Theta Series

Brooks Roberts

University of Idaho

Course notes as of December 10, 2019, with course completion in May 2019
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 $\mathbb{H}_1$ ...................... 37
  2.1 Definition and convergence .......................... 37
  2.2 The Poisson summation formula ..................... 41
  2.3 Differential operators ............................... 49
  2.4 A space of theta series ............................. 54
  2.5 The case $N = 1$ ..................................... 58
  2.6 Example: a quadratic form of level one .......... 60
  2.7 The case $N > 1$ ..................................... 62
  2.8 Example: the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ . 81

3 Notes ........................................................... 89
  3.1 ............................................................ 89
  3.2 ............................................................ 89
  3.3 ............................................................ 89
  3.4 ............................................................ 89
  3.5 ............................................................ 89

A Some tables .................................................. 93
  A.1 Tables of fundamental discriminants ............... 93

Index ............................................................ 95

Symbols .......................................................... 97
List of Tables

A.1 Negative fundamental discriminants between $-1$ and $-100$ . . . 93
A.2 Positive fundamental discriminants between 1 and 100 . . . . . 94
Chapter 1

Background

1.1 Dirichlet characters

Let $N$ be a positive integer. A **Dirichlet character** modulo $N$ is a homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times.$$ 

If $N$ is a positive integer and $\chi$ is a Dirichlet character modulo $N$, then we associate to $\chi$ a function

$$\mathbb{Z} \rightarrow \mathbb{C},$$

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 $\chi(a_1 a_2) = \chi(a_1) \chi(a_2)$;
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 $a \in \mathbb{Z}$. 

1
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 \( f(a_1a_2) = f(a_1)f(a_2) \);
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

\[ f(\epsilon) \chi(\epsilon a) = f(a). \]

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 \( \chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times \) by \( \chi(a + N\mathbb{Z}) = f(a) \) 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

\[ (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M\mathbb{Z})^\times, \]

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

\[ (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M\mathbb{Z})^\times \beta \longrightarrow \mathbb{C}^\times. \]

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 \( N_1 | N \) 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 \( N_1 | N \) and \( \chi(a) = 1 \) for \( a \in \mathbb{Z} \) such that \((a, N) = 1 \) and \( a \equiv 1 \pmod{N_1} \). Then \( f(\chi) | N_1 \).
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

$$f(\chi) = p_1^{\ell_1} \cdots p_t^{\ell_t}, \quad N_1 = p_1^{k_1} \cdots p_t^{k_t}.$$

By definition,

$$M = p_1^\min(\ell_1, k_1) \cdots p_t^\min(\ell_t, k_t).$$

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

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

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, $b \equiv 1 \pmod{p_i^{\ell_i}}$ 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 $\chi(a) = \chi(bc) = \chi(b)\chi(c) = 1$.

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.

Evidently, the conductor of $\left(\frac{\cdot}{p}\right)$ is also $p$, so that $\left(\frac{\cdot}{p}\right)$ 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 \( a \equiv 1 \pmod{f(\chi_1)f(\chi_2)} \). Then \( (a, N_1) = (a, N_2) = 1 \), \( a \equiv 1 \pmod{f(\chi_1)} \), and \( a \equiv 1 \pmod{f(\chi_2)} \). 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 \( M_1|f(\chi_1) \) and \( M_2|f(\chi_2) \). 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 \( a \equiv 1 \pmod{M_1} \). By the Chinese remainder theorem, there exists an integer \( b \) such that \( b \equiv a \pmod{M_1} \), \( b \equiv 1 \pmod{f(\chi_2)} \), and \( (b, N_1) = 1 \). Evidently, \( b \equiv 1 \pmod{f(\chi)} \). 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. \( \square \)

**Lemma 1.1.6.** Let \( p \) be an odd prime. The Legendre symbol \( \left( \frac{x}{p} \right) \) is the only real valued primitive Dirichlet character modulo \( p \). If \( e > 1 \) 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 \( e > 1 \) 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 \( \mathbb{Z}/p^e\mathbb{Z}^\times \). 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 \( \mathbb{Z}/p^e\mathbb{Z}^\times \). Since \( \chi \) has conductor \( p^e \), and since \( x + p^e\mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e\mathbb{Z}^\times \), 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 \( \left( \frac{a}{p} \right) = -1 \) for some \( a \in \mathbb{Z} \); since \( x + p^e\mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e\mathbb{Z}^\times \), this implies that \( \left( \frac{\cdot}{p} \right) = -1 \), so that \( \chi(x) = \left( \frac{x}{p} \right) \). Since \( x + p^e\mathbb{Z} \) is a generator of \( \mathbb{Z}/p^e\mathbb{Z}^\times \) 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 \( p^e \). \( \square \)

**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

\[
\varepsilon_4(1) = 1,
\]

\[
\varepsilon_4(3) = -1.
\]
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 \( f(\varepsilon'_{8}) = 8 \). 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 \( n \equiv 1 \pmod{8} \). It is known that there exists \( a \in \mathbb{Z} \) such that \( n \equiv a^{2} \pmod{p^{e}} \). 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.

## 1.2 Fundamental discriminants

Let \( D \) be a non-zero integer. We say that \( D \) is a **fundamental discriminant** if
\[
D \equiv 1 \pmod{4} \quad \text{and} \quad D \text{ is square-free,}
\]
or
\[
D \equiv 0 \pmod{4}, \quad D/4 \text{ is square-free, and } D/4 \equiv 2 \text{ or } 3 \pmod{4}.
\]
We say that \( D \) is a **prime fundamental discriminant** if
\[
D = -8 \quad \text{or} \quad D = -4 \quad \text{or} \quad D = 8,
\]
or
\[
D = -p \quad \text{for } p \text{ a prime such that } p \equiv 3 \pmod{4},
\]
or
\[
D = p \quad \text{for } p \text{ a prime such that } p \equiv 1 \pmod{4}.
\]
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

$$1 \equiv D \pmod{4}$$

$$\equiv (-1)^r \pmod{4}$$

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

It follows that $r$ is odd. Hence,

$$D = - \prod_{p \in \{p_1, \ldots, p_t\}} p$$

$$= - \left( \prod_{p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \equiv 3 \pmod{4}} p \right)$$

$$= \left( \prod_{p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \equiv 3 \pmod{4}} (-p) \right).$$

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

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 $-p_1 \cdots p_t \equiv 2 \pmod{4}$. 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

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

Each of the factors in the last equation is a prime fundamental discriminant, which proves the lemma in this case. Now assume that \(-p_1 \cdots p_t \equiv 3 \ (\text{mod} \ 4)\). 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 \(p \equiv 3 \ (\text{mod} \ 4)\). We have
\[ 3 \equiv -p_1 \cdots p_t \ (\text{mod} \ 4) \]
\[ -1 \equiv (-1)^{3r} \ (\text{mod} \ 4) \]
\[ 1 \equiv (-1)^r \ (\text{mod} \ 4). \]

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

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

Assume that \(D > 0\) and \(D \equiv 1 \ (\text{mod} \ 4)\). 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 \(p \equiv 3 \ (\text{mod} \ 4)\). We have
\[ 1 \equiv D \ (\text{mod} \ 4) \]
\[ \equiv 3^r \ (\text{mod} \ 4) \]
\[ 1 \equiv (-1)^r \ (\text{mod} \ 4). \]

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

$$D = 4 \prod_{p \in \{p_1, \ldots, p_t\}} p,$$

$$D = 8 \prod_{p \in \{p_2, \ldots, p_t\}} p$$

$$= 8 \left( \prod_{p \in \{p_2, \ldots, p_t\}, p \equiv 1 \pmod{4}} p \right) \times \left( \prod_{p \in \{p_2, \ldots, p_t\}, p \equiv 3 \pmod{4}} p \right)$$

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

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

$$3 \equiv p_1 \cdots p_t \pmod{4}$$
$$-1 \equiv 3^r \pmod{4}$$
$$-1 \equiv (-1)^r \pmod{4}$$
$$1 \equiv (-1)^{r+1} \pmod{4}$$

It follows that $r$ is odd. Hence,

$$D = 4 \prod_{p \in \{p_1, \ldots, p_t\}} p$$

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

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

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

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

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. \qed
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,

$$\chi_{-8}(2) = 0.$$ 

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 $D = -4$ 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
\[ \chi_D(p) = \left(\frac{-q}{p}\right) \]
\[ = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) \]
\[ = (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \]
\[ = (-1)^{\frac{p-1}{2}} ((-1)^{\frac{q-1}{2}})^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \]
\[ = (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \]
\[ = (-1)^{p-1} \left(\frac{p}{q}\right) \]
1.2. FUNDAMENTAL DISCRIMINANTS

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

Also,

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

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

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

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

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

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

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

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

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

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

\[
\chi_D(-1) = 1
\]
Since \( \left( \frac{a}{q} \right) \) and \( \chi_D \) are multiplicative, it follows that \( \left( \frac{a}{q} \right) = \chi_D(a) \) for all \( a \in \mathbb{Z} \). Since \( \left( \frac{a}{q} \right) \) is a primitive Dirichlet character modulo \( q \), it follows that \( \chi_D \) corresponds to a primitive Dirichlet character modulo \( q = |q| = |D| \).

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

\[
\chi_D = \begin{cases} 
\varepsilon_8'' & \text{if } D = -8, \\
\varepsilon_4 & \text{if } D = -4, \\
\varepsilon_8' & \text{if } D = 8, \\
\left( \frac{\cdot}{p} \right) & \text{if } D = -p \text{ is a prime with } p \equiv 3 \pmod{4}, \\
\left( \frac{\cdot}{p} \right) & \text{if } D = p \text{ is a prime with } p \equiv 1 \pmod{4}.
\end{cases}
\] (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

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

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

\[ (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \hookrightarrow (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times, \]

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 \( i \in \{1, \ldots, t\} \).
1.3. QUADRATIC EXTENSIONS

Assume first that $p_i$ is odd. Since $\chi_i$ is primitive, Lemma 1.1.6 implies that $e_i = 1$, and that $\chi_i = \left(\frac{p_i}{D_i}\right)$, 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

$$\{\text{quadratic extensions } K \text{ of } \mathbb{Q}\} \xrightarrow{\sim} \{\text{fundamental discriminants } D, D \neq 1\}$$

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:

$$(p) = \begin{cases} p^2 & \text{if } \chi_D(p) = 0, \\ p \cdot p' & \text{if } \chi_D(p) = 1, \\ p & \text{if } \chi_D(p) = -1. \end{cases}$$

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

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

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

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 [24], or Theorem 25 on page 74 of [13].

**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 $\text{disc}(K) = 4 \cdot (D/4) = D$. \(\square\)

### 1.4 Kronecker Symbol

Let $\Delta$ be a non-zero integer such that $\Delta \equiv 0, 1$ or 2 (mod 4). We define a function,

$$\left( \frac{\Delta}{p} \right) : \mathbb{Z} \to \mathbb{C}$$

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

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

Note that, since by assumption $\Delta \equiv 0, 1$ or 2 (mod 4), the cases $\Delta \equiv 3$ (mod 8) and $\Delta \equiv 7$ (mod 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

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

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
\[
\left( \frac{\Delta}{-n} \right) = \left( \frac{\Delta}{-1} \right) \left( \frac{\Delta}{n} \right)
\]
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 \( \left( \frac{\Delta}{a} \right) \left( \frac{1}{a} \right) = 1 \) for \( a \in \mathbb{Z} \). Thus, \( \left( \frac{1}{a} \right) \) is the unique Dirichlet character modulo 1. It is straightforward to verify that
\[
\left( \frac{\Delta}{ab} \right) = \left( \frac{\Delta}{a} \right) \left( \frac{\Delta}{b} \right)
\]
for \( a, b \in \mathbb{Z} \). Also, we note that \( \left( \frac{\Delta}{1} \right) = 0 \) if and only if \( (a, \Delta) > 1 \).

**Lemma 1.4.1.** Let \( D \) be a non-zero integer such that \( D \equiv 1 \pmod{4} \) or \( D \equiv 0 \pmod{4} \). There exists a unique fundamental discriminant \( D_{td} \) and a unique positive integer \( m \) such that
\[
D = m^2 D_{td}.
\]

**Proof.** We first prove the existence of \( m \) and \( D_{td} \). 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 \( D \equiv 1 \pmod{4} \). Since \( a \) is odd, \( a^2 \equiv 1 \pmod{4} \); therefore, \( b \equiv 1 \pmod{4} \). It follows that \( D = m^2 D_{td} \) with \( m = a \) and \( D_{td} = b \) a fundamental discriminant.

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

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

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

To prove the uniqueness assertion, assume that \( m \) and \( m' \) are positive integers and \( D_{td} \) and \( D_{td}' \) are fundamental discriminants such that \( D = m^2 D_{td} = (m')^2 D_{td}' \). Assume first that \( D_{td} = 1 \). Then \( m^2 = (m')^2 D_{td}' \). This implies
that $D'_{fd}$ is a square; hence, $D'_{fd} = 1$. Therefore, $m^2 = (m')^2$, implying that $m = m'$. Now assume that $D_{fd} \neq 1$. Then also $D'_{fd} \neq 1$, and $D$ is not a square. Set $K = \mathbb{Q}(\sqrt{D})$. We have $K = \mathbb{Q}(\sqrt{D_{fd}}) = \mathbb{Q}(\sqrt{D'_{fd}})$. By Lemma 1.3.2, $\text{disc}(K) = D_{fd}$ and $\text{disc}(K) = D'_{fd}$, so that $D_{fd} = D'_{fd}$. 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 $2 \pmod{4}$. Define

\[
D = \begin{cases} 
\Delta & \text{if } \Delta \equiv 0 \text{ or } 1 \pmod{4}, \\
4\Delta & \text{if } \Delta \equiv 2 \pmod{4}.
\end{cases}
\]

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

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

\[
(Z/\vert D\vert \mathbb{Z})^\times \longrightarrow (Z/\vert D_{fd}\vert \mathbb{Z})^\times \xrightarrow{\chi_{D_{fd}}} \mathbb{C}^\times,
\]

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

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

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

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

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

\[
= \left(\frac{m^2 D_{fd}}{p}\right)
\]

\[
= \left(\frac{D_{fd}}{p}\right)
\]

\[
= \chi_{D_{fd}}(p)
\]

\[
= \alpha(p).
\]
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 $D = m^2D_{fd}$, we must have $D_{fd} \equiv D \pmod{8}$ (since $a^2 \equiv 1 \pmod{8}$ for any odd integer $a$).

