Theta Series

Brooks Roberts

University of Idaho
Contents

1 Background ................................................................. 1
  1.1 Dirichlet characters ................................................. 1
  1.2 Fundamental discriminants ........................................... 6
  1.3 Quadratic extensions ............................................... 15
  1.4 Kronecker Symbol ................................................ 16
  1.5 Quadratic forms .................................................. 19
  1.6 The upper half-plane .............................................. 28
  1.7 Congruence subgroups ............................................. 29
  1.8 Modular forms .................................................... 29
  1.9 The symplectic group ............................................. 31
  1.10 The Siegel upper half-space .................................... 34

2 Classical theta series on $\mathbb{H}_1$ .................................. 39
  2.1 Definition and convergence ....................................... 39
  2.2 The Poisson summation formula .................................. 43
  2.3 Differential operators ........................................... 51
  2.4 A space of theta series ........................................... 56
  2.5 The case $N = 1$ .................................................. 60
  2.6 Example: a quadratic form of level one .......................... 62
  2.7 The case $N > 1$ .................................................. 64
  2.8 Example: the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ .... 83

3 Classical theta series on $\mathbb{H}_n$ .................................. 91
  3.1 Convergence .......................................................... 91
  3.2 The Eicher lemma .................................................. 99

A Some tables ............................................................... 103
  A.1 Tables of fundamental discriminants ............................ 103

Index ................................................................. 105

Symbols ........................................................... 107

Bibliography .......................................................... 110
List of Tables

A.1 Negative fundamental discriminants between $-1$ and $-100$ . . . 103
A.2 Positive fundamental discriminants between $1$ and $100$ . . . . . . 104
Chapter 1

Background

1.1 Dirichlet characters

Let \( N \) be a positive integer. A Dirichlet character modulo \( N \) is a homomorphism
\[
\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.
\]

If \( N \) is a positive integer and \( \chi \) is a Dirichlet character modulo \( N \), then we associate to \( \chi \) a function
\[
\mathbb{Z} \to \mathbb{C},
\]
also denoted by \( \chi \), by the formula
\[
\chi(a) = \begin{cases} 
\chi(a + N\mathbb{Z}) & \text{if } (a, N) = 1, \\
0 & \text{if } (a, N) > 1
\end{cases}
\]
for \( a \in \mathbb{Z} \). We refer to this function as the extension of \( \chi \) to \( \mathbb{Z} \). It is easy to verify that the following properties hold for the extension of \( \chi \) to \( \mathbb{Z} \):

1. \( \chi(1) = 1 \);
2. if \( a_1, a_2 \in \mathbb{Z} \), then \( \chi(a_1a_2) = \chi(a_1)\chi(a_2) \);
3. if \( a \in \mathbb{Z} \) and \( (a, N) > 1 \), then \( \chi(a) = 0 \);
4. if \( a_1, a_2 \in \mathbb{Z} \) and \( a_1 \equiv a_2 \pmod{N} \), then \( \chi(a_1) = \chi(a_2) \).

Let \( N \) be a positive integer, and let \( \chi \) be a Dirichlet character modulo \( N \). We have \( \chi(a)^{\phi(N)} = 1 \) for \( a \in \mathbb{Z} \) with \( (a, N) = 1 \); in particular, \( \chi(a) \) is a \( \phi(N) \)-th root of unity. Here, \( \phi(N) \) is the number of integers \( a \) such that \( (a, N) = 1 \) and \( 1 \leq a \leq N \).

If \( N = 1 \), then there exists exactly one Dirichlet character \( \chi \) modulo \( N \); the extension of \( \chi \) to \( \mathbb{Z} \) satisfies \( \chi(a) = 1 \) for all \( a \in \mathbb{Z} \).
Let $N$ be a positive integer. The Dirichlet character $\eta$ modulo $N$ that sends every element of $(\mathbb{Z}/N\mathbb{Z})^\times$ to 1 is called the principal character modulo $N$. The extension of $\eta$ to $\mathbb{Z}$ is given by

$$\eta(a) = \begin{cases} 1 & \text{if } (a, N) = 1, \\ 0 & \text{if } (a, N) > 1 \end{cases}$$

for $a \in \mathbb{Z}$.

Let $f : \mathbb{Z} \to \mathbb{C}$ be a function, let $N$ be a positive integer, and let $\chi$ be a Dirichlet character modulo $N$. We say that $f$ corresponds to $\chi$ if $f$ is the extension of $\chi$, i.e., $f(a) = \chi(a)$ for all $a \in \mathbb{Z}$.

Let $f : \mathbb{Z} \to \mathbb{C}$, and assume that there exists a positive integer $N$ and a Dirichlet character $\chi$ modulo $N$ such that $f$ corresponds to $\chi$. Assume $N > 1$. Then there exist infinitely many positive integers $N'$ and Dirichlet characters $\chi'$ modulo $N'$ such that $f$ corresponds to $\chi'$. For example, let $N'$ be any positive integer such that $N | N'$ and $N'$ has the same prime divisors as $N$. Let $\chi'$ be the Dirichlet character modulo $N'$ that is the composition

$$(\mathbb{Z}/N'\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times,$$

where the first map is the natural surjective homomorphism. The extension of $\chi'$ to $\mathbb{Z}$ is the same as the extension of $\chi$ to $\mathbb{Z}$, namely $f$. Thus, $f$ also corresponds to $\chi'$.

**Lemma 1.1.1.** Let $f : \mathbb{Z} \to \mathbb{C}$ be a function and let $N$ be a positive integer. Assume that $f$ satisfies the following conditions:

1. $f(1) \neq 0$;
2. if $a_1, a_2 \in \mathbb{Z}$, then $f(a_1 a_2) = f(a_1) f(a_2)$;
3. if $a \in \mathbb{Z}$ and $(a, N) > 1$, then $f(a) = 0$;
4. if $a \in \mathbb{Z}$, then $f(a + N) = f(a)$.

There exists a unique Dirichlet character $\chi$ modulo $N$ such that $f$ corresponds to $\chi$.

**Proof.** Assume that $f$ satisfies 1, 2, 3, and 4. Since $1 = 1 \cdot 1$, we have $f(1) = f(1) f(1)$, so that $f(1) = 1$. Next, we claim that $f(a_1) = f(a_2)$ for $a_1, a_2 \in \mathbb{Z}$ with $a_1 \equiv a_2 \pmod{N}$, or equivalently, if $a \in \mathbb{Z}$ and $x \in \mathbb{Z}$ then $f(a + xN) = f(a)$. Let $a \in \mathbb{Z}$ and $x \in \mathbb{Z}$. Write $x = \epsilon z$, where $\epsilon \in \{1, -1\}$ and $z$ is positive. Then

$$f(a + xN) = \chi(\epsilon(\epsilon a + zN))$$

$$= f(\epsilon) \chi(\epsilon a + zN)$$

$$= f(\epsilon) \chi(\epsilon a + N + \cdots + N)$$
1.1. DIRICHLET CHARACTERS

\[ f(\epsilon) = f(\epsilon_0) \]

Now let \( a \in \mathbb{Z} \) with \((a, N) = 1\); we assert that \( f(a) \neq 0\). Since \((a, N) = 1\), there exists \( b \in \mathbb{Z} \) such that \( ab = 1 + kN \) for some \( k \in \mathbb{Z} \). We have \( 1 = f(1) = f(1 + kN) = f(ab) = f(a)f(b) \). It follows that \( f(a) \neq 0\). We now define a function \( \chi : (\mathbb{Z}/NZ)^\times \to \mathbb{C}^\times \) by \( \chi(a + NZ) = f(a) \) for \( a \in \mathbb{Z} \) with \((a, N) = 1\).

By what we have already proven, \( \alpha \) is a well-defined function. It is also clear that \( \chi \) is a homomorphism. Finally, it is evident that the extension of \( \chi \) to \( \mathbb{Z} \) is \( f \), so that \( f \) corresponds to \( \chi \). The uniqueness assertion is clear.

Let \( p \) be an odd prime. For \( m \in \mathbb{Z} \) define the Legendre symbol by

\[ \left( \frac{m}{p} \right) = \begin{cases} 
0 & \text{if } p \text{ divides } m, \\
-1 & \text{if } (m, p) = 1 \text{ and } x^2 \equiv m \pmod{p} \text{ has no solution } x \in \mathbb{Z}, \\
1 & \text{if } (m, p) = 1 \text{ and } x^2 \equiv m \pmod{p} \text{ has a solution } x \in \mathbb{Z}.
\end{cases} \]

The function \( \left( \frac{\cdot}{p} \right) : \mathbb{Z} \to \mathbb{C} \) satisfies the conditions of Lemma 1.1.1 with \( N = p \). We will also denote the Dirichlet character modulo \( p \) to which \( \left( \frac{\cdot}{p} \right) \) corresponds by \( \left( \frac{\cdot}{p} \right) \). We note that \( \left( \frac{\cdot}{p} \right) \) is real valued, i.e., takes values in \([-1, 0, 1]\).

Let \( \beta \) be a Dirichlet character modulo \( M \). We can construct other Dirichlet characters from \( \beta \) by forgetting information, as follows. Let \( N \) be a positive multiple of \( M \). Since \( M \) divides \( N \), there is a natural surjective homomorphism

\[ (\mathbb{Z}/NZ)^\times \longrightarrow (\mathbb{Z}/MZ)^\times, \]

and we can form the composition \( \chi \)

\[ (\mathbb{Z}/NZ)^\times \longrightarrow (\mathbb{Z}/MZ)^\times \longrightarrow \mathbb{C}^\times. \]

Then \( \chi \) is a Dirichlet character modulo \( N \), and we say that \( \chi \) is induced from the Dirichlet character \( \beta \) modulo \( M \). If \( N \) is a positive integer and \( \chi \) is a Dirichlet character modulo \( N \), and \( \chi \) is not induced from any Dirichlet character \( \beta \) modulo \( M \) for a proper divisor \( M \) of \( N \), then we say that \( \chi \) is primitive.

Let \( N \) be a positive integer, and let \( \chi \) be a Dirichlet character. Consider the set of positive integers \( N_1 \) such that \( N_1 \mid N \) and

\[ \chi(a) = 1 \]

for \( a \in \mathbb{Z} \) such that \((a, N) = 1 \) and \( a \equiv 1 \pmod{N_1} \). This set is non-empty since it contains \( N \); we refer to the smallest such \( N_1 \) as the conductor of \( \chi \) and denote it by \( f(\chi) \).

**Lemma 1.1.2.** Let \( N \) be positive integer, and let \( \chi \) be a Dirichlet character modulo \( N \). Let \( N_1 \) be a positive integer such that \( N_1 \mid N \) and \( \chi(a) = 1 \) for \( a \in \mathbb{Z} \) such that \((a, N) = 1 \) and \( a \equiv 1 \pmod{N_1} \). Then \( f(\chi) \mid N_1 \).
Proof. We may assume that $N > 1$. Let $M = \gcd(f(\chi), N_1)$. We will prove that $\chi(a) = 1$ for $a \in \mathbb{Z}$ such that $(a, N) = 1$ and $a \equiv 1 \pmod{M}$; by the minimality of $f(\chi)$ this will imply that $M = f(\chi)$, so that $f(\chi) | N_1$. Let

$$N = p_1^{e_1} \cdots p_t^{e_t}$$

be the prime factorization of $r(\chi)$ into positive powers $e_1, \ldots, e_t$ of the distinct primes $p_1, \ldots, p_t$. Also, write

$$f(\chi) = p_1^{f_1} \cdots p_t^{f_t}, \quad N_1 = p_1^{k_1} \cdots p_t^{k_t}.$$

By definition,

$$M = p_1^{\min(f_1, k_1)} \cdots p_t^{\min(f_t, k_t)}.$$

Let $a \in \mathbb{Z}$ be such that $(a, N) = 1$ and $a \equiv 1 \pmod{M}$. By the Chinese remainder theorem, there exists an integer $b$ such that

$$b = \begin{cases} 1 \pmod{p_i^{f_i}} & \text{if } f_i \geq k_i, \\ a \pmod{p_i^{k_i}} & \text{if } f_i < k_i \end{cases}$$

for $i \in \{1, \ldots, t\}$, and $(b, r(\chi)) = 1$. Let $c$ be an integer such that $(c, N) = 1$ and $a \equiv bc \pmod{N}$. Evidently, $b \equiv 1 \pmod{p_i^{f_i}}$ and $c \equiv 1 \pmod{p_i^{k_i}}$ for $i \in \{1, \ldots, t\}$, so that $b \equiv 1 \pmod{f(\chi)}$ and $c \equiv 1 \pmod{N_1}$. It follows that $\chi(a) = \chi(bc) = \chi(b)\chi(c) = 1$. \qed

Lemma 1.1.3. Let $N$ be a positive integer, and let $\chi$ be a Dirichlet character modulo $N$. Then $\chi$ is primitive if and only if $f(\chi) = N$.

Proof. Assume that $\chi$ is primitive. By Lemma 1.1.2 $f(\chi)$ is a divisor of $N$. By the definition of $f(\chi)$, the character $\chi$ is trivial on the kernel of the natural map

$$(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/f(\chi)\mathbb{Z})^\times.$$ 

This implies that $\chi$ factors through this map. Since $\chi$ is primitive, $f(\chi)$ is not a proper divisor of $N$, so that $f(\chi) = N$. The converse statement has a similar proof. \qed

Evidently, the conductor of $(\chi \chi')$ is also $p$, so that $(\chi \chi')$ is primitive.

Lemma 1.1.4. Let $N_1$ and $N_2$ be positive integers, and let $\chi_1$ and $\chi_2$ be Dirichlet characters modulo $N_1$ and $N_2$, respectively. Let $N$ be the least common multiple of $N_1$ and $N_2$. The function $f : \mathbb{Z} \rightarrow \mathbb{C}$ defined by $f(a) = \chi_1(a)\chi_2(a)$ for $a \in \mathbb{Z}$ corresponds to a unique Dirichlet $\chi$ character modulo $N$.

Proof. It is clear that $f$ satisfies properties 1, 2 and 4 of Lemma 1.1.1. To see that $f$ satisfies property 3, assume that $a \in \mathbb{Z}$ and $(a, N) > 1$. We need to prove that $f(a) = 0$. There exists a prime $p$ such that $p|a$ and $p|N$. Write $a = pb$ for some $b \in \mathbb{Z}$. Since $f(a) = f(p)f(b)$ it will suffice to prove that $f(p) = 0$, i.e., $\chi_1(p) = 0$ or $\chi_2(p) = 0$. Since $p|N$, we have $p|N_1$ or $p|N_2$. This implies that $\chi_1(p) = 0$ or $\chi_2(p) = 0$. \qed
Let the notation be as in Lemma 1.1.4. We refer to the Dirichlet character \( \chi \) modulo \( N \) as the \textbf{product} of \( \chi_1 \) and \( \chi_2 \), and we write \( \chi_1 \chi_2 \) for \( \chi \).

**Lemma 1.1.5.** Let \( N_1 \) and \( N_2 \) be positive integers such that \( (N_1, N_2) = 1 \), and let \( \chi_1 \) and \( \chi_2 \) be Dirichlet characters modulo \( N_1 \) and modulo \( N_2 \), respectively. Let \( \chi = \chi_1 \chi_2 \), the product of \( \chi_1 \) and \( \chi_2 \); this is a Dirichlet character modulo \( N = N_1 N_2 \). The conductor of \( \chi \) is \( f(\chi) = f(\chi_1) f(\chi_2) \). Moreover, \( \chi \) is primitive if and only if \( \chi_1 \) and \( \chi_2 \) are primitive.

**Proof.** By Lemma 1.1.2 we have \( f(\chi_1) | N_1 \) and \( f(\chi_2) | N_2 \). Since \( N = N_1 N_2 \), we obtain \( f(\chi_1) f(\chi_2) | N \). Assume that \( a \in \mathbb{Z} \) is such that \( (a, N) = 1 \) and \( a \equiv 1 \mod f(\chi_1) f(\chi_2) \). Then \( (a, N_1) = (a, N_2) = 1 \), \( a \equiv 1 \mod f(\chi_1) \), and \( a \equiv 1 \mod f(\chi_2) \). Therefore, \( \chi_1(a) = \chi_2(a) = 1 \), so that \( \chi(a) = \chi_1(a) \chi_2(a) = 1 \).

By Lemma 1.1.2 it follows that we have \( f(\chi) | f(\chi_1) f(\chi_2) \). Write \( f(\chi) = M_1 M_2 \) where \( M_1 \) and \( M_2 \) are relatively prime positive integers such that \( f(\chi_1) | M_1 \) and \( f(\chi_2) | M_2 \). We need to prove that \( M_1 = f(\chi_1) \) and \( M_2 = f(\chi_2) \). Let \( a \in \mathbb{Z} \) be such that \( (a, N_1) = 1 \) and \( a \equiv 1 \mod M_1 \). By the Chinese remainder theorem, there exists an integer \( b \) such that \( b \equiv a \mod M_1 \), \( b \equiv 1 \mod f(\chi_2) \), and \( (b, N) = 1 \). Evidently, \( b \equiv 1 \mod f(\chi) \). Hence, \( 1 = \chi(b) = \chi_1(b) \chi_2(b) = \chi_1(a) \).

By the minimality of \( f(\chi_1) \) we must now have \( M_1 = f(\chi_1) \). Similarly, \( M_2 = f(\chi_2) \). The final assertion of the lemma is straightforward.

**Lemma 1.1.6.** Let \( p \) be an odd prime. The Legendre symbol \( \left( \frac{\cdot}{p} \right) \) is the only real valued primitive Dirichlet character modulo \( p \). If \( e \) is a positive integer with \( e > 1 \), then there exist no real valued primitive Dirichlet characters modulo \( p^e \).

**Proof.** We have already remarked that \( \left( \frac{\cdot}{p} \right) \) is a real valued primitive Dirichlet character modulo \( p \). To prove the remaining assertions, let \( e \) be a positive integer, and assume that \( \chi \) is a real valued primitive Dirichlet character modulo \( p^e \); we will prove that \( \chi = \left( \frac{\cdot}{p} \right) \) if \( e = 1 \) and obtain a contradiction if \( e > 1 \).

Consider \( \mathbb{Z}/p^e \mathbb{Z} \). It is known that this group is cyclic; let \( x \in \mathbb{Z} \) be such that \( (x, p) = 1 \) and \( x + p^e \mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e \mathbb{Z} \). Since \( \chi \) has conductor \( p^e \), and since \( x + p^e \mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e \mathbb{Z} \), we must have \( \chi(x) \neq 1 \). Since \( \chi \) is real valued we obtain \( \chi(x) = -1 \). On the other hand, the function \( \left( \frac{\cdot}{p} \right) \) is also a real valued Dirichlet character modulo \( p^e \) such that \( \left( \frac{x}{p} \right) = -1 \) for some \( a \in \mathbb{Z} \); since \( x + p^e \mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e \mathbb{Z} \), this implies that \( \left( \frac{x}{p} \right) = -1 \), so that \( \chi(x) = \left( \frac{x}{p} \right) \). Since \( x + p^e \mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e \mathbb{Z} \) and \( \chi(x) = -1 = \chi(x) \)

we must have \( \chi = \left( \frac{\cdot}{p} \right) \). We see that if \( e = 1 \), then the Legendre symbol \( \left( \frac{\cdot}{p} \right) \) is the only real valued primitive Dirichlet character modulo \( p \). Assume that \( e > 1 \). It is easy to verify that the conductor of the Dirichlet character \( \left( \frac{\cdot}{p} \right) \) modulo \( p^e \) is \( p \); this is a contradiction since by Lemma 1.1.3 the conductor of \( \chi \) is \( p^e \).

**Lemma 1.1.7.** There are no primitive characters modulo 2. There exists a unique primitive Dirichlet character \( \varepsilon_4 \) modulo 4 = 2^2 which is defined by

\[
\begin{align*}
\varepsilon_4(1) &= 1, \\
\varepsilon_4(3) &= -1.
\end{align*}
\]
There exist two primitive Dirichlet characters \( \varepsilon'_8 \) and \( \varepsilon''_8 \) modulo \( 8 = 2^3 \) which are defined by

\[
\begin{align*}
\varepsilon'_8(1) &= 1, & \varepsilon''_8(1) &= 1, \\
\varepsilon'_8(3) &= -1, & \varepsilon''_8(3) &= 1, \\
\varepsilon'_8(5) &= -1, & \varepsilon''_8(5) &= -1, \\
\varepsilon'_8(7) &= 1, & \varepsilon''_8(7) &= -1.
\end{align*}
\]

There exist no real valued primitive Dirichlet characters modulo \( p^e \) for \( e \geq 4 \).

**Proof.** We have \((\mathbb{Z}/2\mathbb{Z})^\times = \{1\}\). It follows that the unique Dirichlet character modulo 2 has conductor conductor 1; by Lemma 1.1.3, this character is not primitive.

We have \((\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}\). Hence, there exist two Dirichlet characters modulo 4. The non-principal Dirichlet character modulo 4 is \( \varepsilon_4 \); since \( \varepsilon_4(1+2) = -1 \), it follows that the conductor of \( \varepsilon_4 \) is 4. By Lemma 1.1.3, \( \varepsilon_4 \) is primitive.

We have \((\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} = \{1, 3\} \times \{1, 5\}\). The non-principal Dirichlet characters modulo 8 are \( \varepsilon'_8, \varepsilon''_8 \), and \( \varepsilon'_8 \varepsilon''_8 \). Since \( \varepsilon'_8(1+4) = \varepsilon''_8(1+4) = -1 \) we have \( f(\varepsilon'_8) = f(\varepsilon''_8) = 8 \). Since \( (\varepsilon'_8 \varepsilon''_8)(1+4) = 1 \) we have \( f(\varepsilon'_8 \varepsilon''_8) = 4 \). Hence, by Lemma 1.1.3, \( \varepsilon'_8 \) and \( \varepsilon''_8 \) are primitive, and \( \varepsilon'_8 \varepsilon''_8 \) is not primitive.

Finally, assume that \( e \geq 4 \) and let \( \chi \) be a real valued Dirichlet character modulo \( p^e \). Let \( n \in \mathbb{Z} \) be such that \((n, 2) = 1 \) and \( n \equiv 1 \) (mod 8). It is known that there exists \( a \in \mathbb{Z} \) such that \( n \equiv a^2 \) (mod \( p^e \)). We obtain \( \chi(n) = \chi(a^2) = \chi(a)^2 = 1 \) because \( \chi(a) = \pm 1 \) (since \( \chi \) is real valued). By Lemma 1.1.2 the conductor \( f(\chi) \) divides 8. By Lemma 1.1.3, \( \chi \) is not primitive. \( \square \)

### 1.2 Fundamental discriminants

Let \( D \) be a non-zero integer. We say that \( D \) is a **fundamental discriminant** if

\[
D \equiv 1 \pmod{4} \text{ and } D \text{ is square-free,}
\]

or

\[
D \equiv 0 \pmod{4}, D/4 \text{ is square-free, and } D/4 \equiv 2 \text{ or } 3 \pmod{4}.
\]

We say that \( D \) is a **prime fundamental discriminant** if

\[
D = -8 \text{ or } D = -4 \text{ or } D = 8,
\]

or

\[
D = -p \text{ for } p \text{ a prime such that } p \equiv 3 \pmod{4},
\]

or

\[
D = p \text{ for } p \text{ a prime such that } p \equiv 1 \pmod{4}.
\]
1.2. FUNDAMENTAL DISCRIMINANTS

it is clear that if $D$ is a prime fundamental discriminant, then $D$ is a fundamental discriminant.

**Lemma 1.2.1.** Let $D_1$ and $D_2$ be relatively prime fundamental discriminants. Then $D_1D_2$ is a fundamental discriminant.

*Proof.* The proof is straightforward. Note that since $D_1$ and $D_2$ are relatively prime, at most one of $D_1$ and $D_2$ is divisible by 4. □

**Lemma 1.2.2.** Let $D$ be a fundamental discriminant such that $D \neq 1$. There exist prime fundamental discriminants $D_1, \ldots, D_k$ such that

$$D = D_1 \cdots D_k$$

and $D_1, \ldots, D_k$ are pairwise relatively prime.

*Proof.* Assume that $D < 0$ and $D \equiv 1 \pmod{4}$. We may write $D = -p_1 \cdots p_t$ for a non-empty collection of distinct primes $p_1, \ldots, p_t$. Since $D$ is odd, each of $p_1, \ldots, p_t$ is odd and is hence congruent to 1 or 3 mod 4. Let $r$ be the number of the primes $p$ from $p_1, \ldots, p_t$ such that $p \equiv 3 \pmod{4}$. We have

$$1 \equiv D \pmod{4}$$
$$\equiv (-1)^{3r} \pmod{4}$$
$$1 \equiv (-1)^{r+1} \pmod{4}.$$ 

It follows that $r$ is odd. Hence,

$$D = -\prod_{p \in \{p_1, \ldots, p_t\}} p$$
$$= -\left( \prod_{p \equiv 1 \pmod{4}, p \in \{p_1, \ldots, p_t\}} p \right) \times \left( \prod_{p \equiv 3 \pmod{4}, p \in \{p_1, \ldots, p_t\}} p \right)$$

$$D = \left( \prod_{p \equiv 1 \pmod{4}, p \in \{p_1, \ldots, p_t\}} p \right) \times \left( \prod_{p \equiv 3 \pmod{4}, p \in \{p_1, \ldots, p_t\}} -p \right).$$

Each of the factors in the last equation is a prime fundamental discriminant, which proves the lemma in this case.

Assume that $D < 0$ and $D \equiv 0 \pmod{4}$. If $D = -4$, then $D$ is a prime fundamental discriminant. Assume that $D \neq -4$. We may write $D = -4p_1 \cdots p_t$ for a non-empty collection of distinct primes $p_1, \ldots, p_t$ such that $-p_1 \cdots p_t \equiv 2$ or 3 (mod 4). Assume first that $-p_1 \cdots p_t \equiv 2$ (mod 4). Then exactly one of $p_1, \ldots, p_t$ is even, say $p_1 = 2$. Let $r$ be the number of the primes $p$ from $p_2, \ldots, p_t$ such that $p \equiv 3 \pmod{4}$. We have

$$D = -4 \prod_{p \in \{p_1, \ldots, p_t\}} p$$
\[ D = -8 \prod_{p \in \{p_2, \ldots, p_t\}} p \]
\[ = -8 \left( \prod_{p \in \{p_2, \ldots, p_t\}, \, p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, \, p \equiv 3 \pmod{4}} p \right) \]
\[ D = \left( -1 \right)^{r+1} \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, \, p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, \, p \equiv 3 \pmod{4}} p \right) \]

Each of the factors in the last equation is a prime fundamental discriminant, which proves the lemma in this case. Now assume that \(-p_1 \cdots p_t \equiv 3 \pmod{4}\). Then \(p_1, \ldots, p_t\) are all odd. Let \(r\) be the number of the primes \(p\) from \(p_1, \ldots, p_t\) such that \(p \equiv 3 \pmod{4}\). We have
\[ 3 \equiv -p_1 \cdots p_t \pmod{4} \]
\[ -1 \equiv (-1)^3 r \pmod{4} \]
\[ 1 \equiv (-1)^r \pmod{4} \]

It follows that \(r\) is even. Hence,
\[ D = -4 \prod_{p \in \{p_1, \ldots, p_t\}} p \]
\[ = -4 \left( \prod_{p \in \{p_1, \ldots, p_t\}, \, p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \, p \equiv 3 \pmod{4}} p \right) \]
\[ D = (-4) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \, p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \, p \equiv 3 \pmod{4}} p \right) \]

Each of the factors in the last equation is a prime fundamental discriminant, proving the lemma in this case.

Assume that \(D > 0\) and \(D \equiv 1 \pmod{4}\). Since \(D \neq 1\) by assumption, we have \(D = p_1 \cdots p_t\) for a non-empty collection of distinct odd primes \(p_1, \ldots, p_t\). Let \(r\) be the number of the primes \(p\) from \(p_1, \ldots, p_t\) such that \(p \equiv 3 \pmod{4}\). We have
\[ 1 \equiv D \pmod{4} \]
\[ \equiv 3^r \pmod{4} \]
\[ 1 \equiv (-1)^r \pmod{4} \]

We see that \(r\) is even. Therefore,
\[ D = \prod_{p \in \{p_1, \ldots, p_t\}} p \]
\[ = \left( \prod_{p \in \{p_1, \ldots, p_t\}, \, p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \, p \equiv 3 \pmod{4}} p \right) \]
1.2. FUNDAMENTAL DISCRIMINANTS

\[ D = \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 3 \pmod{4}} -p \right). \]

Each of the factors in the last equation is a prime fundamental discriminant, proving the lemma in this case.

Finally, assume that \( D > 0 \) and \( D \equiv 0 \pmod{4} \). We may write \( D = 4p_1 \cdots p_t \) for a non-empty collection of distinct primes \( p_1, \ldots, p_t \) such that \( p_1 \cdots p_t \equiv 2 \) or \( 3 \pmod{4} \). Assume first that \( p_1 \cdots p_t \equiv 2 \pmod{4} \). Then exactly one of \( p_1, \ldots, p_t \) is even, say \( p_1 = 2 \). Let \( r \) be the number of the primes \( p \) from \( p_2, \ldots, p_t \) such that \( p \equiv 3 \pmod{4} \). We have

\[ D = 4 \prod_{p \in \{p_1, \ldots, p_t\}} p = 8 \left( \prod_{p \in \{p_2, \ldots, p_t\}, \ p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, \ p \equiv 3 \pmod{4}} p \right) = ((-1)^r 8) \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, \ p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, \ p \equiv 3 \pmod{4}} -p \right). \]

Each of the factors in the last equation is a prime fundamental discriminant, which proves the lemma in this case. Now assume that \( p_1 \cdots p_t \equiv 3 \pmod{4} \). Then \( p_1, \ldots, p_t \) are all odd. Let \( r \) be the number of the primes \( p \) from \( p_1, \ldots, p_t \) such that \( p \equiv 3 \pmod{4} \). We have

\[
\begin{align*}
3 &\equiv p_1 \cdots p_t \pmod{4} \\
-1 &\equiv 3^r \pmod{4} \\
-1 &\equiv (-1)^r \pmod{4} \\
1 &\equiv (-1)^{r+1} \pmod{4}
\end{align*}
\]

It follows that \( r \) is odd. Hence,

\[ D = 4 \prod_{p \in \{p_1, \ldots, p_t\}} p = 4 \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 3 \pmod{4}} p \right) = (-4) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 3 \pmod{4}} -p \right). \]

Each of the factors in the last equation is a prime fundamental discriminant, proving the lemma in this case. \( \Box \)
CHAPTER 1. BACKGROUND

The fundamental discriminants between $-1$ and $-100$ are listed in Table A.1 and the fundamental discriminants between $1$ and $100$ are listed in Table A.2.

Let $D$ be a fundamental discriminant. We define a function

$$\chi_D : \mathbb{Z} \rightarrow \mathbb{C}$$

in the following way. First, let $p$ be a prime. We define

$$\chi_D(p) = \begin{cases} 
\left(\frac{D}{p}\right) & \text{if } p \text{ is odd}, \\
1 & \text{if } p = 2 \text{ and } D \equiv 1 \pmod{8}, \\
-1 & \text{if } p = 2 \text{ and } D \equiv 5 \pmod{8}, \\
0 & \text{if } p = 2 \text{ and } D \equiv 0 \pmod{4}.
\end{cases}$$

Note that since $D$ is a fundamental discriminant, we have $D \not\equiv 3 \pmod{8}$ and $D \not\equiv 7 \pmod{8}$. If $n$ is a positive integer, and

$$n = p_1^{e_1} \cdots p_t^{e_t}$$

is the prime factorization of $n$, where $p_1, \ldots, p_t$ are primes, then we define

$$\chi_D(n) = \chi_D(p_1)^{e_1} \cdots \chi_D(p_t)^{e_t}. \quad (1.1)$$

This defines $\chi_D(n)$ for all positive integers $n$. We also define

$$\chi_D(-n) = \chi_D(-1)\chi_D(n)$$

for all positive integers $n$, where we define

$$\chi_D(-1) = \begin{cases} 
1 & \text{if } D > 0, \\
-1 & \text{if } D < 0.
\end{cases}$$

Finally, we define

$$\chi_D(0) = \begin{cases} 
0 & \text{if } D \neq 1, \\
1 & \text{if } D = 1.
\end{cases}$$

We note that if $D = 1$, then $\chi_1(a) = 1$ for $a \in \mathbb{Z}$. Thus, $\chi_1$ is the unique Dirichlet character modulo $1$ (which has conductor $1$, and is thus primitive).

**Lemma 1.2.3.** Let $D_1$ and $D_2$ be relatively prime fundamental discriminants. Then

$$\chi_{D_1D_2}(a) = \chi_{D_1}(a)\chi_{D_2}(a)$$

for all $a \in \mathbb{Z}$.

**Proof.** It is easy to verify that $\chi_{D_1D_2}(p) = \chi_{D_1}(p)\chi_{D_2}(p)$ for all primes $p$, $\chi_{D_1D_2}(-1) = \chi_{D_1}(-1)\chi_{D_2}(-1)$, and $\chi_{D_1D_2}(0) = 0 = \chi_{D_1}(0)\chi_{D_2}(0)$. The assertion of the lemma now follows from the definitions of $\chi_D$, $\chi_{D_1}$ and $\chi_{D_2}$ on composite numbers. \(\square\)
Lemma 1.2.4. Let $D$ be a fundamental discriminant. The function $\chi_D$ corresponds to a primitive Dirichlet character modulo $|D|$.

Proof. By Lemma 1.2.2 we can write

$$D = D_1 \cdots D_k$$

where $D_1, \ldots, D_k$ are prime fundamental discriminants and $D_1, \ldots, D_k$ are pairwise relatively prime. By Lemma 1.2.3,

$$\chi_D(a) = \chi_{D_1}(a) \cdots \chi_{D_k}(a)$$

for $a \in \mathbb{Z}$. Lemma 1.1.4 and Lemma 1.1.5 now imply that we may assume that $D$ is a prime fundamental discriminant. For the following argument we recall the Dirichlet characters $\varepsilon_4$, $\varepsilon'_8$ and $\varepsilon''_8$ from Lemma 1.1.7.

Assume first that $D = -8$ so that $|D| = 8$. Let $p$ be an odd prime. Then

$$\chi_{-8}(p) = \left(\frac{-8}{p}\right)$$

$$= \left(\frac{-2}{p}\right)^3$$

$$= \left(\frac{-2}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

$$= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$$

$$= \begin{cases} 1 & \text{if } p \equiv 1,3 \pmod{8} \\ -1 & \text{if } p \equiv 5,7 \pmod{8} \end{cases}$$

Also,

$$\chi_{-8}(2) = 1.$$

We see that $\chi_{-8}(p) = \varepsilon''_8(p)$ for all primes $p$. Also, $\chi_{-8}(-1) = -1 = \varepsilon''_8(-1)$ and $\chi_{-8}(0) = 0 = \varepsilon''_8(0)$. Since $\chi_{-8}$ and $\varepsilon''_8$ are multiplicative, it follows that

$$\chi_{-8} = \varepsilon''_8,$$

so that $\chi_{-8}$ corresponds to a primitive Dirichlet character mod $|−8| = 8$.

