Math. Z. (2013) 275:509–527
DOI 10.1007/s00209-013-1145-x

Mathematische Zeitschrift

Weil representations associated with finite quadratic modules

Fredrik Strömberg

Received: 29 July 2011 / Accepted: 7 February 2013 / Published online: 8 March 2013

Abstract To any finite quadratic module, that is, a finite abelian group together with a non-degenerate quadratic form, it is possible to associate a representation of $\mathrm{Mp}_2(\mathbb{Z})$, the metaplectic cover of the modular group. This representation is usually referred to as a Weil representation and our main result is a general explicit formula for its matrix coefficients. This result completes earlier work by Scheithauer in the case when the representation factors through $\mathrm{SL}_2(\mathbb{Z})$. Furthermore, our formula is given in a such a way that it is easy to implement efficiently on a computer.

Keywords Weil representation · Metaplectic group · Finite quadratic module

Mathematics Subject Classification (2000) 11F27 · 20C25

1 Introduction

The main theorem of this paper is a simple and explicit formula for the matrix coefficients of a certain Weil representation, completing earlier works of Scheithauer [15] and Borcherds [2]. Our original motivation for obtaining such a formula was a need for efficient algorithms to compute vector-valued Poincaré series for this representation. This type of computation was used to prove certain properties of a Rankin–Selberg type convolution of Siegel modular forms of degree 2 [14], and also to study the algebraicity of Fourier coefficients of harmonic weak Maass forms [3]. Another application, for which it is necessary to have an explicit formula for the matrix coefficients of the Weil representation, is to obtain lifting maps from scalar to vector-valued modular forms of half-integral weight in terms of explicit formulas relating the respective Fourier coefficients. This type of map was obtained by Scheithauer [15] for integer weights.

F. Strömberg (✉)
Department of Mathematical Sciences, Durham University,
Science Laboratories, South Rd., Durham, DH1 3LE, UK
e-mail: fredrik.stromberg@durham.ac.uk

The formula stated in the Main Theorem is implemented as part of a package for Sage [21] for performing computations with finite quadratic modules.

1.1 Statement of the main result

Let D be a finite abelian group and $Q : D \mapsto \mathbb{Q}/\mathbb{Z}$ a non-degenerate quadratic form on D, meaning that the function $B(x, y) = Q(x + y) - Q(x) - Q(y)$ is a non-degenerate symmetric bilinear form. The pair $\underline{D} = (D, Q)$ is said to be a *finite quadratic module* (FQM). We associate with $\underline{D}$ a unitary representation, $\rho_{\underline{D}}$, of $\mathrm{Mp}_2(\mathbb{Z})$, the metaplectic cover of the modular group $\mathrm{SL}_2(\mathbb{Z})$, on $\mathbb{C}[D]$, the group algebra of D. If the signature of $\underline{D}$ is even this representation factors through a representation of $\mathrm{SL}_2(\mathbb{Z})$. This representation can be viewed as a special case of a construction carried out by Weil [22] and is therefore usually called the *Weil representation* associated with $\underline{D}$.

A canonical example of a finite quadratic module is the so-called *discriminant form* associated with even lattice together with a non-degenerate bilinear form.

Example 1.1 Let N be a positive integer and L be the lattice $\mathbb{Z}$ with quadratic form $q(x) = Nx^2$ and bilinear form $B(x, y) = 2Nxy$. The discriminant form of L is (D, Q) where $D = L^\#/L \simeq \mathbb{Z}/2N\mathbb{Z}$ and $Q(x) = \frac{1}{4N}x^2 + \mathbb{Z}$. Observe that L has signature 1.

The main purpose of this paper is to obtain a simple explicit formula for the action of $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{Mp}_2(\mathbb{Z})$ on the Weil representation associated with an arbitrary finite quadratic module $\underline{D}$. Our main result is presented in the theorem below. For the precise statement see Theorem 6.4 and Remark 6.8.

Theorem *Let $\underline{D}$ be an FQM with $\underline{D} = (D, Q)$ and bilinear form B. Let $\rho_{\underline{D}}$ be the associated Weil representation, $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $x \in D$. Then*

$$\rho_{\underline{D}}(\widetilde{\mathbf{A}})\mathbf{e}_x = \xi(a, c)\sqrt{|D[c]|/|D|} \sum_{y \in D/D[c]} f_{\mathbf{A}}(x, y)e(B(x_c, bx + y))\mathbf{e}_{dx+cy+x_c}$$

where $\widetilde{\mathbf{A}} = (\mathbf{A}, \sqrt{c\tau + d}) \in \mathrm{Mp}_2(\mathbb{Z})$, $\xi(a, c)$ is an eighth-root of unity, given explicitly by Definition 6.1, x_c is any element in D such that $cQ(y) = B(x_c, y)$ for all $y \in D[c]$ and $f_{\mathbf{A}}(x, y) = e(bdQ(x) + acQ(y) + bcB(x, y))$.

The given formula for ξ is "simple" in the sense that it involves only elementary arithmetic functions, e.g. Kronecker and Hilbert symbols. It is not hard to obtain a formula for $\rho_{\underline{D}}$ as a projective representation, that is, the theorem above with an unknown factor ξ. It is well-known that if $\underline{D}$ is an FQM of level N then $\rho_{\underline{D}}$ factors through the principal congruence subgroup of level N, or its inverse image in $\mathrm{Mp}_2(\mathbb{Z})$. This can be used to obtain explicit formulas for other congruence groups. Cf. e.g. Schoeneberg [16, p. 518], Pfetzer [13, pp. 451-452] and Kloosterman [9, I.§4].

In contrast to these formulas, the earlier formulas for $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{Mp}_2(\mathbb{Z})$ all involved certain sums of Gauss-type with a length depending on the particular element of the group. Cf. e.g. [16, p. 516], [13, p. 450], [9, I. Thm. 1], [18, Prop. 1.6], and [6, Prop. 3.2]. This situation improved when Scheithauer [15] obtained an explicit formula for the root of unity ξ, for any $\mathbf{A}$ in the modular group. However, his results are only valid for discriminant forms associated with lattices of even signature.

The main points of the current paper are that we obtain explicit formulas for the Weil representation associated with *any* finite quadratic module, without restrictions on the signature, and that all Gauss sums are explicitly evaluated and expressed in terms of elementary arithmetic functions. We want to stress that there are two key elements which are necessary for dealing with the case of odd signature. The first is a detailed study of the 2-adic Jordan components of the finite quadratic module. The second is an explicit evaluation of cocycles related to the metaplectic cover $\mathrm{Mp}_2(\mathbb{Z})$.

The following observation is relevant for computational applications. If we are given a finite quadratic module in terms of its Jordan decomposition then we are able to evaluate the matrix coefficients of the Weil representation for any element in $\mathrm{SL}_2(\mathbb{Z})$ or $\mathrm{Mp}_2(\mathbb{Z})$ in a fixed time not depending on the specific element.

1.2 Notational convention and outline of the paper

To simplify the exposition we use $e(x) = e^{2\pi i x}$, $e_r(x) = e(\frac{x}{r})$, $(a, b) = \gcd(a, b)$ and let $\mathrm{sgn}(c)$ be the sign of c with $\mathrm{sgn}(0) = 1$. Furthermore, we always use the Kronecker extension of the Jacobi symbol, $(\frac{c}{d})$. If c and $d > 0$ are odd then this is the usual quadratic residue symbol, and for arbitrary integers we define $(\frac{c}{d})$ by complete multiplicativity, using $(\frac{c}{d}) = \mathrm{sign}(c)(\frac{c}{-d})$, $(\frac{2}{d}) = (\frac{d}{2})$ for odd d, $(\frac{d}{0}) = (\frac{0}{d}) = 1$ if $d = \pm 1$ and 0 otherwise. If p is a prime number and $n \in \mathbb{Z}$ we define the p-adic additive valuation of n by $\mathrm{ord}_p(n) = k$ if p^k is the largest power of p dividing n. This is extended to $\mathbb{Q}$ by setting $\mathrm{ord}_p(\frac{c}{d}) = \mathrm{ord}_p(c) - \mathrm{ord}_p(d)$, and we use $|x|_p = p^{-\mathrm{ord}_p(x)}$ to denote the p-adic absolute value of x. If $\mathrm{ord}_p(c) = k$ we often write $p^k \parallel c$. The field of p-adic numbers, $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, and it is also the field of fractions of the ring of p-adic integers $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. The invertible elements of $\mathbb{Z}_p$ are denoted by $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$. Observe that $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. For any set S we let $|S|$ denote its number of elements. If $a, b \in \mathbb{Z}$ then the Hilbert symbol at infinity is defined as $(a, b)_\infty = -1$ if $a < 0$ and $b < 0$, and $(a, b)_\infty = 1$ otherwise. For $z \in \mathbb{C}$ we use $\sqrt{z} = \sqrt{|z|}\exp(\frac{1}{2} i \mathrm{Arg} z)$ where $\mathrm{Arg} z \in (-\pi, \pi]$ denotes the principal branch. Let $\mathbb{Z}/(r) = \mathbb{Z}/r\mathbb{Z}$. The direct orthogonal sum of A and B is denoted $A \oplus B$ and $A^n = A \oplus \cdots \oplus A$ (n times). The Kronecker delta $\delta_{ij} = 1$ if $i = j$ and otherwise 0.

The structure of the paper is as follows: We begin with a brief overview of the classical theory of quadratic forms over $\mathbb{Q}$ and $\mathbb{Q}_p$, including invariants and canonical forms. We then provide the necessary theory of finite quadratic modules, including en explicit description of their Jordan decompositions. In the following sections we evaluate the relevant Gauss sums, introduce the metaplectic cover of $\mathrm{SL}_2(\mathbb{Z})$ as well as the relevant Weil representations. We then give a precise formulation and proof of the main theorem. The final section contains lemmas which are used in this proof.

2 Quadratic forms and finite quadratic modules

To obtain the simple formula in our main theorem we need to know that every finite quadratic module has a Jordan decomposition, that is, that it can be written as a direct orthogonal sum of certain "simple" modules. To show this we use classical results from the theory of quadratic forms over the p-adic numbers.

2.1 Quadratic spaces and lattices

Let V be a vector space of dimension n over a field F and $q : V \to F$ a *quadratic form*. That is, $q(a\mathbf{x}) = a^2 q(\mathbf{x})$ for all $a \in F$, $\mathbf{x} \in V$ and the function $b : V \times V \to F$, defined by

$b(\mathbf{x}, \mathbf{y}) = q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x}) - q(\mathbf{y})$ is bilinear. The pair $\underline{V} = (V, q)$ is said to be a *quadratic space* over F.