Therefore,

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

$$= \begin{cases} 
1 & \text{if } D_{fd} \equiv 1 \pmod{8}, \\
-1 & \text{if } D_{fd} \equiv 5 \pmod{8},
\end{cases}$$

$$= \chi_{D_{fd}}(2)$$

$$= \alpha(2).$$

To finish the proof we note that

$$
\left( \frac{\Delta}{2} \right) \text{ evaluated at } -1 = \text{sign}(\Delta)
$$

$$= \text{sign}(D)$$

$$= \text{sign}(D_{fd})$$

$$= \chi_{D_{fd}}(-1)$$

$$= \alpha(-1).$$

Since $\Delta = 1$ if and only if $D_{fd} = 1$, the evaluation of $(\frac{\Delta}{2})$ at 0 is $\chi_{D_{fd}}(0) = \alpha(0)$. 

**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

$$
\left( \frac{\Delta_1}{a} \right) \left( \frac{\Delta_2}{a} \right) = \left( \frac{\Delta_1 \Delta_2}{a} \right)
$$

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. 

**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 $A = (a_{i,j}) \in M(f, \mathbb{Z})$ 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

\[
^{t}yAy = \sum_{i,j=1}^{n} a_{i,j}y_iy_j = \sum_{i=1}^{f} a_{i,i}y_i^2 + \sum_{1 \leq i < j \leq f} 2a_{i,j}y_iy_j.
\]

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 \( ^{t}y_iAy_i = a_{i,i} \). This is even, as required. \( \square \)

Suppose that \( A \) is an even integral symmetric matrix. To \( A \) we associate the polynomial

\[
Q(x_1, \ldots, x_f) = \frac{1}{2} \sum_{i,j=1}^{f} a_{i,j}x_ix_j,
\]

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

\[
Q(x) = \frac{1}{2} ^{t}xAx
\]

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

\[
Q(x_1, \ldots, x_f) = \sum_{1 \leq i \leq j \leq f} b_{i,j}x_ix_j
\]

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 \textit{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 $A \in \text{M}(f, \mathbb{Z})$ 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

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

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

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

$$= \text{sign}(\sigma) \prod_{i \in \{1, \ldots, f\}} a_{i,\sigma(i)}$$
CHAPTER 1. BACKGROUND

$= t(\sigma)$.

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 $i \in \{1, \ldots, t\}$ 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 $\det(A') = \det(A)$. 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

$$A = \begin{bmatrix} A_1 & B \\ B & A_2 \end{bmatrix},$$

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

$$\text{adj}(A_1) = \begin{bmatrix} a_{2,2} & -a_{1,2} \\ -a_{1,2} & a_{1,1} \end{bmatrix},$$
By the induction hypothesis, \( \Delta(f) \) is an \((f - 1)\times(f - 1)\) matrix. From (1.4), we obtain

\[
\begin{bmatrix}
1 & 2 \\
-1B & \text{adj}(A_1)
\end{bmatrix}
\begin{bmatrix}
A_1 \\
B
\end{bmatrix}
= \begin{bmatrix}
A_1 & -1B \\
-1B & \text{adj}(A_1)
\end{bmatrix} \cdot \begin{bmatrix}
B \\
\text{det}(A_1) \cdot 1_{f-2}
\end{bmatrix}.
\tag{1.4}
\]

Consider the \((f - 2)\times(f - 2)\) matrix \(-1B\cdot \text{adj}(A_1) \cdot B\). This matrix clearly has integral entries. If \(y \in \mathbb{Z}\), then \(By \in \mathbb{Z}\) and

\[
(1B)(-B\cdot \text{adj}(A_1) \cdot B)y = -B(1B) \cdot \text{adj}(A_1) \cdot (By);
\]

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 \(y \in \mathbb{Z}\), we can apply Lemma 1.5.1 again to conclude that \(-1B\cdot \text{adj}(A_1) \cdot B\) is even. It follows that

\[
A_3 = -1B \cdot \text{adj}(A_1) \cdot B + \text{det}(A_1)A_2
\]

is an \((f - 2)\times(f - 2)\) even integral symmetric matrix. Taking determinants of both sides of (1.4), we obtain

\[
\begin{align*}
\text{det}(A_1)^{f-2} \cdot \text{det}(A) &= \text{det}(A_1) \cdot \text{det}(A_3) \\
\text{det}(A_1)^{f-2} \cdot (-1)^k \text{det}(A) &= (-1) \cdot \text{det}(A_1) \cdot (-1)^{k-1} \text{det}(A_3) \\
\text{det}(A_1)^{f-2} \cdot \Delta(A) &= \Delta(A_1) \cdot \Delta(A_3).
\end{align*}
\]

By the induction hypothesis, \(\Delta(A_1) \equiv 0, 1 \pmod{4}\), and \(\Delta(A_3) \equiv 0, 1 \pmod{4}\). Hence,

\[
\text{det}(A_1)^{f-2} \cdot \Delta(A) \equiv 0, 1 \pmod{4}.
\]

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

Let \(A \in \mathbb{M}(f, \mathbb{R})\). The \textbf{adjoint} of \(A\) is the \(f \times f\) matrix \(\text{adj}(A)\) with entries

\[
\text{adj}(A)_{i,j} = (-1)^{i+j} \text{det}(A(j|i))
\]

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,
\[
A = \det(A) \text{adj}(A)^{-1},
\]
\[
\text{adj}(A) = \det(A) \cdot A^{-1},
\]
\[
A^{-1} = \det(A)^{-1} \cdot \text{adj}(A),
\]
\[
\text{adj}(A)^{-1} = \det(A)^{-1} \cdot A,
\]
\[
\det(\text{adj}(A)) = \det(A)^f - 1.
\]
Assume further that \(A\) is symmetric. We say that \(A\) is positive-definite if the following two conditions hold:

1. If \(x \in \mathbb{R}^f\), then \(Q(x) = \frac{1}{2}^t x A x \geq 0\);

2. if \(x \in \mathbb{R}^f\) and \(Q(x) = \frac{1}{2}^t x A x = 0\), then \(x = 0\).

Since \(A\) is symmetric with real entries, there exists a matrix \(T \in \text{GL}(f, \mathbb{R})\) such that \(^t T^T = T^T T = 1\) (so that \(T^{-1} = ^t T\)) and

\[
^t T A T = T^{-1} A T = \begin{bmatrix}
\lambda_1 & & \\
& \lambda_2 & \\
& & \lambda_3 \\
& & & \ddots \\
& & & & \lambda_f
\end{bmatrix}
\]

(1.5)

for some \(\lambda_1, \ldots, \lambda_f \in \mathbb{R}\) (see the corollary on p. 314 of [7]). The symmetric matrix \(A\) is positive-definite if and only if \(\lambda_1, \ldots, \lambda_f\) are all positive. This implies that if \(A\) is positive-definite, then \(\det(A) > 0\). Assume that \(A\) is positive-definite, and that \(T\) and \(\lambda_1, \ldots, \lambda_f\) are as in (1.5); in particular, \(\lambda_1, \ldots, \lambda_f\) are all positive real numbers. Let

\[
B = T \begin{bmatrix}
\sqrt{\lambda_1} & & \\
& \sqrt{\lambda_2} & \\
& & \sqrt{\lambda_3} \\
& & & \ddots \\
& & & & \sqrt{\lambda_f}
\end{bmatrix} T^{-1}.
\]

(1.6)

The matrix \(B\) is evidently symmetric and positive-definite, and we have

\[A = ^t B B = B B = B^2.\]

(1.7)

**Lemma 1.5.3.** Assume \(f\) is even. Let \(A \in \text{M}(f, \mathbb{Z})\) 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, $\text{adj}(A) = \det(A) \cdot (A^{-1}) = \det(A) \cdot (A')^{-1} = \det(A) \cdot A^{-1} = \text{adj}(A)$, 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

$$t^t (T) \text{adj}(A) t = \det(A) \cdot T A^{-1} T$$

$$= \begin{bmatrix} \det(A) \lambda_1^{-1} & \det(A) \lambda_2^{-1} & \cdots & \det(A) \lambda_f^{-1} \\ & \ddots & \ddots & \\\\ & & \ddots & \det(A) \lambda_f^{-1} \end{bmatrix}.$$ 

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

$$G = \gcd\left\{ \begin{array}{cccc}
\frac{\text{adj}(A)_{1,1}}{2} & \text{adj}(A)_{1,2} & \text{adj}(A)_{1,3} & \cdots & \text{adj}(A)_{1,f} \\
\text{adj}(A)_{1,2} & \frac{\text{adj}(A)_{2,2}}{2} & \text{adj}(A)_{2,3} & \cdots & \text{adj}(A)_{2,f} \\
\text{adj}(A)_{1,3} & \text{adj}(A)_{2,3} & \frac{\text{adj}(A)_{3,3}}{2} & \cdots & \text{adj}(A)_{3,f} \\
\vdots & \vdots & \ddots & \ddots & \\
\text{adj}(A)_{1,f} & \text{adj}(A)_{2,f} & \text{adj}(A)_{3,f} & \cdots & \frac{\text{adj}(A)_{f,f}}{2} \end{array}\right\}$$

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 $G = pg$ 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 $(f - 1)j \geq fk$. Therefore,
\[
j \geq \frac{fk}{f - 1} > k.
\]
This means that $p$ divides $N = \det(A)/G$. \hfill \qed

**Corollary 1.5.5.** Let $f$ be an even positive integer, let $A \in M(f, Z)$ 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 \qed

**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

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

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

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 \(Q(x) = \frac{1}{2} x A x\). Let \(h \in \mathbb{Z}^f\) be such that \(A h \equiv 0 \pmod{N}\). 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 \(A h \equiv 0 \pmod{N}\), there exists \(m \in \mathbb{Z}^f\) such that \(A h = N m\). We have

\[
Q(q) = \frac{1}{2} h A h
\]
\[ 2Q(n) = \frac{1}{2} \left( h + Nb \right) A(h + Nb) \]
\[ = \left( h + Nb \right) A(h + Nb) \]
\[ = \frac{1}{2} \left( hAh + 2N^2 bAb \right) \]
\[ \equiv \frac{1}{2} hAh \pmod{2N^2}. \]

Here \( \frac{1}{2} bAh \equiv 0 \pmod{N} \) because \( Ah \equiv 0 \pmod{N} \) and \( \frac{1}{2} bAb \equiv 0 \pmod{2} \) 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 \( Q(n) \equiv 0 \pmod{N} \).

### 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 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

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

\[(F|\ell \sigma)(z) = \det(\sigma)^{\ell/2}(cz + d)^{-\ell} F\left(\frac{az + b}{cz + d}\right)\]

\[= \det(\sigma)^{\ell/2} j(\sigma, z)^{-\ell} F(\sigma \cdot z)\]

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

\[\Gamma(N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}) : a \equiv b \equiv 1 \pmod{N}, c \equiv d \equiv 0 \pmod{N} \}.\]

The **Hecke congruence subgroup** of level \(N\) is defined to be

\[\Gamma_0(N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, \mathbb{Z}) : c \equiv 0 \pmod{N} \}.\]

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 \(\Gamma(N) \subset \Gamma\).

### 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

\[H(N, R) \to D(R)\]

defined by

\[z \mapsto q(z) = e^{2\pi i z/N}\]

is well-defined. We have \(q(z + N) = q(z)\) for \(z \in H(N, R)\).

**Lemma 1.8.1.** Let \(f : \mathbb{H}_1 \to \mathbb{C}\) 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
\[
f(z) = \sum_{n=0}^{\infty} a(n)e^{2\pi inz/N}
\]
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
\[
(F|_r^T)(z) = \sum_{k=0}^{\infty} b(k)e^{2\pi ikz/M}
\]
for \( z \in H(M, T) \).

**Proof.** For \( z \in H(N, R) \),
\[
f(z) = f(z + M) = \sum_{n=0}^{\infty} a(n)e^{2\pi in(z+M)/N} = \sum_{n=0}^{\infty} a(n)e^{2\pi inz/N} \cdot e^{2\pi iM/N}.
\]
It follows that
\[
a(n) = a(n)e^{2\pi inM/N}
\]
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
\[
f(z) = \sum_{n=0}^{\infty} a(n)e^{2\pi inz/N} = \sum_{n=0}^{\infty} a(n)e^{2\pi i(nM/N)z/M} = \sum_{k=0}^{\infty} b(k)(e^{2\pi iz/M})^k
\]
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 \( \sum_{n=0}^{\infty} a(n)e^{2\pi inz/N} \) 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. \( \square \)
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 $F : \mathbb{H}_1 \rightarrow \mathbb{C}$ 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 $f|_{k\alpha} = f$.
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

$$(F|_{k\sigma})(z) = \sum_{n=0}^{\infty} a(n)q^n = \sum_{n=0}^{\infty} a(n)e^{2\pi n z/N}$$

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

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

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 $I = 1_{2n}$. Let

$$J = \begin{bmatrix} 1_n & 0 \\ -1_n & 0 \end{bmatrix}.$$ 

We note that $J^2 = -1$, $J^{-1} = -J$.

