伽羅瓦群上的戴德金定理與切博塔列夫密度定理

Timo Chang
timo65537@protonmail.com
譯者: 仙女仙女

最後編輯: 2026 年 4 月 19 日

給定不可約多項式 $f(x) \in \mathbb{Q}[x]$, 設 K 爲 $f(x)$ 在體 $\mathbb{Q}$ 上的分裂體 (分裂域), 我們自然會關心: 如何確定其伽羅瓦群 $\mathrm{Gal}(f) := \mathrm{Gal}(K/\mathbb{Q})$? 本文將在前半部證明一個由戴德金 (Dedekind) 提出的定理, 用以刻畫 $\mathrm{Gal}(f)$ 中的某些元素, 並藉此對 $\mathrm{Gal}(f)$ 的結構施加若干限制. 接著, 本文將介紹一個由切博塔列夫 (Chebotarev) 提出的重要而引人注目的結果, 稱爲切博塔列夫密度定理, 其刻畫了質數的分布情形.

1 伽羅瓦群上的戴德金定理

定理 1.1 (戴德金) 設 $f(x) \in \mathbb{Z}[x]$ 爲不可約首一多項式, 對於一切不整除判別式 $\mathrm{disc}(f)$ 的質數 p, 在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中將 $f(x)$ 分解成若干個不可約多項式 $f_i(x)$ 之積, 即 $f(x) = f_1(x)\cdots f_k(x)$. 又設 $\deg f_i = d_i$, 則 $\mathrm{Gal}(f)$ 中含對 $f(x)$ 的根的 $(d_1, \ldots, d_k)$-輪換.

爲簡單起見, 稱 p「給出」$(d_1, \ldots, d_k)$-輪換, 及 $\mathrm{Gal}(f)$ 含 $(d_1, \ldots, d_k)$-輪換.

上述定理可由代數數論一語道破. 基本上, $p \nmid \mathrm{disc}(f)$ 意味著 p 在 K 中不分歧, 而我們所要尋找的元素正是 p 所對應的阿廷 (Artin) 共軛類中的一個 (任何) 元素 (見註記 1.2). 以下將提供具體說明.

證明 設 α 爲 $f(x)$ 在 K 中的任一根, $E := \mathbb{Q}(\alpha)$. 因 $p \nmid \mathrm{disc}(f)$, 故 $p \nmid \mathrm{disc}(E)$, 從而 p 在 E 中不分歧. 又因爲 K 是將 α 的所有共軛元 (即 $f(x)$ 的所有根) 加入 $\mathbb{Q}$ 所得的體擴張, 所以 p 在 K 中同樣不分歧.

取 K 中位於 p 之上的質理想 P, 因爲 P/p 不分歧, 所以分解群 $D(P/p)$ 同構於 $\mathbb{Z}/p\mathbb{Z}$ 上之剩餘體擴張 $\mathcal{O}_K/P$ 的伽羅瓦群. 後者是由符羅貝尼烏斯自同構 σ_p 所生成的循環群, 其中 σ_p 將 $\mathcal{O}_K/p$ 的元素映至其 p 次冪. 設 $\phi := \phi(P/p)$ 爲 $D(P/p) \subseteq \mathrm{Gal}(K/\mathbb{Q})$ 中與 σ_p 相應的元素, 其爲 $D(P/p)$ 中唯一滿足「對於所有 $\alpha \in \mathcal{O}_K$, $\phi(\alpha) \equiv \alpha^p \pmod{P}$」的元素 (換言之, 在 $\mathcal{O}_K/P$ 中, 有 $\overline{\phi(\alpha)} = \overline{\alpha}^p$). 斷言: ϕ 給出所求的輪換.