If $\underline{V}$ has rank n then we can represent q as a homogeneous polynomial of degree n, that is $q(\mathbf{x}) = \sum_{1 \le i, j \le n} c_{ij} x_i x_j$ with $c_{ij} \in F$ and $\mathbf{x} = (x_1, \ldots, x_n) \in V$. The *Gram matrix* of q, or alternatively, of b, is the $n \times n$ symmetric matrix $\mathbf{B}_q = (b_{ij})$ with $b_{ij} = c_{ij} + c_{ji}$. The *determinant* of $\underline{V}$, or of q, is defined as the determinant $\det(\mathbf{B}_q)$. We say that $\underline{V}$ (or alternatively q, or b) is non-degenerate if $\det(\mathbf{B}_q) \neq 0$. This is equivalent to saying that $V^{\perp} = \{\mathbf{x} \in V \mid b(\mathbf{x}, \mathbf{y}) = 0, \forall \mathbf{y} \in V\} = \{0\}$. Note that the Gram matrix $\mathbf{B}_q$ depends on a choice of basis of V but the determinant being zero or non-zero does not.

If $\underline{V}' = (V', q')$ is a quadratic space over F of the same dimension as $\underline{V}$ then we say that $\underline{V}$ and $\underline{V}'$ are equivalent if $q(\mathbf{x}) = q'(A\mathbf{x})$ where $A : V \to V'$ is an isomorphism of vector spaces. If $V = V'$ we say that q and q' are equivalent.

Let $R = \mathbb{Z}$ or $\mathbb{Z}_p$ and suppose that F is the field of fractions of R, that is, $\mathbb{Q}$ or $\mathbb{Q}_p$. A *lattice* in $\underline{V}$ is an R-module $L = Ra_1 \oplus \cdots \oplus Ra_n$ where $\{a_i\}_{i=1}^n$ is an R-basis for V. We say that L is *integral* if $q(x) \in R$ for $x \in L$ and in our case this means that L is also *even* since $b(x, x) = 2q(x) \in 2R$. The dual lattice, $L^{\#}$, of L is given by $L^{\#} = \{x \in V \mid b(x, y) \in R, \forall y \in L\}$. It is easy to see that $L \subseteq L^{\#}$ and that $L^{\#}/L$ is in fact a finite abelian group of order $|\det(\mathbf{B}_q)|$.

For $F = \mathbb{Q}$ we define the *signature* of the lattice L as $\operatorname{sign}(L) = r_+ - r_-$ where r_+ and r_- are the number of positive and negative eigenvalues of the Gram matrix of q.

2.2 Canonical representations of quadratic forms

It is well-known that if p is an odd prime then any quadratic form over $\mathbb{Q}_p$ has a unique canonical form expressed as a linear combination of certain simple quadratic forms. The situation for $p = 2$ is more complicated and the canonical form is not always a unique. However, for our purposes the existence of one is sufficient. The relevant results from Cassels [4, Ch. 8.3] are summarized in Theorem 2.3 below.

Definition 2.1 Let p be a prime and $a \in \mathbb{Z}_p^{\times}$. Define the unary quadratic form q_A^a and the binary quadratic forms q_B and q_C, over $\mathbb{Q}_p$, as follows:

$$q_A^a(x) = ax^2, \quad q_B(x, y) = 2x^2 + 2xy + 2y^2, \quad q_C(x, y) = 2xy.$$

Remark 2.2 Observe that the quadratic forms q_A^a, q_B and q_C all have Gram matrices with integer entries, that is, they are *classically integral* in the sense of [4, p. 111].

Theorem 2.3 *Let p be a prime and q a non-degenerate quadratic form over $\mathbb{Q}_p$. Then q is $\mathbb{Z}_p$-equivalent to a direct sum of quadratic forms of rank one and two where each term is of the form $p^k \tilde{q}$ where $k \in \mathbb{Z}$ and $\tilde{q}$ is one of the canonical forms q_A^a, q_B or q_C. The forms q_B and q_C only appear in the case $p = 2$.*

Remark 2.4 Note that if q has coefficients in $\mathbb{Z}$ then the canonical forms in the previous theorem can be chosen such that $a \in \mathbb{Z}$ for all terms of the form $p^k q_A^a$.

2.3 Finite quadratic modules

Let D be a finite abelian group. A *quadratic form* on D is a function $Q : D \mapsto \mathbb{Q}/\mathbb{Z}$ such that $Q(nx) = n^2 Q(x)$ for all $n \in \mathbb{Z}$ and $x \in D$, and such that the function $B(x, y) = Q(x + y) - Q(x) - Q(y)$ is a bilinear form. We say that Q is *non-degenerate* if B is non-degenerate, that is, if $D^{\perp} = \{x \in D \mid B(x, y) = 0, \forall y \in D\} = \{0\}$, or alternatively, if the map $x \mapsto B(x, \cdot)$ is a group isomorphism between D and $\operatorname{Hom}(D, \mathbb{Q}/\mathbb{Z})$.

Definition 2.5 A *finite quadratic module* (FQM) is a pair $\underline{D} = (D, Q)$, where D is a finite abelian group and $Q : D \to \mathbb{Q}/\mathbb{Z}$ is a non-degenerate quadratic form on D. The *level* of $\underline{D}$ is the smallest positive integer N such that $NQ(x) = 0$ for all $x \in D$.

Let $\underline{D} = (D, Q)$ and $\underline{D}' = (D', Q')$ be two finite quadratic modules. We say that $\underline{D}$ and $\underline{D}'$ are isomorphic, written $\underline{D} \simeq \underline{D}'$, if there exists a group isomorphism $\varphi : D \to D'$ such that $Q = Q' \circ \varphi$. The direct sum of $\underline{D}$ and $\underline{D}'$ is defined as $\underline{D} \oplus \underline{D}' = (D \oplus D', Q \oplus Q')$, where $D \oplus D'$ is a direct sum of groups and $(Q \oplus Q')(x \oplus x') = Q(x) + Q'(x')$. The level of $\underline{D} \oplus \underline{D}'$ is the least common multiple of the level of $\underline{D}$ and the level of $\underline{D}'$.

If d is a non-zero integer we use D_d to denote the set of elements in D of order d and let $D[d]$ and $D[d]^*$ denote the kernel and image in D of the map $x \mapsto dx$. Note that $D[d]^* = dD$ is the orthogonal complement of $D[d]$ and if c is an integer such that $(c, |D|) = (d, |D|)$ then $D[c] = D[d]$ and $D[c]^* = D[d]^*$.

If p is a prime we let $D(p)$ be the p-group of D, that is, $D(p) = \oplus_{k\geq 1} D_{p^k}$. We then define the p-component of $\underline{D}$ as $\underline{D}(p) = (D(p), Q)$, where, with abuse of notation, we use Q to denote the restriction of Q to $D(p)$. Analogously we set $\underline{D}_{p^k} = (D_{p^k}, Q)$.

Definition 2.6 Let $\underline{V} = (V, q)$ be a quadratic space over $\mathbb{Q}$ or $\mathbb{Q}_p$. If L is an integral lattice in $\underline{V}$ then the *discriminant form* of L is the finite quadratic module given by $\underline{D}_L = (L^\#/L, Q)$ where $L^\#$ is the dual lattice of L and $Q(x + L) = q(x) + \mathbb{Z}$ for $x \in L^\#$. Note that in the case of $\mathbb{Q}_p$ we identify $\mathbb{Q}_p/\mathbb{Z}_p$ with $\mathbb{Z}[p^{-1}]/\mathbb{Z}$ via the natural map $z + \mathbb{Z}_p \mapsto z + \mathbb{Z}$, and view this as a subgroup of $\mathbb{Q}/\mathbb{Z}$.

Lemma 2.7 *Let p be a prime, $k \geq 1$ and $D = \mathbb{Z}/(p^k)$. Then there is a one-to-one correspondence between non-degenerate quadratic forms on D with values in $\mathbb{Q}/\mathbb{Z}$ and non-degenerate quadratic forms on D with values in $\mathbb{Z}/(p^k)$.*

Proof Since $Q(x) = \frac{1}{2}B(x, x)$ and $p^k B(x, x) = B(p^k x, x) = 0$ it is clear that $Q(D) \subseteq \frac{1}{2p^k}\mathbb{Z}/\mathbb{Z}$. Let m be an integer and consider the following ring isomorphism $\kappa_m : \frac{1}{m}\mathbb{Z}/\mathbb{Z} \to \mathbb{Z}/(m)$ defined by $\kappa_m(\frac{x}{m} + \mathbb{Z}) = x + m\mathbb{Z}$. If $p > 2$ then we define $q(x) = \kappa_{p^k}(2Q(x))$ and for $p = 2$ we set $q(x) = \kappa_{2^{k+1}}(Q(x))$. Finally, the map $Q \mapsto q$ is invertible since κ_{p^k} is a ring isomorphism and 2 is invertible in $\mathbb{Z}/(p^k)$ if $p > 2$.

We will now show that every finite quadratic module is isomorphic to a direct sum of canonical modules of the following types.

Definition 2.8 Let p be a prime and t an integer not divisible by p. For $k \geq 1$ define the following canonical finite quadratic modules.

$$\underline{A}^t_{p^k} = \left(\mathbb{Z}/(p^k), x \mapsto \frac{tx^2}{p^k} + \mathbb{Z}\right) \quad \text{for } p > 2, \tag{2.1}$$

$$\underline{A}^t_{2^k} = \left(\mathbb{Z}/(2^k), x \mapsto \frac{tx^2}{2^{k+1}} + \mathbb{Z}\right) \quad \text{for } p = 2, \tag{2.2}$$

$$\underline{B}_{2^k} = \left(\mathbb{Z}/(2^k) \oplus \mathbb{Z}/(2^k), (x, y) \mapsto \frac{x^2 + xy + y^2}{2^k} + \mathbb{Z}\right), \tag{2.3}$$

$$\underline{C}_{2^k} = \left(\mathbb{Z}/(2^k) \oplus \mathbb{Z}/(2^k), \frac{xy}{2^k} + \mathbb{Z}\right) \tag{2.4}$$

Remark 2.9 It is easy to verify that $A^t_{p^k}$ is the discriminant form of the integral lattice $\mathbb{Z}_p$ in $(\mathbb{Q}_p, p^{k^*} q^{t^*}_A)$ where $t^* = 4^{-1}t^{-1}$ and $k^* = k$ if $p \neq 2$, and $t^* = t^{-1}$ and $k^* = k - 1$ if $p = 2$. Similarly, B_{2^k} and C_{2^k} (with $k > 0$) are the discriminant forms associated with the integral lattice $\mathbb{Z}_2 \times \mathbb{Z}_2$ in $(\mathbb{Q}_2 \times \mathbb{Q}_2, 2^{k-1}q_B)$ and $(\mathbb{Q}_2 \times \mathbb{Q}_2, 2^{k-1}q_C)$, respectively. Observe that the level of $\underline{A}^t_{p^k}$ is p^k if $p > 2$, the level of $\underline{A}^t_{2^k}$ is 2^{k+1}, and the level of $\underline{B}_{2^k}$ and $\underline{C}_{2^k}$ are both equal to 2^k.