We define

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

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 $^tg \in \text{Sp}(2n, R)$.

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 $^tgJg = J$. This implies that $g^{-1} = J^{-1}gJ = -J^tgJ$.

Now

$$^tg^{-1}Jg^{-1} = J^tgJ^{-1}J = \begin{bmatrix} ad-bc & ad-bc \\ -(ad-bc) & ad-bc \end{bmatrix} = \det(g)J.$$ 

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

$$gJ^tg = gJ^tgJ^{-1}J^{-1} = \begin{bmatrix} ad-bc & ad-bc \\ -(ad-bc) & ad-bc \end{bmatrix} = J.$$

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

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

$$^tAC = ^tCA, \quad ^tBD = ^tDB, \quad ^tAD - ^tCB = 1.$$ 

Proof. This follows by direct computations. \hfill \square 

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

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

It follows that $g \in \text{Sp}(2, R)$ if and only if $\det(g) = 1$, i.e., $g \in \text{SL}(2, R)$. \hfill \square
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 $\text{Sp}(2n, R)$:

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

$$\begin{bmatrix} A & \bar{A}^{-1} \\ \bar{A} & A^{-1} \end{bmatrix}, \quad A \in \text{GL}(n, R),$$

$$\begin{bmatrix} 1 & X \\ 1 & 1 \end{bmatrix}, \quad X \in \text{M}(n, R), \quad \bar{X} = X,$$

$$\begin{bmatrix} 1 & Y \\ 1 & 1 \end{bmatrix}, \quad Y \in \text{M}(n, R), \quad \bar{Y} = Y.$$

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

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

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

$$U = \{ \begin{bmatrix} 1 & X \\ 1 & 1 \end{bmatrix} : X \in \text{M}(n, R), \quad \bar{X} = X \}$$

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

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

for $X \in \text{M}(n, R)$ with $\bar{X} = X$.
Proof. See Satz A 5.4 on page 326 of [4]. \qed

**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. \qed

**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 [2]. \qed

### 1.10 The Siegel upper half-space

Let $n$ be a positive integer. We define $\mathbb{H}_n$ to be the subset of $M(n, \mathbb{C})$ consisting of the matrices $Z = X + iY$ with $X, Y \in M(n, \mathbb{R})$ such that $\text{t}X = X$, $\text{t}Y = Y$, 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. 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 [10]. 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:

\[
\begin{align*}
^tPQ - ^tQ^P &= (Z^tA + ^tB)(CZ + D) - (Z^tC + ^tD)(AZ + B) \\
&= Z^tACZ + Z^tAD + ^tBCZ + ^tBD \\
&\quad - Z^tCAZ - Z^tCB - ^tDAZ - ^tDB \\
&= Z - Z \quad \text{(cf. Lemma 1.9.2)} \\
&= 2iY.
\end{align*}
\]

It follows that

\[
\begin{align*}
^t(v(^tPQ - ^tQ^P)v) &= 2i^tYv \\
^t(v^tPQv) - ^t(v^tQ^Pv) &= 2i^tYv \\
^t(v^tPQv) - ^t(v^tQ^Pv) &= 2i^tYv
\end{align*}
\]
0 = 2i t v Y v
0 = i t v Y v.

Write \( v = v_1 + iv_2 \) with \( v_1, v_2 \in \mathbb{R}^n \). Then

\[
0 = t v_1 Y v_1 + t v_2 Y v_2.
\]

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 \( t PQ = t Q P \). Now

\[
\begin{align*}
\dot{t} PQ - t Q P &= \dot{t}(AZ + B)(CZ + D) - t(CZ + D)(AZ + B) \\
&= (t Z^A + t B)(CZ + D) - (t Z^C + t D)(AZ + B) \\
&= t Z^A CZ + t Z^A AD + t BCZ + t BD \\
&\quad - t Z^C AZ - t Z^C CB - t DAZ - t DB \\
&= 0 \quad (\text{cf Lemma 1.9.2})
\end{align*}
\]

as desired. It follows that \( PQ^{-1} \) is symmetric. Write \( PQ^{-1} = X' + iY' \) where \( X', Y' \in M(n, \mathbb{R}) \) with \( \dot{t} X' = X' \) and \( \dot{t} Y' = Y' \). To complete the proof of the lemma we need to show that \( Y' \) is positive-definite. Now

\[
Y' = \frac{1}{2i} \left( (X' + iY') - (X' + iY') \right)
= \frac{1}{2i} \left( PQ^{-1} - P Q^{-1} \right)
= \frac{1}{2i} \left( (P Q^{-1}) - \dot{t} Q P Q^{-1} \right)
= \frac{1}{2i} \left( Q^{-1} t P - \dot{t} Q P Q^{-1} \right)
= \frac{1}{2i} \left( Q^{-1} (P Q - Q P) Q^{-1} \right)
= \frac{1}{2i} \left( Q^{-1} (2i Y) Q^{-1} \right) \quad (\text{cf. (1.9)})
= \dot{t} Q^{-1} Y Q^{-1}.
\]

Using that \( Y \) is positive-definite, it is easy to verify that \( Y' = \dot{t} Q^{-1} Y Q^{-1} \) 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 $A \in \text{M}(f, \mathbb{R})$ be a positive-definite symmetric matrix, and for $x \in \mathbb{R}^f$ let

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

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

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

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

$$|e^{2\pi i z Q(m)}| = e^{-2\pi \text{Im}(z)Q(m)}$$

37
\[ \leq e^{-2\pi \delta Q(m)} \]
\[ \leq e^{-2\pi \delta^2 \|m\|^2} \]
\[ = q^\|m\|^2 \]
\[ = q^{m_1^2 + \cdots + m_f^2}. \]

where \( q = e^{-2\pi \delta^2}. \) Since \( 0 < q < 1, \) the series
\[ \sum_{n \in \mathbb{Z}} q^{n^2} \]
converges absolutely. This implies that the series
\[ \left( \sum_{n \in \mathbb{Z}} q^{n^2} \right)^f = \sum_{m \in \mathbb{Z}^f} q^{m_1^2 + \cdots + m_f^2} = \sum_{m \in \mathbb{Z}^f} q^{\|m\|^2} \]
converges absolutely. It follows from the Weierstrass \( M \)-test that our series
\[ \sum_{m \in \mathbb{Z}^f} e^{2\pi i z Q(m)} \]
converges absolutely and uniformly on \( \{ z \in \mathbb{H}_1 : \text{Im}(z) \geq \delta \} \) (see, for example, [14], p. 160). Since for each \( m \in \mathbb{Z}^f \) the function on \( \mathbb{H}_1 \) defined by \( z \mapsto e^{2\pi i z Q(m)} \) 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 [14], p. 162).

**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
\[ \text{Im}(z \cdot ^t(w + g)(w + g)) \geq \varepsilon \text{Im}(z \cdot ^tgg), \]
or equivalently
\[ -\text{Im}(z \cdot ^t(w + g)(w + g)) \leq -\varepsilon \text{Im}(z \cdot ^tgg), \]
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

\[
2 \cdot \text{Im}(z^t wg) = 2t^t ag + 2\sigma^t bg,
\]

\[
\text{Im}(z^t ww) = \sigma^t(aa - bb) - 2t^t ab.
\]

It follows that

\[
-2 \cdot \text{Im}(z^t wg) - \text{Im}(z^t ww) \leq (1 - \varepsilon)\text{Im}(z^t g)
\]

\[
\varepsilon \text{Im}(z^t g) \leq \text{Im}(z^t g) + 2 \cdot \text{Im}(z^t wg) + \text{Im}(z^t ww)
\]

\[
\varepsilon \text{Im}(z^t g) \leq \text{Im}(z^t (w + g)(w + g)).
\]

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

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

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 $A = B^TB = BB$ (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
\[
\text{Im}(z^t(w' + g')(w' + g')) \geq \varepsilon \text{Im}(z^tg'g')
\]
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 an 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:
\[
\|B^{-1}(B(g))\| \leq \|B^{-1}\| \|B(g)\|
\]
\[
\|g\| \leq \|B^{-1}\| \|B(g)\|
\]
\[
R \leq \|B^{-1}\| \|B(g)\|
\]
\[
\|B^{-1}R\| \leq \|B(g)\|
\]
\[
T \leq \|B(g)\|.
\]
Therefore, with $g' = B(g)$,
\[
\text{Im}(z^t(w' + g')(w' + g')) \geq \varepsilon \text{Im}(z^tg'g')
\]
\[
\text{Im}(z^t(Bw +Bg)(Bw + Bg)) \geq \varepsilon \text{Im}(z^t(Bg)Bg)
\]
\[
\text{Im}(z^t(w + g)^tBB(w + g)) \geq \varepsilon \text{Im}(z^tg tBBg)
\]
\[
\text{Im}(z^t(w + g)A(w + g)) \geq \varepsilon \text{Im}(z^tgAg)
\]
\[
\text{Im}(z^tQ(w + g)) \geq \varepsilon \text{Im}(z^tQ(g))
\]
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
\[
Q(x) = \frac{1}{2} xAx.
\]
For $z \in \mathbb{H}_1$ and $w = ^t(w_1, \ldots, w_f) \in \mathbb{C}^f$, define
\[
\theta(A, z, w) = \sum_{m \in \mathbb{Z}^f} e^{\pi iz^t(m+w)A(m+w)} = \sum_{m \in \mathbb{Z}^f} e^{2\pi izQ(m+w)}.
\]
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.
2.2. THE POISSON SUMMATION FORMULA

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:

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

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

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

converges. The Weierstrass M-test (see [14], 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 [14], p. 162). \( \square \)

2.2 The Poisson summation formula

Let \( f \) be a positive integer. Let \( g : \mathbb{R}^f \rightarrow \mathbb{C} \) be a function, and write \( g = u + iv \), where \( u, v : \mathbb{R}^f \rightarrow \mathbb{R} \) 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

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

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 [18], or chapter 13 of [12].

**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

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

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

$$g(x) = e^{-2\pi Q(x+w)} = e^{-\pi \langle x+w, Ax + w \rangle}$$

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 $A = t^t BB = BB$ (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

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

for $x \in \mathbb{R}^f$ is in the Schwartz space $S(\mathbb{R}^f)$. Let $w \in \mathbb{C}^f$. The function $g : \mathbb{R}^f \to \mathbb{C}$ defined by

$$g(x) = e^{-\pi \langle x+w, Ax + w \rangle}$$

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

$$(D^\alpha h)(x) = Q_\alpha(x)e^{-\pi \langle x, x \rangle - 2\pi i \langle x, x \rangle}$$
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

\[
|P(x)(D^\alpha h)(x)| = |P(x)Q_\alpha(x)e^{-\pi'xx-2\pi'xv}|
\]

for \( x \in \mathbb{R}^f \). This equality implies that it now suffices to prove that the function defined by \( x \mapsto e^{-\pi'xx} \) 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

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

Proof. By Fubini's theorem

\[
\int_{\mathbb{R}^f} e^{-\pi'(y+w)(y+w)} \, dy = \int_{\mathbb{R}} e^{-\pi(y_1+w_1)^2} \cdots e^{-\pi(y_f+w_f)^2} \, dy
\]

\[
= \left( \int_{\mathbb{R}} e^{-\pi(y_1+w_1)^2} \, dy_1 \right) \cdots \left( \int_{\mathbb{R}} e^{-\pi(y_f+w_f)^2} \, dy_f \right).
\]

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

Then

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

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 [14]) applied to the analytic function \( z \mapsto e^{-\pi z^2} \) we have

\[
0 = \int_{\gamma} e^{-\pi z^2} \, dz = \int_{\gamma_1} e^{-\pi z^2} \, dz + \int_{\gamma_2} e^{-\pi z^2} \, dz + \int_{\gamma_3} e^{-\pi z^2} \, dz + \int_{\gamma_4} e^{-\pi z^2} \, dz.
\]
Using the definitions of these contour integrals, this is:

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

or equivalently,

\[ \int_{-a}^{a} e^{-\pi (y+iv)^2} dy = \int_{-a}^{a} e^{-\pi y^2} dy + \int_{\gamma_2} \gamma_2 e^{-\pi z^2} dz + \int_{\gamma_4} \gamma_4 e^{-\pi z^2} dz. \quad (2.1) \]

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 [14]),

\[ |\int_{\gamma_2} e^{-\pi z^2} dz| \leq ve^{-\pi a^2 + \pi v^2}, \quad |\int_{\gamma_4} e^{-\pi z^2} dz| \leq ve^{-\pi a^2 + \pi v^2}. \]

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. \( \square \)

**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

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

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

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

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

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

for \( x \in \mathbb{R}^f \).

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

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

\[
\int_{\mathbb{R}^J} \exp \left( -\pi \left( 2Q(y + w) + 2i^t xy \right) \right) dy
\]

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

\[
= \int_{\mathbb{R}^J} \exp \left( -\pi \left( t(y + w)A(y + w) + 2i^t yx \right) \right) dy
\]

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

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

\[
(\mathcal{F}g)(x) = \det(B)^{-1} \int_{\mathbb{R}^J} \exp \left( -\pi \left( t(y + Bw)(y + Bw) + 2i^t y B^{-1} x \right) \right) dy.
\]

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 [19]; 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,

\[
(\mathcal{F}g)(x) = \det(A)^{-1/2} \int_{\mathbb{R}^J} \exp \left( -\pi \left( tyy + 2i^t y B w + t(Bw)^t B^{-1} x \right) \right) dy
\]

\[
= \det(A)^{-1/2} \exp(-\pi t^w Aw) \int_{\mathbb{R}^J} \exp \left( -\pi \left( tyy + 2i^t y B w + 2i^t y B^{-1} x \right) \right) dy
\]

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

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

\[
\times \int_{\mathbb{R}^J} \exp \left( -\pi \left( tyy + 2i^t y(Bw + i^t B^{-1} x) \right)
\right.
\]

\[
\left. + t(Bw + i^t B^{-1} x)(Bw + i^t B^{-1} x) \right) dy
\]

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

\[
\times \int_{\mathbb{R}^J} \exp \left( -\pi \left( t(y + Bw + i^t B^{-1} x)(y + Bw + i^t B^{-1} x) \right) \right) dy.
\]

Applying now Lemma 2.2.2, we obtain:

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

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

This completes the calculation.

