# Aspects of Monstrous Moonshine

Ben Allen

Department of Mathematics
The University of Auckland

Supervisor: Dr. Pedram Hekmati

A dissertation submitted in partial fulfillment of the requirements for the degree of BSc(Hons) in Mathematics, The University of Auckland, 2022.

# Abstract

We give an outline of certain aspects of the theory of Monstrous Moonshine, such as the construction of the Leech lattice, the Monster group, the $j$-function, and the Moonshine Module. We also survey some recent generalisations of Monstrous Moonshine.

# Acknowledgement

I would like to thank my supervisor Pedram Hekmati for his guidance, his patience, and most importantly the opportunity to work alongside him.

I would also like to thank my colleagues in the Postgraduate Office for giving me a valuable perspective on Mathematics.

# Contents

# Chapter 1

# Introduction

Monstrous Moonshine is the study of the unexpected link between the largest finite simple sporadic group and a certain modular function. We give an introduction to finite simple groups, and elliptic curves where the modular functions arise. We then give some details on where Monstrous Moonshine originated and where it is currently.

A finite group is simple if it has no proper normal subgroups. A classification of these groups was completed around 1980, see [21]. A finite simple group must be one of the following:

- Cyclic group of prime order,
- Alternating group of index greater than four,
- One of sixteen infinite families of groups of Lie type,
- One of twenty six 'sporadic' groups.

An interesting observation from this classification is the finite family of sporadic groups. The largest group in this family is called the Monster, denoted by $\mathbb{M}$. The difficulty in studying this group may be attributed to its very large order:

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

In $\mathbb{ATLAS}$ [5] is given a collection of character tables for many important finite simple groups, including the sporadic groups. Importantly the Monster has only 194 irreducible representations and thus a conveniently small character table. The four smallest irreducible representations have dimensions 1, 196883, 21296876, and 842609326.

Consider an arbitrary field $\mathbb{F}$. An elliptic curve $E(\mathbb{F})$ is a set of points in $\mathbb{F}^2$ satisfying the Diophantine equation

$$y^2 = x^3 + Ax + B$$

for some $A, B$ in $\mathbb{F}$. Much like other Diophantine equations, elliptic curves have many important applications in Number Theory.

The $j$-invariant is an invariant quantity of elliptic curves which determines precisely when two elliptic curves have isomorphic solution sets. The set of elliptic curves over the complex numbers may be parameterised by a complex variable, which results in $j$ being a complex-valued function. In the variable $q = \exp(2\pi iz)$ the $j$-invariant has the following Fourier expansion.

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots .$$

Monstrous Moonshine is the theory behind the strange link between the Monster group and the $j$-invariant. This connection was first observed by McKay who noticed a rather 'moonshine' relationship between the dimensions of irreducible representations of the Monster and the coefficients of the $j$-invariant, subtract the constant term 744. This is summarised in the McKay relations below:

$$\begin{aligned} 1 &= 1 \\ 196884 &= 196883 + 1 \\ 21493760 &= 21296876 + 196883 + 1 \\ 864299970 &= 842609326 + 21296876 + 2 \cdot 196883 + 2 \cdot 1 \\ &\cdots \end{aligned}$$

Thompson believed that there could exist a graded vector space with each subspace a representation of the Monster. Such a vector space would have the form $V = V_0 \oplus V_1 \oplus V_2 \oplus \cdots$ with *graded dimension*

$$\dim_* V(z) := \dim V_0 \frac{1}{q} + \dim V_1 + \dim V_2 q + \dim V_3 q^2 \cdots .$$

The theory of Monstrous Moonshine is known to have begun out of two conjectures, one of which we can now state:

**Conjecture 1** (Thompson-Mckay)**.** *There exists a vector space $V^\natural = \bigoplus_i V_i$ and a representation $\mathbb{M} \to Aut(V)$ such that*

$$dim_* V = j - 744.$$

The Thompson-McKay Conjecture was proven by Frenkel, Lepowsky, and Meurman using the theory of vertex operators.

$V^\natural$ above is called the moonshine module. It turns out that $V^\natural$ has a much richer structure than initially anticipated. We call a function a *Hauptmodul* if it belongs to a special set of functions we will make precise later, see Subsection 3.3.3. Since each $V_i$ is a representation of

the Monster, we can take the trace of an element $g$ in each representation. This gives what is known as the Thompson-McKay series

$$\mathrm{tr}_g V = \mathrm{tr}(g|_{V_0})\frac{1}{q} + \mathrm{tr}(g|_{V_1}) + \mathrm{tr}(g|_{V_2})q + \mathrm{tr}(g|_{V_3})q^2 + \cdots .$$

When $g = 1$ this returns $j - 744$. This leads us to the second conjecture.

**Conjecture 2** (Conway-Norton)**.** *The vector space $V^\natural = \bigoplus_i V_i$ has a representation $\mathbb{M} \to Aut(V)$ and $tr_g V$ as a Hauptmodul.*

The Conway-Norton Conjecture was proven by Borcherds who was awarded a Fields Medal for his work in 1998.

## 1.1 Overview

In Chapter **2** we develop important structures that were used to originally prove existence of the Monster. Such structures include the Leech lattice; the densest packing of spheres in 24 dimensions, representation theory of finite groups, and the extraspecial 2-groups. An outline of Griess' construction of the Monster group is given. In Chapter **3** we introduce the $j$-invariant in its natural historical setting. We then move to elliptic functions and finally modular functions; specifically their role in Monstrous Moonshine. Chapter **4** introduces affine Lie algebras and vertex operator algebras with motivation from Physics, and gives an outline of the construction of the moonshine module, which itself shadows Griess' construction of the Monster. In Chapter **5** we explore some recent results with moonshine generalised to other sporadic groups.

## 1.2 Prerequisites and Notation

We assume the reader is familiar with introductory Topology, Complex Analysis, Lie Theory, and Group Theory.

Some notation we use may not be standard. We attempt to make a coherent list of such:

- $\mathcal{P}(\Omega)$ denotes the power set; that is, the set of all subsets of $\Omega$;
- $\mathbf{Z}(G)$ denotes the centre of the group $G$;
- $\mathbb{F}$ and $\mathbb{K}$ denote arbitrary fields;
- $\mathrm{Aut}(G)$ is the set of automorphisms of some algebraic structure $G$;
- $\emptyset$ is the empty set;
- $\mathbf{N}_G(H)$ is the normaliser of a subgroup $H$ in a group $G$;
- $\mathbf{C}_G(H)$ is the centraliser of a subgroup $H$ in a group $G$;
- $\mathbf{Conj}(G)$ denotes the set of conjugacy classes of a group $G$;
- A $p$-group is a group of order $p^n$ for some integer $n$ and prime $p$;
- The size of a finite group $G$ is written $|G|$;
- The commutator of group elements $g, h$ is written $[g, h] = ghg^{-1}h^{-1}$;
- If $\star$ is some associative binary operation on $G \times G$, then $G^{\star n}$ is this operation executed on $G \times \cdots \times G$, $n$ copies of $G$;

# Chapter 2

# The Monster

This chapter gives an introduction to codes and integer lattices, character theory in characteristic 0, and extraspecial 2-groups. these structures are important in the construction of the Monster group, of which an outline is given in the final section. Character theory is important historically as being involved in the discovery of the Monster group and Monstrous Moonshine, as discussed in the Introduction.

## 2.1 Golay Code and Leech Lattice

Section **2.1** aims to introduce even codes and integer lattices. Even codes such as the Hamming and Golay codes are constructed. Integer lattices and their automorphism groups are defined, and a method to construct them from codes is given. In particular, we construct the $E_8$ and Leech lattices from the Hamming and Golay codes, respectively.

### 2.1.1 Codes

Let $\Omega$ be a finite set, and $\mathcal{P}(\Omega)$ its power set. The symmetric difference $A \triangle B := (A \setminus B) \cup (B \setminus A)$ of two sets $A$ and $B$ in $\mathcal{P}(\Omega)$ has the following properties:

- $A \triangle B \in \mathcal{P}(\Omega)$;
- $A \triangle A = \emptyset$;
- $A \triangle \emptyset = A$;
- $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
- $A \triangle B = B \triangle A$,

for all $A, B, C \in \mathcal{P}(\Omega)$. Hence we can regard $\mathcal{P}(\Omega)$ as a $\mathbb{Z}_2$-vector space (elementary abelian 2-group) with $\triangle$ for addition and $\emptyset$ as zero.

We call a subspace $\mathfrak{C}$ of $\mathcal{P}(\Omega)$ a *code on* $\Omega$ if the order of every element in $\mathfrak{C}$ is divisible by 2. The only codes we need are those of type II; a code $\mathfrak{C}$ on $\Omega$ is *type II* if

$$|\Omega| \in 4\mathbb{Z},\ |C| \in 4\mathbb{Z} \text{ for all } C \in \mathfrak{C},\ \Omega \in \mathfrak{C}.$$

The *orthogonal complement* $\mathfrak{C}^\perp$ of $\mathfrak{C}$ is the set of elements

$$\mathfrak{C}^\perp := \{S \subset \Omega \mid |S \cap C| \in 2\mathbb{Z}\ \forall\ C \in \mathfrak{C}\} = \{S \subset \Omega \mid b(S, \mathfrak{C}) = 0\}.$$

The above is defined in terms of the bilinear form $b(A, B) = |A \cap B| \pmod 2$ associated to the quadratic form $Q(A) := \frac{1}{2}|A| \pmod 2$. We say a code $\mathfrak{C}$ is *self-orthogonal* if $\mathfrak{C} = \mathfrak{C}^\perp$.

We consider now the following Hamming codes:

**Proposition 2.1.1.** *There exists a self-orthogonal code of type II on* $|\Omega| = 8$.

*Proof.* Let $\Omega = \mathbb{Z}_7 \cup \{\infty\}$, the projective line over $\mathbb{Z}_7$. Divide $\Omega$ into quadratic residues (elements that are squares in $\mathbb{Z}_7$) and non-quadratic residues;

$$Q = \{0, 1, 2, 4\};$$
$$N = \Omega \setminus Q = \{3, 5, 6, \infty\}.$$

Then the spaces

$$\mathfrak{C}_1 := \langle i + N \mid i \in \mathbb{Z}_7 \rangle;$$
$$\mathfrak{C}_2 := \langle -i - N \mid i \in \mathbb{Z}_7 \rangle,$$

are self-orthogonal codes of type II, where $i + N := \{3 + i, 5 + i, 6 + i, \infty\}$.

□

We are now ready to construct the Golay code.

**Definition 2.1.2.** Let $\mathfrak{C}_1, \mathfrak{C}_2, \Omega$ be as before. The Golay code is the following self-orthogonal type II code in $\mathcal{P}(\Omega^3)$:

$$\mathfrak{C}_{12} := \langle (S, S, \emptyset), (S, \emptyset, S), (T, T, T) \mid S \in \mathfrak{C}_1,\ T \in \mathfrak{C}_2 \rangle.$$

$M_{24} := Aut(\mathfrak{C}_{12})$ is one of Mathieu's sporadic simple groups, simplicity is proved in [15] *p.*130.

### 2.1.2 Lattices

Codes can be used to construct lattices; Type II codes give rise to type II lattices. In this subsection we define lattices and show the general idea of constructing lattices from codes, most importantly the Leech lattice. There are several nontrivial constructions of the Leech lattice, however the 'Golay code route' we will use here demonstrates well some important properties required for Monstrous Moonshine.