Lemma 2.10 *Let $\underline{D} = (D, Q)$ and assume that $D \simeq (\mathbb{Z}/(p^k))^n$ where p is a prime and n and k are positive integers. Then $\underline{D}$ is isomorphic to a direct sum of canonical FQMs of the form given in Definition 2.8.*

Proof Let q be the quadratic form on $(\mathbb{Z}/(p^k))^n$ associated with Q by Lemma 2.7 extended in a natural way to dimension n. By choosing representatives for $\mathbb{Z}/(p^k)$ in $\mathbb{Z}$ we obtain a $\mathbb{Z}$-integral quadratic form and then apply Theorem 2.3 and Remark 2.4 to q. We thus obtain a $\mathbb{Z}$-equivalent quadratic form $\tilde{q}$ which is written as a direct sum of canonical $\mathbb{Z}$-integral forms of the types q_A, q_B and q_C. We then reduce mod p^k again and apply Lemma 2.7 to obtain a quadratic form $\tilde{Q}$ on D, which has the desired form. Furthermore, $Q(x) = \tilde{Q}(Ox)$ where O is an automorphism of D. □

Proposition 2.11 *Every finite quadratic module $\underline{D}$ has a Jordan decomposition*

$$\underline{D} = \bigoplus_p \bigoplus_{k \geq 1} \underline{D}_{p^k} \tag{2.5}$$

where the $\underline{D}_{p^k}$'s are isomorphic to (possibly empty) direct sums of Jordan components of the types $\underline{A}^t_{p^k}$, $\underline{B}_{2^k}$ and $\underline{C}_{2^k}$.

Proof If $\underline{D} = (D, Q)$ then, by elementary theory of finite groups, we we can write D as a direct sum of groups of prime-power orders, that is, $D = \bigoplus_p \bigoplus_{k \geq 1} D_{p^k}$ where D_{p^k} denotes the elements of order p^k. From this we obtain a decomposition $\underline{D} = \bigoplus_p \bigoplus_{k \geq 1} \underline{D}_{p^k}$ and then apply Lemma 2.10. □

Let $\underline{D} = (D, Q)$ be a finite quadratic module with associated bilinear form B. The explicit formulas for the Weil representation associated with $\underline{D}$ will contain certain invariants of the Jordan decomposition of $\underline{D}$. Many of these quantities are most conveniently expressed in terms of Gauss sums. For any $x \in D$ and $d \in \mathbb{Z}$ we define the following quadratic Gauss sum

$$\mathscr{G}(d, x; \underline{D}) = \frac{1}{\sqrt{|D|}\sqrt{|D[d]|}} \sum_{y \in D} e(dQ(y) + B(x, y)).$$

It follows from the results of the next section that $\mathscr{G}(d, 0; \underline{D})$ is always an eighth root of unity. We define the *signature* of $\underline{D}$, $\text{sign}(\underline{D})$, as the element of $\mathbb{Z}/(8)$ given by

$$e_8(\text{sign}(\underline{D})) = \mathscr{G}(1, 0; \underline{D}).$$

By Milgram's formula, see for example [12, Appendix 4], it follows that if $\underline{D}$ is the discriminant form of an integral lattice L over $\mathbb{Q}$ then the signature of $\underline{D}$ is equal to the signature of $L \pmod 8$.

From the orthogonality of the Jordan decomposition it follows that $\mathscr{G}(d, x; \underline{D})$ factors into a product over Jordan components. This implies, in particular, that $\text{sign}(\underline{D}) = \sum_p \text{sign}(\underline{D}(p))$, where the sum is taken over all primes. By using Lemmas 3.6–3.8 it is then easy to verify that the signature of a canonical form of type $\underline{A}^t_{2^k}$ is odd and that the signature of any other canonical form is even. As a consequence we see that if the signature of $\underline{D}$ is odd then the Jordan decomposition of $\underline{D}$ must have a direct summand of the form $\underline{A}^t_{2^k}$ and the level of $\underline{D}$ is therefore divisible by 4.

The following two remarks are mainly relevant for the reader who wishes to compare the results and proofs presented in this paper with those of Scheithauer [15].

Remark 2.12 The *genus symbol* of a Jordan decomposition is a shorthand notation which encodes its invariants in the following form. If $p > 2$ then $q^{\pm}$ represents a component $\underline{A}^t_{p^k}$ with $(\frac{2t}{p}) = \pm 1$. For $p = 2$ the symbols $q_t^{\pm}$, q^{-2} and q^{+2} represents $\underline{A}^t_{2^k}$, with $(\frac{t}{2}) = \pm 1$, $\underline{B}_{2^k}$ and $\underline{C}_{2^k}$, respectively. Direct sums are represented by concatenating symbols, for example, $\underline{A}^t_{p^k} \oplus \underline{A}^t_{p^k}$ has symbol $q^{\pm 2}$ and $\underline{A}^3_2 \oplus \underline{A}^1_3$ has $2_3^- 3^-$.

Remark 2.13 If L is an even integral lattice of rank n and p is a prime then it is possible to define the so-called p-signature of L as in [5]. The relationship to our results is given as follows. If $\underline{D}$ is the discriminant form of L then 2-signature$(L) \pmod 8 = \operatorname{sign}(\underline{D}(2))$ and p-signature$(L) \pmod 8 = n - \operatorname{sign}(\underline{D}(p))$. The 2-signature of L is sometimes called the *oddity*.

Example 2.14 Let $N \in \mathbb{Z}^+$ and consider the lattice $L = \mathbb{Z}$ in the quadratic space $(\mathbb{Q}, x \mapsto Nx^2)$. A simple calculation shows that $L^\# = \frac{1}{2N}\mathbb{Z}$ and that the discriminant form of L is $\underline{D}_L = (D, Q)$ where $D = \mathbb{Z}/(2N)$ and $Q(x) = \frac{1}{4N}x^2$.

If we write $2N = p^{m_p} N_p$ with $p \nmid N_p$ for each prime $p \mid 2N$ then the Jordan components are: $\underline{D}(p) = \underline{A}_q^{N_p}$ with $q = p^{m_p}$ for $p > 2$ and $\underline{D}(2) = \underline{A}^t_{2^{m_2}}$ with $t = N_2$ for $p = 2$. It follows from Lemma 3.7 that $\operatorname{sign}(\underline{D}_L(2))$ is equal to $N_2 + 4m$ where $m = 0$ if m_2 is even or $(\frac{N_2}{2}) = 1$ and otherwise $m = 1$. It is harder to compute the signature directly but by Milgram's formula it is clear that $\operatorname{sign}(\underline{D}_L) = \operatorname{sign}(L) = 1$.

Let $\underline{D} = (D, Q)$ be a finite quadratic module, c an integer and $x \in D$. It is clear that the Gauss sum $\mathscr{G}(c, x; D)$ can be expressed as a sum of terms of the form $\psi_{c,x}$ where the map $\psi_{c,x} : D \to \mathbb{C}^*$ is defined by $\psi_{c,x}(y) = e(cQ(y) + B(y, x))$. It is easy to check that $\psi_{c,x}$ is a character on the group $D[c]$ and that it is in fact equal to the trivial character precisely if $x \in D[c]^\bullet$, where the set $D[c]^\bullet$ is defined by

$$D[c]^\bullet = \{x \in D \mid cQ(y) + B(y, x) = 0,\ \forall y \in D[c]\}. \tag{2.6}$$

From [15, Prop. 2.1] it follows that $D[c]^\bullet = x_c + D[c]^*$ where the coset representative x_c can be chosen as in the following definition.

Definition 2.15 Let $q = |c|_2^{-1}$, that is, $q = 2^k$ where $k = \operatorname{ord}_2(c)$. If $k \geq 1$ and $\underline{D}$ has a non-trivial Jordan component of the form $J = \bigoplus_{i=1}^n \underline{A}_q^{t_i}$, with respect to a $\mathbb{Z}$-basis $\{\gamma_i\}$ of J, then we choose $x_c \in J$ in the following way

$$x_c = 2^{k-1} \sum_{i=1}^n \gamma_i \tag{2.7}$$

and otherwise $x_c = 0$.

Note that the definition of x_c depends on the choice of basis $\{\gamma_i\}$. Furthermore, note that $2x_c = cx_c = 0$ and if $(c, |D|) = (d, |D|)$ then $D[c]^\bullet = D[d]^\bullet$ and $x_c = x_d$.

Lemma 2.16 *If $\underline{D}$ is a finite quadratic module and c an integer then*

$$\mathscr{G}(c, x; \underline{D}) = \mathscr{G}(c, x_c; \underline{D}) e(-cQ(y) - B(x_c, y))$$

if $x = x_c + cy$ for some $y \in D$, and otherwise $\mathscr{G}(c, x; \underline{D}) = 0$.

Proof Since $D = D[c] \oplus D[c]^*$ it follows that the Gauss sum factors as a sum over $D[c]$ times a sum over $D[c]^*$. The sum over $D[c]$ is equal to 0 unless $x \in D[c]^\bullet$ because $\psi_{c,x}$ is a character on $D[c]$. The lemma now follows by writing $x = x_c + cy$ and then simplify the remaining Gauss sum by "completing the square". □

3 Evaluation of Gauss sums

In this section we will obtain explicit formulas for Gauss sums of the form $\mathscr{G}(c, 0; \underline{D})$ where c is an integer and $\underline{D}$ is one of the canonical components. We will begin by reviewing the necessary results for the standard quadratic Gauss sums.