Assume that $D = -4$ so that $|D| = 4$. Let $p$ be an odd prime. Then

$$\chi_{-4}(p) = \left(\frac{-4}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^2$$

$$= \left(\frac{-1}{p}\right).$$
\[ = (−1)^\frac{p−1}{2} \]
\[ = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
−1 & \text{if } p \equiv 3 \pmod{4}. 
\end{cases} \]

Also, \( \chi_{−4}(2) = 0, \chi_{−4}(−1) = −1, \) and \( \chi_{−4}(0) = 0. \) We see that \( \chi_{−4}(p) = \varepsilon_{4}(p) \)
for all primes \( p. \) Also, \( \chi_{−4}(−1) − 1 = \varepsilon_{4}(−1) \) and \( \chi_{−4}(0) = 0 = \varepsilon_{4}(0). \) Since \( \chi_{−4} \) and \( \varepsilon_{4} \) are multiplicative, it follows that
\[ \chi_{−4} = \varepsilon_{4}, \]
so that \( \chi_{−4} \) corresponds to a primitive Dirichlet character mod \( |−4| = 4. \)

Assume that \( D = 8. \) Let \( p \) be an odd prime. Then
\[ \chi_{8}(p) = \left(\frac{8}{p}\right) \\
= \left(\frac{2}{p}\right)^3 \\
= \left(\frac{2}{p}\right) \\
= (−1)^\frac{p^2−1}{8} \\
= \begin{cases} 
1 & \text{if } p \equiv 1, 7 \pmod{8}, \\
−1 & \text{if } p \equiv 3, 5 \pmod{8}. 
\end{cases} \]

Also, \( \chi_{8}(2) = 0, \chi_{8}(−1) = 1, \) and \( \chi_{8}(0) = 0. \) We see that \( \chi_{8}(p) = \varepsilon'_{8}(p) \)
for all primes \( p. \) Also, \( \chi_{8}(−1) = 1 = \varepsilon'_{8}(−1) \) and \( \chi_{8}(0) = 0 = \varepsilon'_{8}(0). \) Since \( \chi_{8} \) and \( \varepsilon'_{8} \) are multiplicative, it follows that
\[ \chi_{8} = \varepsilon'_{8}, \]
so that \( \chi_{8} \) corresponds to a primitive Dirichlet character mod \( |8| = 8. \)

Assume that \( D = −q \) for a prime \( q \) such that \( q \equiv 3 \pmod{4}. \) Let \( p \) be an odd prime. Then
\[ \chi_{D}(p) = \left(\frac{−q}{p}\right) \\
= \left(\frac{−1}{p}\right) \left(\frac{q}{p}\right) \\
= (−1)^\frac{p−1}{2} (−1)^\frac{p−1}{2} \left(\frac{q}{p}\right) \\
= (−1)^\frac{p−1}{2} \left(−1\right)^\frac{p−1}{2} \left(\frac{q}{p}\right) \\
= (−1)^\frac{p−1}{2} \left(\frac{q}{p}\right) \\
= (−1)^{p−1} \left(\frac{q}{p}\right) \\
= (−1)^{p−1} \left(\frac{P}{q}\right) \\
= (−1)^{p−1} \left(\frac{P}{q}\right). \]
1.2. FUNDAMENTAL DISCRIMINANTS

\[ = \left( \frac{p}{q} \right). \]

Also,

\[ \chi_D(2) = \begin{cases} 1 & \text{if } -q \equiv 1 \pmod{8}, \\ -1 & \text{if } -q \equiv 5 \pmod{8} \end{cases} \]

\[ = \begin{cases} 1 & \text{if } q \equiv 7 \pmod{8}, \\ -1 & \text{if } q \equiv 3 \pmod{8} \end{cases} \]

\[ = (-1)^{\frac{q^2 - 1}{8}} \]

\[ = \left( \frac{2}{q} \right), \]

and

\[ \chi_D(-1) = 1 \]

\[ = (-1)^{\frac{q-1}{2}} \]

\[ = \left( \frac{-1}{q} \right). \]

Since \( \left( \frac{\cdot}{q} \right) \) and \( \chi_D \) are multiplicative, it follows that \( \left( \frac{\cdot}{q} \right) = \chi_D(a) \) for all \( a \in \mathbb{Z} \). Since \( \left( \frac{\cdot}{q} \right) \) is a primitive Dirichlet character modulo \( q \), it follows that \( \chi_D \) corresponds to a primitive Dirichlet character modulo \( q = | - q | = | D | \).

Assume that \( D = q \) for a prime \( q \) such that \( q \equiv 1 \pmod{4} \). Let \( p \) be an odd prime. Then

\[ \chi_D(p) = \left( \frac{q}{p} \right) \]

\[ = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}} \left( \frac{p}{q} \right) \]

\[ = (-1)^{\frac{q-1}{2} \cdot 2} \left( \frac{p}{q} \right) \]

\[ = \left( \frac{p}{q} \right). \]

Also,

\[ \chi_D(2) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod{8}, \\ -1 & \text{if } q \equiv 5 \pmod{8} \end{cases} \]

\[ = (-1)^{\frac{q^2 - 1}{8}} \]

\[ = \left( \frac{2}{q} \right), \]

and

\[ \chi_D(-1) = 1 \]
\[ = (-1)^{\frac{q-1}{2}} \]
\[ = \left( \frac{-1}{q} \right). \]

Since \( \left( \frac{\cdot}{q} \right) \) and \( \chi_D \) are multiplicative, it follows that \( \left( \frac{a}{q} \right) = \chi_D(a) \) for all \( a \in \mathbb{Z} \). Since \( \left( \frac{\cdot}{q} \right) \) is a primitive Dirichlet character modulo \( q \), it follows that \( \chi_D \) corresponds to a primitive Dirichlet character modulo \( q = |q| = |D| \). \( \square \)

From the proof of Lemma 1.2.4 we see that if \( D \) is a prime fundamental discriminant with \( D > 1 \), then

\[ \chi_D = \begin{cases} 
\varepsilon_s'' & \text{if } D = -8, \\
\varepsilon_4 & \text{if } D = -4, \\
\varepsilon_s' & \text{if } D = 8, \\
\left( \frac{-}{p} \right) & \text{if } D = -p \text{ is a prime with } p \equiv 3 \pmod{4}, \\
\left( \frac{-}{p} \right) & \text{if } D = p \text{ is a prime with } p \equiv 1 \pmod{4}. 
\end{cases} \] (1.2)

**Proposition 1.2.5.** Let \( N \) be a positive integer, and let \( \chi \) be a Dirichlet character modulo \( N \). Assume that \( \chi \) is primitive and real valued (i.e., \( \chi(a) \in \{0, 1, -1\} \) for \( a \in \mathbb{Z} \)). Then there exists a fundamental discriminant \( D \) such that \( |D| = N \) and \( \chi = \chi_D \).

**Proof.** If \( N = 1 \), then \( \chi \) is the unique Dirichlet character modulo 1; we have already remarked that \( \chi_1 \) is also the unique Dirichlet character modulo 1. Assume that \( N > 1 \). Let

\[ N = p_1^{e_1} \cdots p_t^{e_t} \]

be the prime factorization of \( N \) into positive powers \( e_1, \ldots, e_t \) of the distinct primes \( p_1, \ldots, p_t \). We have

\[ (\mathbb{Z}/N\mathbb{Z})^\times \overset{\sim}{\rightarrow} (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_t^{e_t}\mathbb{Z})^\times \]

where the isomorphism sends \( x + N\mathbb{Z} \) to \( (x + p_1^{e_1}\mathbb{Z}, \ldots, x + p_t^{e_t}\mathbb{Z}) \) for \( x \in \mathbb{Z} \). Let \( i \in \{1, \ldots, t\} \). Let \( \chi_i \) be the character of \( (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \) which is the composition

\[ (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \hookrightarrow (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_t^{e_t}\mathbb{Z})^\times \overset{\sim}{\rightarrow} (\mathbb{Z}/N\mathbb{Z})^\times \overset{\chi}{\rightarrow} \mathbb{C}^\times, \]

where the first map is inclusion. We have

\[ \chi(a) = \chi_1(a) \cdots \chi_t(a) \]

for \( a \in \mathbb{Z} \). By Lemma 1.1.5 the Dirichlet characters \( \chi_1, \ldots, \chi_t \) are primitive. Also, it is clear that \( \chi_1, \ldots, \chi_t \) are all real valued. Again let \( i \in \{1, \ldots, t\} \).
Assume first that \( p_i \) is odd. Since \( \chi_i \) is primitive, Lemma 1.1.6 implies that \( e_i = 1 \), and that \( \chi_i = \left( \frac{\cdot}{p_i} \right) \), the Legendre symbol. By (1.2), \( \chi_i = \chi_{D_i} \), where

\[
D_i = \begin{cases} 
  p_i & \text{if } p_i \equiv 1 \pmod{4}, \\
  -p_i & \text{if } p_i \equiv 3 \pmod{4}.
\end{cases}
\]

Evidently, \(|-D_i| = p_i^{e_i}|. Next, assume that \( p_i = 2 \). By Lemma 1.1.7 we see that \( e_i = 2 \) or \( e_i = 3 \) with \( \chi_i = \varepsilon_4 \) if \( e_i = 2 \), and \( \chi_i = \varepsilon_8' \) or \( \varepsilon_8'' \) if \( e_i = 3 \). By (1.2), \( \chi_i = \chi_{D_i} \), where

\[
D_i = \begin{cases} 
  -4 & \text{if } e_i = 2, \\
  8 & \text{if } e_i = 3 \text{ and } \chi_i = \varepsilon_8', \\
  -8 & \text{if } e_i = 3 \text{ and } \chi_i = \varepsilon_8''.
\end{cases}
\]

Clearly, \(|-D_i| = p_i^{e_i}|. To now complete the proof, we note that by Lemma 1.2.1 the product \( D = D_1 \cdots D_t \) is a fundamental discriminant, and by Lemma 1.2.3 we have \( \chi_D = \chi_{D_1} \cdots \chi_{D_t} \). Since \( \chi_{D_1} \cdots \chi_{D_t} = \chi_1 \cdots \chi_t = \chi \) and \(|D| = N\), this completes the proof.

### 1.3 Quadratic extensions

**Proposition 1.3.1.** The map

\[
\{\text{quadratic extensions } K \text{ of } \mathbb{Q}\} \sim \to \{\text{fundamental discriminants } D, D \neq 1\}
\]

that sends \( K \) to its discriminant \( \text{disc}(K) \) is a well-defined bijection. Let \( K \) be a quadratic extension of \( \mathbb{Q} \), and let \( p \) be a prime. Then the prime factorization of the ideal \((p)\) generated by \( p \) in \( \mathfrak{o}_K \) is given as follows:

\[
(p) = \begin{cases} 
  p^2 & (p \text{ is ramified}) \quad \text{if } \chi_D(p) = 0, \\
  p \cdot p' & (p \text{ splits}) \quad \text{if } \chi_D(p) = 1, \\
  p & (p \text{ is inert}) \quad \text{if } \chi_D(p) = -1.
\end{cases}
\]

Here, in the first and third case, \( p \) is the unique prime ideal of \( \mathfrak{o}_K \) lying over \((p)\), and in the second case, \( p \) and \( p' \) are the two distinct prime ideals of \( \mathfrak{o}_K \) lying over \((p)\).

**Proof.** Let \( K \) be a quadratic extension of \( \mathbb{Q} \). There exists a square-free integer \( d \) such that \( K = \mathbb{Q}(\sqrt{d}) \). Let \( \mathfrak{o}_K \) be the ring of integers of \( K \). It is known that

\[
\mathfrak{o}_K = \begin{cases} 
  \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{d} & \text{if } d \equiv 2, 3 \pmod{4}, \\
  \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}.
\end{cases}
\]
By the definition of $\text{disc}(K)$, we have

$$\text{disc}(K) = \begin{cases} \det(\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix})^2 & \text{if } d \equiv 2, 3 \pmod{4}, \\ \det(\begin{pmatrix} 1 & 1 + \sqrt{d} \\ 1 & 1 - \sqrt{d} \end{pmatrix})^2 & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

$$= \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod{4}, \\ d & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

It follows that the map is well-defined, and a bijection. For a proof of the remaining assertion see Satz 1 on page 100 of [28], or Theorem 25 on page 74 of [16].

**Lemma 1.3.2.** Let $D$ be a fundamental discriminant such that $D \neq 1$. Let $K = \mathbb{Q}(\sqrt{D})$, so that $K$ is a quadratic extension of $\mathbb{Q}$. Then $\text{disc}(K) = D$.

**Proof.** Assume that $D \equiv 1 \pmod{4}$. Then $D$ is square-free. From the proof of Proposition 1.3.1 we have $\text{disc}(K) = D$. Assume that $D \equiv 0 \pmod{4}$. Then $K = \mathbb{Q}(\sqrt{D/4})$, with $D/4$ square-free and $D/4 \equiv 2, 3 \pmod{4}$. From the proof of Proposition 1.3.1 we again obtain $\text{disc}(K) = 4 \cdot (D/4) = D$.

### 1.4 Kronecker Symbol

Let $\Delta$ be a non-zero integer such that $\Delta \equiv 0, 1 \pmod{4}$. We define a function,

$$\left( \frac{\Delta}{\cdot} \right) : \mathbb{Z} \rightarrow \mathbb{C}$$

called the **Kronecker symbol**, in the following way. First, let $p$ be a prime. We define

$$\left( \frac{\Delta}{p} \right) = \begin{cases} \left( \frac{\Delta}{p} \right) \text{ (Legendre symbol) if } p \text{ is odd,} \\ 0 & \text{if } p = 2 \text{ and } \Delta \text{ is even,} \\ 1 & \text{if } p = 2 \text{ and } \Delta \equiv 1 \pmod{8}, \\ -1 & \text{if } p = 2 \text{ and } \Delta \equiv 5 \pmod{8}. \end{cases}$$

Note that, since by assumption $\Delta \equiv 0, 1 \pmod{4}$, the cases $\Delta \equiv 3 \pmod{8}$ and $\Delta \equiv 7 \pmod{8}$ do not occur. We see that if $p$ is a prime, then $p | \Delta$ if and only if $\left( \frac{\Delta}{p} \right) = 0$. If $n$ is a positive integer, and

$$n = p_1^{e_1} \cdots p_i^{e_i}$$

we have

$$\left( \frac{\Delta}{n} \right) = \left( \frac{\Delta}{p_1} \right)^{e_1} \cdots \left( \frac{\Delta}{p_i} \right)^{e_i}.$$
1.4. KRONECKER SYMBOL

is the prime factorization of \( n \), where \( p_1, \ldots, p_t \) are primes, then we define

\[
\left( \frac{\Delta}{n} \right) = \left( \frac{\Delta}{p_1} \right)^{e_1} \cdots \left( \frac{\Delta}{p_t} \right)^{e_t}.
\]

This defines \( \left( \frac{\Delta}{n} \right) \) for all positive integers \( n \). We also define

\[
\left( \frac{\Delta}{-n} \right) = \left( \frac{-1}{n} \right) \left( \frac{\Delta}{n} \right)
\]

for all positive integers \( n \), where we define

\[
\left( \frac{\Delta}{-1} \right) = \begin{cases} 
1 & \text{if } \Delta > 0, \\
-1 & \text{if } \Delta < 0.
\end{cases}
\]

Finally, we define

\[
\left( \frac{\Delta}{0} \right) = \begin{cases} 
0 & \text{if } \Delta \neq 1, \\
1 & \text{if } \Delta = 1.
\end{cases}
\]

We note that if \( \Delta = 1 \), then \( \left( \frac{\Delta}{a} \right) \left( \frac{\Delta}{b} \right) = 1 \) for \( a \in \mathbb{Z} \). Thus, \( \left( \frac{\Delta}{1} \right) \) is the unique Dirichlet character modulo 1. It is straightforward to verify that

\[
\left( \frac{\Delta}{a\cdot b} \right) = \left( \frac{\Delta}{a} \right) \left( \frac{\Delta}{b} \right)
\]

for \( a, b \in \mathbb{Z} \). Also, we note that \( \left( \frac{\Delta}{0} \right) = 0 \) if and only if \( (a, \Delta) > 1 \).

**Lemma 1.4.1.** Let \( D \) be a non-zero integer such that \( D \equiv 1 \) (mod 4) or \( D \equiv 0 \) (mod 4). There exists a unique fundamental discriminant \( D_{ld} \) and a unique positive integer \( m \) such that

\[
D = m^2 D_{ld}.
\]

**Proof.** We first prove the existence of \( m \) and \( D_{ld} \). We may write \( D = 2^e a^2 b \), where \( e \) is a positive non-negative integer, \( a \) is a positive integer, and \( b \) is an odd square-free integer.

Assume that \( e = 0 \). Then \( D \equiv 1 \) (mod 4). Since \( a \) is odd, \( a^2 \equiv 1 \) (mod 4); therefore, \( b \equiv 1 \) (mod 4). It follows that \( D = m^2 D_{ld} \) with \( m = a \) and \( D_{ld} = b \) a fundamental discriminant.

The case \( e = 1 \) is impossible because \( D \equiv 1 \) (mod 4) or \( D \equiv 0 \) (mod 4).

Assume that \( e \geq 2 \) and \( e \) is odd. Write \( e = 2k + 1 \) for a positive integer \( k \). Then \( D = m^2 D_{ld} \) with \( m = 2^{k-1} a \) and \( D_{ld} = 8b \) a fundamental discriminant.

Assume that \( e \geq 2 \) and \( e \) is even. Write \( e = 2k \) for a positive integer \( k \). If \( b \equiv 1 \) (mod 4), then \( D = m^2 D_{ld} \) with \( m = 2^k a \) and \( D_{ld} = b \) a fundamental discriminant. If \( b \equiv 3 \) (mod 4), then \( D = m^2 D_{ld} \) with \( m = 2^{k-1} a \) and \( D_{ld} = 4b \) a fundamental discriminant. This completes the proof the existence of \( m \) and \( D_{ld} \).

To prove the uniqueness assertion, assume that \( m \) and \( m' \) are positive integers and \( D_{ld} \) and \( D'_{ld} \) are fundamental discriminants such that \( D = m^2 D_{ld} = (m')^2 D'_{ld} \). Assume first that \( D_{ld} = 1 \). Then \( m^2 = (m')^2 D'_{ld} \). This implies
that $D'_{td}$ is a square; hence, $D'_{td} = 1$. Therefore, $m^2 = (m')^2$, implying that $m = m'$. Now assume that $D_{td} \neq 1$. Then also $D'_{td} \neq 1$, and $D$ is not a square. Set $K = \mathbb{Q}(\sqrt{D})$. We have $K = \mathbb{Q}(\sqrt{D_{td}}) = \mathbb{Q}(\sqrt{D'_{td}})$. By Lemma 1.3.2, $\text{disc}(K) = D_{td}$ and $\text{disc}(K) = D'_{td}$, so that $D_{td} = D'_{td}$. Since this holds we also conclude that $m = m'$.

**Proposition 1.4.2.** Let $\Delta$ be a non-zero integer with $\Delta \equiv 0, 1$ or 2 (mod 4). Define

$$D = \begin{cases} 
\Delta & \text{if } \Delta \equiv 0 \text{ or } 1 \text{ (mod 4)}, \\
4\Delta & \text{if } \Delta \equiv 2 \text{ (mod 4)}. 
\end{cases}$$

Write $D = m^2D_{td}$ with $m$ a positive integer, and $D_{td}$ a fundamental discriminant, as in Lemma 1.4.1. The Kronecker symbol $(\Delta \cdot)$ is a Dirichlet character modulo $|D|$, and is the Dirichlet character induced by the mod $|D_{td}|$ Dirichlet character $\chi_{D_{td}}$.

**Proof.** Let $\alpha$ be the Dirichlet character modulo $|D|$ induced by $\chi_{D_{td}}$. Thus, $\alpha$ is the composition

$$(\mathbb{Z}/|D|\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/|D_{td}|\mathbb{Z})^\times \xrightarrow{\chi_{D_{td}}} \mathbb{C}^\times,$$

extended to $\mathbb{Z}$. Since $\alpha$ and $(\Delta \cdot)$ are multiplicative, to prove that $\alpha = (\Delta \cdot)$ it will suffice to prove that these two functions agree on all primes, on $-1$, and on 0. Let $p$ be a prime.

Assume first that $p$ is odd. If $p|D$, then also $p|\Delta$, so that $\alpha(p)$ and $(\Delta \cdot)$ evaluated at $p$ are both 0. Assume that $(p, D) = 1$. Then also $(p, \Delta) = 1$. Then

$$(\Delta \cdot) \text{ evaluated at } p = \left(\frac{\Delta}{p}\right) \text{ (Legendre symbol)}$$

$$= \begin{cases} 
\left(\frac{\Delta}{p}\right) & \text{if } \Delta \equiv 0 \text{ or } 1 \text{ (mod 4)}, \\
\left(\frac{2}{p}\right)^2 \left(\frac{\Delta}{p}\right) & \text{if } \Delta \equiv 2 \text{ (mod 4)}, 
\end{cases}$$

$$= \begin{cases} 
\left(\frac{\Delta}{p}\right) & \text{if } \Delta \equiv 0 \text{ or } 1 \text{ (mod 4)}, \\
\left(\frac{4\Delta}{p}\right) & \text{if } \Delta \equiv 2 \text{ (mod 4)}, 
\end{cases}$$

$$= \left(\frac{D}{p}\right)$$

$$= \left(\frac{m^2D_{td}}{p}\right)$$

$$= \frac{D_{td}}{p}$$

$$= \chi_{D_{td}}(p)$$

$$= \alpha(p).$$
1.5. QUADRATIC FORMS

Assume next that \( p = 2 \). If \( 2|D \), then also \( 2|\Delta \), so that \( \alpha(2) \) and \( (\frac{\Delta}{2}) \) evaluated at \( 2 \) are both 0. Assume that \( (2,D) = 1 \), so that \( D \) is odd. Then \( D = \Delta \), and in fact \( D \equiv 1 \pmod{4} \). This implies that \( \Delta \equiv 1 \) or \( 7 \pmod{8} \). Also, as \( D \equiv 1 \pmod{4} \), and \( D = m^2D_{\text{ld}} \), we must have \( D_{\text{ld}} \equiv D \pmod{8} \) (since \( a^2 \equiv 1 \pmod{8} \) for any odd integer \( a \)). Therefore,

\[
(\frac{\Delta}{2}) \text{ evaluated at } 2 = \begin{cases} 1 & \text{ if } D \equiv 1 \pmod{8}, \\ -1 & \text{ if } D \equiv 5 \pmod{8}, \end{cases}
\]

\[= \begin{cases} 1 & \text{ if } D_{\text{ld}} \equiv 1 \pmod{8}, \\ -1 & \text{ if } D_{\text{ld}} \equiv 5 \pmod{8}, \end{cases}
\]

\[= \chi_{D_{\text{ld}}}(2)
\]

\[= \alpha(2).\]

To finish the proof we note that

\[
(\frac{\Delta}{-1}) \text{ evaluated at } -1 = \text{sign}(\Delta)
\]

\[= \text{sign}(D)
\]

\[= \text{sign}(D_{\text{ld}})
\]

\[= \chi_{D_{\text{ld}}}(-1)
\]

\[= \alpha(-1).
\]

Since \( \Delta = 1 \) if and only if \( D_{\text{ld}} = 1 \), the evaluation of \( (\frac{\Delta}{a}) \) at 0 is \( \chi_{D_{\text{ld}}}(0) = \alpha(0) \).

**Lemma 1.4.3.** Assume that \( \Delta_1 \) and \( \Delta_2 \) are non-zero integers that satisfy the congruences \( \Delta_1 \equiv 0, 1 \) or 2 \pmod{4} and \( \Delta_2 \equiv 0, 1 \) or 2 \pmod{4}. Then we have \( \Delta_1\Delta_2 \equiv 0, 1 \) or 2 \pmod{4}, and

\[
(\frac{\Delta_1}{a})(\frac{\Delta_2}{a}) = (\frac{\Delta_1\Delta_2}{a}) \tag{1.3}
\]

for all integers \( a \).

**Proof.** It is easy to verify that \( \Delta_1\Delta_2 \equiv 0, 1 \) or 2 \pmod{4}, and that if \( \Delta_1 = 1 \) or \( \Delta_2 = 1 \), then (1.3) holds. Assume that \( \Delta_1 \neq 1 \) and \( \Delta_2 \neq 1 \). Since \( (\frac{\Delta_1}{a}) \), \( (\frac{\Delta_2}{a}) \), and \( (\frac{\Delta_1\Delta_2}{a}) \) are multiplicative, it suffices to verify (1.3) for all odd primes, for 2, \(-1\) and 0. These cases follows from the definitions. \( \square \)

1.5 Quadratic forms

Let \( f \) be a positive integer, which will be fixed for the remainder of this section. In this section we regard the elements of \( \mathbb{Z}^f \) as column vectors.

Let \( A = (a_{i,j}) \in \mathbb{M}(f,\mathbb{Z}) \) be a integral symmetric matrix, so that \( a_{i,j} = a_{j,i} \) for \( i, j \in \{1, \ldots, f\} \). We say that \( A \) is **even** if each diagonal entry \( a_{i,i} \) for \( i \in \{1, \ldots, f\} \) is an even integer.
Lemma 1.5.1. Let $A \in \mathbb{M}(f, \mathbb{Z})$, and assume that $A$ is symmetric. Then $A$ is even if and only if $^t yAy$ is an even integer for all $y \in \mathbb{Z}^f$.

Proof. Let $y \in \mathbb{Z}^f$, with $^t y = (y_1, \ldots, y_f)$. Then

$$^t yAy = \sum_{i,j=1}^{n} a_{i,j} y_i y_j$$

$$= \sum_{i=1}^{f} a_{i,i} y_i^2 + \sum_{1 \leq i < j \leq f} 2 a_{i,j} y_i y_j.$$  

It is clear that if $A$ is even, then $^t yAy$ is an even integer for all $y \in \mathbb{Z}^f$. Assume that $^t yAy$ is an even integer for all $y \in \mathbb{Z}^f$. Let $i \in \{1, \ldots, f\}$. Let $y_i \in \mathbb{Z}^f$ be defined by

$$^t y_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$  

where 1 occurs in the $i$-th position. Then $^t y_i A y_i = a_{i,i}$. This is even, as required.  

Suppose that $A$ is an even integral symmetric matrix. To $A$ we associate the polynomial

$$Q(x_1, \ldots, x_f) = \frac{1}{2} \sum_{i,j=1}^{f} a_{i,j} x_i x_j,$$

and we refer to $Q(x_1, \ldots, x_f)$ as the **quadratic form** determined by $A$. Evidently,

$$Q(x) = \frac{1}{2} ^t x A x$$

with

$$x = \begin{bmatrix} x_1 \\ \vdots \\ x_f \end{bmatrix}.$$  

Since $a_{i,i}$ is even for $i \in \{1, \ldots, f\}$, the quadratic form $Q(x)$ can also be written as

$$Q(x_1, \ldots, x_f) = \sum_{1 \leq i \leq j \leq f} b_{i,j} x_i x_j$$

where

$$b_{i,j} = \begin{cases} a_{i,j} & \text{for } 1 \leq i < j \leq f, \\ a_{i,i}/2 & \text{for } 1 \leq i \leq f \end{cases}$$

is an integer. We denote the **determinant** of $A$ by

$$D = D(A) = \det(A).$$
and the **discriminant** of $A$ by

$$
\Delta = \Delta(A) = (-1)^k \det(A), \quad f = \begin{cases} 2k & \text{if } f \text{ is even,} \\
2k + 1 & \text{if } f \text{ is odd.}
\end{cases}
$$

For example, suppose that $f = 2$. Then every even integral symmetric matrix has the form

$$
A = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}
$$

where $a$, $b$ and $c$ are integers, and the associated quadratic form is:

$$
Q(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2.
$$

For this example we have

$$
D = 4ac - b^2, \quad \Delta = b^2 - 4ac.
$$

**Lemma 1.5.2.** Let $A \in M(f, \mathbb{Z})$ be an even integral symmetric matrix, and let $D = D(A)$ and $\Delta = \Delta(A)$. If $f$ is odd, then $\Delta \equiv D \equiv 0 \pmod{2}$. If $f$ is even, then $\Delta \equiv 0, 1 \pmod{4}$.

**Proof.** Let $A = (a_{i,j})$ with $a_{i,j} \in \mathbb{Z}$ for $i, j \in \{1, \ldots, f\}$. By assumption, $a_{i,j} = a_{j,i}$ and $a_{i,i}$ is even for $i, j \in \{1, \ldots, f\}$.

Assume that $f$ is odd. For $\sigma \in S_f$ (the permutation group of $\{1, \ldots, f\}$, let

$$
t(\sigma) = \text{sign}(\sigma) a_{1, \sigma(1)} \cdots a_{f, \sigma(f)} = \text{sign}(\sigma) \prod_{i \in \{1, \ldots, n\}} a_{i, \sigma(i)}
$$

We have

$$
\det(A) = \sum_{\sigma \in S_f} t(\sigma)
= \sum_{\sigma \in X} t(\sigma) + \sum_{\sigma \in S_f - X} t(\sigma).
$$

Here, $X$ is the subset of $\sigma \in S_f$ such that $\sigma \neq \sigma^{-1}$. Let $\sigma \in S_f$. Then

$$
t(\sigma^{-1}) = \text{sign}(\sigma^{-1}) \prod_{i \in \{1, \ldots, f\}} a_{i, \sigma^{-1}(i)}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{\sigma(i), \sigma^{-1}(\sigma(i))}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{\sigma(i), i}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{i, \sigma(i)}
$$

and the **discriminant** of $A$ by

$$
\Delta = \Delta(A) = (-1)^k \det(A), \quad f = \begin{cases} 2k & \text{if } f \text{ is even,} \\
2k + 1 & \text{if } f \text{ is odd.}
\end{cases}
$$

For example, suppose that $f = 2$. Then every even integral symmetric matrix has the form

$$
A = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}
$$

where $a$, $b$ and $c$ are integers, and the associated quadratic form is:

$$
Q(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2.
$$

For this example we have

$$
D = 4ac - b^2, \quad \Delta = b^2 - 4ac.
$$

**Lemma 1.5.2.** Let $A \in M(f, \mathbb{Z})$ be an even integral symmetric matrix, and let $D = D(A)$ and $\Delta = \Delta(A)$. If $f$ is odd, then $\Delta \equiv D \equiv 0 \pmod{2}$. If $f$ is even, then $\Delta \equiv 0, 1 \pmod{4}$.

**Proof.** Let $A = (a_{i,j})$ with $a_{i,j} \in \mathbb{Z}$ for $i, j \in \{1, \ldots, f\}$. By assumption, $a_{i,j} = a_{j,i}$ and $a_{i,i}$ is even for $i, j \in \{1, \ldots, f\}$.

Assume that $f$ is odd. For $\sigma \in S_f$ (the permutation group of $\{1, \ldots, f\}$, let

$$
t(\sigma) = \text{sign}(\sigma) a_{1, \sigma(1)} \cdots a_{f, \sigma(f)} = \text{sign}(\sigma) \prod_{i \in \{1, \ldots, n\}} a_{i, \sigma(i)}
$$

We have

$$
\det(A) = \sum_{\sigma \in S_f} t(\sigma)
= \sum_{\sigma \in X} t(\sigma) + \sum_{\sigma \in S_f - X} t(\sigma).
$$

Here, $X$ is the subset of $\sigma \in S_f$ such that $\sigma \neq \sigma^{-1}$. Let $\sigma \in S_f$. Then

$$
t(\sigma^{-1}) = \text{sign}(\sigma^{-1}) \prod_{i \in \{1, \ldots, f\}} a_{i, \sigma^{-1}(i)}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{\sigma(i), \sigma^{-1}(\sigma(i))}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{\sigma(i), i}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{i, \sigma(i)}
$$

and the **discriminant** of $A$ by

$$
\Delta = \Delta(A) = (-1)^k \det(A), \quad f = \begin{cases} 2k & \text{if } f \text{ is even,} \\
2k + 1 & \text{if } f \text{ is odd.}
\end{cases}
$$

For example, suppose that $f = 2$. Then every even integral symmetric matrix has the form

$$
A = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}
$$

where $a$, $b$ and $c$ are integers, and the associated quadratic form is:

$$
Q(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2.
$$

For this example we have

$$
D = 4ac - b^2, \quad \Delta = b^2 - 4ac.
$$

**Lemma 1.5.2.** Let $A \in M(f, \mathbb{Z})$ be an even integral symmetric matrix, and let $D = D(A)$ and $\Delta = \Delta(A)$. If $f$ is odd, then $\Delta \equiv D \equiv 0 \pmod{2}$. If $f$ is even, then $\Delta \equiv 0, 1 \pmod{4}$.

**Proof.** Let $A = (a_{i,j})$ with $a_{i,j} \in \mathbb{Z}$ for $i, j \in \{1, \ldots, f\}$. By assumption, $a_{i,j} = a_{j,i}$ and $a_{i,i}$ is even for $i, j \in \{1, \ldots, f\}$.

Assume that $f$ is odd. For $\sigma \in S_f$ (the permutation group of $\{1, \ldots, f\}$, let

$$
t(\sigma) = \text{sign}(\sigma) a_{1, \sigma(1)} \cdots a_{f, \sigma(f)} = \text{sign}(\sigma) \prod_{i \in \{1, \ldots, n\}} a_{i, \sigma(i)}
$$

We have

$$
\det(A) = \sum_{\sigma \in S_f} t(\sigma)
= \sum_{\sigma \in X} t(\sigma) + \sum_{\sigma \in S_f - X} t(\sigma).
$$

Here, $X$ is the subset of $\sigma \in S_f$ such that $\sigma \neq \sigma^{-1}$. Let $\sigma \in S_f$. Then

$$
t(\sigma^{-1}) = \text{sign}(\sigma^{-1}) \prod_{i \in \{1, \ldots, f\}} a_{i, \sigma^{-1}(i)}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{\sigma(i), \sigma^{-1}(\sigma(i))}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{\sigma(i), i}
= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{i, \sigma(i)}
$$
= t(\sigma).

Since the subset \(X\) is partitioned into two element subsets of the form \(\{\sigma, \sigma^{-1}\}\) for \(\sigma \in X\), and since \(t(\sigma) = t(\sigma^{-1})\) for \(\sigma \in S_f\), it follows that

\[
\sum_{\sigma \in X} t(\sigma) \equiv 0 \pmod{2}.
\]

Let \(\sigma \in S_f - X\), so that \(\sigma^2 = 1\). Write \(\sigma = \sigma_1 \cdots \sigma_t\), where \(\sigma_1, \ldots, \sigma_t \in S_f\) are cycles and mutually disjoint. Since \(\sigma^2 = 1\), each \(\sigma_i\) for \(i \in \{1, \ldots, f\}\) is a two cycle. Since \(f\) is odd, there exists \(i \in \{1, \ldots, f\}\) such that \(i\) does not occur in any of the two cycles \(\sigma_1, \ldots, \sigma_t\). It follows that \(t(\sigma) = i\). Now \(a_{i, \sigma(i)} = a_{i, i}\); by hypothesis, this is an even integer. It follows that \(t(\sigma)\) is also an even integer.

Hence,

\[
\sum_{\sigma \in S_f - X} t(\sigma) \equiv 0 \pmod{2},
\]

and we conclude that \(\Delta \equiv D \equiv 0 \pmod{2}\).

Now assume that \(f\) is even, and write \(f = 2k\). We will prove that \(\Delta \equiv 0, 1 \pmod{4}\) by induction on \(f\). Assume that \(f = 2\), so that

\[
A = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}
\]

where \(a, b\) and \(c\) are integers. Then \(\Delta = b^2 - 4ac \equiv 0, 1 \pmod{4}\). Assume now that \(f \geq 4\), and that \(\Delta(A_1) \equiv 0, 1 \pmod{4}\) for all \(f_1 \times f_1\) even integral symmetric matrices \(A_1\) with \(f_1\) even and \(f > f_1 \geq 2\). Clearly, if all the off-diagonal entries of \(A\) are even, then all the entries of \(A\) are even, and \(\Delta(A) \equiv 0 \pmod{4}\). Assume that some off-diagonal entry of \(A\), say \(a = a_{i,j}\) is odd with \(1 \leq i < j \leq f\). Interchange the first and the \(i\)-th row of \(A\), and then the first and the \(i\)-th column of \(A\); the result is an even integral symmetric matrix \(A'\) with \(a\) in the \((1,j)\) position and \(\Delta(A') = \Delta(A)\). Next, interchange the second and the \(j\)-th column of \(A'\), and then the second and the \(j\)-th row of \(A'\); the result is an even integral symmetric matrix \(A''\) with \(a\) in the \((1,2)\)-position and \(\det(A'') = \det(A') = \det(A)\). It follows that we may assume that \((i,j) = (1,2)\).