於 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中, 將 $f(x)$ 分解成不可約因子之積 $f_1(x)\cdots f_k(x)$, 其中 $\deg f_i = d_i$. 由於 $p \nmid \mathrm{disc}(f)$, $f(x)$ 的所有根在取模 P 運算之下相異. 現, 對每個 $i = 1, \ldots, k$, 取 $f_i(x)$ 的一根 $\overline{\alpha_i}$, 注意到符羅貝尼烏斯自同構 σ_p 生成 $\overline{\alpha_i}$ 的所有共軛元, 亦即, $f_i(x)$ 的根由

$$\{\overline{\alpha_i}, \overline{\alpha_i}^p, \ldots, \overline{\alpha_i}^{p^{d_i-1}}\} = \{\overline{\alpha_i}, \overline{\phi(\alpha_i)}, \ldots, \overline{\phi^{d_i-1}(\alpha_i)}\}$$

給出, 且有

$$\overline{\alpha_i}^{p^{d_i}} = \overline{\phi^{d_i}(\alpha_i)} = \overline{\alpha_i}.$$

回到原本的 $f(x)$ 來看, 這表示元素 ϕ 在 $f(x)$ 那些「對應到 $f_i(x)$ 之根」的根上的作用如同一個 d_i-輪換, 證畢. □

註記 1.2 因爲對於 K 中位於 p 之上的不同質理想 P, 各 $\phi(P/p)$ 在共軛意義之下相等, 所以這些元素實際上在 $\mathrm{Gal}(f)$ 的同一個共軛類中, 稱其爲 p 的阿廷共軛類. 特別地, 它們有同型的輪換. 因此, 輪換的形式與 p 上的 P 的選取無關, 這表示「p (而非 P/p) 給出 $(d_1, \ldots, d_k)$-輪換」這個說法是合理的.

在計算一些例子之前, 先來回顧如何判斷四次伽羅瓦群. 設 $f(x) \in \mathbb{Q}[x]$ 爲 4 次不可約多項式, $R_3(f)$ 爲 f 的三次預解式, 則有

$\mathrm{disc}(f)$	$R_3(f)$	$\mathrm{Gal}(f)$
$= \mathbb{Q}$ 的平方數	不可約	A_4
$= \mathbb{Q}$ 的平方數	可約	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\neq \mathbb{Q}$ 的平方數	不可約	S_4
$\neq \mathbb{Q}$ 的平方數	可約	D_4 或 $\mathbb{Z}/4\mathbb{Z}$

另外, 區分 D_4 和 $\mathbb{Z}/4\mathbb{Z}$ 稍微有點專業壁壘高築, 且證明有點百轉千回. (關於這個主題的完整介紹, 請參見 [Con].)

例 1.3 考慮不可約多項式 $f(x) = x^4 + x - 1$, 易知 $\mathrm{disc}(f) = -283$ 不是 $\mathbb{Q}$ 中的平方數, 故 $\mathrm{Gal}(f) = S_4, D_4$, 或 $\mathbb{Z}/4\mathbb{Z}$. 而且, f 的三次預解式爲 $R_3(f) = x^3 + 4x - 1$, 顯然不可約, 因此可推得 $\mathrm{Gal}(f) = S_4$.

我們亦可使用定理 1.1 而不計算三次預解式. 注意到 f 的判別式 (幸好) 是質數, 所以可取若干個小質數 p 並考察 $f(x)$ 在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中的因式分解. 再一次地, 由於 $\mathrm{disc}(f) = -283$ 不是 $\mathbb{Q}$ 中的平方數, 因此 $\mathrm{Gal}(f) = S_4, D_4$, 或 $\mathbb{Z}/4\mathbb{Z}$.

- $p = 2$, 此時在 $(\mathbb{Z}/2\mathbb{Z})[x]$ 中有 $f(x) = x^4 + x + 1$, 故 $\mathrm{Gal}(f)$ 含 (4)-輪換, 但這一點幫助都沒有, 因爲餘下三種可能性含此種元素.
- $p = 3$, 此時在 $(\mathbb{Z}/3\mathbb{Z})[x]$ 中有 $f(x) = x^4 + x + 2$, 但亦無結論.
- $p = 5$, 此時在 $(\mathbb{Z}/5\mathbb{Z})[x]$ 中有 $f(x) = x^4 + x + 4$, 但亦無結論.
- $p = 7$, 此時在 $(\mathbb{Z}/7\mathbb{Z})[x]$ 中分解 $f(x) = x^4 + x + 6$ 得 $f(x) = (x+3)(x^3 + 4x^2 + 2x + 2)$, 故 $\mathrm{Gal}(f)$ 含 $(1, 3)$-輪換, 於是 D_4 和 $\mathbb{Z}/4\mathbb{Z}$ 便不可能發生.

因此, 可得 $\mathrm{Gal}(f) = S_4$.

