Theta Series

Brooks Roberts

University of Idaho

Course notes as of October 3, 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

2 Theta series in one variable .......................... 29
   2.1 Definition and convergence ......................... 29
   2.2 The Poisson summation formula ..................... 33
   2.3 Differential operators ............................... 41

A Some tables ........................................... 47
   A.1 Tables of fundamental discriminants ................. 47

Index ...................................................... 49

Bibliography .............................................. 52

List of Tables

A.1 Negative fundamental discriminants between −1 and −100 . . 47
A.2 Positive fundamental discriminants between 1 and 100 . . . . 48
Chapter 1

Background

1.1 Dirichlet characters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$
f(a + xN) = \chi(\epsilon(a + zN))
= f(\epsilon) \chi(\epsilon a + zN)
= f(\epsilon) \chi(\epsilon a + \underbrace{N + \cdots + N}_z)
$$
Let $a \in Z$ with $(a,N) = 1$; we assert that $f(a) \neq 0$. Since $(a,N) = 1$, there exists $b \in Z$ such that $ab = 1 + kN$ for some $k \in Z$. 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 $\chi(a + NZ) = f(a)$ for $a \in Z$ 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

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

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

$$(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times,$$ 

and we can form the composition $\chi$

$$(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\beta} \mathbb{C}^\times.$$ 

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

CHAPTER 1. BACKGROUND

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 $(\frac{\cdot}{p})$ is also $p$, so that $(\frac{\cdot}{p})$ 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 $f : \mathbb{Z} \to \mathbb{C}$ 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 $\chi_2(p) = 0$. □
Let the notation be as in Lemma 1.1.4. We refer to the Dirichlet character \( \chi \mod N \) as the **product** of \( \chi_1 \) and \( \chi_2 \), and we write \( \chi_1 \chi_2 \) for \( \chi \).

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

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

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 \( a \equiv 1 \mod M_1 \). By the Chinese remainder theorem, there exists an integer \( b \) such that \( b \equiv a \mod M_1 \), \( b \equiv 1 \mod f(\chi_2) \), and \( (b, N) = 1 \). Evidently, \( b \equiv 1 \mod f(\chi) \). Hence, \( 1 = \chi(b) = \chi_1(b)\chi_2(b) = \chi_1(a) \). By the minimality of \( f(\chi_1) \) we must now have \( M_1 = f(\chi_1) \). Similarly, \( M_2 = f(\chi_2) \). The final assertion of the lemma is straightforward. \( \square \)

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

**Proof.** We have already remarked that \( (\frac{x}{p}) \) is a real valued primitive Dirichlet character modulo \( p \). To prove the remaining assertions, let \( e \) be a positive integer, and assume that \( \chi \) is a real valued primitive Dirichlet character modulo \( p^e \); we will prove that \( \chi = (\frac{x}{p}) \) 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 \( (\frac{x}{p}) \) is also a real valued Dirichlet character modulo \( p^e \) such that \( (\frac{x}{p}) = -1 \) 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 \( (\frac{x}{p}) = -1 \), so that \( \chi(x) = (\frac{x}{p}) \). 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 \( \chi = (\frac{x}{p}) \). We see that if \( e = 1 \), then the Legendre symbol \( (\frac{x}{p}) \) 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 \( (\frac{x}{p}) \mod p^e \) 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 \( \varepsilon_4 \mod 4 = 2^2 \) which is defined by

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

\[
\varepsilon'_8(1) = 1, \quad \varepsilon''_8(1) = 1,
\]

\[
\varepsilon'_8(3) = -1, \quad \varepsilon''_8(3) = 1,
\]

\[
\varepsilon'_8(5) = -1, \quad \varepsilon''_8(5) = -1,
\]

\[
\varepsilon'_8(7) = 1, \quad \varepsilon''_8(7) = -1.
\]

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

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

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

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

Finally, assume that \( e \geq 4 \) and let \( \chi \) be a real valued Dirichlet character modulo \( p^e \). Let \( n \in \mathbb{Z} \) be such that \((n, 2) = 1 \) and \( n \equiv 1 \pmod{8} \). It is known that there exists \( a \in \mathbb{Z} \) such that \( n \equiv a^2 \pmod{8} \). 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

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

or

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

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

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

or

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

or

\[
D = p \text{ for } p \text{ a prime such that } p \equiv 1 \pmod{4}.
\]
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 \( D \equiv 1 \) (mod 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 \( p \equiv 3 \) (mod 4). We have

\[
1 \equiv D \quad \text{(mod 4)}
\]

\[
\equiv (-1)^r 3^r \quad \text{(mod 4)}
\]

\[
1 \equiv (-1)^{r+1} \quad \text{(mod 4)}.
\]

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

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

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

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

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

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

\[
D = -4 \prod_{p \in \{p_1, \ldots, p_t\}, p \equiv 1 \text{ (mod 4)}} p
\]
CHAPTER 1. BACKGROUND

