魔群月光

逯晓零

2023 年 7 月 26 日

目录

1 导入

魔群月光 (Monstrous Moonshine) 是什么？是一个我目前所见中觉得名字最好听的定理。虽然它的数学形式并没有想象中的那么美好，或许正是如此导致其不像“费马大定理”和“庞加莱猜想”那么出名，但为了了却心中的愿望，我决定了解并理解它，此文章的核心内容来自于 Borcherds[1] 的“魔群月光和魔群 Lie 超代数”[2]。

2 魔群

我想，什么是群、环、域、模？什么是单群？什么是同构？什么是 Jordan-Holder 定理？无需我再去重复了吧，实在不懂的话，要么去看抽象代数的书，要么去看我写的简介性文章 [13, 11, 12]。

定理 2.1 (Classification Theorem for Finite Simple Groups): 每个有限单群都同构于以下中的一个[1]

(1) 循环群：C_p

(2) 交错群：$A_n, n \geq 5$

(3)Lie 型单群：

(i) 典型群 (Chevalley 群)：

线性：$PSL_n(q), n \geq 2$(并排除 $PSL_2(2), PSL_2(3)$)

[1]常用记号，n 表示整数，p 表示素数，q 表示素数的幂 p^a

酉：$PSU_n(q), n \geq 3$(并排除 $PSU_3(2)$)

辛：$PSp_{2n}(q), n \geq 2$(并排除 $PSp_4(2)$)

正交：$PO_{2n+1}(q), n \geq 3$(并排除 $PO_{2n+1}(2)$)

$PO^+_{2n}(q), PO^-_{2n}(q), n \geq 4$

(ii)Chevalley 群：$G_2(q), q \geq 3; F_4(q); E_6(q), E_7(q); E_8(q)$

(iii)Steinberg 群：${}^2E_6(q);{}^3D_4(q)$

(iv) 铃木 (Suzuki) 群：${}^2B_2(2^{2n+1}), n \geq 1$

(v)Ree 群：${}^2G_2(3^{2n+1}),{}^2F_4(2^{2n+1}), n \geq 1$

(vi)Tits 群：${}^2F_4(2)'$

(4) 散在单群：

(i)Mathieu 群：$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$

(ii) 晶格群：$\mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{McL}, \mathrm{HS}, \mathrm{Suz}, J_2$

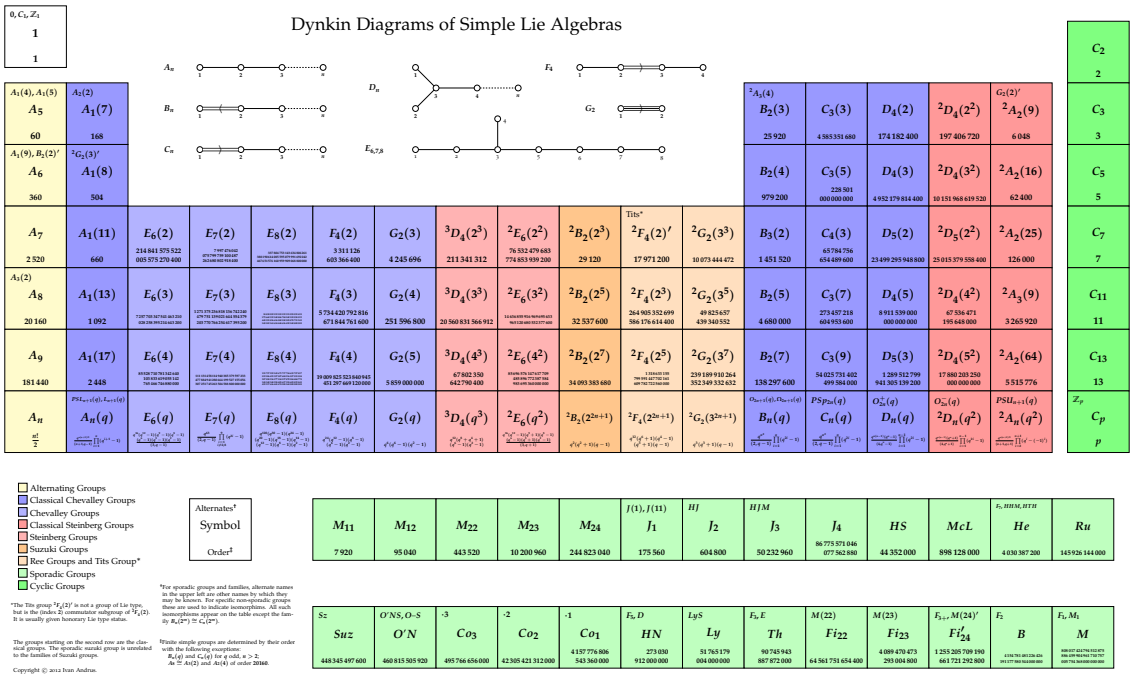
(iii)Fischer 群：$Fi_{22}, Fi_{23}, Fi'_{24}$

(iv) 怪物群：$\mathbb{M}, \mathbb{B}, \mathrm{Th}, \mathrm{HN}, \mathrm{He}$

(v) 贱民：$J_1, J_3, J_4, \mathrm{O'N}, \mathrm{Ly}, \mathrm{Ru}$

在有限单群分类中，比较乱的是 Lie 型单群，由于其中存在各种同构或嵌入关系，导致分类中会出现多种版本，而我们选择的是这本书 [9] 的版本，不过我们更关心的是散在单群，Lie 型单群怎么样就随它去吧。

The Periodic Table Of Finite Simple Groups



群的周期表的原地址

在散在单群中，我们注意到了两个没有以人名命名的群，魔群 $\mathbb{M}$ 和小魔群 $\mathbb{B}$，而前者就是我们这篇文章的研究重点。$\mathbb{M}$ 最早在 [5] 中构造，后来在 [4] 中由 Conway 进行了简化。

想必除了实数 $\mathbb{R}$ 和复数 $\mathbb{C}$，大家对四元数 $\mathbb{H}$ 和八元数 $\mathbb{O}$ 应该有一定程度的理解吧，四元数只是丢失了交换性，还属于结合代数的范畴，理解起来并不困难，所以我们就不讨论了，不懂的话，我推荐你看这本书 [10]，我们重点来介绍一下**八元数**，或称为凯莱数。简单来讲，八元数就是下面形式的数

$$x_\infty + x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6, \forall 0 \leq i \leq 6, x_i, x_\infty \in \mathbb{R}$$

并且后面的形式 e_i 数满足下面的乘法表

表 1: 乘法表

1	$e_0 = l$	$e_1 = i$	$e_2 = j$	$e_3 = il$	$e_4 = k$	$e_5 = kl$	$e_6 = jl$
e_0	-1	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$
e_1	$-e_3$	-1	e_4	e_0	$-e_2$	e_6	$-e_5$
e_2	$-e_6$	$-e_4$	-1	e_5	e_1	$-e_3$	e_0
e_3	e_1	$-e_0$	$-e_5$	-1	e_6	e_2	$-e_4$
e_4	$-e_5$	e_2	$-e_1$	$-e_6$	-1	e_0	e_3
e_5	e_4	$-e_6$	e_3	$-e_2$	$-e_0$	-1	e_1
e_6	e_2	e_5	$-e_0$	e_4	$-e_3$	$-e_1$	-1

如果觉得表格记不住的话，可以使用下面的公式

$$e_n^2 = -1$$

$$e_{n+1}e_{n+2} = e_{n+4} = -e_{n+2}e_{n+1}$$

$$e_{n+2}e_{n+4} = e_{n+1} = -e_{n+4}e_{n+2}$$

$$e_{n+4}e_{n+1} = e_{n+2} = -e_{n+1}e_{n+4}$$

实际上，每一层代数之间都具有复合递归关系

$$\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$$

$$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$$

$$\mathbb{O} = \mathbb{H} \oplus \mathbb{H}l$$

对于复数 $\mathbf{Q}_4 = \{1, i, -1, -i\}$ 可以形成一个交换群，四元数 $\mathbf{Q}_8 = \{1, i, j, k, -1, -i, -j, -k\}$ 可以形成一个非交换群，但八元数呢？连结合性也没有，甚至不能形成一个半群，此时我们需要一个新的代数结构。

