數學傳播 35卷4期, pp. 23-33

怪物與月光 (Monster and Moonshine)
—— 淺談1998年 Fields Medal 得主 Richard Borcherds 的數學工作[1]

演　講 : 林正洪
時　間 : 民國100年11月24日
地　點 : 成功大學 國家理論科學研究中心(南區) 204室
整　理 : 陳麗伍

介紹 (成功大學數學系許瑞麟主任): 很高興今天邀請到我們早年的同伴從中研院回來給這場關於1998年菲爾茲獎得主 Richard Borcherds 數學工作的演講。光看演講的題目就很有吸引力, 我希望大家可以眞正學到些東西, 就讓我們開始吧。

今天的演講題目「怪物與月光」有點不大像數學。如果你來這邊覺得會聽到我談月光怪獸, 對不起, 今天不談月光怪獸, 也不說月光之下的怪獸, 我們今天談的是實實在在的數學問題。也許你會感到疑惑, 爲什麼名字那麼奇怪, 怪獸與月光, 我希望大致解釋一下爲什麼用這樣的名字來看數學問題, 另一個很重要的問題是 Richard Borcherds 在這個月光與怪獸之間做了些什麼事情, 讓他獲得1998年的菲爾茲獎, 這是最主要要說的內容, 當然這之間多少會提到些數學, 有些簡單, 有些較難。但是我希望大家可以趁此機會了解, 其實數學家並不是像大家想像中那樣死板, 我們想的東西其實有很多是跟一般人一樣。

首先, Monster 是什麼, 第二個問題 Moonshine 月光是什麼, 爲什麼用那麼奇怪的名字命名數學問題。當然, 除了解釋是什麼之外, 也會提到爲什麼是有趣的, 或是說爲什麼很特別。接下來, 簡單介紹一下 Richard Borcherds。他的第一篇論文發表的時候只有20出頭, 在25、26歲時就有些非常重要的結果。我也會簡單地講一下他做了什麼事情, 有那些貢獻令我們對 Monster 和 Moonshine 有更好的瞭解。

[1]註: 感謝林正洪教授同意本刊刊載他於成功大學演講的演講紀錄。本文下方註解爲本刊所加, 非原稿所有, 希望能方便讀者閱讀, 並請讀者將本篇與本期「有朋自遠方來」一併閱讀。

什麼是 Monster? 什麼是 Moonshine? 要瞭解這個問題必須要先知道一般人對 Monster 與 Moonshine 的印象是什麼, 接著才延伸到數學問題, 然後你就會發現 Monster 與 Moonshine 這兩個稱呼是有其意義。一旦瞭解它背後的意義, 就會發現這兩個命名一點都不奇怪。

那什麼是 Monster? 根據字典的定義, 所謂的怪物一般是想像的、既大又醜又可怕。我們的重點就在大與可怕。美醜是主觀的我們忽略不多談, 但是, 大是一定要夠的。日本人對 Monster 有其他的想法, 他們的怪物可以是小巧可愛的, 例如皮卡丘等, 與之前的定義相反。目前研究 Monster 的數學家中有很多是日本人, 對他們來說這是非常漂亮、可愛的。

那麼 Moonshine 是什麼? 用中文來說就是月光, 意思是什麼? 一種解釋是不是很亮、模糊不清、但漂亮的。另一種比較靠近我們今天主題的解釋是不大實在、空妄的, 英文有一句厘語「moonshine in the water」, 也就是中文的水中月, 看得到摸不到, 不實在, 虛無飄渺的。所以某種程度來說, 爲什麼命名爲月光, 是因爲它是不實在的, 沒有可以觸摸的方法, 不知道會發生什麼事情。另一種解釋是英文的厘語, moonshine 指的是走私或私釀的酒。如果在網路上搜尋 moonshine, 可以看到許多酒精私釀的圖片。等一下大家就會知道爲什麼要命名爲 moonshine, 因爲它就像私釀酒一樣, 還沒有取得合法的資格。