例 1.4 考慮不可約多項式 $f(x) = x^4 - 2x^2 + 7$. 注意到 $\mathrm{disc}(f) = 2^{10} \cdot 3^2 \cdot 7$ 不是 $\mathbb{Q}$ 中的平方數, 故 $\mathrm{Gal}(f) = S_4, D_4$ 或 $\mathbb{Z}/4\mathbb{Z}$. 另外, f 的三次預解式 $R_3(f) = x^3 + 2x^2 - 28x - 56 = (x + 2)(x^2 - 28)$ 是可約多項式, 因此 $\mathrm{Gal}(f) = D_4$ 或 $\mathbb{Z}/4\mathbb{Z}$.

應用定理 1.1, 僅能考慮不整除 $\mathrm{disc}(f)$ 的質數, 故從 $p=5$ 開始. 因爲在 $(\mathbb{Z}/5\mathbb{Z})[x]$ 中, 有 $f(x)=(x+2)(x+3)(x^2+2)$, 所以 $\mathrm{Gal}(f)$ 含有 $(1,1,2)$-輪換, 其排除了 $\mathbb{Z}/4\mathbb{Z}$, 從而 $\mathrm{Gal}(f)=D_4$.

例 1.5 考慮五次多項式 $f(x)=x^5-x-1$, 不難看出 f 不可約, 且其判別式 $\mathrm{disc}(f)=19\cdot 151$. 首先, 因爲正在考慮的是五次多項式, 所以必有 $5\mid \#(\mathrm{Gal}(f))$. 又由該伽羅瓦群可嵌入 S_5, 可知 $\#(\mathrm{Gal}(f))\mid 5!=120$.

接著, 取 $p=2\nmid \mathrm{disc}(f)$, 那麼在 $(\mathbb{Z}/2\mathbb{Z})[x]$ 中, 有 $f(x)=(x^2+x+1)(x^3+x^2+1)$, 於是 $\mathrm{Gal}(f)$ 含 $(2,3)$-輪換. 特別地, $\mathrm{Gal}(f)$ 含 6 階的元素, 從而 $6\mid \#(\mathrm{Gal}(f))$. 連同先前的觀察, 必可推得 $\#(\mathrm{Gal}(f))=30,60,120$.

注意到不可能是 30, 因爲 S_5 沒有 30 階子群 (爲什麼?). 又 $\mathrm{disc}(f)$ 在 $\mathbb{Q}$ 中不是平方數, 故 $\mathrm{Gal}(f)$ 不包含於 A_5 中. 特別地, $\#(\mathrm{Gal}(f))\neq 60$, 因此 $\mathrm{Gal}(f)=S_5$.

例 1.6 最後, 考慮四次不可約多項式 $f(x)=x^4+5x+5$, 其判別式爲 $\mathrm{disc}(f)=5^3\cdot 11^2$. 類似於例 1.4 的過程可得 $\mathrm{Gal}(f)=D_4$ 或 $\mathbb{Z}/4\mathbb{Z}$. 接著嘗試應用定理 1.1, 經過若干次嘗試與錯誤後, 發現使用小質數根本推不出任何有用的結論, 這也許令你不禁納悶, 是否有「有幫助」的質數存在.

事實上, 答案是否定的. 更進一步的分析 (見 [Con]) 可得 $\mathrm{Gal}(f)=\mathbb{Z}/4\mathbb{Z}$, 所以無論如何試了多少質數, 都只能得到 $(4),(2,2)$ 及 $(1,1,1,1)$ 型的輪換, 但 D_4 亦含這三型的輪換, 因此不可能用先前的策略排除 D_4.

從例 1.6 中, 自然會有一個疑問誕生: 什麼樣的質數會給出特定型的輪換. 或者退而求其次, 有多少個質數給出特定型的輪換. 後者可從切博塔列夫密度定理得到答案, 其關心那些不分歧的質數的「分布行爲」, 這在某種意義上可能能幫助求 $\mathrm{Gal}(f)$.

2 切博塔列夫密度定理

先來透過例 1.3 和例 1.4 作一些數值上的觀察. 找出首 10,000 個不整除 $\mathrm{disc}(f)$ 的質數, 得出特定型的輪換的質數個數, 如表 1.

