數學傳播 47卷1期, pp. 3-14

淺談代數: 從決鬥的數學家到表現理論

中央研究院2022年院區開放科普演講[1]

賴俊儒

歡迎大家來參加中研院開放院區數學所的線上活動。我們今天要從幾個歷史故事出發來講: 代數如何演變成今天的樣貌。

什麼是代數?

那麼什麼是代數? 對一般人來說, 代數就是用符號代替未知數, 進而經由運算, 來解決數學問題, 比方說我們看 $1+2=3$, 我們可以把 1 這個數字換成一個未知數 x, 就可以換句話說, 問你什麼數字加 2 以後會等於 3; 換句話說, 就是來解一元一次方程式。在數學課裡, 我們學到了如何處理稍微更複雜一點的問題, 比方說解這個一元二次方程式

$$x^2+3x=2,$$

又或者這個二元一次聯立方程式

$$\begin{cases} x+y=3, \\ 2x+3y=8, \end{cases}$$

也就是雞兎同籠問題。

但是代數遠遠不止於如此, 對古時候的數學家來說, 代數這門學問, 就是以符號操作來解方程式, 我們今天會以初等代數來稱呼它。而隨著數學在進步, 代數就變成了研究「規則」所衍生出來的數學分支, 比方說我們今天談的線性代數或是抽象代數, 裡面的代數就是指這樣子的代數。最後, 很容易讓人混淆的是, 代數也可以是一種可數名詞, 來描述由這些規則所生成的數學空間, 比方說實數、複數、李代數都是這種意義下的代數。除此之外, 也有數學家創造並以此命名的代數。

文藝復興時期的數學家

首先讓我們回到文藝復興時期。文藝復興起源於義大利, 而後才拓展到歐洲其他國家。最

[1]影片網址 https://www.youtube.com/watch?v=iOTr6uAE5A0.

早的大學就是在義大利的波隆那 (Bologna) 大學。這些大學的存在, 才得以資助數學家一邊做研究一邊教書, 才讓數學有飛躍性的突破。值得一提的是, 當時的數學有記號上的缺陷, 他們不承認小於0的負數, 也不承認有虛數的複數。他們不像我們現在, 可以把二次方程寫出一般式 $ax^2+bx+c=0$, 然後再把它解寫成公式解

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

當時的人必須把小於0的項丟到等式的兩邊, 才能把二次方程化簡而後分類, 然後用食譜一般的形式來記載求解的過程。

最早對三次方程做出突破的數學家, 就是波隆那大學的講師德費羅 (Scipione del Ferro, 1465∼1526)。他當時並沒有選擇將自己的解法公開, 反而將自己的解法寫在筆記本裡面, 作爲決鬥的秘密武器, 死後傳給自己的徒弟和女婿。這裡我們說的決鬥不是像圖中這樣真刀真槍的決鬥, 而是互相出題考對方的頭腦決鬥。當時的大學金主通常會透過決鬥的結果, 來選擇贊助的數學家。當時最出名的決鬥者, 就是這位尼可羅馮大拿 Niccolo Fontanna (1500∼1557), 綽號「口吃的 (Tartaglia)」。他出身窮困, 小的時候被法國士兵砍傷下巴, 導致口吃。他透過一連串的數學決鬥, 獲得了義大利威尼斯大學的教職。馮大拿苦心鑽研, 在德費羅之後也貢獻了三次方程的問題。

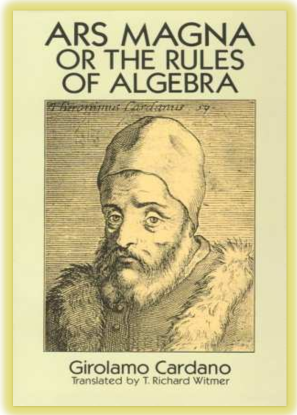
Niccolo Fontanna
(1500∼1557)