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

\textit{Proof.} See page 249 of [12].

\textbf{Lemma 2.2.5.} Let \(f\) be a positive integer. Let \(A \in \text{M}(f, \mathbb{R})\) 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
\[
Q(x) = \frac{1}{2} t^t x A x.
\]
Then there exists a positive real number \(R > 0\) such that
\[
-\text{Im}\left(\left(-\frac{1}{z}\right)^t g A^{-1} g + 2^t g w\right) \leq -\varepsilon \text{Im}\left(\left(-\frac{1}{z}\right) \cdot t^t g A^{-1} g\right),
\]
for \(z \in K_1\), \(w \in K_2\), and all \(g \in \mathbb{R}^f\) such that \(\|g\| \geq R\).

\textit{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 \(A = t^t B B\) (see (1.7)). If \(m \in \mathbb{R}^f\), then we note that
\[
t^t g A^{-1} g = |t^t g A^{-1} g| = |t^t B^{-1} 1 B^{-1} g| = |t^t (B^{-1} g) \cdot (B^{-1} g)| = \|t^t B^{-1} g\|^2 = \left(\frac{1}{\|t^t B\|} \cdot \|t^t B\| \cdot \|t^t B^{-1} g\|^2\right)^2 \geq \left(\frac{1}{\|t^t B\|} \cdot \|g\|^2\right)^2 = \frac{1}{\|t^t B\|^2} \cdot \|g\|^2.
\]
Next, let \(M > 0\) be such that
\[
|\text{Im}(-1/z)|, |\text{Im}(w)| \leq M
\]
2.2. THE POISSON SUMMATION FORMULA

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 $H_1$. Let $\delta > 0$ be such that

$$\text{Im}(-1/z) \geq \delta > 0.$$ 

Let $R > 0$ be such that if $x \geq R$, then

$$\delta(1 - \varepsilon) \cdot \frac{1}{\|tB\|^2} \cdot x^2 \geq 2Mx.$$

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

$$-\text{Im}(2^t g w) = -2^t g b$$

$$\leq 2 \|g b\|$$

$$\leq 2M \|g\|.$$ 

On the other hand,

$$(1 - \varepsilon) \cdot \text{Im}((-1/z)^t g A^{-1} g) = t \cdot g A^{-1} g$$

$$\geq \delta(1 - \varepsilon) \cdot \frac{1}{\|tB\|^2} \cdot \|g\|^2.$$ 

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. \hfill \Box

**Theorem 2.2.6.** Let $f$ be a positive integer. Assume that $f$ is even, and set

$$k = \frac{f}{2}.$$ 

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

$$Q_A(x) = \frac{1}{2}^t x A x, \quad Q_{A^{-1}}(x) = \frac{1}{2}^t x A^{-1} x.$$ 

The series

$$\sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z)^t m A^{-1} m + 2\pi i^t m w}$$

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

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

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 \( X \subseteq \mathbb{Z}^f \) such that for \( m \in \mathbb{Z}^f - X \), \( z \in K_1 \) and \( w \in K_2 \) we have:

\[
|e^{\pi(-1/z)'mA^{-1}m + 2\pi i'mw}| = e^{-\pi \text{Im}\left((-1/z)'mA^{-1}m + 2\pi i'mw\right)} \\
= e^{-\pi \cdot (1/2) \cdot \text{Im}\left((-1/z)'mA^{-1}m\right)} \\
\leq e^{-\pi \text{Im}\left((-1/z)Q_{A^{-1}}(m)\right)} \\
= e^{-2\pi Q_{A^{-1}}(m) \text{Im}(1/(2z))} \\
\leq e^{-2\pi \delta Q_{A^{-1}}(m)} \\
= |e^{2\pi i(\delta i)Q_{A^{-1}}(m)}|.
\]

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

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

converges. The Weierstrass M-test (see [14], p. 160) now implies that the series

\[
\sum_{m \in \mathbb{Z}^f} e^{\pi(-1/z)'mA^{-1}m + 2\pi i'mw}
\]

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 \( (z, w) \mapsto e^{\pi(-1/z)'mA^{-1}m + 2\pi i'mw} \) 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 [14], p. 162).

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

\[
g(x) = e^{-2\pi Q_A(x+w)} = e^{-\pi \cdot (x+w)A(x+w)}
\]

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

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

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

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

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

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

\[
\sum_{m \in \mathbb{Z}^f} e^{2\pi i \cdot itQ_A(m+w)} = \frac{1}{\det(tA)^{1/2}} \sum_{m \in \mathbb{Z}^f} e^{\pi i \cdot (1/(it)) \cdot xA^{-1}x + 2\pi i'xw}
\]
2.3. DIFFERENTIAL OPERATORS

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

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

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

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

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 \( \ell \in C^f \). Then

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

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

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

for \( F \in H(C^f) \).

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

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

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

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

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 [14]) implies that this equality holds for all \( z \in \mathbb{H}_1 \). \( \square \)
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

$$\left( \sum_{i=1}^{f} \ell_{i} \frac{\partial F_{1}}{\partial w_{i}} \right) \cdot F_{2} + F_{1} \cdot \left( \sum_{i=1}^{f} \ell_{i} \frac{\partial F_{2}}{\partial w_{i}} \right) = L_{\ell}(F_{1}) \cdot F_{2} + F_{1} \cdot L_{\ell}(F_{2}).$$

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

$$L_{\ell}(e^{F}) = \sum_{i=1}^{f} \ell_{i} \frac{\partial}{\partial w_{i}} (e^{F})$$

$$= \sum_{i=1}^{f} \ell_{i} \frac{\partial F}{\partial w_{i}} \cdot e^{F}$$

$$= \left( \sum_{i=1}^{f} \ell_{i} \frac{\partial}{\partial w_{i}} \right) \cdot e^{F}$$

$$= L_{\ell}(F) \cdot e^{F}.$$

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:

$$L_{\ell}\left( \ell^{T}(m + w)A(m + w) \right) = 2 \ell^{T}A(m + w),$$

$$L_{\ell}\left( \ell^{T}A(m + w)^{T} \right) = 0,$$

$$L_{\ell}(\ell^{T}mw) = \ell^{T}m.$$

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

**Proof.** We have

$$L_{\ell}\left( \ell^{T}(m + w)A(m + w) \right)$$

$$= L_{\ell}\left( \sum_{i,j=1}^{f} a_{ij}(m_{i} + w_{i})(m_{j} + w_{j}) \right)$$

$$= \sum_{i,j=1}^{f} a_{ij} L_{\ell}\left( (m_{i} + w_{i})(m_{j} + w_{j}) \right)$$

$$= \sum_{i,j=1}^{f} a_{ij} \left( L_{\ell}\left( (m_{i} + w_{i}) \right)(m_{j} + w_{j}) + (m_{i} + w_{i})L_{\ell}\left( (m_{j} + w_{j}) \right) \right)$$

$$= \sum_{i,j=1}^{f} a_{ij} \left( \ell_{i}(m_{j} + w_{j}) + \ell_{j}(m_{i} + w_{i}) \right)$$
2.3. DIFFERENTIAL OPERATORS

\[
\begin{align*}
2.3. \text{ DIFFERENTIAL OPERATORS} & \quad 51 \\
= \sum_{i,j=1}^{f} a_{ij} \ell_i (m_j + w_j) + \sum_{i,j=1}^{f} a_{ij} \ell_j (m_i + w_i) \\
= \ell A(m + w) + (m + w)A\ell \\
= 2 \ell A(m + w).
\end{align*}
\]

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

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

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

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

\[
= 0.
\]

The final assertion of the lemma is straightforward.

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

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

\[ \sum_{m \in \mathbb{Z}} \left( \ell m \right)^r e^{\pi i \left( -1/z \right)} (mA^{-1}m + 2\pi i \cdot mw) \]

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,

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

**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

\[ S_1(z, w) = \sum_{m \in \mathbb{Z}} \left( \ell A(m + w) \right)^r e^{\pi iz \cdot (m+w)A(m+w)} \]

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

\[ \sum_{m \in \mathbb{Z}} L_\ell \left( \left( \ell A(m + w) \right)^r e^{\pi iz \cdot (m+w)A(m+w)} \right) \]

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 [14]). We have for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\), using Lemma 2.3.1 and Lemma 2.3.2,

\[ (L_\ell S_1)(z, w) = \sum_{m \in \mathbb{Z}} L_\ell \left( \left( \ell A(m + w) \right)^r e^{\pi iz \cdot (m+w)A(m+w)} \right) \]

Next, for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\), let

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

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

$$
\left. e^{\pi i (1/z) A^{-1} m} + 2\pi i \cdot m w \right)
$$

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

$$
= 2\pi i \cdot \frac{i^k}{z^{k+r} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} \right) \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} + 2\pi i \cdot m w \right).
$$

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

$$
2\pi i z \sum_{m \in \mathbb{Z}^f} \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} \right) \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} + 2\pi i \cdot m w \right)
$$

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

or equivalently,

$$
\sum_{m \in \mathbb{Z}^f} \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} \right) \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} + 2\pi i \cdot m w \right)
$$

$$
= \frac{i^k}{z^{k+r+1} \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} \right) \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} + 2\pi i \cdot m w \right).
$$

By induction, the proof is complete. \(\square\)

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

$$
(L_{\ell} w) = \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} \right) \left( t^r \cdot e^{\pi i (1/z) A^{-1} m} + 2\pi i \cdot m w \right),
$$

where $w = (w_1, \ldots, w_f)$ and $\ell \in \mathbb{C}^f$ with $t^r \cdot e^{\pi i (1/z) A^{-1} m} = 0$. The elements of $\mathcal{H}_r(A)$ are homogeneous polynomials of degree $r$, and are called spherical functions with respect to $A$. 

2.3. DIFFERENTIAL OPERATORS

53
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

\[
\theta(A, P, h, z) = \sum_{n \in \mathbb{Z}^f, n \equiv h \pmod{N}} P(n) e^{2\pi i z Q(n)}. \tag{2.2}
\]

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

\[
\theta(A, P, h, z) = \theta(A, P, h', z), \tag{2.3}
\]

\[
\theta(A, P, h, z) = (-1)^r \theta(A, P, -h, z), \tag{2.4}
\]

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

\[
\theta(A, P, h, z) \left|_{k+r} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right. = \frac{1}{\sqrt{\det(A)}} \sum_{g \pmod{N}, Ag \equiv 0 \pmod{N}} e^{2\pi i \frac{h^T A g}{N}} \cdot \theta(A, P, g, z) \tag{2.5}
\]

and

\[
\theta(A, P, h, z) \left|_{k+r} \begin{bmatrix} 1 \\ b \end{bmatrix} \right. = e^{2\pi i b \frac{Q(h)}{N}} \theta(A, P, h, z) \tag{2.6}
\]

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

\[
P(w) = (t^T A t)^r.
\]

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

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

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

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

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

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

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

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

\[ = \frac{n}{N}, \]

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

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

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

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

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

Next, consider the map

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

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,

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

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

$$
\sum_{n \in \mathbb{Z}/r} (t^\ell An)^r e^{\pi i z \frac{N An}{N^2}}
= \frac{ik}{z^{k+r} \sqrt{\det(A)}} \sum_{g \in \mathbb{Z}/r \mod N} (t^\ell Ag)^r e^{\pi i (\frac{1}{z} \frac{N Ah}{N^2} + 2\pi i \frac{N Ah}{N^2})}.
$$

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

$$
\sum_{g \in \mathbb{Z}/r \mod N} F(n) = \sum_{g \in \mathbb{Z}/r / NZ/r \mod N} \sum_{m \in NZ/r \mod N} F(g + m) = \sum_{g \equiv 0 \mod N} \sum_{n_1 \equiv g \mod N} F(n_1).
$$

Applying this observation, we have:

$$
\sum_{n \in \mathbb{Z}/r \mod N} (t^\ell An)^r e^{\pi i z \frac{N An}{N^2}} = \frac{ik}{z^{k+r} \sqrt{\det(A)}} \sum_{g \equiv 0 \mod N} \sum_{n_1 \equiv g \mod N} (t^\ell An_1)^r e^{\pi i (\frac{1}{z} \frac{N An_1}{N^2} + 2\pi i \frac{N Ah}{N^2})}.
$$

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

$$
e^{2\pi i \frac{N Ah}{N^2}} = e^{2\pi i \frac{N Ah}{N^2} e^{2\pi i \frac{N Am_1}{N^2}}} = e^{2\pi i \frac{N Ah}{N^2} \frac{N Am_1}{N^2}} e^{2\pi i \frac{N Ah}{N^2}} = e^{2\pi i \frac{N Ah}{N^2}}.
$$

In the last step we used that $Ah \equiv 0 \mod N$, so that $\frac{N Ah}{N^2}$ is an integer. We therefore have:

$$
\sum_{n \in \mathbb{Z}/r \mod N} (t^\ell An)^r e^{\pi i z \frac{N An}{N^2}}
$$
2.4. A SPACE OF THETA SERIES

\[
\frac{i^k}{z^{k+r}\sqrt{\det(A)}} \sum_{g \equiv 0 \pmod{N}} e^{2\pi i \frac{\gamma Ah}{N^2}} \sum_{n_1 \in \mathbb{Z}/l\mathbb{Z}} \left( t^* An_1 \right)^r e^{\pi i \left(-1/z\right) \frac{\lambda_{n_1} An_1}{N^2}}.
\]

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

\[
\frac{(-1)^{k+r} z^{k+r}}{\sqrt{\det(A)}} \sum_{n \equiv h \pmod{N}} \left( t^* An_1 \right)^r e^{\pi i \left(-1/z\right) \frac{\lambda_{n_1} An_1}{N^2}}.
\]

This implies that

\[
\theta(A, P, h, \begin{bmatrix} 1 & b \\ -1 & 1 \end{bmatrix} \cdot z) = \frac{(-i)^{k+r} z^{k+r}}{\sqrt{\det(A)}} \sum_{g \equiv 0 \pmod{N}} e^{2\pi i \frac{\gamma Ah}{N^2}} \theta(A, P, g, z), \quad (2.6)
\]

which is equivalent to (2.4).

