d & 0 \end{bmatrix}\right\} \in M_{2k}(\Delta). \tag{9.4}$$

We do the proof in three steps.

Step I: $k = 1$ and $N\begin{bmatrix} b & a \\ \varepsilon^\rho a^\rho & c \end{bmatrix}$ where $a \in \Delta^*$, $b = \varepsilon^\rho b^\rho$, $c = \varepsilon^\rho c^\rho$, and $l(b), l(c) > l(a)$.

Using coordinates $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ on $M_2(S)$, the integrand becomes

$$\chi(\varepsilon d^\rho y b w^\rho + \varepsilon d^\rho y a x^\rho + d^\rho z a^\rho w^\rho + \varepsilon d^\rho z c x^\rho + dwby^\rho + dwaz^\rho + \varepsilon^\rho dxa^\rho y^\rho + dxcz^\rho). \tag{9.5}$$

Composing the integrand with the measure preserving map $(w, x, y, z) \mapsto (w, x, y, z - yb^\rho a^{-\rho})$, we get

$$\chi(\varepsilon d^\rho y a x^\rho + d^\rho z c^\rho x^\rho - d^\rho y b^\rho a^{-\rho} c^\rho x^\rho + \varepsilon^\rho dxa^\rho y^\rho + dxcz^\rho - dxca^{-1}by^\rho) \times \chi(d^\rho z a^\rho w^\rho + dwaz^\rho). \tag{9.6}$$

Fix x, y, z. The map $w \mapsto \chi(d^\rho z a^\rho w^\rho + dwaz^\rho)$ is a character. Thus, the integral over w vanisheds unless $d^\rho z a^\rho \in \mathscr{D}$—that is, unless $l(z) \geq n - l(z)$.

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Note that when $l(z) \geq n - l(a)$, then $\chi(d^\rho z c^\rho x^\rho + d^\rho x c z^\rho) = 1$ as well. Thus, the integral equals

$$(9.7) \qquad q^{-j_n(a)} \int_{x,y \in S} \chi(\varepsilon d^\rho y a x^\rho - d^\rho y b^\rho a^{-\rho} c^\rho x^\rho + \varepsilon^\rho d x a^\rho y^\rho - d x c a^{-1} b y^\rho) d\mu(x, y) .$$

The argument is

$$(9.8) \qquad dx(\varepsilon^\rho a^\rho - c a^{-1} b) y^\rho + d^\rho \{x(\varepsilon^\rho a^\rho - c a^{-1} b) y^\rho\}^\rho ,$$

where $l(\varepsilon^\rho a^\rho - c a^{-1} b) = l(a)$. Reasoning as before, we conclude that the integral is $q^{-2j_n(a)}$. By (6.3), $j_n(N) = 2j_n(a)$.

Step II: $k = 1$ and $N = (b)$, where $b = \varepsilon^\rho b^\rho$

We allow $b = 0$. In terms of the variable matrix $\begin{pmatrix} x \\ y \end{pmatrix}$, the integrand is

$$(9.9) \qquad \chi(d^\rho y b^\rho x^\rho + dx b y^\rho) .$$

Reasoning as in Step I, we deduce that the integral is $q^{-j_n(b)}$.

Step III: General situation

Let $N \in M_r(\Delta)$ so that $N = \varepsilon^\rho N^*$. Put $H = H_1$. The matrix N determines a hermitian form on S^r. By Remark 6.1, there is $u \in GL_r(S)$ such that

$$(9.10) \qquad u N u^* = \operatorname{diag}\{N_1, \cdots, N_a\}$$

where each N_j is a $b_j \times b_j$ matrix which satisfies the hypothesis of Step I or II. Conjugation by u affects neither the j factor nor the integral, so it suffices to prove the theorem when $N = \operatorname{diag}\{N_1, \cdots, N_a\}$.