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

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

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

Each of the factors in the last equation is a prime fundamental discriminant, which proves the lemma in this case. Now assume that $-p_1 \cdots p_t \equiv 3 \mod 4$. 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 $p \equiv 3 \mod 4$. We have

$$3 \equiv -p_1 \cdots p_t \mod 4$$

$$-1 \equiv (-1)^3 r \mod 4$$

$$1 \equiv (-1)^r \mod 4.$$

It follows that $r$ is even. Hence,

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

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

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

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

Assume that $D > 0$ and $D \equiv 1 \mod 4$. 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 $p \equiv 3 \mod 4$. We have

$$1 \equiv D \mod 4$$

$$\equiv 3^r \mod 4$$

$$1 \equiv (-1)^r \mod 4.$$

We see that $r$ is even. Therefore,

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

$$= \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 1 \mod 4} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 3 \mod 4} p \right)$$
1.2. FUNDAMENTAL DISCRIMINANTS

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

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 \( D \equiv 0 \ (\text{mod } 4) \). 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 \( 3 \ (\text{mod } 4) \). Assume first that \( p_1 \cdots p_t \equiv 2 \ (\text{mod } 4) \). Then exactly one of \( p_1, \ldots, p_t \) is even, say \( p_1 = 2 \). Let \( r \) be the number of the primes \( p \) from \( p_2, \ldots, p_t \) such that \( p \equiv \pm 3 \ (\text{mod } 4) \). We have

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

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

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

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 \( p \equiv \pm 3 \ (\text{mod } 4) \). We have

\[
3 \equiv p_1 \cdots p_t \ (\text{mod } 4)
\]

\[
-1 \equiv 3^r \ (\text{mod } 4)
\]

\[
-1 \equiv (-1)^r \ (\text{mod } 4)
\]

\[
1 \equiv (-1)^{r+1} \ (\text{mod } 4)
\]

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

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

\[
= 4 \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 1 \ (\text{mod } 4)} p \right) \times \left( \prod_{p \in \{p_1, \ldots, p_t\}, \ p \equiv 3 \ (\text{mod } 4)} p \right)
\]

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

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

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

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

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

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

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

Note that since $D$ is a fundamental discriminant, we have $D \not\equiv 3 \pmod{8}$ and $D \not\equiv 7 \pmod{8}$. If $n$ is a positive integer, and $n = p_1^{e_1} \cdots p_t^{e_t}$ is the prime factorization of $n$, where $p_1, \ldots, p_t$ are primes, then we define

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

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

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

for all positive integers $n$, where we define

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

Finally, we define

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

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

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

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

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

**Proof.** It is easy to verify that $\chi_{D_1D_2}(p) = \chi_{D_1}(p)\chi_{D_2}(p)$ for all primes $p$, $\chi_{D_1D_2}(-1) = \chi_{D_1}(-1)\chi_{D_2}(-1)$, and $\chi_{D_1D_2}(0) = 0 = \chi_{D_1}(0)\chi_{D_2}(0)$. The assertion of the lemma now follows from the definitions of $\chi_D$, $\chi_{D_1}$, and $\chi_{D_2}$ on composite numbers. \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 $\epsilon_4, \epsilon_8'$ and $\epsilon_8''$ 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 $\chi_{-8}(p) = \epsilon_8''(p)$ for all primes $p$. Also, $\chi_{-8}(-1) = -1 = \epsilon_8''(-1)$ and $\chi_{-8}(0) = 0 = \epsilon_8''(0)$. Since $\chi_{-8}$ and $\epsilon_8''$ are multiplicative, it follows that

$$\chi_{-8} = \epsilon_8''$$

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)^{p-1}
= \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}, \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}

Also, $\chi_4(2) = 0$, $\chi_4(-1) = -1$, and $\chi_4(0) = 0$. We see that $\chi_4(p) = \varepsilon_4(p)$ for all primes $p$. Also, $\chi_4(-1) - 1 = \varepsilon_4(-1)$ and $\chi_4(0) = 0 = \varepsilon_4(0)$. Since $\chi_4$ and $\varepsilon_4$ are multiplicative, it follows that

$$\chi_4 = \varepsilon_4,$$

so that $\chi_4$ corresponds to a primitive Dirichlet character mod $|4| = 4$.

Assume that $D = 8$. Let $p$ be an odd prime. Then

$$\chi_8(p) = \left(\frac{8}{p}\right)$$
$$= \left(\frac{2}{p}\right)^3$$
$$= \left(\frac{2}{p}\right)$$
$$= (-1)^{\frac{p^2-1}{8}}$$
$$= \begin{cases} 
1 & \text{if } p \equiv 1, 7 \pmod{8}, \\
-1 & \text{if } p \equiv 3, 5 \pmod{8}.
\end{cases}
$$

Also, $\chi_8(2) = 0$, $\chi_8(-1) = 1$, and $\chi_8(0) = 0$. We see that $\chi_8(p) = \varepsilon'_8(p)$ for all primes $p$. Also, $\chi_8(-1) = 1 = \varepsilon'_8(-1)$ and $\chi_8(0) = 0 = \varepsilon'_8(0)$. Since $\chi_8$ and $\varepsilon'_8$ are multiplicative, it follows that

$$\chi_8 = \varepsilon'_8,$$

so that $\chi_8$ corresponds to a primitive Dirichlet character mod $|8| = 8$.

