TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik

Bachelor Thesis

Structure Results and Generators for Congruence Subgroups and Application to the Weil Representation

Johannes Philipp Manuel Struve

Datum der Abgabe

Betreuer: Prof. Dr. Nils Scheithauer
Zweiter Gutachter: Prof. Dr. Jan Bruinier

Contents

Introduction

A fundamental object in algebra is the group, being fundamentally related to the notion of symmetry. The groups of our concern are the Hecke congruence subgroups $\Gamma_0(N)$ of the modular group $\mathrm{SL}_2(\mathbb{Z})$; that is the groups of 2×2 - matrices congruent to an upper triangular matrix modulo N. They occur in the study of modular forms. $\Gamma_0(N)$ contains the principal congruence subgroup $\Gamma(N)$ of matrices congruent to the identity matrix modulo N.

In the first chapter we show that for integers M, N with $M|N$ and respective prime decompositions $M = \prod_{i=1}^n p_i^{b_i}$ and $N = \prod_{i=1}^n p_i^{a_i}$, the identity

$$\Gamma_0(M)/\Gamma(N) \cong \prod_{i=1}^n \Gamma_0\left(p_i^{b_i}\right)/\Gamma\left(p_i^{a_i}\right)$$

holds. We further present various index formulas for quotients of congruence subgroups by $\Gamma(N)$.

The main result of the first chapter is a new proof of this result.

Theorem. *Any subgroup of the modular group containing a Hecke congruence subgroup $\Gamma_0(N)$ is already of Hecke type.*

This was first proved in [New55], however with a small mistake. At the end of this chapter a corrected version of that proof is presented.

In the second chapter a minimal set of generators of $\Gamma_0(N)$ is listed, together with an investigation of the special case where N is a prime power. We prove that the generating set in the prime power case is similar to the generating set of $\Gamma_0(N)$ when N is prime.

Let D be a discriminant form such that the level of D divides the positive integer N. D decomposes uniquely into a direct sum of p-groups. This can be refined into q-groups $D[q] = \{\gamma \in D \mid q\gamma = 0\}$ with $q = p^k$ for a prime p dividing N. We introduce parameters $n_q \geqslant 1$, the rank of $D[q]$ and $\varepsilon_q \in \{\pm 1\}$ depending on the quadratic form of D restricted to $D[q]$. We write this orthogonal decomposition as

$$D = \bigoplus_{q\in Q} D[q^{\varepsilon_q n_q}]$$

assuming a suitable index set $Q \subset \mathbb{Z}$. We prove that

$$\mathbb{C}\left[D\right] \cong \bigotimes_{q \in Q} \mathbb{C}\left[D[q^{\varepsilon_q n_q}]\right].$$

The Weil representation of $\mathrm{SL}_2\left(\mathbb{Z}\right)$,

$$\rho_D : \mathrm{SL}_2\left(\mathbb{Z}\right) \to \mathrm{GL}(\mathbb{C}\left[D\right]),$$

is defined via its action on the standard generators of $\mathrm{SL}_2\left(\mathbb{Z}\right)$. We prove that it respects the tensor product decomposition of $\mathbb{C}\left[D\right]$ in the sense that the diagram

$$\begin{tikzcd}
 & \mathrm{GL}(\mathbb{C}\left[D\right]) \arrow[d, leftrightarrow, "\sim"] \\
\mathrm{SL}_2\left(\mathbb{Z}\right) \arrow[ur, "\rho_D"] \arrow[dr, "\bigotimes_q \rho_{D[q^{\varepsilon n}]]}"'] & \\
 & \mathrm{GL}(\bigotimes_q \mathbb{C}\left[D[q^{\varepsilon n}]\right])
\end{tikzcd}$$

commutes. The main result of the last chapter is a proof of this theorem.

Theorem. *If the level of D divides the positive integer N, then the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0\left(N\right)$ acts in the Weil representation as*

$$M e^{\gamma} = \chi_D\left(M\right) e\left(-bd\gamma^2/2\right) e^{d\gamma}. \tag{$\bigstar$}$$

This is done by verifying ($\bigstar$) for the generators of $\Gamma_0\left(N\right)$ presented in the second chapter, and using the commutativity of the above diagram. This result was known before, but proved differently.

Acknowledgment

It is a pleasure to thank my supervisor Prof. Dr. Nils Scheithauer for providing this wonderful topic, and for offering plenty of time and support, invariably accompanied by a good sense of humour.

I am grateful to all of my friends who proofread this thesis for their support in a number of ways.

Last but not least, I am very grateful to my parents Ilona and Helmut for their support throughout the years, particularly since the beginning of my studies.

Chapter 1

Structure Results for Congruence Subgroups

In the first section of this chapter a few introductory remarks and definitions are given. The second section contains a decomposition of $\Gamma_0(M)/\Gamma(N)$ into a direct product. Afterwards a few index formulas for certain congruence subgroups are exhibited. The most important section is the fourth one, containing the proof that any group Γ such that $\Gamma_0(N) \leqslant \Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ is already equal to $\Gamma_0(D)$ for some $D|N$. In the last section a corrected version of Newman's different proof of the same result is presented.

1.1 Basic Definitions and Remarks

Let N be a positive integer. For the rings $R = \mathbb{Z}$ and $R = \mathbb{Z}/N\mathbb{Z}$ we define $\mathrm{SL}_2(R)$ to be the group of all 2×2 matrices with entries in R and determinant one. $\mathrm{SL}_2(\mathbb{Z})$ is also called the *(full) modular group*. It plays a fundamental role in the theory of modular forms. The group

$$\Gamma(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\}$$

of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that are entry-wise congruent to the identity matrix modulo N is called *principal congruence subgroup* of *level* N. Any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains some $\Gamma(N)$ is called a *congruence subgroup*. For instance, the group

$$\Gamma_1(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N\}$$

of matrices in $\mathrm{SL}_2(\mathbb{Z})$ equivalent to a unitriangular matrix modulo N is a congruence subgroup. Important in this thesis is the group

$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \bmod N\}$$

of matrices in $\mathrm{SL}_2(\mathbb{Z})$ equivalent to a triangluar matrix modulo N. Note that $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. $\Gamma_0(N)$ is called *congruence subgroup of Hecke type* or *Hecke congruence subgroup*. In literature $\Gamma_1(N)$ is sometimes also said to be of Hecke type.

One easily checks that $\Gamma_0(N)$ is a congruence subgroup, that $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, and that

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}), \tag{1.1}$$

since $\Gamma(N)$ is the kernel of reduction modulo N in each component. A proof can be found in [Miy89, p. 104].

The following theorem is well-known. It can for instance be found in [Miy89, p. 96], and it will be referred to in the third chapter.

Theorem 1.1. *The modular group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

1.2 Factorization of $\Gamma_0(M)/\Gamma(N)$

As $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, and $\Gamma(N) \leqslant \Gamma_0(N) \leqslant \Gamma_0(M)$ whenever $M|N$, $\Gamma(N)$ is also normal in $\Gamma_0(M)$. In this section we use the Chinese Remainder Theorem (CRT) to decompose the quotient $\Gamma_0(M)/\Gamma(N)$ into a direct product of factors of the form $\Gamma_0\left(p_i^b\right)/\Gamma\left(p_i^a\right)$.

Theorem 1.2. *Let* $N = \prod_{i=1}^n p_i^{a_i}$ *be the prime decomposition of* N. *Then*

$$\mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^n \mathrm{Mat}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z}) \tag{1.2}$$

and

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^n \mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z}). \tag{1.3}$$

Proof. By the (CRT), the mapping

$$\psi : \mathbb{Z}/N\mathbb{Z} \to \prod_{i=1}^n \mathbb{Z}/p_i^{a_i}\mathbb{Z},$$
$$x \mapsto (x \bmod p_1^{a_i}, \dots, x \bmod p_n^{a_n})$$

is a group isomorphism. Then also

$$\varphi : \mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z}) \to \prod_{i=1}^{n} \mathrm{Mat}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z}),$$

defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod p_1^{a_i}, \ldots, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod p_n^{a_n} \right),$$

yields an isomorphism, the one needed for (1.2). The restriction of φ to $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is an isomorphism between $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\prod_{i=1}^{n} \mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$, proving (1.3). □

Theorem 1.3. *Let $M = \prod_{i=1}^{n} p_i^{b_i}$ and $N = \prod_{i=1}^{n} p_i^{a_i}$ be the respective prime decompositions of M and N and assume that $M|N$ or equivalently, $0 \leqslant b_i \leqslant a_i$ for $i = 1, \ldots, n$. Then*

$$\Gamma_0(M)/\Gamma(N) \cong \prod_{i=1}^{n} \Gamma_0\left(p_i^{b_i}\right)/\Gamma\left(p_i^{a_i}\right).$$

Proof. We define the map

$$\begin{aligned} \varphi : \Gamma_0(M) &\to \prod_{i=1}^{n} \Gamma_0\left(p_i^{b_i}\right)/\Gamma\left(p_i^{a_i}\right), \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \prod_{i=1}^{n} \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma\left(p_i^{a_i}\right) \right) = \prod_{i=1}^{n} \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod p_i^{a_i} \right). \end{aligned}$$

It is a surjective homomorphism with kernel $\Gamma(N)$. The claim follows now from the first isomorphism theorem. □

Note that (1.3) and Theorem 1.3 for $M = 1$ provide another proof of (1.1).