實際上我們所說的 Monster 是什麼, 簡單的說它是個有限群 (finite group)。如果學過代數, 就會知道什麼是有限群, 是在研究些什麼東西。Monster是最大的一個散在單群 (sporadic simple group), 要解釋什麼是單群比較困難, 從簡的解釋就是它沒有正規子群 (normal subgroup)。英文中 sporadic 指的是分散的、不常出現的, 當你研究單群的時候可以發現, 有許多的單群例子, 而 sporadic 是分散的, 沒有一個好的方法說明它是什麼樣的群。在數學裡面若有一個對象 (object) 是 sporadic、exceptional, 也就是不清楚來源, 也不清楚與其它對象之間的關係, 這些東西在某種程度上都是重要的, 必須費心思去研究。

我說它在 sporadic 群中是最大的, 它有多大呢? 這一個群的大小是 $2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$, 也就是 808017424794512875886459904961710757005754368000000000, 長度有54位數。54位數聽起來似乎還好, 但是如果認眞算一下, 是非常可怕的。物理學家說這個數字比我們銀河系中的基本粒子 (中子 neutron、正子 proton) 還多。所以就算想要用電腦處理這個數也是辦不到的, 因爲沒有足夠紀錄的粒子, 尤其當時的電腦還不是很發達。所以當發現有這個既大又可怕的對象 (object) 的時候, 就被命名爲 Monster 怪物。當然在訂名爲 Monster 之前, 也有人稱之爲 Friendly Giant (友善的巨人), 但後來大家還是覺得並不是很友善, 所以還是以 Monster 稱之。

Symbol	**Discoverer**	**Symbol**	**Discoverer**
M_{11}	Mathieu	Co_1	Conway
M_{12}		Co_2	
M_{22}		Co_3	
M_{23}		Fi_{22}	Fischer's 3-transposition groups
M_{24}		Fi_{23}	
$\underline{J_1}$	Janko	Fi'_{24}	
$HJ = J_2$	Hall, Janko	$\underline{LyS}$	Lyons
$\underline{J_3}$	Janko	$\underline{Ru}$	Rudva
$\underline{J_4}$		$\underline{O'N}$	O'Nan
$Held$	Held	$\overline{\mathbb{M}}$ or $\overline{F_1}$	$\overline{\text{Fischer-Griess}}$
HiS	Higman-Sims	$B\mathbb{M}$ or F_2	Fischer's $\{3, 4\}$-transposition group
McL	McLaughlin	Th or F_3	Thompson
Suz	M. Suzuki	Ha or F_5	Harada

Black-involved in the Monster $\mathbb{M}$. Red- not involved in $\mathbb{M}$

圖表 1

Sporadic 群總共有26個不同的群, 其中 Monster 是最大的, 剩下的各有不同的名字, 有5個是 Mathieu 群, Janko[2] 發現了四個, 稱爲 Janko群, Conway[3]發現三個, 是 Conway群, Fischer[4]有三個群, 是 Fisher 群, 其他分別由不同的人發現也都各有命名。在這當中, Monster 和 Baby Monster 也都是由 Fischer 發現的, 不過一般稱爲 Monster 和 Baby Monster, 並沒有用 Fischer 的名字命名。另外, 還有兩個群分別稱爲 Thompson[5] 和 Harada。Harada[6]是我博士班時的指導教授, 從他那邊聽了不少故事, 可以與大家稍作分享。另外, 這個圖表也有稍作區別, 加了上線的就是 Monster 本身, 加了底線的群 與 Monster 沒有直接關係, 黑色的群與 Monster 有直接關係, 是 Monster 的子群或商子群 (quotient subgroup)。一旦清楚理解 Monster 群, 也就知道了其他20個群, 這也是爲什麼大部分的注意力都集中在 Monster 群上, 因爲它不但是最大的群, 還包含了其他20個群。現在大部分的人都稱 Monster 群爲 Fischer-Griess Monster。爲什麼會有人喜歡稱他爲

