數學傳播　45卷3期, pp. 20-25

月光、怪物 (Moonshine and Monster)

林正洪

今天談論的主題 — 月光與怪物 (Moonshine and Monster) 有點不大像數學, 反而有點像手機遊戲或是科幻小說的名字。但我們要談論一個實實在在的數學問題及其歷史。雖然很多數學家會在「月光」的影響下變成怪獸, 但我們不會談月光怪獸, 也不會談論手機遊戲或如何令你變成月光怪獸。也許你會感到疑惑, 爲什麼用那麼奇怪的名字命名數學問題。我希望解釋一下箇中緣由, 也會提到爲什麼這問題是有趣的, 並說明它所引伸出的數學理論。

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。根據字典的定義, 所謂的怪物 (Monster) 一般是想像的、既大又醜又可怕。美醜是主觀的, 所以重點就在大與可怕。不過如果你是 30 歲以下的年輕人, 對 Monster 的印象可能是 PokeMon, 他們可以是小巧可愛的, 與之前的定義是剛好相反。

那 Moonshine 是什麼? 用中文來說就是月光, 意思是什麼? 一種解釋是不太明亮、有點模糊不清, 令人有各種美麗的想像。另一種比較靠近我們今天主題的解釋是不大實在、空妄的, 特別是指一些虛無飄渺的想法。所以某種程度來說, 爲什麼會命名爲月光, 是因爲它是不實在的, 沒有可以觸摸的方法, 有些虛無飄渺。另一種解釋是英國的俚語, moonshine 指的是走私或私釀的烈酒, 一般是指私釀的威士忌。如果你在網路上搜尋 moonshine, 可以看到許多酒精私釀的圖片。等一下大家就會明白爲什麼要命名爲 moonshine, 因爲它就像私釀酒一樣, 還沒有取得合法的地位。

實際上我們所說的 Monster 是什麼, 簡單的來說它是一個有限群 (finite group)。有限群的理論可以說是從19世紀末期, 伽羅瓦 (Evariste Galois) 有關多項式解的工作開始, 他引入很多新的概念。例如, 他以研究解的排列及置換爲課題, 解決了多項式方程是否有開方根解的問題。伽羅瓦稱解的置換爲一個「置換的群組」(a group of permutations), 這是群 (group) 的由來。伽羅瓦也引入置換群、正規子群及單群的概念。伽羅瓦的工作後, 群的概念就慢慢滲入數學的各領域, 是現代數學中一個不可缺的工具。一個子群稱爲正規子群如果它在共軛下是封閉的, 所以子群 H 是群 G 的正規子群如果對於任意 G 的元素 g, $g^{-1}Hg \subset H$。一個群稱爲

單的如果除了它自己及單位群外, 沒有其他正規子群。有限單群的分類是 20 世紀數學上的一個重大成就, 現在我們知道任意一個非交換的有限單群 G 會同構於下列的一個群:

1. 交替群 Alt_n, $n \geq 5$;
2. 一個 Lie 類型的有限單群; 或
   (Lie 類單群有 16 個無限家族, 例如 $PSL_n(q)$, $E_8(q)$ 等)
3. 26 個零星單群 (sporadic simple groups) 之一。

Monster (怪物群) 是這 26 個零星單群中位數最大的一個。英文中 sporadic 指的是零星、分散的、不常出現, 所以當這個群是 sporadic 時, 就不能用一般的方法來說明它是什麼樣的群, 也就是不淸楚它從何以來, 也不淸楚它爲什麼存在, 必須費心思去了解他。Monster 是 sporadic 群中最大的, 但他有多大呢, 會得到一個象徵恐怖的名字?