Assume that $D = -q$ for a prime $q$ such that $q \equiv 3 \pmod{4}$. Let $p$ be an odd prime. Then

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

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

Also,

\[
\chi_D(2) = \begin{cases} 
1 & \text{if } -q \equiv 1 \pmod{8}, \\
-1 & \text{if } -q \equiv 5 \pmod{8}
\end{cases} \\
= \begin{cases} 
1 & \text{if } q \equiv 7 \pmod{8}, \\
-1 & \text{if } q \equiv 3 \pmod{8}
\end{cases} \\
= (-1)^{\frac{q^2+1}{8}} \\
= \left( \frac{2}{q} \right),
\]

and

\[
\chi_D(-1) = -1 \\
= (-1)^{\frac{q^2+1}{8}} \\
= \left( \frac{-1}{q} \right).
\]

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

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

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

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

\[
\chi_D(-1) = 1
\]
\[
\begin{align*}
&= (-1)^{\frac{q-1}{2}} \\
&= \left( \frac{-1}{q} \right).
\end{align*}
\]

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

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

\[
\chi_D = \begin{cases} 
\varepsilon_8^2 & \text{if } D = -8, \\
\varepsilon_4 & \text{if } D = -4, \\
\varepsilon_8' & \text{if } D = 8, \\
\left( \frac{-1}{p} \right) & \text{if } D = -p \text{ is a prime with } p \equiv 3 \pmod{4}, \\
\left( \frac{-1}{p} \right) & \text{if } D = p \text{ is a prime with } p \equiv 1 \pmod{4}.
\end{cases}
\] (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

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

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

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

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 \( \chi_i = \left( \frac{p_i}{\varphi} \right) \), the Legendre symbol. By (1.2), \( \chi_i = \chi_D \), 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), \( \chi_i = \chi_D \), 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. \( \square \)

1.3 Quadratic extensions

**Proposition 1.3.1.** The map

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

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:

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

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

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

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

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

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

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 [18], or Theorem 25 on page 74 of [10].

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

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

### 1.4 Kronecker Symbol

Let $\Delta$ be a non-zero integer such that $\Delta \equiv 0, 1$ or $2 \pmod{4}$. We define a function,

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

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

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

Note that, since by assumption $\Delta \equiv 0, 1$ or $2 \pmod{4}$, the cases $\Delta \equiv 3 \pmod{8}$ and $\Delta \equiv 7 \pmod{8}$ do not occur. We see that if $p$ is a prime, then $p|\Delta$ if and only if $\left( \frac{\Delta}{p} \right) = 0$. If $n$ is a positive integer, and

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

then

$$\left( \frac{n}{p} \right) = \left( \frac{p_1}{p} \right)^{e_1} \cdots \left( \frac{p_t}{p} \right)^{e_t}.$$
1.4. KRONECKER SYMBOL

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

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

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

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

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 \( \left( \frac{\Delta}{a} \right) = 0 \) 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 \( D_{fd} \) and a unique positive integer \( m \) such that

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

**Proof.** We first prove the existence of \( m \) and \( D_{fd} \). 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 \( D = m^2 D_{fd} \) with \( m = a \) and \( D_{fd} = b \) 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 \( D = m^2 D_{fd} \) with \( m = 2^k a \) and \( D_{fd} = 8b \) 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 \( D = m^2 D_{fd} \) with \( m = 2^k a \) and \( D_{fd} = b \) a fundamental discriminant. If \( b \equiv 3 \pmod{4} \), then \( D = m^2 D_{fd} \) with \( m = 2^{k-1} a \) and \( D_{fd} = 4b \) a fundamental discriminant. This completes the proof the existence of \( m \) and \( D_{fd} \).

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

Proposition 1.4.2. Let $\Delta$ be a non-zero integer with $\Delta \equiv 0, 1 \text{ or } 2 \pmod{4}$. 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 $D = m^2 D_{\text{fd}}$ with $m$ a positive integer, and $D_{\text{fd}}$ a fundamental discriminant, as in Lemma 1.4.1. The Kronecker symbol $(\Delta \cdot)$ is a Dirichlet character modulo $|D|$, and is the Dirichlet character induced by the mod $|D_{\text{fd}}|$ Dirichlet character $\chi_{D_{\text{fd}}}$.

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

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

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

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

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

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

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

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

$$= \left(\frac{D_{\text{fd}}}{p}\right)$$

$$= \chi_{D_{\text{fd}}}(p)$$

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

Assume next that \( p = 2 \). If \( 2|D \), then also \( 2|\Delta \), so that \( \alpha(2) \) and \( \left( \frac{\Delta}{2} \right) \) 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 \( D = m^2 D_{ld} \), we must have \( D_{ld} \equiv D \pmod{8} \) (since \( a^2 \equiv 1 \pmod{8} \) for any odd integer \( a \)). Therefore,

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

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

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

To finish the proof we note that

\[
\left( \frac{\Delta}{-1} \right) \text{ evaluated at } -1 = \text{sign}(\Delta) 
= \text{sign}(D) 
= \text{sign}(D_{ld}) 
= \chi_{D_{ld}}(-1) 
= \alpha(-1).
\]

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

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

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

(1.3)

for all integers \( a \).

**Proof.** It is easy to verify that \( \Delta_1 \Delta_2 \equiv 0, 1 \) or \( 2 \pmod{4} \), and that if \( \Delta_1 = 1 \) or \( \Delta_2 = 1 \), then (1.3) holds. Assume that \( \Delta_1 \neq 1 \) and \( \Delta_2 \neq 1 \). Since \( \left( \frac{\Delta_1}{a} \right) \), \( \left( \frac{\Delta_2}{a} \right) \), and \( \left( \frac{\Delta_1 \Delta_2}{a} \right) \) 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 an 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 \( A \in \text{M}(f, \mathbb{Z}) \), and assume that \( A \) is symmetric. Then \( A \) is even if and only if \( {}^t y A y \) is an even integer for all \( y \in \mathbb{Z}^f \).