[2]註: Zvonimir Janko (1932-), 克羅西亞群論學家, 群論中 Janko 群就是以他爲名。
[3]註: John Horton Conway (1937-), 英國數學家, 在組合、幾何、數論、群論、物理等都有很重要的工作。
[4]註: Bernd Fischer (1936), 德國數學家, 以在有限單群的貢獻最爲人所知。
[5]註: John Griggs Thompson (1932-), 美國數學家, 1970年獲頒菲爾茲獎, 2008年獲頒 Abel 獎, 以有限群的研究聞名。
[6]註: Koichiro Harada 原田 耕一郎, 群論學家, 證明了 Gorenstein-Harada 定理。

Friendly Giant, 因爲縮寫 F. G. 同時也是 Fischer 和 Griess[7] 的這兩個姓氏的第一個字母。現在稱 Monster, 則變成了 M。另一種寫法是 F_1、F_2、F_3、F_5, 代表它們與 Fischer 的工作是相關的。

什麼是 Moonshine 呢? 這沒辦法用三言兩語詳細說明, 但是簡單來說它代表 Monster 群指標值 (character) 和數論中一種很重要的函數 — 模函數 (Modular function) 的神秘關係, 是一個完全出乎意料的關係。模函數和群看起來沒有甚麼特別的關係, 在研究數論或黎曼曲面時常會遇到模函數, 但跟有限群好像沒有太大關係。有了這個奇怪的關係, 數學家們第一個想知道的問題就是它是否正確, 第二個問題自然而然地就是爲什麼是正確的。如果是正確的, 有沒有一個好的解釋。當然, 解釋的好壞見仁見智各自認定, 不過總是有一個這樣的關係存在。重點是它把 Monster 的研究推廣到純粹有限群的研究之外, 它帶到數論、李代數、甚至是物理的領域。

在我繼續之前, 先簡單地解釋有限群是什麼。群論可以說是在19世紀初期, 從 Evariste Galois[8]開始的。他有個很重要的工作是有關多項式方程的開方解。他非常的年輕, 過世的時候才21歲, 逝世的原因是與人決鬥。所以可以想像這工作是在18、19歲完成的, 他也曾經入獄, 是個有許多故事的人, 很值得說上一說。爲什麼他那麼重要, 事實上整個有限群論的觀念可說是由他一手所建立的。舉個簡單的例子, 中學的時候學過二次方程式的解, 可以用以下這個特定的方法來做。

$$
\begin{aligned}
& ax^2+bx+c=0 \\
\Rightarrow\ & x^2+\frac{b}{a}x=-\frac{c}{a} \\
\Rightarrow\ & x^2+\frac{bx}{a}+\left(\frac{b}{2a}\right)^2=-\frac{c}{a}+\left(\frac{b}{2a}\right)^2 \\
\Rightarrow\ & \left(x+\frac{b}{2a}\right)^2=\frac{b^2}{4a^2}-\frac{c}{a} \\
\Rightarrow\ & x=\frac{-b+\sqrt{b^2-4ac}}{2a} \quad \text{or} \quad x=\frac{-b-\sqrt{b^2-4ac}}{2a}
\end{aligned}
$$

所以只要利用開方就可以完全解決這個問題。同樣的方法可以套用在三次、四次或更高次的方程式嗎? 如果是三次、四次的方程, 是有類似的方法, 不過解不是這樣清楚、容易, 許多書都可以查到, 但是基本上有個求解的演算法, 只需要利用開方這個程序, 就可以完成。

大約也是在19世紀時, Abel[9]證明了 5次或更高次的方程, 這樣求解的方式是不可行,

[7]註: Robert Griess (1945-), 美國數學家, 詳本期「有朋自遠方來」專訪。

[8]註: Evariste Galois (1811-1832), 法國數學家, 最有名的工作是多項式的可解性, 他的研究奠定了現代代數基石。

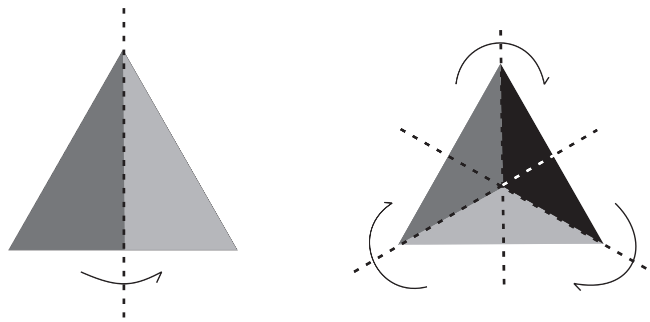
[9]註: Niels Henrik Abel (1802-1829), 挪威數學家, 以證明五次方程的根式解的不可能性和對橢圓函數論的研究聞名, 阿貝爾獎就是爲了紀念他而設立。

