國立臺灣師範大學理學院數學系

碩士論文

Department of Mathematics, College of Science
National Taiwan Normal University
Master's Thesis

與多項式迭代相關的算術問題

Arithmetic Problems Related to Iteration of Polynomials

石毓萱

Shih, Yu-Hsuan

指導教授：夏良忠 博士

Advisor: Hsia, Liang-Chung, Ph.D.

中華民國 109 年 6 月

June 2020

摘要

本篇論文主要分兩部份討論多項式迭代的相關問題:

(一) 零的軌道:
這部份我們會討論多項式 $f(x) = x^d + c$ 迭代後，0 的軌道會是甚麼。

(二) 伽羅瓦群:
這部份我們會介紹有根滿二元樹的自同構，以及整係數多項式迭代後 $f(x) = x^2 + c$ 的伽羅瓦群與有根滿二元樹的自同構關係，並討論對於整係數多項式 $f(x) = x^2 + c$ 迭代後，其伽羅瓦群會是甚麼。

關鍵字：軌道、前週期點、遊蕩點、半直積、圈積、樹的自同構、2-獨立。

目錄

1 零的軌道 **1**
1.1 介紹 1
1.2 先備知識 3
1.3 預備引理 5
1.4 主要定理證明 12

2 伽羅瓦群 **13**
2.1 介紹 13
2.2 先備知識 15
2.2.1 樹的自同構 15
2.2.2 四次多項式的伽羅瓦群 24
2.2.3 2-獨立 25
2.3 預備引理 26
2.4 主要定理證明 29

1 零的軌道

1.1 介紹

算術動態系統是整合了動態系統及數論的數學理論，其探討多項式或有理函數在整數、有理數、p 進位數及幾何點中的迭代特性，而本篇論文主要討論的是多項式迭代相關問題。在多項式迭代的過程中，自然的會想去了解，當點帶入多項式迭代後，得到的值是否有特殊變化或是滿足一些特殊性質，為了方便接下來的討論，我們先給定一些定義:

Definition 1. 假設集合 S，$\phi : S \to S$ 為一映射，對於 S 集合裡的元素 α，稱集合

$$\{\phi(\alpha), \phi^2(\alpha), \ldots, \phi^n(\alpha), \ldots\}$$

是 α 對 ϕ 的軌道 (*orbit*) 簡稱 α 的軌道，其中

$$\phi^n = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{n \text{ 個}}$$

是 ϕ 的 n 次迭代。

Definition 2. 如果 α 的軌道含有有限多個元素，稱 α 是前週期點 (*preperiodic point*)。若 α 的軌道含有無限多個元素，則稱 α 是遊蕩點 (*wandering point*)。

這裡我們主要考慮多項式

$$f_c(x) = x^d + c$$

其中 c 是實數且 d 是自然數時，0 的軌道會是甚麼，其中一個想法便是想要去了解當多項式 $f_c(x) = x^d + c$ 時，0 是否是一個前週期點。而 K. Doerksen 和 A. Haensch[1] 對此有相關的討論，他們研究了在 c 是整數且 $d \geq 2$ 是自然數的情形，結果如下:

Theorem ([1, Lemma 8])**.** 假設整係數多項式 $f_c(x) = x^d + c$，其中 d 爲整數且 $d \geq 2$，則：

(1) 令 $C_n = |f_c^n(0)|$, $f_c^n = \underbrace{f_c \circ f_c \circ \cdots \circ f_c}_{n \text{ 個}}$ 爲 f_c 的 n 次迭代，當數列 $(C_n) = (C_1, C_2, \ldots)$ 爲遞增數列時，0 是一個遊蕩點。

(2) 0 是一個前週期點若且爲若下列任一情況成立：

(a) $c = 0$,

(b) $c = -1$ 且 d 是偶數,

(c) $c = -2$ 且 $d = 2$。

從以上結果可知當 c, d 皆是整數且 $d \geq 2$ 時，在甚麼樣的情況下 0 會是前週期點或是遊蕩點。本篇論文的其中一個目標便是拓展 c 的範圍，對於多項式 $f_c(x) = x^d + c$，其中 c 是在實數中變動的參數，且 $[\mathbb{Q}(c) : \mathbb{Q}] \leq 2$，在這個的假設下，想要了解 0 甚麼時候是前週期點或是遊蕩點。而我們發現 c 拓展到新的範圍後，0 會是前週期點的情況跟 K. Doerksen 和 A. Haensch 他們的結果是一樣的，結果如下：

Theorem 1. 假設多項式 $f_c(x) = x^d + c$，其中 d 爲整數且 $d \geq 2$，c 爲實數且 $[\mathbb{Q}(c) : \mathbb{Q}] \leq 2$，則 0 是一個前週期點若且爲若 c 滿足下列任一情況：

(a) $c = 0$,

(b) $c = -1$ 且 d 是偶數,

(c) $c = -2$ 且 $d = 2$。

接下來分三小節來做介紹，1-2 節將先介紹一些我們會使用到的相關先備知識，1-3 節則會介紹主要定理證明中會使用到的一些引理，1-4 節則是主要定理的證明。

1.2 先備知識

為了在接下來的討論中能有更好的了解,我們先介紹相關的先備知識,包含了一些基本名詞的定義以及一些相關的命題。以下內容參考自 K. Ireland 和 M. Rosen 的「A Classical Introduction to Modern Number Theory」[5]，若要了解更詳細的內容可參考該書目。

Definition 3. 假設 α 是一複數，若存在有理數 $a_0, a_1, a_2, \ldots, a_n$，其中 $a_n \neq 0$ 且 n 為自然數，使得 $a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_0 = 0$，則稱 α 為一個**代數數** (*algebraic number*)。

Definition 4. 假設 ω 是一複數，若存在整數 $b_0, b_1, b_2, \ldots, b_{n-1}$，其中 n 為自然數，使得 $\omega^n + b_{n-1}\omega^{n-1} + b_{n-2}\omega^{n-2} + \cdots + b_0 = 0$，則稱 ω 為一個**代數整數** (*algebraic integer*)。

Definition 5. 假設 K 是複數體的一個子體, 若體 K 是有理數體 $\mathbb{Q}$ 的有限擴張 ($[K:\mathbb{Q}] < \infty$)，則稱 K 為**代數數體** (*algebraic number field*)。若 $[K:\mathbb{Q}] = 2$，則稱 K 為**二次數體**。

Definition 6. 假設 b 為交換環 B 中的一個元素，若 $n \geq 1$ 為自然數且 $a_{n-1}, \ldots, a_1, a_0$ 為交換環 A 中的元素使得 b 滿足 $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$，則稱 b 為 A 上的**整元素** (*integral element*)。如果 B 的每個元素都是 A 上的整元素，則稱 B 為 A 的**整擴張** (B is *integral over* A)。

Definition 7. 若代數數體 K 中的一個環其所有元素都是 $\mathbb{Z}$ 上的整元素，則稱此環為 K 上的**整數環** (*ring of integers*)，通常將整數環記為 $\mathcal{O}_K$。

Definition 8. 假設 A 是 $\mathcal{O}_K$ 的理想 (ideal)，若 $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ 是一組 K 在 $\mathbb{Q}$ 上的基底且 $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$, 則稱 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 A 的一組**整性基底** (*integral basis*)。

Proposition 1. *若 c 是次數爲 2 的代數整數，則 $\mathbb{Q}(c) = \mathbb{Q}(\sqrt{h})$，其中 h 爲非平方整數。同時，$\mathbb{Q}(\sqrt{h})$ 的整數環如下：*

$$\begin{cases} \mathbb{Z}[\sqrt{h}] & \text{若} h \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1}{2}(-1+\sqrt{h})] & \text{若} h \equiv 1 \pmod 4 \end{cases}$$

Proof. 令 $K = \mathbb{Q}(\sqrt{h})$ 且假設 $r + s\sqrt{h} \in \mathcal{O}_K$，其中 r、$s \in \mathbb{Q}$。因為 $[K:\mathbb{Q}] = 2$，所以

$$(x - (r + s\sqrt{h}))(x - (r - s\sqrt{h})) = x^2 - 2rx + r^2 - s^2h \in \mathbb{Z}[x],$$

從上述可知 $2r$、$r^2 - s^2h \in \mathbb{Z}$。假設 $r = \frac{m}{2}$，其中 m 是整數，則 $r^2 - s^2h = \frac{m^2 - 4s^2h}{4} \in \mathbb{Z}$ 表示 $4s^2h \in \mathbb{Z}$，因為 h 是無平方因子的整數，可推得 $2s \in \mathbb{Z}$，故假設 $s = \frac{n}{2}$，其中 n 為整數，$r^2 - s^2h = \frac{m^2 - n^2h}{4} \in \mathbb{Z}$ 表示 $m^2 - n^2h \equiv 0 \pmod 4$。

(1) $h \equiv 2, 3 \pmod 4$

在這情況下, $m^2 - n^2 h \equiv m^2 + 2n^2 \pmod 4$ 或 $m^2 - n^2 h^2 + n^2 \pmod 4$, 因為 $m^2 - n^2 h \equiv 0 \pmod 4$, 表示 $4 | m^2 + 2^{n2}$ 或 $4 | m^2 + n^2$, 推得 m 及 n 皆為偶數, 因此 r 及 s 皆為整數, 則 $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{h}]$。假設 $a + b\sqrt{h} \in \mathbb{Z}[h]$, 其中 a、b 皆為整數, 令 $x = a + b\sqrt{h}$, 可推得 $x^2 - 2ax + a^2 - b^2 h = 0$, 其中 $x^2 - 2ax + a^2 - b^2 h$ 為首一整係數二次多項式, 因此 $a + b\sqrt{h} \in \mathcal{O}_K$ 則 $\mathbb{Z}[\sqrt{h}] \subseteq \mathcal{O}_K$, 故 $\mathcal{O}_K = \mathbb{Z}[\sqrt{h}]$。

(2) $h \equiv 1 \pmod 4$

在這情況下, $m^2 - n^2 h \equiv m^2 - n^2 \equiv 0 \pmod 4$, 可推得 m 跟 n 同時為偶數或奇數, 也就是 $\mathcal{O}_K = \{\frac{m+n\sqrt{h}}{2} | m \equiv n \pmod 2$, 因為 $\frac{m+n\sqrt{h}}{2} = \frac{m+n}{2} + n(\frac{-1+\sqrt{h}}{2})$, 其中 $\frac{m+n}{2}$ 及 n 皆為整數, 則 $\mathcal{O}_K \subseteq \mathbb{Z}[\frac{-1+\sqrt{h}}{2}]$。假設 $a + b(\frac{-1+\sqrt{h}}{2}) \in \mathbb{Z}[\frac{-1+\sqrt{h}}{2}]$, 其中 a、b 皆為整數, 令 $x = a + b(\frac{-1+\sqrt{h}}{2})$, 可推得 $x^2 - (2a - b)x + a^2 - ab + \frac{b^2}{4} - \frac{b^2 h}{4} = 0$, 因為 $h \equiv 1 \pmod 4$, 可知 $\frac{b^2}{4} - \frac{b^2 h}{4}$ 為整數, 所以 $x^2 - (2a - b)x + a^2 - ab + \frac{b^2}{4} - \frac{b^2 h}{4}$ 為首一整係數二次多項式, 因此 $a + b(\frac{-1+\sqrt{h}}{2}) \in \mathcal{O}_K$, 則 $\mathbb{Z}[\frac{-1+\sqrt{h}}{2}] \subseteq \mathcal{O}_K$, 故 $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{h}}{2}]$。

