

國立臺灣師範大學數學系教學碩士班碩士論文

指導教授：洪有情 博士

Galois 理論思想研究

A Study of Ideas in Galois Theory

研究生：楊淑惠

中華民國一百零三年八月

摘 要

十九世紀初，法國數學家 Galois 在他短暫的生命歷程中，留下代數學上極為珍貴的研究成果，並因著他獨創的理論思想，確立了他在數學史上劃時代的地位。

本論文將從西方數學的代數學發展脈絡中，認識 Galois 生長的時代背景與成長際遇，並深入探討 Galois 的數學理論，包括其思維的進路、理論的應用等，而對於 Galois 思想的特性以及文化上的意義也進行深入的研究。

全文共分五章。第一章「緒論」，說明研究動機、文獻探討、研究目的、研究方法等。第二章「Galois 的生平背景」，以數學史的方法進行研究，對於代數學的前人足跡以及 Galois 在求學、研究及對政治狂熱的生平，詳細探討，並以年表呈現。第三章「Galois 理論探討」，從數學的抽象代數角度剖析理論的層層關聯與整體輪廓，並加入許多例子輔以說明，其中不乏古希臘幾何三大難題與正 n 邊形作圖等問題，以作為理論的應用。第四章「Galois 思想的文化意義」，用文化的眼光看待 Galois 思想，包括其理論特性與思想精神等，以及從數學美學的視野賞析 Galois 思想，並延伸至科學、藝術與音樂各領域，處處皆存有其思想的痕跡，最後回歸到數學教育的省思。第五章「結語」，以 Galois 從解決五次方程式根式解問題出發所發展出的理論思想卻能如此深邃豐沛作總結。

本論文研究的核心在第三章、第四章，期使偉大的 Galois 理論思想有新的詮釋。

關鍵字：Galois、數學思想、文化研究

Abstract

In early nineteenth century, the French mathematician Galois left his extremely valuable research results in algebra during the course of his short life. And because of the original theory and ideas which were developed on his own, he established a landmark in the history of mathematics.

This paper provides a view from the development context of algebra in Western mathematics. From knowing the historical background and growth of Galois to exploring the mathematical theory of Galois in depth, including his thinking approach, the application of the theory, and also study deeply in ideas and cultural meanings of Galois.

This paper is divided into five chapters. The first chapter, "Introduction," describes research motivation, purpose, and research methods. The second chapter, "Galois' life context", is the study using the history of mathematical methods to discuss in detail about the generation of predecessors footsteps in algebra, and the understanding of Galois' schooling process, as well as his political fanaticism life. This chapter is chronologically presented.

The third chapter, "Discussion on Galois Theory", analyzes the association and the overall outline in the theory from the perspective of abstract algebra. It is supplemented by adding many examples to illustrate, including the three major problems in ancient Greek geometry, and the issue about whether the regular n-gon can be constructible by ruler and compasses, to apply the theory.

The fourth chapter, "The cultural significance of Galois' thinking", uses cultural vision to look at Galois' ideas, including his theoretical characteristics and ideological spirit, as well as appreciating Galois' thought from the perspective of mathematics aesthetic, and extends to various fields of science, art and music, which finally returns to the reflection of mathematics education. The fifth chapter, "Conclusion", summed the richness of Galois' theoretical ideas, although he starts from solving the problem of the general equation of degree 5 by radicals.

The core of this thesis is in Chapter three and Chapter four, which expects the new interpretation in great ideas of Galois Theory.

Key words : Galois, mathematical thinking, cultural research

誌 謝

自從大學時期接觸了高等代數課程，在腦海中就一直存留著對 Galois 理論深入瞭解的渴望。大學畢業後投身國中數學科教職，遂將 Galois 理論收藏於內心深處，成為一個記憶的圖騰。直到再次回到臺灣師範大學數學系教學碩士班進修，才發現上帝豐富了我各種經歷之後，終於適時地讓我重新面對 Galois 理論。因此，從決定著手研究「Galois 理論思想」的那一刻起，心中就十分篤定且充滿感謝，相信整篇論文的書寫，神必與我同在。

如今論文完成，首先要感謝洪有情教授的指導，引領我對 Galois 理論有更深入的認識，並進行較廣泛的研究；也要感謝論文口試時，劉容真教授所提出的專業論點與意見，英家銘教授悉心指正與寶貴的建議，都讓我銘感於心！

除此之外，由衷感謝師長們在課堂上的傾囊相授，以及數學教碩班同學們在學習中所培養的互助情誼，在日頭赤燄燄的三個暑期當中，為我澆灌了更多的養分。同時也感謝家人全力的支持，以及張美美學姊的從旁鼓勵。您們每一位都是上帝派來的天使。

在此，謹以此篇論文獻給孕育我成長茁壯的家鄉土地——高雄，以撫平今夏遭受嚴重氣爆的傷痛。願 神保守並賜下平安！

2014 年 8 月

目 錄

第一章 緒論	1
第一節 研究動機	1
第二節 文獻探討	2
第三節 研究目的與方法	6
第二章 Galois 的生平背景	7
第一節 代數學的前人足跡	7
第二節 Galois 的生平	19
第三章 Galois 理論探討	49
第一節 思維的進路	49
第二節 理論的應用	87
第四章 Galois 思想的文化意義	99
第一節 思想的特性	100
第二節 美學的視野	111
第三節 藝術的延伸	120
第四節 音樂的對話	128
第五節 數學教育的省思	137
第五章 結語	141
參考文獻	
中文部分	145
英文部分	146

第一章 緒論

本章共分三節：第一節為「研究動機」，第二節為「文獻探討」，第三節為「研究目的與方法」。



第一節 研究動機

在中學數學教育中，解代數方程式一直是重要的一環，而不論國中階段解較低次的方程式，或高中階段處理更複雜的代數方程式，都是在作抽象思維的訓練。十九世紀初的法國數學家伽羅瓦(Évariste Galois 1811-1832 年)更將方程式根式求解的問題轉化成置換群(permutation group)的問題¹，不再直接去計算方程式的解，卻從繁複的計算過程中找出方程式解的本質，並分析代數結構的變化。這種高度抽象的思維，在伽羅瓦之後被其他數學家採用，且更促進了抽象代數的研究。

年輕就逝世的伽羅瓦，在世上雖留下不多的數學著作，卻牽動著往後近百年的學術發展。伽羅瓦的「群」，使得科學的研究開始注重內部結構「關聯」的作用，同時也標誌出創新的數學語言。於是，「群論」的研究接續有學者投入，也使得人們觀看事物的方式有了很大的轉變，「由內而外」的觀點強化了結構的重要性，而群論所作的抽象分析，確能對照於眾多領域，一體適用。

縱覽國內許多數學文化方面的文獻，從數學美學或藝術層面進行的研究尚有開發的空間。研究者因身為國中教師，大學時曾接受過專業的抽象代數教育，且長期進行音樂學習，深感兩者有許多共通之處：數學是思維的藝術，而音樂是時間的藝術，並且它們都有外在形式和內在結構的抽象概念。若能以藝術的角度觀看抽象代數，對於數學所展現的面貌，將會有新的詮釋。

若將伽羅瓦的理論思想視為一件藝術作品，可謂內外兼具。以美學的視野來認識它，其簡單、和諧、新奇等特性所帶出的理性美，可修飾人們的心靈，成為一種美化人生的力量。若將 Galois 理論思想所揭示的結構美學，向各個藝術領域延伸，將可為各種藝術賦予了更深層的理性美。這些方面的思考，成了研究者想迫切研究的主要動機。

也期盼此一研究，能為數學教育導引出另一種不一樣的思考方向。

¹參考康明昌：《幾個有名的數學問題》(新竹市：凡異出版社，民 83 年)，頁 87-88。

第二節 文獻探討

本論文參考了有關數學史、伽羅瓦生平與理論的文獻、抽象代數專書，以及美學哲學類、文化藝術類、數學教育類等文獻，茲分述如下。

一、數學史類

代數學的史蹟部分，在袁小明編著的《數學史》²、以及 Morris Kline 原著，林炎全、洪萬生、楊康景松譯的《數學史》(*Mathematical Thought From Ancient to Modern Times*)上中下三冊³、William P.Berlinghoff 與 Fernando Q.Gouvêa 著，洪萬生、英家銘暨 HPM 團隊譯的《溫柔數學史》⁴(*Math through the Ages : A Gentle History for Teachers and Others*)、王懷權編著的《數學發展史》⁵，探討了數學從古代以來的主要建樹和推展，其中對於不同年代數學觀念的演化，都有很深入的詳述。包括從西方的巴比倫、埃及、古希臘文明所發展出來的數學，以至東方的印度、阿拉伯、中國等地的研究成果，並記載了西方經歷中世紀時期後，數學在 15、16 世紀逐漸復興的活動，以及後來代數學成為數學的一個分支，各種思潮也風起雲湧的概況，都有很清楚的歷史透視。

除此之外，伽羅瓦的生平背景與學術研究，在 Andre Dalmás 原著的《伽羅瓦傳》(*Évariste Galois: révolutionnaire et géomètre*, 巴黎, 1956 年)中譯本⁶，以及 Mario Livio 著，蔡承志譯的《無解方程式：數學天才與對稱性之謎的鬥智之旅》⁷(*The Equation That Couldn't Be Solved : How Mathematical Genius Discovered the Language of Symmetry*)均有許多考據，甚至還有書信、筆記、著作，以及其他相關資料的文件，對於研究伽羅瓦的生平事蹟，提供了相當多珍貴的史料。

歷史上所出現的對於伽羅瓦的研究，除了著重在他的數學成就之外，也有許多是以他傳奇且短暫的一生，作為探討天才的素材。

²袁小明編著：《數學史》(台北市：九章出版社，2003 年)。

³ Morris Kline 原著，林炎全、洪萬生、楊康景松譯：《數學史》上、中、下冊(台北市：九章出版社，上冊民 68 年，中、下冊民 72 年)。

⁴比爾·柏林霍夫(William P.Berlinghoff)與佛南度·韋維亞(Fernando Q.Gouvêa)著，洪萬生、英家銘暨 HPM 團隊譯：《溫柔數學史》(台北市：博雅書屋，2008 年)。

⁵王懷權編著：《數學發展史》(新竹市：協進圖書有限公司，民 70 年)。

⁶達爾馬斯(Andre Dalmás)原著：《伽羅瓦傳》(新竹市：凡異文化事業有限公司，民 75 年)。

⁷ Mario Livio 著，蔡承志譯：《無解方程式：數學天才與對稱性之謎的鬥智之旅》(台北市：臉譜，城邦文化出版：家庭傳媒城邦分公司發行，2008 年)。

二、代數學類

在抽象代數的專業書籍當中，Ian Stewart 所著的《*Galois Theory*》⁸，大學科學叢書③康明昌教授著的《近世代數》⁹、《幾個有名的數學問題》，呂溪木教授著《體與 GALOIS 理論》¹⁰等書都對 Galois 理論有很完整的介紹，也有深入淺出的論述，以供研究者對此一理論作正確的探討。另外，在 Michael Artin 所著，郭晉云譯的《代數》(*Algebra*)¹¹，以及 Garrett Birkhoff 與 Saunders Mac Lane 所著，王連祥、徐廣善譯的《近世代數概論》(*A Survey of Modern Algebra*)¹²，由 David M. Burton 所寫的《*Abstract and Linear Algebra*》¹³，聶靈沼、丁石孫著的《代數學引論》¹⁴，王芳貴編著的《代數學基礎》¹⁵等書籍，也都對代數學的知識闡述相當詳盡，有助於對代數學概念的正確理解。

除此之外，丘維聲著的《數學的思維方式與創新》¹⁶提出了數學思維方式的五個重要環節：觀察、抽象、探索、猜測、論證，¹⁷其中並有專章討論伽羅瓦的創新理論思想，對於讀者的啟發思維訓練與領略數學創新的風采，都有獨到的見解，精闢入裏。而徐誠浩編著的《抽象代數：方法導引》¹⁸一書，是在概念理解之外的另一種幫助，當中對於各種概念從正、反兩面適時地提出例證，可澄清許多模糊的觀念。在張雄、李得虎所編著的《數學方法論與解題研究》¹⁹書中，也有許多數學的創造性思維的本質探討，提供了解題時的思路、方法等的原理與策略。

三、美學哲學與各項文化類

在美學哲學領域的書籍中，徐炎章、吳開朗、唐煌、周金才著的《數學美學思想史》²⁰與徐紀敏著的《科學美學思想史》²¹介紹了古今中外許多數學、科學的美學思想發展。數學的美學思想貫穿於數學的歷史發展脈絡中，並從一些知名數學家的努力追求之下提出了對於數學的審美觀，開啟了數學學術中較為軟調的研究方向。而徐本順、殷啟正著的《數學中的美學方法》

⁸ Ian Stewart：《*Galois Theory*》(新竹市：凡異出版社)。

⁹ 康明昌著：《近世代數》(台北市：聯經出版事業股份有限公司，1988年)。

¹⁰ 呂溪木著：《體與 GALOIS 理論》(台北市：協進圖書有限公司，民72年)。

¹¹ Michael Artin 著，郭晉云譯：《代數》(北京：機械工業出版社，2009年)(華章數學譯叢)。

¹² Garrett Birkhoff、Saunders Mac Lane 著，王連祥、徐廣善譯：《近世代數概論》第5版(北京：人民郵電出版社，2008年)。

¹³ David M. Burton：《*Abstract and Linear Algebra*》(台北市：協進圖書有限公司)。

¹⁴ 聶靈沼、丁石孫著：《代數學引論》(新竹市：凡異出版社，民85年)。

¹⁵ 王芳貴編著：《代數學基礎》(北京：科學出版社，2012年)(北京高等教育「十二五」規劃教材)。

¹⁶ 丘維聲著：《數學的思維方式與創新》(北京：北京大學出版社，2011年)。

¹⁷ 參考丘維聲著：《數學的思維方式與創新》，序言。

¹⁸ 徐誠浩編著：《抽象代數：方法導引》(哈爾濱：哈爾濱工業大學出版社，2013年)。

¹⁹ 張雄、李得虎所編著的《數學方法論與解題研究》(北京：高等教育出版社，2013年)。

²⁰ 徐炎章等著：《數學美學思想史》(台北市：曉園出版社有限公司，1998年)。

²¹ 徐紀敏著：《科學美學思想史》(中國湖南長沙市：湖南人民出版社，1987年)。

²²等書籍中，提出數學美的特徵包括：簡潔、統一、對稱、整齊、奇異、神秘等，其所留下的痕跡是傳遞數學思想精神重要的媒介；同時，J.N.Kapur 著，王慶人譯的《數學家談數學本質》²³一書中，收錄了九百多則數學家和科學家們對於數學本質的言論錄，引領了接受數學訓練的人有更深一層思維的修養，建立數學的文化理念。

從數學的對稱性、語言、結構等各方面出發，也可在許多文化類的書籍或文獻中找到它們的蹤跡，以下將分別陳列。

「對稱性」可說是整個 Galois 思想的源頭，由它所發展出來的 Galois 理論，成為數學史上偉大的創作。在 Mario Livio 著，蔡承志譯的《無解方程式：數學天才與對稱性之謎的鬥智之旅》中將對稱性作了相當多的闡述與探討，當中附上的圖文也有很嚴謹的考證，並且對稱性帶動了「群論」成為數學語言，在 19 世紀之後成為數學新興的分支。

數學語言也是本研究極為重要的一個主題，由 Keith Devlin 著，洪萬生、洪贊天、蘇意雯、英家銘譯的《數學的語言》²⁴(*The Language of Mathematics*)，揭示了數學的抽象概念，可以簡潔的數學語言呈現，其美感與重要性不言可喻。另外，在 Mario Livio 著，蔡承志譯的《無解方程式：數學天才與對稱性之謎的鬥智之旅》中，對於數學語言部分，也有發人深省的觀點。

對於從一個平行公設的替換，所造成歐氏幾何與非歐幾何的結構變化，在許多書籍與期刊雜誌中多有研究與發表，其中包括 M.Kline 著，張祖貴譯的《西方文化中的數學》、歐陽絳著的《數學的藝術》²⁵、張景中著的《數學與哲學》²⁶、Keith Devlin 著，洪萬生、洪贊天、蘇意雯、英家銘譯的《數學的語言》等書，各以不同角度來審視這兩類幾何的異同，與其所帶出的文化意義。

除此之外，許多數學方面的學者所關心的，是數學在人類文化、思想精神的交互影響，以及與歷史上各個不同時期的文學、藝術、音樂、哲學、宗教、自然科學、人文科學等領域的內在聯繫，如何有機地融合為一體？其中以 M.Kline 著，張祖貴譯的《西方文化中的數學》²⁷(*Mathematics in Western Culture*)一書，將數學的思想精神滲透到各文化分支，讓理性美的魅力與全貌藉由它們傳遞出去。又如曹亮吉著的《阿草的數學聖杯》²⁸、世紀文庫的《當數學遇見文化》²⁹中劉柏宏及劉淑如寫的〈數學與音樂的對話〉³⁰、石峰編

²²徐本順、殷啟正著：《數學中的美學方法》(中國大連：大連理工大學出版社，2008年)。

²³J.N.Kapur 著，王慶人譯：《數學家談數學本質》(台北市：儒林圖書有限公司，1992年)。

²⁴Keith Devlin 著，洪萬生、洪贊天、蘇意雯、英家銘譯：《數學的語言》(台北市：商周出版，2011年)。

²⁵歐陽絳著：《數學的藝術》(台北市：九章出版，1994年)。

²⁶張景中著：《數學與哲學》(台北市：九章出版，1996年)。

²⁷M.Kline 著，張祖貴譯：《西方文化中的數學》(台北市：九章出版，1995年)。

²⁸曹亮吉著：《阿草的數學聖杯》(台北市：天下遠見出版股份有限公司，2003年)。

²⁹洪萬生、英家銘、蘇意雯、蘇惠玉、楊瓊如、劉柏宏著：《當數學遇見文化》(台北市：三民書局出版股份有限公司，2010年)。

著的《音樂世界趣談》³¹，都對音樂與數學內在本質的共通特性有一些著墨。這些都可作為本研究的路線。

為了對 Galois 理論思想有較完整的研究，在探討文獻的工作上，研究者以國內外學者或大學教授的著作為主要對象，惟因本身語言文字的有限，外文書多以中譯本為主，另外中文類也涵蓋了一些中國簡體字書籍。但本著知識無國界的信念，以開放的心態吸收前人研究的成果，以作為本研究的基礎。

³⁰ 參考洪萬生等著：《當數學遇見文化》，頁 27-40。

³¹ 石峰編著：《音樂世界趣談》（北京：人民音樂出版社，1986 年）。

第三節 研究目的與方法

本研究有三個最主要目的：第二章擬站在時間的長河來認識伽羅瓦和他的創見與思想；第三章擬深入瞭解 Galois 理論的內容與精髓；第四章則擬從內、外等不同角度來審視伽羅瓦的理論思想，並將其延伸至各個文化層面。

整體而言，本研究以數學文化評論為研究取向，整理國內外學者之二手文獻，並加入研究者的分析，對數學知識脈絡本身及其文化意義進行評論。³²

第二章「Galois 的生平背景」的研究方法，將以時間為主軸，著眼於代數學的發展，而走到伽羅瓦的時代，數學界仍舊為著「五次方程式是否有根式解？」在困惑著。伽羅瓦的生長背景、求學過程、學術際遇、政治參與和愛情追求等，都對其人格與思想造成某種程度的影響。研究者並將以「年表」的方式呈現，使眾多事蹟的發生，能在所屬年代的坐標中找到定位。對於伽羅瓦的生平與背景有了基本的認識，比較能理解其思想的形成模式；從歷史的觀點透視，也能清楚看到伽羅瓦的學術貢獻在數學發展過程中所扮演的角色。

第三章「Galois 理論探討」，將採用丘維聲著的《數學的思維方式與創新》一書中，對於數學思維的五個重要環節的論述。從「觀察—抽象—探索—猜測—論證」³³五種思維進路，以逐步深入探究 Galois 理論的形成全過程。以此方式來認識 Galois 理論思想，或有時仍不免遇到思維處在盤根錯節的狀況下，然而待走過每一種思維的旅程，將會對 Galois 理論思想的內在規律有清楚的認識，從而在繁複的思想中形成井然的結構秩序，這是研究者極力想達成的目標。在本論文第三章中，也引入一些重要或關鍵的例證，作為 Galois 理論外顯和實現的確據，雖然有些是前人早已研究過的，但研究者試圖以較淺顯易懂的方式，提供數學教育工作者參考，以使此理論更能有活潑的生命。

第四章「Galois 思想的文化意義」，研究方法將以不同的視角來認識 Galois 理論思想，分別有：以 Galois 理論思想為主體，由內由外剖析其獨特的風格；檢視 Galois 思想與數學美學所擦出的火花；觀看 Galois 思想滲入各個藝術領域的痕跡，包括「對稱性」遍佈於視覺與聽覺的藝術中；從群的角度思考因著一個平行公設的更易而改變的幾何結構(歐氏幾何與非歐幾何)；著眼於 Galois 思想體系與音樂學在抽象空間與語言符號之間的共通法則；並站在數學教育的立場，思考 Galois 理論思想所帶給數學教育的省思。各種不同的視角源於研究者與 Galois 理論思想所拉開的距離遠近，不同距離感所產生的文化意義也略有差異。

綜合本論文的研究方法，有以時間作為坐標的，也有以思維進路作為里程的，更有以距離感作為變項的。凡此種種，均以 Galois 理論思想作為研究對象的中心，以達成本節一開始所揭櫫的三個主要的研究目的。

³²參考英家銘博士寶貴意見。

³³參考丘維聲著：《數學的思維方式與創新》，內容簡介。在本論文第三章第一節對此五個思維亦有詳細說明。

第二章 Galois 的生平背景

本章共分為兩節，第一節為「代數學的前人足跡」，第二節為「Galois 的生平」。

第一節 代數學的前人足跡

一、方程的萌芽

在西方數學的發展史中，有關代數學最早的文獻記載，出現在古埃及的《林特草卷》，它記錄了接近四千年前(西元前 1650 年之前)人類的心智活動，可以看出當時人類已能運用一元一次方程來解決生活中的問題了。³⁴

而在底格里斯河和幼發拉底河居住的巴比倫人，也大約在四千年前(西元前 1600 年之前)就學會了找尋一元二次方程答案的方法，但是當時的方程和寫法是以語言敘述的；巴比倫人更為了解決天文與曆法的問題，開始有了多個變量的方程組概念，以便處理較複雜的數學。³⁵

他們未必有方程式的概念，但自有一套計算的方法，多半可能是「算術式」的代數運算，也可能是以「幾何式」進入代數的學習。像早期解一元二次方程並未有求根公式，卻從配方法找解，就是由圖形的觀念而來的。³⁶

二、古希臘文化的奠基

古希臘以公設、演譯、推理、邏輯、證明等有系統的方式處理數學，對西方數學的發展影響深遠，至今數學仍用這種嚴謹的方式在演進。

歐幾里得(西元前 325 年-西元前 265 年)是古希臘有名的數學家，他的《幾何原本》是幾何學很重要的教科書，共分為十三卷，其中的第二卷是〈幾何與代數〉，當中就有大量的代數定理是用幾何來證明的。

由於古希臘的數學經常依附在他們擅長的幾何圖形上發展，大約在西元 1 世紀時，古希臘有一位精於測量的數學家海倫(Heron of Alexandria)，曾將幾何量中出現的數抽離出來，以算術化或代數化的型式呈現，揉和古埃及和

³⁴ 參考袁小明編著：《數學史》(台北市：九章出版社，2003 年)，頁 147,190-191。

³⁵ 參考袁小明編著：《數學史》，頁 147,190-191；聶靈沼、丁石孫著：《代數學引論》(新竹市：凡異出版社，民 85 年)，頁 300；呂溪木著：《體與 GALOIS 理論》(台北市：協進圖書有限公司，民 72 年)，頁 3；羅伯·所羅門(Robert Solomon)著，洪慧芳譯：《一本通數學原理》(新北市：繁星多媒體，2012 年)，頁 14。

³⁶ 參考袁小明編著：《數學史》，頁 147,190-191；呂溪木著：《體與 GALOIS 理論》，頁 3。

巴比倫人的數學成就，促進了代數的獨立發展。³⁷

大約在西元 3 世紀時，古希臘出現一位有名的數學家丟番圖(Diophantus of Alexandria)，他的著作《算術》包括了數論、解代數方程式以及方程組的問題。³⁸他引入代數學的未知數，並且為它們創造符號；還率先承認有理數是數，在代數學領域作了很大的貢獻。丟番圖為代數學樹立了思想的架構，堪稱為「代數學之父」。

古希臘文明中的數學，以幾何學大師歐幾里得的《幾何原本》與代數學之父丟番圖的《算術》前後呼應，奠定了當今數學的發展基礎。

接著歐洲進入中世紀時期，在各方面的進步都變得緩慢，經過了上千年的蟄伏，直到 15 世紀才復甦起來。

三、東方文化的活躍

因為數學經常是解決人類生活問題的要角，所以在東方的中國、印度和阿拉伯，代數學同樣有著蓬勃發展。

(一) 中國

以歷史悠久的中國而言，數學的發展源遠流長，一代接一代智慧的累積，有了許多輝煌的成果。尤以西元 1 世紀的《九章算術》是一部經典的數學著作，但因歷經許多學者的增補修改，致作者已不可考；全書共分為九章，以籌算作為整卷書的中心，也有許多篇章皆論及算學與代數。

茲將中國在算術和代數方面的成就，簡略概述如下：³⁹

1. 最早創立「十進位制」的計數方法。
2. 最早形成正、負數概念，並且在《九章算術》〈方程章〉中提出正、負數的運算法則。
3. 《九章算術》〈方田章〉中對分數進行有系統的運算法則。
4. 《九章算術》〈少廣章〉中建立開平方和開立方的方法。
5. 《九章算術》中提出線性方程組的概念。西元 3 世紀時，劉徽提出線性方程組的解法，與「加減消去法」相符。
6. 西元 11 世紀時，中國用「天元術」建立一元高次方程，「天元」就是未知數。從此，代數從算術中獨立出來，而以方程作為主要內容。

³⁷ 參考袁小明編著：《數學史》，頁 147-148。

³⁸ 參考袁小明編著：《數學史》，頁 148。

³⁹ 參考袁小明編著：《數學史》，頁 148-149；維基百科網頁(2013. 9.20)

<http://zh.wikipedia.org/zh-tw/%E4%B9%9D%E7%AB%A0%E7%AE%97%E8%A1%93>

<http://zh.wikipedia.org/zh-tw/%E7%A5%96%E6%B2%96%E4%B9%8B>

<http://zh.wikipedia.org/zh-tw/%E5%A4%A9%E5%85%83%E6%9C%AF>

<http://zh.wikipedia.org/zh-tw/%E5%9B%9B%E5%85%83%E6%9C%AF>

7. 西元 14 世紀初，中國更推廣創立「四元術」，以計算四元高次方程，原則上以消元方法，將四元逐步改為三元、二元，以達一元求解。

(二) 印度

印度與中國、埃及、巴比倫同為四大文明古國，在數學的發展上也有許多貢獻。印度的傳統數學中，在算術和代數方面的成就，整理如下：⁴⁰

1. 建立完整的十進位記數系統。
2. 形成正、負數的概念與計算方法。
3. 提出開方的方法。
4. 用字母和其他符號作為代數的標記法。
5. 推出解線性方程和二次方程的規則，並發現二次方程有兩個根。
6. 處理有無限多組解的不定方程。

(三) 阿拉伯

在西元 7 世紀初崛起於阿拉伯半島的伊斯蘭教，勢力擴張至歐、亞、非三洲，進而吸收古希臘與中國、印度等地區的古典著作，他們將這些著作加以整理修訂，並譯成阿拉伯文保存下來。⁴¹阿拉伯數學的發展，大量透過共同語言的譯文傳承了人類的智慧結晶，對於即將進入文藝復興時期的歐洲，實乃居於承先啟後的重要地位。⁴²

「代數」作為一門學科的名稱，就是阿拉伯人所創。在袁小明編著的《數學史》中，記載如下：

公元 830 年左右，阿拉伯數學家阿爾·花粒子米(Al-Khōwārīzmi, 780-850)寫了一本名為《ilm aljabr wa'l muqabalah》〔此原文寫法有待查考〕的書，原意是《還原(或移項)和對消的科學》。1140 年左右，由阿拉伯文譯成拉丁文時，「al-jabr」變成了「algebra」，.....。1859 年，中國清代數學家李善蘭首次把「algebra」譯為代數學，從此「algebra」的中文意思就是「代數學」了。(頁 150)

花粒子米也用阿拉伯文，編寫了一本關於印度在數字和十進位記數法的著作。後來傳入歐洲，歷經許多世代的改革，始成為今日我們所使用的阿拉伯數字。

⁴⁰ 參考袁小明編著：《數學史》，頁 150；維基百科網頁(2013.9.20)

<http://zh.wikipedia.org/zh-tw/%E4%BB%A3%E6%95%B8>

⁴¹ 參考袁小明編著：《數學史》，頁 150。

⁴² 參考袁小明編著：《數學史》，頁 150。

四、認識未知

代數學漫長的發展進程當中，數學家也遇到許多瓶頸，必須一個一個通過人類心智的反芻與消化，接納了原本混沌且陌生的數，始得以開展柳暗花明又一村的榮景。

以下提出幾個例子，加以說明：

(一) 負數

起初，「負數是一個數」這樣的論述，對於世界各民族而言並不容易接受。從懷疑到接納，經歷了一些轉變的過程，整理如下：⁴³

1. 認為它本質上是不可思議的，是虛構的，是荒謬的，是來擾亂的，是假數...等。
2. 消極的對策：閃躲，全力避開。
積極的解釋：以負債等幫助理解。
3. 13 世紀時，將負數以負債加以解釋。
15 世紀時，負數出現在方程的討論上。
19 世紀以邏輯為基礎所確立的整數系統，才將負數定位。

(二) 無理數

西元前五百多年前，希臘數學家畢達哥拉斯(約西元前 580-西元前 500 年)認為所有的數都可以寫成兩整數相比的值。對於不能寫成兩整數相比的數值，起初也像個頑梗之物，無法讓人理解。經歷的過程十分曲折，整理如下：⁴⁴

1. 認為它本質上是「邪惡之物」，甚至是上帝天衣無縫創造下「不可說」的瀆神之物...等。
2. 消極的處理：如畢達哥拉斯採離散觀點，將它視為「破綻」。
積極的解釋：以算術或幾何處理而承認它，中國和印度則求近似值。
採取的方式：型態上以無限跑遠且不會循環的小數，或以連分數逼近的數呈現。
3. 以邏輯結構為基礎，解決無理數尷尬的定位，也是在 19 世紀時。
西元 1886 年(伽羅瓦之後的年代)，施圖爾茲(Stolz 1842-1905 年，德國數學家)證明了「每一個無理數都可表示成無限不循環小數」，成為今日學界對無理數所接受的定義。

⁴³ 參考袁小明編著：《數學史》，頁 159-164。

⁴⁴ 參考袁小明編著：《數學史》，頁 165-171。

(三) 超越數

在 18 世紀時，瑞士數學家歐拉(Euler 1707-1783 年，瑞士數學家)定義了「超越數」，簡述如下：

形如 $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ ($n \geq 1$, $a_n \neq 0$) 的整係數方程的根都叫「代數數」。不是「代數數」的數，稱為「超越數」。

可見得「代數數」是伴隨著解方程而自然存在的，它可能是有理數，也可能是無理數。但是，「超越數」的定義出現後經過一整個世紀，人們還是無法證明它的存在，也找不到這樣的數。⁴⁵

要認識超越數，的確是件高難度的事。在過去的經驗裡，負數、無理數，甚至是虛數，都是在解方程時就出現它們的蹤跡，困擾了數學家一段時間才逐漸認識它們；但超越數卻隱藏起來，在未現身之前是數學家先猜想有這樣的數，給了定義，然後千方百計想辦法去證明它的存在，並設法找尋它，或用人工的方法形塑它。

在數學家們不斷的努力下，終於有了超越數的一些輪廓，而這些成果大多是在伽羅瓦逝世後才發現的，整理如下：⁴⁶

1. 西元 1844 年，法國數學家劉維(Joseph Liouville 1809-1882 年)證明了超越數的存在。
2. 超越數有無限多個，都屬於無理數。
3. e 、 π 、 $2^{\sqrt{2}}$ 等是超越數。

(四) 虛數

虛數也是在解方程時被發現的，但它不像負數可賦予生活經驗的想像，也不像無理數可用小數或連分數逼近。認識它不是件容易的事，茲簡單整理如下：⁴⁷

1. 認為它本質上是虛構的，幻想的，不切實際的，缺乏實體存在的。
2. 西元 1637 年笛卡爾(René Descartes 1596-1650 年，法國數學家、物理學家、哲學家)將負數的平方根命名為「虛數」。西元 1777 年，瑞士數學家歐拉將 -1 的平方根用 i 表示，並將實數與虛數之和稱為複數。虛數的存在與用途，迫使數學家不得不正視它，遂將實數與虛數統整成更大的數集，賦予運算，成為「複數系」。
3. 西元 1799 年，德國著名的數學家高斯(Gauss 1777-1855 年，德國數學家)證明了「代數基本定理」，鞏固了複數的地位。在西元 1831 年，高斯又為複數建立幾何表示法，複數擺脫了虛構的身分，與實

⁴⁵ 參考袁小明編著：《數學史》，頁 172-173。

⁴⁶ 參考袁小明編著：《數學史》，頁 173-177。

⁴⁷ 參考袁小明編著：《數學史》，頁 178-184；Mario Livio 著，蔡承志譯：《無解方程式》，頁 103。

數分庭抗禮地呈現在人們眼前；從此開拓了解析幾何的發展，也成就了複數域與平面解析幾何間等價的傳奇。

五、驚蟄

歐洲歷經近千年的中世紀時期，人們也在重整古代先人所遺留下的智慧痕跡，甦醒後必有一番新的局面！

以解二次方程而言，巴比倫人雖然遠在三、四千年前就能求其解，古希臘文明也懂得用幾何方式去處理，但他們都尚未發展出用公式去求取二次方程的根。在呂溪木所著的《體與 GALOIS 理論》一書中，記載了：

所謂代數公式解就是由方程式的係數經過加、減、乘、除、開根等有理運算所得的方程式的根，常稱為根式解。(頁 4)

西元 16 世紀，當歐洲告別了中世紀，進入文藝復興時期，許多方面都因解放而蓬勃發展，科學的研究也愈加突破且講求精確。在數學的鑽研上，代數引起了更廣泛的注意，且與算術分流而自成一家，主要表現在以下各方面⁴⁸：

(一) 改進符號

1. 普遍使用符號代替未知數(變數)，甚至代表已知數(一般的係數)。
2. 建立乘冪符號、運算符號、關係符號。

(二) 運算法則

1. 以等量公理的定律看待等式，發展出運算規則。
2. 解方程式成為一門技法。

(三) 探求三次、四次方程式的解

1. 數學家們更致力於尋找三次方程式，甚至四次方程式的解。大多數只能從兩項式著手，例如： $x^3 + ax^2 = 0$ ， $x^3 + ax = 0$ ， $x^3 + a = 0$ ， $x^4 + ax^3 = 0$ ， $x^4 + ax^2 = 0$ ， $x^4 + ax = 0$ ， $x^4 + a = 0$ ；也有數學家挑戰三項式，例如： $x^3 + px^2 + qx = 0$ ， $x^3 + px^2 + q = 0$ ， $x^3 + px + q = 0$ 等式。
2. 以求三次方程式或四次方程式的解，互相競賽。

由此可見，這時候已經開始對方程式的一般表達進行整體處理，使代數學的研究朝向一般的方程式。

⁴⁸參考袁小明編著：《數學史》，頁 151-152。

六、解三次、四次方程式

為了解出三次方程式的根，歐洲的數學家曾透過幾何方式，用「求曲線交點」的作法；在印度的數學家則想出「配成完全立方」再求解；在中國的數學家卻自創「增乘開方法」以找解。不同地域發展出不同的模式，但都有其不盡完美之處，或侷限於某種特例的缺點，因此未能被全面地應用。⁴⁹

在西元 16 世紀的歐洲，常見皇室或統治者願意贊助數學家進行學術研究，數學家也以爭取有名望者的贊助作為提昇專業地位的方法。⁵⁰在許多數學競賽中，解三次方程式是當時經常出現的題目，許多人就刻意將解法隱藏保密，以作為與人挑戰的獨家本領。這種良性的競爭，促使代數學的快速發展，而數學家們莫不急於找出適用於任意三次方程式的求解公式。

在西元 1500 年左右，義大利的數學教授費洛(Scipione del Ferro 1465-1526 年)解出了型如 $x^3 + px = q$ 的三次方程式，並保密了許多年，才傳授給他的學生費歐雷(Antonio Maria Fior, 16 世紀前半)。後來，有一位在義大利威尼斯的數學教師塔塔利亞(Niccolò Tartaglia 1500-1557 年)，自稱發現了型如 $x^3 + px^2 = q$ 的三次方程式的解法，費洛的學生費歐雷遂在 1535 年向塔塔利亞挑戰解三次方程式，約定要在三十天內解出對方所出的三十道題目。結果塔塔利亞苦思到最後一天的清晨，突然豁然開朗，不到兩小時就解出所有題目，獲得勝利，並在欣喜之餘，大方地決定放棄所有該得的賭金。可見得他已掌握了沒有 x^2 項的三次方程式以及沒有 x 項的三次方程式的解法了。雖然這時候都只求出一個根，但三次方程式最困難的部分被破解之後，根的公式就呼之欲出了。⁵¹

當時，在義大利米蘭擔任官方數學教師的卡丹諾(Girolamo Cardano 1501-1576 年)獲悉這項消息之後，以升遷為餌，利誘塔塔利亞將三次方程式的解法透露出來，卡丹諾並承諾絕不洩密。塔塔利亞雖心有提防，仍用詩歌暗語透露了解法；事後卻又後悔不該衝動被說服，並決定放棄卡丹諾的安排，回到威尼斯繼續作個窮教師。⁵²

西元 1543 年，卡丹諾在一次偶然的機會巧遇費洛的女婿，他將他丈人遺留下來的文稿給卡丹諾看，卡丹諾意外發現費洛較塔塔利亞更早發現如何解三次方程式。於是，卡丹諾決定違背自己曾說過的誓言，不再保密。卡丹諾於 1545 年出版了《大術》(*Ars Magna, The Great Art*)一書，將塔塔利亞所

⁴⁹ 參考袁小明編著：《數學史》，頁 198-202, 226-230。

⁵⁰ 參考英家銘、蘇意雯：〈數學與「禮物交換」〉，《當數學遇見文化》，頁 110-121。

⁵¹ 參考比爾·柏林霍夫(William P. Berlinghoff)與佛南度·辜維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》(台北市：博雅書屋，2008 年)，頁 45；羅伯·所羅門(Robert Solomon)著，洪慧芳譯：《一本通數學原理》，頁 62-63；袁小明編著：《數學史》，頁 151, 203；王懷權編著：《數學發展史》，(新竹市：協進圖書有限公司，民 70 年)，頁 310。

⁵² 參考袁小明編著：《數學史》，頁 203；比爾·柏林霍夫(William P. Berlinghoff)與佛南度·辜維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 45-46；王懷權編著：《數學發展史》，頁 311。

發現的方法加以推廣，及於四項俱全的三次式 $x^3 + px^2 + qx + r = 0$ ，整理出解任意三次方程式的完整解法與幾何證明，並列出卡丹諾自己所處理的例子為佐證。雖然書中有特別提到塔塔利亞、費洛兩人的研究貢獻，但如此毀約背信的作為令塔塔利亞十分憤怒，他採取各種公開的抗議，奮力地要聲討卡丹諾，但《大術》所造成的轟動，壓得塔塔利亞未能改變什麼。⁵³

卡丹諾在《大術》這本學術論文中，還收錄了他的學生費拉里(Lodovico Ferrari 1522-1565 年)解四次方程式的方法。費拉里是在 1540 年時，以未滿二十歲的年紀，就將解三次方程式的技巧套用到四次方程式，得出任意四次方程式的一般解法。⁵⁴

至今，人們稱解三次方程式的公式為「卡丹諾公式」，在紀念卡丹諾為繁雜難解的三次和四次方程式找到代數公式解之外，也不要忘了塔塔利亞與費洛這兩位幕後英雄。⁵⁵

卡丹諾的《大術》雖然仍有虛數問題尚未處理，但發表之後確立了西方代數超越東方代數的新里程碑。⁵⁶

七、尋找五次方程式的根

代數學的發展，在 16 世紀歷經了符號的改進、算則的建立、三次與四次方程的求解；進入 17 世紀時，笛卡兒(René Descartes 1596-1650 年，法國哲學家兼數學家、物理學家)創立了用拉丁文的前幾個字母 a、b、c 等作為已知數，後幾個字母 x、y、z 等作為未知數，世人一直沿用至今；而在 18 世紀時，瑞士數學家歐拉也對三次方程的解法進行了較為完整的討論與整理。⁵⁷但這種種的建樹，都無法解決數學家心中另一個更深的疑惑。

這個疑惑源自西元 1545 年卡丹諾發表了《大術》之後，數學家們開始熱衷尋找五次方程式的根。起初，很自然地循著解三次、四次方程式的模式，從一般的五次方程式 $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ 去找公式解，試圖以它的係數經過加、減、乘、除四則運算和開方的方式表示其解，即所謂的「求根式解」。但如此經歷了兩百五十年之久，數學家們仍然處處碰壁，陷在一團迷霧當中。⁵⁸

⁵³ 參考袁小明編著：《數學史》，頁 203-204；Mario Livio 著，蔡承志譯：《無解方程式》，頁 94；比爾·柏林霍夫(William P. Berlinghoff)與佛南度·辜維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 45-46；王懷權編著：《數學發展史》，頁 311。

⁵⁴ 參考袁小明編著：《數學史》，頁 151,204-205；Mario Livio 著，蔡承志譯：《無解方程式》，頁 94；比爾·柏林霍夫(William P. Berlinghoff)與佛南度·辜維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 46；呂溪木著：《體與 GALOIS 理論》，頁 4；王懷權編著：《數學發展史》，頁 311。

⁵⁵ 參考比爾·柏林霍夫(William P. Berlinghoff)與佛南度·辜維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 46；王懷權編著：《數學發展史》，頁 310。

⁵⁶ 參考袁小明編著：《數學史》，頁 204；王懷權編著：《數學發展史》，頁 311。

⁵⁷ 參考丘維聲著：《數學的思維方式與創新》，(北京：北京大學出版社，2011 年)，頁 144。

⁵⁸ 參考袁小明編著：《數學史》，頁 206；聶靈沼、丁石孫著：《代數學引論》，頁 300；Mario Livio

在沿用解三次、四次方程式的舊技巧來解五次方程式時，數學家們常喜歡走熟悉的路，不是想辦法將五次方程式的次數降低成四次、三次，就是消去 x^4 項和 x^3 項，甚至鎖定某幾種五次方程式來求公式解，但這種嘗試仍遇到許多障礙，無法成功。⁵⁹

經歷了漫長時間的努力，數學家們心中也納悶：求五次方程式的解會不會遇到比無理數、虛數等更棘手的數字出現？漸漸地，有些數學家開始轉向，開始去瞭解為何無法求得五次方程式的解？第一個要解決的問題是：「五次方程式確定有解嗎？」第二個要解決的問題是：「一般的五次方程式可以求根式解嗎？」⁶⁰

(一) 方程式解的確存在

數學家們對於「是否任意次的方程式都至少含有一解？」仍是意見分歧，直到德國數學大師高斯在西元 1799 年提出的博士論文，證明：「每一個一元 n 次實係數方程式都恰有 n 個複數根。」這就是後來所稱的「代數基本定理」(The fundamental theorem of Algebra)。⁶¹

有了代數基本定理，就可以確定五次方程式在複數系中恰有五個根的結論。其實代數基本定理更加使得方程論嚴密化，是促進代數發展的重要標竿。⁶²

(二) 一般的五次方程式不能用根式求解

數學家們對於求五次方程式的根一籌莫展的同時，多半持有一個共同的猜想，即「一般的五次方程式不能用根式求解」，但沒有人能證明它。⁶³直到跨越到 19 世紀初時，終於出現了兩位數學家在這方面有了一些貢獻：

1. 保羅·魯菲尼(Paolo Ruffini 1765-1822 年，義大利醫生兼數學家)

保羅·魯菲尼是義大利醫生兼數學家，他在西元 1799 年發表了《方程式通論》(*Teoria generale delle equazioni*)，推論一般的五次方程式不存在統一的根式解。但這篇論文因為篇幅冗長，多達五百多頁，不僅內容迂迴難懂，且有許多缺陋，並未引起學界注意。到了西元 1813 年，他又發表了一篇論文〈回顧代數方程通式的解法〉

著，蔡承志譯：《無解方程式》，頁 102。

⁵⁹ 參考袁小明編著：《數學史》，頁 206；Mario Livio 著，蔡承志譯：《無解方程式》，頁 105-106,108。

⁶⁰ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 103,108-109；比爾·柏林霍夫(William P. Berlinghoff)與佛南度·韋維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 59；羅伯·所羅門(Robert Solomon)著，洪慧芳譯：《一本通數學原理》，頁 119。

⁶¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 108-109；呂溪木著：《體與 GALOIS 理論》，頁 121；王懷權編著：《數學發展史》，頁 312。

⁶² 參考袁小明編著：《數學史》，頁 154。

⁶³ 參考呂溪木著：《體與 GALOIS 理論》，頁 7。

(“Reflections of the Solution of General Algebraic Equations”)，這一次證明較為淺顯，但仍未受到重視。⁶⁴

2. 尼爾斯·阿貝爾(Niels Henrik Abel 1802-1829 年，挪威數學家)

挪威的數學家尼爾斯·阿貝爾，在高中時就曾致力於破解出五次方程式，本以為已順利解出來了，但後來發現解法有錯誤。於是他開始猜想五次方程式未必能以根式求解，遂決定證明它。阿貝爾以嚴謹的論據，運用合乎邏輯的「歸謬法」進行這項證明。⁶⁵

阿貝爾在西元 1824 年就曾以法文撰寫了論文《論代數方程式且證明五次方程通式不可能求根式解》(*Mémoire sur les équations algébriques où démontre l'impossibilité de la resolution de l'équation générale du cinquième degré*)，並為了節省費用，將它濃縮成六頁的小冊子，寄給德國的數學家高斯，但卻石沈大海。經過三十年後在高斯的遺物中竟然發現這本小冊子，原來高斯一直未曾開封研讀。⁶⁶

阿貝爾在西元 1826 年在德國認識了一位工程師，這位工程師十分崇拜阿貝爾，並創辦了 19 世紀德國第一本數學期刊《純數學與應用數學雜誌》(*Journal für die reine und angewandte Mathematik*)，第一期就刊出阿貝爾的六篇論文，其中一篇就是證明一般五次方程式不能用根式求解，此篇的解釋較兩年前的論文更為詳盡清楚。⁶⁷

節錄袁小明編著的《數學史》中對阿貝爾所證的結論，簡述如下：

如果方程 $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$ 的次數 $n \geq 5$ ，那麼這個方程的根不可能用方程的係數 a_1, a_2, \dots, a_n 所組成的根式來表示。(頁 208)

事實上，雖然一般的五次方程式無法求出根式解，但有些特殊的五次方程式卻可以用根式解出；而且後來發現利用一些超越函數可構造出五次方程式的公式解，但當時對於這些情況都仍在探索階段。同樣在袁小明所編著的《數學史》中提到：

⁶⁴ 參考袁小明編著：《數學史》，頁 208；聶靈沼、丁石孫著：《代數學引論》，頁 300；Mario Livio 著，蔡承志譯：《無解方程式》，頁 110-113。

⁶⁵ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 121-122, 124-125；王懷權編著：《數學發展史》，頁 312。

⁶⁶ 參考袁小明編著：《數學史》，頁 153, 208；聶靈沼、丁石孫著：《代數學引論》，頁 300；Mario Livio 著，蔡承志譯：《無解方程式》，頁 126；比爾·柏林霍夫(William P. Berlinghoff)與佛南度·辜維亞(Fernando Q. Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 59；呂溪木著：《體與 GALOIS 理論》，頁 7；羅伯·所羅門(Robert Solomon)著，洪慧芳譯：《一本通數學原理》，頁 119。

⁶⁷ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 128；王懷權編著：《數學發展史》，頁 312。

雖然阿貝爾證明了高於四次的一般方程是不能用根式解出的，但這並不等於一切高於四次的方程都不能用根式解，比如二項方程 $x^n=A$ ，...，還有不少特殊的高次方程都是可以用根式解的。(頁 208)