定义 2.1: (1) 一个 **(组合)** 拟群 ((combinatorial) quasigroup)$(Q,\cdot)$ 指集合 Q 配备一个乘法 $Q\times Q\to Q,(x,y)\mapsto xy$ 使得，等式 $xy=z$ 中的任意两个元素可以唯一决定第三个元素。

(2) 一个 **(方程)** 拟群 ((equational) quasigroup)$(Q,\cdot,/,\backslash)$ 指集合 Q 配备三个二元运算并且满足，$y\backslash(yx)=x$、$x=(xy)/y$、$y(y\backslash x)=x$、$x=(x/y)y$。

上面两种方式定义的拟群是完全一样的，它们的对应关系为

$$xy=z\Leftrightarrow y=x\backslash z,x=z/y$$

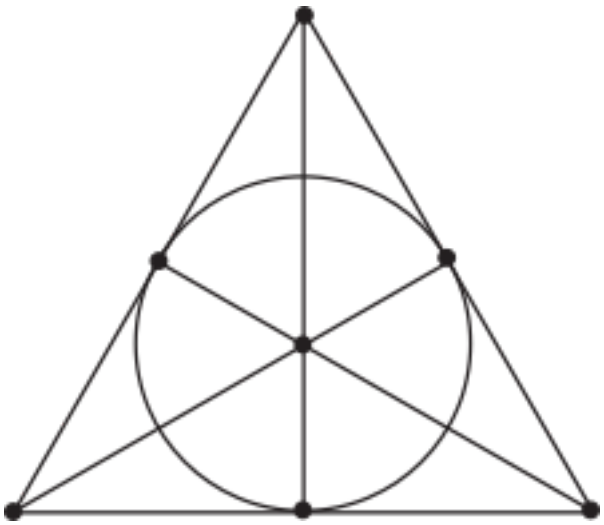
定义 2.2: (1) 如果拟群 $(Q,\cdot)$ 存在单位元 e 满足 $\forall x\in Q,ex=x=xe$，则称 $(Q,\cdot,e)$ 是一个圈 (loop)。

(2) 如果圈 $(Q,\cdot)$ 还满足 Moufang 律,$(xy)(zx)=(x(yz))x$、$x(y(xz))=((xy)x)z$、$((yx)z)x=y(x(zx))$，就把它称为 **Moufang** 圈。

容易验证八元数 $\mathbb{K}=\{1,e_0,...,e_6,-1,-e_0,...,-e_6\}$ 形成一个 Moufang 圈。通过 Moufang 圈，我们可以推出交错律：$(xy)x=x(yx)$、$x(xy)=x(xy)$、$(yx)x=y(xx)$，从而八元数 $\mathbb{O}$ 形成 $\mathbb{R}$ 上的一个 8 维交错代数。不过我们需要的是另一种 Moufang 圈，对于二进制线性空间 $\mathbb{F}_2^n$，我们定义 **Hamming** 距离为

$$H:\mathbb{F}_2^n\times\mathbb{F}_2^n\to\mathbb{N},H(x,y)=\sum_{i=1}^{n}1_{|x_i-y_i|\neq 0}$$

即表示分量中不同坐标的个数。一个 **($[n,k,d]$ 型) 二进制码**指 $\mathbb{F}_2^n$ 的一个 k 维子空间 C 并且满足 $\forall x,y\in C,H(x,y)\geq d$；显然 C 可以由 k 个向量生成，则我们可以把其写成一个 $k\times n$ 的仅由 $\{0,1\}$ 组成的矩阵，并称为这个二进制码的**生成矩阵**。例如，我们考虑下面的仅由七个点 $\{e_0,e_1,e_2,e_3,e_4,e_5,e_6\}$ 组成的 Fano 平面



其上的直线至少包含 3 个点，如果点在线上则记为 1，点不在线上则记为 0，我们记 C 表示 Fano 平面所有直线构成的整体，则 $C\subset\mathbb{F}_2^7$ 构成一个 $[7,4,3]$ 型二进制码，且生成矩阵为

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

所谓的 **Golay 码** $\mathcal{G}_{24}$ 指由下面矩阵生成的 $[24, 12, 8]$ 型二进制码

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

这样研究 Golay 码有些困难，我们考虑进行一定程度的等价。我们不妨记 $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$[2]，所谓的**六进制码** (hexacode)$\mathcal{H}$ 指 $\mathbb{F}_4^6$ 的由下面生成矩阵张成的 3 维子空间

$$\begin{pmatrix} \omega & \overline{\omega} & \overline{\omega} & \omega & \overline{\omega} & \omega \\ \overline{\omega} & \omega & \omega & \overline{\omega} & \overline{\omega} & \omega \\ \overline{\omega} & \omega & \overline{\omega} & \omega & \omega & \overline{\omega} \end{pmatrix}$$

我们可以把它总结为 $[6, 3, 4]$ 型四进制码 (来自于 $\mathbb{F}_4^6$)。我们接着考虑 MOG(Miracle Octad Generator)$C_6 \times \mathbb{F}_4$，它共有 24 个元素，它的每个子集对应一张 4×6 的仅有 0,1(元素在子集内记 1，不在则记 0) 构成的矩阵图。对于每个六进制码 $(x_1, ..., x_6) \in \mathcal{H}$，我们令 $x_i (1 \le i \le 6)$ 匹配集合 $Y_i = \{(i, y)\} \subset C_6 \times \mathbb{F}_4$ 并且满足 $x_i = \sum_{(i,y_j) \in Y_i} y_j$，于是每个 x_i 都可以对应四个子集，例如

$$x_i = 0 \Rightarrow \{(i,0)\}\ \{(i,1),(i,\omega),(i,\overline{\omega})\} \varnothing \{(i,0),(i,1),(i,\omega),(i,\overline{\omega})\}$$

$$x_i = 1 \Rightarrow \{(i,1)\}\ \{(i,0),(i,\omega),(i,\overline{\omega})\}\ \{(i,0),(i,1)\}\ \{(i,\omega),(i,\overline{\omega})\}$$

$$x_i = \omega \Rightarrow \{(i,\omega)\}\ \{(i,0),(i,1),(i,\overline{\omega})\}\ \{(i,0),(i,\omega)\}\ \{(i,1),(i,\overline{\omega})\}$$

$$x_i = \overline{\omega} \Rightarrow \{(i,\overline{\omega})\}\ \{(i,0),(i,1),(i,\omega)\}\ \{(i,0),(i,\overline{\omega})\}\ \{(i,1),(i,\omega)\}$$

[2]这不是四次循环域，而是 $\mathbb{F}_2$ 的二次扩域，$\overline{\omega} = 1 + \omega$ 并且 $\omega, \overline{\omega}$ 是方程 $x^2 + x + 1 \in \mathbb{F}_2[x]$ 的两个根

于是我们将 $(x_1,...,x_6)$ 匹配到子集 $\cup_i Y_i$ 并且进一步限制其对应的矩阵图每一列的奇偶性等于第一行的奇偶性。例如 $(0,1,0,1,\omega,\varpi)\in\mathcal{H}$ 可以匹配到下面的三张矩阵图

$$\begin{pmatrix}1&0&0&0&0&0\\0&1&1&1&0&0\\0&0&1&0&1&0\\0&0&1&0&0&1\end{pmatrix},\begin{pmatrix}1&1&0&0&0&0\\1&1&0&0&1&1\\1&0&0&1&0&1\\1&0&0&1&1&0\end{pmatrix},\begin{pmatrix}1&1&1&0&1&0\\1&1&1&0&0&1\\1&0&1&1&1&1\\1&0&1&1&0&0\end{pmatrix}$$

显然每一个矩阵图都可以对应到 $\mathbb{F}_2^{24}$ 中的一个向量，于是此时六进制码 $\mathcal{H}$ 在 $\mathbb{F}_2^{24}$ 中的对应构成了 Golay 码 $\mathcal{G}_{24}$。这种对应的好处是方便算出 $\mathcal{G}_{24}$ 的权重分布，如果实在搞不懂的话，直接告诉你结论为