□

1.3 預備引理

考慮首一多項式 $f_c(x) = x^d + c$ 屬於 $K[x]$，其中 K 是一數體，這裡我們考慮 K 是實二次數體，d 為自然數，c 為實數且 $[\mathbb{Q}(c) : \mathbb{Q}] \leq 2$，為了方便接下來的討論，我們定義

$$c_n = f_c^n(0)$$

其中

$$f_c^n = \underbrace{f_c \circ f_c \circ \cdots \circ f_c}_{n\text{ 個}}。$$

Lemma 1. *若 c 不是代數整數，則對於多項式 $f_c(x)$，0 是一個遊蕩點。*

Proof. 使用反證法:
假設 0 是一個前週期點, 根據前週期點的定義可得對於一些自然數 $m > n$, $f_c^m(0) = f_c^n(0)$。由於 $f_c^m(0)$ 可以看作以 c 為變數的首一整係數多項式，故存在次數為 m 的首一整係數多項式 $g(x)$ 使得 $f_c^m(0) = g(c)$。同理可得，存在次數為 n 的首一整係數多項式 $h(x)$ 使得 $f_c^n(0) = h(c)$。可以從 $f_c^m(0) = f_c^n(0)$ 推得 $g(c) - h(c) = 0$，且 $g(x) - h(x)$ 是首一多項式，則 c 為一代數整數。 □

Lemma 2. *若 $c > 0$ 且 d 爲任一自然數或是 $c < 0$ 且 d 爲任一奇數，則對於多項式 $f_c(x)$，0 是一個遊蕩點。*

Proof. 已知 $c_1 = f_c(0) = c$,

$$c_2 = f_c^2(0) = f_c(f_c(0)) = c^d + c,$$

(1) 由於 $c > 0$，對於任一自然數 d 可得 $c^d > 0$，則

$$c_2 = c^d + c > c = c_1,$$

假設 $c_n > c_{n-1}$, 則

$$c_{n+1} = f_c^{n+1}(0) = f_c(f_c^n(0)) = f(c_n) = c_n^d + c > c_{n-1}^d + c = c_n,$$

根據數學歸納法，可知數列 $\{c_n\}_{n\in\mathbb{N}}$ 為嚴格遞增數列，該數列含有無限多個元素，故對於多項式 $f_c(x)$，0 是一個遊蕩點。

(2) $c < 0$ 且 d 為任一基數時，可推得 $c^d < 0$，則

$$c_2 = c^d + c < c = c_1,$$

假設 $c_n < c_{n-1} < 0$，由於 d 為奇數, 則

$$c_{n+1} = f_c^{n+1}(0) = f_c(f_c^n(0)) = f(c_n) = c_n^d + c < c_{n-1}^d + c = c_n\,,$$

根據數學歸納法，可知數列 $\{c_n\}_{n\in\mathbb{N}}$ 為嚴格遞減數列，該數列含有無限多個元素，故對於多項式 $f_c(x)$，0 是一個遊蕩點。

□

Lemma 3. *若 $c < -2^{\frac{1}{d-1}}$ 且 d 是任一偶數，則對於多項式 $f_c(x)$，0 是一個遊蕩點。*

Proof. 已知 $c_1 = f_c(0) = c < -2^{\frac{1}{d-1}}$，則

$$c_2 + c_1 = c_1^d + 2c_1 = c_1(c_1^{d-1} + 2) > 0\,,$$

可以推得 $c_2 > -c_1 > 1$ 且因為 d 是偶數

$$c_3 = c_2^d + c > (-c_1)^d + c = c_1^d + c = c_2\,。$$

假設

$$c_{n-1} > c_{n-2} > \cdots > c_3 > c_2 > 1\,,$$

則對於所有 $n \geq 4$ 的整數

$$c_n = c_{n-1}^d + c > c_{n-2}^d + c = c_{n-1}\,。$$

根據數學歸納法，可得數列 $\{c_n\}_{n\in\mathbb{N}}$ 為一嚴格遞增數列，該數列含有無限多個元素，故對於多項式 $f_c(x)$，0 是一個遊蕩點。 □

由 Lemma 2 及 Lemma 3 可知，接下來只需考慮

$$-2^{\frac{1}{d-1}} \leq c < 0$$

且 d 是偶數的情形，由於次數為 1 的代數整數即為整數，而整數的情況在一開始的介紹已說明其結果，故對於多項式 $f_c(x) = x^d + c$，我們假設 $-2^{\frac{1}{d-1}} \leq c < 0$ 且 c 是次數為 2 的代數整數，從 Proposition 1 可知對於一些非平方整數 h 且 $h \geq 2$，$\mathbb{Q}(c) = \mathbb{Q}(\sqrt{h})$，我們可以將 c 寫成 $s + t\sqrt{h}$ 的形式，其中 s 及 t 為有理數。這裡將記作

$$c_n = s_n + t_n\sqrt{h}$$

其中 s_n 及 t_n 皆為有理數且

$$s_1 = s \quad 和 \quad t_1 = t\,。$$

由於

$$c_{n+1} = c_n^d + c = (s_n + t_n\sqrt{h})^d + (s_1 + t_1\sqrt{h}),$$

可知

$$s_{n+1} = \left(\sum_{k\geq 0}\binom{d}{2k} s_n^{d-2k} t_n^{2k} h^k\right) + s_1,$$

$$t_{n+1} = \left(\sum_{k\geq 0}\binom{d}{2k+1} s_n^{d-(2k+1)} t_n^{2k+1} h^k\right) + t_1 \circ$$

Lemma 4. 假設 $-2^{\frac{1}{d-1}} \leq c < 0$ 且 d 爲偶數，若 $s > 0$ 或 $s < -2^{\frac{1}{d-1}}$，則對於多項式 $f_c(x)$，0 是一個遊蕩點。

Proof. **(1)** $s > 0$

d 為偶數可得 $\sum_{k\geq 0}\binom{d}{2k} s_n^{d-2k} t_n^{2k} h^k$ 中，每一項 $s_n^{d-2k} t_n^{2k} h^k \geq 0$,

$$s_2 = (s_1^d + \binom{d}{2} s_1^{d-2} t_1^2 h^1 + \cdots + t_1^d h^{\frac{d}{2}}) + s_1 \geq s_1^d + s_1,$$

由於 $s_1 = s > 0$ 推得 $s_1^d > 0$，則

$$s_2 \geq s_1^d + s_1 > s_1 > 0,$$

同時 $-2^{\frac{1}{d-1}} \leq c = s + t\sqrt{h} < 0$ 且 $s > 0$ 可推得 $t = t_1 < 0$，d 為偶數表示 $\sum_{k\geq 0}\binom{d}{2k+1} s_1^{d-(2k+1)} t_1^{2k+1} h^k$ 中，每一項 $s_1^{d-(2k+1)} t_1^{2k+1} h^k < 0$,

$$t_2 = (\binom{d}{1} s_1^{d-1} t_1 + \binom{d}{3} s_1^{d-3} t_1^3 h^1 + \cdots + \binom{d}{d-1} s_1 t_1^{d-1} h^{\frac{d-2}{2}}) + t_1 < t_1,$$

假設 $s_n > s_{n-1} > \cdots > s_1 > 0$ 且 $t_n < t_{n-1} < \cdots < t_1 < 0$，則

$$s_{n+1} = (s_n^d + \binom{d}{2} s_n^{d-2} t_n^2 h^1 + \cdots + \binom{d}{2k} s_n^{d-2k} t_n^{2k} h^k + \cdots + t_n^d h^{\frac{d}{2}}) + s_1$$

$(\because s_n > s_{n-1} > 0 \therefore$ 對於所有自然數 m，$s_n^m > s_{n-1}^m$，注意這裡每一項都是正的)

$$> (s_{n-1}^d + \binom{d}{2} s_{n-1}^{d-2} t_n^2 h^1 + \cdots + \binom{d}{2k} s_{n-1}^{d-2k} t_n^{2k} h^k + \cdots + t_n^d h^{\frac{d}{2}}) + s_1$$

$(\because t_n < t_{n-1} < 0 \therefore$ 對於所有偶數 m，$t_n^m > t_{n-1}^m > 0)$

$$> (s_{n-1}^d + \binom{d}{2} s_{n-1}^{d-2} t_{n-1}^2 h^1 + \cdots + \binom{d}{2k} s_{n-1}^{d-2k} t_{n-1}^{2k} h^k + \cdots + t_{n-1}^d h^{\frac{d}{2}}) + s_1$$

$$= s_n,$$

$$t_{n+1} = (\binom{d}{1} s_n^{d-1} t_n + \cdots + \binom{d}{2k+1} s_n^{d-(2k+1)} t_n^{2k+1} h^k + \cdots + \binom{d}{d-1} s_n t_n^{d-1} h^{\frac{d-2}{2}}) + t_1$$

$(\because s_n > s_{n-1} > 0 \therefore$ 對於所有自然數 m，$s_n^m > s_{n-1}^m$，注意這裡每一項都是負的)

$$< (\binom{d}{1} s_{n-1}^{d-1} t_n + \cdots + \binom{d}{2k+1} s_{n-1}^{d-(2k+1)} t_n^{2k+1} h^k + \cdots + \binom{d}{d-1} s_{n-1} t_n^{d-1} h^{\frac{d-2}{2}}) + t_1$$

$(\because t_n < t_{n-1} < 0 \therefore$ 對於所有奇數 m，$t_n^m < t_{n-1}^m < 0)$

$$< (\binom{d}{1} s_{n-1}^{d-1} t_{n-1} + \cdots + \binom{d}{2k+1} s_{n-1}^{d-(2k+1)} t_{n-1}^{2k+1} h^k + \cdots + \binom{d}{d-1} s_{n-1} t_{n-1}^{d-1} h^{\frac{d-2}{2}}) + t_1$$

$$= t_n,$$

根據數學歸納法，可知數列 $\{s_n\}_{n\in\mathbb{N}}$ 為一嚴格遞增數列且數列 $\{t_n\}_{n\in\mathbb{N}}$ 為一嚴格遞減數列，因為以 $\mathbb{Q}$ 為係數時，1 和 $\sqrt{h}$ 是線性獨立的，所以數列 $\{c_1, c_2, c_3, \ldots\}$ 含有無限多個元素，故對於多項式 $f_c(x)$，0 是一個遊蕩點。

(2) $s < -2^{\frac{1}{d-1}}$

已知 $s_1 = s < -2^{\frac{1}{d-1}} < -1$，由於 d 為偶數可得 $\sum_{k\geq 0} \binom{d}{2k} s_n^{d-2k} t_n^{2k} h^k$ 中，每一項 $s_n^{d-2k} t_n^{2k} h^k \geq 0$，因此

$$s_2 + s_1 = (s_1^d + \binom{d}{2} s_1^{d-2} t_1^2 h^1 + \cdots + t_1^d h^{\frac{d}{2}}) + 2s_1 \geq s_1^d + 2s_1 = s_1(s_1^{d-1} + 2) > 0,$$

可以推得 $s_2 > -s_1 > 2^{\frac{1}{d-1}} > 1$，則

$$s_3 = (s_2^d + \binom{d}{2} s_2^{d-2} t_n^2 h^1 + \cdots + t_n^d h^{\frac{d}{2}}) + s_1 \geq s_2^d + s_1 > s_2^d - s_2 = s_2(s_2^{d-1} - 1) > s_2$$

假設 $s_n > s_{n-1} > \cdots > s_2 > -s_1 > 2$，則

$$s_{n+1} = (s_n^d + \binom{d}{2} s_n^{d-2} t_n^2 h^1 + \cdots + t_n^d h^{\frac{d}{2}}) + s_1 \geq s_n^d + s_1 > s_n^d - s_n = s_n(s_n^{d-1} - 1) > s_n,$$