1.3 Index Formulas for Congruence Subgroups

Let $N = \prod_{i=1}^{n} p_i^{a_i}$ be the prime decomposition of the positive integer N. Certain index formulae for the chain of subgroups

$$\Gamma(N) \leqslant \Gamma_1(N) \leqslant \Gamma_0(N) \leqslant \mathrm{SL}_2(\mathbb{Z})$$

are exhibited here. From [Miy89, p. 105] we can immediately deduce the following index formulae.

Proposition 1.4. *The index of the principal congruence subgroup of level N in $\mathrm{SL}_2(\mathbb{Z})$ is given by*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{i=1}^{n} (1 - \frac{1}{p_i^2}), \tag{1.4}$$

and

$$[\Gamma_0(N) : \Gamma_1(N)] = N \prod_{i=1}^{n} (1 - \frac{1}{p_i}). \tag{1.5}$$

Proof. By (1.1) the index of $\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is given by $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$. From (1.3) we know that this quantity is given by

$$\prod_{i=1}^{n} |\mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z})|.$$

Miyake proves by induction that $|\mathrm{SL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z})| = p_i^{3a_i}(1 - 1/p_i^2)$ for each $i \in \{1, \ldots, n\}$ (cf. [Miy89, p.106]). He proves (1.5) by showing that the map

$$\varphi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod N$$

is a surjective homomorphism with kernel $\Gamma(N)$ on the previous page. □

Proposition 1.5. *The index of the principal congruence subgroup of level N in $\Gamma_1(N)$ is given by*

$$[\Gamma_1(N) : \Gamma(N)] = N. \tag{1.6}$$

Proof. We define the map

$$\varphi : \Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \bmod N.$$

It is a homomorphism, because

$$\begin{aligned} \varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \varphi \begin{pmatrix} * & ab' + bd' \\ * & * \end{pmatrix} \\ &= ab' + bd' \bmod N \\ &= b + b' \bmod N \\ &= \varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \varphi \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \end{aligned}$$

whenever $a \equiv d' \equiv 1 \bmod N$, which is the case in $\Gamma_1(N)$. Surjectivity of φ is evident. Once again, the First Isomorphism Theorem completes the proof. □

Corollary 1.6. *The index of the Hecke congruence subgroup of level N in $\mathrm{SL}_2(\mathbb{Z})$ is given by*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{i=1}^{n} (1 + \frac{1}{p_i}). \tag{1.7}$$

Furthermore, for any prime p and integer $k \geqslant 1$,

$$\left[\Gamma_0\left(p^{k-1}\right) : \Gamma_0\left(p^k\right)\right] = p. \tag{1.8}$$

Proof. By Lagrange's Theorem,

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] [\Gamma_0(N) : \Gamma_1(N)] [\Gamma_1(N) : \Gamma(N)].$$

Using the previous three propositions this takes the form

$$N^3 \prod_{i=1}^{n} (1 - \frac{1}{p_i^2}) = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] N^2 \prod_{i=1}^{n} (1 - \frac{1}{p_i}),$$

yielding (1.7). This newly deduced result gives (1.8) according to the following.

$$\left[\Gamma_0\left(p^{k-1}\right) : \Gamma_0\left(p^k\right)\right] = \frac{\left[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0\left(p^k\right)\right]}{\left[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0\left(p^{k-1}\right)\right]} = \frac{p^k(1 - \frac{1}{p})}{p^{k-1}(1 - \frac{1}{p})} = p$$

□

1.4 Subgroups containing Hecke Congruence Subgroups

In this section we show that for any group Γ such that $\Gamma_0(N) \leqslant \Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$, for some positive integer N, is necessarily equal to some $\Gamma_0(D)$ with $D|N$.

1.4.1 $\Gamma_0(p)$ is maximal in $\mathrm{SL}_2(\mathbb{Z})$

Let p be a prime. We show that the group generated by $\Gamma_0(p)$ together with some $V \in \mathrm{SL}_2(\mathbb{Z}) \backslash \{V\}$ is already $\mathrm{SL}_2(\mathbb{Z})$. This implies that there are no subgroups properly in between $\Gamma_0(p)$ and the full modular group.
The following proposition can be found in [Apo90, p. 75]. It says that if one multiplies an arbitrary element V of $\mathrm{SL}_2(\mathbb{Z}) \backslash \Gamma_0(p)$ by a suitable power of T, and then by S, one obtains an element of $\Gamma_0(p)$.

Proposition 1.7. *Let p be prime. Then for every V in $\mathrm{SL}_2(\mathbb{Z}) \backslash \Gamma_0(p)$ there exists an element P in $\Gamma_0(p)$ and an integer k, $0 \leqslant k < p$, such that*

$$V = PST^k.$$

From this we can deduce the main result if N is a prime number as follows.

Theorem 1.8. *For each V in $\mathrm{SL}_2(\mathbb{Z}) \backslash \Gamma_0(p)$, the group Γ generated by the set $\Gamma_0(p) \cup \{V\}$ is equal to $\mathrm{SL}_2(\mathbb{Z})$.*

Proof. Let $V' \in \mathrm{SL}_2(\mathbb{Z}) \backslash \Gamma_0(p)$ be arbitrary. We prove that V' is contained in Γ. By Proposition 1.7, there exist P and P' in $\Gamma_0(p)$ and $k, k' \in \mathbb{Z}$ such that

$$V = PST^k$$

and

$$V' = P'ST^{k'}.$$

Then

$$\begin{aligned} V' &= P'ST^{k'} \\ &= P'P^{-1}PST^kT^{-k}T^{k'} \\ &= P'P^{-1}PST^kT^{k'-k}, \end{aligned}$$

because $P^{-1}P = T^kT^{-k} = I$. It follows that

$$V' = P'P^{-1}VT^{k'-k}. \tag{1.9}$$

By assumption, $P', P, V \in \Gamma$. Γ is a group, hence also $P^{-1} \in \Gamma$. As all of the factors in (1.9) are in Γ it follows that V' is contained in Γ. $\square$

1.4.2 Groups between $\Gamma_0\left(p^k\right)$ and $\mathrm{SL}_2(\mathbb{Z})$

In this subsection we inductively prove that if N is a prime power, then any group between $\Gamma_0(N)$ and the modular group is also of Hecke type. The previous subsection provides the induction basis.
In what follows, we will need this simple description of the intersection of two Hecke congruence subgroups.

Lemma 1.9. *Let M, N be integers. Then*

$$\Gamma_0(M) \cap \Gamma_0(N) = \Gamma_0([M, N]),$$

where $[M, N]$ denotes the least common multiple of M and N.

Proof. $\Gamma_0(M) \cap \Gamma_0(N)$ consists exactly of the matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $c \equiv 0 \bmod N$ and $c \equiv 0 \bmod M$. This condition is equivalent to $c \equiv 0 \bmod [M, N]$. □

This proposition is fundamental for the induction step we will use to extend the main theorem for prime numbers to prime powers.