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

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

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

\[ {}^t y_i = (0, \ldots, 0, 1, 0, \ldots, 0) \]

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

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

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

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

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

with

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

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

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

where

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

We denote the **determinant** of \( A \) by

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

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

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

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

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

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

For this example we have

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

**Lemma 1.5.2.** Let $A \in \text{M}(f, \mathbb{Z})$ 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

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

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

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 \(f\) 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 \(\sigma(i) = i\). 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,

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

and we conclude that \(\Delta \equiv D \equiv 0 \mod 2\).

Now assume that \(f\) is even, and write \(f = 2k\). We will prove that \(\Delta \equiv 0, 1 \mod 4\) 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 \(\Delta = b^2 - 4ac \equiv 0, 1 \mod 4\). Assume now that \(f \geq 4\), and that \(\Delta(A_1) \equiv 0, 1 \mod 4\) 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 \(\Delta(A) \equiv 0 \mod 4\). 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

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

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

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

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

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

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

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

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

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

Let \(A \in \text{M}(f, \mathbb{R})\). The adjoint of \(A\) is the \(f \times f\) matrix \(\adj(A)\) with entries
\[
\adj(A)_{i,j} = (-1)^{i+j} \det(A(j|i))
\]
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
\[
\adj(A) = \begin{bmatrix}
d & -b \\
-c & a
\end{bmatrix}.
\]
CHAPTER 1. BACKGROUND

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 \( Q(x) = \langle x, Ax \rangle \geq 0; \)
2. if \( x \in \mathbb{R}^f \) and \( Q(x) = \langle x, Ax \rangle = 0 \), then \( x = 0. \)

Since \( A \) is symmetric, there exists a matrix \( B \in \text{GL}(f, \mathbb{R}) \) such that

\[ ^tB A B = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_f \end{bmatrix}. \quad (1.5) \]

for some \( \lambda_1, \ldots, \lambda_f \in \mathbb{R} \). 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 \( \det(A) > 0. \)

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

\[ ^t(\text{adj}(A)) B = \det(A) \cdot BA^{-1} ^tB \]

\[ = \begin{bmatrix} \det(A)\lambda_1^{-1} & \det(A)\lambda_2^{-1} & \cdots & \det(A)\lambda_f^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \det(A)\lambda_1^{-1} & \cdots & \det(A)\lambda_f^{-1} \end{bmatrix}. \]
1.5. QUADRATIC FORMS

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

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

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

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

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

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

The positive integers \( N \) and \( \det(A) \) have the same set of prime divisors.

**Proof.** The integer \( G \) divides every entry of \( \text{adj}(A) \). Therefore, \( G^f \) divides \( \det(\text{adj}(A)) \). Since \( \det(\text{adj}(A)) = \det(A)^{f-1} \), \( G^f \) divides \( \det(A)^{f-1} \). This implies that \( G \) divides \( \det(A) \). Now by definition, \( G \) is the largest integer \( g \) such that

\[
\frac{1}{g} \text{adj}(A) \text{ is even.}
\]

Since \( \text{adj}(A) = \det(A)A^{-1} \), we therefore have that

\[
\frac{\det(A)}{G} A^{-1} \text{ is even.}
\]

This implies that \( \det(A) G^{-1} \) is in the ideal generated by the level \( N \) of \( A \), i.e., \( N \) divides \( \det(A) G^{-1} \); consequently,

\[
GN \leq \det(A).
\]
On the other hand, $NA^{-1}$ is even. Using $A^{-1} = \det(A)^{-1}\adj(A)$, this is equivalent to
$$\frac{1}{\det(A)N^{-1}\adj(A)} \text{ is even.}$$

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 $\det(A) = p^d$ and $G = p^kg$ with $k$ and $j$ positive integers and $d$ and $g$ integers such that $(d,p) = (g,p) = 1$. From above, $G^j$ divides $\det(A)^{f-1}$. This implies that $(f-1)j \geq fk$. Therefore,
$$j \geq \frac{f}{f-1}k > k.$$ 

This means that $p$ divides $N = \det(A)/G$.

**Corollary 1.5.5.** 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
$$Q(1,0) = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = a,$$
$$Q(0,1) = \frac{1}{2} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = c.$$ 

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
$$Q(x, y) = ax^2 + bxy + cy^2$$
$$= \frac{1}{a} \left( ax + \frac{b}{2}y \right)^2 + \frac{4ac - b^2}{4a} y^2$$
$$= \frac{1}{a} \left( ax + \frac{b}{2}y \right)^2 + \frac{\det(A)}{4a} y^2.$$
1.5. QUADRATIC FORMS

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

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

and Proposition 1.5.4. \qed
Chapter 2

Theta series in one variable

2.1 Definition and convergence

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

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

For \( z \in \mathbb{H}_1 \), define

\[
\theta(A, z) = \sum_{m \in \mathbb{Z}^f} e^{\pi iz^T m A m} = \sum_{m \in \mathbb{Z}^f} e^{2\pi izQ(m)}
\]

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

\[
\{ z \in \mathbb{H}_1 : \operatorname{Im}(z) \geq \delta \}.
\]

