算学小丛書

伽罗华与羣論

L. R. Lieber 著

商务印書館

算学小丛書

伽罗华与羣論

L. R. Lieber 著

算学小丛書

伽罗华与羣論

L. R. Lieber 著

樊畿譯

商務印书館出版

北京东总布胡同10號

〔北京市书刊出版业营业许可証出字第107号〕

新华书店总經售

商务印书館上海厂印刷

統一书号 13017·171

1936年7月初版
1958年2月3版
1958年11月上海第2次印刷
印張 2 3/16
開本 787×1092 1/32
字數 25,000
印數 4,701—5,500
定價(10)¥0.30

引　言

大家都知道：科學知識是與時俱進的，科學是一種活的，蓬勃滋長的東西．然而一般人總把數學看做又老又朽，似乎再也不能滋長發揚的了．的確，在學校裏所教的數學——算術，代數，幾何——在幾世紀前大家早都知道；就是專門學院的教程差不多也有三百多年的歷史．笛卡兒 (Descartes) 之創造解析學和牛頓 (Newton) 之發明微積分，那都是十七世紀的事情．可是，事實是這樣的：數學的範圍甚至比科學的範圍還要來得廣些，就從那個時候起，他已在腳踏實地的向前邁進了．

數學中一些比較新穎的概念是什麼？是不是他們太抽象了——雖然好些概念還是由很年輕的數學天才所創的——使得這一代的青年人連聽都夠不上聽一聽呢？是不是他們距離平常的一般思維方法太遠了，以致不能使一般普通的人們從中得到任何用處和快樂？難道連一般數

學教員對於這些概念也不能有一個認識的機會嗎？不是的！其實是這樣的：那些近代數學上的發展不但能使數學家發生興趣，而且正像微積分一樣，對於科學家也能有相當偉大的幫助．哲學家公認：近代數學與基本的宇宙觀是有直接關係的．心理學家在近代數學中也會看到一種能從偏見中把心胸解放出來的以及能在陳腐的偏見之荒墟上建立起簇新有力之結構來的偉大工具——像是在非歐几里得幾何學之創造中所可以看到的．的確，誰都要珍重現代數學之特殊的旺盛和卓絕的本色．

這本小册子，作者有心想把他當做現代數學中一支的入門，使得那些對於這門數學願作更進一步研究的人們在閱讀時較爲容易些有趣些．

伽羅華與羣論

伽羅華

這本小册子裏所講的是羣論 (Theory of Groups), 羣論是近代數學的一種. 伽羅華 (Évariste Galois) 對於這門數學的理論和應用很多發揚. 伽羅華歿於一百年以前[1], 死的時候還不滿二十一歲. 在他那短促而悲慘的生命中, 於羣論頗多貢獻; 而這門數學在今日已成爲數學中的重要部分了. 自古以來的二十五位大數學家中, 他就是其中之一位[2].

他的一生, 除了在數學上有驚人的成功, 其餘盡是失意的事. 他渴望着進巴黎的 L'Ecole Polytechnique, 但在入學考試時竟失敗了; 過了一年, 他再去應試, 然而仍舊是失敗. 他拿自己研究的結果給歌西 (Cauchy) 和傅利 (Fourier) 二氏看, 這兩人是當時很出色的數學家, 但是他們對

(1) 譯者按: 伽羅華卒於 1832 年, 此書原本係在 1932 年出版, 所以原書作者說: "伽羅華歿於一百年以前".

(2) G. A. Miller in Science, Jan. 22, 1932.

他都沒有注意，而且兩人都把他的稿本拋棄了．他的師長們談起他的時候，常說："他什麼也不懂"．"他沒有智慧，不然就是他把他的智慧隱藏得太好了，使我簡直沒法子去發見他" 他被學校開除了．又因爲是革命黨徒，曾經被拘入獄．他曾與人決鬬，就在這決鬬中他是被殺了(1)．

敬祝他的靈魂安樂！

(1) 在決鬬的前夜，他自己預知必死，倉猝中將自己在數學上的心得草率寫出，交給他的一個朋友（參看 Annales de L'Ecole Normale Superieure, 1896 中 M. P. Dupuy 所作之伽羅華傳，或參閱 David Eugene Smith 所著之 Source Book in Mathematics 一書．

I 羣的重要

在講羣論之先，先把羣論之所以重要的幾個原因之一說一下.

我們都知道數學中一樁要緊的事情是解方程式. 代數方程式(1)可以依他的次數來分類.一次方程式(2)

$$ax+b=0$$

祇要是學過初等代數的小孩子都會解(3),他的解答是

$$x=-b/a.$$

二次方程式

$$ax^2+bx+c=0$$

的解法在初等代數中也有,他的解答是

$$x=(-b\pm\sqrt{b^2-4ac})/2a$$

---

(1) 代數方程式是作

$$a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n=0$$

的形式的方程式,此中 n 是正整數.

(2) $a=0$ 而 $b\neq 0$ 的情形除外.

