Sporadic Groups and Where to Find Them

Lectures by Theo Johnson-Freyd

Canada/USA Mathcamp, July 24–26, 2019

Day 1: Preliminaries

1.1 All the finite simple groups

This class is like going to a zoo or a natural history museum. My goal is to show you most of the sporadic simple groups in their natural habitats. But, like a zoo or natural history museum, I might give a slightly simplified version of the science.

The sporadic groups are the magical beasts of the finite group world. Before we can talk about them, we should talk about the ordinary finite groups. Most finite groups in nature are solvable. Solvable groups are the insects of the finite group world: lots of them, lots of variety, hard to classify, not very exciting. The simple groups are the mammals. Even for the simple groups, most of them are deer or rabbits: pretty normal everyday things that you see a lot. Maybe "muggle groups" is a better name.

The list of all finite simple groups goes:

Muggle groups: These groups all come in infinite families. Most of their behaviour is systematic.

- Cyclic groups of prime order. These are both solvable and simple. They are very boring. Let's ignore them.
- Alternating groups A_n for $n \geq 5$.
- Groups of Lie type. Most of them.

Sporadic groups: These groups come in finite families.

- Mathieu groups. We will construct these groups in the second lecture.
- Leech groups. Third lecture.
- Monstrous groups. Third lecture.
- Pariahs. The other three sets are together the "happy family." "Pariah" is another word for "outcast." We won't talk about these in this class because we don't have the time. About one of these (the third Janko group), Wikipedia writes "J_3 seems unrelated to any other sporadic groups (or to anything else)."

There is also one "squib": the Tits group ${}^2F_4(\mathbb{F}_2)'$ is of "Lie type" for the usual definition, but it lacks some structural properties (namely, a "BN pair") that the other muggle groups (and the Mathieu groups) share.

What is a "Lie type" group? Recall that

Definition. *A field is a set with "addition" and "multiplication" satisfying all usual rules.*

Examples. Some important fields are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is prime. There are other finite fields. For example, -1 is not a square mod 3, and so there is a field $\mathbb{F}_9 = \mathbb{F}_3[\sqrt{-1}]$, just like $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$.

If you work mod 2, then $-1 = +1$ is a square, and so $\mathbb{F}_2[\sqrt{-1}]$ is not a field. But there is no solution mod 2 to $\omega^2 + \omega + 1 = 0$, and so

$$\mathbb{F}_4 = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1 = 0)$$

is a field of order 4. It will be important later. You can think of ω as the complex number $\exp(2\pi i/3)$. Then $\omega^2 = \bar{\omega}$ is its complex conjugate, and we will use complex conjugation on $\mathbb{F}_4$ a bit. As a set, $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$.

Nonexamples. The quaternions $\mathbb{H}$ are important, but they are not a field. $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is not a prime.

The ingredients needed to give a finite simple group of Lie type are a finite field and also a simple Lie group. Actually, what you need is a simple algebraic group. Here is a quasi-definition:

Definition. *An algebraic group is a group of matrices where you haven't decided what field to use for the coefficients of the matrix.*

If you have an algebraic group $\mathcal{G}$, and a field $\mathbb{F}$, then you get an ordinary group $\mathcal{G}(\mathbb{F})$ by declaring that you will use $\mathbb{F}$ for the coefficients of the matrix.

Examples.

$$\mathrm{SL}_n = \{X \text{ an } n \times n \text{ matrix s.t. } \det(X) = 1\}$$
$$\mathrm{O}_n = \{X \text{ an } n \times n \text{ matrix s.t. } X^T X = 1\}$$

It is a good exercise to show that these are both groups.

Nonexamples. The group $\mathrm{SL}_2(\mathbb{R})$ has a double cover $2\mathrm{SL}_2(\mathbb{R})$, analogous to the spin double of $\mathrm{SO}_3(\mathbb{R})$ that I showed in the colloquium. But there is no algebraic group $2\mathrm{SL}_2$, because there is no (nontrivial) double cover $2\mathrm{SL}_2(\mathbb{C})$ of $\mathrm{SL}_2(\mathbb{C})$.

Just like for finite groups, most algebraic groups are solvable, and the rare important ones are simple. There is an ABCDEFG classification of simple algebraic groups which you might have learned if you took the class on root systems earlier this summer. I said already how it works in my colloquium. For any Dynkin diagram (ABCDEFG), you build a lattice L, perhaps together with some decoration called "folding," and then study a string theory with target the dual torus $\mathbb{R}^r/L$, and ask for its automorphisms, and then the magical thing is that actually that string theory is totally algebraic, making sense over any field, so that the answer is an algebraic group (and in fact a simple algebraic group if you start with a simple Dynkin diagram). I won't say more now, but we'll return to this in the last lecture.

Anyway, that gives you the list of simple algebraic groups $\mathcal{G}$. If $\mathcal{G}$ is an algebraic group and $\mathbb{F}$ is a finite field, then $\mathcal{G}(\mathbb{F})$ is a finite group (because there are only finitely many matrices with coefficients in $\mathbb{F}$). If $\mathcal{G}$ is simple, then $\mathcal{G}(\mathbb{F})$ wants to be simple. It actually usually isn't quite simple. First, it might just be too small, and fall apart into a solvable mess. But the main thing that happens is that it isn't simple, but that its derived subgroup $\mathcal{G}(\mathbb{F})'$ — the subgroup generated by commutators $xyx^{-1}y^{-1}$ (warning! the set of commutators is not a subgroup) — is simple. These are the groups of Lie type. More or less,

Definition. *A finite simple group of Lie type is a simple group of the form $\mathcal{G}(\mathbb{F})'$, or you can also decorate a bit where you twist by some automorphisms, but we won't discuss that in this class.*

1.2 The Hexacode

Let $\mathbb{F}$ be a field.

Definition. *A linear code over $\mathbb{F}$ of length n is a vector subspace $\mathcal{C} \subset \mathbb{F}^n$. A word is an element of $\mathbb{F}^n$ (a letter is an element of $\mathbb{F}$), and a code word is an element of $\mathcal{C}$.*

There is a remarkable linear code called the hexacode $\mathcal{C}_6$. It has length 6, hence the name, and it is defined over $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$. I'll write the words in $\mathbb{F}_4^6$, which have length 6, by breaking the letters into blocks of length 2: $ab\,cd\,ef$.

$$\mathcal{C}_6 = \mathrm{Span}\{\omega\bar{\omega}\,\omega\bar{\omega}\,\omega\bar{\omega},\ \bar{\omega}\omega\,\bar{\omega}\omega\,\omega\bar{\omega},\ \bar{\omega}\omega\,\omega\bar{\omega}\,\bar{\omega}\omega,\ \omega\bar{\omega}\,\bar{\omega}\omega\,\bar{\omega}\omega\}.$$

Actually, those four words are linearly dependent — this is not a basis — but any three of them are linearly independent, so $\dim \mathcal{C}_6 = 3$.

Now, here's the cool fact.

Lemma. *Consider the hermitian inner product on $\mathbb{F}_4^6$ defined by $\langle v, v' \rangle = \bar{v} \cdot v' \in \mathbb{F}_4$, where $\cdot$ is the algebraic inner product $v \cdot v' = \sum_{i=1}^6 v_i v_i'$, and $\bar{v}$ is the componentwise complex conjugate of the word v, i.e. $\overline{ab\,cd\,ef} = \bar{a}\bar{b}\,\bar{c}\bar{d}\,\bar{e}\bar{f}$.*

$$\langle v, v' \rangle = 0 \in \mathbb{F}_4 \quad \forall v, v' \in \mathcal{C}_6.$$

Proof. Check it on a basis. [Do an example in class.] □

Corollary. *$v \in \mathcal{C}_6$ iff $\langle v, v' \rangle = 0\ \forall v' \in \mathcal{C}_6$.*

Proof. $\dim \mathcal{C}_6 = 3$. □

Using the Lemma, one can give a recognition principle for hexacode words. A word is in $\mathcal{C}_6$ if and only if it satisfies both

Shape rule Let $0, a, b, c$ be all-different elements of $\mathbb{F}_4$. Then the word should have one of the following shapes:

$$00\,00\,00, \quad 00\,aa\,aa, \quad aa\,bb\,cc, \quad bc\,bc\,bc \quad 0a\,0a\,bc$$

or anything you can get from these shapes by permuting the blocks, or by reversing a pair of blocks.

Sign rule For each block, write down a sign in $\{0, +, -\}$. The rule is: $\mathrm{sign}(00) = 0$, and if $x \neq 0$ then $\mathrm{sign}(0x) = +$, $\mathrm{sign}(x0) = -$, and if $x, y \neq 0$ then $\mathrm{sign}(xy) = \log_\omega y/x$. I mean it is 0 if $y = x$, $+$ if $y = \omega x$, and $-$ if $y = \bar{\omega} x$. Then the signs of the word should be 000 or $+++$ or $+--$ or $-+-$ or $--+$.

[Campers call out words more or less at random, and we check if they are codewords.]

The hexacode has some pretty awesome error correction properties. The zeroth of these is the Lemma above, and the first is that all nonzero hexacode words have at least four nonzero entries. What do I mean by "error correction"? Algebraic coding theory arose in the early 20th century. The question was: you want to send a signal — we're not going to worry about eavesdroppers or anything, but we do worry about noisy channels. Normally, when you can't hear someone on a cell-phone, you get static — you know you missed the signal. So that's one type of noise. Another problem is when a signal comes in, and you think you hear one thing, and the sender sent another. That's even more dangerous. In any case, the goal is to have a code where there's some redundancy built in, so that you can recover from noisy signals, but you also want it to be efficient. For the hexacode, the results are:

Proposition. *A hexacode word can be recovered from any three of its letters — ab?c?? — and any three letters determines a unique hexacode word. Furthermore, any five letters,* one of which might be wrong*, determines a hexacode word.*

[Proof by example.]

Now, this is a class on finite groups, and finally we will meet a slightly-exceptional finite group. What is the group $\mathrm{Aut}(\mathcal{C}_6)$ of automorphisms of the hexacode? An automorphism of a linear code $\mathcal{C} \subset \mathbb{F}^n$ consists of a permutation of the n coordinates, together with multiplying coordinates by nonzero numbers, such that it preserves $\mathcal{C}$ as a set.

I.e. $\mathrm{Aut}(\mathcal{C}) \subset (\mathbb{F}^\times)^n \rtimes S_n$. Note that for $\mathbb{F} = \mathbb{F}_q$ a finite field, $\mathbb{F}^\times \cong C_{q-1}$ is a cyclic group. Cyclic groups are usually written in group theory just by their order, so $\mathrm{Aut}(\mathcal{C}_6) \subset 3^6 \rtimes S_6$.

A few symmetries of $\mathcal{C}_6$ are manifest from the above rules: we can permute the blocks (and don't multiply anything), giving a subgroup $S_3 \subset \mathrm{Aut}(\mathcal{C}_6)$ (in terms of the six coordinates, the order-3 element therein acts as (135)(246)); we can switch any pair of blocks, giving a Klein-4 subgroup $2^2 \subset \mathrm{Aut}(\mathcal{C}_6)$ (e.g. (12)(34)). These two subgroups do not commute, but instead compile to a semidirect product $2^2 \rtimes S_3$.

Exercise: $2^2 \rtimes S_3 \cong S_4$.

Actually, this is part of an amazing fact about the number 6. Look at the hexacode words with no 0s in them. The action by $\mathrm{Aut}(\mathcal{C}_6)$ preserves them as a set. Up to scale, there are 6 of them: two like $aa\,bb\,cc$ (either $b = \omega a$ and $c = \bar{\omega} a$ or $b = \bar{\omega} a$ and $c = \omega a$); and four coming from $bc\,bc\,bc$. Then in addition to the coordinates, these six things are permuted by $\mathrm{Aut}(\mathcal{C}_6)$, and the subgroup $2^2 \rtimes S_3 \cong S_4 \subset \mathrm{Aut}(\mathcal{C}_6)$ acts in the usual way on the set of size 4, and by the "sign" action on the set of size 2.

Anyway, there are more symmetries. For example:

Lemma. $\mathrm{Aut}(\mathcal{C}_6)$ *contains the order-*3 *symmetry which first multiplies the columns by* $\omega, \bar{\omega}, 1, \omega, \bar{\omega}, 1$*, and then applies the permutation* (135)(264)*. I mean:*

$$ab\,cd\,ef \mapsto (\bar{\omega} e)(\omega d)\,(\omega a) f\,c(\bar{\omega} b).$$

Proof. Check that it sends some basis to hexacode words. □

Corollary. $\mathrm{Aut}(\mathcal{C}_6)$ *contains — in fact, it is equal to — a nontrivial triple cover* $3A_6$*.*

Proof. Looking just at the permutation-part, the above symmetry together with $2^2 \rtimes S_3 \cong S_4$ generate the group A_6. But choose an order-3 element of $2^2 \rtimes S_3 \cong S_4$, e.g. $g = (135)(246)$, and write h for the above symmetry; then just in terms of permutations g and h commute, but in fact $gh = \omega hg$, where here $\omega \in \mathrm{Aut}(\mathcal{C}_6)$ means the symmetry that rescales every word by ω. □

This is truly remarkable: the only two alternating groups to have a nontrivial triple cover are A_6 and A_7. So we are already seeing some exceptional behaviour.

Another exceptional phenomenon: we already remarked that $\mathrm{Aut}(\mathcal{C}_6)$ acts on two different sets of size 6, namely the coordinates and the no-zeros hexacode words. In fact, these two actions determine an *outer* automorphism of A_6, and it is not the one coming from S_6. This is the only alternating group with an "extra" outer automorphism.

If you allow complex conjugation, then the automorphism group extends to $3S_6$. Again, the existence of a group "$3S_6$," and the fact that it has actions on two *different* sets of size 6, are both exceptional.

Day 2: Golay's binary code

Yesterday we described the hexacode $\mathcal{C}_6$ over $\mathbb{F}_4$. Our goal today will be to describe Golay's binary code $\mathcal{C}_{24}$, which is a very exceptional linear code over $\mathbb{F}_2$. I'll tell you already: $\mathrm{Aut}(\mathcal{C}_{24}) = \mathrm{M}_{24}$ is the largest Mathieu group, and we will see all the other Mathieu groups as subgroups of M_{24}. Mathieu was interested in highly transitive groups, and showed that other than the symmetric and alternating groups, the only "highly transitive" groups were his exceptional series. $\mathcal{C}_{24}$ gives an alternative method to these groups. I won't describe the way Golay found $\mathcal{C}_{24}$: the version I will give is due to Curtis from the 1970s.

To describe it, I want to mention how I will write words. The length of the words is 24, and I'll arrange them in a 4×6 grid. The rows of the grid will be labeled by the set $\{0, 1, \omega, \bar{\omega}\}$, and the columns by the six coordinates of $\mathcal{C}_6$l. The letters are $\mathbb{F}_2$, which I will think of as the set $\{\emptyset, *\}$: I either draw a "pip" or I don't. So for example

	a	b	c	d	e	f
0	*	*	*			
1				*		
ω				*		*
$\bar{\omega}$		*				

is a word (not a codeword!). Now, to tell you the codewords, again I will have two rules. The **shape rule** says: the column sums should be a hexacode word. It's clear what I mean by column sums? For instance, the above column sums are $0\bar{\omega}\,0\bar{\omega}\,0\omega$, so the above word violates the shape rule. The **sign rule** says: all the columns, and also the top row, have the same number of pips mod 2. So the above word also violates the sign rule.

Exercise: Show that $\mathcal{C}_{24}$ is linear. All this requires is to show that it is closed under + (mod 2), because a closed subspace of $\mathbb{F}_p^n$ is automatically an abelian group, and an abelian subspace is automatically a vector subspace.

How many Golay codewords are there? Well, there are 4^3 hexacode words, because $\dim_{\mathbb{F}_4} \mathcal{C}_6 = 3$. And each letter can be interpreted as a column in 4 different ways, except if I choose "all evens" then I only get 2, and "all odds" is only 2, so if I just apply the sign rule to the columns then I get $(2^6 + 2^6) \times 4^3$ words. Except applying also to the top row forces, for instance, the last column: either it needs a pip in the north east spot, or it needs that spot to be empty, and exactly one of the options will work. So all together $\#\mathcal{C}_{24} = 2^6 \times 4^3 = 2^{12}$. So $\dim \mathcal{C}_{24} = 12$. The following results are not too hard, and follow from the analogues for $\mathcal{C}_6$:

Proposition. *1. $\mathcal{C}_{24}$ is <u>self-dual</u>: $v \in \mathcal{C}_{24}$ iff $v \cdot v' = 0$ $\forall v' \in \mathcal{C}_{24}$.*

2. Define the <u>weight</u> of a word to be its number of pips. The weight of any Golay codeword is divisible by 4, and (other than the empty word) it is always at least 8.

This already gives you a hint that it will have good error correcting properties. For instance:

Proposition. *An <u>octad</u> is a Golay code word of weight 8 (i.e. it has eight pips). Any word of weight 5 completes to a unique octad.*

[Proof by example.]

Definition. $\mathrm{M}_{24} = \mathrm{Aut}(\mathcal{C}_{24}) \subset S_{24}$.

Let's list some subgroups of M_{24}. They will turn out to be maximal, although I won't prove that.

- We built M_{24} from $\mathcal{C}_6$, and remember that $\mathrm{Aut}(\mathcal{C}_6) = 3A_6$, extending to $3S_6$ if you allow complex conjugation, which just reverses the bottom two rows, so is a symmetry. So $3S_6 \subset \mathrm{M}_{24}$. Moreover, if you take any hexacode word $ab\,cd\,ef$, then you can permute the first column by $x \mapsto x + a$, the second by $x \mapsto x + b$, and so on, and this is also a symmetry. As an abelian group, $\mathcal{C}_6 \cong \mathbb{F}_4^3 \cong \mathbb{F}_2^6$, so all together we get a subgroup $2^6 \rtimes 3S_6 \subset \mathrm{M}_{24}$.

- Choose any octad, for example

*	*				
*	*				
*	*				
*	*				

  It turns out that they are all isomorphic under the M_{24} action. The stabilizer (set-wise) of an octad turns out to have shape $2^4 \rtimes \mathrm{GL}_4(\mathbb{F}_2)$. It permutes the eight inhabited cells through an exceptional (!) isomorphism $\mathrm{GL}_4(\mathbb{F}_2) \cong A_8$ (and 2^4 acts trivially). (See, most groups of Lie type and most alternating groups are just themselves, but every once in a while they happen to be isomorphic to each other.) The empty cells can be identified with the abelian group $\mathbb{F}_4^2 \cong \mathbb{F}_2^4$, and $\mathrm{GL}_4(\mathbb{F}_2)$ acts by matrix multiplication on that set, and 2^4 acts by vector addition.

- Who knows some projective geometry? Consider the projective line $\mathbb{P}^1(\mathbb{F}_{23}) = \mathbb{F}_{23} \cup \{\infty\} = \{\infty, 0, 1, 2, \ldots, 22\}$. It has order $\#\mathbb{P}^1(\mathbb{F}_{23}) = 24$. It's acted on by the group $\mathrm{PSL}_2(\mathbb{F}_{23})$, the quotient of $\mathrm{SL}_2(\mathbb{F}_{23})$ by the central subgroup $\left\{\left(\begin{smallmatrix}1 & \\ & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & \\ & -1\end{smallmatrix}\right)\right\}$, via fractional linear transformations:
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : x \mapsto \frac{ax + b}{cx + d}.$$
  Note that you might have to divide by zero, but that's OK because I'm former staff, and in any case Apurva is supervising. **Exercise:** You will never get stuck with $0/0$.

  Define $Q = \{\text{squares}\} = \{0, 1, 4, 9, \ldots\} \subset \mathbb{F}_{23} \subset \mathbb{P}^1(\mathbb{F}_{23})$. (We will decide that ∞ is not a square.) Note that $-1 \notin Q$, so either $+x$ or $-x \in Q$, but not both. Now number the grid by

0		1		2	
	3		4		-5
	6		-7		8
	9		-10		-11

  where you put a sign in to make sure that you only used squares. Also identify $\left(\begin{smallmatrix}& 1\\ -1 & \end{smallmatrix}\right) : x \mapsto -1/x$ with the permutation that switches the middle two rows, and for the columns acts as $(12)(36)(45)$. This lets you fill in the rest of the grid. ($x \in Q$ iff $-1/x \notin Q$.)

  With this identification between $\mathbb{P}^1(\mathbb{F}_{23})$ and the cells in the grid, you find that $\mathrm{PSL}_2(\mathbb{F}_{23}) \subset \mathrm{M}_{24}$.

- Fix one cell — M_{24} is transitive, so it doesn't matter which one. M_{23} is by definition the stabilizer of a point in M_{24}. Who took the group cohomology class? The early cohomology M_{23} vanishes a lot more than for any other finite group. M_{23} acts on the remaining 23 elements. Define a septad as a set of seven pips among those 23 cells extending to an octad if

you add the fixed cell. The septads form the Steiner system for M_{23}, if you know what that is.

- The stabilizer pointwise of a pair of points — it doesn't matter which, by highly-transitivity — is M_{22}. It is another Mathieu group. You can get a Steiner system by declaring sextads to be sets that become octads when you add the other two points. If you just want to stabilizer a pair of points setwise, then you get $M_{22} \rtimes 2$.
- Fix three points. You will get, by pattern recognition, the group M_{21}, extending to $M_{21} \rtimes S_3$ if you permute the three points. Actually, M_{22} and M_{23} are sporadic, but M_{21} is merely exceptional. See, $21 = \#\mathbb{P}^2(\mathbb{F}_4) = 4^2 + 4 + 1$, and you can think of the other three points as $\mathbb{F}_4^\times$. It turns out that $M_{21} \cong \mathrm{PSL}_3(\mathbb{F}_4)$, acting by "fractional linear transformations" on the projective plane $\mathbb{P}^2(\mathbb{F}_4)$, and this extends first to $\mathrm{PGL}_3(\mathbb{F}_4) = \mathrm{PSL}_3(\mathbb{F}_4) \rtimes 3$ and then to $\mathrm{PGL}_3(\mathbb{F}_4) \rtimes (\text{c.c.}) = M_{21} \rtimes S_3$.
- If you pick a dodecad, then its (setwise) stabilizer is M_{12}, extending to $M_{12} \rtimes 2$ upon allowing to reverse the dodecad with its complement. The smaller Mathieu groups are M_{11} — the stabilizer of a point inside a dodecad — and M_{10} — two points. Actually, M_{12} and M_{11} are sporadic, but M_{10} is merely exceptional. In fact, $M_{10} \cong A_6 \cdot 2$, the extension by the outer automorphism we discussed yesterday.

Day 3: Quantization and Gauging

Yesterday, we constructed the first generation of the Happy Family: the Mathieu groups. Today we will construct the second and third generations. You will be able to do the second generation completely rigorously. For the third generation, I'll ask you to take my word for some facts: I'll outline the most direct, most natural construction, but to do it rigorously takes about 500 pages.

3.1 Leech groups

Yesterday we constructed Golay's binary code $\mathcal{C}_{24}$. Today we'll use it to construct the Leech lattice, and then use the Leech lattice to construct the Monster. We will need three facts about $\mathcal{C}_{24}$:

1. It is self-dual.
2. Its words all have weight $4k$.
3. It has no words of weight 4.

Now let me give the idea of the construction of the Leech lattice, and then we'll do it rigorously. The construction takes two steps. The first step is a **quantization** step, and then we **gauge a symmetry**. See, $\mathcal{C}_{24}$ is an object from classical information theory: it is a code made out of classical bits. What is a bit? It is a thing which can be in either of two distinct states. The quantization step replaces bits by qubits. What's a qubit? In quantum mechanics, you are allowed to take superpositions of quantum states, and a qubit is a thing which can be in any superposition of two states. So the states in a qubit form the vector space $\mathbb{C}^2$, with basis the two states of the bit. Actually, a state in quantum mechanics is determined only up to "phase," so actually you get the projective space $\mathbb{P}(\mathbb{C}^2)$ consisting of lines (through the origin) in $\mathbb{C}^2$. The symmetries of the qubit $\mathbb{P}(\mathbb{C}^2)$ is $\mathrm{PSL}_2(\mathbb{C})$, whereas the symmetries of the bit is $\mathbb{Z}/2\mathbb{Z}$, so quantization replaces the group of order 2 with the infinite group $\mathrm{PSL}_2(\mathbb{C})$.

Ok, now the actual construction.

Quantization Remember I told you, on the first day and also in my colloquium, and perhaps you also learned in the root systems class, that there is a bijection between simple Lie groups like $\mathrm{PSL}_2(\mathbb{C})$ and ABCDEFG lattices. In the case of $\mathrm{PSL}_2(\mathbb{C})$ you get the lattice called A_1. This is a one-dimensional lattice, except that the shortest vector has length$^2 = 2$:

$$A_1 = \sqrt{2}\mathbb{Z} \subset \mathbb{R}.$$

If $L \subset \mathbb{R}^n$ is a lattice, its dual lattice is

$$L^* = \left\{ v \in \mathbb{R}^n \text{ s.t. } v \cdot v' \in \mathbb{Z} \ \forall v' \in L \right\}.$$

For example,

$$A_1^* = \frac{1}{\sqrt{2}}\mathbb{Z}.$$

Note that $A_1 \subset A_1^*$, because the dot product on A_1 takes only integral values. Furthermore, the quotient group is

$$A_1^*/A_1 = \mathbb{F}_2.$$

This one of the ways that the qubit (PSL_2) quantizes the bit ($\mathbb{F}_2$).

Now consider the lattice $(A_1)^2 4 \subset \mathbb{R}^{24}$ consisting of all vectors all of whose coordinates are $\sqrt{2}$ times an integer. Its dual is $(A_1^*)^{24}$. Define the lattice:

$$L = (A_1^*)^{24} \underset{\mathbb{F}_2^{24}}{\times} \mathcal{C}_{24} = \left\{ v \in (A_1^*)^{24} \text{ s.t. } v \in \mathbb{C}_{24} \mod (A_1)^{24} \right\} =$$

$$= \left\{ \frac{1}{\sqrt{2}} v \text{ s.t. } v \in \mathbb{Z}^{24} \text{ and } v \in \mathcal{C}_{24} \mod 2 \right\}.$$

The lattice L is a sort of "quantum" version of the Golay code $\mathcal{C}_{24}$.

Lemma. *L is even and self-dual.*

A lattice L is even if $v^2 \in 2\mathbb{Z}$ for all $v \in L$, and self-dual if $L = L^*$ (as subsets of $\mathbb{R}^n$). A fun exercise is to show that if L is even, then $v \cdot v' \in \mathbb{Z}$ for all $v, v' \in L$. (Hint: complete the square.)

Proof. L breaks up as cosets over A_1^{24} indexed by the words in $\mathcal{C}_{24}$. A_1^{24} is even, and evenness for the cosets comes from the fact that all words in $\mathcal{C}_{24}$ have weight divisible by 4. Self-duality comes from the self-duality of $\mathcal{C}_{24}$: consider the inclusions

$$(A_1)^{24} \subset L \subset L^* \subset (A_1^*)^{24};$$

the first and third inclusions are each of index $\#\mathcal{C}_{24} = 2^{12}$; the total inclusion is of index $\#\mathbb{F}_2^{24} = 2^{24}$; so $L \subset L^*$ must be of index 1. □

Gauging This lattice L is not the Leech lattice. To get the Leech lattice, we need to "gauge an order-2 symmetry." The way we will do this is the following. Fix the vector $\theta = \frac{1}{\sqrt{2}}(1, 1, \ldots, 1) \in L$. Note that $\theta^2 = \frac{1}{2}24 = 12$. Consider the map

$$L \to \mathbb{F}_2 : v \mapsto \theta \cdot v \mod 2.$$

The kernel of this map is some sublattice

$$L_0 = \{v \in L \text{ s.t. } \theta \cdot v = 0 \mod 2\}.$$

Note that both inclusions $L_0 \subset L = L^* \subset L_0^*$ have index 2, and so $L_0 \subset L_0^*$ has index 4. In fact, $L_0^*/L_0 = 2^2$ is a Klein-4 group, although I won't prove this. Break up L_0^* into cosets over L_0. They are:

$$L_0^* = L_0 \quad \sqcup \quad \underbrace{L_0 + (\sqrt{2}, 0, \ldots, 0)}_{L \smallsetminus L_0} \quad \sqcup \quad L_0 + \frac{1}{2}\theta \quad \sqcup \quad (L \smallsetminus L_0) + \frac{1}{2}\theta.$$

The first and second cosets make up the original lattice L. Actually, the first and third cosets are also an integral lattice, as are the first and fourth. Note that $(\frac{1}{2}\theta)^2 = \frac{1}{4}12 = 3$ is odd. So the first and third cosets together produce an odd lattice.