做不出來的。但是他只提出了一個做不出來的例子, 並沒有淸楚的列出可行與不可行的方程, 而我們知道有些方程是可行的。

相對之下, Galois 則是把可使用開方處理與不可使用開方處理的條件淸楚寫出。他的想法是革命性的, 在他之前, 重點放在求解的各式方法, 但他卻把重點放在研究解本身的對稱性 (symmetry) 上。何謂解的對稱性? 當有許多解的時候, 可以對解做置換 (permutation) -就是變換它們的相對位置, 但卻不影響解之間的代數性質。Galois稱這些置換爲“a group of permutation of roots”(解的置換群), 大家會想爲什麼這樣的數學要稱爲“群 (group)”, 這裡可以看到“群 (group)”這一說法的起源。在群之外, 他也提出了另一個觀念“體 (field)”, 但我就不多談了。現代一般稱這個群爲 Galois 群, 這個群可以看做對稱群的子群, 以下是一個簡單的例子。

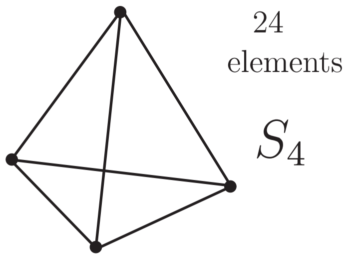
大家都知道 $x^2-2=0$ 這個方程有兩個解, 一個是 $\sqrt{2}$, 另一個是 $-\sqrt{2}$。但是如果從代數的角度來看, $\sqrt{2}$ 和 $-\sqrt{2}$ 是完全一樣, 這兩個解可以隨意調換。而2次以上的方程, 解就無法隨意調換, 因爲會對解的關係造成改變。所以, Galois 提出研究排列結構的想法, 從群的結構排列來確定方程有沒有解。這個觀念在19世紀由一位19歲的人所提出。當然, Galois 並不是第一個提出置換觀念的人, 但這是一個非常重要的觀念。

所以, 群是什麼? 你可以把群視爲研究特定對象 (object) 對稱性的工具。這研究當然不限於有限群, 無限群也是可以做的。簡單的說, 現代群論的研究就是對稱性 (symmetry) 的研究。以全等三角形爲例, 利用反射使它左右交換, 交換後, 這個三角形還是同樣的三角形。如果同時做二次不同的反射, 可以發現, 三角形的頂點被旋轉了, 但是還是三角形, 沒有改變。這樣一來, 這個三角形的對稱群 (group of symmetry) 有六個元素 (element), 三個是反射, 另外三個是旋轉。這樣的群就是現在說的 dihedral 群。



圖表 2

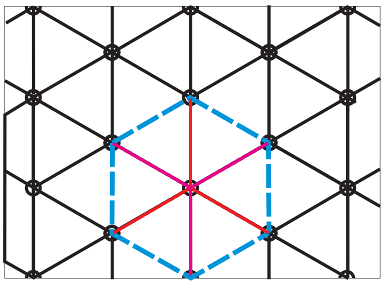
上面是以三角形爲例。如果將同樣的問題應用在四邊形, 正方形, 正五邊形, 正六邊形等上, 可以得到不同的 dihedral 群。如果是三維空間, 以下面這個正四面體的圖爲例, 進行反射之後, 可以看到它的對稱群有24個元素, 一般稱作 S_4。