另一方面德費羅的徒弟費爾 (Fiore) 繼承了秘密筆記本後, 就以爲自己天下無敵, 到處吹噓。於是在 1535 年, 兩人就展開了三次方程的決鬥。決鬥的期限有 50 天, 雙方各出 30 道題目考對方。費爾從筆記本當中學到的解法, 只會解型如 $x^3+ax=b$ 這樣子的三次方程, 因此他就出了 30 道這樣子的題目給馮大拿。另一方面馮大拿知道如何將一般的三次方程化解成這種形式, 所以他就出了各式各樣的三次方程來考費爾。而結果顯而易見; 費爾被馮大拿的各式各樣的問題搞得頭昏腦脹, 但是馮大拿卻在兩個小時之內把費爾的 30 道問題全部解出, 最後大獲全勝、聲名大噪。

而名聲總是容易帶來壞事, 當時米蘭學術界的活躍人物, 就是這位醫生斜槓數學家卡當 (Girolamo Cardano, 1501∼1576)。卡當找上了馮大拿, 以米蘭的工作與人脈作爲籌碼, 求

馮大拿分享三次方程的解法, 並發誓永遠不外洩。但是在 4 年後, 卡當拜訪了德費羅的女婿。他發現在筆記本中德費羅早就破解了三次方程, 於是他想說 : 他寫一本書把德費羅的方法公開, 就不算違背跟馮大拿的誓言。於是卡當就在 1545 年出版了這本《偉大的技術或代數規則》。在書中, 卡當不僅列出了三次方程的解法, 也同時指出四次方程可以化解成三次方程, 因此可以一併解決。這本書幾乎讓卡當成爲那個時代最偉大的人。

Girolamo Cardano (1501~1576)



《偉大的技術或代數規則》

另一方面, 馮大拿簡直氣瘋了。他認爲卡當背棄他的誓言, 用所有你想得到或想不到的惡毒言語來攻擊卡當, 並要求與卡當決鬥。但是當時卡當的地位比馮大拿高太多了, 決鬥對他來講並沒有任何的好處。他只願意讓自己的弟子法拉利出戰。馮大拿起初當然不願意, 直到 1548 年, 馮大拿的故鄉布雷西亞 (Brescia) 大學說 : 如果你願意和法拉利決鬥並獲勝, 那麼我們就會給你一個大學教職。於是馮大拿就答應了這場與法拉利的決鬥。一邊馮大拿只會解三次方程, 另一邊法拉利卻連四次方程都能輕鬆上手, 不意外的, 最後決鬥由法拉利勝出, 馮大拿黯然退場。

拉格朗日的預解式

而下一個重要的數學突破要到 200 年後, 拉格朗日 (Joseph-Louis Lagrange, 1736~1813) 觀察前人對於四次方程解法的規律, 創造了一個預解式 (resolvent) 的概念來輔助解原本的方程。他觀察到在 4 次以下的方程你都可以透過這個預解式的手法把原本要解的方程式次數降低 1。所以當他發現五次方程的預解式次數不減反增, 他便猜測 5 次以上的方程式沒有辦法一樣求解。

Joseph-Louis Lagrange
(1763∼1813)

原方程 $f(x)$ 次數	預解式 $R_f(x)$ 次數	預解式真次數
2	2	1
3	6	2
4	24	3
5	120	24

接下來我們來看看拉格朗日的做法。首先我們看三次方程式

$$0 = f(x) = x^3 + px + q,$$

不妨假設二次項可以設成 0。我們做一個變數代換, 設 $x = y + z$, 其中 y 是我們的新變數, 而 z 是待定項。整理後會得到這個式子

$$0 = y^3 + z^3 + (y + z)(3yz + p) + q.$$

我們發現, 如果 $3yz + p$ 是 0 的話, 式子會簡單許多。因此我們現在決定讓 $z = -p/3y$, 所以原式就可以化解成這個六次式

$$0 = y^3 + q - \frac{p^3}{27}y^{-3}.$$

原方程等於 0, 則這個六次預解式

$$R_f(y) := y^6 + qy^3 - \frac{p^3}{27}.$$

就必須要是0。但是這個預解式其實是一個假的六次式, 他可以寫成一個二次式, 是代入 y 的三次方而成:

$$R_f(y) := y^6 + qy^3 - \frac{p^3}{27} = R'_f(y^3),$$

其中

$$R'_f(y^3) = t^2 + qt - \frac{p^3}{27} = (t - s_1)(t - s_2),$$

我們就可以用公式來算出 R'_f 的兩個解 s_1 和 s_2, 進而回推預解式

$$R_f(y) = (y^3 - s_1)(y^3 - s_2).$$

的兩個解 $\sqrt[3]{s_1}$ 和 $\sqrt[3]{s_2}$。由根與係數關係, 我們可以回推: 這兩個三次方根乘起來會是原預解式的零次項開三次根號

