The Leech lattice

Chen, T.

T. Chen

The Leech lattice: Sphere packings and the Conway groups

Bachelor thesis

14 July 2021

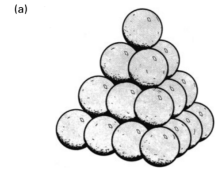
Thesis supervisor: dr. J.B. Vonk

Leiden University
Mathematical Institute

Contents

Introduction

The English mathematician Thomas Harriot was working as a mathematician for the statesman Sir Walter Raleigh in the late 16th and early 17th century when he was one day asked by Raleigh what the most efficient way was to stack cannonballs on a ship. This is a question that a modern-day grocery clerk might ask himself too when stacking apples for display. The problem of packing spheres in the densest possible way is called the sphere packing problem. In 3-dimensional space, the densest packing is given by extending the following configuration, a pyramid with square base, see [CSdlH98].



This conceptually not very complex problem remained unproven for the next four centuries and it was only in 2005 when a proof was published by the American mathematician Thomas Hales using computer assistance, see [Hal05].

The theory of sphere packings that was developed in these centuries has many applications in other sciences such as modern atomic theory and quantum gravity in physics, see [HMR19], and crystallography in chemistry, see [KP81]. The reason for this is that a subset of sphere packings, called the lattice packings, are inherently related to a certain symmetric structure called a lattice which is formed by the center of the spheres in a lattice packing. These lattices occur very often in nature.

This is not nearly the end of the story of sphere packings however since we can easily generalise this 3-dimensional problem to an n-dimensional problem for any $n \in \mathbb{Z}_{>0}$ where we pack n-dimensional spheres in $\mathbb{R}^n$. After this abstraction, many other surprising properties of sphere packings can be discovered and many more connections with other mathematical areas can be made. The ones we will focus on are coding theory and group theory, more precisely error-correcting codes and the Classification Theorem of finite simple groups which is a marvellous subject on its own.

Error-correcting codes are used when transmitting data so that small errors that pop up can be corrected by the receiver. One code in particular that was widely used is the Golay code $\mathcal{G}_{24}$ which was even used by NASA on space missions in the 20th century. A very special 24-dimensional lattice packing can be constructed using the Golay code. This lattice, called the Leech lattice Λ_{24}, was first discovered by John Leech in 1967, see [Lee67], and a year later a truly fascinating connection to group theory was found by John Conway, see [Con68].

Since lattices are very symmetric structures we can look at certain symmetries that form a group together. It turns out that one of the groups related to the symmetry group of the Leech lattice Λ_{24} is a never before discovered group called the first Conway group Co_1. This group is one of the sporadic groups that

play a crucial role in the Classification Theorem of finite simple groups which aims to classify the finite simple groups like how the periodic table classifies all atoms.

The classification consists of a few families containing an infinite number of finite simple groups but there are just 26 more finite simple groups that do not fit into any of these infinite families and are called the sporadic groups. The first sporadic groups were discovered in the 1860s and 1870s by the French mathematician Mathieu, see [Mat61] and [Mat73], and the largest of these Mathieu groups, M_{24}, is the symmetry group of the mentioned Golay code $\mathcal{G}_{24}$.

We see that this mysterious and fascinating Leech lattice has many connections with other mathematical areas and with the help of even another area of math, namely modular forms, it was finally proven in 2017 that the Leech lattice packing is the densest sphere packing in 24-dimensional space, see [CKM$^+$17].

In this thesis, we will give an easy to understand introduction to the Leech lattice for anyone that has basic knowledge of group theory. We start by discussing sphere packings and linear codes and then construct some objects, the hexacode and the Golay code, that will function as stepping stones for the Leech lattice. We will also study the symmetry groups of these three objects and prove the simplicity of the groups M_{24} and Co_1. We will not prove that Λ_{24} produces the densest 24-dimensional sphere packing since these proofs require entirely different techniques than the group theory we want to focus on.

In case the reader is not familiar with simple groups and the Classification Theorem, we advise them to read Appendix B after finishing section 3.3.1. If the reader has gotten curious to study more sporadic groups after finishing the main part of this thesis, they can read Appendix C where the other Mathieu and Conway groups are defined, as well as some other sporadic groups related to Co_1. Lastly, Appendix A contains any non-basic group theory that is needed in the proofs such as semidirect products and commutators.

The added value of this thesis compared to the existing literature is not only that many different sources are combined to give a comprehensive introduction to the Leech lattice but also that many verifications and proofs actually can not be found easily anywhere in the literature. The Leech lattice is usually part of a much bigger story which means not everything is worked out to detail. These proofs and verifications are not that easy however if you do not have a background in this area. This thesis is therefore meant for students or mathematicians active in other areas who want to gain a better understanding of the Leech lattice and the related sporadic groups. After finishing this thesis, the reader will have a solid foundation in this subject to study many other problems related to the Leech lattice.

1 Sphere packings

Our motivation for studying the Leech lattice is the sphere packing problem. What is the most efficient way to stack spheres in n dimensions? We will formalise this question in this chapter and provide some useful definitions and ideas that will help us in determining our approach to studying the Leech lattice. We will mostly follow [Slo02] and Chapters 1 and 2 in [CSdlH98].

Definition 1.1. An n-dimensional *sphere packing* is an infinite set of non-overlapping spheres in $\mathbb{R}^n$ with the same radius. So these spheres are allowed to touch but have pairwise disjoint interiors.

Remark 1.1.1. We use the Euclidean metric on $\mathbb{R}^n$.

We now define what we mean when we say 'most efficient'.

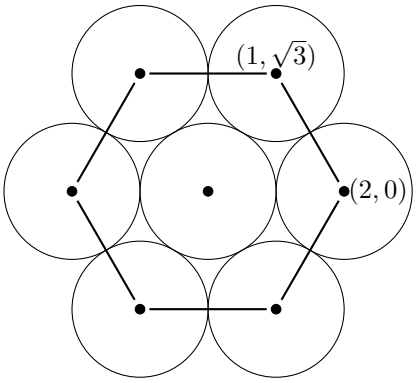
Definition 1.2. Let s_t be the sphere with center at the origin of $\mathbb{R}^n$ and radius t and let Vol be the volume function on $\mathbb{R}^n$. The *density* Δ of a sphere packing P is the limit

$$\Delta(P) = \lim_{t\to\infty} \frac{\sum_{b\in P} \mathrm{Vol}(b \cap s_t)}{\mathrm{Vol}(s_t)}$$

if it exists. In other words, the portion of space taken by the sphere packing.

If P is very symmetric we can calculate the density by dividing $\mathbb{R}^n$ into smaller identical parts. We will look at the *hexagonal sphere packing* in 2 dimensions.

Example 1.3. The *hexagonal sphere packing* in 2 dimensions consists of the circles with radius 1 and centers of the form $x(2,0) + y(1,\sqrt{3})$ with $x, y \in \mathbb{Z}$. The seven circles closest to the origin are then as follows.



It is called the hexagonal packing since the centers of six circles touching a given circle form a regular hexagon.

We can calculate the density of this sphere packing quite easily.

Lemma 1.4. *The density Δ of the 2-dimensional hexagonal sphere packing is $\frac{\pi}{2\sqrt{3}}$.*

Proof. The regular hexagons clearly form a regular tiling of $\mathbb{R}^2$ so the density Δ is equal to the proportion of space taken by the sphere packing in one of these hexagons. The circle and circular sectors of the hexagonal packing form 3 unit circles within one hexagon, so with area formulas we get

$$\Delta = \frac{3\pi}{6\sqrt{3}} = \frac{\pi}{2\sqrt{3}}$$

□

We were able to simplify our calculation because the centers in the hexagonal sphere packing form a simple and symmetric structure. In general, the centers are the most important pieces of information of a sphere packing since we can just choose half of the minimal distance between two centers as the radius of the spheres and recover the original or an even denser sphere packing. One particular type of sphere packing which is the one we will focus on, are the sphere packings whose centers form a type of structure called a *lattice*.

Definition 1.5. An n-dimensional *lattice* is an additive subgroup of $\mathbb{R}^n$ that contains a basis of $\mathbb{R}^n$ and is isomorphic to $\mathbb{Z}^n$. This is equivalent to being of the following form for some linearly independent $b_i \in \mathbb{R}^n$.

$$\mathbb{Z}b_1 + \mathbb{Z}b_2 + \ldots + \mathbb{Z}b_n$$

We call $\{b_1, \ldots, b_n\}$ a *basis* of the lattice.

Remark 1.5.1. The centers of the 2-dimensional hexagonal sphere packing from Example 1.3 form a lattice called A_2.

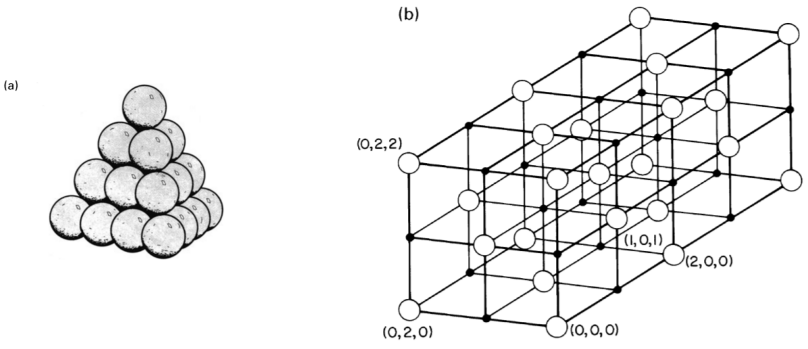
Definition 1.6. A *lattice packing* is a sphere packing whose centers form a lattice.

The lattice packings are the most interesting and studied sphere packings. We give another example which is one of the most well-known lattice packings.

Example 1.7. The 3-dimensional *face-centered cubic (fcc)* lattice is the set

$$\{x(1,1,0) + y(1,0,1) + z(0,1,1) : x, y, z \in \mathbb{Z}\}.$$

In other words, the points whose coordinates add up to an even number. The fcc lattice packing traditionally has the most real-life applications like stacking apples in the supermarket or cannonballs on the battlefield.



The figures are taken from [CSdlH98]. A subset of the sphere packing is depicted in (a) and the open circles in (b) are centers of the sphere packing.

One interesting class of lattices is the following.

Definition 1.8. Let an inner product $x \cdot y$ be given on $\mathbb{R}^n$. A lattice L is called *integral* if for all $x, y \in L$ we have $x \cdot y \in \mathbb{Z}$.

Example 1.9. The 3-dimensional fcc lattice and the 2-dimensional hexagonal lattice from Examples 1.7 and 1.3 are integral.

We now generalise the way we calculated the density of the 2-dimensional hexagonal sphere packing so we can apply it to the 3-dimensional fcc packing and all other lattice packings. To do this, we will first have to define some properties of lattices.

Definition 1.10. Let $B = \{b_1, \ldots, b_n\}$ be a basis of a lattice L. The matrix M with b_i as the i-th row is called a generator matrix of L.

Remark 1.10.1. It is easy to see that $L = \{vB : v \in \mathbb{Z}^n\}$.

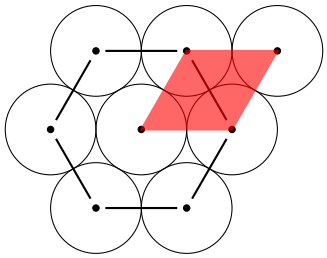
Definition 1.11. Let $B = \{b_1, \ldots, b_n\}$ be a basis of a lattice L. The region consisting of the points

$$\theta_1 b_1 + \ldots + \theta_n b_n \text{ with } 0 \leq \theta_i < 1$$

is called the fundamental region of L given the basis B.

We look at an example of a fundamental region.

Example 1.12. If we pick the basis $\{(2, 0), (1, \sqrt{3})\}$ for the A_2 lattice of the 2-dimensional hexagonal packing, we get the following fundamental region.



We can see that in this case, copies of the fundamental regions can form a tiling, or in higher dimensions a tessellation, of the space $\mathbb{R}^n$ in the following way. Let L be a lattice with some basis B and F its fundamental domain, then the sets of the form

$$u + F = \{u + f : f \in F\}$$

for $u \in L$ are disjoint and cover $\mathbb{R}^n$. We can see that the parts of the spheres within one copy of the fundamental region form exactly one sphere together. It turns out that this is always the case.

Lemma 1.13. *Let L be a lattice. The density of the corresponding lattice packing is*

$$\Delta = \frac{\mathrm{Vol}(\textit{one sphere in the sphere packing})}{\mathrm{Vol}(\textit{fundamental region of } L)}$$

Proof Sketch. There is one sphere per lattice point and the tessellation of $\mathbb{R}^n$ is formed by translating the fundamental region by lattice vectors, so there is also one fundamental region per lattice point. The equality then easily follows from the fact that the copies of the fundamental domain, including the partial spheres within them, are identical. □

Now we just need to calculate the volume of a sphere and the volume of a fundamental region. The first one is easy. If V_n is the volume of the n-dimensional unit sphere and ρ is the radius of the spheres in the sphere packings we get $\mathrm{Vol}(\text{one sphere}) = V_n\rho^n$. The second one follows from the following lemma.

Lemma 1.14. *Let L be a lattice with basis B and corresponding generator matrix M and fundamental region F. We then have*

$$\mathrm{Vol}(F) = |\det M|$$

Proof. This is a well-known fact from linear algebra, see for example [Fis02]. □

Remark 1.14.1. It is easy to prove that $\mathrm{Vol}(F)$ and $|\det M|$ are both independent of the choice of a basis of L.

Our formula for the density of a lattice packing L with generator matrix M and spheres of radius ρ now becomes

$$\Delta(L) = \frac{V_n\rho^n}{|\det M|}$$

This formula simplifies even further if $|\det M| = 1$.

Definition 1.15. An integral lattice is called *unimodular* if its generator matrix has determinant ± 1. Its density is then $\Delta = V_n\rho^n$.

One obstacle to comparing the densities of lattice packings in different dimensions is the fact that V_n decreases rapidly for increasing n. To compensate for this effect, we also define an alternative density.

Definition 1.16. The *center density* δ of an n-dimensional sphere packing is defined as

$$\delta = \frac{\Delta}{V_n}$$

Remark 1.16.1. For a lattice packing L with generator matrix M and sphere of radius ρ we get

$$\delta(L) = \frac{\rho^n}{|\det M|}$$

We can now use these formulas to calculate the densities of the 3-dimensional fcc lattice packing.

Theorem 1.17. *The 3-dimensional fcc lattice packing has densities*

$$\Delta = \frac{\pi}{3\sqrt{2}} \quad \textit{and} \quad \delta = \frac{1}{4}\sqrt{2}$$

Proof. A basis of the fcc lattice is given by $\{(1,1,0),(1,0,1),(1,0,1)\}$ and the corresponding generator matrix has determinant 2. The smallest distance between two lattice points is $\sqrt{2}$, so the fcc lattice packing has spheres of radius $\frac{1}{2}\sqrt{2}$. The values of Δ and δ now follow from the formulas. □

Another related quantity of a lattice packing is its kissing number.

Definition 1.18. The *kissing number* of a lattice packing is the number of spheres that touch a given sphere.

Remark 1.18.1. A higher kissing number does not always result in a denser sphere packing. The problem of the highest kissing number in $\mathbb{R}^n$ is a different problem with a potentially different answer than the sphere packing problem.

1.1 Densest sphere packings

Now that we have defined the mathematical "machinery" for the sphere packing problem, we will discuss some of the advancements made in solving the sphere packing problem over the past few centuries and most notably the past 80 years. This section is purely meant as motivation for studying the Leech lattice and will not reappear in the later chapters.

A question that is relatively easier than finding the n-dimensional sphere packing with the highest density is to find the densest lattice packing because the lattice structure imposes many restrictions. The densest lattice packings for $n \leq 20$ (and some other values) have been found recently with some computer assistance, see [KEG10], [MT13] and [Kal13]. The densest overall sphere packings are however only known for $n \in \{1,2,3,8,24\}$. It is generally not true that the densest lattice packing is also the densest sphere packing since there are dimensions where a non-lattice packing is known to have a higher density than the densest lattice packing. The smallest known example is for $n = 10$, see [Slo02].

Much more is known nonetheless about lattice packings, so we will focus on them. We will look at some families of packings.

Example 1.19. The simplest lattice is obviously $\mathbb{Z}^n$ which is generated by the n vectors $(1,0,\ldots,0)$, $(0,1,\ldots,0),\ldots,(0,0,\ldots,1)$. We can calculate that this packing has center density $\delta = 2^{-n}$.

Example 1.20. A more efficient lattice is the checkerboard lattice D_n defined by

$$D_n = \{x \in \mathbb{Z}^n : x_1 + \ldots + x_n \equiv 0 \mod 2\}$$

It can be calculated that this lattice packing has center density $2^{-\frac{1}{2}(n+2)}$.

Remark 1.20.1. The fcc lattice from Example 1.7 is D_3.

The checkerboard lattices form the densest lattice packings for $n = 3, 4, 5$ and the hexagonal packing is the densest lattice packing for $n = 2$. This last fact was already proven by Lagrange in 1773 and in 1890, Axel Thue gave a non-rigorous proof that this packing is the densest 2-dimensional sphere packing among all packings, including the irregular ones. This last fact is often called Thue's Theorem although the first rigorous proof was published by the Hungarian mathematician László Fejes Tóth, see [FT42].

We now jump to the case $n = 3$. Johannes Kepler already conjectured in 1611 that D_3 is the densest 3-dimensional sphere packing which has been called Kepler's conjecture for this reason. It was proven in 1811 by Gauss that D_3 is the densest lattice packing but it took until very recently in 1998 to prove that D_3 is also the densest sphere packing among non-lattice packings when Thomas Hales announced a proof which was a proof by exhaustion, checking all potential counterexamples and dismissing all of them. This was done with computer assistance and was finally published in 2005, see [Hal05].

We now move on to a construction of lattice packings that produces most (but not all) of the densest known lattice packings. It follows a greedy strategy and is therefore defined recursively.

Definition 1.21. Let Λ_1 be the lattice $\mathbb{Z} \subset \mathbb{R}$. For $n \geq 2$, look at all the n-dimensional lattices L that contain a sublattice isomorphic to a lattice Λ_{n-1} such that $x \cdot x \geq 4$ for all $x \in L \setminus \{0\}$. We select the ones whose generator matrix has smallest determinant. Each selected lattice is a *laminated lattice* Λ_n.

Remark 1.21.1. As follows from the definition, n-dimensional laminated lattices are not unique but for certain values of n they are. More information on laminated lattices can be found in [CS82].

Remark 1.21.2. Λ_2 is the 2-dimensional hexagonal lattice, Λ_3 is the fcc lattice and Λ_{24} is the Leech lattice. These three are the unique laminated lattices (up to isomorphism) in their respective dimensions.

The densest known lattice packings in up to 24 dimensions and their properties are shown in Table 1 taken from [CSdlH98] where K_{11}, K_{12} and K_{13} are non-laminated lattices but are not important for our story. The most interesting of these are the cases $n = 8$ and $n = 24$ since it has been proven extremely recently in 2017 that the lattices $\Lambda_8 \cong E_8$ and Λ_{24} are the densest sphere packings, even among non-lattice packings. See [Via17] and [CKM$^+$17] for proofs.

In this thesis, we will construct Λ_{24}, calculate its densities and kissing number and study some of its relations with other important mathematical objects since Λ_{24} pops up in many other problems besides the sphere packing problem, see [CKM$^+$19]. We will not use the laminated lattice construction of Λ_{24} which is more useful for other purposes but construct the Leech lattice with the help of two linear codes, the hexacode and the Golay code. Afterwards, we will also study its symmetry group which will relate the Leech lattice to the Classification Theorem that is explored in Appendix B.

We will not prove that Λ_{24} is the densest 24-dimensional sphere or why the cases $n = 8$ and $n = 24$ are special since that makes use of a whole different area of mathematics, namely modular forms. The purpose of this thesis is to introduce the reader to the Leech lattice and gain some understanding of this truly fascinating object and its symmetries.

n	Packing	Δ	δ	Kissing number
1	$\Lambda_1 \cong \mathbb{Z}$	1	$\frac{1}{2}$	2
2	$\Lambda_2 \cong A_2$	0.90690	$\frac{1}{6}\sqrt{3}$	6
3	$\Lambda_3 \cong D_3$	0.74048	$\frac{1}{8}\sqrt{2}$	12
4	$\Lambda_4 \cong D_4$	0.61685	$\frac{1}{8}$	24
5	$\Lambda_5 \cong D_5$	0.46526	$\frac{1}{16}\sqrt{2}$	40
6	Λ_6	0.37295	$\frac{1}{24}\sqrt{3}$	72
7	Λ_7	0.29530	$\frac{1}{16}$	126
8	Λ_8	0.25367	$\frac{1}{16}$	240
9	Λ_9	0.14577	$\frac{1}{32}\sqrt{2}$	272
10	Λ_{10}	0.09202	$\frac{1}{48}\sqrt{3}$	336
11	K_{11}	0.06043	$\frac{1}{54}\sqrt{3}$	432
12	K_{12}	0.04945	$\frac{1}{27}$	756
13	K_{13}	0.02921	$\frac{1}{54}\sqrt{3}$	918
14	Λ_{14}	0.02162	$\frac{1}{48}\sqrt{3}$	1422
15	Λ_{15}	0.01686	$\frac{1}{32}\sqrt{2}$	2340
16	Λ_{16}	0.01471	$\frac{1}{16}$	4320
17	Λ_{17}	0.008811	$\frac{1}{16}$	5346
18	Λ_{18}	0.005928	$\frac{1}{24}\sqrt{3}$	7398
19	Λ_{19}	0.004121	$\frac{1}{16}\sqrt{2}$	10668
20	Λ_{20}	0.003226	$\frac{1}{8}$	17400
21	Λ_{21}	0.002466	$\frac{1}{8}\sqrt{2}$	27720
22	Λ_{22}	0.002128	$\frac{1}{6}\sqrt{3}$	49896
23	Λ_{23}	0.001905	$\frac{1}{2}$	93150
24	Λ_{24}	0.001930	1	196560

Table 1: Densities of densest known lattice packings

2 The hexacode $\mathcal{H}_6$

The hexacode is the first object needed to eventually construct the Leech lattice, which produces the densest 24-dimensional sphere packing. The knowledge gained through examining the hexacode will be fundamental for our later exploration of the Leech lattice and its symmetries. We mostly follow Chapter 3 in [CSdlH98].

2.1 Linear codes

The hexacode and the next crucial object, the binary Golay code which will be the center of attention in Chapter 3, are both examples of linear codes, so some relevant definitions and observations on general linear codes will be discussed first to make our exploration of these two codes more straightforward. We will also show how linear codes are related to sphere packings.

However, the reason linear codes were studied in the first place had nothing to do with sphere packings. Another seemingly unrelated practical problem was the motivation for linear codes, namely transmitting messages. Most digital systems use zeroes and ones to pass on information but what happens if one of these numbers gets corrupted? The intended message also gets corrupted. In most circumstances, corruptions are common, so a solution must be found to reliably transmit data. The solution to this is coding theory. Longer segments consisting of multiple digits are used to represent a single digit so that if a corruption happens, the original segment can be recovered. We now define this rigorously.

Definition 2.1. A *q-ary linear code of length n* is a linear subspace $C \subset \mathbb{F}_q^n$ where q is a prime power and n is a positive integer. A *word* is an element of $\mathbb{F}_q^n$ and a *codeword* is an element of C. The *dimension* of the code is the dimension of C as a linear subspace of $\mathbb{F}_q^n$.

Remark 2.1.1. Words are notated in the following way, $u = u_1u_2\dots u_n$ where $u_1, u_2, \dots, u_n$ are the coordinates of $u \in \mathbb{F}_q^n$.

The codewords are exactly the segments that are transmitted. Let us look at an example to understand this abstract definition.

Example 2.2. Recall that $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \omega, \overline{\omega}\}$ where $\omega + \overline{\omega} = 1 = \omega \cdot \overline{\omega}$. We look at the code $E \subset \mathbb{F}_4^6$ of length 6 generated by the words 11 11 00 and 00 11 11. For convenience reasons that will become apparent later, the 6 coordinates of a word in $\mathbb{F}_4^6$ are separated into three pairs of two. This is clearly a 2-dimensional code, so there are exactly $4^2 = 16$ codewords. We can write them all down:

00 00 00	11 11 00	00 11 11	11 00 11	$11\,\overline{\omega\omega}\,\omega\omega$	$\omega\omega\,\overline{\omega\omega}\,11$
	$\omega\omega\,\omega\omega\,00$	$00\,\omega\omega\,\omega\omega$	$\omega\omega\,00\,\omega\omega$	$\omega\omega\,11\,\overline{\omega\omega}$	$\overline{\omega\omega}\,11\,\omega\omega$
	$\overline{\omega\omega}\,\overline{\omega\omega}\,00$	$00\,\overline{\omega\omega}\,\overline{\omega\omega}$	$\overline{\omega\omega}\,00\,\overline{\omega\omega}$	$\overline{\omega\omega}\,\omega\omega\,11$	$11\,\omega\omega\,\overline{\omega\omega}$

If one of these codewords is corrupted in one position, we can still uniquely determine the original codeword. For example 11 01 11 is corrected to 11 00 11. This way, the linear code E forms a 16 symbol alphabet that can be reliably transmitted.

There are also non-linear codes but the linear codes are the most regular and symmetric and have the nicest properties. In this regard, they are similar to lattice packings among the sphere packings. To further show the similarities between linear codes and lattice packings, we now also define a type of norm on $\mathbb{F}_q^n$ which will play the same role as the Euclidean norm on $\mathbb{R}^n$.

Definition 2.3. The *weight* $w(u)$ of a word u is

$$w(u) = |\{i : u_i \neq 0\}|$$

So the number of non-zero coordinates of u.

Definition 2.4. Let C be a code of length n and let $a_k = |\{u \in C : w(u) = k\}|$ be the number of codewords with weight k. Then the *weight distribution* of C is the expression

$$0^{a_0}\ 1^{a_1}\ \dots\ n^{a_n}$$

where all the terms k^{a_k} with $a_k = 0$ are removed.

We look at what these definitions mean for our code E from Example 2.2.

Example 2.5. The code E from Example 2.2 has six words of weight 6, nine words of weight 4 and one word of weight 0, so the weight distribution of E is $0^1\ 4^9\ 6^6$.

Like the Euclidean norm, the weight also imposes a distance function and this allows us to formalise a correspondence between linear codes and sphere packings.

Definition 2.6. The *Hamming distance* $h(u, v)$ between two words u and v is

$$w(u - v) = |\{i : u_i \neq v_i\}|$$

. So the number of positions where the coordinates of u and v differ.