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 \( \varepsilon > 0 \) such that

\[
\varepsilon \| x \| \leq \sqrt{Q(x)},
\]

or equivalently,

\[
\varepsilon^2 \| x \|^2 = \varepsilon^2 (x_1^2 + \cdots + x_f^2) \leq Q(x)
\]

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 \( \operatorname{Im}(z) \geq \delta \). Let \( m = (m_1, \ldots, m_f) \in \mathbb{Z}^f \). Then

\[
|e^{2\pi izQ(m)}| = e^{2\pi \operatorname{Im}(z)Q(m)}
\]
\[ \leq e^{-2\pi \delta Q(m)} \]
\[ \leq e^{-2\pi \delta^2 \|m\|_2^2} \]
\[ = q^{\|m\|_2^2} \]
\[ = q^{m_1^2 + \cdots + m_f^2}. \]

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
\[ (\sum_{n \in \mathbb{Z}} q^{n^2})^f = \sum_{m \in \mathbb{Z}^f} q^{m_1^2 + \cdots + m_f^2} = \sum_{m \in \mathbb{Z}^f} q^{\|m\|_2^2} \]
converges absolutely. It follows from the Weierstrass \( M \)-test that our series
\[ \sum_{m \in \mathbb{Z}^f} e^{2\pi izQ(m)} \]
converges absolutely and uniformly on \( \{z \in \mathbb{H}_1 : \text{Im}(z) \geq \delta\} \) (see, for example, [11], p. 160). Since for each \( m \in \mathbb{Z}^f \) the function on \( \mathbb{H}_1 \) defined by \( z \mapsto e^{2\pi izQ(m)} \) is an analytic function, and since our series converges absolutely and uniformly on every closed disk in \( \mathbb{H}_1, \) it follows that \( \theta(A, \cdot) \) is analytic on \( \mathbb{H}_1 \) (see [11], 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
\[ \text{Im}(z \cdot ^t(w + g)(w + g)) \geq \varepsilon \text{Im}(z \cdot ^t gg), \]
or equivalently
\[ -\text{Im}(z \cdot ^t(w + g)(w + g)) \leq -\varepsilon \text{Im}(z \cdot ^t gg), \]
for \( z \in K_1, \) \( w \in K_2 \) and \( g \in \mathbb{R}^f \) such that \( \|g\| \geq R. \)

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

\[
2 \cdot \text{Im}(z^t wg) = 2t^1ag + 2\sigma^1bg,
\]

\[
\text{Im}(z^t ww) = \sigma(\sigma^aa - \sigma^bb) - 2t^1ab.
\]

It follows that

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

\[
\leq 2t^1ag + 2|\sigma|^1bg + |\sigma|^1aa + |\sigma|^1bb + 2t^1ab
\]

\[
\leq 2t\|a\|\|g\| + 2|\sigma|\|b\|\|g\| + |\sigma|\|a\|^2 + |\sigma|\|b\|^2 + 2t\|a\|\|b\|
\]

\[
\leq 2M^2\|g\| + 2M^2\|g\| + M^3 + M^3 + 2M^3
\]

\[
= 4M^2\|g\| + 4M^3
\]

\[
= 4M^2(\|g\| + M)
\]

\[
\leq (1 - \varepsilon)\delta\|g\|^2
\]

\[
\leq (1 - \varepsilon)t\|g\|^2
\]

\[
= (1 - \varepsilon)\text{Im}(z \cdot 1gg).
\]

Therefore,

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

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

\[
\varepsilon\text{Im}(z \cdot 1gg) \leq \text{Im}(z \cdot 1(w + g)(w + g)).
\]

This is the desired inequality.

□

**Corollary 2.1.3.** 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

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

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 matrix $B \in M(f, \mathbb{R})$ such that $A = tB^tB$. The set $B(K_2)$ is a compact subset of $\mathbb{C}^f$. By Proposition 2.1.2 there exists a positive real number $T > 0$ such that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Let $D$ be a closed disk in $\mathbb{H}_1$, and let $D_1, \ldots, D_f$ be closed disks in $\mathbb{C}^f$. Then $\theta(A, z, w_1, \ldots, w_f)$ converges absolutely and uniformly on $D \times D_1 \times \cdots \times D_f$. The function $\theta(A, z, w_1, \ldots, w_f)$ on $\mathbb{H}_1 \times \mathbb{C}^f$ is analytic in each variable.
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:

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

Here, \( \delta > 0 \) is such that \( \delta \leq \Im(z/2) \) 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 [11], 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 [11], p. 162).

2.2 The Poisson summation formula

Let \( f \) be a positive integer. Let \( g : \mathbb{R}^f \to \mathbb{C} \) be a function, and write \( g = u + iv \), where \( u, v : \mathbb{R}^f \to \mathbb{R} \) are functions. We say that \( g \) is smooth if \( u \) and \( v \) are both infinitely differentiable. Assume that \( g \) is smooth. Let \( (\alpha_1, \ldots, \alpha_f) \in \mathbb{Z}^f_{>0} \). 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 \( \alpha \in \mathbb{Z}^f_{>0} \). 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 [15], or chapter 13 of [9].