$$\sqrt[3]{s_1}\sqrt[3]{s_2} = -p/3,$$

也可以用這個關係回推 y 和 $x(= y + z = y - \frac{p}{3y})$。我們發現不管 y 取 $\sqrt[3]{s_1}$ 和 $\sqrt[3]{s_2}$ 的哪一個, x 都會是同樣的 $\sqrt[3]{s_1} + \sqrt[3]{s_2}$。以上是卡當與馮大拿的做法。

但是拉格朗日的時候就已經知道了複數。他知道三次方根有其他的單位方根 ω, 也因此他可以把 y 的 6 個複數解全部都寫出來: 令 $r_1 = \sqrt[3]{s_1}$, $r_2 = \sqrt[3]{s_2}$, 另四個根用 ω 表示爲 ωr_1, ωr_2, $\omega^2 r_1$, $\omega^2 r_2$。依樣畫葫蘆就可以得到原方程 f 的另外兩個複數根; $f(x) = x^3 + px + q$ 有解

$$x = r_1 + r_2, \quad \omega r_1 + \omega^2 r_2, \quad \omega r_2 + \omega^2 r_1.$$

拉格朗日後來將這種作法推廣, 對於 n 次方程都可以定義他的預解式。

加羅瓦理論

拉格朗日的觀察, 後來被阿貝爾 (Niels Henrik Abel, 1802∼1829) 及加羅瓦 (Évariste Galois, 1811∼1832) 繼承。阿貝爾證明了五次方程不保證有根式解, 也是說它可能有解, 但是這些解不保證可以由有理數加減乘除開根號得到。而加羅瓦進而刻劃出五次方程有根式解的充分必要條件。

Niels Henrik Abel (1802∼1829)

Évariste Galois (1811∼1832)

加羅瓦的理論是大學抽象代數中一個重要的章節。我們在這邊可能只能忽略細節講一些它的精神, 這個精神就是說*方程式只是表象*, *關鍵在從這個表象中抽取關鍵的規則*。比方說我們看這兩個五次式

$$f(x) = x^5 + 3x^2 + 2x - 1,$$
$$g(x) = x^5 + 3x^2 + 2x - 2,$$

肉眼看起來它們長得幾乎一模一樣, 它們只是在常數項中差了一個 1, 但是它們的解卻大大的不同。加羅瓦的理論告訴你, 如何從一個方程式出發, 定義一個所謂的群, 一種新的代數結構。在

這個例子當中雖然這兩個方程式 f 和 g 長得差一點點而已, 但是他們對應的群卻天差地別; 前面的群 G_f 裡面有 10 個元素, 後面的群 G_g 裡面卻有 120 個元素。而加羅瓦定理告訴你說: *方程式保證有根式解的充分必要條件, 是這個群的結構要夠好*。所以我們不再看方程式當中的那些數字, 我們轉而去研究群的結構。從此數學主流對方程式求解失去了興趣, 而加羅瓦理論作爲重要而深刻的工具流傳下來。

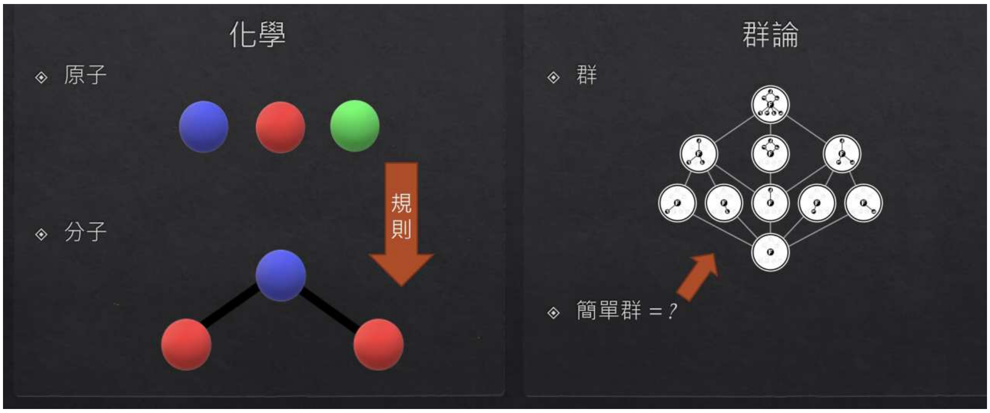
形變群 (Transformation groups)