Monster 群的大小爲

$$\begin{aligned} |M| &= 2^{46}3^{20}5^{9}7^{6}11^{2}13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808017424794512875886459904961710757005754368000000000. \end{aligned}$$

是一個有 54 位數字。54 位數聽起來似乎還好, 但是如果認真算一下, 它是非常可怕的。就算想要用電腦處理這個數也是辦不到的, 因爲沒有足夠記憶體做紀錄, 尤其當時的電腦還不是很發達。所以當發現有這個大又可怕的對象的時候, 就被命名爲 Monster (怪物)。當初也有人希望稱它爲 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。

Sporadic 群總共有 26 個不同的群, 其中 Monster 是最大的群, 剩下的各有不同的名字, 一般都用發現的人來命名, 有 5 個是 Mathieu 群, Janko 發現了四個, 稱爲 Janko 群, Conway 發現三個, 是 Conway 群, Fischer 有三個群, 是 Fischer 群, 其他分別由不同的人發現也都用個別名字來命名。在這當中, Monster 是 Griess 和 Fischer 所發現、Baby Monster 是由 Fischer 所發現的, 不過一般只稱爲 Monster 和 Baby Monster, 並沒有用 Fischer 和 Griess 的名字命名。現在你大約可以理解爲什麼會有人喜歡稱他爲 Friendly Giant, 因爲縮寫 F.G. 同時也是 Fischer 和 Griess 的這兩個姓氏的第一個字母。現在稱 Monster, 則變成了 $\mathbb{M}$。另外, 還有兩個群稱爲 Thompson 和 Harada, 是 Monster 後被發現的。下列是 26 個零星群的符號及其發現者。

26 sporadic groups

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}	
J_1	Janko	Fi'_{24}	
$HJ = J_2$	Hall, Janko	LyS	Lyons
J_3	Janko	Ru	Rudvalis
J_4		$O'N$	O'Nan
$Held$	Held	$\mathbb{M}$ or F_1	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 $\mathbb{M}$.

藍色的就是 Monster 本身, 紅色的群與 Monster 沒有直接關係, 黑色的群是與 Monster 有關, 可以看成 Monster 部分商群。一旦清楚理解 Monster 群, 也大致可以了解其他20 個群, 這也是爲什麼大部分的注意力都是集中在 Monster 群上, 因爲它不但是最大的零星群, 它還包含了其他 20 個群。

那什麼是 Moonshine 呢? 這沒辦法用三言兩語詳細地說明, 但是簡單來說它代表是一個完全在預期之外關於 Monster 群的特徵標 (character) 和模函數 (Modular Function) 的神秘關係。模函數是數論中一類非常重要的函數, 在研究數論或黎曼曲面時會遇到, 但它好像跟有限群沒有任何關係? 當數學家們發現這樣一個奇怪關係時, 第一個想知道的當然就是他是否正確? 第二個問題自然而然就是爲什麼是正確的。如果是正確的, 有沒有一個好的解釋。重點是這類神秘關係把 Monster 的研究推廣到有限群之外, 將 Monster 的研究帶到數論、李代數、甚至是物理的領域。

接下來讓我們說明甚麼是特徵標 (character)。一般來說, 群是一個抽象的東西, 不容易處理, 所以希望用比較熟悉的工具來研究它, 最常使用的工具是矩陣或是所謂的線性變換, 因爲可以做很多實質的計算。這就是所謂表現 (representation) 或線性表現。首先, 我們知道在複數域 $\mathbb{C}$ 上, 所有 $n\times n$ 的可逆矩陣生成一個群, 這個群稱爲一般線性群 (general linear group), 記成 $GL_n(\mathbb{C})$。一個從群 G 到 $GL_n(\mathbb{C})$ 的群同態 (group homomorphism)

$$\rho : G \to GL_n(\mathbb{C})$$

稱爲群 G 的 n 維表現 (n-dimensional representation)。一個特別的例子是把 G 全部對到單位矩陣 (Identity), 這是 G 的表現, 稱爲 trivial representation。有時候單處理矩陣仍然有點困難, 所以也會考慮矩陣的跡 (trace)。跡是指矩陣 A 對角線上各個元素的總和, 一般記

作 $\operatorname{tr} A$。當 $\rho : G \to GL_n(\mathbb{C})$ 是 G 的表現, $\chi_\rho(g) = \operatorname{tr}\rho(g)$ 被稱爲特徵標 (character)。跡是數字比較容易處理, 但如果你只考慮複數域上的表現時, 特徵標本身就足以決定所有的不可約表現, 所以只需要看特徵標就足夠。當 Monster 群剛被發現時, 數學家就嘗試計算它的特徵標及不可約表現, 其中一個發現是, 如果 Monster 存在, 它的最低維表現至少是 196883 維。那就是說你需要 196883×196883 的可逆矩陣來處理 Monster 群, 這自然是不容易。

那 Moonshine 是怎麼被發現的? 說到這裡, 就必須要提到一個非常重要的人物 — John McKay。他有很多重要的發現, 其中以下的一個等式改變了整個對 Monster 群的研究。

$$196884 = 1 + 196883$$

這等式看來很簡單, 小學生都可以理解, 但它確實是一個非常重要的發現。爲什麼?