根據數學歸納法，可知數列 $\{s_n\}_{n\in\mathbb{N}}$ 為一嚴格遞增數列，因為以 $\mathbb{Q}$ 為係數時，1 和 $\sqrt{h}$ 是線性獨立的，所以數列 $\{c_1, c_2, c_3, \ldots, c_n, \ldots\}$ 含有無限多個元素，故對於多項式 $f_c(x)$，0 是一個遊蕩點。

□

Lemma 5. 假設 d 爲偶數，當 $-2^{\frac{1}{d-1}} \leq s \leq 0$ 時，若對於一些整數 $n > 1$ 讓 $s_n > 2$，則對於多項式 $f_c(x)$，0 是一個遊蕩點。

Proof. 對於一些整數 $n > 1$ 讓 $s_n > 2$，由於 d 是偶數可得 $\sum_{k\geq 0} \binom{d}{2k} s_n^{d-2k} t_n^{2k} h^k$ 中，每一項 $s_n^{d-2k} t_n^{2k} h^k \geq 0$，且 $-2^{\frac{1}{d-1}} \leq s \leq 0$ 可得

$$0 \leq s + 2 = s_1 + 2 \leq 2,$$

則

$$s_{n+1} = (s_n^d + \binom{d}{2} s_n^{d-2} t_n^2 h^1 + \cdots + t_n^d h^{\frac{d}{2}}) + s_1 \geq s_n^d + s_1 \geq s_n^2 + s_1 > 2s_n + s_1 > s_n + 2 + s_1 \geq s_n,$$

假設

$$s_{n+k} > s_{n+k-1} > s_n > 2,$$

則

$$s_{n+k+1} = (s_{n+k}^d + \cdots + t_n^d h^{\frac{d}{2}}) + s_1 \geq s_{n+k}^d + s_1 \geq s_{n+k}^2 + s_1 > 2s_{n+k} + s_1 > s_{n+k} + 2 + s_1 \geq s_{n+k},$$

根據數學歸納法，可知數列 $\{s_n, \ldots\}$ 為一嚴格遞增數列，因為以 $\mathbb{Q}$ 為係數時，1 和 $\sqrt{h}$ 是線性獨立的，所以數列 $\{c_1, c_2, c_3, \ldots, c_n, \ldots\}$ 含有無限多個元素，故對於多項式 $f_c(x)$，0 是一個遊蕩點。 □

Lemma 6. 假設 $-2^{\frac{1}{d-1}} \leq c < 0$ 是次數爲 2 的代數整數且 d 爲偶數，若 $\mathbb{Q}(c) = \mathbb{Q}(\sqrt{h})$，則對於所有非平方整數 h 且 $h \geq 2$，對於多項式 $f_c(x)$，0 是一個遊蕩點。

Proof. 從引理 5 可知當 $s > 0$ 或 $s < -2^{\frac{1}{d-1}}$ 時，對於多項式 $f_c(x)$，0 是一個遊蕩點。因此只須討論在 $-2^{\frac{1}{d-1}} \leq s \leq 0$ 的情形。由於 d 是偶數且 $-2^{\frac{1}{d-1}} \leq c < 0$，可知

$$-2 \leq -2^{\frac{1}{d-1}} \leq c = s + t\sqrt{h} < 0,$$

推得

$$-2 - s \leq t\sqrt{h} < -s \tag{1}$$

以下將 h 分成兩種情形作討論:

(I) $h \not\equiv 1 \pmod 4$

根據引理 5 可知在這個情況下，s 和 t 皆為整數。

(a) $s = 0$

此時 $c = t\sqrt{h}$，從不等式 (1), 可知

$$-2 \le t\sqrt{h} < 0。$$

若 $t \le -2$，則

$$c = t\sqrt{h} \le -2\sqrt{h} \le -2\sqrt{2} < -2 \le -2^{\frac{1}{d-1}},$$

與引理的假設矛盾，所以只需檢查 $t = -1$ 的情形。當 $c = -\sqrt{h}$，由於 d 為偶數，可知

$$c_2 = (\sqrt{h})^d - \sqrt{h} = h^{\frac{d}{2}} - \sqrt{h}$$

推得 $s_2 = h^{\frac{d}{2}}$，因為 $\sum_{k\ge 0} \binom{d}{2k} s_n^{d-2k} t_n^{2k} h^k$ 中，每一項 $s_n^{d-2k} t_n^{2k} h^k \ge 0$ 且 $h \ge 2$ ，可知

$$s_3 = (s_2^d + \cdots + t_2^d h^{\frac{d}{2}}) \ge s_2^d = h^{\frac{d^2}{2}} \ge h^2 > 2,$$

根據引理 6，在多項式 $f_c(x)$，0 是一個遊蕩點。

(b) $s \neq 0$

因為 $-2^{\frac{1}{d-1}} \le s < 0$ 且 s 為整數，可堆得 $s = -1$ 或 -2。若 $s = -1$，根據不等式 (1) 可知

$$-1 \le t\sqrt{h} < 1,$$

由於 t 為整數且 $h \ge 2$ 無法滿足上述式子，因此 $s \neq -1$。若 $s = -2$，因為 $-2^{\frac{1}{d-1}} \le s < 0$，則 $d = 2$，根據 $(**)$ 可知 $0 \le t\sqrt{h} < 2$，推得 $t = 1$ 且 $h = 2$ 或 3，此時

$$s_2 = s_1^2 + t_1^2 h = s^2 + t_1^2 h = 4 + h > 2,$$

根據引理 6，在多項式 $f_c(x)$，0 是一個遊蕩點。

(II) $h \equiv 1 \pmod 4$

根據引理 5 可知此時 $c = u + \frac{v(-1+\sqrt{h})}{2}$，其中 u, v 皆為整數，而 $s = \frac{2u-v}{2}$ 且 $t = \frac{v}{2}$。

(a) $s = 0$

從不等式 (1) 可知

$$-2 \le t\sqrt{h} < 0,$$

由於此時 $h \ge 5$, 則 t 唯一可能是 $\frac{-1}{2}$, 但 $s = \frac{2u-v}{2} = 0$ 表示 $v = 2u$ 推得 $t \neq \frac{-1}{2}$, 因此當 $h \equiv 1 \pmod 4$ 時，$s \neq 0$。

(b) $s \neq 0$

由於

$$-2 \leq -2^{\frac{1}{d-1}} \leq s = \frac{2u-v}{2} < 0,$$

可知 s 可能為 $\frac{-1}{2}, -1, \frac{-3}{2}$, 或 -2，但此時 $h \geq 5$，也就是說

$$|t\sqrt{h}| = |v|\frac{\sqrt{h}}{2} \geq \frac{\sqrt{h}}{2} \geq \frac{\sqrt{5}}{2} > 1,$$

推得 $t\sqrt{h} > 1$ 或 $t\sqrt{h} < -1$。

- $s = \frac{-1}{2}$，從不等式 (1) 可知 $\frac{-3}{2} \leq t\sqrt{h} < \frac{1}{2}$，根據上述推得 t 唯一可能是 $\frac{-1}{2}$ 且此時 $h = 5$，若 $d \geq 4$，

  $$s_2 \geq \binom{d}{2} s_1^{d-2} t_1^2 h^1 + t_1^d h^{\frac{d}{2}} + s_1 \geq 5\binom{4}{2}(\frac{-1}{2})^2(\frac{-1}{2})^2 + (\frac{-1}{2})^4\sqrt{5} - \frac{1}{2} > 2,$$

  根據引理 6，在多項式 $f_c(x)$，0 是一個遊蕩點。若 $d = 2$ 且 $c = \frac{-1}{2} - \frac{\sqrt{5}}{2}$，推得 $c_2 = c^2 + c = 1$，$c_3 = c_2^2 + c = \frac{1}{2} - \frac{\sqrt{5}}{2}$，$c_4 = c_3^2 + c = 1 - \sqrt{5}$，$c_5 = c_4^2 + c = \frac{11}{2} - \frac{5\sqrt{5}}{2}$，可知 $s_5 = \frac{11}{2} > 2$，根據引理 6，在多項式 $f_c(x)$，0 是一個遊蕩點。

- $s = -1$，從不等式 (1) 可知 $-1 \leq t\sqrt{h} < 1$，與 $t\sqrt{h} > 1$ 或 $t\sqrt{h} < -1$ 矛盾，故此例不成立。

- $s = \frac{-3}{2}$，從不等式 (1) 可知 $\frac{-1}{2} \leq t\sqrt{h} < \frac{3}{2}$ 且 $t\sqrt{h} > 1$ 或 $t\sqrt{h} < -1$，推得 $1 < t\sqrt{h} < \frac{3}{2}$，$t$ 唯一可能是 $\frac{1}{2}$，此時

  $$s_2 \geq s_1^d + t_1^d h^{\frac{d}{2}} + s_1 \geq (\frac{-3}{2})^2 + 5(\frac{1}{2})^2 + \frac{-3}{2} > 2,$$

  根據引理 6，在多項式 $f_c(x)$，0 是一個遊蕩點。

- $s = -2$，從不等式 (1) 可知 $0 \leq t\sqrt{h} < 2$ 且 $t\sqrt{h} > 1$ 或 $t\sqrt{h} < -1$，推得 $1 < t\sqrt{h} < 2$，t 唯一可能是 $\frac{1}{2}$，表示 $v = 1$，但 $s = \frac{2u-v}{2} = -2$，表示 v 必為偶數，與 $v = 1$ 矛盾，故此例不成立。

從上述可知，當 $-2^{\frac{1}{d-1}} \leq s \leq 0$ 的情形時，在多項式 $f_c(x)$，0 仍舊是一個遊蕩點。 □

1.4 主要定理證明

Theorem. 假設多項式 $f_c(x) = x^d + c$，其中 d 爲整數且 $d \geq 2$，c 爲實數且 $[\mathbb{Q}(c) : \mathbb{Q}] \leq 2$，則 0 是一個前週期點若且爲若滿足下列任一情況：

(a) $c = 0$,

(b) $c = -1$ 且 d 是偶數,

(c) $c = -2$ 且 $d = 2$。

Proof. 考慮多項式 $f_c(x) = x^c + d$，其中 c 為實數且 $[\mathbb{Q}(c) : \mathbb{Q} \leq 2]$，$d$ 為自然數，由 Lemma 2 可知當 c 不為代數整數時，對於多項式 $f_c(x)$，0 會是一個遊蕩點，因此以下討論 c 為代數整數的情形。若 d 為基數，根據 Lemma 3，對於多項式 $f_c(x)$，0 會是一個遊蕩點。若 d 為偶數，則

(1) $c > 0$
由 Lemma 3 可知，對於多項式 $f_c(x)$，0 會是一個遊蕩點。

(2) $c < -2^{\frac{1}{d-1}}$
由 Lemma 4 可知，對於多項式 $f_c(x)$，0 會是一個遊蕩點。

(3) $-2^{\frac{1}{d-1}} \leq c < 0$
由 Lemma 7 可知，對於多項式 $f_c(x)$，0 會是一個遊蕩點。

因此拓展 c 的範圍即 c 為實數且 $[\mathbb{Q}(c) : \mathbb{Q}] \leq 2$ 後，在多項式 $f_c(x) = x^d + c$，對於自然數 d，0 是週期點若且為若 $c = 0, -1, -2$，也就是說，新拓展的範圍不含整數時，對於多項式 $f_c(x)$，0 會是一個遊蕩點。 □