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

注意到 $1+759+2576+759+1=4096=2^{12}=|\mathcal{G}_{24}|$，所以读者大概也能猜到它的含义了，其中每一项 a^b 表示 $|\{(x_1,...,x_{24})\in\mathcal{G}_{24}\mid\sum_{i=1}^{24}|x_i|=a\}|=b$，即分量中 1 的个数为 a 的元素的个数为 b。Mathieu 群 $M_{24}\leq S_{24}$ 由下面的三个元素生成

$$(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23)$$

$$(3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16)$$

$$(1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)(13,22)(15,19)$$

我们可以轻松地构造置换作用 $S_{24}\times\mathbb{F}_2^{24}\to\mathbb{F}_2^{24}$，从而可得 $M_{24}\subset S_{24}$ 是 $\mathcal{G}_{24}\subset\mathbb{F}_2^{24}$ 对应的不变子群。然后，我们定义 $\mathbb{P}=\{-,+\}\times\mathcal{G}_{24}$，即给 Golay 码加上了符号位，并规定投影映射为 $\mathbb{P}\to\mathcal{G}_{24},\pm d\mapsto\tilde{\pm d}=d$，对 $x=(x_1,...,x_{24})\in\mathcal{G}_{24}$ 规定 $|x|=\sum_{i=1}^{24}|x_i|$ 表示分量中 1 的个数，$x\cap y=(x_1y_1,...,x_{24}y_{24})$ 表示 $\mathbb{F}_2^{24}$ 中的乘法，或者视为二进制中的与运算。$\mathbb{P}$ 中的乘法运算为 $\mathcal{G}_{24}$ 中的加法运算，并且相应的符号位满足下面的三个等式

$$d^2=(-1)^{\frac{|\tilde{d}|}{4}},de=(-1)^{\frac{|\tilde{d}\cap\tilde{e}|}{2}}ed,(de)f=(-1)^{|\tilde{d}\cap\tilde{e}\cap\tilde{f}|}d(ef)$$

由于在 $\mathbb{F}_2$ 中有 $1+1=0+0=0$，故 $d^2=dd=\pm\tilde{d}+\tilde{d}=\pm(0,...,0)$，即单位元 $(0,...,0)\in\mathcal{G}_{24}$ 对应到 $\pm1\in\mathbb{P}$，可以证明上面的三个符号等式唯一确定出 $\mathbb{P}$ 的乘法运算，并形成一个 Moufang 可逆圈，单位元为 $1\in\mathbb{P}$，此时我们把 $\mathbb{P}$ 称为 **Parker 圈**，这里的可逆[3]指存在 $\forall x\in\mathbb{P},\exists x^{-1}$ 使得 $(x^{-1})^{-1}=x,x^{-1}(xy)=y=(yx)x^{-1}$。我们把 $\mathbb{P}$ 视为类似于 $\mathbb{O}$ 的一种“数”，考虑一个三维子空间 $\mathbf{P}^3=\{(a,b,c)\in\mathbb{P}^3\mid abc=1\}$ 上的自同态

$$x_d:(a,b,c)\mapsto(d^{-1}ad^{-1},db,cd),d\in\mathbb{P}$$

$$y_d:(a,b,c)\mapsto(ad,d^{-1}bd^{-1},dc)$$

$$z_d:(a,b,c)\mapsto(da,bd,d^{-1}cd^{-1})$$

[3]由于结合性不一定存在，使用 $xx^{-1}=1=x^{-1}x$ 是不可靠的

$$x_\delta = y_\delta = z_\delta : (a,b,c) \mapsto ((-1)^{|\tilde{a}\cap\delta|}a, (-1)^{|\tilde{b}\cap\delta|}b, (-1)^{|\tilde{c}\cap\delta|}c), \delta \in \mathcal{G}_{24}\text{满足}|\delta|\text{是偶数}$$

$$x_\delta : (a,b,c) \mapsto ((-1)^{|\tilde{a}\cap\delta|}a^{-1}, (-1)^{|\tilde{c}\cap\delta|}c^{-1}, (-1)^{|\tilde{b}\cap\delta|}b^{-1}), \delta \in \mathcal{G}_{24}\text{满足}|\delta|\text{是奇数}$$

$$y_\delta : (a,b,c) \mapsto ((-1)^{|\tilde{c}\cap\delta|}c^{-1}, (-1)^{|\tilde{b}\cap\delta|}b^{-1}, (-1)^{|\tilde{a}\cap\delta|}a^{-1})$$

$$z_\delta : (a,b,c) \mapsto ((-1)^{|\tilde{b}\cap\delta|}b^{-1}, (-1)^{|\tilde{a}\cap\delta|}a^{-1}, (-1)^{|\tilde{c}\cap\delta|}c^{-1})$$

$$x_\pi = y_\pi = z_\pi : (a,b,c) \mapsto (\pi(a), \pi(b), \pi(c)), \pi \in M_{24}\text{是偶置换}$$

$$x_\pi : (a,b,c) \mapsto (\pi(a^{-1}), \pi(c^{-1}), \pi(b^{-1})), \pi \in M_{24}\text{是奇置换}$$

$$y_\pi : (a,b,c) \mapsto (\pi(c^{-1}), \pi(b^{-1}), \pi(a^{-1}))$$

$$z_\pi : (a,b,c) \mapsto (\pi(b^{-1}), \pi(a^{-1}), \pi(c^{-1}))$$

此时我们把由上面元素生成的子群记为 $\mathbf{N} \leq \mathrm{End}(\mathbf{P}^3)$，我们记

$$\Omega = (1,...,1) \in \mathbb{P}, |\Omega| = 24$$

$$k_1 = y_\Omega z_{-\Omega} = x_\Omega z_{-1} = x_{-\Omega} y_{-1}$$

$$k_2 = z_\Omega x_{-\Omega} = y_\Omega x_{-1} = y_{-\Omega} z_{-1}$$

$$k_3 = x_\Omega y_{-\Omega} = z_\Omega y_{-1} = z_{-\Omega} x_{-1}$$

选择正规子群 $\mathbf{K} = \{1, k_1, k_2, k_3\} \lhd \mathbf{N}$，可以证明 $\mathbf{N}_0 = \mathbf{N}/\mathbf{K}$ 同构于 $\mathbb{M}$ 的极大子群，于是我们魔群的构造更进了一步。对于加法结构，我们定义商群 $\mathcal{G}_{24}^* = \mathbb{F}_2^{24}/\mathcal{G}_{24}$，并定义 $[d] \in \mathcal{G}_{24}^*$ 的长度为 $|[d]| = \min_{x\in[d]} |x|$，于是它也有类似的权重分布

$$0^1 1^{24} 2^{276} 3^{2024} 4^{1771}$$

我们定义换位子 $[d,e] = d^{-1}e^{-1}de$ 并简记 $x = x_{-1}, y = y_{-1}, z = z_{-1}$，我们将 $\mathbf{N}$ 中满足下面性质的元素

$$x_i^2 = 1 = [x_i, x_j]; \prod_{i\in\delta} x_i = 1, \delta \in \mathcal{G}_{24}, [x_d, x_\delta] = (-1)^{|\tilde{d}\cap\delta| + \frac{1}{4}|\tilde{d}||\delta|}$$

$$x_d^2 = x^{\frac{1}{4}|\tilde{d}|}, [x_d, x_e] = x^{\frac{1}{2}|\tilde{d}\cap\tilde{e}|}, x_{-d} = x x_d, x_d x_e = z^{\frac{1}{4}|\tilde{d}\cap\tilde{e}|} x_{de} x_{\tilde{d}\cap\tilde{e}}$$

生成的子群记为 $\mathbf{Q}_x$，则有 $K_1 = \{1, k_1\} \subset \mathbf{Q}_x$ 且 $|\mathbf{Q}_x| \leq 2^{26}$。我们来构造一个晶格 (Leech lattice)

$$\Lambda_{24} = \{\frac{1}{\sqrt{8}}(a_1,...,a_{24}) \in \mathbb{R}^{24} \mid a_i \in \mathbb{Z}, \sum_{i=1}^{24} a_i \equiv 4a_1 \equiv ... \equiv 4a_{24}(\mathrm{mod}8), (a_1,...,a_{24})\mathrm{mod}4 \in \mathcal{G}_{24}\}$$