We may write

\[
A = \begin{bmatrix} A_1 & B \\ B^t & A_2 \end{bmatrix},
\]

where \(A_2\) is an \((f - 2) \times (f - 2)\) even integral symmetric matrix,

\[
A_1 = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{bmatrix},
\]

and \(B\) is a \(2 \times (f - 2)\) matrix with integral entries. Let

\[
\text{adj}(A_1) = \begin{bmatrix} a_{2,2} & -a_{1,2} \\ -a_{1,2} & a_{1,1} \end{bmatrix},
\]
so that
\[ A_1 \cdot \text{adj}(A_1) = \text{adj}(A_1) \cdot A_1 = \det(A_1) \cdot 1_2. \]

Now
\[
\begin{bmatrix}
1_2 \\
-^tB \cdot \text{adj}(A_1) & \det(A_1) \cdot 1_{f-2}
\end{bmatrix}
\begin{bmatrix}
A_1 & B \\
^tB & A_2
\end{bmatrix} = 
\begin{bmatrix}
A_1 \\
-^tB \cdot \text{adj}(A_1) \cdot B + \det(A_1) A_2
\end{bmatrix}, \tag{1.4}
\]

Consider the \((f-2) \times (f-2)\) matrix \(-^tB \cdot \text{adj}(A_1) \cdot B\). This matrix clearly has integral entries. If \(y \in \mathbb{Z}_{f-2}\), then \(By \in \mathbb{Z}_{f-2}\) and
\[
^t(y)(-^tB \cdot \text{adj}(A_1) \cdot B)y = -^t(By) \cdot \text{adj}(A_1) \cdot (By);
\]
since \(\text{adj}(A_1)\) is even, by Lemma 1.5.1 this integer is even. Since the last displayed integer is even for all \(y \in \mathbb{Z}_{f-2}\), we can apply Lemma 1.5.1 again to conclude that \(-^tB \cdot \text{adj}(A_1) \cdot B\) is even. It follows that
\[
A_3 = -^tB \cdot \text{adj}(A_1) \cdot B + \det(A_1) A_2
\]
is an \((f-2) \times (f-2)\) even integral symmetric matrix. Taking determinants of both sides of (1.4), we obtain
\[
\det(A_1)^{f-2} \cdot \det(A) = \det(A_1) \cdot \det(A_3)
\]
\[
\det(A_1)^{f-2} \cdot (-1)^k \det(A) = (-1) \det(A_1) \cdot (-1)^{k-1} \det(A_3)
\]
\[
\det(A_1)^{f-2} \cdot \Delta(A) = \Delta(A_1) \cdot \Delta(A_3).
\]

By the induction hypothesis, \(\Delta(A_1) \equiv 0, 1 \text{ (mod 4)}\), and \(\Delta(A_3) \equiv 0, 1 \text{ (mod 4)}\). Hence,
\[
\det(A_1)^{f-2} \cdot \Delta(A) \equiv 0, 1 \text{ (mod 4)}.
\]

By hypothesis, \(a_{1,2}\) is odd; since \(f-2\) is even, this implies that \(\det(A_1)^{f-2} \equiv 1 \text{ (mod 4)}\). We now conclude that \(\Delta(A) \equiv 0, 1 \text{ (mod 4)}\), as desired. \(\square\)

Let \(A \in M(f, \mathbb{R})\). The \textbf{adjoint} of \(A\) is the \(f \times f\) matrix \(\text{adj}(A)\) with entries
\[
\text{adj}(A)_{i,j} = (-1)^{i+j} \det \left( A(j|i) \right)
\]
for \(i, j \in \{1, \ldots, n\}\). Here, for \(i, j \in \{1, \ldots, n\}\), \(A(j|i)\) is the \((f-1) \times (f-1)\) matrix that is obtained from \(A\) by deleting the \(j\)-th row and the \(i\)-th column. For example, if
\[
A = \begin{bmatrix}
a & b \\
c & d
\end{bmatrix},
\]
then
\[
\text{adj}(A) = \begin{bmatrix}
d & -b \\
-c & a
\end{bmatrix}.
\]
We have
\[ \text{adj}(A) \cdot A = A \cdot \text{adj}(A) = \det(A) \cdot 1_f. \]
Thus,
\[ A = \det(A)\text{adj}(A)^{-1}, \]
\[ \text{adj}(A) = \det(A) \cdot A^{-1}, \]
\[ A^{-1} = \det(A)^{-1} \cdot \text{adj}(A), \]
\[ \text{adj}(A)^{-1} = \det(A)^{-1} \cdot A, \]
\[ \det(\text{adj}(A)) = \det(A)^{f-1}. \]

We let Sym($f, \mathbb{R}$) be the set of all symmetric elements of $M(f, \mathbb{R})$. Let $A \in$ Sym($f, \mathbb{R}$). We say that $A$ is **positive-definite** if the following two conditions hold:
1. If $x \in \mathbb{R}^f$, then $Q(x) = \frac{1}{2}^t x Ax \geq 0$;
2. if $x \in \mathbb{R}^f$ and $Q(x) = \frac{1}{2}^t x Ax = 0$, then $x = 0$.

We will also write $A > 0$ to mean that $A$ is positive-definite. We say that $A$ is **positive semi-definite** if the first condition holds; we will write $A \geq 0$ to indicate that $A$ is positive semi-definite. Since $A$ is symmetric with real entries, there exists a matrix $T \in GL(f, \mathbb{R})$ such that $^t TT = T^T = 1$ (so that $T^{-1} = ^t T$) and
\[
^t T A T = T^{-1} A T = \begin{bmatrix}
\lambda_1 \\
\lambda_2 \\
\lambda_3 \\
\vdots \\
\lambda_f
\end{bmatrix}
\]
for some $\lambda_1, \ldots, \lambda_f \in \mathbb{R}$ (see the corollary on p. 314 of [10]). The symmetric matrix $A$ is positive-definite if and only if $\lambda_1, \ldots, \lambda_f$ are all positive, and $A$ is positive semi-definite if and only if $\lambda_1, \ldots, \lambda_f$ are all non-negative. It follows that if $A$ is positive-definite, then $\det(A) > 0$, and if $A$ is positive semi-definite, then $\det(A) \geq 0$. Assume that $A$ is positive semi-definite, and that $T$ and $\lambda_1, \ldots, \lambda_f$ are as in (1.5); in particular, $\lambda_1, \ldots, \lambda_f$ are all non-negative real numbers. Let
\[
B = T^{\frac{1}{2}} \begin{bmatrix}
\sqrt{\lambda_1} \\
\sqrt{\lambda_2} \\
\sqrt{\lambda_3} \\
\vdots \\
\sqrt{\lambda_f}
\end{bmatrix} T^{-1}.
\]
(1.6)

The matrix $B$ is evidently symmetric and positive semi-definite, and we have
\[ A = ^t BB = BB = B^2. \]
(1.7)

Also, it is clear that if $A$ is positive-definite, then so is $B$. 

\[ \text{adj}(A) \cdot A = A \cdot \text{adj}(A) = \det(A) \cdot 1_f. \]
Lemma 1.5.3. Assume $f$ is even. Let $A \in M(f, \mathbb{Z})$ be a positive-definite even integral symmetric matrix. The matrix $\text{adj}(A)$ is a positive-definite even integral symmetric matrix.

Proof. We have $\text{adj}(A) = \det(A) \cdot A^{-1}$. Therefore, $\text{adj}(A) = \det(A) \cdot \text{adj}(A^{-1}) = \det(A) \cdot \text{adj}(A) = \text{adj}(A)$, so that $\text{adj}(A)$ is symmetric. To see that $\text{adj}(A)$ is positive-definite, let $T \in \text{GL}(f, \mathbb{R})$ and $\lambda_1, \ldots, \lambda_f$ be positive real numbers such that (1.5) holds. Then

\[
\text{adj}(A)^T T = \det(A) \cdot T \cdot A^{-1} \cdot T
\]

This equality implies that $\text{adj}(A)$ is positive-definite. It is clear that $\text{adj}(A)$ has integral entries. To see that $\text{adj}(A)$ is even, let $i \in \{1, \ldots, f\}$. Then $\text{adj}(A)_{i,i} = \det(A_{i,i})$. The matrix $A_{i,i}$ is an $(f-1) \times (f-1)$ even integral symmetric matrix. Since $f-1$ is odd, by Lemma 1.5.2 we have $\det(A_{i,i}) \equiv 0 \pmod{2}$. Thus, $\text{adj}(A)_{i,i}$ is even.

Let $A \in M(f, \mathbb{Z})$ be an even integral symmetric matrix with $\det(A)$ non-zero. The set of all integers $N$ such that $NA^{-1}$ is an even integral symmetric matrix is an ideal of $\mathbb{Z}$. We define the level of $A$, and its associated quadratic form, to be the unique positive generator $N(A)$ of this ideal. Evidently, the level $N(A)$ of $A$ is smallest positive integer $N$ such that $NA^{-1}$ is an even integral symmetric matrix.

Proposition 1.5.4. Assume $f$ is even. Let $A \in M(f, \mathbb{Z})$ be a positive-definite even integral symmetric matrix. Define

\[
G = \gcd\left(\frac{\text{adj}(A)_{1,1}}{2}, \frac{\text{adj}(A)_{1,2}}{2}, \frac{\text{adj}(A)_{1,3}}{2}, \ldots, \frac{\text{adj}(A)_{1,f}}{2}, \ldots, \frac{\text{adj}(A)_{f,1}}{2}, \frac{\text{adj}(A)_{f,2}}{2}, \frac{\text{adj}(A)_{f,3}}{2}, \ldots, \frac{\text{adj}(A)_{f,f}}{2}\right)
\]

Then $G$ divides $\det(A)$, and the level of $A$ is

\[
N = \frac{\det(A)}{G}
\]

The positive integers $N$ and $\det(A)$ have the same set of prime divisors.
Proof. The integer $G$ divides every entry of $\text{adj}(A)$. Therefore, $G^f$ divides $\det(\text{adj}(A))$. Since $\det(\text{adj}(A)) = \det(A)^{f-1}$, $G^f$ divides $\det(A)^{f-1}$. This implies that $G$ divides $\det(A)$. Now by definition, $G$ is the largest integer $g$ such that
\[
\frac{1}{g}\text{adj}(A) \text{ is even.}
\]
Since $\text{adj}(A) = \det(A)A^{-1}$, we therefore have that
\[
\frac{\det(A)}{G} A^{-1} \text{ is even.}
\]
This implies that $\det(A)G^{-1}$ is in the ideal generated by the level $N$ of $A$, i.e., $N$ divides $\det(A)G^{-1}$; consequently,
\[
GN \leq \det(A).
\]
On the other hand, $NA^{-1}$ is even. Using $A^{-1} = \det(A)^{-1}\text{adj}(A)$, this is equivalent to
\[
\frac{1}{\det(A)N^{-1}\text{adj}(A)} \text{ is even.}
\]
Since $\det(A)N^{-1}$ is a positive integer (we have already proven that $N$ divides $\det(A)$), the definition of $G$ implies that $G \geq \det(A)N^{-1}$, or equivalently,
\[
GN \geq \det(A).
\]
We now conclude that $GN = \det(A)$, as desired.

To see that $N$ and $\det(A)$ have the same set of prime divisors, we first note that (since $N$ divides $\det(A)$) every prime divisor of $N$ is a prime divisor of $\det(A)$. Let $p$ be a prime divisor of $\det(A)$. If $p$ does not divide $G$, then $p$ divides $N$ (because $NG = \det(A)$). Assume that $p$ divides $G$. Write $\det(A) = pd$ and $G = p^kg$ with $k$ and $j$ positive integers and $d$ and $g$ integers such that $(d,p) = (g,p) = 1$. From above, $G^f$ divides $\det(A)^{f-1}$. This implies that
\[
(f-1)j \geq fk. \quad \therefore \quad j \geq \frac{f}{f-1}k > k.
\]
This means that $p$ divides $N = \det(A)/G$. \hfill $\square$

**Corollary 1.5.5.** Let $f$ be an even positive integer, let $A \in M(f, \mathbb{Z})$ be a positive-definite even integral symmetric matrix and let $N$ be the level of $A$. Then $N = 1$ if and only if $\det(A) = 1$.

**Proof.** By Proposition 1.5.4, $N$ and $\det(A)$ have the same set of prime divisors. It follows that $N = 1$ if and only if $\det(A) = 1$. \hfill $\square$

**Corollary 1.5.6.** Let $A$ be a $2 \times 2$ even integral symmetric matrix, so that
\[
A = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}
\]
where $a$, $b$ and $c$ are integers. Then $A$ is positive-definite if and only if $\det(A) = 4ac - b^2 > 0$, $a > 0$, and $c > 0$. Assume that $A$ is positive-definite. The level of $A$ is

$$N = \frac{4ac - b^2}{\gcd(a, b, c)}.$$  

Proof. Assume that $A$ is positive-definite. We have already pointed out that $\det(A) > 0$. Now

$$Q(1, 0) = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = a,$$

$$Q(0, 1) = \frac{1}{2} \begin{bmatrix} 0 & 2a \\ 1 & b \end{bmatrix} \begin{bmatrix} b & 2c \\ 1 & 0 \end{bmatrix} = c.$$  

Since $A$ is positive-definite, these numbers are positive. Assume that $\det(A) = 4ac - b^2 > 0$, $a > 0$, and $c > 0$. For $x, y \in \mathbb{R}$ we have

$$Q(x, y) = ax^2 + bxy + cy^2$$

$$= \frac{1}{a} (ax + \frac{b}{2}y)^2 + \frac{4ac - b^2}{4a} y^2$$

$$= \frac{1}{a} (ax + \frac{b}{2}y)^2 + \frac{\det(A)}{4a} y^2.$$  

Clearly, we have $Q(x, y) \geq 0$ for all $x, y \in \mathbb{R}$. Assume that $x, y \in \mathbb{R}$ are such that $Q(x, y) = 0$. Then since $\det(A) > 0$ and $a > 0$ we must have $ax + \frac{b}{2}y = 0$ and $y = 0$; hence also $x = 0$. It follows that $A$ is positive-definite. The final assertion follows from

$$\text{adj}(A) = \begin{bmatrix} 2c & -b \\ -b & 2a \end{bmatrix}$$

and Proposition 1.5.4.  

\[ \square \]

**Corollary 1.5.7.** Let $f$ be an even positive integer, let $A \in M(f, \mathbb{Z})$ be a positive-definite even integral symmetric matrix and let $N$ be the level of $A$. Let $c$ be a positive integer. Then the level of the positive-definite even integral symmetric matrix $cA$ is $cN$.

Proof. This follows from the formula for level from Proposition 1.5.4.  

\[ \square \]

**Lemma 1.5.8.** Let $f$ be an even positive integer, let $A \in M(f, \mathbb{Z})$ be a positive-definite even integral symmetric matrix and let $N$ be the level of $A$. Define the integral quadratic form $Q(x)$ by $Q(x) = \frac{1}{2} x^t A x$. Let $h \in \mathbb{Z}^f$ be such that $Ah \equiv 0 \pmod{N}$. Then $Q(h) \equiv 0 \pmod{N}$. Also, if $n \in \mathbb{Z}^f$ is such that $n \equiv h \pmod{N}$, then $Q(n) \equiv Q(h) \pmod{N^2}$ and $Q(n) \equiv 0 \pmod{N}$.

Proof. Since $Ah \equiv 0 \pmod{N}$, there exists $m \in \mathbb{Z}^f$ such that $Ah = Nm$. We have

$$Q(q) = \frac{1}{2} q^t h Ah$$


\[ 2Q(n) = (h + Nb)A(h + Nb) \]
\[ = (h + N^2 b)A(h + Nb) \]
\[ = hAh + 2N^2 bAh + N^2 bAb \]
\[ \equiv hAh \pmod{2N^2} \]
\[ \equiv 2Q(h) \pmod{2N^2} \].

Here \( bAh \equiv 0 \pmod{N} \) because \( Ah \equiv 0 \pmod{N} \) and \( bAb \equiv 0 \pmod{2} \) because \( A \) is even. It follows that \( Q(n) \equiv Q(h) \pmod{N^2} \). Finally, since \( Q(h) \equiv 0 \pmod{N} \) and \( Q(n) \equiv Q(h) \pmod{N^2} \), we have \( Q(n) \equiv 0 \pmod{N} \). \( \square \)

1.6 The upper half-plane

Let \( \text{GL}(2, \mathbb{R})^+ \) be the subgroup of \( \sigma \in \text{GL}(2, \mathbb{R}) \) such that \( \det(\sigma) > 0 \). We define and action of \( \text{GL}(2, \mathbb{R})^+ \) on the upper half-plane \( \mathbb{H}_1 \) by

\[ \sigma \cdot z = \frac{az + b}{cz + d} \]

for \( z \in \mathbb{H}_1 \) and \( \sigma \in \text{GL}(2, \mathbb{R})^+ \) such that

\[ \sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \quad (1.8) \]

We define the cocycle function

\[ j: \text{GL}(2, \mathbb{R})^+ \times \mathbb{H}_1 \rightarrow \mathbb{C} \]

by

\[ j(\sigma, z) = cz + d \]

for \( z \in \mathbb{H}_1 \) and \( \sigma \in \text{GL}(2, \mathbb{R})^+ \) as in (1.8). We have

\[ j(\alpha \beta, z) = j(\alpha, \beta \cdot z)j(\beta, z) \]

for \( \alpha, \beta \in \text{GL}(2, \mathbb{R})^+ \) and \( z \in \mathbb{H}_1 \). Let \( F: \mathbb{H}_1 \rightarrow \mathbb{C} \) be a function, and let \( \ell \) be an integer. Let \( \sigma \in \text{GL}(2, \mathbb{R})^+ \). We define

\[ F|_\ell : \mathbb{H}_1 \rightarrow \mathbb{C} \]
by the formula
\[
(F|_\ell \sigma)(z) = \det(\sigma)^{\ell/2}(cz + d)^{-\ell} \cdot F\left(\frac{az + b}{cz + d}\right) \\
= \det(\sigma)^{\ell/2} j(\sigma, z)^{-\ell} F(\sigma \cdot z)
\]
for \(z \in \mathbb{H}_1\). We have
\[
(F|_\ell \alpha)|_\ell \beta = F|_\ell (\alpha \beta)
\]
for \(\alpha, \beta \in \text{GL}(2, \mathbb{R})^+\).

### 1.7 Congruence subgroups

Let \(N\) be a positive integer. The **principal congruence subgroup** of level \(N\) is defined to be
\[
\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, b \equiv c \equiv 0 \pmod{N} \right\}.
\]
The **Hecke congruence subgroup** of level \(N\) is defined to be
\[
\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.
\]
If \(\Gamma\) is a subgroup of \(\text{SL}(2, \mathbb{Z})\), then we say that \(\Gamma\) is a **congruence subgroup** of \(\text{SL}(2, \mathbb{Z})\) if there exists a positive integer \(N\) such that \(\Gamma(N) \subseteq \Gamma\).

### 1.8 Modular forms

Let \(N\) be a positive integer, and let \(R > 0\) be positive number. Let
\[
H(N, R) = \{ z \in \mathbb{H}_1 : \text{Im}(z) > \frac{N \log(1/R)}{2\pi} \}
\]
and
\[
D(R) = \{ q \in \mathbb{C} : |q| < R \}.
\]
The function
\[
H(N, R) \rightarrow D(R)
\]
defined by
\[
z \mapsto q(z) = e^{2\pi iz/N}
\]
is well-defined. We have \(q(z + N) = q(z)\) for \(z \in H(N, R)\).

**Lemma 1.8.1.** Let \(f : \mathbb{H}_1 \rightarrow \mathbb{C}\) be an analytic function, and let \(N\) be a positive integer such that \(f(z + N) = f(z)\) for \(z \in \mathbb{H}_1\). Assume that there exists a real number such that \(0 < R < 1\) and a complex power series
\[
\sum_{n=0}^{\infty} a(n)q^n
\]
that converges for $q \in D(R)$ such that

$$f(z) = \sum_{n=0}^{\infty} a(n) e^{2 \pi i n z / N}$$

for $z \in H(N, R)$. If $M$ is another positive integer such that $f(z + M) = f(z)$ for $z \in \mathbb{H}_1$, then there exists a real number such that $0 < T < 1$ and a complex power series

$$\sum_{k=0}^{\infty} b(k) q^k$$

that converges for $q \in D(T)$ such that

$$(F \mid e^\sigma)(z) = \sum_{k=0}^{\infty} b(k) e^{2 \pi i k z / M}$$

for $z \in H(M, T)$.

**Proof.** For $z \in H(N, R)$,

$$f(z) = f(z + M)$$

$$= \sum_{n=0}^{\infty} a(n) e^{2 \pi i (n + M) z / N}$$

$$= \sum_{n=0}^{\infty} a(n) e^{2 \pi i n z / N} e^{2 \pi i M z / N}$$

$$= \sum_{n=0}^{\infty} a(n) e^{2 \pi i n z / N} = \sum_{n=0}^{\infty} a(n) e^{2 \pi i n M / N} e^{2 \pi i z / N}.$$ 

It follows that

$$a(n) = a(n) e^{2 \pi i n M / N}$$

for all non-negative integers $n$. Hence, for every non-negative integer $n$, if $a(n) \neq 0$, then $nM/N$ is an integer, or equivalently, if $nM/N$ is not an integer, then $a(n) = 0$. Let $z \in H(N, R)$. Then

$$f(z) = \sum_{n=0}^{\infty} a(n) e^{2 \pi i n z / N}$$

$$= \sum_{n=0}^{\infty} a(n) e^{2 \pi i (nM/N) z / M}$$

$$= \sum_{k=0}^{\infty} b(k) (e^{2 \pi i z / M})^k$$

where

$$b(k) = \begin{cases} a(kN/M) & \text{if } kN/M \text{ is an integer}, \\ 0 & \text{if } kN/M \text{ is not an integer}. \end{cases}$$

Because the series $\sum_{n=0}^{\infty} a(n) e^{2 \pi i n z / N}$ converges for $z \in H(N, R)$, the above equalities imply that the power series $\sum_{k=0}^{\infty} b(k) q^k$ converges for $q \in D(R^{N/M})$. Since $H(M, R^{N/M}) = H(N, R)$, the proof is complete.
1.9. THE SYMPLECTIC GROUP

**Definition 1.8.2.** Let \( k \) be a non-negative integer, and let \( \Gamma \) be a congruence subgroup of \( \text{SL}(2, \mathbb{Z}) \). Let \( F : \mathbb{H}_1 \to \mathbb{C} \) be a function on the upper-half plane \( \mathbb{H}_1 \). We say that \( F \) is a **modular form** of weight \( k \) with respect to \( \Gamma \) if the following conditions hold:

1. For all \( \alpha \in \Gamma \) we have \( f|_{\Gamma} \alpha = f \).

2. The function \( F \) is analytic on \( \mathbb{H}_1 \).

3. If \( \sigma \in \text{SL}(2, \mathbb{Z}) \), then there exists a positive integer \( N \) such that \( \Gamma(N) \subset \Gamma \), a real number \( R \) such that \( 0 < R < 1 \), and a complex power series

\[
\sum_{n=0}^{\infty} a(n)q^n
\]

that converges for \( q \in D(R) \), such that

\[
(F|_{\Gamma} \sigma)(z) = \sum_{n=0}^{\infty} a(n)q^n = \sum_{n=0}^{\infty} a(n)e^{2\pi inz/N}
\]

for \( z \in H(N, R) \).

The third condition of Definition 1.8.2 is often summarized by saying that \( F \) is **holomorphic at the cusps** of \( \Gamma \). We say that \( F \) is a **cusp form** if the three conditions in the definition of a modular form hold, and in addition it is always the case that \( a(0) = 0 \); this additional condition is summarized by saying that \( F \) **vanishes at the cusps** of \( \Gamma \). The set of modular forms of weight \( k \) with respect to \( \Gamma \) is a vector space over \( \mathbb{C} \), which we denote by \( M_k(\Gamma) \). The set of cusp forms of weight \( k \) with respect to \( \Gamma \) is a subspace of \( M_k(\Gamma) \), and will be denoted by \( S_k(\Gamma) \).

1.9 The symplectic group

Let \( R \) be a commutative ring with identity 1, and let \( n \) be a positive integer. As usual, we define

\[
\text{GL}(2n, R) = \{ g \in M(2n, R) : \det(g) \in R^\times \}.
\]

Then \( \text{GL}(2n, R) \) is a group under multiplication of matrices; the identity of \( \text{GL}(2n, R) \) is the \( 2n \times 2n \) identity matrix \( 1 = 1_{2n} \). Let

\[
J = \begin{bmatrix}
1_n \\
-1_n
\end{bmatrix}.
\]

We note that

\[
J^2 = -1, \quad J^{-1} = -J.
\]

We define

\[
\text{Sp}(2n, R) = \{ g \in \text{GL}(2n, R) : {}^t Jg = J \}.
\]

We refer to \( \text{Sp}(2n, R) \) as the **symplectic group of degree \( n \) over \( R \)**.
Lemma 1.9.1. If $R$ is a commutative ring with identity and $n$ is a positive integer, then $\text{Sp}(2n, R)$ is a subgroup of $\text{GL}(2n, R)$. If $g \in \text{Sp}(2n, R)$, then $^t g \in \text{Sp}(2n, R)$.

Proof. Evidently, $1 \in \text{Sp}(2n, R)$. Also, it is easy to see that if $g, h \in \text{Sp}(2n, R)$, then $gh \in \text{Sp}(2n, R)$. To complete the proof that $\text{Sp}(2n, R)$ is a subgroup of $\text{GL}(2n, R)$ it will suffice to prove that if $g \in \text{Sp}(2n, R)$, then $g^{-1} \in \text{Sp}(2n, R)$. Let $g \in \text{Sp}(n, R)$. Then $^t g J g = J$. This implies that $g^{-1} = J^{-1}^t g J = -J^t g J$. Now

$$
^t (g^{-1}) J g^{-1} = J g J J J g J \\
= J g J J J g J \\
= -J g J J g J \\
= -J g J J J g^{-1} \\
= -J g J J g^{-1} \\
= J.
$$

Next, suppose that $g \in \text{Sp}(2n, R)$. Then

$$
g J ^t g = g J ^t g J g^{-1} J^{-1} \\
= g J g^{-1} J^{-1} \\
= -J^{-1} \\
= J.
$$

This implies that $g \in \text{Sp}(2n, R)$. □

Lemma 1.9.2. Let $R$ be a commutative ring with identity and let $n$ be a positive integer. Let

$$
g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \text{GL}(2n, R).
$$

Then $g \in \text{Sp}(2n, R)$ if and only if

$$
^t AC = ^t CA, \quad ^t BD = ^t DB, \quad ^t AD - ^t CB = 1.
$$

Proof. This follows by direct computations. □

Lemma 1.9.3. Let $R$ be a commutative ring with identity. Then $\text{Sp}(2, R) = \text{SL}(2, R)$.

Proof. Let $g \in \text{GL}(2, R)$, and write

$$
g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}
$$

for some $a, b, c, d \in R$. A calculations shows that

$$
^t g J g = \begin{bmatrix} ad - bc \\ -(ad - bc) \end{bmatrix} = \det(g) \cdot J.
$$

It follows that $g \in \text{Sp}(2, R)$ if and only if $\det(g) = 1$, i.e., $g \in \text{SL}(2, R)$. □
Lemma 1.9.4. Let $R$ be a commutative ring with identity, and let $n$ be a positive integer. The following matrices are contained in $\text{Sp}(2n, R)$:

$$
J = \begin{bmatrix}
1 & 1 \\
-1 & -1
\end{bmatrix},
\begin{bmatrix}
1 & -1 \\
1 & 1
\end{bmatrix},
\begin{bmatrix}
1 & X \\
1 & 1
\end{bmatrix},
\begin{bmatrix}
1 & Y \\
1 & 1
\end{bmatrix}, \quad X \in M(n, R), \; ^tX = X,
\begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix}, \quad Y \in M(n, R), \; ^tY = Y.
$$

Proof. These assertions follow by direct computations.

Lemma 1.9.5. Let $R$ be a commutative ring with identity, and let $n$ be a positive integer. The sets

$$
P = \{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \text{Sp}(2n, R) : C = 0 \},
$$

$$
M = \{ \begin{bmatrix} A & 0 \\ 0 & A^{-1} \end{bmatrix} : A \in \text{GL}(n, R) \},
$$

$$
U = \{ \begin{bmatrix} 1 & X \\ 1 & 1 \end{bmatrix} : X \in M(n, R), \; ^tX = X \}
$$

are subgroups of $\text{Sp}(2n, R)$. The subgroup $M$ normalizes $U$, and $P = MU = UM$.

Proof. These assertions follow by direct computations.

Let $R$ be a commutative ring with identity. Assume further that $R$ is a domain. We say that $R$ is Euclidean domain if there exists a function $|\cdot| : R \to \mathbb{Z}$ satisfying the following three properties:

1. If $a \in R$, then $|a| \geq 0$.
2. If $a \in R$, then $|a| = 0$ if and only if $a = 0$.
3. If $a, b \in R$ and $b \neq 0$, then there exist $x, y \in R$ such that $a = bx + y$ with $|y| < |b|$.

Any field $F$ is an Euclidean domain with the definition $|a| = 1$ for $a \in F$ with $a \neq 0$ and $|0| = 0$. Also, $\mathbb{Z}$ is an Euclidean domain with the usual absolute value.

Theorem 1.9.6. Let $R$ be an Euclidean domain, and let $n$ be a positive integer. The group $\text{Sp}(2n, R)$ is generated by the elements

$$
J = \begin{bmatrix}
1 & 1 \\
-1 & -1
\end{bmatrix},
\begin{bmatrix}
1 & X \\
1 & 1
\end{bmatrix}
$$

for $X \in M(n, R)$ with $^tX = X$. 

If $g \in \text{Sp}(2n, R)$, then $\det(g) = 1$.

**Proof.** This follows from Theorem 1.9.6.

**Corollary 1.9.7.** Let $R$ be an Euclidean domain, and let $n$ be a positive integer. If $g \in \text{Sp}(2n, R)$, then $\det(g) = 1$.

**Proof.** This follows from Theorem 1.9.6.

**Theorem 1.9.8.** Let $F$ be a field, and let $n$ be a positive integer. Assume that the pair $(2n, F)$ is not $(2, \mathbb{Z}/2\mathbb{Z})$, $(2, \mathbb{Z}/3\mathbb{Z})$ or $(4, \mathbb{Z}/2\mathbb{Z})$. Then the only normal subgroups of $\text{Sp}(2n, F)$ are $\{1\}$, $\{1, -1\}$, and $\text{Sp}(2n, F)$.

**Proof.** See Theorem 5.1 of [4].

### 1.10 The Siegel upper half-space

Let $n$ be a positive integer. We define $\mathbb{H}_n$ to be the subset of $\text{M}(n, \mathbb{C})$ consisting of the matrices $Z = X + tY$ with $X, Y \in \text{M}(n, \mathbb{R})$ such that $^tX = X$, $^tY = Y$, and $Y$ is positive-definite. We refer to $\mathbb{H}_n$ as the **Siegel upper half-space of degree** $n$.

**Lemma 1.10.1.** Let $n$ be a positive integer. The set $\text{Sym}(n, \mathbb{R})^+$ is open in $\text{Sym}(n, \mathbb{R})$.

**Proof.** For $1 \leq k \leq n$ and $V \in \text{Sym}(n, \mathbb{R})$, let $V(k \times k) = (V_{ij})_{1 \leq i,j \leq k}$. An element $V \in \text{Sym}(n, \mathbb{R})$ is positive-definite if and only if $\det(V(k \times k)) > 0$ for $1 \leq k \leq n$. Consider the function

$$f : \text{Sym}(n, \mathbb{R}) \rightarrow \mathbb{R}^n, \quad f(V) = (\det V(1 \times 1), \ldots, \det V(n \times n)).$$

The function $f$ is continuous, and therefore $f^{-1}((\mathbb{R}_{>0})^n)$ is an open subset of $\text{Sym}(n, \mathbb{R})$; since $f^{-1}((\mathbb{R}_{>0})^n)$ is exactly $\text{Sym}(n, \mathbb{R})^+$, the proof is complete.

**Proposition 1.10.2.** Let $n$ be a positive integer. The set $\mathbb{H}_n$ is an open subset of $\text{Sym}(n, \mathbb{C})$.

**Proof.** There is a natural homeomorphism $\text{Sym}(n, \mathbb{C}) \cong \text{Sym}(n, \mathbb{R}) \times \text{Sym}(n, \mathbb{R})$. Under this homeomorphism, $\mathbb{H}_n \cong \text{Sym}(n, \mathbb{R}) \times \text{Sym}(n, \mathbb{R})^+$. By Lemma 1.10.1, the set $\text{Sym}(n, \mathbb{R})^+$ is open in $\text{Sym}(n, \mathbb{R})$. It follows that $\mathbb{H}_n$ is an open subset of $\text{Sym}(n, \mathbb{C})$.

**Proposition 1.10.3.** Let $n$ be a positive integer. Let $Z_1, Z_2 \in \mathbb{H}_n$. Then $(1-t)Z_1 + tZ_2 \in \mathbb{H}_n$ for all $t \in [0, 1]$. In particular, $\mathbb{H}_n$ is convex and pathwise-connected.

**Proof.** Write $Z_1 = U_1 + iV_1$ and $Z_2 = U_2 + iV_2$. Then $(1-t)Z_1 + tZ_2 = (1-t)U_1 + tU_2 + i((1-t)V_1 + tV_2)$ for $t \in [0, 1]$. Since $(1-t)U_1 + tU_2 \in \text{Sym}(n, \mathbb{R})$ for $t \in [0, 1]$, to prove the proposition it will suffice to prove that $f(t) = (1-t)V_1 + tV_2 \in \text{Sym}(n, \mathbb{R})^+$ for $t \in [0, 1]$. Write $V_1 = W^2$ where $W \in \text{Sym}(n, \mathbb{R})^+$ (see (1.7)). Then $W^{-1}f(t)W^{-1} = (1-t) \cdot 1_n + tW^{-1}V_2W^{-1}$
for $t \in [0, 1]$. We have $W^{-1}V_{2}W^{-1} \in \text{Sym}(n, \mathbb{R})^{+}$, and for each $t \in [0, 1]$, $W^{-1}f(t)W^{-1} \in \text{Sym}(n, \mathbb{R})^{+}$ if and only if $f(t) \in \text{Sym}(n, \mathbb{R})$. It follows that we may assume that $V_{1} = 1$. Let $t \in [0, 1]$; we need to prove that $A = f(t)$ is positive-definite. It is clear that $A$ is positive semi-definite. If $B \in M(n, \mathbb{R})$, and $k \in \{1, \ldots, n\}$, then we define $B(k) = (B_{ij})_{1 \leq i, j \leq k}$. Since $A$ is positive semi-definite, by Sylvester’s Criterion for positive semi-definite matrices, we have $\det(A(k)) \geq 0$ for $k \in \{1, \ldots, n\}$; by Sylvester’s Criterion for positive-definite matrices, we need to prove that $\det(A(k)) > 0$ for $k \in \{1, \ldots, n\}$. Assume that there exists $k \in \{1, \ldots, n\}$ such that $\det(A(k)) = 0$. Then

$$\det((1-t)1_{k} + V_{2}(k)) = 0,$$

so that

$$\det((t-1)1_{k} - V_{2}(k)) = 0.$$

It follows that $t - 1$ is an eigenvalue for $V_{2}(k)$; this implies that $t - 1$ is an eigenvalue for $V_{2}$. This is a contradiction since all the eigenvalues of $V_{2}$ are positive, and $t - 1 \leq 0$. \hfill \Box

**Lemma 1.10.4.** Let $k$ be a positive integer. Let $f : \mathbb{H}_{k} \to \mathbb{C}$ be an analytic function. If $f(iU) = 0$ for all $U$ in an open subset $S$ of $\text{Sym}(k, \mathbb{R})^{+}$, then $f = 0$.