The integrand becomes

$$(9.11) \qquad \chi(\textstyle\sum_s \sum_t H x_{ts} N_s (x^*)_{st}) = \prod_{s,t} \chi(H x_{ts} N_s (x^*)_{ts})$$

where x_{ij} varies over $M_{2,b_j}(S)$. The integral becomes

$$(9.12) \qquad \prod_{s=1}^{a} q^{-j_n(N_s)k} = q^{-j_n(N)k} . \qquad \square$$

For $n \in \boldsymbol{Z}$ and $k \in \boldsymbol{Z}^+$, let $H_{k,n}$ be a $2k \times 2k$ matrix which determines a hyperbolic (ρ, ε)-hermitian lattice of denominator $n - \delta$. For $m, k, r \in \boldsymbol{Z}^+$ so $2k \geq r$ and $N \in \Sigma(r : n)^\sharp$, put

$$(9.13) \qquad A_0(k, n, N; m) = \{T \in M_{r,2k}(S) : T \bmod (m) \in A(H_{k,n}, N; m)\}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

where $A(H_{k,n}, N; m)$ is defined in (7.10) with respect to $E(r) = \Sigma(r; n)^\#$. Then $|A(H_{k,n}, N; m)|$ is the measure of the set $A_0(k, n, N; m)$ with respect to the Haar measure μ' on $M_{r,2k}(S)$ such that $\mu'(p^n M_{r,2k}(S)) = 1$. Clearly $\mu' = q^{2mrk\sigma}\mu$.

Let ν denote the Haar measure on $\Sigma(r, \varepsilon^\rho)$ such that $\nu(\Sigma(r; n)) = 1$. For $E \in \Sigma(r: n)^\#$,

$$\int_{\mathfrak{p}^{-m}\Sigma(r;n)} \chi(Ex)d\nu(x) = \begin{cases} 0 & \text{if } E \notin \mathfrak{p}^m\Sigma(r; n)^\#, \\ q^{m\sigma(r)} & \text{if } E \in \mathfrak{p}^m\Sigma(r; n)^\#. \end{cases} \tag{9.14}$$

Then

$$|A(H_{k,n}, N; m)| = q^{2mrk\sigma - m\sigma(r)} \int_{T \in M_{r,2k}(S)} \int_{x \in \mathfrak{p}^{-m}\Sigma(r;n)} \chi((TH_{k,n}T^* - N)x)d\nu(x)d\mu(T)\,. \tag{9.15}$$

Interchanging the order of integration and invoking Theorem 9.1, we get

$$q^{m\sigma(r)-2mkr\sigma}|A(H_{k,n}, N; m)| = \int_{\mathfrak{p}^{-m}\Sigma(r,n)} \chi(-Nx)q^{-j_n(x)k}d\nu(x)\,. \tag{9.16}$$

Define formal power series in an indeterminate t by

$$\begin{aligned} \alpha_n^m(N, t) &= \sum_{x \in \mathfrak{p}^{-m}\Sigma(r;n)/\Sigma(r;n)} \chi(-Nx)t^{-j_n(x)}\,, \\ \alpha_n(N, t) &= \sum_{x \in \Sigma(r,\varepsilon\rho)/\Sigma(r;n)} \chi(-Nx)t^{-j_n(x)}\,. \end{aligned} \tag{9.17}$$

It is routinely verified that $\alpha_n(N, t)$ is a properly defined power series, and that for $t_0 \in \boldsymbol{C}$ with $|t_0|$ sufficiently small, we have $\lim_{m\to\infty}\alpha_n^m(N, t_0) = \alpha_n(-N, t_0)$. Observe that $\alpha_n^m(N, t) = \alpha_n(-N, t)$ and $\alpha_n(N, t) = \alpha_n(-N, t)$.