并对于 $u, v \in \Lambda_{24}$ 引入符号 $\langle u, v\rangle = \frac{1}{8}\sum u_i v_i, \mathrm{type}(u) = \frac{1}{2}\langle u, u\rangle$，则我们有唯一的一个嵌入双射 $\mathbf{Q}_x/\{1,x\} \to \Lambda_{24}/2\Lambda_{24}$ 由下面给出

$$x_i \mapsto \lambda_i = (-3_{\text{在}i\text{处}}, 1_{\text{其它位置}})$$

$$x_d \mapsto \lambda_d = (2_{\text{位置在}d\text{内}}, 0_{\text{其它位置}}), |d| \equiv 0 \text{mod} 8$$

$$x_d \mapsto \lambda_d = (0_{\text{位置在}d\text{内}}, 2_{\text{其它位置}}), |d| \equiv 4 \text{mod} 8$$

并且满足 $[x_r, x_s] = x^{\langle \lambda_r, \lambda_s \rangle}, x_r^2 = x^{\text{type}(\lambda_r)}$。接着定义符号 $x_{r,s} = x_r x_s, x_r^+ = x_{\Omega,r}, x_r^- = x_{-\Omega,r}$，则可以得到它们的对应元素为

$$\lambda_{i,j} = (4_{\text{在}i\text{处}}, -4_{\text{在}j\text{处}}, 0_{\text{其它位置}})$$

$$\lambda_{i,j}^+ = (4_{\text{在}i,j\text{处}}, 0_{\text{其它位置}})$$

$$\lambda_{d,\delta}^+ = (-2_{\text{在}\delta\text{处}}, 2_{\text{在}d-\delta\text{处}}, 0_{\text{其它位置}})$$

$$\lambda_{d,i}^+ = (\mp 3_{\text{在}i\text{处}}, \pm 1_{\text{其它位置}})$$

至此我们已经完成了到魔群的对接，两者相同的证明就看简化的文章 [4]，但为了完整地构造出魔群我们还是需要原来的内容。前面我们构造了 Leech 晶格 Λ_{24}，实际上它还有一种存在性的构造，即我们赋予它几个性质，并可以说明它是唯一存在的。所谓的**晶格** (lattice) 指一个自由交换群 $\Lambda = \mathbb{Z}^r$ 和其上的一个对称双线性形式 $\langle , \rangle : \Lambda \times \Lambda \to \mathbb{R}$。如果双线性形式满足 $\langle , \rangle : \Lambda \times \Lambda \to \mathbb{Z}$ 则称晶格是**整的** (integral)。设 $a_1, ..., a_r \in \Lambda$ 是晶格的基，我们把 $|\Lambda| = |(\langle a_i, a_j \rangle)_{1 \le i,j \le r}|$ 称为晶格的行列式。如果整晶格有 $|\Lambda| = \pm 1$，我们就称晶格是**幺模的** (unimodular)。如果幺模晶格满足 $\forall a \in \Lambda, 2 \mid \langle a, a \rangle$，就称晶格是**偶的** (even)。通常我们会考虑 $\mathbb{R}^n$ 中的晶格，并使用其自带的内积运算 $\langle x, y \rangle = \sum x_i y_i$，我们记 $|a| = \sqrt{\langle a, a \rangle}$，于是我们有下面的定理。

定理 2.2 (Leech **晶格**): *存在唯一的晶格 $\Lambda_{24} \in \mathbb{R}^{24}$ 满足，Λ_{24} 是偶幺模的并且 $\forall 0 \neq a \in \Lambda_{24}, |a| \ge 2$。*

由于 Λ_{24} 是一个交换群，故可以导出自同构群 $Aut(\Lambda_{24})$，此时我们定义

$$\text{Co}_0 = \{g \in Aut(\Lambda_{24}) \mid \forall a, b, \langle g(a), g(b) \rangle = \langle a, b \rangle\}$$

令 $1, -1 \in Aut(\Lambda_{24})$ 分别表示恒等和坐标去负号，我们把 $\text{Co}_1 = \text{Co}_0 / \{-1, 1\}$ 称为 **Conway 群**。顶点代数 (vertex algebra) 具有多种性格迥异的等价定义，由于我们的主题是魔群月光，所以我们采用证明作者 Borcherd 的定义。

定义 2.3: *设 V 是线性空间，且配备了一个无穷个双线性乘法。我们以 $n \in \mathbb{Z}$ 来区分这些乘法 $V \times_n V \to V, (a, b) \mapsto a_n b = a_n(b), a_n \in End(V)$ 并且满足*

(1)$\forall a, b \in V$ 存在足够大的 $n \in \mathbb{Z}$ 使得 $a_n b = 0$

(2) 存在 $1 \in V$ 使得 $\forall n \ge 0, a_n 1 = 0$ 且 $a_{-1} 1 = a$

(3) 乘积满足 Borcherds 恒等式

$$\sum_{i \in \mathbb{Z}} C_m^i (a_{q+i} b)_{m+n-i} c = \sum_{i \in \mathbb{Z}} (-1)^i C_q^i (a_{m+q-i}(b_{n+i} c) - (-1)^q b_{n+q-i}(a_{m+i} c))$$

则把 V 称为一个顶点代数 (vertex algebra)。

在经典定义中，顶点代数的成分为 $(V,|0\rangle,T,Y)$，$V=V_{\bar{0}}\oplus V_{\bar{1}}$ 称为**状态空间**，$|0\rangle\in V_{\bar{0}}$ 称为**真空向量**，$T\in\mathrm{End}(V)$ 称为**无限转化协变算子**，$Y:V\to\mathrm{End}(V)[[z,z^{-1}]]$ 称为**状态场对应**，当然这些成分是存在性的并且满足一定性质。从经典定义到 Borcherd 定义，只需状态场对应即可

$$Y(a,z)=Y(a)(z)=\sum_{n\in\mathbb{Z}}a_nz^{-n-1},a\in V,a_n\in\mathrm{End}(V)$$

而且这个定义是双向的，其给出了 Borcherd 定义到经典定义中的状态场对应，在 Borcherd 定义中存在的 1 对应到经典定义中的 $|0\rangle$，而线性变换则是由 $T:V\to V,a\mapsto a_{-2}1=a_{-2}|0\rangle$ 给出。所以 Borcherd 定义实际是更为简洁的，不过为了适应各种书籍，我们还是将这些符号全部用上比较好 $(V,1=|0\rangle,T,Y,a_n)$，然后引入进一步的概念

定义 2.4: 设 $(V,1=|0\rangle,T,Y,a_n)$ 是顶点代数，$V=\oplus_{n\in\mathbb{Z}}V_n$ 是分次向量空间，满足 $\dim V_n<\infty$(有限维) 且足够小的 n 有 $V_n=0$，对 $v\in V_n$ 我们记 $n=\mathrm{wt}v$(权重) 或者 $n=\deg v$(次数)，如果存在 $\omega\in V$(称之为共形向量)，设

$$Y(\omega,z)=\sum_{n\in\mathbb{Z}}\omega_nz^{-n-1}=L(z)=\sum_{n\in\mathbb{Z}}L_nz^{-n-2}$$

满足下面的性质

(1)[Virasoro 代数]$\exists c_V\in\mathbb{C},[L_m,L_n]=(m-n)L_{m+n}+\frac{1}{12}m(m^2-1)\delta_{m+n,0}c_V$

(2)[共形权重]$L_0v=\mathrm{wt}(v)v$

(3)[转化算子]$T=L_{-1}$

则称 V 是一个顶点算子代数 (VOA,Vertex Operator Algebra)。

于是通过上面的性质，顶点算子代数可以记为 $(V,1=|0\rangle,\omega,Y,a_n)$，即两个特殊元 $1,\omega$ 和一个映射 Y，另外性质 (1) 也给出了一个常数 c_V，我们把它称为顶点算子代数的**中心荷** (central charge)。值得注意的是顶点代数是一个极其庞大的理论，因此我们所能做的就是提一下然后引出我们的主角，它是顶点代数的一个典例，不过并不是 Heisenberg 代数，而是月光模 (moonshine module)$V^\natural$。Lie 代数挺熟悉的吧？就是把代数上的乘法结构替换成了括号 $[,]$ 并满足一系列的性质，线性空间的自同态 $\mathrm{End}(V)$ 上自带一个 Lie 代数结构 $[A,B]=AB-BA$，因此我们在之前能轻松地使用符号 $[L_m,L_n]$。对于一个域 F 上的 Lie 代数 $\mathfrak{g}$，它作为一个向量空间于是我们自然可以拿出其上的一个对称双线性形式 $\langle,\rangle:\mathfrak{g}\times\mathfrak{g}\to F$，并假设其是 $\mathfrak{g}$ 不变的 $\langle[x,y],z\rangle=\langle x,[y,z]\rangle$；$F[t,t^{-1}]$ 是 F 上的交换结合代数，由洛朗级数组成 $\sum_{n=k}^{t}a_nt^n,a_n\in F$；$F^1$ 表示 F 上的一维线性空间，于是我们可以构造一个新的线性空间

$$\hat{\mathfrak{g}}=\mathfrak{g}\otimes_F F[t,t^{-1}]\oplus F^1$$

并定义其上的乘法 $\langle,\rangle:\hat{\mathfrak{g}}\times\hat{\mathfrak{g}}\to\hat{\mathfrak{g}}$ 为

$$\forall g\in\hat{\mathfrak{g}},c\in F^1,[g,c]=[c,g]=0$$

$$\forall x,y\in\hat{\mathfrak{g}},f,g\in F[t,t^{-1}],[x\otimes f,y\otimes g]=[x,y]\otimes fg+\langle x,y\rangle(df\cdot g)_0$$