**Definition 2.1.3.** A lattice $L$ of rank $n$ is a free abelian group generated by an $\mathbb{R}$-linearly independent set of vectors $\{a_1, ..., a_n\} \subset \mathbb{R}^n$. In other words,

$$L = a_1\mathbb{Z} \oplus ... \oplus a_n\mathbb{Z}.$$

With respect to the canonical symmetric nondegenerate bilinear form $\langle \cdot, \cdot \rangle : L \times L \to \mathbb{R}$ on $\mathbb{R}^n$, $L$ is *integral* if $\langle x, y \rangle \in \mathbb{Z}$ for all $x, y \in L$, and *even* (or type II) if $\langle x, x \rangle \in 2\mathbb{Z}$ for all $x \in L$. Define the fundamental parallelepiped for $L$ as the set

$$\mathcal{F}_L = \left\{ \sum_{i=1}^{n} x_i a_i \;\middle|\; x_i \in [0, 1) \right\}.$$

We call a lattice *unimodular* if the volume of $\mathcal{F}_L$ is 1. This is equivalent to requiring $\det(L) := \det(a_1, ..., a_n)$ to be $\pm 1$.

A lattice $L$ is *self-dual* if it equals its dual

$$L^\circ := \{x \in \mathbb{R}^n \mid \langle x, y \rangle \in \mathbb{Z} \ \forall y \in L\}.$$

The automorphism group of a lattice $L$ denoted $\mathrm{Aut}(L)$ is the set of linear operators which permute the basis elements of the lattice. It has the important subgroup

$$\mathrm{O}(L) := \{T \in \mathrm{Aut}(L) \mid \langle Tx, Ty \rangle = \langle x, y \rangle \ \forall x, y \in L\}.$$

**Proposition 2.1.4.** *Let $L$ be a lattice of rank $n$ with associated symmetric nondegenerate bilinear form $\langle \cdot, \cdot \rangle$. Then $Aut(L)$ is a finite group.*

*Proof.* By change of basis $\mathrm{GL}(L)$ is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{Z})$, and is therefore a group with the discrete topology. Extending the bilinear form to the whole space $\mathbb{R}^n$, we see that $\mathrm{Aut}(L) \subseteq \mathrm{GL}(L) \cap O_n(\mathbb{R})$, where

$$O_n(\mathbb{R}) := \{T \in \mathrm{GL}_n(\mathbb{R}) \mid \langle Tx, Ty \rangle = \langle x, y \rangle \ \forall x, y \in \mathbb{R}^n\}.$$

Let $A \in O_n(\mathbb{R})$ have matrix representation $(A_{ij})$ in some fixed basis. Then $A^T A = 1$ has $A_{1i}^2 + ... + A_{ni}^2 = 1$ which implies $|A_{ij}| \leq 1$ for all $i, j$, and thus $O_n(\mathbb{R})$ is compact.

Any discrete subset of a compact set is finite, so $\mathrm{Aut}(L)$ must be finite.

□

*Example* 2.1.5. The most basic of lattices is the integer lattice $\mathbb{Z}$ with basis element 1. $\mathrm{Aut}(\mathbb{Z})=\{-1,1\}$. The fundamental parallelepiped volume is 1 so $\mathbb{Z}$ is unimodular.

We note that every automorphism group of a lattice contains the normal subgroup $\langle -1\rangle$. We need the following identity:

**Proposition 2.1.6** (Index-Determinant Formula)**.** *Let $L$ be a rational lattice, and $M$ a sublattice of $L$ with finite index $[L:M]$. Then*

$$det(L)[L:M]^2 = det(M).$$

*Proof.* See Theorem 2.3.3 in [15]. The proof applies the Smith Normal Form. □

**Proposition 2.1.7.** *Let $\mathfrak{C}$ be a self-orthogonal type II code on $|\Omega| = n$ elements. Define a basis $\{a_1, ..., a_n\}$ of $\mathbb{R}^n$ indexed by $\Omega$ such that $\langle a_i, a_j\rangle = 2\delta_{ij}$, and for short write $a_C = \sum_{k\in C} a_k$. Finally define $Q := \sum_{k\in\Omega} a_k\mathbb{Z}$. Then the lattice*

$$L(\mathfrak{C}) := Q + \sum_{C\in\mathfrak{C}} \frac{1}{2} a_C\mathbb{Z}$$

*is even unimodular.*

*Proof.* $\mathfrak{C}$ is a type II code so $|\Omega| = 4k$ for some $k \in \mathbb{N}$.

Even: Write $L \ni x = x^i a_i$ for $x^i \in \mathbb{Z}$. Then $\langle x, x\rangle = x^i x^j \cdot 2\delta_{ij} = \sum_i 2(x^i)^2 \in 2\mathbb{Z}$. Hence $L$ is even.

Integral: Let $x, y \in L$. Then

$$\langle x, y\rangle = \frac{1}{2}(\langle x+y, x+y\rangle - \langle x, x\rangle - \langle y, y\rangle) \in \mathbb{Z}.$$

Hence $L$ is integral.

Unimodular: $Q$ is a sublattice of $L = L(\mathfrak{C})$ with quotient $L/Q \cong \mathfrak{C}$. From linear algebra $\dim\mathfrak{C} + \dim\mathfrak{C}^\perp = n$ which implies $\dim\mathfrak{C} = 2k$. Since $\mathfrak{C}$ is a vector space over $\mathbb{Z}_2$ we must have $|\mathfrak{C}| = 2^{2k}$, and hence $[L:Q] = 2^{2k}$. It is easy to see that $\det Q = 2^{|\Omega|} = 2^{4k}$, so by Proposition 2.1.6 we have $\det(L) = \det(Q)[L:Q]^{-2} = 2^{4k}\cdot 2^{-4k} = 1$, and therefore $L$ is unimodular. □

*Example* 2.1.8. Let $\mathfrak{C}$ be one of the Hamming codes. Then the lattice $L(\mathfrak{C})$ is isometric to the $E_8$ lattice; the most densely packed lattice in 8 dimensions. This can be seen since $L(\mathfrak{C})$ has rank 8 and $E_8$ is the unique even unimodular lattice of rank 8, see Viazovska's

paper [18], work which won her the 2022 Fields medal.

An important lattice we wish to consider is one of 24 unique lattices called the *Niemeier* lattices.

**Theorem 2.1.9** (Niemeier)**.** *There are exactly* 24 *unique even unimodular lattices of rank* 24*, up to equivalence. Furthermore, there is a unique such lattice with no length-square* 2 *vectors, known as the Leech lattice.*

*Proof.* See Niemeier's famous 1968 classification [1].

□

*Example* 2.1.10. The automorphism group of the Leech lattice $\Lambda$ is nontrivial. Conway's group $\mathrm{Co}_0$ is defined to be this group. Since $\langle -1\rangle \lhd \mathrm{Co}_0$, we have $\mathrm{Co}_1 := \mathrm{Co}_0/\langle -1\rangle$ which is Conway's first sporadic finite simple group. There are two others; $\mathrm{Co}_2$ and $\mathrm{Co}_3$, which are found by fixing specific points in the Leech lattice and then taking the respective automorphism groups, see [2].

**Proposition 2.1.11.** *For some integer lattice* $L$ *define* $L_n := \{a \in L \mid \langle a, a\rangle = n\}$*. The Leech lattice* $\Lambda$ *has the following properties:*

1. $\Lambda_2 = \emptyset$*;*
2. $\Lambda_4 = 196560$*.*

*Proof.* 1 follows from Theorem 2.1.9. For 2 see Theorem 10.4.1 in [15].

□

*Remark* 2.1.12. The set of vectors $L_2$ are called the roots of $L$.

Similar to Example 2.1.8 for the $E_8$ lattice, we can construct the Leech lattice from the Golay code $\mathfrak{C}_{12}$:

Let $\mathfrak{C}_{12}$ be the Golay code and $A := \Omega^3$ the set of elements for this code. Consider the even unimodular lattice (a Niemeier lattice)

$$N := Q + \sum_{C \in \mathfrak{C}_{12}} \frac{1}{2} a_C \mathbb{Z}$$

and the homomorphism $\theta : \mathbb{Q}^{24} \to \mathbb{Q}$ defined by $\theta(x) := \langle \frac{1}{4} a_A, x\rangle$. Since the Golay code is type II we must have $\theta(a_C) \in 2\mathbb{Z}$ for $C \in \mathfrak{C}_{12}$. We can see that $\theta(a_i) = \frac{1}{2}$ for all roots $a_i$ of $N$, so consider the rootless sublattice $M := N \cap \theta^{-1}(\mathbb{Z})$ which has index 2 since $\theta(N) = \frac{1}{2}\mathbb{Z}$. Finally define $\nu_i := \frac{1}{4} a_A - a_i$ for some fixed $i$, which can be seen to have square-length 4. We will show that the lattice $\Lambda := M + \nu_i \mathbb{Z}$ must be the Leech lattice.

- Rootless: This is immediate since $M$ is rootless.
- Unimodular: $\nu_i \notin M$ but $2\nu_i \in M$, so $M$ has index 2 in $\Lambda$. But $M$ has index 2 in $N$, so $\det \Lambda = \det N = 1$ by Proposition 2.1.6.

## 2.2 Character Theory

In this section we recall some well-known results from the classical theory of characters, including orthonormality relations and character tables. $G$ denotes a finite group. All representations are over $\mathbb{C}$.

**Definition 2.2.1.** Let $(\pi, V)$ be some representation of $G$. The *character* $\chi_\pi$ of this representation is defined by

$$\begin{aligned} \chi_\pi : G &\longrightarrow \mathbb{C} \\ g &\mapsto \text{Trace}(\pi(g)). \end{aligned}$$

A character is said to be irreducible if its corresponding representation is irreducible.

**Theorem 2.2.2.** *Let $Irr_{\mathbb{C}}(G)$ denote the set of irreducible characters of $G$ over $\mathbb{C}$. Then $|Irr_{\mathbb{C}}(G)| = |\boldsymbol{Conj}(G)|$ and*

$$|G| = \sum_{\chi \in Irr_{\mathbb{C}}(G)} |\chi(e)|^2.$$

**Theorem 2.2.3.** *Let $\mathcal{C}(G, \mathbb{C})$ denote the set of all functions from $G$ to $\mathbb{C}$ which are constant on the conjugacy classes of $G$. Given the inner product $\langle \cdot, \cdot \rangle$ on $\mathcal{C}(G, \mathbb{C})$ defined by the formula*

$$\langle \sigma, \tau \rangle := \frac{1}{|G|} \sum_{g \in G} \sigma(g)\overline{\tau(g)},$$

*$(\mathcal{C}(G, \mathbb{C}), \langle \cdot, \cdot \rangle)$ is an inner product space with orthonormal basis $Irr_{\mathbb{C}}(G)$.*

*Example* 2.2.4. Characters are constant on conjugacy classes. Thus the above theorems allow us to form a square table, called the character table, consisting of the characters of some group. We show the character table for $S_4$.

| Rep\ Conj | () | (12)(34) | (12) | (1234) | (123) |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $-1$ | $-1$ | 1 |
| $\chi_3$ | 2 | 2 | $\cdot$ | $\cdot$ | $-1$ |
| $\chi_4$ | 3 | $-1$ | 1 | $-1$ | $\cdot$ |
| $\chi_5$ | 3 | $-1$ | $-1$ | 1 | $\cdot$ |

$\mathbb{ATLAS}$ [5] contains the character tables of all the sporadic groups. A table of size $194\times194$ is large enough to describe all irreducible characters of the Monster.