LEMMA 9.2. *Let $n \in \boldsymbol{Z}^+$, $r \in \boldsymbol{Z}^+$, and $N \in \Sigma(r; n)^\# \cap GL_r(\Delta)$. Then there exists $b \in \boldsymbol{Z}^+$ such that $\alpha_n^m(N, t) = \alpha_n(N, t)$ for each $m \geq b$.*

Proof. Let $b \in \boldsymbol{Z}^+$ be the bound in Theorem 7.3 for $\delta_0 = l(\mathscr{D}_n)$ and $E = \Sigma(1; n)^\#$. Remark 7.1 and equation (9.16) imply that $\alpha_n^m(N, q^{-k}) = \alpha_n^b(N, q^{-k})$ for all $M \geq b$ and $k \geq r/2$. Thus, for $m \geq b$ we have $\alpha_n^m(N, t) = \alpha_n^b(N, t)$. It follows that $\alpha_n(N, t) = \alpha_n^b(N, t)$. □

COROLLARY 9.2.1. *For $n \in \boldsymbol{Z}$,*

$$\Sigma(1; n)^\# = \{d + \varepsilon d^\rho\colon\ d \in \mathscr{D}_n\}\,, \tag{9.18}$$

where $\mathscr{D}_n$ and $\Sigma(1; n)^\#$ are given in (9.1). *Equivalently,*

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$$A_{\delta-n} = \{d \in \Sigma(1, \varepsilon)\colon \chi(d \cdot \Sigma(1; n)) = \{1\}\}\,. \tag{9.19}$$

Proof. Clearly (9.18) implies (9.19). Let $b \in \Sigma(1; n)^\sharp - \{0\}$, and put $N = (b)$. By Lemma 9.2, $\alpha_n(N, t)$ is a polynomial whose constant term is obviously 1. It follows that there is $k \in \boldsymbol{Z}^+$ for which $A(H_{k,n}, N; m)$ is not empty for all m greater than some bound. The reasoning of Section 7 (Lemma 7.2 and Theorem 7.3) implies that there is a primitive form-preserving injection of $(c^{-1}bc^{-*})$ into H_k for some $c \in S - \{0\}$. Thus, $c^{-1}bc^{-*} \in A_{\delta-n}$, and our claim follows. □

We can now prove half of the claims in Section 5.

Proof of Lemma 5.1. Let π be a generator of the maximal ideal of S. Then $c \mapsto c\pi^*$ induces an additive isomorphism $\Omega(\pi) \xrightarrow{\sim} \Sigma(1; 1)/\Sigma(1; 2)$. By Lemma 9.2, the character group of $\Sigma(1; 1)/\Sigma(1; 2)$ is $A_{\delta-2}/A_{\delta-1}$. The latter space is isomorphic to $A_\delta/A_{\delta+1}$ under $\bar{c} \mapsto \overline{\pi c \pi^*}$. Now

$$q^{\sigma_1} = [A_\delta\colon \mathfrak{p}A_\delta] = [A_{\delta+1}][A_{\delta+1}\colon \mathfrak{p}A_\delta]\,, \tag{9.20}$$

where we have established that $[A_\delta\colon A_{\delta+1}] = q^{\sigma_4}$. The map θ used in (5.9) is surjective, and so $[A_{\delta+1}\colon \mathfrak{p}A_\delta] = q^{\sigma-\sigma_3-\sigma_2}$. □

Proof of Theorem 5.3 *when* $r = m$. We use the formulas in (8.20), (8.50) and (7.19) with the convention "M" is hyperbolic of denominator $-\delta$ and of rank $2k$ and $n_1 = n_2 = 0$. For $g, h \in \boldsymbol{Z}^+ \cup \{0\}$, $\lambda, \mu \in \{0, 1\}$ and $\eta \in \{-1, 1\}$ such that

$$\mu \leq h\,, \quad \eta = 1 \quad \text{if } \lambda = 1\,, \quad \text{and} \quad \mu = 1 \text{ only if } \lambda = 0\,, \tag{9.21}$$

let $R(g, h, \lambda, \eta, \mu; t)$ be the polynomial

$$\begin{aligned} &\left\{(1 + \eta(1-\mu)q^{(g+h)\sigma_3+\sigma_1+\sigma_2-\sigma}t^{\sigma_3}) \prod_{\alpha=0}^{g+h-1}(1 + q^{\alpha\sigma_3+\sigma_1+\sigma_2-\sigma}t^{\sigma_3})\right\} \\ &\quad \times \prod_{j=0}^{g+h+\lambda-1}(1 - q^{\alpha\sigma_3}t^{\sigma})\,, \end{aligned} \tag{9.22}$$