从而形成一个 Lie 代数，我们把 $\hat{\mathfrak{g}}$ 称为 $(\mathfrak{g}, \langle , \rangle)$ 的**仿射代数** ((untwisted) affine algebra)。接着我们只考虑复空间 $F = \mathbb{C}$，为了区分两个一维复线性空间，我们加一个尾巴 $\mathbb{C}c_1, \mathbb{C}c_2$ 以示差别，并继续构造 Lie 代数为

$$\tilde{\mathfrak{g}} = \hat{\mathfrak{g}} \rtimes \mathbb{C}^1 = \mathfrak{g} \otimes_{\mathbb{C}} \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}c_1 \oplus \mathbb{C}c_2$$

$$[x \otimes t^m + ac_1 + bc_2, y \otimes t^n + a'c_1 + b'c_2] = [x, y] \otimes t^{m+n} - x \otimes b'mt^m + y \otimes bnt^n + \langle x, y \rangle m\delta_{m+n,0}c_1$$

这是一个十分重要的仿射 Kac-Moody 代数，我们来介绍一番吧。如果矩阵 $A = (a_{ij})$ 满足，$a_{ij} \in \mathbb{Z}$、$a_{ii} = 2$、$a_{ij} \leq 0, i \neq j$、$a_{ij} = 0$ 当且仅当 $a_{ji} = 0$，则称 A 是**广义嘉当矩阵**，我们把由广义嘉当矩阵生成的 Lie 代数称为 **Kac-Moody 代数**，如果存在 $u \succ 0$(即所有坐标大于 0) 使得 $Au = 0$，则称这个 Kac-Moody 代数是**仿射**的。

定义 2.5: (1) 设 $\mathfrak{g}$ 是复半单 Lie 代数，如果一个复子空间 $\mathfrak{h} \subset \mathfrak{g}$ 满足，$\forall h_1, h_2 \in \mathfrak{h}, [h_1, h_2] = 0$、$\forall x \in \mathfrak{g} (\forall h \in \mathfrak{h}, [h, x] = 0 \Rightarrow x \in \mathfrak{h})$、$\forall h \in \mathfrak{h}, \mathrm{ad}h$ 可对角化，则称 $\mathfrak{h}$ 是 $\mathfrak{g}$ 的 **Cartan** 子代数。

(2) 如果一个非零线性函子 $\alpha : \mathfrak{h} \to \mathbb{C}$ 满足 $\forall h \in \mathfrak{h}, \exists x \in \mathfrak{g}, [h, x] = \alpha(h)x$ 则称 α 是 $\mathfrak{g}$ 的一个根。于是定义根空间为

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid \forall h \in \mathfrak{h}, [h, x] = \alpha(h)x\}$$

我们用 Φ 表示 $\mathfrak{g}$ 所有根构成的集合，则可以证明一个重要的分解定理

$$\mathfrak{g} = \mathfrak{h} \oplus (\oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha)$$

我们假设 $\mathfrak{g}$ 有限维单 Lie 代数，则容易得到 $\dim \mathfrak{g}_\alpha = 1$ 且 $[\mathfrak{h}, \mathfrak{g}_\alpha] = \mathfrak{g}_\alpha$。我们设 $\Delta = \{\alpha_1, ..., \alpha_r\} \subset \Phi, r = \dim \mathfrak{h}$ 是基，即任意根都可以由它们以整系数线性表示，我们把自由交换群

$$Q = \mathbb{Z}\alpha_1 \oplus ... \oplus \mathbb{Z}\alpha_r$$

称为 $\mathfrak{g}$ 的**根格** (root lattice)。在上面的基础上，我们进一步构造 $\tilde{\mathfrak{g}}$ 的一个子代数为

$$\tilde{\mathfrak{h}} = \oplus_{n<0} (\mathfrak{h} \otimes t^n)$$

从而构造一个 $\tilde{\mathfrak{g}}$-模为 (其中 $S(V)$ 表示线性空间 V 上的对称代数)

$$V_Q = S(\tilde{\mathfrak{h}}) \otimes_{\mathbb{C}} \mathbb{C}[Q]$$

具体内容需要给出作用 $\tilde{\mathfrak{g}} \times V_Q \to V_Q$，对于 $g \otimes t^n, g \notin \mathfrak{h}$ 或 $ac_1 + bc_2$ 均为恒等映射，故主要考虑 $h \otimes t^n \in \tilde{\mathfrak{g}}, h \in \mathfrak{h}$。当 $n = 0$ 时，有 $1 \otimes h(0)(V_Q)$，$1 \in \mathrm{End}(S(\tilde{\mathfrak{h}}))$ 为恒等映射，$h(0) \in \mathrm{End}(\mathbb{C}[Q])$ 满足 $h(0)e^\gamma = \gamma(h)e^\gamma$，其中 $\gamma \in Q$ 且 e^γ 作为群代数 $\mathbb{C}[Q]$ 的基；当 $n \neq 0$ 时，有 $h(n) \otimes 1(V_Q)$，$1 \in \mathrm{End}(\mathbb{C}[Q])$ 为恒等映射，$h(n) \in \mathrm{End}(S(\tilde{\mathfrak{h}}))$ 满足，$n < 0$ 时乘以 $h \otimes t^n$，$n > 0$ 时求导。考虑 $x_\alpha \otimes t^n \in \mathfrak{g}$ 在 V_Q 上的作用可以得到一个自同构 $x_\alpha(n) \in \mathrm{End}(V_Q)$，从而我们可以往顶点代数进行靠拢

$$Y(\alpha,z)=\sum_{n\in\mathbb{Z}}x_\alpha(n)z^{-n-1}$$

基础的代数内容复习地差不多了，接下来我们的目的是说明 Λ_{24} 是某个 Lie 代数的根格，实际上在整个系统中起作用的是 Cartan 子代数 $\mathfrak{h}$，因此我们不如直接从格把它构造出来

$$V_\Lambda=S(\tilde{\mathfrak{h}})\otimes_{\mathbb{Z}}\mathbb{C}[\Lambda_{24}],\mathfrak{h}=\Lambda_{24}\otimes_{\mathbb{Z}}\mathbb{C}$$

我们记 $\hat{\Lambda}=\Lambda_{24}/2\Lambda_{24}$，通过分解 $\mathbb{C}[\Lambda_{24}]=\mathbb{C}[\hat{\Lambda}]/(\kappa+1)\mathbb{C}[\hat{\Lambda}]$ 我们得到一个 $\kappa\in\hat{\Lambda}$，或简单点我们让它来自下面的正合列

$$1\to\langle\kappa\rangle\to\hat{\Lambda}\to\Lambda_{24}\to 1$$

此时我们任意选取一个 Λ_{24}-模为 T 满足 $\forall v\in T,\exists\xi,\kappa v=\xi v$，于是可以构造一个扭空间为

$$V_\Lambda^T=S(\tilde{\mathfrak{h}})\otimes_{\mathbb{Z}+\frac{1}{2}}T$$

接着我们令 θ_0 在这两个空间上的作用为

$$\theta_0:\hat{\Lambda}\to\hat{\Lambda},a\mapsto a^{-1}\kappa^{\frac{\langle a,a\rangle}{2}}$$

$$\theta_0:V_\Lambda\to V_\Lambda,x\otimes i(a)\mapsto\theta_0(x)\otimes i(\theta_0(a))$$

$$\theta_0:V_\Lambda^T\to V_\Lambda^T,x\otimes\tau\mapsto-\theta_0(x)\otimes\tau$$