Definition 3.1 For $a, b \in \mathbb{Q}$ and $c \in \mathbb{Z}$ we define $G(a, b, c)$ as

$$G(a, b, c) = \sum_{n \,(\mathrm{mod} c)} e_c(an^2 + bn).$$

Lemma 3.2 *Let $a, b, c \in \mathbb{Z}$ with $ac \neq 0$. Then*

$$G(a, b, c) = \left|\frac{c}{2a}\right|^{\frac{1}{2}} e_8\left(\operatorname{sign}(2ac) - \frac{2b^2}{ac}\right) G\left(-\frac{c}{2}, -b, 2a\right).$$

Proof Set $S(a, b, c) = G(a/2, b/2, c)$ and apply [1, Thm. 1.2.2]. □

Corollary 3.3 *Let $b, c \in \mathbb{Z}$ and suppose that $c > 0$ is even. Then*

$$G(1, b, c) = \begin{cases} 0 & \text{if } \frac{c}{2} + b \text{ is odd,} \\ \sqrt{2c}\, e_8\left(1 - \frac{2b^2}{c}\right) & \text{if } \frac{c}{2} + b \text{ is even.} \end{cases}$$

Proof By Lemma 3.2 we know that $G(1, b, c) = \sqrt{\frac{c}{2}} e_8\left(1 - \frac{2b^2}{c}\right) G(-\frac{c}{2}, -b, 2)$ and $G(-\frac{c}{2}, -b, 2) = \sum_{n=0}^{1} e(-\frac{1}{2}[\frac{c}{2}n^2 + nb]) = 1 + (-1)^{\frac{c}{2}+b}$. □

Lemma 3.4 *Let $a, c \in \mathbb{Z}$ and suppose that $(a, c) = 1$. Then*

$$G(a, 0, 2) = 1 + (-1)^a, \tag{3.1}$$

$$G(a, 0, c) = \sqrt{2c} \left(\frac{a}{2c}\right) e_8(a) \quad \text{if } c = 2^k \text{ with } k > 1, \tag{3.2}$$

$$G(a, 0, c) = \sqrt{c} \left(\frac{2a}{c}\right) e_8(1 - c) \quad \text{if } c > 0 \text{ is odd,} \tag{3.3}$$

Proof See [1, Ch. 1.5]. □

Lemma 3.5 *Let $a, b, c \in \mathbb{Z}$ and let $t = (a, c)$. Then*

$$G(a, b, c) = 0 \quad \text{if } t \nmid b, \tag{3.4}$$

$$G(a, b, c) = tG(a/t, b/t, c/t) \quad \text{if } t \mid b, \tag{3.5}$$

$$G(a, 0, 2^{k+1}) = 2G(a/2, 0, 2^k) \quad \text{if } k \geq 1. \tag{3.6}$$

Proof These identities are easy to show by dividing $G(a, b, c)$ into t sums of length c/t (with $t = 2$ in the last case). □

Lemma 3.6 *Let $p > 2$ be a prime, $q = p^k$ with $k \geq 1$ and $t \in \mathbb{Z}$ relatively prime to p. If c is a non-zero integer and $q_c = (q, c)$ then*

$$\mathscr{G}(c, 0, \underline{A}_q^t) = \left(\frac{2tc/q_c}{q/q_c}\right) e_8(1 - q/q_c).$$

Proof Note that $|D[c]| = q_c$ and hence $\sqrt{qq_c}\mathscr{G}(c, 0, \underline{A}_q^t) = G(ct, 0, q)$. By (3.5) we see that $G(ct, 0, p^k) = q_c G(tc/q_c, 0, q/q_c)$ and the lemma then follows from (3.3). □

Lemma 3.7 *Let $q = 2^k$ with $k \geq 1$ and $t \in \mathbb{Z}$ odd. If $c \in \mathbb{Z} \setminus \{0\}$ and $q_c = (q, c)$ then*

$$\mathscr{G}(c, 0, \underline{A}_q^t) = \left(\frac{tc/q_c}{q/q_c}\right) \begin{cases} e_8(tc/q_c) & \text{if } q \nmid c, \\ 0 & \text{if } q \parallel c, \\ 1 & \text{if } 2q \mid c. \end{cases}$$

Proof Observe that $|D[c]| = q_c$ and $\sqrt{qq_c}\mathscr{G}(c, 0; \underline{A}_q^t) = G(\frac{1}{2}ct, 0, q)$. The cases $2q \mid c$ and $q \parallel c$ are elementary. If $q \nmid c$ then we use (3.5) and (3.6) to factor out appropriate powers of 2 and obtain $G(\frac{ct}{2}, 0, q) = \frac{1}{2} q_c G(tc/q_c, 0, 2q/q_c)$. Finally we use (3.2). □

Lemma 3.8 *If $q = 2^k$ with $k \geq 1$ and c is a non-zero integer then*

$$\mathscr{G}(c, 0, \underline{B}_q) = \left(\frac{3}{q/q_c}\right), \tag{3.7}$$

$$\mathscr{G}(c, 0, \underline{C}_q) = 1. \tag{3.8}$$

Proof In this case $|D[c]| = q_c^2$ and by definition $qq_c\mathscr{G}(c, 0; \underline{B}_q) = \sum_{n,m=0}^{q-1} e_q(cm^2 + cn^2 + cmn)$ and hence $qq_c\mathscr{G}(c, 0; \underline{B}_q) = \sum_{m=0}^{q-1} e_q(cm^2)G(c, cm, q)$. If $q/q_c = 1$ or 2 the formula for $\mathscr{G}(c, 0, \underline{B}_q)$ follows immediately. If $q/q_c > 2$ then Lemma 3.2 and (3.4) can be used to show that $G(c/q_c, mc/q_c, q/q_c)$ is 0 unless m is even, in which case

$$G(c/q_c, 2nc/q_c, q/q_c) = \sqrt{q/2c}\, e_8(1) e_q(-cn^2) G(-q/2q_c, -2nc/q_c, 2c/q_c).$$

Since $2 \mid q/2q_c$ we see that $G(-q/2q_c, -2nc/q_c, 2c/q_c) = 2G(-q/4q_c, 0, c/q_c)$ and this can be evaluated by (3.3). By summing over n up to $q/2$ and using (3.6) we obtain

$$qq_c\mathscr{G}(c, 0; \underline{B}_q) = q_c\sqrt{qq_c/2}\, e_8(2 - c/q_c) \left(\frac{-q/2q_c}{c/q_c}\right) G(3c/q_c, 0, q/q_c)$$

and by evaluating the latter Gauss sum and using the fact that $(\frac{-1}{d}) = -e_4(1 + d)$ for odd d we obtain (3.7). Since $G(0, b, c) = 0$ unless $c \mid b$ we see immediately that $qq_c\mathscr{G}(c, 0; \underline{C}_q) = \sum_{m=0}^{q-1} G(0, cm, q) = q_c \sum_{m=0}^{q-1} G(0, cm/q_c, q/q_c) = q_c q_c \frac{q}{q_c} = qq_c$. □

The following lemma is easy to show by combining the above lemmas with the orthogonality of the Jordan decomposition.

Lemma 3.9 *If $\underline{D}$ is an FQM with level N and $d \in \mathbb{Z}$ is relatively prime to N then*

$$\mathscr{G}(d, 0; \underline{D}) = \left(\frac{d}{|D|}\right) e_8(\operatorname{sign}(\underline{D}) + (d - 1)\operatorname{sign}(\underline{D}(2))).$$

Lemma 3.10 *Let $q = 2^k$ with $k \geq 1$ and assume that c and t are integers with t odd and $k = \operatorname{ord}_2(c)$. If $x_c \in \underline{A}_q^t$ is chosen as in (2.7) then*

$$\mathscr{G}(c, x_c; \underline{A}_q^t) = 1.$$

Proof It is clear that $x_c = \frac{q}{2}$ and hence $e(cQ(x) + B(x_c, x)) = e_{2q}(ctx^2 + 2tx_c x) = e_2(x^2 + x) = 1$ for all $x \in \mathbb{Z}/(q)$. □

Corollary 3.11 *If $\underline{D}$ is a finite quadratic module with a given Jordan decomposition, c an integer and $q = |c|_2^{-1}$ then*

$$\mathscr{G}(c, x_c; \underline{D}) = \prod_{J \neq \underline{A}_q^t} \mathscr{G}(c, 0; J)$$

where the product is taken over all Jordan components, J, of $\underline{D}$, except for any (if existing) components of the form $\underline{A}_q^t$.

Proof This follows from orthogonality of Jordan decompositions and the fact that if $\underline{D}$ has a non-trivial component $\underline{A}_q^t$ then $x_c \in \underline{A}_q^t$, together with Lemma 3.10. □

4 The metaplectic group

Weil representations associated with finite quadratic modules are representations of $\mathrm{Mp}_2(\mathbb{Z})$, the metaplectic (twofold) cover of $\mathrm{SL}_2(\mathbb{Z})$. Alternatively $\mathrm{Mp}_2(\mathbb{Z})$ can also be described as the central extension of $\mathrm{SL}_2(\mathbb{Z})$ by the group $\{\pm 1\}$. We therefore repeat the most important facts about $\mathrm{Mp}_2(\mathbb{Z})$. Additional details are given by, for example, Gelbart [8].

It is known that $\mathrm{Mp}_2(\mathbb{Z})$ can be realized as the group of pairs $(\mathbf{M}, \pm j_{\mathbf{M}}(\tau))$, where $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $j_{\mathbf{M}}(\tau) = \sqrt{c\tau + d}$. The group law of $\mathrm{Mp}_2(\mathbb{Z})$ is given by

$$(\mathbf{A}, \epsilon_{\mathbf{A}} j_{\mathbf{A}}(\tau))(\mathbf{B}, \epsilon_{\mathbf{B}} j_{\mathbf{B}}(\tau)) = (\mathbf{AB}, \epsilon_{\mathbf{A}}\epsilon_{\mathbf{B}}\sigma(\mathbf{A}, \mathbf{B}) j_{\mathbf{AB}}(\tau)) \tag{4.1}$$

where $\epsilon_{\mathbf{A}}, \epsilon_{\mathbf{B}} \in \{\pm 1\}$ and $\sigma : \mathrm{SL}_2(\mathbb{Z})^2 \to \{\pm 1\}$ is a 2-cocycle on $\mathrm{SL}_2(\mathbb{Z})$. The value of $\sigma(\mathbf{A}, \mathbf{B})$ can be computed explicitly by choosing any τ in the upper half-plane and observe that the following expression holds and is independent of τ:

$$\sigma(\mathbf{A}, \mathbf{B}) = j_{\mathbf{A}}(\mathbf{B}\tau) j_{\mathbf{B}}(\tau) j_{\mathbf{AB}}(\tau)^{-1}. \tag{4.2}$$

For $\mathbf{M} \in \mathrm{SL}_2(\mathbb{Z})$ we define $\widetilde{\mathbf{M}} = (\mathbf{M}, j_{\mathbf{M}(\tau)})$ to be the canonical choice of representative in the inverse image of $\mathbf{M}$ under the covering map. Using the generators $\mathbf{S} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\mathbf{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{Z})$ it is easy to see that $\mathrm{Mp}_2(\mathbb{Z})$ is generated by $\widetilde{\mathbf{S}}$ and $\widetilde{\mathbf{T}}$ with relations $\widetilde{\mathbf{S}}^2 = (\widetilde{\mathbf{S}\mathbf{T}})^3 = \widetilde{\mathbf{Z}}$ and $\widetilde{\mathbf{Z}}^4 = \mathrm{id}_{\mathrm{Mp}_2(\mathbb{Z})}$. To be precise

$$\widetilde{\mathbf{T}} = \left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), 1\right), \quad \widetilde{\mathbf{S}} = \left(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \sqrt{\tau}\right), \quad \widetilde{\mathbf{Z}} = \left(\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), i\right).$$

and $\widetilde{\mathbf{Z}}$ generates the center of $\mathrm{Mp}_2(\mathbb{Z})$. Since $\widetilde{\mathbf{Z}}^2 = \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), -1\right)$ it follows that

$$\mathrm{Mp}_2(\mathbb{Z})/\langle \widetilde{\mathbf{Z}}^2 \rangle \simeq \mathrm{SL}_2(\mathbb{Z}). \tag{4.3}$$