(3) 一次方程式的解法是在紀元前 1700 年發明的，這年代是根據 Ahmes Papyrus 書中的記載. 此抄本是一部最早的數學文獻，現已得美國數學會之贊助而出版.

在紀元前數世紀，巴比倫人 (Babylonians) 已能解這種形狀的方程式了(1).

三次方程式

$$ax^3+bx^2+cx^2+d=0$$

和四次方程式

$$ax^4+bx^3+cx^2+dx+e=0$$

的解法已比解一次、二次的方程式難得多了. 直到十六世紀纔有了解法. 這法子在每本方程式論的書中都可以找到.

當方程式的次數增大時，解法的困難增加得很快. 向來數學家雖都不會解一般高於四次的方程式，可是都相信一定是可能的(2). 直到十九世紀，利用羣論的道理，纔證明了這是不可能的事.

此處讀者應該要懂得透澈的是剛纔所說的"不可能"三個字.

一個問題之能否解決是要看我們對於解答所加的限制條件而定的. 譬如

$$x+5=3$$

(1) 參閱 School and Society, June 18, 1932, p. 833, G. A. Miller 著之 The Oldest Extant Mathematics 一文.

(2) 即如十八世紀的大數學家歐拉 (Euler) 也相信這是可能的.

是能解的，假使我們允許 x 可以是負數的話．設若我們限定 x 不能是負數，那末，這方程式就不能解了

同樣，假使 x 表示銀圓數，方程式

$$2x+3=10$$

是可解的．如果 x 表示人數，這方程式就不能解了，因爲 $x=3\frac{1}{2}$ 沒有意義．

要三等分任意一角，若祇准用直尺與圓規，這是不可能的．但是若許用別的儀器，就可能了．

一個代數式之爲**可約的** (reducible，就是說可以分解因數) 或**不可約的** (irreducible)，要看我們在什麼數域 (Field)[1]中分解因數而定．譬如

$$x^2+1$$

在**實數域** (Field of Real Numbers) 中是不可約的，可是在**複數域** (Field of Complex Numbers) 中卻是可約的，因爲

$$x^2+1=(x+i)(x-i),$$

(1) 一個數域是一個數的集合，其中任二數的和，差或積或商 (但零不許作除數) 仍在這集合中．故所有複數做成一個數域；所有實數也做成一個數域；所有有理數也做成一個數域．但是一切整數的集合不成一個數域．因爲兩個整數的商不一定還是整數．許多有趣的數域的例子，可以在 L.W. Reid 之 The Theory of Algebraic Numbers 書中看到．

此處的 $i=\sqrt{-1}$. 簡單的說：我們若單說一個代數式是可約的或是不可約的，而不說出在什麼數域內，這話是全然沒有意義的.

數學家知道特別說明範圍 (Environment) 的重要. 我們說：一個命辭在什麼範圍中是對的，在什麼範圍中是錯的，甚而至於在什麼範圍中是絕對沒有意義的.

那末，剛纔所說一般高於四次的方程式不能解究竟是什麼意思呢？這問題的答案是：一般高於四次的方程式是不能用根式解的. 所謂‘不能用根式解’是說方程式的根不能用有限次的有理運算 (加、減、乘、除) 和開方表作方程式的係數之函數.

爲要說明這一點，拿一次方程式

$$ax+b=0$$

來看，這方程式的根是.

$$x=-b/a;$$

所以 x 的值可以用 a 除 b 而得，這是一個有理運算！二次方程式

$$ax^2+bx+c=0$$

的兩個根是

$$x=(-b\pm\sqrt{b^2-4ac})/2a,$$

這也可以由有限次的有理運算和開方而得.

同樣,一般的三次、四次方程式的根也可用有限次的有理運算和開方表作係數的函數.換句話說:他們可以用**根式解** (Solvable by Radicals).

可是,若論到高於四次的方程式時,這就不再成立了.當然,這是指一般高於四次的方程式而言,有些特殊的高次方程式還是可以用根式解的.

以後我們將看到怎樣用羣論的原理來證明一般高於四次的方程式是不能用根式解的(1).

我們還可以看到:用羣論的道理來證明以直尺.圓規三等分任意角之不可能是何等簡單而綺麗,正如應用羣論於其他名題一樣!

(1) 若不限定單用有理運算和開方來解高於四次的方程式,關於這點,可參讀 L. E. Dickson 的 Modern Algebraic Theories 以及該書中所指的參考書[這當然不是指近似解法如圖解法或霍納氏法(Horner's method)等而言的,這類近似解法祇在應用數學上有用].

II. 羣是什麼

數學中的系統 (System) 可以說是一部數學的機器 (A Mathematical Machine), 他的主要成分是

(1) 元素 (Element).

(2) 一種運算 (Operation)

例如,

(*a*) (1) 元素是一切整數(正或負或 0);

(2) 運算是加法.

(*b*) (1) 元素是一切有理數[1] (0 除外);

(2) 運算是乘法.