对于作用 $\sigma:V\to V$ 我们使用 V^σ 表示不变子空间，于是我们定义

$$V^\sharp=V_\Lambda^{\theta_0}\oplus(V_\Lambda^T)^{\theta_0}$$

并把它称为**月光模** (Moonshine module)。月光模 $V^\sharp$ 具有顶点算子代数的结构，其存在一个中心荷为 24 的共形向量，并且有着相应的分次结构分解

$$V^\sharp=\bigoplus_{n\in\mathbb{Z}}V_n^\sharp$$

我们可以得到一些简单的结论 $\forall n<-1,V_n^\sharp=0$，且有

$$\dim V_{-1}^\sharp=1,\dim V_0^\sharp=0,\dim V_1^\sharp=196884$$

我们把 $\mathscr{B}=V_1^\sharp$ 称为 **Griess 代数**，实际上我们有

$$\sum_{n\in\mathbb{Z}}(\dim V_n)q^n=J(z)=q^{-1}+0+196884q+...,q=e^{2\pi iz},z\in\mathbb{H}$$

虽然大家可能经常见到这个魔群与模形式的联系式，但这并不是魔群月光猜想的内容，我们还是继续来构造魔群吧。最简单的方式就是 Griess 代数上的等距自同构

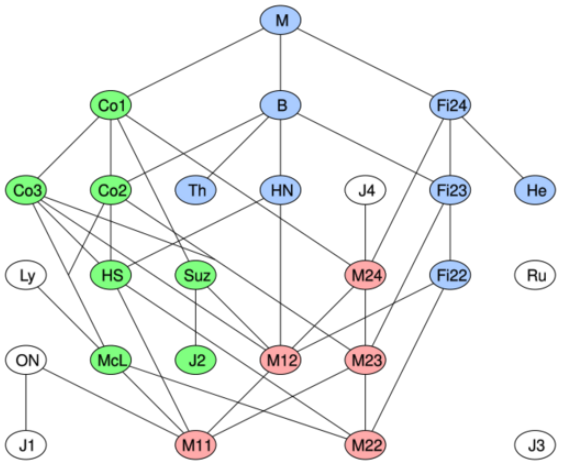
$$\mathbb{M}=\{\sigma\in Aut(\mathscr{B})\mid\langle\sigma(x),\sigma(y)\rangle=\langle x,y\rangle\}$$

另一种定义可以推出这个性质，或者说我们以这个为定义可以推出下面的性质 (一个正合列)

$$1 \to \hat{\Lambda}/K \to C \to \mathrm{Co}_1 \to 1, K = \{\theta_0(a)a^{-1} \mid a \in \hat{\Lambda}\}$$

$$\mathbb{M} = \langle C, \sigma \rangle \subset Aut(V^\sharp), \sigma V^\sharp = V^\sharp, \sigma^2 = 1$$

其表示魔群 $\mathbb{M}$ 是 Conway 群 Co_1 过 $\hat{\Lambda}/K$ 的扩张进一步扩大生成的群，所以虽然魔群 $\mathbb{M}$ 是单群，但这只意味着它没有正规子群，子群倒是一大堆，下面是散在单群的包含关系



其中只有 6 个贱民不是它的子群。我知道就算到了这里，你对魔群 $\mathbb{M}$ 也是懵懂的，要想真正完全搞懂这个群，最好的办法是给出乘法表，但奈何这个群太大不好给出，不过可以通过表示算出来，即Python 实现。在魔群月光猜想证明的文章中，作者也说了，“幸运地是我们不需要知道太多构造的细节”，换句话说，我们讨论魔群，使用魔群，需要的是它的性质，需要的是我们站在巨人的肩膀上，而不是从繁琐的定义中寻找微乎其微的出路。

3 猜想

知道了月光模 $V^\sharp = \bigoplus_{n\in\mathbb{Z}} V_n^\sharp$ 和魔群 $\mathbb{M}$ 这两个对象就能开始探究我们的魔群月光猜想了，另外读者还需要知道，我们导出魔群是将其视为某个线性空间上的自同构子群，通过这种方式，在给出魔群定义的时候就已经自带了一个表示

$$\rho_{\mathbb{M}} : \mathbb{M} \to GL(V^\sharp)$$

或者写成群作用的形式 $\mathbb{M} \times V^\sharp \to V^\sharp, (g, v) \mapsto gv$，它是魔群的一个无限维表示。关于 $SL_2(\mathbb{Z})$ 和模形式的那些事，我觉得没有重复的必要，简单来讲任一同余子群 $\Gamma \subset SL_2(\mathbb{Z})$ 在扩充半平面上的作用 $\Gamma \setminus \overline{\mathbb{H}}(\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\})$ 可以形成一个紧黎曼曲面。对于群 $G \subset SL_2(\mathbb{Z})$，如果黎曼面 $G \setminus \overline{\mathbb{H}}$ 的亏格为 0，则称 G 的亏格为零，此时根据单值化定理，存在黎曼面同构

$$J_G : G \setminus \overline{\mathbb{H}} \to P\mathbb{C}^1$$

显然它可以看成关于同余子群 G 的模函数大军中的一员，(不一定是模形式) 因为上述的两个集合都包含了无穷原点，所以非全纯是完全有可能的，另一方面这个同构至少有两个可控参数系数 $aJ_G \in \mathrm{End}(G\backslash\overline{\mathbb{H}}, P\mathbb{C}^1)$ 和常数项 $J_G+b \in \mathrm{End}(G\backslash\overline{\mathbb{H}}, P\mathbb{C}^1)$，所以我们进一步限制首系数为 1 且常数项为 0，从而得到了唯一的黎曼面同构，我们把它称为 G 的**典型同构** (normalized Hauptmodul)。下面是几个典型的例子

$$J_{\Gamma_0(2)}(z) = q^{-1} + 276q - 2048q^2 + 11202q^3 - 49152q^4 + 184024q^5 + ...$$
$$J_{\Gamma_0(13)}(z) = q^{-1} - q + 2q^2 + q^3 + 2q^4 - 2q^5 - 2q^7 - 2q^8 + q^9 + ...$$
$$J_{\Gamma_0(25)}(z) = q^{-1} - q + q^4 + q^6 - q^{11} - q^{14} + q^{21} + q^{24} - q^{26} + ...$$

请读者注意椭圆曲线得到的不变量 $j(z) = \frac{1728g_2^3(z)}{\Delta(z)}$ 和魔群中见到的 $J(z) = J_{SL_2(\mathbb{Z})}(z)$ 的关系为 $j(z) = J(z) + 744$。对于 $g \in \mathbb{M}$，在表示 $\rho_{\mathbb{M}} : \mathbb{M} \to GL(V^\natural)$ 中根据分次的特性，我们可以对应地把表示矩阵也给直和分解了

$$\rho(g) = \bigoplus_{n\in\mathbb{Z}} (g|V_n^\natural)$$

根据之前的特性可知 $g|V_{-1}^\natural$ 是单值，$g|V_0^\natural$ 为空，$g|V_1^\natural$ 为 196884 阶方阵并对应 Griess 代数 $\mathscr{B}$ 上的表示等等，此时可以构造一个复级数

$$T_g(z) = \sum_{n\in\mathbb{Z}} \mathrm{tr}(g|V_n^\natural)q^n = q^{-1} + \mathrm{tr}(g|V_1^\natural)q + \mathrm{tr}(g|V_2^\natural)q^2 + ...$$

我们把它称为 g 的 **McKay-Thompson 级数**，显然如果取单位元 $g = 1$ 则有 $\mathrm{tr}(g|V_n^\natural) = \dim V_n^\natural$，则有 $T_1(z) = J(z)$，因此如果我们试着把上面的联系进行推广的话就得到了我们的**魔群月光猜想**。