Definition 2.7. The *minimal distance* of a code C is

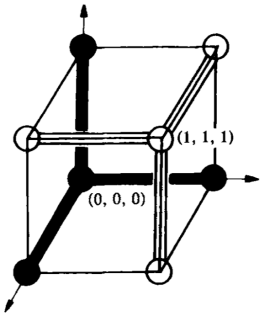
$$d = \min\{h(u, v) : u, v \in C, u \neq v\}$$

Remark 2.7.1. The minimal distance of a linear code is also the minimal weight of a non-zero codeword since $h(u, v) = h(u - v, 0) = w(u - v)$.

Remark 2.7.2. Let $C \subset \mathbb{F}_q^n$ be a code with minimal distance $d > 2r$ for some $r \in \mathbb{Z}_{>0}$, then the 'Hamming spheres' of radius r around the codewords, so the sets $\{v \in \mathbb{F}_q^n : h(u, v) \leq r\}$ for $u \in C$, are disjoint and form an $\mathbb{F}_q$-equivalent of an n-dimensional sphere packing.

Remark 2.7.3. The minimal distance of the code E in example 2.2 is 4 since the minimal non-zero weight is 4. This means that we can form a 6-dimensional Hamming sphere packing in $\mathbb{F}_4^6$ with spheres of radius 1.

We can visualize this type of sphere packing with the following figure taken from [Tho83] that uses the linear code $\{000, 111\} \subset \mathbb{F}_2^3$. The codewords are the centers of the two spheres and the points in the Hamming spheres are the words that will be interpreted as the codeword in the center, so the points with the same colour in the figure. In this case, the minimal distance is $d = 1$, so a single error can be corrected.



We now take a look again at the practical applications of linear codes. One particular instance where the chance of corruption is high and linear codes are therefore useful is outer space. The Golay code which we will cover later is especially interesting in this regard since it was used by NASA for the two Voyager probes launched in 1977 to transmit images that these probes took. These include hundreds of pictures of Jupiter, Saturn, Uranus and Neptune, see [Cur16]. This shows that the Golay code is not just used in the construction of the Leech lattice but is a highly interesting object on its own. That is one of the most exciting aspects of this subject, the fact that different areas of mathematics are combined to obtain the highly unusual and fascinating Leech lattice.

Aside from Remark 2.7.2, there are even more ways we can build sphere packings from codes. We give two constructions from [CSdlH98] to create a sphere packing in $\mathbb{R}^n$ that are relevant for our study of the Leech lattice.

Definition 2.8. Let C be a binary length n linear code with M codewords and a minimal distance d. Then the set

$$A(C) = \{x \in \mathbb{Z}^n : x \equiv c \mod 2 \text{ for some } c \in C\}$$

is a lattice and forms a lattice packing. The radius of the spheres in this packing is $\rho = \frac{1}{2}\min(2, \sqrt{d})$ and the center density is $\delta = M\rho^n 2^{-n}$

Remark 2.8.1. Let C be the binary linear code $\{000, 110, 101, 011\}$ of length 3 then the fcc lattice, defined in Example 1.7, is $A(C)$.

We can adjust this construction to obtain a lattice packing that is often denser. Applying this new construction to the Golay code $\mathcal{G}_{24}$ gives a sublattice of the Leech lattice Λ_{24} with index 2 as we will see in section 4.1.

Definition 2.9. Let C be a binary length n linear code with M codewords and a minimal distance d. Then the set

$$B(C) = \left\{ x \in \mathbb{Z}^n : x \equiv c \mod 2 \text{ for some } c \in C \text{ and } \sum_{i=1}^{n} x_i \equiv 0 \mod 4 \right\}$$

is a lattice and forms a lattice packing. The radius of the spheres in this packing is $\rho = \frac{1}{2}\min(\sqrt{8}, \sqrt{d})$ and the center density is $\delta = M\rho^n 2^{-n-1}$

Remark 2.9.1. If $d > 4$, $B(C)$ is denser than $A(C)$ for n large enough.

Both of these constructions can also be applied to non-linear codes to obtain non-lattice packings. The 10-dimensional sphere packing, mentioned in section 1.1, that is denser than all the 10-dimensional lattice packings can be constructed by applying construction A on a non-linear code.

We now move on to another aspect of linear codes. As we mentioned in the introduction, one of the fascinating properties of the Leech lattice and also the Golay code is that they are exceptionally symmetric and this is the key property we are going to study in this thesis by examining the groups of symmetries of these objects. Therefore, we will first cover the symmetries of a general linear code which are called *automorphisms*.

Definition 2.10. A *monomial transformation* is an $\mathbb{F}_q$-linear map $\mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by

$$(u_1, u_2, \ldots, u_n) \mapsto (c_1 u_{\sigma(1)}, c_2 u_{\sigma(2)}, \ldots, c_n u_{\sigma(n)})$$

where $c_i \in \mathbb{F}_q^*$ and $\sigma \in S_{24}$. In other words, we perform a permutation σ^{-1} on the coordinates and coordinate-wise multiplications with (possibly different) non-zero scalars $c_1, \ldots, c_n$.

Remark 2.10.1. If we consider the associated matrices of monomial transformations w.r.t. the standard basis of $\mathbb{F}_q^n$, then the monomial transformations correspond exactly to the $n \times n$-matrices over $\mathbb{F}_q$ whose rows and columns each contain exactly one non-zero entry.

Definition 2.11. An *automorphism* of a code C is a monomial transformation that preserves C. The automorphisms of a code form a group $\mathrm{Aut}(C)$ under composition.

We look at an example again to get a better understanding of these definitions.

Example 2.12. We once again look at the code E from Example 2.2. Some trivial automorphisms are the scalar multiplications with 1, ω or $\overline{\omega}$ which together generate a subgroup isomorphic to C_3.

Recall that we write down the six coordinates of a word in $\mathbb{F}_4^6$ in three pairs of two coordinates. A family of more exciting automorphisms are then the permutations of these three pairs which can be checked to preserve E and generate a subgroup isomorphic to S_3 together. If we number the coordinate

positions then this S_3 is exactly generated by the permutations (135)(246) and (13)(24).

One last type of automorphism we want to highlight is the transposition of any two coordinates within the same pair, so the permutations (12), (34) and (56) on the coordinates. They generate a subgroup isomorphic to $C_2 \times C_2 \times C_2$ together.

We can look at the associated matrices of two automorphisms of the latter types:

$$\begin{pmatrix} 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{pmatrix}$$

The images of a word u under these automorphisms are $u_3u_4\,u_5u_6\,u_1u_2$ and $u_2u_1\,u_3u_4\,u_6u_5$ respectively.

Aside from the automorphisms, there are many more maps from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$ that preserve a code since the definition of a monomial transformation is quite restrictive. Most of these maps are not important for our purposes but we will have to look at one broader type of code-preserving map which includes the automorphisms.

Definition 2.13. A *semi-automorphism* of a code $C \subset \mathbb{F}_q^n$ is a monomial transformation combined with a field automorphism of $\mathbb{F}_q$, applied on all n coordinates, that preserves C. The semi-automorphisms of a code form a group $\mathrm{Aut}^*(C)$ under composition.

Example 2.14. We look at the code $E \subset \mathbb{F}_4^6$ from example 2.2 again. The only field automorphisms of $\mathbb{F}_4$ are the identity and the conjugation map $^- : \mathbb{F}_4 \mapsto \mathbb{F}_4$, so the map that sends ω to $\overline{\omega}$ and vice versa but preserves 0 and 1. Since E is generated by 00 11 11 and 11 11 00, it is clear that conjugation preserves E, so the semi-automorphisms in this case are just the usual automorphisms and the usual automorphisms composed with conjugation.

2.2 The hexacode

Now that we have looked at linear codes and have a good understanding of them, we can define our object of interest, the hexacode. We mostly follow sections 11.1-11.4 in [CSdlH98] and section 5.2.1 in [Wil09]. Like the linear code E in the examples of the previous section, the hexacode is a code in $\mathbb{F}_4^6$. We keep the convention of writing down the six coordinates in three pairs of two. We give two definitions of the hexacode.

Definition 2.15. The hexacode $\mathcal{H}_6 \subset \mathbb{F}_4^6$ is the linear code generated by the words

$$\omega\overline{\omega}\,\omega\overline{\omega}\,\omega\overline{\omega}, \quad \omega\overline{\omega}\,\overline{\omega}\omega\,\overline{\omega}\omega, \quad \overline{\omega}\omega\,\omega\overline{\omega}\,\overline{\omega}\omega \quad \text{and} \quad \overline{\omega}\omega\,\overline{\omega}\omega\,\omega\overline{\omega}$$

Remark 2.15.1. The generators are not linearly independent since every generator is the sum of the three others.

Definition 2.16. Let $\phi_{a,b,c}$ be the polynomial $aX^2 + bX + c \in \mathbb{F}_4[X]$. The hexacode $\mathcal{H}_6 \subset \mathbb{F}_4^6$ consists exactly of the words $ab\,cd\,ef$ such that

$$c = \phi_{a,b,c}(0), \quad d = \phi_{a,b,c}(1), \quad e = \phi_{a,b,c}(\omega) \quad \text{and} \quad f = \phi_{a,b,c}(\overline{\omega})$$

Remark 2.16.1. It follows easily from this definition that 11 11 00 and 00 11 11 are elements of $\mathcal{H}_6$, so the code E from Example 2.2 is contained in $\mathcal{H}_6$.

These two definitions are both more useful than the other in some cases, so we would like to use both characterisations of the hexacode.

Lemma 2.17. *Definitions 2.15 and 2.16 are equivalent.*

Proof. Let A be the hexacode defined by the first definition and B the one by the second. Since $\mathbb{F}_4$ has characteristic 2 we get the identity $(x+y)^2 = x^2 + y^2$. For $u, v \in B$ it then follows easily from Definition 2.16 that also $u + v \in B$. Furthermore, it follows easily from this definition that B is closed under scalar multiplication, so B is linear. It can also be checked with the definition that the generators of A are contained in B, so it follows that $A \subset B$.

Note that $\dim(B) = 3$ since any first 3 coordinates determine a unique codeword. Taking three out of the four generators of A gives a basis of A, so also $\dim(A) = 3$ and it follows that $A = B$. □

An immediate consequence of Lemma 2.17 is the size of $\mathcal{H}_6$.

Corollary 2.18. $\mathcal{H}_6$ *contains 64 codewords.*

Proof. We saw that $\mathcal{H}_6 \subset \mathbb{F}_4^6$ has dimension 3, so $|\mathcal{H}_6| = 4^3 = 64$. □

Now that we have proven that these two definitions are equivalent, we can use them both for different purposes. The main purpose of the first definition is to verify whether a given automorphism does indeed preserve $\mathcal{H}_6$ by looking at the images of the generators in Definition 2.15. The second definition can be used to check whether a given word is an element of $\mathcal{H}_6$.

Our ultimate goal is to describe the symmetries of the Leech lattice for which the hexacode is a stepping stone, so we are also interested in the symmetries of the hexacode. Understanding these will help us understand the symmetries of the Golay code and in turn, the symmetries of the Leech lattice. Therefore, we will first look at some easily spottable automorphisms of $\mathcal{H}_6$ which are very similar to the automorphisms in Example 2.12.

Lemma 2.19. *Recall that the six coordinates of a word are written down in three pairs of two. The following maps are then contained in* $\mathrm{Aut}(\mathcal{H}_6)$.

- *Scalar multiplication of the whole word with* $1, \omega$ *or* $\overline{\omega}$.
- *Any permutation of the three pairs. So* $(135)(246)$, $(13)(24)$ *etc.*

- *The composition of exactly two transpositions that each switch two coordinates within a pair. We call these a double flip, so* $(12)(34)$ *etc.*

Proof. Check that the images of the generators of $\mathcal{H}_6$ in Definition 2.15 under each automorphism are elements of $\mathcal{H}_6$. □

Example 2.20. The images of the hexacodeword $01\,01\,\omega\overline{\omega}$ under some of these automorphisms are:

Automorphism	Image of $01\,01\,\omega\overline{\omega}$
$u \mapsto (\omega u_1, \omega u_2, \omega u_3, \omega u_4, \omega u_5, \omega u_6)$	$0\omega\,0\omega\,\overline{\omega}1$
$u \mapsto u_3u_4\,u_5u_6\,u_1u_2$	$01\,\omega\overline{\omega}\,01$
$u \mapsto u_2u_1\,u_3u_4\,u_6u_5$	$10\,01\,\overline{\omega}\omega$

Before we look at the other automorphisms in $\mathrm{Aut}(\mathcal{H}_6)$, we will look more closely at the automorphisms we have already seen.

Definition 2.21. $G \subset \mathrm{Aut}(\mathcal{H}_6)$ is the subgroup generated by the automorphisms in Lemma 2.19.

Lemma 2.22. *G is isomorphic to $C_3 \times S_4$.*

Proof. Let N be the subgroup of G generated by the double flips, H the subgroup generated by the permutations of the three pairs and G' the subgroup generated by both of these types of elements. It is easy to check that $N \triangleleft G'$ is a normal subgroup and that the intersection $H \cap N$ is trivial. It follows that G' is an inner semidirect product of H acting on N.

Furthermore, we have that $N \cong V_4$ and $H \cong S_3$ and the action of H on N corresponds to the action of S_3 on V_4 in Example A.9. So we get

$$G' = N \rtimes H \cong V_4 \rtimes S_3 \cong S_4$$

Now let M be the subgroup of G containing the scalar multiplications. We then easily see that $M \triangleleft G$ is a normal subgroup, $M \cong C_3$ and the intersection $M \cap G'$ is trivial. We therefore get that G is a semidirect product of G' acting on M but since M commutes with G' this is just the direct product. So we get

$$G \cong M \times G' \cong C_3 \times S_4$$

□

Since $\mathrm{Aut}(\mathcal{H}_6)$ acts on $\mathcal{H}_6$ in an obvious way we can also look at the action of the subgroup G on $\mathcal{H}_6$.

Lemma 2.23. *The orbits under the action of G on $\mathcal{H}_6$ are as follows:*

Representing element	*Orbit Length*
$01\,01\,\omega\overline{\omega}$	*36*
$\omega\overline{\omega}\,\omega\overline{\omega}\,\omega\overline{\omega}$	*12*
$00\,11\,11$	*9*
$11\,\omega\omega\,\overline{\omega}\overline{\omega}$	*6*
$00\,00\,00$	*1*

Proof. It is clear that the representing elements are elements in different orbits since elements in the same orbit must have the same weight because of the definition of G and it follows from inspection that $00\,11\,11$ and $01\,01\,\omega\overline{\omega}$, and $\omega\overline{\omega}\,\omega\overline{\omega}\,\omega\overline{\omega}$ and $11\,\omega\omega\,\overline{\omega}\overline{\omega}$, are in different orbits.

The orbit lengths can be determined by either writing down all the elements in the orbit or using the orbit-stabiliser theorem, see Lemma B.10, combined with the fact that

$$|G| = |C_3 \times S_4| = |C_3| \times |S_4| = 3 \cdot 4! = 72$$

The lengths of the shown orbits add up to $64 = |\mathcal{H}_6|$, so these are all the orbits. □

Remark 2.23.1. The last three orbits form exactly the code E from Example 2.2.

Remark 2.23.2. We will see this kind of proof a few more times where we count some objects and then find out by adding the numbers that we have counted all the objects.

From the information gained through studying the automorphisms in G, we can also deduce the following fact about the code $\mathcal{H}_6$.

Corollary 2.24. *The weight distribution of* $\mathcal{H}_6$ *is* $0^1\,4^{45}\,6^{18}$.

Proof. Words in the same orbit have the same weight, so this follows directly from Lemma 2.23. □

We now start looking at the other automorphisms of the hexacode. One of them is the linear map $s : \mathbb{F}_4^6 \to \mathbb{F}_4^6$ defined by

$$u \mapsto (\omega u_1, \overline{\omega} u_2, u_3, u_6, u_4, u_5) \tag{1}$$

which indeed preserves $\mathcal{H}_6$. Adjoining this element to G is enough to obtain the whole automorphism group of $\mathcal{H}_6$. The notation used for extensions in the following Theorem can be found in Definition A.6.

Theorem 2.25. $\mathrm{Aut}(\mathcal{H}_6) = \langle s, G\rangle \cong 3 \cdot A_6$

Proof. We will construct a short exact sequence

$$1 \longrightarrow C_3 \xrightarrow{\ f\ } \langle s, G\rangle \xrightarrow{\ g\ } A_6 \longrightarrow 1$$

Let $C_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$. For $f : C_3 \to \langle s, G\rangle$, we take the map that sends x to the scalar multiplication with ω^x. This is clearly an element of G and it can be easily seen that f is an injective group homomorphism.

For the homomorphism g, we will have to do some more work. Let X be the set of axes of $\mathbb{F}_4^6$ and number them from 1 to 6 in the natural way, so for example

$$x_1 = \{00\,00\,00, 10\,00\,00, \omega 0\,00\,00, \overline{\omega} 0\,00\,00\}$$

From the definition of an automorphism, it follows that $\langle s, G\rangle$ acts on the axes in a well-defined manner. This induces a group homomorphism $\langle s, G\rangle \to S_6$. We look at the images of s and the generators of G in Lemma 2.19 under this homomorphism. We use cycle notation for the elements of A_6.

Automorphism(s)	Image(s)
s	(456)
scalar multiplications	identity map
permutations of the three pairs	(13)(24), (15)(26), (35)(36), (135)(246), (153)(264)
double flips	(12)(34), (12)(56), (34)(56)

We see that all the images are even and it can be manually verified that they generate A_6, so it follows that this group homomorphism can be restricted to a group homomorphism $\langle s, G\rangle \to A_6$, we take this homomorphism for g.

Lastly, we have to check that $\mathrm{Im}(f) = \ker(g)$. We know that $\ker(g)$ consists of the automorphisms that fix all the axes, in other words, the automorphisms that only consist of coordinate-wise scalar multiplication and do not permute the coordinates. Let

$$h : \mathbb{F}_4^6 \to \mathbb{F}_4^6, \quad u \mapsto (c_1u_1, c_2u_2, c_3u_3, c_4u_4, c_5u_5, c_6u_6)$$

be contained in $\ker(g)$. It must then be an automorphism of $\mathcal{H}_6$ so

$$h(00\,11\,11) = 00\,c_3c_4\,c_5c_6 \quad \text{and} \quad h(11\,11\,00) = c_1c_2\,c_3c_4\,00$$

must be hexacodewords. It follows from Lemma 2.23 that this can only be the case if $c_1 = c_2 = \ldots = c_6$, so if h is a scalar multiplication. We already know that $\mathrm{Im}(f)$ consists of the scalar multiplications, so it indeed follows that $\mathrm{Im}(f) = \ker(g)$ and we have constructed the desired short exact sequence.

We conclude that $\langle s, G\rangle$ is an extension of A_6 by C_3 and it can be shown that this extension is non-split, so $\langle s, G\rangle \cong 3\cdot A_6$. The same exact reasoning applies to a short exact sequence where we replace $\langle s, G\rangle$ with $\mathrm{Aut}(\mathcal{H}_6)$, so

$$1 \longrightarrow C_3 \xrightarrow{f} \mathrm{Aut}(\mathcal{H}_6) \xrightarrow{g} A_6 \longrightarrow 1$$

We therefore also get $\mathrm{Aut}(\mathcal{H}_6) \cong 3\cdot A_6$. Since all these groups are finite and we have $\langle s, G\rangle \subset \mathrm{Aut}(\mathcal{H}_6)$, it follows that $\mathrm{Aut}(\mathcal{H}_6) = \langle s, G\rangle \cong 3\cdot A_6$. □

Now that we have described $\mathrm{Aut}(\mathcal{H}_6)$ we can look at the semi-automorphisms of $\mathcal{H}_6$. One of them is the map $t : \mathbb{F}_4^6 \to \mathbb{F}_4^6$ defined by

$$u \mapsto (\overline{u_1}, \overline{u_2}, \overline{u_3}, \overline{u_4}, \overline{u_6}, \overline{u_5}) \tag{2}$$

Analogously to the proof of Theorem 2.25, the following statement can be proven.

Theorem 2.26. $\mathrm{Aut}^*(\mathcal{H}_6) = \langle \mathrm{Aut}(\mathcal{H}_6), t\rangle \cong 3\cdot S_6$.

Proof. Construct similar short exact sequences which lead to isomorphisms $\langle \mathrm{Aut}(\mathcal{H}_6), t\rangle \cong 3\cdot S_6$ and $\mathrm{Aut}^*(\mathcal{H}_6) \cong 3\cdot S_6$. Since these groups are finite and $\langle \mathrm{Aut}(\mathcal{H}_6), t\rangle \subset \mathrm{Aut}^*(\mathcal{H}_6)$, the theorem follows. □

3 The binary Golay code $\mathcal{G}_{24}$

Now that we have covered the hexacode and its symmetries we can take the next step and use it to define the Golay code which is a binary code of length 24, so $\mathcal{G}_{24} \subset \mathbb{F}_2^{24}$, and study its symmetries. We mostly follow section 11.5 in [CSdlH98] and section 5.2 in [Wil09] where we fill in some of the details that were left out. First however, we have to introduce some notation that we will use extensively throughout the next chapters.

3.1 Miracle Octad Generator

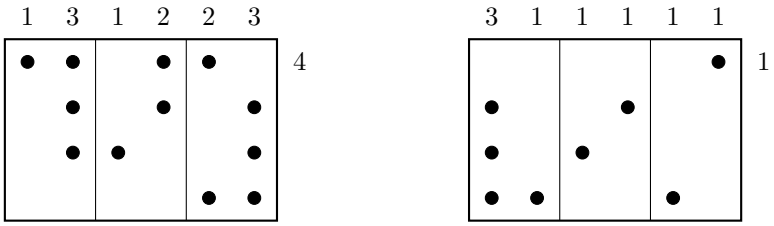
This notation is the *Miracle Octad Generator (MOG)* which was first introduced in 1976 by R.T. Curtis, see [Cur76], as a mathematical tool to write down codewords in the Golay code $\mathcal{G}_{24}$, automorphisms in the Mathieu group M_{24}, vectors in the Leech lattice Λ_{24} and even more. The advantage of the MOG is that it is not just a way to write these down but also makes claims easier to state and verify. $\mathcal{G}_{24}, M_{24}$ and Λ_{24} are the next three main objects of our study, so understanding the MOG is crucial for our goals and we will, therefore, explain the MOG step-by-step.

Firstly, the 24 coordinates of a word in $\mathbb{F}_2^{24}$ are restructured into a 4×6-matrix. The first coordinate corresponds to the leftmost entry of the top row and the direction taken is first from top to bottom within the columns and then from left to right between the columns. Zero-coordinates are indicated by empty matrix entries while one-coordinates are indicated by a dot as the corresponding matrix entry. This way, we get for example the following unfinished MOGs for two words in $\mathbb{F}_2^{24}$.

Example 3.1.

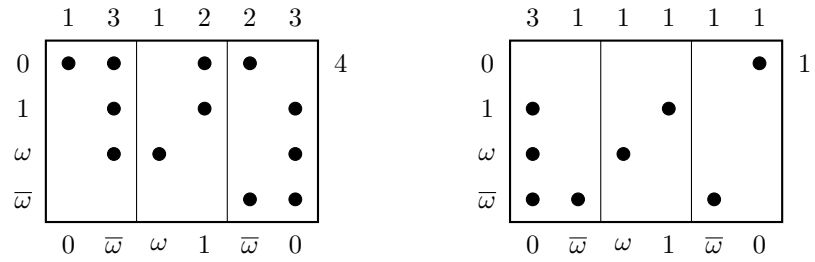
Next, we write down the weights of the six columns on top of the columns and write down the weight of the top row to the right of that row. Similar to the six coordinates in a hexacodeword, we also separate the 6 columns into three pairs of two. For our examples, we then get the following.

Example 3.2.

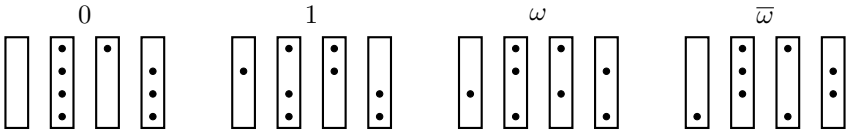


Next, we assign the elements of $\mathbb{F}_4$ as labels to the 4 rows of the MOG. Starting with the top row, the labels are successively $0,\ 1,\ \omega$ and $\overline{\omega}$. Lastly, the *score* of a column is the sum of the row labels of the dots (one-coordinates) in that column. The scores are written down below their corresponding columns. For our examples, we get the following.

Example 3.3.



Remark 3.3.1. Notice that the two example words have the same exact scores. This is possible since different columns can have the same score. The scores of all $2^4 = 16$ columns are as follows.



Every score is obtained by 4 columns, two with even weight and two with odd weight. From now on, we will say that a column is odd (resp. even) if it has odd (resp. even) weight.

3.2 The Golay code

Now that the reader has hopefully understood the rules and conventions of the MOG, we can use it to construct the Golay code which was first discovered in 1949 by the Swiss mathematician Marcel Golay, see [Gol49]. There are many other constructions of the Golay code but the one using the MOG and the hexacode is the most insightful for our purposes, namely studying the symmetries.

Definition 3.4. The *Golay code* $\mathcal{G}_{24} \subset \mathbb{F}_2^{24}$ consists of the length 24 binary words for which the following holds in MOG-notation:

- The weights of the columns and the first row have the same parity mod 2.
- Concatenating the scores, in the natural way, gives a hexacodeword.

We call a Golay codeword odd (resp. even) if the columns are odd (resp. even).

Remark 3.4.1. Scores and weights of the columns and the first row mod 2 are additive. Since $\mathcal{H}_6$ is a linear code, it follows from the definition that $\mathcal{G}_{24}$ is also indeed a linear code.

Because of the MOG-structure, we can interpret every length 24 words as a concatenation of six length 4 words, namely the columns. We can therefore define the following.

Definition 3.5. Let u be a Golay codeword and let a_k be the number of columns in the MOG with weight k. Then the *column distribution* of u is the expression

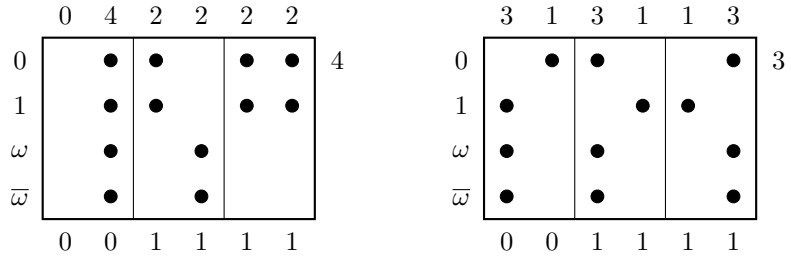
$$0^{a_0}\ 1^{a_1}\ 2^{a_2}\ 3^{a_3}\ 4^{a_4}$$

where the terms k^{a_k} with $a_k = 0$ are removed.