**Proof.** By Proposition 1.10.3, the open subset $\mathbb{H}_{k}$ of $\text{Sym}(k, \mathbb{C})$ is connected. By Proposition 1 on page 3 of [18] it suffices to prove that $f$ vanishes on a non-empty open subset of $\mathbb{H}_{k}$. Let $U$ be any element of $S$. Since $f$ is analytic at $iU$ and $\mathbb{H}_{k}$ is an open subset of $\text{Sym}(k, \mathbb{C})$, there exists $\epsilon > 0$ such that

$$D = \{Z \in \text{Sym}(n, \mathbb{C}) : |Z_{ij} - iU_{ij}| < \epsilon, 1 \leq i \leq j \leq k\} \subset \mathbb{H}_{k},$$

and a power series

$$\sum_{\alpha \in \mathbb{Z}_{\geq 0}^{k}} c_{\alpha}(Z - iU)^{\alpha}$$

that converges absolutely and uniformly on compact subsets of $D$, such that this power series converges to $f(Z)$ for $Z \in D$. Evidently, $iU \in D$. Define

$$D' = \{Y \in \text{Sym}(n, \mathbb{R}) : |Y_{ij} - U_{ij}| < \epsilon, 1 \leq i \leq j \leq k\}.$$

Then $U \in D'$. We may assume that $D' \subset S$. If $Y \in D'$, then $iY \in D$. Define $h : D' \to \mathbb{C}$ by $h(Y) = f(iY)$. We have

$$h(Y) = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^{k}} c_{\alpha}(iY - iU)^{\alpha} = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^{k}} i^{\alpha}|c_{\alpha}|(Y - U)^{\alpha}$$

for $Y \in D'$. The function $h$ is $C^{\infty}$, and we have

$$i^{\alpha}|c_{\alpha}| = \frac{1}{\alpha!}(D^{\alpha}h)(U).$$

Since by assumption $f(iY) = 0$ for $Y \in S$, we have $h = 0$. This implies that $c_{\alpha} = 0$ for $\alpha \in \mathbb{Z}_{\geq 0}^{k}$, which in turn implies that $f$ vanishes on the open subset $D \subset \mathbb{H}_{k}$. \hfill \Box
Lemma 1.10.5. Let \( n \) be a positive integer. Let 
\[
g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \text{Sp}(2n, \mathbb{R})
\]
and \( Z \in \mathbb{H}_n \). Then \( CZ + D \) is invertible, and 
\[
(AZ + B)(CZ + D)^{-1} \in \mathbb{H}_n.
\]

Proof. We follow the argument from [13]. Write \( Z = X + iY \) with \( X, Y \in M(n, \mathbb{R}) \). Define 
\[
P = AZ + B, \quad Q = CZ + D.
\]
We will first prove that \( Q \) is invertible. Assume that \( v \in \mathbb{C}^n \) is such that \( Qv = 0 \); we need to prove that \( v = 0 \). We then have:
\[
\begin{align*}
^t PQ - ^t QP &= (Z^tA + iB)(CZ + D) - (Z^tC + iD)(AZ + B) \\
&= Z^tACZ + Z^tAD + iBCZ + iBD \\
&\quad - Z^tCAZ - Z^tCB - iDAZ - iDB \\
&= Z - \overline{Z} \quad \text{(cf. Lemma 1.9.2)} \\
&= 2iY.
\end{align*}
\]

It follows that 
\[
\begin{align*}
^t v (^t PQ - ^t QP) & = 2i vY \overline{v} \\
^t v^t PQ & - ^t v^t QP \overline{v} = 2i vY \overline{v} \\
^t v^t PQ \overline{v} & - ^t (Qv) \overline{P} \overline{v} = 2i vY \overline{v} \\
0 & = 2i vY \overline{v} \\
0 & = ^t vY \overline{v}.
\end{align*}
\]

Write \( v = v_1 + iv_2 \) with \( v_1, v_2 \in \mathbb{R}^n \). Then 
\[
0 = ^t vY \overline{v} = ^t v_1 Y v_1 + ^t v_2 Y v_2.
\]
Since \( Y \) is positive-definite, the real numbers \( ^t v_1 Y v_1 \) and \( ^t v_2 Y v_2 \) are both non-negative; since the sum of these two numbers is zero, both are zero. Again, since \( Y \) is positive-definite, this implies that \( v_1 = v_2 = 0 \) so that \( v = 0 \). Hence, \( Q \) is invertible. Now we prove that \( PQ^{-1} \) is symmetric. Evidently, \( PQ^{-1} \) is symmetric if and only if \( ^t PQ = ^t QP \). Now
\[
\begin{align*}
^t PQ & - ^t QP = ^t (AZ + B)(CZ + D) - ^t (CZ + D)(AZ + B) \\
&= (Z^tA + iB)(CZ + D) - (Z^tC + iD)(AZ + B) \\
&= Z^tACZ + Z^tAD + iBCZ + iBD \\
&\quad - Z^tCAZ - Z^tCB - iDAZ - iDB \\
&= 0 \quad \text{(cf Lemma 1.9.2)}
\end{align*}
\]
as desired. It follows that \( PQ^{-1} \) is symmetric. Write \( PQ^{-1} = X' + iY' \) where \( X', Y' \in M(n, \mathbb{R}) \) with \( ^tX' = X' \) and \( ^tY' = Y' \). To complete the proof of the lemma we need to show that \( Y' \) is positive-definite. Now

\[
Y' = \frac{1}{2i}((X' + iY') - (X'+iY'))
\]

\[
= \frac{1}{2i}(PQ^{-1} - PQ^{-1})
\]

\[
= \frac{1}{2i}(1(PQ^{-1}) - PQ^{-1})
\]

\[
= \frac{1}{2i}(Q^{-1}P - PQ^{-1})
\]

\[
= \frac{1}{2i}(Q^{-1}(PQ - PQ^-1)Q^{-1})
\]

\[
= \frac{1}{2i}(Q^{-1}YQ^{-1}) \quad \text{(cf. (1.9))}
\]

\[
= Q^{-1}YQ^{-1}.
\]

Using that \( Y \) is positive-definite, it is easy to verify that \( Y' = Q^{-1}YQ^{-1} \) is positive-definite. \( \square \)
Chapter 2

Classical theta series on $\mathbb{H}_1$

2.1 Definition and convergence

Lemma 2.1.1. Let $f$ be a positive integer. Let $A \in M(f, \mathbb{R})$ be a positive-definite symmetric matrix, and for $x \in \mathbb{R}^f$ let

$$Q(x) = \frac{1}{2}^tAx.$$

For $z \in \mathbb{H}_1$, define

$$\theta(A, z) = \sum_{m \in \mathbb{Z}^f} e^{\pi i z^t m Am} = \sum_{m \in \mathbb{Z}^f} e^{2\pi i z Q(m)}$$

For every $\delta > 0$, this series converges absolutely and uniformly on the set

$$\{z \in \mathbb{H}_1 : \text{Im}(z) \geq \delta\}.$$

The function $\theta(A, \cdot)$ is an analytic function on $\mathbb{H}_1$.

Proof. Since $A$ is positive-definite, the function defined by $x \mapsto \sqrt{Q(x)}$ defines a norm on $\mathbb{R}^f$. All norms on $\mathbb{R}^f$ equivalent; in particular, this norm is equivalent to the standard norm $\| \cdot \|$ on $\mathbb{R}^f$. Hence, there exists $\epsilon > 0$ such that

$$\epsilon\|x\| \leq \sqrt{Q(x)},$$

or equivalently,

$$\epsilon^2\|x\|^2 = \epsilon^2(x_1^2 + \cdots + x_f^2) \leq Q(x)$$

for $x = (x_1, \ldots, x_f) \in \mathbb{R}^f$.

Now let $\delta > 0$, and let $z \in \mathbb{H}_1$ be such that $\text{Im}(z) \geq \delta$. Let $m = (m_1, \ldots, m_f) \in \mathbb{Z}^f$. Then

$$|e^{2\pi i z Q(m)}| = e^{-2\pi \text{Im}(z)Q(m)}$$
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

\[ \leq e^{-2\pi\delta Q(m)} \]
\[ \leq e^{-2\pi\delta \varepsilon^2\|m\|^2} \]
\[ = q^{|m|^2} \]
\[ = q^{m_1^2 + \cdots + m_f^2}. \]

where $q = e^{-2\pi\delta \varepsilon^2}$. Since $0 < q < 1$, the series
\[ \sum_{n \in \mathbb{Z}} q^{n^2} \]
converges absolutely. This implies that the series
\[ (\sum_{n \in \mathbb{Z}} q^{n^2})^f = \sum_{m \in \mathbb{Z}^f} q^{m_1^2 + \cdots + m_f^2} = \sum_{m \in \mathbb{Z}^f} q^{\|m\|^2} \]
converges absolutely. It follows from the Weierstrass $M$-test that our series
\[ \sum_{m \in \mathbb{Z}^f} e^{2\pi izQ(m)} \]
converges absolutely and uniformly on $\{z \in \mathbb{H}_1 : \text{Im}(z) \geq \delta\}$ (see, for example, [17], p. 160). Since for each $m \in \mathbb{Z}^f$ the function on $\mathbb{H}_1$ defined by $z \mapsto e^{2\pi izQ(m)}$ is an analytic function, and since our series converges absolutely and uniformly on every closed disk in $\mathbb{H}_1$, it follows that $\theta(A, \cdot)$ is analytic on $\mathbb{H}_1$ (see [17], p. 162). \qed

**Proposition 2.1.2.** Let $f$ be a positive integer. Let $\varepsilon$ be a real number such that $0 < \varepsilon < 1$. Let $K_1$ be a compact subset of $\mathbb{H}_1$, and let $K_2$ be a compact subset of $\mathbb{C}^f$. Then there exists a positive real number $R > 0$ such that
\[ \text{Im}(z \cdot \overline{t}(w + g)(w + g)) \geq \varepsilon \text{Im}(z \cdot \overline{t}gg), \]
or equivalently
\[ -\text{Im}(z \cdot \overline{t}(w + g)(w + g)) \leq -\varepsilon \text{Im}(z \cdot \overline{t}gg), \]
for $z \in K_1$, $w \in K_2$ and $g \in \mathbb{R}^f$ such that $\|g\| \geq R$.

**Proof.** Let $M > 0$ be a positive real number such that
\[ M \geq |\text{Re}(z)|, |\text{Im}(z)|, |\text{Re}(w)|, |\text{Im}(w)| \]
for $z \in K_1$ and $w \in K_2$. Let $\delta > 0$ be such that
\[ \text{Im}(z) \geq \delta > 0 \]
for $z \in K_1$. Let $R > 0$ be such that if $x \in \mathbb{R}$ and $x \geq R$, then
\[ 0 \leq (1 - \varepsilon)\delta x^2 - 4M^2x - 4M^3, \]
or equivalently,
\[ 4M^2(x + M) \leq (1 - \varepsilon)\delta x^2. \]

Now let \( z \in K_1 \), \( w \in K_2 \), and let \( g \in \mathbb{R}^f \) with \( \|g\| \geq R \). Write \( z = \sigma + it \) for some \( \sigma, t \in \mathbb{R} \) with \( t > 0 \). Also, write \( w = a + bi \) with \( a, b \in \mathbb{R}^f \). Then calculations show that
\[
2 \cdot \text{Im}(z^\dagger wg) = 2t \cdot ag + 2\sigma \cdot bg,
\]
\[
\text{Im}(z^\dagger ww) = \sigma(\sigma'aa - bb) - 2t \cdot ab.
\]

It follows that
\[
-2 \cdot \text{Im}(z^\dagger wg) - \text{Im}(z^\dagger ww) \leq (1 - \varepsilon)\text{Im}(z^\dagger gg),
\]
\[
\varepsilon \text{Im}(z^\dagger gg) \leq \text{Im}(z^\dagger gg) + 2 \cdot \text{Im}(z^\dagger wg) + \text{Im}(z^\dagger ww).
\]

This is the desired inequality. \( \square \)

**Corollary 2.1.3.** Let \( f \) be a positive integer. Let \( A \in M(f, \mathbb{R}) \) be a positive-definite symmetric matrix. Let \( \varepsilon \) be real number such that \( 0 < \varepsilon < 1 \). Let \( K_1 \) be a compact subset of \( \mathbb{H}_1 \), and let \( K_2 \) be a compact subset of \( \mathbb{C}^f \). For \( x \in \mathbb{C}^f \), define
\[
Q(x) = \frac{1}{2} x^\dagger Ax.
\]

Then there exists a positive real number \( R > 0 \) such that
\[
\text{Im}(z \cdot Q(w + g)) \geq \varepsilon \text{Im}(z \cdot Q(g)),
\]
or equivalently,
\[
-\text{Im}(z \cdot Q(w + g)) \leq -\varepsilon \text{Im}(z \cdot Q(g)),
\]
for \( z \in K_1 \), \( w \in K_2 \), and all \( g \in \mathbb{R}^f \) such that \( \|g\| \geq R \).
Proof. Since $A$ is a positive-definite symmetric matrix, there exists a positive-definite symmetric matrix $B \in M(f, \mathbb{R})$ such that $A = BB = BB$ (see (1.7)). The set $B(K_2)$ is a compact subset of $\mathbb{C}^f$. By Proposition 2.1.2 there exists a positive real number $T > 0$ such that

$$\text{Im}(z \cdot ^t(w' + g')(w' + g')) \geq \varepsilon \text{Im}(z \cdot ^tg'g')$$

for $z \in K_1$, $w' \in B(K_2)$, and $g' \in \mathbb{R}^f$ with $\|g'\| \geq T$. We may regard the matrix $B^{-1}$ as a operator from $\mathbb{R}^f$ to $\mathbb{R}^f$; as such, $B^{-1}$ is bounded. Hence,

$$\|B^{-1}(g)\| \leq \|B^{-1}\| \|g\|$$

for $g \in \mathbb{R}^f$. Define $R = \|B^{-1}\| T$. Let $z \in K_1$, $w \in K_2$ and $g \in \mathbb{R}^f$ with $\|g\| \geq R$. Then $w' = Bw \in B(K_2)$, and:

$$\|B^{-1}(B(g))\| \leq \|B^{-1}\| \|B(g)\|$$

$$\|g\| \leq \|B^{-1}\| \|B(g)\|$$

$$R \leq \|B^{-1}\| \|B(g)\|$$

$$\|B^{-1}\|^{-1} R \leq \|B(g)\|$$

$$T \leq \|B(g)\|.$$ 

Therefore, with $g' = B(g)$,

$$\text{Im}(z \cdot ^t(w' + g')(w' + g')) \geq \varepsilon \text{Im}(z \cdot ^tg'g')$$

$$\text{Im}(z \cdot ^t(Bw + Bg)(Bw + Bg)) \geq \varepsilon \text{Im}(z \cdot ^tB(Bg)B)$$

$$\text{Im}(z \cdot ^t(w + g) BB(w + g)) \geq \varepsilon \text{Im}(z \cdot ^tg BB)$$

$$\text{Im}(z \cdot ^t(w + g) A(w + g)) \geq \varepsilon \text{Im}(z \cdot ^tg A)$$

$$\text{Im}(z \cdot ^tQ(w + g)) \geq \varepsilon \text{Im}(z \cdot ^tQ)$$

This completes the proof. \hfill \Box

Proposition 2.1.4. Let $f$ be a positive integer. Let $A \in M(f, \mathbb{R})$ be a positive-definite symmetric matrix, and for $x \in \mathbb{R}^f$ let

$$Q(x) = \frac{1}{2} x A x.$$ 

For $z \in \mathbb{H}_1$ and $w = ^t(w_1, \ldots, w_f) \in \mathbb{C}^f$, define

$$\theta(A, z, w) = \sum_{m \in \mathbb{Z}^f} e^{\pi i z^t(m + w) A(m + w)} = \sum_{m \in \mathbb{Z}^f} e^{2\pi i z Q(m + w)}.$$ 

Let $D$ be a closed disk in $\mathbb{H}_1$, and let $D_1, \ldots, D_f$ be closed disks in $\mathbb{C}^f$. Then $\theta(A, z, w_1, \ldots, w_f)$ converges absolutely and uniformly on $D \times D_1 \times \cdots \times D_f$. The function $\theta(A, z, w_1, \ldots, w_f)$ on $\mathbb{H}_1 \times \mathbb{C}^f$ is analytic in each variable.
Proof. We apply Corollary 2.1.3 with $\varepsilon = 1/2$, $K_1 = D$ and $K_2 = D_1 \times \cdots \times D_f$. By this corollary, there exists a finite set $X$ of $\mathbb{Z}^f$ such that for $m \in \mathbb{Z}^f - X$, $z \in K_1$ and $w \in K_2$ we have:

$$|e^{2\pi izQ(m+w)}| = e^{\text{Re}(2\pi izQ(m+w))}$$
$$= e^{-2\pi \text{Im}(zQ(m+w))}$$
$$\leq e^{-2\pi \cdot (1/2) \cdot \text{Im}(zQ(m))}$$
$$= e^{-2\pi Q(m) \text{Im}(z/2)}$$
$$\leq e^{-2\pi \delta Q(m)}$$
$$= |e^{2\pi i(\delta)(Q(m))}|.$$

Here, $\delta > 0$ is such that $\delta \leq \text{Im}(z/2)$ for $z \in D$. By Lemma 2.1.1 the series

$$\sum_{m \in \mathbb{Z}^f} |e^{2\pi i(\delta)(Q(m))}|$$

converges. The Weierstrass $M$-test (see [17], p. 160) now implies that the series

$$\theta(A, z, w) = \sum_{m \in \mathbb{Z}^f} e^{2\pi izQ(m+w)}$$

converges absolutely and uniformly on $D \times D_1 \times \cdots \times D_f$. Since for each $m \in \mathbb{Z}^f$ the function on $\mathbb{H}_1 \times \mathbb{C}_f$ defined by $(z, w) \mapsto e^{2\pi izQ(m+w)}$ is an analytic function in each variable $z, w_1, \ldots, w_f$, and since our series converges absolutely and uniformly on all products of closed disks, it follows that $\theta(A, z, w_1, \ldots, w_f)$ is analytic in each variable (see [17], p. 162).

### 2.2 The Poisson summation formula

Let $f$ be a positive integer. Let $g : \mathbb{R}^f \to \mathbb{C}$ be a function, and write $g = u + iv$, where $u, v : \mathbb{R}^f \to \mathbb{R}$ are functions. We say that $g$ is smooth if $u$ and $v$ are both infinitely differentiable. Assume that $g$ is smooth. Let $(\alpha_1, \ldots, \alpha_f) \in \mathbb{Z}_{>0}^f$. We define

$$D^\alpha g = \left(\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_f}}{\partial x_f^{\alpha_f}}\right)g.$$

We say that $f$ is a Schwartz function if

$$\sup_{x \in \mathbb{R}^f} |P(x)(D^\alpha)(x)|$$

is finite for all $P(X) = P(X_1, \ldots, X_f) \in \mathbb{C}[X_1, \ldots, X_f]$ and $\alpha \in \mathbb{Z}_{>0}^f$. The set $\mathcal{S}(\mathbb{R}^f)$ of all Schwartz functions is a complex vector space, called the Schwartz
space on $\mathbb{R}^f$. If $g \in S(\mathbb{R}^f)$, then we define the **Fourier transform** of $g$ to be the function $\mathcal{F}g : \mathbb{R}^f \to \mathbb{C}$ defined by

$$(\mathcal{F}g)(x) = \int_{\mathbb{R}^f} g(y)e^{-2\pi i xy} \, dy$$

for $x \in \mathbb{R}^f$. If $g \in S(\mathbb{R}^f)$, then the integral defining $\mathcal{F}g$ converges absolutely for every $x \in \mathbb{R}^f$. In fact, if $g \in S(\mathbb{R}^f)$, then $\mathcal{F}g \in S(\mathbb{R}^f)$, and a number of other properties hold; see, for example, chapter 7 of [22], or chapter 13 of [15].

**Lemma 2.2.1.** Let $f$ be a positive integer. Let $A \in M(f, \mathbb{R})$ be a positive-definite symmetric matrix, and for $x \in \mathbb{R}^f$ let

$$Q(x) = \frac{1}{2} x A x.$$  

Let $w \in \mathbb{C}^f$. The function $g : \mathbb{R}^f \to \mathbb{C}$ defined by

$$g(x) = e^{-\pi q(x+w)A(x+w)}$$

for $x \in \mathbb{R}^f$ is in the Schwartz space $S(\mathbb{R}^f)$.

**Proof.** We begin with some simplifications. Also, there exists a positive-definite symmetric matrix $B \in \text{GL}(f, \mathbb{R})$ such that $A = B^{-1}B = BB$ (see (1.7)). The function $g$ is in $S(\mathbb{R}^f)$ if and only if $g \circ B^{-1}$ is in $S(\mathbb{R}^f)$. Now

$$g(B^{-1}x) = e^{-\pi (B^{-1}x+w)B(B^{-1}x+w)}$$

$$= e^{-\pi (B^{-1}x+w)B(B^{-1}x+w)}$$

$$= e^{-\pi (x+Bw)(x+Bw)}.$$  

It follows that we may assume that $A = 1$. Next, let $w = u+iv$ where $u, v \in \mathbb{R}^f$. Since $g$ is in $S(\mathbb{R}^f)$ if and only if the function defined by $x \mapsto g(x-u)$ for $x \in \mathbb{R}^f$ is in $S(\mathbb{R}^f)$, we may also assume that $u = 0$. Now

$$g(x) = e^{-\pi (x+iv)(x+iv)}$$

$$= e^{-\pi x - 2\pi ivx + \pi ivv}$$

$$= e^{\pi ivv} e^{-\pi x - 2\pi ivx}.$$  

Since $e^{\pi ivv}$ is a constant, it suffices to prove that the function $h : \mathbb{R}^f \to \mathbb{C}$ defined by

$$h(x) = e^{-\pi x - 2\pi ivx}$$

for $x \in \mathbb{R}^f$ is contained in $S(\mathbb{R}^f)$. Let $\alpha = (\alpha_1, \ldots, \alpha_f) \in \mathbb{Z}_{\geq 0}^f$. Then there exists a polynomial $Q_\alpha(X_1, \ldots, X_f) \in \mathbb{C}[X_1, \ldots, X_f]$ such that

$$(D^\alpha h)(x) = Q_\alpha(x)e^{-\pi x - 2\pi ivx}$$
2.2. THE POISSON SUMMATION FORMULA

for \( x \in \mathbb{R}^f \). Hence, if \( P(X_1, \ldots, X_f) \in \mathbb{C}[X_1, \ldots, X_f] \), then

\[
|P(x)(D^a h)(x)| = |P(x)Q_\alpha(x)e^{-\pi^\frac{1}{2}x^2 - 2\pi i x v}|
= |P(x)Q_\alpha(x)e^{-\pi^\frac{1}{2}x^2}|
\]

for \( x \in \mathbb{R}^f \). This equality implies that it now suffices to prove that the function defined by \( x \mapsto e^{-\pi x^2} \) for \( x \in \mathbb{R}^f \) is contained in \( \mathcal{S}(\mathbb{R}^f) \). This is a well-known fact that can be proven using L'Hôpital's rule.

Lemma 2.2.2. Let \( f \) be a positive integer. If \( w \in \mathbb{C}^f \), then

\[
\int_{\mathbb{R}^f} e^{-\pi^\frac{1}{2}(y+w)^2} dy = \int_{\mathbb{R}^f} e^{-\pi^\frac{1}{2}y^2} dy.
\]

Proof. By Fubini's theorem

\[
\int_{\mathbb{R}^f} e^{-\pi^\frac{1}{2}(y+w)^2} dy = \int_{\mathbb{R}^f} e^{-\pi^\frac{1}{2}y_1^2} \cdots e^{-\pi^\frac{1}{2}y_f^2} dy
= \left( \int_{\mathbb{R}} e^{-\pi^\frac{1}{2}(y_1+w_1)^2} dy_1 \right) \cdots \left( \int_{\mathbb{R}} e^{-\pi^\frac{1}{2}(y_f+w_f)^2} dy_f \right).
\]

It thus suffices to prove the lemma when \( f = 1 \). Write \( w = u + iv \) with \( u, v \in \mathbb{R} \). Then

\[
\int_{\mathbb{R}} e^{-\pi^\frac{1}{2}(y+u+iv)^2} dy = \int_{\mathbb{R}} e^{-\pi^\frac{1}{2}(y+iv)^2} dy.
\]

To complete the proof we will use Cauchy's theorem. Assume, say, \( v > 0 \). Let \( a > 0 \), and let \( \gamma = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 \) be the closed piecewise smooth curve as below:

By Cauchy's theorem (see chapter 2 of [17]) applied to the analytic function \( z \mapsto e^{-\pi z^2} \) we have

\[
0 = \int_{\gamma_1} e^{-\pi z^2} dz + \int_{\gamma_2} e^{-\pi z^2} dz + \int_{\gamma_3} e^{-\pi z^2} dz + \int_{\gamma_4} e^{-\pi z^2} dz.
\]
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

Using the definitions of these contour integrals, this is:

$$0 = \int_{-a}^{a} e^{-\pi y^2} \, dy + \int_{\gamma_2} e^{-\pi z^2} \, dz - \int_{-a}^{a} e^{-\pi (y+iv)^2} \, dy + \int_{\gamma_4} e^{-\pi z^2} \, dz,$$

or equivalently,

$$\int_{-a}^{a} e^{-\pi (y+iv)^2} \, dy = \int_{-a}^{a} e^{-\pi y^2} \, dy + \int_{\gamma_2} e^{-\pi z^2} \, dz + \int_{\gamma_4} e^{-\pi z^2} \, dz. \tag{2.1}$$

On the curves $\gamma_2$ and $\gamma_4$ the function $z \mapsto e^{-\pi z^2}$ is bounded by $e^{-\pi a^2 + \pi v^2}$.

Therefore (see Theorem 3 on page 81 of [17]),

$$|\int_{\gamma_2} e^{-\pi z^2} \, dz| \leq ve^{-\pi a^2 + \pi v^2}, \quad |\int_{\gamma_3} e^{-\pi z^2} \, dz| \leq ve^{-\pi a^2 + \pi v^2}.$$

These bounds imply that

$$\lim_{a \to \infty} \int_{\gamma_2} e^{-\pi z^2} \, dz = \lim_{a \to \infty} \int_{\gamma_4} e^{-\pi z^2} \, dz = 0.$$

Letting $a \to \infty$ in (2.1), we thus obtain

$$\int_{-\infty}^{\infty} e^{-\pi (y+iv)^2} \, dy = \int_{-\infty}^{\infty} e^{-\pi y^2} \, dy.$$

This is the desired result. If $v < 0$, then there is a similar proof. \qed

**Lemma 2.2.3.** Let $f$ be a positive integer. Let $A \in M(f, \mathbb{R})$ be a positive-definite symmetric matrix, and for $x \in \mathbb{R}^f$ let

$$Q(x) = \frac{1}{2} {}^t x A x.$$

Let $w \in \mathbb{C}^f$. Define $g : \mathbb{R}^f \to \mathbb{C}$ by

$$g(x) = e^{-2\pi Q(x+w)} = e^{-\pi {}^t(x+w) A(x+w)}$$

for $x \in \mathbb{R}^f$. Then

$$(\mathcal{F}g)(x) = \det(A)^{-1/2} e^{2\pi i {}^t x w} e^{-\pi {}^t x A^{-1} x}$$

for $x \in \mathbb{R}^f$.

**Proof.** There exists positive-definite symmetric matrix $B \in \text{GL}(f, \mathbb{R})$ such that $A = {}^t B B = B B$ (see (1.7)). Let $x \in \mathbb{R}^f$. Then:

$$(\mathcal{F}g)(x) = \int_{\mathbb{R}^f} \exp(-2\pi Q(y+w)) \exp(-2\pi i {}^t x y) \, dy$$
Applying now Lemma 2.2.2, we obtain:

\[ (Fg)(x) = \exp \left( -\pi \left( \begin{array}{c} 2Q(y + w) + 2i^t xy \end{array} \right) \right) dy \]

\[ = \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} (y + w)A(y + w) + 2i^t xy \end{array} \right) \right) dy \]

\[ = \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} (y + w)B(y + w) + 2i^t (By)B^{-1} x \end{array} \right) \right) dy \]

\[ = \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} (By + Bw)(By + Bw) + 2i^t (By)B^{-1} x \end{array} \right) \right) dy \]

\[ = \det(B)^{-1} \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} (y + Bw)(y + Bw) + 2i^t B^{-1} x \end{array} \right) \right) dy. \]

In the last step we used the formula for a linear change of variables (see Theorem 2.20, (e) on page 50 and section 2.23 of [23]; note also that det(A) and det(B) are positive, as A and B are positive-definite symmetric matrices). Now \( \det(B)^2 = \det(A) \), so that \( \det(A)^{-1/2} = \det(B) \). Hence,

\[ (Fg)(x) \]

\[ = \det(A)^{-1/2} \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} \left( \begin{array}{c} yy + 2i^t yBw + Bw \end{array} \right) \right) \right) dy \]

\[ = \det(A)^{-1/2} \exp(-\pi^t w Aw) \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} \left( \begin{array}{c} yy + 2i^t yBw + 2i^t B^{-1} x \end{array} \right) \right) \right) dy \]

\[ = \det(A)^{-1/2} \exp(-\pi^t w Aw) \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} \left( \begin{array}{c} yy + 2i^t y(Bw + i^t B^{-1} x) \end{array} \right) \right) \right) dy \]

\[ \times \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} \left( \begin{array}{c} yy + 2i^t y(Bw + i^t B^{-1} x) \end{array} \right) \right) \right) dy \]

\[ = \det(A)^{-1/2} \exp \left( -\pi^t w Aw \right) \exp \left( \pi^t (Bw + i^t B^{-1} x)(Bw + i^t B^{-1} x) \right) \]

\[ \times \int_{\mathbb{R}^j} \exp \left( -\pi \left( \begin{array}{c} \left( \begin{array}{c} yy + 2i^t y(Bw + i^t B^{-1} x) \end{array} \right) \right) \right) dy. \]

Applying now Lemma 2.2.2, we obtain:

\[ (Fg)(x) = \det(A)^{-1/2} \exp \left( 2\pi^t xw - \pi^t xA^{-1} x \right) \int_{\mathbb{R}^j} \exp \left( -\pi^t yy \right) dy \]
\[(\mathcal{F}g)(x) = \det(A)^{-1/2} \exp(2\pi i x w - \pi x A^{-1} x)\].

Here, we have used the well-known classical fact that
\[
\int_{\mathbb{R}^f} \exp(-\pi^i y^j) dy = 1.
\]

This completes the calculation. \(\Box\)

**Theorem 2.2.4** (Poisson summation formula). Let \(f\) be a positive integer. Let \(g \in S(\mathbb{R}^f)\). Then
\[
\sum_{m \in \mathbb{Z}^f} g(m) = \sum_{m \in \mathbb{Z}^f} (\mathcal{F}g)(m),
\]
where both series converge absolutely.

*Proof.* See page 249 of [15]. \(\Box\)

**Lemma 2.2.5.** Let \(f\) be a positive integer. Let \(A \in M(\mathbb{R}^f)\) be a positive-definite symmetric matrix. Let \(\varepsilon\) be real number such that \(0 < \varepsilon < 1\). Let \(K_1\) be a compact subset of \(\mathbb{H}_1\), and let \(K_2\) be a compact subset of \(\mathbb{C}^f\). For \(x \in \mathbb{C}^f\), define
\[
Q(x) = \frac{1}{2} x A x.
\]
Then there exists a positive real number \(R > 0\) such that
\[
-\text{Im} \left( \frac{1}{z} \cdot \mathcal{F}A^{-1} g + \mathcal{F}g \right) \leq -\varepsilon \text{Im} \left( \frac{1}{z} \cdot \mathcal{F}A^{-1} g \right),
\]
for \(z \in K_1, w \in K_2,\) and all \(g \in \mathbb{R}^f\) such that \(\|g\| \geq R\).

*Proof.* This proof is similar to the proof of Proposition 2.1.2. First of all, there exists a positive-definite symmetric matrix \(B \in \text{GL}(f, \mathbb{R})\) such that \(A = B^T B\) (see (1.7)). If \(m \in \mathbb{R}^f\), then we note that
\[
\mathcal{F}A^{-1} g = |\mathcal{F}A^{-1} g|
= |\mathcal{F}B^{-1} B^{-1} g|
= |\mathcal{F}(B^{-1} g) \cdot (B^{-1} g)|
= \|\mathcal{F}B^{-1} g\| \|\mathcal{F}B^{-1} g\|
\geq \left( \frac{1}{\|B\|} \|\mathcal{F}B\| \|\mathcal{F}B^{-1} g\| \right)^2
= \left( \frac{1}{\|B\|} \|g\| \right)^2
= \frac{1}{\|B\|^2} \|g\|^2.
\]

Next, let \(M > 0\) be such that
\[
|\text{Im}(-1/z)|, |\text{Im}(w)| \leq M
\]
for \(z \in K_1\) and \(w \in K_2\); note that the set consisting of \(-1/z\) for \(z \in K_1\) is also a compact subset of \(\mathbb{H}_1\). Let \(\delta > 0\) be such that
\[
\text{Im}(-1/z) \geq \delta > 0.
\]
Let \(R > 0\) be such that if \(x \geq R\), then
\[
\delta(1 - \varepsilon) \cdot \frac{1}{\|B\|^2} \cdot x^2 \geq 2Mx.
\]
Now \(z \in K_1\), \(w \in K_2\), and \(g \in \mathbb{R}^f\) with \(\|g\| \geq R\). Write \(-1/z = \sigma + it\) for \(\sigma, t \in \mathbb{R}\) and \(w = a + bi\) for \(a, b \in \mathbb{R}^f\). We have
\[
-\text{Im}(2^t g w) = -2^t gb \leq 2|gb| \leq 2M\|g\|.
\]
On the other hand,
\[
(1 - \varepsilon) \cdot \text{Im}((-1/z)^t g A^{-1} g) = t \cdot g A^{-1} g \geq \delta(1 - \varepsilon) \cdot \frac{1}{\|B\|^2} \cdot \|g\|^2.
\]
It follows that
\[
-\text{Im}(2^t g w) \leq (1 - \varepsilon) \cdot \text{Im}((-1/z)^t g A^{-1} g) - \text{Im}((-1/z)^t g A^{-1} g + 2^t g w) \leq -\varepsilon \cdot \text{Im}((-1/z)^t g A^{-1} g).
\]
This is the desired result.

**Theorem 2.2.6.** Let \(f\) be a positive integer. Assume that \(f\) is even, and set
\[
k = \frac{f}{2}.
\]
Let \(A \in \mathbb{M}(f, \mathbb{R})\) be a positive-definite symmetric matrix, and for \(x \in \mathbb{R}^f\) let
\[
Q_A(x) = \frac{1}{2} x A x, \quad Q_{A^{-1}}(x) = \frac{1}{2} x A^{-1} x.
\]
The series
\[
\sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z)^t m A^{-1} m + 2\pi i b m w}
\]
converges absolutely and uniformly for \((z, w) \in D \times D_1 \times \cdots \times D_f\), where \(D\) is any closed disk in \(\mathbb{H}_1\), and \(D_1, \ldots, D_f\) are any closed disks in \(\mathbb{C}^f\). The function that sends \((z, w) \in \mathbb{H}_1 \times \mathbb{C}^f\) to this series is analytic in each variable. We have
\[
\theta(A, z, w) = \frac{i^k}{z^k \sqrt{\text{det}(A)}} \sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z)^t m A^{-1} m + 2\pi i b m w}
\]
for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\).
Proof. We apply Lemma 2.2.5 with \( \varepsilon = 1/2, K_1 = D, \) and \( K_2 = D_1 \times \cdots \times D_f. \) By this corollary, there exists a finite set \( X \) of \( \mathbb{Z}^f \) such that for \( m \in \mathbb{Z}^f - X, \) \( z \in K_1 \) and \( w \in K_2 \) we have:

\[
|e^{\pi((-1/2)^{m}A_{-1}^{-1}m + 2\pi i \wedge w)}| = e^{-\pi \text{Im}\left((-1/2)^{m}A_{-1}^{-1}m\right)}
\]

\[
= e^{-\pi \text{Im}\left((-1/2)^{m}Q_{A-1}(m)\right)}
\]

\[
\leq e^{-\pi \delta Q_{A-1}(m)}
\]

\[
eq |e^{2\pi i(\delta z)Q_{A-1}(m)}|
\]

Here, \( \delta > 0 \) is such that \( \delta \leq \text{Im}(-1/(2z)) \) for \( z \in D. \) By Lemma 2.1.1 the series

\[
\sum_{m \in \mathbb{Z}^f} |e^{2\pi i(\delta z)Q_{A-1}(m)}|
\]

converges. The Weierstrass M-test (see [17], p. 160) now implies that the series

\[
\sum_{m \in \mathbb{Z}^f} e^{\pi((-1/2)^{m}A_{-1}^{-1}m + 2\pi i \wedge w)}
\]

converges absolutely and uniformly on \( D \times D_1 \times \cdots \times D_f. \) Since for each \( m \in \mathbb{Z}^f \) the function on \( \mathbb{H}_1 \times \mathbb{C}^f \) defined by \( (z,w) \mapsto e^{\pi((-1/2)^{m}A_{-1}^{-1}m + 2\pi i \wedge w}) \) is an analytic function in each variable \( z, w_1, \ldots, w_f, \) and since our series converges absolutely and uniformly on all products of closed disks, it follows that this series is analytic in each variable (see [17], p. 162).