命题 3.1 (Conway-Norton conjecture): *对每一个 $g \in \mathbb{M}$，存在一个亏格为 0 的子群 $G \subset SL_2(\mathbb{R})$ 使得*

$$T_g(z) = J_G(z)$$

你可能注意到了上面的群有点不太一样，实际上，我们要给 $G \subset SL_2(\mathbb{R})$ 加上一个可被 $SL_2(\mathbb{Z})$ **约化** (commensurable)，简单来讲就是下面的两个指数是有限的

$$[SL_2(\mathbb{Z}) : SL_2(\mathbb{Z}) \cap G], [G : SL_2(\mathbb{Z}) \cap G]$$

从而我们可以说明 $G\backslash\overline{\mathbb{H}}$ 同样可以形成一个紧黎曼曲面，进而可以得到一个 Hauptmodul，也就是说后面的内容不过是附加的罢了，干脆得到所有的 Hauptmodul，并说明所有的 McKay-Thompson 级数都是 Hauptmodul 也是没问题的。

4 证明

你觉得我真的会讲证明吗？当然不会了，因为就算是 Borcherds 自己的内容也是不够支撑完整证明的，需要很多前人的经验做铺垫，因此我所能做的就是告诉证明的基本路径并告诉你，Borcherds 完成了一些什么样的工作。

魔群内容

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

设子群 $\Gamma_0(N) \leq SL_2(\mathbb{R})$，我们记正规化子为

$$\mathcal{N}(N) = N_{SL_2(\mathbb{R})}(\Gamma_0(N)) = \{a \in SL_2(\mathbb{R}) \mid a\Gamma_0(N)a^{-1} = \Gamma_0(N)\}$$

设 h 是满足 $h^2 \mid N$ 的 24 的最大因子，并做因式分解 $N = hn$，接着我们再记一个子群

$$T(N) = \{\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} \in SL_2(\mathbb{R}) \mid a, b, c, d \in \mathbb{Z}, ad - bcn/h = 1\}$$

则有 $\Gamma_0(N) \lhd T(N)$，因此 $T(N) \subset \mathcal{N}(N)$。显然在 $SL_2(\mathbb{R})$ 中，$T(N)$ 与 $\Gamma_0(n/h)$ 是共轭的，还能证明分解

$$\mathcal{N}/T \cong \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$$

同构右边因子 $\mathbb{Z}_2$ 的个数为 n/h 中不同素因子的个数，于是在魔群月光中，我们会限制群 G 进一步满足条件

$$\exists N, T(N) \subset G \subset \mathcal{N}(N)$$

当 $N = p$ 为素数时，$h = 1, T(N) = \Gamma_0(p)$ 且有

$$[\mathcal{N}(p) : T(p)] = 2$$

在 [8] 中证明了，$\mathcal{N}(p)$ 的亏格为 0 当且仅当

$$p \in \{2, 3, 5, 7, 11, 17, 19, 23, 29, 31, 41, 47, 59, 71\}或p \mid |\mathbb{M}|$$

因为认为魔群和模形式具有联系是十分自然的想法，另一方面我们对诱导出 Hauptmodul 的群的限制也是合理的。我们注意到相似矩阵的迹是相同的，因此共轭元表示的迹也是相等的，更进一步，我们有

$$\forall h \in \mathbb{M}, T_g(z) = T_{hgh^{-1}}(z)$$

因此考虑魔群月光时，我们主要应该关注共轭类中的代表元，我们先来考虑 $\mathbb{M}$ 中有哪些共轭类？总共有 194 个 (其对应 194 个不可约复表示)，在这里可以看到所有的共轭类，它们一般以“数字 (1-119)[4]+ 字母 (A-J)[5]”进行表示，例如 1A、2B、6E 等，它可以由两个元 $a \in 2B, b \in 3B$ 进行表现 (来自这里，注意不是表示)

$$(\text{Hurwitz group})\mathbb{M} = \langle a, b \mid a^2, b^3, (ab)^7 \rangle$$

[4]表示元素的阶

[5]区别相同阶下不同的共轭类

它还有一种通过 Coxeter 群 Y_{443} 的表现，比较复杂，有兴趣的读者可以看这篇文章 [6, 7]。在共轭类表中还展示了中心化子的大小，例如 $|C_{\mathbb{M}}(1A)| = |\mathbb{M}|$，因此其共轭类的大小为 $|\mathbb{M}|/|C_{\mathbb{M}}(1A)| = 1$，实际上这个共轭类 1A 包含的就是 $\mathbb{M}$ 的单位元。上面我们说群 $T(N) \subset G \subset \mathcal{N}(N)$ 是存在性的，而这个存在性是可以构造的，令 $g \in \mathbb{M}$，设 N 是满足下式的最小正整数 (此处的作用方式为模群元素作用于模函数)

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} T_g(z) = T_g(z)$$

设 n 是 g 的阶 (即 $g^n = 1, g^k \neq 1, 1 \leq k < n$)，则有 $n \mid N$，再令 $h = N/n$，则进一步有 $h \mid 24$，此时可以构造出群为

$$G_g = \{A \in SL_2(\mathbb{R}) \mid \exists \zeta \in \mathbb{C}, \zeta^h = 1, AT_g(z) = \zeta T_g(z)\}$$

此时就能通过这个群导出 $J_{G_g}(z)$ 了，从构造方式来看 $J_{G_g} = T_g(z)$ 的可能性确实很大。有了这些基础，我们来说一下魔群月光猜想提出的论文 [3] 中一些重要表的含义。表 1，就是一系列数字

$$1, 196883, 21296876, 842609326, 18538750076, 19360062527, 293553734298, ...$$

它是 $\mathbb{M}$ 全部不可约表示的维数，表 1a，是 $j(z)$ 函数的系数 $a_i = \dim V_i^\sharp (-1 \leq i \leq 24)$ 和前几个分次表示的不可约分解，例如第七行

$$333202640600 \;\; a_5, H_5 = 4 \;\; 5 \;\; 3 \;\; 2 \;\; 1 \;\; 1 \;\; 1$$

说明 $j(z) = q^{-1} + 744 + ... + 333202640600q^5 + ..., \dim V_5^\sharp = 333202640600$，并且有相应的表示分解

$$\dim V_5^\sharp = 4{\cdot}1{+}5{\cdot}196883{+}3{\cdot}21296876{+}2{\cdot}842609326{+}18538750076{+}19360062527{+}293553734298$$

表 2，是共轭类的一些性质，“name” 和 “symbol” 顾名思义，“primepowers” 表示素数次指数映射可能落在的共轭类，“F” 原文献找不到了无从考证，不过目前来看起不来什么作用，“D” 和 “C” 都是 $g \in \mathbb{M}$ 对应导出的同余子群 $G_g \leq SL_2(\mathbb{Z})$ 的两个性质，可以用来区分拥有相同阶的共轭类，例如 26A 和 26B，它们导出的同余子群的尖点个数分别是 1 和 2，最后是中心化子的阶数，使用 “魔群阶数除以中心化子的阶数” 可以得到共轭类的元素个数。表 2a，是几个具体的中心化子实例，主要由一些常见群构造出来。表 3 和表 3a，是诱导出的模形式的一些性质，我们基本用不到。真正在证明中起作用的是表 4，它给出了诱导模形式 $J_{G_g}(z) = \sum_{i=-1}^{\infty} c_g(i) q^i$ 的前 12 个系数 $c_g(i), -1 \leq i \leq 10$，第一个系数 $c_g(-1) = 1$ 是固定的，第二个系数 $c_g(0) = 0$ 本来应该也是固定的，但这样就太浪费格子了，于是就令它表示 Rademacher 常数，这是什么我也不知道，不过它与我们的证明没啥关系就别管了。

复现公式

在魔群月光中起决定证明作用的是**复现公式** (replication formulae)，其意思是通过几个数来复现整个函数。这种性质在模形式中，我们其实是见过的，比如对于特征模形式 $f(\tau)=\sum_{i=1}^{\infty}a_iq^i\in M_k(N,\chi)$，我们只需要知道素数处的系数 a_p 就能算出所有整数处的系数

$$a_1=1,a_{p^r}=a_pa_{p^{r-1}}-\chi(p)p^{k-1}a_{p^{r-2}},a_{mn}=a_ma_n,(m,n)=1$$

而我们的希望就是让复现公式发生在“Thompson 级数”和“Hauptmodul”上，前者就是 Borcherds 的主要工作，而后者由于那时模形式的蓬勃发展，导致分散在各个作者中，我们先来讲一讲复现公式的通论，主要在模形式 Hauptmodul 这边。如果离散子群 $G\leq SL_2(\mathbb{R})$ 满足，$\exists N,\Gamma_0(N)\leq G$ 且 $\begin{pmatrix}1&t\\0&1\end{pmatrix}\in G\Rightarrow t\in\mathbb{Z}$，我们就称 G 是**月光型的** (moonshine-type)。我们给定一个函数 $f(z)=q^{-1}+\sum_{n=1}^{\infty}a_nq^n,q=e^{2\pi iz}$，可知对每个 $n\in\mathbb{N}$ 存在唯一的首一多项式 $F_n(z)$ 使得

$$q\to0,F_n(f(z))=\frac{1}{q^n}+O(q)$$

我们将其称为 f 的 **Faber 多项式**，实际上，它具有生成函数

$$\frac{qf'(q)}{z-f(q)}=\sum_{n=0}^{\infty}F_n(z)q^n$$

可以算得

$$F_0(z)=1,F_1(z)=z,F_2(z)=z^2-2a_1,...,F_{n+1}(z)=zF_n(z)-\sum_{k=1}^{n-1}a_{n-k}F_k(z)-(n+1)a_n$$