## 2.3 Extraspecial 2-Groups

This section provides a light introduction to the theory of extraspecial 2-groups. We begin with standard $p$-group theory, such as nilpotency, and Frattini subgroups, to motivate the definition of extraspecial $p$-groups. We then give a method to construct larger such groups from the smallest when $p = 2$, which evidently gives a classification of extraspecial 2-groups.

**Proposition 2.3.1.** *Let $G$ be a finite group, and $G'$ its derived group. If $N \trianglelefteq G$, then $G' \leq N$ if, and only if, $G/N$ is abelian.*

*Proof.* Suppose $G/N$ is abelian. Choose any $a, b \in G$. By hypothesis:

$$\begin{aligned}[a,b]N &= aNbNa^{-1}Nb^{-1}N \\ &= N,\end{aligned}$$

so $[a, b] \in N$. Since $a, b$ were arbitrary, $G' \leq N$.

Conversely suppose that $G' \leq N$. Again choose any $a, b \in G$. Then:

$$\begin{aligned}aNbN &= abN \\ &= ab[b^{-1}, a^{-1}]N \\ &= baN \\ &= bNaN,\end{aligned}$$

hence $G/N$ is abelian.

□

**Definition 2.3.2.** A group $G$ is *nilpotent* if $G$ has a normal series

$$G = G_0 \rhd G_1 \rhd ... \rhd G_r = 1$$

such that

$$\frac{G_i}{G_{i+1}} \leq Z\left(\frac{G}{G_{i+1}}\right)$$

for all $0 \leq i \leq r - 1$. Such a normal series is called a *central series*.

Any abelian group is nilpotent. An important property of nilpotent groups is the following:

**Proposition 2.3.3.** *Given a nilpotent group $G$, let $H$ be a proper subgroup of $G$. Then $H < \mathbf{N}_G(H)$.*

*Proof.* We know that $G$ has a central series:

$$G = G_0 \rhd G_1 \rhd ... \rhd G_r = 1.$$

We first show that $[G_i, G] \leq G_{i+1}$ for all $0 \leq i \leq r-1$.

$$\begin{aligned} \frac{G_i}{G_{i+1}} \leq Z\left(\frac{G}{G_{i+1}}\right) &\iff [xG_{i+1}, yG_{i+1}] \leq G_{i+1} \text{ for } x \in G_i,\ y \in G \\ &\iff [x,y]G_{i+1} \leq G_{i+1} \\ &\iff [x,y] \in G_{i+1} \\ &\iff [G_i, G] \leq G_{i+1}. \end{aligned}$$

For $H < G$ choose $k$ such that $G_k \leq H$ and $G_{k-1} \not\leq H$. Then $[G_{k-1}, H] \leq G_k \leq H$ and thus $G_{k-1} > H$ normalises $H$.

□

For a fixed prime $p$, a $p$-group is a group in which the order of every element is a power of $p$. Next we shall consider several properties of finite $p$-groups.

**Proposition 2.3.4.** *Every finite $p$-group is nilpotent.*

*Proof.* See 5.2.4 in [3]. This is an extension of Proposition 2.3.3.

□

**Corollary 2.3.5.** *Let $M < P$ be a maximal subgroup of a finite $p$-group $P$. Then $M \lhd P$.*

Let $G$ be some finite group. The *Frattini subgroup* $\mathbf{Frat}(G)$ of $G$ is the intersection of all maximal subgroups of $G$. This subgroup is normal, which can be seen by taking the intersection of all maximal subgroups as images of automorphisms of $G$. Then apply the special case of inner-automorphisms. The next proposition will motivate the definition for extraspecial groups.

**Proposition 2.3.6.** *Let $P$ be some finite $p$-group for some prime $p$. Then the quotient $P/\mathbf{Frat}(P)$ is isomorphic to a direct sum of copies of $\mathbb{Z}_p$.*

*Proof.* First we show that $P' \leq \mathbf{Frat}(P)$. Choose any maximal subgroup $M < P$. By Proposition 2.3.3, $M$ is normal in $P$. The index of $M$ in $P$ is $p$, so the quotient $P/M$ is cyclic of order $p$. Thus $P/M$ is abelian, and therefore $P' \leq M$. But $M$ was arbitrary, so $P' \leq \mathbf{Frat}(P)$.

Secondly we show that $x^p \in \mathbf{Frat}(P)$ for all $x \in P$. Since $P/M$ is cyclic, $xM \in P/M$ has $x^pM = (xM)^p = M$, and thus $x^p \in M$. Again, $M$ was arbitrary, so $x^p \in P/M$.

Any element in $P/\mathbf{Frat}(P)$ has the form $x\mathbf{Frat}(P)$ for some $x \in P$. We then have $(x\mathbf{Frat}(P))^p = x^p\mathbf{Frat}(P) = \mathbf{Frat}(P)$, so every element in $P/\mathbf{Frat}(P)$ has order $p$, and therefore $P/\mathbf{Frat}(P)$ is isomorphic to the direct sum of copies of $\mathbb{Z}_p$.

□

We arrive at the type of $p$-group we wish to study; a type so defined to maximise this direct sum of $\mathbb{Z}_p$'s.

**Definition 2.3.7.** Let $P$ be a finite $p$-group. $P$ is called *extraspecial* if $\mathbf{Frat}(P) = \mathbf{Z}(P)$ and $|\mathbf{Z}(P)| = p$.

*Example* 2.3.8. The dihedral group $\mathcal{D}_4$ of 8 elements is an extraspecial 2-group. In fact, if we define the product

$$\mathcal{D}_4 \boxtimes \mathcal{D}_4 := \mathcal{D}_4 \times \mathcal{D}_4 / \{(u,u) \in \mathbf{Z}(\mathcal{D}_4) \times \mathbf{Z}(\mathcal{D}_4)\}$$

and extend this naturally to finitely many $\mathcal{D}_4$, we get $(\mathcal{D}_4)^{\boxtimes n}$ as an extraspecial 2-group for all $n$.

Evidently every extraspecial 2-group can be formed along the lines of the above example. Extraspecial 2-groups have order $2^{1+2n}$ for some $n \in \mathbb{N}$. There are two types:

- $2_+^{1+2n} \cong (\mathcal{D}_4)^{\boxtimes n}$;
- $2_-^{1+2n} \cong (\mathcal{D}_4)^{\boxtimes (n-1)} \boxtimes \mathcal{Q}_8$,

where $\mathcal{Q}_8$ is the quaternion group. For a proof of this see [6].

## 2.4 Griess' Method

In finite group theory many of the sporadics satisfy a *hypothesis*: A group $G$ satisfies the hypothesis $\mathcal{H}(\omega, L)$ if there is an involution $z \in G$ such that its centraliser $C = \mathbf{C}_G(z)$ has an extraspecial subgroup $Q = 2_+^{2\omega+1}$ such that $C/Q \cong L$, and such that $z$ is not weakly closed in $Q$ relative to $G$ (see Definition 2.4.1). The idea is to list all groups satisfying a certain

hypothesis. If this list has only one group, then we can define said group in terms of the hypothesis.

We define what it means to be weakly closed relative to some overgroup.

**Definition 2.4.1.** Let $H \leq K \leq G$ be groups. We say that $H$ is weakly closed in $K$ relative to $G$ if whenever $g^{-1}Hg \leq K$ we have $g^{-1}Hg \leq H$.

This means that for any hypothesis above we have $z \notin \mathbf{C}_G(Q)$. This condition is important because occasionally the extraspecial 2-group will also require $\mathbf{C}_G(Q) = \mathbf{Z}(Q)$; one of the many conditions in the definition of a *large extraspecial 2-group*, see [9].

*Example* 2.4.2. Fischer's Baby Monster $\mathbb{B}$ satisfies the hypothesis $\mathcal{H}(11, \mathrm{Co}_2)$, where $\mathrm{Co}_2$ is Conway's second sporadic group and is the unique such group. See [9]

The existence of any group is usually done by constructing it as the automorphism group of some algebraic structure. For the sporadics this is unsurprisingly a difficult task. Griess proved the existence of the Monster group by constructing it as the automorphism group of a 196884-dimensional commutative nonassociative algebra $\mathcal{B}$ known as the Griess algebra. We give an outline of the method he used as it is mirrored in the proof of the Thompson-McKay Conjecture (see Conjecture 1).

1. Construct the group $C$ above as a well-chosen extension of $\mathrm{Co}_1$ by $Q \cong 2^{1+24}_+$;
2. Define a vector space $\mathcal{B}$ such that $C$ acts on it in some way; the action is given in [4], the details of which are omitted due to their complicated nature;
3. Define an algebra structure on $\mathcal{B}$ such that $C$ is invariant under this structure, and hence $C \subseteq \mathrm{Aut}(\mathcal{B})$;
4. Define an involution $\sigma$ such that $\sigma \notin C$ and $\sigma$ is invariant under the structure above, and hence $\sigma \in \mathrm{Aut}(\mathcal{B})$;
5. Show that the group $G := \langle C, \sigma \rangle \subseteq \mathrm{Aut}(\mathcal{B})$ is isomorphic to the Monster; that is, show that $G$ is simple and has $|G| = |\mathbb{M}|$.

A uniqueness argument finally shows that $\mathbb{M}$ is defined as the simple group satisfying the hypothesis $\mathcal{H}(12, \mathrm{Co}_1)$. A complete uniqueness proof is given in [8]

# Chapter 3

# The $j$-Invariant

In this chapter we introduce elliptic curves and a function which parametrises their isomorphism classes, known as the $j$-function. We then consider complex tori and their relation to elliptic curves over the complex numbers, which gives us a meromorphic form of the $j$-function. Finally we consider $q$-expansions of important meromorphic functions such as the $j$-function and theta series of integer lattices; in particular for the Leech lattice in Chapter 2.

## 3.1 Elliptic Curves

The aim of this section is to introduce elliptic curves over an arbitrary field. We do this by first considering a general cubic in normal form, and define what it means for two such cubics to be isomorphic. We then use appropriate changes of variables to reduce the number of terms in the cubic, which results in the Weierstrass form of the cubic. The Weierstrass form allows us to more readily define elliptic curves. Finally we introduce the well-known $j$-invariant, which precisely determines when two elliptic curves are isomorphic.

We begin our study of elliptic curves by considering the set of solutions of a general cubic polynomial over some field $\mathbb{F}$, with characteristic not equal to 2 nor 3, in its *normal form*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.1}$$

The notation of the constants becomes clearer after considering isomorphisms between normal form cubics.

**Definition 3.1.1.** An *admissible change of variables* is one of the form

$$x = u^2\overline{x} + r, \quad y = u^3\overline{y} + su^2\overline{x} + t, \tag{3.2}$$

where $u, r, s, t \in \mathbb{F}$, $u \neq 0$.