We will look at some examples of Golay codewords and their column distributions.

Example 3.6. The left word in example 3.3 is not a Golay codeword since the weights of the columns and the first row do not all have the same parity mod 2. The weights in the right word are all odd and the scores form the word $0\overline{\omega}\,\omega 1\,\omega 0$ which can be checked to be in the hexacode. So the right word is a Golay codeword and has column distribution $3^1\ 1^5$.

Example 3.7. It is easy to construct a Golay codeword from the definition. Just pick a hexacodeword, for instance 00 11 11, and for each coordinate pick a corresponding column such that all columns have the same parity and the weight of the first row also has that parity. We can get, for example, the following even and odd Golay codeword with column distributions $4^1\ 2^4\ 0^1$ and $3^3\ 1^3$ this way.



We will now begin our exploration of the Golay code and its symmetries. First of all, we are interested in how many Golay codewords there are and how they can be characterised.

Lemma 3.8. *$\mathcal{G}_{24}$ is a 12-dimensional linear code with 4096 codewords.*

Proof. We count the number of Golay codewords with the same scores, in other words, that correspond to the same hexacodeword. Let an arbitrary hexacodeword be given and look at the corresponding even Golay codewords. There are exactly two even columns that correspond to each coordinate of this hexacodeword, so we can then create 2^6 even words in MOG-notation that have the desired scores.

Lastly, these have to satisfy the criterion that the first row has even weight. Notice that out of the two even columns per coordinate, one has a dot in the top row and one does not. Equivalently, one contributes 1 to the weight of the first row and one contributes 0. It follows that to form a Golay codeword, the last column is uniquely determined by the previous five, so we find 2^5 even Golay codewords.

Analogously, we find 2^5 odd Golay codewords. So we see that every hexacodeword has 2^6 corresponding Golay codewords and we know from Corollary 2.18 that $|\mathcal{H}_6| = 64$, so we get

$$|\mathcal{G}_{24}| = 64 \cdot 2^6 = 4096 = 2^{12} \text{ and } \dim(\mathcal{G}_{24}) = 12$$

□

Theorem 3.9. *The weight distribution of $\mathcal{G}_{24}$ is $0^1\ 8^{759}\ 12^{2576}\ 16^{759}\ 24^1$.*

Proof. We use $\mathbf{0}$ for the word consisting of 24 zeroes and $\mathbf{1}$ for the word consisting of 24 ones. It can be verified with the definition that $\mathbf{0}, \mathbf{1} \in \mathcal{G}_{24}$. There are no other words with weights 0 or 24, so the terms 0^1 and 24^1 in the weight distribution are correct.

Since $\mathcal{G}_{24}$ is linear and $\mathbf{1} \in \mathcal{G}_{24}$, we get that $u \in \mathcal{G}_{24}$ iff $\mathbf{1} - u \in \mathcal{G}_{24}$. Note that

$$w(\mathbf{1} - u) = 24 - w(u) \quad \text{and} \quad \mathbf{1} - u \neq u$$

So the number of words with weight k is equal to the number of words with weight $24 - k$. So if the term 8^{759} is correct, the term 16^{759} is also correct.

We now show that the terms 8^{759} and 12^{2576} are correct. Just like in lemma 3.8, we approach this by combinatorially constructing Golay codewords from their corresponding hexacodeword, but now we also pay attention to the weights of these Golay codewords.

We look at all the possible columns in Remark 3.3.1 and give each column a characteristic (x, y) where x is the weight of the column and y is the value of the entry in the top row. Note that the columns corresponding to $1, \omega$ and $\overline{\omega}$ have the same characteristics, namely $(1,0), (3,1), (2,1)$ and $(2,0)$ while the columns for 0 have characteristics $(0,0), (4,1), (1,1)$ and $(3,0)$. Also note that for a MOG-word corresponding to a hexacodeword, the weights of the columns and the first row determine its weight and whether it is a Golay codeword, so the characteristics give all the necessary information of the columns. This means that we can treat the coordinates 1, ω and $\overline{\omega}$ the same but not 0, so we have to classify the hexacodewords by their number of zeroes or equivalently their

number of non-zeroes which is their weight. It is now a classic combinatorial counting exercise to determine the number of even and odd Golay codewords of weights 8 and 12 that correspond to a hexacodeword with a certain weight. These numbers are:

Weight of the hexacodeword	even GCW of weight 8	odd GCW of weight 8	even GCW of weight 12	odd GCW of weight 12
0	15	6	0	20
4	8	6	16	20
6	0	6	32	20

We also know from Corollary 2.24 that the weight distribution of $\mathcal{H}_6$ is $0^1\,4^{45}\,6^{18}$. So we find

$$21 + 14 \cdot 45 + 6 \cdot 18 = 759 \quad \text{Golay codewords of weight 8}$$
$$20 + 36 \cdot 45 + 52 \cdot 18 = 2576 \quad \text{Golay codewords of weight 12}$$

We have now verified the terms 0^1, 8^{759}, 12^{2576}, 16^{759} and 24^1. These account for

$$1 + 759 + 2576 + 759 + 1 = 4096 = |\mathcal{G}_{24}| \quad \text{Golay codewords}$$

So there are no Golay codewords of weight other than 0, 8, 12, 16 or 24 and the weight distribution is indeed $0^1\,8^{759}\,12^{2576}\,16^{759}\,24^1$. □

Remark 3.9.1. The weights of all Golay codewords are divisible by 4 and the minimal weight and distance of $\mathcal{G}_{24}$ is 8.

We will encounter the 759 words with a minimal weight of 8 a few more times, so we give them a name and classify them.

Definition 3.10. An *octad* is a Golay codeword of weight 8.

Remark 3.10.1. It follows from the table in the proof of Theorem 3.9 that there are 384 odd octads and 375 even octads.

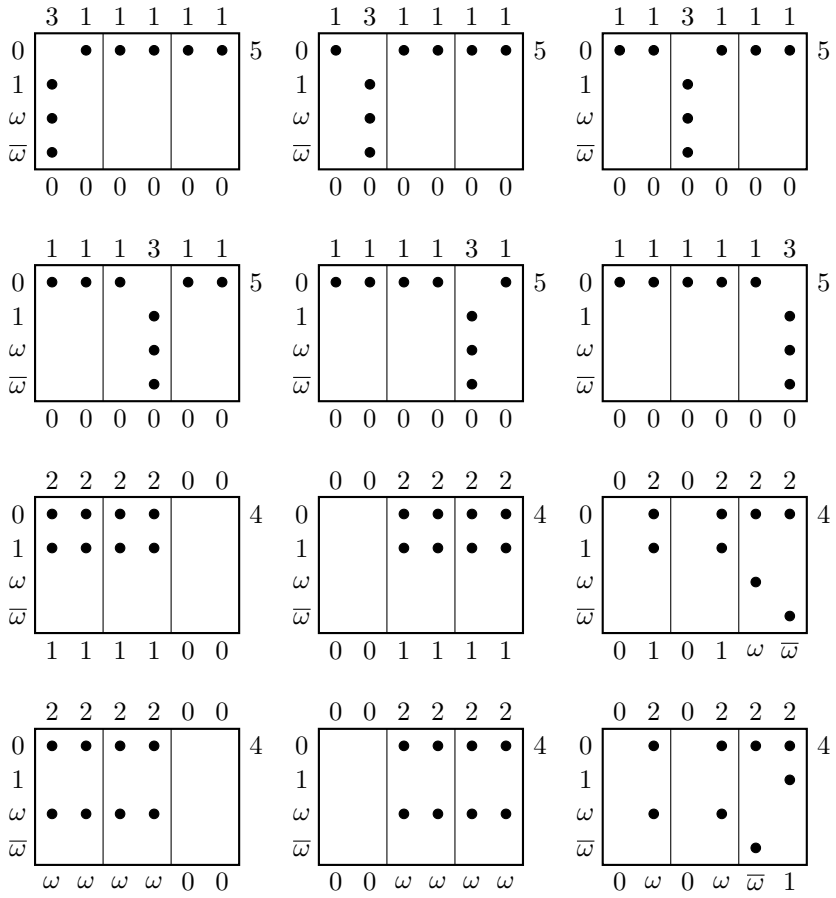
Corollary 3.11. *The 384 odd octads all have column distribution* $3^1\,1^5$. *Of the even octads, 15 have column distribution* $4^2\,0^4$ *and the other 360 have column distribution* $2^4\,0^2$

Proof. The odd octads can only consist of columns of weight 1 and 3, so for the whole MOG-word to have weight 8, the column distribution must necessarily be $3^1\,1^5$.

An even octad can only potentially have the column distributions $4^2\,0^4$, $4^1\,2^2\,0^3$ and $2^4\,0^2$. There are exactly $\binom{6}{2} = 15$ of the first type and these all correspond to the hexacodeword $00\,00\,00$. There are none of the second type since they would correspond to a hexacodeword with exactly 4 zeroes, so of weight 2 but we know from Corollary 2.24 that these do not exist. So we conclude that the remaining 360 even octads then have column distribution $2^4\,0^2$. □

We have already characterised the elements of $\mathcal{G}_{24}$ quite a bit and know almost as much about the Golay code as the hexacode. One last necessary piece of information before we move on to the automorphisms of the Golay code is a basis of $\mathcal{G}_{24}$.

Example 3.12. It can be easily verified that the following 12 elements, taken from [Gri98], form a basis of $\mathcal{G}_{24}$. The first 6 elements generate all the 2^6 Golay codewords whose scores form the hexacodeword 00 00 00 and the latter 6 elements make it so the Golay codewords corresponding to the other hexacodewords are also obtained.



Similarly to the generators of $\mathcal{H}_6$, this basis of $\mathcal{G}_{24}$ can be used to verify that the automorphisms we will use do indeed preserve $\mathcal{G}_{24}$. This is done by checking that the images of the basis elements are contained in $\mathcal{G}_{24}$.

3.3 The Mathieu group M_{24}

Now that we have a good understanding of $\mathcal{G}_{24}$ and what its codewords look like, we can start exploring the many symmetries of the Golay code.

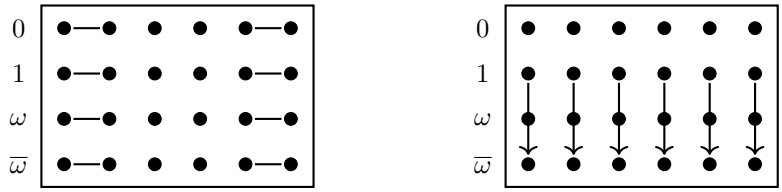
Definition 3.13. The *Mathieu group* M_{24} is the automorphism group $\mathrm{Aut}(\mathcal{G}_{24})$ of the Golay code.

Remark 3.13.1. Note that every monomial transformation of $\mathbb{F}_2^{24}$ is just a permutation of the coordinates since 1 is the only non-zero scalar in $\mathbb{F}_2$. We can therefore interpret M_{24} as a subgroup of S_{24} and because of the MOG-structure we will at times specifically interpret them as maps $\{1, 2, \ldots, 6\} \times \mathbb{F}_4 \to \{1, 2, \ldots, 6\} \times \mathbb{F}_4$.

Remark 3.13.2. Since there are no non-trivial field automorphisms of $\mathbb{F}_2$, we also have $M_{24} = \mathrm{Aut}^*(\mathcal{G}_{24})$.

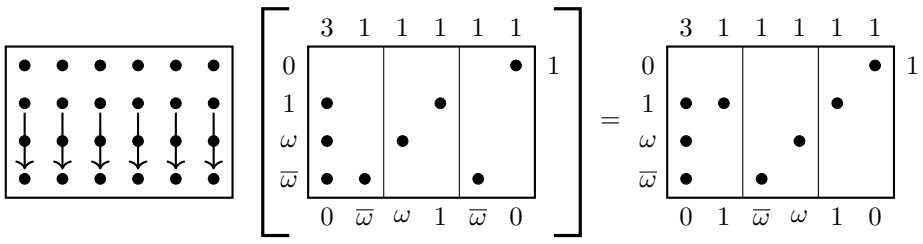
As mentioned, we will use the MOG-notation to depict elements of M_{24} and in general, monomial transformations of $\mathbb{F}_2^{24}$. For this, we will introduce some new conventions. Firstly, we will remove the weights and the scores since those do not apply here and all 24 positions in the MOG will contain dots. Let a monomial transformation be given and interpret it as a permutation of these 24 positions. We now represent this permutation in the MOG by drawing lines between the permuted positions and their images. In case there is a cycle of length at least 3, we also draw an arrowhead to indicate the direction of the cycle. We get, for example, the following monomial transformations this way.

Example 3.14. The left monomial transformation swaps the first column with the second and the fifth column with the sixth. The right example cyclically permutes the second, third and fourth row.



We will also look at some examples of applying these automorphisms on specific Golay codewords. We indicate the argument of an automorphism in M_{24} by putting it in square brackets.

Example 3.15. We apply the right automorphism from Example 3.14 on the right Golay codeword from Example 3.3 and get the following.



3.3.1 The subgroup $2^6{:}\,3\cdot S_6$

Just like with the automorphism group of the hexacode in the previous section, we will first look at some specific automorphisms contained in M_{24} and the subgroup generated by them to get a feel of this group M_{24}. Since the Golay code is constructed with the help of the hexacode, it would be convenient if our knowledge about the symmetries of the hexacode also transfers to the Golay code. It turns out that this is the case.

Definition 3.16. We define a map $\varphi : \mathrm{Aut}(\mathcal{H}_6) \to M_{24}$ as follows. For an automorphism of the hexacode defined by

$$u \mapsto (c_1 u_{\sigma(1)}, c_2 u_{\sigma(2)}, c_3 u_{\sigma(3)}, c_4 u_{\sigma(4)}, c_5 u_{\sigma(5)}, c_6 u_{\sigma(6)})$$

for some $\sigma \in S_6$ and non-zero scalars c_i, the image under φ is the automorphism of $\mathcal{G}_{24}$ that maps the entry in column i with label λ to the entry in column $\sigma^{-1}(i)$ with label $c_{\sigma^{-1}(i)}\lambda$, so we get

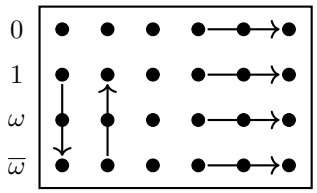
$$\varphi(u) : \{1,\dots,6\} \times \mathbb{F}_4 \to \{1,\dots,6\} \times \mathbb{F}_4 \qquad (i,\lambda) \mapsto (\sigma^{-1}(i), c_{\sigma^{-1}(i)}\lambda)$$

Remark 3.16.1. If we have an automorphism $f \in \mathrm{Aut}(\mathcal{H}_6)$ and a Golay codeword u with scores $v \in \mathcal{H}_6$. Then the the Golay codeword $\big(\varphi(f)\big)(u)$ will have scores $f(u)$. So $\varphi(f) \in M_{24}$ applied on the scores of the MOG is the automorphism $f \in \mathrm{Aut}(\mathcal{H}_6)$.

Because of our construction of the Golay code with the MOG and the hexacode scores, these are quite natural automorphisms. Let us look at some examples.

Example 3.17. The monomial transformations in Example 3.14 are contained in $\mathrm{Im}(\varphi)$. The left example corresponds to a double flip and the right example corresponds to scalar multiplication with ω. Both of these are elements of $\mathrm{Aut}(\mathcal{H}_6)$ as mentioned in Lemma 2.19.

Another example is the image of the automorphism s of the hexacode which was defined in (1) in the previous chapter. The image of a word $u_1u_2\,u_3u_4\,u_5u_6$ under this automorphisms is $(\omega u_1, \overline{\omega} u_2, u_3, u_6, u_4, u_5)$. The automorphism $\varphi(s)$ is then as follows.

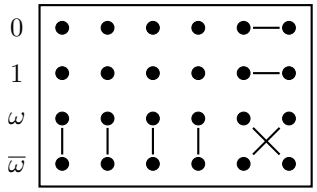


We also have more hexacode-preserving maps that we can embed into M_{24}, namely the semi-automorphisms. One of them was the map t defined in (2). The image of a word u under this semi-automorphism is $(\overline{u_1}, \overline{u_2}, \overline{u_3}, \overline{u_4}, \overline{u_6}, \overline{u_5})$.

Definition 3.18. The map φ can be extended to a map $\varphi^* : \mathrm{Aut}^*(\mathcal{H}_6) \to M_{24}$ where conjugation is achieved by swapping the last two rows with each other.

Remark 3.18.1. It can be easily checked that φ^* is a group homomorphism.

Example 3.19. The automorphism $\varphi^*(t) \in M_{24}$ is represented as follows.



We see that all (semi-)automorphisms of the hexacode can be naturally embedded in M_{24}. But there are even more automorphisms of the Golay code we can already describe. Not only can we embed the automorphisms of the hexacode in M_{24} but also the hexacode itself.

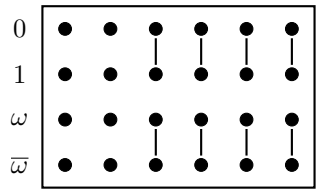
Definition 3.20. We define a map $\psi : \mathcal{H}_6 \to M_{24}$ as follows. Let a hexacodeword u be given. Then its image under ψ is the automorphism of the Golay code which maps the entry in column i with label λ to the entry in column i with label $\lambda + u_i$. So we get

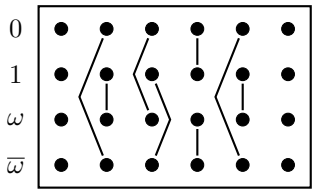
$$\psi(u) : \{1, \ldots, 6\} \times \mathbb{F}_4 \to \{1, \ldots, 6\} \times \mathbb{F}_4 \qquad (i, \lambda) \mapsto (i, \lambda + u_i)$$

Remark 3.20.1. If we consider $\mathcal{H}_6$ as an additive group, it can be easily checked that ψ is a group homomorphism.

Remark 3.20.2. For a hexacodeword u and a Golay codeword g with scores $v \in \mathcal{H}_6$ we get that the Golay codeword $\big(\psi(u)\big)(g)$ has scores $v + u$ if g is odd and v if g is even. This follows from the fact that only the non-zero entries in a Golay codeword contribute to the score and $\mathbb{F}_4$ has characteristic 2.

Example 3.21. A trivial example is $\psi(00\,00\,00)$ which is just the identity map on $\mathbb{F}_2^{24}$. Let us look at two more exciting examples such as $\psi(00\,11\,11)$ and $\psi(0\overline{\omega}\,\omega 1\,\omega 0)$. We then get the following MOG-representations.





Remark 3.21.1. Note that for all the images under ψ, we get either the identity or the composition of two disjoint transpositions within each column.

We now know two types of automorphisms of the Golay code, corresponding to elements of $\mathcal{H}_6$ or elements of $\mathrm{Aut}^*(\mathcal{H}_6)$. We will investigate these automorphisms further before moving on to the other automorphisms as we did with the group G for the hexacode.

Lemma 3.22. $\mathrm{Im}(\varphi^*) \cong 3 \cdot S_6$ *and* $\mathrm{Im}(\psi) \cong 2^6$.

Proof. It follows easily from Definitions 3.18 and 3.20 that φ^* and ψ are injective group homomorphisms. We therefore get

$$\mathrm{Im}(\varphi^*) \cong \mathrm{Aut}^*(\mathcal{H}_6) \cong 3 \cdot S_6 \quad \text{and} \quad \mathrm{Im}(\psi) \cong \mathcal{H}_6$$

As an additive group, it is easy to see that $\mathcal{H}_6$ is an abelian group with 2^6 elements where each except 00 00 00 has order 2. So it is an elementary abelian group and $\mathrm{Im}(\psi) \cong 2^6$. □

We will now look at the subgroup generated by the images of φ^* and ψ. The notation used for extensions can be found in Definition A.6.

Definition 3.23. The subgroup $H = \langle\, \mathrm{Im}(\varphi^*), \mathrm{Im}(\psi) \,\rangle$ is the subgroup of M_{24} generated by the images of φ^* and ψ.

Theorem 3.24. *H is isomorphic to $2^6{:}\,3 \cdot S_6$.*

Proof. We will show that H is the semi-direct product of $\mathrm{Im}(\psi)$ and $\mathrm{Im}(\varphi^*)$. As maps $\{1, 2, \ldots, 6\} \times \mathbb{F}_4 \to \{1, 2, \ldots, 6\} \times \mathbb{F}_4$, we get for $u \in \mathcal{H}_6$ and $f \in \mathrm{Aut}(\mathcal{H}_6)$

$$\psi(u) : (i, \lambda) \mapsto (i, \lambda + u_i) \quad \text{and} \quad \varphi^*(f) : (i, \lambda) \mapsto (\sigma^{-1}(i), c_{\sigma^{-1}(i)}\lambda)$$

for some $\sigma \in S_6$ and non-zero scalars c_i.

We first have to prove that $\mathrm{Im}(\psi)$ is normal in H. We can check that the following holds for $u, v \in \mathcal{H}_6$ and $f \in \mathrm{Aut}(\mathcal{H}_6)$.

$$\psi(u)^{\psi(v)} = \psi(v) \circ \psi(u) \circ \psi(v)^{-1} = (i, \lambda) \mapsto (i, \lambda + u_i) = \psi(u)$$
$$\psi(u)^{\varphi^*(f)} = \varphi^*(f) \circ \psi(u) \circ \varphi^*(f)^{-1} = (i, \lambda) \mapsto (i, \lambda + c_i u_{\sigma(i)}) = \psi(f(u))$$

The equality $\psi(u)^{\varphi^*(f)} = \psi(f(u))$ also holds if f is a semi-automorphism, so we see that $\mathrm{Im}(\psi)$ is preserved by conjugation with the generators of H, so $\mathrm{Im}(\psi) \triangleleft H$ is normal.

Lastly, we have to check that the intersection $\mathrm{Im}(\psi) \cap \mathrm{Im}(\varphi^*)$ is trivial. Let an automorphism in this intersection be given. It is then simultaneously of the form

$$(i, \lambda) \mapsto (i, \lambda + u_i) \quad \text{and} \quad (i, \lambda) \mapsto (\sigma^{-1}(i), c_{\sigma^{-1}(i)} u_i)$$

for some $u \in \mathcal{H}_6$, $\sigma \in S_6$ and $c_i \in \mathbb{F}_4^*$. It clearly follows that σ must be the identity map from which follows that the equality $\lambda + u_i = c_i u_i$ must hold for all i and $\lambda \in \mathbb{F}_4$. It is easy to see that this only holds for $u_i = 0$ and $c_i = 1$. So the intersection $\mathrm{Im}(\varphi^*) \cap \mathrm{Im}(\psi)$ is indeed trivial.

We conclude that H is the semi-direct product of $\mathrm{Im}(\psi)$ and $\mathrm{Im}(\varphi^*)$. It then follows from Lemma 3.22 and the fact that semi-direct products are the same as split extensions that

$$H = \mathrm{Im}(\psi) \rtimes \mathrm{Im}(\varphi^*) \cong 2^6 \rtimes 3 \cdot S_6 = 2^6{:}\,3 \cdot S_6$$

□

We now know a considerable amount of information about this subgroup $2^6{:}\,3\cdot S_6 \subset M_{24}$, so it is time to move on to the group M_{24} itself. As mentioned in the introduction, M_{24} is one of the 26 sporadic groups, the groups that do not fit nicely into one of the infinite families of finite simple groups in the Classification Theorem. We would like to explore this property more, so we will specifically prove that M_{24} is a simple group in the next few sections.

A detailed exploration of finite simple groups can be found in Appendix B where we mention that Iwasawa's lemma, see [Iwa41], is the easiest way of proving that a certain finite group is simple. We advise the reader to read through Appendix B and specifically section B.2 involving actions.

Observation 3.25. *We need to meet the following conditions to apply Iwasawa's lemma on M_{24} and conclude that M_{24} is simple.*

1. *M_{24} is finite and perfect*
2. *A faithful and primitive action of M_{24} on some set X.*
3. *A point stabiliser H with a normal, abelian subgroup A.*
4. *The conjugates of A generate M_{24}.*

We can already verify one part of the first condition.

Remark 3.25.1. M_{24} is finite since it is the automorphism group of a (finite) linear code.

By far the hardest part of applying Iwasawa's lemma is finding the right action of M_{24} on some set X. We could try the natural action of M_{24} on the Golay code or the action on the 24 coordinates of the MOG but it turns out that both of these do not meet the conditions of Iwasawa's lemma. Specifically, condition 4. can not be met since the normal, abelian subgroups of point stabilisers are not large enough to generate M_{24} together with its conjugates in these cases.

Instead of immediately finding the right action, we could also choose a suitable group H and a normal, abelian subgroup $A \subset H$ and then reverse engineer the right set X and the right action of M_{24} on X. We have already suggestively defined a subgroup H in Definition 3.23 and this is indeed the one we will choose for Iwasawa's lemma. We have also already seen that H contains the normal abelian subgroup $\mathrm{Im}(\psi) = 2^6$ which contains 64 elements. That is relatively many and we will see that choosing this group for our A will meet condition 4. Now we just have to find the right action and set X and then verify all the conditions.

3.4 Sextets and tetrads

We will spend this section on discovering such a suitable primitive action. One necessary condition is that $2^6{:}\,3\cdot S_6$ should be a point stabiliser of some element of X, so we have to find some kind of element that is preserved by $2^6{:}\,3\cdot S_6$. It is not immediately clear from the definition what that would be. We know

that $2^6{:}3\cdot S_6$ contains the automorphisms $\varphi^*(f)$ and $\psi(u)$ for $f \in \mathrm{Aut}^*(\mathcal{H}_6)$ and $u \in \mathcal{H}_6$. These are all very different automorphisms but there is one thing that they all preserve. We can see that MOG-entries within the same column stay within the same column when we apply one of those automorphisms. The elements $\psi(u)$ only permute entries within the same column and the elements $\varphi^*(f)$ permute whole columns with each other. So we see that this structure is preserved by $2^6{:}3\cdot S_6$.

To put it more precisely, this specific partition of the 24 MOG-positions into 6 groups of 4, namely the 6 columns, is preserved. The set X on which we will define an action of M_{24} consists of these kinds of partitions of the MOG into 6 groups of 4. We will, however, not include all possible partitions in X but only certain partitions so that the action we will define is indeed primitive and faithful as required. The partitions of the MOG into 6 groups of 4 positions that are included in X will be called *sextets*.

3.4.1 Cosets

We now have an intuitive feeling of what our set X is going to be but we will first define these sextets rigorously and get a better feeling of which partitions are included in X. To do this, we will have to look at the cosets of $\mathcal{G}_{24}$ within $\mathbb{F}_2^{24}$. Specifically, we will look at representatives of minimal weight of these cosets. The cosets where the minimal representative has weight 4 will induce the partitions we are interested in, so the sextets. We need the next two lemmas to count the number of these cosets and sextets.