**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

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

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

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

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

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

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

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

$$g(x) = e^{-\pi \langle x+iv \rangle (x+iv)} = e^{-\pi \langle x \rangle x - 2\pi i \langle x \rangle v + \pi \langle v \rangle v} = e^{\pi \langle v \rangle v} e^{-\pi \langle x \rangle x - 2\pi i \langle x \rangle v}.$$ 

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

$$h(x) = e^{-\pi \langle x \rangle x - 2\pi i \langle x \rangle v}$$

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

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

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

\[
= |P(x)Q_\alpha(x)e^{-\pi^\prime xx}|
\]

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

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

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

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

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 [11]) 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:

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

or equivalently,

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

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 [11]),

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

These bounds imply that

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

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

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

This is the desired result. If \( v < 0 \), then there is a similar proof. \( \square \)

**Lemma 2.2.3.** Let \( f \) be a positive integer. Let \( A \in \mathbb{M}(f, \mathbb{R}) \) 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

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

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

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

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

**Proof.** There exists \( B \in \text{GL}(f, \mathbb{R}) \) such that \( A = B^T B \). Let \( x \in \mathbb{R}^f \). Then:

\[ (\mathcal{F}g)(x) = \int_{\mathbb{R}^f} \exp(-2\pi Q(y+w)) \exp(-2\pi i \, x y) \, dy \]
\[ \begin{align*}
\mathcal{F}(g)(x) &= |\det(B)|^{-1/2} \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^i(y + w)(y + Bw + 2i^jB^{-1}x) \right) \right) dy \\
&= |\det(A)|^{-1/2} \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iyBw + t^i(Bw)Bw + 2i^jy^iB^{-1}x \right) \right) dy \\
&= |\det(A)|^{-1/2} \exp(-\pi t^iwAw) \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iyBw + 2i^jy^iB^{-1}x \right) \right) dy \\
&= |\det(A)|^{-1/2} \exp(-\pi t^iwAw) \exp \left( \pi t^i(Bw + i^jB^{-1}x)(Bw + i^jB^{-1}x) \right) \\
&\quad \times \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iy(Bw + i^jB^{-1}x) \right. \right. \\
&\quad \left. \left. \left. + t^i(Bw + i^jB^{-1}x)(Bw + i^jB^{-1}x) \right) \right) dy \\
&= |\det(A)|^{-1/2} \exp \left( -\pi t^iwAw \right) \exp \left( \pi t^iB^{-1}x \right) \\
&\quad \times \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iy(Bw + i^jB^{-1}x) \right. \right. \\
&\quad \left. \left. \left. + t^i(Bw + i^jB^{-1}x)(Bw + i^jB^{-1}x) \right) \right) dy.
\end{align*} \]

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 [16]). Now \(|\det(B)|^2 = |\det(A)|^2\), so that \(|\det(A)|^{1/2} = |\det(B)|^1\). Hence,

\[ \begin{align*}
(Fg)(x) &= |\det(A)|^{-1/2} \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iyBw + t^i(Bw)Bw + 2i^jy^iB^{-1}x \right) \right) dy \\
&= |\det(A)|^{-1/2} \exp(-\pi t^iwAw) \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iyBw + 2i^jy^iB^{-1}x \right) \right) dy \\
&= |\det(A)|^{-1/2} \exp(-\pi t^iwAw) \exp \left( \pi t^i(Bw + i^jB^{-1}x)(Bw + i^jB^{-1}x) \right) \\
&\quad \times \int_{\mathbb{R}^f} \exp \left( -\pi \left( t^iyy + 2t^iy(Bw + i^jB^{-1}x) \right. \right. \\
&\quad \left. \left. \left. + t^i(Bw + i^jB^{-1}x)(Bw + i^jB^{-1}x) \right) \right) dy.
\end{align*} \]

Applying now Lemma 2.2.2, we obtain:

\[ \begin{align*}
(Fg)(x) &= |\det(A)|^{-1/2} \exp \left( 2\pi t^iB^{-1}x - \pi t^iB^{-1}x \right) \int_{\mathbb{R}^f} \exp \left( -\pi t^iyy \right) dy.
\end{align*} \]
\[(Fg)(x) = |\det(A)|^{-1/2} \exp \left(2\pi \text{tr} xw - \pi \text{tr} A^{-1} x\right).\]

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

This completes the calculation. \(\square\)

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

**Proof.** See page 249 of [9]. \(\square\)

**Lemma 2.2.5.** Let \(f\) be a positive integer. Let \(A \in M(f, \mathbb{R})\) be a positive-definite symmetric matrix. Let \(\varepsilon\) be a real number such that \(0 < \varepsilon < 1\). Let \(K_1\) be a compact subset of \(\mathbb{H}_f\), and let \(K_2\) be a compact subset of \(\mathbb{C}^f\). For \(x \in \mathbb{C}^f\), define
\[Q(x) = \frac{1}{2} \text{tr} Ax.\]

Then there exists a positive real number \(R > 0\) such that
\[-\text{Im}(\text{tr} \frac{1}{z} gA^{-1} g + 2 \text{tr} g w) \leq -\varepsilon \text{Im}(\text{tr} (-1/z) \cdot \text{tr} A^{-1} g),\]
for \(z \in K_1\), \(w \in K_2\), and all \(g \in \mathbb{R}^f\) such that \(\|g\| \geq R\).