Proposition 1.10. *For $k \geqslant 1$, $\Gamma_0(p^k)$ is a maximal subgroup of $\Gamma_0(p^{k-1})$.*

Proof. By (1.8), the index of $\Gamma_0(p^k)$ in $\Gamma_0(p^{k-1})$ is prime. The claim now follows from Lagrange's theorem. □

We now know that for any prime p and integer $k \geqslant 1$, there are no subgroups contained properly between $\Gamma_0(p^k)$ and $\Gamma_0(p^{k-1})$. We still need to show that it is impossible for a group to contain $\Gamma_0(p^k)$, some element of $\mathrm{SL}_2(\mathbb{Z}) \backslash \Gamma_0(p^{k-1})$, but none of $\Gamma_0(p^{k-1}) \backslash \Gamma_0(p^k)$, because such a group would not be of Hecke type. To do so, we use the matrix

$$U_n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in \Gamma_0(n),$$

which is practical due to its simplicity. Note that

$$U_{nn'} = U_n^{n'} \text{ and } U_{n+n'} = U_n U_{n'}.$$

The next lemma allows us to make use of this matrix.

Lemma 1.11. *Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma_0(p^k) \leqslant \Gamma$ for some $k > 1$, and $\Gamma \backslash \Gamma_0(p^{k-1})$ be nonempty. Then $U_{p^{k-1}}$ is an element of Γ.*

Proof. Let

$$V = \begin{pmatrix} a & b \\ cp^l & d \end{pmatrix} \in \Gamma \backslash \Gamma_0(p^{k-1})$$

such that $p \nmid c$ and $l < k-1$. Since $p \nmid d$, the Extended Euclidean Algorithm (EEA) can be used to find integers y and y' satisfying

$$yd + y'p^{k-l} = 1$$

and $p \nmid y$. Multiplying by c and subtracting cyd implies

$$c + (-cy)d = cy'p^{k-l}.$$

Let $x = -cy$ be the coefficient of d. It follows that

$$VU_{xp^l} = \begin{pmatrix} * & * \\ p^l(c+dx) & * \end{pmatrix} = \begin{pmatrix} * & * \\ cy'p^k & * \end{pmatrix} \in \Gamma_0\left(p^k\right) \subset \Gamma,$$

whence also $U_{xp^l} = V^{-1}(VU_{xp^l}) \in \Gamma$. Because $p \nmid c$ and $p \nmid y$, the number p does also not divide x. Therefore, the (EEA) can be used again to find another two integers z and z', for which

$$zx + z'p^{k-l} = 1$$

holds. Now it is apparent that

$$\begin{aligned} U_{p^{k-1}} &= \left(U_{p^l}\right)^{p^{k-1-l}} \\ &= \left(U_{p^l(zx+z'p^{k-l})}\right)^{p^{k-1-l}} \\ &= \left(U_{p^lzx+z'p^k}\right)^{p^{k-1-l}} \\ &= \left(U_{p^lzx}U_{z'p^k}\right)^{p^{k-1-l}} \\ &= \left(\left(U_{xp^l}\right)^z \left(U_{p^k}\right)^{z'}\right)^{p^{k-1-l}}. \end{aligned}$$

Since $U_{xp^l} \in \Gamma$ and $U_{p^k} \in \Gamma_0\left(p^k\right) \subset \Gamma$, it follows that $U_{p^{k-1}} \in \Gamma$. □

Combining the previous results, we are now ready to inductively prove the main result of this chapter for $N = p^k$.

Theorem 1.12. *All groups Γ such that $\Gamma_0\left(p^k\right) \leqslant \Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ are of the form $\Gamma_0(p^n)$ for some $n \leqslant k$.*

Proof. We prove this by induction on k. The statement is trivial for $k = 0$, since $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. Theorem 1.8 proves the statement for $k = 1$. Now let $k > 1$ be arbitrary and assume that the statement holds for each $n < k$. Let Γ be a group such that

$$\Gamma_0\left(p^k\right) \leqslant \Gamma \leqslant \mathrm{SL}_2(\mathbb{Z}). \tag{1.10}$$

Then by Lemma 1.9 intersecting (1.10) with $\Gamma_0\left(p^{k-1}\right)$ yields

$$\Gamma_0\left(p^k\right) \leqslant \Gamma \cap \Gamma_0\left(p^{k-1}\right) \leqslant \Gamma_0\left(p^{k-1}\right).$$

By Proposition 1.10 it follows that either

$$\Gamma \cap \Gamma_0\left(p^{k-1}\right) = \Gamma_0\left(p^{k-1}\right)$$

or

$$\Gamma \cap \Gamma_0\left(p^{k-1}\right) = \Gamma_0\left(p^k\right). \tag{1.11}$$

In the first case, either $\Gamma = \Gamma_0\left(p^{k-1}\right)$ and the statement is proved, or Γ contains $\Gamma_0\left(p^{k-1}\right)$ and an element of $\mathrm{SL}_2(\mathbb{Z}) \setminus \Gamma_0\left(p^{k-1}\right)$ and application of the induction hypothesis to $\Gamma_0\left(p^{k-1}\right)$ and $n = k-1$ yields the result. In the second case either $\Gamma = \Gamma_0\left(p^k\right)$ and the statement is proved, or Γ has to contain an element V of $\mathrm{SL}_2(\mathbb{Z}) \setminus \Gamma_0\left(p^{k-1}\right)$. Suppose there existed such a V. By Lemma 1.11 it follows that $U_{p^{k-1}}$ is in Γ. Clearly $U_{p^{k-1}} \in \Gamma_0\left(p^{k-1}\right)$, but this contradicts (1.11), so no such V can exist. This completes the proof. $\square$

1.4.3 Groups between $\Gamma_0(N)$ and $\mathrm{SL}_2(\mathbb{Z})$

In this section we prove the main theorem for arbitrary positive integers N. To do so, we work in the quotient $\Gamma_0(M)/\Gamma(N)$. This requires multiple applications of the Fourth Isomorphism Theorem, also known as Lattice Isomorphism Theorem for groups. It can be found for example in [DF03, p. 99]. It states that there is a bijection between the subgroups of a group containing a common normal subgroup, and the subgroups of the quotient by this normal subgroup, preserving many properties. As shown above, $\Gamma_0(M)/\Gamma(N)$ decomposes into a direct product. The next lemma allows us to deal with subgroups between direct products of groups.

Lemma 1.13. *If $G = A \times B$ is a group, and $C \leqslant G$ is a subgroup, then C is of the form $\{(a_i, b_i) \mid i \in I\}$, and $\{a_i \mid i \in I\}$ and $\{b_i \mid i \in I\}$ are subgroups of A and B, respectively.*

Proof. Recall that A is normal in G, and the quotient of G by A is simply B. Therefore, the image of C under the quotient map, which is in this case the projection to the second component, is $\{b_i \mid i \in I\}$. By symmetry, the statement is proved. $\square$

We are now ready to prove the main result of this chapter.

Theorem 1.14. *Let M, N be positive integers such that $M|N$, and let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma_0(N) \leqslant \Gamma \leqslant \Gamma_0(M)$. Then there exists an integer D such that $M|D|N$ and $\Gamma = \Gamma_0(D)$.*

Proof. Let $M = \prod_{i=1}^n p_i^{b_i}$ and $N = \prod_{i=1}^n p_i^{a_i}$ be the respective prime decompositions of M and N. Since $M|N$ we have that $0 \leqslant b_i \leqslant a_i$ for $i = 1, \ldots, n$. Then the fourth isomorphism theorem applied to reduction modulo $\Gamma(N)$ gives

$$\underbrace{\Gamma_0(N)/\Gamma(N)}_{\cong \prod_{i=1}^n \Gamma_0\left(p_i^{a_i}\right)/\Gamma\left(p_i^{a_i}\right)} \leqslant \Gamma/\Gamma(N) \leqslant \underbrace{\Gamma_0(M)/\Gamma(N)}_{\cong \prod_{i=1}^n \Gamma_0\left(p_i^{b_i}\right)/\Gamma\left(p_i^{a_i}\right)}.$$

Lemma 1.13 can obviously be extended to arbitrary finite products using induction. Then we can use it to deduce that $\Gamma/\Gamma(N)$, as a subgroup of a direct product, has the form $\{(g_1^i, ..., g_n^i)|i \in I\}$, where each $G_j := \{g_j^i|i \in I\}$ is a subgroup of $\Gamma_0\left(p_j^{b_j}\right)/\Gamma\left(p_j^{a_j}\right)$ containing $\Gamma_0\left(p_j^{a_j}\right)/\Gamma\left(p_j^{a_j}\right)$. By the Fourth Isomorphism Theorem, and Theorem 1.12, for all j there is an integer c_j such that $b_j \leqslant c_j \leqslant a_j$ and

$$G_j \cong \Gamma_0\left(p_j^{c_j}\right)/\Gamma\left(p_j^{a_j}\right).$$

Thus, for $D = \prod_{i=1}^n p_i^{c_i}$,

$$\Gamma/\Gamma(N) \cong \prod_{j=1}^n \Gamma_0\left(p_j^{c_j}\right)/\Gamma\left(p_j^{a_j}\right) \cong \Gamma_0(D)/\Gamma(N).$$

We may apply the Fourth Isomorphism Theorem again and obtain

$$\Gamma \cong \Gamma_0(D).$$

□

1.5 Morris Newman's Result

After completing the results of the previous sections, we found that Morris Newman had already proved Theorem 1.14 in 1955. His proof is similar to ours in section 1.4.2 but works for arbitrary N using Dirichlet's theorem on arithmetic progressions. There is also a little mistake in the original proof found in [New55]. Namely, induction is done on the number of distinct prime divisors of M. However, it needs to be done on the total number $P(M)$ of divisors of M.