這個原本是數學家的猜想，經過證明而有了結論，成為代數學上繼「代數基本定理」之後又豎立的一個重要的標竿。從此，方程式的研究方向作了調整，不再聚焦於解方程式，更多廣泛、多元的相關研究，亟待新的發現能為代數學開闢新境！

八、另闢蹊徑

數學家們雖然花了兩百五十年的時間在摸索五次方程式的解，在不斷地失敗當中也開始思考：如果二次方程式的根有其公式，三次方程式的根也有另一個公式，四次方程式的根又是不同於二次、三次的公式，...，如此繼續下去，相異次數的方程式都擁有一個專屬自己的根的公式；那豈不是會有無限多個公式嗎？所有這些公式必定是服膺於某些個規律吧！而要找尋這些規律，必須從二次、三次和四次方程式根的公式去觀察，以推測更高次方程式的根該有的線索，包括方程式的根與係數之間的關係等都應列入考慮。而投注心力去探討這些規律，或許是值得的，說不定有可能從中獲得五次方程式的解。⁶⁸

以二次方程式 $ax^2+bx+c=0$ ($a \neq 0$) 而言，假設 x_1 、 x_2 為其兩根，則有 $x_1+x_2=-\frac{b}{a}$ ， $x_1x_2=\frac{c}{a}$ 。而其兩根的公式是 $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$ ，也可以表示成 $\frac{1}{2} [(x_1+x_2) \pm \sqrt{(x_1+x_2)^2-4x_1x_2}]$ 。當時有些數學家發現方程式是否能以公式求解，牽動著推定解的置換排列性質。這種新穎的研究概念與範疇，令一些數學家相當振奮。⁶⁹

在西元 1770 年，數學家約瑟夫—路易·拉格朗日(Joseph-Louis Lagrange 1736-1718 年，生於義大利，父系為法國)發表了一篇研究論文《論代數方程式解法的沿革》(*Reflections on the Resolution of Algebraic Equations*)，除了解釋以二次、三次和四次方程式求解途徑不適用於五次方程式外，又引進置換排列的討論⁷⁰。節錄自 Mario Livio 著，蔡承志譯的《無解方程式》一書中的記載如下：

⁶⁸ 參考袁小明編著：《數學史》，頁 206-207。

⁶⁹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 106-107。

⁷⁰ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 107-108。

拉格朗日成就了一項重要的發現，方程式的特性及是否能夠求解，都視該方程式在置換排列情況下的一些對稱性而言。(頁 108)

拉格朗日曾試圖以符合原五次方程式的預解函數找解，希望這些低於五次的函數能提供出路，但仍沒有獲得成功。雖然拉格朗日沒能解五次方程式，也未證明出五次方程式沒有根式解，但他注意到：分析各種方程式之根的重排結果，可以進一步理解方程式的所有根。這個嶄新的思想，蘊含着置換群的概念，對後來的阿貝爾和伽羅瓦都有許多啟發，並提供了日後徹底解決方程式解的基礎。拉格朗日可稱為群論研究的開路先鋒。⁷¹

⁷¹參考袁小明編著：《數學史》，頁 153,208；Mario Livio 著，蔡承志譯：《無解方程式》，頁 108；比爾·柏林霍夫(William P.Berlinghoff)與佛南度·辜維亞(Fernando Q.Gouvêa)著，洪萬生、英家銘團隊譯：《溫柔數學史》，頁 59。

第二節 Galois 的生平

一、出生

在西元 1811 年 10 月 25 日深夜，距離法國巴黎 18 公里的布爾拉林(Bourg-la-Reine)小城⁷²，誕生了一位數學界的傳奇人物—埃瓦里斯特·伽羅瓦(Évariste Galois)。⁷³

二、家庭

當埃瓦里斯特·伽羅瓦出生時，法國正是拿破崙執政時期。他的父親尼古拉-加布瑞爾·伽羅瓦(Nicolas-Gabriel Galois)擔任布爾拉林城內一所男校的校長，這所學校創於法國大革命(1789-1799 年)之前，從創校以來都由伽羅瓦家族的人擔任校長。⁷⁴

埃瓦里斯特·伽羅瓦的母親愛得萊德-瑪利亞·德芒特(Adélaïde-Marie Demante)是一位巴黎法學專家的女兒，深諳經典古書，可謂出自書香世家。一生活力充沛，享年八十四歲。⁷⁵

尼古拉-加布瑞爾·伽羅瓦與愛得萊德-瑪利亞·德芒特結婚後，育有二子一女。埃瓦里斯特·伽羅瓦是長子，上有姊姊，下有弟弟。⁷⁶

當埃瓦里斯特·伽羅瓦未滿四歲時，法國正好在拿破崙「百日王朝」(1815.3.14-1815.6.22)期間，他的父親開始擔任布爾拉林小城的市長。歷經拿破崙滑鐵盧戰役失敗，結束「百日王朝」，波旁王朝復辟(1815.7-1830.7)，他都盡心盡力忠於職守。直到 1829 年 7 月，因政治因素被誹謗，終以自殺結束生命。長達十五年的市政經營，頗受市民愛戴。⁷⁷

埃瓦里斯特·伽羅瓦的父親，將十五年的青春都奉獻給布爾拉林城，竭盡心力為市民付出，在當時的確換來市民的感念與尊敬；但埃瓦里斯特·伽羅瓦對數學的熱忱付出，卻在他生前一再地被漠視，直到逝世多年才獲得遲來的肯定，影響學術界甚鉅，如平地一聲雷！⁷⁸

⁷² 參考達爾馬斯 (Andre Dalmás) 原著：《伽羅瓦傳》(新竹市：凡異文化事業有限公司，民 75 年)，頁 1。

⁷³ 參考 Mario Livio 著，蔡承志譯：《無解方程式：數學天才與對稱性之謎的鬥智之旅》(台北市：臉譜，城邦文化出版：家庭傳媒城邦分公司發行，2008 年)，頁 144。

⁷⁴ 參考達爾馬斯原著：《伽羅瓦傳》，頁 2； Mario Livio 著，蔡承志譯：《無解方程式》，頁 144。

⁷⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 2-3； Mario Livio 著，蔡承志譯：《無解方程式》，頁 351。

⁷⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 2-3； Mario Livio 著，蔡承志譯：《無解方程式》，頁 349。

⁷⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 2、8； Mario Livio 著，蔡承志譯：《無解方程式》，頁 146、153。

⁷⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 1。

三、啟蒙

數學家埃瓦里斯特·伽羅瓦在十二歲之前都未入學。童年時雖在家中成長，但家庭教育相當注重智慧的啟發與人格的培養，尤其灌輸他自由的思想。

他的父親是個充滿文采的人。雖然公務繁忙，但在餘暇時不忘創作詩詞或編寫劇本，作品中常引出巧思妙語，讓人會心一笑，甚而拍案叫絕！又因為個性風趣，加上知識淵博且涵養深厚，總是受到許多人的歡迎。兒子埃瓦里斯特·伽羅瓦在耳濡目染之下，也能遣詞造句、舞文弄墨，玩味詩詞的韻味與律動。⁷⁹

他的母親則親自教導他古典文學及宗教教義，讓他從小就接觸拉丁文和希臘文化中的經典文學，小伽羅瓦的學前教育也因此奠下極佳的基礎。母親的思想獨立且大器，凡事在計畫下總能堅定完成。埃瓦里斯特·伽羅瓦的性格與母親有許多相似之處，嚴肅的外表下包覆著深情的內心，自小就是個做事十分認真且才智兼備的孩子。⁸⁰

父母親都崇尚自由主義，憎惡昔日的君主專政，使埃瓦里斯特·伽羅瓦小小的心靈也灌溉了自由的思想。

埃瓦里斯特·伽羅瓦的母親原本作了周詳的計畫，準備在他滿十歲之後，送他到法國東北部的漢斯(Reims)入學。但他看起來如此弱小，母親的心實在捨不得讓他隻身離家，遂取消了計畫。這樣的決定，讓她多教導了兒子兩年，也延續了埃瓦里斯特·伽羅瓦與家人相處的時光。雖然他的母親積極地對兒子的教育投注心血，在他童稚時開啟了他的智慧，但埃瓦里斯特·伽羅瓦在長大外出求學之後，與他的母親漸疏離，卻對於父親念念不忘。⁸¹

四、進入中學

當伽羅瓦十二歲時，離開了家鄉及父母，前往巴黎就學。在 1823 年 10 月進入路易大帝皇家中學(lycée Louis-le-Grand)，這所學校於 16 世紀創校，曾經培育出許多傑出的校友。伽羅瓦從此開始住在校舍，學習在團體中獨立的生活。⁸²

學校在學業方面的教導備受各方的肯定，但過於嚴苛的管理手段，或盤查、或控制、或約束等不開明作法，使學校像個大悶鍋，好似一座監獄一般。而來自四面八方的學生齊聚校園，匯集了眾多的政治思想，混雜著各種流派的思潮，使得校園內很不平靜，聚眾鬧事或謠言滿天飛已是司空見慣的事，

⁷⁹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 144。

⁸⁰ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 146。達爾馬斯原著：《伽羅瓦傳》，頁 3。

⁸¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 146。達爾馬斯原著：《伽羅瓦傳》，頁 3。

⁸² 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 146。達爾馬斯原著：《伽羅瓦傳》，頁 3。

校方的嚴厲監控只會帶來反效果，無法壓制層出不窮的違紀行為。⁸³

學校每日的作息時間，從清晨五點半到晚上八點半，全部排滿各種學習活動，卻吝於讓學生有喘息的時間；若有違規者，還須接受監禁的特別處分。

84

十二歲以前的伽羅瓦，在一個氣氛和樂的家庭長大，突然來到這樣一個嚴峻冷酷又粗暴管理的環境，受到相當大的震撼！

伽羅瓦入學時，適逢校長也是剛奉派到任不久，因為作風保守，引起學生們的疑慮，擔心耶穌會建校時的作風將回流，而開始醞釀罷課，以表達不滿。1824年1月28日是個引爆點，正當學校進行禮拜時，許多學生採取不合作的態度，於集會唱讚美詩歌時故意保持緘默，在用餐時亦拒絕遵循君主時代形式化的儀式。校方堅持以鐵腕作風，在未通知家長的情況下，直接就開除了數十名學生。⁸⁵

雖然伽羅瓦沒有受到牽連，但一切看在眼裡，更體認到「專制」的可怕。他自幼就培養出堅定的信念，正義感驅使他行事要光明磊落；然而目睹同學們僅是勇敢地表達心聲，卻在恐怖及嚴酷的紀律下慘遭無情的對待，心情大受影響。原本年輕單純的心，蒙上了揮之不去的陰霾，性格上也有了一些變化。

伽羅瓦進入中學的前兩年(法國中學的學制，以伽羅瓦入學年齡應就讀第四級，再依序進入第三級、第二級、第一級、最終級。因此這兩年是第四級與第三級。)⁸⁶，因著母親為他奠下的古典文學根基，輕鬆地獲得優異成績，包括拉丁語、希臘文翻譯、數學理解能力等，均有很好的表現，也都能領取獎學金。但就讀第二級時，伽羅瓦的學業成績開始呈現不穩定，主要原因是耳疾的痛苦困擾了他好幾個月，親人又不能在身邊照顧他，使他心情相當沮喪，無法專心學習。⁸⁷

五、重修一年迷上數學

雖然伽羅瓦曾以希臘語作文，參加國家獎學金的作文比賽，獲得佳績。但1826年10月新學期開始，修辭學進階課程的難度較以往加深不少，伽羅瓦對古典文學的興趣由濃轉淡，逐漸失去以往的熱忱。但他的志氣未消，上課仍安份守己，大致上還得到老師的肯定。⁸⁸

只是當時新來的校長觀念和作法都相當保守，評估伽羅瓦的學習狀況，認為他仍不夠成熟，且判斷能力不足，無法消化這樣的高級課程。因此，在

⁸³ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 147。

⁸⁴ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 147。

⁸⁵ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 147。

⁸⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 4、109。

⁸⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 4；Mario Livio 著，蔡承志譯：《無解方程式》，頁 147-148。

⁸⁸ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 148。

1827 年 1 月，強迫伽羅瓦降級，重修第三年(第二級)的課程。這是伽羅瓦在求學過程中第一次遭受打擊，他父親接獲通知也感到不可思議。⁸⁹

上帝關了一扇門，必定又為他開了另一扇窗。重修一年，伽羅瓦決定選讀初級數學的補充課程。該校規定人文學科是必修課程，為主要科目；而對於喜愛科學的同學，可於第二級時選修初級數學的補充課程。在跌倒的這一年，他開始接觸正規學校的數學課程，在這裡，他發現自己強烈的研究興趣，如噴泉般疾速地躍出...。⁹⁰

幾何學方面，教師採用勒讓德爾(Legendre 1752-1833 年，法國數學家)的《幾何原理》(*Elements de Geometrie*)為教科書。撰寫的數學家勒讓德爾，以活潑生動的創造力貫串全書，當中所蘊含的數學思維使伽羅瓦為它著迷，愛不釋手；並且在研讀它的同時，宛如在欣賞一部藝術作品般，讚嘆不已！他用很短的時間就讀完這一本書，並清晰地掌握了基礎幾何的結構與輪廓。⁹¹

而在代數學方面，學校所選定的教科書讓伽羅瓦覺得味如嚼蠟，他把課本冷落在角落，不屑一顧；而對於教師還選擇照本宣科地授課，總是按部就班地教著繁瑣的解題技巧，他也不以為然。伽羅瓦並不是讀不懂這些內容，只是課堂上教的這些旁枝末節，顯得無趣而且缺乏挑戰性，他需要的是吸收大師級數學家們的見解，因此他直接去讀拉格朗日(Lagrange 1736-1813 年，法國數學家)在代數學的著作。雖然年僅十五歲，卻饑渴般地尋求知識。對於專業數學家所看的代數分析傑作，已能深入瞭解，包括方程的數值解、解析函數理論，以及函數演算等研究論文。⁹²

六、挫折下的沈潛

1827 年伽羅瓦再度面對修辭學進階課程的學習，這時候他在各方面已經更成熟了，全方位的發展使他位於優等生的行列。但因為他閱讀了許多數學學者的著作，培養了宏觀的視野，事事都以科學的精神掌握住重點，以至於缺乏耐性去應付老師們瑣碎的細節要求，乖僻的個性使他變得更暴躁易怒。縱使他對數學情有獨鍾，仍不忘兼顧其他科目，在國家考試當中依然得到獎學金，這也激勵了他挑戰升學考試的決心。⁹³

他用沉靜的方式，盡情地徜徉於自己的數學天地；他清楚知道自己可與代數分析方面的大師們對話，一心渴望衝向更高的學術殿堂與他們較量！此時，伽羅瓦對於歐拉(Euler 1707-1783 年，瑞士數學家)、高斯(Gauss 1777-1855

⁸⁹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 148。

⁹⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 4-5；Mario Livio 著，蔡承志譯：《無解方程式》，頁 148。

⁹¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 148；達爾馬斯原著：《伽羅瓦傳》，頁 5。

⁹² 參考康明昌：《幾個有名的數學問題》，(新竹市：凡異出版社，民 83 年)，頁 114；Mario Livio 著，蔡承志譯：《無解方程式》，頁 149；達爾馬斯原著：《伽羅瓦傳》，頁 5。

⁹³ 參考達爾馬斯原著：《伽羅瓦傳》，頁 6。

年，德國數學家)和雅科比(Jacobi 1804-1851 年，德國數學家)等人的著作，已經有相當的認識了。⁹⁴

綜合理工學院(École polytechnique)在法國是許多數學家聚集之所，創於 1794 年法國大革命期間。伽羅瓦躍躍欲試，鎖定該校為升學的目標。可是，初級數學課的老師弗尼爾(Venier)有他的看法，認為伽羅瓦最大的問題是思想過於跳躍，缺乏循序漸進的功夫。如此一來，即使他天賦異稟又有獨特的創意，但敘事與表達未必能條理分明，在某些層面的根基還須加強，否則在考試時將相對地吃虧。弗尼爾老師勸伽羅瓦擬定計畫並慎重地準備，但伽羅瓦不理會，就提前一年參加綜合理工學院入學考。⁹⁵

伽羅瓦落榜了！原本滿懷期望，年少的他夢想破滅，心情盪到谷底，難免覺得這個世界對他不公平，也可能造成日後偏執的想法。

七、獨創性的研究

1828 年 10 月，伽羅瓦脫離初級數學課程，進入高級數學班上課。教這門課的老師是路易-保羅-埃米爾·理查(Louis-Paul-Émile Richard 1795-1849 年)，年僅三十三歲的理查老師，常利用課餘時間進修，吸收了許多當代數學的新知識，並竭盡所能、不藏私地傳授給他的學生們。他擅長啟發學生思想，講課風格很有個人特色，在他的學生當中，有些人後來成了有名的法國數學家，可謂桃李滿天下。在今日的文獻記載中，就出現多位數學名人對他表示感謝與尊敬，包括勒威耶(Leverrier)、塞瑞特(Serret)、埃爾米特(Hermite 1822-1901 年，法國數學家)，還有伽羅瓦。⁹⁶

尋找五次方程式的解已困擾數學界很長一段時間，伽羅瓦就曾耗掉兩個月的時間鑽研其中，本以為自己已導出公式解，後來才發現解法中有誤，竟是與阿貝爾(Abel 1802-1829 年，挪威數學家)犯相同的迷思。於是，想法靈動的伽羅瓦決定跳脫原來的思考路線，重新開闢新的領域，探討代數方程式是否有解的課題。年紀輕輕，才只有十七歲，就以獨創的理論，在方程式論的研究上，有了劃時代意義的發現。⁹⁷

理查老師果然是識千里馬的伯樂，他十分激賞伽羅瓦在數學方面的天賦，曾寫道：「這名學生遠遠地凌駕於其他同學之上。」「這名學生只適合研究尖端領域的高等數學。」他甚至認為：若是巴黎綜合理工學院有免試入學的機會，伽羅瓦絕對夠資格申請！⁹⁸

法國在 1818 年有了第一個專業的數學雜誌，是由法國數學家熱爾貢

⁹⁴ 參考達爾馬斯原著：《伽羅瓦傳》，頁 6。

⁹⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 6；Mario Livio 著，蔡承志譯：《無解方程式》，頁 150。

⁹⁶ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 150；達爾馬斯原著：《伽羅瓦傳》，頁 6-7；康明昌：《幾個有名的數學問題》，頁 115；王懷權編著：《數學發展史》頁 343。

⁹⁷ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 149-150。

⁹⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 7；Mario Livio 著，蔡承志譯：《無解方程式》，頁 150。

(Gergonne 1771-1859 年)所創辦的《純粹和應用數學年報》(*Annales de mathématiques pures et appliquées*)。1829 年 3 月 1 日，伽羅瓦在該雜誌的三月號期刊中，發表了他的第一篇數學論文〈對循環連分數定理的證明〉，這篇文章雖然不是十分重要，也完全看不出在他腦中所建構創新理論的蛛絲馬跡，但初試啼聲就讓他的同學們佩服不已，將他視為一顆閃亮星星。⁹⁹

理查老師真是位惜才的好老師，他鼓勵伽羅瓦把他所研究的發現，整理成有系統的理論，撰寫成論文，交給當時法國最具權威的數學大師奧古斯丁·路易·柯西(Augustin Louis Cauchy 1789-1857 年)審查，並希望能被他提到法國科學院發表。一向對理查老師相當信服的伽羅瓦，照著老師的建議，分別在 1829 年 5 月 25 日與 6 月 1 日各交了一篇專論給柯西，內容都是關於方程式論的研究。此時，伽羅瓦尚未滿十八歲，就完成了他那曠世鉅作的論文，在數學發展史上，從未出現如此年輕的數學家！¹⁰⁰

八、屋漏偏逢連夜雨

伽羅瓦將重要的手稿交給柯西之後，心中充滿期待，靜候科學院的回音，怎奈 1829 年 7 月 2 日，晴天霹靂的消息攪擾了一切。原本伽羅瓦正躍躍欲試，準備再次參加巴黎綜合理工學院的入學考，此時卻遭逢人生中極其悲痛的事—父親自殺身亡。事發地點離伽羅瓦就讀的中學很近，他父親選擇在巴黎的公寓住宅裡結束一生。¹⁰¹

起因是老伽羅瓦擔任布爾拉林市長將近十五年，在政治傾向上一直是屬於自由黨人，他對於君主專政相當反感。但 1824 年查理十世登基之後，教會和保皇勢力再度抬頭，布爾拉林小城隨後來了一位好耍心機的年輕牧師，對老伽羅瓦市長相當不友善，暗中掣肘。年輕牧師利用市長擅長作詩的聲望，故意在市區散發數篇不入流且卑劣、諷刺性的短詩，並加上造假的市長簽名，設計污衊市長的名譽，誹謗市長的人格。老伽羅瓦一向為人正派，行事作風高雅，被這些齷齪的行徑陷害，抑鬱終日，覺得自己跳到塞納河也洗不清，終於受不了這樣的屈辱，遂來到巴黎自家住處，吸入瓦斯以死明志。¹⁰²

在安葬當天，老伽羅瓦的遺體送回布爾拉林市區，那位年輕的牧師還惺惺作態來參加葬禮彌撒，憤怒的市民群起騷動，與牧師起了嚴重的衝突，牧師果然被痛打一番。可以想像：伽羅瓦聽聞父親被惡意中傷，以至於憂鬱尋短，風雲驟變的景況早已使他備感無助；接著又目睹父親在紛亂的情況下，以不合禮儀的喪禮下葬，真是雪上加霜。伽羅瓦年輕的心，不免對世事更加

⁹⁹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 7；Mario Livio 著，蔡承志譯：《無解方程式》，頁 151。

¹⁰⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 7；Mario Livio 著，蔡承志譯：《無解方程式》，頁 151-152。

¹⁰¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 153；達爾馬斯原著：《伽羅瓦傳》，頁 2,8；康明昌：《幾個有名的數學問題》，頁 115；王懷權編著：《數學發展史》，頁 343。

¹⁰² 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 153；達爾馬斯原著：《伽羅瓦傳》，頁 8；康明昌：《幾個有名的數學問題》，頁 115；王懷權編著：《數學發展史》，頁 343。

懷疑、不安，導致性格愈加憤世嫉俗。¹⁰³

一個月之後，伽羅瓦在 1829 年 8 月 3 日二度參加巴黎綜合理工學院的入學考，卻仍然名落孫山。這樣的結果，讓理查老師和所有同學都不敢置信。認識他的人都知道：他的卓越數學天份是超乎常人的。在如此重要的考試當中落榜，非比尋常。於是有了種種猜測與謠傳，認為伽羅瓦平日習慣於在腦中思考，不擅於循序漸進地表達邏輯推理，又沒有板書經驗，使得主考官跟不上他的思路，在口試這一關就相對吃虧；也可能和主考官是為了某個數學觀點而起了爭執，激怒了主考官；或是他的父親剛去世不久，心情尚未平復等等。但無論是何種臆測，落榜已是歷史的事實。而綜合理工學院規定每人至多只能參加兩次入學考，自此，伽羅瓦已永遠被該校拒於門外了。¹⁰⁴

因為伽羅瓦的父親辭世使家中頓失經濟來源，而理查老師一心仍希望伽羅瓦繼續深造，於是伽羅瓦決定轉考高等師範學院(École normale)。這所學校創建於 1795 年法國大革命期間，之後經過一些變革，又於 1826 年改為兩年制預科學院(École préparatoire)，直到 1830 年才復名為高等師範學院，並改為修業三年。而伽羅瓦參加入學考時仍是預科學院，他在 1829 年 10 月 25 日以預備生資格被錄取入學，直到 1830 年 2 月 20 日才成為正式的高等師範學院學生，選擇科學學門作為主修，在學期間可領取公費，畢業後要為國家服務。學校的生活方式極為傳統與保守，祈禱與懺悔都是每日、每月的例行功課，與修道院極為相似。¹⁰⁵

九、此曲只應天上有

進入高等師範學院前，還有一件事讓伽羅瓦錯愕不已。就是在 1829 年 6 月將獨創理論的論文手稿交給柯西之後，沈寂了六個月，竟然被柯西給耽延了。¹⁰⁶直到 1830 年 1 月 18 日，柯西去函科學院致歉，節錄自 Mario Livio 著，蔡承志譯的《無解方程式》一書中，此封道歉函部分內容如下：

我本當於今日向科學院提報，首先是關於年輕人伽羅瓦研究成果的一篇報告，其次是關於原根分析判定的專論，且應在文中說明我們該如何分解此判定結果……。現因微恙居家休養。我深感遺憾無法出席本日會議，懇請為我安排在下次會議提報前述兩文。(頁 152)

¹⁰³ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 153；達爾馬斯原著：《伽羅瓦傳》，頁 8。

¹⁰⁴ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 154-155；達爾馬斯原著：《伽羅瓦傳》，頁 7-8。

¹⁰⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 8-9；Mario Livio 著，蔡承志譯：《無解方程式》，頁 155；康明昌：《幾個有名的數學問題》，頁 115。

¹⁰⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 7；Mario Livio 著，蔡承志譯：《無解方程式》，頁 152；康明昌：《幾個有名的數學問題》，頁 115。

後來，在隔次會議上，柯西就不再提起伽羅瓦的論文。

伽羅瓦十分納悶，不知柯西為何沒有再將他的論文提交科學院？但他實在等得不耐煩，遂決定將作品稍作修改，積極想角逐數學成就大獎。數學成就大獎是法國科學院在 1829 年 6 月宣佈新設立的獎項，截止收件日期為 1830 年的 3 月 1 日。伽羅瓦對自己的發現有絕對的信心，這篇題目為《論方程式得以根式求解的條件》(*On the conditions That an Equation Be Solvable by Radicals*)的論文，終於趕在 2 月底前向科學院交稿。¹⁰⁷

這一次論文手稿的命運更加坎坷，它落到科學院常任秘書約瑟夫·傅立葉(Joseph Fourier 1768—1830 年)的手中，傅立葉將它帶回家審查，卻不幸於當年的 5 月 16 日過世，那篇稀世珍寶的論文就不見蹤影了。論文離奇失蹤，使得當年競逐數學成就大獎的名單裡根本找不到伽羅瓦的論文，但伽羅瓦依然被蒙在鼓裡。等到宣布已逝的阿貝爾(Abel 1802-1829 年，挪威數學家)和年輕的雅可比(Jacobi 1804-1851 年，德國數學家)獲得數學大獎時，一切都來不及了。自己看重的論文卻一再地被弄丟，心中的怨氣只能往肚裡吞，真是啞巴吃黃蓮，有苦說不出！¹⁰⁸

但在這期間，伽羅瓦的文章曾兩度刊載在《菲魯薩克學報》(*Ferrusac's Bulletin*)，一次是 1830 年的四月號，另一次是同年的六月號。該學報的四月號發表了一篇伽羅瓦對於獨創理論所寫的〈一份有關解代數方程的研究報告〉；接著，六月號又有兩篇伽羅瓦的作品，一篇為〈有關解代數方程的筆記〉，另一篇為〈有關數論的筆記〉，而且順序的編排是兩篇伽羅瓦的文章中間夾著柯西的論文，足見年僅十八歲的伽羅瓦，已經可與當代頂尖數學家並駕齊驅了。¹⁰⁹

伽羅瓦的論文，具有開疆拓土的新眼光，它是一個相當高級的創造工程。在新開闢的領域當中，解決了糾纏數學界很長一段時間的疑點。

十、大學開始熱衷政治

1830 年伽羅瓦在高等師範學院就讀時所寫成的數學著作，已更能展現他思想的獨創性與敏銳度。除了繼續研究熱愛的數學之外，伽羅瓦所關注的層面也開始有了變化。

伽羅瓦在高等師範學院認識了一位學長，名字叫作奧古斯特·舍瓦烈(Auguste Chevalier)，他有一位就讀巴黎綜合理工學院的哥哥，名叫米歇爾·

¹⁰⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 9；Mario Livio 著，蔡承志譯：《無解方程式》，頁 152；王懷權編著：《數學發展史》，頁 343。

¹⁰⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 9；Mario Livio 著，蔡承志譯：《無解方程式》，頁 152-153；康明昌：《幾個有名的數學問題》，頁 115；王懷權編著：《數學發展史》，頁 343。

¹⁰⁹ 參考馮曉華：〈劉維爾的開脫〉，《西安電子科技大學學報》第 16 卷第 4 期(2006 年 7 月)，頁 144-148；達爾馬斯原著：《伽羅瓦傳》，頁 9-10；Mario Livio 著，蔡承志譯：《無解方程式》，頁 156。

舍瓦烈(Michel Chevalier 1806-1879 年，法國經濟學家)，兄弟倆都篤信聖西門主義(Saint-Simonianism)。雖然伽羅瓦並未跟隨奧古斯特參與聖西門主義，但他們兄弟倆的思想對伽羅瓦有很大的影響，並開啟了伽羅瓦在政治與社會方面的嶄新眼界。¹¹⁰

自從查理十世 1824 年登基之後，有兩股勢力不斷威脅著他的政權。一個是以學生和勞工為主體的共和派(republican)，此一派別是以法國大革命的思潮為理念主軸，走的是實現理想的路線；另一個是奧爾良派(Orléanist)，則以推翻查理十世，擁戴奧爾良公爵路易-菲利浦(Louis-Philippe)為目標，奪權的痕跡鑿斧斑斑。¹¹¹

法國在 1830 年 7 月的國會選舉中，反對勢力獲壓倒性的勝利。查理十世遂在 7 月 25 日頒布新法令，限制出版自由、解散新選出的國會議員，意圖以新的選舉法保住政權。奧爾良派在 7 月 27 日發表文章，呼籲民眾起義，引發街頭暴動，是為「七月革命」。當時許多綜合理工學院的學生也參與其中，走上街頭，創造了「光榮三日」(Trois Glorieuses)的歷史。而師範學院的學生，被校長吉尼奧(M.Guigniault)鎖在校園內，禁止學生參加街頭運動，甚至揚言準備召喚警察，來維持學校的秩序。7 月 28 日夜晚，伽羅瓦曾試圖越牆外出，但沒有成功。¹¹²

七月革命共有將近四千人死亡，查理十世下台，流亡英國，且奧爾良公爵路易-菲利浦於 8 月 9 日加冕登基。面對這種局勢，師範院校長立即見風轉舵，率領全校師生向臨時政府表達擁戴之意，投機的心態有著像牆頭草般的作為。然而，數學家柯西作法卻截然不同，他展現骨氣，與自己效忠的波旁王朝同進退，遂離開了法國。年輕熱血的伽羅瓦，看在眼裡，對於校長的人品與行徑，更加感到不齒。¹¹³

伽羅瓦在 1830 年暑假回到家鄉布爾拉林，他對政治所表現出的狂熱，讓家人及兒時玩伴都感到十分驚訝，很難想像眼前所見的這個熱情洋溢、提倡民權的激進青年，就是從前那個弱小、保守的孩子。伽羅瓦返回學校之後，加入了校外的「人民之友會」(Société des Amis du Peuple)組織，這是一個支持共和的好戰派團體，師範學院只有他一個人入會，因此結識了許多校外的異議份子，這些人後來多成為有名的政治領袖。除此之外，伽羅瓦也參加了「國民自衛軍砲兵隊」，對政治活動的投入，日益加深。¹¹⁴

在伽羅瓦的心中，「政治活動」和「科學發明」同等重要。但學校校長規定：「好學生不宜過問政治」，使伽羅瓦更加不予苟同。1830 年 12 月 5 日，

¹¹⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 10；Mario Livio 著，蔡承志譯：《無解方程式》，頁 156。

¹¹¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 156。

¹¹² 參考達爾馬斯原著：《伽羅瓦傳》，頁 11-12；Mario Livio 著，蔡承志譯：《無解方程式》，頁 156-158；康明昌：《幾個有名的數學問題》，頁 116。

¹¹³ 參考達爾馬斯原著：《伽羅瓦傳》，頁 10；Mario Livio 著，蔡承志譯：《無解方程式》，頁 158。

¹¹⁴ 參考達爾馬斯原著：《伽羅瓦傳》，頁 13-15；Mario Livio 著，蔡承志譯：《無解方程式》，頁 158；康明昌：《幾個有名的數學問題》，頁 116。

在《學院公報》(*La gazette des écoles*)刊出一篇批評師範學校長的文章，措詞辛辣。文中直指他假道學、善鑽營，並附上一封信函，是來自師範學院某位學生的手筆，譏諷校長在七月的行為搖擺不定、趨炎附勢，是機會主義者，並表示有 46 位學生可以作見證。雖然沒有署名，但一般人認為是伽羅瓦所寫，校長與伽羅瓦的關係日漸緊張，面臨攤牌。¹¹⁵

12 月 9 日校長將伽羅瓦送回家，並向教育主管單位作報告。在校內則唆使學生告密，或進行訪談，以蒐集證據，羅織伽羅瓦的罪名。在 12 月 12 日的《學院公報》上，又刊出一篇有 20 位學生簽名的〈師範學院學生們的抗議書〉，抗議《學院公報》日前詆毀校長的文章是扭曲事實。伽羅瓦也在 12 月 30 日寫了一封公開信給師範學院的學生們，表示他本人無所求，只請大家憑良心說誠實話，如果每個人都保持沈默，就變成支持權力者的決定了。但卻沒有得到該有的聲援，學生們多選擇了明哲保身。當時，只有《憲法報》(*Le Constitutionnel*)於 12 月 12 日披露了師範學院學生伽羅瓦的遭遇。¹¹⁶

在 1831 年 1 月 2 日，《學院公報》刊出伽羅瓦的一篇文章：〈談數學教育的改革—包括教師、教科書和主考官〉。文中伽羅瓦對於巴黎中學生學習數學的看法，整理成以下幾點：¹¹⁷

- (一) **科學工作者**：不該因政治觀點或宗教信仰的異同，而影響科學工作者的職務或功績認定。
- (二) **數學學習方法**：中學生學習數學，是否有人引導他們領會真正的科學精神呢？還是把推理能力當作另類記憶在學習呢？學習數學的方法是否愈來愈像語文的方法呢？
- (三) **數學學習內容**：最一般性、重要的代數定理被忽略了。卻要學生去讀那些無用、冗長的理論，以及一些未必正確的運算，或是浪費時間去論證許多顯而易見的結果。
- (四) **數學教科書**：書商們急於推銷主考官的著作，使得各種資料來源多樣，他們就更有利可圖。致使科學教科書的出版，常摻雜著不同風格，有選錄學者高深理論的內容，也有中小學生初級認知的推論，成為大總匯版。
- (五) **主考官**：對每個定理，考生是否要在口袋裡準備多個答案？若遇到四個主考官，就要以四種不同的答案應付？多年下來，已出現一門新學科，它是專門研究主考官的特殊癖好和情緒反應。

¹¹⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 15-17；Mario Livio 著，蔡承志譯：《無解方程式》，頁 158-160；康明昌：《幾個有名的數學問題》，頁 116。

¹¹⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 16-18；Mario Livio 著，蔡承志譯：《無解方程式》，頁 160-161；康明昌：《幾個有名的數學問題》，頁 116。

¹¹⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 42-43。

以當時伽羅瓦勇於針砭之言，對照古今中外的數學教育制度，果然是振聳發聵之聲。雖然伽羅瓦總是以勇於衝撞現行體制的姿態出現，但對於 1831 年 1 月 8 日被學校開除的結果仍須接受。¹¹⁸

伽羅瓦被開除後，失去了領取公費的經濟來源，於是隔天在《學院公報》刊登廣告，在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本一書中，節錄這篇廣告部分內容如下：

1 月 18 日(星期四)，伽羅瓦先生將講授高等代數。以後每逢星期四下午 1 時 15 分，將在索爾奔納街第 5 號，凱洛特(Caillot)小書舖進行講課。該講課以不滿足專科學校所講授的代數而希望深造者為對象。講座將向聽眾介紹不曾公開講授過的若干理論。其中某些理論完全是獨創的。(頁 20)

授課地點是他的朋友所開的一家書店，剛開始有一些政治理念相近的朋友來捧場，但因為課程太艱深，就紛紛不來了。曲高和寡是必然。¹¹⁹

一個只有十九歲的少年，願意向眾人宣講自己創新的思想、研究的成果，以作為謀生的方式，在當代科學史上，也是絕無僅有的。

十一、向科學院三度叩關

1831 年年初，伽羅瓦雖面臨被學校開除的命運，但科學院卻請伽羅瓦重新遞交論文。一年前曾在傅立葉手中遺失的論文，再度以新版面貌提交，題目為：《方程式得以根式求解的條件》(*The Conditions for Resolvability of Equations by Radicals*)。1 月 17 日由泊松(Siméon Denis Poisson 1781-1840 年，法國數學家)與拉克魯瓦(Sylvestre François Lacroix 1765-1843 年，法國數學家)兩位科學院院士負責審閱。伽羅瓦有了前一年不悅的經驗，特別在論文前附加一篇短箋，請負責審閱的院士至少要從頭到尾讀完他的作品。¹²⁰

但是經過了兩、三個月，科學院仍然沒有任何回應。伽羅瓦決定在 3 月 31 日寫信給科學院院長，筆者將信中所提整理成以下幾點：¹²¹

(一)說明他去年應徵數學成就大獎的著作，主要內容是開發了一些判斷準則，以作為分辨方程式是否可用根式求解的依據。

(二)因為現今的數學家並不否認存在這樣的論述，但工程實在艱鉅，科學院

¹¹⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 18；康明昌：《幾個有名的數學問題》，頁 116。

¹¹⁹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 20；Mario Livio 著，蔡承志譯：《無解方程式》，頁 162。

¹²⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 20-21；Mario Livio 著，蔡承志譯：《無解方程式》，頁 162；康明昌：《幾個有名的數學問題》，頁 116；王懷權編著：《數學發展史》，頁 343。

¹²¹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 21、44；Mario Livio 著，蔡承志譯：《無解方程式》，頁 162-163。

的審查就預想不可能由他一人獨力完成。在達爾馬斯原著《伽羅瓦傳》中，伽羅瓦這封信描述前一年的論文下場如下：

第一、因為我叫伽羅瓦。第二、因為我是個大學生。於是我的研究報告被埋沒在委員會裏。我接到通知說它遺失了。(頁 44)

(三)特別祈請院長轉詢泊松和拉克魯瓦兩位科學院院士，今年是打算讓他的手稿再度遺失？還是會向科學院提交論文報告？

伽羅瓦這封信態度相當堅定，他很希望當代數學家能夠和他起共鳴。但他的著作中，有許多都是跨越時代、直達未來的內容，當時顯赫一時的學者們仍然無法理解伽羅瓦所言。伽羅瓦的理論，在伽羅瓦的年代註定是孤獨的，在未來的年代才被人們像珍寶一般地捧在手心。

十二、被捕獲釋

自從路易-菲利浦於 1830 年 8 月掌權之後，共和派的勢力也日益增長，使新政府感到威脅，惶惶然無法心安。政府很技巧地在 1830 年底解散了國民自衛軍，卻仍有十九名砲手不願解除武裝。他們被逮捕之後，於 1831 年 4 月接受審訊，通稱為「十九人審判案」，當時法庭大廈湧進了大批社會青年、學生及勞工。被告席上並未自我辯護，卻趁此機會極力宣揚共和派的理念。結果案情急轉直下，全體被告都獲判無罪。¹²²

為了慶祝十九名砲手獲釋，人民之友會於 1831 年 5 月 9 日舉辦了大型宴會，地點選定在郊區的布爾根飯店(Aux Vendanges de Bourgogne restaurant)。大約有兩百名共和派人士與會，並邀請了亞力山大·仲馬(即大仲馬 Alexandre Dumas 1803-1870 年，法國小說家)和一些生物學家、政治家或在其他領域的名人參加。¹²³

餐會進入尾聲後，互相舉杯並祝酒，在場所有大人物的祝詞都是預先擬妥的，而且彼此都很小心未發表演說，以免引起警察注意。原本以為可以平和地結束這場聚會，但現場有一群熱血澎湃的年輕人，他們士氣高昂，無法忍受領袖們平平淡淡且略帶敷衍的祝詞，憤慨的情緒油然而生。此時，伽羅瓦站起來，高舉酒杯，並拿著一把匕首，說：「敬路易-菲利浦！」多數人報以熱烈掌聲或歡呼狂叫；也有人可能沒有看到刀子，回以噓聲要轟他下來。現場頓時一片混亂。¹²⁴

¹²² 參考達爾馬斯原著：《伽羅瓦傳》，頁 19、22；Mario Livio 著，蔡承志譯：《無解方程式》，頁 163。

¹²³ 參考達爾馬斯原著：《伽羅瓦傳》，頁 22-23；Mario Livio 著，蔡承志譯：《無解方程式》，頁 163；康明昌：《幾個有名的數學問題》，頁 116。

¹²⁴ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23；Mario Livio 著，蔡承志譯：《無解方程式》，頁 163-164；

此時，亞歷山大·仲馬和鄰座的一位朋友，怕久待受到牽連，識時務者為俊傑，遂趕緊從窗台溜開。當晚的騷動與喧嚷持續沸騰，伽羅瓦一夕之間變成了大夥兒的英雄。宴會結束後，許多人還意猶未盡，徹夜在街上狂歡。¹²⁵

第二天早上，警察搜索伽羅瓦母親的住處，逮捕了伽羅瓦，他隨即被關到聖佩拉吉監獄(Saint-Pélagie prison)裡，這是伽羅瓦第一次體驗監獄生活。案情調查了五個星期，直到 1831 年 6 月 15 日終於送交審判。¹²⁶

《學院公報》在 5 月 12 日刊出一篇簡短的報導，節錄自達爾馬斯著的《伽羅瓦傳》中譯本的參考資料(註 43)中，記錄此篇簡訊部分內容如下：

...有很多人舉杯祝酒，這時有個狂人怒氣衝天，忿然離席，從衣袋裡拔出刀子，在空中揮舞起來，高聲喊道：『我要向路易-菲利浦宣誓...。』這個狂人就是伽羅瓦。¹²⁷(頁 112)

6 月 15 日在法院開庭時，伽羅瓦被起訴的罪名是：「教唆謀害法國國王的人身與性命未遂罪」。此案由竇本(Dupont)擔任被告的辯護律師，伽羅瓦自述自己私下在為人講授數學課。雖然這時候他的高等代數課程已經停止了，但由他的自述內容可知，他對數學仍然有很深的執著。¹²⁸

《辯論雜誌》在 1831 年 6 月 16 日刊載了這一案的起訴記錄，在此將伽羅瓦的答辯整理出幾個重點：¹²⁹

- (一) 伽羅瓦確曾向製刀匠訂購了一把匕首，他坦承自己有攜帶刀子的癖好，並辯稱有些醫生在照料傷者的過程也常會隨身帶著這種刀子。伽羅瓦說當天在布爾根飯店集會時，正是用它來切雞肉的；而當晚離開飯店時，把刀子給丟掉了。
- (二) 伽羅瓦表示，當晚他邊拿著刀子揮舞，邊說著：「敬路易-菲利浦，**如果他背叛了我們的話。**」大家聽到第一句話就開始大聲喧嘩，使得第二句話只有鄰座幾個人聽到而已。伽羅瓦解釋自己會說這樣的話，是因為對國王的擔憂，擔心一旦他背叛了人民，會對人民進行剝削，所以國王也需要接受檢視。

康明昌：《幾個有名的數學問題》，頁 116。

¹²⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23；Mario Livio 著，蔡承志譯：《無解方程式》，頁 164。

¹²⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23；Mario Livio 著，蔡承志譯：《無解方程式》，頁 164；

康明昌：《幾個有名的數學問題》，頁 116。

¹²⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23、112；Mario Livio 著，蔡承志譯：《無解方程式》，頁 164。

¹²⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23-24、65-77。

¹²⁹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23-24、65-77；Mario Livio 著，蔡承志譯：《無解方程式》，頁 164-165。

(三)伽羅瓦聲稱自己的思想與剛被釋放的十九名砲手是一樣的，有罪與無罪的判定應該要一致。

伽羅瓦滿腔熱血且不願屈服的堅定態度，使得他的答辯慷慨激昂，遇到敏感的政治問題也能正面抨擊。竇本律師適時地引用另一案的例子，指出飯店並非公開場合，不算當眾發表言論，認為被告沒有犯罪行為。經過了半小時的討論，法官裁定伽羅瓦無罪釋放。¹³⁰

十三、Galois 的論文未獲肯定

伽羅瓦於 1831 年初交給法國科學院的論文，如石沈大海般毫無音訊。雖然後來伽羅瓦又寫了一封信給科學院院長，追問論文審查的結果，但仍沒有激起任何漣漪。

接著，伽羅瓦因政治案件被捕，就在 1831 年 6 月 15 日受審當天，《全球報》(*Le globe*)報導了這位新聞人物的事蹟，它披露了極具才華的伽羅瓦在學界受到的不公平對待。文中並指出伽羅瓦將研究的論文投遞科學院，卻一再地被弄丟，無緣角逐數學成就大獎。後來伽羅瓦將那一篇專論重寫，再次遞交科學院，負責的泊松院士耽延至今，尚未審閱，使得伽羅瓦五個月來一直等不到結果。這樣一篇為伽羅瓦發出不平之鳴的文章，很可能是伽羅瓦的好朋友舍瓦烈兄弟主筆。¹³¹

科學院終於在 1831 年 7 月 4 日有了回音，泊松和拉克魯瓦提出了審查報告。在康明昌所著的《幾個有名的數學問題》一書中，記載審查結果如下：

我們努力去瞭解 Galois 先生的證明。許多推論並不夠清楚，也沒有寫得讓別人能夠判斷其嚴密性。我們實在不瞭解這篇論文。原作者聲稱，這篇論文只是一個豐富的理論的一部份。通常，把一個理論完整的寫出來，其每一部份會彼此印證，這個理論也比較容易理解。因此，除非原作者把他的全部研究成果寫出來，我們實在不能對這篇論文做出一個明確的決定。(頁 117)

為什麼代數學上如此上等的創見，在當時卻無法被巴黎科學院認可？原因應可歸納為以下幾點：¹³²

¹³⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 23-24、65-77；Mario Livio 著，蔡承志譯：《無解方程式》，頁 164-165。

¹³¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 165-166。

¹³² 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 166-167；康明昌：《幾個有名的數學問題》，頁 117、146-147；馮曉華：〈劉維爾的開脫〉，《西安電子科技大學學報》第 16 卷第 4 期 (2006 年 7 月)，頁 144-148。

- (一) **論述不足**：任何人所提的論述，如果超出人類的知識、理性或經驗時，一定要特別清楚闡明。年輕的伽羅瓦，文筆的確不夠清晰，有些說明尚有缺失，還須補述。
- (二) **知識落差**：伽羅瓦的判斷準則是運用新觀念「群論」，「群論」在當時是創新的理論，超乎兩位審閱學者的想像，且與當時已有的知識有很大的落差。
- (三) **風格新穎**：當時的數學家對於抽象代數的風格還相當陌生，和過往的研究模式有許多的不同。節錄康明昌著的《幾個有名的數學問題》書中的一段敘述如下：

二十世紀的數學家 J.Dieudonné 曾表示(1962)，Galois 強調觀念性的證明(le caractère conceptuel des mathématiques)，他厭惡掩蓋關鍵性想法的冗長的計算(les longs calculs masquant les idées directrices)，這正是近世數學的風格。對於這種風格，十九世紀大部分的數學家是非常陌生的，尤其是專攻數學物理的 Poisson。(頁 117)

- (四) **學界封閉**：科學院未能展開雙臂，歡迎、賞識他人的研究成果，包括阿貝爾(Abel)、伽羅瓦及鵬思列(V.Poncelet 1789-1867 年，射影幾何學家)都曾是法國科學院的遺珠。節錄康明昌著的《幾個有名的數學問題》一書中的註釋(註十二)，如下：

當時巴黎科學院的院士們的研究態度，Abel 曾經這樣描述：「每個人只關心自己的問題，毫不留意別人的研究成果。大家只想講，卻沒有人想聽。」(頁 146-147)

果然，在 1831 年 7 月 11 日的科學院會議當中，否決了伽羅瓦的論文。

十四、再度入獄

7 月 14 日為法國革命紀念日(Bastille Day)，是為了紀念 1789 年的這一天，人民起義搗毀巴士底獄的壯舉。在 1831 年 7 月 14 日，為了要求政府當局有更多的社會變革，以建立自由平等的社會，共和派計畫於巴士底獄廣場發動一場群眾的示威遊行，並安排種植自由之樹的活動，以紀念法蘭西共和國成立 43 周年。政府因擔心暴動，在數天前就宣佈禁止遊行，加派警力維安，並對許多激進份子的行動蒐證監視，伺機在 7 月 13 日晚上準備逮捕一些共和派的領袖。伽羅瓦當時未住在家中，已搬出去在伯納路(rue des Bernardins)