定义 4.1: 设 $\mathbb{H}$ 上的函数 $f(z)=q^{-1}+\sum_{n=1}^{\infty}a_nq^n$。如果对任意正整数 n 和 $a\mid n$，存在与 $f(z)$ 相同形式的函数 $f_a(z)$ 满足

$$\forall n\geq1,F_n(f(z))=\sum_{\substack{ad=n\\0\leq b<d}}f_a(\frac{az+b}{d})$$

则称 f 是一个复现函数 (replicable function)

比如 $J(z)$ 就是一个复现函数，只不过存在的函数均相等 $J_a(z)=J(z)$，即有

$$F_n(J(z))=\sum_{\substack{ad=n\\0\leq b<d}}J(\frac{az+b}{d})$$

定理 4.1: 我们记 $F_n(f(z))=\frac{1}{q^n}+n\sum_{m=1}^{\infty}H_{m,n}q^m$ 则，$f(z)$ 是复现函数当且仅当，对任意 $mn=rs,(m,n)=(r,s)$ 均有 $H_{m,n}=H_{r,s}$。

对 $f(z)=q^{-1}+\sum_{n=1}^{\infty}a_nq^n$ 的显然系数公式是 $a_n=H_{n,1}$，有关复现函数的一个核心猜想是

猜想 4.2: *任意有理系数的复现函数 $f(z)$，要么是月光型同余子群 G 的 Hauptmodul$J_G(z)$、要么是以下三种函数之一 $(f(z)=q^{-1},f(z)=q^{-1}+q,f(z)=q^{-1}-q)$。*

它其实是魔群月光反过来的猜想，通论虽然还有许多有趣的东西，但我们还是尽快回归正题吧，复现函数最重要的性质就是少量系数的级数决定性质。我们记 $g\in\mathbb{M}$ 对应的 Hauptmodul 为 $J_{G_g}=q^{-1}+\sum_{n=1}^{\infty}c_g(n)q^n$，则有下面四个复现公式 $(k\geq 1)$

$$c_g(4k)=c_g(2k+1)+\frac{1}{2}c_g(k)^2-\frac{1}{2}c_{g^2}(k)+\sum_{j=1}^{k-1}c_g(j)c_g(2k-j)$$

$$\begin{aligned}c_g(4k+1)=&c_g(2k+3)-c_g(2)c_g(2k)+\frac{1}{2}c_g(2k)^2+\frac{1}{2}c_{g^2}(2k)\\&+\frac{1}{2}c_g(k+1)^2-\frac{1}{2}c_{g^2}(k+1)+\sum_{j=1}^{k}c_g(j)c_g(2k+1-j)\\&+\sum_{j=1}^{k-1}c_{g^2}(j)c_g(4k-4j)+\sum_{j=1}^{2k-1}(-1)^jc_g(j)c_g(4k-j)\end{aligned}$$

$$c_g(4k+2)=c_g(2k+2)+\sum_{j=1}^{k}c_g(j)c_g(2k+1-j)$$

$$\begin{aligned}c_g(4k+3)=&c_g(2k+4)-c_g(2)c_g(2k+1)-\frac{1}{2}c_g(2k+1)^2+\frac{1}{2}c_{g^2}(2k+1)\\&+\sum_{j=1}^{k+1}c_g(j)c_g(2k+3-j)+\sum_{j=1}^{k}c_{g^2}(j)c_g(4k+2-4j)\\&+\sum_{j=1}^{2k}(-1)^jc_g(j)c_g(4k+2-j)\end{aligned}$$

公式看得眼花缭乱了，其实不要紧，只要知道这样一件事实，如果我们知道了所有 $g\in\mathbb{M}$ 对应的系数 $c_g(1),c_g(2),c_g(3),c_g(5)$，就能计算出所有 $c_g(i),i=4,i>5$，至于 $c_{g^2}(i)$ 也不要紧反正它也是 $\mathbb{M}$ 中的元素。对于所有 Hauptmodul 的复现公式，由 M.Koike 在论文“On Replication Formula and Hecke Operators”中证明，但这篇文章已经无从考证，找不到了，鉴于它是研究较为深入的模函数的内容，就姑且当它是对的吧。

完成证明

通过上面的内容我们知道，要想完成魔群月光的证明，只需要完成两件事，一是证明 Thompson 级数的复现公式，二是前几项系数的比较，后者有多种方式来计算，比如直接从表示，又或者通过 Dedekind 函数 $\eta(z)$ 等等，所以证明的核心放在了第一件事上，而这也正是 Borcherds 在证明论文 [2] 中 3-8 节的主要工作 (有些性质分散到了 Borcherds 的一些其它的文章中)，第 9 节就是叙述我们所说的证明过程。由于在代数这边，我们并不具备分析性质，所以 Thompson 级数复现公式的证明和 Hauptmodul 复现公式的证明并不是一回事，在已有内容的前提下，前者显

然更困难些。证明过程就不讲了，用到了广义 Kac-Moody 代数、无鬼定理 (No-ghost theorem)、魔群 Lie 代数 (monster Lie algebra) 等工具，最终的结果都是得到复现公式的核心推导用公式

$$p^{-1}\exp(-\sum_{i>0}\sum_{m>0,n\in\mathbb{Z}}\mathrm{Tr}(g^i \mid V_{mn})\frac{p^{mi}q^{ni}}{i}) = \sum_{m\in\mathbb{Z}}\mathrm{Tr}(g^i \mid V_m)p^m - \sum_{n\in\mathbb{Z}}\mathrm{Tr}(g^i \mid V_n)q^n$$

从这个公式推出 4 个复现公式，其实还有较长的一段路，不过都是共用的性质，所以在论文中也没有说明推出过程，据说详细的过程在 M.Koike 的那篇论文里，所以我也没办法把它写出来，就只能到此为止了。

5 尾声

遗憾地告诉你，有关魔群月光的内容全部结束了，由于参考资料的过于稀缺，这也是无可奈何的，还请见谅。

参考文献

[1] R. E. Borcherds, *Pdf, dvi and plain tex files of papers and preprints by r. e. borcherds*, https://math.berkeley.edu/~reb/papers/index.html, 1984.

[2] Richard E. Borcherds, *Monstrous moonshine and monstrous lie superalgebras*, Inventiones mathematicae **109** (1992), 405–444.

[3] J. H. Conway and S. P. Norton, *Monstrous Moonshine*, Bulletin of the London Mathematical Society **11** (1979), no. 3, 308–339.

[4] John H. Conway, *A simple construction for the fischer-griess monster group*, Inventiones mathematicae **79** (1985), 513–540.

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

[6] A.A Ivanov, *Constructing the monster via its y-presentation*, Combinatorics, Paul Erds is Eighty, Bolyai Society Mathematical Studies **Vol. 1** (1993), 253–270.

[7] ———, *Y-groups via transitive extension*, Journal of Algebra **218** (1999), no. 2, 412–435.

[8] Andrew P. Ogg, *Automorphismes de courbes modulaires*, 1975.

[9] Robert Arnott Wilson, *The finite simple groups*, 2009.

[10] 孟道骥, 抽象代数 *ii:* 结合代数, 科学出版社, 2011.

[11] 逯晓零, 代数分析几何简介, 地址, 2023.

[12] ———, 数论大观园, 2023.

[13] ———, 朗兰兹纲领简介, 地址, 2023.