在加羅瓦理論當中, 方程式只是表象, 重要的是當中的規則, 也就是它的加羅瓦群。在看起來不相關的其他領域, 也有類似的現象, 比方說李 (Marius Sophus Lie, 1842∼1899) 和克萊因 (Felix Klein, 1849∼1925) 研究的形變, 他們透過收集離散與連續形變的規則, 定義出現在所謂的有限群及無限的李群; 而話鋒一轉代數突然就從研究方程式怎麼解, 變成研究這些數學結構的分類。

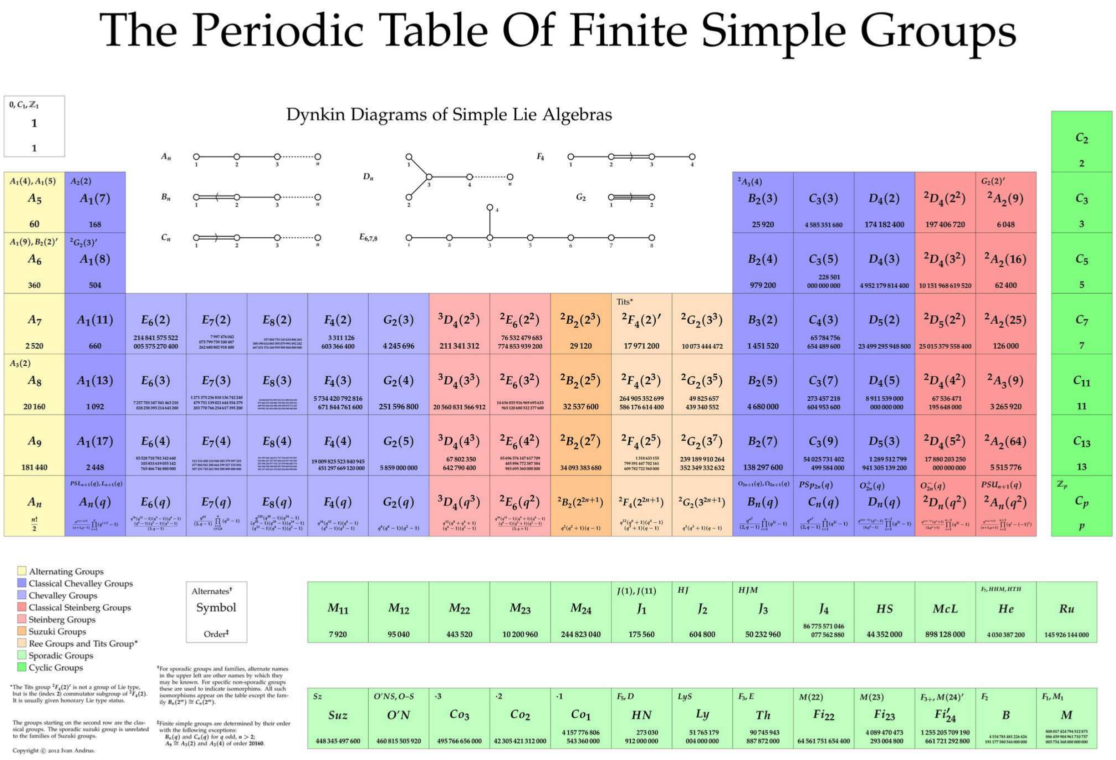
Marius Sophus Lie (1842∼1899)
連續形變 ⇒ (無限) 李代數