To obtain an expression for $\sigma(\mathbf{A}, \mathbf{B})$ which does not involve an auxiliary variable τ we need the following symbols. For $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ define $c_{\mathbf{M}} = c$, $d_{\mathbf{M}} = d$,

$$\sigma_{\mathbf{M}} = \begin{cases} c & \text{if } c \neq 0, \\ d & \text{if } c = 0, \end{cases} \quad \text{and} \quad s(\mathbf{M}) = \begin{cases} 1 & \text{if } c \neq 0, \\ \mathrm{sign}(d) & \text{if } c = 0. \end{cases}$$

Theorem 4.1 *For any* $\mathbf{A}, \mathbf{B} \in \mathrm{SL}_2(\mathbb{Z})$ *we can express* $\sigma(\mathbf{A}, \mathbf{B})$ *as*

$$\sigma(\mathbf{A}, \mathbf{B}) = \mu(\mathbf{A}, \mathbf{B})\, s(\mathbf{A}) s(\mathbf{B}) s(\mathbf{AB})^{-1}$$

where $\mu(\mathbf{A}, \mathbf{B}) = (\sigma_{\mathbf{A}}\sigma_{\mathbf{AB}}, \sigma_{\mathbf{B}}\sigma_{\mathbf{AB}})_\infty$ *and* $(\cdot, \cdot)_\infty$ *denotes the Hilbert symbol at infinity.*

Proof Use the fact that (4.2) is independent of the choice of τ, set $\tau = iy$ and then let $y \to \infty$. The theorem is then proven by a careful analysis of all the possible cases for the lower rows of **A** and **B**. (For a related result see Maaß [11, p. 115].)

Remark 4.2 Kubota [10] introduced the cocycle μ and showed that there is only one two-fold central extension of $\mathrm{SL}_2(\mathbb{R})$. We therefore know that μ and σ must be related by a trivial cocycle. We could not find the precise relationship (as given by the previous theorem) in the literature and therefore decided to include it.

The following lemmas are essentially direct applications of Theorem 4.1.

Lemma 4.3 *Let* $\mathbf{A}, \mathbf{B} \in \mathrm{SL}_2(\mathbb{Z})$ *and* $m, n \in \mathbb{Z}$. *Then*

$$\sigma(\mathbf{A}, \mathbf{T}^m) = \sigma(\mathbf{T}^m, \mathbf{A}) = 1, \tag{4.4}$$

$$\sigma(\mathbf{A}, \mathbf{B}\mathbf{T}^m) = \sigma(\mathbf{A}, \mathbf{B}) = \sigma(\mathbf{T}^m\mathbf{A}, \mathbf{B}), \tag{4.5}$$

$$\sigma(\mathbf{S}\mathbf{T}^m, \mathbf{S}\mathbf{T}^n) = \mathrm{sign}(m), \tag{4.6}$$

$$\sigma(\mathbf{A}, \mathbf{S}) = \begin{cases} -1 & \text{if } c_{\mathbf{A}} \geq 0 \text{and } d_{\mathbf{A}} < 0, \\ 1 & \text{otherwise.} \end{cases} \tag{4.7}$$

Lemma 4.4 *Let* $\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $c > 0$. *If* $m \in \mathbb{Z}^+$, $n \in \mathbb{Z}$ *and* $cn - d > 0$ *then*

$$\sigma(\mathbf{M}\mathbf{T}^{-n}\mathbf{S}\mathbf{T}^{-m}\mathbf{S}, \mathbf{S}\mathbf{T}^m\mathbf{S}\mathbf{T}^n) = 1.$$

5 The Weil representation

In this section let $\underline{D} = (D, Q)$ be a fixed finite quadratic module of level N with associated bilinear form B and a fixed, chosen, Jordan decomposition. The Weil representation associated with $\underline{D}$ is a unitary finite-dimensional representation of $\mathrm{Mp}_2(\mathbb{Z})$ on $\mathbb{C}[D]$, the group algebra of D. We view $\mathbb{C}[D]$ as a vector space of dimension $|D|$ over $\mathbb{C}$ with basis vectors denoted by $\mathbf{e}_x$, $x \in D$. We are only interested in the particular type of Weil representations defined below and have an emphasis on explicit formulas. A more comprehensive theoretical background is given by, for example, Gelbart [8] or Skoruppa [19].

Definition 5.1 The Weil representation $\widetilde{\rho}_{\underline{D}} : \mathrm{Mp}_2(\mathbb{Z}) \to \mathbb{C}[D]$ associated with $\underline{D}$ is defined by the following action of the generators. If $x \in D$ then

$$\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{T}})\mathbf{e}_x = e(Q(x))\mathbf{e}_x,$$

$$\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}})\mathbf{e}_x = \sigma_w(\underline{D})\frac{1}{\sqrt{|D|}}\sum_{y\in D} e(-B(x, y))\mathbf{e}_y$$

where $\sigma_w(\underline{D}) = \mathscr{G}(-1, 0; \underline{D})$.

The eighth-root of unity $\sigma_w(\underline{D})$ is usually called the Witt-invariant of $\underline{D}$ and it is clear that $\sigma_w(\underline{D}) = e_8(-\mathrm{sign}(\underline{D}))$. To show that $\widetilde{\rho}_{\underline{D}}$, defined as above on the generators, and extended multiplicatively, indeed defines a representation, we need to verify that it respects the relations in $\mathrm{Mp}_2(\mathbb{Z})$. It is sufficient to show that $\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}})^8\mathbf{e}_x = \widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}}\widetilde{\mathbf{T}})^{12}\mathbf{e}_x = \mathbf{e}_x$ for all $x \in D$. By using the definition of $\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}})$ and computing $\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}})^2\mathbf{e}_x$ directly and in addition use Lemma 5.2 (below) to evaluate $\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}}\widetilde{\mathbf{T}})^3\mathbf{e}_x$ it is easy to show that

$$\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{Z}})\mathbf{e}_x = \widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}})^2\mathbf{e}_x = \widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}}\widetilde{\mathbf{T}})^3\mathbf{e}_x = \sigma_w(\underline{D})^2\mathbf{e}_{-x}. \tag{5.1}$$

Since $\sigma_w(\underline{D})^8 = 1$ we immediately conclude that $\widetilde{\rho}_{\underline{D}}$ is a representation.

Lemma 5.2 *Let m and n be integers and suppose that m is positive. If $x \in D$ then*

$$\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}}\widetilde{\mathbf{T}}^{n})\mathbf{e}_x = \sigma_w(\underline{D})|D|^{-\frac{1}{2}}e(nQ(x))\sum_{y\in D}e(-B(x,y))\mathbf{e}_y$$

$$\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}}\widetilde{\mathbf{T}}^{m}\widetilde{\mathbf{S}}\widetilde{\mathbf{T}}^{n})\mathbf{e}_x = \sigma_w(\underline{D})^2\sqrt{|D[m]|/|D|}\,\mathscr{G}(m,x_m,\underline{D})e(nQ(x)) \times \sum_{y\in D/D[m]} e(-mQ(y)-B(x_m,y))\mathbf{e}_{x_m+my-x}.$$

Proof The first equation is simply obtained by first applying $\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{T}}^n)$ and then $\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{S}})$ to $\mathbf{e}_x$. By a similar argument, as well as identifying the Gauss sum, it follows that

$$\sqrt{|D|}\rho_{\underline{D}}(\widetilde{\mathbf{S}}\widetilde{\mathbf{T}}^{m}\widetilde{\mathbf{S}}\widetilde{\mathbf{T}}^{n})\mathbf{e}_x = \sigma_w(\underline{D})^2 e(nQ(x)\sqrt{|D[m]|}\sum_{z\in D}\mathscr{G}(m,z+x;\underline{D})\mathbf{e}_z.$$

The lemma then follows by using Lemma 2.16 and observe that to sum over $x+z=x_m+my\in D[m]^{\bullet}$ is equivalent to sum over $y\in D/D[m]$. □

From the relation (4.3) it is clear that the behavior of $\widetilde{\rho}_{\underline{D}}$ on the subgroup $\langle\widetilde{\mathbf{Z}}^2\rangle$ determines whether $\widetilde{\rho}_{\underline{D}}$ factors through a representation of $\mathrm{SL}_2(\mathbb{Z})$ or not. Since

$$\widetilde{\rho}_{\underline{D}}(\widetilde{\mathbf{Z}}^2)\mathbf{e}_x = \sigma_w(\underline{D})^4\mathbf{e}_x$$

for all $x\in D$ we see that $\widetilde{\rho}_{\underline{D}}$ factors through a representation of $\mathrm{SL}_2(\mathbb{Z})$ precisely if $\sigma_w(\underline{D})^4 = 1$, or equivalently, if $\mathrm{sign}(\underline{D})$ is even. It follows that if we define

$$\rho_{\underline{D}}(\mathbf{A}) = \widetilde{\rho}_{\underline{D}}((\mathbf{A}, j_{\mathbf{A}}))$$

for $\mathbf{A}\in\mathrm{SL}_2(\mathbb{Z})$ then $\rho_{\underline{D}}:\mathrm{SL}_2(\mathbb{Z})\to\mathbb{C}[D]$ is a representation of $\mathrm{SL}_2(\mathbb{Z})$ if the signature of $\underline{D}$ is even, and otherwise it is a *projective* representation. In the latter case we have the following multiplicative relation for any $\mathbf{A},\mathbf{B}\in\mathrm{SL}_2(\mathbb{Z})$:

$$\rho_{\underline{D}}(\mathbf{A})\rho_{\underline{D}}(\mathbf{B}) = \sigma(\mathbf{A},\mathbf{B})\rho_{\underline{D}}(\mathbf{AB}). \tag{5.2}$$