之前提過 1 是 trivial 表現的維數, 196883 是 Monster 群最小不可約表現的維數。196884 則跟橢圓 j-函數 (elliptic j-function) 的 q 展開有關。橢圓 j-函數是一個重要的模函數, 它是一個全純週期函數, 所以可以把它展開成傅立葉級數。設 $q = 2^{2\pi iz}$, j 的 q — 展開式可寫成

$$j(q) = q^{-1} + 744 + 196884q + \text{higher order terms}$$

John McKay 覺得式子中的 196884, 好像和 Monster 有點關係, 但又不太確定, 所以寫了一封信給 John Thompson (當時最有名的群論學者), 詢問他對這事的看法。一開始, Thompson 認爲這兩者之間可能不會有重要關係, 後來, 他做了很多的計算, 很快地就改變主意。他跟 McKay 做出了以下的猜想。他們猜測怪物群存在一個無窮維整數分級的表現 $V = \oplus_{n\ge 0} V_n$, 使得它的 graded dimension

$$\operatorname{ch} V = \sum_{n=0}^{\infty} \dim V_n q^{n-1} = j(q) - 744.$$

他們還猜測, 如果考慮分級跡 (graded trace) $T_g(q) = \sum_{n=0}^{\infty} \operatorname{tr} g|_{V_n} q^{n-1}$, $q = e^{2\pi iz}$, $g \in$ Monster, 這也是一個模函數。函數 $T_g(q)$ 一般稱爲 McKay-Thompson 級數。
McKay-Thompson 猜想強烈暗示怪物群 (一個有限群) 最自然的表現可能是無限維的, 這表示背後可能有我們還不了解的結構存在。

這個猜想出現之後, 數學家們就開始計算有關級數 $T_g(q)$ 的一些性質及它可不可能是模函數 (modular function)。Conway 和 Norton 花了很久的時間去計算 $T_g(q)$ 的各級係數, 得到許多的數字但又不知道如何處理, 就去圖書館, 翻開一些有關模函數的書籍, 在一本 19 世紀末的書中, 看到許多數字跟他們算出來的一模一樣。因爲是一模一樣, 他就猜測 McKay-Thompson 級數 $T_g(q)$ 應該就是書中所討論的函數。這之間有很多的巧合, 但是從這些巧合可以看到 McKay — Thompson 猜想並不是一個很輕率的東西, 而是有實際證據, 它背後

應有非常漂亮的理論, 這些函數以前的人就已經研究過。Conway 和 Norton 發現 McKay-Thompson 級數跟其中的 171 個模函數相關, 這些函數很特別, 它們的 modular curve 都是 genus zero, 同時它們可以在模曲線上生成整個函數域。這類的函數稱爲 hauptmodul of genus 0, 而 Conway 和 Norton 所發現的 171 個函數全部都是 hauptmodul of genus 0。這是一個非常有意思的發現, 爲什麼 Monster 會跟曲線的 genus 有關? 這個 genus 0 的特性到目前都沒有很好的解釋。

Modular Curves, Modular group 和相對的函數域在 Monster 還沒出現之前, 在數論中就被廣泛討論及研究。其中 Ogg 證明以下的定理:

Theorem (Ogg): *Let p be a prime. The group $\Gamma_0^+(p)$ has the genus zero property if and only if* $p \in \{2,3,5,7,11,13,17,19,23,29,31,41,47,59,71\}$.

