

代數學是應用數學系的基礎課程之一，在大學階段的學習重點為抽象代數 (Abstract Algebra)。代數學的主要內容是由公設出發，因此會有點抽象，但應用方面相較於理論卻非常具體實在。代數學的主軸在群 (Groups)、環 (Rings)、體 (Fields) 的代數結構，了解代數的結構以後，就能夠解決許多難題，其中最典型的例子就是證明了「只用尺規作圖，不能三等分任意角」。

群論的起源可追溯到十六世紀初，當時有許多數學家都致力於解一元多次方程的根並發展出根式解，其中一元二次、三次及四次方程式都先後被找出根式解，但是一元五次或更高次方程式的根式解卻一直沒有成功。在十八世紀末，Lagrange 提供了一元四次以下的方程式統一的解法，但是這樣的解法也無法求出一元五次方程式的根式解。

受到 Lagrange 的影響，Abel 和 Galois 便有了不同的看法，他們開始懷疑這種根式解的存在性，於是他們轉向研究方程式及其解的一般性質，這些研究便發展出「群」的結構：包含一個集合、一個二元運算 (Binary Operation)，並且必須滿足四種性質 (封閉性、結合律、單位元素以及反元素)。

在十九世紀初，Abel 利用群的概念證實了五次或更高次的代數方程其一般根式解並不存在。而 Galois 則提出，一個給定的方程式「何時有根式解」有一定的判斷準則。經由 Lagrange、Abel、Galois 等人的努力，解方程式的問題也在此告一段落。

群論本身不但極具內涵，它的觀念也有很廣泛的應用。舉例來說，十九世紀的挪威數學家 Sophus Lie 爲了研究微分方程的解而發展出李群；接著 Felix Klein 和 Elie Cartan 則利用李群來對空間的對稱性質進行研究，是幾何學的一大創舉。在二十世紀前半，大量的物理學家開始利用這些研究來測量宇宙的對稱與曲率，其後楊振寧先生在研究理論物理的工作也廣泛地利用到群論的概念；除此之外，群論在晶體學和化學上的應用也非常出色。

環的結構則是由一個集合加上的兩個二元運算，並且滿足某些性質所組成。舉例來說，整數以及一般的加法和乘法就可以構成一個環；另外，所有係數為有理數的多項式所形成的集合，再加上多項式的加法與乘法也是環的另一個例子。

考慮由 n 階的方形矩陣配上矩陣的加法和乘法，同樣也具有環的結構，而線性代數即為一門從矩陣出發的學科，因此線性代數也是代數學的重要內容之一。此外，環在應用上也可用來研究一些數論上的問題。

體的結構其實是環的一種，但是體需要滿足的性質比較多，最主要的差別在於乘法的交換律，及非零元素都有乘法反元素。前面環的部份所提到整數的例子就不是一個體，而有理數、實數及複數所形成的集合都是體的重要的例子。除了這些具有無窮個元素的體非常有用之外，有限體（Finite Field）也非常地重要。例如由 0、1 所成的集合，適當定義加法及乘法就可以形成兩個元素的有限體。有限體在數位訊息錯誤的糾正理論中扮演非常重要的角色，所以我們能由數位光碟機聽到音樂是「體」的一個應用。

在代數學的應用方面，除了上述的幾個例子以外，將代數學做應用所延伸出的「編碼學」和「密碼學」也是非常重要的一塊。進入數位化時代的二十一世紀，無論是聲音或是影像等資訊，都需要透過用數位化的方式做處理，而最重要的就是要保持訊號的傳遞和讀取不會有差異，因此，數位訊號就必須經過特殊的人為處理，即是所謂的「編碼」（Coding）。而在現代生活中，不論是電腦上網、電子郵件、線上購物、信用卡的使用、甚至是門禁管制系統等等，各種涉及隱私或資訊安全都需要密碼，因此，密碼學的發展以及加密與解密的技術，將會是科技時代不可或缺的知職。

上述文章為本系研究生詹博翔依據（1）國立交通大學應用數學系課程介紹 — 代數學（2）國立中央大學數學系課程簡介 — 應用代數（3）群論的起源 — 曹亮等相關資料撰寫初稿，經本系余屹正教授修改潤飾完成。