圖表 3

同一個群, 可以用很多不同的方法去討論。上面例子中的群都是由反射所生成, 所以稱之爲反射群。

接下來讓我們使用三角形的邊進行反射, 每個邊都不停的反射, 這時候會產生一個新的結構, 這個結構在數學稱之爲 lattice (格子), 因爲這些點是一格一格的, 這個結構在數學中有個特定的名字稱爲 A_2, 並且這個結構是赫赫有名的。當然, 這個 A_2 格子的對稱性與之前的三角形一模一樣, 六個元素。接下來如果我們只考慮下圖虛線連結的六個點, 一個新的系統就形成了, 這個系統被稱爲根系統 (root system)。保持這個根系統的反射群就是一般所謂的 Weyl 群。這些反射群不單單出現在數學中, 化學裡面有許多晶體也是由六邊形與三角形所構成, 甚至, 許多鑽石的切割方法是與三維反射群有關, 所以, 這不只是單純在數學上碰得到, 很多其它的領域都會有相同的問題。



圖表 4

順帶一提的是一個稱作 E_8 的根系統, 是八維的。一、二年前紐約時報刊登了關於 E_8 的消息, 有一群科學家用了多年的時間去計算在 E_8 裡面發生的事情, 如果把這個八維的 E_8 圖案壓在平面上, 會產生一個非常漂亮的圖案, 這個圖案被時裝設計師運用在服裝的設計上。事實上, 數學裡 E_8 的重要性不亞於 Monster。

當然一般來說, 處理一個抽象群不太容易。很多時候我們需要利用比較熟悉的工具來研究它, 例如三角形、四邊形等, 最常使用的工具是矩陣, 因爲大部分的人, 高中之後就知

道怎麼利用矩陣做計算。所謂表示 (representation), 簡單來說就是利用矩陣來量化一個抽象的群。一個從群 G 到 $n \times n$ 可逆矩陣的同態 (homomorphism) 被稱為 G 的一個 n 維表示。比方說一個 24×24 的矩陣就是 24 維。舉例來說, 如果把 G 全部對到單位元 (Identity), 就是一個表示, 一般稱為 trivial representation, 因為沒有任何變更, 當然就是 trivial。另外, 之前提到的 A_2 Weyl 群有個2維的表示, E_8 Weyl 群有個8維的表示。如果單看同態, 還是有點困難, 有時候我們會考慮它的 trace, trace是數字, 比較好計算, 這個數字函數一般稱之為 (指示標) character。如果只考慮複數中的不可約表示, 指示標就可唯一決定表示本身, 所以只需要看 character 就可以了。Monster群的 character 與 modular 函數又有些奇怪的關係。

那麼 Monster 是怎麼發現的? 讓我說一些歷史。

之前提過, 很多群的類型都是反射群。反射的階數是2, 做一次後, 反過來再做一次, 作用就互相抵消。數學上, 階數為 2 的元素 (element) 被稱為對合元 (involution)。什麼樣的群是由對合元所產生的。如果只要求單群, 幾乎每個單群都是由對合元所生成, 所以對研究單群的數學家來說, 這是個非常重要的問題? 但這樣還是很困難, 因為兩個對合元互乘後, 階數可以是任意的。所以 70 年代初, B. Fischer 問了以下的問題:

假設群 G 由一組對合元 D 所生成, 同時滿足下面的條件:

1. 任意兩個 D 的元素 g 和 h, 如果 $g \neq h$, 則 g 和 h 互乘後的階數是 2 或 3;
2. G 是 almost simple (即它的交換子子群 (commutator subgroup) 是單的)。

這類的群稱為3-對換群 (3-transposition groups), 這個3就是乘積的階數是3以下。

有哪些 G 可以滿足這些條件? 剛剛提到的對稱群就滿足這個條件。事實上, 有很多有限體上的矩陣群都滿足這個條件, 不過當然並不是每種矩陣群都滿足這個條件。剛開始的時候, Fischer 覺得除了這些以外就沒有了, 希望把它們全部找出來並做分類, 他發現了三個不同的群 Fi_{22}, Fi_{23} 與 Fi_{24}。3 完成了, 那麼4呢? 所以他繼續做 gh 的階數是 2、3 或4的情況, 也就是所謂的3,4-對換群 ($\{3,4\}$-transposition groups), 也有些結果, 並發現了一個新的單群, 現在稱為 Baby Monster (BM)。每當一個新的單群出現, 數學家就開始探討它有什麼特別的地方, 比如說它的擴張 (extensions)、它的自同構群 (automorphism group)–即是群本身的對稱性等。當時很多人在進行這樣的研究。Fischer 和 Griess 分別找到一些證據顯示可能有下面這樣的單群 G 存在:

G 有個 2 階的元素 t, 使得 t 的中心化子群 (centralizer)

$$C_G(t) = \{x \in G \mid xt = tx\}$$

同構於 Baby Monster 的 2 階擴張 (double cover)。

他們分別找到證據顯示這個群是存在的, 這就是現在說的 Monster 群。

這個群的存在與否當時還沒確定, 但如果存在的話, 是什麼樣的呢? 他們發現這個群一定是 6 置換群, 會有兩個2階的共軛類 (conjugacy classes), 簡言之就是有兩類型的對合元 (involution)。Monster群的不可約表示的維數最小是 196883, 也就是起碼要用 196883×196883 矩陣。這樣的大小即便是現在的電腦都沒辦法處理。另外如假設這 196883 維的不可約表示存在, 可以算出 character table。不單如此, Simon Norton[10] 在做完 character table 之後, 發現這個 196883 的表示有個可交換但非結合的代數結構。當然這個代數結構相對 Monster 是不變的, 也就是 Monster 會保存乘積。所以, 所有的東西都是建構在196883的表示是存在的。Thompson 在 1979 年有一篇文章, 討論如果眞的有這個 196883 的表示, Monster 群會是唯一的。所以問題都在如何把這個196883的表示做出來。

1982年 Griess 發表了這個196883的代數的論文, 實際上, 他在 1980 年就已經公布了這個結果。這件事在當時是一件非常轟動的事情, 還上了報紙新聞, 因爲 196883 是一個這麼龐大的矩陣, 加上那時候的電腦技術也不甚發達, 所以沒有人相信這個群可以那麼快就做出來。沒想到, Griess 用手就把它算出來, 發表的論文也不過是一百頁左右。除了把這個 196883 的代數算出來, 他也證明了 Monster 是存在的。

後來 Conway 跟 Griess 將原來的做法簡單化, 把196883加了一個單位元變成196883+1, 因爲這是代數結構, 所以希望有單位元, 比較容易處理。這樣做的好處是容易處理, 壞處是維度又變大了。

接下來要談 Moonshine 關係的發現。說到發現, 就必須要提到一個很偉大的觀察者–John McKay[11]。他發現 $196884 = 1 + 196883$。這個看來平平無奇的算式, 確實是一個非常重要的發現。之前提過1, 196883 是 Monster 群不可約表示的維數。196884即和一個很重要的模函數–古典的橢圓 j-函數有關, j-函數是一個週期函數 (periodic function) , 可以用 Fourier Series 展開, 設 $q = e^{2\pi iz}$, j-函數的展開式爲

$$j(q) = q^{-1} + 744 + 196884q + \text{高次項},$$

196884是一次項的係數。John McKay 覺得兩者之間好像有點關係, 但是不知道是什麼, 所了寫封信給 John Thompson, 詢問他知不知道這事。一開始, Thompson 認爲這兩者之間不會有關係, 覺得沒有任何的重要性, 後來, 他做了很多的計算, 很快地改變主意。跟 McKay 做出了以下的猜想:

---

[10]註: Simon Norton (1952-), 英國群論學家。

[11]註: John McKay (1939-), 群論學家, 有許多著名的猜想, 包含怪獸月光及代數幾何中的 McKay Correspondence 等。

是否存在一個有階的無限維 Monster 表示 $V = \bigoplus_{n=-1}^{\infty} V_n$, 使得這個表示的指示標 (graded character)