Lemma 3.26. *A coset of $\mathcal{G}_{24}$ in $\mathbb{F}_2^{24}$ can not have two different representatives of weight at most 3.*

Proof. We know from Theorem 3.9 that the weight distribution of $\mathcal{G}_{24}$ is

$$0^1\, 8^{759}\, 12^{2576}\, 16^{759}\, 24^1$$

So the minimal weight/distance of the Golay code is 8. If there would be a coset with two different representatives of weight at most 3, then their difference, which is the same as their sum since we work in $\mathbb{F}_2$, would be a Golay codeword and have a non-zero weight of at most 6 which is not possible. This proves the lemma by contradiction. □

Definition 3.27. We call two words u, v in $\mathbb{F}_2^{24}$ *disjoint* if they do not have a one-coordinate in the same position.

Remark 3.27.1. Since we work in $\mathbb{F}_2$, this is equivalent to $w(u+v) = w(u)+w(v)$.

Lemma 3.28. *A coset of $\mathcal{G}_{24}$ in $\mathbb{F}_2^{24}$ can not have two non-disjoint representatives of weight at most 4.*

Proof. The same principle as in the proof of Lemma 3.26 applies since the difference (or sum) of two non-disjoint representatives of weight at most 4 has a non-zero weight of at most 6 because the one-coordinates in the same position in both representatives cancel each other. □

Using these lemmas we can now count the number of cosets with a minimal representative of weight 4.

Theorem 3.29. *There are exactly 1771 cosets of $\mathcal{G}_{24}$ whose minimal representative has weight 4.*

Proof. We know from Lemma 3.8 that $\dim(\mathcal{G}_{24}) = 12$ and $\mathcal{G}_{24} \subset \mathbb{F}_2^{24}$, so there are exactly $2^{24-12} = 2^{12} = 4096$ cosets of the Golay code. We know from Lemma 3.26 that each word of weight at most 3 is contained in a unique coset. This way, we count exactly

$$\binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} = 2325 \text{ cosets}$$

with a minimal representative of weight at most 3. We now look at the words of weight 4. Because of the same argument as in the two lemmas, all these words can not be in one of the 2325 already found cosets. From Lemma 3.28, it follows that at most 6 words of weight 4 can be contained in the same coset since it is impossible to have 7 disjoint words of weight 4. We therefore find at least

$$\binom{24}{4} \Big/ 6 = 1771 \text{ more cosets}$$

We have now accounted for at least $2325 + 1771 = 4096$ different cosets but that is also the total number of cosets, so we have found them all. We conclude that there are exactly 1771 cosets with a minimal representative of weight 4 and all of these 1771 cosets contain exactly 6 disjoint representatives of weight 4. □

Remark 3.29.1. This is another "count some objects and then find out those are all of them" proof.

We can now define how these cosets induce the desired partitions.

Definition 3.30. Each of the 1771 cosets in Theorem 3.29 contains 6 disjoint representatives of weight 4. We place each representative in the MOG and form a group of the 4 positions that contain a dot, so the one-coordinates. Such a group is called a *tetrad*. The 6 tetrads in the same coset are disjoint, so they form a partition of the 24 positions into 6 groups of 4. This partition is called a *sextet*. We define X to be the set of sextets.

Remark 3.30.1. It follows from Theorem 3.29 that $|X| = 1771$ since different cosets determine different sextets.

Remark 3.30.2. Every choice of 4 positions of the MOG form a tetrad that is contained in a sextet since every word of weight 4 is contained in one of the 1771 cosets from Theorem 3.29.

Remark 3.30.3. Look at two tetrads in a sextet. The MOG-word that has one-coordinates in exactly the positions of these two tetrads is a Golay codeword since the result is the sum of two representatives of the same coset which must give an element of $\mathcal{G}_{24}$.

We have finally defined the set X on which we will let M_{24} act, so let us look at some elements of X to get a better feeling of this set. Once again, the MOG comes in handy and we will introduce some conventions to specifically represent sextets.

We will not write down row labels, weight and scores since they do not apply to sextets. The positions in the same tetrad will be given the same number and if possible, lines will be drawn to separate the different tetrads from each other. This gives, for example, the following 2 MOGs.

Example 3.31.

1	2	3	4	5	6
1	2	3	4	5	6
1	2	3	4	5	6
1	2	3	4	5	6

1	1	3	3	5	5
1	1	3	3	5	5
2	2	4	4	6	6
2	2	4	4	6	6

The left sextet in this example will be necessary for our proof of the simplicity of M_{24}, so we will give it a name.

Definition 3.32. K is the left sextet in Example 3.31.

Before we study the action of M_{24} on the sextets, we will define an important characteristic of sextets that we will need.

Definition 3.33. Let a sextet be given and look at the column distributions of its 6 tetrads. We pick the distribution that has the highest coefficient for the 4-term and if there is a tie, the highest coefficient for the 3-term, etc. We also remove the 0-term in the picked distribution. This is the *characteristic* of the sextet.

Let us look at some examples again.

Example 3.34. K has characteristic 4^1 and the other sextet in Example 3.31 has characteristic 2^2. The following two MOGs also represent sextets which can be checked by verifying that any choice of two tetrads forms an octad in the Golay code together. They have characteristics $3^1\,1^1$ and $2^1\,1^2$ respectively.

1	2	3	3	3	3
2	1	4	4	4	4
2	1	5	5	5	5
2	1	6	6	6	6

1	1	1	2	5	6
1	2	2	2	4	3
3	5	6	4	3	6
4	6	5	3	5	4

We will take a closer look at the characteristics of the sextets.

Lemma 3.35. *There is* 1 *sextet of characteristic* 4^1, 90 *of* 2^2, 240 *of* $3^1\,1^1$ *and* 1440 *of* $2^1\,1^2$.

Proof. From Remark 3.30.2, we can count the number of tetrads with each column distribution. We get the following numbers.

Column distribution	Number of tetrads
4^1	6
2^2	540
$3^1\,1^1$	480
$2^1\,1^2$	3840
1^4	5760

The tetrads with distribution 4^1 are exactly the tetrads of K, so there is indeed one sextet of characteristic 4^1. Because of the parity condition for Golay codewords and the fact that two tetrads form an octad together, tetrads with distribution 2^2 can not be in the same sextet as any tetrad with one of the three bottom distributions. They must then be contained in sextets with 6 tetrads of type 2^2, so we find $540/6 = 90$ sextets of characteristic 2^2.

With similar parity arguments and the column distributions of octads found in Corollary 3.11, we can deduce that there are exactly 240 sextets containing 2 tetrads of distribution $3^1\,1^1$ and 4 tetrads of distribution 1^4. And there are 1440 sextets with 2 tetrads of distribution 1^4 and 4 tetrads of distribution $2^1\,1^2$. □

3.4.2 Transitivity and the order of M_{24}

We now have enough information about sextets to move on to studying the action of M_{24} on the set X of sextets. We take the natural action of M_{24} on X, namely the one induced by the natural action of M_{24} on the 24 points of the MOG. Just like with $\mathrm{Aut}(\mathcal{H}_6)$ previously, we will first look at the action of a subgroup, in this case $H = 2^6{:}\,3\cdot S_6$, on X.

Lemma 3.36. *The orbits of X under the action of H consist exactly of the sextets with the same characteristic.*

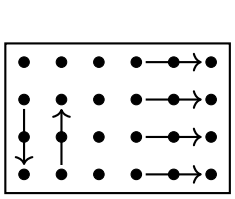
Proof. It is clear from the definition of H, as the group generated by the elements of $\mathrm{Im}(\varphi)$ and $\mathrm{Im}(\psi)$, that H preserves characteristics of sextets, so sextets with different characteristics can not be in the same orbit.

Now we just have to show that sextets with the same characteristic are contained in the same orbit. It is easy in this case to explicitly construct an element of H that maps one sextet to the other. We will show this by example but the general approach will become clear. We will take the following two sextets for our proof by example.

1	1	1	2	5	6
1	2	2	2	4	3
3	5	6	4	3	6
4	6	5	3	5	4

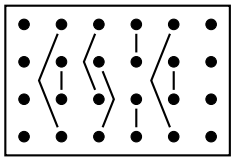
5	3	6	2	3	1
5	4	5	1	4	1
4	6	1	6	2	3
3	6	2	5	2	4

Note that every tetrad is contained in a unique sextet, so if we find an automorphism that maps the left 1-tetrad to the right 1-tetrad, it also maps the left sextet to the right sextet. We will now find the right element of H. We first want to correctly permute the columns containing 1s. This is always possible since $\mathrm{Im}(\varphi^*) \subset H$ acts on the columns like a full S_6. Here, we can take the permutation (15)(26) on the columns followed by the automorphism $\varphi^*(s)$, defined in Example 3.17.



$$\left[\begin{array}{cc|cccc} 5&6&1&2&1&1\\ 4&3&2&2&1&2\\ \hline 3&6&6&4&3&5\\ 5&4&5&3&4&6 \end{array}\right] = \begin{array}{|cc|cccc|} \hline 5&6&1&1&2&1\\ 5&6&2&2&2&1\\ \hline 4&4&6&5&4&3\\ 3&3&5&6&3&4\\ \hline \end{array}$$

We now pick an automorphism $\psi(u)$ for some $u \in \mathcal{H}_6$ such that the 1s in the columns are mapped to the right position. By inspection of the 1s, this hexacodeword must be of the form $??\,\omega 1\,?0$. It follows from Definition 2.16 that any 3 coordinates can be extended to a hexacodeword. In this case, we get $u = 0\overline{\omega}\,\omega 1\,\overline{\omega}0$. Applying $\psi(0\overline{\omega}\,\omega 1\,\overline{\omega}0)$ then gives us



$$\left[\begin{array}{cc|cccc} 5&6&1&1&2&1\\ 5&6&2&2&2&1\\ \hline 4&4&6&5&4&3\\ 3&3&5&6&3&4 \end{array}\right] = \begin{array}{|cc|cccc|} \hline 5&3&6&2&3&1\\ 5&4&5&1&4&1\\ 4&6&1&6&2&3\\ 3&6&2&5&2&4\\ \hline \end{array}$$

□

We now move on to the action of the full group M_{24} on the sextets. This is the action that will meet the conditions of Iwasawa's lemma together with the choice of subgroups H and $A = \mathrm{Im}(\psi) = 2^6$. We already implicitly claimed that H is the point stabiliser of the sextet K consisting of the six columns. We will verify that now.

Lemma 3.37. *The point stabiliser $(M_{24})_K$ of the sextet K under the action of M_{24} is $H = 2^6{:}\,3 \cdot S_6$.*

Proof. It is clear that $H \subset (M_{24})_K$. We now prove the reverse inclusion. Let an automorphism $f \in (M_{24})_K$ be given. We will prove that $f \in H$. First of all, f preserves the sextet K, so the column structure. It therefore acts on the columns like some $\sigma \in S_6$. We know that H acts on the columns like a full S_6, so there is some $g \in H$ which acts like σ^{-1} on the columns. Now look at $g \circ f$ which then not only preserves K but also the tetrads of K, so the columns themselves.

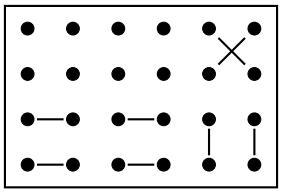
We look at the images of $(i, 0)$, the entry in column i with label 0, under $g \circ f$. Let these images be (i, u_i). By looking at the image under $g \circ f$ of the first basis element in Example 3.12, we know that $u_1u_2\,u_3u_4\,u_5u_6$ must be a hexacodeword since those are the scores of the image and we know that $g \circ f$ preserves the Golay code. Now let $h = \psi(u_1u_2\,u_3u_4\,u_5u_6) \circ g \circ f$. We then know that h preserves the columns and maps $(i, 0)$ to $(i, 0)$.

Now look at the images under h of the 7th, 8th, 10th and 11th element of the basis in Example 3.12 and the two corresponding Golay codewords with scores $\overline{\omega\omega}\,\overline{\omega\omega}\,00$ and $00\,\overline{\omega\omega}\,\overline{\omega\omega}$. It follows easily from our knowledge of the hexacode, the definition of the Golay code and the fact that $h \in M_{24}$ that h is the automorphism corresponding to a scalar multiplication in $\mathrm{Aut}(\mathcal{H}_6)$. It follows that $h \in H$ and therefore also $f \in H$. We see that $(M_{24})_K \subset H$ and thus $(M_{24})_K = H$. □

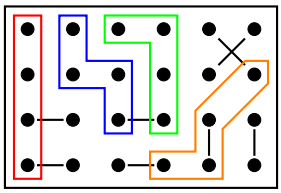
Another condition of Iwasawa's lemma is that the action of M_{24} on the sextets is primitive. A prerequisite for primitive actions is that they are transitive, so we check that first.

Lemma 3.38. *The action of M_{24} on the set X of sextets is transitive.*

Proof. Look at the following monomial transformation which we will call α.



It can be checked that $\alpha \in M_{24}$ with the basis elements from Example 3.12. It is also easy to check that α fuses the four orbits from Lemma 3.36, in other words, for every choice of two orbits (under the action of H), there is a sextet in one that is mapped to a sextet in the other. Like previously, we can concentrate on the tetrads since they determine a unique sextet. The claim then follows by checking the images of the following tetrads, indicated by coloured boundaries.



It follows from Lemma 3.35 that the four orbits, so the four characteristics, are indeed fused by α and therefore there is only one orbit for the action of M_{24} on X, so M_{24} acts transitively on the sextets. □

One useful aspect of actions is that we can use the orbit-stabiliser theorem to calculate the order of the group if we know the sizes of the orbit and stabiliser

of an element. We now know those sizes for the sextet K, so an important intermediate result is the order of M_{24}.

Corollary 3.39. $|M_{24}| = 244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$

Proof. We know from Lemma 3.37 that $(M_{24})_K = 2^6{:}\,3 \cdot 3S_6$ and from Lemma 3.38 that $M_{24}K = X$, so we get with the orbit-stabiliser theorem that

$$\begin{aligned} |M_{24}| &= |(M_{24})_K| \cdot |M_{24}K| = |2^6{:}\,3 \cdot 6| \cdot |X| \\ &= 2^6 \cdot 3 \cdot 6! \cdot 1771 = 244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 \end{aligned}$$

□

Remark 3.39.1. Notice that $|M_{24}|$ is divisble by $20 \cdot 21 \cdot 22 \cdot 23 \cdot 24$. As we will after Lemma C.4, this is not a coincidence.

3.5 Simplicity of M_{24}

As mentioned, the action of M_{24} on the sextets is not only transitive but also primitive which is necessary for Iwasawa's lemma, so we will prove that now.

Theorem 3.40. *The action of M_{24} on the set X of sextets is primitive.*

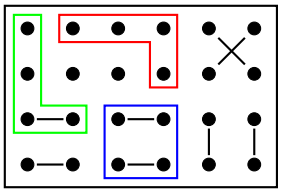
Proof. We already saw that M_{24} acts transitively. Now assume that M_{24} does not act primitively on the sextets, so there is some non-trivial partition of X that is preserved by M_{24}. We clearly have $M_{24} \neq (M_{24})_K = H$, so M_{24} does not always preserve the sextet K which means that K can not be in a singleton set in this partition. So K is contained in an imprimitivity block, name this block B, and there is at least one more sextet $L \in B$. We will show that all the sextets must be contained in B which is not possible by the definition of an imprimitivity block, so this would prove the claim.

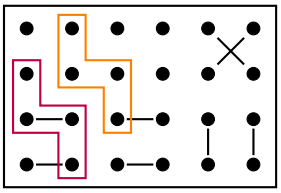
Let an arbitrary $f \in H$ be given, we then get

$$\{K, f(L)\} = \{f(K), f(L)\} \subset f(B)$$

We know that $f(B) = B$ or $f(B) \cap B = \emptyset$ by definition but clearly $K \in f(B) \cap B$, so the last option is not possible. We get $f(B) = B$ and therefore $f(L) \in B$. So we see that the orbit of L under the action of H must be contained in B. It follows from Lemma 3.35 that all sextets with the same characteristic as L are elements of B. Now all we have to do is show that for each characteristic, there is some sextet in B since then all sextets are in B.

We will look at the automorphism α from Lemma 3.38 again and some new tetrads indicated by the coloured boundaries.





We can see that α is contained in the stabilisers of the sextets corresponding to the three left sextets. These three sextets all have different characteristics, so at least one of them is contained in B. Assume wlog that the blue one is contained in B and call it S. The sextets corresponding to the two right sextets have the same characteristic and are then also contained in B. We can now apply the same trick we did with $H = (M_{24})_K$ to $\alpha \in (M_{24})_S$ and get that the images of the right two sextets under α are contained in B. These have characteristics $2^2\,1^2$ and $3^1\,1^1$ respectively, so there is at least one sextet of each characteristic in B It follows that B contains all sextets which is not possible. So by contradiction, it is proven that M_{24} works primitively on the sextets. □

With this Theorem, we have proven the most difficult condition of Iwasawa's lemma for our action. There are 2 important remaining conditions. The conjugates of $A = 2^6 = \mathrm{Im}(\psi)$ need to generate M_{24} and M_{24} needs to be perfect. We focus on the conjugates first.

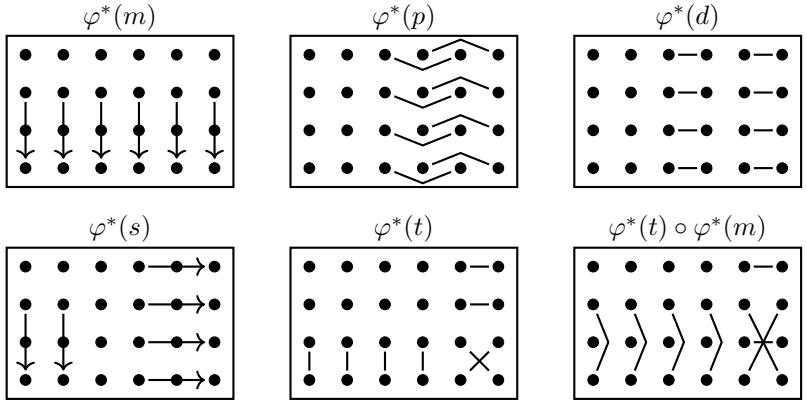
Definition 3.41. J is the subgroup of M_{24} generated by the conjugates of A.

Remark 3.41.1. By definition, J is closed under conjugation.

We want to prove that $J = M_{24}$ which is just a matter of writing down conjugates of A until we have enough to generate M_{24}. We first prove the following intermediate result.

Lemma 3.42. *The subgroup $H = 2^6{:}\,3 \cdot S_6$ is contained in J.*

Proof. We know that H is generated by the elements in $\mathrm{Im}(\varphi^*)$ and $\mathrm{Im}(\psi) = 2^6$. By definition, $\mathrm{Im}(\psi) \subset J$, so we only need to show that the image of $\varphi^* : \mathrm{Aut}^*(\mathcal{H}_6) \to M_{24}$ is contained in J. We know from Lemma 2.19, Theorem 2.25 and Theorem 2.26 that $\mathrm{Aut}^*(\mathcal{H}_6)$ is generated by scalar multiplications, permutations of coordinate pairs, double flips, the automorphism s and the semi-automorphism t. So it is enough to show that the following elements of M_{24} are contained in J where m is a scalar multiplication, p is a permutation of the the coordinate pairs and d is a double flip.



If all these elements are in J, then also the other permutations of coordinate pairs, scalar multiplications and double flips are in J since they are either conjugates of the shown elements or generated by them. For the proof that these elements are in J, we have to look at the following sextets.

1	1	3	3	5	5
1	1	3	3	5	5
2	2	4	4	6	6
2	2	4	4	6	6

1	2	3	3	3	3
2	1	4	4	4	4
2	1	5	5	5	5
2	1	6	6	6	6

1	1	3	3	5	5
2	2	4	4	6	6
1	1	3	3	5	5
2	2	4	4	6	6

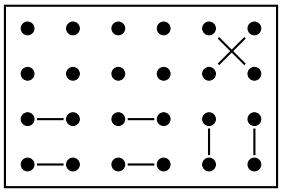
It is easy to see that $\varphi^*(t)$ preserves the left sextet, $\varphi^*(d)$ preserves the middle sextet and $\varphi^*(t) \circ \varphi^*(m)$ preserves the right sextet. Since M_{24} acts transitively on the sextets, we know that the point stabilisers are conjugates. So these three automorphisms are conjugates of elements in H and from inspection, it follows that they are conjugates of some automorphism $\psi(0a\,0a\,bc) \in A$ since within each tetrad they are either the identity or the composition of two transpositions which was also the case for $A = \mathrm{Im}(\psi)$ and the sextet K, see Remark 3.21.1. So these elements are all contained in J.

It then also follows that $\varphi^*(m) \in J$ and we see that $\varphi^*(d)^{\varphi^*(s)} = \varphi^*(p)$, so this element is also in J since J is closed under conjugation. Lastly, we see that $\varphi^*(s)$ preserves the middle sextet and is a conjugate of $\varphi^*(m)$, so all the required elements are in J and we conclude that $H \subset J$. □

We can now prove that $J = M_{24}$.

Lemma 3.43. *The conjugates of A generate M_{24}.*

Proof. It follows from Lemma 3.42 that $H \subset J$. We also know that the following automorphism α is contained in J since just like $\varphi^*(t)$ in Lemma 3.42, it preserves the left sextet and it follows that it is a conjugate of some $\psi(0a\,0a\,bc) \in A$.



Since $H \subset J$ and $\alpha \in J$, it follows from the proof of Lemma 3.38 that J acts transitively on the sextets and $J_K = H$, so with the orbit-stabiliser theorem we get

$$|J| = |J_K| \cdot |JK| = |H| \cdot |X| = |M_{24}|$$

We also clearly have $J \subset M_{24}$, so it follows that $J = M_{24}$. □

Next, we have to check that the group M_{24} is perfect but this actually follows quite easily from the fact that the conjugates of A generate M_{24}.

Corollary 3.44. *The automorphism group M_{24} is perfect.*

Proof. We have to prove that the commutator group $[M_{24}, M_{24}]$ generated by the commutators is the whole group M_{24}. The following equality for $u \in \mathcal{H}_6$ can be easily checked

$$[\psi(u), \varphi^*(m)] = \psi(u)\varphi^*(m)(\psi(u))^{-1}(\varphi^*(m))^{-1} = \psi(u)\psi(\omega u) = \psi(\overline{\omega}u)$$

It follows easily that the image of ψ is contained in $[M_{24}, M_{24}]$, so $A \subset [M_{24}, M_{24}]$. We also know that conjugates of commutators are commutators, so it follows that $J \subset [M_{24}, M_{24}]$ but it then follows from Lemma 3.43 that $M_{24} = [M_{24}, M_{24}]$, so M_{24} is perfect. □

Now, we only have one condition remaining that we need to check. M_{24} needs to act faithfully on the sextets.

Lemma 3.45. *M_{24} acts faithfully on the set X of sextets.*

Proof. We have to show that there is no non-identity element of M_{24} that preserves all the sextets. Assume there is such an automorphism f. We interpret f as an element in S_{24} and it can then be written as a product of disjoint cycles. We will construct a tetrad T such that its sextet S is not preserved by f.

First assume that f contains a cycle of at least length 3. Pick a position a in this cycle and put a, $f(a)$ and two random elements which are not $f(f(a))$ in T. We then clearly get that $f(T)$ and T are unequal and non-disjoint, so $f(S) \neq S$.

Now assume that there are at least two cycles of length 2 in f, say (ab) and (cd). Then pick $T = \{a, b, c, e\}$ where $d \neq e$ and we also get $f(S) \neq S$. Lastly, assume that there is only one cycle (ab) of length 2 and all other cycles have length 1. Then pick $T = \{a, c, d, e\}$ where $c, d, e \neq b$ and in this case too, we get $f(S) \neq S$. We conclude that M_{24} acts faithfully on the sextets. □

We have completed all the hard work and we can finally apply Iwasawa's lemma to prove the simplicity of M_{24}.

Theorem 3.46. *The automorphism group M_{24} is simple.*

Proof. We use Iwasawa's lemma where X is the set of sextets, $H = 2^6{:}\,3 \cdot S_6$ and $A = 2^6$. The conditions with the references to their proofs are then as follows.

1. M_{24} is finite (Remark 3.25.1) and perfect (Corollary 3.44).
2. M_{24} acts faithfully (Lemma 3.45) and primitively (Theorem 3.40) on X.
3. There is a point stabiliser H (Lemma 3.37) with a normal, abelian subgroup A (Theorem 3.24).
4. The conjugates of A generate M_{24}. (Lemma 3.43)

We conclude that M_{24} is simple. □

We end our study of the Golay code and its automorphism group M_{24} with this important result. The main results we have obtained are the dimension, weight distribution and a basis of $\mathcal{G}_{24}$, the simplicity of M_{24} and a good understanding of the automorphisms in M_{24}, especially the elements of H.

4 The Leech lattice Λ_{24}

With the knowledge of $\mathcal{G}_{24}$ and M_{24} from the previous section, we can finally define the main object of this thesis, the Leech lattice Λ_{24}. We will mostly follow section 5.4 in [Wil09] where we fill in many details that were left out. Unlike the Golay code and the hexacode, Λ_{24} is a lattice and not a linear code. One might expect that this means our study of the Leech lattice will be very different from our study of the Golay code. This is not the case however and it turns out that there will be many similar notions and proofs. This is why we will not provide as detailed proofs as for the Golay code in most cases. Most of them require a lot of calculating and verifying which the reader should be able to do themselves by mirroring the proofs in the previous chapter for the Golay code.

4.1 Construction of the Leech lattice

Like how we defined the Golay code with the help of the hexacode, we will now give a definition of the Leech lattice that uses the Golay code. It was first constructed by John Leech in 1967, see [Lee67], although Witt claims to have found the Leech lattice in 1940, see [Wit98]. There are many other constructions of the Leech lattice but the one we present here gives us the most information for our purposes.

Definition 4.1. The Leech lattice $\Lambda_{24} \subset \mathbb{R}^{24}$ consists of the vectors $x = (x_1, \ldots, x_{24}) \in \mathbb{Z}^{24}$ for which the following conditions hold:

- There is an $m \in \{0, 1\}$ for which $x_i \equiv m \mod 2$ for all $1 \leq i \leq 24$.
- $\sum_{i=1}^{24} x_i \equiv 4m \mod 8$.
- For all $k \in \{0, 1, 2, 3\}$ the word $u_k \in \mathbb{F}_2^{24}$ defined by

$$(u_k)_i = \begin{cases} 1 & \text{if } x_i \equiv k \mod 4 \\ 0 & \text{otherwise} \end{cases}$$

  is a Golay codeword.