2 伽羅瓦群

2.1 介紹

在上一部份我們討論了特殊多項式迭代後 0 的軌道，接下來將討論對於首一二次整係數多項式迭代後的伽羅瓦群。我們的問題始源於 R.W.K. Odoni，一開始他提到了對於任意特徵數為 0 的體，討論滿足某些條件的多項式其伽羅瓦群會是甚麼樣子，完整敘述如下：

Theorem ([3, Lemma 1.1]). 令 K 是任意特徵數爲 0 的體，整數 $k \geq 2$ 且 $t \in K$，假設 K 包含了所有 1 的 k 次方根，而 $(0 \neq)\phi(X) \in K[X]$ 使得 $\phi(X^k + t)$ 在 K 上是可分的 *(separable)*，則 $\phi(X)$ 在 K 上亦是可分的，且若 $\mathrm{Gal}(\phi(X)/K) \cong H$，則存在一個 $\mathrm{Gal}(\phi(X^k + t)/K)$ 到 $C_k \wr H$ 的正準嵌射 *(canonical injection)*，其中 C_k 是階爲 k 的循環群。

接著他討論多項式迭代後的伽羅瓦群會是甚麼，假設 K 是任意特徵數為 0 的體且 T 和 X 在 K 上是代數獨立的，考慮體 $K(X,T)$ 上的多項式 $f_n(X,T) = x^{k(n)} + T$ 討論，其中整數 $n \geq 1$ 且整數 $k(n) \geq 2$，我們可以將 T 看作一個參數，X 看作一個變數，結果如下：

Theorem ([3, Theorem 1]). 假設 $F_1(X,T) = f_1(X,T)$，$F_{n+1}(X,T) = F_n(f_{n+1}(X,T),T)$，則

(1) 對於所有整數 $n \geq 1$，$F_n(X,T)$ 是次數爲 $k(1)\cdots k(2)$ 的首一多項式 *in* X，且在 $K(T)$ 中是不可約的。

(2) 假設 $\bar{K}$ 是 K 的代數閉包，則 $F_n(X,T)$ 在 $\bar{K}(T)$ 上的伽羅瓦群會同構圈積 *(wreath product)*

$$\Omega_n = G_n \wr (G_{n-1} \wr (\cdots \wr (G_2 \wr G_1)\cdots))$$

其中對於每個 $i \leq n$，G_i 是階爲 $k(i)$ 的循環群，且是對符號 $1,\cdots,k(i)$ 自然置換的作用。

當多項式的伽羅瓦群會同構一些循環群的圈積時,我們就稱這個伽羅瓦群是滿的 (full), 另外將 $G_n \wr (G_{n-1} \wr (\cdots \wr (G_2 \wr G_1)\cdots))$。接著我們想去觀察當體為有理數 $\mathbb{Q}$ 的情形，多項式的伽羅瓦群會是甚麼樣子，M. Stoll 針對整係數多項式 $f(x) = x^2 + a$ 做了相關討論，其中 $-a$ 為非平方數，他提出了 a 在甚麼樣的條件下，會讓多項式迭代後的伽羅瓦群會是滿的，其結果如下：

Theorem ([2, Theorem]). 若整數 a 滿足下列其中一個性質時：

(1) $a > 0$，且 $a \equiv 1 \pmod 4$*;*

(2) $a > 0$，且 $a \equiv 2 \pmod 4$*;*

(3) $a < 0$，且 $a \equiv 0 \pmod 4$，同時 $-a$ 是一非平方整數*;*

則對於所有整數 $n \geq 1$，

$$\mathrm{Gal}(f^n/\mathbb{Q}) \cong \underbrace{C_2 \wr (C_2 \wr (\cdots \wr (C_2 \wr C_2) \cdots))}_{n \text{ 個 } C_2}$$

其中 f^n 是 $f := x^2 + a$ 的 n 次迭代，爲了方便討論，以下將記作

$$\underbrace{C_2 \wr (C_2 \wr (\cdots \wr (C_2 \wr C_2) \cdots))}_{n \text{ 個 } C_2} = [C_2]^n \text{。}$$

到這裡我們並不知道當 a 在上述三個條件以外時，其多項是迭代後的伽羅瓦群會是甚麼樣子，這個問題顯然是不容易解決的，因此本篇論文的另一個目標，便是討論在迭代一次及兩次後，甚麼樣的情形下多項式的伽羅瓦群會是滿的，若是不滿的，那麼迭代一次的伽羅瓦群會是甚麼樣子，目前我們所做的成果如下:

Theorem 2. 假設整係數多項式 $f_c(x) := x^2 + c$，其中 c 不爲 0，$f_c^0(x) = x$，對於所有整數 $n \geq 0$，令 $f_c^{n+1}(x) := f_c(f_c^n)(x) = (f_c^n(x))^2 + c$，$K_0 = \mathbb{Q}$，且 K_n 是 f^n 在 $\mathbb{Q}$ 上的分裂體 *(splitting field)*，則：

(1) 若 $c = 3$，則 $\mathrm{Gal}(K_2/\mathbb{Q}) = D_4$ 且 $[K_3 : K_2] = 8$。

(2) 若 $c = -n^2$，其中 n 爲非零整數，則 $\mathrm{Gal}(K_2/\mathbb{Q}) = C_2 \times C_2$ 且 $K_1 = \mathbb{Q}$。

(3) 若 $c = -m^2 - 1$，其中 m 爲非零整數，則 $\mathrm{Gal}(K_2/\mathbb{Q}) = C_4$。

而上述第三個情形有更一般化的結果，H.-C. Li[9] 針對多項式 $f(x) = x^2 - (4k+1)$ 做了相關的討論，其中 k 是自然數，$4k+1$ 是非平方整數，也就是我們第三個例子當 m 為偶數時，其結果如下:

Theorem ([9])**.** 對於所有 $n \geq 3$，$\mathrm{Gal}(K_n/\mathbb{Q}) \cong C_4[[C_2]^{n-2}]$。

接下來同樣分三小節來做介紹, 2-2 節將先介紹一些我們會使用到的相關先備知識, 2-3 節則會介紹一些與主要定理相關的引理，2-4 節則是主要定理的證明。

2.2 先備知識

2.2.1 樹的自同構

這裡我們首先介紹樹的自同構相關知識，以及多項式迭代後的伽羅瓦群與樹的自同構關係，以下內容主要參考自 J.J. Rotman 的「An Introduction to the Theory of Groups, CH7」[6] 以及 H.-C. Li[8]。

Definition 9 ([6, Page 167])**.** 假設 G 是一個群，K 是 G 的一個子群，若對於 G 的任意子群 Q 滿足 $K \cap Q = 1$ 且 $KQ = G$ 則稱 Q 是一個在 G 中 K 的補群 (*complement*)

Definition 10 ([6, Page 167])**.** 假設 G 是一個群，$K \triangleleft G$ 且 K 有一個補群 $Q_1 \cong Q$，則稱 G 是 K 對 Q 的半直積 (*semidirect product*)，記作 $G = K \rtimes Q$。

Theorem ([6, Page 170])**.** 給定群 Q 和群 K 及一個同態映射 $\theta : Q \to \mathrm{Aut}(K)$，則 $G = K \rtimes_\theta Q$ 可定義爲一個包含所有序對 $(a, x) \in K \times Q$ 配上下列運算的群

$$(a, x)(b, y) = (a\theta_x(b), xy)$$

其中 $(b, y) \in K \times Q$。

Definition 11 ([6, Page 172])**.** 假設 D 和 Q 是一個群，Ω 是一個有限 Q-集 (Q-set)，$K = \prod_{\omega\in\Omega} D_\omega$ 其中對於所有 $\omega \in \Omega$，$D_\omega \cong D$。當 Q 對 K 的作用是 $q \cdot (d_\omega) = (d_{qw})$ 其中 $q \in Q$ 且 $(d_\omega) \in \prod_{\omega\in\Omega} D_\omega$，則 D 對 Q 的圈積 (*wreath product*) 是一個 K 對 Q 的半直積，記作 $D \wr_\Omega Q$，若清楚 Ω 為何者時，我們將省略 Ω 記作 $D \wr Q$。

Definition 12 ([6, Page 174])**.** 一個圖 (*graph*)Γ 是由非空頂點集 (*vertices set*)V 所組成，其中頂點彼此間的關係稱做邊 (*edge*)，對於相異頂點 $u, v \in V$，將邊記做 $u \sim v$，邊滿足對稱性 ($u \sim v \Rightarrow v \sim u$) 與反自身性 ($u \nsim u$)。

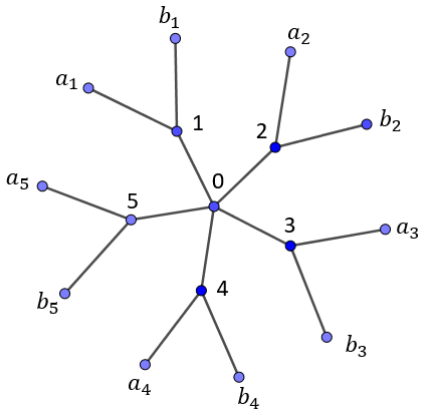
Definition 13. 樹 (*tree*) 是一種圖，其任意兩個頂點間存在唯一一條路徑且不具有迴路，在這裡稱頂點為節點。

Definition 14 ([6, Page 174])**.** 一個樹 T 對於其節點的自同構 (automorphism) 是一個對射 (bijection)

$$\phi : V \to V$$

使得 u、$v \in V$ 是相鄰節點若且唯若 $\phi(u)$、$\phi(v)$ 是相鄰節點。此自同構記作 $\mathrm{Aut}(T)$。

為了能夠更好的了解甚麼是一個樹的自同構，因此我們在這裡給簡單的例子。



Example 1 ([6, Page 174])**.** 考慮上圖 Γ
若 $\phi \in \mathrm{Aut}(\Gamma)$，則 ϕ 會固定 (fix) 節點 0，且 ϕ 會對 $\Omega = \{1, 2, 3, 4, 5\}$ 排列 (permute)，對於所有的 i，

$$\phi(a_i) = a_{\phi(i)} \text{ 且 } \phi(b_i) = b_{\phi(i)}$$

或

$$\phi(a_i) = b_{\phi(i)} \text{ 且 } \phi(b_i) = a_{\phi(i)} \text{。}$$

Definition 15. 有根樹 (*rooted* tree) 是挑選出某個特殊節點的樹，該特殊節點稱為樹的根 (*root*)。有根樹中任一節點的階層 (*leavel*) 為該節點與根的路徑中邊的個數，而任意兩相鄰的節點，階層數較小的稱為雙親節點 (*parents*)，階層數較大的稱為子女節點 (*children*)，若節點無子女節點，則稱做葉子 (*leaves*)。在圖上，通常將根畫在最下方即最底層。

Definition 16. 有根二元樹 (*rooted binary tree*) 是有根樹的一種，其每個節點最多只有兩個分支。若每個節點都具有兩個分支，則又叫做有根滿二元樹 (*rooted full binary tree*)。

為了方便討論，以下將 T_n 表示為 n-階層的有根滿二元樹。已知 T_n 是一個 n-階層的有根滿二元樹，我們可以將 T_n 看成是一個 (n-1)-階層的滿有根二元樹 T_{n-1} 且在每個 T_{n-1} 的葉子上加上 1-階層的有根滿二元樹 T_1'，也就是說，我們可以將 T_n 看成是 $(T_1')^M \times T_{n-1}$，其中 M 是 T_{n-1} 的個數。T_n 上的每片葉子我們用 (y, j) 來表示，其中 j 是 T_{n-1} 上的葉子，而 y 是 T_1' 上的葉子。