$$\mathrm{ch}V = \sum_{n=-1}^{\infty} \dim V_n q^n = j(q) - 744.$$

另外, 序列

$$T_g(q) = \sum_{n=-1}^{\infty} \mathrm{tr}(g \mid v_n) q^n, \qquad g \in M$$

將是一個模函數 (modular function)。

從前做數論的人沒有想過會有這樣的東西, 當有了這個猜想以後, 數學家們如 Conway, Norton 等人開始計算試著解釋 $T_g(q)$, 或者探索 $T_g(q)$ 是不是 modular function, 花了很久的時間算這個東西, 算完之後, 得到許多的數字也不知道該怎麼辦, 到圖書館去查19世紀末的書, 看到許多數字跟剛剛算出來的一模一樣。因爲一模一樣, 所以他就列出這些所有可能的函數, 一共有171個。當然這之間有很多的巧合, 但是從這些巧合可以發現這些函數不是一些無用的東西, 是有意義的, 以前就經常有人研究它。這些函數非常特別, 是所謂的 hauptmodul of genus 0。在此稍微解釋一下 2 維的 compact surface 可以用 genus 去分類。球體就是 genus 0。至於 hauptmodul 的意思是指這個函數可產生其它所有同類的函數, 這我就不再解釋, 因爲是比較技術性的東西。

另外, 還有一個數論中有關 $SL_2(Z)$ 同餘子群 (congruence subgroup) 的定理。設

$$SL_2(Z) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ac - bd = 1 \right\}$$

a, b, c, d 都是整數。當 n 是一個整數, 它的子群

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) \middle| c \equiv 0 \mod n \right\}$$

稱爲一個同餘子群。給定這樣的一個子群, 可以製造一個黎曼曲面, 這個黎曼曲面的 genus 就稱爲這個子群的 genus。

Ogg[12] 證明若 p 爲質數 (prime), $\Gamma_0(p)^+$ 是一個 genus 0群若且惟若 $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71$, 我們注意到這些質數正是可以整除 Monster 階數的質數。可整除 Monster 階數的質數是一個集合, 使 $\Gamma_0(p)^+$ 成爲 genus 0 群的質數又是另一個集合, 這兩個質數的集合竟然一模一樣。這個定理在 Monster 還沒出現之前就被

[12]註: Andrew Pollard Ogg (1934-), 美國數學家, 研究領域包含數論、模形式 (modular forms)。

證明了, 所以這個定理出現在 Monster 與 Conway-Norton 工作之前。當 Ogg 證明這個定理以後, 有一次他去聽演講, 聽到有關 Monster 的描述, 發現可整除 Monster 階數的質數和他定理中的質數完全一樣, 於是他懸賞了一瓶 Jack Daniels (威士忌) 給任何一個可以證明兩者之間關係的人, 到現在仍在懸賞中。

而 Moonshine 這個名稱的由來就是因爲 Conway, Norton 等人嘗試去解釋這個關係, 但當時完全沒有足夠的證據, 也沒有證明。他們發表的文章也是數學論文中的一篇奇葩, 因爲沒有太多的定理, 也少有證明, 只有觀察與計算。這樣的數學論文是非常少有的。也是因爲這個關係在當時還沒完全“合法”, 所以被稱爲 moonshine 也就一點都不奇怪。

1983年時 Frenkel[13] -Lepowsky[14] -Meurman[15] 使用物理學中的頂點算子 (vertex operator) 做出了 McKay 和 Thompson 所猜想的 Monster 模, 頂點算子的方法對群論來說是全新的, 這些頂點算子開始時是物理學家在1960年代所發明的。在 Frenkel, Lepowsky 和 Meurman 發表了他們文章後不久, Borcherds 在美國科學院的 proceedings 上發表了「Vertex algebras, Kac-Moody algebras, and the Monster」[16]。他在這篇文章中, 定義了一個新的代數系統, 稱爲頂點代數 (vertex algebra)。在文章中他提到 vertex algebra 與 Kac-Moody 和 Monster 的關係, 最特別的是他提到 Frenkel-Lepowsky-Meurman 的 Monster 模是個頂點代數。要注意的是這篇文章是在 proceedings 上發表的, 所以文章很短沒有辦法把證明納入。後來, Frenkel-Lepowsky-Meurman 修改他的一些定義, 引入頂點算子代數 (vertex operator algebra) 的觀念, 證明 Monster 模是頂點算子代數, 不單如此, Monster 是這個頂點算子代數的自同構群, 所以 Monster 描述一個很大代數系統的對稱性 (symmetry)。這個 module 現在稱爲月光頂點算子代數 (Moonshine Vertex Operator Algebra)。在證明中 Frenkel-Lepowsky-Meurman 等人必須要用到 Griess 的結果, 所以 Griess 的工作也是非常重要的。