Now fix \( w \in \mathbb{C}^f. \) Define \( g : \mathbb{R}^f \to \mathbb{C} \) by

\[
g(x) = e^{-\pi Q_{A}(x+w)} = e^{-\pi \wedge (x+w)A(x+w)}
\]

for \( x \in \mathbb{R}^f. \) Then by Lemma 2.2.3,

\[
(Fg)(x) = \text{det}(A)^{-1/2}e^{-\pi xA^{-1}x + 2\pi i \wedge x}
\]

for \( x \in \mathbb{R}^f. \) By Theorem 2.2.4, the Poisson summation formula, we have:

\[
\sum_{m \in \mathbb{Z}^f} e^{-2\pi Q_{A}(m+w)} = \sum_{m \in \mathbb{Z}^f} \text{det}(A)^{-1/2}e^{-\pi \wedge xA^{-1}x + 2\pi i \wedge x}
\]

\[
\sum_{m \in \mathbb{Z}^f} e^{2\pi i \cdot Q_{A}(m+w)} = \text{det}(A)^{-1/2} \sum_{m \in \mathbb{Z}^f} e^{\pi i \cdot (-1/2)^{m}xA^{-1}x + 2\pi i \wedge x}
\]

Let \( t > 0. \) Replacing \( A \) by \( tA, \) we obtain similarly,

\[
\sum_{m \in \mathbb{Z}^f} e^{2\pi i \cdot tA \wedge Q_{A}(m+w)} = \frac{1}{\text{det}(tA)^{1/2}} \sum_{m \in \mathbb{Z}^f} e^{\pi i \cdot (-1/(2it)) \wedge xA^{-1}x + 2\pi i \wedge x}
\]
\[ = \frac{i^k}{(it)^k \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/(it)) A^{-1} x + 2 \pi i \cdot x w} \]

\[ \sum_{m \in \mathbb{Z}^f} e^{2 \pi i \cdot z Q_A(m+w)} = \frac{i^k}{z^k \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z) A^{-1} x + 2 \pi i \cdot x w} \]

\[ \theta(A, z, w) = \frac{i^k}{z^k \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z) A^{-1} x + 2 \pi i \cdot x w}, \]

for \( z \in \mathbb{H}_1 \) of the form \( z = it \) for \( t > 0 \). Since both sides of the last equation are analytic functions in \( z \) for \( z \in \mathbb{H}_1 \), the Identity Principle (see p. 307 of [17]) implies that this equality holds for all \( z \in \mathbb{H}_1 \).

\[ \square \]

### 2.3 Differential operators

Let \( f \) be a positive integer. Let \( H(\mathbb{C}^f) \) be the \( \mathbb{C} \)-algebra of all functions

\[ F : \mathbb{C}^f \to \mathbb{C} \]

that are analytic in each variable. Let \( \ell = (\ell_1, \ldots, \ell_f) \in \mathbb{C}^f \). We define a \( \mathbb{C} \) linear map

\[ L_\ell : H(\mathbb{C}^f) \to H(\mathbb{C}^f) \]

by

\[ L_\ell(F) = \sum_{i=1}^{f} \ell_i \frac{\partial F}{\partial w_i}. \]

**Lemma 2.3.1.** Let \( f \) be a positive integer, and let \( \ell \in \mathbb{C}^f \). Then

\[ L_\ell(F_1 \cdot F_2) = L_\ell(F_1) \cdot F_2 + F_1 \cdot L_\ell(F_2) \]

for \( F_1, F_2 \in H(\mathbb{C}^f) \). Also,

\[ L_\ell(e^F) = L_\ell(F) \cdot e^F \]

for \( F \in H(\mathbb{C}^f) \).

**Proof.** Let \( F_1, F_2 \in H(\mathbb{C}^f) \). We have

\[ L_\ell(F_1 \cdot F_2) = \sum_{i=1}^{f} \ell_i \left( \frac{\partial}{\partial w_i} (F_1 \cdot F_2) \right) \]

\[ = \sum_{i=1}^{f} \ell_i \left( \frac{\partial F_1}{\partial w_i} \cdot F_2 + F_1 \cdot \frac{\partial F_2}{\partial w_i} \right) \]

\[ = \sum_{i=1}^{f} \ell_i \frac{\partial F_1}{\partial w_i} \cdot F_2 + \sum_{i=1}^{f} \ell_i F_1 \cdot \frac{\partial F_2}{\partial w_i}. \]
\[ \sum_{i=1}^{f} \ell_i \frac{\partial F_1}{\partial w_i} \cdot F_2 + F_1 \cdot \left( \sum_{i=1}^{f} \ell_i \frac{\partial F_2}{\partial w_i} \right) = L_\ell(F_1) \cdot F_2 + F_1 \cdot L_\ell(F_2). \]

Let \( F \in H(C^f) \). Then:

\[ L_\ell(e^F) = \sum_{i=1}^{f} \ell_i \frac{\partial}{\partial w_i} (e^F) = \sum_{i=1}^{f} \ell_i \frac{\partial F}{\partial w_i} \cdot e^F = \left( \sum_{i=1}^{f} \ell_i \frac{\partial F}{\partial w_i} \right) \cdot e^F = L_\ell(F) \cdot e^F. \]

This completes the proof. \( \square \)

**Lemma 2.3.2.** Let \( f \) be a positive integer and let \( A \in M(f, \mathbb{R}) \) be a positive-definite symmetric matrix. Assume that \( \ell \in C^f \) is such that

\[ \ell^t A \ell = 0. \]

Let \( m \in C^f \) be fixed, and let \( r \) be a non-negative integer. Then:

\[ L_\ell\left( \ell^t (m + w) A (m + w) \right) = 2 \ell^t A (m + w), \]
\[ L_\ell\left( \ell^t A (m + w) \right)^r = 0, \]
\[ L_\ell\left( \ell^t mw \right) = \ell^t m. \]

Here, all functions are variables in \( w \in C^f \).

**Proof.** We have

\[
\begin{align*}
L_\ell\left( \ell^t (m + w) A (m + w) \right) &= L_\ell\left( \sum_{i,j=1}^{f} a_{ij} (m_i + w_i)(m_j + w_j) \right) \\
&= \sum_{i,j=1}^{f} a_{ij} L_\ell((m_i + w_i)(m_j + w_j)) \\
&= \sum_{i,j=1}^{f} a_{ij} \left( L_\ell((m_i + w_i))(m_j + w_j) + (m_i + w_i)L_\ell((m_j + w_j)) \right) \\
&= \sum_{i,j=1}^{f} a_{ij} (\ell_i (m_j + w_j) + \ell_j (m_i + w_i))
\end{align*}
\]
\[= \sum_{i,j=1}^{f} a_{ij} \ell_i (m_j + w_j) + \sum_{i,j=1}^{f} a_{ij} \ell_j (m_i + w_i)\]
\[= ^{\ell}A(m + w) + ^{\ell}(m + w)A\ell\]
\[= 2^{\ell}A(m + w).\]

We prove the second assertion by induction on \(r\). The assertion is clear if \(r = 0\). For \(r = 1\), we have:

\[L_\ell(^{\ell}A(m + w)) = L_\ell\left(\sum_{i,j=1}^{f} a_{ij} \ell_i (m_j + w_j)\right)\]
\[= \sum_{i,j=1}^{f} a_{ij} \ell_i L_\ell(m_j + w_j)\]
\[= \sum_{i,j=1}^{f} a_{ij} \ell_i \ell_j\]
\[= ^{\ell}A\ell\]
\[= 0.\]

Assume now that \(r \geq 2\) and that the claim holds for the non-negative integers \(0, 1, \ldots, r - 1\). Then

\[L_\ell\left(^{\ell}A(m + w)\right)^r\]
\[= L_\ell\left(^{\ell}A(m + w) \cdot \left(^{\ell}A(m + w)\right)^{r-1}\right)\]
\[= L_\ell\left(^{\ell}A(m + w) \cdot \left(^{\ell}A(m + w)\right)^{r-1} + ^{\ell}A(m + w) \cdot L_\ell\left(^{\ell}A(m + w)\right)^{r-1}\right)\]
\[= 0 \cdot \left(^{\ell}A(m + w)\right)^{r-1} + ^{\ell}A(m + w) \cdot 0\]
\[= 0.\]

The final assertion of the lemma is straightforward.

\[\square\]

**Proposition 2.3.3.** Let \(f\) be a positive even integer, and let \(A \in M(f, \mathbb{R})\) be a positive-definite symmetric matrix. Define

\[k = \frac{f}{2}.\]

Let \(\ell \in \mathbb{C}^f\) be such that

\[^{\ell}A\ell = 0.\]

For every non-negative integer \(r\) the series

\[\sum_{m \in \mathbb{Z}^f} \left(^{\ell}A(m + w)\right)^r e^{\pi iz^t(m + w)A(m + w)}\]
and
\[ \sum_{m \in \mathbb{Z}} (i\ell m)^r e^{\pi i(-1/z)^m A^{-1} m + 2\pi i m w} \]
converge absolutely and uniformly for \((z, w) \in D \times D_1 \times \cdots \times D_f\), where \(D\) is any closed disk in \(\mathbb{H}_1\), and \(D_1, \ldots, D_f\) are any closed disks in \(\mathbb{C}^f\). Both series define functions on \(\mathbb{H}_1 \times \mathbb{C}^f\) that are analytic in each variable. Moreover,
\[ \sum_{m \in \mathbb{Z}} \left( i\ell A(m + w) \right)^r e^{\pi i z^m (m + w) A(m + w)} \]
\[ = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}} \left( i\ell m \right)^r e^{\pi i(-1/z)^m A^{-1} m + 2\pi i m w}. \]

**Proof.** We prove this result by induction on \(r\). The case \(r = 0\) is Theorem 2.2.6. Assume the claims hold for \(r\); we will prove that they hold for \(r + 1\). Let
\[ S_1(z, w) = \sum_{m \in \mathbb{Z}} \left( i\ell A(m + w) \right)^r e^{\pi i z^m (m + w) A(m + w)} \]
for \(s \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\). Let \(D\) be any closed disk in \(\mathbb{H}_1\), and let \(D_1, \ldots, D_f\) be any closed disks in \(\mathbb{C}^f\). Since the above series converge absolutely and uniformly on \(D \times D_1 \times \cdots \times D_f\) to \(S_1\), and since the terms of this series are analytic functions in each of the variables \(z, w_1, \ldots, w_f\), the series
\[ \sum_{m \in \mathbb{Z}} L_\ell \left( \left( i\ell A(m + w) \right)^r e^{\pi i z^m (m + w) A(m + w)} \right) \]
converges absolutely and uniformly on \(D \times D_1 \times \cdots \times D_f\) to the analytic function \(L_\ell S_1\) (see p. 162 of [17]). We have for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\), using Lemma 2.3.1 and Lemma 2.3.2,
\[
L_\ell S_1(z, w) = \sum_{m \in \mathbb{Z}} L_\ell \left( \left( i\ell A(m + w) \right)^r e^{\pi i z^m (m + w) A(m + w)} \right) \\
= \sum_{m \in \mathbb{Z}} L_\ell \left( \left( i\ell A(m + w) \right)^r e^{\pi i z^m (m + w) A(m + w)} \right) \\
+ \left( i\ell A(m + w) \right)^r L_\ell \left( e^{\pi i z^m (m + w) A(m + w)} \right) \\
= \sum_{m \in \mathbb{Z}} \left( i\ell A(m + w) \right)^r \cdot L_\ell \left( \pi i z^m (m + w) A(m + w) \right) \cdot e^{\pi i z^m (m + w) A(m + w)} \\
= 2\pi i z \sum_{m \in \mathbb{Z}} \left( i\ell A(m + w) \right)^{r+1} e^{\pi i z^m (m + w) A(m + w)}.
\]
Next, for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\), let
\[ S_2(z, w) = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}} \left( i\ell m \right)^r e^{\pi i(-1/z)^m A^{-1} m + 2\pi i m w}. \]
2.3. DIFFERENTIAL OPERATORS

Comments similar to those above apply to $S_2$ and the series defining $S_2$. For $S_2$ we have for $z \in \mathbb{H}_1$ and $w \in \mathbb{C}^f$, using Lemma 2.3.1 and Lemma 2.3.2,

\[
(L_\ell S_2)(z, w) = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} L_\ell \left( \frac{\pi i}{z} t^{\ell} m e^{\pi i (1/z) A^{-1} m + 2\pi i w} \right)
\]

\[
= \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} L_\ell \left( e^{\pi i (1/z) A^{-1} m + 2\pi i w} \right) \right)
\]

\[
= \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} L_\ell \left( \left( \pi i (1/z) A^{-1} m + 2\pi i w \right) \right) \right)
\]

\[
= 2\pi i \cdot \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} L_\ell \left( \left( \pi i (1/z) A^{-1} m + 2\pi i w \right) \right) \right)
\]

\[
= 2\pi i \cdot \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} L_\ell \left( \left( \pi i (1/z) A^{-1} m + 2\pi i w \right) \right) \right)
\]

Since $(L_\ell S_1)(z, w) = (L_\ell S_2)(z, w)$, we have for $(z, w) \in \mathbb{H}_1 \times \mathbb{C}^f$,

\[
2\pi i z \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} A(m + w) \right)^{r+1} e^{\pi i z (m + w) A(m + w)}
\]

\[
= 2\pi i \cdot \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} L_\ell \left( \left( \pi i (1/z) A^{-1} m + 2\pi i w \right) \right) \right)
\]

or equivalently,

\[
\sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} A(m + w) \right)^{r+1} e^{\pi i z (m + w) A(m + w)}
\]

\[
= \frac{i^k}{z^{k+r+1} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \frac{\pi i}{z} L_\ell \left( \left( \pi i (1/z) A^{-1} m + 2\pi i w \right) \right) \right)
\]

By induction, the proof is complete.

Let $f$ be a positive even integer, and let $A \in M(f, \mathbb{R})$ be a positive-definite symmetric matrix. For $r$ a non-negative integer, we let $\mathcal{H}_r(A)$ be the $\mathbb{C}$ vector space spanned by the polynomials in $w_1, \ldots, w_f$ given by

\[
\left( \frac{\pi i}{z} \ell A \right)^r
\]

where $w = (w_1, \ldots, w_f)$ and $\ell \in \mathbb{C}^f$ with $\ell A \ell = 0$. The elements of $\mathcal{H}_r(A)$ are homogeneous polynomials of degree $r$, and are called **spherical functions** with respect to $A$. 

2.4 A space of theta series

Lemma 2.4.1. Let $f$ be a positive even integer, and define $k = f/2$. Let $A \in M(f, \mathbb{Z})$ be an even symmetric positive-definite matrix, and let $N$ be the level of $A$. Define the quadratic form $Q(x)$ in $f$ variables by

$$Q(x) = \frac{1}{2} x^t A x.$$

Let $r$ be a non-negative integer, and let $P \in \mathcal{H}_r(A)$. Let $h \in \mathbb{Z}^f$ be such that $Ah \equiv 0 \pmod{N}$.

For $z \in \mathbb{H}_1$ define

$$\theta(A, P, h, z) = \sum_{n \in \mathbb{Z}^f, n \equiv h \pmod{N}} P(n) e^{2\pi i z Q(n) / N^2}.$$

This series converges absolutely and uniformly on closed disks in $\mathbb{H}_1$ to an analytic function. If $h, h' \in \mathbb{Z}^f$ are such that $Ah \equiv 0 \pmod{N}$, $Ah' \equiv 0 \pmod{N}$, and $h \equiv h' \pmod{N}$, then

$$\theta(A, P, h, z) = \theta(A, P, h', z), \quad (2.2)$$
$$\theta(A, P, h, z) = (-1)^r \theta(A, P, -h, z), \quad (2.3)$$

for $z \in \mathbb{H}_1$. For $h \in \mathbb{Z}^f$ with $Ah \equiv 0 \pmod{N}$ and $P \in \mathcal{H}_r(A)$ we have

$$\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{\det(A)}} \sum_{g \pmod{N}, Ag \equiv 0 \pmod{N}} e^{2\pi i \frac{h^t A h}{N^2}} \theta(A, P, g, z) \quad (2.4)$$

and

$$\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} 1 \\ b \end{bmatrix} = e^{2\pi i b \frac{Q(h)}{N^2}} \theta(A, P, h, z) \quad (2.5)$$

for $z \in \mathbb{H}_1$. Let $P \in \mathcal{H}_r(A)$, and let $V(A, P)$ be the $\mathbb{C}$ vector space spanned by the functions $\theta(A, P, h, \cdot)$ for $h \in \mathbb{Z}^f$ with $Ah \equiv 0 \pmod{N}$. The $\mathbb{C}$ vector space $V(A, P)$ is a right $\text{SL}(2, \mathbb{Z})$ module under the $|_{k+r}$ action.

Proof. The assertions (2.2) and (2.3) follow from the involved definitions.

To prove (2.4) and (2.5), let $h \in \mathbb{Z}^f$ with $Ah \equiv 0 \pmod{N}$ and $P \in \mathcal{H}_r(A)$. Using the definition of $\mathcal{H}_r(A)$, it is clear that may assume that the polynomial $P$ is of the form

$$P(w) = (\ell^t A \ell)^r.$$

for some $\ell \in \mathbb{C}^f$ such that $\ell^t A \ell = 0$. We recall from Proposition 2.3.3 that
2.4. A SPACE OF THETA SERIES

\[ \sum_{m \in \mathbb{Z}^f} \left( \ell A(m + w) \right)^r e^{\pi i z \left( (m+w) A(m+w) \right)} \]

\[ = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^r e^{\pi i (-1/z) (mA^{-1}m + 2\pi i mw)} . \]

for \( z \in \mathbb{H}_1 \) and \( w \in \mathbb{C}^f \). Replacing \( w \) with \( h/N \), we obtain:

\[ \sum_{m \in \mathbb{Z}^f} \left( \ell A(m + \frac{h}{N}) \right)^r e^{\pi i z \left( (m+\frac{h}{N}) A(m+\frac{h}{N}) \right)} \]

\[ = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^r e^{\pi i (-1/z) (mA^{-1}m + 2\pi i \frac{mh}{N})} . \]

Let \( m \in \mathbb{Z}^f \). Then

\[ m + \frac{h}{N} = \frac{h + mN}{N} = \frac{n}{N}, \]

where \( n = h + mN \). The map

\[ \mathbb{Z}^f \sim \rightarrow \{ n \in \mathbb{Z}^f : n \equiv h \pmod{N} \} \]

defined by \( m \mapsto n = h + mN \) is a bijection, the inverse of which is given by \( n \mapsto (n - h) \). It follows that

\[ N^{-r} \sum_{n \in \mathbb{Z}^f, n \equiv h \pmod{N}} \left( \ell An \right)^r e^{\pi i z \left( nA^{-1}n \right) / N^2} \]

\[ = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^r e^{\pi i (-1/z) (mA^{-1}m + 2\pi i \frac{mh}{N})} . \]

Next, consider the map

\[ \mathbb{Z}^f \sim \rightarrow \{ g \in \mathbb{Z}^f : Ag \equiv 0 \pmod{N} \} \]

defined by \( m \mapsto g = NA^{-1}m \); note that \( NA^{-1}m \in \mathbb{Z}^f \) for \( m \in \mathbb{Z}^f \) because \( NA^{-1} \) is integral by the definition of the level \( N \). This map is a bijection, with inverse defined by \( g \mapsto m = N^{-1}Ag \). Hence,

\[ N^{-r} \sum_{n \in \mathbb{Z}^f, n \equiv h \pmod{N}} \left( \ell An \right)^r e^{\pi i z \left( nA^{-1}n \right) / N^2} \]

\[ = N^{-r} \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{g \in \mathbb{Z}^f, Ag \equiv 0 \pmod{N}} \left( \ell Ag \right)^r e^{\pi i (-1/z) \left( Ag \right) A^{-1}Ag + 2\pi i \frac{gh}{N}}. \]
Canceling the common factor $N^{-r}$, we get:

$$
\sum_{n \in \mathbb{Z}^f} \left( t \ell A n \right)^r e^{\pi i \frac{n_1 A n}{N^2}} = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{g \in \mathbb{Z}^f} \sum_{Ag \equiv 0 \pmod{N}} \left( t \ell A g \right)^r e^{\pi i \left( -1/z \right) \frac{n_1 A g}{N^2} + 2\pi i \frac{\nu_1 A h}{N^2}}.
$$

The set of $g \in \mathbb{Z}^f$ such that $Ag \equiv 0 \pmod{N}$ is a subgroup of $\mathbb{Z}^f$; this subgroup in turn contains the subgroup $NZ^f$. We may therefore sum in stages on the right-hand side. Let $F(g)$ be the summand on the right-hand side for $g \in \mathbb{Z}^f$ with $Ag \equiv 0 \pmod{N}$. The form of this summation in stages is then:

$$
\sum_{g \in \mathbb{Z}^f} F(n) = \sum_{g \in \mathbb{Z}^f / NZ^f} \sum_{m \in NZ^f} F(g + m) = \sum_{g \equiv 0 \pmod{N}} \sum_{n_1 \in \mathbb{Z}^f} F(n_1),
$$

Applying this observation, we have:

$$
\sum_{n \in \mathbb{Z}^f} \left( t \ell A n \right)^r e^{\pi i \frac{n_1 A n}{N^2}} = \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{Ag \equiv 0 \pmod{N}} \sum_{n_1 \equiv g \pmod{N}} \left( t \ell A n_1 \right)^r e^{\pi i \left( -1/z \right) \frac{n_1 A n_1}{N^2} + 2\pi i \frac{\nu_1 A h}{N^2}}.
$$

Let $g \in \mathbb{Z}^f$ with $Ag \equiv 0 \pmod{N}$ and let $n_1 \in \mathbb{Z}^f$ with $n_1 \equiv g \pmod{N}$. Write $n_1 = g + Nm$ for some $m \in \mathbb{Z}^f$. Then

$$
e^{2\pi i \frac{\nu_1 A h}{N^2}} = e^{2\pi i \frac{\nu_1 A h}{N^2}} e^{2\pi i \frac{m A h}{N^2}}
= e^{2\pi i \frac{\nu_1 A h}{N^2}} e^{2\pi i \frac{m A h}{N^2}}
= e^{2\pi i \frac{\nu_1 A h}{N^2}}.
$$

In the last step we used that $Ah \equiv 0 \pmod{N}$, so that $\frac{m A h}{N}$ is an integer. We therefore have:

$$
\sum_{n \in \mathbb{Z}^f} \left( t \ell A n \right)^r e^{\pi i \frac{n_1 A n}{N^2}}
$$
2.4. A SPACE OF THETA SERIES

\[\frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{g \equiv 0 (\text{mod } N)} e^{2\pi i \frac{\gamma A h}{N^2}} \sum_{n_1 \in \mathbb{Z}^f / \mathbb{Z}} \left( \frac{\ell A n_1}{N} \right)^r e^{\pi i \left(-\frac{1}{z}\right) \frac{\gamma A n_1}{N}}.\]

Interchanging \(z\) and \(-1/z\), we obtain:

\[\sum_{n_1 \in \mathbb{Z}^f / \mathbb{Z}} \left( \frac{\ell A n_1}{N} \right)^r e^{\pi i \left(-\frac{1}{z}\right) \frac{\gamma A n_1}{N}} = \frac{(-1)^{k+r} z^{k+r}}{\sqrt{\det(A)}} \sum_{g \equiv 0 (\text{mod } N)} e^{2\pi i \frac{\gamma A h}{N^2}} \sum_{n_1 \in \mathbb{Z}^f / \mathbb{Z}} \left( \frac{\ell A n_1}{N} \right)^r e^{\pi iz \frac{\gamma A n_1}{N}}.\]

This implies that

\[\theta(A, P, h, \begin{bmatrix} 1 & b \\ -1 & 1 \end{bmatrix} \cdot z) = \frac{(-1)^{k+2r} z^{k+r}}{\sqrt{\det(A)}} \sum_{g \equiv 0 (\text{mod } N)} e^{2\pi i \frac{\gamma A h}{N^2}} \theta(A, P, g, z),\]

which is equivalent to (2.4).

Next, let \(b \in \mathbb{Z}\). We have

\[\theta(A, P, h, z) \big|_{k+r} \begin{bmatrix} 1 & b \\ -1 & 1 \end{bmatrix} = \theta(A, P, h, z + b)\]

\[= \sum_{n \equiv h (\text{mod } N)} P(n) e^{2\pi i (z+b) \frac{Q(n)}{N^2}} \]

\[= \sum_{n \equiv h (\text{mod } N)} P(n) e^{2\pi i \frac{Q(n)}{N^2}} e^{2\pi i z \frac{Q(n)}{N^2}}\]

\[= e^{2\pi i \frac{Q(h)}{N^2}} \sum_{n \equiv h (\text{mod } N)} P(n) e^{2\pi i z \frac{Q(n)}{N^2}} \quad \text{(cf. Lemma 1.5.8)}\]

\[= e^{2\pi i \frac{Q(h)}{N^2}} \theta(A, P, h, z).\]

This is (2.5).

Finally, the vector space \(V(A, P)\) is mapped into itself by \(\text{SL}(2, \mathbb{Z})\) via the \(|_{k+r}\) right action because \(\text{SL}(2, \mathbb{Z})\) is generated by the matrices

\[\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\]

and because (2.4) and (2.5) hold. \(\square\)
2.5 The case $N = 1$

**Proposition 2.5.1.** Let $f$ be a positive even integer, and define $k = f/2$. Let $A \in \text{M}(f, \mathbb{Z})$ be an even symmetric positive-definite matrix, and let $N$ be the level of $A$. By Corollary 1.5.5 $N = 1$ if and only if $\det(A) = 1$; assume that $N = 1$ so that also $\det(A) = 1$. Then $f$ is divisible by 8. Let $r$ be a non-negative integer, and let $P \in \mathcal{H}_r(A)$. The $\mathbb{C}$ vector space $V(A, P)$ has dimension at most one, and is spanned by the theta series

$$
\theta(A, P, 0, z) = \sum_{n \in \mathbb{Z}^f} P(n) e^{2\pi i z Q(n)}.
$$

We have

$$
\theta(A, P, 0, z) \big|_{k+r} = \theta(A, P, 0, z) (2.7)
$$

for all $\alpha \in \text{SL}(2, \mathbb{Z})$, and $\theta(A, P, 0, z)$ is a modular form of weight $k + r$ with respect to $\text{SL}(2, \mathbb{Z})$.

**Proof.** Let $h \in \mathbb{Z}^f$; since $N = 1$, we have $Ah \equiv 0 \pmod{N}$. Now

$$
\theta(A, P, h, z) = \sum_{n \in \mathbb{Z}^f, n \equiv h \pmod{1}} P(n) e^{2\pi i z Q(n)}
$$

for all $h \in \mathbb{Z}^f$. It follows that $V(A, P)$ is at most one-dimensional, and is spanned by the function $\theta(A, P, 0, z)$. By Lemma 2.4.1, we have

$$
\theta(A, P, 0, z) \big|_{k+r} \begin{bmatrix} 1 & \alpha \\ -1 & 1 \end{bmatrix} = i^k \theta(A, P, 0, z),
$$

(2.8)

$$
\theta(A, P, 0, z) \big|_{k+r} \begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix} = \theta(A, P, 0, z)
$$

(2.9)

for $b \in \mathbb{Z}$. Since $\text{SL}(2, \mathbb{Z})$ is generated by the elements

$$
\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}
$$

it follows that there exists a function $t : \text{SL}(2, \mathbb{Z}) \to \mathbb{C}^\times$ such that

$$
\theta(A, P, 0, z) \big|_{k+r} \alpha = t(\alpha) \cdot \theta(A, P, 0, z)
$$

(2.10)

for $\alpha \in \text{SL}(2, \mathbb{Z})$ and for all non-negative integers $r$ and $P \in \text{SL}(2, \mathbb{Z})$. We claim that $t(\alpha) = 1$ for all $\alpha \in \text{SL}(2, \mathbb{Z})$. Assume that $r = 0$ and let $P \in \mathcal{H}_0(A)$ be the polynomial such that $P(X_1, \ldots, X_f) = 1$. Then the function $\theta(A, P, 0, z)$ is
not identically zero. Since \( \theta(A, P, 0, z) \) is not identically zero, and since \( |k| \) is a right action, equation (2.10) implies that \( t \) is a homomorphism. Also, by (2.8) and (2.9) we have
\[
t(\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}) = i^k, \quad t(\begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix}) = 1
\]
for \( b \in \mathbb{Z} \). Now
\[
\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}.
\]
Applying these matrices to \( \theta(A, P, 0, z) \) we obtain:
\[
\theta(A, P, 0, z)|_k \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix} = \theta(A, P, 0, z)|_k \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}
\]
\[
i^{2k} \theta(A, P, 0, z) = (-1)^k \theta(A, P, 0, z).
\]
Since \( \theta(A, P, 0, z) \) is not identically zero, we have \( i^{2k} = (-1)^k \). We also have the matrix identity
\[
\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -b \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix}
\]
for \( b \in \mathbb{Z} \). Applying these matrices to \( \theta(A, P, 0, z) \), we find that:
\[
i^{2k} \theta(A, P, 0, z) = (-1)^k \theta(A, P, 0, z)|_k \begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix}
\]
for \( b \in \mathbb{Z} \). Since \( i^{2k} = (-1)^k \), this implies that
\[
\theta(A, P, 0, z)|_{k+r} \begin{bmatrix} 1 & 1 \\ b & 1 \end{bmatrix} = \theta(A, P, 0, z)
\]
for \( b \in \mathbb{Z} \). Therefore, \( t \) is trivial on all matrices of the form
\[
\begin{bmatrix} 1 & b \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & b \\ b & 1 \end{bmatrix}
\]
for \( b \in \mathbb{Z} \). Since these matrices generate \( \text{SL}(2, \mathbb{Z}) \) it follows that the homomorphism \( t \) is trivial. This proves (2.7) for all \( \alpha \in \text{SL}(2, \mathbb{Z}) \), for all non-negative integers \( r \) and \( P \in \mathcal{H}_r(A) \). Also, since \( t \) is trivial, we must have \( i^k = 1 \). Write \( k = 4a + b \) where \( a \) and \( b \) are non-negative integers with \( b \in \{0, 1, 2, 3\} \). Then
\[
1 = i^k = (i^4)^a i^b = i^b.
\]
This equality implies that \( 4|k \), so that \( 8|f \).

Given what we have already proven, to complete the proof that \( \theta(A, P, 0, z) \) is a modular form of weight \( k + r \) for \( \text{SL}(2, \mathbb{Z}) \), it will suffice to prove that \( \theta(A, P, 0, z) \) is holomorphic at the cusps of \( \text{SL}(2, \mathbb{Z}) \), i.e., that the third condition of the definition of a modular form holds (see section 1.7). Clearly, the smallest positive integer \( N \) such that \( \Gamma(N) \subset \text{SL}(2, \mathbb{Z}) \) is \( N = 1 \). Let \( \sigma \in \text{SL}(2, \mathbb{Z}) \). We have already proven that \( \theta(A, P, 0, z)|_{k+r} \sigma = \theta(A, P, 0, z) \). Thus, to complete
the proof we need to prove the existence of a positive number $R$ and a complex power series

$$
\sum_{m=0}^{\infty} a(m)q^m
$$

that converges in $D(R) = \{q \in \mathbb{C} : |q| < R\}$ such that

$$
\theta(A, P, 0, z) = \sum_{m=0}^{\infty} a(m)e^{2\pi imz}
$$

for $z \in H(1, R) = \{z \in \mathbb{H}_1 : \text{Im}(z) > -\log(R)\}$ (note that $H(1, R)$ is mapped into $D(R)$ under the map defined by $z \mapsto e^{2\pi iz}$). Consider the power series

$$
\sum_{n \in \mathbb{Z}} P(n)q^{Q(n)} \quad (2.11)
$$

in the complex variable $q$. Let $q$ be any element of $\mathbb{C}$ with $|q| < 1$. Since $q = e^{2\pi iz}$ for some $z \in \mathbb{H}_1$, and since

$$
\sum_{n \in \mathbb{Z}} P(n)e^{2\pi izQ(n)} = \sum_{n \in \mathbb{Z}} P(n)q^{Q(n)}
$$

converges absolutely by Lemma 2.4.1, it follows that the power series (2.11) converges absolutely at $q$. Hence, the radius of convergence of the power series (2.11) is greater than 0, and in fact at least 1 (see Theorem 8 on p. 172 of [17]). Since by the definition of $\theta(A, P, 0, z)$ we have

$$
\theta(A, P, 0, z) = \sum_{n \in \mathbb{Z}} P(n)e^{2\pi izQ(n)},
$$

for $z \in \mathbb{H}_1$, the proof is complete. \hfill \Box

### 2.6 Example: a quadratic form of level one

If the level $N$ of $A$ is 1, so that the $\theta(A, P, h, z)$ are modular forms with respect to $\text{SL}(2, \mathbb{Z})$, then necessarily $8|f$ by Proposition 2.5.1. Assume that $f = 8$. Up to equivalence, there is the only positive-definite even integral symmetric matrix $A$ in $\text{M}(8, \mathbb{Z})$ with $\det(A) = 1$. This matrix arises in the following way. Consider the root system $E_8$ inside $\mathbb{R}^8$. To describe this root system with 240 elements, let $e_1, \ldots, e_8$ be the standard basis for $\mathbb{R}^8$. The root system $E_8$ consists of the 112 vectors

$$
\delta_1 e_i + \delta_2 e_k \quad \text{where} \ 1 \leq i, k \leq 8, \ i \neq k, \ \text{and} \ \delta_1, \delta_2 \in \{\pm 1\}
$$

and the 128 vectors

$$
\frac{1}{2}(\epsilon_1 e_1 + \cdots + \epsilon_8 e_8) \quad \text{where} \ \epsilon_1, \ldots, \epsilon_8 \in \{\pm 1\} \ \text{and} \ \epsilon_1 \cdots \epsilon_8 = 1.
$$
2.6. EXAMPLE: A QUADRATIC FORM OF LEVEL ONE

Every element of $E_8$ has length $\sqrt{2}$. As a base for this root system we can take the 8 vectors

\[
\begin{align*}
\alpha_1 &= \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7 + e_8), \\
\alpha_2 &= e_1 + e_2, \\
\alpha_3 &= -e_1 + e_2, \\
\alpha_4 &= -e_2 + e_3, \\
\alpha_5 &= -e_3 + e_4, \\
\alpha_6 &= -e_4 + e_5, \\
\alpha_7 &= -e_5 + e_6, \\
\alpha_8 &= -e_6 + e_7.
\end{align*}
\]

Every element of $E_8$ can be written as a $\mathbb{Z}$ linear combination of $\alpha_1, \ldots, \alpha_8$ such that all the coefficients are either all non-negative or all non-positive. Let $A$ be the Cartan matrix of $E_8$ with respect to the above base; this turns out to be

\[
A = \begin{bmatrix}
2 & -1 & & & & & & \\
-1 & 2 & -1 & & & & & \\
& -1 & 2 & -1 & & & & \\
& & -1 & 2 & -1 & & & \\
& & & -1 & 2 & -1 & & \\
& & & & -1 & 2 & -1 & \\
& & & & & -1 & 2 & \\
& & & & & & -1 & 2
\end{bmatrix}.
\]

Clearly, $A$ is the matrix of $(\cdot, \cdot)$ with respect to the ordered basis $\alpha_1, \ldots, \alpha_8$ for $\mathbb{R}^8$; hence, $A$ is positive-definite. Evidently $A$ is an even integral symmetric matrix, and a computation shows that $\det(A) = 1$. Since $\det(A) = 1$, the level of $A$ is $N = 1$. The quadratic form $Q$ is given by:

\[
Q(x_1, x_2, x_3, \ldots, x_8) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2
\]

\[
- x_1x_3 - x_2x_4 - x_3x_4 - x_4x_5 - x_5x_6 - x_6x_7 - x_7x_8.
\]

Let $r = 0$, and let $1 \in \mathcal{H}_0(A)$ be the constant polynomial. The theta series

\[
\theta(A, z) = \theta(A, 1, 0, z) = \sum_{m \in \mathbb{Z}^8} e^{2\pi i Q(m)}
\]

is a non-zero modular form for $\text{SL}(2, \mathbb{Z})$ of weight $8/2 = 4$. We may also write

\[
\theta(A, z) = \sum_{n=0}^{\infty} r(n) e^{2\pi in}
\]

where

\[
r(n) = \# \{ m \in \mathbb{Z}^8 : Q(m) = n \}.
\]
It is known that the dimension of the space of modular forms for SL(2, \mathbb{Z}) of weight 4 is one (see Proposition 2.26 on p. 46 of [26]). Moreover, this space contains the Eisenstein series
\[ E(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) e^{2\pi i n z} \]
where
\[ \sigma_3(n) = \sum_{a|n, a > 0} a^3 \]
for positive integers \( n \). Since \( r(0) = 1 \), we have \( \theta(A, z) = E(z) \). Thus,
\[ r(n) = 240 \cdot \sigma_3(n) \]
for all positive integers \( n \). Evidently, \( 240 \cdot \sigma_3(1) = 240 \). Thus, there are 240 solutions \( m \in \mathbb{Z}^8 \) to the equation \( Q(m) = 1 \). These 240 solutions are exactly the coordinates of the elements of \( E_8 \) when the elements of \( E_8 \) are written in our chosen base (note that the coordinates are automatically in \( \mathbb{Z} \), as this is property of a base for a root system).