$f(x)$	$\mathrm{Gal}(f)$	(4)	$(1,3)$	$(2,2)$	$(1,1,2)$	$(1,1,1,1)$
x^4+x-1	S_4	2496	3322	1244	2545	393
x^4-2x^2+7	D_4	2520	0	3738	2508	1234

表 1

注意到各質數個數與 10,000 的比非常接近表 2. 事實上, 這些分布的結果以 $\mathrm{Gal}(f)$ 中的共軛類的「大小」測量. 具體來說有如下定理.

定理 2.1 (切博塔列夫密度定理) 設 L/K 爲有限伽羅瓦數體擴張, 伽羅瓦群爲 G, $C\subseteq G$ 爲共軛類, M_C 爲 K 滿足如下條件的質理想 $\mathfrak{p}$ 的全體: $\mathfrak{p}$ 在 L 中不分歧, 且存在位於 $\mathfrak{p}$ 上的 L 的質理想 $\mathfrak{P}$ 使得符羅貝尼烏斯自同構 $\phi(\mathfrak{P}/\mathfrak{p})\in C$. 那麼, M_C 有 (自然) 密度 $\#(C)/\#(G)$. 換言之,

$$\lim_{n\to+\infty}\frac{\#\{\mathfrak{p}\in M_C : N\mathfrak{p}\le n\}}{\#\{\mathfrak{p} : N\mathfrak{p}\le n\}}=\frac{\#(C)}{\#(G)}.$$

$f(x)$	$\mathrm{Gal}(f)$	(4)	$(1,3)$	$(2,2)$	$(1,1,2)$	$(1,1,1,1)$
x^4+x-1	S_4	$1/4$	$1/3$	$1/8$	$1/4$	$1/24$
x^4-2x^2+7	D_4	$1/4$	0	$3/8$	$1/4$	$1/8$

表 2

現將切博塔列夫密度定理應用於戴德金定理的設定上. 設有共軛類 $C \subseteq \mathrm{Gal}(f)$, 其含 $(d_1,\dots,d_k)$-輪換, 則由定理 1.1 的證明, 可知 p 給出該型的輪換的充要條件爲在 p 上存在質理想 P 使得 $\phi(P/p) \in C$. 又依定義, 這也等價於 $p \in M_C$, 故問有多少質數給出特定型的輪換, 等價於問集合 M_C「多大」, 而後者由定理 2.1 即得答案, 這也解釋了我們的數值資料.

在表 1 及表 2 中, 設 $f(x)=x^4+x-1$, $\mathrm{Gal}(f)=S_4$, 並考慮含 (4)-輪換的共軛類 C. 不難看出 $\#(C)=6$, 故依定理 2.1, 給出 (4)-輪換的質理想的密度爲 $\#(C)/\#(G)=6/24=1/4$, 這與我們的數值實驗相吻合.

另一方面, 設 $f(x)=x^4-2x^2+7$, $\mathrm{Gal}(f)=D_4$. 注意到不整除 $\mathrm{disc}(f)$ 的首 10,000 個質數都沒有給出 $(1,3)$-輪換, 這現象可謂不負衆望, 因爲 D_4 不含有 $(1,3)$-輪換.

基於數值資料, 也可猜測相應的伽羅瓦群. 在例 1.6 中已看出戴德金定理對於多項式 $f(x)=x^4+5x+5$ 無法直接應用, 但仍可做類似的計算得下表:

$f(x)$	$\mathrm{Gal}(f)$	(4)	$(1,3)$	$(2,2)$	$(1,1,2)$	$(1,1,1,1)$
x^4+5x+5	?	5025	0	2492	0	2483

由於 $\mathrm{disc}(f)=5^3\cdot 11^2$ 不是 $\mathbb{Q}$ 中的平方數, 因此 $\mathrm{Gal}(f)=S_4, D_4$, 或 $\mathbb{Z}/4\mathbb{Z}$. 更有甚者, $(1,1,1,1)$-輪換 (其對應只含有單位元的共軛類) 出現頻率爲 $2483/10000\approx 1/4$, 且由定理 2.1 可知該數應接近 $1/\#(G)$, 故可猜測 $\#(G)=4$ 及 $G=\mathbb{Z}/4\mathbb{Z}$, 而確實是這樣. (不過當然, 這不是證明.)

參考資料

[Con] Keith Conrad. *Galois groups of cubics and quartics (not in characteristic 2)*. Expository papers. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf.