El Grupo Monstruo y la Conjetura Monster Moonshine

Por: Ian Castellanos

Grupos Simples

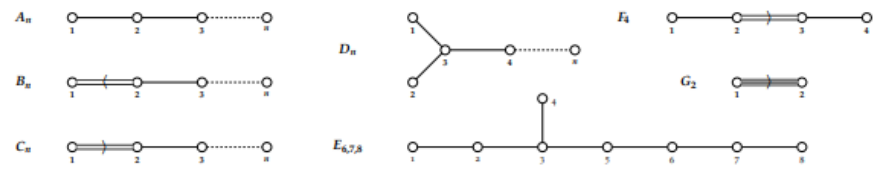
- Un **grupo simple** es aquel en el que sus únicos subgrupos normales son el grupo identidad y él mismo.
- Esto hace que los grupos simples no puedan partirse en subgrupos.
- **Teorema de la clasificación de grupos simples finitos**:
  $Sea\ G\ un\ grupo\ simple\ finito. Entonces\ G\ es\ uno\ de\ los\ siguientes$:
  - $Un\ grupo\ cíclico\ de\ orden\ primo$.
  - Un grupo alternante
  - Un miembro de una de las 16 familias infinitas de grupos de Lie.
  - $Una\ de\ las\ 26\ excepciones\ de\ grupos\ esporádicos$

Grupos Simples Esporádicos

- Grupos de Mathieu: $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$
- Grupos de Janko: J_1, J_2 o HJ, J_3 o HJM, J_4
- Grupos de Conway: Co_1, Co_2, Co_3
- Grupos de Fischer: $Fi_{22}, Fi_{23}, Fi_{24}$ o F_{3+}
- Grupo de Highman-Sims: HS
- Grupo de McLaughlin: McL
- Grupo de Held: He o F_{7+} o F_7
- Grupo de Rudvalis: Ru
- Grupo de Suzuki: Suz o F_{3-}
- Grupo O'Nan: $O'N(ON)$
- Grupo de Harada-Norton: HN o F_{5+} o F_5
- Grupo de Lyons: Ly
- Grupo de Thompson: Th o$F_{3|3}$ o F_3
- Grupo Monstruo Bebé: $\mathbb{B}$ o F_{2+} o F_2
- Grupo Monstruo: $\mathbb{M}$ o F_1

The Periodic Table Of Finite Simple Groups

Dynkin Diagrams of Simple Lie Algebras



$0, C_1, \mathbb{Z}_1$ 1 1																C_2 2
$A_1(4), A_1(5)$ A_5 60	$A_2(2)$ $A_1(7)$ 168											$^2A_3(4)$ $B_2(3)$ 25 920	$C_3(3)$ 4 585 351 680	$D_4(2)$ 174 182 400	$^2D_4(2^2)$ 197 406 720	$G_2(2)'$ $^2A_2(9)$ 6 048	C_3 3
$A_1(9), B_2(2)'$ A_6 360	$^2G_2(3)'$ $A_1(8)$ 504											$B_2(4)$ 979 200	$C_3(5)$ 228 501 000 000 000	$D_4(3)$ 4 952 179 814 400	$^2D_4(3^2)$ 10 151 968 619 520	$^2A_2(16)$ 62 400	C_5 5
A_7 2 520	$A_1(11)$ 660	$E_6(2)$ 214 841 575 522 005 575 270 400	$E_7(2)$	$E_8(2)$	$F_4(2)$ 3 311 126 603 366 400	$G_2(3)$ 4 245 696	$^3D_4(2^3)$ 211 341 312	$^2E_6(2^2)$ 76 532 479 683 774 853 939 200	$^2B_2(2^3)$ 29 120	Tits* $^2F_4(2)'$ 17 971 200	$^2G_2(3^3)$ 10 073 444 472	$B_3(2)$ 1 451 520	$C_4(3)$ 65 784 756 654 489 600	$D_5(2)$ 23 499 295 948 800	$^2D_5(2^2)$ 25 015 379 558 400	$^2A_2(25)$ 126 000	C_7 7
$A_3(2)$ A_8 20 160	$A_1(13)$ 1 092	$E_6(3)$	$E_7(3)$	$E_8(3)$	$F_4(3)$ 5 734 420 792 816 671 844 761 600	$G_2(4)$ 251 596 800	$^3D_4(3^3)$ 20 560 831 566 912	$^2E_6(3^2)$	$^2B_2(2^5)$ 32 537 600	$^2F_4(2^3)$ 264 905 352 699 586 176 614 400	$^2G_2(3^5)$ 49 825 657 439 340 552	$B_2(5)$ 4 680 000	$C_3(7)$ 273 457 218 604 953 600	$D_4(5)$ 8 911 539 000 000 000 000	$^2D_4(4^2)$ 67 536 471 195 648 000	$^2A_3(9)$ 3 265 920	C_{11} 11
A_9 181 440	$A_1(17)$ 2 448	$E_6(4)$	$E_7(4)$	$E_8(4)$	$F_4(4)$ 19 009 825 523 840 945 451 297 669 120 000	$G_2(5)$ 5 859 000 000	$^3D_4(4^3)$ 67 802 350 642 790 400	$^2E_6(4^2)$	$^2B_2(2^7)$ 34 093 383 680	$^2F_4(2^5)$	$^2G_2(3^7)$ 239 189 910 264 352 349 332 632	$B_2(7)$ 138 297 600	$C_3(9)$ 54 025 731 402 499 584 000	$D_5(3)$ 1 289 512 799 941 305 139 200	$^2D_4(5^2)$ 17 880 203 250 000 000 000	$^2A_2(64)$ 5 515 776	C_{13} 13
A_n $\frac{n!}{2}$	$PSL_{n+1}(q), L_{n+1}(q)$ $A_n(q)$	$E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$	$^3D_4(q^3)$	$^2E_6(q^2)$	$^2B_2(2^{2n+1})$	$^2F_4(2^{2n+1})$	$^2G_2(3^{2n+1})$	$O_{2n+1}(q), \Omega_{2n+1}(q)$ $B_n(q)$	$PSp_{2n}(q)$ $C_n(q)$	$O_{2n}^+(q)$ $D_n(q)$	$O_{2n}^-(q)$ $^2D_n(q^2)$	$PSU_{n+1}(q)$ $^2A_n(q^2)$	Z_p C_p p

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Ree Groups and Tits Group*
- Sporadic Groups
- Cyclic Groups

*The Tits group $^2F_4(2)'$ is not a group of Lie type, but is the (index 2) commutator subgroup of $^2F_4(2)$. It is usually given honorary Lie type status.

The groups starting on the second row are the classical groups. The sporadic suzuki group is unrelated to the families of Suzuki groups.

Alternates†
Symbol
Order‡

†For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups those are used to indicate isomorphisms. All such isomorphisms appear on the table except the family $B_n(2^m) \cong C_n(2^m)$.

‡Finite simple groups are determined by their order with the following exceptions:
$B_n(q)$ and $C_n(q)$ for q odd, $n > 2$;
$A_8 \cong A_3(2)$ and $A_2(4)$ of order **20160**.

M_{11} 7 920	M_{12} 95 040	M_{22} 443 520	M_{23} 10 200 960	M_{24} 244 823 040	$J(1), J(11)$ J_1 175 560	HJ J_2 604 800	HJM J_3 50 232 960	J_4 86 775 571 046 077 562 880	HS 44 352 000	McL 898 128 000	F_5, HHM, HTH He 4 030 387 200	Ru 145 926 144 000				
Sz Suz 448 345 497 600	$O'NS, O\text{–}S$ $O'N$ 460 815 505 920	$\cdot 3$ Co_3 495 766 656 000	$\cdot 2$ Co_2 42 305 421 312 000	$\cdot 1$ Co_1 4 157 776 806 543 360 000	F_5, D HN 273 030 912 000 000	LyS Ly 51 765 179 004 000 000	F_5, E Th 90 745 943 887 872 000	$M(22)$ Fi_{22} 64 561 751 654 400	$M(23)$ Fi_{23} 4 089 470 473 293 004 800	$F_{3+}, M(24)'$ Fi'_{24} 1 255 205 709 190 661 721 292 800	F_2 B 4 154 781 481 226 426 191 177 580 544 000 000	F_1, M_1 M 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000				

Grupo Monstruo

- El grupo Monstruo $\mathbb{M}$ es el más grande de los grupos simples esporádicos de manera que $|\mathbb{M}| \approx 8 \times 10^{53}$
- Es un grupo de rotaciones en 196,883 dimensiones i.e., cada elemento es expresado en una matriz de $196{,}883 \times 196{,}883$.

Clases de Conjugados

- Sea $\gamma \in G$, es un grupo finito, entonces se define la clase de conjugados como:
- $c(\gamma) = \{g\gamma g^{-1} | g \in G\}$
- Se dice que $c(\gamma)$ parte el grupo G.

Representaciones

- *La **Teoría de Representaciones** es el estudio de como las simetrías ocurren en la naturaleza; esto es, el estudio de como los grupos actúan por medio de transformaciones lineales en espacios vectoriales* (Wadsley S., 2021).
- Una **representación** ρ de un grupo G en un espacio vectorial V es un homomorfismo de grupo $\rho: G \to GL(V)$, donde $GL(V)$ es el grupo de transformaciones lineales invertibles de V.
- **Notación**: (ρ, V)

Ejemplo de Representaciones

- $S_3 = \{e, (123), (132), (12), (13), (23)\}$
- Se considera el subespacio:

$V = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$

Se elige como bases $v_1 = (1, -1, 0)$ y $v_2 = (1, 0, -1)$.

Entonces las representaciones son:

$$\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \rho((12)) = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix},\ \rho((123)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

Representaciones

- **G-invariante**: Sea la representación $\rho: G \to GL(V)$. Se dice que un subespacio $k - lineal\ W$ de W es $G - invariante$ si
$$\rho(g)(W) \subseteq W, \forall g \in G$$

i.e. $\rho(g)(w) \in W \forall g \in G\ \&\ w \in W$

- En ese caso se llama a W una **subrepresentación de V.**
- **Subrepresentación propia:** Se le llama a una subrepresentación $W\ de\ V$ si $W \neq V\ \&\ W \neq 0$
- Se dice que $V \neq 0$ es **irreducible** si no tiene subrepresentaciones propias.

Representaciones

- Hay tantos irreducibles en G como $c(\gamma)$ en G.
- Toda representación de un grupo G es isomorfa a la suma directa de irreducibles
- i.e., dado un cambio de bases de V se puede asumir que ρ es evaluada en matrices cuadradas diagonales cuyos tamaños son las dimensiones de los irreducibles

Representaciones del Grupo Monstruo

- Se tiene el supuesto [por Conway & Norton] de que el menor irreducible no trivial de $\mathbb{M}$ es de dimensión 196883.
- Asimismo, se tiene que $\mathbb{M}$ tiene 194 dimensiones irreducibles.
- Se tiene la sucesión de dimensiones de irreducibles como:
  - $(r_n)_{n=1,\ldots,194} = 1, 196883,\ 21296876, 842609326, \ldots$

Toro complejo

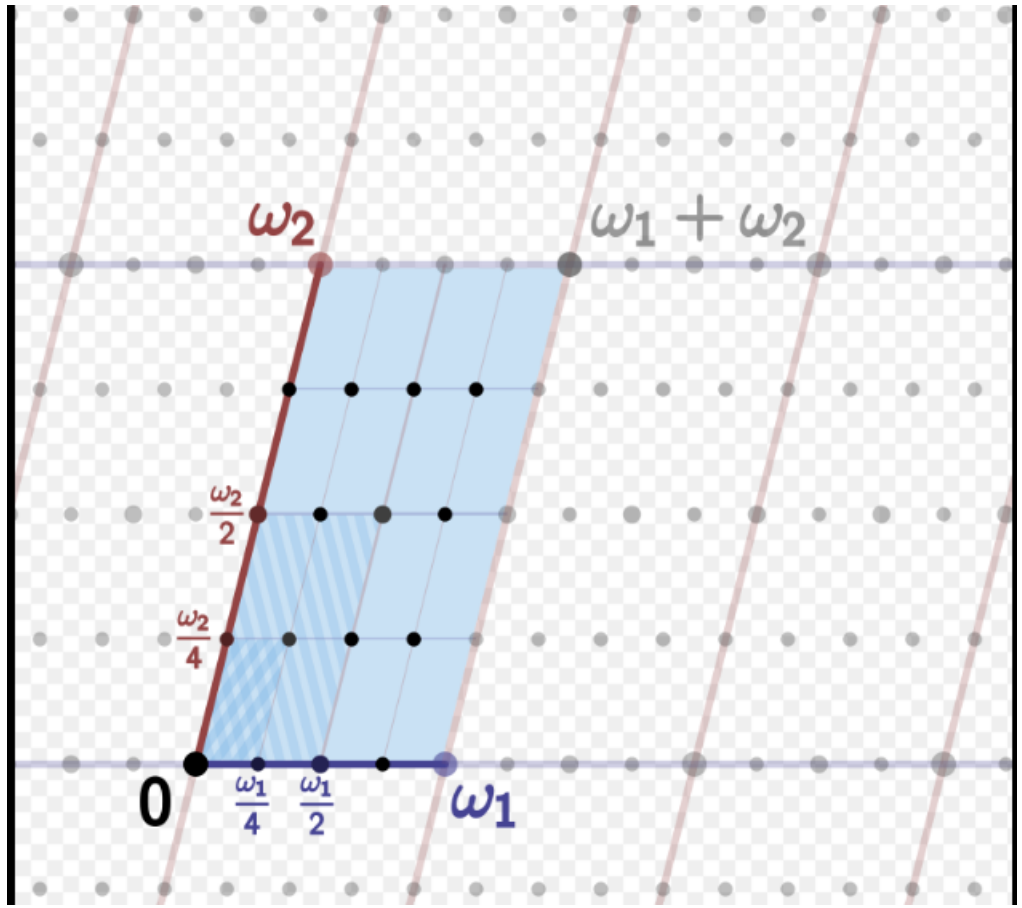
- Sea el lattice (enrejado), si $\exists \omega_1, \omega_2, \in \mathbb{C}^{\times}, \tau = \frac{\omega_1}{\omega_2} \in \mathcal{H}$, donde $\mathcal{H}$ es el semiplano de Poincaré, se define entonces:

$\Lambda = \omega_1\mathbb{Z} \bigoplus \omega_2\mathbb{Z}$ con base $\{\omega_1, \omega_2\}$, de manera $\Lambda \in \mathbb{Z}$

- El **toro complejo** se define como:

$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$ es un grupo abeliano bajo la suma en $\mathbb{C}$.

Toro complejo



Toro complejo

- Si se considera el toro complejo como una clase de equivalencia de lattices (rejas) en $\mathbb{C}$, siendo la relación de equivalencia la multiplicación.
- Entonces en cada clase hay un lattice $\Lambda_\tau, \tau \in \mathcal{H}$, cuya base tiene la forma $(a\tau + b, c\tau + d)$ para $(a, b, c, d) \in \mathbb{Z}^2 \ni ad - bc = 1$

Transformaciones lineales fraccionales

- Una transformación lineal fraccional (aquí considerada en el semiplano de Poincaré superior $\mathcal{H}$) es una función:

$$T(z) = \frac{az + b}{cz + d} \ni a, b, c, d \in \mathbb{C} \ \& \ ad - bc \neq 0$$

Esta transformación es representada por la matriz $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Y se escribe $\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$

Grupos Modulares

- Son funciones complejas que tienen un gran grupo de simetrías relacionadas al grupo de matrices. Para un anillo R se definen los grupos:
- $GL_2(R) = \{\gamma \in M_{2\times 2}(R) | \det(\gamma) \neq 0\}$ Grupo lineal general en R
- $SL_2(R) = \{\gamma \in GL_2(R) | \det(\gamma) = 1\}$ Grupo lineal especial en R
- $PSL_2(R) = SL_2(R)/\{\pm I\}$ Grupo especial de proyecciones en R

Grupos Modulares

- $SL_2(\mathbb{Z})$ es el grupo modular homogéneo

Se tiene que $\langle S, T \rangle$ genera el grupo de manera que:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ni S^2 = -1 \ \& \ T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z}$$

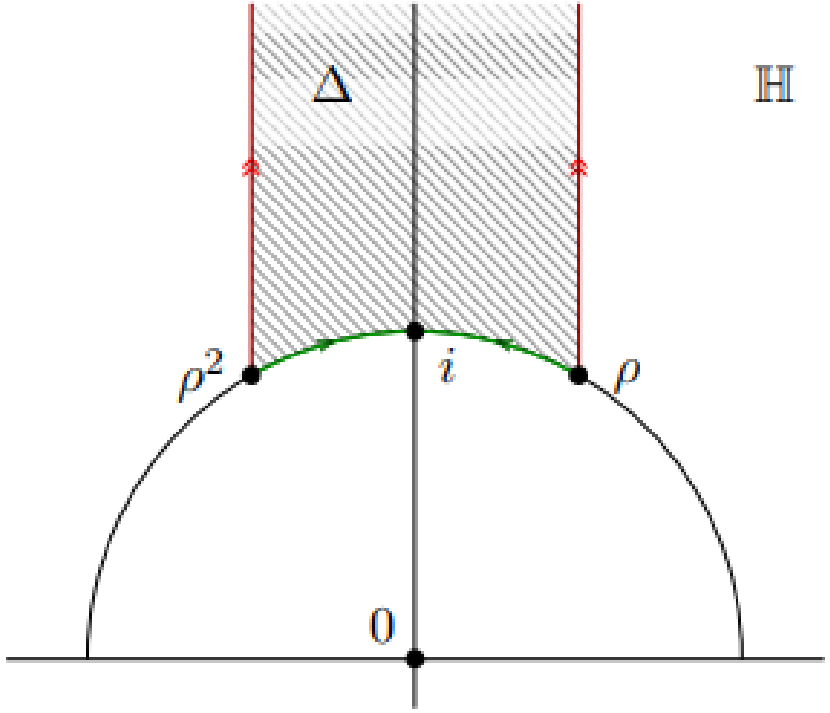
- $PSL_2(\mathbb{Z})$ es el grupo modular inhomogéneo