Abusing notation we also refer to $\rho_{\underline{D}}$ as the Weil representation associated with $\underline{D}$. The main theorem is formulated as an explicit formula for $\rho_{\underline{D}}$ but it is not difficult to recover the corresponding formula for $\widetilde{\rho}_{\underline{D}}$. If $\mathbf{A}\in\mathrm{SL}_2(\mathbb{Z})$ then the relation

$$\widetilde{\rho}_{\underline{D}}((\mathbf{A},-j_{\mathbf{A}})) = \sigma_w(\underline{D})^4\rho_{\underline{D}}(\mathbf{A}).$$

follows immediately from the fact that $(\mathbf{A},\varphi(\tau)) = \widetilde{\mathbf{Z}}^2(\mathbf{A},-\varphi(\tau))$. In the same spirit it is possible to use (5.1) and Theorem 4.1 to obtain an expression relating $\rho_{\underline{D}}(-\mathbf{A})$ and $\rho_{\underline{D}}(\mathbf{A})$. Set $\delta=-\mathrm{sgn}(c)$ if $c\neq 0$ and $\delta=\mathrm{sgn}(d)$ if $c=0$. Then

$$\rho_{\underline{D}}(-\mathbf{A})\mathbf{e}_x = \delta\,\sigma_w(\underline{D})^2\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_{-x}. \tag{5.3}$$

Recall that $\Gamma(N)$, the *principal congruence subgroup* of level N, of $\mathrm{SL}_2(\mathbb{Z})$, is defined as the subgroup consisting of all matrices which are (entry-wise) congruent to $\begin{pmatrix}1&0\\0&1\end{pmatrix}\pmod N$. Any subgroup $\Gamma\subseteq\mathrm{SL}_2(\mathbb{Z})$ which contains $\Gamma(N)$ is said to be a congruence subgroup of level N. We are only interested in two other groups: $\Gamma_0(N)$ and $\Gamma_0^0(N)$ which consist of all matrices $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ with $c\equiv 0\pmod N$ and $b\equiv c\equiv 0\pmod N$, respectively. Note that

$$\Gamma(N)\subseteq\Gamma_0^0(N)\subseteq\Gamma_0(N)\subseteq\mathrm{SL}_2(\mathbb{Z})$$

and that the inclusions are strict unless $N = 1$. The basic idea behind the proof of the explicit formula in our main theorem is that we want to extend a known formula for $\rho_{\underline{D}}$ on elements of $\Gamma_0(N)$. This is done by using the formulas on the generators $\mathbf{S}$ and $\mathbf{T}$ together with an explicit description of the quotient $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$.

The action of the subgroups $\Gamma(N)$, $\Gamma_0^0(N)$ and $\Gamma_0(N)$ on the Weil representation, as given in Lemmas 5.5 and 5.6 below, was obtained for certain discriminant forms already by Schoeneberg [16] and Pfetzer [13] in terms theta functions. See also Ebeling [6, Ch. 3.1] (based on lectures and notes of Hirzebruch and Skoruppa), Borcherds [2, Thm. 5.4], Eichler [7, p. 49] and Skoruppa [19,20].

Definition 5.3 If $d \in \mathbb{Z}$ is relatively prime to N then we define

$$\varepsilon_{\underline{D},d} = \mathscr{G}(1; 0; \underline{D})/\mathscr{G}(d, 0; \underline{D}). \tag{5.4}$$

Definition 5.4 If $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we define the map $\varepsilon_{\underline{D}} : \mathrm{SL}_2(\mathbb{Z}) \to \{\pm 1\}$ by

$$\varepsilon_{\underline{D}}(\mathbf{A}) = \begin{cases} \left(\frac{c}{d}\right) & \text{if } \mathrm{sign}(\underline{D}) \text{ is odd,} \\ 1 & \text{otherwise,} \end{cases}$$

and if $\mathbf{A} \in \Gamma_0(N)$ then we define $\chi_{\underline{D}} : \Gamma_0(N) \to \{e_8(k) \mid k \in \mathbb{Z}/8\mathbb{Z}\}$ by

$$\chi_{\underline{D}}(\mathbf{A}) = \varepsilon_{\underline{D}}(\mathbf{A})\varepsilon_{\underline{D},d}^{-1}.$$

Lemma 5.5 *If* $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *and* $x \in D$ *then*

$$\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_x = \begin{cases} \varepsilon_{\underline{D}}(\mathbf{A})\mathbf{e}_x & \textit{if } \mathbf{A} \in \Gamma(N), \\ \chi_{\underline{D}}(\mathbf{A})\mathbf{e}_{dx} & \textit{if } \mathbf{A} \in \Gamma_0^0(N). \end{cases}$$

The above lemma implies that the Weil representation, $\rho_{\underline{D}}$, associated with $\underline{D}$ factors through $\Gamma(N)$ if the signature of $\underline{D}$ is even. If the signature is odd then N is divisible by 4 and the Weil representation, $\widetilde{\rho}_{\underline{D}}$, factors through the group

$$\widetilde{\Gamma(N)}^* = \{(\mathbf{A}, v_\theta(\mathbf{A})j_{\mathbf{A}}(\tau)) \mid \mathbf{A} \in \Gamma(N)\}$$

where v_θ is the multiplier system of the Jacobi theta function $\theta(\tau) = \sum_{n\in\mathbb{Z}} e(\tau n^2)$. Recall that θ is a weight $\frac{1}{2}$ modular form on $\Gamma_0(4)$ and multiplier system given by

$$v_\theta(\mathbf{A}) := j_{\mathbf{A}}(\tau)^{-1}\frac{\theta(\mathbf{A}\tau)}{\theta(\tau)} = \left(\frac{c}{d}\right)\varepsilon_d^{-1}, \quad \text{for all } \mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4) \tag{5.5}$$

(see, for example [17, §2]) where

$$\varepsilon_d = \left(\frac{2}{d}\right)e_8(1-d) = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ i & \text{if } d \equiv 3 \pmod N). \end{cases} \tag{5.6}$$

In the main theorem we extend the formulas for the action of $\Gamma_0(N)$ to that of $\mathrm{SL}_2(\mathbb{Z})$ and in the lemma below we extend the action of $\Gamma_0^0(N)$ to that of $\Gamma_0(N)$. Since some of the key principles are present in both cases we give the details of the proof below.

Lemma 5.6 *If* $\underline{D}$ *has level* N, $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ *and* $x \in D$ *then*

$$\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_x = e(bdQ(x))\chi_{\underline{D}}(\mathbf{A})\mathbf{e}_{dx}.$$

Proof Let $n \equiv -bd \pmod{N}$. Then $na \equiv -bda \equiv -b \pmod{N}$ and $\mathbf{A} = \mathbf{X}\mathbf{T}^{-n}$ with $\mathbf{X} = \begin{pmatrix} a & an+b \\ c & cn+d \end{pmatrix} \in \Gamma_0^0(N)$. Using lemma 4.3 and the fact that $N \mid c$ we see that

$$\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_x = \rho_{\underline{D}}(\mathbf{X})\rho_{\underline{D}}(\mathbf{T}^{-n})\mathbf{e}_x = e(bdQ(x))\rho_{\underline{D}}(\mathbf{X})\mathbf{e}_x = \varepsilon_{\underline{D}}(\mathbf{X})\varepsilon_{\underline{D},d}^{-1}\mathbf{e}_{dx}.$$

In the last step we used that $\mathscr{G}(d+nc, 0; \underline{D}) = \mathscr{G}(d, 0, \underline{D})$ and therefore $\varepsilon_{\underline{D},nc+d} = \varepsilon_{\underline{D},d}$. It remains to show that $\varepsilon_{\underline{D}}(\mathbf{X}) = \varepsilon_{\underline{D}}(\mathbf{A})$. If the signature of $\underline{D}$ is even then $\varepsilon_{\underline{D}}(\mathbf{X}) = \varepsilon_{\underline{D}}(\mathbf{A}) = 1$. Assume that the signature is odd and $c \neq 0$. Recall the quadratic reciprocity law for the Kronecker symbol: if x and y are any non-zero integers then

$$\left(\frac{x}{y}\right) = (x, y)_\infty \left(\frac{y}{x}\right) e_8((x_2 - 1)(y_2 - 1)), \tag{5.7}$$

where x_2 and y_2 denote the odd parts of x and y. By using (5.7) twice together with elementary properties of the Kronecker and Hilbert symbols it is easy to show that $(\frac{c}{nc+d}) = (\frac{c}{d})e_8((c_2 - 1)cn)$. Since the signature is odd we know that $4 \mid c$ and therefore $\varepsilon_{\underline{D}}(\mathbf{X}) = (\frac{c}{nc+d}) = (\frac{c}{d}) = \varepsilon_{\underline{D}}(\mathbf{A})$. Observe that if $c = 0$ then $\mathbf{A} = \mathbf{T}^b$ if $a = 1$, and $\mathbf{Z}\mathbf{T}^{-b}$ if $a = -1$. In the second case we obtain the desired formula by using (5.3). □

Remark 5.7 It should be remarked that it is possible prove Lemma 5.6 directly by using the generators of $\Gamma_0(N)$ and some very meticulous calculations.

6 The main theorem

Definition 6.1 Let $\underline{D}$ be a finite quadratic module with a given Jordan decomposition and a and c relatively prime integers. If $c \neq 0$ then we define the eighth root of unity

$$\xi(a, c) = e_4(-\text{sign}(\underline{D}))\,\xi_0\,\xi_2 \prod_J \xi(J)$$

where the product is taken over all non-trivial Jordan components, J, of $\underline{D}$ and the factors are defined as follows. If p is a prime and J has order p^k with $k > 0$ then

$$\begin{aligned} \xi(J) &= \mathscr{G}(c, 0; J) \quad \text{if } p \nmid c, \\ \xi(J) &= \left(\frac{-a}{|J|}\right)\mathscr{G}(-ac, x_c; J) \quad \text{if } p \mid c. \end{aligned}$$

If the signature of $\underline{D}$ is even then we set $\xi_0 = \xi_2 = 1$. If the signature of $\underline{D}$ is odd then

$$\xi_0 = \left(\frac{-a}{c}\right)(-a, c)_\infty$$

and

$$\xi_2 = \begin{cases} 1 & \text{if } c \text{ is odd,} \\ e_8(-(a+1)(c_2 - 1 + \text{sign}(\underline{D}(2))) & \text{if } c \text{ is even,} \end{cases}$$

where c_2 is the odd part of c. The definition is then completed by setting $\xi(1, 0) = 1$ and $\xi(-1, 0) = e_4(-\text{sign}(\underline{D}))$. For the case $a = 0$ recall that by our definitions in Sect. 1.2 we have $(\frac{0}{\pm 1}) = (0, \pm 1)_\infty = 1$.

Remark 6.2 Observe that the values of $\mathscr{G}(c, 0; J)$ and $\mathscr{G}(-ac, x_c; J)$ are given by simple arithmetic functions, explicitly obtained from Lemmas 3.6–3.8.