with the convention that the bracketed product is 1 if $g + h = 0$. Suppose $C \in \Phi_r$ such that $N[C] \in \Sigma(r; S)^\sharp$. Express the lattice determined by $N[C]$ as $L \perp D$ where L is unramified and $s(D) > \delta$. Then the summand in (7.19) corresponding to the coset of C is $R(g, \operatorname{rank}(D), \theta, \eta(L), \operatorname{def}(D); q^{-k})$ where $2g + \lambda = \operatorname{rk}(L)$. Consequently, $\alpha(N, t) = \alpha_0(N, t)$ agrees with the sum of polynomials $R(g, \operatorname{rank}(D), \lambda, \eta(L), \operatorname{def}(D); t)$ taken over cosets C. Some simple identities are

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

(9.23) $R(g, h, \lambda, \eta, \mu; t) \mid R(g-1, h+2, \lambda, \eta', \mu'; t)$,
$R(g, h, \lambda, \eta, 1; t) \mid R(g, h, \lambda, \eta, 0; t)$,
$R(g, 0, 0, \eta, 0; t) \mid R(g-1, 1, 1, 1, 0; t) \mid R(g-1, 2, 0, \eta, \mu; t)$,
$R(g, 0, 0, \eta, 0; t) \mid R(g, 1, 0, 1, 0; t) \mid R(g-1, 2, 1, 1, 0; t)$.

The expression in Theorem 5.3 divides every term. If N determines a δ-modular lattice, then $\alpha(N, t)$ equals the term corresponding to $C = 1$. □

Once we find $\alpha(0, t)$ for 0 any square zero matrix, the remainder of Theorem 5.3 follows by direct calculation. For the rest of this paper, fix π a generator of the ideal $\mathfrak{m}$, and recall that $q_0 = |S/\pi S|$. For $r \in \boldsymbol{Z}^+$, let $I(r)$ be the set of all tuples $(a_1, \cdots, a_t; b_1, \cdots, b_t) \in \boldsymbol{Z}^{2t}$ such that

(9.24.a) $t \in \boldsymbol{Z}^+$,

(9.24.b) $a_j > 0$ for each index j,

(9.24.c) $0 \leq b_1 < b_2 < \cdots < b_t$,

(9.24.d) $\sum_{j=1}^{t} a_j = r$.

Put $d(a_1, \cdots, a_t; b_1, \cdots, b_t) = \operatorname{diag}\{\pi^{b_1}, \cdots, \pi^{b_1}, \pi^{b_2}, \cdots, \pi^{b_2}, \pi^{b_t}, \cdots, \pi^{b_t}\}$, where the term π^{b_j} appears a_j times. Also, put

(9.25) $f(n) = \prod_{j=1}^{n}(1 - q_0^{-j})$ for $n \in \boldsymbol{Z}^+$, and
$f(a_1, \cdots, a_t; b_1, \cdots, b_t) = \prod_{j=1}^{t} f(a_t)$.

Let $\xi = (a_1, \cdots, a_t; b_1, \cdots, b_t) \in I(r)$. If $k \in \boldsymbol{Z}$ so that $b_1 \geq k (b_1\ k)$, we write $\xi \geq k$ ($\xi > k$) and let $\xi - k$ denote $(a_1, \cdots, a_t; b_1 - k, \cdots, b_t - k)$.

We need

THEOREM 9.3. *Let* $r \in \boldsymbol{Z}^+$, $\xi = (a_1, \cdots, a_t; b_1, \cdots, b_t) \in I(r)$, *and put* $\theta = d(\xi)$.

(A) *The additive group* $\operatorname{End}_S(S^r/S^r\theta)$ *has order*

(9.26) $q_0^{\kappa_1}$ *where* $\kappa_1 = \sum_{j=1}^{k} b_j a_j^2 + \sum_{i<j} 2b_i a_i a_j$

and the group $\operatorname{Aut}_S(S^r/S^r\theta)$ *has order* $f(\xi) \mid \operatorname{End}_S(S^r/S^r\theta)|$.