租房獨居，因此當晚逃過一劫。¹³³

不過，在 7 月 14 日中午，伽羅瓦和另外一名國立古文書學院(École des chartes)法律系的學生埃內斯特·杜沙特雷(Ernest Duchatelet)，一同在新橋(Pont Neuf)上被逮捕。當時他們兩人都穿著國民自衛軍的制服，伽羅瓦的身上更配有刀槍等武器，準備帶領約六百名群眾參加示威活動。警察將他們兩人先關在道芬(Dauphine)街的警察局拘留所內，當晚立即送到聖佩拉吉監獄。

¹³⁴

而一整天的示威活動，警方也逮捕了許多人，尤其是晚上在愛麗舍宮廣場(Champs-Élysées)，警察們打扮成工人，成功地突襲了共和派的場子。第二天的報紙大篇幅地報導警方這次的行動，多位有名的激進人士都落網，名單當中，也包括年輕的伽羅瓦。¹³⁵

伽羅瓦和杜沙特雷被關在聖佩拉吉監獄，直到 1831 年 10 月 23 日才出庭受審。在羈押近百日當中，伽羅瓦受到上級「特別關照」的看管，他們清楚知道伽羅瓦與共和派的淵源。¹³⁶

若要將伽羅瓦以陰謀顛覆政府入罪，似乎證據不足，反而易弄巧成拙，使陪審團作出無罪的判決。最後伽羅瓦和杜沙特雷兩人以「非法著軍服罪」被起訴，而伽羅瓦外加一條「攜帶武器」的罪名。杜沙特雷被判應繼續再監禁三個月，而伽羅瓦總共被判了九個月的刑期。¹³⁷

伽羅瓦對於判決不服，他認為隨身攜帶防衛武器在當時的法國社會已不是新鮮事，對他加重刑責有失公正，於是又對法院提起上訴。然而，巴黎法院在 1831 年 12 月 3 日作出最後的判決，裁定維持原判。伽羅瓦必須在聖佩拉吉監獄繼續服刑。¹³⁸

十五、獄中生活

聖佩拉吉監獄裡關的犯人，除了政治犯之外，還有刑事犯和未成年犯兩類。囚房分成三種等級，有單人囚室、七八人合住的中型囚室，以及六十人合住的大牢房。¹³⁹

政治犯又有許多派別，其中共和派人數佔最多。獄方對政治犯的管訓不會太嚴，大多尚能以較人道的的方式對待，活動空間可延伸至院子裡，也可進出販賣部消費。住單人囚室的多半來頭不小，必定是有錢有勢且能自己負擔

¹³³ 參考達爾馬斯原著：《伽羅瓦傳》，頁 24-25；Mario Livio 著，蔡承志譯：《無解方程式》，頁 167；康明昌：《幾個有名的數學問題》，頁 117。

¹³⁴ 參考達爾馬斯原著：《伽羅瓦傳》，頁 25；Mario Livio 著，蔡承志譯：《無解方程式》，頁 167-169；康明昌：《幾個有名的數學問題》，頁 117。

¹³⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 25；Mario Livio 著，蔡承志譯：《無解方程式》，頁 169。

¹³⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 25；Mario Livio 著，蔡承志譯：《無解方程式》，頁 169。

¹³⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 25-26；Mario Livio 著，蔡承志譯：《無解方程式》，頁 169。

¹³⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 26；Mario Livio 著，蔡承志譯：《無解方程式》，頁 169。

¹³⁹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 26；Mario Livio 著，蔡承志譯：《無解方程式》，頁 170。

生活費的犯人，他們還可在監獄裡的餐廳自購食物；至於社會閱歷不多且非犯下嚴重罪刑的，就關在中型囚室裡；而毫無背景的窮人只能住進六十人的大牢房裡。¹⁴⁰

在監獄的院子裡附設了一間酒館，大多數政治犯的日間活動都耗在這間酒館裡。伽羅瓦身體羸弱，不喜愛飲酒，常在獄中的庭園邊踱步邊深思，反覆在腦中進行獨創理論的建構，加上沉靜憂鬱的個性，要在如此吵雜的環境中生存相當辛苦。¹⁴¹

監獄裡的共和派囚犯，在夜間多會秘密聚集，參加他們所謂的「晚禱」儀式，有時找到藍、白、紅三種顏色的組合就象徵性地代表國旗，在喧嘩聲中輕唱著馬賽進行曲，互相鼓舞著士氣，有時還會演戲悼念七月革命犧牲的共和派同志。¹⁴²

伽羅瓦的獄中生活情形，從三個人的著作或筆記可窺端倪：¹⁴³

(一) 樊尚·拉斯拜爾(François-Vincent Raspail 1794-1878 年，法國生物學家)所寫的《在巴黎獄中書簡》(Letters on the Prisons Paris)。

拉斯拜爾是人民之友會的領袖，也是伽羅瓦的獄中難友。他雖被判處十五個月的重刑，但在監獄裡住的環境比伽羅瓦優，可以佔用單人囚室，因此較有可能安靜思考或工作。¹⁴⁴他的《在巴黎獄中書簡》中曾提起伽羅瓦在獄中的一些事情，整理如下：

那年的 7 月 29 日，正當囚犯紀念「光榮三日」進入第三天，一發子彈從監獄正面的隱士之井路(rue du Puits de l'Ermitage)射入伽羅瓦的囚室，射傷一名犯人。隨後囚犯代表團面見典獄長共商此事，伽羅瓦也是代表之一，顯然他在會中指控槍手是一名獄卒，還當場羞辱典獄長。於是伽羅瓦被關進地牢，囚犯群情激憤，暴力相向。拉斯拜爾引述一名囚犯對典獄長說的話：「伽羅瓦這個年輕人並沒有惡言相向，你自己很清楚；他跟你說話的時候，口氣就像他的數學那樣冷靜。」其他囚犯都發言表示贊同：「伽羅瓦被關進地牢！這群混帳雜種！他們和我們的小學者有仇。」囚犯喧囂聲援，然後採取行動占領監獄，不過只鬧了一天就恢復秩序。獄方唯恐暴動加劇，只得把伽羅瓦釋出地牢。(節錄自 Mario Livio 著，蔡承志譯：《無解方程式》，頁 171)

¹⁴⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 26；Mario Livio 著，蔡承志譯：《無解方程式》，頁 170。

¹⁴¹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 26-27；Mario Livio 著，蔡承志譯：《無解方程式》，頁 171-172。

¹⁴² 參考達爾馬斯原著：《伽羅瓦傳》，頁 26；Mario Livio 著，蔡承志譯：《無解方程式》，頁 172。

¹⁴³ 參考《無解方程式》，頁 170。

¹⁴⁴ 參考達爾馬斯原著：《伽羅瓦傳》，頁 27。

伽羅瓦不常豪飲酗酒，顯然經常被獄友戲弄灌醉，喝得不省人事。「年輕人，你只能喝水。」他們常調侃他：「喔，贊尼特！[囚犯為伽羅瓦取的綽號]¹⁴⁵別和共和派那幫人攪和，回去搞你的數學。」有一次這個年輕人又被灌酒，醉言醉語地向拉斯拜爾吐露父親死後心中的悲苦：「我失去父親，再也沒有人取代他的地位。」接著他又說了一句，卻是一語成讖：「我會為了一個風騷賤貨，和人決鬥而死。」拉斯拜爾和其他幾名囚犯想讓伽羅瓦在床上躺好，他大醉，神智不清地高喊：「你們看不起我，你們都是我的朋友啊！你們沒錯，像我這樣罪行重大的人應該自殺！」囚犯迅速群起制止，伽羅瓦這才尋死不得。(節錄自 Mario Livio 著，蔡承志譯：《無解方程式》，頁 171)

有一次，拉斯拜爾目睹伽羅瓦被別人挑釁賭酒的慘況，也寫下了如下句子：

寬容這位柔弱而大無畏的少年吧！三年之中，科學在他額上劃下六十年深思熟慮也不會更深的皺紋。為了科學和德行，請愛護他的性命吧！再過三年，他必將成為真正的科學家。(節錄自達爾馬斯原著：《伽羅瓦傳》中譯本，頁 27-28)

(二) 熱拉爾·德·奈瓦爾(Gérard de Nerval 1808-1855 年，法國浪漫主義作家)的詩作《我的監獄生活》

奈瓦爾曾在 1832 年 2 月在聖佩拉吉監獄被關了幾天，他在《我的監獄生活》作品中，記錄了離開監獄前與伽羅瓦的一段交情，節錄部分如下：¹⁴⁶

當時是五點鐘，有個同桌吃飯的人把我送到門口，吻了我一下，答應他一旦獲釋，就來拜訪。他自己必須再坐兩三個月牢。他就是不幸的伽羅瓦。可是我從此再也見不著他了，他出獄的第二天就被殺害了。(節錄自達爾馬斯原著：《伽羅瓦傳》中譯本，頁 27)

(三) 伽羅瓦的姊姊娜塔莉-泰奧多爾·伽羅瓦(Nathalie-Théodore Galois 1808-?)的文章。

娜塔莉-泰奧多爾和伽羅瓦手足情深，伽羅瓦在獄中時她經常探訪，關心他的身心健康。她曾在日記中寫下：

¹⁴⁵譯者註。

¹⁴⁶參考達爾馬斯原著：《伽羅瓦傳》，頁 27；Mario Livio 著，蔡承志譯：《無解方程式》，頁 171。

這樣呼吸不到新鮮空氣，還要忍受五個月！哪裡還有希望，我怕他的身體狀況會嚴重惡化。他已經疲累不堪。他完全無法自拔，對其他一切念頭都不聞不問，沾染了一種陰鬱性情，讓他的心態比實際年齡更老。他的雙眼無神，看起來就像五十歲的人。(節錄自 Mario Livio 著，蔡承志譯：《無解方程式》，頁 171-172)

在獄中的環境雖然吵雜，伽羅瓦還是努力地擠壓出時間來，寫下腦中所想。在伽羅瓦離世後，他的兩篇序文被他的好朋友奧古斯特·舍瓦烈發現，都是在聖佩拉吉監獄內完成的。由這兩篇序文的內容看來，他想完成兩部著作的心願相當明顯。¹⁴⁷

十六、墜入情網

歐洲在 1832 年的春天爆發了一次霍亂的大流行，巴黎的衛生單位也進入緊急狀態，伽羅瓦因此在 3 月 16 日獲得假釋，遷移到一間療養院。離開了蹲伏八個月的聖佩拉吉監獄，來到位於拉契尼路(rue de Lourcine)的西慰佛爾特里埃康復之家(Sieur Faultrier house of health)，伽羅瓦距離重獲自由已經指日可待了。而康復之家除了有醫療服務外，其實仍不時要受到警察局的監督。¹⁴⁸

伽羅瓦假釋之後與外界聯繫的機會增加了，也因此認識了未滿十七歲的少女史蒂芬妮·迪摩特爾(Stéphanie Potterin du Motel)。主要是迪摩特爾家族與康復之家都住在同一棟建築裡，近水樓台，伽羅瓦與史蒂芬妮彼此互有好感。史蒂芬妮的父親曾經是拿破崙時期的軍官，她在家中還有一個比她小一歲的弟弟。¹⁴⁹

伽羅瓦因從小就在母親的羽翼下成長，很少和其他女生有接觸交往，有一次在獄中酒後向拉斯拜爾傾吐：「我不喜歡女人，...」但一旦陷入愛情的漩渦中仍無法自拔。史蒂芬妮一開始可能極欣賞伽羅瓦的才華與熱情，不久之後就逐漸冷淡下來，甚至拒絕伽羅瓦的追求。伽羅瓦自己也十分矛盾，情感陷得太深，理智上又不願放棄對研究的堅持。人生的第一次戀愛就走得如此跌跌撞撞，他更加地厭惡自己、懷恨在心，宛如世界末日將至。¹⁵⁰

伽羅瓦在 1832 年 4 月 29 日監禁期滿，重獲自由。身體雖獲得了自由，心靈被捆綁卻未得釋放。在 1832 年 5 月有幾封書信的史料，得以讓後人拼湊出伽羅瓦當時的心情：

¹⁴⁷ 參考達爾馬斯原著：《伽羅瓦傳》，頁 28、53-58；Mario Livio 著，蔡承志譯：《無解方程式》，頁 172。

¹⁴⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 28；Mario Livio 著，蔡承志譯：《無解方程式》，頁 173-174。

¹⁴⁹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 174。

¹⁵⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 29、44-46；Mario Livio 著，蔡承志譯：《無解方程式》，頁 174-176。

(一) 伽羅瓦不完整地抄錄下史蒂芬妮寫給伽羅瓦的兩封信內容。

伽羅瓦曾將史蒂芬妮的兩封信內容，親手抄寫在一張紙上，只可惜片片斷斷的詞句顯得殘缺不全，但看出她提議分手、不再交往。其中一封寫於 5 月 14 日，另一封可能在幾天之後。¹⁵¹

(二) 伽羅瓦於 1832 年 5 月 25 日寫給好友奧古斯特·舍瓦烈的一封信。

當時舍瓦烈兄弟與一些聖西門主義的信徒們，因崇尚社會性的活動，一同組成了一個小型社區，過著田園式的生活。他們也曾向伽羅瓦招手，表示歡迎加入，但未打動伽羅瓦的心。節錄伽羅瓦寫給奧古斯特·舍瓦烈書信的部分內容如下：¹⁵²

你充滿使徒慈悲的信函，帶給我一絲平安。不過，我感受到的情緒是這麼強烈，我怎麼能泯除殘留的痕跡？……我的快樂沒了，我這輩子永遠沒有快樂，毫無指望了。(節錄自 Mario Livio 著，蔡承志譯：《無解方程式》，頁 176)

你說我再也不能做研究了，真希望你的殘酷預言不是真的。但我要坦承，你說的或許有幾分事實；想當學者的人必須全心投入當個學者。我的情感背棄我的理智。你說：「這令人惋惜！」這點我就不多說了。(節錄自 Mario Livio 著，蔡承志譯：《無解方程式》，頁 176)

6 月 1 日我會來找你。我希望我們在六月的前兩個星期，能多見幾次面。我在 15 日左右要前往多芬(Dauphine)。(節錄自 Mario Livio 著，蔡承志譯：《無解方程式》，頁 176)

該信的附言如下：

我重讀你的來信時，注意到你有一句話，責備我陶醉在曾經玷污我的心、頭、胸和雙手的腐臭氣息之中。這種激烈的責備恐怕在暴力制度擁護者那裡找不到的。陶醉！我對一切，甚至對榮譽的愛好也都感到失望了。我所憎恨的世界怎麼還會玷污我呢？請好好地想一想吧。(節錄自達爾馬斯原著：《伽羅瓦傳》中譯本，頁 45-46)

¹⁵¹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 174-175。

¹⁵² 參考達爾馬斯原著：《伽羅瓦傳》，頁 28-29、44-46；Mario Livio 著，蔡承志譯：《無解方程式》，頁 175-176。

十七、決鬥赴死

在 1832 年 5 月 29 日，即伽羅瓦在赴約決鬥前夕，曾寫下三封信。後人將它們刊載於 1832 年 9 月號的《百科全書派評論》中。

(一)致全體共和派同志

節錄自達爾馬斯著的《伽羅瓦傳》中譯本第三章的這封信部分內容如下：

我請求我的愛國朋友們不要責備我不是為自己的祖國而獻出生命。(中略)。

蒼天作證，我曾經用盡辦法拒絕這場決鬥，只是出於迫不得已才接了挑戰。我後悔對這些不善於冷靜地傾聽真情的人說了招來不幸的實話。但是，我終歸是說了真話。我將帶著不受謊言、不受愛國者的血所沾染的良心到墳墓裏去。

永別了！我已經為公共的幸福獻出了自己大部份的生命。
不要責備殺死我的人。他們是誠摯的.....(頁 47)

(二)給 N.L.和 V.D.兩位朋友

節錄自達爾馬斯原著《伽羅瓦傳》中譯本的部分內容如下：

親愛的朋友們！

有兩個愛國者約我決鬥.....我無法拒絕。

請原諒我沒有通知你們之中的任何一個人。

我的對手們要我提出保證不預先通知任何一位愛國者。

你們的任務很簡單：你們應當證實，我是違背自己的意願而參加決鬥的，也就是說，用盡一切辦法希望和平調解事情之後，才進行決鬥的；你們還應當證實，我對無聊的事，甚至像上述的無聊事，也無善於撒謊。

不要忘了我！因為命運不讓我活到祖國知道我的名字的時候。

我至死還是你們的朋友。(頁 48)

(三)致好友奧古斯特·舍瓦烈

節錄自 Mario Livio 著《無解方程式》一書中的部分譯文如下：

我親愛的朋友，

我已經做出幾項新的解析成果。第一項和方程式理論有關，

其他幾項和積分函數有關。

我研究方程式理論，發現可以用根式求方程式解[得以公式求解]¹⁵³的條件：這樣一來，我得以讓這項理論更顯精闢，也得以描述方程式的所有可能變換，就算不能以公式求解者亦不例外。

上述內容寫成了三篇專論。(中略)

你知道，我親愛的奧古斯特，這幾項主題並沒有道盡我探究發現的全貌。.....我沒有時間了，而我對那個浩瀚領域的見解也尚未充分發展。(中略)

公開徵請雅可比[Carl Gustav Jacob Jacobi 1804-1851 年，德國數學家]或高斯[Carl Friedrich Gauss 1777-1855 年，德國數學家]提供意見，並非為了評斷是非，而是要權衡這些定理的價值輕重。在此之後，我希望有人會覺得釐清這團迷霧可有所得。我衷心擁抱你。(蔡承志譯，頁 179)

伽羅瓦留下科學上極為珍貴的遺產，在方程式論方面，不同於以往探究方程式如何求解，他轉往研究代數結構的方向，創造了 Galois 理論與群論，使近世代數的發展成為數學的一個重要分支。

除了這三封信之外，伽羅瓦還對他的幾篇論文作了一些註解與校正的工作，並且在桌上留有字條，寫著：「還須補充這個論據，但我現在沒時間了。」並標示著「1832 年」。¹⁵⁴

1832 年 5 月 30 日清晨，雙方約在岡提勒的葛拉塞爾湖(Glacier at Gentilly)附近決鬥，伽羅瓦被子彈射中腹部，倒地不起，上午九點多被送到科尚(Cochin)醫院。伽羅瓦的家人當中，只有弟弟阿爾弗雷德(Alfred Galois)接到通知，趕到醫院之後難過不已，伽羅瓦還對弟弟說：「不要哭！我在二十歲就死去，需要全部的勇氣啊！」伽羅瓦在此情況下，可能仍無法忘懷父親之死與牧師間的糾葛，遂表示不想接受牧師的祈禱。在 1832 年 5 月 31 日上午十點左右，伽羅瓦結束了他的一生，時年二十一歲。¹⁵⁵

在數學史上，從未出現這麼年輕就有如此偉大成就的數學家。但很可惜的是，他卻在短暫的一生中，經歷到比別人更多的挫敗遭遇。

伽羅瓦的死訊傳開來，巴黎警方為了防範葬禮可能使許多共和派人士聚集，引起騷動。於是警方從 6 月 1 日起就加強了各項防備，希望在 6 月 2 日所舉行的伽羅瓦葬禮能安然落幕。葬禮當天大約來了兩、三千人，包括他的親朋好友、人民之友會的會友，還有一些大學生，送葬隊伍還受到警方的監

¹⁵³譯者註。

¹⁵⁴參考達爾馬斯原著：《伽羅瓦傳》，頁 29-30；Mario Livio 著，蔡承志譯：《無解方程式》，頁 179-180。

¹⁵⁵參考達爾馬斯原著：《伽羅瓦傳》，頁 30；Mario Livio 著，蔡承志譯：《無解方程式》，頁 180-181；康明昌：《幾個有名的數學問題》，頁 117-118。

視，一路走到巴黎郊區的公墓，伽羅瓦終於在此被埋葬了。¹⁵⁶

伽羅瓦的葬禮總算平和地完成，沒有造成群眾運動。主因是共和派突然接獲另一消息，指拿破崙的將領拉馬克將軍(General Lamarque)在 6 月 1 日逝世。雖然在伽羅瓦的葬禮上仍有一些批評政府的言論，但共和派正醞釀一次更大規模的動員計畫，將在 6 月 5 日拉馬克將軍的葬禮時起義(即法國歷史上 1832 年的「六月暴動」，共造成 800 人喪命)。¹⁵⁷

法國里昂的《先驅報》(*Le Précurseur*)在 6 月 4 日刊載了一篇伽羅瓦辭世的報導。此地方報十分崇尚自由主義，並與人民之友會親近。該篇刊出的部分內容雖有謬誤，但提及與伽羅瓦決鬥的對手是比他年輕的 L.D.，他們曾經是朋友，不忍舉槍互瞄對方，遂以隨機方式決定命運，因只有一把槍配備了子彈，不幸的伽羅瓦終成槍下亡魂。¹⁵⁸

1832 年 9 月，伽羅瓦逝世三個月後，他的好友奧古斯特·舍瓦烈寫了一篇文章，哀悼這位命運多舛的好友伽羅瓦，並在《百科全書派評論》(*Revue Encyclopédique*)發表。顯然，生前最瞭解伽羅瓦的知己，首推奧古斯特·舍瓦烈。¹⁵⁹

十八、遲來的尊榮

伽羅瓦在決鬥的前一天，寫給好友奧古斯特·舍瓦烈的信中，曾提到要請求德國數學家雅可比或高斯，對於這些定理的重要性公開表示看法。舍瓦烈遵照伽羅瓦的遺願，將數學論文寄給他們兩人，但仍沒有接到任何反應。

伽羅瓦的弟弟阿爾弗雷德將伽羅瓦生前留下的所有數學著作手稿，都集中到奧古斯特·舍瓦烈的手中，兩人並加以整理，然而所找的出版商都沒有意願為他出版。舍瓦烈想起伽羅瓦中學時敬愛的理查老師，遂將這些珍貴的遺產交給他，理查老師對這一著作的價值堅信不疑，遂請他的另一位傑出學生埃爾米特善加保存。包括伽羅瓦課堂的十二本筆記手稿，埃爾米特也加以珍藏，經過多年之後才輾轉成為法國科學院的圖書館館藏。¹⁶⁰

直到伽羅瓦逝世十一年以後，法國數學家約瑟夫·劉維(Joseph Liouville 1809-1882 年)從埃爾米特那兒閱讀了伽羅瓦的作品之後，十分敬佩。遂於 1843 年 9 月 4 日，在巴黎科學院上公開宣揚伽羅瓦的研究成就，並於 1846 年將伽羅瓦的著作刊登在《純數學與應用數學》(*Journal de mathématiques pures et appliqués*)雜誌上，這是劉維主編的數學期刊，他向世人引介伽羅瓦精確的理論，並揭示他研究方法的深刻性。在這一刻，才讓世人認清伽羅瓦

¹⁵⁶ 參考達爾馬斯原著：《伽羅瓦傳》，頁 31；Mario Livio 著，蔡承志譯：《無解方程式》，頁 189-190。

¹⁵⁷ Mario Livio 著，蔡承志譯：《無解方程式》，頁 190。

¹⁵⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 30-31；Mario Livio 著，蔡承志譯：《無解方程式》，頁 181-183。

¹⁵⁹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 31；Mario Livio 著，蔡承志譯：《無解方程式》，頁 190。

¹⁶⁰ 參考達爾馬斯原著：《伽羅瓦傳》，頁 6,31；Mario Livio 著，蔡承志譯：《無解方程式》，頁 190。

在數學上的偉大貢獻，也確立了他在數學史上劃時代的地位。¹⁶¹

在伽羅瓦生前，曾指名希望德國數學家雅可比或高斯能提供意見。事隔十多年，雅可比終於在劉維創辦的數學期刊中閱讀了伽羅瓦的遺作，之後就主動聯絡伽羅瓦的弟弟阿爾弗雷德，極力想挖掘伽羅瓦所有的論述。¹⁶²

法國和德國的數學教育，體認到伽羅瓦理論對於數學觀念與思想方法的重要性與前瞻性，率先在 1856 年將伽羅瓦理論正式納入高等代數課程。不過，這時候距離伽羅瓦逝世已經過了二十四年。¹⁶³

巴黎高等師範學院在 1895 年創校一百週年時，由研究群論的挪威數學家索菲斯·李(Sophus Lie 1842-1899 年) 發表了一篇《伽羅瓦對數學發展的影響》的論文，並且將伽羅瓦收錄在《學校百年年鑒》中，他是收錄名單中唯一的數學家兼前校友，顯見該校以此校友為榮。1909 年 6 月 13 日，校長朱爾·坦奈里(Jules Tannery)更親自到伽羅瓦的家鄉故居獻掛紀念扁額，代表校方向這位一代才子致歉，並大力宣揚他的偉大榮耀。¹⁶⁴

19 世紀初伽羅瓦在學術界的出現，宛如夜空中閃過的流星。但他的思想遠遠超越他所生長的時代，因此被學術界一再地漠視；歷經數十年，才像古物出土般被逐漸地發掘。他對近代數學的貢獻與影響，實際上不是流星，而是一顆明亮的恆星！

¹⁶¹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 31-32；Mario Livio 著，蔡承志譯：《無解方程式》，頁 190-191；康明昌：《幾個有名的數學問題》，頁 118。

¹⁶² 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 191。

¹⁶³ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 191。

¹⁶⁴ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 191。

Galois 年譜

西元	年齡	事 紀	備 註
1811		<ul style="list-style-type: none"> • 10.25 深夜，埃瓦里斯特·伽羅瓦(Évariste Galois)在法國距離巴黎 18 公里的布爾拉林(Bourg-la-Reine)小城出生。父親尼古拉-加布瑞爾·伽羅瓦(Nicolas-Gabriel Galois)擔任布爾拉林城內一所男校的校長，母親愛得萊德-瑪利亞·德芒特(Adélaïde-Marie Demante) 出自書香世家。埃瓦里斯特·伽羅瓦(Évariste Galois)家中還有一位姊姊(之後還會有一位弟弟)。 	<ul style="list-style-type: none"> • 法國拿破崙執政時期
1815	4	<ul style="list-style-type: none"> • 伽羅瓦的父親開始擔任布爾拉林的市長，伽羅瓦喜隨父親玩味詩詞；母親則是伽羅瓦在古典文學的啟蒙老師。 	<ul style="list-style-type: none"> • 拿破崙「百日王朝」(3.14 至 6.22)
1823	12	<ul style="list-style-type: none"> • 10 月開始進入巴黎路易大帝皇家中學(lycée Louis-le-Grand)就讀第四級，離家住校，每日作息時間緊湊，排滿各種學習活動。 	
1824	13	<ul style="list-style-type: none"> • 學業成績優異，領取獎學金。 • 10 月就讀中學第三級。 	<ul style="list-style-type: none"> • 1.28 學校對數十名學生直接鐵腕開除。 • 查理十世登基。
1825	14	<ul style="list-style-type: none"> • 學業成績優異，領取獎學金。 • 就讀中學第二級，受耳疾之苦學業成績開始不穩。 	
1826	15	<ul style="list-style-type: none"> • 10 月進到中學第一級，在修辭學進階課程的興趣由濃轉淡，逐漸失去以往的熱忱。 	

1827	16	<ul style="list-style-type: none"> • 1 月被迫從修辭學進階課程降級，重修中學第二級。 • 轉而選讀初級數學的補充課程，發現自己強烈的研究興趣。 • 幾何學方面，由勒讓德爾(Legendre)的《幾何原理》(<i>Elements de Geometrie</i>)教科書，清晰地掌握了基礎幾何的結構與輪廓。 • 代數學方面，對學校教科書不屑一顧，直接去讀拉格朗日(Lagrange)在代數學的著作。 • 10 月第二次就讀中學第一級，再度學習修辭學進階課程。 	
1828	17	<ul style="list-style-type: none"> • 學業成績優異，領取國家考試的獎學金。 • 對於歐拉(Euler)、高斯(Gauss)和雅科比(Jacobi)等人的著作，有相當的認識。 • 提前一年參加綜合理工學院入學考卻落榜。 • 10 月就讀中學最終級，進入高級數學班上課，受理查(Richard)老師啟發，影響甚鉅。 • 耗掉兩個月鑽研五次方程式的解，本以為已導出公式解，後來發現解法有誤，決定跳脫原來的思考，開闢新領域，探討代數方程式是否有解的課題。 	
1829	18	<ul style="list-style-type: none"> • 3 月 1 日在《純粹和應用數學年報》(<i>Annales de mathématiques pures et appliquées</i>)期刊中，發表了第一篇數學論文〈對循環連分數定理的證明〉。 • 受到理查老師的鼓勵，5 月 25 日與 6 月 1 日分別交了兩篇專論給柯西，內容都是關於方程式論的研究，希望提到法國科學院發表。 • 7 月 2 日父親在巴黎的公寓住宅裡自殺身亡。 	

		<ul style="list-style-type: none"> • 8月3日第二度參加巴黎綜合理工學院入學考，仍名落孫山。 • 轉考高等師範學院(<i>École normale</i>)，10月25日以預備生資格錄取入學。 	
1830	19	<ul style="list-style-type: none"> • 1月18日柯西去函科學院致歉，表示因身體不適，未能出席提報伽羅瓦的論文。 • 2月20日正式成為高等師範學院學生，主修科學，領取公費，畢業後要為國家服務。 • 2月底向科學院交《論方程式得以根式求解的條件》(<i>On the conditions That an Equation Be Solvable by Radicals</i>)的論文稿，積極想角逐數學成就大獎。 • 在《菲魯薩克學報》(<i>Ferrusac's Bulletin</i>)四月號發表了一篇獨創理論〈一份有關解代數方程的研究報告〉。 • 伽羅瓦想角逐數學成就大獎的手稿，落到科學院常任秘書傅立葉(<i>Fourier</i>)手中，傅立葉卻不幸於5月16日過世，那篇論文就不見蹤影了。 • 在《菲魯薩克學報》六月號又有兩篇伽羅瓦的作品，分別是〈有關解代數方程的筆記〉及〈有關數論的筆記〉。 • 在高等師範學院認識了學長奧古斯特·舍瓦烈(<i>Auguste Chevalier</i>)和他的哥哥，兩兄弟的思想開啟了伽羅瓦對政治與社會的眼界。 • 不服師範學院校長吉尼奧(<i>M. Guigniault</i>)於「七月革命」時，將師範學院的學生鎖在校園內，禁止參加街頭運動。伽羅瓦在7月28日夜間曾試圖越牆外出，但未成功。 • 在校外加入了「人民之友會」，也參加了「國民自衛軍砲兵隊」，結識了許多校外的異議份子，對政治活動的投入，日益加深。 	<ul style="list-style-type: none"> • 1830年6月法國科學院數學成就大獎由已逝的阿貝爾(<i>Abel</i>)和年輕的雅可比(<i>Jacobi</i>)獲獎。 • 法國在7月的國會選舉中，反對勢力獲壓倒性的勝利。 • 查理十世在7月25日頒布新法令，試圖保住政權。 • 奧爾良派在7月27日呼籲民眾起義，引發「七月革命」。當時許多綜合理工學院的學生也參與，是為「光榮三日」。 • 七月革命共有將近四千人死亡，查理十世下台，流亡英國。

		<ul style="list-style-type: none"> • 12月5日在《學院公報》(<i>La gazette des écoles</i>)所刊出的一篇批評師範學院校長的文章，措詞辛辣，一般人認為是伽羅瓦所寫。 • 12月9日強迫被校長送回家，校長並向教育主管單位作報告。 • 12月30日在《學院公報》寫了一封公開信尋求聲援，但學生們多選擇自保。 	<ul style="list-style-type: none"> • 奧爾良公爵路易-菲利浦於8月9日加冕登基；師範學院校長向臨時政府輸誠。 • 路易-菲利浦於年底解散了國民自衛軍。
1831	20	<ul style="list-style-type: none"> • 1月2日在《學院公報》刊出文章：〈談數學教育的改革—包括教師、教科書和主考官〉。 • 1月8日被路易大帝皇家中學開除。 • 1月18日開始，在索爾奔納街第5號，凱洛特(Caillot)小書舖講授高等代數課程。 • 年初重新向科學院遞交一年前遺失的論文：《方程式得以根式求解的條件》(<i>The Conditions for Resolvability of Equations by Radicals</i>)，並特別附上一篇短箋，請審閱的院士要從頭到尾讀完他的作品。 • 3月31日寫信給科學院院長，說明自己論文的主要內容，並希望今年勿再遺失，能順利向科學院提交。 • 5月9日在布爾根飯店舉辦的大型宴會上，拿著一把匕首舉杯向敬路易-菲利浦祝酒，引起一片譁然。 • 5月10日早上，在母親住處被逮，關進聖佩拉吉監獄裡。 • 6月15日送交法庭審判，以「教唆謀害法國國王的人身與性命未遂罪」被起訴。竇本律師指飯店並非公開場合，不算當眾發表言論，認為被告沒有犯罪行為。法官裁定無罪釋放。 • 7月4日科學院由泊松、拉克魯瓦院士對伽羅瓦的論文提出審查報告，表達尚未能認可。 	<ul style="list-style-type: none"> • 國民自衛軍，有十九名砲手不願解除武裝。4月接受審訊，通稱為「十九人審判案」，最後全體都獲判無罪。 • 人民之友會於5月9日在布爾根飯店舉辦大型宴會，歡慶「十九人審判案」獲判無罪。約有兩百名共和派人士與會。

		<ul style="list-style-type: none"> • 7 月 11 日的科學院會議，否決了伽羅瓦的論文。 • 7 月 14 日中午，和另外一名學生埃內斯特·杜沙特雷在新橋(Pont Neuf)上被逮捕，當晚立即被送到聖佩拉吉監獄。 • 10 月 23 日以「非法著軍服罪」被起訴，外加「攜帶武器」的罪名，出庭受審，被判了九個月的刑期。 • 雖對法院提起上訴，巴黎法院在 12 月 3 日作出最後的判決，裁定維持原判，須在聖佩拉吉監獄繼續服刑。 	<ul style="list-style-type: none"> • 7 月 14 日共和派於巴士底獄廣場發動示威遊行，以紀念法蘭西共和國成立 43 周年。
1832	21	<ul style="list-style-type: none"> • 3 月 16 日獲得假釋，遷移到一間療養院，離開聖佩拉吉監獄，來到西慰佛爾特里埃康復之家(Sieur Faultrier house of health)。 • 認識未滿十七歲的少女史蒂芬妮·迪摩特爾(Stéphanie Potterin du Motel)，初嘗戀愛滋味。 • 4 月 29 日監禁期滿，重獲自由。 • 5 月 29 日赴約決鬥前夕，寫了三封信：(一)致全體共和派同志 (二)給 N.L.和 V.D.兩位朋友 (三)致好友奧古斯特·舍瓦烈。 • 5 月 29 日赴約決鬥前夕，將自己的幾篇論文作了一些註解與校正的工作。 • 5 月 30 日清晨，在岡提勒的葛拉塞爾湖(Glacier at Gentilly)附近與人決鬥，被子彈射中腹部，倒地不起，上午九點多被送到科尚(Cochin)醫院。 • 5 月 31 日上午十點左右，結束了一生，時年二十一歲。 	<ul style="list-style-type: none"> • 歐洲在春天爆發霍亂的大流行。

第三章 Galois 理論探討

早在 16 世紀時，以具體數字為係數的方程式，無論形式或次數多麼複雜，數學家已能求得解的近似值。但對於以字母作為係數的一般方程式，並不適合以近似值求解，只能尋求公式解。終於在數學家的努力下，一次、二次、三次以及四次的一般方程式都找到了公式解，而這些解的型態完全是以係數的加、減、乘、除和開方所造成，稱之為「根式解」。¹⁶⁵

19 世紀的數學，無論是在代數、幾何或分析上，都顯現出一些叛逆的性格，傳統的路線不再是唯一的選擇，追求革新的思潮逐漸興起。¹⁶⁶

伽羅瓦在中學時曾研讀過拉格朗日的著作《代數方程式分解和解析函數理論》(Resolution of Algebraic Equations and Theory of Analytic Functions)。拉格朗日考慮將方程式的根進行置換的想法，觸動了伽羅瓦的靈感，即將開拓出代數的一片新天地。¹⁶⁷

對於擱淺許久的五次一般方程式的解法，拉格朗日極力尋求突破，卻仍沒有進展。雖然阿貝爾終於證明出：「五次一般方程式不可能以係數的四則運算和開方法得其解」，但伽羅瓦卻找到一個判斷準則，可判定任意五次或更高次方程式是否可用根式表出其解？伽羅瓦的這個發現，比阿貝爾的結論更具主動性與高度，意義也更廣。¹⁶⁸

本章將深入探討 Galois 理論，文中所提到的體都是指特徵值為零的體，共分為二節：第一節為「思維的進路」，第二節為「理論的應用」。

第一節 思維的進路

數學研究源自於發現問題，目的在於解決問題，其所使用的研究方法必定有數學思想在支撐著。節錄自張雄、李得虎編著的《數學方法論與解題研究》一書中，對於數學思想的描述如下：

數學思想是在數學研究活動中的根本想法，是對數學對象的本質認識，是對具體的數學知識和方法做更進一步的認識過程中提煉概括形成的一般性觀點。(頁 6)

¹⁶⁵ 參考達爾馬斯原著：《伽羅瓦傳》，頁 35。

¹⁶⁶ 參考袁小明編著：《數學史》，頁 210。

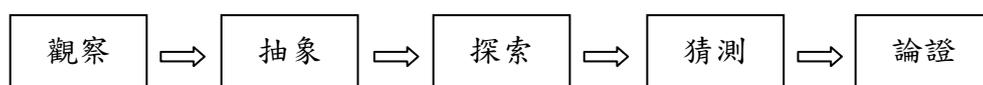
¹⁶⁷ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 149。

¹⁶⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 38；Mario Livio 著，蔡承志譯：《無解方程式》，頁 151；袁小明編著：《數學史》，頁 208。

伽羅瓦的思想相當獨特，充滿真知灼見，在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本曾記述著：

伽羅瓦對煩瑣累贅的計算方法感到不可抑制的厭惡，因此，他的表述極其簡單扼要。但是他所寫的一切，都因為具有數學家不倦鑽研的思想而放出異彩；他的每一部著作，彷彿都是一次新的大膽的躍進；先前已達到的又落到後面，不再使作者發生興趣了。伽羅瓦的洞察力是驚人的。(頁 33)

數學思想主要是由數學的思維方式所帶動。以下將針對數學思維方式的五個重要環節：觀察、抽象、探索、猜測、論證，¹⁶⁹來認識 Galois 理論的形成。



數學思維方式的五個重要環節

一、觀察

觀察是指主體通過感官對客體的認識過程。在張雄、李得虎所編著的《數學方法論與解題研究》一書中，記載著：

在心理學中，觀察被看做是一種有目的、有計劃、有步驟的感知活動，是一種主動的、對思維起積極作用的感知活動。(頁 22)

伽羅瓦為了探尋五次方程式是否有根式解，觀察方程式的所有解的屬性，找到了關鍵的原因，說明如下：

(一)對稱性

以 Galois 理論的創立而言，最初是為了尋求高次代數方程式的求解公式，這個問題困擾數學家達兩百多年之久。伽羅瓦就是觀察者，也是主體；「高次代數方程式能否用根式表出其解？」是客體。伽羅瓦對這個問題進行解剖與觀察，發現以往總是以方程式的次數作為分類標準，其實只掌握到外觀的形式，並沒有抓住方程式的內在本體，而主控內在本體的精髓卻是「方程式解的對稱性」。

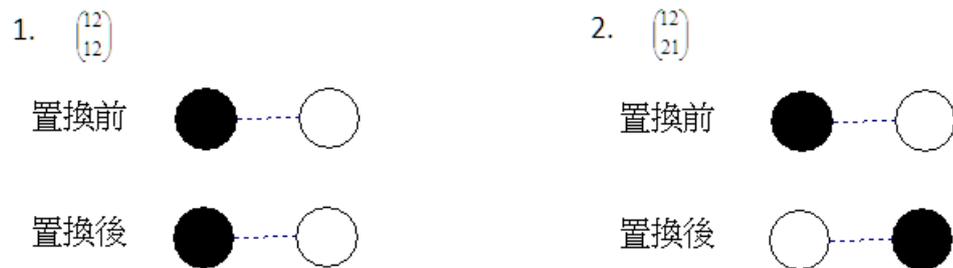
在 Mario Livio 所著，蔡承志譯的《無解方程式》一書中提到：

¹⁶⁹參考丘維聲著：《數學的思維方式與創新》，頁 1。

在伽羅瓦之前，方程式一律依次方數歸類，如二次、三次、五次等。伽羅瓦發現，對稱性是更重要的方程式特性。根據次方數來把方程式分門別類，就像依尺寸來把玩具盒裡的木頭積木分門別類。伽羅瓦想出依對稱性來區分方程式類別，這相當於領悟到，積木更重要的基本特性是形狀——圓形、方形或三角形。(頁 211)

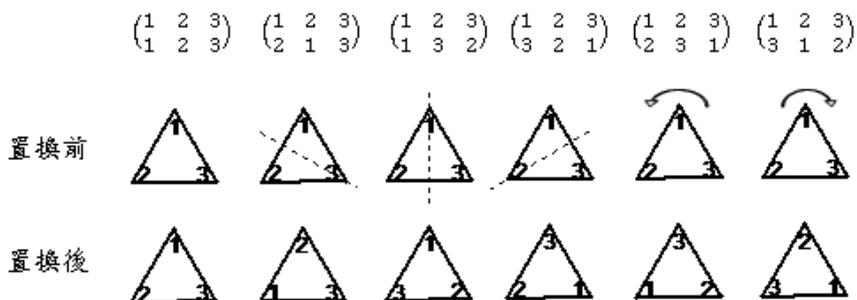
一般的對稱性表現，常見於二度空間的平移、旋轉、鏡射和滑移鏡射，或是三度空間的螺旋對稱，這些都屬於幾何變換；而對於任何事物或概念進行置換排列，也是對稱性的另一種形式表現。¹⁷⁰

以兩個物件(1 代表黑、2 代表白)為例，只有兩種置換： $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ 與 $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ 。第一種是單位置換，保持原狀；第二種是兩者互換位置。有時候我們將這兩種置換記為 e 及(1 2)。如下圖：



再以正三角形為例，三個頂點分別以 1、2、3 代表，將其位置交換，得到 3!種(即 6 種)置換，分別是 $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ 、 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 、 $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ 、 $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ 、 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ 、 $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ 。其中第一種是單位置換，保持原狀；第二、第三及第四種各將其中兩頂點對換了一次；最後兩種則是進行了兩次對換頂點的結果。有時候我們將這六種置換依序記為 e、(1 2)、(2 3)、(1 3)、(1 2 3)、(1 3 2)。觀察下圖，應可感覺到它們所散發出來的對稱性格，有原封不動、鏡射、旋轉等。

¹⁷⁰ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 35-36。



(二) 方程式的專屬群

由代數基本定理知道：一元 n 次方程式恰有 n 個解。若這 n 個解都是相異的，將這 n 個解進行重排，則會有 $n!$ 種置換產生，形成一個群。

但每一個方程式都會服從於某些「預解式」，這些預解式是由方程式的推定解(因可能尚未得其解，暫稱為推定解)所形成。例如 $x^2 + ax + b = 0$ 的推定解為 x_1 、 x_2 ，則 $x_1 + x_2 = -a$ ， $x_1x_2 = b$ 都是預解式；又如 $x^4 + x^3 + x^2 + x + 1 = 0$ 有四個推定解 x_1 、 x_2 、 x_3 、 x_4 ，則 $x_1x_2x_3x_4 = 1$ 也是其中一個預解式。¹⁷¹拉格朗日就曾經試圖以低於原方程式次數的預解式找解，但沒有成功。

如前述， n 次方程式的 n 個相異解會有 $n!$ 種置換。將這 $n!$ 種置換作用在所有的預解式，可能某些置換已開始違逆當中的預解式了；但有一批忠誠的置換，卻仍永遠服從於所有的預解式(無論所列出的預解式有多少個!)，將這一批忠心耿耿的置換聚集起來，就產生了一個置換群，就是此方程式專屬的「Galois 群」。

伽羅瓦一定嗅到每一個 Galois 群中，各個置換之間也存在著某些對稱關係，這樣獨到的觀點，使他造就出更豐沛的理論。因此，Galois 群稱得上是方程式對稱性的代言人。

例如假設二次方程式 $x^2 + ax + b = 0$ 的解為 x_1 、 x_2 ，將 x_1 、 x_2 進行重排，得到兩種置換： $\begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix}$ 、 $\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}$ 。預解式 $x_1 + x_2 = -a$ ， $x_1x_2 = b$ 在 $\begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix}$ 單位置換下必然不變；在 $\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}$ 置換下得 $x_2 + x_1 = -a$ ， $x_2x_1 = b$ ，仍然成立。因此， $x^2 + ax + b = 0$ 的 Galois 群就是包括兩種置換的 $\left\{ \begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix} \right\}$ 。¹⁷²

換句話說，當數學家們觀察二次、三次、四次方程式的求解公式，試圖找出更高次方程式求解線索時，伽羅瓦承續了拉格朗日所看見卻未

¹⁷¹參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 151。

¹⁷²參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 211。

竟的成果。他明確地觀察到：「方程式解的排列理論」就是整個問題的核心，而每一個方程式的 Galois 群都有其個別的對稱特性。¹⁷³

在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本，記述了伽羅瓦在聖佩拉吉監獄所寫的研究報告中的一段話，就可看出他對研究的路線所抱持的自信，如下：

使計算聽命於自己的意志，把數學運算歸類，學會按照難易程度，而不是按照它們的外部特徵加以分類——這就是我所理解的未來數學家的任務，也是我所要走的道路。(頁 56)

伽羅瓦除了在研究問題時有如上驚人的洞察力之外，他對科學的觀察也是超越一般人的。在聖佩拉吉監獄所寫的研究報告中，還敘述了一段深具遠見的看法，仍節錄自達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本：

從最先進的數學家們致力於求得嚴整性這一確定不移的事實中，可以有把握地作出結論說，同時掌握幾種運算的必要性變得越來越迫切了，因為人的智力沒有足夠的時間來詳細研究細節。(頁 56)

對照今日的科學發展，伽羅瓦已經看到「同時掌握幾種運算的必要性」是未來世界的常態，他的感知活動的確領先於同時期的研究。

二、抽象

抽象是指從眾多的事件當中，抽取共有的、本質性的特徵和屬性，並捨棄非本質的內容。若以數學方式進行抽象思維，可將不重要的細節省略或剔除，只把最重要的觀點展現出來；而展現的方法是從各種不同的情境中，找到它們共同的關係、結構或模式。

伽羅瓦為了揭開高次方程式的神秘面紗，他抓住了方程式解最重要的本質乃「解的對稱性」這個特徵。但這個共同的特徵隱藏在方程式的 Galois 群中，因此有必要將置換群抽離出來研究，找出組成元素的關係，明白整體的結構，以建立可遵循的模式。伽羅瓦從方程式解進化到群的研究，就是抽象思維的表現。

「群」(Group)有聚集、會合的意思，更有依照類別區分的意涵。伽羅瓦所討論的置換群是最早被認識的群，它的組成「元素」是幾個文字所產生的置換，而一個置換接續一個置換的動作可視為「運算」，因此群中元素經過運算後仍是群中元素。當時尚未有抽象群的定義，但伽羅瓦對於這樣的運算，

¹⁷³ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 151；袁小明編著：《數學史》，頁 208。

制定了一些定律作為規範，如此建立了一個有結構的集合，就稱為「置換群」。

174

在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本，就記載著：

群的概念是在伽羅瓦著作提出之前不久才出現的。但是在他那個時代，它却像是一個沒有靈魂的軀體，是偶爾出現在數學上的、人為臆斷的大量概念之一。(中略)，群是具有某種共同特性的對象的總和...。(頁36)

伽羅瓦曾經在中學時，耗費兩個月時間找尋五次方程式的公式解，從繁複的計算當中，洞悉了方程式求解的本質。¹⁷⁵之後，伽羅瓦懂得跳脫，他在分析問題時，不再倚賴計算，只求預知該如何計算就好了。換句話說，他的重點著重在：研究什麼情況下會遇到方根的出現？在這個明確的目標下，他進到置換群中進行更深入的研究。

(一) 正規子群

如果把 n 個文字進行重排，形成的群稱為 n 元對稱群，記成 S_n ，而 S_n 的子群就稱為置換群，因此 S_n 本身也是個置換群。很容易發現：在 n 大於 2 時， S_n 都不會是交換群。