La base de este grupo es $\{T, S\}$ definidos como antes

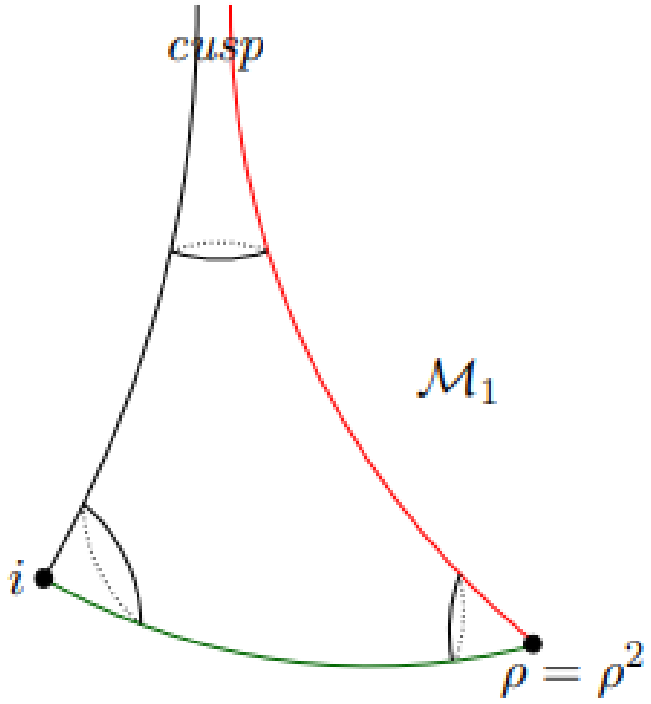
Dominio fundamental

- Es un subconjunto $\Delta \subset \mathcal{H}$, que es simplemente conectado (no tiene agujeros).
- Contiene exactamente un punto de cada órbita bajo la acción de $PSL_2(\mathbb{Z})$.
- **Espacio modular del toro complejo:** $M_1 = \mathcal{H}/PSL_2(\mathbb{Z})$
  - Se identifica el elemento $\rho = e^{2\pi i/3} = \rho^2$
  - Este es producido por la acción $\gamma\tau = \frac{a\tau+b}{c\tau+d}$

Dominio fundamental



$$(\tau \in \Delta) \;\Leftrightarrow\; |\tau| \geq 1 \text{ and } -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq \frac{1}{2}$$



Funciones Modulares

- Una función de $\mathcal{H}$ invariante bajo la acción de $PSL_2(\mathbb{Z})$:

$$f(\tau) = f(M * \tau) = f\left(\frac{a\tau + b}{c\tau + d}\right)$$

Por definición de invariante cumple con las condiciones:

$f(\tau + 1)f(\tau)$ & $f\left(-\frac{1}{\tau}\right) = f(\tau)$

Una función definida así sobre $PSL_2(\mathbb{Z})$ es una **función modular**

Formas modulares

- Dado que el estudio de las funciones modulares es complicado, para su estudio se usan las **formas modulares**:
- Una **forma modular f de peso $2k$**, $k \in \mathbb{N}$ es una función holomórfica en $\mathcal{H}$, tal que:

$$f(\tau) = (c\tau + d)^{2k} f\left(\frac{a\tau + b}{c\tau + d}\right) \forall M \in PSL_2(\mathbb{Z})$$

de manera que crece exponencialmente de manera que $\Im(\tau) \to \infty$

Serie de Eisenstein

- Es una forma modular de peso $2k$, definida como sigue:

$$G_{2k}(\tau) = \sum_{\omega \in \Lambda_\tau} \frac{1}{\omega^{2k}}$$

Formas modulares

De la teoría de formas modulares se tiene que el conjunto M_k de formas modulares es un espacio vectorial complejo.

Asimismo, se tiene que M es el anillo polinomial $M = \mathbb{C}[G_4, G_6]$.

Es posible buscar funciones modulares como los cocientes de formas modulares del mismo pero sobre los elementos de M_0, que consisten en funciones modulares constantes.

Se elige M_{12} para construir dichas funciones modulares más simples porque $k = 12$ es el menor valor para el cual $\dim(M_k) > 1$.

J-invariante de Klein

- Es la razón de elementos de M_{12} linealmente independientes expresada como:

$$j(\tau) = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} \ni g_2 = 60G_4, g_3 = 140G_6$$

Es una función modular.

Se tiene que toda función modular es una fracción racional de j.

De igual manera, el campo de funciones modulares es $\mathbb{C}(j)$.

Expansiones-q

- Tanto las formas como las funciones modulares han de satisfacer $f(\tau+1)=f(\tau)$ para que admitan una descomposición de Fourier en términos de $q=e^{2\pi i\tau}$.
- Bajo $\tau \to q(\tau)$, el plano $\mathcal{H}$ tiende al disco unitario.
- Entonces para todo $f[\{q\}]$ es invariante bajo $\tau \to \tau+1$
- Se tiene que los coeficientes de la expansión q de j son enteros, siendo sus primeros términos:
- $j(\tau)=\sum_{n=-1}^{\infty} c(n)q^n=\frac{1}{q}+744+196884q+21493760q^2+\cdots$
- $\tilde{j}=j-744$ se dice que es la función j normalizada.