Definition 17 ([8, Page 1-Page2])**.** 假設 G 是一個群，考慮

$$G^n = \underbrace{G \times \cdots \times G}_{n \text{ 個}}$$

以及 $\sigma \in S_n$ 對 G^n 作用，若 $\bar{p} = (p^{(1)}, \cdots, p^{(i)}, \cdots, p^{(n)}) \in G^n$，也就是說 $\bar{p}$ 的第 i 項是 $p^{(i)}$，當 $\bar{p}$ 經由指標的排列後形成 G^n 的另一個元素時，我們用 $p_i^{(j)}$ 來表示其第 i 項是原來

$\bar{p}$ 的第 j 項 $p^{(j)}$。考慮左作用 (left action):

$$\sigma * \bar{p} = (\dots, p^{(i)}_{\sigma(i)}, \dots)$$

也就是說 $\sigma * \bar{p}$ 的第 $\sigma(i)$ 項就是原來 $\bar{p}$ 的第 i 項 (或是 $\sigma * \bar{p}$ 的第 i 項就是原來 $\bar{p}$ 的第 $\sigma^{-1}(i)$ 項)。

以下證明上述左作用確實是 S_n 對 G^n 的群作用，由於 S_n 的單位元素對所有 G^n 的元素作用還會是該元素本身這件事是顯然的，因此這裡我們檢查是否有結合律:
假設 $\bar{p} = (\cdots, p^{(i)}, \cdots)$，以及 $\sigma、\tau \in S_n$，根據定義，

$$(\tau\sigma) * \bar{p} = (\cdots, p^{(i)}_{\tau\sigma(i)}, \cdots)$$

表示 $(\tau\sigma) * \bar{p}$ 的第 $\tau\sigma(i)$ 項就是原來的 $p^{(i)}$，另外根據定義，

$$\tau * (\sigma * \bar{p}) = \tau * (\cdots, p^{(i)}_{\sigma(i)}, \cdots) = (\cdots, p^{(i)}_{\tau\sigma(i)}, \cdots)$$

也就是說 $\tau * (\sigma * \bar{p})$ 的第 $\tau\sigma(i)$ 項是 $\sigma * \bar{p}$ 的第 $\sigma(i)$ 項也就是 $p^{(i)}$，因此有結合律

$$(\tau\sigma) * \bar{p} = \tau * (\sigma * \bar{p}) \ 。$$

另外我們可以將 σ 視為 $\mathrm{Aut}(G^n)$ 的元素:

$$\sigma : G^n \to G^n$$
$$\bar{p} \mapsto \sigma * \bar{p}$$

以下為其證明: 假設 $\bar{q} = (\cdots, q^{(i)}, \cdots)$

- 一對一 (one to one):
  若 $\sigma(\bar{p}) = \sigma(\bar{q})$，則

  $$\sigma * \bar{p} = (\cdots, p^{(i)}_{\sigma(i)}, \cdots) = \sigma * \bar{q} = (\cdots, q^{(i)}_{\sigma(i)}, \cdots)$$

  可推得 $p^{(i)} = q^{(i)}$，也就是 $\bar{p} = \bar{q}$。

- 映成 (onto):
  對於所有的 $\bar{p} \in G^n$，取 $\sigma^{-1}(\bar{p}) \in G^n$，則可知

  $$\sigma(\sigma^{-1}(\bar{p})) = \bar{p}。$$

- 群同態 (group homomorphism):
  假設 $\bar{q} = (\cdots, q^{(i)}, \cdots)$，已知 $\bar{p}\bar{q} = (\cdots, p^{(i)}q^{(i)}, \cdots)$，則 $\sigma * (\bar{p}\bar{q})$ 的第 $\sigma(i)$ 項會是 $\bar{p}\bar{q}$ 的第 i 項 $p^{(i)}q^{(i)}$ 也就是

$$\sigma * (\bar{p}\bar{q}) = (\cdots, p^{(i)}_{\sigma(i)}q^{(i)}_{\sigma(i)}, \cdots)。$$

  而

$$(\sigma * \bar{p})(\sigma * \bar{q}) = (\cdots, p^{(i)}_{\sigma(i)}, \cdots)(\cdots, q^{(i)}_{\sigma(i)}, \cdots) = (\cdots, p^{(i)}_{\sigma(i)}q^{(i)}_{\sigma(i)}, \cdots)$$

  表示 $(\sigma * \bar{p})(\sigma * \bar{q})$ 的第 $\sigma(i)$ 項會是 $\bar{p}\bar{q}$ 的第 i 項 $p^{(i)}q^{(i)}$ ，因此有

$$\sigma * (\bar{p}\bar{q}) = (\sigma * \bar{p})(\sigma * \bar{q})。$$

Definition 18. 假設 $\sigma \in Aut(T_n)$，定義

$$\sigma = ((a_1, \ldots, a_M), d),$$

其中 M 是 T_{n-1} 上葉子的個數，$d \in Aut(T_{n-1})$，$a_1, \ldots, a_M \in Aut(T_1')$。

σ 作用在 T_n 上，可以想成是先用 d 來移動 T_{n-1} 上的 M 片葉子，接著分別用 $a_1, \ldots, a_M$ 對 M 個 T_1' 作用。

Definition 19. 對於 $(y, j) \in T_n$，我們有

$$\sigma(y, j) = ((a_1, \ldots, a_M), d)(y, j) = (a_{d(j)}(y), d(j))。$$

對於 Definition 18 我們給一個簡單的看法，已知 $\sigma = ((a_1, \ldots, a_M), d)$，而 σ 對 (y, j) 作用的方式是先將 j 移動到 $d(j)$ 的位置，接著再從 $(a_1, \cdots, a_M)$ 的挑第 $d(j)$ 項也就是 $a_{d(j)}$ 對 y 作用，若要了解更詳細的內容可參考 [6, Page 172-173]。

Lemma 7 ([8, H.-C. Li])**.** 假設 $\Gamma = \{1, \ldots, M\}$，其中 M 是 T_n 上第 $n-1$ 階層的節點個數，則

$$\mathrm{Aut}(T_n) \cong \mathrm{Aut}(T_1') \wr_\Gamma \mathrm{Aut}(T_{n-1})。$$

Proof. 假設 $\mathrm{Aut}(T_n)$ 的兩個元素為

$$\sigma = (\bar{c}, d) = ((c_1, \cdots, c_M), d)$$

$$\tau = (\bar{c}', d') = ((c_1', \cdots, c_M'), d')$$

且 (y, j) 是 T_n 上的葉子，其中 c_i、$c_i' \in \mathrm{Aut}(T_1')$，$d$、$d' \in \mathrm{Aut}(T_{n-1})$ 以及 y 是 T_1' 上的葉子，j 是 T_{n-1} 上的葉子。令

$$\tau\sigma = (\bar{c}'', d'') = ((c_1'', \cdots, c_M''), d'')$$

根據定義可知

$$\tau\sigma(y,j) = (c''_{d''(j)}(y)), d''(j))。$$

另外已知

$$\tau\sigma(y,j) = \tau(\sigma(y,j)) = \tau(c_{d(j)}(y), d(j)) = (c'_{d'(d(j))}(c_{d(j)}(y)), d'(d(j)))\ ,$$

因此可推得

$$c''_{d''(j)} = c'_{d'(d(j))}c_{d(j)}及d'' = d'd$$

也就是說

$$\tau\sigma = (\bar{c}', d')(\bar{c}, d) = (\bar{c}'', d'd)$$

其中 $\bar{c}''$ 的第 $(d'd)(j)$ 項是 $c'_{d'(d(j))}c_{d(j)}$，然而 $c'_{d'(d(j))}$ 是 $\bar{c}'$ 的第 $(d'd)(j)$ 項，$c_{d(j)}$ 為 $\bar{c}$ 的第 $d(j)$ 項也是 Definition 17 介紹的左作用 $d' * \bar{c}$ 的第 $(d'd)(j)$ 項，故可知 $\bar{c}'(d' * \bar{c})$ 的第 $(d'd)(j)$ 項亦為 $c'_{d'(d(j))}c_{d(j)}$，所以有以下式子

$$(\bar{c}', d')(\bar{c}, d) = (\bar{c}'(d' * \bar{c}), d'd) \tag{2}$$

其中 $\bar{c}'(d' * \bar{c}) \in \mathrm{Aut}(T'_1)^M = \underbrace{\mathrm{Aut}(T'_1) \times \cdots \times \mathrm{Aut}(T'_1)}_{M\ 個}$，$d'd \in \mathrm{Aut}(T_{n-1})$。以下我們證明式子 (2) 定出了一個群，由於式子 (2) 已說明了封閉性且存在單位元素 $(id_{\mathrm{Aut}(T'_1)^M}, id_{\mathrm{Aut}(T_{n-1})})$ 是顯然的 (以下將省略 id 的下標)，因此以下說明反元素與結合律:

- 反元素:
  由於

  $$(\bar{c}, d)(d^{-1} * \bar{c}^{-1}, d^{-1}) = (\bar{c}(d * (d^{-1} * \bar{c}^{-1})), dd^{-1}) = (\bar{c}((dd^{-1}) * \bar{c}^{-1}), id) = (\bar{c}\bar{c}^{-1}, id) = (id, id)$$

  $$(d^{-1} * \bar{c}^{-1}, d^{-1})(\bar{c}, d) = ((d^{-1} * \bar{c}^{-1})(d^{-1} * \bar{c}), d^{-1}d) = (d^{-1} * \bar{c}^{-1}\bar{c}, id) = (d^{-1} * id, id) = (id, id)$$

  因此可知對於任意元素 $(\bar{c}, d)$ 存在反元素 $(d^{-1} * \bar{c}^{-1}, d^{-1})$。

- 結合律:

  $$(\bar{c}'', d'')((\bar{c}', d')(\bar{c}, d)) = (\bar{c}'', d'')(\bar{c}'(d' * \bar{c}), d'd) = (\bar{c}''(d'' * (\bar{c}'(d' * \bar{c}))), d''d'd)$$

  $$((\bar{c}'', d'')(\bar{c}', d'))(\bar{c}, d) = (\bar{c}''(d'' * \bar{c}'), d''d')(\bar{c}, d) = ((\bar{c}''(d'' * \bar{c}'))((d''d') * \bar{c}), d''d'd)$$

  前面有證過左作用是一個群同態，因此有

  $$\bar{c}''(d'' * (\bar{c}'(d' * \bar{c})) = \bar{c}''(d'' * \bar{c}')(d'' * (d' * \bar{c})) = \bar{c}''(d'' * \bar{c}')((d''d') * \bar{c})$$

  故

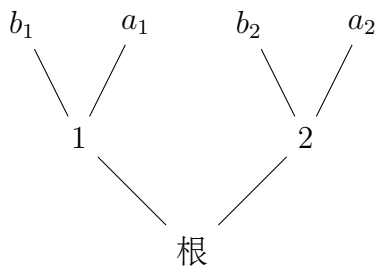
  $$(\bar{c}'', d'')((\bar{c}', d')(\bar{c}, d)) = ((\bar{c}'', d'')(\bar{c}', d'))(\bar{c}, d)$$

由於式子 (2) 是一個群結構且定法與半直積相同，因此可知

$$\mathrm{Aut}(T_n) \cong \mathrm{Aut}(T_1')^M \rtimes \mathrm{Aut}(T_{n-1}) \cong \mathrm{Aut}(T_1') \wr_\Gamma \mathrm{Aut}(T_{n-1})$$