**Proof.** This proof is similar to the proof of Proposition 2.1.2. First of all, there exists \(B \in \text{GL}(f, \mathbb{R})\) such that \(A = \text{tr} BB\). If \(m \in \mathbb{R}^f\), then we note that
\[\text{tr} gA^{-1} g = |\text{tr} gA^{-1} g|\]
\[= |\text{tr} gB^{-1} B^{-1} g|\]
\[= |\text{tr} (B^{-1} g) \cdot (B^{-1} g)|\]
\[= \|\text{tr} B^{-1} g\|^2\]
\[= \left( \frac{1}{\|B\|} \cdot \|B\| \cdot \|B^{-1} g\| \right)^2\]
\[\geq \left( \frac{1}{\|B\|} \cdot \|g\| \right)^2\]
\[= \frac{1}{\|B\|^2} \cdot \|g\|^2.\]

Next, let \(M > 0\) be such that
\[|\text{Im}\left(-\frac{1}{z}\right)|, |\text{Im}(w)| \leq M\]
for \( z \in K_1 \) and \( w \in K_2 \); note that the set consisting of \(-1/z\) for \( z \in K_1 \) is also a compact subset of \( \mathbb{H}_1 \). Let \( \delta > 0 \) be such that
\[
\text{Im}(-1/z) \geq \delta > 0.
\]

Let \( R > 0 \) be such that if \( x \geq R \), then
\[
\delta (1 - \varepsilon) \cdot \frac{1}{\|tB\|^2} \cdot x^2 \geq 2Mx.
\]

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
\[
-\text{Im}(2^t gw) = -2^t gb
\]
\[
\leq 2|gb| \
\leq 2M\|g\|.
\]

On the other hand,
\[
(1 - \varepsilon) \cdot \text{Im}((-1/z)^t gA^{-1} g) = t \cdot gA^{-1} g
\]
\[
\geq \delta (1 - \varepsilon) \cdot \frac{1}{\|tB\|^2} \cdot \|g\|^2
\]

It follows that
\[
-\text{Im}(2^t gw) \leq (1 - \varepsilon) \cdot \text{Im}((-1/z)^t gA^{-1} g)
\]
\[
-\text{Im}((-1/z)^t gA^{-1} g + 2^t gw) \leq -\varepsilon \cdot \text{Im}((-1/z)^t gA^{-1} g).
\]

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

**Theorem 2.2.6.** Let \( f \) be a positive integer. Assume that \( f \) is even, and set
\[
k = \frac{f}{2}.
\]

Let \( A \in \text{M}(f, \mathbb{R}) \) 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
\[
\sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z)^t m A^{-1} m + 2\pi i \cdot mw}
\]
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
\[
\theta(A, z, w) = \frac{i^k}{z^k \sqrt{\det(A)}} \sum_{m \in \mathbb{Z}^f} e^{\pi i (-1/z)^t m A^{-1} m + 2\pi i \cdot mw}
\]
for \( z \in \mathbb{H}_1 \) and \( w \in \mathbb{C}^f \).
Proof. We apply Lemma 2.2.5 with \( \varepsilon = 1/2, K_1 = D, \) and \( K_2 = D_1 \times \cdots \times D_f. \) By this corollary, there exists a finite set \( X \) of \( \mathbb{Z}^f \) such that for \( m \in \mathbb{Z}^f - X, z \in K_1 \) and \( w \in K_2 \) we have:

\[
|e^{\pi(-1/2)\cdot m A^{-1} m + 2\pi i \cdot m w}| = e^{-\pi \text{Im}((-1/2) \cdot m A^{-1} m)}
\]

for \( x = m A^{-1} m + 2\pi i \cdot m w \)

\[
e^{-\pi \cdot (1/2) \cdot \text{Im}((-1/2) \cdot m A^{-1} m)}
\]

\[
\leq e^{-\pi \cdot \text{Im}((-1/2) \cdot Q_{A^{-1}}(m))}
\]

\[
e^{-2\pi Q_{A^{-1}}(m) \cdot \text{Im}(1/(2z))}
\]

\[
\leq e^{-2\pi \delta Q_{A^{-1}}(m)}
\]

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

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 [11], p. 160) now implies that the series

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

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 \((z, w) \mapsto e^{\pi(-1/2)\cdot m A^{-1} m + 2\pi i \cdot m w} \) 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 this series is analytic in each variable (see [11], 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,

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

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

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

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

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

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

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

for \( z \in \mathbb{H}_1 \) of the form \( z = it \) for \( t > 0 \). Since both sides of the last equation are analytic functions in \( z \) for \( z \in \mathbb{H}_1 \), the Identity Principle (see p. 307 of [11]) implies that this equality holds for all \( z \in \mathbb{H}_1 \).

2.3 Differential operators

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

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

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

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

by

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

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

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

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

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

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

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

\[
L_{\ell}(F_1 \cdot F_2) = \sum_{i=1}^{f} \ell_i \frac{\partial}{\partial w_i} (F_1 \cdot F_2)
= \sum_{i=1}^{f} \ell_i \left( \frac{\partial F_1}{\partial w_i} \cdot F_2 + F_1 \cdot \frac{\partial F_2}{\partial w_i} \right)
= \sum_{i=1}^{f} \ell_i \frac{\partial F_1}{\partial w_i} \cdot F_2 + \sum_{i=1}^{f} \ell_i F_1 \cdot \frac{\partial F_2}{\partial w_i},
\]
Let $F \in H(\mathbb{C}^f)$. Then:

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

This completes the proof. $\square$

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

$$\ell A \ell^T = 0.$$

Let $m \in \mathbb{C}^f$ be fixed, and let $r$ be a non-negative integer. Then:

$$L_\ell\left( \ell (m + w) A(m + w) \right) = 2 \ell A(m + w),$$

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

$$L_\ell(\ell m) = \ell m.$$

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

**Proof.** We have

$$L_\ell\left( \ell (m + w) A(m + w) \right)$$

$$= L_\ell\left( \sum_{i,j=1}^f a_{ij}(m_i + w_i)(m_j + w_j) \right)$$

$$= \sum_{i,j=1}^f a_{ij} L_\ell\left( (m_i + w_i)(m_j + w_j) \right)$$

$$= \sum_{i,j=1}^f a_{ij} \left( L_\ell((m_i + w_i))(m_j + w_j) + (m_i + w_i)L_\ell((m_j + w_j)) \right)$$

$$= \sum_{i,j=1}^f a_{ij} (\ell_i(m_j + w_j) + \ell_j(m_i + w_i))$$
2.3. DIFFERENTIAL OPERATORS

\[ \ell \sum_{i,j=1}^{f} a_{ij} \ell_i (m_j + w_j) + \ell \sum_{i,j=1}^{f} a_{ij} \ell_j (m_i + w_i) \]
\[ = \ell A(m + w) + \ell(m + w)A \ell \]
\[ = 2 \ell A(m + w). \]

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

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

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

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

The final assertion of the lemma is straightforward. \( \square \)

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

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

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

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

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

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

**Proof.** We prove this result by induction on \(r\). The case \(r = 0\) is Theorem 2.2.6. Assume the claims hold for \(r\); we will prove that they hold for \(r + 1\). Let \(S_1(z, w) = \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^r e^{\pi i (m + w) A(m + w)} \) 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 \(z, w, \ldots, w_f\), the series
\[ \sum_{m \in \mathbb{Z}^f} L_{\ell} \left( \left( \ell m \right)^r e^{\pi i (m + w) A(m + w)} \right) \]
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 [11]). We have for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\), using Lemma 2.3.1 and Lemma 2.3.2,
\[
(L_{\ell} S_1)(z, w) = \sum_{m \in \mathbb{Z}^f} L_{\ell} \left( \left( \ell m \right)^r e^{\pi i (m + w) A(m + w)} \right) = \sum_{m \in \mathbb{Z}^f} L_{\ell} \left( \left( \ell m \right)^r e^{\pi i (m + w) A(m + w)} + \left( \ell m \right)^r L_{\ell} e^{\pi i (m + w) A(m + w)} \right) = \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^r L_{\ell} e^{\pi i (m + w) A(m + w)} = 2 \pi i z \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^{r+1} e^{\pi i (m + w) A(m + w)}. \]
Next, for \(z \in \mathbb{H}_1\) and \(w \in \mathbb{C}^f\), let
\[ S_2(z, w) = \frac{\frac{ik}{z^{k+r} \sqrt{|\det(A)|}}} \sum_{m \in \mathbb{Z}^f} \left( \ell m \right)^r e^{\pi i (m + w) A(m + w)}. \]
Since \( (r) \) are homogeneous polynomials of degree \( r \), by induction, the proof is complete.

or equivalently,

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

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

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

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

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

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

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

or equivalently,

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

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

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

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

\[
(i \ell A w)^r
\]

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

Some tables

A.1 Tables of fundamental discriminants

| \(-3 = -3\) | \(-35 = (-7) \cdot 5\) | \(-68 = (-4) \cdot 17\) |
| \(-4 = -4\) | \(-39 = (-3) \cdot 13\) | \(-71 = -71\) |
| \(-7 = -7\) | \(-40 = (-8) \cdot 5\) | \(-79 = -79\) |
| \(-8 = -8\) | \(-43 = -43\) | \(-83 = -83\) |
| \(-11 = -11\) | \(-47 = -47\) | \(-84 = (-4) \cdot (-3) \cdot (-7)\) |
| \(-15 = (-3) \cdot 5\) | \(-51 = (-3) \cdot 17\) | \(-87 = (-3) \cdot 29\) |
| \(-19 = -19\) | \(-52 = (-4) \cdot 13\) | \(-88 = (-11) \cdot 8\) |
| \(-20 = (-4) \cdot 5\) | \(-55 = (-11) \cdot 5\) | \(-91 = (-7) \cdot 13\) |
| \(-23 = -23\) | \(-56 = (-7) \cdot 8\) | \(-95 = (-19) \cdot 5\) |
| \(-24 = (-3) \cdot 8\) | \(-59 = -59\) |
| \(-31 = -31\) | \(-67 = -67\) |

Table A.1: Negative fundamental discriminants between \(-1\) and \(-100\), factored into products of prime fundamental discriminants.
Table A.2: Positive fundamental discriminants between 1 and 100, factored into products of prime fundamental discriminants.
Index

adjoint, 23

determinant, 20
Dirichlet character, 1
  conductor, 3
  induced, 3
  Legendre symbol, 3
  primitive, 3
  principal, 2
  product, 5
discriminant, 21

even integral symmetric matrix, 19
  level, 25
extension of a Dirichlet character, 1

Fourier transform, 34

fundamental discriminant, 6
  prime, 6

Kronecker symbol, 16

Legendre symbol, 3

prime fundamental discriminant, 6

quadratic form, 20
  level, 25

real valued, 3

Schwartz function, 33
Schwartz space, 34
smooth function, 33
spherical functions, 45
Bibliography