We say two cubics are *isomorphic* if there exists an admissible change of variables between them. A quick calculation gives the coefficients $\overline{a}_i$ of

$$\overline{y}^2 + \overline{a}_1\overline{x}\overline{y} + \overline{a}_3\overline{y} = \overline{x}^3 + \overline{a}_2\overline{x}^2 + \overline{a}_4\overline{x} + \overline{a}_6$$

in terms of $u, r, s, t$, and $a_j$:

- $u\overline{a}_1 = a_1 + 2s$;
- $u^2\overline{a}_2 = a_2 - a_1 s + 3r - s^2$;
- $u^3\overline{a}_3 = a_3 + a_1 r + 2t$;
- $u^4\overline{a}_4 = a_4 - a_3 s + 2a_2 r - a_1(t + rs) + 3r^2 - 2st$;
- $u^6\overline{a}_6 = a_6 + a_4 r - a_3 t + a_2 r^2 - a_1 rt + r^3 - t^2$.

We transform the cubic from normal form into the *Weierstrass form*

$$y^2 = x^3 + Ax + B, \tag{3.3}$$

which has only two coefficients to work with. We first make the substitution $(x, y) = (x', \frac{1}{2}(y' - a_1x' - a_3))$ (requiring char $\mathbb{F} \neq 2$) which gives

$$(y')^2 = 4(x')^3 + b_2(x')^2 + 2b_4x' + b_6, \tag{3.4}$$

where

- $b_2 = 4a_2 + a_1^2$;
- $b_4 = 2a_4 + a_1a_3$;
- $b_6 = 4a_6 + a_3^2$.

Under the same admissible change of variables as before, the $\overline{b}_i$'s become

- $u^2\overline{b}_2 = b_2 + 12r$;
- $u^4\overline{b}_4 = b_4 + rb_2 + 6r^2$;
- $u^6\overline{b}_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3$.

The next step is to *depress* the right-hand side of equation 3.4; that is, to make the substitution $(x', y') = (x'' - b_2/12, 2y'')$ (requiring char $\mathbb{F} \neq 3$), removing the degree 2 term, which gives

$$(y'')^2 = (x'')^3 - \frac{c_4}{48}x'' - \frac{c_6}{864}, \tag{3.5}$$

where

- $c_4 = b_2^2 - 24b_4$;
- $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

Again under our admissible change of variables, the $\overline{c}_i$'s become

- $u^4\overline{c}_4 = c_4$;
- $u^6\overline{c}_6 = c_6$.

Now that we have transformed our cubic curve into Weierstrass form, we can define an elliptic curve.

**Definition 3.1.2.** An *elliptic curve* is a cubic curve which can be put in the form

$$y^2 = x^3 + Ax + B = f(x)$$

with $f$ having no repeated roots.

In other words, $f$ and its derivative share no roots. See Figure 3.1 for an example of an elliptic curve.

We can define a constant, called the discriminant, of a cubic curve, which determines when such a curve is elliptic. We use the *resultant* of $f$ and its derivative.

**Proposition 3.1.3.** *Let $R$ be a Unique Factorisation Domain and $f, g$ polynomials in $R[x]$ given by*

$$f(x) = a_m x^m + ... + a_1 x + a_0 \quad \textit{and} \quad g(x) = b_n x^n + ... + b_1 x + b_0.$$

*The resultant $R(f,g)$ of $f$ and $g$ is the element of $R$ given by the following $(m+n)\times(m+n)$ determinant:*

$$R(f,g) := \left| \begin{pmatrix} a_0 & a_1 & \cdots & a_m & & & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{m-1} & a_m & & & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & & a_0 & a_1 & \cdots & \cdots & a_m \\ b_0 & b_1 & \cdots & b_{n-1} & b_n & & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & & b_{n-1} & b_n & & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & b_0 & b_1 & & \cdots & \cdots & b_n \end{pmatrix} \right|$$

*Let $f, g$ and $R$ be as above. Then $f$ and $g$ have a common factor of strictly positive degree in $R[x]$ if, and only if, $R(f,g) = 0$.*

*Proof.* This is a consequence of Theorem 4.2 of the Appendix of Chapter 2 in [11], the proof of which uses greatest-common-divisor methods of polynomials.

□

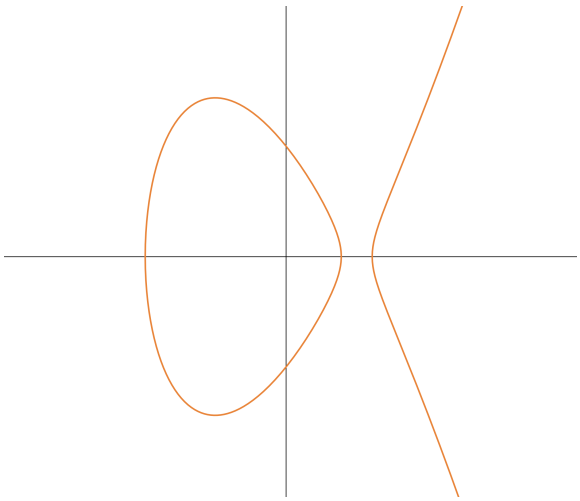

Figure 3.1: The elliptic curve $y^2 = x^3 - 5x + 4$

*Example* 3.1.4. Let $f(x) = ax^2 + bx + c$ and $g(x) = f'(x) = 2ax + b$ be polynomials in $\mathbb{Q}[x]$. The resultant of $f$ and $g$ is

$$\begin{aligned} R(f,g) &= \left| \begin{pmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{pmatrix} \right| \\ &= a(4ac - b^2), \end{aligned}$$

which gives an expression for the discriminant of the quadratic $f$.

Applying the resultant to an arbitrary cubic curve $C$ shows that $C$ is an elliptic curve if, and only if, its resultant is non-zero. From this we define the *discriminant* of a cubic curve to be $\Delta := -16R(f, f')$, where the factor of $-16$ is solely for computational simplicity.

A cubic curve in Weierstrass form 3.3 has discriminant $\Delta = -16(4A^3 + 27B^2)$. Substituting in the coefficients of equation 3.5 gives the relation $12^3\Delta = c_4^3 - c_6^2$.

It can be seen that under our admissible change of variables, $u^{12}\overline{\Delta} = \Delta$, which leads us to the $j$-invariant:

**Proposition 3.1.5.** *Let $E$ be an elliptic curve such that $\Delta \neq 0$. Define the $j$-invariant as the function on the set of elliptic curves given by*

$$j(E) := \frac{c_4^3}{\Delta}. \tag{3.6}$$

*Then $j$ is invariant under any admissible change of variables.*

It is immediate to see that two elliptic curves are isomorphic if, and only if, their corresponding $j$-invariants are equal.

## 3.2 Elliptic Functions

This section on elliptic functions is split into two subsections:

The first demonstrates that the set of solutions of a given elliptic curve over $\mathbb{C}$ can be turned into a Lie group isomorphic to a real 2-torus. The second subsection uses elliptic functions to associate an elliptic curve to a given complex torus. Then, using the result of the first subsection, associates a complex torus to a given elliptic curve.

The main result is that there is a bijection between the set of complex tori and the set of elliptic curves.

### 3.2.1 Elliptic Curve Group Law

An elliptic curve $E$ in normal form (Equation 3.1) can be written as a homogeneous polynomial

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{3.7}$$

with domain $\mathbb{P}^2(\mathbb{C}) := \mathbb{C}^3 \setminus \{0,0,0\}/\sim$, where

$$[x,y,z] \sim [x',y',z'] \iff [x',y',z'] = [\lambda x, \lambda y, \lambda z] \ for\ \lambda \in \mathbb{C}^*.$$

Here $\mathbb{P}^2$ is the complex projective plane. Call $\infty := [0,1,0]$ the *point at infinity*.

For a given elliptic curve $E$ over $\mathbb{C}$ we denote $E(\mathbb{C}) = \{[x,y,z] \in \mathbb{P}^2 \mid F(x,y,z) = 0;\ z \neq 0\} \cup \{\infty\}$. Since $F$ is homogeneous, for $z \neq 0$ this is equivalent to $F(x,y,1) = 0$ which returns the normal form.

Let $P, Q \in E(\mathbb{C})$. We write $PQ$ for the third point of intersection of the line passing through $P$ and $Q$. $PQ \in E(\mathbb{C})$ since $\mathbb{C}$ is algebraically closed. We define $P + Q := \infty(PQ)$; that is, the third point intersecting the line through $\infty$ and $PQ$ in $\mathbb{P}^2$. It can be seen that $\infty$ is the identity for this group operation. We note that $E(\mathbb{C})$ forms an abelian group. Since $E$ is over $\mathbb{C}$, $E(\mathbb{C})$ is a smooth topological group.

**Theorem 3.2.1.** *Let $E$ be an elliptic curve over $\mathbb{C}$. Then $E(\mathbb{C})$ is an abelian Lie group.*

We need the following theorem.

**Theorem 3.2.2.** *A real compact connected abelian Lie group is isomorphic to a real torus.*

*Proof.* This is a classical result in the theory of Lie groups. □

**Proposition 3.2.3.** *Let $E$ be an elliptic curve over $\mathbb{C}$. Then $E(\mathbb{C})$ is a real 2-dimensional compact connected abelian Lie group; hence $E(\mathbb{C}) \cong \mathbb{T}^2 = \mathbb{S}^1 \times \mathbb{S}^1$.*

*Proof.* $E(\mathbb{C})$ is an abelian Lie group following Theorem 3.2.1.

For compactness, let $F(X, Y, Z)$ be the homogeneous polynomial of $E$ given by equation 3.7. It is easy to see that since $F$ is continuous and $F : E(\mathbb{C}) \to \{0\}$, $E(\mathbb{C})$ is closed. Since $E(\mathbb{C}) \subseteq \mathbb{P}^2$, it is enough to show that $\mathbb{P}^2$ is compact. Let

$$U_i := \{[x_1, x_2, x_3] \in \mathbb{P}^2 \mid x_i \neq 0\}.$$

Then $U_1 = \{[1, \alpha, \beta] \in \mathbb{P}^2 \mid \alpha, \beta \in \mathbb{C}\} \cong \mathbb{C}^2$ topologically. $U_i$ are open in and finitely cover $\mathbb{P}^2$.

Connectedness follows since $\mathbb{C}$ is algebraically closed; that is, any line connecting disconnected components of the group over $\mathbb{Q}$ or $\mathbb{R}$ has solutions over $\mathbb{C}$ and must thus connect these components.

Finally, since $E$ provides a relation between $x, y$ in the point $[x, y, 1]$, $E(\mathbb{C})$ is 1-dimensional over $\mathbb{C}$ and therefore 2-dimensional over $\mathbb{R}$.

□

### 3.2.2 Complex Tori

An elliptic function is a meromorphic function which is doubly-periodic. Given two $\mathbb{R}$-linearly independent complex numbers $\omega_1$ and $\omega_2$, we define a complex lattice as $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. The elliptic functions we will study are those with periods $\omega_1$ and $\omega_2$. The reason for this association is seen when one quotients $\mathbb{C}$ by $\Lambda$. $\mathbb{C}/\Lambda$ is called a *complex torus* since it is homeomorphic to the 2-torus. Elliptic functions associated to $\Lambda$ are simply meromorphic functions on $\mathbb{C}/\Lambda$.