其中 $\Gamma = \{1, \cdots, M\}$。 □

Example 2. 考慮階層為 2 的有根滿二元樹 T_2，如下圖:



$\mathrm{Aut}(T_2)$ 作用在 T_2 上，作用的方式便是根的位置不變，接著決定第一層的兩個節點 1、2 位置不變或是位置交換，最後再決定 a_1、b_1 位置不變或是位置交換及 a_2、b_2 位置不變或是位置交換，由此可知

$$\mathrm{Aut}(T_2) \cong (\mathrm{Aut}(T_1') \times \mathrm{Aut}(T_1')) \rtimes \mathrm{Aut}(T_1) \cong (C_2 \times C_2) \rtimes C_2 = C_2 \wr C_2 = [C_2]^2 \text{。}$$

Lemma 8.

$$\mathrm{Aut}(T_n) \cong [C_2]^n \text{。}$$

Proof. 由於 $\mathrm{Aut}(T_1) \cong C_2$ 且從 Example 2 可知 $\mathrm{Aut}(T_2) \cong [C_2]^2$，假設

$$\mathrm{Aut}(T_k) \cong [C_2]^k$$

則根據 Lemma 7,

$$\mathrm{Aut}(T_{k+1}) \cong \mathrm{Aut}(T_1') \wr \mathrm{Aut}(T_k) \cong C_2 \wr [C_2]^k = [C_2]^{k+1}$$

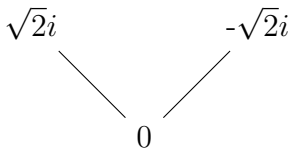
根據數學歸納法,

$$\mathrm{Aut}(T_n) \cong [C_2]^n \text{。}$$

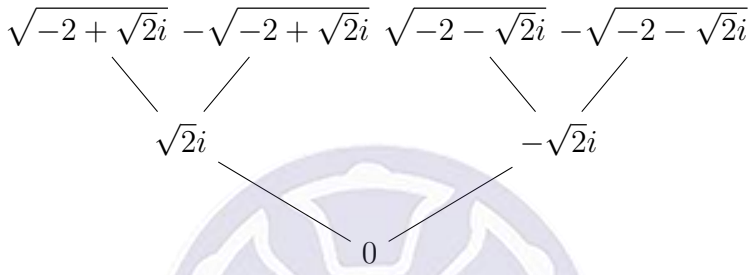
□

假設整係數多項式 $f(x) := x^2 + c$，$f^0(x) := x$，對於所有整數 $n \geq 0$，$f^{n+1}(x) := f(f^n(x)) = (f^n(x))^2 + c$ ，K_n 是 $f^n(x)$ 在 $\mathbb{Q}$ 上的分裂體。多項式 n 次迭代後的零根可以想成是 T_n 上的葉子，其中樹的根固定為 0，我們舉一個簡單的例子說明。

Example 3. 考慮整係數多項式 $f(x) = x^2 + 2$，其一次迭代的零根，也就是 $f(x)$ 的零根為 $\sqrt{2}i$、$-\sqrt{2}i$，則其對應到的有根滿二元樹 T_1 如下：



而二次迭代的零根，也就是 $f^2(x) = (x^2+2)^2 + 2$ 的零根為 $\sqrt{-2+\sqrt{2}i}$、$\sqrt{-2-\sqrt{2}i}$、$-\sqrt{-2+\sqrt{2}i}$、$-\sqrt{-2-\sqrt{2}i}$，其對應到的有根滿二元樹如下：



在這裡伽羅瓦群的元素對多項式一次迭代的零根作用也就是對 T_1 的葉子作用，對多項式二次迭代的零根作用也就是對 T_2 的葉子作用。假設 σ 是迭代二次的伽羅瓦群元素，其作用如下

$$\begin{cases} \sigma(\sqrt{-2+\sqrt{2}i}) = -\sqrt{-2+\sqrt{2}i} \\ \sigma(\sqrt{-2-\sqrt{2}i}) = -\sqrt{-2-\sqrt{2}i} \end{cases},$$

已知

$$f(\sqrt{-2+\sqrt{2}i}) = \sqrt{2}i$$

也就是說 $\sqrt{-2+\sqrt{2}i}$ 及 $\sqrt{2}i$ 是兩相鄰節點，則

$$f(\sigma(\sqrt{-2+\sqrt{2}i})) = (-\sqrt{-2+\sqrt{2}i})^2 + 2 = (-2+\sqrt{2}i) + 2 = \sqrt{2}i$$

而

$$\sigma(\sqrt{2}i) = \sigma((\sqrt{-2+\sqrt{2}i})^2 + 2) = \sigma((\sqrt{-2+\sqrt{2}i}))^2 + 2 = \sqrt{2}i$$

因此可得

$$f(\sigma(\sqrt{-2+\sqrt{2}i})) = \sigma(\sqrt{2}i)$$

表示 $\sigma(\sqrt{-2+\sqrt{2}i})$ 及 $\sigma(\sqrt{2}i)$ 亦為相鄰節點，故 $\sigma \in \mathrm{Aut}(T_2)$。

Theorem ([3, Theorem 2]). 假設整係數多項式 $f(x) = x^2 + t$，K_n 是 $f^n(x)$ 的分裂體 *(splittind field)*，其多項式迭代後的伽羅瓦群與樹的自同構有對應關係：

$$\rho : \mathrm{Gal}(K_n/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(T_n)。$$

Proof. 假設 $f^n(x)$ 是 $f(x)$ n 次迭代後的整係數多項式, $\Lambda = \{\lambda_1, \cdots, \lambda_m\}$, 其中 $f^n(\lambda_i) = 0$。考慮整係數多項式 $f^n(x^2+t)$, 令 β_j、$-\beta_j$ 是 $x^2+t = \lambda_j$ 的根。若 $\sigma \in \mathrm{Gal}(f(x^2+t)/\mathbb{Q})$, 假設 $\sigma|_L = d$, $\bar{c} = (c_1, \cdots, c_m)$, 其中 $c_i \in C_2$, 則

$$\sigma(\lambda_j) = \lambda_d(j)$$

$$\sigma(\beta_j) = (-1)^{c_{d(j)}}\beta_{d(j)}$$

因此有以下對應關係:

$$\begin{array}{ccc} \rho : \mathrm{Gal}(f^n(x^2+c)/\mathbb{Q}) & \hookrightarrow & C_2 \wr_\Lambda \mathrm{Gal}(f^n(x)/\mathbb{Q}) \\ \sigma & \mapsto & (\bar{c}, d) \end{array}$$

以下證明 ρ 是一對一 (one to one) 且是一個群同態 (group homomorphism)。假設 $\sigma、\sigma' \in \mathrm{Gal}(f^n(x^2+t)/\mathbb{Q})$, $\rho(\sigma) = (\bar{c}, d)$, $\rho(\sigma') = (\bar{c}', d')$, 其中 $\bar{c} = (c_1, \cdots, c_m)$、$\bar{c}' = (c'_1, \cdots, c'_m)$

(1) 一對一:
假設

$$\rho(\sigma) = (\bar{c}, d) = (\bar{c}', d') = \rho(\sigma')$$

則

$$\sigma(\lambda_i) = \lambda_{d(j)} = \lambda_{d'(j)} = \sigma'(\lambda_j)$$

$$\sigma(\beta_j) = (-1)^{c_{d(j)}}\beta_{d(j)} = (-1)^{c'_{d(j)}}\beta_{d'(j)} = \sigma'(\beta_j)$$

故可知

$$\sigma = \sigma'。$$

(2) 群同態: (這裡將 C_2 的運算用加法表示)
已知

$$\rho(\sigma')\rho(\sigma) = (\bar{c}', d')(\bar{c}, d) = (\bar{c}' + (d' * \bar{c}), d'd)$$

從

$$(\sigma'\sigma)(\lambda_j) = \sigma'(\sigma(\lambda_j)) = \sigma'(\lambda_{d(j)}) = \lambda_{d'(d(j))}$$

可推得

$$\sigma'\sigma|_L = d'd$$

且

$$(\sigma'\sigma)(\beta_j) = \sigma'(\sigma(\beta_j)) = \sigma'((-1)^{c_{d(j)}}\beta_{d(j)}) = (-1)^{c_{d(j)}}\sigma'(\beta_{d(j)}) = (-1)^{c_{d(j)}+c'_{d'd(j)}}\beta_{d'(d(j))}$$

假設

$$\rho(\sigma'\sigma) = (\bar{c}'', d'd)$$

從 $\sigma'\sigma$ 對 β_j 的作用可知 $\bar{c}''$ 的 $d'd(j)$ 項是 $c_{d(j)} + c'_{d'd(j)}$，同時 $c_{d(j)}$ 表示是 $\bar{c}$ 的第 $d(j)$ 項，也可看成是 $d' * \bar{c}$ 的第 $d'd(j)$ 項，且 $c'_{d'(d(j))}$ 表示是 $\bar{c}'$ 的第 $d'd(j)$ 項，因此 $c_{d(j)} + c'_{d'd(j)}$ 即為 $\bar{c}' + (d' * \bar{c})$ 的第 $d'd(j)$ 項，故推得

$$\rho(\sigma'\sigma) = (\bar{c}' + (d' * \bar{c}), d'd) = \rho(\sigma')\rho(\sigma)$$

接著我們用上述結果來證明多項式迭代後的伽羅瓦群與樹的自同構的對應關係，已知 $n = 1$ 時

$$\mathrm{Gal}(f(x)/\mathbb{Q}) \hookrightarrow C_2$$

則

$$\mathrm{Gal}(f^2(x)/\mathbb{Q}) = \mathrm{Gal}(f(x^2+t)/\mathbb{Q}) \hookrightarrow C_2 \wr_\Lambda \mathrm{Gal}(f(x)/\mathbb{Q}) \hookrightarrow C_2 \wr_\Lambda C_2 = [C_2]^2$$

假設 $n = k$ 有以下關係

$$\mathrm{Gal}(f^k(x)/\mathbb{Q}) \hookrightarrow [C_2]^k$$

則 $n = k + 1$ 時，可推得

$$\mathrm{Gal}(f^{k+1}(x)/\mathbb{Q}) = \mathrm{Gal}(f^k(x^2+t)/\mathbb{Q}) \hookrightarrow C_2 \wr_\Lambda \mathrm{Gal}(f(x)^{k+1}/\mathbb{Q}) \hookrightarrow C_2 \wr_\Lambda [C_2]^{k+1} = [C_2]^{k+2}$$

從 Lemma 8 可知 $\mathrm{Aut}(T_n) \cong [C_2]^n$，故可推得

$$\mathrm{Gal}(f^n(x)/\mathbb{Q}) = \mathrm{Gal}(K_n/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(T_n)。$$

□

2.2.2 四次多項式的伽羅瓦群

這裡要介紹一些判斷四次多項式伽羅瓦群的相關工具，主要參考 J.S. Miline 的「Field and Galois Theory, CH4」[4] 。假設對於體 F，首一四次多項式 $f(x) \in F[x]$，E 是 $f(x)$ 的分裂體 (splitting field)，已知在 E 上 $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$，其中 α_1、α_2、α_3、α_4 是相異的，考慮下列三個值:

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$$

$$\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$$

$$\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

已知

$$\alpha - \beta = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$$

$$\alpha - \gamma = \alpha_1(\alpha_2 - \alpha_4) + \alpha_3(\alpha_4 - \alpha_2) = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$$

$$\beta - \gamma = \alpha_1(\alpha_3 - \alpha_4) + \alpha_2(\alpha_4 - \alpha_3) = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$$