伽羅瓦在研究置換群時，巧妙地運用了一種名為「正規子群」(Normal Subgroup)的神奇寶貝，透過它不僅透視了整個置換群，也完成了重要的使命。

正規子群其實也是子群的一種，它的特色是「左陪集和右陪集完全相同」，讓我們來認識它。即若 G 是一個群，假設「乘」代表其運算， H 是它的一個子群。將 G 中任一元素 a 左乘 H 中的每個元素，會得出一個集合，這個集合所含的元素個數恰好和 H 一樣多，以 aH 表示，稱為左陪集；同樣地，也可將 a 右乘 H 中的每個元素，得右陪集 Ha 。通常 aH 不一定和 Ha 相同，但如果 H 是正規子群，它可以讓每一個 G 中元素 a ，獲得 $aH=Ha$ 的保證。這就是正規子群最可愛的地方。

值得一提的是，每一個群 G 至少有兩個正規子群，一個是僅有單位元素的 $\{e\}$ ，另一個就是 G 本身。若 H 為 G 的正規子群且 G 是交換群時， aH 中的每一個元素 ah 必與 ha 相同；若 H 為 G 的正規子群且 G 是不可交換群時， aH 中的每一個元素 ah 必與 Ha (也是 aH)內某一元素 $h'a$ 相同。

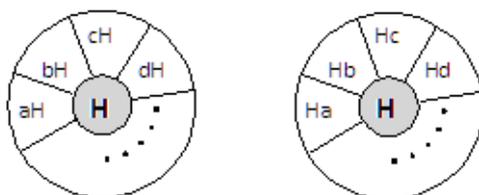
當 H 為 G 的子群，且 G 有 n 個元素， H 有 m 個元素，因為子群元素個數必是母群元素個數的因數，所以 m 是 n 的因數。又因為 H 的每一個左陪集或右陪集所含的元素個數都與 H 的元素個數一樣多(即 m 個)，所

¹⁷⁴ 參考袁小明編著：《數學史》，頁 210-212。

¹⁷⁵ 參考康明昌：《幾個有名的數學問題》，頁 88。

以 H 的左陪集個數和右陪集個數相同，都是 $(n \div m)$ 個。

雖然 G 可裂解成 $(n \div m)$ 個 H 的左陪集的拼圖， G 也可裂解成 $(n \div m)$ 個 H 的右陪集的拼圖，卻只有在 H 為 G 的正規子群時，兩者的裂解方式才會完全相同。對於母群 G ，只有正規子群能在左、右陪集的分割上達成一致；也就是 G 中的元素都被分配到各自歸屬的隊伍，而且不論是在左陪集或右陪集的整隊之下，屬於同一隊的成員永遠都會在同一隊中。



正規子群的左陪集與右陪集完全相同

以三元對稱群 $S_3 = \{e, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ 為例， $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ 是其子群。可檢驗得 $eH = He = H$ ， $(1\ 2\ 3)H = H(1\ 2\ 3) = H$ ， $(1\ 3\ 2)H = H(1\ 3\ 2) = H$ ； $(1\ 2)H = H(1\ 2) = \{(1\ 2), (2\ 3), (1\ 3)\}$ ， $(2\ 3)H = H(2\ 3) = \{(1\ 2), (2\ 3), (1\ 3)\}$ ， $(1\ 3)H = H(1\ 3) = \{(1\ 2), (2\ 3), (1\ 3)\}$ 。因此 H 是 S_3 的一個正規子群，並且 S_3 的六個元素可被正規子群 H 分成兩隊： e 、 $(1\ 2\ 3)$ 、 $(1\ 3\ 2)$ 都在 H 中； $(1\ 2)$ 、 $(2\ 3)$ 、 $(1\ 3)$ 都在另一隊。

(二) 合成因子

由前述知，若母群有 n 個元素，它的一個正規子群有 m 個元素，則可產生左(右)陪集個數是 $(n \div m)$ 個，這個整數稱為「合成因子」。今假設母群 G 中，找到一個極大的正規子群 H_1 (不可以是 G)，合成因子為 p_1 ； H_1 中又找到一個極大的正規子群 H_2 (不可以是 H_1)，合成因子為 p_2 ；...，以此類推，繁衍下去，直到某個 $H_k = \{e\}$ 。這個極大正規子群家族代代所產生的關聯，可寫下連串的合成因子列 (p_1, p_2, \dots, p_k) ，這串合成因子列正好可作為母群 G 的家族族譜。¹⁷⁶特別值得一提的是： G 的家族族譜排列順序可能更動，不過卻一定是這 k 個數的排列。

伽羅瓦細心地推敲，發現這個族譜隱藏著上帝的密碼，它竟然是牽動著方程式產生根式解的源頭。¹⁷⁷

再來看 n 元對稱群 S_n ，因每一個 S_n 中的奇置換與偶置換各佔一半，我們將所有偶置換(對換偶數次)所形成的子群稱為 S_n 的交錯子群，以 A_n 表示，那麼 A_n 的元素個數是 $\frac{n!}{2}$ 個，並且也很容易檢驗 A_n 是 S_n 的一個極

¹⁷⁶ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 212-213。

¹⁷⁷ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 212-213。

大正規子群。

例如： $S_3 = \{e, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ ， $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ 是 S_3 的極大正規子群，可知第一代的合成因子是 $6 \div 3 = 2$ ；又 A_3 的極大正規子群是 $\{e\}$ ，則第二代的合成因子是 $3 \div 1 = 3$ 。綜合上述， S_3 的極大正規子群家族繁衍出 S_3 、 A_3 、 $\{e\}$ ，其合成因子列為 $(2, 3)$ 。

進一步探討 S_4 ，它共有 $4! = 24$ 個元素，而 A_4 是 S_4 的一個極大正規子群，且 A_4 有 12 個元素，可知第一代的合成因子是 $24 \div 12 = 2$ ；在 A_4 當中又可找到一個極大正規子群 $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ ， K 有 4 個元素，則第二代的合成因子是 $12 \div 4 = 3$ ；在 K 中再找到一個極大正規子群 $H = \{e, (1\ 2)(3\ 4)\}$ ， H 有 2 個元素，則第三代的合成因子是 $4 \div 2 = 2$ ；最後， H 的極大正規子群只能是 $\{e\}$ ，則第四代的合成因子是 $2 \div 1 = 2$ 。綜合上述， S_4 的極大正規子群家族繁衍出 S_4 、 A_4 、 K 、 H 、 $\{e\}$ ，其合成因子列為 $(2, 3, 2, 2)$ 。

伽羅瓦用抽象的觀點研究方程式解，選擇了分析「群」的結構，因為他的努力，使群的概念深入數學中，扮演了相當重要的角色。以下是節錄自達爾馬斯(Andre Dalmás)著《伽羅瓦傳》中譯本的記載：

群的概念的建立，使數學家們擺脫了研究大量的、各式各樣的理論的繁重負擔。原來人們只要指出這些理論是可能的就行了。由於這些理論就其本質而言都是十分類似的，所以用同樣一句話就足以表白它們。
(頁 38-39)

同樣在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本有另一段記載，看到群論成為數學的一個分支，聯繫著科學各領域的發展：

伽羅瓦的「群」，...，一再表明，確定新聯繫在科學上會起著多大的作用。其中每一項發現都標誌著科學家所使用的語言的重要改進。(頁 39)

伽羅瓦秉持著先人開疆拓土的精神，為數學發展覓得一片優聖美地。

三、探索

探索是為解決疑問，多方尋求答案的研究過程。就好比前方的道路不確定，必須摸石過河一般。在數學上經常用到分析、歸納、類比，甚至直覺、聯想等方法進行探索。以下就一步一步來探索 Galois 理論的基本定理如何建立起來：

(一) 分裂體

對於任何一個多項式 $f(x)$ ，如果它的各項係數都落在體 F 中，則用 $f(x) \in F[x]$ 表示。在此我們只討論特徵值為零的體，例如 \mathbb{Q} 、 \mathbb{R} 、 \mathbb{C} 等，而不討論 \mathbb{Z}_2 、 \mathbb{Z}_5 等特徵值不為零的體。因此，若看到 $f(x) \in \mathbb{Q}[x]$ ，就代表 $f(x)$ 的所有係數都是有理數體 \mathbb{Q} 中的元素。

要認清 n 次方程式 $f(x)=0$ 的所有解，必須作一些建構的工作。若 $f(x) \in F[x]$ ，且 $f(x)=0$ 的所有解為 x_1, x_2, \dots, x_n ，則我們建構一個更高階的體為 $F(x_1, \dots, x_n)$ ，它是由體 F 結合 $f(x)=0$ 的所有解所構築生成的新體，而且是包含 F 和 $\{x_1, \dots, x_n\}$ 的最小體，將 $F(x_1, \dots, x_n)$ 稱為 $f(x)$ 在 F 上的分裂體 (Splitting Field of $f(x)$ over F)。

這個新體 $F(x_1, \dots, x_n)$ 也是一個體，今若將 $f(x)$ 視為新體 $F(x_1, \dots, x_n)$ 上的多項式時， $f(x)$ 可寫成一次式的乘積，型如 $f(x) = k(x-x_1)(x-x_2)\dots(x-x_n)$ ，其中 $k \in F \subseteq F(x_1, \dots, x_n)$ 。也就是說， $f(x)$ 在新體 $F(x_1, \dots, x_n)$ 上會毫無保留地裂解開來。

這個新體該如何構築呢？先從添加一個元素看起。若 $\alpha \in F$ ，結合體 F 和 α 所構成的體 $F(\alpha)$ 仍然是 F ；而若 $\alpha \notin F$ ，在體 F 上加進這個外來元素 α

所構成的體，實際上可表成 $F(\alpha) = \left\{ \frac{f_1(\alpha)}{f_2(\alpha)} \mid f_1(x), f_2(x) \in F[x], f_2(\alpha) \neq 0 \right\}$ 。

不難理解，當 $f(x)=0$ 的所有解為 x_1, x_2, \dots, x_n 時， $f(x)$ 在 F 上的分裂體 $F(x_1, \dots, x_n) = F(x_1, \dots, x_{n-1})(x_n) = F(x_1, \dots, x_{n-2})(x_{n-1})(x_n) = \dots = F(x_1)(x_2)\dots(x_n)$ 。

先以次數較低的多項式來認識分裂體。例如 $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ ， $f(x)=0$ 的兩個解是 $x = \sqrt{2}, -\sqrt{2}$ ，則 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$ ，又 $-\sqrt{2}$ 是 $\sqrt{2}$ 的加法反元素， $-\sqrt{2}$ 原本就在 $\mathbb{Q}(\sqrt{2})$ 中，因此分裂體可簡寫為 $\mathbb{Q}(\sqrt{2})$ ，它的每一個元素都可表為 $\frac{m+n\sqrt{2}}{p+q\sqrt{2}}$ ，其中 $m, n, p, q \in \mathbb{Q}$ ，且 $p+q\sqrt{2} \neq 0$ 。事實上， $\mathbb{Q}(\sqrt{2})$ 的每一個元素也可以經過分母有理化寫成 $a+b\sqrt{2}$ ，其中 $a, b \in \mathbb{Q}$ 。即 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2}) = \left\{ \frac{m+n\sqrt{2}}{p+q\sqrt{2}} \mid m, n, p, q \in \mathbb{Q}, \text{ 且 } p+q\sqrt{2} \neq 0 \right\} = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 。

再舉一例， $g(x) = x^3 + 1 = (x+1)(x^2 - x + 1) \in \mathbb{Q}[x]$ ， $g(x)=0$ 的三個解是 $x = -1, \frac{1 \pm \sqrt{3}i}{2}$ ，則 $g(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}\left(-1, \frac{1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}\right) = \mathbb{Q}\left(\frac{1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}\right) = \mathbb{Q}(\sqrt{3}i) = \left\{ \frac{m+n\sqrt{3}i}{p+q\sqrt{3}i} \mid m, n, p, q \in \mathbb{Q}, \text{ 且 } p+q\sqrt{3}i \neq 0 \right\} = \{a+b\sqrt{3}i \mid a, b \in \mathbb{Q}\}$ 。

以上兩個例子中， $f(x) \in \mathbb{Q}[x]$ 是 \mathbb{Q} 上的既約多項式 (Irreducible Polynomial)；而 $g(x) \in \mathbb{Q}[x]$ 可分解為 $(x+1)$ 和 (x^2-x+1) 的乘積，所以 $g(x)$ 不是 \mathbb{Q} 上的既約多項式。要深入探討 Galois 理論，我們著眼於既約多項式。若能瞭解每一個既約多項式的分裂體，再拓展至任何多項式的分裂體並不困難。例如 $h(x) = h_1(x)h_2(x) \in \mathbb{Q}[x]$ ，其中 $h_1(x)$ 、 $h_2(x)$ 為 \mathbb{Q} 上的既約多項式，若我們得到 $h_1(x) \in \mathbb{Q}[x]$ 的分裂體為 $\mathbb{Q}(\alpha_1, \dots, \alpha_m)$ ， $h_2(x) \in \mathbb{Q}[x]$ 的分裂體為 $\mathbb{Q}(\beta_1, \dots, \beta_n)$ ，則 $h(x) \in \mathbb{Q}[x]$ 的分裂體就是 $\mathbb{Q}(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ 了。

(二) 體的擴展

任何體 F ，加進外來元素以構築生成新體 E ，就是一個體的擴展，以 E/F 表示，此時也稱 E 為 F 的擴展體 (Extension field of F)，而 F 稱為 E 的一個子體 (Subfield)。例如 \mathbb{C}/\mathbb{R} 、 \mathbb{R}/\mathbb{Q} 、 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 、 $\mathbb{Q}(\sqrt[3]{2}, \frac{-1+\sqrt{3}i}{2})/\mathbb{Q}$ 、 $\mathbb{Q}(\pi)/\mathbb{Q}$ 都是體的擴展。因此，若 $f(x) \in F[x]$ 在 F 上的分裂體是 E ，則 E/F 也是一個體的擴展。

當我們在體 F 上加進單一元素 α 時，稱 $F(\alpha)/F$ 為單擴展。如果 α 是某個方程式的根，且這個方程式的所有係數屬於 F ，則 α 是 F 上的代數元，稱 $F(\alpha)/F$ 是單代數擴展；否則，稱 $F(\alpha)/F$ 是單超越擴展。

不過，單代數擴展或單超越擴展完全取決於給定的體。例如 $2\pi i$ 在實數體 \mathbb{R} 上為代數元，但 $2\pi i$ 在有理數體 \mathbb{Q} 上卻是超越元！

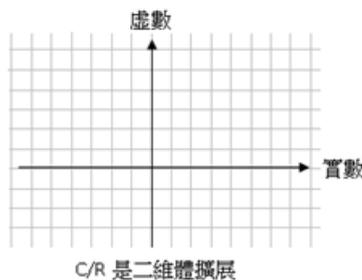
為了認識 Galois 理論，如果沒有特別說明，我們將以加進代數元的體擴展進行討論，而對於加進超越元的體擴展較少關注。

想從一塊土地上蓋房子，須打穩地基，進行空間規劃，建立樑柱結構，方能搭築成形；在體的擴展當中，也經歷類似的過程。當體 E 為體 F 的擴展體時，也就是 E/F ， E 可視為一個佈於 F 上的向量空間，其維度以 $[E:F]$ 表示。如果 $[E:F] < \infty$ ，稱 E/F 是有限的體擴展；當存在 E/K 且 K/F 時，還可得到 $[E:F] = [E:K][K:F]$ 的結論。

而若 α 為 F 上的代數元，即 $F(\alpha)/F$ 為單代數擴展時， $F[x]$ 中唯一存在一個最能表現 α 的內涵與精神的既約多項式，設為 $m(x) \in F[x]$ ，它的首項係數是 1，且 $m(x) = 0$ 是以 α 為根的最低次方程式，我們稱 $m(x)$ 為 α 在 F 上的最小多項式 (the minimum polynomial)。此時，若最小多項式的次數為 n ，則 $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ 可為 $F(\alpha)$ 在 F 上向量空間的一組基底，體擴展維度 $[F(\alpha):F] = \deg(m(x)) = n$ (即 α 在 F 上的最小多項式的次數)。

先看兩個單擴展的例子。例如 $\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$ ，且 i 在實數體 \mathbb{R} 上的最小多項式是 $x^2 + 1$ ，因此 $\{1, i\}$ 是 \mathbb{C} 佈於 \mathbb{R} 上向量空間的一組基底， $[\mathbb{C}:\mathbb{R}] = \deg(x^2 + 1) = 2$ 。又如 $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ ，且 $\sqrt[3]{2}$ 在有理數體 \mathbb{Q} 上的最小多項式是 $x^3 - 2$ ，因此 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ 是 $\mathbb{Q}(\sqrt[3]{2})$ 佈於 \mathbb{Q} 上的向量空間的一組基底， $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$

$$= \deg(x^3 - 2) = 3。$$



再看另一個體擴展的例子。若 $\omega = \frac{-1+\sqrt{3}i}{2}$ ，如何找尋 $[Q(\sqrt[3]{2}, \omega) : Q]$ 呢？因為 ω 是 $x^2 + x + 1 = 0$ 的一個解， ω 在 $Q(\sqrt[3]{2})$ 上的最小多項式是 $x^2 + x + 1$ ，則 $[Q(\sqrt[3]{2}, \omega) : Q] = [Q(\sqrt[3]{2}, \omega) : Q(\sqrt[3]{2})] \times [Q(\sqrt[3]{2}) : Q] = 2 \times 3 = 6$ ，且 $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$ 可作為 $Q(\sqrt[3]{2}, \omega)$ 佈於 Q 上的向量空間的一組基底。

至於若 α 為 F 上的超越元，即 $F(\alpha)/F$ 為單超越擴展時， $1, \alpha, \alpha^2, \dots$ 為線性獨立，對於每一個正整數 n ， $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ 都可作為 $F(\alpha)$ 佈於 F 上的向量空間基底的一部分，所以 $[F(\alpha) : F] = \infty$ 。例如 π 是 Q 上的超越元，則 $[Q(\pi) : Q] = \infty$ 。

而 $[R : Q]$ ，可想像 R 中有無限多個無理數(如 $\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots$ 或其他超越數)，有些是 Q 上的代數元，有些是 Q 上的超越元，僅看 R 中佈於 Q 上的超越元就有無限多個，且彼此為線性獨立，因此 $[R : Q] = \infty$ 。

回到 Galois 理論要探究的主題，必須瞭解方程式的所有解所處的環境；分裂體是這些所有解的「居所」，它和原本方程式的係數所屬的體有多少維度的落差？這一點的確必須分辨清楚。以下列舉三個例子作說明：

例1 $f(x) = x^4 - x^2 + 1 \in Q[x]$ ，由 $f(x) = (x^4 + 2x^2 + 1) - 3x^2 = (x^2 + 1)^2 - (\sqrt{3}x)^2$
 $= (x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1)$ ，得 $f(x) = 0$ 的解為 $x = \frac{-\sqrt{3} \pm i}{2}, \frac{\sqrt{3} \pm i}{2}$ 。

因此 $f(x)$ 在 Q 上的分裂體為 $Q(\frac{-\sqrt{3}+i}{2}, \frac{-\sqrt{3}-i}{2}, \frac{\sqrt{3}+i}{2}, \frac{\sqrt{3}-i}{2}) = Q(\sqrt{3}, i)$ ；

此時 $[Q(\sqrt{3}, i) : Q] = [Q(\sqrt{3}, i) : Q(\sqrt{3})][Q(\sqrt{3}) : Q] = 2 \times 2 = 4$ ，

且 $\{1, \sqrt{3}, i, \sqrt{3}i\}$ 可作為其向量空間的一組基底。

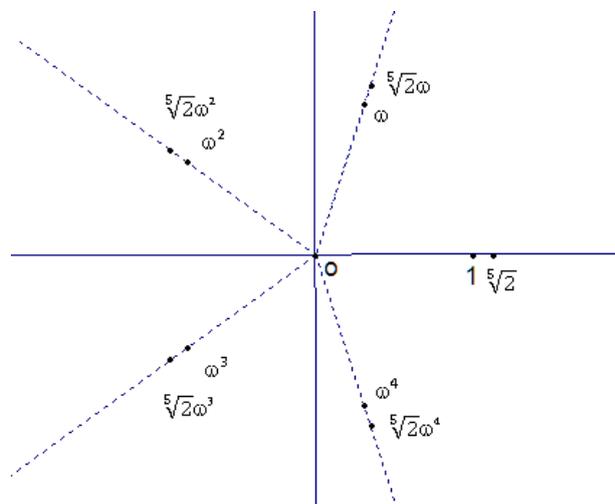
例2 當 p 為質數時， $f(x) = x^p - 1 \in \mathbb{Q}[x]$ ， $f(x) = 0$ 的解為 $1, \omega, \omega^2, \dots, \omega^{p-1}$ ，

其中 $\omega = e^{\frac{2\pi i}{p}} = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ ，因此 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(1, \omega, \omega^2, \dots, \omega^{p-1}) = \mathbb{Q}(\omega)$ ；又 ω 滿足 $x^{p-1} + x^{p-2} + \dots + x + 1 = 0$ ，且 $x^{p-1} + x^{p-2} + \dots + x + 1$ 是 $\mathbb{Q}[x]$ 中的既約多項式，所以 ω 在 \mathbb{Q} 上的最小多項式是 $x^{p-1} + x^{p-2} + \dots + x + 1$ ，此時 $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ 。

附帶說明：若 $n \in \mathbb{N}$ ，因 $x^n = 1$ 的解為 $1, \omega, \omega^2, \dots, \omega^{n-1}$ （其中 $\omega = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ ），則 $x^n = a$ （其中 $a > 0$ ）的解為 $\sqrt[n]{a}, \sqrt[n]{a}\omega, \sqrt[n]{a}\omega^2, \dots, \sqrt[n]{a}\omega^{n-1}$ 。所以，當 $a > 0$ 時， $g(x) = x^n - a \in \mathbb{Q}[x]$ ， $g(x) = 0$ 的所有解為 $x = \sqrt[n]{a}, \sqrt[n]{a}\omega, \sqrt[n]{a}\omega^2, \dots, \sqrt[n]{a}\omega^{n-1}$ ，其中 $\omega = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ 。

例3 $f(x) = x^5 - 2 \in \mathbb{Q}[x]$ 。 $f(x) = x^5 - 2 = 0$ 的解為 $x = \sqrt[5]{2}, \sqrt[5]{2}\omega, \sqrt[5]{2}\omega^2,$

$\sqrt[5]{2}\omega^3, \sqrt[5]{2}\omega^4$ ，其中 $\omega = e^{\frac{2\pi i}{5}} = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$ ，則 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt[5]{2}, \omega, \omega^2, \omega^3, \omega^4) = \mathbb{Q}(\sqrt[5]{2}, \omega)$ ；此時 $[\mathbb{Q}(\sqrt[5]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}, \omega) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 5 \times 4 = 20$ 。（因為 5 為質數，由例 2 知 $x^4 + x^3 + x^2 + x + 1$ 是 ω 在 \mathbb{Q} 上的最小多項式，可得 $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ 的結果。）

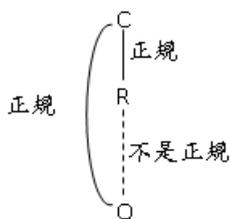


(三)正規擴展

體的擴展也是五花八門、琳瑯滿目。但有一種體的擴展比較特殊，將它稱為「正規擴展」(Normal Extention)，它像獲得認證一般，屬於擴展健全的品牌。

所謂 E/F 為正規擴展(或稱 E 為 F 的正規擴展體)，意指：不僅 E/F 是一個體的代數擴展，且任何 $F[x]$ 中的既約多項式 $f(x)$ ，只要 $f(x)=0$ 在 E 中有一解，則其所有解都會在 E 中被找到。意即 E/F 這個體的擴展中， E 對待 $F[x]$ 中所有的既約多項式 $f(x)$ ，堅持一個基本態度，就是：若 E 要接納 $f(x)=0$ 的其中一個解， E 就要收容它的所有解。(愛屋及烏！)

由代數基本定理，可知 C/Q 、 C/R 都是正規擴展，但 R/Q 就不是正規擴展了。例如 $f(x)=x^3-2 \in Q[x]$ 為既約多項式，且 $f(x)=0$ 的解為 $x=\sqrt[3]{2}$ 、 $\sqrt[3]{2}\omega$ 、 $\sqrt[3]{2}\omega^2$ ，其中 $\omega^2+\omega+1=0$ 。但三個解當中， $\sqrt[3]{2}$ 在 R 內，而 $\sqrt[3]{2}\omega$ 、 $\sqrt[3]{2}\omega^2$ 卻不在 R 內，因此 R/Q 就不是正規擴展。

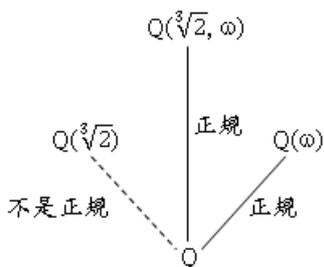


對於 E/F 的擴展維度是有限時(即 $[E:F] < \infty$)， E 總是可以表成 F 與單一元素所生成的體，例如 $E=Q(\sqrt{5}, \sqrt{7})=Q(\sqrt{5}+\sqrt{7})$ 等。當 E/F 為正規擴展時， E 中的每一個元素在 F 上的最小多項式，其所有解都會存在於 E 中。所以，若 E/F 為有限維度的正規擴展時，存在 $\alpha \in E$ ，使得 $E=F(\alpha)$ ，這時候， E 是 α 在 F 上的最小多項式的分裂體！

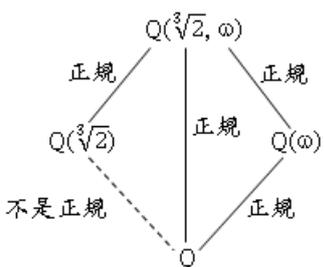
反過來說，若 $f(x) \in F[x]$ ，且 E 為 $f(x)$ 在 F 上的分裂體，則 E 不僅是 F 的擴展體， E 更是 F 的正規擴展體。因此，若 E 是 $F[x]$ 中某一個多項式的分裂體，則 E/F 必定是正規擴展。

再次引用前述例子， $f(x)=x^3-2 \in Q[x]$ ，且 $f(x)=0$ 的解為 $x=\sqrt[3]{2}$ 、 $\sqrt[3]{2}\omega$ 、 $\sqrt[3]{2}\omega^2$ (其中 $\omega^2+\omega+1=0$)，又 $Q(\sqrt[3]{2}, \omega)$ 為 $f(x)$ 在 Q 上的分裂體，則 $Q(\sqrt[3]{2}, \omega)/Q$ 就是一個正規擴展。

至於 $Q(\sqrt[3]{2})/Q$ 和 $Q(\omega)/Q$ 是否為正規擴展呢？先觀察 $Q(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a, b, c \in Q\}$ ，它包含 $f(x)=0$ 的一個解 $\sqrt[3]{2}$ ，但不包含另外兩個解 $\sqrt[3]{2}\omega$ 、 $\sqrt[3]{2}\omega^2$ ，因此 $Q(\sqrt[3]{2})/Q$ 不是正規擴展。另一方面，由於 ω 、 ω^2 是另一個方程式 $g(x)=x^2+x+1=0$ 的兩個解， $Q(\omega) = \{a+b\omega+c\omega^2 \mid a, b, c \in Q\} = Q(\omega, \omega^2)$ ，它是 $g(x)$ 在 Q 上的分裂體，因此 $Q(\omega)/Q$ 是一個正規擴展。



上面的例子，再探索一個問題： $Q(\sqrt[3]{2}, \omega)/Q(\sqrt[3]{2})$ 和 $Q(\sqrt[3]{2}, \omega)/Q(\omega)$ 是否為正規擴展呢？答案是肯定的。因為 $Q(\sqrt[3]{2}, \omega)$ 既然是 $f(x) \in Q[x]$ 的分裂體，無庸置疑地， $Q(\sqrt[3]{2}, \omega)$ 就一定是 $f(x) \in Q(\sqrt[3]{2})[x]$ 的分裂體， $Q(\sqrt[3]{2}, \omega)$ 也一定是 $f(x) \in Q(\omega)[x]$ 的分裂體。(我們只把 $f(x)$ 的係數為體 Q 上的元素換到較大的體 $Q(\sqrt[3]{2})$ 或 $Q(\omega)$ 而已！) 因此，我們得到一個結論：若 E/F 為正規擴展， M 是介於 E 和 F 之間的體，則 E/M 也是正規擴展。(但 M/F 卻不一定是正規擴展。)



(四) Galois 群

循著伽羅瓦探索的路徑，從以下三個部分來認識 Galois 群：

1. 體擴展上的 Galois 群

對於有限維度的體擴展 E/F ，考慮 E 上的一個自同構 $\sigma : E \rightarrow E$ ，並且限定 σ 在 F 時為恆等映射(即 $\sigma(a) = a, \forall a \in F$)，即 E 的底層有一塊如鐵板般的 F 是永遠無法撼動的，則將 σ 稱為 E 上的 F -自同構。若將所有這種 E 上的 F -自同構全部集合起來，以函數的合成作為運算，則形成一個群，稱為 E 在 F 上的 Galois 群，記為 $\text{Gal}(E/F)$ 。即 $\text{Gal}(E/F) = \{ \sigma : E \rightarrow E \text{ 是 } E \text{ 上的自同構} \mid \sigma(a) = a, \forall a \in F \}$ 。

很明顯地可以看出： $\text{Gal}(E/F)$ 是 E 上的自同構群(即 $\text{Aut}(E)$)的子群。由於 E/F 為有限維度的體擴展，則 E/F 可以表成單擴展，而 E 是佈於 F 上的向量空間，所有 E 上的 F -自同構的個數不會超過任一組基底的個數。因此， $|\text{Gal}(E/F)| \leq [E : F]$ 。¹⁷⁸

¹⁷⁸ $|\text{Gal}(E/F)|$ 指 $\text{Gal}(E/F)$ 的元素個數，稱為 $\text{Gal}(E/F)$ 群的「階」(order)。

例如 $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{ \text{恆等映射, 共軛映射} \}$, 原因是 $\mathbb{C} = \mathbb{R}(i)$, 若取 $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$, 由 $[\sigma(i)]^2 = \sigma(i^2) = \sigma(-1) = -1 \in \mathbb{R}$, $\sigma(i)$ 為 $x^2 = -1$ 或 $x^2 + 1 = 0$ 的解, 可得 $\sigma(i) = \pm i$ 。因此 $\forall a + bi \in \mathbb{C}$, 在 $\text{Gal}(\mathbb{C}/\mathbb{R})$ 中包含 σ_1 及 σ_2 兩種映射, 其中 $\sigma_1(a + bi) = a + bi$, $\sigma_2(a + bi) = a - bi$ 。這兩種映射都是複數體 \mathbb{C} 上的自同構, 且不會改變實數體 \mathbb{R} 上的元素, 所以 $\text{Gal}(\mathbb{C}/\mathbb{R})$ 共有 2 個元素。因 $|\text{Gal}(\mathbb{C}/\mathbb{R})| = 2$ 且 $[\mathbb{C}:\mathbb{R}] = 2$, 符合 $|\text{Gal}(\mathbb{C}/\mathbb{R})| \leq [\mathbb{C}:\mathbb{R}]$ 。

再例如 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{ \text{恆等映射} \}$, 原因是 $\mathbb{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q} \}$ 為包含 \mathbb{Q} 和 \mathbb{Q} 上的代數元 $\sqrt[3]{2}$ 的單擴展體, 若 $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, 由於 $[\sigma(\sqrt[3]{2})]^3 = \sigma((\sqrt[3]{2})^3) = \sigma(2) = 2 \in \mathbb{Q}$, $\sigma(\sqrt[3]{2})$ 為 $x^3 = 2$ 或 $x^3 - 2 = 0$ 的解, 可得 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ 或 $\sqrt[3]{2}\omega$ 或 $\sqrt[3]{2}\omega^2$ 。但 σ 是 $\mathbb{Q}(\sqrt[3]{2})$ 上的自同構, 而 $\sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$ 都不在 $\mathbb{Q}(\sqrt[3]{2})$ 中, 所以 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ 是唯一的可能。這代表了 $\mathbb{Q}(\sqrt[3]{2})$ 中的任一元素 $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ (其中 $a, b, c \in \mathbb{Q}$) 經過 σ 映射後, 得 $\sigma(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = \sigma(a) + \sigma(b)\sigma(\sqrt[3]{2}) + \sigma(c)(\sigma(\sqrt[3]{2}))^2 = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$, 因此 σ 必為恆等映射, 此時 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 只有 1 個元素。因 $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$ 且 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, 符合 $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| \leq [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$ 。¹⁷⁹

2. 方程式的 Galois 群

若 $f(x) \in F[x]$ 為 n 次多項式, 且 $f(x)$ 在 F 上的分裂體是 E , 則 $\text{Gal}(E/F)$ 稱為 $f(x) = 0$ 在 F 上的 Galois 群。當 $[E:F] < \infty$ 且 $f(x) = 0$ 的 n 個解兩兩不相等時, 則 $|\text{Gal}(E/F)| = [E:F]$ 。

這時候, 每一個 $\sigma \in \text{Gal}(E/F)$ 會將 $f(x) = 0$ 的某一個解映射到 $f(x) = 0$ 的某一個解; 即若 x_1, \dots, x_n 為 $f(x) = 0$ 的 n 個解, 則 $\sigma(x_1), \dots, \sigma(x_n)$ 仍為 $f(x) = 0$ 的 n 個解(次序可能變動), 但 x_1, \dots, x_n 彼此在 F 中所形成的某些關係式, 依序替換成 $\sigma(x_1), \dots, \sigma(x_n)$ 仍然成立。

例如 $x^2 - 4x + 1 = 0$ 的兩個解為 $x = 2 + \sqrt{3}, 2 - \sqrt{3}$, 設 $\alpha = 2 + \sqrt{3}$, $\beta = 2 - \sqrt{3}$, 在 \mathbb{Q} 中 $\alpha + \beta = 4$ 及 $\alpha\beta = 1$ 的關係式, 經 $\sigma(\alpha) = \beta, \sigma(\beta) = \alpha$ 映射後, 替換成 $\beta + \alpha = 4$ 及 $\beta\alpha = 1$, 仍然成立。

因此, 每一個 $\sigma \in \text{Gal}(E/F)$, 肩負著將 $f(x) = 0$ 的 n 個解在相關的規範下進行重排的任務; 所以 n 次方程式 $f(x) = 0$ 在 F 上的 Galois 群 $\text{Gal}(E/F)$, 等同於之前在「觀察思維」時所提及的「方程式專屬的置換群」。以下列舉幾個例子, 加以說明:

¹⁷⁹ 因為 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 不是正規擴展, 所以 $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| \neq [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$ 。

例1 $f_1(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$, $f_1(x) = 0$ 可整理成 $(x^2 - 2)(x^2 - 3) = 0$, 則 $x = \pm\sqrt{2}, \pm\sqrt{3}$ 為其解, 它們兩兩不相等。

(1) $f_1(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 。

(2) 欲列出 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 的所有元素。可分階段進行如下：

① 先考慮包含 \mathbb{Q} 和 \mathbb{Q} 上的代數元 $\sqrt{2}$ 的單擴展體 $\mathbb{Q}(\sqrt{2})$, 因為 $\sqrt{2}$ 在 \mathbb{Q} 上的最小多項式是 $x^2 - 2 \in \mathbb{Q}[x]$, 而 $x^2 - 2 = 0$ 的兩根為 $\pm\sqrt{2}$, 令 $\text{id}, \sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ 為 $\text{id}(\sqrt{2}) = \sqrt{2}, \sigma(\sqrt{2}) = -\sqrt{2}$ 。

② 再考慮包含 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{2})$ 上的代數元 $\sqrt{3}$ 的單擴展體： $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 因為 $\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多項式是 $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$, 而 $x^2 - 3 = 0$ 的兩根為 $\pm\sqrt{3}$, 令 $\text{id}, \tau \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}))$ 為 $\text{id}(\sqrt{3}) = \sqrt{3}, \tau(\sqrt{3}) = -\sqrt{3}$ 。

③ 最後再將 $H_1 = \{\text{id}, \sigma\}$ 與 $H_2 = \{\text{id}, \tau\}$ 合成得 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \tau\sigma (= \sigma\tau)\}$ ¹⁸⁰, 它們的映射情形如下：

$$\begin{aligned} \text{id} : \begin{bmatrix} \sqrt{2} & \rightarrow & \sqrt{2} \\ \sqrt{3} & \rightarrow & \sqrt{3} \end{bmatrix}, & \quad \sigma : \begin{bmatrix} \sqrt{2} & \rightarrow & -\sqrt{2} \\ \sqrt{3} & \rightarrow & \sqrt{3} \end{bmatrix}, \\ \tau : \begin{bmatrix} \sqrt{2} & \rightarrow & \sqrt{2} \\ \sqrt{3} & \rightarrow & -\sqrt{3} \end{bmatrix}, & \quad \tau\sigma : \begin{bmatrix} \sqrt{2} & \rightarrow & -\sqrt{2} \\ \sqrt{3} & \rightarrow & -\sqrt{3} \end{bmatrix}. \end{aligned}$$

以下列出各種運算的結果：

$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$	id	σ	τ	$\sigma\tau (= \tau\sigma)$
$\sqrt{2} \rightarrow$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$-\sqrt{2} \rightarrow$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$-\sqrt{3} \rightarrow$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$

因此 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong K_4$ (Klein 四元群)。

(3) $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 共有 4 個元素, 而 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$,

所以 $|\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ 。

¹⁸⁰ $H_1 = \{\text{id}, \sigma\}$ 是指 $\mathbb{Q}(\sqrt{2})$ 上的 \mathbb{Q} -同構所成的集合, $H_2 = \{\text{id}, \tau\}$ 是指 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 上的 $\mathbb{Q}(\sqrt{2})$ -同構所成的集合, 而 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 是指 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 上的 \mathbb{Q} -同構所成的集合。事實上, 將 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 中的 id 及 σ 的定義域限制在 $\mathbb{Q}(\sqrt{2})$ 時才是 H_1 中的 id 及 σ 。但為了方便起見, 在 H_1 與 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 時都以相同符號代表。 H_2 同理。

例2 $f_2(x) = x^3 - 2 \in \mathbb{Q}[x]$, $f_2(x) = 0$ 的解為兩兩不相等的 $x = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, 其中 $\omega^2 + \omega + 1 = 0$ 且 $\omega^3 = 1$ 。

(1) $f_2(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 。

(2) 欲列出 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 的所有元素，可分階段進行如下：

① 先考慮 ω 在 \mathbb{Q} 上的最小多項式是 $x^2 + x + 1 \in \mathbb{Q}[x]$ ，

而 $x^2 + x + 1 = 0$ 的兩根為 ω 及 ω^2 ，

令 $\text{id}, \tau \in \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ 為 $\text{id}(\omega) = \omega, \tau(\omega) = \omega^2$ 。

② 再考慮 $\sqrt[3]{2}$ 在 $\mathbb{Q}(\omega)$ 上的最小多項式是 $x^3 - 2 \in \mathbb{Q}(\omega)[x]$ ，

$x^3 - 2 = 0$ 的解為 $x = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ ，

令 $\text{id}, \sigma_1, \sigma_2 \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega))$ 為

$\text{id}(\sqrt[3]{2}) = \sqrt[3]{2}, \sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$ 。

③ 最後再將 $\{\text{id}, \tau\}$ 與 $\{\text{id}, \sigma_1, \sigma_2\}$ 合成得 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) =$

$\{\text{id}, \sigma_1, \sigma_2, \tau, \sigma_1\tau, \sigma_2\tau\}$ ，它們的映射情形如下：

$\text{id} : \begin{bmatrix} \omega & \rightarrow & \omega \\ \sqrt[3]{2} & \rightarrow & \sqrt[3]{2} \end{bmatrix}, \quad \tau : \begin{bmatrix} \omega & \rightarrow & \omega^2 \\ \sqrt[3]{2} & \rightarrow & \sqrt[3]{2} \end{bmatrix}, \quad \sigma_1 : \begin{bmatrix} \omega & \rightarrow & \omega \\ \sqrt[3]{2} & \rightarrow & \sqrt[3]{2}\omega \end{bmatrix},$

$\sigma_2 : \begin{bmatrix} \omega & \rightarrow & \omega \\ \sqrt[3]{2} & \rightarrow & \sqrt[3]{2}\omega^2 \end{bmatrix}, \sigma_1\tau : \begin{bmatrix} \omega & \rightarrow & \omega^2 \\ \sqrt[3]{2} & \rightarrow & \sqrt[3]{2}\omega \end{bmatrix}, \sigma_2\tau : \begin{bmatrix} \omega & \rightarrow & \omega^2 \\ \sqrt[3]{2} & \rightarrow & \sqrt[3]{2}\omega^2 \end{bmatrix}。$

以下列出各種運算的結果：

$\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$	id	σ_1	σ_2	τ	$\sigma_1\tau$ ($=\tau\sigma_2$)	$\sigma_2\tau$ ($=\tau\sigma_1$)
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\sqrt[3]{2}\omega \rightarrow$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$
$\sqrt[3]{2}\omega^2 \rightarrow$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$

因此， $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$ (三元對稱群) $\cong D_3$ (二面體群)。

(3) $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)$ 共有 $3! = 6$ 個元素，而 $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 2 \times 3 = 6$ ，

所以 $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})| = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$ 。

例3 $f_3(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$ ， $f_3(x) = 0$ 共有四個解，且兩兩不相等。

其解為 $x = \pm\sqrt{2 + \sqrt{3}}$ 、 $\pm\sqrt{2 - \sqrt{3}}$ 。

(1) $f_3(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt{2 + \sqrt{3}}, \sqrt{2 - \sqrt{3}}) = \mathbb{Q}(\sqrt{2 + \sqrt{3}})$

(因為 $\sqrt{2 - \sqrt{3}}$ 為 $\sqrt{2 + \sqrt{3}}$ 在體 $\mathbb{Q}(\sqrt{2 + \sqrt{3}})$ 中的乘法反元素)。

(2) 欲列出 $\text{Gal}(\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q})$ 的所有元素，而 $\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q}$ 是單

代數擴展， $\sqrt{2 + \sqrt{3}}$ 在 \mathbb{Q} 上的最小多項式恰是 $f_3(x)$ ，因此，可

令 id 、 σ_1 、 σ_2 、 $\sigma_3 \in \text{Gal}(\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q})$ ，分別為：

$$\text{id}(\sqrt{2 + \sqrt{3}}) = \sqrt{2 + \sqrt{3}} \quad , \quad \sigma_1(\sqrt{2 + \sqrt{3}}) = -\sqrt{2 + \sqrt{3}} \quad ,$$

$$\sigma_2(\sqrt{2 + \sqrt{3}}) = \sqrt{2 - \sqrt{3}} \quad , \quad \sigma_3(\sqrt{2 + \sqrt{3}}) = -\sqrt{2 - \sqrt{3}} \quad .$$

以下列出各種運算的結果：¹⁸¹

$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$	id	σ_1	σ_2	σ_3
$\sqrt{2 + \sqrt{3}} \rightarrow$	$\sqrt{2 + \sqrt{3}}$	$-\sqrt{2 + \sqrt{3}}$	$\sqrt{2 - \sqrt{3}}$	$-\sqrt{2 - \sqrt{3}}$
$-\sqrt{2 + \sqrt{3}} \rightarrow$	$-\sqrt{2 + \sqrt{3}}$	$\sqrt{2 + \sqrt{3}}$	$-\sqrt{2 - \sqrt{3}}$	$\sqrt{2 - \sqrt{3}}$
$\sqrt{2 - \sqrt{3}} \rightarrow$	$\sqrt{2 - \sqrt{3}}$	$-\sqrt{2 - \sqrt{3}}$	$\sqrt{2 + \sqrt{3}}$	$-\sqrt{2 + \sqrt{3}}$
$-\sqrt{2 - \sqrt{3}} \rightarrow$	$-\sqrt{2 - \sqrt{3}}$	$\sqrt{2 - \sqrt{3}}$	$-\sqrt{2 + \sqrt{3}}$	$\sqrt{2 + \sqrt{3}}$

可以檢驗得知 $(\sigma_1)^2 = (\sigma_2)^2 = (\sigma_3)^2 = \text{id}$ ，因此 $\text{Gal}(\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q})$

$\cong K_4$ 。

(3) $\text{Gal}(\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q})$ 共有 4 個元素，而 $[\mathbb{Q}(\sqrt{2 + \sqrt{3}}) : \mathbb{Q}] = 4$ ，

所以 $|\text{Gal}(\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2 + \sqrt{3}}) : \mathbb{Q}]$ 。

¹⁸¹ 因為 $\sqrt{2 + \sqrt{3}}$ 的乘法反元素為 $\sqrt{2 - \sqrt{3}}$ ，所以 $\sigma_1(\sqrt{2 - \sqrt{3}}) = \frac{1}{\sigma_1(\sqrt{2 + \sqrt{3}})} = \frac{1}{-\sqrt{2 + \sqrt{3}}} = -\sqrt{2 - \sqrt{3}}$ ，
 $\sigma_2(\sqrt{2 - \sqrt{3}}) = \frac{1}{\sigma_2(\sqrt{2 + \sqrt{3}})} = \frac{1}{\sqrt{2 - \sqrt{3}}} = \sqrt{2 + \sqrt{3}}$ ， $\sigma_3(\sqrt{2 - \sqrt{3}}) = \frac{1}{\sigma_3(\sqrt{2 + \sqrt{3}})} = \frac{1}{-\sqrt{2 - \sqrt{3}}} = -\sqrt{2 + \sqrt{3}}$ 。

例4 $f_4(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$, $f_4(x) = 0$ 的解為 $x = \omega, \omega^2, \omega^3, \omega^4$

(其中 $\omega = e^{\frac{2\pi i}{5}} = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}$), 兩兩不相等。

(1) $f_4(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\omega, \omega^2, \omega^3, \omega^4) = \mathbb{Q}(\omega)$ 。

(2) 欲列出 $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ 的所有元素，

而 $\mathbb{Q}(\omega)/\mathbb{Q}$ 是單代數擴展， ω 在 \mathbb{Q} 上的最小多項式恰是 $f_4(x)$ ，

因此，可令 $\text{id}, \sigma_1, \sigma_2, \sigma_3 \in \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ ，

分別為 $\text{id}(\omega) = \omega, \sigma_1(\omega) = \omega^2, \sigma_2(\omega) = \omega^3, \sigma_3(\omega) = \omega^4$ 。

由於 $\omega^5 = 1$ ，以下列出各種運算的結果：

$\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$		id	σ_1	σ_2	σ_3
ω	\rightarrow	ω	ω^2	ω^3	ω^4
ω^2	\rightarrow	ω^2	ω^4	ω	ω^3
ω^3	\rightarrow	ω^3	ω	ω^4	ω^2
ω^4	\rightarrow	ω^4	ω^3	ω^2	ω

可檢驗得 $(\sigma_1)^4 = \text{id}, (\sigma_2)^4 = \text{id}, (\sigma_3)^2 = \text{id}$ ，故 $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_4$ 。

(3) $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ 共有 4 個元素 (以 σ_1 或 σ_2 為生成元素的四階循環群)，

而 $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ ，所以 $|\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}]$ 。

3. 一般方程式的 Galois 群

當 F 為特徵值為 0 的體， F 上的一般 n 次多項式指的是 $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ ，其中最高次係數為 1，其他係數以文字 a_1, \dots, a_n 替代，可把 a_1, \dots, a_n 視為 F 上相互獨立的超越元素。

若 $f(x) = 0$ 的 n 個解為 x_1, \dots, x_n ，則 $f(x) = (x - x_1)(x - x_2)\dots(x - x_n)$ ，

比較係數可得 $a_1 = (-1)^1 \sum_{i=1}^n x_i = -(x_1 + x_2 + \dots + x_n)$ ，

$a_2 = (-1)^2 \sum_{i < j} x_i x_j = (x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n)$ ，

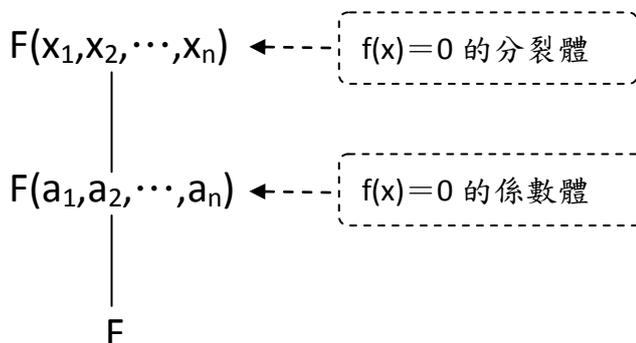
$a_3 = (-1)^3 \sum_{i < j < k} x_i x_j x_k$ ，