Theorem 1.15 (Newman). *Let Γ be a group such that $\Gamma_0(MN) \leqslant \Gamma \leqslant \Gamma_0(N)$. Then $\Gamma = \Gamma_0(DN)$ for some $D|M$.*

Proof. For any N, if $P(M) = 1$ then $\Gamma_0(N) \leqslant \Gamma \leqslant \Gamma_0(N)$, such that $\Gamma = \Gamma_0(N)$. Suppose the theorem holds for all N and for all M such that $P(M) < k$, and let M be such that $P(M) = k$. Let $M = rm$ where r is a proper nontrivial divisor of M. Then $\Gamma_0(rmN) \subseteq \Gamma \subseteq \Gamma_0(N)$ and intersecting by $\Gamma_0(rN)$ gives

$$\Gamma_0(rmN) \subseteq \Gamma \cap \Gamma_0(rN) \subseteq \Gamma_0(rN).$$

Here we have that $P(m) < k$, so we may apply the induction hypothesis to m. If $P(M)$ denoted the number of prime divisors of M as in the original proof, then

$P(m) = k$ would still be possible.
We obtain

$$\Gamma \cap \Gamma_0(rN) = \Gamma_0(r'rN)$$

for some $r'|m$. It follows

$$\Gamma_0(r'rN) \subseteq \Gamma \subseteq \Gamma_0(N).$$

If there is an r such that $r' \neq m$ then $\Gamma = \Gamma_0(DN)$ for some $D|r'r|M$ from applying the induction hypothesis to $r'r$. Otherwise, for each r, $r' = m$. Then for every proper divisor r of M, $\Gamma \cap \Gamma_0(rN) = \Gamma_0(MN)$. This implies that if

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma$$

either $Nc \equiv 0 \mod MN$ and $M|c$ or $Nc \not\equiv 0 \mod MN$ and therefore $(M, c) = 1$. Suppose now that $\Gamma \neq \Gamma_0(MN)$, so that $\Gamma_0(MN) \subset \Gamma \subseteq \Gamma_0(N)$. Then Γ must contain an element

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$$

where $(M, c) = 1$. Since $T \in \Gamma_0(MN) \subseteq \Gamma$, Γ also contains

$$T^x \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \begin{pmatrix} a + Ncx & b + dx \\ Nc & d \end{pmatrix}$$

for every $x \in \mathbb{Z}$.
The next part is similar to the proof of Lemma 1.11.
Since $ad - Nbc = 1$ also $(a, Nc) = 1$, and so the arithmetic progression $\{a + Ncx\}$ contains an infinite number of primes, by Dirichlet's theorem. Hence, there is an x such that $(a + Ncx, M) = 1$. That is, Γ contains an element

$$\begin{pmatrix} a_0 & b_0 \\ Nc_0 & d_0 \end{pmatrix}.$$

where $(a_0, M) = (c_0, M) = 1$. For an integer y, consider now

$$U_{Ny} \begin{pmatrix} a_0 & b_0 \\ Nc_0 & d_0 \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \\ N(a_0 y + c_0) & Nb_0 y + d_0 \end{pmatrix}.$$

Since $(a_0, M) = 1$, we can find a y such that $a_0 y + c_0 \equiv 0 \mod M$. For this y,

$$U_{Ny} \begin{pmatrix} a_0 & b_0 \\ Nc_0 & d_0 \end{pmatrix} \in \Gamma_0(MN) \subset \Gamma.$$

Hence, $U_{Ny} \in \Gamma$. Since $(c_0, M) = 1$ and $a_0 y + c_0 \equiv 0 \bmod M$ it is true that $(y, M) = 1$. Hence, integers u, v can be found such that $uy + vM = 1$. Then Γ contains $U_{Ny}^u U_{MN}^v = U_N$. Because the representatives of $\Gamma_0(MN)$ in $\Gamma_0(N)$ are generated by T and U_N, it follows that $\Gamma_0(N) \subseteq \Gamma$, and since $\Gamma \subseteq \Gamma_0(N)$, $\Gamma = \Gamma_0(N)$. $\square$

Chapter 2

Generators of $\Gamma_0(N)$

All generators of $\Gamma_0(N)$ presented here were obtained using the well-known Reidemeister-Schreier process (cf. [New74, p.347-356]). In 1929, Rademacher computed a presentation of $\Gamma_0(N)$ in the case where N is prime (cf. [Rad29]). In 1973, Chuman generalized this presentation to arbitrary integers N, as can be seen in [Chu73]. However, in 2002 Orive noticed crucial mistakes and misprints in Chuman's work, causing him to recompute the generators and relations. Among other things, he found additional relations on the generators. These were used to exhibit a minimal generating set for $\Gamma_0(N)$, published in [Ori02].

2.1 Notation

For each proper divisor t of N, let

$$\Phi_t = \{x_{t,i} \mid 1 \leqslant i \leqslant \varphi(t, N/t)\}$$

be a complete system of representatives of $(\mathbb{Z}/(t, N/t)\mathbb{Z})^\times$. Here φ denotes Euler's totient function. The Chinese Remainder Theorem implies that the natural map $\mathbb{Z}/(N/t)\mathbb{Z} \to (\mathbb{Z}/(t, N/t)\mathbb{Z})^\times$ is surjective. Hence, we may make the selection $0 < x_{t,i} < N/t$ and $(x_{t,j}, N/t) = 1$. Now, let

$$M := \bigcup_{\substack{t \mid N \\ 1<t<N}} t\Phi_t.$$

Furthermore, for an integer a let $n(a)$ be the smallest positive integer such that $n(a)a^2 \equiv 0 \bmod N$.

Let $a \in \{1, \ldots, N-1\}$ be coprime to N, and fix $\hat{a}$ to be the inverse of $-a$, that is

$a\hat{a} \equiv -1 \bmod N$. We put

$$V_a = ST^aT^{-\hat{a}}S = \begin{pmatrix} \hat{a} & 1 \\ -a\hat{a}-1 & -a \end{pmatrix}.$$

For any two pairs (a, b) and $(\hat{a}, \hat{b})$ solving the congruence

$$(ab-1)(\hat{a}\hat{b}-1) \equiv -a\hat{a} \bmod N \tag{2.1}$$

we put

$$W_{a,b} = ST^aST^bST^{-\hat{b}}ST^{-\hat{a}}S = \begin{pmatrix} -b\hat{b}\hat{a}+b-\hat{a} & -b\hat{b}-1 \\ a\hat{a}b\hat{b}-\hat{a}\hat{b}-ab+a\hat{a}+1 & a-\hat{b}+ab\hat{b} \end{pmatrix}.$$

Note that V_a and $W_{a,b}$ are in $\Gamma_0(N)$.

2.2 Generators

In [Ori02, p. 53] we find a minimal generating set. On page 41 he presents the fundamental relations obtained from the Reidemeister-Schreier-process.

Theorem 2.1 (Orive)**.** *Let*

$$H = \{V_a \mid 1 \leqslant a \leqslant N-1, (a, N) = 1\}$$

and

$$H' = \{W_{a,b} \mid a \in M, b \in \{1, \dots, n(a)-1\}, (1-ab, N) > 1\}.$$

Then $\Gamma_0(N)$ is generated in $\mathrm{PSL}_2(\mathbb{Z})$ by $G := H \cup H'$.

We are interested in $\mathrm{SL}_2(\mathbb{Z})$ rather than $\mathrm{PSL}_2(\mathbb{Z})$.