Remark 6.3 From the definitions of the Gauss sums, together with the fact that any odd prime which divides $|D|$ also divides N, it follows immediately that if the signature of $\underline{D}$ is even then $\xi(a, c)$ depends only on the values of a and c modulo N.

Theorem 6.4 *Let $\underline{D} = (D, Q)$ be a finite quadratic module with bilinear form B and $\rho_{\underline{D}}$ the associated Weil representation. If $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $x \in D$ then*

$$\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_x = \xi(a, c)\sqrt{\frac{|D[c]|}{|D|}} \sum_{y \in D/D[c]} f_{\mathbf{A}}(x, y) e(B(x_c, bx + y))\mathbf{e}_{dx+cy+x_c},$$

where $\xi(a, c)$ is given by Definition 6.1, x_c is any element in D such that $cQ(y) = B(x_c, y)$ for all $y \in D[c]$ and

$$f_{\mathbf{A}}(x, y) = e(bdQ(x) + acQ(y) + bcB(x, y)).$$

Proof Let N be the level of $\underline{D}$. If $c = 0$ then $\mathbf{A} \in \Gamma_0(N)$ and the theorem follows directly from Lemma 5.6. Assume that $c \neq 0$. We first observe that it is possible to choose coset representatives of $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$ of the form $\mathbf{V}_{m,n} = \mathbf{ST}^m\mathbf{ST}^n$. Let m and n be integers, with m positive, such that:

$$cn - d > 0, \quad (cn - d, N) = 1, \quad (cn - d)m \equiv c \pmod N, \tag{6.1}$$

$$cn - d - 1 \equiv m - c \equiv 0 \pmod 8) \text{ if } 2 \nmid c \quad \text{and} \tag{6.2}$$

$$an - b \equiv m + ac \equiv 0 \pmod 8 \text{ if } 2 \mid c. \tag{6.3}$$

To show that it is possible to choose such m and n we use elementary facts about solutions of linear congruence equations. We then define $\mathbf{X} \in \Gamma_0(N)$

$$\mathbf{X} = \mathbf{AV}_{m,n}^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} (an - b)m - a & an - b \\ (cn - d)m - c & cn - d \end{pmatrix}. \tag{6.4}$$

Hence $\mathbf{A} = \mathbf{XV}_{m,n}$ and by Lemma 4.4 it follows that $\rho_{\underline{D}}(\mathbf{A}) = \rho_{\underline{D}}(\mathbf{X})\rho_{\underline{D}}(\mathbf{V}_{m,n})$. The factor $\rho_{\underline{D}}(\mathbf{V}_{m,n})$ is evaluated with the help of Lemmas 4.3 and 5.2. By applying $\rho_{\underline{D}}(\mathbf{X})$ to $\mathbf{e}_{x_m+my-x}$ in the inner sum and using the definition of $\chi_{\underline{D}}(\mathbf{X})$ we obtain

$$\begin{aligned}\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_x &= \sigma_w(\underline{D})^2\sqrt{|D[m]|/|D|}\ \chi_{\underline{D}}(\mathbf{X})\sigma_w(\underline{D})\mathscr{G}(m, x_m, \underline{D})\mathscr{G}(d', 0; \underline{D}) \\ &\quad\times \sum_{z \in D/D[m]} e(nQ(x) - mQ(z) - B(x_m, z) + b'd'Q(x_m + mz - x))\mathbf{e}_{d'(x_m+mz-x)}.\end{aligned}$$

Since $(d', N) = 1$ it follows that $(m, N) = (c, N)$, $|D[m]| = |D[c]|$ and $x_c = x_m$. Hence

$$d'(x_m + mz - x) = x_c + cz - (cn - d)x = x_c + cy + dx$$

where $y = z - nx$. Note that if $x_c \neq 0$ then c is even and by assumption $an \equiv b \pmod 8$. In this case a is odd and therefore $n \equiv b \pmod 2$ and thus $B(x_m, z) = B(x_c, nx + y) = B(x_c, bx + y)$. If we now define

$$\widetilde{f}_{\mathbf{A}}(x, y) = e(nQ(x) - mQ(y + nx) + b'd'Q(x_m + m(y + nx) - x)) \quad \text{and} \tag{6.5}$$

$$\widetilde{\xi}(a, c) = \varepsilon_{\underline{D}}(\mathbf{X})\mathscr{G}(-1, 0; \underline{D})^3\mathscr{G}(m, x_c, \underline{D})\mathscr{G}(d', 0, \underline{D}) \tag{6.6}$$

then

$$\rho_{\underline{D}}(\mathbf{A})\mathbf{e}_x = \widetilde{\xi}(a, c)\sqrt{|D[c]|/|D|} \sum_{y \in D/D[c]} \widetilde{f}_{\mathbf{A}}(x, y)e(B(x_c, bx + y))\mathbf{e}_{x_c+cy+dx}$$

and it is clear that it remains only to show that $\widetilde{\xi}(a,c) = \xi(a,c)$ and $\widetilde{f_{\mathbf{A}}}(x,y) = f_{\mathbf{A}}(x,y)$ (independent of the choice of n and m).

We begin with the simpler case of $f_{\mathbf{A}}$. If $x_c \neq 0$ then $b' \equiv 0 \pmod 8$, which implies that $b'Q(x_c) = 0$ and therefore

$$\widetilde{f_{\mathbf{A}}}(x,y) = e(acQ(y+nx) + (b'd'+n)Q(x) - b'cB(y+nx,x))$$

where we used that $d'm \equiv c \pmod N$ and $b'cm - m \equiv mad' \equiv ac \pmod N$. By expanding $Q(y+nx)$ and $B(y+nx,x)$ and collecting terms we obtain

$$\widetilde{f_{\mathbf{A}}}(x,y) = e(acQ(y) + (b'd'+n+acn^2-2b'cn)Q(x) + (acn-b'c)B(y,x)).$$

Using the definitions $b' = an-b$ and $d' = cn-d$ we see that

$$b'd'+n+acn^2-2b'cn = b'(-d-cn)+n+acn^2 = bd+n(1+cb-ad) = bd$$

and it follows immediately that $\widetilde{f_{\mathbf{A}}}(x,y) = e(acQ(y)+bdQ(x)+bcB(y,x)) = f_{\mathbf{A}}(x,y)$.

It remains to show that $\widetilde{\xi}(a,c) = \xi(a,c)$. By orthogonality it is clear that

$$\widetilde{\xi}(a,c) = \varepsilon_{\underline{D}}(\mathbf{X})\mathscr{G}(-1,0;J)^2 \prod_J \mathscr{G}(-1,0;J)\mathscr{G}(m,x_c,J)\mathscr{G}(d',0;J)$$

where the product is taken over all non-trivial Jordan components, J, of $\underline{D}$. First of all, observe that if the signature of $\underline{D}$ is even then $\varepsilon_{\underline{D}}(\mathbf{X}) = 1$. Otherwise, if the signature is odd, then it follows from Lemma 6.11 that $\varepsilon_{\underline{D}}(\mathbf{X}) = (-a,c)_\infty(\frac{-a}{c})$ if c is odd and $(-a,c)_\infty(\frac{-a}{c})e_8((a+1)(c_2+1))$ if c is even.

Let $p > 2$ be a prime which divides N. If $p \nmid c$ then $md' \equiv c \pmod p$ and if $p \mid c$ then $md' = m(cn-d) \equiv -md \pmod p$ and $ad \equiv 1 \pmod p$. Together with the explicit formula in Lemma 3.6 it follows that if $J = \underline{A}^t_{p^k}$ then

$$\mathscr{G}(-1,0;J)\mathscr{G}(m,0,J)\mathscr{G}(d',0;J) = \begin{cases} \mathscr{G}(c,0;J) & \text{if } p \nmid c \text{ and} \\ \left(\frac{-a}{|J|}\right)\mathscr{G}(-ac,0;\underline{A}^t_q) & \text{otherwise.} \end{cases} \tag{6.7}$$

If $p = 2$ then (6.7) holds in this case as well, with the modification that the second row is multiplied by $e_8(-\operatorname{sign}(J)(a+1))$. This is easy to show if J is of the form B_{2^k} or C_{2^k}. The most complicated case, which is also not covered by [15], is that of $J = \underline{A}^t_{2^k}$. For clarity we present the details for this case in Lemma 6.10. □

Remark 6.5 It should now be evident that in order to treat the case of odd signature (which is the case not covered by the analogous results in [15]) we had to deal with three major obstacles. The first two are related to the metaplectic group and consist of determining $\varepsilon_{\underline{D}}(\mathbf{X})$ and evaluating the the cocycle $\sigma(\mathbf{A},\mathbf{B})$ explicitly (for various choices of $\mathbf{A}$ and $\mathbf{B}$). The third problem is related to the Jordan components of the type $\underline{A}^t_{2^k}$ and consists of calculating $\mathscr{G}(-1,0;J)\mathscr{G}(m,0;J)\mathscr{G}(d',0;J)$ for this component and show that the resulting expression is independent of the parameters m and n.

Remark 6.6 Note that the formula of the main theorem is a priori dependent on the choice of Jordan decomposition, as well as possibly a choice of x_c. However, since the definition of ρ does not depend on these choices it is clear that the left-hand side, and therefore also the right-hand side of the formula are in fact both independent of these choices (for each $x \in D$).

Remark 6.7 It is not difficult to verify that when the signature of $\underline{D}$ is even then the formula of Theorem 6.4 coincides with the one in [15, Thm. 4.7] for the dual representation defined by $\rho^*_{\underline{D}}(\mathbf{A}) = \bar{\rho}_{\underline{D}}(\mathbf{A})$. Observe that, in this case, $\rho^*_{\underline{D}}(\mathbf{A}) = \rho_{\underline{D}}(\mathbf{A}^{-1})^{\mathrm{T}}$ where T denotes the matrix transpose.

Remark 6.8 If $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $x, z \in D$ then $\rho_{\underline{D}}(\mathbf{A})$ has matrix coefficients

$$\rho_{\underline{D}}(\mathbf{A})_{x,z} = \xi(a,c)\sqrt{|D[c]|/|D|}\, f_{\mathbf{A}}(x,y) e(B(x_c, bx + y)), \quad x, z \in D$$

if there is an element $y \in D$ such that $z = dx + x_c + cy$ and otherwise $\rho_{\underline{D}}(\mathbf{A})_{x,z} = 0$.