.....，

$a_n = (-1)^n x_1 x_2 \dots x_n$ ；

這些 $f(x)$ 的係數 a_1, \dots, a_n 本身都是 x_1, \dots, x_n 的函數，換句話說，可以寫成 $a_1(x_1, \dots, x_n), a_2(x_1, \dots, x_n), \dots, a_n(x_1, \dots, x_n)$ ，我們將 a_1, \dots, a_n 稱為 x_1, \dots, x_n 這 n 個變元的基本對稱函數。

觀察可知， $f(x)$ 的係數所在的體為 $F(a_1, \dots, a_n)$ 。此時 $f(x)$ 在 $F(a_1, \dots, a_n)$ 上的分裂體就是 $F(a_1, \dots, a_n, x_1, \dots, x_n)$ ，但由於 a_1, \dots, a_n 都是 x_1, \dots, x_n 的函數，所以 $f(x)$ 在 $F(a_1, \dots, a_n)$ 上的分裂體可寫成 $F(x_1, \dots, x_n)$ 。



因為 a_1, \dots, a_n 是 x_1, \dots, x_n 這 n 個變元所構成的基本對稱函數，所以 $F(a_1, \dots, a_n)$ 是所有 x_1, \dots, x_n 的對稱有理分式所構成的體。想找尋 $\text{Gal}(F(x_1, \dots, x_n)/F(a_1, \dots, a_n))$ 的元素，必須從 $F(x_1, \dots, x_n)$ 中的自同構找起，且在 $F(a_1, \dots, a_n)$ 中應是恆等映射。每一個 $F(x_1, \dots, x_n)$ 中的自同構都將 x_1, \dots, x_n 進行了一次置換；而無論 x_1, \dots, x_n 如何置換，並不會改變任何 x_1, \dots, x_n 的對稱有理分式。因此所有 $F(x_1, \dots, x_n)$ 中的自同構，在 $F(a_1, \dots, a_n)$ 中必是恆等映射。由此可知 $\text{Gal}(F(x_1, \dots, x_n)/F(a_1, \dots, a_n)) \cong S_n$ ，且 $|\text{Gal}(F(x_1, \dots, x_n)/F(a_1, \dots, a_n))| = n!$ 。

由於 $f(x) = 0$ 在 $F(x_1, \dots, x_n)$ 中的 n 個解兩兩不相等，所以 $[F(x_1, \dots, x_n) : F(a_1, \dots, a_n)] = |\text{Gal}(F(x_1, \dots, x_n)/F(a_1, \dots, a_n))| = n!$ 。這表示若 $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$ 為一般 n 次多項式(係數都是文字)，且 E 是 $f(x)$ 在 F 上的分裂體，則 $\text{Gal}(E/F) \cong S_n$ ，且 $[E : F] = n!$ 。

(五) Galois 理論的基本定理

若 $f(x) \in F[x]$ 為 n 次多項式，且 $f(x)$ 在 F 上的分裂體是 E ，要認清 $f(x) = 0$ 的所有解的面貌，包括是否能表成根式解等，必須從 E/F 體的擴展情形著手。在伽羅瓦之前的數學家們，致力於研究「是否能將足夠多的開方根元素加入 F ，而擴展成 E ？」然而伽羅瓦卻探索體擴展 E/F 結構的複雜程度，他發現 E/F 結構的複雜程度可由 E/F 的 Galois 群完全表現出來；至於之前數學家們所努力尋找的答案，也只不過是伽羅瓦的整盤研究計劃中的一個小分支而已。¹⁸²伽羅瓦開創了「Galois 群」這個新的研究工具，帶來了許多方便，在康明昌所寫的《幾個有名的數學問題》一書中，提到：

¹⁸² 參考康明昌：《幾個有名的數學問題》，頁 111。

從表面上，把體的結構的問題轉變成置換群的問題，似乎把問題簡化了，因為置換群頂多只有有限個元素，只有有限多種子群。事實上，的確有一些問題從體的角度考慮是非常困難，從置換群的角度來觀察卻是不難理解的。(頁 111)

Galois 理論的基本定理經後人整理成三大部分，包括：

- (1) E 和 F 的中間體集與 Gal(E/F)的子群集之間存在一個一對一的對應。
- (2) 體擴展的維度與 Galois 群的階數(元素個數)問題。
- (3) 體的正規擴展與 Galois 群的正規子群的關係。茲將其詳述如下：

Galois 理論的基本定理

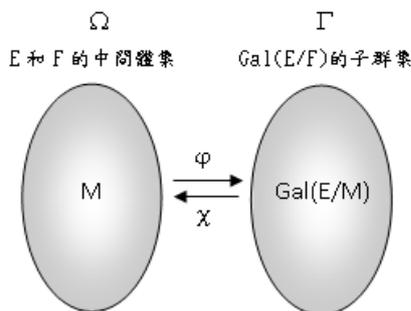
設 $f(x) \in F[x]$ 且 E 為 $f(x)$ 在 F 上的分裂體， $f(x)=0$ 的解兩兩不相等。

令 $\Omega = \{M \mid M \text{ 為體且 } F \subseteq M \subseteq E\}$ ， $\Gamma = \{H \mid H \text{ 為 Gal}(E/F)\text{ 的子群}\}$ 。

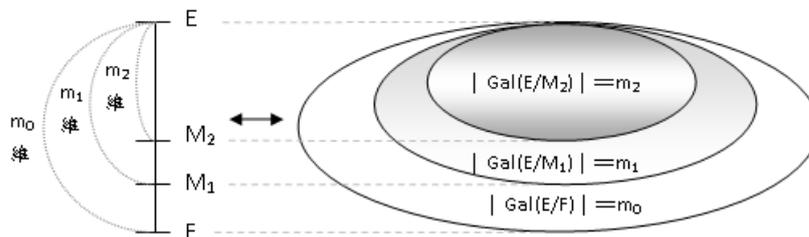
定義 $\phi : \Omega \rightarrow \Gamma$ 為 $\phi(M) = \text{Gal}(E/M)$ ，

$\chi : \Gamma \rightarrow \Omega$ 為 $\chi(H) = \{a \in E \mid \sigma(a) = a, \forall \sigma \in H\} = H$ 的固定體。

- (1) $\chi \circ \phi = \text{id}_{(\Omega)}$ ， $\phi \circ \chi = \text{id}_{(\Gamma)}$ 。即 ϕ 與 χ 互為逆映射。



- (2) $[E : M] = |\text{Gal}(E/M)|$ 且 $[M : F] = \frac{|\text{Gal}(E/F)|}{|\text{Gal}(E/M)|}$ ， $\forall M \in \Omega$ 。



- (3) 設 $M \in \Omega$ ， M/F 為正規擴展 $\Leftrightarrow \text{Gal}(E/M)$ 為 $\text{Gal}(E/F)$ 的正規子群。

此時， $\text{Gal}(M/F) \cong \frac{\text{Gal}(E/F)}{\text{Gal}(E/M)}$ (註：此為商群)。

一般而言，對於 $f(x) \in F[x]$ ， E 為 $f(x)$ 在 F 上的分裂體，且 $f(x) = 0$ 的解兩兩不相等。則可依下列步驟，完全透視 E 和 F 中間體的結構：
 (1)先找 $\text{Gal}(E/F)$ (2)再找 $\text{Gal}(E/F)$ 的所有子群 (3)最後再找 $\text{Gal}(E/F)$ 的每一個子群的固定體。以下舉引三例加以說明：

例1 $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ ， $f(x) = 0$ 的四個解為 $x = \pm i, \pm\sqrt{2}$ ，則 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(i, \sqrt{2})$ 。

(1) $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ 的元素映射情形有如下選擇：

$$i \begin{cases} \rightarrow i \\ \rightarrow -i \end{cases}, \quad \sqrt{2} \begin{cases} \rightarrow \sqrt{2} \\ \rightarrow -\sqrt{2} \end{cases}$$

因此 $|\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})| = 2 \times 2 = 4$ 。

$$\text{今令 } \sigma : \begin{bmatrix} i & \rightarrow & -i \\ \sqrt{2} & \rightarrow & \sqrt{2} \end{bmatrix}, \quad \tau : \begin{bmatrix} i & \rightarrow & i \\ \sqrt{2} & \rightarrow & -\sqrt{2} \end{bmatrix},$$

則 $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) = \{ \text{id}, \sigma, \tau, \sigma\tau (= \tau\sigma) \} \cong K_4$ 。

(2) $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ 的子群有 $\{ \text{id} \}, \{ \text{id}, \sigma \}, \{ \text{id}, \tau \}, \{ \text{id}, \sigma\tau \}, \{ \text{id}, \sigma, \tau, \sigma\tau \}$ 。

(3) $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$ ，而 $\{ 1, i, \sqrt{2}, \sqrt{2}i \}$ 可為 $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ 的一組基底。

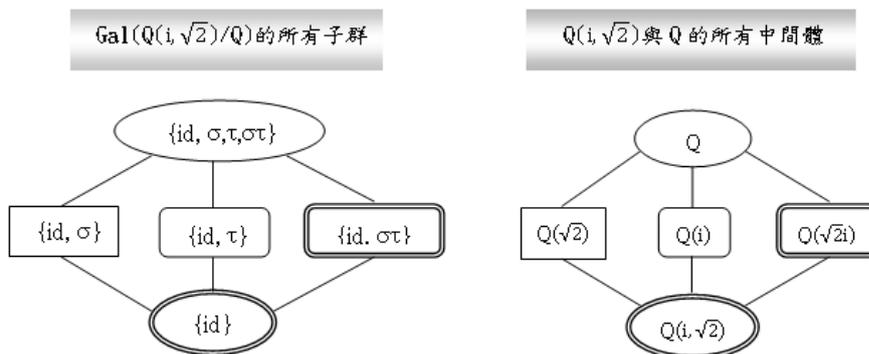
① $\{ \text{id} \}$ 的固定體為 $\mathbb{Q}(1, i, \sqrt{2}, \sqrt{2}i) = \mathbb{Q}(i, \sqrt{2})$ 。

② $\{ \text{id}, \sigma \}$ 的固定體為 $\mathbb{Q}(\sqrt{2})$ 。

③ $\{ \text{id}, \tau \}$ 的固定體為 $\mathbb{Q}(i)$ 。

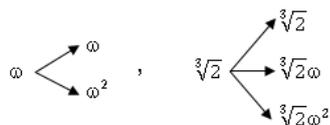
④ $\sigma\tau : \begin{bmatrix} i & \rightarrow & -i \\ \sqrt{2} & \rightarrow & -\sqrt{2} \\ \sqrt{2}i & \rightarrow & \sqrt{2}i \end{bmatrix}$ ，得 $\{ \text{id}, \sigma\tau \}$ 的固定體為 $\mathbb{Q}(\sqrt{2}i)$ 。

⑤ $\{ \text{id}, \sigma, \tau, \sigma\tau \}$ 的固定體為 \mathbb{Q} 。



例2 $f(x)=x^3-2\in\mathbb{Q}[x]$, $f(x)=0$ 的三個解為 $x=\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, 其中 $\omega=\frac{-1+\sqrt{3}i}{2}$ 。則 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 。

(1) 因為 ω 在 \mathbb{Q} 上的最小多項式是 $x^2+x+1\in\mathbb{Q}[x]$, 而 $x^2+x+1=0$ 的兩根為 ω 及 ω^2 , 又因為 $\sqrt[3]{2}$ 在 $\mathbb{Q}(\omega)$ 上的最小多項式是 $x^3-2\in\mathbb{Q}(\omega)[x]$, $x^3-2=0$ 的解為 $x=\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, 所以 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 的元素映射情形有如下選擇：



因此 $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})| = 2 \times 3 = 6$ 。

可令 $\tau: \begin{bmatrix} \sqrt[3]{2} & \rightarrow & \sqrt[3]{2} \\ \omega & \rightarrow & \omega^2 \end{bmatrix}$, $\sigma: \begin{bmatrix} \sqrt[3]{2} & \rightarrow & \sqrt[3]{2}\omega \\ \omega & \rightarrow & \omega \end{bmatrix}$, 其中 $\tau^2 = \text{id}$, $\sigma^3 = \text{id}$,

¹⁸³則 $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = \{ \text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \} \cong S_3$ 。

$\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$	id	σ	σ^2	τ	$\sigma\tau (= \tau\sigma^2)$	$\sigma^2\tau (= \tau\sigma)$
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\omega \rightarrow$	ω	ω	ω	ω^2	ω^2	ω^2

(2) $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 的子群有 $\{ \text{id} \}$ 、 $\{ \text{id}, \sigma, \sigma^2 \}$ 、 $\{ \text{id}, \tau \}$ 、 $\{ \text{id}, \sigma\tau \}$ 、 $\{ \text{id}, \sigma^2\tau \}$ 、 $\{ \text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$ 。

(3) $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)] [\mathbb{Q}(\omega) : \mathbb{Q}] = 3 \times 2 = 6$,

而 $\{ 1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega \}$ 可為 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ 的一組基底。

① $\{ \text{id} \}$ 的固定體為 $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 。

② $\{ \text{id}, \sigma, \sigma^2 \}$ 的固定體為 $\mathbb{Q}(\omega)$ 。

③ $\{ \text{id}, \tau \}$ 的固定體為 $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$ 。

④ $\{ \text{id}, \sigma\tau \}$ 的固定體為 $\mathbb{Q}(\sqrt[3]{4}\omega)$ 。¹⁸⁴

⑤ $\{ \text{id}, \sigma^2\tau \}$ 的固定體為 $\mathbb{Q}(\sqrt[3]{2}\omega)$ 。

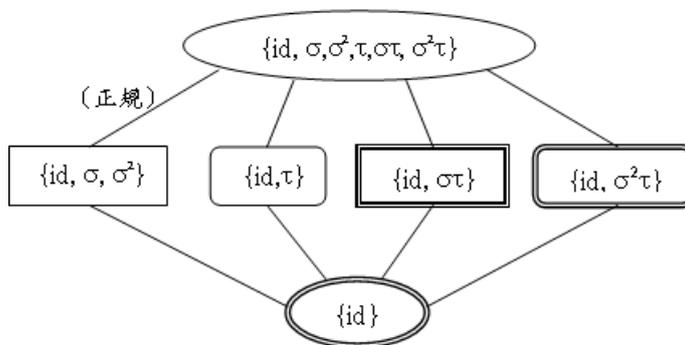
⑥ $\{ \text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau \}$ 的固定體為 \mathbb{Q} 。

¹⁸³ 此處的 σ, σ^2 , 即本論文頁 65 的 σ_1, σ_2 。

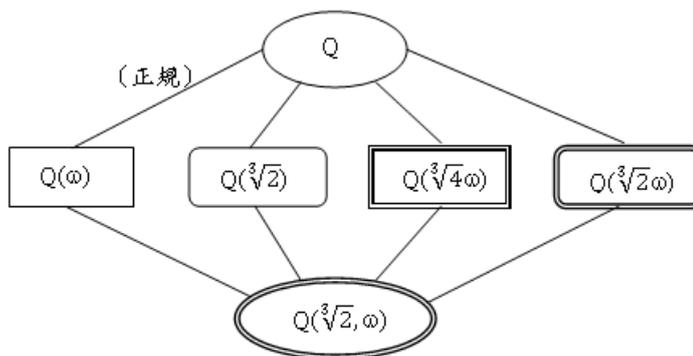
¹⁸⁴ $\mathbb{Q}(\sqrt[3]{4}\omega)$ 亦可寫成 $\mathbb{Q}(\sqrt[3]{2}\omega^2)$, 因為 $\sqrt[3]{4}\omega$ 的乘法反元素是 $\sqrt[3]{2}\omega^2$ 。

- (4) 在 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 與 \mathbb{Q} 的所有中間體當中，除了 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 及 \mathbb{Q} 之外，僅有 $\mathbb{Q}(\omega)$ 為 \mathbb{Q} 的正規擴展；同樣地，在 $\{\text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ 的所有子群當中，除了 $\{\text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ 本身及 $\{\text{id}\}$ 之外，僅有 $\{\text{id}, \sigma, \sigma^2\}$ 為 $\{\text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ 的正規子群。
- (5) $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 的一階子群 $\{\text{id}\}$ ，它的固定體 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 對於 \mathbb{Q} 是 $6 \div 1 = 6$ 維擴展體；二階子群 $\{\text{id}, \tau\}$ 、 $\{\text{id}, \sigma\tau\}$ 、 $\{\text{id}, \sigma^2\tau\}$ 的固定體分別是 $\mathbb{Q}(\sqrt[3]{2})$ 、 $\mathbb{Q}(\sqrt[3]{4}\omega)$ 、 $\mathbb{Q}(\sqrt[3]{2}\omega)$ ，它們對於 \mathbb{Q} 是 $6 \div 2 = 3$ 維擴展體；三階子群 $\{\text{id}, \sigma, \sigma^2\}$ 的固定體是 $\mathbb{Q}(\omega)$ ，它對於 \mathbb{Q} 是 $6 \div 3 = 2$ 維擴展體；六階子群 $\{\text{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ 的固定體是 \mathbb{Q} ，它對於 \mathbb{Q} 是 $6 \div 6 = 1$ 維擴展體。

$\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ 的所有子群



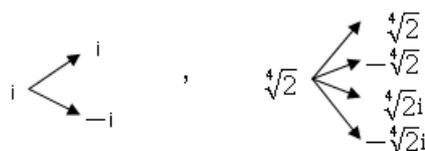
$\mathbb{Q}(\sqrt[3]{2}, \omega)$ 與 \mathbb{Q} 的所有中間體



例3 $f(x)=x^4-2\in\mathbb{Q}[x]$, $f(x)=0$ 的四個解為 $x=\pm\sqrt[4]{2}$ 、 $\pm\sqrt[4]{2}i$ 。則 $f(x)$ 在 \mathbb{Q} 上的分裂體為 $\mathbb{Q}(\sqrt[4]{2}, i)$ 。

(1) 因為 i 在 \mathbb{Q} 上的最小多項式是 x^2+1 , 而 $x^2+1=0$ 的解為 $x=\pm i$;

又因為 $\sqrt[4]{2}$ 在 $\mathbb{Q}(i)$ 上的最小多項式恰是 x^4-2 , 而 $x^4-2=0$ 的四個解就是 $x=\pm\sqrt[4]{2}$ 、 $\pm\sqrt[4]{2}i$, 所以 $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ 的元素映射情形有如下選擇:



因此 $|\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 2 \times 4 = 8$ 。

可令 $\tau : \begin{bmatrix} \sqrt[4]{2} & \rightarrow & \sqrt[4]{2} \\ i & \rightarrow & -i \end{bmatrix}$, $\sigma : \begin{bmatrix} \sqrt[4]{2} & \rightarrow & \sqrt[4]{2}i \\ i & \rightarrow & i \end{bmatrix}$,

其中 τ 為二階循環元素 (即 $\tau^2 = \text{id}$), σ 為四階循環元素 (即 $\sigma^4 = \text{id}$),

則 $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \{ \text{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3 \} \cong D_4$ (二面體群)。

$\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$	id	σ	σ^2	σ^3	τ	$\tau\sigma$ ($=\sigma^3\tau$)	$\tau\sigma^2$ ($=\sigma^2\tau$)	$\tau\sigma^3$ ($=\sigma\tau$)
$\sqrt[4]{2} \rightarrow$	$\sqrt[4]{2}$	$\sqrt[4]{2}i$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}i$	$\sqrt[4]{2}$	$-\sqrt[4]{2}i$	$-\sqrt[4]{2}$	$\sqrt[4]{2}i$
$i \rightarrow$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

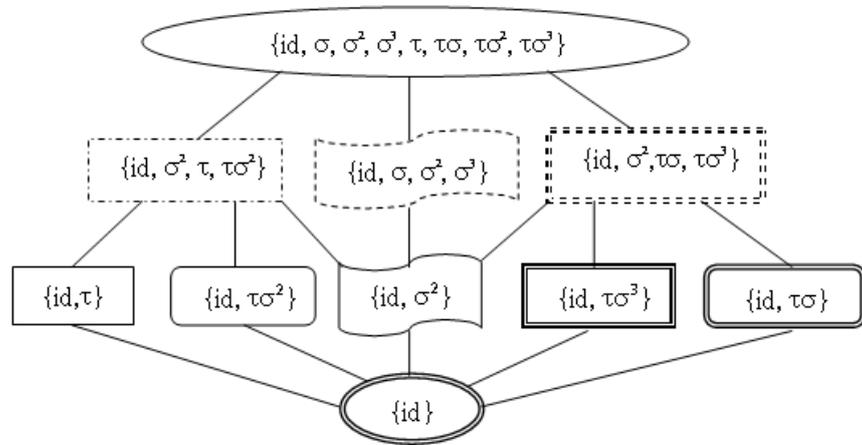
(2)

Gal(Q(√[4]{2}, i)/Q) 的子群		備註
1 階	{ id }	$\cong \{0\}$
2 階	{ id, σ^2 }	$\cong Z_2$
	{ id, τ }	$\cong Z_2$
	{ id, $\tau\sigma$ }	$\cong Z_2$
	{ id, $\tau\sigma^2$ }	$\cong Z_2$
	{ id, $\tau\sigma^3$ }	$\cong Z_2$
4 階	{ id, $\sigma, \sigma^2, \sigma^3$ }	$\cong Z_4$
	{ id, $\sigma^2, \tau, \tau\sigma^2$ }	$\cong K_4$
	{ id, $\sigma^2, \tau\sigma, \tau\sigma^3$ }	$\cong K_4$
8 階	{ id, $\sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3$ }	$\cong D_4$ (二面體群)

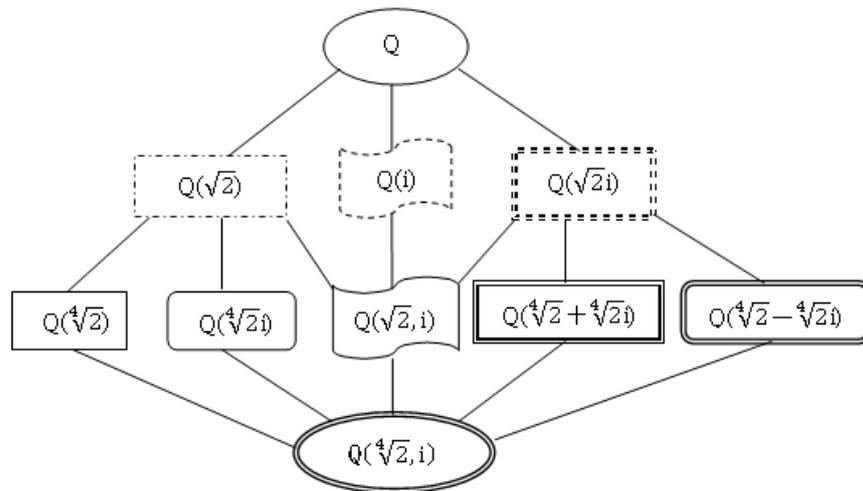
(3) $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] [\mathbb{Q}(i) : \mathbb{Q}] = 4 \times 2 = 8$ ，而
 $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}, i, \sqrt[4]{2}i, \sqrt{2}i, \sqrt[4]{8}i\}$ 可為 $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ 的一組基底。

Gal($\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$)子群	對應的固定體 (設 M)	$[\mathbb{M} : \mathbb{Q}]$ = $\frac{8}{\text{子群的階數}}$
$\{\text{id}\}$	$\mathbb{Q}(\sqrt[4]{2}, i)$	$8 \div 1 = 8$
$\{\text{id}, \sigma^2\}$ $\{\text{id}, \tau\}$ $\{\text{id}, \tau\sigma\}$ $\{\text{id}, \tau\sigma^2\}$ $\{\text{id}, \tau\sigma^3\}$	$\mathbb{Q}(\sqrt{2}, i)$ $\mathbb{Q}(\sqrt[4]{2})$ $\mathbb{Q}(\sqrt[4]{2} - \sqrt[4]{2}i)$ $\mathbb{Q}(\sqrt[4]{2}i)$ $\mathbb{Q}(\sqrt[4]{2} + \sqrt[4]{2}i)$	$8 \div 2 = 4$
$\{\text{id}, \sigma, \sigma^2, \sigma^3\}$ $\{\text{id}, \sigma^2, \tau, \tau\sigma^2\}$ $\{\text{id}, \sigma^2, \tau\sigma, \tau\sigma^3\}$	$\mathbb{Q}(i)$ $\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}(\sqrt{2}i)$	$8 \div 4 = 2$
$\{\text{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$	\mathbb{Q}	$8 \div 8 = 1$

Gal($\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$)的所有子群



$\mathbb{Q}(\sqrt[4]{2}, i)$ 與 \mathbb{Q} 的所有中間體



有了 Galois 理論的基本架構，對於混亂的局面有了更清晰的歸位，在達爾馬斯(Andre Dalmass)著的《伽羅瓦傳》中譯本記載：

在分析求解的方程式時，他把某種運算群與這個方程聯繫起來，並證明方程的特性反映在該群的特點上。既然不同的方程可以「有」同一個群，那麼，無須研究所有這些方程，只須研究與之相適應的群就可以了。(頁 36)

四、猜測

猜測是在探索的基礎上所產生的想法，在整個數學思維的過程當中，開創出登上新台階的方向。它是一種預見的數學思維，從已獲得的性質中展望前景，對於問題的特點與環境進行評估與判斷，並猜想出可能採取的方法或答案。¹⁸⁵

伽羅瓦對於任何給定的方程式，先找出它對應的 Galois 群，再從 Galois 群的特性剖析，可對方程式解的屬性一目瞭然。在此，伽羅瓦猜測：方程式「可以根式解」的判斷準則與對應的 Galois 群的「某種表現形式」有關聯。這要從「根式擴展」到「可解群」的概念講起。

(一) 尋找路徑

為了進一步瞭解伽羅瓦的思想，我們以四次一般方程式 $f(x) = x^4 + px^2 + q = 0$ (缺少 x^3 項及 x 項) 為例作說明。¹⁸⁶

先由 $f(x) = x^4 + px^2 + q = 0$ 得到 $x^2 = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$ ；再解得原四次方程式的四個解為 $x = \pm \sqrt{\frac{-p + \sqrt{p^2 - 4q}}{2}}$ 或 $\pm \sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}$ 。我們可令 $x_1 = \sqrt{\frac{-p + \sqrt{p^2 - 4q}}{2}}$ 、 $x_2 = -\sqrt{\frac{-p + \sqrt{p^2 - 4q}}{2}}$ 、 $x_3 = \sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}$ 、 $x_4 = -\sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}$ 。若將 $\{x_1, x_2, x_3, x_4\}$ 視為 $\{1, 2, 3, 4\}$ ，考慮 $f(x) = 0$ 在各種不同的體上的 Galois 群，如下：

1. $f(x) = 0$ 在係數體 $Q(p, q)$ 上的 Galois 群 G 。

承接拉格朗日的預解式想法，可得 $x_1 + x_2 = 0, x_3 + x_4 = 0$ ①； G 是 S_4 中滿足 ① 式的置換組成的集合， $G = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 4\ 2\ 3), (1\ 3\ 2\ 4)\}$ ，共有 8 個元素。

2. $f(x) = 0$ 在體 $Q(p, q, \sqrt{p^2 - 4q})$ 上的 Galois 群 H_1 。

由於新加入的 $\sqrt{p^2 - 4q}$ 可寫成 $\sqrt{p^2 - 4q} = (x_1)^2 - (x_3)^2$ ②，又因為 $x_1 + x_2 = 0, x_3 + x_4 = 0$ ，所以 $(x_1)^2 = (x_2)^2, (x_3)^2 = (x_4)^2$ 。在 G 中滿足 ② 式的置換組成的集合為 $H_1 = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ ， H_1 為 G 的子群，共有 4 個元素。

¹⁸⁵ 參考丘維聲著：《數學的思維方式與創新》，頁 149；張雄、李得虎所編著的《數學方法論與解題研究》(北京：高等教育出版社，2013 年)，頁 275。

¹⁸⁶ 參考 Morris Kline 原著，林炎全、洪萬生、楊康景松譯：《數學史》中冊(台北市：九章出版社，民 72 年)，頁 417-420；丘維聲著：《數學的思維方式與創新》，頁 148-149。

3. $f(x)=0$ 在體 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}})$ 上的 Galois 群 H_2 。

由於新加入的 $\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}$ 可寫成 $\sqrt{\frac{-p-\sqrt{p^2-4q}}{2} = \frac{x_3-x_4}{2}}$③, 在 H_1 中滿足 ③ 式的置換組成的集合為 $H_2 = \{ e, (1\ 2) \}$, H_2 為 H_1 的子群, 共有 2 個元素。

4. $f(x)=0$ 在體 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}, \sqrt{\frac{-p+\sqrt{p^2-4q}}{2}})$ 上的 Galois 群 H_3 。

由於新加入的 $\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}}$ 可寫成 $\sqrt{\frac{-p+\sqrt{p^2-4q}}{2} = \frac{x_1-x_2}{2}}$④, 在 H_2 中滿足 ④ 式的置換組成的集合為 $H_3 = \{ e \}$, H_3 為 H_2 的子群, 僅有恆等置換 1 個元素。

從 $Q(p, q)$ 擴展成 $Q(p, q, \sqrt{p^2 - 4q})$ 時, 令添加的元素 $\sqrt{p^2 - 4q} = \alpha_1$, 則 $(\alpha_1)^2 \in Q(p, q)$; 從 $Q(p, q, \sqrt{p^2 - 4q})$ 擴展成 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}})$ 時, 令添加的元素 $\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}} = \alpha_2$, 則 $(\alpha_2)^2 \in Q(p, q, \sqrt{p^2 - 4q})$; 從 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}})$ 擴展成 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}, \sqrt{\frac{-p+\sqrt{p^2-4q}}{2}})$ 時, 令添加的元素 $\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}} = \alpha_3$, 則 $(\alpha_3)^2 \in Q(p, q, \sqrt{p^2 - 4q}) \subseteq Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}})$ 。

由上可知, 在 $Q(p, q) \subseteq Q(p, q, \sqrt{p^2 - 4q}) \subseteq Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}) \subseteq Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}, \sqrt{\frac{-p+\sqrt{p^2-4q}}{2}})$ 體擴展鏈中, 每次添加的元素的平方都會屬於前一個體。這表示前一個體將自身的某些元素經加、減、乘、除、開方後, 再添加進去原來的體, 就可形成後一個體, 直到含蓋 x_1, x_2, x_3, x_4 的體 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}, \sqrt{\frac{-p+\sqrt{p^2-4q}}{2}})$ 為止。而 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}, \sqrt{\frac{-p+\sqrt{p^2-4q}}{2}})$ 可由 $Q(p, q)$ 逐步擴展得到, 因此 $f(x)=0$ 的所有解都可由原方程式的係數作加、減、乘、除及開方後得到, 也就是原四次方程式可以用根式求解。

讓我們列出 $Q(p, q) \subseteq Q(p, q, \sqrt{p^2 - 4q}) \subseteq Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}) \subseteq Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}, \sqrt{\frac{-p + \sqrt{p^2 - 4q}}{2}})$ 體擴展鏈，可得對應的 G 的子群鏈 $G \supseteq H_1 \supseteq H_2 \supseteq H_3 = \{e\}$ 。由此發現，原四次方程式係數所在的體若擴展到 $Q(p, q, \sqrt{p^2 - 4q}, \sqrt{\frac{-p - \sqrt{p^2 - 4q}}{2}}, \sqrt{\frac{-p + \sqrt{p^2 - 4q}}{2}})$ 時，能含蓋方程式的所有解，其所對應的 Galois 群(即 H_3)會是單位子群。透過這些分解過程，可以找到伽羅瓦當時對「根式解判斷準則」所猜測的想法。

(二) 根式擴展

要探求方程式的根式解，先來認識根式擴展體。以下先從根式擴展的原始定義開始，進而調整為質數維度的擴展鏈，作為對照可解群的理論根據，並抓住伽羅瓦在數學思維中尋求突破的蛛絲馬跡。

1. 基本定義

設 $F_0 = F; F_1 = F(\alpha_1)$ ，其中存在正整數 n_1 使得 $(\alpha_1)^{n_1} \in F_0; F_2 = F_1(\alpha_2) = F(\alpha_1, \alpha_2)$ ，其中存在正整數 n_2 使得 $(\alpha_2)^{n_2} \in F_1 = F(\alpha_1)$ ；依此規律進行有限次，若可得 $K = F_m = F(\alpha_1, \dots, \alpha_m)$ ，其中存在正整數 n_m 使得 $(\alpha_m)^{n_m} \in F_{m-1} = F(\alpha_1, \dots, \alpha_{m-1})$ ，就稱 K/F 為根式擴展。此時， $F = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_m = K$ ，形成一個體的擴展鏈。

任何多項式 $f(x) \in F[x]$ ，若 E 為 $f(x)$ 在 F 上的分裂體，且存在 K/F 為根式擴展，使得 $F \subseteq E \subseteq K$ ，這時候，我們稱 $f(x)$ 可以用根式求解。換句話說， $f(x) \in F[x]$ 可用 F 中的元素經過有限次的加、減、乘、除及開任意次方以求得所有解。

例如 $f(x) = (x^2 + 2x - 1)(x^3 - 2) \in Q[x]$ ， $f(x) = 0$ 的解為 $x = -1 \pm \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ ，其中 $\omega = \frac{-1 + \sqrt{3}i}{2}$ 。此時， $f(x)$ 在 Q 上的分裂體為 $Q(\sqrt{2}, \sqrt[3]{2}, \omega) = Q(\sqrt{2}, \sqrt[3]{2}, \sqrt{3}i)$ ，它是 Q 的根式擴展，其中 $(\sqrt{2})^2 = 2 \in Q, (\sqrt[3]{2})^3 = 2 \in Q(\sqrt{2}), (\sqrt{3}i)^2 = -3 \in Q(\sqrt{2}, \sqrt[3]{2})$ ，並且 $Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2}, \sqrt[3]{2}) \subset Q(\sqrt{2}, \sqrt[3]{2}, \sqrt{3}i)$ 。所以 $f(x) \in Q[x]$ 可以用根式求解。

又例如 $g(x) = x^4 + 2x^2 + 2 \in Q[x]$ ，則 $g(x) = 0$ 的解為 $x = \pm\sqrt{-1 + \sqrt{-1}}, \pm\sqrt{-1 - \sqrt{-1}}$ 。此時， $g(x)$ 在 Q 上的分裂體為 $Q(\sqrt{-1 + \sqrt{-1}}, \sqrt{-1 - \sqrt{-1}}) = Q(\sqrt{-1}, \sqrt{-1 + \sqrt{-1}}, \sqrt{-1 - \sqrt{-1}})$ ，其中 $(\sqrt{-1})^2 = -1 \in Q, (\sqrt{-1 + \sqrt{-1}})^2 = -1 + \sqrt{-1} \in Q(\sqrt{-1}), (\sqrt{-1 - \sqrt{-1}})^2 = -1 - \sqrt{-1} \in$

$Q(\sqrt{-1}, \sqrt{-1 + \sqrt{-1}})$ ，並且 $Q \subset Q(\sqrt{-1}) \subset Q(\sqrt{-1}, \sqrt{-1 + \sqrt{-1}}) \subset Q(\sqrt{-1}, \sqrt{-1 + \sqrt{-1}}, \sqrt{-1 - \sqrt{-1}})$ 。所以 $g(x) \in Q[x]$ 可以用根式求解。

2. 質數維度擴展鏈

在有理數體 Q 上，令 $\zeta_n = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ ，則 $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ 是 $x^n - 1 = 0$ 的所有解，將 $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ 稱為 n 次單位根。此時， $Q(\zeta_n)$ 是 $x^n - 1$ 在 Q 上的分裂體， $Q(\zeta_n)/Q$ 稱為 n 階分圓擴展，它是正規擴展。

多項式 $f(x) = x^n - a \in Q[x] (a > 0)$ 的所有解為 $x = \sqrt[n]{a}, \sqrt[n]{a}\zeta_n, \sqrt[n]{a}\zeta_n^2, \dots, \sqrt[n]{a}\zeta_n^{n-1}$ 。此時， $Q(\zeta_n, \sqrt[n]{a})$ 為 $f(x) \in Q[x]$ 的分裂體，這時候形成一個體擴展鏈 $Q \subset Q(\zeta_n) \subset Q(\zeta_n, \sqrt[n]{a})$ ，其中 $(\zeta_n)^n = 1 \in Q$ ， $(\sqrt[n]{a})^n = a \in Q \subset Q(\zeta_n)$ ，並且 $Q(\zeta_n)/Q$ 與 $Q(\zeta_n, \sqrt[n]{a})/Q(\zeta_n)$ 都是正規擴展。觀察這個體擴展鏈分成兩部分：前段 $Q \subset Q(\zeta_n)$ 是 n 階分圓擴展；後段 $Q(\zeta_n) \subset Q(\zeta_n, \sqrt[n]{a})$ 則可再細分為擴展維度都是質數的正規擴展鏈。

例如當 $n = 2 \times 3$ 時， $f(x) = x^6 - 2 \in Q[x]$ 的分裂體為 $Q(\zeta_6, \sqrt[6]{2})$ ，其中 $\zeta_6 = e^{\frac{2\pi i}{6}} = \cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6}$ ，這時候形成一個正規擴展鏈 $Q \subset Q(\zeta_6) \subset Q(\zeta_6, \sqrt[6]{2})$ 。前段 $Q \subset Q(\zeta_6)$ 屬於分圓擴展；後段 $Q(\zeta_6) \subset Q(\zeta_6, \sqrt[6]{2})$ 可再細分為 2 維與 3 維的正規擴展鏈。如下：

$$\boxed{Q(\zeta_6)} \subseteq \boxed{Q(\zeta_6)((\sqrt[6]{2})^2) = Q(\zeta_6, \sqrt[3]{2})} \subseteq \boxed{Q(\zeta_6, \sqrt[3]{2})((\sqrt[6]{2})^3) = Q(\zeta_6, \sqrt[3]{2}, \sqrt{2}) = Q(\zeta_6, \sqrt[6]{2})}$$

↑ 3 維擴展 ↑ 2 維擴展

因此，正規擴展鏈可改為 $Q \subset Q(\zeta_6) \subset Q(\zeta_6, \sqrt[3]{2}) \subset Q(\zeta_6, \sqrt[3]{2}, \sqrt{2}) = Q(\zeta_6, \sqrt[6]{2})$ 。

由以上的分解，對於根式擴展 K/F ，我們不妨重新以另一個方式說明：當 F 和 K 之間可形成一串單擴展鏈 $F = F_0 \subset F_1 \subset \dots \subset F_m = K$ ，其中 $F_i = F_{i-1}(\alpha_i)$ ，且 $\alpha_i^{n_i} \in F_{i-1}$ ， $i = 1, 2, \dots, m$ 時，令 $n = n_1 n_2 \dots n_m$ ， ζ 為 n 次單位根，設 $\bar{F} = F(\zeta)$ ，則 \bar{F} 和 K 之間可形成一串單擴展鏈 $\bar{F} = \bar{F}_0 \subset \bar{F}_1 \subset \dots \subset \bar{F}_s = K$ ，滿足 $\bar{F}_i = \bar{F}_{i-1}(\beta_i)$ ，且 $\beta_i^{p_i} \in \bar{F}_{i-1}$ ， p_i 為質數， $i = 1, 2, \dots, s$ 。

因此，若 K/F 為根式擴展，且其中的體 F 已包含了擴展時可能須添加的所有單位根(即上一段的 \bar{F})，則根式擴展 K/F 會形成一串擴展維度都是質數的擴展鏈。

同樣地，若多項式 $f(x) \in F[x]$ 可以用根式求解， E 為 $f(x)$ 在 F 上的分裂體，且其中 F 已包含了根式擴展時可能須添加的所有單位根，則存在一串擴展維度都是質數的正規擴展鏈 $F = F_0 \subset F_1 \subset \dots \subset F_r = K$ (r 為某個正整數)，使得 $F \subseteq E \subseteq K$ 。

(三) 可解群

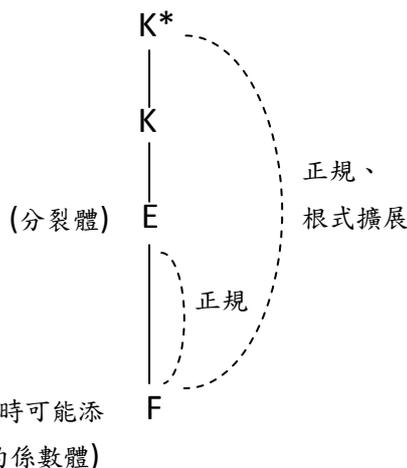
由 Galois 理論的基本概念，可以猜測：若 $f(x)$ 為可用根式求解的多項式，則對應到方程式 $f(x)=0$ 的 Galois 群 G ，也會有一串正規子群鏈 $G = G_0 \supset G_1 \supset \dots \supset G_r = \{e\}$ ，其中對於每一個 $i=1, \dots, r$ ， G_i 為 G_{i-1} 的正規子群，並且 $|G_{i-1}/G_i|$ 為質數。

我們把符合上述這些條件的群 G 稱為「可解群」(Solvable Group)。若 G 為有限可解群， G 的正規子群鏈串接方式不一定會唯一，但長度卻一定，且 G 的階數應恰是所有這些質數的乘積。

想確立這樣的猜測是正確的，我們來進行以下的分析與討論：

若 $f(x) \in F[x]$ 可以用根式求解， E 為 $f(x)$ 在 F 上的分裂體，且體 F 已包含根式擴展時可能須添加的所有單位根，則存在一串擴展維度都是質數的正規擴展鏈 $F = F_0 \subset F_1 \subset \dots \subset F_r = K$ (r 為某個正整數)，使得 $F \subseteq E \subseteq K$ 。

我們可以將 K 作有限擴展(加進可用根式表示的元素的共軛元)，形成 $K^* \supseteq K$ ，使 K^*/F 為正規擴展，也是根式擴展。



由 Galois 理論的基本定理知， F 到 K^* 所形成質數維度的正規擴展鏈，可對應出 $\text{Gal}(K^*/F)$ 的一串正規子群鏈 $\text{Gal}(K^*/F) \supset \text{Gal}(K^*/F_1) \supset \text{Gal}(K^*/F_2) \supset \dots \supset \{e\}$ 且 $\forall i, | \text{Gal}(K^*/F_{i-1}) / \text{Gal}(K^*/F_i) |$ 為質數。因此， $\text{Gal}(K^*/F)$ 為可解群。

因為 K^*/F 為正規擴展，且 E/F 為正規擴展，所以 K^*/E 為正規擴展。由 Galois 理論的基本定理知： $\text{Gal}(K^*/E)$ 為 $\text{Gal}(K^*/F)$ 的正規子群且

$$\text{Gal}(E/F) \cong \frac{\text{Gal}(K^*/F)}{\text{Gal}(K^*/E)}。$$

換句話說， $\text{Gal}(E/F)$ 為 $\text{Gal}(K^*/F)$ 的同態像(Homomorphic Image)，由於 $\text{Gal}(K^*/F)$ 為可解群，可以推得 $\text{Gal}(E/F)$ 也為可解群。

事實上，伽羅瓦證明：若多項式 $f(x) \in F[x]$ 的分裂體為 E ，則「 $f(x)$ 可以用根式求解」與「 $\text{Gal}(E/F)$ 為可解群」是同步存在的，彼此互為充分必要的條件。

本節在討論「抽象思維」時曾提到的極大正規子群家族，若其每一個合成因子都是質數，就是此處的 $\text{Gal}(E/F)$ 為可解群的情況了。

若 $f(x)$ 為多項式，則 $f(x)=0$ 的 Galois 群必是有限群，將有限群的階數進行質因數分解，可以掌握正規子群的分布與性質。那個困擾數學家們幾百年的方程式根式求解問題，只要不困在分裂體的環境中，勇敢地走出來，到 $f(x)=0$ 的 Galois 群的國度裏，就能從另一個嶄新的座標看清楚所有的肌理。

伽羅瓦是以基本定理中正規擴展與正規子群的對應為基礎，讓思維大膽出走，的確為數學界開闢了一片新天新地。

五、論證

有了精準的猜測之後，就必須進行嚴密的論證。而論證的策略先以「類比」的方法，將根式擴展與可解群之間相同的屬性加以延伸；並以「模擬」的方法建立了可解群的檢驗法，來進行考察與實驗；最後再「轉化」歸結為方程式根式求解的問題來討論。以下將詳細說明。

(一) S_n 的可解性

既然方程式的 Galois 群都是對稱群的子群，「對稱群是否為可解群？」成為重要的檢驗指標。

1. $S_2 = \{e, (12)\}$ 有 $2! = 2$ 個元素，找到的正規子群鏈為 $S_2 \supset \{e\}$ ，且合成因子列為 (2) ，是質數，所以 S_2 是可解群。

2. $S_3 = \{e, (12), (23), (13), (123), (132)\}$ 有 $3! = 6$ 個元素，找到的正規子群鏈為 $S_3 \supset A_3 \supset \{e\}$ ，其中 $A_3 = \{e, (123), (132)\}$ 為所有 S_3 的偶置換所形成的交錯子群， A_3 共有 $\frac{3!}{2} = 3$ 個元素，合成因子列為 $(2, 3)$

(即 $\frac{6}{3}, \frac{3}{1}$) 都是質數，所以 S_3 是可解群。

3. $S_4 = \{e, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (132), (142), (143), (243), (1234), (1243), (1324), (1342), (1423), (1432)\}$ 有 $4! = 24$ 個元素，找到的正規子群鏈為 $S_4 \supset A_4 \supset K_4 \supset \{e, (12)(34)\} \supset \{e\}$ ，其中 S_4 的交錯子群 A_4 有 $\frac{4!}{2} = 12$ 個元素， $K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$

有 4 個元素， $\{e, (1\ 2)(3\ 4)\}$ 有 2 個元素，合成因子列為 $(2, 3, 2, 2)$ (即 $\frac{24}{12}, \frac{12}{4}, \frac{4}{2}, \frac{2}{1}$) 都是質數，所以 S_4 是可解群。

4. $n \geq 5$ 時， S_n 有正規子群 A_n 。而 A_n 中每個元素都是偶置換，它們都可以表示成一些長度為 3 的輪換(簡稱 3-輪換)的乘積。例如 i, j, k, l 為四個不同的數，則兩對換有公共元素時 $(i\ j)(i\ k) = (i\ k\ j)$ ，兩對換無公共元素時 $(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (j\ k\ i)(k\ l\ j)$ 。若 H 為 A_n 的正規子群，當 $H \neq \{e\}$ 時， H 至少有一個 3-輪換元素(證明一)，且 H 必包含所有的 3-輪換元素¹⁸⁷(證明二)，因此 $H = A_n$ 。所以 $n \geq 5$ 時，找到 S_n 的正規子群鏈為 $S_n \supset A_n \supset \{e\}$ 。此時， S_n 有 $n!$ 個元素， A_n 有 $\frac{n!}{2}$ 個元素，合成因子列為 $(2, \frac{n!}{2})$ ，但 $\frac{n!}{2}$ 不是質數 (以 $n=5$ 為例，合成因子列為 $(2, 60)$ ，而 60 不是質數。) 因此， $n \geq 5$ 時， S_n 不是可解群。

¹⁸⁷ 參考洪有情教授講義的證明。亦可參考聶靈沼、丁石孫著：《代數學引論》，頁 82-84。

(證明一)

若 $n \geq 5$ 時， H 為 A_n 的正規子群， $H \neq \{e\}$ ，則 H 至少有一個 3-輪換元素。

〈pf〉 (1) $H \subseteq A_n \Rightarrow H$ 中的元素都是偶置換。

$\Rightarrow H$ 中的元素，除了 e 以外，至少會將 n 個字母中的 3 個字母更換位置(不動的字母至多為 $n-3$ 個)。

(2) 假設 H 不包含任何 3-輪換的元素

$\because |H| < \infty$ 且 $H \neq \{e\}$

$\Rightarrow H$ 中必能找到讓最多個字母不動的置換，設為 $\sigma (\neq e)$ 。

將 σ 寫成互斥輪換的乘積，則 σ 可能有兩種情形：

① σ 全為 2-輪換的乘積。(以下將說明此 σ 不存在)

$\because \sigma$ 為偶置換 $\Rightarrow \sigma$ 至少是兩個 2-輪換的乘積

$\Rightarrow \sigma$ 至少更換了 4 個字母位置，

設此 4 個字母為 a, b, c, d ，且

$$\sigma = (a\ b)(c\ d)(\cdot\cdot)\dots \in H$$

取 $m \neq a, b, c, d$ ，並令 $\tau = (c\ d\ m) \in A_n$

($n \geq 5$ ，所以至少有 a, b, c, d, m 五個字母)