Corollary 2.2. *$\Gamma_0(N)$ is generated in $\mathrm{SL}_2(\mathbb{Z})$ by $G \cup \{-I\}$.*

Proof. This is true because $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, so that any element in $\mathrm{SL}_2(\mathbb{Z})$ can be written as $\pm IP$ where P is a product of elements of G. □

When we refer to "the generators", we mean $G \cup \{-I\}$.
A part of the statement of Lemma 4 in [Ori02, p. 38] is

Lemma 2.3. *Given $a \in M$ and $b \in \{1, \dots, n(a)-1\}$ such that $(1-ab, N) > 1$, there exists a unique pair $(\hat{a}, \hat{b})$ with $\hat{a} \in M, \hat{b} \in \{1, \dots, n(\hat{a})-1\}$ and $\left(1-\hat{a}\hat{b}, N\right) > 1$, which satisfies* (2.1)*.*

There are not a lot of such pairs (a, b) described above. In particular, if N is a prime power, we find that there are none. This is never considered in [Ori02].

Proposition 2.4. *If $N = p^n$ is a prime power, then there is no pair of numbers (a, b) such that $a \in M, b \in \{1, \ldots, n(a) - 1\}$ and $(1 - ab, N) > 1$.*

Proof. Let $n > 1$. If $a \in M$, then it is of the form $a = p^m x$ with $1 \leqslant m < n$, a positive integer x with $\left(x, p^{n-k}\right) = 1$. This implies $(x, p) = 1$. By [Ori02, p. 37],

$$n(a) = \frac{N}{gg'}$$

with

$$g' = (a, p^n) = p^k \left(x, p^{n-k}\right) = p^k$$

and

$$g = \left(p^n, p^{n-m}\right).$$

There are two cases to consider. The first one is $n - m \leqslant m$ such that $g = p^{n-m}$. Then

$$n(a) = \frac{p^n}{p^{n-m}p^m} = 1.$$

In that case the set $\{1, \ldots, n(a) - 1\}$ is empty, and hence, no such b can exist. The second case is $m \leqslant n - m$ such that $g = p^m$. Then

$$(ab - 1, N) = (p^m xb - 1, p^n),$$

and

$$(p^m xb - 1, p^n) > 1 \Leftrightarrow (p^m xb - 1, p) > 1 \Leftrightarrow p | p^m xb - 1.$$

This is equivalent to the existence of an integer c such that

$$1 = p(p^{m-1}xb - c),$$

which can only be true if $p = \pm 1$. □

Hence, if N is a prime power, then the set G in 2.1 contains no $W_{a,b}$. This is summarized as follows.

Theorem 2.5. *$\Gamma_0\left(p^k\right)$ is generated in $\mathrm{SL}_2(\mathbb{Z})$ by the set*

$$\{V_a \mid 1 \leqslant a \leqslant N - 1, (a, N) = 1\} \cup \{-I\}.$$

Chapter 3

The Weil Representation of $\Gamma_0(N)$

This chapter is based on Scheithauer's paper on the Weil Representation ρ_D of $\mathrm{SL}_2(\mathbb{Z})$, in which he gives an explicit formula for it on the group algebra of a discriminant form of even signature in terms of the genus of the discriminant form. His paper also provides the necessary background information and convenient notation, which we will carry over.
After a short introduction into the Weil representation of $\mathrm{SL}_2(\mathbb{Z})$ and declaration of common and convenient notation in the first section, a couple of useful facts and formulae are stated. Then an explicit formula for the action of $\Gamma_0\left(p^k\right)$ under ρ_D using the group's generators is determined. Afterwards, the Weil representation is proved to be expressible as a tensor product representation with respect to any direct orthogonal sum decomposition of the underlying discriminant form. In the final section we apply this result to the Jordan decomposition of D. This allows us to compute an explicit formula for the action of $\Gamma_0(N)$ via the previously determined formula for the action of $\Gamma_0\left(p^k\right)$. In particular, this yields another proof that $\Gamma(N)$ acts trivially in the Weil representation.

3.1 Introduction

The Weil representation can be defined in a very general setting. For details, see [LV80]. For readability, convenient notation is introduced. In this entire chapter, let D be a discriminant form of even signature such that the level of D divides the positive integer N. The abbreviation $e(x) = e(2\pi i x)$ is commonly used.
Consider the decomposition

$$D = \bigoplus_{q \in Q} D[q^{\varepsilon_q n_q}]$$

mentioned in the introduction. We stick to the notation in [Sch09], which provides, like [Str13, p. 5], a good reference for the possible Jordan components that can occur. If q is a power of an odd prime p, the nontrivial p-adic Jordan components of exponent q are $D[q^{\varepsilon_q n_q}]$. In that case we define $\gamma_p(q^{\varepsilon_q n_q}) = e(-p - \operatorname{excess}(q^{\varepsilon_q n_q}))$. If $p = 2$, the nontrivial even 2-adic Jordan components of exponent $q = 2^k$ are $D[q^{\varepsilon_q 2n_q}]$, in which case we define $\gamma_2(D[q^{\varepsilon_q 2n_q}]) = e(\operatorname{oddity}(D[q^{\varepsilon_q 2}])/8)$. The possible odd nontrivial 2-adic Jordan components of exponent $q = 2^k$ are denoted by $D[q_t^{\varepsilon_q n_q}]$, for which we define $\gamma_2(D[q_t^{\varepsilon_q n_q}]) = e\left(\operatorname{oddity}\left(D[q_t^{\varepsilon_q n_q}]\right)/8\right)$. Whenever Jordan components of D are mentioned, we assume that a fixed Jordan decomposition has been chosen.

The Weil representation

$$\rho_D : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}(\mathbb{C}[D])$$

of $\mathrm{SL}_2(\mathbb{Z})$ on the group algebra $\mathbb{C}[D]$ is defined on the generators T, and S of $\mathrm{SL}_2(\mathbb{Z})$ by the action on a basis element $e^\gamma \in D$ by

$$\begin{aligned} Te^\gamma &:= \rho_D(T)e^\gamma := e\left(-\gamma^2/2\right) e^\gamma \\ Se^\gamma &:= \rho_D(S)e^\gamma := \frac{e(\operatorname{sign}(D)/8)}{\sqrt{|D|}} \sum_{\beta \in D} e(\gamma\beta)\, e^\beta. \end{aligned}$$

Any integer c acts by multiplication on D. We put

$$D^c = cD = \{c\gamma \mid \gamma \in D\}$$

to be the c-fold multiple of the elements of D, and

$$D_c = \{\gamma \in D \mid c\gamma = 0\}$$

to be the kernel of that map. We further define

$$D^{c*} = \{\alpha \in D \mid c\gamma^2/2 + \alpha\gamma = 0 \bmod 1\}.$$

Then

$$D^{c*} = x_c + D^c,$$

where $x_c = 0$ except if $2^k \mid\mid c$ and if the 2-adic block of type 2^k is odd. In that case $x_c = \left(2^{k-1}, \ldots, 2^{k-1}\right)$. The map

$$D^{c*} \to \mathbb{Q}/\mathbb{Z}, \quad x_c + c\gamma \mapsto (x_c + c\gamma)_c^2/2 := c\gamma^2/2 + x_c\gamma \bmod 1$$

is well-defined.

3.2 Useful Facts and Formulae

The next results are scattered across [Sch09]. This proposition is critical for the evaluation of Gauss sums.

Proposition 3.1. *Let $\alpha \in D^{c*}$. Then*

$$\sum_{\mu \in D} e\left(c\mu^2/2 + \alpha\mu\right) = \varepsilon_c e\left(-\alpha_c^2/2\right)\sqrt{|D_c||D|},$$

with

$$\varepsilon_c = \prod_{2|q\nmid c} \gamma_2(D[(q/q_c)^{\varepsilon_q n_q}]) e\left((c/q_c - 1)\text{oddity}\left(D[(q/q_c)^{\varepsilon_q n_q}]\right)/8\right)\left(\frac{c/q_c}{(q/q_c)^{n_q}}\right)$$
$$\prod_{\substack{p|q\nmid c \\ p \text{ odd}}} \gamma_p(D[(q/q_c)^{\varepsilon_q n_q}])\left(\frac{c/q_c}{(q/q_c)^{n_q}}\right).$$

Here $q_c = (q, c)$.

The action of an element ST^aST^b under ρ_D is determined. We will use this to compute the action of ST^aST^bS.