Conway 和 Norton 所提出的171個函數, 後來在1992年被 Borcherds 證明了, 並在1998年獲頒菲爾茲獎。他是如何證明的呢? 他用了很繁複的步驟。他先利用 Frenkel-Lepowsky-Meurman 的月光頂點算子代數製造了一個更大的頂點代數。接著他使用物理學弦論中的“沒鬼定理” (“no-ghost” theorem) 建造了一個李代數 (Lie algebra), 這是一個廣義 Kac-Moody 代數, 目前也被稱爲 Borcherds 代數, 最初也是由 Borcherds 所提出。由此可以看出, 爲了解決這個問題, 他提出了許多全新的觀念, 非常重要, 是以前所不知道

[13]註: Igor Borisovich Frenkel (1952-), 俄裔美籍數學家, 主要研究領域在表現理論與數學物理。

[14]註: James (Jim) Lepowsky (1944-), 美國數學家, 研究領域包含李帶數與頂點代數。

[15]註: Arne Meurman (1956-), 瑞典數學家, 研究領域包含有限群與頂點代數。

[16]註: Borcherds, Richard E., Vertex algebras, Kac-Moody algebras, and the Monster., *Proc. Nat. Acad. Sci. U.S.A.* 83 (1986), no. 10, 3068-3071.

的。最後, 他利用李代數指示標 (character) 理論和上同調方法計算了 McKay-Thompson series 的係數, 並證明 Conway 和 Norton 的猜想。由此可以看到, Borcherds 做了兩件非常重要的事情, 首先, 他理解到要解決這個問題, 必須要用到李代數的指示標 (Charatcer) 的理論, 因此他花了不少功夫去確立廣義 Kac-Moody 代數的指示標理論。另外, 他發現研究 Monster 使用頂點算子代數是必須的。以上這些都是非常重要的創見, 他獲獎的原因就在這裡, 因爲完全是以前的人沒想到的。不過, 如果仔細去看歷史, 會發現大部分工作不是他一個人完成, 是許多人的貢獻而成的。

到此, 我們發現這個領域令人驚訝地把許多看似完全沒有關聯的東西連在一起。第一個當然是有限群, 第二個是模函數, 第三個是李代數的理論, 最後甚至連物理都扯入, 把弦論也帶進來了, 因爲頂點算子代數最原始的觀點都是從弦論那邊得來。

簡單的說, 頂點算子代數就是物理上的保角場論 (conformal field theory) 的代數結構, 而 Monster 是這種代數結構的對稱性 (symmetry)。所以最後, 有一個直到目前爲止都還沒有人能夠回答的問題, Monster 是不是跟實實在在的物理有關? 可不可能是宇宙中的一種目前還未知的對稱性? 研究物理場論都會提到對稱性。當然這個很大, 因爲我們的宇宙是非常非常大的。

結語 (成功大學數學系許瑞麟主任): 這次是一場很難有機會聽到的演講, 從故事的開頭就談到許多數學最基本的東西及其典故。一般研究生做數學研究的時候, 都是比較偏重技術性, 從定義定理開始, 即便不知道這些定理的由來, 也還是繼續進行技術性的邏輯推導。但是我覺得不管從任何角度來看, 我們做研究都必須知道故事的來龍去脈及源頭, 這樣才能提供繼續往下走的動力。很謝謝林教授今天帶給我們的演講, 就算不是做這個領域, 相信聽了演講之後, 還是可以有一個最基礎的認識。如果以爲已經有了一個概念成形, 就算對內容細節還不甚理解, 我以爲這場演講的目的也已經達成。

—本文演講者林正洪教授任職中央研究院數學研究所, 整理者陳麗伍爲中央研究院數學研究所助理—