(B) *The sets* $U_r \backslash U_r \theta U_r$ *and* $U_r \theta U_r / U_r$ *are finite and share the common order*

(9.27) $\dfrac{f(r)}{f(\xi)} q_0^{\kappa_2}$ *where* $\kappa_2 = \sum_{i<j} (b_j - b_i) a_i a_j$.

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

(C) *As formal Dirichlet series in the variable q^{-s}, we have the equality*

$$\sum_{D \in U_r \backslash \Phi_r} q^{-\nu(D)s} = \prod_{j=0}^{r-1} (1 - q^{\sigma_3(j-s)})^{-1} . \tag{9.28}$$

Proof. The results are well-known when $\Delta = F$. The classical proofs apply to the non-commutative case, so we omit them. □

Let $m \in \boldsymbol{Z}^+$. Define a diagonal matrix of order m to be a diagonal matrix θ such that each diagonal entry λ satisfies $l(\lambda) = m$. If $r, k \in \boldsymbol{Z}^+$ and θ and θ' are diagonal matrices of order m of sizes $r \times r$ and $k \times k$, respectively, then

$$\theta M_{r,k}(S)\theta'^{-1} = \theta^{-1} M_{r,k}(S)\theta' = M_{r,k}(S) . \tag{9.29}$$

In what follows, we freely identity $\theta \in \Delta$ with a matrix of the form $\theta 1_r$.

From [3; (4.4), (4.5)] with the choice $T = 0$, we see that

$$\Big(\sum_{D \in U_r \backslash \Phi_r} q^{-\nu(D)s}\Big)\alpha(0_r, q^{-s}) = \Big(\sum_{D \in U_r \backslash \Phi_r} R(D) q^{-\nu(D)s}\Big) . \tag{9.30}$$

Again, although the proof of this fact is given under the assumptions $\mathrm{char}(F) = 0$ and $\varepsilon \in \{1, -1\}$, the argument holds in general. We next turn to the quantities $\Omega(D)$ and $R(D)$ for $D \in \Phi_r$. If $\alpha, \beta \in U_r$, then $R(\alpha D \beta) = R(D)$. Let $r_1, r_2 \in \boldsymbol{Z}^+$, $D_1 \in \Phi_{r_1}$, $D_2 \in \Phi_{r_2}$, and $\theta \in S - \{0\}$ such that $\theta D_1^{-1} \in \Phi_{r_1}$ and $D_2 \theta^{-1} \in \Phi_{r_2}$. Let $r = r_1 + r_2$, and decompose any matrix $C \in M_r(S)$ by

$$C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} \quad \text{where} \quad \begin{matrix} C_{11} \in M_{r_1}(S), & C_{12} \in M_{r_1 \times r_2}(S) , \\ C_{21} \in M_{r_2 \times r_1}(S) & C_{22} \in M_{r_2}(S) . \end{matrix} \tag{9.31}$$

Put $D = \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix}$. Our assumptions imply that if $T \in M_{r_1, r_2}(S)$ then

$$D_2 T D_1^{-*} = D_2 \theta^{-1} (\theta T \theta^{-*})(\theta^* D_1^{-1*}) \in M_{r_1, r_2}(S) . \tag{9.32}$$

Direct calculation shows that for a choice of submatrices (C_{11}, C_{12}, C_{22}), either there is no $C \in \Omega(D)$ with the assigned parts, or

$$C_{11} \in \Omega(D_1) , \tag{9.33.a}$$

$$C_{22} \in \Omega(D_2) , \tag{9.33.b}$$

and then there is exactly one such C. We get an obvious isomorphism

$$\begin{aligned} &\Omega(D)/D\Sigma(r, S) \xrightarrow{\sim} \Omega(D_1)/D_1\Sigma(r_1, S) \\ &\qquad \times \Omega(D_2)/D_2\Sigma(r_2, S) M_{r_1, r_2}(S)/D_1 M_{r_1, r_2}(S) , \\ &\Longrightarrow R(D) = R(D_1) \cdot R(D_2) \cdot q^{r_2 \nu(D_1)} . \end{aligned} \tag{9.34}$$

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

Equation (9.34) is true if $r_1 = 0$ or $r_2 = 0$. A simple induction implies that if $\alpha \in S - \{0\}$, then $R(\alpha 1_r) = R(\alpha)^r q^{r(r-1)\nu(\alpha)/2}$ for all r.