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

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

\[= \theta(A, P, h, z + b)
\]

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

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

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

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

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

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

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

**Proposition 2.5.1.** Let $f$ be a positive even integer, and define $k = f/2$. Let $A \in M(f, \mathbb{Z})$ 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

$$
\left. \theta(A, P, 0, z) \right|_{k+r} = \theta(A, P, 0, z)
$$

(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

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

$$
= \sum_{n \in \mathbb{Z}^f \atop n \equiv 0 \pmod{1}} P(n)e^{2\pi i z Q(n)}
$$

$$
= \theta(A, P, 0, z).
$$

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

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

(2.8)

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

(2.9)

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

$$
\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}
$$

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

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

(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
2.5. THE CASE N = 1

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

\[
t\left(\begin{array}{cc}
-1 & 1 \\
1 & 0
\end{array}\right) = i^k, \quad t\left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right) = 1
\]

for \( b \in \mathbb{Z} \). Now

\[
\left(\begin{array}{cc}
-1 & 1 \\
1 & 0
\end{array}\right) \left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right) = \left(\begin{array}{cc}
-1 & -1 \\
-1 & 1
\end{array}\right).
\]

Applying these matrices to \( \theta(A, P, 0, z) \) we obtain:

\[
\theta(A, P, 0, z)|_k \left(\begin{array}{cc}
1 & -1 \\
1 & 0
\end{array}\right) = \theta(A, P, 0, z)|_k \left(\begin{array}{cc}
-1 & 1 \\
-1 & 0
\end{array}\right)
\]

\[
i^{2k} \theta(A, P, 0, z) = (-1)^k \theta(A, P, 0, z).
\]

Since \( \theta(A, P, 0, z) \) is not identically zero, we have \( i^{2k} = (-1)^k \). We also have the matrix identity

\[
\left(\begin{array}{cc}
1 & -b \\
1 & 0
\end{array}\right) \left(\begin{array}{cc}
1 & 1 \\
0 & 1
\end{array}\right) = \left(\begin{array}{cc}
-1 & -1 \\
-1 & 1
\end{array}\right) \left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right)
\]

for \( b \in \mathbb{Z} \). Applying these matrices to \( \theta(A, P, 0, z) \), we find that:

\[
i^{2k} \theta(A, P, 0, z) = (-1)^k \theta(A, P, 0, z)|_k \left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right)
\]

for \( b \in \mathbb{Z} \). Since \( i^{2k} = (-1)^k \), this implies that

\[
\theta(A, P, 0, z)|_{k+r} \left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right) = \theta(A, P, 0, z)
\]

for \( b \in \mathbb{Z} \). Therefore, \( t \) is trivial on all matrices of the form

\[
\left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right), \quad \left(\begin{array}{cc}
1 & b \\
0 & 1
\end{array}\right)
\]

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 $z \in H(1, R) = \{ z \in \mathbb{H}_1 : \text{Im}(z) > -\frac{\log(R)}{2\pi} \}$ (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 [14]). 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. \[ \square \]

### 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

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

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

$$\alpha_1 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7 + e_8),$$
$$\alpha_2 = e_1 + e_2,$$
$$\alpha_3 = -e_1 + e_2,$$
$$\alpha_4 = -e_2 + e_3,$$
$$\alpha_5 = -e_3 + e_4,$$
$$\alpha_6 = -e_4 + e_5,$$
$$\alpha_7 = -e_5 + e_6,$$
$$\alpha_8 = -e_6 + e_7.$$

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 $A = ((\alpha_i, \alpha_j))_{1 \leq i, j \leq 8}$. Here, $(\cdot, \cdot)$ is the usual inner product on $\mathbb{R}^8$. Explicitly, we have:

$$A = \begin{pmatrix}
2 & -1 & & & & & & \\
-1 & 2 & -1 & & & & & \\
2 & -1 & 2 & -1 & & & & \\
1 & -1 & 2 & -1 & -1 & & & \\
2 & -1 & 2 & -1 & -1 & & & \\
1 & -1 & 2 & -1 & -1 & 2 & & \\
2 & -1 & 2 & -1 & -1 & 2 & 2 & \\
1 & -1 & 2 & -1 & -1 & 2 & 2 & 2
\end{pmatrix}.$$

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:

$$Q(x_1, x_2, x_3, \ldots, x_8) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2$$
$$- x_1 x_3 - x_2 x_4 - x_3 x_4 - x_4 x_5 - x_5 x_6 - x_6 x_7 - x_7 x_8.$$

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

$$\theta(A, z) = \sum_{n=0}^{\infty} r(n) e^{2\pi i n}$$

where

$$r(n) = \# \{ m \in \mathbb{Z}^8 : Q(m) = n \}.$$
It is known that the dimension of the space of modular forms for $\text{SL}(2, \mathbb{Z})$ of weight 4 is one (see Proposition 2.26 on p. 46 of [22]). Moreover, this space contains the Eisenstein series

$$E(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)e^{2\pi inz}$$

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 $\text{SL}(2, \mathbb{Z})$

**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

$$\theta(A, P, h, z) = \sum_{\substack{g \pmod{cN} \\ g \equiv h \pmod{N}}} \theta(cA, P, g, cz)$$

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:

$$\theta(A, P, h, z) = \sum_{n \in \mathbb{Z}^f \cap \mathbb{Z}N} P(n)e^{2\pi izQ(n)/N} = \sum_{g \in \mathbb{Z}^f/c\mathbb{N}^f} \sum_{n_1 \in c\mathbb{N}^f} P(g + n_1)e^{2\pi izQ(g+n_1)/N^2}.$$
2.7. THE CASE $N > 1$

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

$$cN\mathbb{Z}^I \sim \{m \in \mathbb{Z}^I : m \equiv g \pmod{cN}\}$$

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

$$\theta(A, P, h, z) = \sum_{g \pmod{cN}} \sum_{m \equiv g \pmod{cN}} P(m)e^{2\pi i \frac{Q(m)}{N}}$$

$$= \sum_{g \equiv h \pmod{N}} \sum_{m \equiv g \pmod{cN}} P(m)e^{\pi i z \frac{mAm}{(cN)^2}}$$

$$= \sum_{g \equiv h \pmod{N}} \sum_{m \equiv g \pmod{cN}} P(m)e^{\pi i z \frac{mAm}{(cN)^2}}$$

$$= \sum_{g \equiv h \pmod{N}} \theta(cA, P, g, cz).$$

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

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

and assume that $c \neq 0$. Let

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

Define a function

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

by

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

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,

$$s_\alpha(g_1, g_2) = e^{-2\pi i \left(\frac{tA(g_1) + dQ(g_1)}{cN} \right)} s_\alpha(0, g_2 + dg_1) \quad (2.12)$$

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 $g, g' \in \mathbb{Z}^I$ with $g \equiv g' \pmod{cN}$ and $g \equiv g' \equiv g_2 \pmod{N}$. Write $g' = g + cNm$ for some $m \in \mathbb{Z}^I$. Then

$$e^{2\pi i \left(\frac{aQ(g') + bQ(g_1)}{cN} + \frac{dQ(g_1)}{cN} \right)} = e^{2\pi i \left(\frac{aQ(g + cNm) + bQ(g_1) + dQ(g_1)}{cN} \right)}$$
\[ e^{2\pi i \left( \frac{aQ(g) + \alpha N \cdot b s t + \alpha c^2 Q(m) + \alpha b_1 A g + c N \cdot b_2 A m + d Q(g_1)}{c N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{aQ(g) + b s t + dQ(g_1)}{c N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{aQ(g) + b_1 A g + dQ(g_1)}{c N^2} \right)}, \]
where in the last step we used that \( A g \equiv A g_1 \equiv 0 \pmod{N} \). It follows that \( s_\alpha \) is well-defined.

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

\[ e^{-2\pi i \left( \frac{b s \cdot g_1 + \alpha b s \cdot (c N) Q(g_1)}{N^2} \right)} s_\alpha(0, g_2 + d g_1) \]
\[ = \sum_{\substack{g \equiv g_2 + d g_1 \pmod{N}}} e^{-2\pi i \left( \frac{b s \cdot g_1 + \alpha b s \cdot (c N) Q(g_1)}{N^2} \right)} e^{2\pi i \left( \frac{aQ(g)}{c N^2} \right)} \]
\[ = \sum_{\substack{g \equiv g_2 \pmod{c N}}} e^{2\pi i \left( \frac{aQ(g) + b s \cdot b_1 A g + c N \cdot \alpha b s \cdot (c N) Q(g_1) - d c Q(g_1)}{c N^2} \right)} \]
\[ = \sum_{\substack{g \equiv g_2 \pmod{c N}}} e^{2\pi i \left( \frac{aQ(g) + b s \cdot b_1 A g + c N \cdot \alpha b s \cdot (c N) Q(g_1) + d Q(g_1)}{c N^2} \right)} \]
\[ = \sum_{\substack{g \equiv g_2 \pmod{c N}}} e^{2\pi i \left( \frac{aQ(g) + b s \cdot b_1 A g + c N \cdot \alpha b s \cdot (c N) Q(g_1) + d Q(g_1)}{c N^2} \right)} \]

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

\[ e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c q g)}{N^2} \right)} = e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c q g - h c N m)}{N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c N m)}{N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c q g) - h c q g m}{N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c q g) - h c q g m}{N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c q g) - h c q g m}{N^2} \right)} \]
\[ = e^{2\pi i \left( \frac{b s \cdot g_1 (a d g - h c q g) - h c q g m}{N^2} \right)} \]
where the last step follows because \( A g_1 \equiv 0 \pmod{N} \). We therefore have:

\[ e^{2\pi i \left( \frac{b s \cdot g_1 + \alpha b s \cdot (c N) Q(g_1)}{N^2} \right)} s_\alpha(0, g_2 + d g_1) = \sum_{\substack{g \equiv g_2 \pmod{c N}}} e^{2\pi i \left( \frac{aQ(g) + b s \cdot b_1 A g + c N \cdot \alpha b s \cdot (c N) Q(g_1)}{c N^2} \right)} \]
\[ e^{2\pi i \left( \frac{b s \cdot g_1 + \alpha b s \cdot (c N) Q(g_1)}{N^2} \right)} s_\alpha(0, g_2 + d g_1) = s_\alpha(g_1, g_2). \]
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 $m \in \mathbb{Z}^f$. Then

$$s_\alpha(g'_1, g_2) = e^{-2\pi i \left( \frac{b g_1 + dQ(g'_1)}{N} \right)} s_\alpha(0, g_2 + dg'_1)$$

$$= e^{-2\pi i \left( \frac{b g_1 + dQ(g'_1)}{N} \right)} s_\alpha(0, g_2 + d(g_1 + Nm))$$

$$= e^{-2\pi i \left( \frac{b g_1 + dQ(g'_1)}{N} \right)} s_\alpha(0, g_2 + d(g_1 + dNm))$$

$$= e^{-2\pi i \left( \frac{b g_1 + dQ(g'_1)}{N} \right)} s_\alpha(0, g_2 + dg_1)$$

$$= s_\alpha(g_1, g_2).$$

Here we used that $Ag_1 \equiv Ag_2 \equiv 0 \pmod{N}$. This completes the proof.

**Lemma 2.7.3.** 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 $P \in H_r(A)$. Let $h \in \mathbb{Z}^f$ be such that

$$Ah \equiv 0 \pmod{N}.$$

Let

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

and assume that $c$ is a positive integer. Then

$$\theta(A, P, h, z) \mid_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \frac{1}{i^{k+2r}c_k \sqrt{\det(A)}} \sum_{g \equiv 0 \pmod{N}} s_\alpha(g, h) \cdot \theta(A, P, g, z), \quad (2.13)$$

where $s_\alpha$ is defined in Lemma 2.7.2.