如果仔細對比, 你會發現 $\{2,3,5,7,11,13,17,19,23,29,31,41,47,59,71\}$ 這 13 個質數正好就是可整除 Monster 階數 (order) 的質數。Ogg 有一次去聽演講時, 聽到有關 Monster 的描述, 其中整除 Monster 階數的質數和他定理中的質數剛好一模一樣, 這樣的巧合當然引起大家的好奇。Ogg 懸賞了一瓶 Jack Daniels (威士忌的品牌) 給任何一個可以說明兩者之間的關係的人。

現在你可以比較理解 Moonshine 這個名稱的由來, Conway-Norton 試圖去解釋 Monster 群和模函數的某種關係, 也對 Ogg 的問題給出某些證據, 但並沒有給出好的解釋, 也沒有證明。他們發表的文章在數學的文獻中也是非常少有, 完全沒有定理, 也沒有證明, 只有觀察與計算。所以, 他們所討論的關係及現象, 嚴格來說仍未獲得「合法」的地位, 有點像釀製「不合法」的威士忌, 所以被稱爲 moonshine 也就一點都不奇怪。

在計算完 Monster 群的特徵標後, Simon Norton 開始考慮特徵標一些 symmetric square 的分解, 他發現 Monster 群那個 196883 維的表現有一個可交換但非結合的代數結構。這個代數結構相對 Monster 群的作用是不變的, 也就是說 Monster 會保存其乘積。所以, 所有的東西都建構在這個 196883 維的表現上。Thompson 在1979 年有一篇文章, 討論如果真的存在這個 196883 維的表現, 就可以證明 Monster 群的唯一性。所以現在所有的東西都落在如何把這個196883 維的代數構造出來。1982 年 Griess 證明這個 196883 維的代數存在, 同時證明 Monster 群是這個的代數結構的自同構群的子群。這件事在當時是一件非常轟動的事情, 還上了紐約時報的新聞。後來 Conway 跟 Griess 將原來的做法簡單化, 把 196883 加了一個單位變成196883+1, 因爲這是一個代數, 所以希望是有單位元, 比較容易處理。

1983 年, Frenkel-Lepowsky-Meurman 使用物理學上的 vertex operator 構造出 McKay-Thompson 猜想中那個 Monster 的表現, 一般稱爲 Moonshine 模。在 Frenkel, Lepowsky 和 Meurman 發表了他們文章後不久, Borcherds 在美國科學院的一個雜誌上發

表了一篇名爲《 Vertex algebras, Kac-Moody algebras, and the Monster》的文章。這篇文章中, 他定義了一個新的代數系統, 稱爲頂點代數 (vertex algebra), 並探討 vertex algebra、Kac-Moody 代數和 Monster 間的關係, 最重要的是他提到 Frenkel-Lepowsky-Meurman 的 Moonshine 模是一個頂點代數。後來, Frenkel-Lepowsky-Meurman 修改了一些他的定義, 引入頂點算子代數 (vertex operator algebra) 的觀念。他們證明 Moonshine 模是頂點算子代數, 不單如此, 他們也證明 Monster 群是這個頂點算子代數的自同構群, 那就是說 Monster 群是描述一個龐大代數系統的對稱性 (symmetry)。這個模現在稱爲月光頂點算子代數 (Moonshine Vertex Operator Algebra)。「頂點算子代數」簡單來說就是研究物理上的保角場論 (conformal field theory) 的一種代數方法, 而 Monster 是這種代數結構或是某種物理系統的對稱性。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? 它可不可能是宇宙中一種目前還未知的對稱性?

Conway 和 Norton 有關 McKay-Thompson 級數的猜想, 後來在 1992 年被 Borcherds 證明了, Borcherds 也在1998 年獲頒菲爾茲獎 (Fields Medal)。

到此, 你會發現這個領域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, 特別是零星群和 Monster 的理論, 第二個是模函數, 第三個是李代數的理論, 甚至連物理都扯入了, 把弦論也帶進來了, 並使用很多弦論的觀點, 這是近代數學令人非常興奮的一個發展。但仔細想想, 整個理論源自一個非常簡單, 看來絕不重要的等式, 加上各種各樣的巧合所形成。所以在數學上過度的巧合往往背後都有其原因, 只要大家願意細心去了解和研究, 常常都會有意想不到的收穫。

—本文作者任職中央研究院數學研究所—