Definition. *The (even) Leech lattice is the union of the first and fourth cosets. The odd Leech lattice is the union of the first and third cosets.*

Proposition. *The Leech lattice is even. For both the even and odd Leech lattices, the shortest nonzero vectors have length$^2 \geq 3$ (so ≥ 4 for the even Leech lattice).*

Proof. We must show that $v^2 \in 2\mathbb{Z}$ for $v \in$ Leech. For $v \in L_0$ this is true because L was even. For the other coset, note that $v = v_0 + (\sqrt{2}, 0, \ldots, 0) + \frac{1}{2}\theta$ where $v_0 \in L_0$, and so

$$v^2 = \underbrace{(v_0 + (\sqrt{2}, 0, \ldots, 0))^2}_{=\text{even}} + \underbrace{\left(\frac{1}{2}\theta\right)^2}_{=3} + \underbrace{2v_0 \cdot \frac{1}{2}\theta}_{=v_0\cdot\theta=\text{even}} + \underbrace{2(\sqrt{2}, 0, \ldots, 0) \cdot \frac{1}{2}\theta}_{=(\sqrt{2},0,\ldots,0)\cdot\theta=1}.$$

This shows that Leech is even.

For the second statement, the only vectors of length $\sqrt{2}$ in L are $(\sqrt{2}, 0, \ldots, 0)$ and its friends, and these are not in L_0. Actually, this is already a nontrivial statement: it uses that there are no short words in $\mathcal{C}_{24}$. So anyway $v^2 \geq 4$ for $v \in L_0$. The union of the third and fourth cosets consists of vectors $v = v' + \frac{1}{2}\theta$ where $v' \in L$. So the question is to show that $\frac{1}{2}\theta$ is at least distance 3 from all of L. And again this follows from the lack of short words in $\mathcal{C}_{24}$. $\square$

So we have defined the Leech lattice. Let's talk about its symmetries.

Definition. *Conway's largest group is* $\mathrm{Co}_0 = \mathrm{Aut}(\text{Leech})$.

It is not quite a simple group. Indeed, the symmetry $-\mathrm{id} : v \mapsto -v$ is in the centre of Co_0.

Definition. $\mathrm{Co}_1 = \mathrm{Co}_0/\{\pm\mathrm{id}\}$.

It turns out that Co_1 is simple sporadic. Let's talk about some subgroups. Actually, let's talk about subgroups of Co_0, which are much the same as subgroups of Co_1.

- We built Co_0 from $\mathcal{C}_{24}$, and everything, including vector θ, was preserved by $\mathrm{Aut}(\mathcal{C}_{24}) = \mathrm{M}_{24}$ permuting the 24 coordinates. So $\mathrm{M}_{24} \subset \mathrm{Co}_0$. Also, you could switch the sign of any coordinate and get a symmetry of the lattice L. Those sign switches don't preserve θ, but we don't really need them to: we only need to preserve the sublattice L_0 (equivalently, the function $v \mapsto \theta \cdot v \mod 2$). It turns out that if you switch a bunch of signs all at the same time, and *if the coordinates you choose make up a Golay codeword*, then you preserve L_0. So this gives a copy of $\mathcal{C}_{24} \cong 2^{12} \subset \mathrm{Co}_0$, and together you get a (maximal!) subgroup $\mathcal{C}_{24} \rtimes \mathrm{M}_{24} \subset \mathrm{Co}_0$.

- So far you could reasonably believe that Aut(Leech) was merely the group $\mathcal{C}_{24} \rtimes \mathrm{M}_{24}$. And, indeed, for the odd Leech lattice, the full symmetry group is exactly $\mathcal{C}_{24} \rtimes \mathrm{M}_{24}$.

  Let me convince you, however, that Aut(Leech) is bigger than that. We built Leech from the lattice called L, which we built from compounding $\mathcal{C}_{24}$ and A_1^{24}:

$$L = \mathcal{C}_{24}.A_1^{24} \overset{\mathbb{Z}/2}{\rightsquigarrow} \text{Leech}$$

  We could also build Leech directly from the hexacode.

  To explain this, I need to define the $\underline{D_4 \text{ lattice}}$. This is a sublattice of the quaternions $\mathbb{H}$. Just like with $A_1 = \sqrt{2}\mathbb{Z} \subset \mathbb{R}$, there is a factor of $\sqrt{2}$, and the rest is:

$$\frac{1}{\sqrt{2}} D_4 = \left\{ a + bi + cj + dk \text{ s.t. all } a, b, c, d \in \mathbb{Z} \text{ or all } a, b, c, d \in \frac{1}{2} + \mathbb{Z} \right\} \subset \mathbb{H}.$$

  It turns out that $D_4^*/D_4 \cong \mathbb{F}_4$ — this is actually a statement about the noncommutative subring $\frac{1}{\sqrt{2}} D_4 \subset \mathbb{H}$ — and so there is a lattice

$$L' = \mathcal{C}_6.D_4^6$$

  built from compounding the hexacode $\mathcal{C}_6$ with D_4^6. It turns out that L' is even and self-dual.

  Furthermore, the construction from yesterday, in which we built $\mathcal{C}_{24}$ from $\mathcal{C}_6$, was actually a "gauging" $L' \overset{\mathbb{Z}/2}{\rightsquigarrow} L$, and so we can get from L' to Leech in two steps:

$$L' \overset{\mathbb{Z}/2}{\rightsquigarrow} L \overset{\mathbb{Z}/2}{\rightsquigarrow} \text{Leech}.$$

  These two steps "commute": you can actually get directly from L' to Leech by gauging a Klein-4 group $(\mathbb{Z}/2)^2$:

$$L' \overset{(\mathbb{Z}/2)^2}{\rightsquigarrow} \text{Leech}.$$

  What are the symmetries of this construction? Well, L' was built from $\mathcal{C}_6$, and so among its symmetries is the group $3A_6$. But also $(\mathbb{Z}/2)^2$ has symmetries. In particular, it has a $\underline{\text{triality}}$ symmetry of order 3, which it turns out acts on the whole construction.

  All together, we find that Co_0 contains a subgroup of shape $3 \times 3A_6$. The $3A_6$ part is inside $\mathcal{C}_{24} \rtimes \mathrm{M}_{24}$, but $3 \times 3A_6 \not\subset \mathcal{C}_{24} \rtimes \mathrm{M}_{24}$. So $\mathcal{C}_{24} \rtimes \mathrm{M}_{24} \subsetneq \mathrm{Co}_0$.