**Proof.** We have

$$\theta(A, P, h, z) \mid_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= j(\alpha, z)^{-k-r} \theta(A, P, h, \begin{bmatrix} az + b \\ cz + d \end{bmatrix})$$
\[ = j(\alpha, z)^{-k-r} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} \theta(cA, P, g, c \cdot \frac{az + b}{cz + d}) \]

\[ = j(\alpha, z)^{-k-r} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} \theta(cA, P, g, -\frac{1}{cz + d} + a) \]

\[ = j(\alpha, z)^{-k-r} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} e^{2\pi i \frac{Q_{cA}(g)}{cN} \theta} \left( cA, P, g, -\frac{1}{cz + d} \right) \]

\[ = j(\alpha, z)^{-k-r} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} e^{2\pi i \frac{Q(g)}{cN} \theta} \left( cA, P, g, -\frac{1}{cz + d} \right) \]

\[ = (-1)^{k+r} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} e^{2\pi i \alpha} \left( \theta(cA, P, g, \cdot) \right) \left[ -1 \right]^{k+r} (cz + d) \]

\[ = \frac{i^k(-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} e^{2\pi i \alpha} \left( \theta(cA, P, g, \cdot) \right) \left[ -1 \right]^{k+r} (cz + d) \]

\[ = \frac{i^k(-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g \pmod{cN}, g \equiv h \pmod{N}} e^{2\pi i \alpha} \left( \theta(cA, P, g, \cdot) \right) \left[ -1 \right]^{k+r} (cz + d) \]

\[ = \frac{i^k(-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g_1 \pmod{cN}, (cA)g_1 \equiv 0 \pmod{cN}} e^{2\pi i \alpha} \left( \theta(cA, P, g_1, \cdot) \right) \left[ -1 \right]^{k+r} (cz + d) \]

\[ = \frac{i^k(-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g_1 \pmod{cN}, (cA)g_1 \equiv 0 \pmod{cN}} e^{2\pi i \alpha} \left( \theta(cA, P, g_1, \cdot) \right) \left[ -1 \right]^{k+r} (cz + d) \]

\[ = \frac{i^k(-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g_1 \pmod{cN}, (cA)g_1 \equiv 0 \pmod{cN}} s_\alpha(g_1, h) \theta(cA, P, g_1, c) \]

\[ = \frac{i^k(-1)^{k+r}}{\sqrt{\det(cA)}} \sum_{g_1 \pmod{cN}, (cA)g_1 \equiv 0 \pmod{cN}} s_\alpha(g_1, h) \theta(cA, P, g_1, c) \]
2.7. THE CASE N > 1

\[ \sum_{g_1 \in \mathbb{Z}^f / N \mathbb{Z}^f} \sum_{m \in \mathbb{Z}^f / c N \mathbb{Z}^f} s_{\alpha}(g_1 + m, h) \theta(cA, P, g_1 + m, cz) \]

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

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

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

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

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 \(A \in M(f, \mathbb{Z})\) 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

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

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

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

for \(g \in Y(A)\).

**Proof.** To see that \(s\) is well defined, let \(g, q_1, q_2 \in Y\) and assume that \(q_2 = q_1 + Nq_3\) for some \(q_3 \in \mathbb{Z}^f\). Then

\[ ^t gAq_2 = ^t gAq_1 + N^t gAq_3 \]

\[ = ^t gAq_1 + N^t (Ag)Aq_3 \]
\[ \equiv \frac{1}{N} gAq_1 \pmod{N^2} \]

because \( Ag \equiv 0 \pmod{N} \). This implies that

\[ e^{2\pi i \frac{gAq_1}{N^2}} = e^{2\pi i \frac{gAq_2}{N^2}}, \]

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

\[ \frac{1}{N} gAq = N \frac{1}{N} m(Aq) \equiv 0 \pmod{N^2}, \]

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

\[ s(g) = \sum_{q \in Y(A)/NZ^f} e^{2\pi i \frac{gAq}{N^2}} = \sum_{q \in Y(A)/NZ^f} 1 = \#Y(A)/NZ^f. \]

Finally, assume that \( g \not\equiv 0 \pmod{N} \). Then there exists \( m \in \mathbb{Z} \) such that \( \frac{1}{N} gm \not\equiv 0 \pmod{N} \). This implies that \( \frac{1}{N} gNm \not\equiv 0 \pmod{N^2} \). Let

\[ q_1 = NA - 1 m. \]

This implies that \( e^{2\pi i \frac{gAq_1}{N^2}} \neq 1 \). Since the function \( Y(A)/NZ^f \to \mathbb{C}^\times \) defined by \( q \mapsto e^{2\pi i \frac{gAq}{N^2}} \) is a character, and since this character is non-trivial at \( q_1 \), it follows that summing this character over the elements of \( Y(A)/NZ^f \) gives 0; this means that \( s(g) = 0 \).

**Proposition 2.7.5.** 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

\[ Q(x) = \frac{1}{2} x Ax. \]

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

\[ Ah \equiv 0 \pmod{N}. \]

Let

\[ \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \]

and assume that \( d \) is a positive integer. Then

\[ \theta(A, P, h, z) \mid_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \left( \frac{1}{q^k} \sum_{q \equiv h \pmod{dN}} e^{2\pi i \frac{hQ(q)}{N^2}} \right) \cdot \theta(A, P, ah, z). \quad (2.14) \]
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:
\[
\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}
= (\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix}) \left[ \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right] 
= (\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} b & a \\ d & c \end{bmatrix}) \left[ \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right] 
= \frac{1}{i^{k+2r}d^{k}/\sqrt{\det(A)}} \sum_{q \pmod{N}} s_\alpha(q, h) \theta(A, P, q, z) \bigg|_{k+r} \begin{bmatrix} 1 & -1 \end{bmatrix}
= \frac{1}{i^{2r}d^{k}/\det(A)} \sum_{g \pmod{N}} \sum_{q \pmod{N}} s_\alpha(q, h) e^{2\pi i \frac{\nu gAq}{N^2}} \theta(A, P, g, z). 
\]
We can calculate the inner sum as follows:
\[
\sum_{q \pmod{N}} s_\alpha(q, h) e^{2\pi i \frac{\nu gAq}{N^2}} 
= \sum_{q \pmod{N}} s_\alpha(0, h - cq) e^{-2\pi i \left( \frac{-c gAq + \nu Q(q)}{N^2} \right)} e^{2\pi i \frac{\nu gAq}{N^2}} \quad (\text{cf. (2.12)})
= s_\alpha(0, h) \sum_{q \pmod{N}} e^{2\pi i \left( \frac{(h + g)Aq}{N^2} \right)} e^{2\pi i \left( \frac{-cQ(q)}{N^2} \right)} \quad (\text{cf. Lemma 1.5.8})
= s_\alpha(0, h) \sum_{q \pmod{N}} e^{2\pi i \left( \frac{(g + ah)Aq}{N^2} \right)} \quad (\text{cf. Lemma 2.7.4})
= s_\alpha(0, h) \times \begin{cases} 0 & \text{if } g \not\equiv -ah \pmod{N}, \\
\#Y(A)/N\mathbb{Z}l & \text{if } g \equiv -ah \pmod{N} \end{cases} \quad (\text{cf. Lemma 2.7.4}). 
\]
It follows that
\[
\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (2.15) 
\]
\[ \frac{\#Y(A)/NZ^f}{i^{2r}d^k \det(A)} \cdot s_\alpha(0, h) \cdot \theta(A, P, -ah, z) \]

\[ = \frac{(-1)^r \#Y(A)/NZ^f}{i^{2r}d^k \det(A)} \cdot s_\alpha(0, h) \cdot \theta(A, P, ah, z) \quad \text{(cf. (2.3))} \]

\[ = \frac{\#Y(A)/NZ^f}{d^k \det(A)} \cdot s_\alpha(0, h) \cdot \theta(A, P, ah, z). \]  

(2.16)

The definition of \( s_\alpha \) asserts that:

\[ s_\alpha(0, h) = \sum_{q \pmod{dN} \equiv h \pmod{N}} e^{2\pi i \left( \frac{qQ(n)}{dN} \right)}. \]

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

\[ \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \]  

so that \( \alpha = \begin{bmatrix} -1 \\ 1 \end{bmatrix} \).

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. \( \square \)

**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. \( \square \)

**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

\[ Q(x) = \frac{1}{2} x^t Ax. \]
2.7. THE CASE $N > 1$

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

$$
\theta(A, P, h, z) \bigg|_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = e^{2\pi i \frac{abQ(h)}{N^2}} \cdot \chi_A(d) \cdot \theta(A, P, ah, z) \quad (2.17)
$$

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

$$
g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N). \quad (2.18)
$$

If $d > 0$, then define

$$
\alpha(g) = \frac{1}{d^k} \sum_{q \in \mathbb{Z} / d\mathbb{Z}^f} e^{2\pi i \frac{abQ(q)}{N^2}}
$$

and if $d < 0$, define

$$
\alpha(g) = (-1)^k \alpha(\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}) = (-1)^k \alpha(\begin{bmatrix} -1 & \cdot \\ -1 & -1 \end{bmatrix}) g.
$$

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

$$
\theta(A, 1, 0, z) \bigg|_{k^g} = \left( \frac{1}{d^k} \sum_{q \in \mathbb{Z} / d\mathbb{Z}^f} e^{2\pi i \frac{abQ(q)}{dN^2}} \right) \cdot \theta(A, 1, 0, z)
$$
Assume that \(d\lt0\). Then by what we just proved,

\[
\theta(A, 1, 0, z)\big|_{+g} = \alpha(g) \cdot \theta(A, 1, 0, z)
\]

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

\[
\alpha(gg')\theta(A, 1, 0, z) = \alpha(g) \cdot \theta(A, 1, 0, z)\big|_{+g'}
\]

\[
\alpha(gg') = \alpha(g)\alpha(g')
\]

(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 \(d \gt 0\). Fix such a \(g\). If \(d = 1\) then it is clear that \(\alpha(g) \in \mathbb{Q}\). Assume that \(d \gt 1\). Then \(c \neq 0\) (recall that \(ad - bc = 1\)). Let \(n\) be an integer such that \(nc + d \gt 0\). Then

\[
\alpha\left[\begin{array}{cc} 1 & n \\ 1 & 1 \end{array}\right] \alpha(g) = \alpha\left[\begin{array}{cc} a & an + b \\ c & cn + d \end{array}\right]
\]

or

\[
1 \cdot \alpha(g) = \alpha\left[\begin{array}{cc} a & an + b \\ c & cn + d \end{array}\right]
\]

\[
\alpha(g) = \alpha\left[\begin{array}{cc} a & an + b \\ c & cn + d \end{array}\right].
\]

By the definition of \(\alpha\), this implies that

\[
\alpha(g) = \frac{1}{(cn + d)^k} \sum_{q \in \mathbb{Z}/d\mathbb{Z}} e^{2\pi i \frac{(an + b)Q(q)}{cn + d}}.
\]
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

\[ g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \]

then

\[ \chi_A(d) = \alpha\left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right). \tag{2.20} \]

Assume first that \( d > 0 \). By definition,

\[ \alpha(g) = \frac{1}{d^k} \sum_{q \in \mathbb{Z}^2/d\mathbb{Z}^2} e^{2\pi i \frac{\text{tr}(q)}{d}} \]

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 74

CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

We have:

and let $h$ be such that $Z = \left[ a \ b \ b \ N \right]$. Assume, therefore, that $(d, N) > 0$, 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),

$$\chi_A(d) = \alpha\left(\begin{bmatrix} a & b \\ N & d \end{bmatrix}\right) \cdot 1$$

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

$$\chi_A(d_1d_2) = \chi_A(d_1)\chi_A(d_2) = \chi_A(d_1d_2 + b_2N)$$

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

$$g = \left[ a \ b \ b \ N \right] \in \Gamma_0(N)$$

and let $h \in Y(A)$, i.e., $h \in \mathbb{Z}^f$ with $Ah \equiv 0 \pmod{N}$. First assume that $d > 0$.

We have:

$$\frac{1}{d^k} \sum_{q (\mod dN)} \sum_{q \equiv h (\mod N)} e^{2\pi i \frac{hq(g)}{dN}}$$
2.7. THE CASE $N > 1$

\[
\left| \frac{1}{d^k} \sum_{q \equiv k \mod N} e^{2\pi i \frac{bQ(q)}{dN^2}} \right|_{k+r} = \theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \theta(A, P, h, z)_{k+r} \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = (-1)^{k+r} \theta(A, P, h, z)_{k+r} \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = (-1)^{k+r} e^{2\pi i \frac{abQ(h)}{N^2}} \cdot \chi_A(-d) \cdot \theta(A, P, (-a)h, z) = (-1)^{k+r} e^{2\pi i \frac{abQ(h)}{N^2}} (-1)^k \cdot \chi_A(d) \cdot (-1)^k \theta(A, P, ah, z) \quad (\text{cf. (2.3))}
\]

This equality and (2.14) now imply (2.17) if $d > 0$. Assume that $d < 0$. We then have:

\[
\theta(A, P, h, z)_{k+r} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \theta(A, P, h, z)_{k+r} \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = (-1)^{k+r} \theta(A, P, h, z)_{k+r} \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = (-1)^{k+r} e^{2\pi i \frac{abQ(h)}{N^2}} \cdot \chi_A(-d) \cdot \theta(A, P, (-a)h, z) = (-1)^{k+r} e^{2\pi i \frac{abQ(h)}{N^2}} (-1)^k \cdot \chi_A(d) \cdot (-1)^k \theta(A, P, ah, z) \quad (\text{cf. (2.3))}
\]
\[ = e^{2\pi i \frac{ahQ(h)}{N^2}} \cdot \chi_A(d) \cdot \theta(A, P, ah, z). \]