If $m = 0$, then the Leech lattice vector is called even, if $m = 1$, it is called odd.

Remark 4.1.1. It is easy to check that this definition indeed gives a lattice.

Remark 4.1.2. In the third condition, for two choices of k we have $u_k = \mathbf{0}$ since either all coordinates are odd or all are even. If $m = 1$, then we clearly have $u_1 = \mathbf{1} - u_3$, so it is only necessary to check that one of them is in $\mathcal{G}_{24}$.

This construction is related to the general construction of a lattice from a code mentioned in Definition 2.9 since

$$2B(\mathcal{G}_{24}) = \left\{ 2x : x \equiv u \mod 2 \text{ for some } u \in \mathcal{G}_{24} \text{ and } \sum_{i=1}^{24} x_i \equiv 0 \mod 4 \right\}$$

contains exactly half of the lattice points of Λ_{24}, namely the even Leech lattice vectors. The other half is given by the translated lattice $2B(\mathcal{G}_{24})+(-3,1,\ldots,1)$. The lattice $B(\mathcal{G}_{24})$ was first noticed by Leech in 1964, see [Lee64], but he later noticed that one more translated copy of $B(\mathcal{G}_{24})$ could be fit into the holes of the former lattice and discovered the Leech lattice which was published in 1967, see [Lee67].

Let us look at some examples to get a better understanding of this definition, especially the last condition relating the Leech lattice to the Golay code. Once again, we use MOGs to denote Leech lattice vectors. Zero-coordinates are indicated by empty entries while we write down the values of the other coordinates.

Example 4.2. The first two conditions in Definition 4.1 are easy to check. We give the numbers that are 1 mod 4 a red colour and the numbers that are 2 mod 4 a blue colour. For the third condition, we then need to check that the red or blue positions form a Golay codeword together which is the case for the following four vectors.

0	4					
1	4					
ω						
$\overline{\omega}$						
	0	0	0	0	0	0

0						
1	2	2	2	2		
ω	2	2	2	2		
$\overline{\omega}$						
	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	0

0	−3	1	1	1	1	1
1	1	1	1	1	1	1
ω	1	1	1	1	1	1
$\overline{\omega}$	1	1	1	1	1	1
	0	0	0	0	0	0

0	3	−1	−1	−1	−1	1
1	1	−1	−1	1	−1	−1
ω	1	−1	1	−1	−1	−1
$\overline{\omega}$	1	1	−1	−1	1	−1
	0	$\overline{\omega}$	ω	1	$\overline{\omega}$	0

It also follows easily from the definition how we can find Leech lattice vectors.

Example 4.3. Pick some Golay codeword. Then pick an $m \in \{0,1,2,3\}$ and in the positions of the Golay codeword, put integers m mod 4. In the other positions, put integers $m+2$ mod 4. Now check whether the sum of the coordinates is $4m$ mod 8. If not, add 4 to a random coordinate. We can get, for example, the following Leech lattice vector when we choose the right Golay codeword from Example 3.7 and $m = 0$.

0	2	8	−4	2	−2	12
1		6	10	8	−8	2
ω	4	−6	8	−2	6	8
$\overline{\omega}$	4	2		−6	−2	4
	0	0	1	1	1	1

Now that we have a better understanding of what a Leech lattice vector is and what they look like, we would like to classify them in some way as we did with the Golay codewords. One important aspect we studied was the weight of a codeword which was an $\mathbb{F}_q^n$-equivalent of the Euclidean norm. We therefore want to also assign a weight to the Leech lattice vectors which we can define with the Euclidean norm. The standard dot product in $\mathbb{R}^{24}$ would work in this case but it follows with some modular arithmetic that the standard dot product of two Leech lattice vectors is always divisible by 8. We therefore define the following scaled inner product.

Definition 4.4. We work with the inner product $x \cdot y$ on $\mathbb{R}^{24}$ defined by

$$x \cdot y = \frac{1}{8} \sum_{i=1}^{24} x_i y_i$$

Remark 4.4.1. This is the smallest scaling of the standard dot product such that $x \cdot y$ is an integer for all $x, y \in \Lambda_{24}$ so that Λ_{24} is integral. The top two Leech lattice vectors in Example 4.2 have inner product 1 and the two on the left have inner product -1.

Remark 4.4.2. Another approach frequently used in the literature is to use the standard dot product but scale the Leech lattice by a factor $\frac{1}{\sqrt{8}}$. In our case, this would make some presentations unnecessarily complicated.

We can now define a weight function on the Leech lattice.

Definition 4.5. The *weight* of a vector $x \in \Lambda_{24}$ is defined as $w(x) = x \cdot x$.

Remark 4.5.1. Note that $w(\lambda x) = \lambda^2 w(x)$ for all $\lambda \in \mathbb{Z}$ and $x \in \Lambda_{24}$.

Remark 4.5.2. It follows with some modular arithmetic that $w(x)$ is even for all Leech lattice vectors x.

Example 4.6. All the Leech lattice vectors in Example 4.2 have weight 4 while the vector in Example 4.3 has weight 100.

For the rest of this section, our strategy is analogous to what we did while defining the weight of a vector. Namely, thinking about what we did with the Golay code and trying to find equivalent concepts, elements or objects for the Leech lattice.

4.2 Minimal vectors

One piece of information that was very important for our study of the Golay code was its weight distribution. We can not determine a usual weight distribution since a lattice contains an infinite number of vectors but the number of vectors with a certain weight is finite since lattices are discrete. We can therefore define the following generating series for a lattice.

Definition 4.7. Let L be a lattice. Its *theta function* is given by the following expression.

$$\Theta_L(\tau) = \sum_{x \in L} e^{\pi i \tau \cdot w(x)}$$

For even integral lattices like Λ_{24} we can express the theta function in nicer terms.

Remark 4.7.1. Let a_k be the number of Leech lattice vectors with weight $2k$ and let $q = e^{\tau}$, we then get

$$\Theta_{\Lambda_{24}}(\tau) = \sum_{k=0}^{\infty} a_k q^k$$

The theta function $\Theta_{\Lambda_{24}}$ is actually a modular form and plays a huge role in the proof that Λ_{24} is the densest 24-dimensional sphere packing, see [CKM+17]. We will not go into the details since this thesis does not focus on modular forms but while studying the automorphism group of Λ_{24}, we will need the values of $a_0, \ldots, a_4$, so we will give the relevant vectors a name.

Definition 4.8. A Leech lattice vector x is called a *short vector* if $w(x) \leq 8$.

Remark 4.8.1. The coordinates of a short vector are in $\{-8, -7, \ldots, 7, 8\}$

We now want to determine the values of $a_0, \ldots, a_4$. While counting the number of Leech lattice vectors of a certain weight, there are multiple cases that need to be handled differently. We first introduce a characteristic for short vectors that identifies these cases. This characteristic is very reminiscent of the column distribution of a Golay codeword or the characteristic of a sextet.

Definition 4.9. Let x be a short Leech lattice vector and let a_k be the number of coordinates with value k or $-k$. The expression

$$(8^{a_8}, 7^{a_7}, 6^{a_6}, 5^{a_5}, 4^{a_4}, 3^{a_3}, 2^{a_2}, 1^{a_1}, 0^{a_0})$$

where the terms with $a_k = 0$ are removed, is the *characteristic* of x.

Example 4.10. The Leech lattice vectors in Example 4.2 are all short. They have characteristics $(4^2, 0^{22})$, $(2^8, 0^{16})$ and $(3, 1^{23})$.

We can now start counting the short vectors. We already mentioned in Remark 4.5.2 that every Leech lattice vector has even weight and it is clear that there is exactly one Leech lattice vector of weight 0. So the following four lemmas are sufficient.

Lemma 4.11. *There are no short vectors of weight 2.*

Proof. It follows from some simple arithmetic that a Leech lattice vector of weight 2 would have characteristic $(4^1, 0^{23})$ or $(2^4, 0^{20})$. The first one can not meet the first condition in Definition 4.1 while the second one can not meet the third condition since there are no weight 4 Golay codewords. □

Lemma 4.12. *There are 196560 short vectors of weight 4.*

Proof. It follows from some basic arithmetic that a Leech lattice vector of weight 4 can only have characteristic $(3^1, 1^{23})$, $(2^8, 0^{16})$, $(4^2, 0^{22})$ or $(4^1, 2^4, 0^{19})$. The last case does not meet the third condition in Definition 4.1. We count the number of short vectors of the other characteristics. These are simple combinatorial problems.

In the case of $(3^1, 1^{23})$ we have 24 options for the position of the ± 3. Furthermore, we have 2^{24} choices for the signs of all the coordinates. However, most of these do not give a Leech lattice vector since u_1 and u_3 (as in Definition 4.1) have to be Golay codewords. We know from Lemma 3.8 that there are $2^{12} = 4096$ Golay codewords, so exactly 4096 choices for the signs give a Leech lattice vector. In total, we count

$$4096 \cdot 24 = 98304 \text{ short vectors of characteristic } (3^1, 1^{23})$$

For $(4^2, 0^{22})$, all the vectors of this characteristic automatically meet all the conditions in Definition 4.1. There are $\binom{24}{2}$ choices for the positions of the ± 4-coordinates and we have 2^2 sign choices. So we count

$$\binom{24}{2} \cdot 4 = 1104 \text{ short vectors of characteristic } (4^2, 0^{22})$$

For $(2^8, 0^{16})$, we must have that u_2 is a Golay codeword, so the eight coordinates with value 2 or -2 must form an octad. We know from Theorem 3.9 that there are 759 octads. Furthermore, there are 2^8 sign choices but only half of them meet the second condition in Definition 4.1, having the total sum of the coordinates be divisible by 8, and give a Leech lattice vector. We count

$$759 \cdot 2^7 = 97152 \text{ short vectors of characteristic } (2^8, 0^{16})$$

In total, we find 98304+1104+97152 = 196560 short vectors of weight 4. □

The proofs for the short vectors of weight 6 and 8 are analogous to the proof of Lemma 4.12 but are even longer because of more possible characteristics. Therefore, we will just write down the characteristics and the number of short vectors per characteristic and leave it as an exercise to the reader to verify them.

Lemma 4.13. *There are 16773120 short vectors of weight 6.*

Proof. The factor 2576 in the last row comes from the number of weight 12 Golay codewords, see Theorem 3.9. All the numbers indeed add up to 16773120.

Characteristic	Combinatorial interpretation	Number of short vectors
$(5, 1^{23})$	$24 \cdot 2^{12}$	98304
$(3^3, 1^{21})$	$\binom{24}{3} \cdot 2^{12}$	8290304
$(4, 2^8, 0^{15})$	$759 \cdot 16 \cdot 2^8$	3108864
$(2^{12}, 0^{12})$	$2576 \cdot 2^{11}$	5275648

□

Lemma 4.14. *There are 398034000 short vectors of weight 8.*

Proof. The numbers below add up to 398034000.

Characteristic	Combinatorial interpretation	Number of short vectors
$(5, 3^2, 1^{21})$	$\binom{24}{2} \cdot 22 \cdot 2^{12}$	24870912
$(3^5, 1^{19})$	$\binom{24}{5} \cdot 2^{12}$	174096384
$(8, 0^{23})$	$24 \cdot 2$	48
$(6, 2^7, 0^{16})$	$759 \cdot 8 \cdot 2^7$	777216
$(4^4, 0^{20})$	$\binom{24}{4} \cdot 2^4$	170016
$(4^2, 2^8, 0^{14})$	$759 \cdot \binom{16}{2} \cdot 2^9$	46632960
$(4, 2^{12}, 0^{11})$	$2576 \cdot 12 \cdot 2^{12}$	126615552
$(2^{16}, 0^8)$	$759 \cdot 2^{15}$	24870912

□

As with the hexacode and Golay code, we want to find generators and a basis of Λ_{24}. Our knowledge about the short vectors is enough to find these.

Theorem 4.15. *The Leech lattice is generated by the short vectors of weight 4.*

Proof. Let $x \in \Lambda_{24}$ be randomly given. We will show that x can be written as the sum of short vectors of weight 4. We can assume that x is even since if it is odd we add a short vector of characteristic $(3, 1^{23})$ to get an even vector. Now the word u_2, consisting of all positions with a coordinate 2 mod 4, is a Golay codeword. We know from the basis in Example 3.12 that the Golay code is generated by the octads, so we can add suitable short vectors of characteristic $(2^8, 0^{16})$ so that all the coordinates of x become divisible by 4.

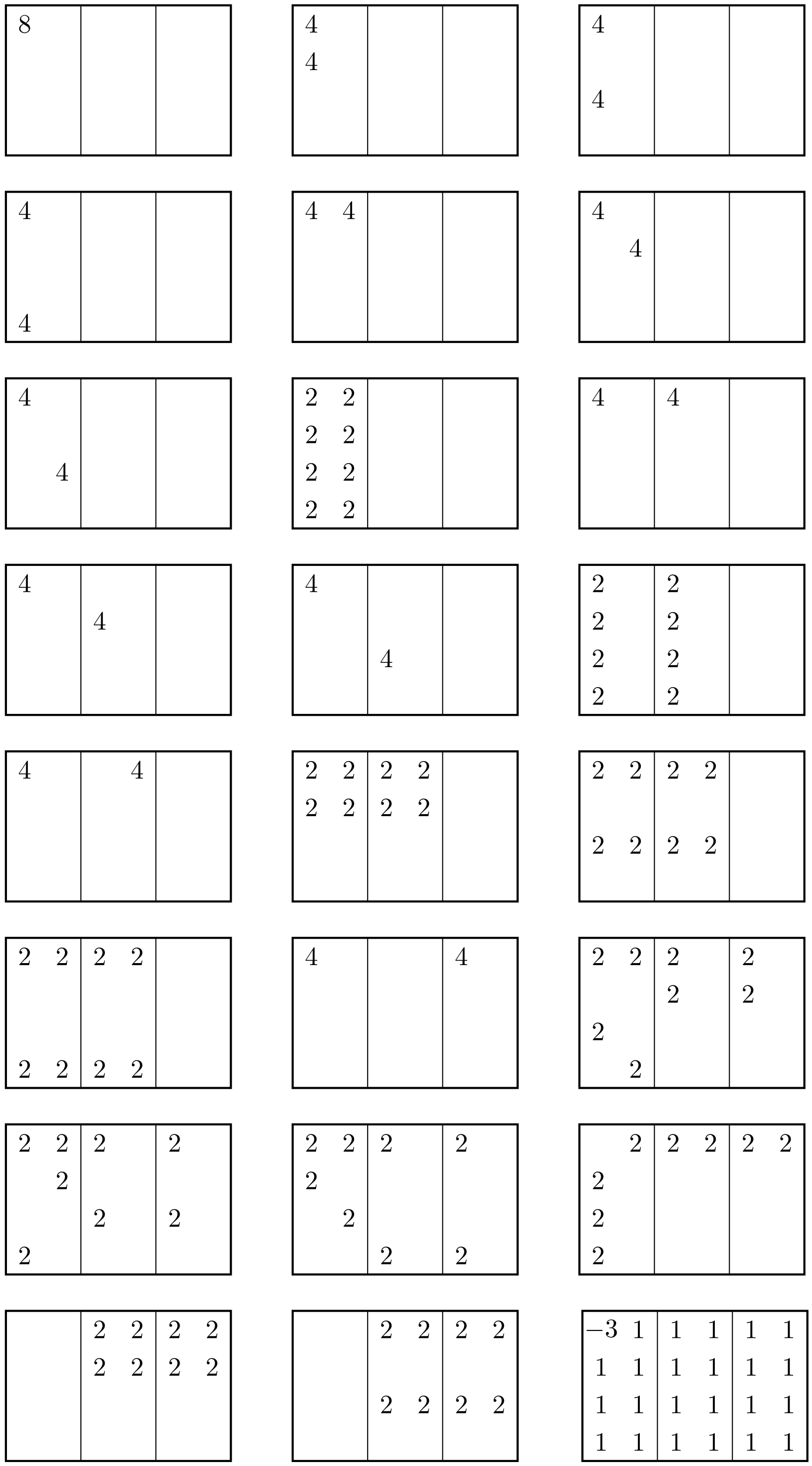
Now note that a short vector of characteristic $(8, 0^{23})$ can be easily written as the sum of two short vectors of characteristic $(4^2, 0^{22})$, for example

$$(8, 0, \ldots, 0) = (4, -4, \ldots, 0) + (4, 4, \ldots, 0)$$

Now add or subtract vectors of characteristic $(8, 0^{23})$ to x so that all coordinates become 0 or 4. The sum of all coordinates needs to be divisible by 8, so there is an even number of fours in x which can then easily be written as the sum of short vectors of characteristic $(4^2, 0^{22})$. So x is in the linear span of the short vectors of weight 4 and we see that Λ_{24} is generated by these vectors. □

It follows from Lemma 4.12 and Theorem 4.15 that we have found a set of 196560 generators for the Leech lattice. However, most of these are not necessary since Λ_{24} is 24-dimensional. We can write down an explicit 24 element basis.

Corollary 4.16. *The following* 24 *Leech lattice vectors, taken from [CSdlH98], form a basis of* Λ_{24}.



Proof. It is easy to see that all of these vectors are indeed in the Leech lattice. We put these 24 vectors in standard vector notation and then put them into a 24×24 matrix M as columns from left to right. We get an upper triangular matrix with determinant 8^{12}, so these vectors are linearly independent.

Let $L \subset \Lambda_{24}$ be the sublattice generated by these 24 linearly independent vectors. We have that M is a generator matrix of L and since we use the scaled inner product, the volume also gets scaled by 8^{-12}. The corresponding fundamental region F therefore has volume 1.

Let M' be a generator matrix of Λ_{24}. Since $\Lambda_{24} \subset \mathbb{Z}^{24}$ is integral, the volume of the fundamental region F' of Λ_{24} has integer volume and we get the following inequality from linear algebra for the index of L inside Λ_{24}.

$$[\Lambda_{24} : L] = \frac{|\det(M)|}{|\det(M')|} = \frac{\mathrm{Vol}(F)}{\mathrm{Vol}(F')} = \frac{1}{\mathrm{Vol}(F')} \leq 1$$

So it follows that $[\Lambda_{24} : L] = 1$ and therefore $L = \Lambda_{24}$ and the 24 shown vectors form a basis of Λ_{24}. □

4.3 Leech lattice packing

Before we move on to studying the symmetries of the Leech lattice, we explore the sphere packing induced by the Leech lattice which was our motivation to go on a journey to define the Leech lattice. We will determine some of the properties of this sphere packing. As mentioned in chapter 1, the proof that the Leech lattice packing is indeed the densest 24-dimensional sphere packing requires extensive knowledge of modular forms which is not the focus of this thesis. We refer the curious reader to [CKM$^+$17] for this proof.

We follow the approach mentioned in Remark 4.4.2, so we use the usual standard inner product instead of the scaled one but scale the whole Leech lattice with a factor $\frac{1}{\sqrt{8}}$. Note that the weights of the vectors remain the same after this change. We choose the basis from Corollary 4.16 and look at the corresponding generator matrix M. We can then show the following.

Theorem 4.17. *The Leech lattice packing has densities*

$$\Delta(\Lambda_{24}) = \frac{\pi^{12}}{12!} \quad \textit{and} \quad \delta(\Lambda_{24}) = 1$$

Proof. It follows that

$$\det(M) = 8^{12} \cdot \left(\frac{1}{\sqrt{8}}\right)^{24} = 1$$

so Λ_{24} is a unimodular lattice. Furthermore, the minimal weight of a Leech lattice vector is 4, so the minimal distance between two Leech lattice points is $\sqrt{4} = 2$. This means that the spheres in the Leech lattice packing have radius

$\rho = 1$. With the formulas from Chapter 1 we then get

$$\delta = \frac{\rho^n}{|\det M|} = \frac{1^{24}}{1} = 1$$
$$\Delta = V_{24} \cdot \delta = \frac{\pi^{12}}{12!}$$

□

Lastly, we determine the kissing number of Λ_{24} which is quite easy to do now.

Lemma 4.18. *The kissing number of the Leech lattice is 196560*

Proof. The kissing number is the number of spheres that touch a given sphere. We can choose the sphere with center $(0, \ldots, 0)$ and the kissing number becomes the number of lattice points whose distance to the origin is $2\rho = 2$. In other words, the number of Leech lattice vectors of weight 4. It now follows from Lemma 4.12 that the kissing number is 196560. □

4.4 The Conway group Co_0

We now move on to studying the symmetries of the Leech lattice which we will study in a very similar way to M_{24}. We have previously only defined automorphisms for linear codes, so we define what we consider an automorphism of a lattice.

Definition 4.19. Let $L \subset \mathbb{R}^n$ be a lattice. An $\mathbb{R}$-linear map $\mathbb{R}^n \to \mathbb{R}^n$ is called an *automorphism* of L if it preserves L and preserves the inner product so

$$f(L) = L \quad \text{and} \quad f(x) \cdot f(y) = x \cdot y$$

The automorphisms of L form a group $\mathrm{Aut}(L)$.

Remark 4.19.1. Automorphisms also preserve weights. The inner product preserving condition is equivalent to the associated matrix A being orthogonal, so $AA^{\mathrm{T}} = I_n$ and $\det(A) = \pm 1$.

Definition 4.20. The group Co_0 is the automorphism group $\mathrm{Aut}(\Lambda_{24})$ of the Leech lattice. It was first discussed by John Conway in [Con68] and [Con69].

Remark 4.20.1. Every automorphism in Co_0 is defined uniquely by its action on the 196560 short vectors of weight 4. We can interpret Co_0 as a subgroup of S_{196560}, a group of order $196560! \approx 3.4 \times 10^{955127}$, so Co_0 is finite.

An important difference between automorphisms of a lattice and automorphisms of a code is that we do not just restrict ourselves to monomial transformations, permutations of the coordinates combined with coordinate-wise scalar multiplications, but consider many more linear maps, namely all the orthogonal transformations. One undesirable consequence of this is that in general there is

no easier way to represent automorphisms of the Leech lattice than just writing down the corresponding 24×24-matrix (w.r.t. to the standard basis of $\mathbb{R}^{24}$). In some cases, we can adjust the MOG to represent an automorphism or describe the 24×24-matrix using smaller matrices like in the following example.

Example 4.21. The linear map $\beta : \mathbb{R}^{24} \to \mathbb{R}^{24}$, inspired by a similar element in [Gri98], whose associated matrix is the following block matrix

$$\left(\begin{array}{c|c|c|c|c|c} -Bl & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & Bl & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & Bl & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & Bl & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & Bl & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & Bl \end{array}\right) \quad \text{where} \quad Bl = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

is an automorphism of Λ_{24}. It is easy to check that the matrix of β is orthogonal and that β preserves the Leech lattice by checking that the images of the basis elements in Corollary 4.16 are Leech lattice vectors.

Remark 4.21.1. β acts like $-Bl$ on the first column and Bl on the other columns in the MOG-notation of a Leech lattice vector.

Let us look at an example of an automorphism in action.

Example 4.22. We get the following if we apply β on the 21st basis element in Corollary 4.16.

$$\beta \left[\begin{array}{c|ccc|cc} & 2 & 2 & 2 & 2 & 2 \\ 2 & & & & & \\ 2 & & & & & \\ 2 & & & & & \end{array}\right] = \begin{array}{|cc|cc|cc|} \hline 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 \\ \hline \end{array}$$

4.4.1 The subgroup $2^{12}{:}\, M_{24}$

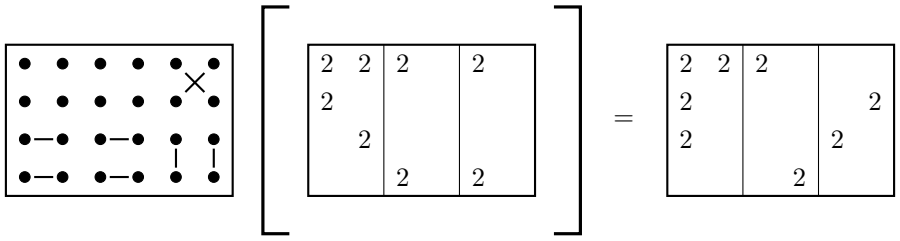
We now proceed to the automorphisms that we can represent with the MOG. These automorphisms are related to the elements of $\mathcal{G}_{24}$ and M_{24} and generate a subgroup $2^{12}{:}\, M_{24}$. This is almost identical to the subgroup $2^6{:}\, 3 \cdot S_6 \subset M_{24}$ that was built from automorphisms related to elements of $\mathcal{H}_6$ and $\mathrm{Aut}^*(\mathcal{H}_6)$. We first define how we embed M_{24} and $\mathcal{G}_{24}$ into Co_0.

Definition 4.23. We define a group homomorphism $\Phi : M_{24} \to \mathrm{Co}_0$ where $\Phi(f)$ is the linear map that acts on the coordinates of $\mathbb{R}^{24}$ like f acts on the coordinates of $\mathbb{F}_2^{24}$.

Remark 4.23.1. It follows from Definition 4.1 that Φ is well-defined and we clearly have that Φ is injective, so $\mathrm{Im}(\Phi) \cong M_{24}$.

The homomorphism Φ is a very natural homomorphism. So natural in fact, that we can just use the same MOG for $\Phi(f)$ as for f. We will take a look at an example.

Example 4.24. Let $\alpha \in M_{24}$ be defined as in Lemma 3.38. We then get the following if we apply $\Phi(\alpha)$ to the 20th basis element in Corollary 4.16. The result is indeed a Leech lattice vector.



We also embed the Golay code itself, interpreted as an additive group, into Co_0 as follows.

Definition 4.25. We define a group homomorphism $\Psi : \mathcal{G}_{24} \to \mathrm{Co}_0$ where $\Psi(u)$ is the linear map that sends the coordinates x_i of a Leech lattice vector x to

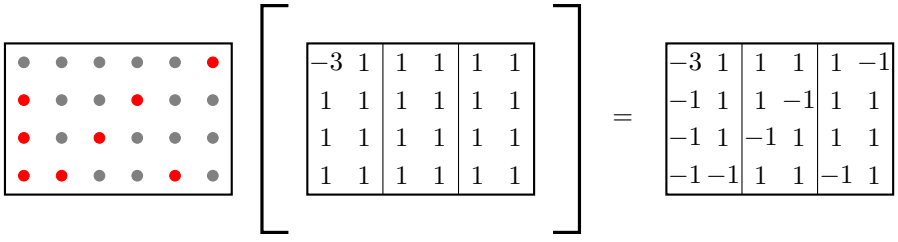
$$x_i \mapsto \begin{cases} x_i & \text{if } u_i = 0 \\ -x_i & \text{if } u_i = 1 \end{cases}$$

So it switches the signs at the positions of the one-coordinates and is the identity at the zero-coordinates.