$\because H$ 為 A_n 的正規子群

$$\Rightarrow \tau^{-1}\sigma\tau = (m\ d\ c)(a\ b)(c\ d)(\cdot\cdot)\dots(c\ d\ m) \in H$$

又由 $\sigma(c) = d$ ， $\tau^{-1}\sigma\tau(c) = m$ 知 $\sigma \neq \tau^{-1}\sigma\tau$

$$\Rightarrow \sigma^{-1}\tau^{-1}\sigma\tau \neq e \text{ (單位置換)}$$

此時找到 $\sigma^{-1}\tau^{-1}\sigma\tau \in H$ ($\because \sigma^{-1} \in H$ 且 $\tau^{-1}\sigma\tau \in H$) 且 $\sigma^{-1}\tau^{-1}\sigma\tau \neq e$ 。

檢驗各字母經置換 σ 和 $\sigma^{-1}\tau^{-1}\sigma\tau$ 後映射的結果，分兩組討論(一組為 a, b, c, d, m ，另一組為其他的字母)：

置換 \ 字母	a	b	c	d	m	a,b,c,d,m 以外的字母	
						被 σ 固定	被 σ 更換
σ	★	★	★	★	(不明)	全部固定	★
$\sigma^{-1}\tau^{-1}\sigma\tau$	a	b	★	★	★	全部固定	全部固定 或 只有 1 個不固定

(★ 表示映射後已更換為其他字母)

由上表看出， n 個字母中，第一組(σ 至多只固定了字母 m ，而 $\sigma^{-1}\tau^{-1}\sigma\tau$ 固定了 a, b 兩個字母)和第二組都是 σ 固定的字母數不比 $\sigma^{-1}\tau^{-1}\sigma\tau$ 多。整體而言， σ 固定的字母數仍較 $\sigma^{-1}\tau^{-1}\sigma\tau$ 少，此與「 $\sigma (\neq e)$ 為 H 中讓最多個字母不動的置換」產生矛盾。

$\therefore \sigma$ 不可能全為 2-輪換的乘積。

② σ 的乘積中至少有一個 n -輪換 ($n \geq 3$)。(以下將說明此 σ 不存在)

$\because \sigma$ 不可能只更換 3 個字母(設 H 不包含任何 3-輪換), 也不可能只更換 4 個字母(因 $(a b c d)$ 不是偶置換)。

$\Rightarrow \sigma$ 至少更換了 5 個字母, 設為 a, b, c, k, l , 且 a, b, c 這 3 個字母在同一個 n -輪換 ($n \geq 3$) 中。

設 $\sigma = (a b c \dots) \dots$, 並令 $\tau = (c k l) \in A_n$

$\because H$ 為 A_n 的正規子群

$\Rightarrow \tau^{-1}\sigma\tau = (l k c)(a b c \dots) \dots (c k l) \in H$

又由 $\sigma(b) = c$, $\tau^{-1}\sigma\tau(b) = l$ 知 $\sigma \neq \tau^{-1}\sigma\tau$

$\Rightarrow \sigma^{-1}\tau^{-1}\sigma\tau \neq e$ (單位置換)

此時找到 $\sigma^{-1}\tau^{-1}\sigma\tau \in H$ ($\because \sigma^{-1} \in H$ 且 $\tau^{-1}\sigma\tau \in H$) 且 $\sigma^{-1}\tau^{-1}\sigma\tau \neq e$ 。

檢驗各字母經置換 σ 和 $\sigma^{-1}\tau^{-1}\sigma\tau$ 後映射的結果, 分兩組討論(一組為 a, b, c, k, l , 另一組為其他的字母):

置換 \ 字母	a	b	c	k	l	a, b, c, k, l 以外的字母	
						被 σ 固定	被 σ 更換
σ	★	★	★	★	★	全部固定	★
$\sigma^{-1}\tau^{-1}\sigma\tau$	a	★	★	★	★	全部固定	(不明)

(★ 表示映射後已更換為其他字母)

由上表看出, n 個字母中, 第一組(σ 沒有固定任何字母, 而 $\sigma^{-1}\tau^{-1}\sigma\tau$ 固定了字母 a) 和第二組都是 σ 固定的字母數不比 $\sigma^{-1}\tau^{-1}\sigma\tau$ 多。整體而言, σ 固定的字母數仍較 $\sigma^{-1}\tau^{-1}\sigma\tau$ 少, 此與「 $\sigma(\neq e)$ 為 H 中讓最多個字母不動的置換」產生矛盾。

$\therefore \sigma$ 的乘積中不會有 n -輪換 ($n \geq 3$)。

(3) 由(2)知: 若 $n \geq 5$ 時, A_n 不可能有「既非 $\{e\}$, 也不包含任何 3-輪換的元素」的正規子群。

\therefore 若 $n \geq 5$ 時, H 為 A_n 的正規子群, $H \neq \{e\}$, 則 H 至少有一個 3-輪換元素。

(證明二)

若 $n \geq 5$ 時， H 為 A_n 的正規子群， $H \neq \{e\}$ ，則 H 包含所有的 3-輪換元素。

〈pf〉(1) 由證明一知道 $n \geq 5$ 時，若 H 為 A_n 的正規子群， $H \neq \{e\}$ ，則 H 至少有一個 3-輪換元素。設此 3-輪換為 $(ijk) \in H$ 。在 n 個字母當中，要證明 H 包含所有的 3-輪換元素，可設 i', j', k' 為 n 個字母的任 3 個字母，並證 $(i' j' k') \in H$ 。

(2) 令 $\sigma \in S_n$ 為 $\sigma(i) = i', \sigma(j) = j', \sigma(k) = k'$ ，即 $\sigma: \begin{bmatrix} i & \rightarrow & i' \\ j & \rightarrow & j' \\ k & \rightarrow & k' \end{bmatrix}$

$$\Rightarrow \sigma(ijk)\sigma^{-1} = (i' j' k')$$

① 若 $\sigma \in A_n$

$$\Rightarrow (i' j' k') \in H (\because H \text{ 為 } A_n \text{ 的正規子群})$$

② 若 $\sigma \notin A_n$

$\because n \geq 5$ ，可取異於 i', j', k' 的另 2 個字母 r, s ，再造一個偶置換 $(rs)\sigma \in A_n$ ($\because \sigma$ 為奇置換)。

$$\begin{aligned} \Rightarrow [(rs)\sigma] (ijk) [(rs)\sigma]^{-1} \\ &= (rs) [\sigma(ijk)\sigma^{-1}] (rs)^{-1} \\ &= (rs)(i' j' k')(rs)^{-1} \\ &= (i' j' k') \in H (\because H \text{ 為 } A_n \text{ 的正規子群}) \end{aligned}$$

(3) 由(2)知，

若 $n \geq 5$ 時， H 為 A_n 的正規子群， $H \neq \{e\}$ ，則 H 包含所有的 3-輪換元素。

(二) 五次以上方程式無法根式求解

當我們以加、減、乘、除及開方法找方程式的公式解時，面對的是文字係數的一般方程式。前文在「探索思維」討論 Galois 群時，曾推導出 n 次一般方程式 $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0$ (a_1, \dots, a_n 為文字係數) 的 Galois 群與 S_n 同構。

S_n 在 $n \leq 4$ 時為可解群，在 $n \geq 5$ 時不為可解群。我們也發現：次數不大於 4 的方程式都已被證實可以用根式求解；而若 $n \geq 5$ 時，至少有一個一般 n 次多項式 $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F(a_1, \dots, a_n)[x]$ ，使得 $f(x) = 0$ 的 Galois 群和 S_n 同構，因此不為可解群，所以 $f(x) = 0$ 不能用根式求解。

事實上，仍有一些五次或更高次的方程式可以找到根式解。例如 $x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ 與 $x^6 - 1 = 0$ 有相同的分裂體； $x^6 - 1 =$

$(x^3 + 1)(x^3 - 1) = (x + 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1)$ ，因此 $x^6 - 1 = 0$ 的解為 $x = \pm 1$ ， $\frac{1 \pm \sqrt{-3}}{2}$ ， $\frac{-1 \pm \sqrt{-3}}{2}$ ，與 $x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ 的解為 $x = -1$ ， $\frac{1 \pm \sqrt{-3}}{2}$ ， $\frac{-1 \pm \sqrt{-3}}{2}$ 都是可以用根式求解的。

然而另一個例子 $x^5 - x^4 - x^3 - x^2 - x - 1 = 0$ 就無法用根式求解，所以伽羅瓦證實仍存在一些新數是無法用根式表示出來的。

在 Mario Livio 所著，蔡承志譯的《無解方程式》一書中提到：

伽羅瓦為每則方程式設想出一組與該方程式相關的「遺傳密碼」— 該方程式的伽羅瓦群(Galois group)— 並證明伽羅瓦群的特性，可以決定方程式能不能以公式求解〔實為根式求解〕。(頁 151)

回顧本節的討論，我們由數學的五個重要思維方式：觀察、抽象、探索、猜測、論證，逐步認識了 Galois 理論的形成，並看到它解決了存在數學界許久的謎團。「Galois」儼然成為「創新」的代名詞。援引達爾馬斯(Andre Dalmass)所著的《伽羅瓦傳》中譯本的內容，作為本節的結束：

伽羅瓦說：「我在這裏進行分析之分析」，這種想法表明了他竭力想使這些新的、像辭匯表那樣地具有實用意義的基元得到使用。群論首先是數學語言的整理。(頁 39)

伽羅瓦的革命性，不僅在於他使這個理論具有生命，他的獨創性又賦予這個理論以必要的完整性；伽羅瓦還指出，這一理論富有成效，他並且把它運用到解代數方程的具體習題上。正因為如此，伽羅瓦是群論的真正創始人。(頁 36)

第二節 理論的應用

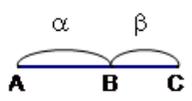
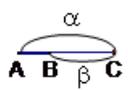
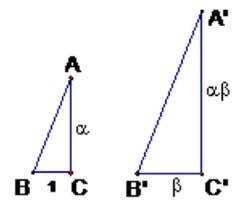
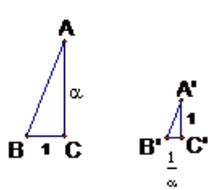
Galois 理論解決了代數上懸宕多時的方程式根式解問題。同樣地，它也跨足到幾何上，為一些古老的問題提供強而有力的證明。以下就以體擴展維度的概念，討論尺規作圖如何造數，進而說明解決古希臘時期幾何的三大難題。

一、尺規造數

(一)可造數

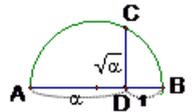
選取某固定長的線段作為單位長，如果我們以無刻度的直尺和圓規作圖，能作出長度為 $|\alpha|$ (其中 $\alpha \in \mathbb{R}$) 的線段，就把 α 稱為可造數 (Constructible number)。並將所有可造數所形成的集合設為 W ，即 $W = \{\alpha \in \mathbb{R} \mid \alpha \text{ 為可造數}\}$ ，則 W 為一個體，且所有的有理數都是可造數，因此 $\mathbb{Q} \subset W \subset \mathbb{R}$ 。

要說明 W 為一個體，只要說明：當 $\alpha, \beta \in W$ 且均為正數時， $\alpha + \beta$ 、 $\alpha - \beta$ 、 $\alpha \cdot \beta$ 、 $\frac{1}{\alpha}$ 都在 W 中即可。以圖示呈現：

	圖 示	說 明
$\alpha + \beta$		在一直線上取 A、B、C 三點，使 B 介於 A、C 之間，且 $\overline{AB} = \alpha$ ， $\overline{BC} = \beta$ ，則 $\overline{AC} = \alpha + \beta$ 。
$\alpha - \beta$		在一直線上取 A、B、C 三點，使 B 介於 A、C 之間，且 $\overline{AC} = \alpha$ ， $\overline{BC} = \beta$ ，則 $\overline{AB} = \alpha - \beta$ 。
$\alpha \cdot \beta$		作 $\triangle ABC \sim \triangle A'B'C'$ ， 且 $\angle ACB = \angle A'C'B' = 90^\circ$ ， $\overline{AC} = \alpha$ ， $\overline{BC} = 1$ ， $\overline{B'C'} = \beta$ ，則 $\overline{A'C'} = \alpha \cdot \beta$ 。
$\frac{1}{\alpha}$		作 $\triangle ABC \sim \triangle A'B'C'$ ， 且 $\angle ACB = \angle A'C'B' = 90^\circ$ ， $\overline{AC} = \alpha$ ， $\overline{BC} = 1$ ， $\overline{A'C'} = 1$ ，則 $\overline{B'C'} = \frac{1}{\alpha}$ 。

至於 $\alpha, \beta \in W$ 且為負數時，以上各情形亦不難獲得相同的結論。由此可得 W 為 R 的一個子體，且 $Q \subset W \subset R$ 。

如果 α 是正的可造數，則 $\sqrt{\alpha}$ 也是可造數。如下圖所示：

	圖 示	說 明
$\sqrt{\alpha}$		<p>在一直線上取 A、D、B 三點，使 D 介於 A、B 之間，且 $\overline{AD} = \alpha$，$\overline{DB} = 1$，並以 \overline{AB} 為直徑作半圓，再作過 D 且垂直 \overline{AB} 的直線交半圓於 C 點，則 $\overline{CD} = \sqrt{\alpha}$。</p>

由以上的討論，得到一個結論：對任何可造數進行加、減、乘、除、開平方根(開平方根僅限於正的可造數進行)等運算之後，仍然是可造數。

(二)可造點

由於 $W = \{ \alpha \in R \mid \alpha \text{ 為可造數} \}$ ，且 $Q \subset W \subset R$ 。我們可以擴充到座標平面 $R^2 (= R \times R)$ 上。如果 $\alpha, \beta \in W$ ，則 $(\alpha, \beta) \in W \times W$ 是 R^2 上的一個點，稱 (α, β) 為可造點(Constructible Point)。當我們用直尺連接兩個可造點所形成的直線叫可造直線；而以一个可造點為圓心，一個可造數為半徑，用圓規畫一個圓，此圓叫可造圓。

當我們作圖時，任意兩條相異可造直線的交點、任意一條可造直線與一個可造圓的交點、任意兩個相異可造圓的交點，都是座標平面上的可造點；每一個可造點的 x 座標值或 y 座標值都會是可造數。以下選定有理數體 Q 為此可造體，從 $Q \times Q$ 平面出發，將這三種作圖的交點加以討論：

1. 兩條相異可造直線的交點。

設 $(x_1, y_1), (x_2, y_2) \in Q \times Q$ ，連接此兩點的可造直線為 $(x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1)$ ，可簡化為 $a_1x + b_1y + c_1 = 0$ (其中 $a_1, b_1, c_1 \in Q$)；同理，另一條可造直線可設為 $a_2x + b_2y + c_2 = 0$ (其中 $a_2, b_2, c_2 \in Q$)。因

此，解聯立方程式 $\begin{cases} a_1x + b_1y + c_1 = 0 \dots \textcircled{1} \\ a_2x + b_2y + c_2 = 0 \dots \textcircled{2} \end{cases}$ 就可找到此兩直線的交點。

(1) 若這兩條相異直線互相平行，則聯立方程式無解，兩直線沒有交點，無法產生新的可造點。

(2) 若這兩條相異直線有一個交點，則解得 $x = \frac{b_1c_2 - b_2c_1}{a_1b_2 - a_2b_1}$ ，

$y = \frac{-(a_1c_2 - a_2c_1)}{a_1b_2 - a_2b_1}$ ，此時交點 $(\frac{b_1c_2 - b_2c_1}{a_1b_2 - a_2b_1}, \frac{-(a_1c_2 - a_2c_1)}{a_1b_2 - a_2b_1}) \in \mathbb{Q} \times \mathbb{Q}$ ，仍在

原來的 $\mathbb{Q} \times \mathbb{Q}$ 平面上，沒有產生新的可造點。

例：在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，兩條可造直線分別為 $2x - \frac{1}{2}y = \frac{4}{3}$ 及 $y = 5x - \frac{19}{6}$ ，

$$\text{解 } \begin{cases} 2x - \frac{1}{2}y = \frac{4}{3} \\ y = 5x - \frac{19}{6} \end{cases} \text{ 得 } x = \frac{1}{2}, y = -\frac{2}{3}, \text{ 此交點 } (\frac{1}{2}, -\frac{2}{3}) \in \mathbb{Q} \times \mathbb{Q}.$$

2. 一條可造直線與一個可造圓的交點。

設一條可造直線為 $ax + by + c = 0$ (其中 $a, b, c \in \mathbb{Q}$)，一個可造圓為 $(x - h)^2 + (y - k)^2 = r^2$ (其中 $h, k, r \in \mathbb{Q}$)。解聯立方程式

$$\begin{cases} ax + by + c = 0 \dots\dots\dots \textcircled{1} \\ (x - h)^2 + (y - k)^2 = r^2 \dots \textcircled{2} \end{cases} \text{ 可找到它們的交點。由 } \textcircled{1} \text{ 式得}$$

$$y = \frac{-ax - c}{b} \dots \textcircled{3}, \text{ 將 } \textcircled{3} \text{ 式代入 } \textcircled{2} \text{ 式得 } (x - h)^2 + (\frac{-ax - c}{b} - k)^2 = r^2, \text{ 整理得型}$$

如 $Ax^2 + Bx + C = 0$ (其中 $A, B, C \in \mathbb{Q}$) 的式子。此時，有三種情況：

(1) 若 $B^2 - 4AC < 0$ ，聯立方程式無實數解，圖形沒有交點，無法產生新的可造點。

(2) 若 $B^2 - 4AC = 0$ ，聯立方程式僅有一組解， $x = \frac{-B}{2A} \in \mathbb{Q}, y = \frac{-a(\frac{-B}{2A}) - c}{b} \in \mathbb{Q}$ ，圖形的唯一交點為可造直線與可造圓的切點，此切點仍是 $\mathbb{Q} \times \mathbb{Q}$ 平面上的點，並未產生新的可造點。

(3) 若 $B^2 - 4AC > 0$ ，聯立方程式有兩組解， $x = \frac{-B + \sqrt{B^2 - 4AC}}{2A}$ ，

$$y = \frac{-a(\frac{-B + \sqrt{B^2 - 4AC}}{2A}) - c}{b} \text{ 及 } x = \frac{-B - \sqrt{B^2 - 4AC}}{2A}, y = \frac{-a(\frac{-B - \sqrt{B^2 - 4AC}}{2A}) - c}{b}, \text{ 圖形有}$$

兩個交點。令 $\varepsilon = B^2 - 4AC$ ，則聯立方程式的解形如 $\begin{cases} x = \alpha \pm m\sqrt{\varepsilon} \\ y = \beta \pm n\sqrt{\varepsilon} \end{cases}$

(其中 $\alpha, \beta, m, n, \varepsilon \in \mathbb{Q}$ ，且 $\varepsilon > 0$)。此時，若 $\sqrt{\varepsilon} \in \mathbb{Q}$ (即 ε 是某個有理數的平方)，圖形交點仍在 $\mathbb{Q} \times \mathbb{Q}$ 平面；若 $\sqrt{\varepsilon} \notin \mathbb{Q}$ ，則產生了新的可造點，圖形交點所在的平面會從 $\mathbb{Q} \times \mathbb{Q}$ 平面擴展到 $\mathbb{Q}(\sqrt{\varepsilon}) \times \mathbb{Q}(\sqrt{\varepsilon})$ 平面。

例：(1) 在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，要求可造直線 $x+y=5$ 和可造圓 $x^2+y^2=2^2$

的交點，可解 $\begin{cases} x+y=5 \dots\dots ① \\ x^2+y^2=2^2 \dots\dots ② \end{cases}$ ，由①式得 $y=5-x\dots\dots ③$ ，

將③式代入②式得 $x^2+(5-x)^2=4$ ，化簡得 $2x^2-10x+21=0$ 。
因為 $(-10)^2-4 \times 2 \times 21 = -68 < 0$ ，所以聯立方程式無實數解，
圖形沒有交點，無法產生新的可造點。

(2) 在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，要求可造直線 $y=2$ 和可造圓 $x^2+y^2=2^2$ 的交

點，可解 $\begin{cases} y=2 \dots\dots\dots ① \\ x^2+y^2=2^2 \dots\dots ② \end{cases}$ ，將①式代入②式得 $x^2+4=4$ ，

解出 $x=0, y=2$ 為唯一一組解。圖形的交點 $(0, 2)$ 恰是直線與圓的切點，仍是 $\mathbb{Q} \times \mathbb{Q}$ 平面上的點，並未產生新的可造點。

(3) 在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，要求可造直線 $x-y=1$ 和可造圓 $x^2+y^2=2^2$

的交點，可解 $\begin{cases} x-y=1 \dots\dots\dots ① \\ x^2+y^2=2^2 \dots\dots ② \end{cases}$ ，由①式得 $y=x-1\dots\dots ③$ ，

將③式代入②式得 $x^2+(x-1)^2=4$ ，化簡得 $2x^2-2x-3=0$ ，

解出 $x=\frac{1 \pm \sqrt{7}}{2}$ 。當 $x=\frac{1+\sqrt{7}}{2}$ 時， $y=\frac{-1+\sqrt{7}}{2}$ ；當 $x=\frac{1-\sqrt{7}}{2}$ 時， $y=\frac{-1-\sqrt{7}}{2}$ 。

圖形有兩個交點 $(\frac{1+\sqrt{7}}{2}, \frac{-1+\sqrt{7}}{2})$ 及 $(\frac{1-\sqrt{7}}{2}, \frac{-1-\sqrt{7}}{2})$ ，它們都是可造點，
所在的平面從 $\mathbb{Q} \times \mathbb{Q}$ 平面擴展到 $\mathbb{Q}(\sqrt{7}) \times \mathbb{Q}(\sqrt{7})$ 平面了。

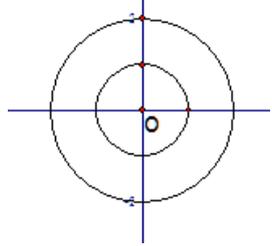
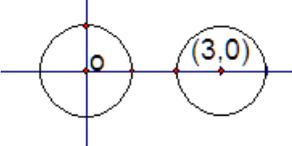
3. 兩個相異可造圓的交點。

設兩個可造圓為 $(x-h_1)^2+(y-k_1)^2=r_1^2$ 及 $(x-h_2)^2+(y-k_2)^2=r_2^2$
(其中 $h_1, h_2, k_1, k_2, r_1, r_2 \in \mathbb{Q}$)。

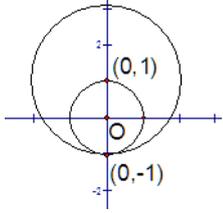
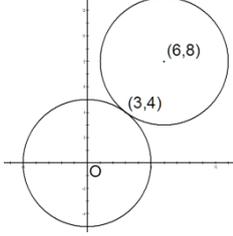
解聯立方程式 $\begin{cases} (x-h_1)^2+(y-k_1)^2=r_1^2 \dots\dots ① \\ (x-h_2)^2+(y-k_2)^2=r_2^2 \dots\dots ② \end{cases}$ 時，將①式減②

式，得 $(-2h_1+2h_2)x+(-2k_1+2k_2)y=r_1^2-r_2^2-h_1^2+h_2^2-k_1^2+k_2^2$ ，即
型如 $Ax+By=C\dots\dots ③$ (其中 $A, B, C \in \mathbb{Q}$)。此時將③式與①式(或③式與②式)
聯立，解得與「2. 一條可造直線與一個可造圓的交點」相類似的答案，
可能未產生新的可造點，也可能產生某些新的可造點；而交點若非仍在
 $\mathbb{Q} \times \mathbb{Q}$ 平面上，就是擴展到某個 $\mathbb{Q}(\sqrt{\mu}) \times \mathbb{Q}(\sqrt{\mu})$ 平面了。(其中 $\mu \in \mathbb{Q}$ ，
 $\mu > 0$ ，且任何有理數的平方都不是 μ 。)

例：(1)

$\mathbb{Q} \times \mathbb{Q}$ 平面上 兩個可造圓方程式	圖 形	結 論
$x^2 + y^2 = 1^2$ $x^2 + y^2 = 2^2$		兩圓無交點，無法產生新的可造點。
$x^2 + y^2 = 1^2$ $(x-3)^2 + y^2 = 1^2$		兩圓無交點，無法產生新的可造點。

(2)

$\mathbb{Q} \times \mathbb{Q}$ 平面上 兩個可造圓方程式	圖 形	結 論
$x^2 + y^2 = 1^2$ $x^2 + (y-1)^2 = 2^2$		兩圓有一個交(切)點(0, -1)，它仍在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，並未產生新的可造點。
$x^2 + y^2 = 5^2$ $(x-6)^2 + (y-8)^2 = 5^2$		兩圓有一個交(切)點(3, 4)，它仍在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，並未產生新的可造點。

(3)

<p>$\mathbb{Q} \times \mathbb{Q}$ 平面上 兩個可造圓方程式</p>	<p>圖 形</p>	<p>結 論</p>
<p>$x^2 + y^2 = 5^2$ $(x-6)^2 + y^2 = 5^2$</p>		<p>兩圓有兩個交點(3,4)及(3,-4)，它們仍在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，並未產生新的可造點。</p>
<p>$x^2 + y^2 = 1^2$ $(x-1)^2 + (y-1)^2 = 1^2$</p>		<p>兩圓有兩個交點(1,0)及(0,1)，它們仍在 $\mathbb{Q} \times \mathbb{Q}$ 平面上，並未產生新的可造點。</p>
<p>$x^2 + y^2 = 1^2$ $(x-1)^2 + y^2 = 1^2$</p>		<p>兩圓有兩個交點$(\frac{1}{2}, \frac{\sqrt{3}}{2})$及$(\frac{1}{2}, -\frac{\sqrt{3}}{2})$，它們都是新的可造點，所在的平面從 $\mathbb{Q} \times \mathbb{Q}$ 平面擴展到 $\mathbb{Q}(\sqrt{3}) \times \mathbb{Q}(\sqrt{3})$ 平面了。</p>
<p>$x^2 + y^2 = 1^2$ $(x-2)^2 + (y+1)^2 = 3^2$</p>		<p>兩圓有兩個交點$(\frac{-6+\sqrt{11}}{10}, \frac{3+2\sqrt{11}}{10})$及$(\frac{-6-\sqrt{11}}{10}, \frac{3-2\sqrt{11}}{10})$，它們都是新的可造點，所在的平面從 $\mathbb{Q} \times \mathbb{Q}$ 平面擴展到 $\mathbb{Q}(\sqrt{11}) \times \mathbb{Q}(\sqrt{11})$ 平面了。</p>

(三) 可造數的定理

綜合以上所討論的尺規作圖，當產生可造點 (α_1, α_2) ，就能找到可造數 α_1 與 α_2 的過程。我們可以知道：若 $\alpha \in W$ 為可造數，因為 $Q \subset W \subset R$ ，則可以找到一串符合根式擴展的體擴展鏈 $Q \subset Q(\sqrt{\varepsilon_1}) \subset Q(\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}) \subset \dots \subset Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_n}) \subset W$ (其中 n 是正整數)，使得 $\alpha \in Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_n})$ 。特別要說明的是： $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ 均為正數，且對於每一個 $i=1, 2, \dots, n$ ，都會滿足 $\sqrt{\varepsilon_i} \notin Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_{i-1}})$ ，可是卻有 $(\sqrt{\varepsilon_i})^2 \in Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_{i-1}})$ 的情形。

例如 $Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2}, \sqrt{5 + \sqrt{2}}) = Q(\sqrt{2}, \sqrt{k})$ ，其中 $k=5 + \sqrt{2}$ 。此時，

$\sqrt{2} \notin Q$ 但 $(\sqrt{2})^2 = 2 \in Q$ ， $\sqrt{k} = \sqrt{5 + \sqrt{2}} \notin Q(\sqrt{2})$ 但 $(\sqrt{k})^2 = 5 + \sqrt{2} \in Q(\sqrt{2})$ 。由此可見，可造數含有一個或數個平方根號，它們可能各自獨立存在也可能反覆重疊。

因為 $[Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_n}) : Q] = [Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_n}) : Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_{n-1}})] \times [Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_{n-1}}) : Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_{n-2}})] \times \dots \times [Q(\sqrt{\varepsilon_1}) : Q] = 2^n$ ，又因為 $[Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_n}) : Q] = [Q(\sqrt{\varepsilon_1}, \dots, \sqrt{\varepsilon_n}) : Q(\alpha)] \times [Q(\alpha) : Q]$ ，所以 $[Q(\alpha) : Q]$ 必可整除 2^n 。

於是有了以下結論：若 $\alpha \in W$ 為可造數，則 α 是 Q 上的代數元，而且 α 在 Q 上的最小多項式的次數為 2 的乘冪，即存在 t 為正整數或 0 ，使得 $[Q(\alpha) : Q] = 2^t$ 。 (註： $t=0$ 時，則 $\alpha \in Q \subset W$)

二、幾何學三大問題

早在古希臘時期，就有的幾何學三大問題為：倍積問題、方圓問題、三等分任意角問題，將伽羅瓦所提出的理論加以應用，都可獲得解決，分述如下：

(一) 倍積問題

所謂「倍積問題」，是以尺規為工具作一個正立方體，使它的體積等於某給定正立方體體積的二倍。這時候，假設給定的正立方體的一稜長為 1 ，所求作的正立方體的一稜長為 x ，則有 $x^3 = 2$ (即 $x^3 - 2 = 0$)的關係式產生，因此可得 $x = \sqrt[3]{2}$ 。

在尺規作圖中， $\sqrt[3]{2}$ 是否為可造數呢？我們可以發現 $\sqrt[3]{2}$ 在 Q 上的最小多項式為 $x^3 - 2$ ，因此 $[Q(\sqrt[3]{2}) : Q] = \deg(x^3 - 2) = 3$ ，而 3 不是 2 的乘冪，所以 $\sqrt[3]{2}$ 不是可造數。

「倍積問題」是個用尺規為工具不可能完成的問題。

(二) 方圓問題

所謂「方圓問題」，是要以尺規為工具作一個正方形，使它的面積等於某給定圓的面積。這時候，假設給定的圓的半徑為 1，所求作的正方形邊長為 x ，則有 $x^2 = \pi$ (即 $x^2 - \pi = 0$) 的關係式產生，因此可得 $x = \sqrt{\pi}$ 。

在尺規作圖中， $\sqrt{\pi}$ 是否為可造數呢？我們可以用反證法來說明。如果 $\sqrt{\pi}$ 是可造數，則 π 也是可造數，因此 π 是 \mathbb{Q} 上的代數元，這與「 π 是 \mathbb{Q} 上的超越數」互相矛盾。所以， $\sqrt{\pi}$ 不是可造數。

「方圓問題」是個用尺規為工具不可能完成的問題。

(三) 三等分任意角問題

所謂「三等分任意角問題」，是要以尺規為工具將任意角三等分。要說明此問題不可能完成，只須舉出一個角作為例子，證明無法用尺規作圖將該角三等分即可。

例如 60° 角，假設可用尺規作圖將它三等分，得出 20° 角。因 $\cos 60^\circ = \frac{1}{2} \in \mathbb{Q}$ 為可造數，則 $\cos 20^\circ$ 也會是可造數。但由三倍角的餘弦函數公式

得 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ ，令 $\theta = 20^\circ$ 代入得 $\cos 60^\circ = 4\cos^3 20^\circ - 3\cos 20^\circ$ ，

若設 $x = \cos 20^\circ$ ，則上式可改為 $\frac{1}{2} = 4x^3 - 3x$ ，整理成 $x^3 - \frac{3}{4}x - \frac{1}{8} = 0$ 。而

$x^3 - \frac{3}{4}x - \frac{1}{8}$ 在 \mathbb{Q} 上為既約多項式，它也是 $\cos 20^\circ$ 在 \mathbb{Q} 上的最小多項式，

所以 $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = \deg(x^3 - \frac{3}{4}x - \frac{1}{8}) = 3$ ，而 3 並不是 2 的乘冪，因此

得出 $\cos 20^\circ$ 不是可造數，這與我們的假設互相矛盾。可見得假設錯誤，事實上是： 60° 角不可以用尺規作圖三等分。

既然找到一個角 (60°) 不能用尺規作圖三等分，我們得到一個結論：「三等分任意角」是個用尺規為工具不可能完成的問題。雖然仍有某些特殊角 (例如 45° 、 90° 、 135° 、 $180^\circ \dots$ 等) 可用尺規作圖三等分，但想要以尺規為工具將任意角進行三等分作圖，是不可能的。

從伽羅瓦所提出的理論中的體擴展概念，間接地解決了古希臘幾何學三大問題。雖然到了 18、19 世紀幾何學的重心逐漸轉向，不再獨衷歐式幾何，有些數學家開始研究非歐幾何、射影幾何、微分幾何等其他新課題了，然而，這些經過好幾個世紀的古老數學問題，的確帶動了許多數學家的研究與投入，在過程當中也發展了許多研究的工具與方法，豐富了數學的發展。

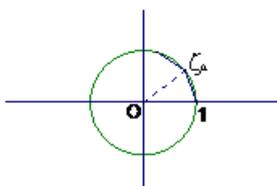
三、正 n 邊形的作圖問題

在平面幾何中，有些正 n 邊形是可以尺規作出圖形的，例如正三邊形、正四邊形(正方形)、正五邊形、正六邊形等，然而並非所有的正 n 邊形都可以尺規作出圖形來的。從伽羅瓦理論中的體擴展概念，可以證明：以尺規為工具，並不能作出所有正 n 邊形的圖形來。

例如 n=9 時，假設正九邊形可以用尺規作出圖形，則其內角與外角都可用尺規作出。它的每一個外角為 $\frac{360^\circ}{9} = 40^\circ$ ，既然 40° 角可用尺規作出，則將其二等分之後的 20° 角也可用尺規作出，所以 $\cos 20^\circ$ 為可造數。但由前文知道 $\cos 20^\circ$ 並不是可造數，因此產生矛盾。可見正九邊形並不可以用尺規為工具作出圖形來。

到底哪些正 n 邊形可以用尺規作出圖形呢？不難理解：正 n 邊形可以用尺規作出圖形的充要條件是可用尺規作圖將一個圓周 n 等分，此與圓的半徑大小無關。若以複數平面的原點為圓心，半徑設為 1，實數 1 作為其中一個等分點，則圓周的 n 等分點恰好是 $x^n = 1$ 的 n 個解 $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ ，其中 $\zeta_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ 。換句話說，「正 n 邊形可以用尺規為工具作出圖形來」

若且唯若「 $\zeta_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ 為可造數」。



(一) n 為質數時

以 $n=p$ 為質數的情形觀之， $\zeta_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ 在 \mathbb{Q} 上的最小多項式為 $x^{p-1} + x^{p-2} + \dots + x + 1$ ，因此 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ 。若 $p-1 = 2^t (t \in \mathbb{N})$ ，則 ζ_p 為可造數，也就可以用尺規作出正 p 邊形，而此時 $n=p=2^t+1$ 。換句話說，若 n 為型如 $2^t+1 (t \in \mathbb{N})$ 的質數，則正 n 邊形可以用尺規為工具作出圖形來。

讓我們來看看型如 $2^t+1 (t \in \mathbb{N})$ 的數是否都為質數呢？

t	1	2	3	4	5	6	7	8	9	10
2^t+1	3	5	9	17	33	65	129	257	513	1025
是否為質數	○	○	×	○	×	×	×	○	×	×

觀察上表，可以發現 $t=1,2,\dots,10$ 時，只有在 $t=1$ 或 2 或 4 或 8 時 2^t+1 才是質數。事實上，若 $2^t+1(t \in \mathbb{N})$ 為質數時， t 的質因數只可能是 2 。證明如下：¹⁸⁸

若 $2^t+1(t \in \mathbb{N})$ 為質數時， t 的質因數只可能是 2 。

(證明) 假設 t 有異於 2 的質因數

\Rightarrow 存在奇數 q ，使得 $t=2^mq$ ，其中 m 為正整數或 0 ，

此時 $2^t+1 = (2^{2^m})^q+1 = (2^{2^m})^q+1$

$\because q$ 為奇數

$\Rightarrow (2^{2^m}+1) \mid ((2^{2^m})^q+1)$

$\Rightarrow (2^{2^m}+1) \mid (2^t+1)$

$\Rightarrow 2^t+1$ 有因數 $(2^{2^m}+1)$

$\therefore 2^t+1$ 不為質數

這與前提「 2^t+1 為質數」產生了矛盾。

因此假設錯誤。

但對於所有的 $t=2^m(m=0,1,2,\dots)$ ，型如 2^t+1 的數是否都一定會是質數呢？法國數學家費馬(Pierre de Fermat 1601-1665 年)曾聲稱只要 $t=2^m(m=0,1,2,\dots)$ ， 2^t+1 就是質數。在 $m=0,1,2,3,4$ 時， $2^{2^m}+1$ 的確是質數，但歐拉(Euler 1707-1783 年，瑞士數學家)卻發現在 $m=5$ 時， 641 為 $2^{2^5}+1$ 的因數， $2^{2^5}+1$ 不是質數了。雖然如此，今只要是型如 $2^{2^m}+1$ 的質數，就被稱為「費馬質數」。至今瞭解的有 $3, 5, 17, 257, 65537$ 都是費馬質數，所以正三邊形、正五邊形、正 17 邊形、正 257 邊形、正 65537 邊形都可用尺規為工具作出圖形來。

(二) n 不限為質數時

至於在 n 不限為質數的情況下，哪些正 n 邊形可以用尺規作出圖形呢？高斯(Gauss 1777-1855 年，德國數學家)證明了以下定理：當 $n=2^k p_1 p_2 \dots p_s$ (其中 $k \geq 0$ ， p_1, p_2, \dots, p_s 為相異的費馬質數)時，正 n 邊形可用尺規為工具作出圖形來；反之，若可用尺規為工具作出正 n 邊形來，則 n 的質因數分解為 2 的乘冪與某些相異的(也可能都沒有)費馬質數的乘積。

以下列出 $n \leq 20$ 時，可用尺規為工具作出的正 n 邊形有：

n	3	4	5	6	8	10	12	15	16	17	20
質因數分解	3	2^2	5	2×3	2^3	2×5	$2^2 \times 3$	3×5	2^4	17	$2^2 \times 5$

¹⁸⁸ 參考洪有情教授講義的證明。

實際以尺規進行正 n 邊形作圖的數學家，往往投注許多年日與心力才完成作圖。在王芳貴編著的《代數學基礎》一書中就有以下這段記載：

$p=17$ 是費馬素數〔質數〕，故正 17 邊形是可以尺規作出的。在幾何上，1796 年高斯尺規作出了這個正 17 邊形，並以此為榮，希冀後人能在其墓碑上鏤刻一個正 17 邊形。1832 年，德國數學家力西羅〔Friedrich Julius Richelot (1808–1875)〕作出了正 257 邊形，作圖過程整整寫了 80 頁。其后蓋爾美斯〔德國數學家〕用了十年時間〔其手稿裝滿一整個手提箱，至今被德國哥庭根大學收藏著〕，作出了正 65537 邊形。(頁 153)

Galois 理論的提出，引發了數學界陣陣漣漪，從 Mario Livio 著，蔡承志譯的《無解方程式》一書中的這段話得到印證：

伽羅瓦輝煌精湛的觀點並不是憑空冒出來的。那些觀點解決了一個問題，問題的根源可以一直追溯至古巴比倫時代。儘管如此，之前毫不相干的幾種領域，卻因伽羅瓦掀起這場革命才匯總於一爐。(頁 332)

第四章 Galois 思想的文化意義

在 19 世紀初，伽羅瓦因鑽研數學，提出了迥異於當代的理論思想，不僅見解新穎獨到，且研究風格也自成一派。Galois 理論這一個深邃的思想，在數學史上所帶出來獨樹一格的創見，其特性內外兼具，將在本章進行較深入的探討。

除此之外，伽羅瓦站在歷史的洪流中，其思想與許多文化層面的發展都息息相關，讓人看到數學雖揭橥基礎科學的純粹性，卻神奇地滲透到各領域的細胞當中。在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，就有如下記載：

在人類文明中，數學如果脫離了其豐富的文化基礎，就會被簡化成一系列的技巧，它的形象也就被完全歪曲了。(前言，頁 vii)

的確，當我們看一齣舞台劇時，不會只看劇情的發展，我們同時也在欣賞其中的服裝、佈景、光線、音樂、對白、聲響等；同樣地，數學的魅力絕不是單單存在於技法上，而是由它的整套思想所散發出來的。伽羅瓦的理論不僅在數學史上造成極大的震撼，其思想的豐富性在文化上亦處處留下痕跡。

本章嘗試從不同的文化層面來認識 Galois 思想，共分為五節：第一節「思想的特性」，第二節「美學的視野」，第三節「藝術的延伸」，第四節「音樂的對話」，第五節「數學教育的省思」。期使此研究能達到拋磚引玉之效，引出更多人願意繼續投注心力開發此園地，以發掘 Galois 思想更多的文化意義！

第一節 思想的特性

Galois 理論宛若被丟在歷史洪流中的一塊璞玉，現身時原是沾滿塵泥，未能引起人們的注意；待被有識之士發覺後，才成為眾人關愛的珍寶。本節將以伽羅瓦的理論思想為主體，從其表現形式、深層洞見，到蘊含的主要精神等，均加以剖析其所呈現的獨特風格。

一、表現形式

伽羅瓦因為年輕就逝世，所留下的數學著作有限。今彙集整理他曾投遞到科學院的論文和發表在期刊雜誌的著作，以及一些筆記、書信等資料，可以看出伽羅瓦記錄思想的方式，也是獨特而不凡的。

(一) 小而美

伽羅瓦的著作雖然不多，且篇幅不大，卻都包含著他深刻的思想，蘊藏著充滿秩序、和諧的美感。茲將伽羅瓦的著作表列如下：¹⁸⁹

伽羅瓦生前	遞 科 學 院	<ul style="list-style-type: none"> • 1829 年交了兩篇專論給柯西，內容都是關於方程式論的研究。 • 1830 年交論文：《論方程式得以根式求解的條件》角逐數學成就大獎。 • 1831 年交論文：《方程式得以根式求解的條件》。
	發 表 於 雜 誌	<ul style="list-style-type: none"> • 1829 年 3 月 1 日在《純粹和應用數學年報》(<i>Annales de mathématiques pures et appliquées</i>)，發表數學論文〈對循環連分數定理的證明〉。 • 1830 年在《菲魯薩克學報》(<i>Ferrusac's Bulletin</i>) 四月號發表了一篇獨創理論〈一份有關解代數方程的研究報告〉。 • 1830 年在《菲魯薩克學報》六月號又有兩篇伽羅瓦的作品，分別是〈有關解代數方程的筆記〉及〈有關數論的筆記〉。
伽羅瓦死後	書 信	<ul style="list-style-type: none"> • 1832 年 5 月 29 日赴約決門前夕，致好友奧古斯特·舍瓦烈的信。
	期 刊 雜 誌	<ul style="list-style-type: none"> • 1846 年在約瑟夫·劉維的《純數學與應用數學》(<i>Journal de mathématiques pures et appliquées</i>)雜誌第 10 卷，發表伽羅瓦的作品：根式可解的方程式。 • 1897 年由法國數學學會出版的《伽羅瓦數學作品集》。1951 年以新版出版。 • 1908 年哥底葉威臘爾父子出版社以單行本出版：《埃瓦里斯特·伽羅瓦手稿》收錄伽羅瓦的數學筆記。

¹⁸⁹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 77-78。

除此之外，在 1866 年數學家塞雷特(J.A. Serret 1819-1885 年)亦在他的《高等代數教程》(*Cours d'algèbre supérieure*)(第三版)中，對伽羅瓦的思想概念作了敘述與介紹。它以教科書的方式呈現，由伽羅瓦的置換群理論出發，釐清方程式可否根式解的觀念。

在 1870 年數學家約登(Camille Jordan 1838-1922 年)於他所發表的《置換論》(*Traité des substitutions et des équations algébriques*)一書中，對於 Galois 理論有了全面而完整的闡釋。¹⁹⁰

在伽羅瓦的著作中，以 1846 年約瑟夫·劉維為他所發表的 60 頁手稿，為學術研究立了新的標竿，成為劃時代的代表。在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本，就記載著：

伽羅瓦的數學著作，至少是那些保存下來的，共有六十小頁。從來還沒有像篇幅這樣小的著作曾經給作者帶來如此之高的聲譽。
(頁 33)

(二)簡單扼要

伽羅瓦的論述摒棄了繁瑣的計算，只專注於如何「預見」該面臨的計算，那是一個路線的引導，因此像路標一樣簡單扼要。況且伽羅瓦選擇走一條自關的道路，天才的跳躍思考，顯現在前進的速度較一般人更快。雖然他的思慮清晰，但書寫的步驟簡略，交代不夠清楚，以至於生前所投遞的論文，總讓人以為缺乏說服力的證明，而未受科學院的青睞。

以下節錄自達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本記載：

伽羅瓦對繁瑣累贅的計算方法感到不可抑制的厭惡，因此，他的表述極其簡單扼要。但是他所寫的一切，都因為具有數學家不倦鑽研的思想而放出異彩；他的每一部著作，彷彿都是一次新的大膽的躍進；先前已達到的又落到後面，不再使作者發生興趣了。伽羅瓦的洞察力是驚人的。他對待讀者的態度有時似乎很傲慢(他並不怎麼關心讀者的興趣)，但實際上這不過是思想十分獨特、具有堅定的目的性的例證而已。(頁 33)

伽羅瓦的表述方式，的確傳達了一位開拓者的積極態度。雖然他的論文未能詳細闡述想法細節與進行完整連貫的包裝，但以二十歲的年輕生命，為數學界所留下的遺產卻是頗具份量且不容小覷的。最難得的，是這簡要的理論背後，所帶出的「結構」思維，改變了人們觀看事物的視角，延續至今仍不見消退。

¹⁹⁰參考 Morris Kline 原著，林炎全、洪萬生、楊康景松譯：《數學史》(中冊)(台北市：九章出版社，民 72 年)，頁 417；康明昌：《幾個有名的數學問題》，頁 119；袁小明編著：《數學史》，頁 209。

二、深層洞見

伽羅瓦為了傳達其深層的思想，創造和運用了許多獨特的研究工具，使其研究的理論呈現應有的節奏，如此精準的洞見更促成了群論的發展，沛然莫之能禦。在張雄、李得虎編著的《數學方法論與解題研究》一書中，就記述著：

數學方法的產生和數學理論知識的產生是比翼雙飛、共同發展的，有時候方法先於理論，有時候則是理論派生方法，更多情況下則是兩者齊頭並進。(頁 3)

伽羅瓦在認識了當時數學家們已達到的數學成就之後，面對他想解決的數學問題，並不依循眾多數學家們所研究的方式。他的目光看得極遠，選擇了找尋一個可決定科學長期發展的理論。他要完成的事情不僅僅是解決表面問題而已，還有內部深層要探究，因此所採用的方法也十分獨特，整理如下：

(一) 引入「結構」思維

伽羅瓦對於學校選用的代數教科書，不重推理只重計算技巧，感到不屑一顧。他希望不必進行計算就能找到「預見」如何計算的途徑¹⁹¹；也看清人的腦力無法同時承載許多細節，因此，特別期待能有同時掌握幾種運算的系統。要完成這樣的任務，必須對感興趣的事物有清楚的結構分析，這個明智的判斷讓伽羅瓦奠定了天才的地位。

伽羅瓦要建立一套數學結構，運用抽象推理，將一些外表看來相當不同的概念，用相同的結構來描述，藉此以釐清所有模糊或糾纏不清的概念。¹⁹²

「結構」思維的開發，的確帶領人類向前跨越了一大步，而這也正是「群」逐漸萌芽的階段。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，記載了如下的敘述：

然而，賦予數學結構多方面用途的卻正是抽象思考。於是數學結構才得以在多門學科和多方面概念環境一體適用。(頁 221)

(二) 建立「體」的雛形

在伽羅瓦的研究過程當中，先認識了多項式係數所在的體，再引進「分裂體」的概念，且規範了體擴展的維度以及定義正規擴展，使方程式與其解所在的環境，能明確地確定下來，不再像飄散在空中的棉絮般

¹⁹¹ 參考達爾馬斯原著：《伽羅瓦傳》，頁 34。

¹⁹² 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 223。

無所適從。

伽羅瓦探討方程式根式解的可能性時，也由「體」的概念出發，悉心觀察四次一般方程式獲得根式解的關鍵環節，分析並整理出其特徵，再以此所得到的結論，推測 n 次一般方程式可根式求解的環境。若缺乏「體」的穩固存在，所有的研究可能都找不到根基，這是伽羅瓦聰明抉擇的另一明證。