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 \( \eta \neq 1 \), 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

\[
W(\chi)W(\bar{\chi}) = \left( \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}} \right) \cdot \left( \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \bar{\chi}(b)e^{2\pi i \frac{b}{p}} \right)
\]

\[
= \left( \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}} \right) \cdot \left( \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(b)^{-1}e^{2\pi i \frac{b}{p}} \right)
\]

\[
= \left( \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a}{p}} \right) \cdot \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(b')e^{2\pi i \frac{b}{p}}
\]

\[
= \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(ab')e^{2\pi i \frac{a+b}{p}}
\]

\[
= \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(ab)e^{2\pi i \frac{a+b}{p}}
\]

\[
= \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)e^{2\pi i \frac{a+1}{p}}
\]

\[
= \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) \left( -1 + \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} e^{2\pi i \frac{a+b}{p}} \right)
\]

\[
= \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a) \left( -1 + \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \frac{a+b}{p}} \right)
\]
2.7. THE CASE \(N > 1\)

\[
\sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \equiv 0 \pmod{p}} \chi(a)(-1 + \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \frac{(a+1)b}{p}}) \\
+ \sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \not\equiv 0 \pmod{p}} \chi(a)(-1 + \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \frac{(a+1)b}{p}}) \\
= \chi(-1)(-1 + p) \\
+ \sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \not\equiv 0 \pmod{p}} \chi(a)(-1 + 0) \quad (\text{cf. } (2.21)) \\
= \chi(-1)(p - 1) - \sum_{a \in \mathbb{Z}/p\mathbb{Z}, a+1 \not\equiv 0 \pmod{p}} \chi(a) \\
= \chi(-1)(p - 1) - (-\chi(-1) + \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)) \\
= \chi(-1)(p - 1) - (-\chi(-1) + 0) \quad (\text{cf. } (2.21)) \\
= p\chi(-1).
\]

This completes the proof. \(\square\)

**Lemma 2.7.9.** 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 \(A\). 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

\[
(\mathbb{Z}/\det(A)\mathbb{Z})^\times \xrightarrow{(\Delta)} (\mathbb{Z}/N\mathbb{Z})^\times \\
\downarrow \chi_A \\
\{\pm 1\}
\]

commutes. We have

\[
\chi_A(d) = \left(\frac{\Delta}{d}\right) = \left(\frac{(-1)^k \det(A)}{d}\right) \quad (2.22)
\]

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 \(\chi_A(d) = (\Delta\right)^d\) 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 [11]), 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

\[
\begin{bmatrix}
  a_1 \\
  \vdots \\
  a_f
\end{bmatrix}
\equiv
\begin{bmatrix}
  \alpha_1 \\
  \vdots \\
  \alpha_f
\end{bmatrix}
\pmod{p}.
\]

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^m A m}{p}}
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{2^m A m}{p}}
= \frac{1}{p^k} \cdot \sum_{m \in \mathbb{Z}/p\mathbb{Z}} e^{2\pi i \cdot \frac{1^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^m A U m}{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} \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} (1 + \left(\frac{M_i}{p}\right)) \cdot e^{2\pi i \cdot \frac{2a_i m_i}{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^{\pi i \cdot \frac{m_i}{p}}
2.7. THE CASE $N > 1$

\[
\begin{align*}
    &= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \frac{2a_i}{p} \right) \sum_{m_i \in \mathbb{Z}/p\mathbb{Z}} \left( \frac{m_i}{p} \right) e^{2\pi i \frac{m_i}{p}} \\
    &= \frac{1}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \frac{2a_i}{p} \right) W\left( \frac{1}{p} \right) \\
    &= \frac{W\left( \frac{1}{p} \right)^f}{p^k} \cdot \prod_{1 \leq i \leq f} \left( \frac{2a_i}{p} \right) \\
    &= \left( \frac{W\left( \frac{1}{p} \right)^2}{p^k} \right)^k \cdot \left( \frac{2^f a_1 \cdots a_f}{p} \right) \\
    &= \left( \frac{p\left( \frac{1}{p} \right)^2}{p^k} \right)^k \cdot \left( \frac{2^f \text{det}(U)^2 \text{det}(A)}{p} \right) \quad \text{(cf. Lemma 2.7.8)} \\
    &= \left( \frac{(-1)^k}{p} \right) \cdot \left( \frac{\text{det}(A)}{p} \right) \\
    &= \left( \frac{-1^k \text{det}(A)}{p} \right) \\
    &= \left( \frac{\Delta}{p} \right) \\
    &= \left( \frac{\Delta}{d} \right).
\end{align*}
\]

This completes the proof. \hfill \Box

**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

\[ Q(x) = \frac{1}{2} t x A x. \]

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

\[ Ah \equiv 0 \pmod{N}. \]

The analytic function $\theta(A, P, h, z)$ on $\mathbb{H}_1$ defined by

\[ \theta(A, P, h, z) = \sum_{n \equiv 0 \pmod{N}} P(n) e^{2\pi i \frac{Q(n)}{N}} \]

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

$$\theta(A, P, h, z)_{k+r, \alpha} = e^{2\pi i \frac{abQ(h)}{N^2}} \cdot \chi_A(d) \cdot \theta(A, P, ah, z).$$

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, $Q(h) \equiv 0 \pmod{N^2}$; this implies that $e^{2\pi i \frac{abQ(h)}{N^2}} = 1$. 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 $\sigma \in SL(2, \mathbb{Z})$ 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

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

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 $g \in Y(A)/N\mathbb{Z}^f$ from Lemma 2.4.1. By Lemma 2.4.1 the vector space $V(A, P)$ is preserved by $SL(2, \mathbb{Z})$ under the $|k+r|$ action. It follows that there exist constants $c(g) \in \mathbb{C}$ for $g \in Y(A)/N\mathbb{Z}^f$ such that

$$\theta(A, P, h, z)_{k+r} = \sum_{g \in Y(A)/N\mathbb{Z}^f} c(g) \cdot \theta(A, P, g, z).$$

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

$$\sum_{n \equiv g \pmod{N}} P(n)q^{\frac{Q(n)}{N}}$$
2.8. Example: The quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$

In this example we let

$$A = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$$
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 \( Y(A) \):
\[
\begin{align*}
h_0 &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad h_1 = \begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad h_2 = \begin{bmatrix} 2 \\ 2 \\ 0 \\ 0 \end{bmatrix}, \quad h_3 = \begin{bmatrix} 2 \\ 2 \\ 2 \\ 0 \end{bmatrix}, \quad h_4 = \begin{bmatrix} 2 \\ 2 \\ 2 \\ 2 \end{bmatrix}.
\end{align*}
\]
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:
\[
\begin{align*}
\theta(h_0) &= 1 + 8q_4^4 + 24q_4^8 + 32q_4^{12} + 24q_4^{16} + 48q_4^{20} + \cdots, \\
\theta(h_1) &= 2q_4 + 12q_4^5 + 26q_4^9 + 28q_4^{13} + 36q_4^{17} + 64q_4^{21} + \cdots.
\end{align*}
\]
2.8. EXAMPLE: THE QUADRATIC FORM $X_1^2 + X_2^2 + X_3^2 + X_4^2$

**Proposition 2.8.2.** Let

$\theta(h_2) = 4q_4^2 + 16q_4^6 + 24q_4^{10} + 32q_4^{14} + 52q_4^{18} + 48q_4^{22} + \cdots,$

$\theta(h_3) = 8q_4^3 + 16q_4^7 + 24q_4^{11} + 48q_4^{15} + 40q_4^{19} + 48q_4^{23} + \cdots,$

$\theta(h_4) = 16q_4^4 + 64q_4^{12} + 96q_4^{16} + 128q_4^{20} + 208q_4^{24} + 192q_4^{36} + \cdots.$

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

$$\dim M_2(\Gamma_0(2)) = 1$$ and

$$\dim M_2(\Gamma_0(4)) = 2.$$  

**Proof.** See, for example, Proposition 1.40 on page 23, Proposition 1.43 on page 24, and Theorem 2.23 on page 46 of [22].

**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,

$$M_2(\Gamma_0(4)) = \langle \theta(h_0), \theta(h_4) \rangle,$$

$$M_2(\Gamma_0(2)) = \langle \theta(h_0) + \theta(h_4) \rangle.$$  

**Proof.** By (2.4) we have

$$\theta(h_0)|_2 \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = -\frac{1}{4}(\theta(h_0) + 4 \cdot \theta(h_1) + 6 \cdot \theta(h_2) + 4 \cdot \theta(h_3) + \theta(h_4)),$$

$$\theta(h_1)|_2 \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = -\frac{1}{4}(\theta(h_0) + 2 \cdot \theta(h_1) - 2 \cdot \theta(h_3) - \theta(h_4)),$$

$$\theta(h_2)|_2 \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = -\frac{1}{4}(\theta(h_0) - 2 \cdot \theta(h_2) + \theta(h_4)),$$

$$\theta(h_3)|_2 \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = -\frac{1}{4}(\theta(h_0) - 2 \cdot \theta(h_1) + 2 \cdot \theta(h_3) - \theta(h_4)),$$

$$\theta(h_4)|_2 \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = -\frac{1}{4}(\theta(h_0) - 4 \cdot \theta(h_1) + 6 \cdot \theta(h_2) - 4 \cdot \theta(h_3) + \theta(h_4)).$$

By (2.5) we have:

$$\theta(h_0)|_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \theta(h_0),$$

$$\theta(h_1)|_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = i\theta(h_1),$$
CHAPTER 2. CLASSICAL THETA SERIES ON $\mathbb{H}_1$

\[ \theta(h_2) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = -\theta(h_2), \]
\[ \theta(h_3) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = -i\theta(h_3), \]
\[ \theta(h_4) \bigg|_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \theta(h_4). \]

Since $\text{SL}(2, \mathbb{Z})$ is generated by
\[ \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \]
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 $\dim W \neq 1$. Assume that $\dim W = 1$; 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
\[ F_1 \bigg|_2 \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \beta \left( \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right) F_1 \]
\[ a(\theta(h_0) + \theta(h_4)) - b\theta(h_2) = a\beta \left( \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right)(\theta(h_0) + \theta(h_4)) + b\beta \left( \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right)\theta(h_2). \]

This equality implies that $a = 0$ or $b = 0$. If $a = 0$ and $b \neq 0$, then
\[ F_1 \bigg|_2 \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} = \beta \left( \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \right) F_1 \]
\[ -\frac{b}{\theta(h_0) - 2 \cdot \theta(h_2) + \theta(h_4)} = \beta \left( \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \right)\theta(h_2). \]

This is a contradiction. Similarly, the case $a \neq 0$ and $b = 0$ leads to a contradiction. Thus, $V_1$ is irreducible.

To prove that $V_2$ is irreducible, let $W$ be a non-zero $\text{SL}(2, \mathbb{Z})$ subspace of $V_2$; we need to prove that $W = V_2$. An argument similar to that in the last paragraph proves that $W$ cannot be one-dimensional. Assume that $W$ is two-dimensional; we will obtain a contradiction. The formulas for the action of
\[ \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \]
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 The formulas for the action of
\[ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \]
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

\[
F|_2 \gamma = F \quad \text{for } \gamma \in \Gamma_0(2)
\]

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),

\[
\theta(h)|_2 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} = \frac{1}{i^k 2^2 \sqrt{\det(A)}} \sum_{g \in Y(A)/4\mathbb{Z}^4} s_\alpha(g, h) \theta(g)
\]

\[
= \frac{1}{-2^4} \sum_{g \in Y(A)/4\mathbb{Z}^4} s_\alpha(g, h) \theta(g). \tag{2.26}
\]

Let \(g \in Y(A)\), and write \(g = 2g'\) for some \(g' \in \mathbb{Z}^4\). We obtain

\[
s_\alpha(g, h) = \sum_{x \in \mathbb{Z}^4/4\mathbb{Z}^4} e^{2\pi i \left( \frac{Q(x) + hAx + Q(g)}{8} \right)}
\]

\[
= e^{2\pi i \left( \frac{Q(g)}{8} \right)} \sum_{x \in \mathbb{Z}^4/4\mathbb{Z}^4} e^{2\pi i \left( \frac{Q(x) + hAx}{8} \right)}
\]
\[ \theta(h) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_4) \]

\[ \theta(h_0) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_4) \]

\[ \theta(h_1) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_3) \]

\[ \theta(h_2) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_2) \]

\[ \theta(h_3) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_1) \]

\[ \theta(h_0) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_4) \]

\[ \theta(h_1) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_3) \]

\[ \theta(h_2) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_2) \]

\[ \theta(h_3) \bigg|_2 \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} = \theta(h_1) \]
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

\[ F|_2 \gamma = \theta(h_0)|_2 \gamma + \theta(h_4)|_2 \gamma \]

\[ = \theta(h_0)|_2 \gamma \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \theta(h_4)|_2 \gamma \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \]

\[ = \theta(h_0)|_2 \begin{bmatrix} a - 2b \\ 2(c - d) \\ 2c + d \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \theta(h_4)|_2 \begin{bmatrix} a - 2b \\ 2(c - d) \\ 2c + d \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \]

\[ = \theta(h_0)|_2 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \theta(h_4)|_2 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \]

\[ = \theta(h_4) + \theta(h_0) \]

\[ = F. \]

This proves our claim about $F$. \qed

**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

\[ 8 \cdot \sum_{m > 0, m|n, \ m \not\equiv 0 \pmod{4}} m. \]

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 [23]. Trivially, the function \( E(z) \) is contained in \( M_2(\Gamma_0(4)) \). The function

\[
E(z) \bigg|_2 \left[ \begin{array}{c} 2 \\ 1 \end{array} \right] = E(2z)
\]

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

\[
\theta(h_0, z) = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + 48q^5 + 96q^6 + 64q^7 + \cdots,
\]

\[
E(z) = \frac{1}{24} + q + q^2 + 4q^3 + q^4 + 6q^5 + 4q^6 + 8q^7 + \cdots,
\]

\[
E(2z) = \frac{1}{24} + q^2 + 4q^3 + q^4 + 6q^5 + 6q^6 + 4q^7 + \cdots.
\]

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

\[
a(n) = 8b(n) + 16c(n)
\]

\[
= \begin{cases} 
8\sigma_1(n) - 32\sigma_1(n/4) & \text{if } 4 | n, \\
8\sigma_1(n) & \text{if } n \text{ is even and } n/2 \text{ is odd}, \\
8\sigma_1(n) & \text{if } n \text{ is odd},
\end{cases}
\]

\[
= 8 \cdot \sum_{m > 0, m | n, m \not\equiv 0 \pmod{4}} m.
\]

This completes the proof. \( \square \)
Chapter 3

Notes

3.1
Let \( f \) be an even positive integer, and let \( A \in \text{M}(f, \mathbb{Z}) \) be an even integral symmetric positive-definite matrix. Let \( N \) be the level of \( A \). We know that \( N = 1 \) if and only if \( \det(A) = 1 \) (cf. Corollary 1.5.5). Also, we know that if \( c \) is a positive integer, then \( cA \) has level \( cN \) (cf. Corollary 1.5.7). Is it the case that if \( N = 2 \), then \( A = 2B \) for some \( B \in \text{M}(f, \mathbb{Z}) \) with \( B \) an even integral symmetric positive-definite matrix of level 1?