### 2.7 The case \( N > 1 \)

The action of SL(2, \mathbb{Z})

**Lemma 2.7.1.** Let \( f \) be a positive even integer, and define \( k = f/2 \). Let \( A \in M(f, \mathbb{Z}) \) be an even symmetric positive-definite matrix, and let \( N \) be the level of \( A \). Let \( c \) be a positive integer; by Corollary 1.5.7, the level of \( cA \) is \( cN \). Let \( r \) be a non-negative integer. We have \( \mathcal{H}_r(cA) = \mathcal{H}_r(A) \). Let \( h \in \mathbb{Z}^f \) be such that \( Ah \equiv 0 \pmod{N} \) and let \( P \in \mathcal{H}_r(A) \). If \( g \in \mathbb{Z}^f \) is such that \( g \equiv h \pmod{N} \), then \( (cA)g \equiv 0 \pmod{cN} \) so that \( \theta(cA, P, g, \cdot) \) is defined, and
\[ \theta(A, P, h, z) = \sum_{g \pmod{cN}} \theta(cA, P, g, cz) \]
for \( z \in \mathbb{H}_1 \).

**Proof.** If \( \ell \in \mathbb{C}^f \), then \( \ell A \ell = 0 \) if and only if \( \ell (cA) \ell = 0 \); this observation, and the involved definitions, imply that \( \mathcal{H}_r(cA) = \mathcal{H}_r(A) \). Next, let \( z \in \mathbb{H}_1 \). Then:
\[ \theta(A, P, h, z) = \sum_{n \in \mathbb{Z}^f, n \equiv h \pmod{N}} P(n) e^{2\pi i z Q(n) / N^2} \]
\[ = \sum_{g \in \mathbb{Z}^f/cN} \sum_{n_1 \in cN \mathbb{Z}^f} P(g + n_1) e^{2\pi i z Q(g + n_1) / N^2} . \]
2.7. THE CASE $N > 1$

Let $g \in \mathbb{Z}^f$ with $g \equiv h \pmod{N}$. There is a bijection

$$c\mathbb{Z}^f \xrightarrow{\sim} \{ m \in \mathbb{Z}^f : m \equiv g \pmod{cN} \}$$

given by $n_1 \mapsto m = g + n_1$. Hence,

$$\theta(A,P,h,z) = \sum_{g \equiv h \pmod{N}} \sum_{m \in \mathbb{Z}^f} P(m) e^{2\pi i \frac{\epsilon m Am}{N}} = \sum_{g \equiv h \pmod{N}} \sum_{m \in \mathbb{Z}^f} P(m) e^{\pi i \frac{\epsilon m Am}{cN}}$$

This completes the proof. \(\square\)

**Lemma 2.7.2.** Let $f$ be a positive even integer. Let $A \in M(f, \mathbb{Z})$ be an even symmetric positive-definite matrix, and let $N$ be the level of $A$. Let

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}),$$

and assume that $c \neq 0$. Let

$$Y(A) = \{ m \in \mathbb{Z}^f : Am \equiv 0 \pmod{N} \}.$$

Define a function

$$s_\alpha : Y(A) \times Y(A) \rightarrow \mathbb{C}$$

by

$$s_\alpha(g_1, g_2) = \sum_{g \equiv h \pmod{N}} e^{2\pi i \frac{\epsilon (aQ(g_1) + b g_1 g_2 + dQ(g_2))}{cN^2}}.$$

The function $s_\alpha$ is well-defined. If $g_1, g_1', g_2, g_2' \in Y(A)$ and $g_1 \equiv g_1' \pmod{N}$ and $g_2 \equiv g_2' \pmod{N}$, then $s_\alpha(g_1, g_2) = s_\alpha(g_1', g_2')$. Moreover,

$$s_\alpha(g_1, g_2) = e^{-2\pi i \frac{\epsilon (b g_2 A g_1 + b d Q(g_1))}{N^2}} s_\alpha(0, g_2 + d g_1) \quad (2.12)$$

for $g_1, g_2 \in Y(A)$.

**Proof.** To prove that $s_\alpha$ is well-defined, let $g_1, g_2 \in Y(A)$, and $g, g' \in \mathbb{Z}^f$ with $g \equiv g' \pmod{cN}$ and $g \equiv g' \equiv g_2 \pmod{N}$. Write $g' = g + cN m$ for some $m \in \mathbb{Z}^f$. Then

$$e^{2\pi i \frac{\epsilon (aQ(g') + b g_1 g' + dQ(g_1))}{cN^2}} = e^{2\pi i \frac{\epsilon (aQ(g + cN m) + b g_1 (g + cN m) + dQ(g_1))}{cN^2}}$$

by (2.12).

This completes the proof.
where in the last step we used that \( A_0 \equiv A_1 \equiv 0 \pmod{N} \). It follows that \( s_\alpha \) is well-defined.

Next we prove (2.12). Let \( g_1, g_2 \in Y(A) \). Then

\[
\begin{align*}
  e^{-2\pi i \left( \frac{b_1 g_2 A_{11} + b_1 d Q(g_1)}{N^2} \right)} s_\alpha(0, g_2 + dg_1) \\
  = \sum_{g \equiv g_2 + dg_1 \pmod{N}} e^{-2\pi i \left( \frac{b_1 g_2 A_{11} + b_1 d Q(g_1)}{N^2} \right)} e^{2\pi i \left( \frac{a Q(g)}{c N^2} \right)} \\
  = \sum_{g \equiv g_2 + dg_1 \pmod{N}} e^{2\pi i \left( \frac{a Q(g) - b c b_1 g_2 A_{11} - b c d Q(g_1)}{c N^2} \right)} \\
  = \sum_{g \equiv g_2 \pmod{N}} e^{2\pi i \left( \frac{a Q(g) + b_1 A_2 (a d g - b c g_2) + d Q(g_1)}{c N^2} \right)},
\end{align*}
\]

Let \( g \in \mathbb{Z} \) with \( g \equiv g_2 \pmod{N} \). Write \( g_2 = g + N m \) for some \( m \in \mathbb{Z} \). Then

\[
\begin{align*}
  e^{2\pi i \left( \frac{b_1 A_2 (a d g - b c g_2)}{c N^2} \right)} \\
  = e^{2\pi i \left( \frac{b_1 A_2 (a d g - b c N m)}{c N^2} \right)} \\
  = e^{2\pi i \left( \frac{b_1 A_2 g}{c N^2} \right)} e^{2\pi i \left( \frac{-b c N m (A_2 g_1) m}{c N^2} \right)} \\
  = e^{2\pi i \left( \frac{b_1 A_2 g}{c N^2} \right)} e^{2\pi i \left( \frac{-b c N m (A_2 g_1) m}{N^2} \right)} \\
  = e^{2\pi i \left( \frac{b_1 A_2 g}{c N^2} \right)},
\end{align*}
\]

where the last step follows because \( A_2 g_1 = 0 \pmod{N} \). We therefore have:

\[
\begin{align*}
  e^{-2\pi i \left( \frac{b_1 g_2 A_{11} + b_1 d Q(g_1)}{N^2} \right)} s_\alpha(0, g_2 + dg_1) \\
  = \sum_{g \equiv g_2 \pmod{N}} e^{2\pi i \left( \frac{a Q(g) + b_1 A_2 g + d Q(g_1)}{c N^2} \right)} \\
  e^{-2\pi i \left( \frac{b_1 g_2 A_{11} + b_1 d Q(g_1)}{N^2} \right)} s_\alpha(0, g_2 + dg_1) = s_\alpha(g_1, g_2).
\end{align*}
\]
This completes the proof of (2.12).

Finally, let \( g_1, g'_1, g_2, g'_2 \in Y(A) \) with \( g_1 \equiv g'_1 \pmod{N} \) and \( g_2 \equiv g'_2 \pmod{N} \). It is evident from the definition of \( s_\alpha \) that \( s_\alpha(g_1, g_2) = s_\alpha(g_1, g'_2) \). Write \( g'_1 = g_1 + Nm \) for some \( m \in \mathbb{Z} \).

Then
\[
\begin{align*}
\theta(A, P, g_1, g_2) &= e^{-2\pi i \left( \frac{b}{N} \cdot Ag_1 + dQ(g_1) \right)} \cdot s_\alpha(0, g_2 + d)
\end{align*}
\]

Let \( r \) be a non-negative integer, and let \( P \in H_r(A) \). Let \( h \in \mathbb{Z} \) be such that \( Ah \equiv 0 \pmod{N} \).

Let
\[
\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \SL(2, \mathbb{Z}),
\]
and assume that \( c \) is a positive integer. Then
\[
\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{i^{k+2r}c^k \sqrt{\det(A)}} \sum_{g \pmod{N}} s_\alpha(g, h) \cdot \theta(A, P, g, z), \tag{2.13}
\]

where \( s_\alpha \) is defined in Lemma 2.7.2.

Proof. We have
\[
\begin{align*}
\theta(A, P, h, z) &\bigg|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\
&= j(\alpha, z)^{-k-r} \theta(A, P, h, a \frac{z + b}{cz + d})
\end{align*}
\]
\begin{align*}
&= j(\alpha, z)^{-k-r} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} \theta(cA, P, g, \frac{a}{c}z + \frac{b}{d}c) \\
&= j(\alpha, z)^{-k-r} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} \theta(cA, P, g, -\frac{1}{c}z + \frac{a}{d}) \\
&= j(\alpha, z)^{-k-r} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} e^{2\pi i \Omega(cA, g) \frac{Q(cA, g)}{cN}} \theta(cA, P, g, -\frac{1}{c}z + \frac{a}{d}) \\
&= j(\alpha, z)^{-k-r} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} e^{2\pi i \Omega(g) \frac{Q(g)}{cN}} \theta(cA, P, g, -\frac{1}{c}z + \frac{a}{d}) \\
&= (-1)^{k+r} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} e^{2\pi i \Omega(g) \frac{Q(g)}{cN}} (\theta(cA, P, g, \cdot)|_{k+r} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix})(c\alpha + d) \\
&= \frac{i^k (-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} e^{2\pi i \Omega(g) \frac{Q(g)}{cN}} \sum_{g_1 \equiv h \pmod{cN} \atop g_1 \equiv 0 \pmod{cN}} e^{2\pi i \frac{T_{g_1}(cA, g_1)}{cN} \Omega(cA, g_1)} \theta(cA, P, g_1, cz + d) \\
&= \frac{i^k (-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} e^{2\pi i \Omega(g) \frac{Q(g)}{cN}} \sum_{g_1 \equiv h \pmod{cN} \atop g_1 \equiv 0 \pmod{cN}} e^{2\pi i \frac{T_{g_1}(cA, g_1)}{cN} \Omega(cA, g_1)} e^{2\pi i \frac{T_{Q(g_1)}(cA, g_1)}{cN} \Omega(cA, g_1)} \theta(cA, P, g_1, cz) \\
&= \frac{i^k (-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} e^{2\pi i \frac{T_{Q(g_1)}(cA, g_1)}{cN} \Omega(cA, g_1)} \theta(cA, P, g_1, cz) \\
&= \frac{i^k (-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} \sum_{g_1 \equiv h \pmod{cN} \atop g_1 \equiv 0 \pmod{cN}} s_\alpha(g_1, h) \theta(cA, P, g_1, cz) \\
&= \frac{i^k (-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \equiv h \pmod{cN} \atop g \in \mathbb{Z}/cN\mathbb{Z}} \sum_{g_1 \equiv h \pmod{cN} \atop g_1 \equiv 0 \pmod{cN}} s_\alpha(g_1, h) \theta(cA, P, g_1, cz)
\end{align*}
2.7. THE CASE $N > 1$

\[
\frac{i^k(-1)^k+1}{\sqrt{\det(cA)}} \sum_{g_1 \in \mathbb{Z}^f/\mathbb{Z}^f} \sum_{m \in \mathbb{Z}^f/c\mathbb{Z}^f} s_{\alpha}(g_1 + m, h) \theta(cA, P, g_1 + m, cz)
\]

\[
= \frac{i^k(-1)^k+1}{\sqrt{\det(cA)}} \sum_{g_1 \in \mathbb{Z}^f/\mathbb{Z}^f} s_{\alpha}(g_1, h) \sum_{m \in \mathbb{Z}^f/c\mathbb{Z}^f} \theta(cA, P, g_1 + m, cz)
\]

\[
= \frac{i^k(-1)^k+1}{\sqrt{\det(cA)}} \sum_{g_1 \in \mathbb{Z}^f/\mathbb{Z}^f} s_{\alpha}(g_1, h) \sum_{g' \equiv g_1 (\text{mod } N)} \theta(cA, P, g', cz)
\]

\[
= \frac{i^k(-1)^k+1}{\sqrt{\det(cA)}} \sum_{g_1 \in \mathbb{Z}^f/\mathbb{Z}^f} s_{\alpha}(g_1, h) \sum_{g' \equiv g_1 (\text{mod } N)} \theta(cA, P, g', cz)
\]

\[
= \frac{1}{i^k+2rc^k\sqrt{\det(A)}} \sum_{g_1 \equiv 0 (\text{mod } N)} s_{\alpha}(g_1, h) \cdot \theta(A, P, g_1, z).
\]

Here, we used Lemma 2.7.2. □

The action of $\Gamma_0(N)$

Lemma 2.7.4. Let $f$ be an even positive integer, let $A \in \mathbb{M}(f, \mathbb{Z})$ be a positive-definite even integral symmetric matrix and let $N$ be the level of $A$. Let

\[
Y(A) = \{ g \in \mathbb{Z}^f : Ag \equiv 0 (\text{mod } N) \}.
\]

Define a function

\[
s : Y(A) \rightarrow \mathbb{C}
\]

by

\[
s(g) = \sum_{q \equiv 0 (\text{mod } N)} e^{2\pi i \frac{g A q}{N}} = \sum_{q \in Y(A)/\mathbb{Z}^f} e^{2\pi i \frac{\chi_A q}{N}}
\]

for $g \in Y(A)$. The function $s$ is well-defined and

\[
s(g) = \begin{cases} 
0 & \text{if } g \not\equiv 0 \pmod{N}, \\
\#Y(A)/\mathbb{Z}^f & \text{if } g \equiv 0 \pmod{N}
\end{cases}
\]

for $g \in Y(A)$.

Proof. To see that $s$ is well defined, let $g, q_1, q_2 \in Y$ and assume that $q_2 = q_1 + Nz_3$ for some $z_3 \in \mathbb{Z}^f$. Then

\[
{\chi}_A q_2 = {\chi}_A q_1 + N{\chi}_A z_3
\]

\[
= {\chi}_A q_1 + N{\chi}(Ag)z_3
\]
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

\[ g \equiv t g A q \pmod{N^2}, \]

because $A g \equiv 0 \pmod{N}$. This implies that

\[ e^{2\pi i \frac{t g A q}{N^2}} = e^{2\pi i \frac{t g A q}{N^2}}, \]

so that $s$ is well-defined. To prove the second assertion, assume first that $g \equiv 0 \pmod{N}$. Write $g = N m$ for some $m \in \mathbb{Z}^f$. Let $q \in Y(A)$. Then

\[ t g A q = N t g A q \equiv 0 \pmod{N^2} \]

since $A q \equiv 0 \pmod{N}$ because $q \in Y(A)$. It follows that

\[ s(g) = \sum_{q \in Y(A)/N \mathbb{Z}^f} e^{2\pi i \frac{t g A q}{N^2}} = \sum_{q \in Y(A)/N \mathbb{Z}^f} 1 = \#Y(A)/N \mathbb{Z}^f. \]

Finally, assume that $g \not\equiv 0 \pmod{N}$. Then there exists $m \in \mathbb{Z}^f$ such that $t g m \not\equiv 0 \pmod{N}$. This implies that $t g N m \not\equiv 0 \pmod{N^2}$. Let $q_1 = N A^{-1} m$. Then $q \in Y(A)$ because $A q = N m \equiv 0 \pmod{N}$. Also,

\[ t g A q_1 = g N m \not\equiv 0 \pmod{N^2}. \]

This implies that $e^{2\pi i \frac{t g A q_1}{N^2}} \not= 1$. Since the function $Y(A)/N \mathbb{Z}^f \to \mathbb{C}^\times$ defined by $q \mapsto e^{2\pi i \frac{t g A q}{N^2}}$ is a character, and since this character is non-trivial at $q_1$, it follows that summing this character over the elements of $Y(A)/N \mathbb{Z}^f$ gives 0; this means that $s(g) = 0$. \qed

**Proposition 2.7.5.** Let $f$ be a positive even integer, and define $k = f/2$. Let $A \in \mathbb{M}(f, \mathbb{Z})$ be an even symmetric positive-definite matrix, and let $N$ be the level of $A$. Define the quadratic form $Q(x)$ in $f$ variables by

\[ Q(x) = \frac{1}{2} t x A x. \]

Let $r$ be a non-negative integer, and let $P \in \mathcal{H}_r(A)$. Let $h \in \mathbb{Z}^f$ be such that

\[ A h \equiv 0 \pmod{N}. \]

Let

\[ \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \]

and assume that $d$ is a positive integer. Then

\[ \theta(A, P, h, z) \left|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right. = \left. \frac{1}{d^k} \sum_{q \pmod{dN}} q \left( \frac{h}{dN} \right) \cdot \theta(A, P, ah, z). \right. \tag{2.14} \]
Proof. We will abbreviate 
\[ \alpha = \begin{bmatrix} b & -a \\ d & -c \end{bmatrix}. \]

Applying first Lemma 2.7.3 (note that \(d > 0\)), and then (2.4), we obtain:

\[
\theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}
= \left( \theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \right)_{k+r}
= \left( \theta(A, P, h, z)_{k+r} \begin{bmatrix} b & a \\ d & -c \end{bmatrix} \begin{bmatrix} 1 & -1 \end{bmatrix} \right)
= \frac{1}{i^{k+2r}d^k \sqrt{\det(A)}} \sum_{q \ (\text{mod } N)} s_\alpha(q, h) \theta(A, P, q, z)_{k+r} \begin{bmatrix} 1 & -1 \end{bmatrix}
= \frac{1}{i^{2r}d^k \det(A)} \sum_{q \ (\text{mod } N)} g \ (\text{mod } N) Aq \equiv 0 \ (\text{mod } N) Aq \equiv 0 \ (\text{mod } N) \sum_{q \ (\text{mod } N)} s_\alpha(q, h) e^{2\pi i \frac{t_y Aq}{N^2}} \theta(A, P, g, z)
= \frac{1}{i^{2r}d^k \det(A)} \sum_{g \ (\text{mod } N)} \frac{1}{q \ (\text{mod } N)} Aq \equiv 0 \ (\text{mod } N) Aq \equiv 0 \ (\text{mod } N)
\]

We can calculate the inner sum as follows:

\[
\sum_{q \ (\text{mod } N)} s_\alpha(q, h) e^{2\pi i \frac{t_y Aq}{N^2}}
= \sum_{q \ (\text{mod } N)} s_\alpha(0, h - cq) e^{-2\pi i \left(-\frac{\gamma h Aq + \sigma Q(q)}{N^2}\right)} e^{2\pi i \frac{t_y Aq}{N^2}} \quad (\text{cf. (2.12)})
= s_\alpha(0, h) \sum_{q \ (\text{mod } N)} e^{2\pi i \left(\frac{(q+h) Aq}{N^2}\right)} e^{2\pi i \left(-\frac{\sigma Q(q)}{N^2}\right)} \quad (\text{cf. Lemma 1.5.8})
= s_\alpha(0, h) \sum_{q \ (\text{mod } N)} e^{2\pi i \left(\frac{(q+h) Aq}{N^2}\right)} \quad (\text{cf. Lemma 2.7.4})
= s_\alpha(0, h) \times \begin{cases} 0 & \text{if } g \not\equiv -ah \ (\text{mod } N), \\ \#Y(A)/N\mathbb{Z}/f & \text{if } g \equiv -ah \ (\text{mod } N) \end{cases} \quad (\text{cf. Lemma 2.7.4}).
\]

It follows that

\[
\theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \sum_{q \ (\text{mod } N)} s_\alpha(0, h) e^{2\pi i \frac{t_y Aq}{N^2}} \theta(A, P, q, z)_{k+r} \begin{bmatrix} 1 & -1 \end{bmatrix}
= \theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}
\]

(2.15)
\[ \frac{\#Y(A)/NZ^f}{i^{2r}d^k \det(A)} \cdot s_\alpha(0, h) \cdot \theta(A, P, -ah, z) \]
\[ = \frac{(-1)^r \#Y(A)/NZ^f}{i^{2r}d^k \det(A)} \cdot s_\alpha(0, h) \cdot \theta(A, P, ah, z) \quad \text{(cf. (2.3))} \]
\[ = \frac{\#Y(A)/NZ^f}{d^k \det(A)} \cdot s_\alpha(0, h) \cdot \theta(A, P, ah, z). \quad (2.16) \]

The definition of \( s_\alpha \) asserts that:
\[ s_\alpha(0, h) = \sum_{q \equiv h \pmod{dN}} e^{2\pi i \left( \frac{qQ(q)}{dN} \right)}. \]

Finally, to determine \( \#Y(A)/NZ^f \), assume that \( h = 0, r = 0 \), and that \( P \) is the element of \( \mathcal{H}_0(A) \) such that \( P(X_1, \ldots, X_f) = 1 \). Then the function
\[ \theta(A, 1, 0, z) = \sum_{n \in \mathbb{Z}^f} e^{2\pi izQ(n)} \]
is not identically zero. Also, let
\[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \text{so that} \quad \alpha = \begin{bmatrix} -1 \\ 1 \end{bmatrix}. \]

Then \( s_\alpha(0, 0) = 1 \), and (2.16) asserts that:
\[ \theta(A, 1, 0, z) = \frac{\#Y(A)/NZ^f}{d^k \det(A)} \cdot \theta(A, 1, 0, z). \]

We conclude that
\[ \#Y(A)/NZ^f = \det(A). \]

This completes the proof.

**Lemma 2.7.6.** Let \( f \) be a positive even integer, let \( A \in M(f, \mathbb{Z}) \) be an even symmetric positive-definite matrix, and let \( N \) be the level of \( A \). Let
\[ Y(A) = \{ h \in \mathbb{Z}^f : Ah \equiv 0 \pmod{N} \}. \]

Then
\[ \#Y(A)/NZ^f = \det(A). \]

**Proof.** This was proven in the proof of Proposition 2.7.5.

**Lemma 2.7.7.** Let \( f \) be a positive even integer, and define \( k = f/2 \). Let \( A \in M(f, \mathbb{Z}) \) be an even symmetric positive-definite matrix, and let \( N \) be the level of \( A \). Assume that \( N > 1 \). Define the quadratic form \( Q(x) \) in \( f \) variables by
\[ Q(x) = \frac{1}{2} x^t Ax. \]
Define
\[ \chi_A : \mathbb{Z} \rightarrow \mathbb{C} \]
by
\[ \chi_A(d) = \frac{1}{d^k} \cdot \sum_{m \in \mathbb{Z}/d\mathbb{Z}} e^{2\pi i \frac{Q(m)}{d}} \]
for \( d \in \mathbb{Z} \) with \((d,N) = 1\) and \( d > 0\), by
\[ \chi_A(d) = (-1)^k \chi_A(-d) \]
for \( d \in \mathbb{Z} \) with \((d,N) = 1\) and \( d < 0\), and by
\[ \chi_A(d) = 0 \]
for \( d \in \mathbb{Z} \) with \((d,N) > 1\).

Then \( \chi_A \) is a well-defined real-valued Dirichlet character modulo \( N \). Moreover, if \( r \) is a non-negative integer, \( h \in \mathbb{Z}^f \) is such that \( Ah \equiv 0 \pmod{N} \), and \( P \in \mathcal{H}_r(A) \), then
\[ \theta(A,P,h,z)|_{k+r} = e^{2\pi i \frac{ahq(h)}{N^2}} \cdot \chi_A(d) \cdot \theta(A,P,ah,z) \] (2.17)
for \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \).

Proof. Define a function \( \alpha : \Gamma_0(N) \rightarrow \mathbb{C} \)
in the following way. Let
\[ g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N). \] (2.18)
If \( d > 0 \), then define
\[ \alpha(g) = \frac{1}{d^k} \sum_{q \in \mathbb{Z}/d\mathbb{Z}} e^{2\pi i \frac{\mathcal{L}(q)}{d}} \]
and if \( d < 0 \), define
\[ \alpha(g) = (-1)^k \alpha \left( \begin{bmatrix} -a \\ -c \\ -d \end{bmatrix} \right) = (-1)^k \alpha \left( \begin{bmatrix} -1 \\ -1 \end{bmatrix} g \right) \]
Note that \( d \neq 0 \) since \( ad - bc = 1 \) and \( N > 1 \) (by assumption). Our first goal will be to prove that \( \alpha \) takes values in \( \mathbb{Q}^\times \) and is in fact a homomorphism from \( \Gamma_0(N) \) to \( \mathbb{Q}^\times \). Let \( P = 1 \in \mathcal{H}_0(A) \) be the polynomial in \( f \) variables such that \( P(X_1, \ldots, X_f) = 1 \). Let \( g \) be as in (2.18), and assume \( d > 0 \). Then by (2.14) we have
\[ \theta(A,1,0,z)|_{k+g} = \left( \frac{1}{d^k} \sum_{q \in \mathbb{Z}/d\mathbb{Z}} e^{2\pi i \frac{\mathcal{L}(q)}{dN^2}} \right) \cdot \theta(A,1,0,z) \]
CHAPTER 2. CLASSICAL THETA SERIES ON \( \mathbb{H} \)

\[
\begin{align*}
\theta(A, 1, 0, z) & = \left( \frac{1}{\alpha} \sum_{q \in \mathbb{Z}/d \mathbb{Z}} e^{2\pi i \cdot \frac{Q(q)}{d}} \right) \cdot \theta(A, 1, 0, z) \\
& = \left( \frac{1}{\alpha} \sum_{q \in \mathbb{Z}/d \mathbb{Z}} e^{2\pi i \cdot \frac{Q(q)}{d}} \right) \cdot \theta(A, 1, 0, z)
\end{align*}
\]

Thus, \( \theta(A, 1, 0, z) \big|_k g = \alpha(g) \cdot \theta(A, 1, 0, z) \).

Assume that \( d < 0 \). Then by what we just proved,

\[
\begin{align*}
\theta(A, 1, 0, z) \big|_k g & = \theta(A, 1, 0, z) \big|_k \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix} g \\
& = (-1)^k \theta(A, 1, 0, z) \big|_k \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix} g \\
& = (-1)^k \alpha(-g) \theta(A, 1, 0, z) \\
& = \alpha(g) \cdot \theta(A, 1, 0, z).
\end{align*}
\]

Thus,

\[
\theta(A, 1, 0, z) \big|_k g = \alpha(g) \cdot \theta(A, 1, 0, z)
\]

for all \( g \in \Gamma_0(N) \). Since \( \theta(A, 1, 0, z) \) is non-zero, this formula also implies that \( \alpha(g) \neq 0 \) for all \( g \in \Gamma_0(N) \). Thus, \( \alpha \) actually takes values in \( \mathbb{C}^\times \). Let \( g, g' \in \Gamma_0(N) \). Then

\[
\begin{align*}
\theta(A, 1, 0, z) \big|_k (gg') & = \theta(A, 1, 0, z) \big|_{k g'} \\
\alpha(gg') \theta(A, 1, 0, z) & = \alpha(g) \cdot \theta(A, 1, 0, z) \big|_{k g'} \\
\alpha(gg') \theta(A, 1, 0, z) & = \alpha(g) \alpha(g') \theta(A, 1, 0, z).
\end{align*}
\]

Since \( \theta(A, 1, 0, z) \neq 0 \), we have

\[
\alpha(gg') = \alpha(g) \alpha(g') \quad (2.19)
\]

for \( g, g' \in \Gamma_0(N) \). We have already noted that \( \alpha(g) \) is non-zero for all \( g \in \Gamma_0(N) \); we will now show that \( \alpha \) takes values in \( \mathbb{Q}^\times \). To prove this it will suffice to prove that \( \alpha(g) \in \mathbb{Q} \) for \( g \) as in (2.18) with \( d > 0 \). Fix such a \( g \). If \( d = 1 \) then it is clear that \( \alpha(g) \in \mathbb{Q} \). Assume that \( d > 1 \). Then \( c \neq 0 \) (recall that \( ad - bc = 1 \)). Let \( n \) be an integer such that \( nc + d > 0 \). Then

\[
\begin{align*}
\alpha \left( \begin{bmatrix} 1 & n \\ 1 & 1 \end{bmatrix} \right) \alpha(g) & = \alpha \left( \begin{bmatrix} 1 & n \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) \\
& = \alpha \left( \begin{bmatrix} a & an + b \\ c & cn + d \end{bmatrix} \right) \\
1 \cdot \alpha(g) & = \alpha \left( \begin{bmatrix} a & an + b \\ c & cn + d \end{bmatrix} \right) \\
\alpha(g) & = \alpha \left( \begin{bmatrix} a & an + b \\ c & cn + d \end{bmatrix} \right).
\end{align*}
\]

By the definition of \( \alpha \), this implies that

\[
\alpha(g) = \frac{1}{(cn + d)^k} \sum_{q \in \mathbb{Z}/d \mathbb{Z}} e^{2\pi i \cdot \frac{(an + b)Q(q)}{cn + d}}.
\]
2.7. THE CASE $N > 1$

It is clear from this formula that
\[
\alpha(g) \in \mathbb{Q}(\zeta_{nc+d})
\]
where $\zeta_{nc+d} = e^{2\pi i/(nc+d)}$ is a primitive $nc + d$-th root of unity. Assume that $c > 0$. Then $c + d > 0$, and
\[
\alpha(g) \in \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{c+d}).
\]
Since $c$ and $d$ are non-zero and relatively prime (because $ad - bc = 1$), $d$ and $c + d$ are relatively prime. This implies that $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{c+d}) = \mathbb{Q}$, so that $\alpha(g) \in \mathbb{Q}$. Assume that $c < 0$. Then $(-1)c + d > 0$, and
\[
\alpha(g) \in \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{-c+d}).
\]
Since $-c$ and $d$ are non-zero and relatively prime, $d$ and $-c + d$ are relatively prime, and $\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_{-c+d}) = \mathbb{Q}$, so that $\alpha(g) \in \mathbb{Q}$. This completes the argument that $\alpha(g) \in \mathbb{Q}$ for $g \in \Gamma_0(N)$.

Now we prove the claims about $\chi_A$. We need to prove that the four conditions of Lemma 1.1.1 hold for $\chi_A$. It is immediate from the formula for $\chi_A$ that $\chi_A(1) = 1$; this proves the first condition. The third condition, that $\chi_A(d) = 0$ for $d \in \mathbb{Z}$ such that $(d,N) > 1$, follows from the definition of $\chi_A$.

To prove the remaining conditions we first make a connection to $\alpha$. We will prove that if $d \in \mathbb{Z}$ with $(d,N) = 1$, and
\[
g = \left[ \begin{array}{cc} a & b \\ c & d \end{array} \right] \in \Gamma_0(N)
\]
then
\[
\chi_A(d) = \alpha(g).
\]
Assume first that $d > 0$. By definition,
\[
\alpha(g) = \frac{1}{d^k} \sum_{q \in \mathbb{Z}^2/d\mathbb{Z}^2} e^{2\pi i \frac{Q(q)}{d}}
\]
The summands in this formula are contained in $\mathbb{Q}(\zeta_d)$, where $\zeta_d = e^{2\pi i/d}$. Since $(b, d) = 1$, there exists an element $\sigma$ of $\text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ such that $\sigma(\zeta_d) = \zeta_d^b$. We have $\sigma^{-1}(\zeta_d^b) = \zeta_d$. Applying $\sigma^{-1}$ to both sides of the above formula, and using that $\alpha(g) \in \mathbb{Q}$, we obtain:
\[
\alpha(g) = \frac{1}{d^k} \sum_{q \in \mathbb{Z}^2/d\mathbb{Z}^2} e^{2\pi i \frac{Q(q)}{d}}
\]
\[
\alpha(g) = \chi_A(d).
\]
This proves (2.20) for the case $d > 0$. Assume that $d < 0$. Using the previous case, and the definition of $\alpha$, we have:
\[
\chi_A(d) = (-1)^k \chi_A(-d)
\]
Dirichlet character modulo $N$

We have proven that all the conditions of Lemma 1.1.1; by this lemma we have:

$$h \in \mathbb{Z}^d \text{ such that } Z \alpha^0 \equiv 0 \text{ (mod } h).$$

This proves (2.20) in all cases.

Now we will prove the fourth condition of Lemma 1.1.1, which asserts that $\chi_A(d) = \chi_A(d + N)$ for all $d \in \mathbb{Z}$. Let $d \in \mathbb{Z}$. If $(d, N) > 1$, then $(d + N, N) > 1$, and $\chi_A(d) = 0 = \chi_A(d + N)$. Assume that $(d, N) = 1$. Then there exists $a, b \in \mathbb{Z}$ such that $ad - bN = 1$. By (2.20),

$$\alpha\left(\begin{bmatrix} a & b \\ N & d \end{bmatrix} \right) = \alpha\left(\begin{bmatrix} a & b \\ N & d \end{bmatrix}\right) \alpha\left(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\right)$$

$$\chi_A(d + N) = \chi_A(d) \cdot 1$$

To prove the remaining second condition of Lemma 1.1.1 let $d_1, d_2 \in \mathbb{Z}$. If $(d_1, N) > 0$ or $(d_2, N) > 0$, then evidently $\chi_A(d_1d_2) = 0 = \chi_A(d_1)\chi_A(d_2)$. Assume, therefore, that $(d_1, N) = (d_2, N) = 1$. There exist $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ and $\varepsilon_2 \in \{\pm 1\}$ such that be such that $a_1d_1 - b_1N = 1$, $a_2d_2 - b_2\varepsilon_2N = 1$, and $b_2 \geq 0$. Then

$$\chi_A(d_1)\chi_A(d_2) = \chi_A(d_1d_2 + b_2N)$$

$$\chi_A(d_1)\chi_A(d_2) = \chi_A(d_1d_2 + \underbrace{N + \cdots + N}_{b_2})$$

We have proven that all the conditions of Lemma 1.1.1; by this lemma $\chi_A$ is a Dirichlet character modulo $N$. Since (2.20) holds, and since $\alpha(g) \in \mathbb{Q}^\times$ for all $g \in \Gamma_0(N)$, it follows that $\chi_A$ is real-valued.