Before introducing the most important of elliptic functions we need the following result:

**Proposition 3.2.4.** *For a complex lattice $\Lambda$ the series*

$$\sum_{\omega \in \Lambda^*} \frac{1}{\omega^s} \tag{3.8}$$

*converges absolutely for all $s > 2$.*

*Proof.* Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Any element in $\Lambda$ has the form $n_1\omega_1 + n_2\omega_2$. Since $\Lambda$ is discrete, there exists a $\delta > 0$ such that $|n_1\omega_1 + n_2\omega_2| \geq \delta(|n_1| + |n_2|)$ for all $n_i \in \mathbb{Z}$. There are $4n$ pairs $(n_1, n_2)$ such that $|n_1| + |n_2| = n$, so

$$\begin{aligned}\sum_{\omega \in \Lambda^*} \frac{1}{|\omega^s|} &\leq \frac{1}{\delta^s} \sum_{(n_1,n_2) \in (\mathbb{Z}^2)^*} \frac{1}{(|n_1| + |n_2|)^s} \\ &\leq \frac{1}{(4\delta)^s} \sum_{n \geq 1} \frac{1}{n \cdot n^s},\end{aligned}$$

which converges when $s - 1 > 1$ by the $p$-series test.

□

The series in equation 3.8 for $s = 2k$ is denoted $G_{2k}$, $k > 1$. Note that for odd $s$ the series is zero.

**Definition 3.2.5.** Let $\Lambda$ be a complex lattice. The $\wp$-function and $\xi$-function with respect to $\Lambda$ defined over the complex plane are the series'

$$\wp(z;\Lambda) = \wp(z) := \frac{1}{z^2} + \sum_{\omega\in\Lambda^*}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right),$$
$$\xi(z;\Lambda) = \xi(z) := \frac{1}{z} + \sum_{\omega\in\Lambda^*}\left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

These series are absolutely convergent since they both grow like $\sum_\omega 1/\omega^3$.

It can be seen that $\wp(z)$ is elliptic with respect to $\Lambda$ and $\xi'(z) = -\wp(z)$. Our next task is to show that $\wp$ satisfies a very special differential equation. We begin by writing $\xi$, then $\wp$, in terms of the series' $G_{2k}$.

The geometric series has

$$\frac{1}{z-\omega} = -\sum_{n\geq 0}\frac{z^n}{\omega^{n+1}}$$

for $|z| < |\omega|$. Plugging this into $\xi$ gives

$$\begin{aligned}\xi(z) &= \frac{1}{z} - \sum_{\omega\in\Lambda^*}\sum_{n\geq 2}\frac{z^n}{\omega^{n+1}}\\ &= \frac{1}{z} - \sum_{k\geq 2} G_{2k} z^{2k-1},\end{aligned}$$

which finally has

$$\wp(z) = \frac{1}{z^2} - \sum_{k\geq 2}(2k-1)G_{2k}z^{2k-2}. \tag{3.9}$$

The differential equation we seek is first-order and non-linear.

**Proposition 3.2.6.** *Let $\Lambda$ be a complex lattice. The Weierstrass $\wp$-function on $\Lambda$ satisfies the following differential equation:*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3, \tag{3.10}$$

*where $g_2 = 60G_4$ and $g_3 = 140G_6$.*

*Proof.* We write the first few terms of $\wp'^2,\ 4\wp^3$, and $g^2\wp$ in series:

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \cdots \\
\wp'(z) &= -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + \cdots \\
\wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \cdots \\
4\wp(z)^3 &= 4\wp(z)\left(\frac{1}{z^2} + 6G_4 + 10G_6 z^2 + \cdots\right) \\
&= \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + \cdots \\
60G_2 = 4\wp(z) &= \frac{60G_4}{z^2} + 180G_4^2 z^2 + \cdots .
\end{aligned}$$

Then

$$f(z) := \wp'^2 - 4\wp^3 + 60G_4\wp + 140G_6$$

is easily seen as an elliptic function with no poles, hence holomorphic. Since $f$ is defined on the compact complex torus $C/\Lambda$, it is bounded. By Liouville's theorem $f$ is constant. But the constant term of $f$ is zero, so $f = 0$.

□

Now we can associate to every complex torus $\mathbb{C}/\Lambda$ an elliptic curve $E$ of the form

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

with $g_2 = 60G_4,\ g_3 = 140G_6$, and show that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

To get the associated complex lattice $\Lambda$ from a given elliptic curve $E$ one considers integrating around the two non-contractible circles of the torus of $E(\mathbb{C})$. This gives the two periods of $\Lambda$ such that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. The detailed calculations are given in [11] (Chapter 9 Section 6).

Recall the $j$-function of an elliptic curve given in equation 3.6. One sees that equation 3.10 has the form of equation 3.4 with $b_2 = 0$. Plugging $g_2/2, g_3$ in place of $b_4, b_6$ in the $j$-function formula gives

$$j(\Lambda) = 12^3 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}. \tag{3.11}$$

Finally, two complex lattices $\Lambda$ and $\Omega$ are said to be *homothetic* if there exists a complex number $\lambda \in \mathbb{C}^*$ such that $\Omega = \lambda\Lambda$. Every complex lattice is homothetic to a complex lattice $\Lambda_\tau := 1\mathbb{Z} \oplus \tau\mathbb{Z}$, where $\tau$ is a complex number with positive imaginary part. We call $\tau$ the *complex period* of $\Lambda_\tau$.

**Lemma 3.2.7.** *Two complex tori $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_\sigma$ are isomorphic if, and only if, $\Lambda_\tau$ and $\Lambda_\sigma$ are homothetic.*

## 3.3 Modular Functions

In this section we define modular functions of weight $2k$. We show that a rather general class of modular functions of weight 0 are periodic and therefore have a Fourier series. We then define the important class of functions called Hauptmoduln. Finally we consider basic theory of modular forms and integer lattices, allowing us to arrive at a particularly interesting result relating the $j$-function and the Leech lattice.

### 3.3.1 Modular Functions and Congruence Subgroups

In the previous section we showed that two elliptic curves are isomorphic if, and only if, their corresponding complex tori are analytically isomorphic. We would like to know, given any two complex numbers in the upper half-plane $\mathbb{H}$, whether or not their respective elliptic curves are isomorphic. Following lemma 3.2.7, it is enough to show that the homothety of two complex tori is an equivalence relation on $\mathbb{H}$. However we instead use $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$, which will be explained shortly.

**Proposition 3.3.1.** *The full modular group $\mathbb{SL}_2(\mathbb{Z})$ is the set of all invertible integral valued matrices with determinant one. The Möbius action*

$$\bullet : \mathbb{SL}_2(\mathbb{Z}) \times \mathbb{H}^* \to \mathbb{H}^* \text{ given by}$$
$$\left( \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tau \right) \mapsto \frac{a\tau + b}{c\tau + d}$$

*defines an equivalence relation on the upper half-plane $\mathbb{H}$. Furthermore, two complex tori are homothetic if, and only if, their corresponding complex periods are equivalent with respect to the Möbius action.*

The set of equivalence classes above is written $X(1) = X_{\mathbb{SL}_2(\mathbb{Z})} := \mathbb{H}^*/\mathbb{SL}_2(\mathbb{Z})$, and is called a modular curve. It can be seen that the elements of this modular curve are in one-to-one correspondence with the isomorphism classes of elliptic curves. In other words, the $j$-function is constant on the equivalence classes of $\mathbb{H}^*$ as an elliptic function.

The points $\mathbb{Q} \cup \{\infty\}$ are equivalent under the action of $\mathbb{SL}_2(\mathbb{Z})$, and so form an element in the modular curve $X_{\mathbb{SL}_2(\mathbb{Z})}$. This point is called the *point at infinity*, and is added to ensure $X_{\mathbb{SL}_2(\mathbb{Z})}$ is isomorphic to the 2-sphere; that is, this added point is the "north pole" in the stereographic projection of the sphere onto $\mathbb{C} \cup \{\infty\}$.

Generally a modular curve is the set $X_\Gamma := \mathbb{H}^*/\Gamma$ for some subgroup $\Gamma$ of $\mathbb{SL}_2(\mathbb{Z})$, which can be seen to be locally diffeomorphic to $\mathbb{C}$.

We now define modular functions on the upper half-plane, which are heavily linked with the elliptic functions of the previous section.

**Definition 3.3.2.** Let $k \in \mathbb{Q}$ and $\Gamma$ be a discrete subgroup of $\mathbb{SL}_2(\mathbb{Z})$. A *modular form* of level $\Gamma$ and weight $2k$ is a holomorphic function $f : \mathbb{H}^* \to \mathbb{H}^*$ with finitely many poles such that for all $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ and $\tau \in \mathbb{H}$ we have

$$f(\gamma \bullet \tau) = (c\tau + d)^{2k} f(\tau).$$

The space of all such functions is denoted $\mathcal{M}_{2k}(\Gamma)$.

*Example* 3.3.3. The elliptic functions $G_{2k}$ in the previous section, known as Eisenstein series, are modular forms of level $\mathbb{SL}_2(\mathbb{Z})$ and weight $2k$. To see this, let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$, $\tau \in \mathbb{H}$. Then

$$\begin{aligned} G_{2k}(\gamma \bullet \tau) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m + \gamma \bullet \tau n)^{2k}} \\ &= \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \left( \frac{c\tau + d}{(bn + dm) + \tau(an + cm)} \right)^{2k} \\ &= (c\tau + d)^{2k} G_{2k}(\tau). \end{aligned}$$

Our main functions of study are a variation of modular forms, called modular functions. These are modular forms of weight zero without the restriction of being holomorphic; that is, they are meromorphic and completely invariant under the action of their weight group $\Gamma$. Modular forms are 'more common', and we can simply construct modular functions from quotients of modular forms.

*Example* 3.3.4. The $j$-function in equations 3.6 and 3.11 is a modular function of level $\mathbb{SL}_2(\mathbb{Z})$. This can be seen by either constructing $j$ from the modular forms $G_4$ and $G_6$, or by observing that $j$ is constant on the equivalence classes of $\mathbb{H}^*$.

Now we consider some discrete subgroups of $\mathbb{SL}_2(\mathbb{Z})$.

**Definition 3.3.5.** The *principal congruence subgroup of level* $n$ is the subgroup $\Gamma(n)$ of $\mathbb{SL}_2(\mathbb{Z})$ defined by

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{SL}_2(\mathbb{Z}) \;\middle|\; a, d \equiv 1 \mod n;\ c \equiv 0 \mod n \right\}.$$

A subgroup of $\mathbb{SL}_2(\mathbb{Z})$ is called a *congruence subgroup* if it contains $\Gamma(n)$ for some $n \in \mathbb{N}$.

*Example* 3.3.6. The *Hecke congruence subgroup of level n* given by

$$\Gamma_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod n \right\}$$

is a congruence subgroup for all $n \in \mathbb{N}$.

*Remark* 3.3.7. If a modular form or function has level $\Gamma_0(n)$ we sometimes write weight $n$ instead. Note that $\Gamma_0(1) = \mathbb{SL}_2(\mathbb{Z})$.

### 3.3.2 Periodic Functions and Laurent Series

We consider subgroups $\Gamma$ of $\mathbb{SL}_2(\mathbb{Z})$ which contain $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ such that any modular function $f$ of level $\Gamma$ and any weight satisfies $f(\tau + 1) = f(T \cdot \tau) = f(\tau)$ for all $\tau \in \mathbb{H}^*$. It can be seen that $T \in \Gamma(n)$, thus $T$ is in any congruence group.