Remark 4.25.1. It is easy to see again with Definition 4.1 that Ψ is well-defined and injective. We know from Lemma 3.8 that $|\mathcal{G}_{24}| = 2^{12}$ and each has order 2 since $\mathbb{F}_2$ has characteristic 2. So we see $\mathrm{Im}(\Psi) \cong \mathcal{G}_{24} = 2^{12}$.

We can also represent the images of Ψ in MOG-notation. One possibility is to represent $\Psi(u)$ with the MOG of u as a Golay codeword but for compatibility with the MOGs of the images $\Phi(f)$ we make a slight change. All entries will have dots but the zero-coordinates will have grey dots while the one-coordinates, where sign changes occur, have red dots. An example of applying such an automorphism is as follows.

Example 4.26. We take the right word in Example 3.3 for u and we get the following if we apply $\Psi(u)$ to the last basis element in Corollary 4.16.



As with the subgroup $H = 2^6{:}\,3 \cdot S_6$ of M_{24}, we look at the subgroup generated by the images of Φ and Ψ. We call this subgroup I. Then the following Theorem easily follows.

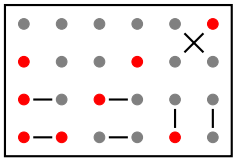
Theorem 4.27. *The subgroup $I = \langle \operatorname{Im}(\Phi), \operatorname{Im}(\Psi) \rangle$ is isomorphic to $2^{12}{:}\,M_{24}$.*

Proof. This is analogous to the proof of Theorem 3.24. □

Remark 4.27.1. It can be shown that I consists exactly of all the monomial transformations, so permutations of the coordinates combined with coordinate-wise scalar multiplications, that preserve Λ_{24}.

It also follows from this Theorem that every element of I can be uniquely written as $\Psi(u) \circ \Phi(f)$ for some $u \in \mathcal{G}_{24}$ and $f \in M_{24}$. We can now represent the elements of I with MOGs in a unique way. The element $\Psi(u) \circ \Phi(f)$, note the order of $\Psi(u)$ and $\Phi(f)$, is represented by combining the MOGs of $\Phi(f)$ and $\Psi(u)$, so the dots of the one-coordinates of u are red while the dots of the zero-coordinates of u are grey. We draw the lines for the permutation f between the dots as usual. Take a look at the following example.

Example 4.28. We take u and f as in Examples 4.24 and 4.26. Applying $\Psi(u) \circ \Phi(f)$ to the vector in Example 4.3 gives the following equation.



$$\left[\begin{array}{cc|cc|cc} 2 & 8 & -4 & 2 & -2 & 12 \\ & 6 & 10 & 8 & -8 & 2 \\ 4 & -6 & 8 & -2 & 6 & 8 \\ 4 & 2 & & -6 & -2 & 4 \end{array}\right] = \left[\begin{array}{cc|cc|cc} 2 & 8 & -4 & 2 & 2 & 8 \\ & 6 & 10 & -8 & 12 & -2 \\ 6 & 4 & 2 & 8 & -2 & 4 \\ -2 & -4 & -6 & & -6 & 8 \end{array}\right]$$

To get a better understanding of this subgroup $2^{12}{:}\,M_{24}$ we take a look at its action on the short vectors. This is well-defined since automorphisms preserve weight.

Lemma 4.29. *The orbits of the short vectors under the action of $2^{12}{:}\,M_{24}$ consist exactly of the vectors with the same characteristic except for the characteristic $(2^{16}, 0^8)$ which splits into 16 different orbits.*

Proof. It is clear from the definition of $2^{12}{:}\,M_{24}$ and the characteristic in Definition 4.9 that short vectors of different characteristics are not in the same orbit. The full proof consists of separate small proofs for each characteristic using certain facts about the Golay codewords and subgroups of M_{24}. We will demonstrate two of them.

For the characteristic $(4^2, 2^8, 0^{14})$, we explicitly calculate the number of elements in its orbit and show that it is the total number of elements of this characteristic, namely 46632960 as in Lemma 4.14. Let a random vector x of this characteristic be given. First of all, the subgroup $\operatorname{Im}(\Phi)$ gives 759 images

of x by permuting the 8 coordinates of ± 2 since M_{24} is transitive on octads, see Lemma C.7.

There are another $\binom{16}{2}$ images for each of those 759 images by permuting the 2 coordinates of ± 4 since it is known that the octad stabiliser in M_{24} is 2-transitive on the remaining 16 points. Lastly, it can be checked that there are exactly 8 elements of $\mathrm{Im}(\Psi)$ that preserve x, so the total number of images is

$$759 \cdot \binom{16}{2} \cdot \frac{|\mathrm{Im}(\Psi)|}{8} = 759 \cdot \binom{16}{2} \cdot 2^9 = 46632960$$

For the characteristic $(2^{16}, 0^8)$, we can calculate in the same way that each vector x has

$$759 \cdot \frac{|\mathrm{Im}(\Psi)|}{2} = 759 \cdot 2^{11} = 1554432 \text{ images}$$

since the positions of the zeroes form an octad u and then the stabiliser $(\mathrm{Im}(\Psi))_x$ consists exactly of the two elements $\Psi(\mathbf{0})$ and $\Psi(u)$. Together with the transitivity of M_{24} on octads, we get the number $759 \cdot 2^{11}$. The total number of vectors of this characteristic is $759 \cdot 2^{15}$, so there are $2^4 = 16$ different orbits for this characteristic. □

Remark 4.29.1. This lemma does not agree with [Wil09] which claims that the characteristic $(2^{16}, 0^8)$ splits into only 2 orbits for this action. It is true that these vectors split into 2 orbits for a different action, see Lemma 4.40.

We now have a good understanding of this subgroup $2^{12}{:}\, M_{24} \subset \mathrm{Co}_0$, so we proceed to studying the full automorphism group Co_0. The last main goal of this thesis to make our story complete is to connect the Leech lattice to the story of finite simple groups and especially the sporadic groups. For the Golay code, we proved that its automorphism group is simple, so we would also like to do that for the Leech lattice. Unfortunately, the group Co_0 itself is not simple.

Lemma 4.30. *The automorphism group Co_0 of the Leech lattice is not simple.*

Proof. The elements $\Psi(\mathbf{0})$ and $\Psi(\mathbf{1})$ clearly form a subgroup $C_2 \subset \mathrm{Co}_0$. Their associated matrices are respectively I_{24} and $-I_{24}$ and it is easy to see that $C_2 \triangleleft \mathrm{Co}_0$ is a non-trivial normal subgroup, so Co_0 is not simple. □

It turns out that this subgroup C_2 is the center of Co_0 and that taking the quotient group of Co_0 by this C_2 results in a simple group. We define this group.

Definition 4.31. The first Conway group is the quotient group

$$\mathrm{Co}_1 = \mathrm{Co}_0 / \{\Psi(\mathbf{0}), \Psi(\mathbf{1})\} \cong \mathrm{Co}_0 / C_2$$

Co_1, just like M_{24}, is one of the sporadic groups. We will spend the rest of this chapter on proving that Co_1 is simple. Our strategy for this is identical to the case of M_{24}. We will find some action of Co_1 on some set and then verify the conditions of Iwasawa's lemma to obtain the simplicity of Co_1. These conditions require a point stabiliser of this action with a normal abelian subgroup. A

subgroup of Co_0 that fits this description is the subgroup $I = 2^{12}{:}\, M_{24}$ which also contains C_2 as a subgroup, so we take the quotient group of I and define the following group.

Definition 4.32. We define the group $I' = I/C_2 \cong 2^{11}{:}\, M_{24}$

Like the subgroup $H = 2^6{:}\, 3 \cdot S_6$ for the Golay code, this group I' will indeed be the point stabiliser we will look at. As a reminder, the conditions of Iwasawa's lemma we need to check then become the following.

1. Co_1 is finite and perfect
2. A faithful and primitive action of Co_1 on some set Y.
3. A point stabiliser I' with a normal, abelian subgroup B'.
4. The conjugates of B' generate Co_1.

We will take $B = 2^{12} \triangleleft 2^{12}{:}\, M_{24}$ as our normal abelian subgroup of I and the corresponding normal abelian subgroup is $B' = 2^{11} \triangleleft I'$. Furthermore, the conditions all mention Co_1, I' and B' but the proofs of many of them will follow from facts about Co_0, I and B. For example, we already know from Remark 4.20.1 that Co_0 is finite, so it follows that Co_1 is finite.

4.5 Crosses

We spend the next few pages on finding the right set Y and the right action of Co_0 (resp. Co_1) on Y. A necessary condition is that $I = 2^{12}{:}\, M_{24}$ (resp. I') is a point stabiliser. This does not provide us with many ideas for a suitable action however, so we will just try to mirror the ideas in section 3.4 and try to tweak them to make them suitable for Co_1 and Λ_{24}.

4.5.1 Cosets

The action we found in section 3.4 was the action of M_{24} on the sextets which were sets of weight 4 words contained in the same coset of $\mathcal{G}_{24} \subset \mathbb{F}_2^{24}$. We will therefore look at cosets related to Λ_{24} and representatives of minimal weight of these cosets. Looking at the cosets of Λ_{24} in a bigger set such as $\mathbb{R}^{24}$ or $\mathbb{Z}^{24}$ does not provide any meaningful information but we can change our approach and look at the cosets of some set within the Leech lattice. The easiest lattice contained in Λ_{24} is the double Leech lattice $2\Lambda_{24} = \{2x : x \in \Lambda_{24}\}$ and looking at its cosets within Λ_{24} will provide us with the right action. We will first need the following lemmas to define our action.

Lemma 4.33. $\Lambda_{24}/2\Lambda_{24} \cong \mathbb{F}_2^{24}$ *and there are* $2^{24} = 16777216$ *cosets of* Λ_{24} *in* $2\Lambda_{24}$.

Proof. This follows from the fact that Λ_{24} is a lattice and thus $\Lambda_{24} \cong \mathbb{Z}^{24}$. $\square$

Lemma 4.34. *If two short vectors x, y are contained in the same coset of $2\Lambda_{24}$ in Λ_{24}, then either*

$$y = \pm x \qquad or \qquad x \cdot y = 0 \text{ and } w(x), w(y) = 8$$

Proof. It is clear that $y = \pm x$ and x are in the same coset, so assume $y \neq \pm x$. We know that the minimal non-zero weight of a Leech lattice vector is 4, so it follows that the minimal non-zero weight of a vector in $2\Lambda_{24}$ is $2^2 \cdot 4 = 16$.

Since x and y are in the same coset we find $x - y \in 2\Lambda_{24}$ and $x + y = x - y + 2y \in 2\Lambda_{24}$. Therefore $w(x \pm y) = 0$ or $w(x \pm y) \geq 16$ but the first case does not occur since $y \neq \pm x$. Now look at the following inequality which follows from the definition of the inner product and the fact that x and y are short.

$$16 \leq w(x \pm y) = (x \pm y) \cdot (x \pm y) = w(x) + w(y) \pm 2(x \cdot y) \leq 16 \pm 2(x \cdot y)$$

It now follows easily that we must have $x \cdot y = 0$ and $w(x), w(y) = 8$. □

Remark 4.34.1. Two vectors $x, y \in \mathbb{R}^{24}$ are called perpendicular if $x \cdot y = 0$.

We see that two short vectors are not in the same coset except for negatives and perpendicular vectors of weight 8. This is very similar to the case of the cosets of $\mathcal{G}_{24}$ in $\mathbb{F}_2^{24}$ where disjoint words of weight 4 could be in the same coset. The set X of sextets we were interested in, corresponded exactly to the cosets with disjoint representatives of weight 4. The same will happen here and the set Y will exactly correspond to the cosets of $2\Lambda_{24}$ in Λ_{24} with perpendicular representatives of weight 8. We first count the number of these cosets.

Theorem 4.35. *There are 8292375 cosets of $2\Lambda_{24}$ in Λ_{24} whose minimal representative has weight 8.*

Proof. We know from Lemma 4.12 and 4.13 that there is one Leech lattice vector of weight 0, 196560 of weight 4 and 16773120 of weight 6. It follows from Lemma 4.34 that two of these vectors can only be in the same coset if they are each other's negatives. These short vectors are therefore contained in exactly

$$1 + \frac{196560}{2} + \frac{16773120}{2} = 8484841 \text{ cosets}$$

We move on to the short vectors of weight 8. They are not contained in any of the already found 8484841 cosets and two of them can only be contained in the same coset if they are perpendicular or each other's negatives. It is known from linear algebra that perpendicular vectors are linearly independent and since we work in $\mathbb{R}^{24}$, we can then at most have 24 vectors that are mutually perpendicular to each other. This means that together with their negatives, we can at most have 48 short vectors of weight 8 in the same coset. We know from Lemma 4.14 that there are 398034000 short vectors of weight 8, so the total number of cosets we have now found is at least

$$8484841 + \frac{398034000}{48} = 16777216 = 2^{24}.$$

So we have found all the cosets of $2\Lambda_{24}$ in Λ_{24} and we get that each of these $\frac{398034000}{48} = 8292375$ cosets contains exactly 48 vectors of weight 8. □

We can now finally define our set Y.

Definition 4.36. A set of 48 short vectors of weight 8 that are in the same coset $\Lambda_{24}/2\Lambda_{24}$ is called a *cross*. The set Y is the set of 8292375 crosses.

Remark 4.36.1. Every short vector of weight 8 is contained in a unique cross.

Unfortunately, there is no way to represent a cross with the MOG, so we will have to use words to describe the crosses. The following cross is often called the *standard cross*.

Example 4.37. Let v_i be the vector with an 8 in the i-th position and zeroes everywhere else. It is clear that $v_i \cdot v_j = 0$ for $i \neq j$, so $\{\pm v_1, \pm v_2, \ldots, \pm v_{24}\}$ forms a cross. We call this cross R and it consists of all 48 short vectors of characteristic $(8^1, 0^{23})$.

Another type of cross is the *sextet cross* which is related to the sextets in the previous chapter.

Example 4.38. Let T be a random sextet and look at the vectors of characteristic $(4^4, 0^{20})$ whose ± 4-positions form one of the tetrads in T. There are exactly $6 \cdot 2^4 = 96$ of them and it easy to check that they form two crosses. One containing the vectors with an even number of -4 coordinates and one containing the vectors with an odd number of -4 coordinates.

In general, it is not that hard to find a cross.

Example 4.39. Take a short vector x of weight 8. Now take random short vectors y of weight 4. If $x \pm 2y$ has weight 8, it is contained in the same cross as x. Continue doing this until you have 24 perpendicular vectors. Together with their negatives, they form a cross.

We can also look at the characteristics of the vectors in the same cross. It would be straightforward if only vectors with the same characteristic are contained in the same cross but this is not the case.

Lemma 4.40 ([CF09])**.** *The 8292375 crosses are classified as follows in regards to the characteristics of their vectors.*

Type	*Characteristics*	*Number of crosses*
Standard	$(8, 0^{23})$	1
Sextet	$(4^4, 0^{20})$	3542
Octad	$16\times\ (6, 2^7, 0^{16})$	48576
	$32\times\ (2^{16}, 0^8)$	
Triad	$6\times\ (5, 3^2, 1^{21})$	4145152
	$42\times\ (3^5, 1^{19})$	
Involution	$32\times\ (4^2, 2^8, 0^{14})$	1457280
	$16\times\ (2^{16}, 0^8)$	
Duum	$(4, 2^{12}, 0^{11})$	2637824

Proof. It is easy (but not short) to verify this claim with the numbers in Lemma 4.14 and following the approach mentioned in Example 4.39. For example, we have $v_1 + v_2 = 2v_3$ for the following Leech lattice vectors, so v_1 and v_2 are in the same cross.

v_1

−6	2		
2	2		
2	2		
2	2		

v_2

		2	2	2	2
		2	2	2	2
		2	2	2	2
		2	2	2	2

v_3

−3	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1

Applying this idea repeatedly will give that there are 16 vectors of characteristic $(6, 2^7, 0^{16})$ and 32 of characteristic $(2^{16}, 0^8)$ in this cross. The same can be done for all other types. □

Remark 4.40.1. The characteristic $(2^{16}, 0^8)$ is the only one contained in two different crosses, the octad and involution crosses. This might explain the statement in [Wil09] mentioned in Remark 4.29.1.

We will now define the action of Co_1 on the set Y of crosses that we will use for Iwasawa's lemma but we first look at the action of Co_0 on Y.

Lemma 4.41. *The action of Co_0 on the vectors of weight 8 induces a well-defined action of Co_0 on the crosses.*

Proof. This follows from the fact that f is linear, so $f(-x) = -f(x)$, and the fact that f is orthogonal, so for two perpendicular vectors $x, y \in \Lambda_{24}$ we also have that $f(x)$ and $f(y)$ are perpendicular. □

Corollary 4.42. *The action of Co_0 on the crosses induces a well-defined action of Co_1 on the crosses.*

Proof. Remember that $\mathrm{Co}_1 = \mathrm{Co}_0/\{\Psi(\mathbf{0}), \Psi(\mathbf{1})\}$, so we just have to check that the action of $\Psi(\mathbf{1})$ on the crosses is the identity. $\Psi(\mathbf{1})$ is just the map $x \mapsto -x$, so this follows from the fact that x and $-x$ are always in the same cross. □

We have now defined the actions of Co_0 and Co_1 on the crosses. One requirement was that $I = 2^{12}{:}\, M_{24}$ is the point stabiliser of one of these crosses for the action of Co_0. We check this requirement.

Lemma 4.43. *The point stabiliser $(Co_0)_R$ of the cross R, defined in Example 4.37, is the group $I = 2^{12}{:}\, M_{24}$.*

Proof. We know that R consists exactly of all short vectors of characteristic $(8^1, 0^{23})$, so clearly $I \subset (\mathrm{Co}_0)_R$. We also know from Remark 4.27.1 that I consists exactly of the monomial transformations that preserve Λ_{24}, so if the point stabiliser is bigger than I, we have some automorphism f which preserves Λ_{24} and R and is not a monomial transformation. This means that in its associated matrix there is some column, assume wlog the first one, with at least two non-zero entries. It then easily follows that $f(8, 0, \ldots, 0) \notin R$, so f does not preserve R. We conclude that $(\mathrm{Co}_0)_R = I$. □

4.5.2 Transitivity and the order of Co_0

Now all that is left to do is to verify all the conditions of Iwasawa's lemma for the action of Co_1 on the crosses we have just defined. One of the conditions is primitivity which requires transitivity, so we prove that first. For this, we will first look at the action of $I = 2^{12}\colon M_{24}$ on the crosses.

Lemma 4.44. *The orbits of the action of I on the crosses are exactly the types in Lemma 4.40.*

Proof. We know from Lemma 4.29 that the automorphisms in $I = 2^{12}\colon M_{24}$ preserve the characteristics of the weight 8 vectors, so it is clear that if two crosses are in the same orbit, they must have the same type.

Now take two random crosses of the same type. They then have representing elements x and y which have the same characteristic. We can also always choose x and y such that the characteristic is not $(2^{16}, 0^8)$. It then follows from Lemma 4.29 that x and y are in the same orbit for the action of $2^{12}\colon M_{24}$ on the short vectors, so it easily follows that the two corresponding crosses are in the same orbit for the action of $2^{12}\colon M_{24}$ on the crosses. This proves the claim. □

With this, we can prove the transitivity of Co_0, and therefore Co_1, on the crosses.

Theorem 4.45. *The action of Co_0 on the set Y of crosses is transitive.*

Proof. We have determined the orbits of the action of the subgroup $I \subset \mathrm{Co}_0$ on the crosses, so now we just have to find an automorphism that fuses these 6 orbits. An element that suffices is $\beta \in \mathrm{Co}_0$, defined in Example 4.21 as

$$\left(\begin{array}{c|c|c|c|c|c} -Bl & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & Bl & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & Bl & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & Bl & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & Bl & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & Bl \end{array}\right) \quad \text{where} \quad Bl = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

The following 6 short vectors of weight 8 are representatives of the 6 types of crosses, one for each cross. Calculating the images of these vectors, and subsequently their crosses, is enough to verify that the 6 orbits are fused by β, so Co_0 is transitive on the crosses.

8		

4 4 4 4		

−6 2 2 2	2 2 2 2	

2	2	2	2	4
2	2	2	2	
4				

2	4	2		2
	2		2	2
	2		2	2
	2		2	2

3	3	3	3	3	1
1	1	1	1	1	−1
1	1	1	1	1	−1
1	1	1	1	1	−1

□

An important consequence of the transitivity of Co_0 on the crosses is that we can now finally calculate the order of Co_0.

Corollary 4.46. *The order of Co_0 is 8 315 553 613 086 720 000.*

Proof. Applying the orbit-stabiliser theorem on the action of Co_0 on the crosses, together with the information of Lemma 4.43 and Theorem 4.45 gives us the following equation.

$$\begin{aligned}|\mathrm{Co}_0| &= (\mathrm{Co}_0)_R \cdot (\mathrm{Co}_0 R) = |2^{12}{:}\, M_{24}| \cdot |Y| = 2^{12} \cdot 2448230 \cdot 8292375 \\ &= 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 8\,315\,553\,613\,086\,720\,000\end{aligned}$$

□

Remark 4.46.1. It follows immediately that

$$|\mathrm{Co}_1| = \frac{|\mathrm{Co}_0|}{2} = 4\,157\,776\,806\,543\,360\,000$$

4.6 Simplicity of Co_1

We will spend this last section on verifying the other conditions of Iwasawa's lemma. First of all, we have to check that Co_1 acts primitively on the crosses which is equivalent to Co_0 acting primitively on the crosses.

Theorem 4.47. *The action of Co_0 on the crosses is primitive.*

Proof. Our approach is identical to the proof of Theorem 3.40. First note that we already know that Co_0 acts transitively. Now assume Co_0 does not act primitively on the crosses. Then there is some non-trivial partition of Y that is preserved by Co_0. Since Co_0 acts transitively, the standard sextet R can not be contained in a singleton set and is contained in some imprimitivity block P. There is at least one other cross in P, call it Q. It then follows from Lemma 4.44 that all crosses of the same type as Q are contained in P since for $f \in I$ we have

$$\{R, f(Q)\} = \{f(R), f(Q)\} \subset f(P)$$

So $f(P) \cap P \neq \emptyset$ and therefore $f(P) = P$ and $f(Q) \in P$ for all $f \in I$. We can now also see that the automorphism β is contained in the stabilisers of the crosses with the following representatives.

4		
4		
4		
4		

2	−6		
2	2		
2	2		
2	2		

5	−3	−3	−3	−3	−3
−3	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1

4	2	2	2	2
−4	2	2	2	2
	−2	−2	−2	−2
	−2	−2	−2	−2

2	4	2		
2		2		
2			2	2
−2			2	2

We can check this by verifying that $x - \beta(x) \in 2\Lambda_{24}$ for these 5 vectors. Just like in Theorem 3.40, we can deduce from this that for each type, there is a cross in P and therefore all crosses are in P which contradicts the fact that P is an imprimitivity block. We conclude that Co_0 acts primitively on the crosses. □

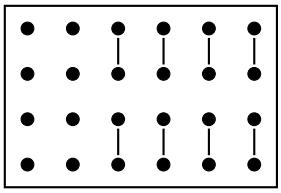
We now have three conditions left to check. Namely that the conjugates of B' generate Co_1, that Co_1 is perfect and that the action of Co_1 on Y is faithful. We now check the first of these three which is equivalent with the conjugates of B generating Co_0. Therefore, we define the following group.

Definition 4.48. U is the subgroup of Co_0 generated by the conjugates of $B = 2^{12}$.

We now check the condition that U is equal to Co_0. We first prove the following lemma.

Lemma 4.49. *The subgroup $I = 2^{12}{:}M_{24}$ is contained in U.*

Proof. Let $f = \psi(00\,11\,11) \in M_{24}$ and look at the element $\Phi(f) \in I$ and the sextet cross S defined by the following short vector of weight 8.



4		
4		
4		
4		

Note that the cross S consists of the 48 vectors which contain four ± 4's in one column of which an even number are $+4$'s and an even number are -4's. It is easy to check that $\Phi(f)$ is contained in the stabiliser $(\mathrm{Co}_0)_S$.

Since Co_0 is transitive on the crosses, the point stabilisers are conjugates and we get that $\Phi(f)$ is the conjugate of some element in I. We will show that it is the conjugate of an element in B. For this, We look at the action of $\Phi(f)$ on the vectors in S. It can be checked that for each vector $x \in S$, we have $\Phi(f)(x) = \pm x$, so it either preserves x or swaps it with its negative but it does not swap x with one of the perpendicular vectors to x. It therefore acts as a

sign change and this action is identical to the action of $\mathrm{Im}(\Psi) = B \subset I$ on the vectors of the standard cross R. It follows that $\Phi(f)$ is the conjugate of some element in B, so $\Phi(f) \in U$.

It is easy to check for conjugates $g \in M_{24}$ of f that $\Phi(g)$ is a conjugate of $\Phi(f)$ and therefore $\Phi(g) \in U$ since U is closed under conjugation. Since M_{24} is simple and f is not contained in the centre of M_{24}, we get that the conjugates of f generate M_{24} and we get $\mathrm{Im}(\Phi) \subset U$. By definition we also have $\mathrm{Im}(\Psi) \subset U$, so it follows from Theorem 4.27 that $I \subset U$. □

We can now prove that $U = \mathrm{Co}_0$.

Lemma 4.50. *The conjugates of B generate Co_0.*

Proof. It is easy to check that $\beta \in \mathrm{Co}_0$ from Example 4.21 is also contained in the stabiliser of the cross S from the proof of the previous lemma and that it also acts like sign changes on the vectors in S. We conclude that β is also a conjugate of some element in B and therefore $\beta \in U$, so together with Lemma 4.49 it follows that $\langle I, \beta \rangle \subset U$.

We can prove that $\langle I, \beta \rangle$ acts transitively on the crosses with the same ideas as in the proof of Theorem 4.45, so it follows with the orbit-stabiliser theorem that $|\langle I, \beta \rangle| = |\mathrm{Co}_0|$ and therefore

$$\mathrm{Co}_0 = \langle I, \beta \rangle \subset U$$

We conclude that $U = \mathrm{Co}_0$. □

We now check that Co_1 is perfect which is equivalent to Co_0 being perfect. This follows quite easily from the fact that the conjugates of B generate Co_0.

Lemma 4.51. *The group Co_0 is perfect.*

Proof. We first prove that all elements of B are commutators. The following equality holds for $u \in \mathcal{G}_{24}$ and $f \in M_{24}$.

$$[\Psi(u), \Phi(f)] = \Psi(u)\Phi(f)\Psi(u)^{-1}\Phi(f)^{-1} = \Psi(u + f^{-1}(u))$$

It is easy to see that every element of $\mathcal{G}_{24}$ can be written as $u + f^{-1}(u)$ for some $u \in \mathcal{G}_{24}$ and $f \in M_{24}$, so it follows that $B = \mathrm{Im}(\Psi) \subset [\mathrm{Co}_0, \mathrm{Co}_0]$. We know that conjugates of commutators are also commutators, so it follows that $\mathrm{Co}_0 = U \subset [\mathrm{Co}_0, \mathrm{Co}_0]$ and Co_0 is perfect. □

Lastly, we have to check that Co_1 acts faithfully on the crosses.