It remains to prove (2.17). Let

$$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$$

and let $h \in Y(A)$, i.e., $h \in \mathbb{Z}^d$ with $Ah \equiv 0 \text{ (mod } N)$. First assume that $d > 0$. We have:

$$\frac{1}{d^k} \sum_{\substack{q \text{ (mod} \ N) \\ q \equiv h \text{ (mod } N)}} e^{2\pi i \frac{b\nu(q)}{d^k}}$$
2.7. THE CASE \( N > 1 \)

\[
\sum_{q \in \mathbb{Z}^d/d\mathbb{Z}^d, \; q \equiv h \pmod{N}} e^{2\pi i \frac{h \cdot Q(q)}{dN^2}} = \frac{1}{d^k} \sum_{q \in \mathbb{Z}^d/d\mathbb{Z}^d, \; q \equiv ad-h \pmod{N}} e^{2\pi i \frac{h \cdot \Re(Q(q))}{dN^2}} (ad \equiv 1 \pmod{N})
\]

\[
= \frac{1}{d^k} \sum_{q \in \mathbb{Z}^d/d\mathbb{Z}^d, \; q \equiv ad-h \pmod{N}} \sum_{q_1 \in \mathbb{Z}^d/d\mathbb{Z}^d} e^{2\pi i \frac{h \cdot \Re(Q(q)+q_1)}{dN^2}}
\]

\[
= \frac{1}{d^k} \sum_{q_1 \in \mathbb{Z}^d/d\mathbb{Z}^d} e^{2\pi i \frac{h \cdot 2^{d^2}Q(h)+ahdN^2hAm+bN^2Q(m)}{dN^2}}
\]

\[
= \frac{1}{d^k} \cdot e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} \cdot \sum_{m \in \mathbb{Z}^d/d\mathbb{Z}^d} e^{2\pi i \frac{h \cdot \Re(Q(m))}{N}} e^{2\pi i \frac{h \cdot \Re(Q(m))}{d}}
\]

\[
= e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} \cdot \frac{1}{d^k} \cdot \sum_{m \in \mathbb{Z}^d/d\mathbb{Z}^d} e^{2\pi i \frac{h \cdot \Re(Q(m))}{d}} (ad = 1 + bc, N|c, \text{Lemma 1.5.8})
\]

\[
= e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} \cdot \alpha(g)
\]

\[
= e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} \cdot \chi_A(d) \quad \text{(cf. (2.20))}
\]

In summary, if \( d > 0 \), then

\[
\sum_{q \pmod{dN^2}, \; q \equiv h \pmod{N}} e^{2\pi i \frac{h \cdot \Re(Q(q))}{dN^2}} = \frac{1}{d^k} \sum_{q \equiv h \pmod{N}} e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} \cdot \chi_A(d).
\]

This equality and (2.14) now imply (2.17) if \( d > 0 \). Assume that \( d < 0 \). We then have:

\[
\theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}
= \theta(A, P, h, z)_{k+r} \begin{bmatrix} -1 & -1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}
= (-1)^{k+r} \theta(A, P, h, z)_{k+r} \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}
= (-1)^{k+r} \cdot e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} \cdot \chi_A(-d) \cdot \theta(A, P, (-a)h, z)
= (-1)^{k+r} e^{2\pi i \frac{ah \cdot d^2Q(h)}{N^2}} (-1)^k \cdot \chi_A(d) \cdot (-1)^r \theta(A, P, ah, z) \quad \text{(cf. (2.3))}
\]
\[ = e^{2\pi i \frac{ahQ(h)}{N^2}} \cdot \chi_A(d) \cdot \theta(A, P, ah, z). \]

This completes the proof. \(\square\)

Calculation of \(\chi_A\)

**Lemma 2.7.8.** Let \( p \) be a prime, and let \( \chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times \) be a Dirichlet character modulo \( p \). We define the **Gauss sum** \( W(\chi) \) to be the complex number

\[ W(\chi) = \sum_{a=0}^{p-1} \chi(a)e^{2\pi i \frac{a}{p}} = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}}. \]

If \( \chi \) is trivial, then \( W(\chi) = 0 \). If \( \chi \) is non-trivial, then

\[ W(\chi)W(\bar{\chi}) = \chi(-1)p. \]

**Proof.** Let \( G \) be a finite group. In this proof we will the following fact:

If \( \eta \in \text{Hom}(G, \mathbb{C}^\times) \) and \( \eta \not= 1 \), then \( \sum_{g \in G} \eta(g) = 0. \) (2.21)

Assume that \( \chi = 1 \). Consider the function \( \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^\times \) defined by \( a \mapsto e^{2\pi i \frac{a}{p}} \). This function is a non-trivial element of \( \text{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{C}^\times) \). The assertion \( W(\chi) = 0 \) follows from (2.21).

Next, assume that \( \chi \) is non-trivial. In the following computation, if \( b \in (\mathbb{Z}/p\mathbb{Z})^\times \), then we will denote the inverse of \( b \) in \( (\mathbb{Z}/p\mathbb{Z})^\times \) by \( b' \), so that \( bb' = 1 \). We have

\[ W(\chi)W(\bar{\chi}) = \left( \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}} \right) \cdot \left( \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(b)e^{2\pi i \frac{b}{p}} \right) \]

\[ = \left( \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}} \right) \cdot \left( \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(b^{-1})e^{2\pi i \frac{b}{p}} \right) \]

\[ = \left( \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}} \right) \cdot \left( \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(b')e^{2\pi i \frac{b'}{p}} \right) \]

\[ = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(ab')e^{2\pi i \frac{ab'}{p}} \]

\[ = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(ab')e^{2\pi i \frac{ab'}{p}} \]

\[ = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{(a+1)b}{p}} \]

\[ = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} e^{2\pi i \frac{(a+1)b}{p}} \]

\[ = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) \left( -1 + \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \frac{(a+1)b}{p}} \right) \]
2.7. THE CASE $N > 1$

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)( -1 + \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \frac{(a+1)b}{p}} ) + \sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \not\equiv 0 \pmod{p}} \chi(a)( -1 + \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \frac{(a+1)b}{p}} )$$

$$= \chi(-1)( -1 + p ) + \sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \not\equiv 0 \pmod{p}} \chi(a)( -1 + 0 ) \quad \text{(cf. (2.21))}$$

$$= \chi(-1)(p-1) - \sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \not\equiv 0 \pmod{p}} \chi(a)$$

$$= \chi(-1)(p-1) - ( - \chi(-1) + \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) )$$

$$= \chi(-1)(p-1) - ( - \chi(-1) + 0 ) \quad \text{(cf. (2.21))}$$

$$= p\chi(-1).$$

This completes the proof.

Lemma 2.7.9. Let $f$ be a positive even integer, and define $k = f/2$. Let $A \in M(f,\mathbb{Z})$ be an even symmetric positive-definite matrix, and let $N$ be the level of $A$. Assume that $N > 1$. We recall from Lemma 1.5.4 that $N$ divides $\det(A)$, and that $\det(A)$ and $N$ have the same set of prime divisors. Define $\chi_A : \mathbb{Z} \to \mathbb{C}$ as in Lemma 2.7.7; by this lemma, $\chi_A$ is a Dirichlet character modulo $N$. Let $\Delta = \Delta(A) = (-1)^k \det(A)$ be the discriminant of $A$. Let $(\Delta)$ be the Kronecker symbol from section 1.4, which is a Dirichlet character modulo $\det(A)$ by Proposition 1.4.2 and Lemma 1.5.2. Then the diagram

$$(\mathbb{Z}/\det(A)\mathbb{Z})^\times \quad \xrightarrow{\chi_A} \quad (\mathbb{Z}/N\mathbb{Z})^\times$$

commutes. We have

$$\chi_A(d) = \left( \frac{\Delta}{d} \right) = \left( \frac{(-1)^k \det(A)}{d} \right) \quad \text{(2.22)}$$

for $d \in \mathbb{Z}$.

Proof. By Lemma 1.5.4, $N$ divides $\det(A)$, and $\det(A)$ and $N$ have the same set of prime divisors. To prove the assertions of this lemma it will suffice to prove that $\chi_A(d) = (\Delta)$ for $d \in \mathbb{Z}$ with $(d,N) = 1$. Let $d \in \mathbb{Z}$ with $(d,N) = 1$; then $(d,\det(A)) = 1$. By Dirichlet’s theorem about infinitely many primes in arithmetic progressions (see, for example, Theorem 155 on p. 125 of [14]), there
exists an odd prime \( p \) such that \( p \equiv d \pmod{\det(A)} \). Then \((p, N) = 1\) and \( p \equiv d \pmod{N} \). Regard \( A \) as an element of \( M(f, \mathbb{Z}/p\mathbb{Z}) \). We have \( \det(A) \in (\mathbb{Z}/p\mathbb{Z})^\times \). It follows that there exists a matrix \( U \in M(f, \mathbb{Z}) \) and \( a_1, \ldots, a_f \in \mathbb{Z} \) such that \((a_1, p) = \cdots = (a_f, p) = 1\), \((\det(U), p) = 1\), and

\[
{U}^t A U \equiv \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_f \end{bmatrix} \pmod{p}.
\]

We have

\[
\chi_A(d) = \chi_A(p)
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{Q(m)}{p}}
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{Q(2m)}{p}}
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{4^i m A m}{p}}
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2^i m A m}{p}}
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2^i U(m) A(U(m))}{p}}
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2^i U(A) U(m)}{p}}
\]

\[
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2(a_1 m_1^2 + \cdots + a_f m_f^2)}{p}}
\]

\[
= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2a_i m_i^2}{p}}
\]

\[
= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2a_i m_i}{p}} + \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{m_i}{p} \right) e^{2\pi i \cdot \frac{2a_i m_i}{p}} \right)
\]

\[
= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{m_i}{p} \right) e^{2\pi i \cdot \frac{2a_i m_i}{p}} \quad \text{(cf. (2.21))}
\]

\[
= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{2a_i m_i}{p} \right) e^{2\pi i \cdot \frac{m_i}{p}}
\]
2.7. THE CASE $N > 1$

$$\frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \frac{2a_i}{p} \right) \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{m_i}{p} \right) e^{2\pi i \frac{m_i}{p}}$$

$$= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \frac{2a_i}{p} \right) W \left( \frac{1}{p} \right)$$

$$= \frac{W \left( \frac{1}{p} \right)^k}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \frac{2a_i}{p} \right)$$

$$= \left( \frac{W \left( \frac{1}{p} \right)^k}{p^k} \right) \cdot \left( \frac{2^f a_1 \cdots a_f}{p} \right)$$

$$= \left( \frac{W \left( \frac{1}{p} \right)^k}{p^k} \right) \cdot \left( \frac{2^f \det(U)^2 \det(A)}{p} \right)$$

$$= \left( \frac{(-1)^k \det(A)}{p} \right) \cdot \left( \frac{\det(A)}{p} \right)$$

$$= \left( \frac{\Delta}{p} \right) \cdot \left( \frac{\Delta}{d} \right)$$

This completes the proof. \qed

**Theorem 2.7.10.** Let $f$ be a positive even integer, and define $k = f/2$. Let $A \in \text{M}(f, \mathbb{Z})$ be an even symmetric positive-definite matrix, and let $N$ be the level of $A$. Define the quadratic form $Q(x)$ in $f$ variables by

$$Q(x) = \frac{1}{2} x A x.$$ 

Let $r$ be a non-negative integer, and let $P \in \mathcal{H}_r(A)$. Let $h \in \mathbb{Z}^f$ be such that

$$Ah \equiv 0 \pmod{N}.$$ 

The analytic function $\theta(A, P, h, z)$ on $\mathbb{H}_1$ defined by

$$\theta(A, P, h, z) = \sum_{m \in \mathbb{Z}^f \atop m \equiv 0 \pmod{N}} P(n) e^{2\pi i \frac{Q(m)}{N}}$$

for $z \in \mathbb{H}_1$ from Lemma 2.4.1 is a modular form of weight $k + r$ with respect to $\Gamma(N)$. If $r > 0$, then $\theta(A, P, h, z)$ is a cusp form.

**Proof.** The case $N = 1$ is Proposition 2.5.1. We may thus assume that $N > 1$. Let

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(N).$$
Then $\alpha \in \Gamma_0(N)$. By (2.17), we have
\[
\theta(A, P, h, z)|_{k+r, \alpha} = e^{2\pi i \frac{abQ(h)}{N}} \cdot \chi_A(d) \cdot \theta(A, P, ah, z).
\]
Since $\alpha \in \Gamma(N)$ we have $a \equiv d \equiv 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$. By Lemma 2.7.7, $\chi_A$ is a Dirichlet character modulo $N$; hence, $\chi_A(d) = 1$. By Lemma 1.5.8, $Q(h) \equiv 0 \pmod{N}$. Hence, $e^{2\pi i \frac{abQ(h)}{N}} = 1$. Since $a \equiv 1 \pmod{N}$, we see that $ah \equiv h \pmod{N}$; by (2.2), this implies that $\theta(A, P, ah, z) = \theta(A, P, h, z)$. We now have
\[
\theta(A, P, h, z)|_{k+r, \alpha} = \theta(A, P, h, z).
\]
To prove that $\theta(A, P, h, z)$ is a modular form of weight $k + r$ with respect to $\Gamma(N)$ we still need to prove that $\theta(A, P, h, z)$ is holomorphic at the cusps of $\Gamma(N)$, as defined in section 1.8. Clearly, $N$ is the smallest positive integer $M$ such that $\Gamma(M) \subset \Gamma(N)$. To prove that $\theta(A, P, h, z)$ is holomorphic at the cusps of $\Gamma(N)$, and is a cusp form if $r > 0$, it will suffice to prove that for each $\sigma \in \text{SL}(2, \mathbb{Z})$ there exists a power series
\[
\sum_{m=0}^{\infty} a(m)q^m
\]
that converges in $D(1) = \{ q \in \mathbb{C} : |q| < 1 \}$ such that
\[
\theta(A, P, h, z)|_{k+r, \sigma} = \sum_{m=0}^{\infty} a(m)e^{2\pi im/N}
\]
for $z \in \mathbb{H}_1$, and $a(0) = 0$ if $r > 0$. Let
\[
\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}).
\]
We recall the set $Y(A) = \{ g \in \mathbb{Z}^f : Ag \equiv 0 \pmod{N} \}$, and the finite-dimensional vector space $V(A, P)$ spanned by the theta series $\theta(A, P, g, z)$ for $g \in Y(A)/\mathbb{N}\mathbb{Z}^f$ from Lemma 2.4.1. By Lemma 2.4.1 the vector space $V(A, P)$ is preserved by $\text{SL}(2, \mathbb{Z})$ under the $|_{k+r}$ action. It follows that there exist constants $c(g) \in \mathbb{C}$ for $g \in Y(A)/\mathbb{N}\mathbb{Z}^f$ such that
\[
\theta(A, P, g, z)|_{k+r, \sigma} = \sum_{g \in Y(A)/\mathbb{N}\mathbb{Z}^f} c(g) \cdot \theta(A, P, g, z).
\]
(2.23)
Let $g \in Y(A)$. By Lemma 1.5.8, for every $n \in \mathbb{Z}^f$ with $n \equiv g \pmod{N}$, the number $Q(n)/N$ is a non-negative integer. Consequently, we may consider the power series
\[
\sum_{n \in \mathbb{Z}^f, n \equiv g \pmod{N}} P(n)q^{\frac{Q(n)}{N}}
\]
(2.24)
2.8. EXAMPLE: THE QUADRATIC FORM $X_1^2 + X_2^2 + X_3^2 + X_4^2$

In the complex variable $q$. Let $q \in D(1)$. There exists $z \in \mathbb{H}_1$ such that $q = e^{2\pi iz/N}$. Since

$$\sum_{n \in \mathbb{Z}^f \atop n \equiv g \pmod{N}} P(n)q^\frac{Q(n)}{N} = \sum_{n \in \mathbb{Z}^f \atop n \equiv g \pmod{N}} P(n)e^{2\pi iz^N} = \theta(A, P, g, z)$$

converges absolutely by Lemma 2.4.1, it follows that the power series (2.24) converges absolutely at $q$. Hence, the radius of convergence of (2.24) is at least 1. Consequently, the radius of convergence of the finite linear combination of power series

$$\sum_{g \in Y(A)/NZ^f} c(g) \sum_{n \in \mathbb{Z}^f \atop n \equiv g \pmod{N}} P(n)q^\frac{Q(n)}{N}$$

(2.25)

is also at least 1. Denote this power series by

$$\sum_{m=0}^\infty a(m)q^m.$$ 

By construction,

$$\theta(A, P, h, z)|_{k+r, \sigma} = \sum_{m=0}^\infty a(m)e^{2\pi im/N}$$

for $z \in \mathbb{H}_1$. This proves that $\theta(A, h, P, z)$ is a modular form of weight $k + r$ with respect to $\Gamma(N)$. Finally, assume that $r > 0$; we need to prove that $a(0) = 0$. From above,

$$a(0) = \sum_{g \in Y(A)/NZ^f} c(g) \sum_{n \in \mathbb{Z}^f \atop n \equiv g \pmod{N}} P(n)$$

$$= \sum_{g \in Y(A)/NZ^f} c(g) \sum_{n \in \mathbb{Z}^f \atop n \equiv g \pmod{N}} P(n)$$

$$= c(0)P(0)$$

$$= c(0) \cdot 0$$

$$= 0.$$ 

Here, $P(0) = 0$ because $P$ is a homogeneous polynomial in $r > 0$ variables.  \( \square \)

2.8 Example: the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$

In this example we let

$$A = \begin{bmatrix} 2 & 0 & 2 & 2 \\ 0 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix}$$
so that
\[ Q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2. \]

Evidently,
\[ N = 4 \quad \text{and} \quad k = 2. \]

Also, \( \chi_A \) is the trivial character of \((\mathbb{Z}/4\mathbb{Z})^\times\). We will simplify the notation for \( \theta(A, 1, h, z) \) for \( h \in Y(A) \), and write:
\[ \theta(h) = \theta(A, 1, h, z). \]

Let \( V \) be the \( \mathbb{C} \) vector space spanned the \( \theta(h) \) for \( h \in Y(A) \):
\[ V = \langle \theta(h) : h \in Y(A) \rangle. \]

By Theorem 2.7.10, we have \( V \subset M_2(\Gamma(4)) \). If \( h \in \mathbb{Z}^4 \), then \( h \in Y(A) \) if and only if \( Ah \equiv 0 \pmod{4} \), i.e., \( h \equiv 0 \pmod{2} \). Define the following elements of \( Y(A) \):
\[
\begin{align*}
h_0 &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, &
    h_1 &= \begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, &
    h_2 &= \begin{bmatrix} 2 \\ 2 \\ 0 \\ 0 \end{bmatrix}, &
    h_3 &= \begin{bmatrix} 2 \\ 2 \\ 2 \\ 0 \end{bmatrix}, &
    h_4 &= \begin{bmatrix} 2 \\ 2 \\ 2 \\ 2 \end{bmatrix}.
\end{align*}
\]

The vector space \( V \) is spanned by the five modular forms
\[ \theta(h_0), \quad \theta(h_1), \quad \theta(h_2), \quad \theta(h_3), \quad \theta(h_4). \]

For \( z \in \mathbb{H}_1 \), define
\[ q_4 = e^{2\pi i z/4}. \]

We have:
\[
\begin{align*}
\theta(h_0) &= \sum_{m \in \mathbb{Z}^4} q_4^{4m_1^2 + 4m_2^2 + 4m_3^2 + 4m_4^2}, \\
\theta(h_1) &= \sum_{m \in \mathbb{Z}^4} q_4^{(2m_1+1)^2 + 4m_2^2 + 4m_3^2 + 4m_4^2}, \\
\theta(h_2) &= \sum_{m \in \mathbb{Z}^4} q_4^{(2m_1+1)^2 + (2m_2+1)^2 + 4m_3^2 + 4m_4^2}, \\
\theta(h_3) &= \sum_{m \in \mathbb{Z}^4} q_4^{(2m_1+1)^2 + (2m_2+1)^2 + (2m_3+1)^2 + 4m_4^2}, \\
\theta(h_4) &= \sum_{m \in \mathbb{Z}^4} q_4^{(2m_1+1)^2 + (2m_2+1)^2 + (2m_3+1)^2 + (2m_4+1)^2}.
\end{align*}
\]

Calculations show that:
\[
\begin{align*}
\theta(h_0) &= 1 + 8q_4^4 + 24q_4^8 + 32q_4^{12} + 24q_4^{16} + 48q_4^{20} + \cdots, \\
\theta(h_1) &= 2q_4 + 12q_4^2 + 26q_4^3 + 28q_4^5 + 36q_4^7 + 64q_4^9 + \cdots.
\end{align*}
\]
2.8. EXAMPLE: THE QUADRATIC FORM $X_1^2 + X_2^2 + X_3^2 + X_4^2$

$\theta(h_2) = 4q_4^2 + 16q_4^6 + 24q_4^{10} + 32q_4^{14} + 52q_4^{18} + 48q_4^{22} + \cdots$

$\theta(h_3) = 8q_4^3 + 16q_4^7 + 24q_4^{11} + 48q_4^{15} + 40q_4^{19} + 48q_4^{23} + \cdots$

$\theta(h_4) = 16q_4^4 + 64q_4^{12} + 96q_4^{20} + 128q_4^{28} + 208q_4^{36} + 192q_4^{44} + \cdots$

These expansions show that $\theta(h_0), \ldots, \theta(h_4)$ are linearly independent, so that

$$\dim \mathbb{C} V = 5.$$

**Lemma 2.8.1.** We have

$$\dim M_2(\Gamma_0(2)) = 1 \quad \text{and} \quad \dim M_2(\Gamma_0(4)) = 2.$$

**Proof.** See, for example, Proposition 1.40 on page 23, Proposition 1.43 on page 24, and Theorem 2.23 on page 46 of [26].

**Proposition 2.8.2.** Let

$$V_1 = \langle \theta(h_0) + \theta(h_4), \theta(h_2) \rangle, \quad V_2 = \langle \theta(h_0) - \theta(h_4), \theta(h_1), \theta(h_3) \rangle,$$

so that

$$V = V_1 \oplus V_2.$$

Then $V_1$ and $V_2$ are irreducible $\text{SL}(2, \mathbb{Z})$ subspaces of $V$. Moreover,

$$M_2(\Gamma_0(4)) = \langle \theta(h_0), \theta(h_4) \rangle,$n

$$M_2(\Gamma_0(2)) = \langle \theta(h_0) + \theta(h_4) \rangle.$$

**Proof.** By (2.4) we have

$$\begin{align*}
\theta(h_0) &= -\frac{1}{4}(\theta(h_0) + 4 \cdot \theta(h_1) + 6 \cdot \theta(h_2) + 4 \cdot \theta(h_3) + \theta(h_4)), \\
\theta(h_1) &= -\frac{1}{4}(\theta(h_0) + 2 \cdot \theta(h_1) - 2 \cdot \theta(h_3) - \theta(h_4)), \\
\theta(h_2) &= -\frac{1}{4}(\theta(h_0) - 2 \cdot \theta(h_2) + \theta(h_4)), \\
\theta(h_3) &= -\frac{1}{4}(\theta(h_0) - 2 \cdot \theta(h_1) + 2 \cdot \theta(h_3) - \theta(h_4)), \\
\theta(h_4) &= -\frac{1}{4}(\theta(h_0) - 4 \cdot \theta(h_1) + 6 \cdot \theta(h_2) - 4 \cdot \theta(h_3) + \theta(h_4)).
\end{align*}$$

By (2.5) we have:

$$\begin{align*}
\theta(h_0) &= \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \theta(h_0), \\
\theta(h_1) &= \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = i \theta(h_1),
\end{align*}$$

$$\begin{align*}
\theta(h_2) &= \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \theta(h_2), \\
\theta(h_3) &= \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \theta(h_3), \\
\theta(h_4) &= \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \theta(h_4).
\end{align*}$$
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

$$\theta(h_2)\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = -\theta(h_2),$$
$$\theta(h_3)\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = -i\theta(h_3),$$
$$\theta(h_4)\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \theta(h_4).$$

Since $\text{SL}(2, \mathbb{Z})$ is generated by
$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$
the above equations imply that $V_1$ and $V_2$ are $\text{SL}(2, \mathbb{Z})$ subspaces of $V$.

To see that $V_1$ is irreducible as an $\text{SL}(2, \mathbb{Z})$ space, let $W \subset V_1$ be a $\text{SL}(2, \mathbb{Z})$ subspace. We need to prove that $W = 0$ or $W = V_1$, and to prove this it suffices to prove that $\text{dim } W \neq 1$. Assume that $\text{dim } W = 1$; we will obtain a contradiction. Let $a, b \in \mathbb{C}$ be such that $F_1 = a(\theta(h_0) + \theta(h_4)) + b\theta(h_2)$ is a basis for $W$. Since $W$ is one-dimensional, $\text{SL}(2, \mathbb{Z})$ acts on $W$ by a character $\beta : \text{SL}(2, \mathbb{Z}) \to \mathbb{C}^\times$. $F_1$ is fixed by $\text{SL}(2, \mathbb{Z})$. Now
$$F_1\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \beta(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix})F_1$$
$$a(\theta(h_0) + \theta(h_4)) - b\theta(h_2) = a\beta(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix})(\theta(h_0) + \theta(h_4)) + b\beta(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix})\theta(h_2).$$

This equality implies that $a = 0$ or $b = 0$. If $a = 0$ and $b \neq 0$, then
$$\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}$$
show that $W$ can contain at most one of $\theta(h_0) - \theta(h_4)$, $\theta(h_1)$ and $\theta(h_3)$; otherwise, $W = V_2$, a contradiction. Consider the quotient $V_2/W$. This $\text{SL}(2, \mathbb{Z})$ space is one-dimensional. Hence, $\text{SL}(2, \mathbb{Z})$ acts on $V_2/W$ by a character $\delta : \text{SL}(2, \mathbb{Z}) \to \mathbb{C}^\times$. Let $p : V_2 \to V_2/W$ be the projection map. We have
$$F_1\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$
2.8. EXAMPLE: THE QUADRATIC FORM $X_1^2 + X_2^2 + X_3^2 + X_4^2$

imply that

$$p(\theta(h_0) - \theta(h_4)) = \delta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} p(\theta(h_0) - \theta(h_4)),$$

$$ip(\theta(h_1)) = \delta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} p(\theta(h_1)),$$

$$-ip(\theta(h_3)) = \delta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} p(\theta(h_3)).$$

Since at least two of $p(\theta(h_0) - \theta(h_4))$, $p(\theta(h_1))$, and $p(\theta(h_3))$ are non-zero, these equations imply that

$$\delta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

is equal to at least two distinct elements of $\{1, i, -i\}$, a contradiction. Thus, $V_2$ is irreducible.

By Lemma 2.8.1 we have $\dim M_2(\Gamma_0(4)) = 2$ and $\dim M_2(\Gamma_0(2)) = 1$. By Lemma 2.7.7 and Theorem 2.7.10, the functions $\theta(h_0)$ and $\theta(h_4)$ are contained in $M_2(\Gamma_0(4))$. Since $\theta(h_0)$ and $\theta(h_4)$ are linearly independent, $\theta(h_0)$ and $\theta(h_4)$ form a basis for $M_2(\Gamma_0(4))$. Finally, we need to prove that

$$F = \theta(h_0) + \theta(h_4)$$

is contained in $M_2(\Gamma_0(2))$. It will suffice to prove that

$$F|_{\gamma} = F$$

for $\gamma \in \Gamma_0(2)$ for $\gamma \in \Gamma_0(2)$. We begin with some preliminary calculations. Let $h \in Y(A)$; we write $h = 2h'$ for some $h' \in \mathbb{Z}^4$. Let

$$\alpha = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}.$$

By (2.13),

$$\theta(h)|_2 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} = \frac{1}{i^k 2^2 \sqrt{\det(A)}} \sum_{g \in Y(A)/4\mathbb{Z}^4} s_{\alpha}(g, h) \theta(g)$$

$$= \frac{1}{-2^4} \sum_{g \in Y(A)/4\mathbb{Z}^4} s_{\alpha}(g, h) \theta(g).$$

Let $g \in Y(A)$, and write $g = 2g'$ for some $g' \in \mathbb{Z}^4$. We obtain

$$s_{\alpha}(g, h) = \sum_{\substack{x \in \mathbb{Z}^4/4\mathbb{Z}^4 \\ x \equiv h \pmod{4}}} e^{2\pi i \frac{Q(x) + hAx + Q(g)}{4}}$$

$$= e^{2\pi i \frac{Q(g)}{4}} \sum_{\substack{x \in \mathbb{Z}^4/4\mathbb{Z}^4 \\ x \equiv h \pmod{4}}} e^{2\pi i \frac{Q(x) + hAx}{4}}$$
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

\[\begin{align*}
\theta(h) &= e^{2\pi i \left( \frac{Q(h)}{32} \right)} \sum_{y \in \mathbb{Z}^4/2\mathbb{Z}^4} e^{2\pi i \left( \frac{Q(h) + 2^{\frac{1}{4}}(g+h)y + 16Q(y)}{32} \right)} \\
&= e^{2\pi i \left( \frac{Q(h)}{32} \right)} \sum_{y \in \mathbb{Z}^4/2\mathbb{Z}^4} e^{2\pi i \left( \frac{Q(h) + 2^{\frac{1}{4}}(g+h)y + 16Q(y)}{32} \right)} \\
&= e^{2\pi i \left( \frac{Q(h)}{32} \right)} \sum_{y \in \mathbb{Z}^4/2\mathbb{Z}^4} e^{2\pi i \left( \frac{8^{\frac{1}{4}}(g+h)y + 16Q(y)}{32} \right)} \\
&= e^{2\pi i \left( \frac{Q(h)}{32} \right)} \sum_{y \in \mathbb{Z}^4/2\mathbb{Z}^4} e^{2\pi i \left( \frac{8^{\frac{1}{4}}(g+h)y + 16Q(y)}{32} \right)} \\
&= e^{2\pi i \left( \frac{Q(h)}{32} \right)} \sum_{y \in \mathbb{Z}^4/2\mathbb{Z}^4} e^{2\pi i \left( \frac{8^{\frac{1}{4}}(g+h)y + 16Q(y)}{32} \right)}.
\end{align*}\]

The function $\mathbb{Z}^4/2\mathbb{Z}^4 \to \mathbb{C}^\times$ defined by

\[y \mapsto e^{2\pi i \left( \frac{(g'+h')y + Q(y)}{2} \right)}\]

is a homomorphism. This homomorphism is trivial if and only if every entry of $g' + h'$ is odd, or equivalently, $g + h \equiv h_4 \pmod{4}$. Therefore,

\[s_\alpha(g, h) = e^{2\pi i \left( \frac{Q(g+h)}{32} \right)} \sum_{y \in \mathbb{Z}^4/2\mathbb{Z}^4} e^{2\pi i \left( \frac{(g'+h')y + Q(y)}{2} \right)} \]

\[s_\alpha(g, h) = \begin{cases} 
-2^4 & \text{if } g + h \equiv h_4 \pmod{4}, \\
0 & \text{if } g + h \not\equiv h_4 \pmod{4}.
\end{cases}\]

Consequently,

\[\theta(h) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \frac{1}{-2^4} \sum_{g \in Y(A)/4\mathbb{Z}^4} s_\alpha(g, h) \theta(g) = \theta(h_4 - h).\]

This implies that:

\[\theta(h_0) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \theta(h_4),\]
\[\theta(h_1) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \theta(h_3),\]
\[\theta(h_2) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \theta(h_2),\]
\[\theta(h_3) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \theta(h_1),\]
2.8. EXAMPLE: THE QUADRATIC FORM $X_1^2 + X_2^2 + X_3^2 + X_4^2$

$$\theta(h_4)|_2 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} = \theta(h_0).$$

Since $F \in M_2(\Gamma_0(4))$, to prove that $F|_{2\gamma} = F$ for $\gamma \in \Gamma_0(2)$, it will suffice to prove that $F|_{2\gamma} = F$ for $\gamma \in \Gamma_0(2)$ of the form

$$\gamma = \begin{bmatrix} a & b \\ 2c & d \end{bmatrix}$$

where $c$ is an odd integer; we note that since $ad - 2bc = 1$, $d$ is also odd. Let $\gamma \in \Gamma_0(2)$ have this form. Then

$$F|_{2\gamma} = \theta(h_0)|_{2\gamma} + \theta(h_4)|_{2\gamma}$$

$$= \theta(h_0)|_{2\gamma} \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \theta(h_4)|_{2\gamma} \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$

$$= \theta(h_0)|_{2\gamma} \begin{bmatrix} a - 2b \\ 2(c - d) \\ 2c + d \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \theta(h_4)|_{2\gamma} \begin{bmatrix} a - 2b \\ 2(c - d) \\ 2c + d \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$

$$= \theta(h_0)|_{2\gamma} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \theta(h_4)|_{2\gamma} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} (c - d \text{ is even})$$

$$= \theta(h_4) + \theta(h_0)$$

$$= F.$$

This proves our claim about $F$. \hfill \Box

**Proposition 2.8.3** (Jacobi’s four square theorem). If $n$ is a positive integer, then the number of $(x, y, z, w) \in \mathbb{Z}^4$ such

$$x^2 + y^2 + z^2 + w^2 = n$$

is

$$8 \cdot \sum_{m > 0, \gcd(m, n) \neq 0, (m \equiv 0 \mod 4)} m.$$ 

In particular, every positive integer is a sum of four squares.

**Proof.** We have

$$\theta(h_0, z) = \sum_{n=0}^{\infty} a(n)q^n$$

where

$$a(n) = \# \{m \in \mathbb{Z}^4 : Q(m) = n \}$$

for each non-negative integer $n$. The modular form $\theta(h_0, z)$ is contained in $M_2(\Gamma_0(4))$. By Lemma 2.8.1, the dimension of $M_2(\Gamma_0(4))$ is two, and the dimension of $M_2(\Gamma_0(2))$ is one. The vector space $M_2(\Gamma_0(2))$ is spanned by

$$E(z) = \frac{1}{24} + \sum_{n=1}^{\infty} b(n)q^n$$
where \( q = e^{2\pi iz} \) for \( z \in \mathbb{H}_1 \); here, for positive integers \( n \),

\[
b(n) = \begin{cases} 
\sigma_1(n) - 2\sigma_1(n/2) & \text{if } n \text{ is even,} \\
\sigma_1(n) & \text{if } n \text{ is odd.}
\end{cases}
\]

For this, see Theorem 5.8 on page 88 of [27]. Trivially, the function \( E(z) \) is contained in \( M_2(\Gamma_0(4)) \). The function

\[
E(z) \bigg|_2 \begin{bmatrix} 2 \\ 1 \end{bmatrix} = E(2z)
\]

is also contained in \( M_2(\Gamma_0(4)) \). We have

\[
E(2z) = \frac{1}{24} + \sum_{n=1}^{\infty} c(n)q^n
\]

where

\[
c(n) = \begin{cases} 
\sigma_1(n/2) - 2\sigma_1(n/4) & \text{if } n \text{ is divisible by 4,} \\
\sigma_1(n/2) & \text{if } n \text{ is even and } n/2 \text{ is odd,} \\
0 & \text{if } n \text{ is odd}
\end{cases}
\]

for positive integers \( n \). The two modular forms \( E(z) \) and \( E(2z) \) form a basis for \( M_2(\Gamma_0(4)) \). Hence, there exist \( c_1, c_2 \in \mathbb{C} \) such that

\[
\theta(h_0, z) = c_1 \cdot E(z) + c_2 \cdot E(2z).
\]

Calculations show that

\[
\theta(h_0, z) = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + 48q^5 + 96q^6 + 64q^7 + \cdots,
\]

\[
E(z) = \frac{1}{24} + q + q^2 + 4q^3 + q^4 + 6q^5 + 4q^6 + 8q^7 + \cdots,
\]

\[
E(2z) = \frac{1}{24} + q^2 + q^4 + 4q^6 + q^8 + 6q^{10} + 4q^{12} + \cdots.
\]

Using these expansions to solve for \( c_1 \) and \( c_2 \), we find that:

\[
\theta(h_0, z) = 8 \cdot E(z) + 16 \cdot E(2z).
\]

It follows that

\[
a(n) = 8b(n) + 16c(n)
\]

\[
= \begin{cases} 
8\sigma_1(n) - 32\sigma_1(n/4) & \text{if } 4 \mid n, \\
8\sigma_1(n) & \text{if } n \text{ is even and } n/2 \text{ is odd,} \\
8\sigma_1(n) & \text{if } n \text{ is odd,}
\end{cases}
\]

\[
= 8 \cdot \sum_{\substack{m > 0, m \mid n, \\
m \not\equiv 0 \pmod{4}}} m.
\]

This completes the proof. \( \square \)
Chapter 3

Classical theta series on $\mathbb{H}_n$

3.1 Convergence

Let $m$ and $n$ be positive integers. If $A \in M(m, \mathbb{C})$ and $X \in M(m \times n, \mathbb{C})$, then we define

$$A[X] = ^tXAX.$$ 

Lemma 3.1.1. Let $m$ and $n$ be positive integers, and let $A \in M(m, \mathbb{Z})$ be an even positive-definite symmetric integral matrix. For every $N \in M(m \times n, \mathbb{Z})$ the $n \times n$ integral matrix $A[N]$ is an even positive semi-definite symmetric matrix.

Proof. Let $N \in M(m \times n, \mathbb{Z})$. Set $B = A[N]$. It is clear that $B$ is integral and symmetric. Let $x \in \mathbb{R}^n$. Then $^txBx = ^t(Nx)A(Nx) \geq 0$. It follows that $B$ is positive semi-definite. \hfill \box

Assume that $A \in M(m, \mathbb{Z})$ and $B \in M(n, \mathbb{Z})$ are even symmetric integral matrices. Assume further that $A$ is positive-definite, and that $B$ is positive semi-definite. We say that $A$ represents $B$ if there exists $N \in M(m \times n, \mathbb{Z})$ such that

$$A[N] = B.$$ 

We let

$$r(A, B) = \# \{ N \in M(m \times n, \mathbb{Z}) : A[N] = B \}.$$ 

Lemma 3.1.2. Let $m$ and $n$ be positive integers, and let $A \in M(m, \mathbb{Z})$ and $B \in M(n, \mathbb{Z})$ be even symmetric integral matrices with $A$ positive-definite and $B$ positive semi-definite. The set $\{ N \in M(m \times n, \mathbb{Z}) : A[N] = B \}$ is finite, so that $r(A, B)$ is a non-negative integer.