The function $f$ has period 1 and thus may be expanded in a Fourier series

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n \tau} = \sum_{n=0}^{\infty} a_n q^n, \tag{3.12}$$

where $a_n \in \mathbb{C}$. This is called the $q$-expansion of $f$. More precisely, any modular function of level $\Gamma$, $\Gamma$ a congruence subgroup, has a $q$-expansion.

One can show that $G_{2k}$ has $q$-expansion

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geq 1} \frac{n^{2k-1} q^n}{1 - q^n},$$

where $\zeta$ is the Riemann Zeta function. Plugging the above into equation 3.11 of the $j$-function gives

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \tag{3.13}$$

following a routine calculation. Notice that these coefficients are closely related to the dimension of irreducible representations of the Monster group of Chapter 2, subtract the constant term 744. From now on we write $J(\tau) := j(\tau) - 744$ as the $J$-function.

### 3.3.3 Hauptmoduln

It can be seen that any modular function of level $\Gamma$ is naturally a meromorphic function on the modular curve $X_\Gamma$, and the set of all such functions form a field. The aim of this subsection is to show that this field of meromorphic functions $\mathcal{M}(X_\Gamma)$ is finitely generated.

We say $\Gamma$ has genus zero if $X_\Gamma$ has genus zero topologically; that is, if it is homeomorphic to the 2-sphere.

Let $\Gamma$ be a genus zero congruence subgroup. The meromorphic functions $f \in \mathcal{M}(X_\Gamma)$ have

$$f : X_\Gamma \to \mathbb{C}_\infty := \mathbb{C} \cup \{\infty\} \cong \mathbb{P}^1.$$

The next theorem shows that if $f$ has at least one pole, then the meromorphic function field defined on some modular curve is finitely generated.

**Proposition 3.3.8.** *Let $f : X_\Gamma \to \mathbb{C}_\infty$ be a meromorphic function on some modular curve $X_\Gamma$ associated to some congruence subgroup $\Gamma$, and let $pol(f)$ denote the number of poles of $f$. Then*

$$[\mathcal{M}(X_\Gamma) : \mathbb{C}(f)] \leq pol(f), \tag{3.14}$$

*where $\mathbb{C}(f)$ is the quotient field generated by $f$.*

*Proof.* This is a specialised form of Proposition 1.17 in [10].

□

Considering only genus zero modular curves $X_\Gamma$, we see that $X_\Gamma \cong \mathbb{S}^2 \cong \mathbb{C}_\infty$, so there exists a bijection, say $J_\Gamma \in \mathcal{M}(X_\Gamma)$, such that $J_\Gamma(X_\Gamma) = \mathbb{C}_\infty$. Since $J_\Gamma$ is a bijection there is a unique $z \in X_\Gamma$ such that $J_\Gamma(z) = \infty$. Thus $J_\Gamma$ has a unique pole, so we may write the Laurent series as

$$J_\Gamma(\tau) = \frac{1}{q} + \sum_{n \geq 0} a_n q^n \tag{3.15}$$

for complex $a_n$.

This bijection has a unique pole, so a simple application of Proposition 3.3.8 shows that $\mathcal{M}(X_\Gamma) = \mathbb{C}(J_\Gamma)$. Such a function that generates the meromorphic function field of a genus zero modular curve is called a *Hauptmodul*.

The $j$-function in equation 3.13 is a Hauptmodul of $\mathbb{SL}_2(\mathbb{Z})$ since it is a bijection from $\mathbb{SL}_2(\mathbb{Z})$ onto $\mathbb{C}_\infty$.

### 3.3.4 Modular Forms and Extremal Lattices

**Theorem 3.3.9.** *The normalised Eisenstein functions $E_{2k} := \frac{G_{2k}}{2\zeta(2k)}$ are modular forms. The complex vector space $\mathcal{M}_{2k}(\mathbb{SL}_2(\mathbb{Z}))$ has basis elements $E_4^a E_6^b$ for integers $a, b \geq 0$ with $4a + 6b = 2k$.*

Recall that the discriminant of an elliptic curve is $\Delta = \frac{c_4^3 - c_6^2}{12^3}$. It can be seen that $\Delta$ is a modular form of level 1 and weight 12 by substituting $G_4$ and $G_6$ into the above formula appropriately. However we 'normalise' the discriminant to get what is known as the *modular discriminant*

$$\begin{aligned}\Delta(\tau) &= \frac{E_4^3(\tau) - E_6^2(\tau)}{12^3} \\ &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots .\end{aligned}$$

Most importantly this allows us to write the classical $j$-function as

$$j(\tau) = \frac{E_4^3(\tau)}{\Delta(\tau)}.$$

Important modular forms are the *theta series* defined in terms of some chosen even unimodular lattice $L$. They are given as

$$\theta_L(\tau) := \sum_{\alpha \in L} q^{\frac{\langle \alpha, \alpha \rangle}{2}} = \sum_{n \in \mathbb{Z}} L_{2n} q^n$$

where $q = e^{2\pi i \tau}$ and $L_n$ is defined in Proposition 2.1.11.

**Proposition 3.3.10.** *Let $L$ be an even unimodular lattice of rank $n$. Then $\theta_L$ is a modular form of level 1 and weight $n/2$.*

*Proof.* We use the following Jacobi identity, where $L$ is an even lattice:

$$\theta_L(\tau) = \left(\sqrt{\frac{\tau}{i}}\right)^{\frac{n}{2}} \frac{1}{\det(L)} \theta_{L^*}(\tau).$$

The result follows when the identity is applied to an even unimodular lattice. The identity itself follows from the Poisson Summation Formula.

□

*Example* 3.3.11. The Leech lattice $\Lambda$ has theta function

$$\theta_\Lambda(\tau) = 1 + 196560q^2 + 196773120q^3 + 398034000q^4 + \cdots ,$$

see Theorem 10.5.1 in [15]. We can write this in a more informative way. We note that the Eisenstein series $E_4^3$ of weight 12 has the formula

$$E_4^3(\tau) = 1 + 720q + 179280q^2 + 16954560q^3 + 396974160q^4 + \cdots .$$

Using Theorem 3.3.9 we see that $\mathcal{M}_{12}$ has basis $E_4^3$ and $E_6^2$. Thus $E_4^3$ and $\Delta$ form

another basis for $\mathcal{M}_{12}$. By Proposition 3.3.10 $\theta_\Lambda$ is a modular form of weight 12, so we can write this theta series in terms of $E_4^3$ and $\Delta$; that is, $\theta_\Lambda = \alpha E_4^3 + \beta\Delta$ for some constants $\alpha$ and $\beta$. Comparing coefficients we get

$$\theta_\Lambda(\tau) = E_4^3(\tau) - 720\Delta(\tau).$$

Finally, dividing through by $\Delta$ gives the beautiful formula

$$\frac{\theta_\Lambda(\tau)}{\Delta(\tau)} = j(\tau) - 720 = J(\tau) + 24. \tag{3.16}$$

# Chapter 4

# The Moonshine Module

This chapter aims to introduce some of the required machinery to understand the construction of the Moonshine Module. The story begins with Lie algebras, vertex operator algebras, and partition functions. An important example given in Section 4.2 constructs a vertex operator algebra from a Lie algebra. We then consider vertex operator algebras constructed from lattices. Finally the Moonshine Module construction is outlined, and a summary in relation to the Thompson-McKay Conjecture is given.

## 4.1 Lie Algebras and Affine Algebras

In this section we define the Lie algebra and its affinisation. We construct the universal, tensor, and symmetric algebras of a Lie algebra, the former and latter being important in the construction of lattice vertex operator algebras. We also show that the universal algebra has a well-defined basis; a fact also known as the Poincaré-Birkhoff-Witt Theorem.

**Definition 4.1.1.** A Lie algebra over $\mathbb{K}$ is a $\mathbb{K}$-algebra $\mathfrak{l}$ where its algebra product $[\cdot,\cdot] : \mathfrak{l} \times \mathfrak{l} \to \mathfrak{l}$, here called the Lie bracket, satisfies the following:

- $[x, y] = -[y, x]$;
- $[x, [y, z]] = [[x, y], z] + [y, [x, z]]$,

for any $x, y, z \in \mathfrak{l}$.

*Example* 4.1.2. Any vector space $V$ can be made into a Lie algebra by defining $[x, y] = 0$ for any $x, y \in V$. Such a Lie algebra is said to be abelian.

*Example* 4.1.3. An important Lie algebra is the affine Lie algebra. Let $\mathfrak{g}$ be some finite-dimensional Lie algebra. The affinisation of $\mathfrak{g}$ is the centrally extended loop algebra

$$\hat{\mathfrak{g}} = \mathfrak{g} \otimes \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}C$$

where $C$ is a central element (i.e. $[x, C] = 0$ for all $x \in \hat{\mathfrak{g}}$) and the Lie bracket is

$$[a \otimes t^m, b \otimes t^n] = [a, b] \otimes t^{m+n} + m\delta_{m+n,0}C.$$

This Lie algebra is infinite dimensional.

**Definition 4.1.4.** Let $\mathfrak{g}$ be a finite-dimensional Lie algebra. The *tensor algebra* $T(\mathfrak{g})$ of $\mathfrak{g}$ is the graded vector space

$$T(\mathfrak{g}) := \bigoplus_{i \geq 0} T^i(\mathfrak{g}) = \mathbb{K} \oplus \mathfrak{g} \oplus (\mathfrak{g} \otimes \mathfrak{g}) \oplus (\mathfrak{g} \otimes \mathfrak{g} \otimes \mathfrak{g}) \oplus \cdots$$

where elements are to have only finitely many non-zero entries. We note that multiplication in the tensor algebra is the tensor product defined by

$$(v_1 \otimes ... \otimes v_n) \otimes (w_1 \otimes ... \otimes w_m) := v_1 \otimes ... \otimes v_n \otimes w_1 \otimes ... \otimes w_m$$

for $v_i, w_j$ elements in the tensor algebra. Thus the algebraic structure on the tensor algebra comes from the direct sum and the tensor product.

Consider the ideals of this algebra generated by the sets

$$I_u = \{a \otimes b - b \otimes a - [a, b] \mid a, b \in \mathfrak{g}\}, \text{ and}$$

$$I_s = \{a \otimes b - b \otimes a \mid a, b \in \mathfrak{g}\}.$$

The corresponding quotient algebras $\mathfrak{U}(\mathfrak{g}) := T(\mathfrak{g})/\langle I_u \rangle$ and $S(\mathfrak{g}) := T(\mathfrak{g})/\langle I_s \rangle$ are the *universal enveloping* and *symmetric* algebras of $\mathfrak{g}$, respectively. It can be seen that $\mathfrak{U}(\mathfrak{g})$ is a filtered associative algebra, while the symmetric algebra is graded commutative:

$$S(\mathfrak{g}) := \bigoplus_{i \geq 0} S^i(\mathfrak{g}) = \mathbb{K} \oplus \mathfrak{g} \oplus (\mathfrak{g} \odot \mathfrak{g}) \oplus (\mathfrak{g} \odot \mathfrak{g} \odot \mathfrak{g}) \oplus \cdots$$

where $\odot$ is the symmetric tensor product.