Let $r \in \boldsymbol{Z}^+$, $D \in \Phi_r$, and let θ be an $r \times r$ diagonal matrix of order m. The map $C \mapsto \theta^* C \theta$ induces an isomorphism

$$\Omega(\theta D\theta^*)/(\theta D\theta^*)\Sigma(r, S) \xrightarrow{\sim} \Omega(D)/D(\theta^*\Sigma(r, S)\theta) \tag{9.35}$$

$$\Longrightarrow R(\theta D\theta^*) = R(D)\iota(\theta)\,.$$

From Definition 7.1, we get $\iota(\theta) = q^{r(r-1)m\sigma_3 + rm\sigma_5}$.

For $k, r \in \boldsymbol{Z}^+$, define

$$\beta_k(r, s) = \sum_{\xi \in I(r), \xi \geq k} R(d(\xi))\,|\,U_r \backslash U_r d(\xi) U_r\,|\,q^{-\nu(d(\xi))s}\,. \tag{9.36}$$

We use the convention that $\beta_k(0, s) = 1$ for all k. Then $\beta_0(r, s)$ is the righthand side of (9.30). Note that for $k, r, m \in \boldsymbol{Z}^+$,

$$\beta_{m+2k}(r, s) = q^{r(r-1)k\sigma_3 + rk\sigma_5 - 2rk\sigma_3 s}\beta_m(r, s) \tag{9.37}$$

since

$$\begin{aligned} &\nu(d(\xi + 2k)) = \nu(d(\xi)) + 2rk\sigma_3\,, \\ &|\,U_r \backslash U_r d(\xi + 2k) U_r| = |\,U_r \backslash U_r d(\xi) U_r|\,, \\ &R(d(\xi + 2k)) = R(\pi^k d(\xi)(\mu^k)^*) = q^{r(r-1)k\sigma_3 + rk\sigma_5} R(d(\xi))\,. \end{aligned} \tag{9.38}$$

We get recursive formulas involving β_0 and β_1 by relating the relevant quantities for $\xi \in I(r)$ with the analogous quantities for a shorter tuple $\xi' \in I(r')$ where $r' < r$.

Let $\xi = (a_1, \cdots; \cdots, b_t) \in I(r)$. We assume that $t > 1$. Express $b_1 = 2k + \lambda$ where $k \in \boldsymbol{Z}$ and $\lambda \in \{0, 1\}$. Let $\xi' = (a_2, \cdots; b_2 - 2k, \cdots, b_t - 2k)$. To simplify the formulas which follow, put $a = a_1$. Note that $\xi' > \lambda$. Then

$$\begin{aligned} &\nu(d(\xi)) = 2rk\sigma_3 + \lambda a\sigma_3 + \nu(d(\xi'))\,, \\ &|\,U_r \backslash U_r\, d(\xi) U_r| = \frac{f(r)}{f(a)f(r-a)} q^{a\nu(d(\xi')) - \lambda a(r-a)\sigma_3}\,|\,U_r \backslash U^r d(\xi') U_r|\,, \\ &R(d(\xi)) = q^{r(r-1)k\sigma_3 + rk\sigma_5 + \lambda a\sigma_3\{2r-a-1\}/2 + \lambda a\sigma_4} R(d(\xi'))\,. \end{aligned} \tag{9.39}$$

With obvious conventions on "0×0" matrices, the formulas are true when $t = 1$.