Example 6.9 Let $N \in \mathbb{Z}^+$ and consider $\underline{D}_N = (\mathbb{Z}/(2N), \frac{x^2}{4N})$ and the associated Weil representation $\rho_{\underline{D}_N}$. In this case it is possible to obtain a very simple expression for the root of unity, $\xi(a,c)$. If $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $c \neq 0$ then

$$\xi(a,c) = (a,c)_\infty \left(\frac{a2N/(2N,c)}{c/(2N,c)}\right) e_8(c_2 N_2 \delta a - c_2(N_2, c_2))$$

where $\delta = 1$ if $|2N/c|_2 \geq 1$ and otherwise $\delta = 0$. To prove this we have to use the explicit formulas for the Gauss sums and the quadratic reciprocity law (5.7). It is not difficult to show that the above expression is equivalent to that given in [14, Thm. 3].

In general it does not seem to be possible to simplify $\xi(a,c)$ for an arbitrary matrix $\mathbf{A}$. However, if $\underline{D}$ has level N and $\mathbf{A} \in \Gamma_0(N)$ then it is possible to simplify the expression for $\chi_{\underline{D}}(\mathbf{A})$ using Lemma 3.9. If $\mathbf{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ then $\chi_{\underline{D}}(\mathbf{A}) = (\frac{d}{|D|})$ if $4 \nmid N$ and otherwise, if we set $s = \mathrm{sign}(\underline{D})$ and $r = \mathrm{sign}(\underline{D}) + (\frac{-1}{|D|}) - 1$ then

$$\chi_{\underline{D}}(\mathbf{A}) = \left(\frac{d}{|D|2^s}\right)\left(\frac{c}{d}\right)^s \varepsilon_d^{-r} = \left(\frac{d}{|D|2^s}\right) \times \begin{cases} v_\theta(\mathbf{A}) & \text{if } r \equiv 1 \pmod 4, \\ \overline{v_\theta}(\mathbf{A}) & \text{if } r \equiv 3 \pmod 4, \\ \left(\frac{-1}{d}\right) & \text{if } r \equiv 2 \pmod 4, \\ 1 & \text{if } r \equiv 0 \pmod 4. \end{cases}$$

To compare with similar formulas by Borcherds [2] note that $\overline{v}_\theta(\mathbf{A}) = (\frac{-1}{d}) v_\theta(\mathbf{A})$.

6.1 Two lemmas containing details for the proof of the main theorem

Lemma 6.10 *Let the notation be as in Theorem 6.4 with $c \neq 0$. Assume that $m, n, \mathbf{X}, a', b', c'$ and d' are as in (6.1)–(6.4). If $q = 2^k$ with $k > 1$ and $\underline{A}_q^t$ is a non-trivial Jordan component of $\underline{D}$ then $\mathscr{G}(d', 0; \underline{A}_q^t)\mathscr{G}(m, x_m; \underline{A}_q^t)$ equals*

$$\mathscr{G}(1,0;\underline{A}_q^t) \times \begin{cases} \mathscr{G}(c, 0; \underline{A}_{2^k}^t) & \text{if } c \text{ is odd}, \\ \mathscr{G}(-ac, x_c; \underline{A}_q^t)\left(\frac{-a}{q}\right) e_8(-\mathrm{sign}(\underline{A}_q^t)(a+1)) & \text{if } c \text{ is even.} \end{cases}$$

Proof Assume that c is even and $q \nmid c$. Then $b' \equiv 0 \pmod 8$ and $d'a' = b'c' + 1 \equiv 1 \pmod 8$. It follows that $d' \equiv a' \equiv -a \equiv 1 \pmod 8$. If $q_c = (c, N)$ then $(m, c) = q_c$ and by Lemma 3.7 we immediately obtain

$$\mathscr{G}(d', 0; \underline{A}_q^t)\mathscr{G}(m, 0; \underline{A}_q^t) = \left(\frac{-at}{q}\right) e_8(-ta) \left(\frac{tm/q_c}{q/q_c}\right) e_8(tm/q_c).$$

Since $q \nmid c$ and the level of the component $\underline{A}_q^t$ is $2q$ it follows that $4 \mid N/q_c$ and therefore $\frac{m}{q_c} \equiv d' \frac{c}{q_c} \equiv -\frac{ac}{q_c} \pmod 4$. By using (5.6) we see that

$$e_8(tm/q_c) = \left(\frac{tm}{2}\right) e_8(1) \varepsilon_{tm/q_c}^{-1} = \left(\frac{-mac/q_c^2}{2}\right) e_8(-act/q_c).$$

Furthermore, if $q/q_c \geq 2$ then $2q/q_c$ is either equal to 4 or N/q_c is divisible by 8. In the latter case $d'a' \equiv -ad' \equiv 1 \pmod 8$ and $\frac{m}{q_c} \equiv -\frac{ac}{q_c} \pmod 8$. In both cases it is clear that $(\frac{tm/q_c}{q/q_c})e_8(tm/q_c) = (\frac{-act/q_c}{q/q_c})e_8(-act/q_c)$. We conclude that

$$\begin{aligned}\mathcal{G}(d', 0; \underline{A}_q^t)\mathcal{G}(m, 0; \underline{A}_q^t) &= \left(\frac{t}{q}\right)\left(\frac{-a}{q}\right)e_8(-ta - act/q_c)\left(\frac{-act/q_c}{q/q_c}\right) \\ &= \mathcal{G}(1, 0; \underline{A}_q^t)\mathcal{G}(-ac, 0; \underline{A}_q^t)\left(\frac{-a}{q}\right)e_8(-(a+1)t).\end{aligned}$$

Since a is odd it follows from Lemma 3.7 that $e_8(-(a+1)t) = e_8(-(a+1)\mathrm{sign}(\underline{A}_q^t))$. This proves the lemma in this case. The cases of odd c and $q \mid c$ are analogous. The only difference is that when $2^k \parallel c$ then $\mathcal{G}(m, x_m; \underline{A}_q^t) = \mathcal{G}(-ac, x_c; \underline{A}_q^t) = 1$.

Lemma 6.11 *Let the notation be as in Theorem 6.4 and assume that the signature of $\underline{D}$ is odd. Let m, n and $\mathbf{X}$ be as in (6.1)–(6.4) and let c_2 be the odd part of c. Then*

$$\varepsilon_{\underline{D}}(\mathbf{X}) = \left(\frac{-a}{c}\right)(c, -a)_\infty \begin{cases} 1 & \text{if } c \text{ is odd}, \\ e_8((c_2+1)(a+1)) & \text{if } c \text{ is even}. \end{cases}$$

Proof By definition $\varepsilon_{\underline{D}}(\mathbf{X}) = (\frac{(cn-d)m-c}{cn-d})$. Since $cn - d$ is positive and odd it follows that $(\frac{(cn-d)m-c}{cn-d}) = (\frac{-c}{cn-d})$. By the quadratic reciprocity law we see that $(\frac{-c}{cn-d}) = (\frac{cn-d}{-c})e_8((-c_2-1)(cn-d-1))$. If c is odd then $cn - d \equiv 1 \pmod 8$ and the statement then follows from the fact that $ad \equiv 1 \pmod c$ and $(\frac{-a}{|c|}) = (\frac{-a}{c})(c, -a)_\infty$. If c is even we use that $cn - d \equiv -a \pmod 8$. □

Acknowledgments I would like to thank Nils Scheithauer for clarifying details of [15], Nils-Peter Skoruppa for sharing thoughts about Weil representations in general, and the manuscript [19], in particular. I would also like to thank Stephan Ehlen for his extensive assistance with proof reading the manuscript and in simplifying Theorem 4.1.

References

1. Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi Sums. Canadian Mathematical Society Series of Monographs and Advanced Texts. Wiley, New York (1998)
2. Borcherds, R.E.: Reflection groups of Lorentzian lattices. Duke Math. J. **104**(2), 319–366 (2000). doi:10.1215/S0012-7094-00-10424-3
3. Bruinier, J.H., Strömberg, F.: Computation of harmonic weak Maass forms. Exp. Math. **21**(2), 117–131 (2011)
4. Cassels, J.W.S.: Rational Quadratic Forms. London Mathematical Society Monographs, vol. 13. Academic Press Inc., London (1978)
5. Conway, J.H., Sloane, N.J.A.: On the classification of integral quadratic forms. In: Conway, J.H., Sloane, N.J.A. (eds.) Sphere Packings, Lattices and Groups, pp. 352–405. Die Grundlehren der mathematischen Wissenschaften, vol. 290, Springer, New York (1999)
6. Ebeling, W.: Lattices and Codes. Friedrich Vieweg & Sohn, Braunschweig (1994)
7. Eichler, M.: Introduction to the Theory of Algebraic Numbers and Functions. Pure and Applied Mathematics, vol. 23. Academic Press, New York (1966)
8. Gelbart, S.: Weil's Representation and the Spectrum of the Metaplectic Group. Lecture Notes in Mathematics, vol. 530. Springer, Berlin (1976)
9. Kloosterman, H.D.: The behaviour of general theta functions under the modular group and the characters of binary modular congruence groups. I, II. Ann. Math. (2) **47**, 317–375, 376–447 (1946)
10. Kubota, T.: Topological covering of SL(2) over a local field. J. Math. Soc. Jpn. **19**, 114–121 (1967)
11. Maass, H.: Lectures on Modular Functions of One Complex Variable, 2nd edn. Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 29. Tata Institute of Fundamental Research, Bombay (1983)

12. Milnor, J., Husemoller, D.: Symmetric Bilinear Forms. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73. Springer, New York (1973)
13. Pfetzer, W.: Die Wirkung der Modulsubstitutionen auf mehrafache Thetareihen zu quadratischen Formen ungerader Variablenzahl. Arch. Math. **4**, 448–454 (1953)
14. Ryan, N., Skoruppa, N., Strömberg, F.: Numerical computation of a certain Dirichlet series attached to Siegel modular forms of degree two. Math. Comput. **81**(280), 2361–2376 (2012)
15. Scheithauer, N.R.: The Weil representation of $SL_2(\mathbb{Z})$ and some applications. Int. Math. Res. Not. **8**, 1488–1545 (2009)
16. Schoeneberg, B.: Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen. Math. Ann. **116**(1), 511–523 (1939)
17. Shimura, G.: On modular forms of half integral weight. Ann. Math. **97**, 440–481 (1973)
18. Shintani, T.: On construction of holomorphic cusp forms of half integral weight. Nagoya Math. J. **58**, 83–126 (1975)
19. Skoruppa, N.-P.: Finite quadratic modules, Weil representations and vector valued modular forms. (2013, preprint)
20. Skoruppa, N.P.: Über den Zusammenhang zwischen Jacobiformen und Modulformen halbganzen Gewichts. Bonner Math. Schriften, no. 159. University of Bonn, Bonn (1985)
21. Stein, W., et al.: Sage mathematics software (Version 5.3). The Sage Development Team (2012). http://www.sagemath.org
22. Weil, A.: Sur certains groupes d'opérateurs unitaires. Acta Math. **111**, 143–211 (1964)