(*c*) (1) 元素是某幾個文字 (如 x_1, x_2, x_3) 的置換 (Substitution);

(2) 運算是將一個置換跟着另一個置換 (這個

(1) 一個有理數是一個可以寫做兩個整數的商的數. 譬如 3/5 是一個有理數, 但是 $\sqrt{2}$ 不是有理數, 因爲 $\sqrt{2}$ 不能表作兩個整數之商的形狀; 這事實的證明,可參考Rietz and Crathorne : College Algebra, p. 23.

且待以後再解釋)

(d) (1) 元素是下圖的旋轉，轉的度數是 60° 或是 60° 的倍數；

(2) 運算是如 (c) 中一般，將一個旋轉跟着另一個旋轉.

從這麼一個簡單的出發點着手，看去似乎弄不出什麼東西來，然而這樣討論下去所得的結果會令人詫異的！

這種系統若能滿足下列四條性質，就稱爲羣 (Group)：

1. 假使兩個元素(1) 用那規定的運算結合時，所得的結果還是系統中的一個元素.

例如：

在 (a) 中，一個整數加到另一個整數上去的結果還是一個整數.

在 (b) 中，兩個有理數相乘的結果還是一個有理數.

在 (c) 中，設有一個置換將 x_1 代作 x_2，x_2 代作 x_3，x_3 代

(1) 這兩個元素不必相異，也可以是同一個元素.

作 x_1, 卽是將

$$x_1 \quad x_2 \quad x_3$$

換作

$$x_2 \quad x_3 \quad x_1$$

若在這置換之後跟着另一個置換, 假設這另一個置換是將 x_2 代作 x_3, x_3 代作 x_1, x_1 代作 x_2 的, 那末, 這兩個置換結合的結果是一個將

$$x_1 \quad x_2 \quad x_3$$

換作

$$x_3 \quad x_1 \quad x_2$$

的置換.

在 (*d*) 中,設在一個 60° 的旋轉 (逆時針方向) 之後跟着一個 120° 的旋轉 (逆時針方向), 其結果是一個 180° 的旋轉 (逆時針方向).

2. 系統中必須含有主元素 (Identity Element). 所謂主元素是這樣性質的元素: 他與系統中任意另一個元素結合的結果仍是那另一個元素.

例如,

在 (*a*) 中, 主元素是 0, 因爲 0 與任何整數相加的結果

還是那個整數.

在 (*b*) 中, 主元素是 1, 因爲任意一個有理數用 1 乘了之後的積還是那個有理數.

在 (*c*) 中, 主元素是那個將 x_1 代作 x_1, x_2 代作 x_2, x_3 代作 x_3 的置換, 因爲任意一個置換和這個置換結合的結果還是那個置換.

在 (*d*) 中, 主元素是那個 360° 的旋轉, 因爲系統中的任意一個旋轉和這個旋轉結合的結果還是那個旋轉.

3. 每個元素必須有一個**逆元素** (Inverse Element). 所謂一個元素的逆元素是這樣規定的: 一個元素和他的逆元素用系統中的運算結合的結果是主元素.

例如,

在 (*a*) 中, 3 的逆元素是 -3, 因爲 3 加 -3 的和是 0.

在 (*b*) 中, a/b 的逆元素是 b/a, 因爲 a/b 和 b/a 相乘的積是1.

在 (*c*) 中, 將 x_1 代作 x_2, x_2 代作 x_3, x_3 代作 x_1 的置換的逆元素是那個將 x_2 代作 x_1, x_3 代作 x_2, x_1 代作 x_3 的置換. 因爲這兩個置換結合的結果是那個將 x_2 代作 x_2, x_3 代作 x_3, x_1 代作 x_1 的置換.

在 (d) 中，那個 60° 的旋轉（逆時針方向）的逆元素是一個 −60° 的旋轉(就是說：一個順時針方向的 60° 的旋轉). 因爲這兩個旋轉結合的結果和那個 360° 的旋轉一樣.

4. **結合律**(1) (Associative Law) 必須成立.

因爲一個羣(2) 必須具備上述的四條性質，所以在 (a) 中若把 0 去掉，那系統就不成爲羣了，因爲那麼一來，系統裏沒有主元素.

一切整數用乘法作系統中的運算不成一羣. 譬如拿 3 來說，他的逆元素 1/3 不在系統中.

所以一個系統之是否成羣，不但要看他的元素，還要看他的運算纔能決定.

讀者所當注意的是：

(1) 元素不必一定是數，可以是一種運動[如在 (d) 中]，

(1) 設 a, b, c 是任意三個元素，又設運算用記號 ○ 來表示. 那末結合律就是說

$$(a \circ b) \circ c = a \circ (b \circ c).$$

例如，在 (a) 中，

$$(3+4)+5=3+(4+5)$$

所以結合律在 (a) 中能成立，同樣，結合律在 (b), (c), (d) 中都成立.

(2) 關於羣的例子，可參看 L. C. Mathewson : Elementary Theory of Finite Groups.