Lemma 4.52. *The action of Co_1 on the set Y of crosses is faithful.*

Proof. This is equivalent to $\Psi(\mathbf{0})$ and $\Psi(\mathbf{1})$ being the only elements that preserve all the crosses for the action of Co_0 on the crosses. So assume some $f \in \mathrm{Co}_0$ preserves all the crosses and is not one of these two elements.

Since f preserves the standard cross R we get $f \in (\mathrm{Co}_0)_R = I = 2^{12}{:}\, M_{24}$. So f is of the form $\Psi(u) \circ \Phi(g)$ for some $u \in \mathcal{G}_{24}$ and $g \in M_{24}$. By looking at

the action of f on all the sextet crosses, we can conclude that g must preserve all the sextets but we know from Lemma 3.45 that M_{24} acts faithfully on the sextets, so g is the identity and $f = \Psi(u)$.

It now also follows from Example 4.38 that u must intersect each tetrad in each sextet in an even number of positions since otherwise the even and odd cross corresponding to a sextet are swapped by f. However, since $u \neq \mathbf{0}, \mathbf{1}$, we can easily choose some tetrad that intersects u in an odd number of positions and then f does not preserve the corresponding sextet crosses. We conclude that such an f does not exist, so Co_1 acts faithfully on the crosses. □

We have now checked all the conditions of Iwasawa's lemma and can apply it to prove the simplicity of Co_1.

Theorem 4.53. *Co_1 is a simple group.*

Proof. We apply Iwasawa's lemma where Y is the set of crosses, $I' = 2^{11}{:}\, M_{24}$ and $B' = 2^{11}$. The verified conditions are then as follows.

1. Co_1 is finite (Remark 4.20.1) and perfect (Lemma 4.51).
2. The action of Co_1 on Y is faithful (Lemma 4.52) and primitive (Theorem 4.47).
3. I' is a point stabiliser (Lemma 4.43) with a normal, abelian subgroup B' (Theorem 4.27).
4. The conjugates of B' generate Co_1 (Lemma 4.50).

We conclude that Co_1 is simple. □

This wraps up our exploration of the Leech lattice and the main part of this thesis.

5 Conclusion

Over the course of this thesis, we have gone from the very easy to state sphere packing problem to error-correcting linear codes, lattices and finite simple groups. We first studied sphere packings and lattice packings and looked at the recent developments in answering the sphere packing problem which motivated our choice to study the Leech lattice Λ_{24}.

Next, we gave an introduction to the study of linear codes and their connections to sphere packings. We examined the hexacode $\mathcal{H}_6$ and binary Golay code $\mathcal{G}_{24}$ which is built from the hexacode and determined their sizes, weight distributions, a basis and their automorphism groups. For the Golay code, we introduced the Miracle Octad Generator which is a type of notation that is crucial to master for anyone interested in the Leech lattice and related topics.

The next step was to study the automorphism group M_{24} of the Golay code. We first looked at the subgroup $2^6{:}\,3\cdot S_6$ which we built from $\mathrm{Aut}(\mathcal{H}_6)$. Afterwards, we set our goal to prove the simplicity of M_{24}. Our strategy for this was to apply Iwasawa's lemma on a suitable action of M_{24} on some set. We constructed an action of M_{24} on the sextets, sets of six disjoint weight 4 vectors contained in the same coset of $\mathcal{G}_{24}$ in $\mathbb{F}_2^{24}$. We verified all the conditions of Iwasawa's lemma and on the way, we calculated the order of M_{24}.

We then set our sights on the Leech lattice, the crown jewel of this thesis. We defined it using the Golay code and started translating concepts of linear codes to lattices. While doing this, our study of Λ_{24} became pretty straightforward since we just followed the strategy for the Golay code but with some little adjustments. We found a basis of the Leech lattice and characterised the minimal and short vectors.

Lastly, we studied the automorphism group $\mathrm{Aut}(\Lambda_{24}) = \mathrm{Co}_0$ and specifically the subgroup $2^{12}{:}\,M_{24}$ built from the Mathieu group M_{24}. We defined the quotient group Co_1 and went on to prove the simplicity of this group. We did this by applying Iwasawa's lemma on the action of Co_1 on the set of crosses, sets of 48 weight 8 vectors contained in the same coset of $2\Lambda_{24}$ in Λ_{24}. We verified all the conditions, calculated the order of Co_0 and Co_1 and concluded this thesis with the simplicity of Co_1.

This forms the end of our investigation of the Leech lattice but there is far more one can learn about it. An obvious next step is to study the proof that the Leech lattice packing is the densest 24-dimensional sphere packing. This was proven in 2017, see [CKM$^+$17]. As mentioned previously, this proof makes use of modular forms. Another option if one is interested in sphere packings is to study the lattice E_8 which produces the densest 8-dimensional sphere packing. This lattice is related to the Leech lattice and its automorphism group is also a very special simple, although not sporadic, group that has applications in theoretical physics.

If the reader is interested in finite simple groups, we recommend studying many of the sporadic groups that are contained in M_{24} and Co_1 as subgroups. An overview can be found in Appendix C and another valuable resource is the

ATLAS of finite simple groups, see [CCN$^+$85] and [WWT$^+$]. Another option is to build upwards and construct a sporadic group containing Co_1. This way, the king of sporadic groups, the monster group M, can be constructed using a maximal subgroup that is an extension of Co_1, see [Con85] and section 5.8 in [Wil09].

Lastly, we can study the connections of the Leech lattice Λ_{24} to other objects and areas of mathematics we have not mentioned yet. One of the most important of these is studying M_{24}, Co_1 and the monster group with representation theory. Furthermore, aside from using modular forms to prove the optimality of the Leech lattice packing, there is a much deeper connection between modular functions and Co_1 and more importantly, the monster group. These two areas are connected by the theory of vertex algebras, which also have applications in physics. This connection was first conjectured in 1978 when the mathematician John McKay noticed a relationship between the coefficients of the Fourier expansion of some special modular function and the dimensions of representations of the monster group. This connection was coined 'monstrous moonshine', see [CN79], and it was eventually proven by the American mathematician Richard Borcherds using the monster vertex algebra, see [Bor92]. All of this goes far beyond this thesis but we mention this to make it apparent to the reader that this is a rich topic of which we have barely scratched the surface.

It is also entirely possible that another construction of the Leech lattice or another connection to a different mathematical area will be found in the (near) future since most of the advancements in this subject have taken place in just the past 50 years. There are still many mysteries surrounding the Leech lattice and related objects, most notably the monster group. For example, there is a statement about Riemann surfaces that only holds for the prime factors of the order of the monster group, see [Ogg75]. This potential connection has still not been explained. John Conway, one of the most influential mathematicians in the study of finite simple groups, has said the following about the monster group in 2014, see [Har14].

> There's never been any kind of explanation of why it's there, and it's obviously not there just by coincidence. It's got too many intriguing properties for it all to be just an accident.

We therefore encourage everyone interested in this topic to explore it further and potentially make contributions to this field of study.

References

[And12] Ivan Andrus. The Periodic Table Of Finite Simple Groups. `https://irandrus.files.wordpress.com/2012/06/periodic-table-of-groups.pdf`, 2012. Accessed: 11-07-2021.

[AS04a] Michael Aschbacher and Stephen D Smith. The Classification of Quasithin Groups: I. Structure of Strongly Quasithin K-groups. *Mathematical Surveys and Monographs*, 111, 2004.

[AS04b] Michael Aschbacher and Stephen D Smith. The Classification of Quasithin Groups: II. Main Theorems: The Classification of Simple QTKE-groups. *Mathematical Surveys and Monographs*, 112, 2004.

[Bor92] Richard E Borcherds. Monstrous moonshine and monstrous Lie superalgebras. *Inventiones mathematicae*, 109:405–444, 1992.

[Cam99] Peter J. Cameron. *Permutation Groups*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[CCN+85] John Horton Conway, Robert Turner Curtis, Simon Phillips Norton, Richard Alan Parker, and Robert Arnott Wilson. *ATLAS of Finite Groups*. Oxford University Press, Oxford, 1985.

[CF09] R.T. Curtis and B.T. Fairbairn. Symmetric representation of the elements of the Conway group 0. *Journal of Symbolic Computation*, 44(8):1044–1067, 2009.

[CKM+17] Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):1017–1033, 2017.

[CKM+19] Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska. Universal optimality of the E_8 and Leech lattices and interpolation formulas, 2019.

[CN79] J. H. Conway and S. P. Norton. Monstrous Moonshine. *Bulletin of the London Mathematical Society*, 11(3):308–339, 1979.

[Con68] J. H. Conway. A perfect group of order 8,315,553,613,086,720,000 and the sporadic simple groups. *Proceedings of the National Academy of Sciences*, 61(2):398–400, 1968.

[Con69] J. H. Conway. A Group of Order 8,315,553,613,086,720,000. *Bulletin of the London Mathematical Society*, 1(1):79–88, 1969.

[Con85] J. H Conway. A simple construction for the Fischer-Griess monster group. *Inventiones mathematicae*, 79(3):513–540, 1985.

[CS82] J. H. Conway and N. J. A. Sloane. Laminated Lattices. *Annals of Mathematics*, 116(3):593–620, 1982.

[CSdlH98] John Conway, Neil J. A Sloane, and P de la Harpe. *Sphere Packings, Lattices and Groups*, volume 290 of *Grundlehren der mathematischen Wissenschaften, A Series of Comprehensive Studies in Mathematics*. Springer New York, New York, NY, third edition, 1998.

[Cur76] R. T. Curtis. A new combinatorial approach to M24. *Mathematical Proceedings of the Cambridge Philosophical Society*, 79(1):25–42, 1976.

[Cur16] R.T. Curtis. Error-correction and the binary Golay code. *London Mathematical Society Impact150 Stories*, pages 51–58, 2016.

[Fis02] Robert F. H. Fischer. *Appendix C: Introduction to Lattices*, pages 421–437. 2002.

[FT42] László Fejes Tóth. Über die dichteste Kugellagerung. *Mathematische Zeitschrift*, 48(1):676–684, 1942.

[GLS94] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups*, volume 40.1 of *Mathematical Surveys and Monographs*. 1994.

[Gol49] Marcel Jules Edouard Golay. Notes on Digital Coding. *Proceedings of the IRE*, 37:657, 1949.

[Gri76] Robert L Griess. The structure of the "Monster" simple group. In William R. Scott and Fletcher Gross, editors, *Proceedings of the Conference on Finite Groups*, pages 113–118. Academic Press, 1976.

[Gri82] Robert L Griess. The friendly giant. *Inventiones mathematicae*, 69(1):1–102, 1982.

[Gri98] Robert L Griess. *Twelve Sporadic Groups*. Springer Monographs in Mathematics. Springer-Verlag Berlin Heidelberg, 1998.

[Hal05] Thomas C. Hales. A Proof of the Kepler Conjecture. *Annals of Mathematics*, 162(3):1065–1185, 2005.

[Har14] Brady Haran. Life, Death and the Monster (John Conway) - Numberphile. `https://www.youtube.com/watch?v=xOCe5HUObD4`, May 2014. Accessed: 12-07-2021.

[HMR19] Thomas Hartman, Dalimil Mazac, and Leonardo Rastelli. Sphere packing and quantum gravity. *Journal of High Energy Physics*, 2019(12), 2019.

[HS68] Donald G Higman and Charles C Sims. A simple group of order 44,352,000. *Mathematische Zeitschrift*, 105(2):110–113, 1968.

[HS08] Koichiro Harada and Ronald Solomon. Finite groups having a standard component L of type M_{12} or M_{22}. *Journal of Algebra*, 319(2):621–628, 2008.

[HW68] Marshall Hall and David Wales. The simple group of order 604,800. *Journal of Algebra*, 9(4):417–450, 1968.

[Isa08] I. Martin Isaacs. *Finite group theory*, volume 92 of *Graduate studies in mathematics*. American Mathematical Society, Providence, RI, 2008.

[Iwa41] Kenkiti Iwasawa. Über die Einfachheit der speziellen projektiven Gruppen. *Proceedings of the Imperial Academy*, 17(3):57 – 59, 1941.

[Jan66] Zvonimir Janko. A new finite simple group with abelian Sylow 2-subgroups and its characterization. *Journal of Algebra*, 3(2):147–186, 1966.

[Jan76] Zvonimir Janko. A new finite simple group of order 86 775 571 046 077 562880 which possesses $m24$ and the full covering group of $m22$ as subgroups. *Journal of Algebra*, 42(2):564–596, 1976.

[Kal13] Yoav Kallus. Statistical mechanics of the lattice sphere packing problem. *Physical review. E, Statistical, nonlinear, and soft matter physics*, 87:063307, 2013.

[KEG10] Yoav Kallus, Veit Elser, and Simon Gravel. Method for dense packing discovery. *Physical review. E, Statistical, nonlinear, and soft matter physics*, 82:056707, 2010.

[KP81] Padmanabhan Krishna and Dhananjai Pandey. Close-Packed Structures. *International union of crystallography commission on crystallographic teaching, first series pamphlets*, 5, 1981.

[Lee64] John Leech. Some Sphere Packings in Higher Space. *Canadian Journal of Mathematics*, 16:657–682, 1964.

[Lee67] John Leech. Notes on Sphere Packings. *Canadian Journal of Mathematics*, 19:251–267, 1967.

[Mat61] Émile Mathieu. Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables. *Journal de Mathématiques Pures et Appliquées*, 6:241–323, 1861.

[Mat73] Émile Mathieu. Sur la fonction cinq fois transitive de 24 quantités. *Journal de Mathématiques Pures et Appliquées*, 18:25–46, 1873.

[McL69] Jack McLaughlin. A simple group of order 898,128,000. In Richard Brauer, editor, *Theory of Finite Groups: A Symposium*, pages 109–111, 1969.

[Mil98] G.A. Miller. On the supposed five-fold transitive function of 24 elements and 19!/48 values. *Messenger of Mathematics*, 27:187–190, 1898.

[MT13] Etienne Marcotte and Salvatore Torquato. Efficient linear programming algorithm to generate the densest lattice sphere packings. *Physical review. E, Statistical, nonlinear, and soft matter physics*, 87:063303, 2013.

[Ogg75] Andrew P. Ogg. Automorphismes de courbes modulaires. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 16(1), 1974-1975.

[Slo02] N. J. A Sloane. The Sphere-Packing Problem. 2002.

[Ste17] P. Stevenhangen. *Algebra 1.* Leiden, 2017.

[Suz69] Michio Suzuki. A simple group of order 448,345,497,600. In Richard Brauer, editor, *Theory of Finite Groups: A Symposium*, pages 113–119, 1969.

[Tho83] Thomas M. Thompson. *From Error-correcting Codes Through Sphere Packings to Simple Groups.* Number no. 21 in The Carus Mathematical Monographs. Mathematical Association of America, 1983.

[Via17] Maryna S. Viazovska. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185(3):991–1015, 2017.

[Wil83] Robert Wilson. The complex leech lattice and maximal subgroups of the Suzuki group. *Journal of Algebra*, 84(1):151–188, 1983.

[Wil09] Robert Wilson. *The finite simple groups*. Graduate texts in mathematics. Springer, London [etc.], 2009.

[Wit37a] Ernst Witt. Die 5-fach transitiven Gruppen von Mathieu. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 12:256–264, 1937.

[Wit37b] Ernst Witt. über Steinersche Systeme. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 12:265–275, 1937.

[Wit98] Ernst Witt. *Collected Papers - Gesammelte Abhandlungen.* Springer-Verlag, Berlin, New York, 1998.

[WWT+] Robert Wilson, Peter Walsh, Jonathan Tripp, Ibrahim Suleiman, Richard Parker, Simon Norton, Simon Nickerson, Steve Linton, John Bray, and Rachel Abbott. ATLAS of Finite Group Representations. `http://brauer.maths.qmul.ac.uk/Atlas/v3/`. Accessed: 25-06-2021.

A Miscellaneous group theory

In this chapter, we give some necessary definitions in group theory that are used in various other proofs or explanations. We assume the reader has already followed a basic introduction to group theory. In this chapter, G is always a group, its identity element is e and we use 1 for the trivial group $\{e\}$. We mostly follow [Isa08] and [Ste17].

Definition A.1. Two elements $a, b \in G$ are said to be *conjugate* if there is some $g \in G$ such that $b = gag^{-1}$. If this is the case, we write $b = a^g$.

Definition A.2. A subgroup $H \subset G$ is called *normal* if it is preserved by conjugation, so $gHg^{-1} = H$ for all $g \in G$. If this is the case, we write $H \triangleleft G$.

Definition A.3. Let $H_1, H_2 \subset G$ be subgroups. The *product* of H_1 and H_2 is the set

$$H_1H_2 = \{h_1h_2 : h_1 \in H_1, h_2 \in H_2\}$$

Remark A.3.1. In most cases, H_1H_2 is not a subgroup but if H_2 and/or H_1 is normal in G, it is a subgroup since we have $H_1H_2 = \langle H_1, H_2\rangle$ in this case.

Definition A.4. An abelian grooup G is called an *elementary abelian group* if its order is a prime power p^k and all elements of $G \setminus \{e\}$ have order p. In this case, we write $G = p^k$.

Remark A.4.1. We have seen that the hexacode and the Golay code as additive groups are elementary abelian groups $\mathcal{H}_6 = 2^6$ and $\mathcal{G}_{24} = 2^{12}$.

We used the theory of semidirect products and short exact sequences for the groups $\mathrm{Aut}(\mathcal{H}_6) = 3\cdot A_6$ and $\mathrm{Aut}^*(\mathcal{H}_6) = 3\cdot S_6$ and the subgroups $2^6{:}\,3\cdot S_6 \subset M_{24}$ and $2^{12}{:}\,M_{24} \subset \mathrm{Co}_0$. We will now cover the part of this theory that we used.

Definition A.5. Let A, B, C be groups and $f : A \to B$ and $g : B \to C$ be group homomorphisms. The following sequence

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

is called a *short exact sequence* if f is injective, g is surjective and $\mathrm{Im}(f) = \ker(g)$. In this case, B is called an *extension* of C by A.

Definition A.6. The extension in Definition A.5 is *split* if there is some group homomorphism $s : C \to B$ such that $g \circ s$ is the identity on C. We denote a split extension by $A{:}\,C$ and a non-split extension by $A\cdot C$.

The easiest extension is of course the usual Cartesian product $A \times C$ with the group operation $(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1, x_2y_2)$. This is called the *direct product*. We look at a more interesting type of extension.

Definition A.7. Let N and H be groups and let a group action, see Definition B.6, of H on N be given. Let ${}^{h}n = \sigma(h)(n)$. The *semidirect product* of H acting on N is then the Cartesian product $N \times H$ with the following group operation.

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 {}^{h_1} n_2, h_1 h_2)$$

We denote this group with $N \rtimes_\sigma H$ or $N \rtimes H$ if the action is obvious.

The definition we have given is the outer semidirect product since the groups N and H are not related to each other. However, it often happens that these groups are contained in some larger group G which we want to be the extension of these 2 groups N and H. In these cases, there are extra relationships, so the definition is slightly different but equivalent.

Definition A.8. Let N and H be subgroups of G such that

- The intersection $N \cap H$ is trivial,
- The subgroup $N \lhd G$ is normal,
- The product NH is equal to G.

The group G is then called the *inner semidirect product* of H and N.

Remark A.8.1. It is an easy exercise to see that G is isomorphic to $N \rtimes_\sigma H$ where σ is the action of H on N given by conjugation as elements of G.

Remark A.8.2. It can be checked that every semidirect product $N \rtimes_\sigma H$ is a split extension of H by N and that every split extension of H by N is isomorphic to a semidirect product $H \rtimes_\sigma N$ for some action σ of H on N.

We look at an example of a semidirect product.

Example A.9. Identify S_3 and V_4 as subgroups of S_4 in the natural way so

$$S_3 = \{e, (12), (13), (23), (123), (132)\} \text{ and } V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

We clearly have $S_3 \cap V_4 = 1$ and it is easy to check that $V_4 S_3 = S_4$. Furthermore, it is easy to see that $V_4 \lhd S_4$ is a normal subgroup, so S_4 is an inner semidirect product of S_3 and V_4 and is therefore isomorphic to $V_4 \rtimes_\sigma S_3$ where σ is the action of S_3 on V_4 by applying conjugation as elements in S_4.

We now move on to the last topic in this chapter, commutators. We will use Corollary A.14 in the proof of Iwasawa's lemma, in Lemma B.20.

Definition A.10. Let elements $a, b \in G$ be given. The commutator of these two elements is given by

$$[a, b] = aba^{-1}b^{-1}$$

Remark A.10.1. Note that $[a, b] = e$ iff a and b commute.

Definition A.11. The commutator subgroup $[G, G]$ of G is the subgroup generated by all the commutators in G.

Remark A.11.1. The commutator subgroup $[G, G]$ is normal in G since conjugates of commutators are clearly commutators by the identity

$$[a, b]^g = [a^g, b^g]$$

Definition A.12. G is called *perfect* if $[G, G] = G$. In other words, if the commutators generate G.

Lemma A.13. *Let a normal subgroup $N \triangleleft G$ be given and assume the quotient group G/N is abelian. Then we have $[G, G] \subset N$.*

Proof. Look at the natural homomorphism $f : G \to G/N$. Since G/N is abelian, it follows easily that each commutator in G is contained in $\ker(f) = N$ because of the following equality.

$$f([x, y]) = f(x)f(y)f(x^{-1})f(y^{-1}) = f(x)f(x^{-1})f(y)f(y^{-1}) = f(e) = \overline{e}$$

So we conclude $[G, G] \subset N$. □

Corollary A.14. *Let G be a perfect group. Then there is no non-trivial abelian quotient group G/N.*

Proof. Assume a quotient group G/N is abelian. It follows from Lemma A.13 that $G = [G, G] \subset N$, so $G = N$ and $G/N = \{e\}$ is trivial. This proves the claim. □

We need one more group-theoretic result for the proof of Iwasawa's lemma.

Lemma A.15. *Let $N \triangleleft G$ be a normal subgroup and let $H \subset G$ be a subgroup. Then the following groups are isomorphic.*

$$H/(H \cap N) \cong HN/N$$

Proof. Restricting the quotient map $G \to G/N$ gives a map $H \to G/N$ with kernel $H \cap N$ and image HN/N. The claim follows. □

B Finite simple groups and actions

We prove in this thesis that M_{24} and Co_1 are finite simple groups. In this chapter, we will give more information about the topic of finite simple groups and show why this simple to state problem is such an interesting subject and occupied hundreds of mathematicians for decades. We also give a proof of Iwasawa's lemma which is our method for proving the simplicity of M_{24} and Co_1. We mostly follow Chapters 1 and 2 in [Wil09] and Chapter 1 in [Isa08].

B.1 Classification theorem of finite simple groups

A natural question that arises when working with any kind of object is 'What are all the different types of this object?'. In chemistry, this object can be molecules or in number theory, it can be the natural numbers $\mathbb{N}$. In both cases, we can reduce this problem by looking at their building blocks. So chemists look at atoms which make up molecules through bonding and number theorists look at prime numbers which make up the natural numbers by multiplication. We can then ask the same question for the groups. What are all the groups and what are their building blocks? It turns out that if we limit ourselves to finite groups, there is an answer to this question and the building blocks have the following property.

Definition B.1. A group G is *simple* if there is no non-trivial normal subgroup $1 \subsetneq N \subsetneq G$.

Finite groups are built from the finite simple groups in the following way.

Definition B.2. A *composition series* of a finite group G is a series

$$1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G_n = G$$

such that each quotient group G_{i+1}/G_i is non-trivial and simple. These quotient groups are called the *composition factors*.

Remark B.2.1. It is clear by definition that each finite group has a composition series. We start with $1 \triangleleft G$ and just insert arbitrary normal subgroups that fit into the series until it is not possible anymore which means that all the quotients at that point are simple.

We see that every finite group can be 'factorised' into finite simple groups like how natural numbers have a prime factorisation. Like the prime factorisation, the composition series of a finite simple group is unique. We will state this theorem without proof.

Theorem B.3 (Jordan-Hölder Theorem)**.** *The composition factors of the composition series of a finite group G are unique up to isomorphism and permutation.*

One difference with prime factorisation however, is that two non-isomorphic groups can have the same composition series up to isomorphism and permutation.

Now that we have seen that finite simple groups form the building blocks of all finite groups, we want to find or at least classify all finite simple groups. There is one very easy family of finite simple groups.

Lemma B.4. *The cyclic groups C_p of prime order are simple.*

Proof. The group C_p contains no non-trivial subgroup, so also certainly no non-trivial normal subgroup. □

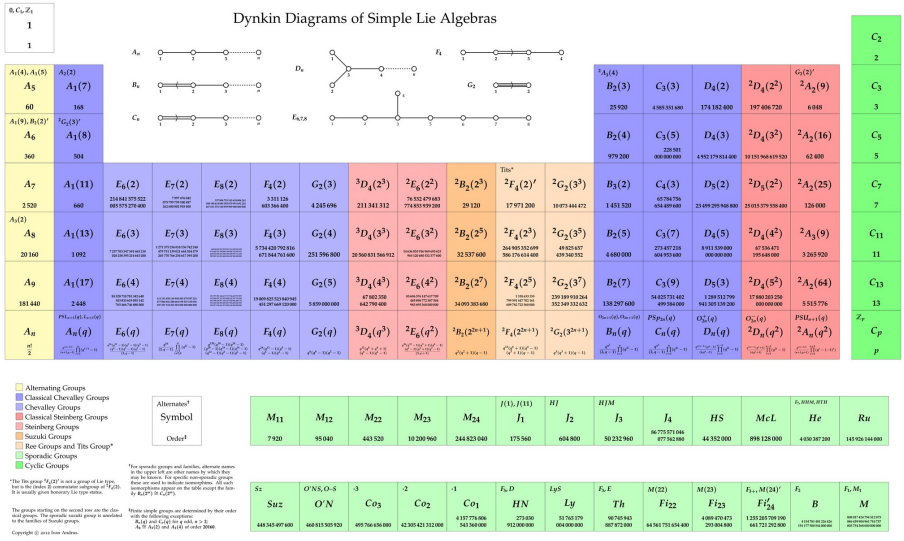
One more family of finite simple groups is the following.

Lemma B.5. *The alternating groups A_n are simple for $n \geq 5$.*

Proof. This is not quite as easy to prove. See [Wil09] for a proof. □

Besides these cyclic and alternating groups, there are many more finite simple groups that fit into such infinite families. It is beyond the scope of this thesis to cover these families but they are represented in the following figure, taken from [And12], which mimics the periodic table of elements in chemistry.