(三) 直搗「置換群」陣營

伽羅瓦沒有直接研究方程式本身，卻針對方程式所有解的排列特性加以分析，並確認這些解的置換排列與對稱性的確有關聯。而每一個方程式會依照它的係數體和分裂體之間的關係，產生一個它所對應的置換群(即 Galois 群)。若按照置換群的運算方式歸類，可得到各種不同結構的置換群。例如 (Z_4, \circ) 與 (K_4, \circ) 同為四個元素的群，但結構明顯有差異，如下：

\circ	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

\circ	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

然而，許多時候卻會發現：某些不同樣式的方程式卻是對應到相同的置換群。於是，伽羅瓦不想大量研究各式各樣紛雜的方程式，而專注於置換群的分析與瞭解。

在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本，就記載著：

在分析求解的方程時，他把某種運算群與這個方程聯繫起來，並證明方程的特性反映在該群的特點上。既然不同的方程可以「有」同一個群，那麼，無須研究所有這些方程，只須研究與之相適應的群就可以了。(頁 36)

早在 1815 年，法國數學家柯西就曾寫過一篇置換群的論文，但尚未深入地研究出重要結論，因此像是沒有靈魂的軀體。直到 1831 年伽羅瓦寄給泊松那一篇論文，才正式討論群論，雖然這時候所談的也只是置換群，但因賦予了它的完整性，此時所出現的群才像是有了生命。¹⁹³

¹⁹³ 參考康明昌：《幾個有名的數學問題》，頁 120。

伽羅瓦聰明地掌握了數學上的重要語言—置換群，它的所有結構就明明白白地講述了對稱的特性。研究分析置換群，可整理列出各種「結構表」，在必要時可為失序的混亂景象，提供一個核對比較的參照標準，以找到它歸屬的類別。伽羅瓦以淺白的「置換群」作為數學語言的表達，實則傳遞了相當有深度的思想。

在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，記載了如下的敘述：

儘管發明時心中並沒有遠大目標，最終群論卻成為一切對稱性的「官方」語言。乍看之下，置換排列在群論中扮演這般重要的角色讓人略感訝異。畢竟，儘管大家都很熟悉對稱性，在我們的日常生活中，置換排列卻不是那麼引人矚目。在日常生活中，置換排列若隱若現，有時還見於最料想不到的地方，但生活中確實可以發現置換排列。(頁 214)

到了 1878 年，英國數學家亞瑟·凱萊(Arthur Cayley 1821-1895 年)證明了一個重要定理，說明所有的群都有與之對應且性質相同的置換群，更加呼應了伽羅瓦的睿智判斷。節錄 Mario Livio 著，蔡承志譯的《無解方程式》的敘述如下：

凱萊定理說明，基本上，任何群都是某置換群的副本(與某置換群同構)，和群元件及元件間執行哪些運算都不相干。我們以這項定理為基礎，領悟到群是一種抽象實體。(中略)...我們可以用任意群來著手處理，把群的細部特徵剝除盡淨，最後只剩最質樸的根本要素。(頁 221)

由伽羅瓦所關注且率先登場的置換群，牽引出「群論」的諸多研究，影響後來學術界甚鉅。因此，伽羅瓦配得被冠上「群論創始人」的尊榮。

(四) 善用「映射」傳輸

伽羅瓦為了發展構思的理論，靈活地運用了代數變換中的「映射」工具。今至少提出三處地方，加以說明。

1. Galois 群的元素是一個映射

為了按照某種規律(符合預解式)，忠實地將方程式的每一解運送至方程式的某一解，伽羅瓦設計了方程式分裂體的自同構，使它保持對係數體作恆等映射，而所有這些自同構形成方程式的 Galois 群。方程式的 Galois 群中的每一個元素，是一個自同構，也是一個映射。

2. Galois 群視為置換群也是一個映射

伽羅瓦成功地在方程式的 Galois 群與某個置換群之間建置同構，無縫接軌，使 Galois 群視為某個置換群的副本，包括該置換群的運算、結構等，全部都在此 Galois 群中顯現。這兩者之間的同構關係，也是一個映射。

3. 體擴展的中間體與 Galois 群的子群之間存在一個映射

Galois 理論中，對於體擴展的中間體與 Galois 群的子群之間的聯繫，找到一個一一對應的映射作為銜接，並體現理論的知識內容。在丘維聲所著的《數學的思維方式與創新》書中的記載提到：

伽羅瓦在發現了四次一般方程的根式升鏈與群 G 的遞降子群列之間有密切聯繫後，抽象出有限伽羅瓦擴張〔正規擴展〕 E/F 的中間域集〔體集〕與伽羅瓦群 $G = \text{Gal}(E/F)$ 的子群集之間存在一一對應。(頁 163)

當我們觀察 Galois 理論中這個「映射」的傳輸功能，可以發現它有幾個特點：

- (1) 一對一雙向可逆。
- (2) 體擴展維度與 Galois 群子群的階數，關係恆定。
- (3) 體的正規擴展與 Galois 群的正規子群，同生同滅。

(五) 界定「正規子群」與「合成因子」

在 Galois 理論中，由於有限正規體擴展 E/F 的中間體集與 $\text{Gal}(E/F)$ 群的子群集之間，存在有一一對應，若中間體 M 恰使 M/F 為正規體擴展，也將自然地帶出 $\text{Gal}(E/F)$ 群的正規子群 $\text{Gal}(E/M)$ ；因此，是在某種條件存在之下，才有 $\text{Gal}(E/F)$ 群的正規子群的誕生。伽羅瓦認真整理，並界定出「正規子群」乃左陪集與右陪集相同的子群；也將 Galois 群的階數除以正規子群的階數稱為「合成因子」。

有了「正規子群」與「合成因子」，伽羅瓦才能繼續發展「可解群」的概念，進而解決方程式根式求解的問題。

綜觀伽羅瓦所採取的研究方法，處處充滿創意。他擅於建構思想的空間，並且總在疑似閉鎖處重新開展新路，其不拘泥且靈活的手法，令人敬佩。在張雄、李得虎編著的《數學方法論與解題研究》一書中，就記載著：

為解決實踐上和理論上提出的各類數學問題，勢必創造出各種不同的數學方法，相應的數學知識也就接踵而來。例如，為尋求高次代數方程求根公式問題，不知多少數學家為之努力，創立了許多的方

法和理論，直到伽羅瓦(Galois)創立了「群論」，才使這一向人類智慧挑戰的難題得到徹底解決。伽羅瓦群論是近代數學的重大突破，被稱為『群論』思想方法，然而卻是源於那個代數難題。(頁 7)

三、思想精神

「Galois 理論」是近世代數很重要的里程碑，其孕育的源頭，來自於伽羅瓦個人的特質、數學發展的進程，以及時代的演進等因素。然而，成就一個偉大的思想，正是這些源頭當中的優質因素巧妙融合精煉的成果。

觀察伽羅瓦的成長過程，發現他的性格有幾個特點：

性格特點	說 明
革命精神	伽羅瓦對於時勢常提出針砭，力圖改變現狀，願意承擔風險。
高度企圖心	伽羅瓦具有熾烈的想像力，嚮往開創新局。
專注鑽研	伽羅瓦的「預見」並非偶然，而是來自於天才專一心志的覺察能力。
自主支配	伽羅瓦懂得掌控各種存在的條件，以達成目的。

因為具有以上各種性格特點，伽羅瓦的創造力十足。

而具有獨特創造力的曠世奇才，能夠徹底改變數學風貌，在科學史上留下劃時代的地位，重要的關鍵就在於時機已成熟。在達爾馬斯(Andre Dalmas)著的《伽羅瓦傳》中譯本，就記載著：

十九世紀初期，代數變換已變得如此複雜，以致向前進展實際上已經成為不可能的事情了。...數學家們不再能夠「預見」了。甚至拉格朗日也無法把擱淺的解代數方程的問題向前推進(伽羅瓦卻做到了這點)。.....必須尋找新道路的時機來到了。決定這一時機的決不是偶然性，而是必然性。天才的特徵就在於能覺察到這種必然性，並且立即對它產生反應。(頁 38)

以下，我們將對於 Galois 理論的思想精神，作更細部的探討與分析。

(一) 獨特創新的洞察力

伽羅瓦以他獨特的眼光，看見方程式解彼此間的特性乃取決於方程式背後的結構關係。他從這一洞見中尋索解開謎團之鑰，認識到方程式解宛如形成一個社群，在這個社群的組織網絡，可以從梳理當中找到方程式各個解的定位。因此，伽羅瓦感興趣的是研究方程式解的置換群，他知道在這個新領域中有他要找的答案。

節錄 Mario Livio 著，蔡承志譯的《無解方程式》的敘述如下：

伽羅瓦的洞見根本是個奇蹟。科學史上常見超乎時代「憑空」生成的發現，……這些都是時機成熟的觀念。(頁 210)

當數學家有超凡的洞見時，即使是一點微小的亮光，卻可能帶出令人驚奇的效果。因為 Galois 理論走一條獨特新穎的道路，不同於當時一般人的想法，致使他生前那微小的亮光一再地被輕忽，直到伽羅瓦死後才陸續被重視與推崇。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，有如下的記載：

許多數學家每思及伽羅瓦，都有相同的敬畏感受。伊利諾大學的約瑟夫·羅特曼(Joseph Rotman)曾對我說：「伽羅瓦的群發明是個神來之筆。畢竟，在那同一時代研究根式可解性問題的偉大數學家阿貝爾，並沒有構思出群論。確實，似乎只有柯西才能賞識伽羅瓦的成就，他在 1840 年代〔伽羅瓦過世後 8 年〕返回法國途中領悟到這點，後來柯西深入鑽研群的學理課題，這才發展出其他數學領域的群論應用。」牛津大學代數學家彼得·紐曼(Peter Neumann)也說：「伽羅瓦對於群的根本道理具有超凡洞見，不過他還有同等超凡的悟性，能領會我們該如何把群運用於方程式理論—最後更發展出我們如今所稱的伽羅瓦理論(最終這構成現代方程式理論)。」(頁 210-211)

(二) 大膽躍進的勇氣

伽羅瓦因熱衷於政治，追隨共和派的運動，培養了革命的勇敢精神，也反映在他對學術的態度上。他急於打破不合時宜的局勢，試圖建立新的秩序；他定睛於未來，懷著使命必達的企圖心。

在伽羅瓦的理論思想中，可見他從方程式的係數體出發，以「體擴展」解構原係數體，再建立新的較大的係數體，大破大立的精神，逐步進逼方程式的分裂體，造成各個係數體與分裂體之間活動空間的限縮，降低方程式解彼此置換的可能性，也讓方程式的所有解一一現形。他的論證方式指引了科學長期發展的方向，並奠定了結構概念的

基礎。

在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，有如下的記載：

伽羅瓦對哪種方程式能夠以公式求解提出的證明，就是突破思考框架的具體表現—為了解答代數方程式的問題，他發展出一個完整的嶄新數學分支。(頁 326)

由此可見，伽羅瓦在思想上是大膽躍進的，他不願受制於舊傳統的約束，他要開創新局。在言談中也曾出現「未來數學家的使命」、「所選擇的道路」等想法。¹⁹⁴縱觀伽羅瓦在世的歲月極為短暫，卻活出了超越世代的學術生命。

(三) 抽絲剝繭的探究心

伽羅瓦規劃了前進的路線之後，還必須將整個思想概念落實建立。因此對於每個環節都要清楚掌握，「群」的結構更要仔細剖析，才能自主支配各種狀況；尤其若想研究任何特殊問題(例如方程式的根式解)時，必須用科學方法對於群的元素加以分析，再藉由遵循群的結構及邏輯推演所得到的一般理論，找到或預見所要探究的結論。

在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本，就記載著：

伽羅瓦說：「我在這裏進行分析之分析」，這種想法表明了他竭力求使這些新的、像辭匯表那樣地具有實用意義的基元得到使用。群論首先是數學語言的整理。(頁 39)

在整套理論構建的過程當中，伽羅瓦引進了相當多新穎的觀念，包括 Galois 群、正規子群(Normal Subgroup)、同構(Isomorphism)、單群(Simple Group)、合成群(Composite Group)、可解群(Solvable Group)等。有了這些觀念，理論的框架更為紮實穩固，也使伽羅瓦的立論更加有了秩序。

(四) 協同合作的器度

伽羅瓦的生活經驗，包括求學、政治狂熱、愛情等方面的遭遇，都成了澆灌他學術研究的養分。事實上，數學家伽羅瓦的學術研究模式，總帶著革命者伽羅瓦的積極態度與社會性格。在達爾馬斯(Andre Dalmás)著的《伽羅瓦傳》中譯本，就記載著：

¹⁹⁴參考達爾馬斯原著：《伽羅瓦傳》，頁 21。

伽羅瓦早在聖佩拉吉監獄裏，就想到未來科學家們的團結：「科學家生來並不比其他人要過孤獨的生活；他們也是屬於特定時代的人，而且遲早要協同合作。到了那時候，將有多少時間騰出來用於科學。」

大概，沒有一位科學家有過伽羅瓦那樣把科學理想與社會理想結合起來的；大概，這種結合從來不曾引起來自政府方面如此瘋狂的迫害的。(頁 39)

伽羅瓦專注於獨創的 Galois 群。他掌握變動的因子，從群的結構變化去探究問題的根源。如以方程式的係數體進行擴展，相對地將使方程式對應的 Galois 群之結構更改並縮小；尤其是當方程式的係數體進行「根式擴展」時，對應的 Galois 群所表現出的更像是具有組織的聚合，此時衍生的「正規子群」可作為代表。

另一方面，「同構」的運用充分銜接了不同領域的相關性，而能夠合作的基礎，就在於「結構」的相通性；儘管外表看來極其不同的事物，在「結構」的整規之下，可達成一致性，並共同完成更偉大的理論。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，有如下的記載：

伽羅瓦離家赴死之前，把一批文稿留在書桌上，我們在其中一頁發現幾則批註，裡面夾雜了數學塗鴉和幾項革命理念。……提出共和宣言之後，接著又是數學分析，彷彿從頭到尾就是個完整的思維。顯然在伽羅瓦心中，團結和不可分割的概念，對數學及革命精神一體適用。群論正發揮了這種功能——讓各色各樣看似無關的學科，從根本上整合構成不可分割的模式。(頁 333-334)

不論是「群」或「同構」，Galois 思想掌握了以抽象的聚合模式，探討內部相關與外部聯繫所形成的秩序，使得學術研究也顯現了協同合作的器度。

(五) 登高俯瞰的眼光

伽羅瓦看待問題時，不會拘泥於問題本身，他的眼光會從「點」擴張到「線」或「面」，甚至更拉高視野，看到縱深「立體的空間」。以研究「五次一般方程式是否可以根式表其解？」為例，由於各個數學家所在乎的事情不相同，選擇的研究方式也有差異；然而伽羅瓦直接去尋找「方程式可以根式求解的判斷準則」，待判斷準則有了成果之後，自然就能水到渠成地引出「特徵值為零的體上的 n 次一般方程

式，在 $n \geq 5$ 時無法以根式表其解」的結論。

在丘維聲所著的《數學的思維方式與創新》書中的記載提到：

「會當凌絕頂，一覽眾小山」。居高臨下，關鍵問題解決了，其他問題就迎刃而解了。(頁 163)

伽羅瓦佔據了制高點，看待事物能掌握全貌，對於研究的路線也能夠精準抉擇。當時他拾級而上到達制高點的階梯，卻是未能引起一般人注意的「排列變換」，在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，有如下的記載：

我們分析排列特性後就有把握預測最後結果，並且不必實際動手試驗。這也是伽羅瓦理論背後的基本哲理。他發現一種巧妙的作法，只要檢視方程式解的排列對稱特性，就可以藉此判定方程式是否能夠求解。(頁 204)

而在達爾馬斯(Andre Dalmat)著的《伽羅瓦傳》中譯本也記載著：

如果有足夠深邃的智慧，能夠立即掌握到不僅是我們已知的東西，而且是各種各樣一般的數學真理的全部總和，那麼就有可能借助某些普通原理中的同樣方法，合乎邏輯地、又似乎機械地引申出這些真理；這樣，就不會再有科學家在研究工作中所常碰到的障礙和困難了。(頁 50)

伽羅瓦的思想因具備了以上所列：獨特創新的洞察力、大膽躍進的勇氣、抽絲剝繭的探究心、協同合作的器度、登高俯瞰的眼光等精神，開創了數學史上獨一無二的新思維，並導引出極為有價值、全新的研究領域。

第二節 美學的視野

自古，從人類有數學活動開始，數學美學思想與數學活動就已是相伴相生。回首觀看數學的歷史，會發現遠在古希臘數學的發展中，就經常出現令人讚嘆的美感。近代英國著名的數學家哈代(Godfrey H. Hardy 1877-1947 年)在《一個數學家的自白》(A Mathematician's Apology)一書中，就曾提出：

現在也許難以找到一個受過教育的人，對於數學美的魅力全然無動於衷。數學美可能很難定義，但它的確是一種真實的美，和任何其他的美一樣。

195

後來有一些研究數學的學者，相當醉心於數學美的種種特性，遂更深入探討形成這種美感的因素，發現不論是在形式上或內容中，數學常表現出簡單、統一、對稱、秩序、新奇、神秘等美感。而伽羅瓦的生命雖極為短暫，但所鑽研的學術思想卻能如此深邃，背後必定具有對於「美」極強烈的崇高敬意！

其實，「美學」(Aesthetics) 這個名詞是由德國哲學家鮑姆嘉通(Baumgarten 1714-1762 年)在 1735 年首次使用的，主要研究美的本質及其意義，可作為哲學的一個分支。

在數學美的分類當中，大致可區分為三大特徵：簡單美、和諧美、奇異美。¹⁹⁶以下將探討伽羅瓦思想與數學美學所擦出的火花。

一、簡單美

人類從認識生存的環境開始，就相信上帝創造宇宙本著簡單的原則進行。義大利科學家伽利略(Galileo Galilei, 1564-1642 年)就曾說過：「數學是上帝用來書寫宇宙的語言。」¹⁹⁷因此，簡單美成為數學美的首要特徵。

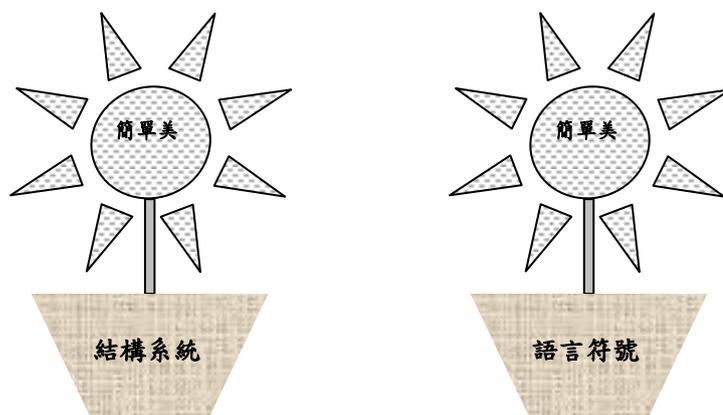
數學的簡單美可從兩方面表現出來：一個是「結構系統」，另一個則是「語言符號」。前者美感的來源奠基於深層的組織，後者美感的來源則仰賴於表層的傳達。但無論源頭為何，它們都像豐沛的土壤般孕育出簡單美的花朵來。

代數學不僅將符號代替常數或變數以進行各種運算，也對各種抽象化的結構進行研究。無疑地，代數學的興起，使數學在簡單美的實現上發揮得淋漓盡致。

¹⁹⁵ 轉引自徐炎章等著：《數學美學思想史》(台北市：曉園出版社有限公司，1998 年)，序。

¹⁹⁶ 參考徐炎章等著：《數學美學思想史》，頁 22。

¹⁹⁷ 轉引自徐炎章等著：《數學美學思想史》，頁 122。



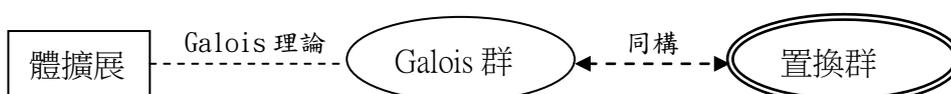
「結構系統」簡化複雜的理論，幫助人類深入瞭解數學的奧妙。節錄自徐本順、殷啟正所著的《數學中的美學方法》¹⁹⁸一書中的記載，如下：

所謂結構美，正如法國數學家龐加萊〔Jules Henri Poincaré 1854 - 1912 年〕所說：「數學的結構美是指一種內在的美，它來自各部分的和諧秩序，並能為純粹的理智所領會，可以說，正是這種內在美給了滿足我們感官的五彩繽紛美景的骨架，使我們面對一個秩序井然的整體，能夠預見數學定理。」(頁 80)

「語言符號」可以降低人類在思考時的腦力勞動，可稱職地作為數學的傳達工具。節錄自徐本順、殷啟正所著的《數學中的美學方法》一書中的記載如下：

數學語言是一種特殊的語言，因為它有一整套的數學符號系統。(中略)。一個世界範圍內公認的某種符號系統，能夠突破各民族語言的隔閡而成為全人類共同的統一的表述工具。(中略)。數學語言借助於數學符號把思維運算(過程)扼要地表現出來，並能準確地、深刻地把現象的結構表現為其不變式。(頁 80-81)

在「結構系統」方面，我們看到 Galois 理論銜接了方程式的「Galois 群」和「體擴展」的關係，也看到「置換群」與方程式的「Galois 群」的結構系統有其共通性，更在「可解群」的檢驗方法下透視了方程式「根式擴展」的可能性。伽羅瓦將他深刻的思想以如此完美的體系呈現，令人驚豔不已！



¹⁹⁸徐本順、殷啟正著：《數學中的美學方法》(中國大連：大連理工大學出版社，2008 年)。

在「語言符號」方面，伽羅瓦成功地標舉了「置換群」的功用，它將任一方程式所有解的對稱性表露無遺。若將有限置換群表列成一個符號表，當我們查看時，只要掌握與方程式的 Galois 群同構的置換群，就可解讀方程式根式解的秘密！將置換群作為數學語言的符號，是伽羅瓦的創見，它也帶動了後來群論的發展。

置換群表列

置換群	極大正規子群列	合成因子列	是否為可解群
S_2	$\{e\}$	2	是
S_3	$A_3 \cdot \{e\}$	2, 3	是
S_4	$A_4 \cdot K_4 \cdot \{e, (1\ 2)(3\ 4)\} \cdot \{e\}$	2, 3, 2, 2	是
S_5	$A_5 \cdot \{e\}$	2, 60	否
$S_n (n > 5)$	$A_n \cdot \{e\}$	$2, \frac{n!}{2}$	否

德國偉大的科學家愛因斯坦(Albert Einstein 1879-1955 年)曾說過：

「我們在尋求一個能把觀察到的事實聯結到一起的思想體系，它將具有最大可能的簡單性。」¹⁹⁹

Galois 思想能充分掌握「體擴展—Galois 群—置換群」之間的結構系統，並整理出「置換群」的合成因子列作為語言符號，讓原本混亂的「五次一般方程式是否有根式解？」問題，變得有秩序且散發單純的美感。

二、和諧美

任何事物在動態中若能達到有秩序的平衡狀態，就會呈現一種和諧美。數學一直在傳達著統一、對稱、整齊等特性，因此，和諧美也是數學美當中不可或缺的特徵。以下是和諧美幾個主要表現形式的描述：

¹⁹⁹轉引自徐炎章等著：《數學美學思想史》，頁 320。

表現形式	描 述
統 一	部分與部分，部分與整體之間的和諧、協調。 ²⁰⁰
對 稱	<ol style="list-style-type: none"> 1. 物體(圖形)在某種變換條件下，其相同部分間有規律重覆的現象，稱為對稱。 2. 一個物體(圖形)在對稱變換後重合於另一個物體(圖形)的變換，是「相互對稱」。²⁰¹ 3. 一個物體(圖形)在對稱變換(異於恆等變換)後仍重合於本身的變換，是「自身對稱」。²⁰² 4. 空間有軸對稱、中心對稱、鏡對稱； 時間有周期、節奏對稱、旋律對稱。²⁰³
整 齊	有條理；有次序；有規則。

18 世紀時，在德國有一位精通美學的科學家康德(Immanuel Kant 1724-1804 年)，雖然他在科學上有許多輝煌的成績，但後人對他的印象卻以哲學家居多。康德對於科學美學的思想有較深刻的見解，當時在歐洲的科學研究，有不少觀點都印證了康德的說法。在徐紀敏著的《科學美學思想史》中有一段記載如下：

康德認為宇宙的美並不完全在於它的現存部分，還應當追溯到它的形成過程。像過去那樣用孤立、靜止的方法來研究自然界的美是遠遠不夠的了，而是要用聯繫、發展的觀點來研究自然界的美。(頁 327)

伽羅瓦出生於康德逝世後不久，我們在伽羅瓦的理論思想中所看到的一些美學呈現，的確可對照於康德的見解，最主要是將「發展變化」納入了美學領域的觀點²⁰⁴。

對於伽羅瓦的理論思想所表現的和諧美，整理如下：

²⁰⁰ 參考徐本順、殷啟正著：《數學中的美學方法》，頁 89。

²⁰¹ 參考徐炎章等著：《數學美學思想史》，頁 300。

²⁰² 參考徐炎章等著：《數學美學思想史》，頁 300。

²⁰³ 參考徐本順、殷啟正著：《數學中的美學方法》，頁 93。

²⁰⁴ 參考徐紀敏著：《科學美學思想史》(中國湖南長沙市：湖南人民出版社，1987 年)，頁 344-345。

(一) 統一性

1. 體擴展與 Galois 群之間的聯繫，都能統一協調出和諧美。
2. Galois 群與同構的置換群之間的關係密不可分，幾乎是同步運作。

(二) 對稱性

1. 方程式所有解彼此之間的對稱性，是整個 Galois 理論的核心思想。
2. 一般方程式的各項係數，都可表示成方程式所有解的基本對稱函數。對稱性又在此顯現。

(三) 整齊性

1. 正規體擴展是充滿秩序感的「發展變化」。
2. 正規子群的界定，能保有整齊的美感，並與正規體擴展相互呼應。

其中「對稱性」這個美學因素在 Galois 理論的思想中占了極重要的地位，而由伽羅瓦前導所帶出的群論研究更彰顯了它的重要性。在徐本順、殷啟正所著的《數學中的美學方法》一書中，有如下記載：

抽象的群概念與對稱性這一美學因素密切相關，對稱性的抽象分析在建立群概念方面有著重要意義。它和抽象的網絡概念一樣，都是從現實世界中看上去互不相干的對象，經過對稱的抽象分析而建立起來的。
(頁 96-97)

伽羅瓦的理論之所以如此優美，是他掌握了方程式解的運動法則，並在置換群的結構上作了相當多的分析，以探求其規律。在徐紀敏著的《科學美學思想史》中有一段記載如下：

他〔康德〕認為，數學分析是最適宜描述宇宙運動規律的方法。由數學分析所表述的理論，可以得到人們的讚美，它的美甚至可以達到眩人耳目的程度。(頁 331)

追求數學的美感一直是許多數學家的信念。法國數學家龐加萊(Jules Henri Poincaré 1854-1912 年)就曾說過：

數學家們非常重視他們的方法和理論是否優美，這並非是華而不實的作風。那麼，到底是什麼使我們感到一個解答、一個證明優美呢？那就是各個部分之間的和諧、對稱和恰到好處的平衡。一句話，那就是井然有序，統一協調，從而使我們對整體和細節都能有個清楚的認識和理解，這正是產生重要成果的原因所在。²⁰⁵

²⁰⁵ 轉引自徐炎章等著：《數學美學思想史》，頁 313。

三、奇異美

數學之所以迷人，還有一個極重要的特徵，就是奇異美。奇異美包含了出人意料、新奇感和神秘感等美感經驗。以下是奇異美的幾個主要表現形式的描述：

表現形式	描 述
出人意料	對原本熟悉的事物，竟有意想不到的功用或詮釋，而產生讚嘆。
新奇感	對陌生的事物，感到新鮮、奇特。
神秘感	對事物的過程或結果充滿謎樣的疑惑，卻有所期待。

在伽羅瓦的創見中，處處顯出奇異美，分列如下：

(一) 出人意料

1. 方程式的根式解

從 15 世紀到 18 世紀的三百年間，數學家們竭盡心力尋找一元五次方程式的根，卻始終無所斬獲。最主要是人們循著舊有的模式尋根，從方程式的外在形式探求卻永不得其法；直到伽羅瓦開創新路徑，從方程式的內部結構分析，才得到解答。伽羅瓦的研究方式完全不在世人的預料中，令人讚嘆不已！

2. 置換群

置換群在方程式的根式解意外現身且擔任要角，讓世人大感意外。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，記載了如下的敘述：

儘管發明時心中並沒有遠大目標，最終群論卻成為一切對稱性的「官方」語言。乍看之下，置換排列在群論中扮演這般重要的角色讓人略感訝異。畢竟，儘管大家都很熟悉對稱性，在我們的日常生活中，置換排列卻不是那麼引人矚目。在日常生活中，置換排列若隱若現，有時還見於最料想不到的地方，但生活中確實可以發現置換排列。(頁 214)

3. 同構

同構有時可為彼此不同族類的兩群搭起橋樑。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中，有如下記載：

然而，就算排列如此重要，光憑排列本身決無法道出群論的全貌—群所含的抽象概念遠比排列更浩瀚。特別是，若是兩項不同的問題，能以彼此同構(也就是具有相同結構)的群來描述特性，就構成一個重要的線索，可由此窺見兩項問題的關聯密切得超乎你的預料。(頁 221)

4. 尺規造數、幾何學三大問題、正 n 邊形作圖

這些古老的問題存在了上千年，在人類腦海中的印象，早已是被認證過的難題了，卻因著 Galois 理論思想而獲得解決，算是 Galois 理論帶來的意外收穫。

(二) 新奇感

1. Galois 理論

伽羅瓦所作的研究，風格新穎獨特，致使未獲同時期學界所接受，並造成其學術價值延後被肯定。

2. Galois 群

當時，Galois 群是一個創新的名詞，其定義本身就充滿新奇感，尤以「置換」作為 Galois 群的元素，更是產生動態的美感。

3. 正規子群

當時「群」的概念剛起步，「正規子群」是伽羅瓦所創，對一般學者是一個陌生的名詞，卻能與正規體擴展形成相互呼應的聯繫，無不令人嘖嘖稱奇。

4. 可解群

「方程式是否可以根式求解？」原本是方程式的事，卻由一個宛若外星人的新興名詞—可解群—來完成任務，在當時是頗令人感到好奇的！

(三) 神秘感

1. 合成因子列

伽羅瓦把方程式可否根式解之謎交付給「合成因子列」，它變成方程式的一組密碼，彷彿上帝的秘密就藏在其中。

2. 抽象結構

一般人大多只會從看得到的事物去推想，甚少從看不到的事物去臆測。伽羅瓦所研究的抽象結構理論，沈靜地向內部探索卻充滿堅定的力量，好似一趟尋幽訪勝之旅！

其實，奇異美不是一蹴可及的。德國數學家克羅內克(Leopold Kronecker 1823-1891 年)在 1874 年發表了一篇論文，對於奇異美的功能有了一番闡述：

一旦人們闖入了所謂的奇異性的大門，研究工作馬上就會碰到真正的困難，然而，也立即會在它的深邃處發現新觀點、新知識的豐富保障。²⁰⁶

雖然伽羅瓦的研究在他生前未受肯定，但在他逝世十一年後由法國數學家約瑟夫·劉維引介紹給世人，才造成數學界的震驚。研究伽羅瓦思想的風潮一波接著一波，也連帶地造成各相關領域的重視，紛紛對抽象結構的研究產生了興趣，「結構主義」因此在伽羅瓦逝世百年後興起。

結構主義是 1933 年在法國的布爾巴基(Bourbaki)學派所提出的，此學派發表了《數學原本》(*Elements of mathematics*)學術著作，當中並認為數學乃是一門研究抽象結構的科學。²⁰⁷在徐炎章等所著的《數學美學思想史》一書中，有如下記載：

結構主義則是先從全局觀點來分析各個數學分支之間的結構差異和內在聯繫，然後再對每門數學深入分析其基本結構的組成方式，與形式化公理方法相比，結構主義則是更高一步、更深一層的抽象和概括。這樣做不僅有助於挖掘外表上相距甚遠的各個數學理論之間的內在親緣關係，解除一般數學理論中非本質的界限，而且有助於擴大數學理論的應用範圍，為數學在人類活動各個方面得到最廣泛的應用打下穩固的基礎。(頁 240)

從古希臘以來，數學的發展就帶著一種審美觀，不論是學習數學的學生或研究數學的學者，常在探尋的過程中欣賞到其中所蘊含的種種秩序、和諧與意涵，而感受愉悅的樂趣。在 J.N.Kapur 所著的《數學家談數學本質》²⁰⁸一書中，引述了法國數學家龐加萊(Henri Poincare)曾說過的一段話：

首先，內行們從數學中得到樂趣，就像人們從繪畫和音樂中得到的一樣。他們欣賞數和形的精美的和諧，他們驚奇地看到，新的發現向他們展示了意外的前景並因而給他們帶來歡樂，儘管美學並未介入，但這難道沒有美學特徵嗎？只有少數幾個有特權的人可以說欣賞了它的全部美，但在最高的藝術中不也正是如此嗎？(頁 26)

²⁰⁶ 轉引自徐炎章等著：《數學美學思想史》，頁 26。

²⁰⁷ 參考徐炎章等著：《數學美學思想史》，頁 239。

²⁰⁸ J.N.Kapur 著，王慶人譯：《數學家談數學本質》(台北市：儒林圖書有限公司，1992 年)。

伽羅瓦思想的歷史價值，可上及三百年前的五次方程式獲得解決，甚至追溯到古希臘三大幾何問題的探討；而在其後的學界，因著群論的發揚光大，各領域也風起雲湧地將結構分析納入研究。伽羅瓦成為劃時代的偉大數學家，已是公認的事實。伽羅瓦以其極短暫的生命所發出的一點點亮光，卻貫串照亮了兩千年來的學術界。如此微小火苗，終成熊熊火炬傳遞漫延開來，其美學價值自是不言而喻的！

第三節 藝術的延伸

伽羅瓦思想席捲整個世紀之後，仍像一顆閃亮的星星般灼灼發亮，它像藝術品一樣讓人津津樂道，所散發出來的藝術特質是不同於感性美的「理性美」。英國數學家哈代(Godfrey Harold Hardy 1877-1947 年)曾將數學比喻為藝術：「數學定理的美麗在很大程度上依賴其嚴肅性」。²⁰⁹

本節將從兩方面來探討 Galois 思想在藝術(尤其是視覺藝術)上所滲入的痕跡，包括追蹤形式的或形狀的「對稱群」，以及立足不同場域所開創出的「多視角」。

一、追蹤「對稱群」

(一) 形式的

伽羅瓦在尋找方程式的根式解時，將方程式的所有解玩弄於掌心之中，尤其對各解間的對稱性特別感興趣。雖然它不是任何形狀的對稱，卻是高度抽象以形式呈現的對稱。

例如在有理係數的方程式 $x^4 - 7x^2 + 10 = 0$ 中，因可將左式分解，方程式改寫成 $(x^2 - 2)(x^2 - 5) = 0$ ，其解為 $x = \sqrt{2}$ 或 $-\sqrt{2}$ 或 $\sqrt{5}$ 或 $-\sqrt{5}$ 。若分別以 a 、 b 、 c 、 d 代替 $\sqrt{2}$ 、 $-\sqrt{2}$ 、 $\sqrt{5}$ 、 $-\sqrt{5}$ 時，則 a 和 b 交換不會改變 $x^2 - 2 = 0$ ，稱 a 和 b 之間存在有「代數對稱」；類似地， c 和 d 交換不會改變 $x^2 - 5 = 0$ ，稱 c 和 d 之間也存在有「代數對稱」。

於是針對方程式解的置換狀況，我們可以構築出一個對稱群： $\{e, (a\ b), (c\ d), (a\ b)(c\ d)\}$ ，這個對稱群中元素(置換)與元素(置換)的組合，仍是保有原「代數對稱」特性的元素(置換)，它們是一群捍衛對稱特性的勇士所組成的群體，我們將此對稱群稱為原方程式的 Galois 群。

(二) 形狀的

在平面上所見的對稱變換，包括平移、鏡射、旋轉或它們之間的簡單組合。²¹⁰若是圖形經變換後看起來仍與變換前一樣(圖形上的點可能已移動了位置)，則此圖形是對稱圖形。

圓形是最明顯的對稱圖形，當它對圓心作任何角度的旋轉，或是在任一直徑作鏡射，以至於經過有限次旋轉與鏡射的組合變換之後，看起來仍與變換前相同。因此，這些所有變換的總集合，就形成了一個圓形的對稱群。

²⁰⁹ 參考鄭毓信著：《數學教育哲學》，頁 72；J.N.Kapur 著，王慶人譯：《數學家談數學本質》，頁 303。

²¹⁰ 參考曹亮吉著：《阿草的數學聖杯》(台北市：天下遠見出版股份有限公司，2003 年)，頁 233。

在 Keith Devlin 所著，洪萬生、洪贊天、蘇意雯、英家銘譯的《數學的語言》²¹¹中記述著：

一個圖形的對稱群是一個數學結構，就某一意義上來說，它捕捉了圖形可見的對稱程度。以圓為例，它的對稱群是無限的，因為對於一個圓的旋轉，存在著無限多種可能的角度，而且，也有無限多條可能的直徑可以被鏡射。圓的對稱變換群的豐富性對應了視覺對稱的高等級—「完美對稱」(perfect symmetry)，這是我們注視著圓時就能觀察到的。(頁 253)

比較一個正 n 邊形的對稱變換與圓形的對稱變換，可以發現有許多的差異。此時，旋轉變換不再接受任何角度了，只剩 n 種旋轉(模 360 度，即忽略旋轉圈數)能保持圖形相同；鏡射變換也減少為 n 種。將這些篩選出來的旋轉變換、鏡射變換，以及它們之間的有限次變換組合聚集起來，就可形成正 n 邊形的對稱群。

對於任一個完全不對稱的圖形，它也有一個對稱群，此對稱群只包含單位變換這個元素。所以，圖形的對稱群無所不在。

在人類的心智活動中，到處可見從具象昇華到抽象的情形，對稱性即為一例。節錄自 Keith Devlin 所著，洪萬生、洪贊天、蘇意雯、英家銘譯的《數學的語言》一段文字如下：

幾何學始於我們週遭世界的可見模式：形狀的模式。但是我們的眼睛感知到了其他的模式：可見的模式並不總是形狀，而在於形式。對稱的模式就是一個明顯的例子。一抹雪片或一朵花的對稱，清楚地與那些物體明顯的幾何一致性有關。對稱的研究捕捉了形狀更深刻、更抽象的面向之一。因為我們總是察覺這些深層的、抽象的模式為美，它們的數學研究可以被描述為美感中的數學。(頁 249)

由此可見，在各類藝術的呈現當中，不論是形狀上或形式上的對稱性變換，都有著 Galois 思想的核心觀點；而此一觀點並非伽羅瓦所創，卻是緣於伽羅瓦站在對的位置，致使得以窺見上帝創造中，精心鋪設「對稱」的美麗痕跡。

²¹¹ Keith Devlin 著，洪萬生、洪贊天、蘇意雯、英家銘譯：《數學的語言》(台北市：商周出版，2011 年)。

二、開創「多視角」

伽羅瓦的研究工作不僅證明及解答了數學上的重要問題，更重要的意義，則在於他不拘泥於舊思維卻勇於開創新局的精神。

西元 19 世紀以來，面對科學與藝術的蓬勃發展，我們以伽羅瓦開放且嚴謹的態度，來審視各種新興的結構體系，會有更多的看見。以下將從「結構是本質」出發，開拓「典範可轉移」的視角，再進而看清「現代藝術的崛起」。

(一) 結構是本質

Galois 理論運用抽象結構來進行探討，將繁瑣的問題化約為統整的思想，解決了困擾數學家們數百年之謎。對於數學上許多方面的研究，如果都以內在結構作為思考，將會歸在同一種學問當中。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中就有如下記載：

事實上，龐加萊還認為「整個數學就是群的學問」。先前看似完全無關的領域，如代數方程理論，各色各樣的幾何學，甚至數論(藉由尤拉和高斯的開創性研究成果)，霎時由單一基本結構統合為一。
(頁 238)

起先，數學研究的對象在於空間形式和數量關係。後來，形式從空間出走，關係也脫離了數量，數學開始研究純形式與純關係。當不侷限於空間和數量時，所抽象出來的形式和關係，稱之為「結構」²¹²，例如代數結構、平面幾何結構、拓樸結構、序結構等。而一個集合可以同時有幾個結構，而形成「系統」，例如實數系具有代數結構(運算)、序結構(大小)、拓樸結構(連續)等。²¹³

20 世紀 30 年代開始，在法國有一群數學家，以尼古拉·布爾巴基(Nicolas Bourbaki)為筆名，撰寫現代高等數學的著作。他們認為用「公理方法」可以將數學看成一種統一的科學。節錄自張景中所著的《數學與哲學》中的記載如下：

數學推理的長鏈背後還有更本質的東西。這種更本質的東西，真正反映了數學特點的東西是什麼呢？布爾巴基學派稱之為「結構」。
(頁 104)

²¹² 參考張景中著：《數學與哲學》，頁 118。

²¹³ 參考張景中著：《數學與哲學》，頁 112。

而在人類的生存環境中，我們搜索著熟悉或類似的場景，由許多活動記錄也可理解：結構是事物的本質。諸如：地圖和實際的地理狀況、流程圖和會議的進行、玩具模型與真實物品，都有相同或相似的結構。

又如許多語言學家投入分析不同語言的結構，且致力釐清多種語言之間相互的關聯。以台灣原住民所使用的語言屬於「南島語系」而言，就具有許多古南島語的特徵。在李筱峰所著的《台灣史 101 問》²¹⁴書中記載：

台灣在荷蘭人及大量漢語族人移入之前，即已居住有達數千、數萬年的原住民族，他們都屬於南島民族。

從語言的觀點看，台灣的原住民(不論是所謂的「高山族」或「平埔族」)，使用的語言屬於「南島語系」(Austronesian language family)，或稱「馬來亞玻利尼西亞語系」(Malayo-Polynesian language family)，與南太平洋區域住民，像印尼、馬來西亞、菲律賓、玻里尼西亞.....的語言同屬於南島語系。(中略)

一九八四年，語言學者 Robert Blust 提出南島語源自台灣的論說，因為透過語料的蒐集、分析，發現台灣原住民的語言分歧最多，且具有最多南島語的特徵。(頁 33-34)

語言藉由其結構的共通性，作為傳遞情感意念的工具，其流通性也自然地擴散開來。但歷史的殘酷現象，卻說明了強權的侵害也包括語言的霸凌，很可惜地，致使許多具優美特質的語言在地球上逐漸消失。

同樣地，各種藝術藉由不同素材與表現手法的呈現，傳達了其本質的部分，也由此激發了人們的情感；而為了追求美的價值，數學也發展出對於結構的研究。在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，有如下記載：

事實上，對美感愉悅的尋求，一直影響並刺激著數學的發展。從一大堆自相誇耀的主題或模式中，數學家們有意或無意之中，總是選擇那些具有美感的問題。古典時期的希臘人鑽研幾何，是因為幾何的形式和邏輯結構對他們來說是美好的。他們重視發現自然界中的幾何關係，並不是因為這些發現能幫助他們更好地征服自然，而是因為這些發現揭示了美的結構。(頁 480)

同樣地，當我們從許多不同領域或學科當中，提取抽象的屬性或概念，可能會發現它們具有相同的本質；並能藉此在視覺、聽覺、觸覺等方面搭建出熟悉的結構思維，盡情遨遊於其中。²¹⁵藝術的理性美於焉產生！

²¹⁴ 李筱峰著：《台灣史 101 問》(台北市：玉山社，2013 年)。

²¹⁵ 參考 M.Kline 著，張祖貴譯：《西方文化中的數學》，頁 476。

(二) 典範可轉移

伽羅瓦擺脫了傳統路線，不再從方程式的外在形式去尋求根式解，卻從方程式解的內在本質去認識問題。他靈活地從一個熟悉的結構轉移到另一個新開發的結構，兩者並不衝突，卻成功地豎立了代數學發展的新標竿。以同樣的開放角度觀看幾何學的發展，也可清楚地看到兩千年來在人們腦中早已根深柢固的歐氏幾何，於 19 世紀時也面臨了幾種非歐幾何的出現，歐氏幾何不再是唯一的典範。

歐幾里得的《幾何原本》是在西元前 300 年左右寫成的，流傳兩千多年且遍佈各地，並曾翻譯成多種語言發行，其印刷量在西方是僅次於聖經的書籍。《幾何原本》一書共分為 13 卷，在書中定義了 23 個幾何名詞，並對一些未加證明卻公認的命題列成 5 條公理及 5 條公設。其中公理是關於量的命題，公設則是關於幾何的命題，當中第五條公設為：若一直線與其它兩直線相交，以至該直線一側的兩內角之和小於兩直角，則那兩直線延伸足夠長後必相交於該側。²¹⁶數學家們發現第五條公設敘述冗長複雜，作為不證自明的公設太牽強，延續到西元 1800 年時，這條公設已經成為幾何學「不完美」的標誌。

在 19 世紀時，陸續出現不同於歐氏的幾何，包括羅巴切夫斯基(Никола́й Ива́нович Лобачёвский 1792-1856 年，俄羅斯數學家)，以及鮑耶(János Bolyai 1802-1860 年，匈牙利數學家)都嘗試更換第五條公設，並在新的結構體系中推出新的幾何學理論。偉大的數學家高斯也研究非歐幾何，但未公開發表，直到他逝世後被披露生前對非歐幾何關注的文獻，非歐幾何因此而有了確切的立足點。其後相繼有黎曼的幾何、射影幾何、拓樸學研究，它們並非為了挑戰歐氏平面幾何的地位，只不過是選擇了另一種結構而發展出另一套的幾何學。

在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，有如下記載：

幾何學的四個不同的分支—歐氏幾何、射影幾何、以及兩種非歐幾何。誠如我們所看到的那樣，這些分支顯得各不相同，並且有時還彼此不相容、不協調。然而，近代一個最令人欣喜的數學上的貢獻表明：射影幾何可以被看作是公理性的基礎，這樣，其他三種幾何中的結果，都可以看作是射影幾何中的特殊定理。換句話說，所有這四種幾何的內容現在已經形成了一個和諧的整體。(頁 479)

以黎曼幾何為例，它和歐氏幾何有些定理不同。例如一條直線的所有垂線在黎曼幾何中交於一點(可思想地球的經度線)，在歐氏幾何卻是不相交；又如黎曼幾何的「不存在平行線」、「直線不能無限延長」、「三角形內

²¹⁶參考張景中著：《數學與哲學》(台北市：九章出版，1996 年)

角和大於 180° 」等定理雖不符歐氏幾何的結構，但在球面幾何將「大圓」視為直線的結構下卻是合宜的。

古時候人類的活動區域多只侷限於小範圍，所看到的地面是平坦的感覺，因此歐氏平面幾何率先取得了研究這個世界的主導權。兩千年的發展下來，甚至代數方程與幾何概念也相互解釋，彼此形成一個和諧且似乎牢不可破的結構體系。但平面幾何不可能是唯一的真理，當我們將球面放到歐氏幾何的框架中時，必然會發現許多「不合身」的定理。因著非歐幾何的創立，人們開始認識到「數學空間」和「物理空間」是有區別的；歐氏幾何可以在數學空間中建立王國，卻不能精確描述物理空間的真實狀態。以往人們將兩者視為相同的習慣與思維，必須徹底地重新調整。

在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，有如下一段話頗發人深省：

確實，歐氏幾何被應用了數千年，它也適合人們長期以來所形成的思維習慣。(中略)。空間非常巨大，而我們所接觸的區域相對來說，不過是地球表面上的一個點。我們誰知道火星表面的世界的幾何，或者甚至是地球表面上空十英里的事情呢？比起成百條曾經在一段日子裏很有效，但最終必定還是為人們所拋棄了的科學定律來，歐氏幾何不一定會比那些定律好。(頁 428)

根據德國數學家菲利克斯·克萊因(Felix Christian Klein 1849-1925 年)在 1872 年發表了《埃爾蘭根綱領》(Erlangen Program)，當中將各種幾何統一在一個理論框架下。此框架選用幾何變換所組成的「群」作為工具，而在所給定變換群下不變的幾何性質，就構築出對應的幾何，因此不同幾何有不同的變換群。例如歐氏幾何變換群是保角保距的剛性運動群，同樣地，射影幾何、拓樸學或其他非歐幾何，也都各自為保持某種特性而有自己的變換群。