由於 α_1、α_2、α_3、α_4 是相異的，所以可知 α、β、γ 亦是相異的。

Definition 20 ([4, Page 50]). $g(x) = (x-\alpha)(x-\beta)(x-\gamma) \in F[\alpha,\beta,\gamma][x]$ 稱為 $f(x)$ 的預解三次式 (*resolvent cubic*)。

Theorem 3 ([4, Page 50]). 假設多項式 $f(x) = x^4 + bx^3 + cx^2 + dx + e$，則 $f(x)$ 的預解三次式爲

$$g(x) = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \text{。}$$

Theorem 4 ([4, Page 50]). 假設 $M = F(\alpha,\beta,\gamma)$，若 $f(x)$ 在體 F 下是不可約 *(irreducible)* 的可分 *(separable)* 四次多項式，則我們可以用以下的表格來判斷 $f(x)$ 的伽羅瓦群。以下將 $f(x)$ 的伽羅瓦群記作 G_f：

G_f	$[E:M]$	$[M:F]$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

2.2.3 2-獨立

以下內容主要參考自 D.M. Burton 的「Elementary Number Theory,CH9」[7] 及 M. Stoll 的「Galois groups over $\mathbb{Q}$ of some iterated polynomials」[2]。

Definition 21. 繆比烏斯函數 (*mobius function*)μ 是指以下的函數:

$$\mu(n) = \begin{cases} 1 & \text{若 n=1} \\ (-1)^k & \text{若 } n = p_1 p_2 \dots p_k \text{ 無平方因數，其中 } p_i \text{ 為質數} \\ 0 & \text{若 } n \text{ 有大於 1 的平方因數} \end{cases}$$

Definition 22 ([7, Page 175])**.** 若 p 是一個奇質數，a 是一個整數，且 $gcd(a,p) = 1$，則勒讓德符號 (*Legendre symbol*) 定義為下:

$$(\frac{a}{p}) = \begin{cases} 1 & \text{對於某個整數 } x \text{ 使得 } x^2 \equiv a \pmod{p} \\ -1 & \text{不存在整數 } x \text{ 使得 } x^2 \equiv a \pmod{p} \end{cases}$$

Theorem 5 ([7, Page 177])**.** *若 p 是一個奇質數，則*

$$(\frac{-1}{p}) = \begin{cases} 1 & \text{若 } p \equiv 1 \pmod{4} \\ -1 & \text{若 } p \equiv 3 \pmod{4} \end{cases} \text{。}$$

若想了解上述定理證明，可參考 [7, Page 171-177]。

Definition 23 ([2, Definition])**.** 對於非零有理數 $a_1, a_2, \dots, a_n$，若在 $\mathbb{F}_2$-向量空間 $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ 中，其剩餘類 (residue class) 是線性獨立的，則稱 $a_1, a_2, \dots, a_n$ 是2-獨立 (2-*independent*)。

假設整係數多項式 $f(x) = x^2 + c$，其中 $-c$ 為非平方整數，令 $f^0(x) = x$，對於整數 $n \geq 1$，$f^{n+1}(x) = f(f^n(x)) = (f^n(x))^2 + c$，$c_1 = -c$，$c_n = f^n(0)$，$b_n = \prod_{d|n} c_d^{\mu(\frac{n}{d})}$。

Theorem 6 ([2, Lemma 1.2])**.** *若 $c_1, c_2, \dots, c_n$ 在 $\mathbb{Q}$ 上皆為非平方數，則 $f^n(x)$ 是不可約有理多項式。*

Theorem 7 ([3, Theorem])**.** *對於所有自然數 n，K_n 為 $f^n(x)$ 的分裂體 (splitting field)，以下敘述是等價的:*

(a) $\mathrm{Gal}(K_n/\mathbb{Q}) \cong [C_2]^n$*;*

(b) $c_1, c_2, \dots, c_n$ *是 2-獨立;*

(c) $b_1, b_2, \dots, b_n$ *是 2-獨立。*

2.3 預備引理

假設整係數多項式 $f(x) = x^2 + c$，其中 $-c$ 為非平方整數，令 $f^0(x) = x$，對於整數 $n \geq 1$，$f^{n+1}(x) = f(f^n(x)) = (f^n(x))^2 + c$，$c_1 = -c$，$c_n = f^n(0)$ 且

$$b_n = \prod_{d|n} c_d^{\mu(\frac{n}{d})},$$

為了方便接下來的證明，我們先列出一些 b_n 的值:

$$b_1 = \prod_{d|1} c_d^{\mu(\frac{1}{d})} = c_1^{\mu(1)} = -c$$

$$b_2 = \prod_{d|2} c_d^{\mu(\frac{2}{d})} = c_1^{\mu(2)} \times c_2^{\mu(1)} = \frac{1}{-c} \times (c^2 + c) = -c - 1$$

$$b_3 = \prod_{d|3} c_d^{\mu(\frac{3}{d})} = c_1^{\mu(3)} \times c_3^{\mu(1)} = \frac{1}{-c} \times [(c^2 + c)^2 + c] = -c(c+1)^2 - 1$$

Lemma 9. 對於整數 n、m，當 $c \neq -n^2$ 或 $c \neq -m^2 - 1$ 時，b_1、b_2 是 2-獨立。

Proof. 這裡要去討論 b_1、b_2、b_1b_2 這三種情形在甚麼樣的狀況下會同時是非平方整數，也就是說當任一 b_1、b_2、b_1b_2 為平方整數時，b_1、b_2 就不會是 2-獨立，因此我們分別對 b_1、b_2、b_1b_2 討論:

(i) b_1:
$\sqrt{b_1} = \sqrt{-c} \notin \mathbb{Z} \Leftrightarrow$ 對於整數 n，$c \neq -n^2$。

(ii) b_2:
$\sqrt{b_2} = \sqrt{-(c+1)} \notin \mathbb{Z} \Leftrightarrow$ 對於整數 m，$c + 1 \neq -m^2$。

(iii) b_1b_2:
$\sqrt{b_1b_2} = \sqrt{c^2 + c} \notin \mathbb{Z} \Leftrightarrow$ 對於整數 s，$c^2 + c \neq s^2$。
已知對於所有 $c > 0$,

$$c^2 < c^2 + c = c(c+1) < (c+1)^2,$$

則對於整數 s，$c^2 + c \neq s^2$ 。同時對於所有 $c < 0$,

$$(c+1)^2 \leqslant c^2 + c = c(c+1) < c^2,$$

但 $c(c+1) = (c+1)^2$ 若且為若 $c = -1$，所以對於整數 s，當 $c \neq -1$，則 $c^2 + c \neq s^2$。

綜合上述可得，對於整數 n、m，當 $c \neq -n^2$ 或 $c \neq -m^2 - 1$，b_1、b_2 是 2-獨立。 □

從 Theorem 7 及 Lemma 9，可知對於整數 n、m 當整數 c 不為 $-n^2$ 或 $-m^2-1$ 時，$\mathrm{Gal}(K_2/\mathbb{Q}) \cong [C_2]^2$。

Lemma 10. *對於整數 n、m，當 $c \neq 3$、$c \neq -n^2$ 或 $c \neq -m^2-1$ 時，b_1、b_2、b_3 是 2-獨立。*

Proof. 這裡原本要討論 c 在甚麼情形下會使得 b_1、b_2、b_3、b_1b_2、b_1b_3、b_2b_3、$b_1b_2b_3$ 皆為非平方整數，但從 Lemma 9 可知 $c=-n^2$ 和 $c=-m^2-1$ 時，b_1、b_2 不會是 2-獨立，表示在這情形下，b_1、b_2、b_3 也不會是 2-獨立，因此以下只需討論排除 $c=-n^2$ 和 $c=-m^2-1$，c 甚麼時候會讓 b_3、b_1b_3、b_2b_3、$b_1b_2b_3$ 皆為非平方整數。

(i) b_3:
假設 $b_3=-c(c+1)^2-1=v^2$，其中 v 為整數，則對於所有整除 c 的質因數 p，可得 $v^2 \equiv -1 \pmod{p}$，也就是說 $(\frac{-1}{p})=1$，根據 Theorem 5，$p=2$ 或 $p=4k+1$ 其中 k 為整數。相同的，對於所有整除 $c+1$ 的質數 p' 可得 $p'=2$ 或 $p'=4k'+1$ 其中 k' 為整數。若 $c+1$ 為偶數，則 $v^2 \equiv -1 \pmod{4}$，但已知任何平方數模 4 皆會餘 1，因此 $c+1$ 不可能為偶數，也就是說 $c+1$ 為奇數，表示 c 為偶數。

- 若 $c \equiv 0 \pmod{4}$，則 $v^2 \equiv -1 \pmod{4}$，如同上述說明，此情形不成立。
- 若 $c \equiv 2 \pmod{4}$，則 $c+1 \equiv 3 \pmod{4}$，但剛剛證明了任何 $c+1$ 的質因數皆為 $4k+1$ 的形式，其中 k 為整數，也就是說 $c+1 \equiv 1 \pmod{4}$，與 $c+1 \equiv 3 \pmod{4}$ 矛盾，故此情形亦不成立。

綜合上述所說，可知對於所有整數 c，b_3 為一非平方整數，即對於所有整數 c，$\sqrt{b_3} \notin \mathbb{Z}$。

(ii) b_1b_3:
已知

$$b_1b_3=-c(-c(c+1)^2-1)=c^2(c+1)^2+c,$$

若 $c>0$ 可得

$$c^2(c+1)^2 < c^2(c+1)^2+c < (c(c+1)+1)^2 = c^2(c+1)^2+2c(c+1)+1,$$

因為 c 是整數，且連續整數間不存在完全平方數，故可推得此時 b_1b_3 非完全平方數。若 $c<0$，可得當 $c \neq -1$ 時，

$$(c(c+1)-1)^2 = c^2(c+1)^2-2c(c+1)+1 < c^2(c+1)^2+c < c^2(c+1)^2,$$

因為 c 是整數，且連續整數間不存在完全平方數，故可推得 $c \neq -1$ 時 b_1b_3 非完全平方數。綜合上述可知對於所有整數 c，當 $c \neq -1$ 時，$\sqrt{b_1b_3} \notin \mathbb{Z}$。

(iii) b_2b_3:

假設 $\sqrt{b_2b_3}=\sqrt{(c+1)(c(c+1)^2+1)}\in\mathbb{Z}$，因為 $\gcd(c+1,c(c+1)^2+1)=1$，所以可知 $(c+1,c(c+1)^2+1)=(u^2,v^2)$ 或 $(-u^2,-v^2)$ 其中 u、v 為非零正整數。根據一開始的假設，我們不討論 $c=-m^2-1$ 的情形，也就是 $c+1=-m^2$ 的情形，因此這裡只針對 $(c+1,c(c+1)^2+1)=(u^2,v^2)$ 討論，已知 $u=\sqrt{c+1}$, 可推得

$$v^2=c(c+1)^2+1=u^4(u^2-1)+1=u^6-u^4+1=(u^3-\frac{u}{2})^2+1-\frac{u^2}{4}.$$

當 $u\neq 1$或2 時會滿足下列不等式

$$(u^3-\frac{u}{2}-1)^2<(u^3-\frac{u}{2})^2+1-\frac{u^2}{4}<(u^3-\frac{u}{2})^2.$$

若 u 是偶數，則 v^2 會介於兩個連續整數之間，但 v 是一個整數，所以可知 u 必為奇數，則

$$(u^3-\frac{u}{2})^2+1-\frac{u^2}{4}=v^2=(u^3-\frac{u}{2}-\frac{1}{2})^2,$$

上述方程式整理後可得

$$4u^3-u^2-2u+3=(u+1)(4u^2-5u+3)=0,$$

由此可知此方程式無正整數解，與 u 為正整數的假設矛盾，故當 $u\neq 1$或2 即 $c\neq 0$或3 和 $c\neq -m^2-1$ 時，$\sqrt{b_2b_3}\notin\mathbb{Z}$。