Proposition 3.2. *Let $\gamma \in D$ and $a, b \in \mathbb{Z}$. Then*

$$ST^aST^be^\gamma = e\left(\text{sign}(D)/4\right)\varepsilon_{-a}\frac{\sqrt{|D_a|}}{\sqrt{|D|}}e\left(-b\gamma^2/2\right)\sum_{\beta \in D^{a*}} e\left(\beta_a^2/2\right)e^{\beta-\gamma}$$

The following remarks will be used commonly.

Lemma 3.3. *Let c be an integer. Then*

$$D_c^\perp = D^c, cx_c = 0, \alpha_c^2/2 = -\alpha_{-c}^2/2 \tag{3.1}$$

If $(c, N) = (d, N)$ then

$$D_c = D_d, D^c = D^d, D^{c*} = D^{d*} \tag{3.2}$$

In particular, if $(c, N) = 1$ then

$$D^c = D, D_c = \{0\}, \tag{3.3}$$

and

$$\varepsilon_c = e\left(\text{sign}(D)/8\right)\left(\frac{c}{|D|}\right)e\left((c-1)\text{oddity}(D)/8\right) \tag{3.4}$$

and if $c \equiv 0 \bmod N$ *then*

$$D^c = 0, \quad D_c = D, \quad \varepsilon_c = 1. \tag{3.5}$$

Furthermore,

$$1 = e(\operatorname{sign}(D)/4)\left(\frac{-1}{|D|}\right) e(-\operatorname{oddity}(D)/4), \tag{3.6}$$

and

$$\chi_D(a) = \left(\frac{a}{|D|}\right) e((a-1)\operatorname{oddity}(D)/8)$$

defines a quadratic Dirichlet character modulo N.

The factors γ_p *are multiplicative, and the oddity formula*

$$\operatorname{sign}(D) + \sum_{p \geqslant 3} p - \operatorname{excess}(D) = \operatorname{oddity}(D) \bmod 8,$$

which is equivalent to

$$\prod_p \gamma_p(D) = e(\operatorname{sign}(D)/8),$$

holds.

3.3 The Action of $\Gamma_0\left(p^k\right)$

In order to compute the Weil representation of $\mathrm{SL}_2(\mathbb{Z})$, Scheithauer determines the representation of $\Gamma_0(N)$ first.

Theorem 3.4. *If the level of* D *divides the positive integer* N*, then the matrix* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ *acts in the Weil representation as*

$$Me^\gamma = \chi_D(M)\, e\left(-bd\gamma^2/2\right) e^{d\gamma}. \tag{$\bigstar$}$$

The rest of this section is dedicated to a proof of this theorem in the case where $N = p^k$ is a prime power. The following theorem justifies that determining the explicit formula for the action of $\Gamma_0(N)$ can be reduced to validating ($\bigstar$) for its generators.

Theorem 3.5. *If the matrices*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad M' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

act in the Weil representation according to ($\bigstar$)*, then so does* MM'.

Proof. We have that

$$MM' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Then by associativity and the induction hypothesis,

$$\begin{aligned}(MM')e^\gamma = M(M'e^\gamma) &= \chi_D\left(M'\right) e\left(-b'd'\gamma^2/2\right) Me^{d'\gamma} \\ &= \chi_D\left(M\right) e\left(-b'd'\gamma^2/2\right) \chi_D\left(M'\right) e\left(-bd(d'\gamma)^2/2\right) e^{dd'\gamma} \\ &= \chi_D\left(M\right) \chi_D\left(M'\right) e\left(-b'd'\gamma^2/2 - bd(d'\gamma)^2/2\right) e^{dd'\gamma}.\end{aligned}$$

Using that χ_D is multiplicative and simplifying $-b'd'\gamma^2/2 - bd(d'\gamma)^2/2$ we get

$$\begin{aligned}(MM')e^\gamma &= \chi_D\left(MM'\right) e\left(-(adb'd' + bdd'^2)\gamma^2/2\right) e^{dd'\gamma} \\ &= \chi_D\left(MM'\right) e\left(-(ab' + bd')dd'\gamma^2/2\right) e^{dd'\gamma}.\end{aligned}$$

Since $c \equiv 0 \bmod N$,

$$(MM')e^\gamma = \chi_D\left(MM'\right) e\left(-(ab' + bd')(cb' + dd')\gamma^2/2\right) e^{(cb'+dd')\gamma}.$$

$\square$

In the second chapter the generators of $\Gamma_0\left(p^k\right)$ were determined. All that is left to do is to verify ($\bigstar$) for each one of these generators. By syntactic induction, using Theorem 3.5 as the induction step, it follows that ($\bigstar$) holds for all elements of $\Gamma_0\left(p^k\right)$. The first generator we investigate is as simple as its action under ρ_D.

Proposition 3.6. *The matrix $-I$ acts according to ($\bigstar$), that is*

$$-Ie^\gamma = e\left(\mathrm{sign}(D)/4\right) e^{-\gamma}.$$

Proof. As $-I = S^2$, we have that

$$-Ie^\gamma = \frac{e\left(\mathrm{sign}(D)/4\right)}{|D|} \sum_{\beta,\mu \in D} e\left(\gamma\beta + \mu\beta\right) e^\mu \quad = \frac{e\left(\mathrm{sign}(D)/4\right)}{|D|} \sum_{\beta,\mu \in D} e\left(\mu\beta\right) e^{\mu-\gamma}.$$

The map $\beta \mapsto e\left(\mu\beta\right)$ is a character of D, because for any $\beta, \beta' \in D$,

$$e\left(\mu(\beta + \beta')\right) = e\left(\mu\beta\right) e\left(\mu\beta'\right).$$

The statement now follows from the fact that this character is trivial if and only if $\mu \in D^\perp$, that is $\mu = 0$. $\square$

As announced, we can compute and simplify the formula for the action of an arbitrary element of the form ST^aST^bS under ρ_D. We will use this for the special case where $ab \equiv -1 \bmod N$.

Lemma 3.7. *For any $a, b \in \mathbb{Z}$ we have that*

$$ST^aST^bSe^\gamma = e\left(3/8\mathrm{sign}(D)\right)\varepsilon_{-a}\frac{\sqrt{|D_a|}}{|D|}\sum_{\beta\in D}\sum_{\mu\in D^{a*}} e\left(\gamma\beta - b\beta^2/2 + \mu_a^2/2\right)e^{\mu-\beta}.$$

Proof. By definition,

$$ST^aST^bSe^\gamma = \frac{e\left(\mathrm{sign}(D)/8\right)}{\sqrt{|D|}}\sum_{\beta\in D} e\left(\gamma\beta\right)ST^aST^be^\beta.$$

Applying Proposition 3.2 to $ST^aST^be^\beta$ gives the desired formula. $\square$

Here, $(\bigstar)$ is verified for the last family $\{V_a \mid 1 \leqslant a \leqslant N-1, (a,N)=1\}$ of generators of $\Gamma_0(N)$.

Proposition 3.8. *The matrix $V_a = ST^aST^{-\hat{a}}S$ acts according to $(\bigstar)$, that is*

$$V_ae^\gamma = \chi_D(-a)\,e\left(a\gamma^2/2\right)e^{-a\gamma}.$$

Proof. By Lemma 3.7,

$$V_ae^\gamma = e\left(3\mathrm{sign}(D)/8\right)\varepsilon_{-a}\frac{\sqrt{|D_a|}}{|D|}\sum_{\beta\in D}\sum_{\mu\in D^{a*}} e\left(\gamma\beta + \hat{a}\beta^2/2 + \mu_a^2/2\right)e^{\mu-\beta}.$$

Since $(a,N)=1$, equation (3.3) implies that $D^{a*}=D$ and $|D_a|=1$. Therefore,

$$V_ae^\gamma = e\left(3\mathrm{sign}(D)/8\right)\varepsilon_{-a}|D|^{-1}\sum_{\beta\in D}\sum_{\mu\in D} e\left(\gamma\beta + \hat{a}\beta^2/2 + a\mu^2/2\right)e^{a\mu-\beta}.$$

For each $\mu \in D$, the map $\beta \mapsto a\mu - \beta$ is an automorphism of D. Hence, we may substitute $\beta' = a\mu - \beta$ and get

$$V_ae^\gamma = e\left(3\mathrm{sign}(D)/8\right)\varepsilon_{-a}|D|^{-1}\xi,$$

with

$$\xi = \sum_{\beta'\in D}\sum_{\mu\in D} e\left(a\gamma\mu - \gamma\beta' + \hat{a}\left(a\mu-\beta'\right)^2/2 + a\mu^2/2\right)e^{\beta'}.$$