在 Mario Livio 著，蔡承志譯的《無解方程式》一書中就有如下記載：

然而，根據克萊因的激進觀念，世上還有遠比前述更繁複多端的幾何學。另外有些變換型式或能扭曲、延展的物件，還得以定義出新式幾何學。換句話說，把所有幾何學統合為一的基本骨幹概念，就是對稱群(symmetry group)。(中略)。根據克萊因的見解，數學家定義幾何學時必須提供一組變換群，並指出在這類變換情況下依舊保持不變的一群實體。(頁 237-238)

人們隨著新創的幾何學，建立了不同的空間觀。歐氏幾何原來不容侵犯的角色，也漸漸卸除那份尊容；而非歐幾何正是造成思想解放的重要因

素，它對科學、哲學、藝術，乃至於宗教，都形成了革命性的影響。因此，人們的想像力和創造力更自由地發揮，眾多的創作像雨後春筍般不斷地冒出新芽。

(三) 現代藝術的崛起

在 Galois 理論中，設 $f(x) \in F[x]$ 且 E 為 $f(x)$ 在 F 上的分裂體，則 E 和 F 的中間體集與 $\text{Gal}(E/F)$ 的子群集之間存在對應關係。如果將 Galois 理論看成是一件藝術品，其中包含了數個和諧共處且有層次的結構(中間體)，並由相應的 $\text{Gal}(E/F)$ 的子群傳達出來。這與 19 世紀以來各種現代藝術的表現手法極其相似，多元的融合體展現出更為豐富的藝術觀。

自古以來，繪畫藝術為了寫實地呈現某主題，原本扮演著很重要的角色，但自從照相、錄影等技術發明後，這項功能遂逐漸消退，於是藝術出現了新的路線。視覺藝術家們開始嘗試各種新的視角，選用不同的材料或創作方式，甚至以抽象作為表達。

在 19 世紀末以法國巴黎為中心的印象派(Impressionism)，以及 20 世紀從德國興起的表現主義(Expressionism)，都對現代藝術產生了很大的影響。其中印象派畫家強調人們並沒有看到物體，卻只看到物體所反射出來的光。因此視覺藝術逐漸嘗試透過繪畫、雕塑、建築、設計、裝置等，試圖捕捉各種光線、意象、不同的空間感等，以表現內心的情感或找尋更多新的感動。透過開創多視角的創作，已成為現代藝術所追求的表達方式之一。

若在兩個不同對象之間找到相似情形，從而推演出其他方面也會有類似之處，稱為「類比」。我們發現：Galois 理論在中間體的更迭中，對應到 Galois 群之不同子群的結構變化，正吻合了現代藝術「多視角」的創作觀念；而現代藝術的多元面貌也反映出某些 Galois 思想的精神。如前所述，歐氏幾何和各種非歐幾何所呈現的旨趣各不相同(有的憑藉觸覺，有的憑藉視覺或其他感覺)，乃因其背後皆有不同變換群的理論作為基礎；將此論述類比於藝術方面的發展，必然促使我們對於藝術的未來走向有了更多的期待與想像。

在現代藝術的多面向創作中，除了感性美的表達之外，若能同時觀照形式、結構等理性因素，將有加乘效果。在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，就有如下記載：

不管怎樣，數學確實不像音樂、繪畫和詩那樣過多地藉助情感。一個人完全有理由堅持認為，藝術的基本功能是激發人的情感。(中略)。事實上，現代的純藝術強調繪畫的理論化和正規化，強調線條與形式的使用，強調藝術技巧方面的問題。這些藝術創作在更大程度上要依靠理性，而不是情感。(頁 477-478)

伽羅瓦雖然專注於他的數學研究，但在構思這個偉大理論的同時，也間接引領了創作的走向，開展出不同於以往的藝術風格。在 J.N. kapur 所編的《數學家談數學本質》一書中，引述了德國數學家普林希姆(Alfred Pringsheim 1850-1941 年)曾說過的一段話：

真正的數學家總是同時在很大程度上也是一個藝術家、一個建築師或一個詩人。數學家們還在現實世界之外依靠智慧創造了一個理想世界，後者雖然可以從前者領悟到，但數學家試圖把它發展成為一個最完美的世界，並且正從各個方向去探索它。(頁 222)

若將「Galois 群」視為一幅寫生作品，其眾正規子群宛如代表著各種不同的基本色彩，而每個合成因子就是描摹的線條。Galois 群寫實地呈現方程式的原始面貌，與方程式的外觀無關，卻對方程式解的本質作了精闢入裏的解剖與呈現。

Galois 思想所開展的理論創作，從表淺走向深層，其藝術價值不僅顯現方程式豐富且清晰的肌理，更揭示出上帝所創造令人讚嘆的完美。藝術工作若能孕育如 Galois 思想的肥沃土壤，並以真摯的情感灌溉，必能壟闢出兼具理性美與感性美的美好天地！

第四節 音樂的對話

自古以來，音樂和數學就息息相關。在畢達哥拉斯(約前 580-前 500 年，古希臘哲學家、數學家和音樂理論家)時代，就曾以五度音的循環來定出音階；到了中世紀的教育，並將算術、幾何、天文、音樂合稱為「四藝」(quadrivium)；到了巴洛克時期(1650-1750 年)，音樂的發展更創造了許多的曲式與風格。

節錄自 M.Kline 著，張祖貴譯的《西方文化中的數學》²¹⁷一書中，有如下記載：

從畢達哥拉斯時代開始，音樂研究在本質上就被認為是數學性的，與數學聯成一體了。這種聯繫構成了中世紀教育的內容，中世紀的教學課程包括算術、幾何、球面幾何學(天文學)、音樂，這就是著名的四藝。相應地，這四門課程分別被認為是純粹的數學、靜止的數學、運動的數學以及對數字的應用，因而這些課程通過數字而進一步相互聯繫起來了。(頁 295)

音樂是以聲音作為媒介，妝點時間的藝術。當音樂進行時，以調性格律組織各音階，以節奏有機聚合各節拍，以音色變化表現聲音的質感，以力度強弱製造稜角，以和聲擴充聽覺的層次與空間；音樂家更常以各種曲式變化，在心中譜寫出某種結構模式，如同建築師所學畫的平面構圖一般，因此稱「音樂是一種流動的建築」。

然而，每個人對音樂的敏銳度不同，將各種聲音頻率轉化為音樂的訓練，或對音樂型式的認識深淺，都會影響到人們對一首樂曲的感受。德國詩人兼科學家約翰·沃爾夫岡·歌德(Johann Wolfgang von Goethe 1749-1832 年)曾說：「每個人都只從音樂中聽到他聽得到的部分而已。」²¹⁸對於一般人而言(尤其是數學家)，其所聽到的音樂，因著多樣的音樂織度，必然是兼具理性美與感性美的。

以下將從兩方面來探討 Galois 思想與音樂的對話模式，包括追蹤顯現或隱藏的「對稱群」，以及開展抽象空間的「語言符號」。

一、追蹤「對稱群」

在音樂學當中，經常被研究的包括兩部分：一種是研究音樂內在結構的形式，著重在各種音樂要素如調性、節奏、音色、力度、和聲等，在一定時間內依照原則或秩序所產生的音樂結構；另一種則是研究音樂外在的曲式編排，如二段曲式、三段曲式、賦格曲(Fugue)、奏鳴曲式(Sonata)、輪旋曲式(Rondo)、變奏曲式

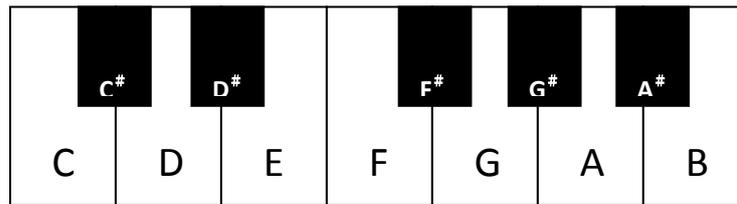
²¹⁷ M.Kline 著，張祖貴譯：《西方文化中的數學》(台北市：九章出版，1995 年)

²¹⁸ 參考劉炬渭著：《默觀無限美》(台北市：時報文化，2004 年)，頁 15。

(Variation)等，不同時期盛行的曲式也不大相同。

Galois 思想揭發對稱群的重要性，不論是在音樂的內在結構或外在曲式，都留下了斑斑可考的對稱群痕跡。節錄 Mario Livio 著，蔡承志譯的《無解方程式》一書中記載如下：

音樂在對稱性中扮演要角是顯而易見的。因此，群論能漂亮地描述音樂結構和曲式，完全是意料中事。鋼琴鍵盤的音符可以作為群—樂關係的最簡單實例。(頁 307)



以下將從音樂的內在結構和外部曲式，追蹤「對稱群」留下的痕跡：

(一) 結構的

伽羅瓦思想所建立的群的結構，應用到音樂中巴哈(Johann Sebastian Bach 1685-1750 年，德國音樂家)的平均律系統(Equally tempered system)，可以看出若對八度的 12 個半音進行移調恰可構成一個群。

音高是由頻率(每秒振動數)來決定，如中央 C 為 261.6Hz(赫茲)，A 為 440 Hz，而八度(octave)代表頻率比恰為 2，因此高音 C 的頻率為 523.2Hz，低音 C 的頻率為 130.8Hz。八度音程在鋼琴上共分成 12 個半音，琴鍵上的音分別為 C、C[#]、D、D[#]、E、F、F[#]、G、G[#]、A、A[#]、B，然後再重覆 C、C[#]、D、D[#]、...，相鄰兩音之間的關係稱為半音，其頻率比則為 1.05946，主要是 $(1.05946)^{12} \doteq 2$ 。無論從哪一個音開始上升或下降，音程的感覺是相同的，例如小三度隔 3 個半音，大三度隔 4 個半音，完全四度隔 5 個半音，完全五度隔 7 個半音等。

當我們將一首樂曲在調性上作轉移，例如 C 大調改為 D 大調，代表樂曲中的每一個音高都移動了兩個半音，這時候聽到的音樂旋律和節奏不變，但聽者可能產生更高亢的情緒。音樂的美妙之處，其實有數學原理在背後操縱，而每一次移調的改變，就是一次音樂中的對稱變換。若 r 代表音高的頻率乘上 1.05946 倍， r^n (n 為整數)代表音高的頻率乘上 $(1.05946)^n$ 倍，則 $\{1, r, r^2, \dots, r^{11}\}$ 對於乘法運算可形成一個循環群，這個群與模 12 的加法運算群 $(\mathbb{Z}_{12}, +)$ 同構。

當音樂的變化更多元，許多音樂家就嘗試各種不同的作曲手法，製造出更多的聽覺樂趣。在 Mario Livio 著，蔡承志譯的《無解方程式》一書中就有如下記載：

維也納作曲界採用三種基本運算方式，包括音列轉位(row inversion)、逆行(retrogression)和逆行轉位(retrograde inversion)。若採用音列轉位，下行音程由上行音程取代，上行音程則改變為下行音程。舉例來說，倘若原始音列從 C 開始，上行完全四度到 F，轉位後的音列便下行完全四度到 G。逆行讓旋律的跳躍順序逆轉。倘若原始音列最後跳躍是上行大三度，改成新的音列後，便成為其首次跳躍。最後，逆行轉位同時運用音列轉位和逆行。很容易想通箇中道理，這三種變換加上單位元(「無任何作為」)，構成一個「尾隨」運算群，這裡特別指出，這個群的每個元件都是本身的逆元。(頁 310-311)

可以看出這個「尾隨」運算群和 Klein 四元群(即 K_4)同構。

(二)曲式的

在音樂的各種曲式當中，「卡農」(Canon)是一種利用對位法的複音音樂，它由一個聲部先唱(奏)，另一個聲部再緊接著唱(奏)出相同的音樂，兩聲部之間的距離保持恆定，以產生連綿不絕、亦步亦趨的追趕模式，並製造出此起彼落的效果。輪唱就是一種卡農的曲式。

輪唱也是一種對稱變換，例如兒歌「蝴蝶蝴蝶生得真美麗，頭戴著金絲身穿花花衣，你愛花兒花更愛你，你會跳舞花又甜蜜。」曲子共分四句 A、B、C、D，當進行輪唱時(如下圖)，為歌曲在時間的順序上作平移，形成與模 4 的加法運算群($Z_4, +$)同構。

```

A B C D A B C D
  A B C D A B C
    A B C D A B
      A B C D A
        .....
          .....

```

兒歌“蝴蝶”輪唱曲排列

這樣的曲式，在音樂史中最著名的當推帕海貝爾(Johann Pachelbel 1653-1706 年，德國作曲家)的《D 大調卡農》(Canon in D Major)，這首樂曲僅以八個低音作為基礎，重覆奏出 28 次，搭配由三把小提琴輪奏出的上聲部，交織出令人心曠神怡的美妙樂音。由此可以清晰地感受到對稱性變換所形成的理性結構，成就了永世流傳的名曲。

卡農

The image displays a musical score for a Canon in G major, 4/4 time. It is divided into two systems. The first system shows the beginning of the piece, with the first three staves (Upper Voice 1, 2, and 3) containing rests, and the bass line starting with a G4. The second system shows the continuation of the piece, with all four staves (Upper Voice 1, 2, 3, and Bass) playing. The key signature is one sharp (F#) and the time signature is 4/4.

節錄自 M.Kline 著，張祖貴譯的《西方文化中的數學》中的如下記載：

在音樂中，數學的作用還推廣到了作曲本身。一些大師如巴赫〔巴哈〕、勛伯格(Schoenberg)〔荀白克〕為音樂作曲構造、發展了大量的數學理論。在這樣的理論指導之下，音樂作品創作的方式，與其說是不可言傳的、精神上的感受，倒不如說是冷靜的推理。(頁 311)

在伽羅瓦之前的古典作曲家，包括偉大的音樂家巴哈，他們在創作各式各樣的樂曲時並不曾思考群的理論。²¹⁹而因為群本身就是對稱性的語言，群與音樂如影隨形，它可能隱藏在音樂的形式(音樂的內在結構)中，也可能表現於音樂的曲式(音樂曲子的外在結構)中。

在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，有如下記載：

從畢達哥拉斯時代到 19 世紀的若干年時間內，數學家 and 音樂家，其中包括希臘人、羅馬人、阿拉伯人、歐洲人，都試圖弄清音樂聲音的本質，擴大音樂與數學二者之間的聯繫。音階體系、和聲學理論和旋律配合法得到了人們廣泛詳細的研究，並且重新建立起了完備的體系。(頁 295)

²¹⁹ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 310。

即使群論的興起是最近兩百多年的事，但從遠古以來，群的對稱性語言早已隨著音樂發展滲透於其中了。

二、開展抽象空間的「語言符號」

Galois 理論思想所帶出的 Galois 群，成為數學結構中的語言；在音樂領域中也有類似的語言符號，與 Galois 群一樣揭示著某個抽象空間，有著異曲同工之妙！

(一) 抽象空間

各種不同性質的事物，若以抽象的觀點，就其本身在某些範疇內進行特殊規律的運動，都可視為是一個抽象空間。

在伽羅瓦的研究當中，體 F 的擴展體可視為 F 上的向量空間。因此，若 $f(x) \in F[x]$ 且 E 為 $f(x)$ 在 F 上的分裂體，則 E 是 F 上的向量空間；且 E 和 F 之間的任何中間體 M 也會是 F 上的向量空間，所以在體 F 之上可構築出層層疊疊的向量空間。向量空間就是一種抽象空間。

在體的結構探討中，也可歸類出某些特殊形式的體擴展，如此所形成的向量空間遵循著某種規格的架構，宛若表現出不同的建築風貌般。例如體 F 的正規擴展或是根式擴展鏈，在 F 上所形成大大小小的向量空間，都標誌著獨特的變換基調。

與此相類似地，在音樂領域中，透過音程、節奏、音色、和聲、力度、調性、曲式、織體等方面，形成了一個多維度的聲響空間。²²⁰當每一個獨特的聲響，在適當時間有次序地呈現出來，形成交織重疊的時間藝術，我們的聽覺體系也因此擴展出多層次的聲響空間。聲響空間也是一種抽象空間。

我們欣賞一首交響曲時，就像是走進一棟建築物般，其結構與裝置來自於樂曲的曲式與多聲部織體鋪設，所以音樂是一種流動的建築！²²¹而不同時期的音樂家作曲手法也有差異，以歐洲音樂史觀之，15、16 世紀文藝復興時期以清唱複音音樂為主，音樂是由線條的對位慢慢凝聚成塊狀的和弦；²²²17 至 18 世紀中葉的巴洛克時期，以「數字低音」(Basso continuo)為主要特徵，這是一個即興的低音基礎，並與高音聲部美妙地結合在一起，形成和諧的音樂；²²³古典時期大約指西元 1750 年 (巴哈去世)到西元 1827 年(貝多芬去世)，這個時期強調結構的形式美，由聲音傳

²²⁰ 參考石峰編著：《音樂世界趣談》(北京：人民音樂出版社，1986 年)，頁 12。

²²¹ 參考石峰編著：《音樂世界趣談》，頁 12。

²²² 參考劉炬渭著：《默觀無限美》，頁 24-25。

²²³ 參考堀內敬三著，邵義強譯：《西洋音樂史》(台北市：大陸書店，民 84 年)，頁 34；劉炬渭著：《默觀無限美》，頁 30-31。

達抽象的理念，表現得理性、客觀、秩序與自然；²²⁴西元 1810 至 1900 年的浪漫時期，音樂旋律更有熱情及個性，和聲的配置更豐富，調性的選擇也更多元，並在樂曲中加入詩與敘述等要素，發展出標題音樂，也有一些表現民族音樂特性的國民樂派崛起。²²⁵20 世紀之後的聽覺藝術不斷創新，如雨後春筍般蓬勃發展，甚至出現無調音樂、不諧和音、極簡、電子等音樂，以開發人們對於宇宙聲音的敏銳度，其中以荀白克(Arnold Schönberg 1874-1951 年，奧地利音樂理論家)的無調音樂，將既有的音樂理論拆毀與重建，揚棄和聲上的均衡，創造出新秩序、新容貌、新價值的新音樂理論，最令人震撼！²²⁶

如此的聲響空間，匯聚了眾多音樂的元素變化，搭建出比體擴展所形成的向量空間更須用心靈感受的結構體系。節錄劉炬涓著《默觀無限美》中的敘述如下：

聲音作為音樂原材，本是無貌無形的。一直要等到音樂欣賞者對它傾注全身心的熱情，它才開始展現出它的形式及意蘊，而也就在這有你融入的剎那間，它一下子美了起來，聲音不再只是聲音，而成了音樂。此時我們環顧原來只是「可見」的周遭，一一都已經變成了「可感」的宇宙，就正因為你能簡單、真誠地融入音樂裡，任何橫阻，皆不存在。(頁 19)

這裡所提到「可感」的宇宙，就是在聆聽音樂時所出現的「抽象空間」。

(二) 語言符號

為了將抽象概念以簡潔、清晰的方式加以認識，人類文明遂發展出各種語言以濃縮抽象概念，並用符號傳達出精確的語意。

在數學當中，有許多表現抽象概念與結構的語言符號，如數字符號、運算符號、集合符號、邏輯符號、幾何符號、代數符號…等，不一而足。可以說整個數學學習模式就是用抽象的語言符號作為溝通的橋樑，與此相類似地，音樂的發展過程同樣仰賴抽象的語言符號；只是數學是以心智的運作為主軸，而音樂則是以聽覺感知作為主導。

然而，語言符號僅是一種意念傳達的圖案，真正賦予它生命的是背後宏偉深遠的思想與情感。數學家與音樂家對語言符號的拿捏與應用，必須精準掌握，才能開展心中建構的抽象空間。

節錄 Keith Devlin 著，洪萬生、洪贊天、蘇意雯、英家銘譯的《數學的語言》中的敘述如下：

²²⁴ 參考劉炬涓著：《默觀無限美》，頁 35。

²²⁵ 參考堀內敬三著，邵義強譯：《西洋音樂史》，頁 135。

²²⁶ 參考劉炬涓著：《默觀無限美》，頁 45；堀內敬三著，邵義強譯：《西洋音樂史》，頁 181。

在今日，數學書籍總是到處充塞著符號；但是，數學記號並不等於數學，其情況就如同記譜法並不等於音樂一樣。樂譜的一頁呈現一段音樂；當樂譜上的音符被唱出來或者被樂器演奏時，你就可以得到音樂本身。也就是說，在它的表演中，音樂變得有了生命，並且成為我們生命的一部分。這對於數學也是一樣，書頁上的符號只不過是數學的一種表現(representation)。要是讓一位有素養的表演者(譬如，某人受過數學訓練)來讀的話，印刷頁上的符號就會有了生命——正如同抽象的交響曲一樣，數學在讀者的心靈之中存活與呼吸。

給定數學與音樂這麼強烈的相似性，兩者都有各自抽象的記號，並且都被各自的抽象法則所支配，如果說很多(或許大多數)數學家也擁有音樂天分，那是一點也不令人驚訝。(頁 17-18)

事實上，語言符號常以一種簡單、統一、對稱、整齊的優美姿態出現，背後所隱藏的卻往往是深刻、奧妙、奇異、來自上帝完美創造下的概念與結構。

伽羅瓦將所有方程式的「Galois 群」作為一套測定標準，除可檢測方程式各解間的對稱特性，以及判斷可否根式求解之外，又可透視方程式係數體到分裂體之間的體擴展結構。當我們對於方程式各解一無所知時，想探討方程式係數體到分裂體之間體擴展所形成的向量空間，難度較高；這時，「Galois 群」卻像一棟建築物的電源開關，藉由它則大大小小的向量空間皆可一目瞭然。因此，「Galois 群」成功地扮演開啟向量空間的密碼。

伽羅瓦為了判斷方程式能不能根式求解而發明了檢測工具「Galois 群」，促成數學界對於群論的研究發展，並成為一套描述所有事物對稱特性的語言，²²⁷「置換群」更作為表達此語意的符號。像這樣創新且如同辭典般實用的語言，在其他領域也曾出現，例如科學界使用法國科學家拉瓦錫(Antonio Laurent Lavoisier 1743-1794 年)的「化學命名法」²²⁸，音樂界的記譜等。因此，掌握明確且富表達力的語言，是通往各門學問的捷徑。

以科學的原理來認識人類對聲音的接收器，人的耳朵所能聽到的聲波頻率大約只是每秒 20 次(20 赫茲)到每秒 20000 次(20000 赫茲)左右，在這有限的範圍內，作曲家將聽覺所能感知到的音樂，濃縮記錄成樂譜，因此樂譜成了用音樂傳遞情感的語言符號。

²²⁷ 參考 Mario Livio 著，蔡承志譯：《無解方程式》，頁 192。

²²⁸ 參考達爾馬斯原著：《伽羅瓦傳》，頁 39。

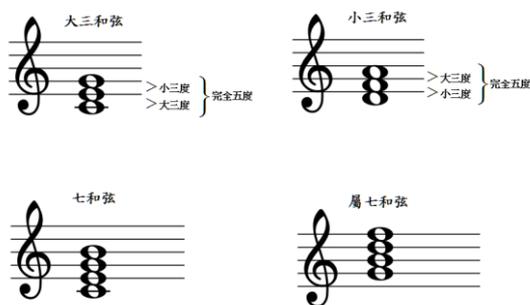
早期的樂譜以字母加符號來記錄音樂，逐漸發展成今日通用的五線譜系統，以時值作為橫坐標，以音高頻率作為縱坐標；²²⁹到了 19 世紀在歐洲開始有首調唱名法，是將 do, re, mi, fa, sol, la, si(或 ti)的 do 移到大調的主音位置，la 移到小調的主音位置，爾後再演變成以阿拉伯數字和一些特殊符號作為記錄的簡譜系統。²³⁰

透過樂譜這樣的語言符號，我們得以從旋律的起伏、節拍的律動、音量的大小、音色的轉換，構築出一個音響的空間。事實上，欣賞音樂是在欣賞各種時間組合的藝術。²³¹在石峰編著的《音樂世界趣談》一書中，有如下記載：

通過記譜，音樂就可以凝結為一個視覺形象。各種符號譜都在不同程度上反映出音樂本身的空間結構，即音高、時值、音程關係等。(中略)現代五線譜也是一種理想的音樂圖象，它把音樂空間結構轉化為平面空間的圖象，具有形象鮮明的特點。(頁 118-119)

在音樂當中，不論是聲音的本質或是結構等方面，處處有數學上的特徵。以和聲理論與 Galois 理論進行對照，和聲學從巴洛克時期的「數字低音」²³²，逐漸發展至今有各種和弦類型，這些和聲系統與 Galois 群一樣都建立了一套模型，將原有的知識、結構檢索出來成為語言符號，當我們要認識和聲或方程式時，只要找到這些語言符號的索引，就能解讀正確的內容，進而開展有層次美感且整體和諧的聲響空間或向量空間(體擴展空間)。

《和弦譜例》



²²⁹ 參考石峰編著：《音樂世界趣談》，頁 175。

²³⁰ 參考石峰編著：《音樂世界趣談》，頁 155。

²³¹ 參考石峰編著：《音樂世界趣談》，頁 10。

²³² 巴洛克時期的作曲家將高音曲調作為主旋律聲部，以歌聲或樂器表現；低音伴奏曲調是為大鍵琴、魯特琴等樂器所寫的和弦基礎，作曲家多半在低音的上下方寫一個數字，彈奏者可彈出那個音的和弦級數，並在一個和弦(數字)與一個和弦(數字)之間即興地作各種變化，此種低音和弦持續不間斷，稱為「數字低音」(Basso continuo)。

本節從「追蹤對稱群」、「開展抽象空間的語言符號」兩個角度為 Galois 思想與音樂作連結，事實上，數學家 and 音樂家的思路走向是類似的。在 M.Kline 著，張祖貴譯的《西方文化中的數學》一書中，有如下記載：

在代數、微積分以及高等分析等數學領域，第一流的數學家依靠的是像作曲家那樣的靈感。作曲家們覺得自己把握了一個主題，一個樂章，經過適當的發展和修改，就會形成美妙的音樂。經驗和有關的音樂知識使作曲家能夠得心應手地進行創作。類似地，數學家們預感到一個合乎某一公理的結論，經驗和數學知識引導他們的思路進入正確的軌道。當然，在形成一個正確的、令人滿意的定理之前，一兩次修正是必要的。但是，數學家和音樂家基本上是受一種神聖的靈感所驅動，這種靈感使得他們能夠在打下基石之前就能洞悉大廈的全貌。(頁 468)

伽羅瓦在探索數學定理時，也許不曾思想到與音樂的關聯。然而，我們藉由抽象思維的共通性作為對話的基礎，萃取了 Galois 理論思想的主旋律，順應它的節奏與律動，將可構築出一棟宛如音樂創作般的建築。此時，整個 Galois 理論思想所汨流出的，是根基穩固且層次分明的美感，如同一首曲風自然且清新獨特的樂曲，沁入人們的心靈！

第五節 數學教育的省思

Galois 理論在數學發展的過程當中扮演了關鍵性的角色，不僅解決了困擾數學界許久的問題，也為代數學指引出一條新的道路。在鄭毓信所著的《數學教育哲學》一書中記載著：

他〔波萊爾 Borel 1871-1956 年，法國數學家〕指出，伽羅華〔伽羅瓦〕理論一般被視為數學上最優美的篇章之一，而這主要地就是基於數學的考慮：首先，它解決了關於方程的一個很古老而在當時又是最為重要的問題。其次，它是一項內容非常豐富的理論，遠遠超出了原來的根式求解問題的範圍。第三，它的依據只是幾個非常典雅而簡潔的原理，是以新的概念建築起來的新結構下提出的原理，顯示了巨大的獨創性。第四，這些新觀點和新概念，尤其是群的概念，開闢了新的道路，對整個數學具有持續的影響…。(頁 73)

Galois 思想對於數學教育自然也帶來了某種程度的衝擊。以下就從學生、教師、教學等三方面，提出一些省思並加以探討。

一、學生方面

伽羅瓦所留給世人的印象是年輕且勇於開創未來。雖然他來不及面對未來就離開人世，但他所揭示的「未來數學家的使命」²³³卻真的臨到。節錄自達爾馬斯原著《伽羅瓦傳》中譯本書中的部分內容如下：

如果了解伽羅瓦的數學著作，甚至最不成熟的讀者也會感覺到，他的著作中的一切都是朝向未來的。(頁 21)

年輕學子是未來世界的主人翁，面對瞬息萬變的 E 世代來臨，在數學學習的路途上，必須充實多方面「帶著走」的數學能力，以作為未來面對種種挑戰的最大利器。特別值得一提的是：「帶著走」的數學能力必定包括抽象思維的訓練。

而伽羅瓦雖然不是數學教育專家，卻研究出以對稱群作為數學的語言，引進一套放諸四海皆準的實用語彙，讓數學結構的學習能夠應用到其它學科，在概念上是一體適用的。在歐陽絳所著的《數學的藝術》²³⁴一書中記載著：

²³³ 參考達爾馬斯原著：《伽羅瓦傳》，頁 21。

²³⁴ 歐陽絳著：《數學的藝術》(台北市：九章出版，1994 年)

C.迪爾曼說得好：「數學也是一種語言，而且就其結構和內容而言，它是現實中優於任何普通語言的最完美的語言；事實上，由於它為每一個人所理解，數學可稱為語言的語言。自然界彷彿用它說話，世界的創造者用它說話，世界的保護者仍在用它說話。」(頁 271)

因此，學生們若願意在不同階段學習正確且實用的數學語言，必能成功地踏上入門的階梯，並可進一步認識數學堂奧之美。

人類天生有克服困難的本能，在山窮水盡疑無路時，最大的快樂來自於發現柳暗花明又一村的驚喜。伽羅瓦的研究動機強烈，他靈活地掌握「猜想」與「證明」之間的運作，終於完成了偉大的理論。反思我們的教育環境，也應提供給小學生在數學學習活動中，能接觸更多具啟發性的教具或參與有趣的數學遊戲，以達到引起興趣的目的。而中學生的數學學習，可以「猜想—證明—猜想—證明」這種螺旋的方式²³⁵，提供過關斬將的思考環境。對於大學數學系所的學生，當勉勵他們以伽羅瓦為榜樣，主動研讀各類專業書籍，徜徉於數學的王國中。學生唯有在主動學習下，才能享受無窮樂趣。

二、教師方面

伽羅瓦提出方程式解的判斷準則，像攀登峰頂般居高臨下，五次方程式根式解問題自然就迎刃而解；他更安排方程式的係數遊走在不同的擴展體中，以找到所對應的 Galois 群的子群。反思數學教師也常擔任導遊角色，引領學生上山下海進行多視角的探索，以體驗數學之美，並一窺其神秘與趣味。

另外，我們從 Galois 理論看到：可解群的判斷準則只是合成因子列，但背後其實有著極深邃的思想主軸。由此也可思想：數學教育經常從數量的學習導向性質的分析，致使許多數學教師僅停留在教育學生運算的技法上，卻忽略了更高遠的目標—即介紹整個學習內容的結構與輪廓。就以伽羅瓦的中學代數課為例，他曾遇到只重繁瑣解題過程的教師，其教學方式扼殺了不少學生的興趣，值得每一位教師引以為鑑。

而伽羅瓦在中學時另一位數學教師—理查老師，卻成功地使許多學生原本閉塞的頭腦得以開啟、心智得以甦醒；當中也培育出不少能飛善躍的千里馬，這位識才的伯樂不愧是隱身幕後的推手。以此期勉今在崗位上的每一位數學教師，平時就必須多充實數學史與吸收新的知識，並能適性適才地帶領學生，進行有效的教學，以傳遞真正具有數學生命與價值的學問。

教育是國家百年大計，教育政策也應重視師資的培育計畫。製造過多的流浪教師不僅是國家資源的浪費，更無利於教師素質的提昇。而為了幫助學生建立正確的數學觀，數學教師應接受完整的師資養成教育，包括中學數學教師必須修完抽象代數等課程。

²³⁵ 參考歐陽絳著：《數學的藝術》，頁 272。

三、教學方面

數學本身就是一種藝術—思維的藝術。²³⁶因此，數學教育的本質，就是訓練學生理性思考來面對世界，以梳理出和諧的秩序。在 Galois 理論中強調方程式解的對稱性，就是將這項美的特質經由抽象思維推向高峰。因此，數學教學其實可視為藝術課程。

在 J.N.kapur 所編的《數學家談數學本質》一書中，引述了美國數學家 R.H.Bing (1914-1986 年)曾說過的一段話：

數學教師不僅要傳授事實與理解，還要講出數學魅力和挑戰的閃光。他應該引導他的好學生們觀看數學之美，給他們嘗到支配著數學家的興趣的那種數學型的滋味，啟發學生的想像力，並使他們願意從事和渴望從事長期的艱苦工作，以獲得對其具有挑戰味道的結果。(頁 108)

以國中課程古典幾何的推理證明而言，正是一種培養欣賞整體數學結構美的訓練。惜因義務教育與學生心智成熟度兩方面未能取得平衡點，致使幾何證明的邏輯思考教育未臻完善，這方面的學習或可以選修方式進行。

另外，數學的學習雖是一種純淨的思維運動，在某種程度上是與外界隔絕的。但當它的內部建構已經成熟時，卻須對外部的客觀世界進行反映。²³⁷由伽羅瓦開路的「群論」，就明白地說明團結合作的重要性。人是群性的動物，每個個體是社會結構的一部分，每個領域的教學也是整體文化結構的一環，這方面的認識，在台灣近幾年的數學教育已逐漸受到重視。因此，數學教學仍須與社會、文化的脈動相互連結。

早在 1831 年，伽羅瓦就在《學院公報》發表〈談數學教育的改革—包括教師、教科書和主考官〉的文章，對當時的數學教育提出針砭之言。²³⁸以一個二十歲的年輕人就能清楚看出彼時數學教育的困境，對照今日台灣的教育環境，是否也應破除不利於教育發展的結構性阻礙？值得深思！

台灣的教育近幾年來也在進行改革，數學教育應回歸專業思考，改革也須與時俱進。十二年國教上路，數學教育的走向，亟待有遠見且能拋開政治利益的專家學者一齊努力，以使數學教育能達到最理想的目標。

²³⁶ 參考歐陽絳著：《數學的藝術》，頁 273。

²³⁷ 參考鄭毓信、李國偉合著：《數學哲學中的革命》(台北市：九章出版，1999 年)，頁 181。

²³⁸ 參考本論文，頁 28。

第五章 結語

研究 Galois 理論思想，先從伽羅瓦的人格養成與一生際遇進行瞭解。

我們發現伽羅瓦很幸運地出生在一個家庭教育良好的環境下，有一個愉快而充實的童年；在中學時遇到極為賞識他的理查老師，導引並鼓勵伽羅瓦在學術道上的研究工作；進入高等師範學院後更認識了舍瓦烈兄弟，開啟了伽羅瓦對政治與社會的眼界。

雖然如此，伽羅瓦在短暫的生命歲月中，遭受到的挫敗卻遠遠多於一般人。在求學路上，他於中學時重讀一年，兩度報考綜合理工學院均不幸落榜，在唸高等師範學院時又被學校開除；在數學學術研究上，伽羅瓦向法國科學院三度叩關，都意外地落空，甚至與數學成就大獎擦身而過；而伽羅瓦在 18 歲時父親自殺身亡，震撼了他的心靈，連青春期唯一一次的墜入愛情中，都飽嘗著失戀的傷痛；伽羅瓦更因政治因素兩度被捕入獄，前後共在監獄裡度過數個月的時光。

伽羅瓦一生跌跌撞撞，卻也總是在烏雲籠罩之下，透露一些亮光。他在數學道上，走出創新的路線，為代數學指引出未來的方向；他對政治的狂熱，急於打破不合時宜的局勢，試圖建立新的秩序。兩相對照，可以明顯看出伽羅瓦不願受制於舊傳統的約束，卻帶著開創新局的膽識。事實上，數學家伽羅瓦的學術研究模式，總帶著革命者伽羅瓦的積極態度與社會性格。然而，正因為他具備這樣的人格特質，肯為愛赴難，終造成一種毀滅性的結局，使正值青春的年輕生命嘎然而止！

自從 1843 年法國數學家約瑟夫·劉維在巴黎科學院上公開宣揚伽羅瓦的研究成果，並於 1846 年將伽羅瓦的著作刊登在《純數學與應用數學》(*Journal de mathématiques pures et appliquées*)雜誌上之後，研究 Galois 理論與思想的風潮持久未歇。在查考各種相關文獻時，發現有的從抽象代數的結構性質導入，有的從對稱特性鋪陳，有的則從數學史觀點來認識伽羅瓦，由此可感受伽羅瓦理論與思想的多面向。而本論文循著「觀察→抽象→探索→猜測→論證」的思維進路，走進伽羅瓦的數學國度，期能進一步體認伽羅瓦研究時的想法。

19 世紀初代數學之謎：「五次一般方程式是否能用根式求解？」它啟動了伽羅瓦偉大的研究工程。伽羅瓦為了揭開高次方程式的神秘面紗，觀察到方程式解最重要的本質乃「各解間的對稱性」這個特徵，但這個共同的特徵隱藏在方程式的 Galois 群中。

在伽羅瓦之前的數學家們，為了尋找方程式的根式解，致力於研究「將足夠多的開方根元素加入方程式的係數體，是否能使它擴展成方程式的分裂體？」然而伽羅瓦卻探索體擴展結構的複雜程度，他發現體擴展結構的複雜程度可由其所對應的置換群(Galois 群)完全表現出來。將置換群抽離出來研究，是伽羅瓦進行抽象思維活動的設計。

若 $f(x)$ 為多項式，則 $f(x)=0$ 的 Galois 群必是有限群，將有限群的階數進行質

因數分解，可以掌握正規子群的分布與性質。探討置換群的好處是它的元素個數有限，容易掌握；伽羅瓦研究置換群中元素的組成關係，以掌握複雜的結構問題(體的擴展)。那個困擾數學家們幾百年的方程式根式求解問題，只要不困在分裂體的環境中，勇敢地走出來，到 $f(x)=0$ 的 Galois 群的國度裏，就能從另一個嶄新的座標看清楚所有的肌理。

要認識伽羅瓦思考的主軸，可先從四次一般方程式求根式解的過程中，找尋各解間的對稱性，再分析其結構變化，以猜測五次或更高次一般方程式可以根式求解的路徑。伽羅瓦以基本定理中正規擴展與正規子群的對應為基礎，讓思維大膽出走，的確為數學界開闢了一片新天新地。

在整套理論構建的過程當中，伽羅瓦引進了相當多新穎的觀念，包括 Galois 群、正規子群(Normal Subgroup)、同構(Isomorphism)、單群(Simple Group)、合成群(Composite Group)、可解群(Solvable Group)等。有了這些觀念，理論的框架更為紮實穩固，也使伽羅瓦的立論更加有了秩序。這使他成功地找到任意方程式可否用根式求解的判斷準則。至於之前數學家們所努力尋找的「五次一般方程式是否能用根式求解？」的答案，也只不過是伽羅瓦的整盤研究計劃中的一個小分支而已。伽羅瓦開創了「Galois 群」這個新的研究工具，帶來了許多方便。

Galois 思想的歷史價值，可上及擱置兩、三百年的五次方程式根式解問題，甚至追溯到古希臘三大幾何難題，全都獲得了解決；而在其後的學界，因著群論的發揚光大，各領域也風起雲湧地將結構分析納入研究。伽羅瓦成為劃時代的偉大數學家，已是公認的事實；伽羅瓦以其極短暫的生命所發出的一點點亮光，卻貫串照亮了兩千年來的學術界。

Galois 理論思想的表現形式雖然簡單扼要，但卻傳達了一位開拓者的積極態度。雖然他的論文未能詳細闡述想法細節與進行完整連貫的包裝，但以二十歲的年輕生命，為數學界所留下的遺產卻是頗具份量且不容小覷的。最難得的，是 Galois 理論背後所帶出的「結構」思維，改變了人們觀看事物的視角，延續至今仍不見消退。

從伽羅瓦獨特的研究方法可以看出其理論思想的深層洞見，某些不同樣式的方程式卻是對應到相同的置換群。於是，伽羅瓦不想大量研究各式各樣紛雜的方程式，而專注於置換群的分析與瞭解。他建立了一套數學結構，運用抽象推理，將一些外表看來相當不同的概念，用相同的結構來描述，藉此以釐清所有模糊或糾纏不清的概念。

伽羅瓦聰明地掌握了數學上的重要語言——「置換群」，它的所有結構就明明白白地講述了對稱的特性。研究分析置換群，可整理列出各種「結構表」，在必要時可為失序的混亂景象，提供一個核對比較的參照標準，以找到它歸屬的類別。伽羅瓦以淺白的「置換群」作為數學語言的表達，實則傳遞了相當有深度的思想。

在第四章第一節中，研究者將 Galois 理論的思想精神歸納出以下幾點：「獨特創新的洞察力」顯示伽羅瓦對於未知的精準透視，「大膽躍進的勇氣」表現出

伽羅瓦研究時的速度感，「抽絲剝繭的探究心」說明伽羅瓦在進行分析中的分析，「協同合作的器度」此向外延伸的觀念促使伽羅瓦建立了群的概念，「登高俯瞰的眼光」則來自於伽羅瓦提昇高度而有比別人更寬廣的視界。

從美學的視野來看 Galois 思想，可以由 Galois 理論所看重的「結構體系」與作為「語言符號」的置換群中，顯出簡單美；也可由對稱性的抽象分析，以及正規體擴展與 Galois 群的正規子群間的聯繫，表現出統一、對稱、整齊的和諧美；伽羅瓦用一個出人意料的「置換群」去解決方程式根式解問題，更造出方程式的 Galois 群、正規子群、可解群等創新的概念，以解讀上帝充滿奇異美的創造奧秘。

伽羅瓦思想席捲整個世紀之後，仍像一顆閃亮的星星般灼灼發亮，它像藝術品一樣讓人津津樂道，所散發出來的藝術特質是不同於感性美的「理性美」。以「對稱性」而言，代數學中有伽羅瓦探討方程式各解間的對稱性，幾何學則有平移、鏡射、旋轉等組合，而音樂的平均律系統、移調、卡農、輪唱或各種曲式變化等，都存有「對稱性」的痕跡，甚至「群」的結構體系也隱身於各類藝術之中。

對於數學上許多方面的研究，如果都以內在結構作為思考，將會歸在同一種學問當中。以歐氏幾何和非歐幾何為例，將歐氏幾何的第五條公設更換，可形成新的結構體系而推出新的幾何學理論。各種幾何有各自選用幾何變換所組成的「群」作為工具，而在所給定變換群下不變的幾何性質，就構築出對應的幾何，因此不同幾何有不同的變換群。例如歐氏幾何變換群是保角保距的剛性運動群，同樣地，射影幾何、拓樸學或其他非歐幾何，也都各自為保持某種特性而有自己的變換群。

同樣地，當我們從許多不同領域或學科當中，提取抽象的屬性或概念，可能會發現它們具有相同的本質；並能藉此在視覺、聽覺、觸覺等方面搭建出熟悉的結構思維，盡情遨遊於其中。藝術的理性美於焉產生！

Galois 思想在數學教育上所帶出來的省思是很廣泛且多面向的，包括抽象思維、數學語言、藝術層面等在數學教學中所扮演的角色與地位，都須教育工作者與決策掌權者加以重視。值此十二年國教剛起步，各不同年齡階段的學習內容都須專家學者共同討論與規劃。研究者在此也期盼數學師資的培育課程能更重視抽象代數的學習，並將數學教學視為一門藝術課程。

最後，我們看到伽羅瓦細心地推敲，從方程式的 Galois 群中的合成因子列，找出上帝的密碼，它竟然是牽動著方程式產生根式解的源頭。19 世紀伽羅瓦的出現是上帝差派來的天使，伽羅瓦將上帝創造宇宙其中一個小小的記號揭示給世人觀看。

文末，由衷感謝伽羅瓦所帶來上帝的啟示，並以新約聖經哥林多前書第二章第 9 節的經文，獻給所有的朋友們：

如經上所記：

「神為愛他的人所預備的是眼睛未曾看見，
耳朵未曾聽見，人心也未曾想到的。」

參考文獻

中文部分

- 王芳貴編著：《代數學基礎》，中國北京：科學出版社，2012年。
- 王懷權編著：《數學發展史》，新竹市：協進圖書有限公司，民70年。
- 丘維聲著：《數學的思維方式與創新》，中國北京：北京大學出版社，2011年。
- 石峰編著：《音樂世界趣談》，中國北京：人民音樂出版社，1986年。
- 呂溪木著：《體與 GALOIS 理論》，台北市：協進圖書有限公司，民72年。
- 李筱峰著：《台灣史 101 問》，台北市：玉山社，2013年。
- 洪萬生、英家銘、蘇意雯、蘇惠玉、楊瓊如、劉柏宏著：《當數學遇見文化》，台北市：三民書局出版股份有限公司，2010。
- 袁小明編著：《數學史》，台北市：九章出版社，2003年。
- 徐本順、殷啟正著：《數學中的美學方法》，中國大連：大連理工大學出版社，2008。
- 徐炎章等著：《數學美學思想史》，台北市：曉園出版社有限公司，1998年。
- 徐紀敏著：《科學美學思想史》，中國湖南長沙市：湖南人民出版社，1987年。
- 徐誠浩編著：《抽象代數：方法導引》，中國哈爾濱：哈爾濱工業大學出版社，2013。
- 康明昌著：《近世代數》，台北市：聯經出版事業股份有限公司，1988年。
- 康明昌著：《幾個有名的數學問題》，新竹市：凡異出版社，民83年。
- 曹亮吉著：《阿草的數學聖杯》，台北市：天下遠見出版股份有限公司，2003年。
- 張景中著：《數學與哲學》，台北市：九章出版，1996年。
- 張雄、李得虎所編著的《數學方法論與解題研究》，中國北京：高等教育出版社，2013。
- 馮曉華：〈劉維爾的開脫〉，《西安電子科技大學學報》第16卷第4期（2006年7月），頁144-148。
- 劉炬渭著：《默觀無限美》，台北市：時報文化，2004年。
- 歐陽絳著：《數學的藝術》，台北市：九章出版，1994年。
- 鄭毓信、李國偉合著：《數學哲學中的革命》，台北市：九章出版，1999年。
- 聶靈沼、丁石孫著：《代數學引論》，新竹市：凡異出版社，民85年。
- 堀內敬三著，邵義強譯：《西洋音樂史》，台北市：大陸書店，民84年。
- Garrett Birkhoff、Saunders Mac Lane 著，王連祥、徐廣善譯：《近世代數概論》第5版，中國北京：人民郵電出版社，2008年。
- J.N.Kapur 著，王慶人譯：《數學家談數學本質》，台北市：儒林圖書有限公司，1992年。
- Morris Kline 原著，林炎全、洪萬生、楊康景松譯：《數學史》上冊，台北市：九章出版社，民68年。

參考文獻

- Morris Kline 原著，林炎全、洪萬生、楊康景松譯：《數學史》中冊，台北市：九章出版社，民 72 年。
- Morris Kline 原著，林炎全、洪萬生、楊康景松譯：《數學史》下冊，台北市：九章出版社，民 72 年。
- Keith Devlin 著，洪萬生、洪贊天、蘇意雯、英家銘譯：《數學的語言》，台北市：商周出版，2011 年。
- 比爾·柏林霍夫(William P.Berlinghoff)與佛南度·辜維亞(Fernando Q.Gouvêa)著，洪萬生、英家銘暨 HPM 團隊譯：《溫柔數學史》，台北市：博雅書屋，2008 年。
- 羅伯·所羅門(Robert Solomon)著，洪慧芳譯：《一本通數學原理》，新北市：繁星多媒體，2012 年。
- Michael Artin 著，郭晉云譯：《代數》，中國北京：機械工業出版社，2009 年。(華章數學譯叢)。
- M.Kline 著，張祖貴譯：《西方文化中的數學》，台北市：九章出版，1995 年。
- Mario Livio 著，蔡承志譯：《無解方程式：數學天才與對稱性之謎的鬥智之旅》，台北市：臉譜，城邦文化出版：家庭傳媒城邦分公司發行，2008 年。
- 達爾馬斯 (Andre Dalmas) 原著：《伽羅瓦傳》中譯本，新竹市：凡異文化事業有限公司，民 75 年。
- 《聖經》(新約全書)，國際基甸會。

英文部分

- David M. Burton :《*Abstract and Linear Algebra*》，台北市：協進圖書有限公司。
- Ian Stewart :《*Galois Theory*》，新竹市：凡異出版社。