Felix Klein (1849∼1925)
離散形變 ⇒ 有限群論

而做這些研究, 其實就很像以前的化學家, 他們發現新的元素, 他們研究分子由哪些原子構成。



而那個時候的群論學家就是挑出一個群, 看看我們要怎麼把它拆解成最基本的元素, 也就是所謂的簡單群。而他們的研究成果就可以寫成這個偉大的定理: 簡單群分類定理; 也就是說, 所有的簡單群有三大家族: 構造相對簡單的交替群以及循環群, 以及用李代數表現理論構造的李型有限群; 除此之外還有 26 個例外。



Andrus, Ivan. (2012). https://irandrus.wordpress.com/2012/06/17/the-periodic-table-of-finite-simple-groups/

這個簡單群分類定理的證明一點都不簡單, 它必須要結合一百多年來一百多篇論文的結果才算完成:

- ⊛ 1832年 加羅瓦構造最初的簡單群 - 交替群 (alternating group A_n),
- ⊛ 1955年 謝瓦來 (Chevalley) 透過李代數構造李型簡單群,
- ⊛ 1982年 格里斯 (Griess) 構造最複雜的簡單群 - 怪物群 (monster group M),
- ⊛ 2008年 結合一百多年來一百多篇論文, 第一代證明完成。

而近十年來有一些人在著手於第二代證明; 他們已經先知道答案了, 所以可以把第一代證明當中摸索的過程簡化。但即使如此他們也估計要到 2024 年才可以把證明所有的細節寫完, 估計要達到 5000 多頁。

代數成為一種結構

最後我們來看看代數作爲一種數學結構是什麼意思。這個動機還是要回到當初的解方程式。我們看卡當公式解這個三次方程 $x^3 = 15x + 4$ 可以寫出他的解如下

$$x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}.$$

以當時的觀念來說, 根號裡面不可以有負數, 所以這個公式應該是無效的。這個方程應該沒有解。但是你可以真的去算, 明明你代入 $x = 4$ 檢驗, 可以確認它是這個三次方程的一個解。那怎麼辦呢? 龐貝里 (Bombelli) 就提出了虛數的概念; 只要我們忍受一個無意義的符號 i, 滿足這個算法, 它這個符號乘以本身 $i * i = -1$, 那麼你就可以將這兩個三次根號裡面的東西化簡成 2 ± 11 那個無意義的符號, 而 $(2 \pm i)^3 = 2 \pm 11i$, 所以 x 就會是 $(2+i)+(2-i)$; 兩個無意義的符號消掉, 你就可以得到 4 這個解。

但是這個虛數 i 的乘法, 以當時的幾何觀念來講是不自然的。它不是當單純的向量的加法; 這個複數空間上必須要有一個額外的乘法。而任何形同 $a+bi$ 的複數, 其乘法結構都可以只被這兩個生成元 1 和 i 的乘法表決定。所以人們當時就定義代數是一種複數的推廣, 只要包含係數域、生成元和乘法表, 你都可以把這個新的數學結構叫做一個代數。

	1	i
1	1	i
i	i	-1

「代數」就是種複數的推廣, 當中的資料包含了 (1) 係數域 (2) 生成元 (3) 乘法表。

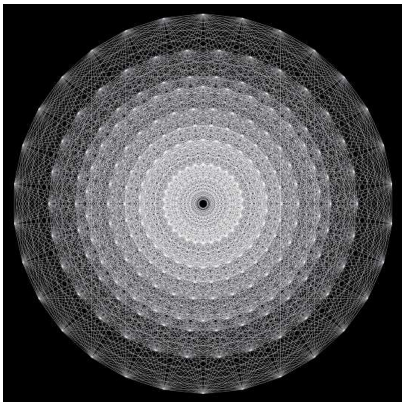
在這個發現之後數學家嘗試去把複數推廣成更複雜的代數, 比方說漢米爾頓 (Hamilton) 的四元數, 可以拿實數作爲他的係數域。他把生成元從兩個 1 和 i 推廣成四個 1、i、j、k。他把乘法表可以明確的寫出來, 就可以定出一個非交換代數:

$x*y$	$y=1$	i	j	k
$x=1$	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

更甚之, 你的代數當中的生成元甚至並不需要是一個數字, 比方說你可以看 n 階方陣形成的矩陣代數, 當中每個生成元都是一個基本矩陣, 也就是說矩陣當中非 0 即 1, 而且恰有一個地方是 1。因此你就可以用矩陣的乘法規則, 來定義你的代數規則, 從而定義出一個新的代數。而從此開始, 代數這個數學分支就變成是在研究代數這個數學空間。