Since $(a\mu-\beta')^2/2 = a^2\mu^2/2 - a\mu\beta' + \beta'^2/2$ and by assumption $a\hat{a} = -1 \bmod N$, the expression simplifies to

$$\begin{aligned}a\gamma\mu - \gamma\beta' + \hat{a}\left(a\mu-\beta'\right)^2/2 + a\mu^2/2 &= a\gamma\mu - \gamma\beta' - a\mu^2/2 + \mu\beta' + \hat{a}\beta'^2/2 + a\mu^2/2\\ &= \hat{a}\beta'^2/2 - \gamma\beta' + (a\gamma+\beta')\mu,\end{aligned}$$

and thus,

$$\xi = \sum_{\beta' \in D} e\left(\hat{a}\beta'^2/2 - \gamma\beta'\right) \sum_{\mu \in D} e\left((a\gamma + \beta')\mu\right) e^{\beta'}.$$

As above, the mapping $\mu \mapsto e\left((a\gamma + \beta')\mu\right)$ is a character of D for each $\beta' \in D$. It is trivial if and only if $a\gamma + \beta' \in D^{\perp} = \{0\}$. Hence, the only surviving term in the outer sum in ξ is the one where $\beta' = -a\gamma$. We see now that ξ has the form

$$\xi = |D| e\left(\hat{a}(-a\gamma)^2/2 + a\gamma^2\right) e^{-a\gamma}.$$

Since

$$\hat{a}(-a\gamma)^2/2 = \hat{a}a^2\gamma^2/2 = -a\gamma^2/2 \bmod 1,$$

ξ takes the form

$$\xi = |D| e\left(a\gamma^2/2\right) e^{-a\gamma}.$$

Combining these results we obtain

$$\begin{aligned} V_a e^{\gamma} &= e\left(3/8\operatorname{sign}(D)\right) \varepsilon_{-a} e\left(a\gamma^2/2\right) e^{-a\gamma} \\ &= \left(\frac{-a}{|D|}\right) e\left((-a-1)\operatorname{oddity}(D)/8\right) e\left(a\gamma^2/2\right) e^{-a\gamma} \\ &= \chi_D\left(-a\right) e\left(a\gamma^2/2\right) e^{-a\gamma}, \end{aligned}$$

where we used (3.5). □

This completes the proof of Theorem 3.4 for $N = p^k$.

3.4 Tensor Products of Weil Representations

Let $D = D' \oplus D''$ be a discriminant form with $D' \perp D''$, such that D' and D'' are also discriminant forms. We show that

$$\mathbb{C}\left[D\right] \cong \mathbb{C}\left[D'\right] \otimes \mathbb{C}\left[D''\right],$$

and that the Weil representation respects this decomposition in the sense that the diagram

$$\begin{tikzcd} & \mathrm{GL}(\mathbb{C}\left[D\right]) \arrow[d, leftrightarrow, "\sim"] \\ \mathrm{SL}_2\left(\mathbb{Z}\right) \arrow[ur, "\rho_D"] \arrow[dr, "\rho_{D'} \otimes \rho_{D''}"'] & \\ & \mathrm{GL}(\mathbb{C}\left[D'\right] \otimes \mathbb{C}\left[D''\right]) \end{tikzcd}$$

commutes. Our first concern is the decomposition of the group algebra.

Theorem 3.9. *If the discriminant form can be written as the orthogonal direct sum $D = D' \oplus D''$, then*

$$\mathbb{C}[D] \cong \mathbb{C}[D'] \otimes_{\mathbb{C}} \mathbb{C}[D''].$$

Proof. If R is a commutative ring, and A and B are free R-modules with bases $\{a_i | i \in I\}$ and $\{b_j \,|\, j \in J\}$, respectively, then $A \otimes_R B$ is free with basis $\{a_i \otimes b_i \,|\, (i, j) \in I \times J\}$. It follows that for two groups A' and B',

$$R[A' \oplus B'] \cong R[A'] \otimes_R R[B']$$

under the correspondence

$$r(a, b) \leftrightarrow r(a \otimes b).$$

In our case we get

$$\mathbb{C}[D] \cong \mathbb{C}[D' \oplus D''] \cong \mathbb{C}[D'] \otimes \mathbb{C}[D''].$$

□

We will now prove that "ρ_D distributes over $\otimes$", by verifying the statement for the standard generators T and S of $\mathrm{SL}_2(\mathbb{Z})$, and then extending it to the whole modular group by syntactic induction.

Theorem 3.10. *The action of the generators S and T of $\mathrm{SL}_2(\mathbb{Z})$ respects $\otimes$ in the sense that for the unique representation $e^\gamma \otimes e^\delta \in D' \otimes D''$ of an element of D we have that*

$$\rho_D(T)e^\gamma \otimes e^\delta = \rho_{D'}(T)e^\gamma \otimes \rho_{D''}(T)e^\delta,$$

and

$$\rho_D(S)e^\gamma \otimes e^\delta = \rho_{D'}(S)e^\gamma \otimes \rho_{D''}(S)e^\delta.$$

Proof. By definition of the action of T,

$$\rho_D(T)e^\gamma \otimes e^\delta = e\left(-(\gamma + \delta)^2/2\right) e^\gamma \otimes e^\delta.$$

Since $(\gamma, \delta) = 0$,

$$\rho_D(T)e^\gamma \otimes e^\delta = e\left(-\gamma^2/2 - \delta^2/2\right) e^\gamma \otimes e^\delta.$$

A simple calculation yields

$$\begin{aligned}\rho_D(T)e^\gamma \otimes e^\delta &= e\left(-\gamma^2/2\right) e\left(-\delta^2/2\right) e^\gamma \otimes e^\delta \\ &= e\left(-\gamma^2/2\right) e^\gamma \otimes e\left(-\delta^2/2\right) e^\delta \\ &= \rho_{D'}(T)e^\gamma \otimes \rho_{D''}(T)e^\delta.\end{aligned}$$

The proof of the second part is similar. $\rho_D(S)$ acts as

$$\begin{aligned}
\rho_D(S)e^\gamma \otimes e^\delta &= \xi \sum_{\beta\in D} e(\beta(\gamma+\delta))e^\gamma \otimes e^\delta \\
&= \xi \sum_{\beta'\in D'} \sum_{\beta''\in D''} e((\beta'+\beta'')\gamma)e((\beta'+\beta'')\delta)e^\gamma \otimes e^\delta \\
&= \xi \sum_{\beta'\in D'} \sum_{\beta''\in D''} e(\beta'\gamma)\, e(\beta''\delta)\, e^\gamma \otimes e^\delta \\
&= \xi \sum_{\beta'\in D'} e(\beta'\gamma) \sum_{\beta''\in D''} e(\beta''\delta)\, e^\gamma \otimes e^\delta
\end{aligned}$$

with

$$\xi = \frac{e(\mathrm{sign}(D)/8)}{\sqrt{|D|}} = \frac{e\left(\mathrm{sign}\left(D'\right)/8 + \mathrm{sign}\left(D''\right)/8\right)}{\sqrt{|D'||D''|}}.$$

Hence, $\rho_D(S)$ acts on $e^\gamma \otimes e^\delta$ as

$$\begin{aligned}
&\frac{e\left(\mathrm{sign}\left(D'\right)/8\right)}{\sqrt{|D'|}} \sum_{\beta'\in D'} e(\beta'\gamma)\, e^{\gamma'} \otimes \frac{e\left(\mathrm{sign}\left(D''\right)/8\right)}{\sqrt{|D''|}} \sum_{\beta''\in D''} e(\beta''\delta)\, e^\delta \\
=&\rho_{D'}(S)e^\gamma \otimes \rho_{D''}(S)e^\delta.
\end{aligned}$$

□

The induction step is simple, and the desired result is the following.