The Periodic Table Of Finite Simple Groups



There are 16 more families of finite simple groups, all of Lie type which we will not define here. There is some slight overlap between these 16 families but the idea is clear.

As you might have noticed, there are 26 more finite simple groups at the bottom of the figure which are not contained in an infinite family. These groups

are called the *sporadic* groups. The first sporadic groups that were discovered are the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24} which were discovered in the 19th century by the French mathematician Mathieu, see [Mat61] and [Mat73]. It was long thought that these were the only 'leftover' groups among the finite simple groups until almost a century later in 1965, the next sporadic group, the Janko group J_1, was discovered by the Croatian mathematician Zvonimir Janko and published a year later, see [Jan66]. All the remaining 20 sporadic groups were found in the next decade, ending with the publication of the Janko group J_4 in 1976, see [Jan76]. There are many relations between these sporadic groups which will be discussed further in Appendix C.

The next step was to prove that these groups are indeed all the finite simple groups which is called the classification theorem of finite simple groups. This theorem was extremely hard to prove and required proving many smaller theorems. The classification theorem was considered complete a few times but new gaps were found and resolved. In the end, it took tens of thousands of pages in hundreds of articles by about a hundred mathematicians. After a period of almost 50 years, the last big gap was resolved in 2004 by American mathematicians Aschbacher and Smith, see [AS04a] and [AS04b]. The Classification Theorem was one of the greatest achievements and biggest efforts of 20th-century mathematics.

There is no central publication that compiles all these proofs that together are called the first generation proof. A second generation proof that is shorter and more efficient is currently being published with 9 volumes (11, if counting the contributions from Aschbacher and Smith) already out as of 2021 and it is estimated that it will fill 5000 pages. This revision project was originally led by Daniel Gorenstein, see [GLS94] for the first volume. There are also still some sceptics of the completeness of the proof since not all parts of the proof have been intensively checked. The most recently found gap was resolved in 2008, see [HS08].

B.2 Actions

We will obviously not cover the proof of the classification theorem. We just focus on proving the simplicity of M_{24} and Co_1. There are numerous ways one can prove that a certain finite group is simple. The definition alone was enough to prove the simplicity of C_p and together with some calculation, it is also enough to prove the simplicity of A_n for $n \geq 5$. Usually, the definition alone is not enough and another lemma or theorem needs to be used.

One of the easiest of these is Iwasawa's lemma which will be stated and proved in section B.3. The statement and proof both require knowledge of group actions, so we will first spend a section on studying the relevant definitions and ideas for group actions.

Definition B.6. A *group action* of a group G on some set X is a group homomorphism $\sigma : G \to S(X)$ where $S(X)$ consists of all bijections from X to X. We denote $\sigma(g)(x)$ with $g(x)$ for $g \in G$ and $x \in X$.

Remark B.6.1. The following rules must hold for a group action.

$$e(x) = x \text{ for all } x \in X \quad \text{and} \quad (gh)(x) = g(h(x)) \text{ for all } g, h \in G \text{ and } x \in X$$

We can look at some easy examples.

Example B.7. S_n acts on a set of n points in a natural way. The cyclic group C_n acts on a regular n-gon as the n rotations that preserve this figure.

There are some sets and subgroups that are related to group actions.

Definition B.8. The *orbit* of an element $x \in X$ under a group action of a group G on X is the set

$$Gx = \{g(x) : g \in G\} \subset X$$

So the elements that can be reached from x by applying the group action.

Remark B.8.1. The set X is partitioned into disjoint orbits.

Definition B.9. The *point stabiliser* of an element $x \in X$ is the subgroup

$$G_x = \{g \in G : g(x) = x\} \subset G$$

So the group elements that preserve x.

There is a special relationship between orbits and stabilisers since it is trivial to see that the map $g \mapsto g(x)$ induces a bijection $G/G_x \to Gx$. An immediate consequence is the following famous fact called the *orbit-stabiliser theorem*.

Lemma B.10. *Let a finite group G act on some set X. We then have the following equality.*

$$|G| = |Gx| \cdot |G_x|$$

We now look at some properties a group action can have. In all these cases, we look at the action of a group G on a set X where $\sigma : G \to S(X)$ is the corresponding homomorphism.

Definition B.11. A group action is called *faithful* if σ is injective. In other words, only the element $e \in G$ preserves every element of X.

Definition B.12. A group action is called *transitive* if for some $x \in X$ we have $Gx = X$, so the set X consists of exactly one orbit. This is equivalent with saying that for every $x, y \in X$, there exists some $g \in G$ such that $g(x) = y$.

Transitivity makes the orbits easier to study since there is only one of them but it also makes the stabiliser more useful because of the following fact.

Lemma B.13. *The point stabilisers for a transitive group action are all conjugates and therefore isomorphic.*

Proof. Let $x, y \in X$ be arbitrarily given. Since the group action is transitive we have some $g \in G$ such that $g(x) = y$. It is now easy to see that $G_y = gG_xg^{-1}$. □

We can now also generalise the concept of transitivity.

Definition B.14. A group action is called *n-transitive* if for all distinct $x_1, x_2, \ldots, x_n \in X$ and distinct (but not necesarilly distinct with the previous elements) $y_1, y_2, \ldots, y_n \in X$, there exists some $g \in G$ such that

$$g(x_i) = y_i \text{ for all } 1 \leq i \leq n$$

Example B.15. S_n is n-transitive and A_n is $(n-2)$-transitive

There is another important property that is stronger than transitivity but weaker than 2-transitivity.

Definition B.16. A transitive group action is called *primitive* if there is no non-trivial partition of X that is preserved by all elements of G. So for every non-trivial partition and elements x, y in the same set, there exists a $g \in G$ such that $g(x)$ and $g(y)$ are not in the same set of the partition.

Remark B.16.1. The trivial partitions are the partitions

$$\{X\} \quad \text{and} \quad \{\{x_1\}, \{x_2\}, \ldots\}$$

So taking the whole group or taking all the singleton subsets.

We can define primitivity in a more useful way with the following definition.

Definition B.17. A proper non-singleton subset $B \subsetneq X$ is called an *imprimitivity block* if for all $g \in G$ we have either $g(B) = B$ or $g(B) \cap B = \emptyset$.

Remark B.17.1. It is easy to see that a group action is primitive iff there is no imprimitivity block.

The last thing we will do before moving to Iwasawa's lemma is proving that the point stabilisers for a primitive group action have the following group-theoretic property.

Definition B.18. A subgroup $H \subset G$ is called *maximal* if there is no subgroup $H \subsetneq G' \subsetneq G$.

Lemma B.19. *The point stabilisers of a primitive group action are maximal.*

Proof. The group action is primitive and therefore transitive. It follows from Lemma B.13 that we can look at a specific point stabiliser, so let an arbitrary $x \in X$ be given and look at the point stabiliser G_x.

Assume that G_x is not maximal, so there exists a subgroup $G_x \subsetneq H \subsetneq G$. Now let $B = \{h(x) : h \in H\}$. We will prove that $B = X$. First assume that $B \neq X$, we will show that B is an imprimitivity block which contradicts the primitivity of the group action.

First note that $G_x \subsetneq H$, so B is not a singleton set. Now let $g \in G$ be arbitrarily given and assume that B and $g(B)$ are not disjoint. Then there exist some $h_1, h_2 \in H$ such that $h_1(x) = (gh_2)(x)$ but it easily follows from this that

$$h_2^{-1} g h_1 \in G_x \subset H$$

so $g \in H$ and $g(B) = B$. We see that B is an imprimitivity block which is not possible.

We conclude that $B = X$. We now have for all $g \in G$ that $g(x) \in X = B$, so there is some $h \in H$ such that $g(x) = h(x)$. It then follows that

$$h^{-1} g \in G_x \subset H$$

so $g \in H$. We see that $H = G$ which contradicts $H \subsetneq G$. We conclude that G_x is a maximal subgroup of G. □

B.3 Iwasawa's lemma

We can now finally state and prove Iwasawa's lemma which was first used in 1941, see [Iwa41], to prove the simplicity of certain projective groups.

Lemma B.20 (Iwasawa's Lemma)**.** *Let G be a group that meets the following conditions.*

1. *G is finite and perfect.*
2. *G acts primitively and faithfully on some set X.*
3. *The point stabiliser H contains a normal, abelian subgroup A.*
4. *The conjugates of A generate G.*

Then G is simple.

Proof. We prove by contradiction that G is simple if all the conditions are met. So assume G is not simple and meets all the conditions. We will use all the conditions to construct a non-trivial abelian quotient group of G which is in contradiction with the fact that G is perfect because of Corollary A.14.

We start with the non-simplicity of G from which follows that there is a non-trivial normal subgroup $N \triangleleft G$. Since $N \neq 1$, it contains at least one element $n \neq e$ and then there must be some $x \in X$ such that $n(x) \neq x$ since the action of G on X is faithful. Since the action is primitive and therefore transitive, we can choose a specific point stabiliser and we take $H = G_x$. Note that now $N \nsubseteq H$.

Since N is normal, we know from Remark A.3.1 that HN is a subgroup of G such that $H \subsetneq HN$ since N is not contained in H. We also know that H is maximal from Lemma B.19, so it follows that $G = HN$ and every element $g \in G$ can be written as $g = hn$ with $h \in H$ and $n \in N$.

We now look at the conjugates of A who generate G. It now follows from the fact that $A \triangleleft H$ is normal in H, $N \triangleleft G$ is normal in G, and Remark A.3.1

that every conjugate of A is of the following form for some $g \in G$, $h \in H$ and $n \in N$.

$$g^{-1}Ag = n^{-1}h^{-1}Ahn = n^{-1}An \subset \langle A, N \rangle = AN$$

So the conjugates of A are all contained in the subgroup $AN \subset G$ and since they generate G we get $G = AN$.

We look at the quotient group G/N and it follows from Lemma A.15 that

$$G/N = AN/N \cong A/(A \cap N)$$

Since A is abelian, it follows that the quotient group G/N is abelian and this quotient group is non-trivial since N was a proper subgroup of G. It follows from Corollary A.14 that G is not perfect which was one of the conditions, so we get a contradiction. We conclude that any group G meeting the conditions must be simple. $\square$

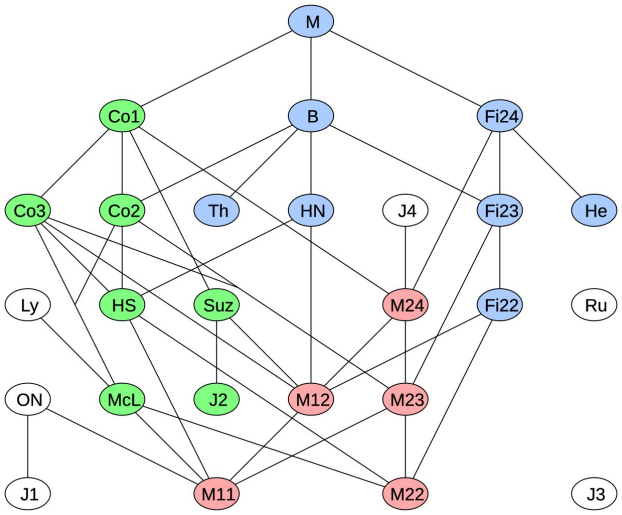
C More finite simple groups

This chapter is meant for anyone that is curious about the other sporadic groups. We mostly follow sections 5.2-5.6 in [Wil09]. As we mentioned, there are many relations between these sporadic groups. We define the type of relation we consider.

Definition C.1. A *subquotient* of a group G is a quotient group of a subgroup of G.

Example C.2. The Conway group Co_1 contains a subgroup $I' = 2^{11}{:}M_{24}$ which clearly has a quotient group isomorphic to M_{24}, so M_{24} is a subquotient of Co_1.

The subquotient-relations between the sporadic groups are depicted in the following figure where G is connected with a lower group H if it contains a subquotient N isomorphic to H and there is no simple subquotient in between N and G.



The red nodes are the Mathieu groups, the first discovered simple groups. They are often called the first generation. The green nodes are the second generation consisting of the subquotients of Co_1 that are not subquotients of M_{24}. The third generation are the blue nodes which are the subquotients of the Monster group M that are not subquotients of Co_1. Together, the 20 groups of the three generations are called the happy family while the 6 groups of the white nodes are called the pariahs.

In this chapter, we will not prove all these subquotient relationships but we will just define the other 10 sporadic groups (besides M_{24} and Co_1) in the first and second generation in a way that relates them to M_{24} and Co_1. We will not prove that these groups are simple but these proofs can be found in [Wil09] and in most cases are similar to our proofs for the simplicity of M_{24} and Co_1.

C.1 Mathieu groups

We start with the first generation, so the Mathieu groups, first discovered by Mathieu, see [Mat61] and [Mat73]. When Mathieu first discovered these groups, many mathematicians did not believe him and some even tried to disprove him, see [Mil98]. The doubts were removed when the German mathematician Witt constructed the Mathieu groups in two different ways, see [Wit37a] and [Wit37b]. The latter constructed them as the automorphism groups of Steiner systems which is one of the other ways to construct the Golay code, see Remark C.6.1.

We will define M_{23}, M_{22}, M_{12} and M_{11} as subgroups of M_{24} and determine their orders. On the way, we will also show and need some properties of the actions of the Mathieu groups on certain sets related to $\mathcal{G}_{24}$. The first property we will need is the 5-transitivity of M_{24} acting on 24 points, specifically the action on the 24 MOG positions. We first prove the following.

Lemma C.3. *M_{24} acts 4-transitively on 24 points.*

Proof. Let points $x_1, \ldots, x_4$ and $y_1, \ldots, y_4$ be given like in the definition of n-transitivity. We interpret them as MOG positions and let T_x and T_y be the tetrads containing respectively $x_1, \ldots, x_4$ and $y_1, \ldots, y_4$. Let S_x and S_y be the corresponding sextets.

We know from Lemma 3.38 that M_{24} acts transitively on the sextets, so there is some $f \in M_{24}$ such that $f(S_x) = S_y$. Furthermore, it is easy to see that the stabiliser $2^6{:}\,3 \cdot S_6$ of the standard sextet K with columns as tetrads is transitive on these columns/tetrads. Since the action is transitive, all sextet stabilisers are conjugates and therefore this property also holds for the stabiliser of S_y, we can therefore assume that also $f(T_x) = T_y$ since if not, we can compose it with an automorphism that sends $f(T_x)$ to T_y. We therefore know that

$$f(\{x_1, x_2, x_3, x_4\}) = \{y_1, y_2, y_3, y_4\}$$

Now we just need to show that the tetrad stabiliser of T_y acts like an S_4 on $\{y_1, y_2, y_3, y_4\}$. Since the actions on the sextets and tetrads are transitive we can look at a specific tetrad. We take the first column in the sextet K. With elements of $\mathrm{Im}(\psi)$ we can clearly achieve the permutations e, (12)(34), (13)(24) and (14)(23) on the 4 points in the tetrads. Furthermore, the automorphism $\varphi^*(t)$, from Example 3.19 gives the permutation (34) and scalar muliplication gives (234). These together generate S_4. So we can compose f with some automorphism g such that $g(f(x_i)) = y_i$ and we conclude that the action of M_{24} on 24 points is 4-transitive. □

We can now prove the 5-transitivity of M_{24} acting on 24 points.

Lemma C.4. *M_{24} acts 5-transitively on 24 points.*

Proof. Let $x_1, \ldots, x_5$ and $y_1, \ldots, y_5$ be given like in the definition of n-transitivity. Since M_{24} acts 4-transitively there is some $f \in M_{24}$ such that $f(x_i) = y_i$ for $1 \leq i \leq 4$. Now we just need to show that the point-wise stabiliser of $\{y_1, \ldots, y_4\}$

acts transitively on the remaining 20 points since then we can compose f with an automorphism g that preserves $y_1, \ldots, y_4$ and sends $f(x_5)$ to y_5.

Because of the 4-transitivity of M_{24}. We can look wlog at 4 specific points. We choose the points in the third column. Now we want to permute $f(x_5)$ to y_5 while preserving these 4 points. If $f(x_5)$ is not in the same column as y_5, we can permute it to the same column by applying double flips, permutations of the column pairs and the automorphism $\varphi(s)$ from Example 3.17. Now $f(x_5)$ is in the same column as y_5 and it follows easily that we can apply an automorphism of the form $\psi(aa\,00\,aa)$ for some $a \in \mathbb{F}_4$. □

An immediate consequence of this is that $|M_{24}|$ needs to be divisible by $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20$ which we saw in Remark 3.39.1. Another consequence is that we can define the following groups.

Definition C.5. For $1 \leq k \leq 5$, we define the group M_{24-k} as the stabiliser of k points for the action of M_{24} on 24 points.

The following statements are known about these 5 groups. The orders of the group follow from the fact that $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$

- M_{19} is not simple and has order 48.
- M_{20} is isomorphic to $2^4{:}\,A_5$. It is not simple and has order 960.
- M_{21} has order 20160 and is simple but not sporadic.
- M_{22} and M_{23} are simple sporadic groups and their orders are 443520 and 10200960 respectively.

Proofs of the simplicity using Iwasawa's lemma on a suitable action can be found in [Wil09].

Another useful result that follows from the 5-transitivity on points is the following.

Lemma C.6. *For every 5 points in the MOG, there is a unique octad that has one-coordinates in these 5 positions.*

Proof. It follows easily from the 5-transitivity that every 5 points can be extended to an octad. This way we find at least

$$\binom{24}{5} \Big/ \binom{8}{5} = 759 \text{ octads}$$

Once again everything falls into place since there are exactly 759 octads in $\mathcal{G}_{24}$, so every 5 points are contained in a unique octad. □

Remark C.6.1. The octads are said to form a $S(5, 8, 24)$ *Steiner system* by interpreting the octads as subsets of 24 points containing exactly the points corresponding to one-coordinates. In this way, every 5 points are contained in a unique subset of size 8. More about this property can be found in Chapter 5 of [Gri98].

The following important result that we used in the proof of Lemma 4.12 now follows.

Lemma C.7. *M_{24} acts transitively on the octads.*

Proof. For any two octads O_1 and O_2, there is an element f of M_{24} that permutes 5 one-coordinates of O_1 to 5 one-coordinates in O_2. Since M_{24} preserves weight of Golay codewords and there is a unique octad containing 5 points, we conclude $f(O_1) = O_2$, so the action of M_{24} on octads is transitive. □

We now move on to M_{12} and M_{11} which are called the small Mathieu groups. They were actually discovered by Mathieu before the large Mathieu groups and M_{12} can be constructed as the automorphism group of the ternary Golay code, which is a subspace of $\mathbb{F}_3^{12}$ built from a ternary tetracode instead of the quaternary hexacode for the binary Golay code and M_{24}. There even is a miniMOG which is a special 4×3-array for calculations in the ternary Golay code and M_{12}.

We will however construct it as a subgroup of M_{24} but more about the other construction can be found in [CSdlH98]. It can be proven that M_{24} is also transitive on the duodecads, the 2576 Golay codewords of weight 12, so we can define the following group.

Definition C.8. The group M_{12} is the duodecad stabiliser for the action of M_{24} on the duodecads. It has order $\frac{|M_{24}|}{2576} = 95040$.

It can be proven that M_{12} acts 5-transitively on the 12 points not in the duodecad. This can be proven most easily with the other construction of M_{12}. These multiply transitive groups are extremely rare. In fact, M_{24} and M_{12} are the only finite groups not of the form S_n or A_n with a 5-transitive action, see [Cam99]. This is also how Mathieu discovered these groups since he was trying to construct multiply transitive groups, see [Mat61] and [Mat73]. Because of the 5-transitivity we can also define the following groups.

Definition C.9. For $1 \leq k \leq 5$, we define the group M_{12-k} as the stabiliser of k points for the action of M_{12} on 12 points.

The following is known about these 5 groups where the orders come from the fact that $|M_{12}| = 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$.

- M_7, M_8, M_9 and M_{10} are not simple and have orders 1, 8, 72 and 720 respectively. M_8 is isomorphic to the quaternion group and M_{10} is isomorphic to a non-split extension $2 \cdot A_6$.
- M_{11} is a simple sporadic group of order 7920.

This finishes the first generation of sporadic groups.

C.2 Conway groups

We move on to the second generation of the sporadic groups. In this section, we will define the sporadic group Co_2 and Co_3 as subgroups of Co_0. They were discovered together with Co_1 by Conway, see [Con68] and [Con69]. We need the following lemmas to define these groups.

Lemma C.10. *Co_0 acts transitively on the short vectors of weight 4.*

Proof. We know from Lemma 4.29 that the orbits of the action of $2^{12}{:}M_{24}$ on the short vectors of weight 4 are just the characteristics, so $(4^2, 0^{22})$, $(2^8, 0^{16})$ and $(3, 1^{23})$. We look at the automorphism $\beta \in \mathrm{Co}_0$, defined in Example 4.21 as

$$\left(\begin{array}{c|c|c|c|c|c} -Bl & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & Bl & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & Bl & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & Bl & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & Bl & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & Bl \end{array}\right) \quad \text{where} \quad Bl = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

It follows easily from looking at the images under β of the following three Leech lattice vectors of weight 4 that the three characteristic orbits are fused by β and that therefore Co_0 acts transitively on the short vectors of weight 4.

$$\begin{array}{|cc|cc|} \hline 4 & 4 & & \\ & & & \\ & & & \\ & & & \\ \hline \end{array} \qquad \begin{array}{|cc|cc|c|} \hline 2 & 2 & 2 & 2 & 2 \\ & & & & & 2 \\ & & & & & 2 \\ & & & & & 2 \\ \hline \end{array} \qquad \begin{array}{|cc|cc|cc|} \hline -3 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ \hline \end{array}$$

□

Lemma C.11. *Co_0 acts transitively on the short vectors of weight 6.*

Proof. The proof is analogous to the proof of Lemma C.10. So with the same automorphism $\beta \in \mathrm{Co}_0$ but with different Leech lattice vectors whose images show that the orbits for the action of $2^{12}{:}M_{24}$ are fused by β. □

We can now define the 2 other simple sporadic Conway groups found by John Conway, see [Con68] and [Con69]. As with all the other simple groups in this chapter, a proof of their simplicity can be found in [Wil09].

Definition C.12. The stabiliser for the action of Co_0 on Λ_{24} of a short vector of weight 4 is called the *second Conway group* Co_2.

Definition C.13. The stabiliser for the action of Co_0 on Λ_{24} of a short vector of weight 6 is called the *third Conway group* Co_3.

We can then also calculate the orders of these two groups with the orbit-stabiliser theorem and the fact that these actions are transitive. It follows from

Lemma 4.12 and 4.13 that

$$|\mathrm{Co}_2| = \frac{|\mathrm{Co}_0|}{196560} = 42\,305\,421\,312\,000 = 2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$
$$|\mathrm{Co}_3| = \frac{|\mathrm{Co}_0|}{16773120} = 495\,766\,656\,000 = 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$

C.3 Other groups

In this last section, we will cover the remaining 4 sporadic groups from the 2nd generation and also mention the Monster group M. All lemmas and properties of these groups will be stated without proof since these proofs are more complex and not the focus of this thesis.

We will first construct the Higman-Sims group HS and the McLaughlin group McL as subgroups of Co_3. These two groups were originally constructed in different ways, see [HS68] and [McL69]. We need the following lemma for the Higman-Sims group.

Lemma C.14. *Let Co_3 be the stabiliser of a Leech lattice vector v of weight 6. There are exactly 11178 short vectors u of weight 4 such that $u \cdot v = -2$. The action of Co_3 on these vectors is transitive.*

Definition C.15. Let $u, v \in \Lambda_{24}$ such that $w(v) = 6$, $w(u) = 4$ and $u \cdot v = -2$. Then the Higman-Sims group is the stabiliser

$$\mathrm{HS} = ((\mathrm{Co}_0)_v)_u = (\mathrm{Co}_3)_u$$

Remark C.15.1. The order of this group is

$$|\mathrm{HS}| = \frac{|\mathrm{Co}_3|}{11178} = 44352000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$$

The McLaughlin group is defined in a very similar way.

Lemma C.16. *Let Co_3 be the stabiliser of a Leech lattice vector v of weight 6. There are exactly 552 short vectors u of weight 4 such that $u \cdot v = -3$. The action of Co_3 on these vectors is transitive.*

Definition C.17. Let $u, v \in \Lambda_{24}$ such that $w(v) = 6$, $w(u) = 4$ and $u \cdot v = -3$. Then the McLaughlin group is the stabiliser

$$\mathrm{McL} = ((\mathrm{Co}_0)_v)_u = (\mathrm{Co}_3)_u$$

Remark C.17.1. The order of this group is

$$|\mathrm{McL}| = \frac{|\mathrm{Co}_3|}{552} = 898128000 = 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$$

The remaining 2 simple sporadic groups of the 2nd generation are the Suzuki group Suz and the second Janko group J_2, also called the Hall-Janko group HJ.

They were first defined in 1969 and 1968 respectively, see [Suz69] and [HW68]. They were constructed independently from the Leech lattice but can be defined as subquotients of Co_1, specifically, there are subgroups of Co_1 isomorphic to $(A_5 \times \mathrm{J}_2){:}\,2$ and $3 \cdot \mathrm{Suz}\,{:}\,2$. We do not have the necessary prerequisites however for this construction.

We can however sketch a conceptually more interesting way to construct these groups. This method involves a complex lattice over the Eisenstein integers.

Definition C.18. Let $\zeta \in \mathbb{C}$ be the element $e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{3}i}{2}$. The *Eisenstein integers* are then the ring $\mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\}$.

Now we need the ternary Golay code, the same one we mentioned while discussing M_{12}. In the same way we constructed a lattice in $\mathbb{Z}^{24}$ based on the binary Golay code, we can construct a complex lattice in $\mathbb{Z}[\zeta]^{12}$ based on the ternary Golay code. The automorphism group of this lattice is the extension $6 \cdot \mathrm{Suz}$ and Suz contains the extension $\mathrm{J}_2{:}\,2$ as a maximal subgroup, see [Wil83]. This concludes our exposition of the 2nd generation simple sporadic groups.

We now quickly mention the 3rd generation of simple sporadic groups without going into the details. By far the largest sporadic group is the monster group M which has order

$$\begin{aligned}&808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000\\ &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71\end{aligned}$$

Out of the 26 sporadic groups, 20 are subquotients of M. The monster group was first predicted to exist in 1973 (unpublished) by Bernd Fischer and in 1976 by Robert Griess, see [Gri76]. The first construction was given by Griess in 1982, see [Gri82]. The monster group has even more fascinating properties than the Mathieu and Conway groups and as mentioned in the conclusion, is a good next step if one is interested in finite simple groups.