- The Leech sporadic groups are the sporadic subgroups of Co_0 (other than the Mathieu groups). For instance:

$$\mathrm{Co}_2 = \mathrm{Stab}(\text{vector of length } \sqrt{4}), \qquad \mathrm{Co}_3 = \mathrm{Stab}(\text{vector of length } \sqrt{6}),$$
$$\mathrm{McL} = \mathrm{Stab}(\text{triangle with sides of length } \sqrt{4}, \sqrt{4}, \sqrt{6}),$$
$$\mathrm{HS} = \mathrm{Stab}(\text{triangle with sides of length } \sqrt{4}, \sqrt{6}, \sqrt{6})$$

  All vectors of length $\sqrt{4}$ in Leech form a single Co_0-orbit, as do all vectors of length $\sqrt{6}$, as do all triangles built therefrom. The first two are due to Conway, and the others are due to McLaughlin and to Higman and Sims.

  There are two more important Leech groups. First, the hexacode construction provides the Leech lattice with a "quaternionic structure," meaning that it identifies $\mathbb{R}^{24} \supset \text{Leech}$ with

$\mathbb{H}^6$. The subgroup of Co_0 compatible with this structure is Janko's second group J_2 (also due to Hall), or rather (because of $\pm\mathrm{id}$) its double cover $2\mathrm{J}_2$. Intermediate between Co_0 and J_2 is the group of symmetries preserving a complex structure. This is the six-fold cover of Suzuki's sporadic group: $\mathrm{Co}_0 \supset 6\mathrm{Suz}$. (Warning: Suzuki also has one of the sequences of Lie-type finite simple groups named after him.)

3.2 Monstrous groups

To finish, I will (outline how to) build the Monster sporadic group and its subgroups. We'll repeat the trick from earlier: first we will **quantize**, and then we will **gauge**. This time the input is the Leech lattice itself.

Quantization: Suppose that $L \subset \mathbb{R}^n$ is an even, preferably self-dual, lattice. I told you at my colloquium that you can build from it a "chiral string theory" in which a quantum string flies through the torus $\mathbb{R}^n/L$. The standard name for this quantum system is "V_L." Such a string theory has some manifest symmetries: you can translate along the torus, and you can also apply lattice symmetries:

$$(\mathbb{R}^n/L).\,\mathrm{Aut}(L) \subset \mathrm{Aut}(V_L).$$

(Warning: due to "quantum anomalies," the extension typically does not split — usually $\mathrm{Aut}(L) \not\subset \mathrm{Aut}(V_L)$.)

I told you at the colloquium that there are also quantum symmetries, and you will have to take my word for it, but they are in bijection with vectors in L of length $\sqrt{2}$. In particular, for a typical lattice (like $L = \mathcal{C}_{24}.A_1^{24}$ from the previous section) there are quantum symmetries, but the Leech lattice has no vectors of length $\sqrt{2}$, and so *for the Leech lattice there no quantum symmetries*:

$$\mathrm{Aut}(V_{\mathrm{Leech}}) = (\mathbb{R}^{24}/\mathrm{Leech}).\,\mathrm{Aut}(\mathrm{Leech}) = (\mathbb{R}^{24}/\mathrm{Leech}).\mathrm{Co}_0.$$

Gauging: The torus $\mathbb{R}^{24}/\mathrm{Leech}$ is an abelian group. Consider the (manifest) symmetry $x \mapsto -x$. We will "gauge" this symmetry. I won't tell you how this works, but it is a quantum version of the passage $\mathcal{C}_{24}.A_1^{24} \rightsquigarrow$ Leech from earlier, where you pass to a subsystem (analogous to L_0) and then extend to a different larger system.

The resulting system — the quantum theory describing a chiral string traveling inside the quotient space $(\mathbb{R}^{24}/\mathrm{Leech})/(x \equiv -x)$ — is traditionally called "$V^\natural$."

What are the manifest symmetries? Well, we still have all of the automorphisms of Leech, except we've made $x \mapsto -x$ be the identity, so we have $\mathrm{Co}_1 = \mathrm{Co}_0/(\pm\mathrm{id})$. The translations are mostly destroyed by the gauging: if you translate by $x \in \mathbb{R}^{24}/\mathrm{Leech}$, that's probably not the same as translating by $-x$, but they have to be. But a few translations are preserved: the 2^{24} many points in $\mathbb{R}^{24}/\mathrm{Leech}$ that already solved $x = -x$ even without gauging. Finally, there's an order-2 symmetry that comes from the gauging procedure itself:

$$2.2^{24}.\mathrm{Co}_1 = 2^{1+24}.\mathrm{Co}_1 \subset \mathrm{Aut}(V^\natural).$$

Definition. *The Monster group is* $\mathbb{M} = \mathrm{Aut}(V^\natural)$.

So far, you could reasonably believe that $\mathbb{M}$ consisted merely of $2^{1+24}.\mathrm{Co}_1$. And indeed there is an "odd" version of $V^\natural$ (called "the fermionic Beauty and the Beast model") for which the whole

automorphism group does have shape $2^{1+24}.\mathrm{Co}_1$ (warning: a slightly different group of that shape, because of some "anomalies"), just like the odd Leech lattice had merely $\mathcal{C}_{24} \rtimes \mathrm{M}_{24}$ symmetries. But I will prove (well, outline) to you that $\mathbb{M}$ contains more, "quantum," symmetries.

The argument repeats what we did earlier. As earlier, let us write $L = \mathcal{C}_{24}.A_1^{24}$. Then we built Leech by gauging L: $L \overset{\mathbb{Z}/2}{\rightsquigarrow}$ Leech. This survives quantization:

$$V_L \overset{\mathbb{Z}/2}{\rightsquigarrow} V_{\text{Leech}} \overset{\mathbb{Z}/2}{\rightsquigarrow} V^\natural.$$

The first $\rightsquigarrow$ involved passing to a sublattice $L_0 \subset L$ of index 2, and the second involved $x \mapsto -x$, and so these two things commute, and you can actually gauge directly

$$V_L \overset{(\mathbb{Z}/2)^2}{\rightsquigarrow} V^\natural.$$

The Klein-4 group $(\mathbb{Z}/2)^2$ has a triality automorphism of order 3. It's not completely obvious that it acts on $V^\natural$, because one of the $\mathbb{Z}/2$s involved passing to a sublattice, whereas the other involved $x \mapsto -x$. Here's where the quantum symmetries of V_L kick in: it turns out that these two $\mathbb{Z}/2$s are conjugate *via a quantum symmetry of* V_L, which does have quantum symmetries because L has vectors of length $\sqrt{2}$.