Let $r \in \boldsymbol{Z}^+$. Let us introduce some more notation. Put $f(0) = 1$. If $\xi = (a_1, \cdots, a_t) \in (\boldsymbol{Z}^+ \cup \{0\})^t$ so that $\sum_j a_j \leq r$, then put

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

$$P_{\xi}^{r} = f(r)\{f(a_1)\cdots f(a_t)\cdot f(r - \Sigma_j a_j)\}^{-1}. \tag{9.40}$$

Reducing each $\xi \in I(r)$ to $\xi' \in I(r')$, we get

$$\begin{aligned}\beta_0(r, s) &= \sum_{b=1}^{r}\sum_{k=0}^{\infty}\sum_{\lambda=0}^{1} P_b^r q^{\lambda b\sigma_4 + k\{r-1)\sigma_3 + r\sigma_5 - 2r\sigma_3 s\} + \lambda b\sigma_3\{(b-1/2)-s\}}\beta_{\lambda+1}(r-b, s-b)\\ &= (1 - q^{r\{(r-1)\sigma_3+\sigma_5-2\sigma_3 s\}})^{-1}\sum_{b=1}^{r} P_b^r\{\beta_1(r-b, s-b)\\ &\quad + q^{b\sigma_4+(r-b)\sigma_5+\sigma_3\{(r-b)(r+b-1)+(b(b-1)/2)-(2r-b)s\}}\beta_0(r-b, s-b)\}.\end{aligned} \tag{9.41}$$

Decompose $\{\xi \in I(r)\colon \xi \geq 1\}$ into $\{\xi \in I(r)\colon \xi \geq 2\}$ and $\cup_a\{\xi \in I(r)\colon \xi = (a, \cdots; 1, \cdots)\}$.

$$\beta_1(r, s) = \sum_{b=0}^{r} P_b^r q^{b\sigma_4+(r-b)\sigma_3\{(r-b)(r+b-1)+(b(b-1)/2)-(2r-b)s\}}\beta_0(r-b, s-b). \tag{9.42}$$

Substitute (9.42) into (9.41). Multiply both sides by $(1 - q^{r\{(r-1)\sigma_3+\sigma_5-2\sigma_3 s\}})$ and then add $q^{r\{(r-1)\sigma_3+\sigma_5-2\sigma_3 s\}}\beta_0(r, s)$ to each side. Note that $P_e^r P_b^{r-e} = P_{e+b}^r P_b^{e+b}$ for $e, b, r \in Z^+ \cup \{0\}$ such that $r \geq e + b$. We get

$$\begin{aligned}&\beta_0(r, s)\\ &= \sum_{b=0}^{r}\{P_e^r q^{\sigma_3\{(r-e)(r+e-1)-2(r-e)s\}+(r-e)\sigma_5}\beta_0(r-e, s-e)\sum_{b=0}^{e} P_b^e q^{\sigma_3\{b(e-b)s\}+b(b-1)/2+b\sigma_4}\}.\end{aligned} \tag{9.43}$$

We now cite the classical identity

$$\prod_{b=0}^{n-1}(1 + y^b t) = \sum_{b=0}^{n} Y_b^n y^{b(n-b)+(b(b-1)/2)} t^b, \tag{9.44}$$

where y and t are indeterminates and

$$Y_b^n = \frac{\prod_{j=b+1}^{n}(1 - y^{-j})}{\sum_{j=1}^{n-b}(1 - y^{-j})}. \tag{9.45}$$

Put $t = q^{\sigma_4-\sigma_3 s}$ and $y = q^{\sigma_3}$. We have

$$\begin{aligned}&\beta_0(r, s)\\ &= \sum_{e=0}^{r}\left\{P_e^r q^{\sigma_3\{(r-e)(r+e-1)-2(r-e)s\}+(r-e)\sigma_5}\beta_0(r-e, s-e)\prod_{b=0}^{e-1}(1 + q^{b\sigma_3+\sigma_4-\sigma_3 s})\right\}.\end{aligned} \tag{9.46}$$