Proof. By §1.5, there exists $T \in \text{GL}(m, \mathbb{R})$ and positive numbers $\lambda_1, \ldots, \lambda_m$
such that $^tT = T$ and
\[
D = ^tTAT = \begin{bmatrix}
\lambda_1 \\
\lambda_2 \\
\lambda_3 \\
\vdots \\
\lambda_m
\end{bmatrix}.
\]

Define Let $N \in M(m \times n, \mathbb{Z})$. We have $A[N] = B$ if and only if $D[TN] = B$. Write $TN = [(TN)_1 \cdots (TN)_n]$ where $(TN)_1, \ldots, (TN)_n \in \mathbb{R}^m$ are column vectors. We have
\[
B_{jj} = (^t(TN)_jD(TN))_j = \sum_{i=1}^{m} \lambda_i(TN)_{ij}^2
\]
for $1 \leq j \leq n$. Let $S$ be the set of $X \in M(m \times n, \mathbb{R})$ such that
\[
B_{jj} = \sum_{i=1}^{m} \lambda_i X_{ij}^2
\]
for $1 \leq j \leq n$. It follows that $\{N \in M(m \times n, \mathbb{Z}) : A[N] = B\}$ is contained in $T^{-1}S \cap M(m \times n, \mathbb{Z})$. The set $S$ is compact, so that $T^{-1}S$ is also compact. Since $T^{-1}S$ is compact and $M(m \times n, \mathbb{Z})$ is a discrete subset of $M(m \times n, \mathbb{R})$, the set $T^{-1}S \cap M(m \times n, \mathbb{Z})$ is finite. \hfill \qed

**Lemma 3.1.3.** Let $n$ be a positive integer. Let $S, T \in M(n, \mathbb{R})$ be positive semi-definite symmetric matrices. Then $\text{tr}(ST) \geq 0$.

**Proof.** Arguing as before (1.7), there exist positive semi-definite symmetric matrices $U, V \in M(n, \mathbb{R})$ such that $S = U^2$ and $T = V^2$. Now
\[
\text{tr}(ST) = \text{tr}(UUVV) = \text{tr}(VVUV) = \text{tr}(^t(V)^tUUV) = \text{tr}(^t(UV)UV).
\]

Let $W = UV$. Then
\[
\text{tr}(ST) = \text{tr}(^tWW) = \sum_{k=1}^{n} \left( \sum_{j=1}^{n} ^t(W)_{kj}W_{jk} \right) = \sum_{k=1}^{n} \left( \sum_{j=1}^{n} W_{jk}W_{jk} \right) = \sum_{k=1}^{n} \left( \sum_{j=1}^{n} W_{jk}^2 \right)
\]
3.1. CONVERGENCE

\[ \geq 0. \]

This completes the proof. \(\square\)

**Lemma 3.1.4.** Let \( K \) be a compact subset of \( \text{Sym}(n, \mathbb{R}) \). Assume that \( S > 0 \) for \( S \in K \). Then there exists \( \delta > 0 \) such that \( S - \delta > 0 \) for all \( S \in K \).

**Proof.** Let \( S \in K \). Since \( S \) is positive-definite, there exists \( T \in \text{GL}(n, \mathbb{R}) \) such that \( TT = T^T T = 1 \) and

\[
A = T^T \begin{bmatrix}
\lambda_1 \\
\lambda_2 \\
\lambda_3 \\
\vdots \\
\lambda_n
\end{bmatrix} T
\]

for some positive numbers \( \lambda_1, \ldots, \lambda_n \in \mathbb{R} \). Let \( \epsilon_S > 0 \) be a positive number such and \( \lambda_1 > \epsilon_S, \ldots, \lambda_n > \epsilon_S \). Let \( x \in \mathbb{R}^n \) with \( x \neq 0 \). Then

\[
T^x (S - \epsilon_S) x = T^x \begin{bmatrix}
\lambda_1 \\
\lambda_2 \\
\lambda_3 \\
\vdots \\
\lambda_n
\end{bmatrix} T x - \epsilon_S T^x x
\]

\[
= (T x) \begin{bmatrix}
\lambda_1 - \epsilon_S \\
\lambda_2 - \epsilon_S \\
\lambda_3 - \epsilon_S \\
\vdots \\
\lambda_n - \epsilon_S
\end{bmatrix} T x
\]

\[ > 0. \]

It follows that \( S - \epsilon_S > 0 \). Hence, \( S \in \epsilon_S + \text{Sym}(n, \mathbb{R})^+ \). By Lemma 1.10.1, set \( \text{Sym}(n, \mathbb{R})^+ \) is open in \( \text{Sym}(n, \mathbb{R}) \). The sets \( \epsilon_S + \text{Sym}(n, \mathbb{R})^+ \) form an open cover for \( K \). Since \( K \) is compact, this cover has a finite subcover \( \text{Sym}(n, \mathbb{R})^+ + \epsilon_{S_1}, \ldots, \text{Sym}(n, \mathbb{R})^+ + \epsilon_{S_k} \) for some \( S_1, \ldots, S_k \in K \). Let \( \delta = \min(\epsilon_{S_1}, \ldots, \epsilon_{S_k}) \). Now let \( S \in K \). Then \( S \in \text{Sym}(n, \mathbb{R})^+ + \epsilon_{S_i} \) for some \( i \in \{1, \ldots, k\} \). Hence, \( S - \epsilon_{S_i} \in \text{Sym}(n, \mathbb{R})^+ \). This implies that \( S - \epsilon_{S_i} > 0 \), so that \( S > \epsilon_{S_i} \geq \delta \), as desired. \(\square\)

**Lemma 3.1.5.** Let \( m \) and \( n \) be positive integers. Let \( M, N \in \text{M}(m \times n, \mathbb{R}) \). Then

\[
|\text{tr}(T^M N)| \leq \sum_{i=1}^n ||M_i|| ||N_i||.
\]

Here, for \( P \in \text{M}(m \times n, \mathbb{R}) \), we write \( P = [P_1 \cdot \cdots \cdot P_n] \), where \( P_i \in \mathbb{R}^m \) for \( 1 \leq i \leq n \) are column vectors.
Proof. We have

\[|\text{tr}(^tMN)| = |\text{tr}[^t[M_1 \cdots M_n][N_1 \cdots N_n]|] = \sum_{i=1}^n |^tM_iN_i| \leq \sum_{i=1}^n \|M_i\|\|N_i\|,\]

where in the last step we used the Cauchy-Schwarz inequality. \qed

**Lemma 3.1.6.** Let \( k \) be a positive integer, and let \( \delta > 0 \) and \( M > 0 \) be positive real numbers. Then there exists positive numbers \( R > 0 \) and \( \epsilon > 0 \) such that if \( x_1 \geq 0, \ldots, x_k \geq 0 \) and

\[x_1^2 + \cdots + x_k^2 \geq R,\]

then

\[-\delta(x_1^2 + \cdots + x_k^2) + 2M(x_1 + \cdots + x_k) + M \leq -\epsilon(x_1^2 + \cdots + x_k^2).\]

Proof. Let \( \epsilon \) be any positive number such that \( 0 < \epsilon < \delta \). Let \( m \in \mathbb{R} \) be such that

\[m \leq (\delta - \epsilon)x^2 - 2Mx - M\]

for all \( x \in \mathbb{R} \). There exists a positive number \( T \) such that if \( x \geq T \), then

\[-(k - 1)m \leq (\delta - \epsilon)x^2 + 2Mx - M.\]

Now define \( R = T^2k \). Assume that \( x_1 \geq 0, \ldots, x_k \geq 0 \) and \( x_1^2 + \cdots + x_k^2 \geq R \). Then for some \( i \in \{1, \ldots, k\} \) we have \( x_i^2 \geq R/k \), i.e., \( x_i \geq \sqrt{R/k} = T \). It follows that

\[(\delta - \epsilon)(x_1^2 + \cdots + x_k^2) - 2M(x_1 + \cdots + x_k) - M \geq (\delta - \epsilon)x_i^2 - 2Mx_i - M + (k - 1)m \geq -(k - 1)m + (k - 1)m \geq 0.\]

This completes the proof. \qed

**Lemma 3.1.7.** Let \( m \) and \( n \) be positive integers, and let \( A \in M(m, \mathbb{R}) \) be a positive-definite symmetric matrix. Let \( K \) be a compact subset of \( \mathbb{H}_n \), and let \( K_1 \) and \( K_2 \) be compact subsets of \( M(m \times n, \mathbb{C}) \). There exists a positive real number \( R > 0 \) and a positive constant \( \epsilon \) such that such that

\[
\text{Re}(\pi tr(ZA[N - Y])) + 2\pi \text{tr}(^tNX) - \pi \text{tr}(^tXY)) \leq -\epsilon \sum_{i=1}^n \|N_i\|^2
\]
for $Z \in K$, $X \in K_1$, $Y \in K_2$ and $N \in M(m \times n, \mathbb{R})$ with
\[
\sum_{i=1}^{n} \|N_i\|^2 \geq R.
\]
Here, for $N \in M(m \times n, \mathbb{R})$, we write $N = [N_1 \cdots N_n]$, where $N_i \in \mathbb{R}^m$ for $1 \leq i \leq n$ are column vectors.

**Proof.** We first prove that we may assume that $A = 1$. To see this, assume that the assertion holds for $1 = 1_m$. Since $A$ is positive-definite, there exists a positive-definite symmetric matrix $B \in M(n, \mathbb{R})$ such that $A = B^2$ (see (1.7)). Define $K'_1 = B^{-1}(K_1)$ and $K'_2 = B(K_2)$. Since we are assuming that the assertion holds for $1 = 1_m$, there exists a positive real number $R > 0$ and a positive constant $\epsilon$ such that
\[
\text{Re} (\pi i \tr (Z^t (N' - Y')(N' - Y'))) + 2\pi i \tr (\bar{N}' X') - \pi i \tr (\bar{X}' Y') \leq -\epsilon \cdot \sum_{i=1}^{n} \|N'_i\|^2
\]
for $Z \in K$, $X' \in K'_1 = B(K_1)$, $Y' \in B^{-1}(K_2)$ and $N' \in M(m \times n, \mathbb{R})$ with
\[
\sum_{i=1}^{n} \|N'_i\|^2 \geq R.
\]
Regard the matrix $B^{-1}$ as operator from $\mathbb{R}^m$ to $\mathbb{R}^m$. Then $B$ is continuous and hence bounded. Therefore, there exists a positive constant $\|B^{-1}\|$ such that
\[
\|B^{-1}(g)\| \leq \|B^{-1}\| \|g\|
\]
for $g \in \mathbb{R}^m$. Define $T = \|B^{-1}\|^2R$. Let $N \in M(m \times n, \mathbb{R})$ with
\[
\sum_{i=1}^{n} \|N_i\|^2 \geq T.
\]
Define $N' = BN$. Then
\[
\sum_{i=1}^{n} \|N'_i\|^2 = \sum_{i=1}^{n} \|(BN)_i\|^2 = \sum_{i=1}^{n} \|BN_i\|^2 \geq \sum_{i=1}^{n} \|B^{-1}\|^{-2} \|B^{-1}\|^2 \|BN_i\|^2 \geq \sum_{i=1}^{n} \|B^{-1}\|^{-2} \|B^{-1}BN_i\|^2 = \sum_{i=1}^{n} \|B^{-1}\|^{-2} \|N_i\|^2
\]
CHAPTER 3. CLASSICAL THETA SERIES ON $\mathbb{H}_N$

$$= \|B^{-1}\|^{-2} \sum_{i=1}^{n} \|N_i\|^2$$

$$\geq \|B^{-1}\|^{-2} T$$

$$= R.$$

Let $Z \in K$, $X \in K_1$ and $Y \in K_2$. Then $X' = B^{-1}(X) \in K'_1$ and $Y' = B(Y) \in K'_2$. Since

$$\text{Re}(\pi \tr(Z'(N' - Y')(N' - Y'))) + 2\pi \tr(\imath N' X' - \pi \tr(\imath X' Y'))$$

$$= \text{Re}(\pi \tr(Z'(BN - BY)(BN - BY)) + 2\pi \tr(\imath (BN)B^{-1}X)$$

$$- \pi \tr(\imath (B^{-1}X)BY))$$

$$= \text{Re}(\pi \tr(Z'(N - Y)BB(N - Y)) + 2\pi \tr(\imath NX) - \pi \tr(\imath XY))$$

$$= \text{Re}(\pi \tr(Z'(N - Y)A(N - Y)) + 2\pi \tr(\imath NX) - \pi \tr(\imath XY))$$

$$= \text{Re}(\pi \tr(ZA[N - Y]) + 2\pi \tr(\imath NX) - \pi \tr(\imath XY)),$$

and,

$$-\epsilon \cdot \sum_{i=1}^{n} \|N'_i\|^2 = -\epsilon \cdot \sum_{i=1}^{n} \|BN_i\|^2$$

$$= -\epsilon \cdot \sum_{i=1}^{n} \|B^{-1}\|^{-2}\|B^{-1}\|^2 \|BN_i\|^2$$

$$\leq -\epsilon \cdot \sum_{i=1}^{n} \|B^{-1}\|^{-2} \|N_i\|^2$$

$$= -\epsilon \|B^{-1}\|^{-2} \sum_{i=1}^{n} \|N_i\|^2.$$

we conclude that

$$\text{Re}(\pi \tr(ZA[N - Y]) + 2\pi \tr(\imath NX) - \pi \tr(\imath XY)) \leq -\epsilon \|B^{-1}\|^{-2} \sum_{i=1}^{n} \|N_i\|^2.$$

It follows that we may assume that $A = 1 = 1_m$.

We now prove the lemma for $A = 1 = 1_m$. Since $K$, $K_1$ and $K$ are compact, there exists a positive number $M > 0$ such that

$$\|(V Y_1 + U Y_2 - \imath X_2)\| \leq M, \quad \text{for } 1 \leq i \leq n,$$

$$|\tr(\imath X_1 Y_2 + \imath X_2 Y_1 - U(\imath Y_1 Y_2 + \imath Y_2 Y_1)) - V(\imath Y_1 Y_1 + \imath Y_2 Y_2)| \leq M$$

for $Z = U + iV \in K$, $X = X_1 + iX_2 \in K_1$ and $Y = Y_1 + iY_2 \in K_2$ where $U, V, X_1, X_2, Y_1$ and $Y_2$ are real matrices. By Lemma 3.1.4 there exists $\delta > 0$ such that $\text{Im}(Z) - \delta > 0$ for all $Z \in K$. Let $N \in M(m \times n, \mathbb{R})$. Then $\imath N N \geq 0$. 
3.1. CONVERGENCE

Hence, by Lemma 3.1.3, we have \(\text{tr}(\text{Im}(Z) - \delta^1NN) \geq 0\) for \(N \in M(m \times n, \mathbb{R})\), or equivalently,

\[-\text{tr}(\text{Im}(Z)^1NN) \leq -\delta \text{tr}^1NN\text{ for } N \in M(m \times n, \mathbb{R}).\]  \hfill (3.1)

Let \(Z \in K\), \(X \in K_1\) and \(Y \in K_2\). Write \(Z = U + iV\) for \(U, V \in M(n \times n, \mathbb{R})\) with \(U = U\), \(V = V\), and \(V > 0\). Also, write \(X = X_1 + iX_2\) and \(Y = Y_1 + iY_2\) for \(X_1, X_2, Y_1, Y_2 \in M(m \times n, \mathbb{R})\). We have

\[
\pi^{-1}\text{Re}(\pi \text{tr}(Z^1(N - Y)(N - Y)) + 2\pi \text{tr}(^1NX) - \pi \text{tr}(^1XY)) \\
= -\pi^{-1}\text{Im}(\pi \text{tr}(Z^1(N - Y)(N - Y)) + 2\pi \text{tr}(^1NX) - \pi \text{tr}(^1XY)) \\
= -\text{tr}(V^1NN) + 2\text{tr}(V^1Y_1N) + 2\text{tr}(U^1Y_2N) - 2\text{tr}(^1NX_2) \\
+ \text{tr}(^1X_1Y_2 + ^1X_2Y_1 - U(^1Y_1Y_2 + ^1Y_2Y_1)) - V(^1Y_1Y_1 + ^1Y_2Y_2)) \\
= -\text{tr}(V^1NN) + 2\text{tr}(V^1Y_1 + U^1Y_2 - ^1X_2)N \\
+ \text{tr}(^1X_1Y_2 + ^1X_2Y_1 - U(^1Y_1Y_2 + ^1Y_2Y_1)) - V(^1Y_1Y_1 + ^1Y_2Y_2)) \\
\leq -\delta \text{tr}(^1NN) + 2\text{tr}(V^1Y_1 + U^1Y_2 - ^1X_2)N | \\
+ |\text{tr}(^1X_1Y_2 + ^1X_2Y_1 - U(^1Y_1Y_2 + ^1Y_2Y_1)) - V(^1Y_1Y_1 + ^1Y_2Y_2))| \\
= -\delta \sum_{i=1}^n \|N_i\|^2 + 2\text{tr}(V^1Y_1 + U^1Y_2 - ^1X_2)N | \\
+ |\text{tr}(^1X_1Y_2 + ^1X_2Y_1 - U(^1Y_1Y_2 + ^1Y_2Y_1)) - V(^1Y_1Y_1 + ^1Y_2Y_2))| \\
\leq -\delta \sum_{i=1}^n \|N_i\|^2 + 2M \sum_{i=1}^n \|N_i\| + M.
\]

By Lemma 3.1.6, there exists positive numbers \(R > 0\) and \(\epsilon > 0\) such that

\[-\delta \sum_{i=1}^n \|N_i\|^2 + 2M \sum_{i=1}^n \|N_i\| + M \leq -\epsilon \sum_{i=1}^n \|N_i\|^2\]

for

\[\sum_{i=1}^n \|N_i\|^2 \geq R.\]

This completes the proof. \(\square\)

**Proposition 3.1.8.** Let \(m\) and \(n\) be positive integers, and let \(A \in M(m, \mathbb{R})\) be a positive-definite symmetric matrix. For \(Z \in \mathbb{H}_n\), \(X, Y \in M(m \times n, \mathbb{C})\), define

\[
\theta(A, Z, X, Y) = \sum_{N \in M(m \times n, \mathbb{Z})} \exp \left( \pi \text{tr}(ZA[N - Y]) + 2\pi \text{tr}(^1NX) - \pi \text{tr}(^1XY) \right).
\]
If $D$, $D_1$ and $D_2$ are products of closed disks in $C$ such that $D \subset \mathbb{H}_n$ and $D_1, D_2 \subset M(m \times n, \mathbb{C})$, then the series $\theta(A, Z, X, Y)$ converges absolutely and uniformly on $D \times D_1 \times D_2$. The resulting function $\theta(A, Z, X, Y)$ defined on $\mathbb{H}_n \times M(m \times n, \mathbb{C}) \times M(m \times n, \mathbb{C})$ is analytic in each complex variable.

Proof. Let $D$, $D_1$ and $D_2$ be products of closed disks in $C$ such that $D \subset \mathbb{H}_n$ and $D_1, D_2 \subset M(m \times n, \mathbb{C})$. By there exists a positive real number $R > 0$ and a positive constant $\epsilon$ such that such that

$$\text{Re}(\pi i \text{tr}(ZA[N - Y]) + 2\pi i \text{tr}(^tNX) - \pi i \text{tr}(^tXY)) \leq -\epsilon \cdot \sum_{i=1}^{n} ||N_i||^2$$

for $Z \in D$, $X \in D_1$, $Y \in D_2$ and $N \in M(m \times n, \mathbb{R})$ with

$$\sum_{i=1}^{n} ||N_i||^2 \geq R.$$

Hence,

$$|\exp(\pi i \text{tr}(ZA[N - Y]) + 2\pi i \text{tr}(^tNX) - \pi i \text{tr}(^tXY))| = \exp(\text{Re}(\pi i \text{tr}(ZA[N - Y]) + 2\pi i \text{tr}(^tNX) - \pi i \text{tr}(^tXY)))$$

$$\leq \exp(-\epsilon \cdot \sum_{i=1}^{n} ||N_i||^2)$$

for $Z \in D$, $X \in D_1$, $Y \in D_2$ and all but finitely many $N \in M(m \times n, \mathbb{Z})$. The series

$$\sum_{N \in M(m \times n, \mathbb{Z})} \exp(-\epsilon \cdot \sum_{i=1}^{n} ||N_i||^2)$$

converges. The Weierstrass $M$-test (see [17], p. 160) now implies that the series $\theta(A, Z, X, Y)$ converges absolutely and uniformly on $D \times D_1 \times D_2$. Since for each $N \in M(m \times n, \mathbb{Z})$ the function on $\mathbb{H}_n \times M(m \times n, \mathbb{C}) \times M(m \times n, \mathbb{C})$ defined by

$$(Z, X, Y) \mapsto \exp(\pi i \text{tr}(ZA[N - Y]) + 2\pi i \text{tr}(^tNX) - \pi i \text{tr}(^tXY))$$

is an analytic function in each complex variable and since our series converges absolutely and uniformly on all products of closed disks, the function $\theta(A, Z, X, Y)$ is analytic in each variable (see [17], p. 162).

**Corollary 3.1.9.** Let $m$ and $n$ be positive integers, and let $A \in M(m, \mathbb{Z})$ be an even positive-definite symmetric integral matrix. For $Z \in \mathbb{H}_n$, define

$$\theta(A, Z) = \sum_{N \in M(m \times n, \mathbb{Z})} \exp(\pi i \text{tr}(A[N]Z)).$$

If $D$ is a product of closed disks in $C$ such that $D \subset \mathbb{H}_n$ then the series $\theta(A, Z)$ converges absolutely and uniformly on $D$. The resulting function $\theta(A, Z)$ defined
on $\mathbb{H}_n$ is analytic in each complex variable. Moreover,
\[
\theta(A, Z) = \sum_{B \in \text{Sym}(n, Z)_{\text{even}}, B \geq 0} r(A, B) \exp(\pi i \text{tr}(BZ)).
\]

### 3.2 The Eicher lemma

Let $k$ be a positive integer. For $Z \in \mathbb{H}_k$, $R \in M(k, 1, \mathbb{R})$, and $X, Y \in M(k, 1, \mathbb{C})$ define
\[
g(Z, R, X, Y) = \exp(\pi i \langle R - Y \rangle Z(R - Y) + 2\pi i \langle RX \rangle - \pi i \langle XY \rangle) \tag{3.2}
\]

**Lemma 3.2.1.** Let $k$ be a positive integer, $U \in \text{Sym}(k, \mathbb{R})^+$ and $X, Y \in M(k, 1, \mathbb{C})$. The function $g(iU, \cdot, X, Y)$ is contained in the Schwartz space
\[
S(M(k, 1, \mathbb{R})) = S(\mathbb{R}^k)
\]
(see section 2.2 for the definition of the Schwartz space).

**Proof.** Write $X = X_1 + iX_2$ and $Y = Y_1 + iY_2$ for $X_1, X_2, Y_1, Y_2 \in M(k, 1, \mathbb{R})$. Also, write $U = V^2$ for some $V \in \text{Sym}(k, \mathbb{R})^+$ (see (1.7)). Since $\exp(-\pi i \langle XY \rangle)$ is constant, it suffices to prove that the function defined by
\[
R \mapsto \exp(-\pi i \langle R - Y \rangle U(R - Y) + 2\pi i \langle RX \rangle)
\]
is contained $S(M(k, 1, \mathbb{R}))$. Since $S(M(k, 1, \mathbb{R}))$ is mapped to itself by the map induced by $R \mapsto R + Y_2$, we may assume that our function has the form
\[
R \mapsto \exp(-\pi i \langle R - iY_2 \rangle U(R - iY_2) + 2\pi i \langle RX \rangle)
\]
Let $R \in M(k, 1, \mathbb{R})$. Then
\[
\exp(-\pi i \langle R - Y \rangle U(R - Y) + 2\pi i \langle RX \rangle)
= \exp(-\pi i \langle R - iY_2 \rangle V(R - iY_2) + 2\pi i \langle RX \rangle)
= \exp(-\pi i \langle VR - iY_2 \rangle (VR - iY_2) + 2\pi i \langle RX \rangle).
\]
Since $S(M(k, 1, \mathbb{R}))$ is mapped to itself by the map induced by $R \mapsto V^{-1}R$, we may assume that our function has the form
\[
R \mapsto \exp(-\pi i \langle R - iY_2 \rangle (R - iY_2) + 2\pi i \langle RX \rangle)
\]
For $R \in M(k, 1, \mathbb{R})$ we have:
\[
\exp(-\pi i \langle R - iY_2 \rangle (R - iY_2) + 2\pi i \langle RX \rangle)
= \exp(-\pi i \langle RR - 2\pi iRX_2 + \pi i Y_2 \rangle + i(2\pi i RX_1 + \pi i Y_2 + \pi i Y_2 R)).
\]
Since $\exp(\pi i Y_2 Y_2)$ is constant, we see that it suffices to prove that the function $h : M(k, 1, \mathbb{R}) \to \mathbb{C}$ defined by
\[
h(R) = \exp(-\pi i \langle RR - 2\pi iRX_2 + i(2\pi i RX_1 + \pi i Y_2 + \pi i Y_2 R))
\]
is contained $S(M(k, 1, \mathbb{R})).$ Let $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{Z}_{\geq 0}^k$ and $P(X_1, \ldots, X_k) \in \mathbb{C}[X_1, \ldots, X_k];$ we need to prove that $|P(R)(D^\alpha h)(R)|$ is bounded as a function of $R \in M(k, 1, \mathbb{R}).$ To see this, we note that there exists a polynomial $Q_\alpha(X_1, \ldots, X_k) \in \mathbb{C}[X_1, \ldots, X_k]$ such that

$$(D^\alpha h)(R) = Q_\alpha(R)h(R).$$

for $R \in M(k, 1, \mathbb{R}).$ For $R \in M(k, 1, \mathbb{R})$ we have

$$|P(R)(D^\alpha h)(R)| = |P(R)Q_\alpha(R)\exp\left(-\pi^4 RR - 2\pi^4 RX_2\right)|$$

$$= |P(R)Q_\alpha(R)\exp\left(-\pi^4 (R + X_2)(R + X_2) - \pi^4 X_2 X_2\right)|$$

$$= |\exp(-\pi^4 X_2 X_2)P(R)Q_\alpha(R)\exp\left(-\pi^4 (R + X_2)(R + X_2)\right)|.$$  \hspace{1cm} (3.3)

It is well-known that the function

$$R \mapsto \exp\left(-\pi^4 RR\right)$$

is contained $S(M(k, 1, \mathbb{R})).$ As above, this implies that

$$\exp\left(-\pi^4 (R + X_2)(R + X_2)\right)$$

is also contained $S(M(k, 1, \mathbb{R})).$ This implies that (3.3) is bounded. \hfill \square

**Lemma 3.2.2.** Let $k$ be a positive integer. Let $U \in \text{Sym}(k, \mathbb{R})^+$ and $X, Y \in M(k, 1, \mathbb{C}).$ The Fourier transform (see section 2.2) of the Schwartz function $g(iU, \cdot, X, Y)$ is given by

$$\mathcal{F}(g(iU, \cdot, X, Y))(R) = \det(U)^{-1/2}g(-iU)^{-1}, -R, Y, -X).$$

**Proof.** Let $R \in M(k, 1, \mathbb{R}).$ We recall that for $Z \in \mathbb{H}_k$, the function $g$ is given by:

$$g(Z, R, X, Y) = \exp \left(\pi i \frac{1}{1} (R - Y)Z(R - Y) + 2\pi i \frac{1}{1} RX - \pi i \frac{1}{1} XY\right).$$

Therefore,

$$\mathcal{F}(g(iU, \cdot, X, Y))(R)$$

$$= \int_{\mathbb{R}^k} \exp \left(-\pi \frac{1}{1} (r - Y)U(r - Y) + 2\pi i \frac{1}{1} rX - \pi i \frac{1}{1} XY\right) \exp(-2\pi i \frac{1}{1} r) \, dr$$

$$= \exp(-\pi \frac{1}{1} X Y) \int_{\mathbb{R}^k} \exp \left(-\pi \left[\frac{1}{1} (r - Y)U(r - Y) - 2\pi i \frac{1}{1} rX + 2\pi i \frac{1}{1} Rd\right]\right) \, dr.$$
For the penultimate equality, we used Lemma 2.2. Therefore, we obtain:

\[
\begin{align*}
\det(U)^{-1/2} \exp(-\pi \frac{1}{r}VY(VY)(VY)) \int_{\mathbb{R}^k} \exp \left( -\pi \left[ \frac{1}{r}rr + 2 \frac{1}{r}rQ \right] \right) dr \\
= \det(U)^{-1/2} \exp(-\pi \frac{1}{r}UY) \int_{\mathbb{R}^k} \exp \left( -\pi \left[ \frac{1}{r}rr + 2 \frac{1}{r}rQ + \frac{1}{r}QQ - \frac{1}{r}QQ \right] \right) dr \\
= \det(U)^{-1/2} \exp(-\pi \frac{1}{r}UY + \pi \frac{1}{r}QQ) \int_{\mathbb{R}^k} \exp \left( -\pi \left[ \frac{1}{r}(r + Q)(r + Q) \right] \right) dr \\
= \det(U)^{-1/2} \exp(-\pi \frac{1}{r}UY + \pi \frac{1}{r}QQ) \int_{\mathbb{R}^k} \exp(-\pi \frac{1}{r}rr) dr \\
= \det(U)^{-1/2} \exp(-\pi \frac{1}{r}UY + \pi \frac{1}{r}QQ).
\end{align*}
\]

For the penultimate equality, we used Lemma 2.2. Therefore,

\[
\mathcal{F}(g(iU, \cdot, X, Y))(R) = \det(U)^{-1/2} \exp(-\pi i \frac{1}{r}XY) \exp(-\pi \frac{1}{r}YY + \pi \frac{1}{r}QQ) \\
= \det(U)^{-1/2} \exp(-\pi \frac{1}{r}XY - \pi \frac{1}{r}XV^{-1}W^{-1}X + \pi \frac{1}{r}RV^{-1}W^{-1}X \\
+ \pi \frac{1}{r}YV^{-1}X - \pi \frac{1}{r}YY + \pi \frac{1}{r}XY - \pi \frac{1}{r}RV^{-1}W^{-1}R \\
+ \pi \frac{1}{r}XX^{-1}YY - \pi \frac{1}{r}RV^{-1}W^{-1}R - i\pi \frac{1}{r}RV^{-1}YY.
\]

\[Q = -YY + \frac{1}{r}V^{-1}(-X + R) = -YY - i\frac{1}{r}V^{-1}X + i\frac{1}{r}V^{-1}R.\]
\[ -i\pi Y^t V^t V^{-1}R + \pi Y^t VVY \]
\[ = \det(U)^{-1/2} \exp \left( -i\pi Y^t XY - \pi Y^t UX^{-1}X + \pi Y^t RU^{-1}X \right. \]
\[ + i\pi Y^t UY + \pi Y^t UX^{-1}X \]
\[ + i\pi Y^t YX - \pi Y^t RU^{-1}X - i\pi Y^t Y \]
\[ - i\pi Y^t R + \pi Y^t YUY \]
\[ = \det(U)^{-1/2} \exp \left( -\pi \left[ Y^t UX^{-1}X - Y^t RU^{-1}X + Y^t UX^{-1}X + Y^t RU^{-1}X \right] \right) \]
\[ - 2i\pi Y^t RY + i\pi Y^t YX \]
\[ = \det(U)^{-1/2} \exp \left( -\pi \left[ (R - X)U^{-1}(R - X) \right] \right) \]
\[ - 2i\pi Y^t RY - i\pi Y^t Y(-X) \]
\[ = \det(U)^{-1/2} \exp \left( \pi i \left[ (R - X)(-iU)^{-1}(R - X) \right] \right) \]
\[ - 2i\pi Y^t RY - i\pi Y^t Y(-X) \]
\[ = \det(U)^{-1/2} \exp \left( \pi i \left[ -(R - (-X))(-(iU)^{-1})(R - (-X)) \right] \right) \]
\[ + 2i\pi Y^t (-R)Y - i\pi Y^t Y(-X) \]
\[ = \det(U)^{-1/2} g(-iU)^{-1}, -R, Y, -X. \]

This completes the proof. \qed
Appendix A

Some tables

A.1 Tables of fundamental discriminants

| $-3 = -3$ | $-35 = (-7) \cdot 5$ | $-68 = (-4) \cdot 17$ |
| $-4 = -4$ | $-39 = (-3) \cdot 13$ | $-71 = -71$ |
| $-7 = -7$ | $-40 = (-8) \cdot 5$ | $-79 = -79$ |
| $-8 = -8$ | $-43 = -43$ | $-83 = -83$ |
| $-11 = -11$ | $-47 = -47$ | $-84 = (-4) \cdot (-3) \cdot (-7)$ |
| $-15 = (-3) \cdot 5$ | $-51 = (-3) \cdot 17$ | $-87 = (-3) \cdot 29$ |
| $-19 = -19$ | $-52 = (-4) \cdot 13$ | $-88 = (-11) \cdot 8$ |
| $-20 = (-4) \cdot 5$ | $-55 = (-11) \cdot 5$ | $-91 = (-7) \cdot 13$ |
| $-23 = -23$ | $-56 = (-7) \cdot 8$ | $-95 = (-19) \cdot 5$ |
| $-24 = (-3) \cdot 8$ | $-59 = -59$ | |
| $-31 = -31$ | $-67 = -67$ | |

Table A.1: Negative fundamental discriminants between $-1$ and $-100$, factored into products of prime fundamental discriminants.
Table A.2: Positive fundamental discriminants between 1 and 100, factored into products of prime fundamental discriminants.
Index

A
adjoint ...................... 23

C
congruence subgroup .... 29
cusp form ................. 31

D
determinant .............. 20
Dirichlet character ...... 1
  conductor ............. 3
  induced ............... 3
  Legendre symbol ..... 3
  primitive ............. 3
  principal ............. 2
  product ............... 5
discriminant ........... 21

E
Euclidean domain ....... 33
even integral symmetric matrix 19
  level .................. 25
extension of a Dirichlet character 1

F
Fourier transform ........ 44
fundamental discriminant 6
  prime .................. 6

G
Gauss sum ............... 78

H
Hecke congruence subgroup 29
  holomorphic at the cusps 31

K
Kronecker symbol ....... 16

L
Legendre symbol ........ 3

M
modular form ............ 31

P
positive semi-definite ... 24
positive-definite ........ 24
prime fundamental discriminant .. 6
principal congruence subgroup .. 29

Q
quadratic form .......... 20
  level .................. 25

R
real valued ............... 3
represents ................ 91

S
Schwartz function ....... 43
Schwartz space .......... 44
Siegel upper half-space .. 34
smooth function .......... 43
spherical functions ...... 55
symplectic group ......... 31

V
vanishes at the cusps .... 31
Symbols

\(A > 0\), \(A\) is a positive-definite symmetric real matrix

\(A[X] = \begin{pmatrix} X \end{pmatrix} A [\begin{pmatrix} X \end{pmatrix}]\) for \(A \in M(m, \mathbb{C})\) and \(X \in M(m \times n, \mathbb{C})\)

\(A \geq 0\), \(A\) is a positive semi-definite symmetric real matrix

\(M_k(\Gamma)\), the space of modular forms of weight \(k\) with respect to \(\Gamma\)

\(S_k(\Gamma)\), the space of cusp forms of weight \(k\) with respect to \(\Gamma\)

\(\Gamma(N)\), the principal congruence subgroup

\(\Gamma_0(N)\), the Hecke congruence subgroup

\(\text{Sp}(2n, \mathbb{R})\), the symplectic group of degree \(n\) over \(\mathbb{R}\) (\(2n \times 2n\) matrices)

\(\text{Sym}(m, \mathbb{R})\), the set of \(m \times m\) symmetric matrices over \(\mathbb{R}\)

\(\mathbb{H}_n\), the Siegel upper half-space of degree \(n\)

\(r(A, B)\), the number of ways \(A\) represents \(B\)
Bibliography