(iv) $b_1b_2b_3$:

對於 $N\in\mathbb{Z}$，若 $N=p^kN'$，其中 p 是質數且 $p\nmid N'$，我們將記作 $v_p(N)=k$。已知

$$b_1b_2b_3=-c(-c-1)(-c(c+1)^2-1),$$

若對於整數 n，$|c|\neq n^2$，則存在一個質數 p 使得 $v_p(c)$ 是奇數，因為 b_1、b_2、b_3 是互質的，則 $v_p(b_1b_2b_3)$ 是奇數，故此時 $\sqrt{b_1b_2b_3}\notin\mathbb{Z}$。若 $|c|=n^2$，根據一開始的假設，我們不討論 $c=-n^2$ 的情形，因此只討論 $c=n^2$，因為

$$b_1b_2b_3=-n^2(n^2+1)(n^2(n^2+1)^2+1)<0,$$

負數不可能為平方數，表示此時 $\sqrt{b_1b_2b_3}\notin\mathbb{Z}$，綜合上述所說，在 $c\neq -n^2$ 時 $\sqrt{b_1b_2b_3}\notin\mathbb{Z}$。

□

從 Theorem 7 及 Lemma 10，可知對於整數 n、m，當整數 c 不為 3，$-n^2$ 或 $-m^2-1$ 時，$\mathrm{Gal}(K_3/\mathbb{Q})\cong[C_2]^3$。

2.4 主要定理證明

Theorem. 假設整係數多項式 $f_c(x) := x^2 + c$，其中 c 不爲 0，$f_c^0(x) = x$，對於所有整數 $n \geq 0$，令 $f_c^{n+1}(x) := f_c(f_c^n)(x) = (f_c^n(x))^2 + c$，$K_0 = \mathbb{Q}$，且 K_n 是 f_n 在 $\mathbb{Q}$ 上的分裂體 *(splitting field)*，則：

(1) 若 $c = 3$，則 $\mathrm{Gal}(K_2/\mathbb{Q}) = D_4$ 且 $[K_3 : K_2] = 8$。

(2) 若 $c = -n^2$，其中 n 爲非零整數，則 $\mathrm{Gal}(K_2/\mathbb{Q}) = C_2 \times C_2$ 且 $K_1 = \mathbb{Q}$。

(3) 若 $c = -m^2 - 1$，其中 m 爲非零整數，則 $\mathrm{Gal}(K_2/\mathbb{Q}) = C_4$。

Proof. 以下針對三種情形分別證明:

(1) 若 $c = 3$，從 Lemma 9 可知

$$\mathrm{Gal}(K_2/\mathbb{Q}) \cong [C_2]^2,$$

以下我們證明

$$[C_2]^2 \cong D_4$$

令 $C_2 = \{0, 1\}$，根據圈積的定義 (詳細內容可參考 [6])

$$[C_2]^2 = (C_2 \times C_2) \rtimes C_2$$

因此定義其元素為 $((p, q), r)$，其中 $(p, q) \in C_2 \times C_2$，$r \in C_2$，當 $r = 0$ 表示其作用為位置不變，$r = 1$ 表示其作用為位置交換，換句話說，如果 $r = 0$ 則 r 作用在 (p, q) 上得 (p, q)，如果 $r = 1$ 則 r 作用在 (p, q) 上得 (q, p)。考慮 $[C_2]^2$ 的兩個元素 $a = ((1, 0), 1)$、$b = ((1, 1), 1)$ 由於

$$a^2 = ((1, 0), 1)((1, 0), 1) = ((1, 1), 0)$$

$$a^4 = ((1, 1), 0)((1, 1), 0) = ((0, 0), 0)$$

$$b^2 = ((1, 1), 1)((1, 1), 1) = ((0, 0), 0)$$

且

$$ba = ((1, 1), 1)((1, 0), 1) = ((1, 0), 0)$$

可知

$$(ba)^2 = ((1, 0), 0)((1, 0), 0) = ((0, 0), 0)$$

可推得

$$bab = a^{-1}$$

且 a、b 可生成 8 個元素 $((i,j),k)$，其中 i、j、k 為 0 或 1，因此

$$[C_2]^2 \cong D_4$$

另外從 Lemma 10 得知當 $c = 3$ 時 $\mathrm{Gal}(K_3/\mathbb{Q}) \ncong [C_2]^3$， 表示 $[K_2 : \mathbb{Q}] = 8$ 但 $[K_3 : \mathbb{Q}] \neq 128$，而我們使用電腦計算可得 $[K_3 : \mathbb{Q}] = 64$，也就是說 $[K_3 : K_2] = 8$。

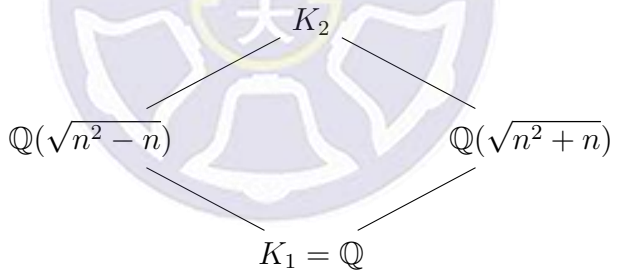
(2) 若 $c = -n^2$，其中 n 為非零整數，已知

$$f_c^2(x) = (x^2 - n^2)^2 - n^2 = (x^2 - n^2 + n)(x^2 - n^2 - n),$$

以下我們要證明 $\mathbb{Q}(\sqrt{n^2 - n}) \neq \mathbb{Q}(\sqrt{n^2 + n})$，假設 $a + b\sqrt{n^2 - n} = \sqrt{n^2 + n}$，其中 a、b 皆為有理數，因為

$$(a + b\sqrt{n^2 - n})^2 = a^2 + 2ab\sqrt{n^2 - n} + b^2(n^2 - n) = (\sqrt{n^2 + n})^2 = n^2 + n,$$

可推得 $2ab\sqrt{n^2 - n} \in \mathbb{Q}$，但 $n^2 - n = n(n-1)$ 不為平方整數，所以 $2ab\sqrt{n^2 - n}$ 不可能為有理數，故可得 $\mathbb{Q}(\sqrt{n^2 - n}) \neq \mathbb{Q}(\sqrt{n^2 + n})$ 。另外已知下圖關係



接著證明 $[K_2 : K_1] = 4$，已知 $K_2 = K_1(\sqrt{n^2 - n}, \sqrt{n^2 + n})$，可得

$$[K_2 : K_1] = [K_2 : \mathbb{Q}(\sqrt{n^2 - n})][\mathbb{Q}(\sqrt{n^2 - n}) : K_1],$$

已知 $[\mathbb{Q}(\sqrt{n^2 - n}) : K_1] = 2$ 且因為 $\sqrt{n^2 + n}$ 在 $\mathbb{Q}(\sqrt{n^2 - n})$ 上的最小多項式次數會小於多項式 $x^2 - (n^2 + n)$ 的次數，表示 $[K_2 : \mathbb{Q}(\sqrt{n^2 - n})] \leq 2$，假設 $[K_2 : \mathbb{Q}(\sqrt{n^2 - n})] = 1$，表示 $\sqrt{n^2 + n} \in K_2 = \mathbb{Q}(\sqrt{n^2 - n})$，令 $\sqrt{n^2 + n} = a + b\sqrt{n^2 - n}$，其中 a、b 皆為有理數，可知

$$(\sqrt{n^2 + n} - b\sqrt{n^2 - n})^2 = (n^2 + n) - 2b\sqrt{n^4 - n^2} + b^2(n^2 - n) = a^2,$$

因為 n^2+n、$b^2(n^2-n)$、a^2 皆為有理數, 表示 $2b\sqrt{n^4-n^2}$ 亦為有理數, 但 n^2、n^2-1 為連續整數，可知 n^4-n^2 不為平方整數，則 $\sqrt{n^4-n^2}$ 不為有理數，與 $2b\sqrt{n^4-n^2}$ 為有理數矛盾，因此 $[K_2:\mathbb{Q}(\sqrt{n^2-n})]=2$，故 $[K_2:K_1]=4$，而階 (order) 為 4 的伽羅瓦群可能為 C_4 或 $C_2\times C_2$，但我們知道只有四個自同構，$\sqrt{n^2+n}$ 送到自己或是送到 $-\sqrt{n^2+n}$ 配上 $\sqrt{n^2-n}$ 送到自己或是送到 $-\sqrt{n^2-n}$，然後每一個自同構都是階為 2 的，所以顯然不會是 C_4，故 $\mathrm{Gal}(K_2/\mathbb{Q})=C_2\times C_2$ 且 $K_1=\mathbb{Q}$ 。

(3) 當 $c=-m^2-1$ 時，$c_1=m^2+1$，$c_2=m^2(m^2+1)$，因為任一平方整數加一必為非平方整數，連續非零整數相乘亦為非平方整數，因此 $c_1=m^2+1$，$c_2=m^2(m^2+1)$ 皆為非平方整數。接著從 Theorem 6 可知 $f^2(x)=x^4+2x^2c^2+c^2+c$ 為不可約的有理多項式，從 Theorem 3 得到 $f^2(x)$ 的預解三次式

$$\begin{aligned} g(x) &= (x-\alpha)(x-\beta)(x-\gamma) \\ &= x^3-2cx^2-4(c^2+c)x+8c(c^2+c) \\ &= (x-2c)[x^2-4(c^2+c)] \end{aligned}$$

由於 c 和 $c+1$ 連續非零整數，可知 $4(c^2+c)$ 是非平方整數，因此 $x^2-4(c^2+c)$ 是不可約的有理多項式，則有以下關係

$$\begin{array}{c} \mathbb{Q}(\alpha,\beta,\gamma) \\ \Big| \\ 2 \\ \Big| \\ \mathbb{Q} \end{array}$$

根據 Theorem 4 的圖表可知 $\mathrm{Gal}(K_2/\mathbb{Q})$ 可能為 C_4 或 D_4，但 $\mathrm{Gal}(K_2/\mathbb{Q})\ncong[C_2]^2=D_4$，故可得 $\mathrm{Gal}(K_2/\mathbb{Q})=C_4$。

□

參考文獻

[1] K. Doerksen and A. Haensch, Primitive prime divisors in zero orbits of polynomials. Integers 12 (2012), no. 3, 465—472.

[2] M. Stoll, Galois groups over $\mathbb{Q}$ of some iterated polynomials, Arch. Math. (Basel) 59 (1992) 239-244.

[3] R. W. K. Odoni, Realising wreath products of cyclic groups as Galois groups. Mathematika, 35(1):101-113, 1988.

[4] J. S. Milne, Fields and Galois Theory, Available at www.jmilne.org/math/, 2018, ch4.

[5] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Grad. Texts in Math. 84, Springer, New York, 1990.

[6] J. J. Rotman, An Introduction to the Theory of Groups, forth edition, GTM 148, Springer-Verlag, New York, 1995, ch7.

[7] D. M. Burton, Elementary Number Theory, seventh ed., W. C. Brown Publishers, Dubuque, IA, 2011, ch9.

[8] H.-C. Li, Tree Automorphisms and Wreath Product, private note.

[9] H.-C. Li, Arboreal Galois representation for a certain type of quadratic polynomials, Arch. Math. (Basel) 114 (2020), no. 3, 265—269.