$x*y$	$y=\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$
$x=\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	0	0
$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	0	0	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$
$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	0	0
$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	0	0	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$

表現理論



Root system of type E8

Johann Carl Friedrich Gauss (1777~1855)

而代數研究當中一個重要的工具就是表現理論。表現理論的前身, 是高斯 (Johann Carl Friedrich Gauss, 1777~1855) 在數論方面的工作。當年他考慮這個問題: 什麼樣子的整數 n 可以寫成下面的整係數二次形式?

$$F = ax^2 + 2bxy + cy^2.$$

他發明了行列式

$$D_F = b^2 - ac.$$

對於每個這樣的二次形式, 都定義一個複數。他把這些二次形式收集起來, 得到一個交換群

$$G_d = \{F \mid D_F = d\},$$

他並對這個交換群定義所謂的特徵標 (character)

$$X_d : G_d \to \mathbb{C}\backslash\{0\},$$

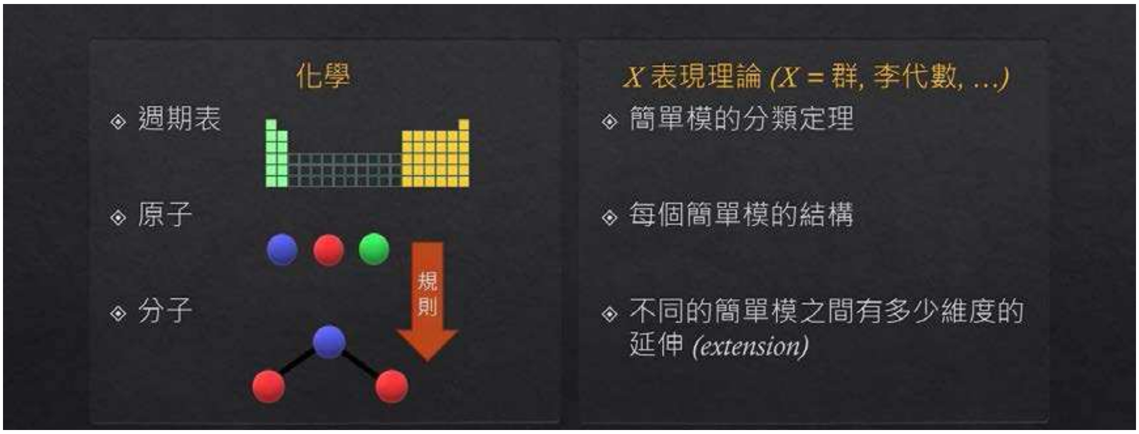
來解決這個數論問題。我們在此不詳細解釋高斯的工作, 但是我們可以注意到: 在這個數論問題當中, 二次形式也只是表象, 就如同方程式也只是表象而已。重要的是, 你可以對於這個表象、這個二次形式, 來賦予一個複數來解決問題。

Ferdinand Georg Frobenius
(1849～1917)