Divine inspiration suggests the substitution

$$B(m, s) = \beta_0\left(m, s + \frac{\sigma_5}{2\sigma_3} - 1 + m\right)\prod_{b=0}^{m-1}(1 + q^{(b+1-m)\sigma_3+\sigma_4-(\sigma_5/2)-\sigma_3 s})^{-1}, \tag{9.47}$$

where the new functions satisfy

https://doi.org/10.1017/S0027763000001252 Published online by Cambridge University Press

(9.48.a) $B(0, s) = 1$,

(9.48.b) $B(m, s) = \sum_{k=0}^{m} P_k^m p^{\sigma_3(-k(k-1)-2ks)} B(k, s)$ for each $m \in Z^+$.

Clearly (9.48.a, b) uniquely determine the family of functions $\{B(m, s); m \in Z^+\}$. We claim that

(9.49) $$B(m, s) = \prod_{b=0}^{m-1} (1 - q^{-\sigma_3(b+2s)})^{-1}.$$

With the substitution $y = q^{-\sigma_3}$ and $t = q^{-2\sigma_3 s}$, and after dividing by the expression $B(m, s)$ given in (9.49), we may derive (9.48.b) from

LEMMA 9.4. *Regard Y_b^n given in* (9.45) *as a rational function in the variable y. For t, y indeterminates,*

(9.50) $$1 = \sum_{k=0}^{n} Y_k^n(y^{-1}) y^{k(k-1)} t^k \prod_{j=k}^{n-1} (1 - y^j t).$$

Proof. It suffices to verify (9.50) for substitutions $y = q$ where q is a positive integral power of a prime. But this follows from (7) in [4; Proposition 1 of Section 5] after substituting $x = 1/t$, $z = 0$, and then multiplying both sides by t^n. □

The remaining work is straightforward computation.

REFERENCE

[1] Hel Braun, Hermitian modular functions, I, II, Ann. of Math. (2), **50, 51** (1949, 1950), 827–855, 92–104.
[2] D. Bump, Automorphic Forms on $GL(3, R)$ Springer Verlag, Lecture Notes in Mathematics, **1083**, New York, 1984.
[3] P. Feit, Poles and resiudes of Eisenstein series for symplectic and unitary groups, Memoirs of the Amer. Math. Soc., **346** (1986).
[4] J. Goldman and G.-C. Rota, On the foundations of combinatorical theory IV, Studies in Appl. Math., **49** (1970), 239–258.
[5] Y. Kitaoka, Dirichlet series in the theory of Siegel modular forms, Nagoya Math. J., **95** (1984), 73–84.
[6] ——, Local densities of quadratic forms and fourier Coefficients of Eisenstein Series, Nagoya Math. J., **103** (1986), 149–160.
[7] H. Maass, Springer Lecture Notes, Vol. **216**, 300–318.
[8] O. T. O'Meara, Introduction to Quadratic Forms, Springer-Verlag, New York, 1973.
[9] I. Reiner, Maximal Orders, Academic Press, New York, 1975.
[10] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan, **15** (1963), 33–65.
[11] ——, Arithmetic of unitary groups, Ann. of Math., **79** (1964), 369–409.
[12] ——, On Eisenstein series, Duke Math. J., **50** (1983), 417–476.

[13] ——, On Eisenstein series of half-integral weight, Duke Math. J., **52** (1985), 281–314.
[14] C. L. Siegel, Uber die analytische Theorie der quadratischen Formen, Ann. of Math., **36** (1935), 527–606.
[15] ——, Gesammelte Abh., Vol. II, 125–137.
[16] J. Sturm, The critical values of the zeta functions associated to the symplectic group, Duke Math. J., **48** (1981), 327–350.
[17] T. Tsukamoto, On the local theory of quaternionic anti-hermitian forms, J. Math. Soc. Japan, **13** (1961), 387–400.
[18] R. Weissauer, Eisensteinreihen vom Gewicht n+1 zur Siegelschen Modulgruppe n-ten Grades, Math. Ann., **268** (1984), 357–377.

Department of Mathematics
University of Chicago
Chicago, Illinois
60637