In order to work with the enveloping algebra we need to ensure the existence of a basis. The following well-known theorem states that any given basis of a Lie algebra determines a basis for its enveloping algebra:

**Theorem 4.1.5** (Poincaré-Birkhoff-Witt)**.** *Let $v_1, ..., v_n$ be an ordered basis for a Lie algebra $\mathfrak{g}$. Then $\{v_1^{\otimes a_1} \otimes \cdots \otimes v_n^{\otimes a_n} \mid a_i \in \mathbb{N}\}$ is a basis for $\mathfrak{U}(\mathfrak{g})$.*

*Proof.* See [16]. □

## 4.2 Vertex Operator Algebras

This section gives an introduction to the algebraic structures called vertex operator algebras (VOA's); they have relations to both Mathematics and Physics. The first part of this section introduces the classical partition function, important in Physics. The second part of this section gives the definition of an important Lie algebra called the Virasoro algebra, and finally the definition of a VOA. The relation of VOA's with the partition functions of Physics is also introduced.

### 4.2.1 Classical Partition Function

Let $\mathcal{H}$ be a Hilbert space with Hermitian form $\langle\cdot|\cdot\rangle$, where we are using bra-ket notation, and $H$ the Hamiltonian. The eigenvalues $E_n$ of $H$ are related by

$$H|\varphi_n\rangle = E_n|\varphi_n\rangle$$

where $\varphi_n$ are the eigenvectors of $H$. We note that these eigenvectors can be normalised to form an orthonormal basis for $\mathcal{H}$ with respect to $\langle\cdot|\cdot\rangle$. We define the classical partition function of a system $(\mathcal{H}, H)$ by

$$\mathcal{Z} := \mathrm{tr}_{\mathcal{H}} e^{-\beta H},$$

where $\beta := (k_B T)^{-1}$ is the inverse of temperature $T$ and $k_B$ is the Boltzmann constant. We will show that this form is equivalent to the partition function given in Statistical Mechanics:

$$\begin{aligned}
\mathcal{Z} &= \sum_{n\geq 0} \frac{(-\beta)^n \mathrm{tr}_{\mathcal{H}}(H^n)}{n!} = \sum_{n\geq 0} \frac{(-\beta)^n \sum_{k\geq 1}\langle\varphi_k|H^n|\varphi_k\rangle}{n!} \\
&= \sum_{n\geq 0} \frac{(-\beta)^n \sum_{k\geq 1} E_k^n\langle\varphi_k|\varphi_k\rangle}{n!} = \sum_{k\geq 1}\sum_{n\geq 0} \frac{(-\beta)^n E_k^n}{n!} \\
&= \sum_{k\geq 1} e^{-\beta E_k} = \sum_{m\geq 1} d(m) e^{-\beta E_m}.
\end{aligned}$$

The last line has $d(n)$ which counts the number of duplicate eigenvalues, while the second to last line is the familiar partition function. This form has useful applications in physics. For example, $\mathcal{Z}$ can be used to calculate a system's expected free energy $\langle E\rangle = -\frac{\partial \ln \mathcal{Z}}{\partial \beta}$. Other values such as the Helmholtz and Gibbs free energy, entropy, and heat capacity can also be derived from it.

### 4.2.2 Virasoro and Vertex Operator Algebras

The Virasoro algebra $\mathfrak{Vir}$, with central charge $c \in \mathbb{C}$, is the Lie algebra spanned by generators $L_n$ for $n \in \mathbb{Z}$ and $c$, with Lie bracket relations $[L_m, c] = 0$ and

$$[L_m, L_n] = (m-n)L_{m+n} + \frac{c}{12}m(m+1)(m-1)\delta_{m+n,0}.$$

We can thus write $\mathfrak{Vir}_c = \bigoplus_n \mathbb{C}L_n \oplus \mathbb{C}c$ with a $\mathbb{Z}$-gradation. This algebra occurs naturally when examining infinitesimal conformal transformations of a surface. Let such a surface be a complex torus. We can represent this torus with the modular parameter $\tau$ in the upper half-plane, which we have shown classifies complex tori up to modular transformations, which are themselves conformal transformations. From [17] the partition function of this surface is given by

$$\mathcal{Z}_{\mathcal{H}}(\tau) = \mathrm{tr}_{\mathcal{H}}(q^{L_0 - c/24}\overline{q}^{\overline{L_0} - \overline{c}/24})$$

where $q = e^{2\pi i\tau}$ and $\tau = i\frac{\beta}{2\pi} + \mu$ with $\mu$ the spin potential. From now on we only consider holomorphic CFT's; that is, when the partition function is meromorphic; that is, when $\mathcal{Z}_{\mathcal{H}}(\tau) = \mathrm{tr}_{\mathcal{H}}(q^{L_0 - c/24})$. Here $L_0$ plays the role of the Hamiltonian.

A vertex operator algebra (VOA) is a quadruple $(V, Y, \mathbf{1}, \omega)$, where $V = \bigoplus_{n\in\mathbb{Z}} V_n$ is a $\mathbb{Z}$-graded linear space and

$$Y : V \to \mathfrak{F}(V),\ v \mapsto Y(v,z) = \sum_n v_n z^{-n-1},$$

$$\mathbf{1}, \omega \in V,$$

- $Y(\omega, z) = \sum_n L_n z^{-n-2}$ with a constant $c$ such that

$$[L_m, L_n] = (m-n)L_{m+n} + \frac{c}{12}(m^3 - m)\delta_{m+n,0}\mathrm{Id}_V;$$

- $V_n = \{v \in V \mid L_0 v = nv\}$;
- $\dim V_n < \infty$, $V_n = 0$ for $n << 0$;
- $Y(L_{-1}u, z) = \partial Y(u, z)$.

*Example* 4.2.1. We construct the Heisenberg VOA (CFT for one free boson).
Let $A = \mathbb{C}a$ be a 1-dimensional vector space. Perform the affinization

$$\hat{A} = A \otimes \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}K$$

as in Example 4.1.3, with central element $K$ and Lie bracket

$$[a \otimes t^m, a \otimes t^n] = m\delta_{n+m,0}K.$$

Define $\hat{A}^{\geq} = \langle a \otimes t^n \mid n \geq 0 \rangle$ and $\hat{A}^{-} = \langle a \otimes t_n \mid n < 0 \rangle$, each of which is an ideal and subalgebra, respectively. Let $h \in \mathbb{C}$, and write $\mathbb{C}v_h$ as an $\hat{A}^{\geq}$-module with action

$$(a \otimes t^n) \cdot v_h = h\delta_{n,0} v_h;$$
$$K \cdot v_h = v_h.$$

Then

$$M_h := \mathrm{Ind}_{\mathcal{U}(\hat{A}^{\geq})}^{\mathcal{U}(\hat{A})} \mathbb{C}v_h \cong \mathcal{U}(\hat{A}^{-}) \otimes \mathbb{C}v_h$$

is the induced module which will be our VOA. Writing $a \otimes t^n$ as $a_n \in \mathrm{End}(M_h)$, and $a(z) = \sum_n a_n z^{-n-1}$ for a formal variable $z$. For $h = 0$ we have $a = a_{-1}v_0$ and

- $Y(a, z) = a(z)$;
- $\mathbf{1} = v_0$;
- $\omega = \frac{1}{2} a_{-1}^2 \mathbf{1}$;
- $c = 1$,

which gives $M_0$ a VOA structure.

If $v \in V_n$ then we say $v$ has homegeneity $n$. The idea is to interpret $L_0$ as the energy operator, then the homogeneity of $v \in V$ can be interpreted as its energy level.

Our space of states or Fock space in a VOA is $V$. Each $V_n$ is an eigenspace of $L_0$ which must be spanned by some basis, which is how we define dim $V_n$. When we take the trace of $q^{L_0 - c/24}$ with respect to the basis of $V$ we are of course counting the number of basis elements for each $V_n$ and 'pinning' this number to $q^n$. Hence the partition function of a VOA $V$ takes the form

$$\mathcal{Z}_V(\tau) = q^{-c/24} \sum_{n \in \mathbb{Z}} \dim\, V_n q^n$$

which provides motivation for the definition of VOA's; that is, if we can determine a VOA structure on a Fock space then we can easily determine its partition function. Interesting VOA's are those with central charge $c$ a multiple of 24. We can construct such VOA's using extremal lattices.

Like in Statistical Mechanics, we call the coefficient of $q^n$ the degeneracy (number of states) at that energy level, which in this case is dim $V_n$. If the partition function of a VOA is a modular function; that is, invariant under all elements of the modular group $\mathbb{SL}_2(\mathbb{Z})$, then we say the partition function is *modular invariant* or *modular*.

## 4.3 Lattice VOA's

This section introduces an important class of VOA's constructed from lattices, called Lattice VOA's; their importance in Monstrous Moonshine is shown in the following section.

**Definition 4.3.1.** Let $L$ be an even lattice. The lattice VOA $\mathcal{V}(L)$ is defined as

$$\mathcal{V}(L) := S(\mathfrak{h}_{\mathbb{Z}}^{-}) \otimes \mathbb{C}[L],$$

where $\mathfrak{h} = L \otimes \mathbb{C}$. The VOA structure is presented in [12].

We would like to find the partition function of a lattice VOA and determine when it is modular. Note that the partition function of a tensor product is the product of their respective partition functions, which can be seen by multiplying out the gradings of the VOA's through the tensor product, determining the partition function, and then factorising back to the required form. We first sate the partition function of $S(\mathfrak{h}_{\mathbb{Z}}^{-})$ for an arbitrary vector space $\mathfrak{h}$.

**Proposition 4.3.2.** *Define the eta function $\eta(\tau) = q^{-1/24}\prod_{n\geq 1}(1-q^n)$ with $q = e^{2\pi i\tau}$. Then*

$$\mathcal{Z}_{S(\mathfrak{h}_{\mathbb{Z}}^{-})}(\tau) = \frac{1}{\eta(\tau)^{\dim\mathfrak{h}}}.$$

*Proof.* See Section 1.10 in [7].

□

We state the well-known modular properties of the eta function.

**Proposition 4.3.3.** *The eta function defined above is meromorphic on the upper half-plane. For all $\tau \in \mathfrak{h}$ we have the following:*

$$\eta(\tau+1) = e^{\frac{\pi i}{12}}\eta(\tau);$$
$$\eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau}\eta(\tau).$$

*Proof.* This is a classical result. An application of the definition of $\eta$ gives the first identity, and an application of the Poisson Summation Formula gives the second identity.

□

Notice that the partition function in Proposition 4.3.2 is not modular. However, using the modular properties of $\eta$ given in Proposition 4.3.3 it is easy to see that $\eta(\tau)^{24k}$ is a modular form of weight $12k$ for some $k \in \mathbb{Z}_{>0}$.

If we consider $\mathbb{C}[L] = \sum_{n\geq 0} \mathbb{C}L_{2n}$ as a graded vector space, then the corresponding partition function must be

$$\mathcal{Z}_{\mathbb{C}[L]}(\tau) = \sum_{n\geq 0} L_{2n} q^n = \theta_L(\tau).$$

Hence

$$\mathcal{Z}_{\mathcal{V}(L)}(\tau) = \frac{\theta_L(\tau)}{\eta(\tau)^{\text{rank } L}}$$

which is modular for rank $L = 24k$ by Proposition 3.3.10.