3.2
As regards the basis problem, how would elements of \( \text{M}_k(\text{SL}(2, \mathbb{Z})) \) be obtained?

3.3
As concerns the general connection between classical theta series on \( \mathbb{H}_1 \) and Eisenstein series, the reference to Siegel’s work on page 110 of [21] is relevant.

3.4
It might be interesting to consider when classical theta series with \( r = 0 \) are cuspidal using (2.13).

3.5
Formula (2.13) suggests that there might be a representation of \( \text{SL}(2, \mathbb{Z}) \) of dimension \( \# Y(A)/NZ^f \) of which \( V(A, P) \) is a quotient. Is this true? Let
Y(A)/NZ^f = \{g_1, \ldots, g_t\}. One would have to verify that the appropriate function

$$S : \text{SL}(2, \mathbb{Z}) \to \text{GL}(t, \mathbb{C})$$

is a homomorphism, that is, that

$$S(\alpha \beta) = S(\alpha) S(\beta) \text{ for } \alpha, \beta \in \text{SL}(2, \mathbb{Z}). \quad (3.1)$$

The group \(\text{SL}(2, \mathbb{Z})\) is generated by

$$W = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}, \quad U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$ 

It follows that to verify (3.1) holds for all \(\alpha\) and \(\beta\), it would suffice to check that (3.1) holds for all \(\alpha\) and for \(\beta \in \{W, U\} \). Let

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

There are three cases for \(\alpha\):

**Case 1.** Assume that \(c \neq 0\). Then:

$$S(\alpha) = \frac{1}{i^{k+2r}e^{k\sqrt{i \det(A)}}} \begin{bmatrix} s_\alpha(g_1, g_1) & \cdots & s_\alpha(g_t, g_1) \\ \vdots & \ddots & \vdots \\ s_\alpha(g_1, g_t) & \cdots & s_\alpha(g_t, g_t) \end{bmatrix}. $$

**Case 2.** Assume that \(c = 0, a = d = 1\). Then

$$S(\alpha) = S\left( \begin{bmatrix} 1 & b \\ 1 \end{bmatrix} \right) = \begin{bmatrix} e^{2\pi ib \frac{Q(g_1)}{N^2}} \\ \vdots \\ e^{2\pi ib \frac{Q(g_t)}{N^2}} \end{bmatrix}. $$

**Case 3.** Assume that \(c = 0, a = d = -1\). Then

$$S(\alpha) = S\left( \begin{bmatrix} -1 & b \\ -1 \end{bmatrix} \right) = \begin{bmatrix} (-1)^k e^{-2\pi ib \frac{Q(g_1)}{N^2}} \\ \vdots \\ (-1)^k e^{-2\pi ib \frac{Q(g_t)}{N^2}} \end{bmatrix}. $$

Assume that \(\alpha\) is as in Case 1, and that \(\beta = U\). Then

$$S(\alpha) S(\beta) = S(\alpha) S(U) \quad = \frac{1}{i^{k+2r}e^{k\sqrt{i \det(A)}}} \begin{bmatrix} e^{2\pi i \frac{Q(g_1)}{N^2}} s_\alpha(g_1, g_1) & \cdots & e^{2\pi i \frac{Q(g_t)}{N^2}} s_\alpha(g_t, g_1) \\ \vdots & \ddots & \vdots \\ e^{2\pi i \frac{Q(g_1)}{N^2}} s_\alpha(g_1, g_t) & \cdots & e^{2\pi i \frac{Q(g_t)}{N^2}} s_\alpha(g_t, g_t) \end{bmatrix}. $$
On the other hand,
\[ \alpha \beta = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix}. \]

It follows that, for \( i, j \in \{1, \ldots, t\} \),
\[
 s_{\alpha \beta}(g_i, g_j) = \sum_{g \equiv g_i, (\text{mod } N)} e^{\frac{iQ(g)+t}{cN^2}} s_{\alpha}(g, g_j) e^{\frac{iQ(g)}{cN^2}}
 = e^{\frac{Q(g_j)}{cN^2}} s_{\alpha}(g_i, g_j).
\]

This verifies (3.1) under the given assumptions.
Assume that \( \alpha \) is as in Case 2, and that \( \beta = U \). Then (3.1) is easily verified.
Assume that \( \alpha \) is as in Case 3, and that \( \beta = U \). We have
\[
 S(\alpha)S(U) = \begin{bmatrix} (-1)^k + i e^{-2\pi i \frac{Q(g_1)}{N^2}} \\ \vdots \\ e^{2\pi i \frac{Q(g_1)}{N^2}} \end{bmatrix}
 \begin{bmatrix} (-1)^k + r e^{-2\pi i \frac{Q(g_1)}{N^2}} \\ \vdots \\ e^{2\pi i \frac{Q(g_1)}{N^2}} \end{bmatrix}
 = \begin{bmatrix} (-1)^k e^{-2\pi i (b-1) \frac{Q(g_1)}{N^2}} \\ \vdots \\ (-1)^k e^{-2\pi i (b-1) \frac{Q(g_t)}{N^2}} \end{bmatrix}
 = S\left( \begin{bmatrix} -1 & b-1 \\ -1 & -1 \end{bmatrix} \right)
 = S\left( \begin{bmatrix} -1 & b \\ -1 & 1 \end{bmatrix} \right)
 = S(\alpha U).
\]

This verifies (3.1) under the given assumptions.
Assume that \( \alpha \) is as in Case 1, and that \( \beta = W \). We have
\[
 S(\alpha)S(W) = \frac{1}{i^{k+2r}c^k \sqrt{\det(A)}} \begin{bmatrix} s_{\alpha}(g_1, g_1) & \cdots & s_{\alpha}(g_1, g_t) \\ \vdots & \ddots & \vdots \\ s_{\alpha}(g_t, g_1) & \cdots & s_{\alpha}(g_t, g_t) \end{bmatrix}
\]
\[
\sum_{k=1}^{t} s_\alpha(g_k; g_t) e^{2\pi i \frac{\nu_1 A g_k}{N^2}} = \sum_{k=1}^{t} \sum_{\substack{g \pmod{cN} \\ g \equiv g_t \pmod{N}}} e^{2\pi i \left( \frac{S(g) + \nu_2 A g + d \nu_1 g_k}{cN^2} \right)} e^{2\pi i \frac{\nu_1 A g_k}{N^2}}
\]
Appendix A

Some tables

A.1 Tables of fundamental discriminants

<table>
<thead>
<tr>
<th>Discriminant</th>
<th>Factorization</th>
<th>Discriminant</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-3 = -3$</td>
<td>$-35 = (-7) \cdot 5$</td>
<td>$-68 = (-4) \cdot 17$</td>
</tr>
<tr>
<td>$-4 = -4$</td>
<td>$-39 = (-3) \cdot 13$</td>
<td>$-71 = -71$</td>
</tr>
<tr>
<td>$-7 = -7$</td>
<td>$-40 = (-8) \cdot 5$</td>
<td>$-79 = -79$</td>
</tr>
<tr>
<td>$-8 = -8$</td>
<td>$-43 = -43$</td>
<td>$-83 = -83$</td>
</tr>
<tr>
<td>$-11 = -11$</td>
<td>$-47 = -47$</td>
<td>$-84 = (-4) \cdot (-3) \cdot (-7)$</td>
</tr>
<tr>
<td>$-15 = (-3) \cdot 5$</td>
<td>$-51 = (-3) \cdot 17$</td>
<td>$-87 = (-3) \cdot 29$</td>
</tr>
<tr>
<td>$-19 = -19$</td>
<td>$-52 = (-4) \cdot 13$</td>
<td>$-88 = (-11) \cdot 8$</td>
</tr>
<tr>
<td>$-20 = (-4) \cdot 5$</td>
<td>$-55 = (-11) \cdot 5$</td>
<td>$-91 = (-7) \cdot 13$</td>
</tr>
<tr>
<td>$-23 = -23$</td>
<td>$-56 = (-7) \cdot 8$</td>
<td>$-95 = (-19) \cdot 5$</td>
</tr>
<tr>
<td>$-24 = (-3) \cdot 8$</td>
<td>$-59 = -59$</td>
<td></td>
</tr>
<tr>
<td>$-31 = -31$</td>
<td>$-67 = -67$</td>
<td></td>
</tr>
</tbody>
</table>

Table A.1: Negative fundamental discriminants between $-1$ and $-100$, factored into products of prime fundamental discriminants.
<table>
<thead>
<tr>
<th>Discriminant</th>
<th>Factored as</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>37 = 37</td>
</tr>
<tr>
<td>5</td>
<td>40 = 8 \cdot 5</td>
</tr>
<tr>
<td>8</td>
<td>41 = 41</td>
</tr>
<tr>
<td>12 = (-4)(-3)</td>
<td>44 = (-4) \cdot (-11)</td>
</tr>
<tr>
<td>13</td>
<td>53 = 53</td>
</tr>
<tr>
<td>17</td>
<td>56 = (-8) \cdot (-7)</td>
</tr>
<tr>
<td>21 = (-3)(-7)</td>
<td>57 = 57</td>
</tr>
<tr>
<td>24 = (-8)(-3)</td>
<td>60 = (-4) \cdot (-3) \cdot 5</td>
</tr>
<tr>
<td>28 = (-4)(-7)</td>
<td>61 = 61</td>
</tr>
<tr>
<td>29</td>
<td>65 = (-8) \cdot (-7)</td>
</tr>
<tr>
<td>33</td>
<td>69 = (-3)(-23)</td>
</tr>
<tr>
<td></td>
<td>73 = 73</td>
</tr>
<tr>
<td></td>
<td>76 = (-4) \cdot (-19)</td>
</tr>
<tr>
<td></td>
<td>77 = (-7) \cdot (-11)</td>
</tr>
<tr>
<td></td>
<td>85 = 5 \cdot 15</td>
</tr>
<tr>
<td></td>
<td>88 = (-8) \cdot (-11)</td>
</tr>
<tr>
<td></td>
<td>89 = 89</td>
</tr>
<tr>
<td></td>
<td>92 = (-4) \cdot (-23)</td>
</tr>
<tr>
<td></td>
<td>93 = (-3) \cdot (-31)</td>
</tr>
<tr>
<td></td>
<td>97 = 97</td>
</tr>
</tbody>
</table>

Table A.2: Positive fundamental discriminants between 1 and 100, factored into products of prime fundamental discriminants.
## Index

<table>
<thead>
<tr>
<th>Letter</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>adjoint</td>
<td>23</td>
</tr>
<tr>
<td>C</td>
<td>congruence subgroup</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>cusp form</td>
<td>31</td>
</tr>
<tr>
<td>D</td>
<td>determinant</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Dirichlet character</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>conductor</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>induced</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Legendre symbol</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>primitive</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>principal</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>product</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>discriminant</td>
<td>21</td>
</tr>
<tr>
<td>E</td>
<td>Euclidean domain</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>even integral symmetric matrix</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>level</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>extension of a Dirichlet character</td>
<td>1</td>
</tr>
<tr>
<td>F</td>
<td>Fourier transform</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>fundamental discriminant</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>prime</td>
<td>6</td>
</tr>
<tr>
<td>G</td>
<td>Gauss sum</td>
<td>76</td>
</tr>
<tr>
<td>H</td>
<td>Hecke congruence subgroup</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>holomorphic at the cusps</td>
<td>31</td>
</tr>
<tr>
<td>K</td>
<td>Kronecker symbol</td>
<td>16</td>
</tr>
<tr>
<td>L</td>
<td>Legendre symbol</td>
<td>3</td>
</tr>
<tr>
<td>M</td>
<td>modular form</td>
<td>31</td>
</tr>
<tr>
<td>P</td>
<td>prime fundamental discriminant</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>principal congruence subgroup</td>
<td>29</td>
</tr>
<tr>
<td>Q</td>
<td>quadratic form</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>level</td>
<td>25</td>
</tr>
<tr>
<td>R</td>
<td>real valued</td>
<td>3</td>
</tr>
<tr>
<td>S</td>
<td>Schwartz function</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Schwartz space</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Siegel upper half-space</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>smooth function</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>spherical functions</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>symplectic group</td>
<td>31</td>
</tr>
<tr>
<td>V</td>
<td>vanishes at the cusps</td>
<td>31</td>
</tr>
</tbody>
</table>
Symbols

$M_k(\Gamma)$, the space of modular forms of weight $k$ with respect to $\Gamma$ .......... 31
$S_k(\Gamma)$, the space of cusp forms of weight $k$ with respect to $\Gamma$ ............ 31
$\Gamma(N)$, the principal congruence subgroup ..................................... 29
$\Gamma_0(N)$, the Hecke congruence subgroup ....................................... 29
$\text{Sp}(2n, \mathbb{R})$, the symplectic group of degree $n$ over $\mathbb{R}$ ............ 31
$\mathbb{H}_n$, the Siegel upper half-space of degree $n$ ......................... 34
Bibliography