The end result is that you get an extra triality symmetry in $\mathbb{M}$: in addition to $[2^{25}].\mathrm{M}_{24} \subset [2^{25}].\mathrm{Co}_1 \subset \mathbb{M}$, you also have an element of order 3 *which is not in* $[2^{25}].\mathrm{Co}_1$. So:

$$\mathbb{M} \supsetneq 2^{1+24}.\mathrm{Co}_1.$$

It is in fact generated by $2^{1+24}.\mathrm{Co}_1$ together with this triality element. The full subgroup of $\mathbb{M}$ "containing" $3 \times \mathrm{M}_{24}$ is

$$2^{2+11+22}.(S_3 \times \mathrm{M}_{24}) \subset \mathbb{M}.$$

The Monster sections are the sporadic groups inside $\mathbb{M}$ (and not already inside Co_1). One of the easiest ways to give a subgroup is as the centralizer of some element. The order of $\mathbb{M}$ is

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

In particular, for the primes $p \geq 17$, there is (at most) one centralizer of an element of order p. Also it turns out that there is only one conjugacy class of elements of order 11, and in any case these are all large primes and pretty boring. The "small primes" are $2, 3, 5, 7, 13$. They are the ones for which the Sylow p-subgroup — I assume you know what that is — is noncommutative. They are also the primes p such that $p - 1$ divides 24 — the number 24 is very magical in this story.

In any case, if I fix a prime p, then I will name the conjugacy classes of order p by the names "pA," "pB," ..., where (if possible) the rule is that the centralizers are ordered alphabetically by size:

$$\#C(p\mathrm{A}) > \#C(p\mathrm{B}) > \dots.$$

For the Monster $\mathbb{M}$, for the interesting primes $p \in \{2, 3, 5, 7, 13\}$, it turns out that you can always do this (and for the boring primes, sometimes there are multiple conjugacy classes but they are powers of each other and so have the same centralizer).

Remarkably — this really is special to $\mathbb{M}$, and is an example of all sort of extra order and symmetry that it enjoys — for each of the interesting primes $p \in \{2, 3, 5, 7, 13\}$, there are exactly two conjugacy classes pA and pB, except that there is also a third class of order 3 called of course

3C. Even better, the centralizers follow a systemmatic pattern. The groups $C(p\mathrm{B})$ are all of shape $p^{1+d}.X$ where $X \subset \mathrm{Co}_1$ and $d = 24/(p-1)$. In particular:

$$C(2\mathrm{B}) = 2^{1+24}.\mathrm{Co}_1, \quad C(3\mathrm{B}) = 3^{1+12}.2\mathrm{Suz}, \quad C(5\mathrm{B}) = 5^{1+6}.2\mathrm{J}_2.$$

These are interesting and important, but don't give new sporadic groups. What's going on is that there are also gauging procedures $V_{\mathrm{Leech}} \overset{\mathbb{Z}/p}{\rightsquigarrow} V^\natural$ for these primes p, and the cases $p = 3$ and $p = 5$ have to do with the complex and quaternionic structures on Leech.

The other centralizers provide most of the remaining Monstrous sporadic groups:

$$C(2\mathrm{A}) = 2\mathbb{B}, \quad C(3\mathrm{A}) = 3\mathrm{Fi}'_{24}, \quad C(3\mathrm{C}) = 3 \times \mathrm{Th}, \quad C(5\mathrm{A}) = 5 \times \mathrm{HN}, \quad C(7\mathrm{A}) = 7 \times \mathrm{He}.$$

$\mathbb{B}$ is the "Baby Monster," Fi stands for "Fischer," Th for "Thompson," HN for "Harada–Norton," and He for "Held."

Fi'_{24} is the largest of a trio of Fischer groups. It is very closely related to M_{24} — it is the latter's direct granddaughter. There are two other Fischer groups, Fi_{23} and Fi_{22}, which are the granddaughters of M_{23} and M_{22}. They enjoy

$$2\mathrm{Fi}_{22} \subset \mathrm{Fi}_{23} \subset \mathrm{Fi}'_{24}.$$

Actually, there is one more, which you should think of as "Fi_{21}," but just like $\mathrm{M}_{21} = \mathrm{PSL}_3(\mathbb{F}_4)$ it isn't sporadic, but rather it is $\mathrm{PSU}_6(\mathbb{F}_2)$.

And that's the complete list of Happy Family sporadic groups in their natural habitats!

Further reading

- *Wikipedia* has quite excellent discussion of sporadic groups. I have been told that a lot of it was written by Richard Borcherds, who is an excellent writer, but I haven't asked him.
- *The ATLAS of Finite Groups*, the paper copy. It is out of print, and humongous, and has lots of nice short essays about all of the groups (sporadic and exceptional) that it includes. Unfortunately, although the data tables from the ATLAS are available online, I cannot find the essays anywhere except the print copy.
- Conway and Sloane, *Sphere Packings, Lattices, and Groups*, 1993. Many articles and edited lectures. Day 2 (and the second half of Day 1) was drawn almost verbatim from the Chapter 11: The Golay Codes and The Mathieu Group.
- Griess, *Twelve Sporadic Groups*, 1998. A Springer yellow book.
- Gannon, *Moonshine beyond the Monster*, 2006. Very funny, with lots of deep mathematics and physics. Emphasizes that the McKay correspondence (Egyptian fractions $\to$ finite groups $\to$ Lie groups) that I described in my colloquium is an example of "moonshine."