Corollary 3.11. *For any matrix $M \in \mathrm{SL}_2(\mathbb{Z})$,*

$$\rho_D(M)e^\gamma \otimes e^\delta = \rho_{D'}(M)e^\gamma \otimes \rho_{D''}(M)e^\delta. \tag{3.7}$$

Proof. We show that if $M, M' \in \mathrm{SL}_2(\mathbb{Z})$ satisfy (3.7), then also MM' satisfies (3.7). Using the induction hypothesis and that ρ_D is a representation,

$$\begin{aligned}
\rho_D(MM')e^\gamma \otimes e^\delta &= \rho_D(M)\left(\rho_{D'}(M')e^\gamma \otimes \rho_{D''}(M')e^\delta\right) \\
&= \rho_{D'}(M)\rho_{D'}(M')e^\gamma \otimes \rho_{D''}(M)\rho_{D''}(M')e^\delta \\
&= \rho_{D'}(MM')e^\gamma \otimes \rho_{D''}(MM')e^\delta.
\end{aligned}$$

Since we proved (3.7) for the generators T and S of $\mathrm{SL}_2(\mathbb{Z})$, it follows that (3.7) holds for all $M \in \mathrm{SL}_2(\mathbb{Z})$. □

3.5 Junction: Action of $\Gamma_0(N)$ and $\Gamma(N)$

Let $Q \subset \mathbb{Z}$ be an index set for the Jordan decomposition of D, i.e.

$$D = \bigoplus_{q\in Q} D[q^{\varepsilon_q n_q}].$$

Whenever $\bigotimes_q$ or $\bigoplus_q$ occurs, q runs through Q. Because the Jordan components are pairwise orthogonal, we can extend the results from the previous section to this decomposition of D, that is

$$\mathbb{C}[D] \cong \bigotimes_{q\in Q} \mathbb{C}[D[q^{\varepsilon_q n_q}]],$$

and $\rho_D = \otimes_q \rho_{D[q^{\varepsilon_q n_q}]}$ such that the diagram

$$\begin{tikzcd} & \mathrm{GL}(\mathbb{C}[D]) \arrow[dd, leftrightarrow, "\sim"] \\ \mathrm{SL}_2(\mathbb{Z}) \arrow[ur, "\rho_D"] \arrow[dr, "\bigotimes_q \rho_{D[q]}"'] & \\ & \mathrm{GL}(\bigotimes_p \mathbb{C}[D[q]]) \end{tikzcd}$$

commutes. We can now prove the main result of this chapter.

Theorem 3.12. *Let D be a discriminant form such that the level of D divides the positive integer N. Then the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ acts in the Weil representation as*

$$Me^\gamma = \chi_D(M)\, e\left(-bd\gamma^2/2\right) e^{d\gamma}. \tag{$\bigstar$}$$

Proof. The element $1e^\gamma$ of $\mathbb{C}[D]$ can be uniquely represented as

$$e^\gamma = \bigotimes_{q\in Q} e^{\gamma_q},$$

with $e^{\gamma_q} \in D[q^{\varepsilon_q n_q}]$. From Corollary 3.11 it follows that

$$\rho_D(M)e^\gamma = \rho_D(M) \bigotimes_{q\in Q} e^{\gamma_q} = \bigotimes_{q\in Q} \rho_{D[q^{\varepsilon_q n_q}]}(M)e^{\gamma_q}.$$

Now let $q \in Q$. Then the matrix M is in $\Gamma_0(q) \subseteq \Gamma_0(N)$. Furthermore, for $p \in Q$ with $q \neq p$, it is true that the levels of the corresponding Jordan blocks $D[q^{\varepsilon_q n_q}]$ and $D[p^{\varepsilon_p n_p}]$ are coprime. In this situation, the level of $D[q^{\varepsilon_q n_q}]$ divides the prime power q. In section 3.3 we proved that ($\bigstar$) holds if N is a prime power. Thus,

$$\begin{aligned} \rho_D(M)e^\gamma &= \bigotimes_{q\in Q} \chi_{D[q^{\varepsilon_q n_q}]}(M)\, e\left(-bd\gamma_q^2/2\right) e^{\gamma_q} \\ &= \prod_{q\in Q} \chi_{D[q^{\varepsilon_q n_q}]}(M)\, e\left(-bd\gamma_q^2/2\right) \bigotimes_{q'\in Q} e^{\gamma_{q'}} \\ &= \prod_{q\in Q} \chi_{D[q^{\varepsilon_q n_q}]}(M)\, e\left(-bd\gamma_q^2/2\right) e^{\gamma} \end{aligned}$$

where we first applied Corollary 3.11 and secondly ($\bigstar$) for prime powers, proved in section 3.3. Now since

$$\left(\frac{a}{|D[q^{\varepsilon_q n_q}]|}\right)\left(\frac{a}{|D[p^{\varepsilon_p n_p}]|}\right) = \left(\frac{a}{|D[q^{\varepsilon_q n_q}] \oplus D[p^{\varepsilon_p n_p}]|}\right),$$

and

$$\operatorname{sign}\left(D[q^{\varepsilon_q n_q}]\right) + \operatorname{sign}\left(D[p^{\varepsilon_p n_p}]\right) = \operatorname{sign}\left(D[q^{\varepsilon_q n_q}] \oplus D[p^{\varepsilon_p n_p}]\right),$$

it is easy to see that

$$\chi_{D[q^{\varepsilon_q n_q}]}(M)\,\chi_{D[p^{\varepsilon_p n_p}]}(M) = \chi_{D[q^{\varepsilon_q n_q}]\oplus D[p^{\varepsilon_p n_p}]}(M).$$

$D[q^{\varepsilon_q n_q}]$ and $D[p^{\varepsilon_p n_p}]$ are orthogonal. Thus,

$$\gamma_q^2/2 + \gamma_p^2/2 = (\gamma_q + \gamma_p)^2/2.$$

These facts imply that

$$\prod_{q \in Q} \chi_{D[q^{\varepsilon_q n_q}]}(M)\, e\left(-bd\gamma_q^2/2\right) = \chi_D(M)\, e\left(-bd\gamma^2/2\right),$$

and therefore

$$\rho_D(M)e^{\gamma} = \chi_D(M)\, e\left(-bd\gamma^2/2\right) e^{\gamma}.$$

□

Note that as a special case we obtain that the action of $\Gamma(N)$ is trivial. This was first found out by Schoeneberg.

Bibliography

[Apo90] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory.* Springer New York, New York, NY, 1990.

[Chu73] Yasuhiro Chuman. Generators and Relations of $\Gamma_0(N)$. *J. Math. Kyoto Univ.*, 13(2):381–390, 1973.

[DF03] David Dummit and Richard Foote. *Abstract Algebra, 3rd Edition.* John Wiley and Sons, 2003.

[LV80] Gerard Lion and Michele Vergne. *The Weil representation, Maslov index and Theta series.* Birkhaeuser Basel, 1980.

[Miy89] Toshitsune Miyake. *Modular Forms.* Springer Berlin Heidelberg, Berlin, Heidelberg, 1989.

[New55] Morris Newman. Structure theorems for modular subgroups. *Duke Math. J.*, 22(1):25–32, 03 1955.

[New74] M. F. Newman, editor. *Proceedings of the Second International Conference on The Theory of Groups: Australian National University, August 13–24, 1973.* Springer Berlin Heidelberg, Berlin, Heidelberg, 1974.

[Ori02] Antonio Lascaurain Orive. Some presentations for $\Gamma_0(N)$. *Conformal Geomentry and Dynamics*, 6:33–60, May 2002.

[Rad29] Hans Rademacher. Über die Erzeugenden von Kongruenzuntergruppen der Modulgruppe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 7(1):134–148, Dec 1929.

[Sch09] Nils R. Scheithauer. The Weil representation of $\mathrm{SL}_2(\mathbb{Z})$ and some applications. *International Mathematics Research Notices*, 2009(8):1488–1545, 2009.

[Str13] Fredrik Strömberg. Weil representations associated with finite quadratic modules. *Mathematische Zeitschrift*, 275(1):509–527, Oct 2013.

Thesis Statement pursuant to §23 paragraph 7 of APB TU Darmstadt

I herewith formally declare that I, Johannes Philipp Manuel Struve, have written the submitted thesis independently. I did not use any outside support except for the quoted literature and other sources mentioned in the paper. I clearly marked and separately listed all of the literature and all of the other sources which I employed when producing this academic work, either literally or in content. This thesis has not been handed in or published before in the same or similar form.

I am aware, that in case of an attempt at deception based on plagiarism (§38 Abs. 2 APB), the thesis would be graded with 5,0 and counted as one failed examination attempt. The thesis may only be repeated once.

In the submitted thesis the written copies and the electronic version for archiving are identical in content.

Place, Date

Signature of author