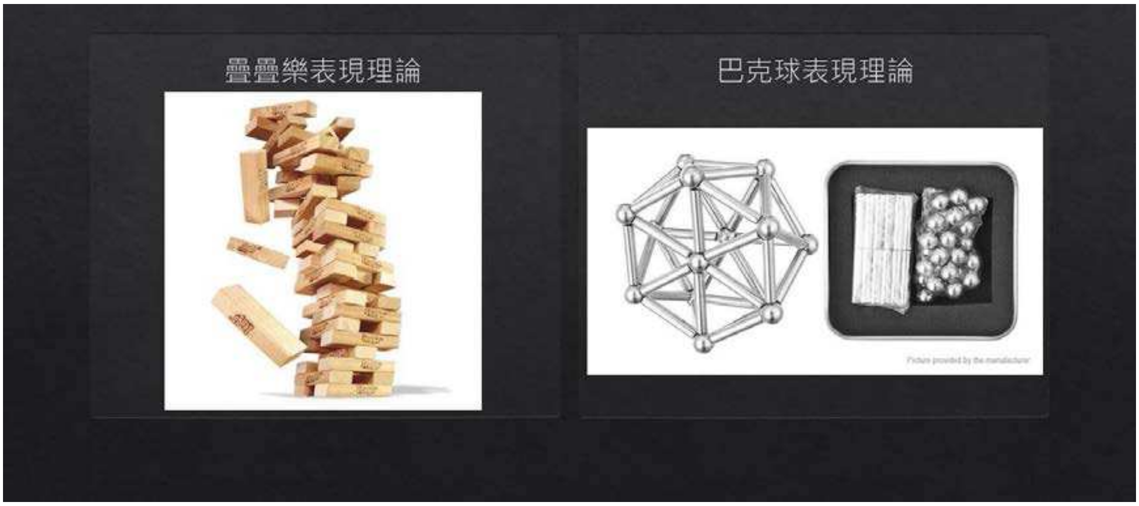
之後, 福比尼 (Ferdinand Georg Frobenius , 1849～1917) 觀察高斯的特徵標理論。特徵標當中將每一個群裡面的元素送到一個非0的複數, 那豈不就是一個 1×1 的可逆矩陣? 那我們爲什麼不把這個 1 改成任何一個數字 n? 福比尼這樣子做: 他把每個抽象的元素、每個抽象的規則都賦予一個具體的矩陣來研究, 就變成我們今天所說的群表現。福比尼因此隻手奠定了表現理論的基礎。除了剛剛提到的簡單群分類定理以外, 表現理論仍然是 21 世紀數學的主流分支, 許多費爾茲獎的得主的工作也都和表現理論習習相關。

我們用淺顯的語言來說, *表現理論就是同時研究表象與規則*。我們剛剛看到的幾個重要的問題: 解方程式或者是高斯的數論問題, 都有一個表象, 但是這個表象上面我們會有一些規則作用於其中。把這些規則收集起來就會形成一個代數, 代數以矩陣的形式作用在模上面。而今日表現理論的重要問題就是在研究這些模的性質與分類。

打個比方, 我們今天只要選定任何一組規則, 就是選定了一個代數, 來研究它的模的分類以及性質。這就像一個平行宇宙一樣, 它在這個宇宙裡面有自己的元素週期表, 跟其他已知的週期表可能長得不一樣, 每個週期表裡面的元素性質也會跟其他人不一樣。哪些原子間可以以什麼方式組成分子? 這個規則也會跟其他的宇宙不一樣。所以對於每一個給定的代數我們都想要去研究, 簡單模要怎麼樣分類? 簡單模有什麼樣的性質? 什麼樣子的維度? 不同的簡單模之間有多少維度延伸?



這些延伸是什麼意思呢? 再來打個比方, 我們今天可能考慮一個疊疊樂宇宙; 這個宇宙中就只有一種原子, 就是這個長方形的木塊。然後你可以用任何你想要的方式把木塊碰在一起, 反正他們總是會滑開, 我們就說這個延伸是無聊的。另一方面我們可以考慮這個巴克球表現理論世界: 這個世界中我們只有兩種原子, 沒有磁性的鐵球、或者是有磁性的鐵棒, 球跟球之間不互相作用, 但是鐵棒的磁性可以把球黏在一起, 而且一個鐵棒的兩端各只能黏一顆球。我們就可以研究這個宇宙裡面的延伸, 它稍微比疊疊樂複雜一點, 但是也不會複雜到哪裡去。



回顧

最後我們來回顧一下今天所提到的內容。數學家一開始認爲代數就是以符號操作來解方程式, 所以我們一開始看卡當公式和拉格朗日的預解式, 都可以感受到濃濃的操作意味。接著話鋒一轉, 代數突然沒有要研究那麼實際的直接的問題了, 而是研究那些問題當中的規則所衍生出來的數學分支。我們剛剛看到的加羅瓦定理、群論與表現理論都是這樣子例子的代數。再來代數變成可數名詞, 是來形容那些用規則所生成的數學空間, 比方說實數代數以及李代數, 給我們豐富的例子來抽象化、一般化。之前提到的那些規則。最後代數經過數百年的累積演化成今天的面貌, 或許今天看影片的你, 也能接著踩上巨人的肩膀。謝謝大家今天的收看, 我們有緣再見。

—本文演講者賴俊儒任職於中央研究院數學所—