*Example* 4.3.4. Let $\Lambda$ be the Leech lattice. Then from Example 3.3.11 we must have

$$\mathcal{Z}_{\mathcal{V}(\Lambda)}(\tau) = J(\tau) + 24$$

where $J$ is the $J$-function.

## 4.4 $\mathbb{Z}_2$-Orbifold Construction of $V^\natural$

In this section we give an outline of the construction of the Moonshine Module using what we have covered so far in previous sections. Any details omitted can be found in the book [7].

The following construction is similar to the construction of the Monster group in Section 2.4.

1. Recall that the Monster group $\mathbb{M}$ is the unique simple group satisfying the hypothesis $\mathcal{H}(12, \text{Co}_1)$. Furthermore, the group $2_+^{24}{\cdot}\text{Co}_1$ is a maximal subgroup since $\mathbb{M}$ was generated in Section 2.4 by this subgroup along with an involution. For further verification, see [20] for a near-complete list of the maximal subgroups of $\mathbb{M}$.
2. The Leech lattice $\Lambda$ has automorphism group $\text{Co}_0 \cong 2{\cdot}\text{Co}_1$.
3. Construct the lattice VOA $\mathcal{V}(\Lambda)$ which has discrete automorphism group $C \cong 2_+^{1+24}{\cdot}\text{Co}_1$. Importantly we have $\mathcal{Z}_{\mathcal{V}(\Lambda)}(\tau) = J(\tau) + 24$, see Example 4.3.4.
4. Let $\theta = -1$ be the central element in $\text{Co}_0$. Notably $\theta$ can be lifted to an automorphism of $\mathcal{V}(\Lambda)$, and thus we can form a new VOA by considering the eigenspaces of each gradation of $\mathcal{V}(\Lambda)$ with respect to the action of $\theta$, in direct sum with a carefully constructed 'twisted' section. The resulting VOA is called the Moonshine Module, written $V^\natural$. This is the $\mathbb{Z}_2$-orbifold process; precisely since $\langle\theta\rangle \cong \mathbb{Z}_2$.
5. Construct an automorphism $\sigma \notin C$ of $V^\natural$; this process is called triality.
6. Show that $\langle C, \sigma\rangle \cong \mathbb{M}$ is the full automorphism group of $V^\natural$ with $\mathcal{Z}_{V^\natural}(\tau) = J(\tau)$.

## 4.5 Summary

In the previous section we gave an outline of the construction of the Moonshine Module. In particular, the $J$-function introduced in Chapter 3 is the partition function and the Monster group introduced in Chapter 2 is the automorphism group. The Moonshine Module $V^\natural$ is indeed a vector space which satisfies all conditions of the Thompson-McKay Conjecture 1 in the Introduction.

# Chapter 5

# More Moonshine

The 26 sporadic groups can be partitioned into two sets:

1. The Happy Family: The collection of sporadics which can be found as subgroups of the Monster up to some extension:
   - First Generation (The Mathieu groups) $M_{11}$, $M_{12}$, $M_{22}$, $M_{23}$, and $M_{24}$;
   - Second Generation (The Leech Lattice groups[1]) $\mathrm{Co}_1$, $\mathrm{Co}_2$, $\mathrm{Co}_3$, $Suz$, $McL$, $HS$, and $HJ$;
   - Third Generation $\mathbb{M}$, $\mathbb{B}$, $\mathrm{Fi}_{22}$, $\mathrm{Fi}_{23}$, $\mathrm{Fi}'_{24}$, $Th$, $He$, and $HN$;
2. The Pariahs: The collection of sporadics which are not in the Happy Family.
   - $J_1$, $J_3$, $J_4$, $Ru$, $\mathrm{O'N}$, and $Ly$.

As one would expect it is more likely to find moonshine for Happy Family sporadics.

## 5.1 Happy Family

In this section we look at some results by Larissa Queen relating moonshine to Happy Family sporadics. We then consider a moonshine theory for groups $He$, $Th$, and $HJ$, which is at this time conjectural.

### 5.1.1 The Results of Queen

The Thompson-McKay series' of the conjugacy classes $2A$, $3C$, $5A$, $7A$ in the Monster correspond to the sporadic groups $\mathbb{B}$, $Th$, $HN$, $He$. An explanation of the notation for the conjugacy classes of the Monster can be found in the $\mathbb{ATLAS}$ [5].

[1] Automorphisms of sublattices of the Leech Lattice

### 5.1.2 Held, Thompson, and Hall-Janko

The Held sporadic group $He$ is known to satisfy the hypothesis $\mathcal{H}(3, PSL_3(2))$. Furthermore, $2_+^{1+6} \cdot PSL_3(2)$ is a maximal subgroup. It may be possible to replicate the construction of the moonshine module $V^\natural$ for the Held group.

The double cover $2 \cdot PSL_3(2)$ has 3 irreducible representations of degree 6 over $\mathbb{C}$. Choosing an appropriate basis one could construct an even lattice inside such a representation with $2 \cdot PSL_3(2)$ as the automorphism group. The associated lattice VOA has discrete automorphism group $2_+^{1+6} \cdot PSL_3(2)$. Finally an orbifolding could produce the required VOA to have $He$ as the automorphism group.

Similarly the Thompson and Hall-Janko sporadic groups $Th$ and $J_2$ satisfy the hypotheses $\mathcal{H}(4, A_9)$ and $\mathcal{H}(2, A_5)$, respectively, and both are maximal subgroups. In the general case, the constructions probably rely on the Schur cover of the quotient group being perfect, which is true in these cases. (The perfectness of $\mathrm{Co}_0$ is exploited in the construction of the Monster).

It must be noted however that the constructions of the Monster and the Moonshine Module are delicate, and replicating such constructions for the proposed groups above is likely not possible. Indeed any lattices constructed above would not be unimodular, so a VOA constructed from these processes would not have modular partition functions, see Section 4.3. For an account of the maximal groups above see [20].

## 5.2 Pariahs

In this section we discuss some recent results on moonshine theories of two Pariah sporadics; namely the O'Nan group O′N and the Rudvalis group $Ru$.

### 5.2.1 O'Nan

The O'Nan group O′N is the $12^{th}$ largest sporadic and $2^{nd}$ largest pariah, with group order

$$|\mathrm{O'N}| = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31.$$

There is a moonshine for this group, proven in [19]. We state the main theorem.

**Theorem 5.2.1.** *There exists a graded* O′N*-module*

$$W = \bigoplus_{0<m\equiv 0,3 \pmod 4} W_m$$

*and weight* $3/2$ *modular forms* $F_{[g]}$ *for each* $[g] \in Conj(\mathrm{O'N})$ *such that*

$$F_{[g]}(\tau) := -\frac{1}{q^4} + 2 + \sum_{0<m\equiv 0,3 \pmod 4} Trace(g|_{W_m}) q^m$$

*is a Hauptmodul for the group* $\Gamma_0(4|g|) < \mathbb{SL}_2(\mathbb{R})$.

The proof uses the theory of singular moduli; the study of rational values of the $j$-invariant. The paper remarks that at the time of publication $W$ is not given a VOA structure, but suggests one may exist given that

$$\sum_{m,n\equiv 0 \pmod 2} Trace(g|_{W_m}) q^{m+\frac{n^2}{4}} + \sum_{m,n\equiv 1 \pmod 2} Trace(g|_{W_m}) q^{m+\frac{n^2}{4}}$$

is the derivative of the $J$-function up to a constant.

As an example, for the conjugacy class of the identity $e \in \mathrm{O'N}$, the corresponding Hauptmodul is

$$F_{[e]}(\tau) = -\frac{1}{q^4} + 2 + 26752q^3 + 143376q^4 + 8288256q^7 + 26124256q^8 + \cdots,$$

with congruence group $\Gamma_0(4)$ and $[\Gamma_0(1) : \Gamma_0(4)] = 6$.

### 5.2.2 Rudvalis

The papers [13] and [14] construct a quadruple $(A_{Ru}, Y, \mathbf{1}, \Omega_{Ru})$ as a self-dual enhanced $U(1)$-VOA of rank 28, with full automorphism group isomorphic to $\mathbb{Z}_7 \times Ru$.

# Bibliography


[1] H.V. Niemeyer. "Definite Quadratische Formen der Diskriminante 1 und Dimension 24". In: *Doctoral Dissertation, Göttingen* (1968).

[2] J.H. Conway. "A group of order 8,315,553,613,086,720,000". In: *Bull. London Math. Soc.* 1.1 (1969), pp. 79–88.

[3] John S. Rose. *A Course on Group Theory*. Cambridge University Press, 1978.

[4] Robert L. Griess. "The friendly giant". In: *Inventiones mathematicae* 69 (1982), pp. 1–102.

[5] John H. Conway. *Atlas of Finite Groups : Maximal Subgroups and Ordinary Characters for Simple Groups*. Clarendon Press ; Oxford University Press, 1985.

[6] Michael. Aschbacher. *Finite Group Theory*. Cambridge University Press, 1986.

[7] I. Frenkel, J. Lepowsky, and A. Meurman. *Vertex Operator Algebras and the Monster*. Academic Press, 1988.

[8] Robert L. Griess, Ulrich Meierfrankenfeld, and Yoav Segev. "A Uniqueness Proof for the Monster". In: *Annals of Mathematics* 130.3 (1989), pp. 567–602. ISSN: 0003486X. URL: http://www.jstor.org/stable/1971455 (visited on 10/28/2022).

[9] M. Aschbacher. *Sporadic Groups*. Cambridge University Press, 1994.

[10] R. Miranda. *Algebraic Curves and Riemann Surfaces*. American Mathematical Society, 1995.

[11] D. Husemöller. *Elliptic Curves*. Springer-Verlag New York, Inc., 2004.

[12] J. Lepowsky and H. Li. *Introduction to Vertex Operator Algebras and Their Representations*. Birkhäuser, 2004.

[13] J.F. Duncan. "Moonshine for Rudvalis's sporadic group I". In: *arXiv:math/0609449* (2006), p. 56.

[14] J.F. Duncan. "Moonshine for Rudvalis's sporadic group II". In: *arXiv:math/0611355* (2006), p. 31.

[15] R. L. Griess Jr. *An Introduction to Groups and Lattices: Finite Groups and Positive Definite Rational Lattices*. Higher Education Press, 2011.

[16] Anne V. Shepler and Sarah Witherspoon. *Poincare-Birkhoff-Witt Theorems*. 2014. eprint: arXiv:1404.6497.

[17] H. Jockers. *Conformal Field Theory*. 2016. eprint: https://www.math.uni-hamburg.de/home/stern/Notes/CFT/Notes_CFT.pdf.

[18] Maryna Viazovska. "The sphere packing problem in dimension 8". In: (2016). DOI: 10.4007/annals.2017.185.3.7. eprint: arXiv:1603.04246.

[19] J.F.R. Duncan, N.H. Mertens, and K. Ono. "O'Nan moonshine and arithmetic". In: *arXiv:1702.03516* (2017), p. 40.

[20] Robert A. Wilson. *Maximal subgroups of sporadic groups*. 2017. eprint: arXiv:1701.02095.

[21] M. Aschbacher. "The Status of the Classification of the Finite Simple Groups". In: *Notices of the Am. Math. Soc.* 51.7 (), pp. 736–740.