Conjetura de Thompson

- Existe una representación infinito dimensional $\left(\rho_{\sharp}, V^{\sharp}\right) = \bigoplus_{i\geq -1} V_i^{\sharp}$ de $\mathbb{M}$, de manera que para cada $V_i^{\sharp}$ es la $expansión - q$ de la $j - invariante\ normalizada$

$$\tilde{j}(\tau) = \sum_{i\geq -1} \dim(V_i^{\sharp})\, q_i$$

Serie de McKay-Thompson

- Se estudia la siguiente serie, porque la dimensión de una representación es la traza de $\rho(e)$.

$$T_{[g]} = \sum_{i \geq -1} Tr\left(\rho_{\sharp}(g)_{|V_i^{\sharp}}\right) q^i = \frac{1}{q} + \sum_{n=0}^{\infty} H_n([g]) q^n$$

Se tiene que hay una de estas series por cada clase de conjugación $[g]$ de $\mathbb{M}$.

En la serie, $g \in \mathbb{M}$ es cualquier representación de $[g]$.

H_n es una clase de funciones de $\mathbb{M}$.

Conjetura Monster Moonshine

- **Conmensurable:** Dos subgrupos son conmensurables si su intersección es finita.
- Se tiene que las funciones en $\mathcal{H}$ que son $PSL_2(\mathbb{Z}) - invariantes$ son las funciones modulares
- Se sabe que todas estás pueden ser expresadas como funciones racionales de J o de manera equivalente, como funciones racionales de $\tilde{j}$.
- De esta manera $\tilde{j}$ es **el Hauptmodul normalizado** de $PSL_2(\mathbb{Z})$.

Conjetura Monster Moonshine

- Existe una representación infinita-dimensional $\left(\rho_{\mathbb{M}}, V^{\sharp} = \bigoplus V_i^{\sharp}\right)$ del grupo monstruo, tal que cada $V_i^{\sharp}$ es finito-dimensional, y de tal manera que para cada clase de conjugación $[g]$ la serie de McKay-Thompson $T_{[g]}$ es la expansión-q del Hauptmodul normalizado de un subgrupo $\Gamma_{[g]} \leq PSL_2(\mathbb{R})$ conmensurable con $PSL_2(\mathbb{Z})$.

Referencias

- Tatitscheff V.(2019) A short introduction to Monstrous Moonshine. Université de Strasbourg et CNRS.
- S.a.(s.f.) Complex Tori. Reed College. https://people.reed.edu/~jerry/311/tori.pdf
- Royster Dr. David.C. (2008) Non-Euclidean Geometry. https://www.ms.uky.edu/~droyster/courses/spring08/math6118/Classnotes/Chapter10.pdf
- Stewart I.N. & Tall D.O. (1983) Complex Analysis. Cambridge University Press.

- Chamizo F. (2025) The modular group and some relatives. http://matematicas.uam.es/~fernando.chamizo/asignaturas/2425cryptography/lectures/lecture01.pdf
- Keith C. (s.f.) $SL_2(\boldsymbol{Z})$. https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf
- Hruza J. & Trachsler M. (2019) The modular group and the fundamental domain. https://metaphor.ethz.ch/x/2019/fs/401-4110-19L/sc/modulargroup.pdf
- Earl R. (2014) Groups and Group Actions. https://www.maths.ox.ac.uk/system/files/attachments/Groups%20and%20Group%20Actions%20Lecture%20Notes.pdf
- Zagier D. (1991) Modular Forms of One Variable. https://people.mpim-bonn.mpg.de/zagier/files/tex/UtrechtLectures/UtBook.pdf

- Klein's j-function: https://people.reed.edu/~jerry/311/j.pdf
- Milne J.S. (2017) Modular Functions and Modular Forms (Elliptic Modular Curves) https://www.jmilne.org/math/CourseNotes/MF.pdf
- Wadsley S. (2021) Representation Theory. https://www.dpmms.cam.ac.uk/~sjw47/2021RepTh.pdf
- Gallian J.A (2021) Contemporary Abstract Algebra. Tenth Edition. University of Minesota Duluth.