

List of Theorem

Joey Yu Hsu, MD

June 10, 2024

since 2024/06/07

Contents

0.1	LyX Chinese environment	11
0.2	LyZ: linking Zotero and LyX	11
0.3	list of theorem module	11
0.4	coloring	11
0.4.1	single coloring	11
0.4.2	recolor = coloring with regular expression (= RegEx = re)	12
0.5	TikZ	14
0.5.1	TikZ-CD = tikz-cd: commutative diagram	14
1	group theory	17
2	Galois theory	19
3	probability theory	29

list of definition

定義 1.0.1 (group)	17
定義 1.0.2 (homomorphism)	18
定義 2.0.1 (reducible polynomial vs. irreducible polynomial)	19
定義 2.0.2 (Galois group)	22
定義 3.0.1 (exponential family)	29

list of theorem

定理 1.0.1	17
定理 1.0.2	17
定理 1.0.3 (rearrangement theorem)	17
定理 1.0.4 ($C_3 = \mathbb{Z}_3 \trianglelefteq S_3 = D_3$)	17
定理 1.0.5 (kernel of homomorphism)	18
定理 2.0.1 (Abel-Ruffini theorem)	19
引理 2.0.1 (irreducible polynomial factor lemma)	20
引理 2.0.2 (variable represented by roots)	20
引理 2.0.3 (roots represented by variable)	20
引理 2.0.4 (root rearrangement by variable conjugate)	21
定理 3.0.1 (Bonferroni inequality)	29

list of example

範例 2.0.1 (Galois group of $x^2 + 1 = 0$)	21
範例 2.0.2 (Galois group of $ax^2 + bx + c = 0, a \neq 0$)	24
範例 2.0.3 (Galois group of $x^3 - 2x = 0$)	26
範例 2.0.4 (Galois group of $x^4 - 4x^3 - 4x^2 + 8x - 2 = 0$)	26

List of Figures

1	learn TikZ-CD = tikz-cd in one picture 2	16
---	--	----

0.1 LyX Chinese environment

<https://latexlyx.blogspot.com/2012/06/lyx.html>

2014年09月21日 晚上10:58

匿名：Language 那邊改成 Chinese Traditional 之後，Definition 就變成定義，Example 就變成範例，有沒有辦法維持他們是英文的？

2014年09月22日 上午11:23

Mingyi Wu：這個是 LyX 的特性之一。UI 的語言設定，與編輯區的語言是分開的。就算 UI 設定為 English，如果檔案語言設定為 Chinese，那麼編輯區出現的一些如 Chapter, Section, Definition 等名稱，會自動變成中文。也就是說檔案的語言設定值，會影響 LyX 文字編輯區內呈現的語言。若使用數學模組或一些數學論文 document class 的時候，甚至連輸出的檔案內容都會根據語言設定而變。(也就是 Definition 變成 定義)

所以您說的狀況，可能有2種情況：

1. Definition 在 LyX 編輯區內變成中文，但輸出檔案時檔案還是出現 Definition 這個只是編輯區呈現的問題，沒辦法只改一部份。如果真的希望檔案設定成中文，但所有介面看起來都要是英文的環境，您可以直接刪掉中文翻譯檔，這樣所有介面都會變成英文的。以我的環境，繁體中文的翻譯檔路徑在(for Windows): C:\Program Files (x86)\LyX 2.1\Resources\locale\zh-TW\LC_MESSAGES\LyX2.1.mo 把這個檔名改掉，這樣 LyX 就找不到中文翻譯檔，都會以預設的英文呈現。

2. 如果您的問題是輸出的檔案會出現中文的「定義」問題，不管介面顯示。這個問題跟另外一個檔案有關，C:\Program Files (x86)\LyX 2.1\Resources\layouttranslations 您可以用任何文字編輯器開啟此檔，找到 Translation zh-TW 這行以下的設定改成您喜歡的，或是直接把這個檔名改掉或刪掉檔案，這樣輸出檔案也不會自動翻譯了。

<https://latexlyx.blogspot.com/2013/06/lyx-2.html>

0.2 LyZ: linking Zotero and LyX

<https://forums.zotero.org/discussion/78442/connecting-zotero-and-lyx>

<https://github.com/wshanks/lyz/releases>

0.3 list of theorem module

<https://tex.stackexchange.com/questions/672794/list-of-theorems-not-working-in-lyx>

<https://github.com/Udi-Fogiel/LyX-thmtools>

0.4 coloring

<https://stackoverflow.com/questions/2116944/insert-programming-code-in-a-lyx-document>

<https://tex.stackexchange.com/questions/53260/lyx-is-ignoring-typewriter-font-setting-for-program-listings>

<https://tex.stackexchange.com/questions/534581/tex-compilation-after-regex-replace>

0.4.1 single coloring

```
\def\zl{ {\color{blue} z_{\scriptscriptstyle l}} }
```

also can be put into “preamble”

$$0 = \frac{\partial}{\partial z_l} (\|h(z_{l-1}) \cdot w_l - z_l\| + \lambda \|h(z_l) \cdot w_{l+1} - z_{l+1}\|)$$

0.4.2 recolor = coloring with regular expression (= RegEx = re)

<https://tex.stackexchange.com/questions/83101/option-clash-for-package-xcolor>

Now, the problem was that another package (pgfplots, in this case) had already loaded the xcolor package without options, so loading it after pgfplots with the table option produces the clash. One way to prevent the problem was already presented (using table as class option); another solution is to load xcolor with the table option before pgfplots

```
\usepackage{expl3,xparse}
\usepackage[dvipsnames]{xcolor}
```

```
\ExplSyntaxOn
\NewDocumentCommand{\recolor}{m}
{
  \tl_set:Nn \l_tmpa_tl { #1 }
  \regex_replace_all:nnN { 2 } { \c{color}{red}{2} } \l_tmpa_tl
  \tl_use:N \l_tmpa_tl
}
\ExplSyntaxOff
```

$$c^2 = a^2 + b^2$$

```
\ExplSyntaxOn
\RenewDocumentCommand{\recolor}{m}
{
  \tl_set:Nn \l_tmpa_tl { #1 }

  % e, \rho^2
  \regex_replace_all:nnN { \be\b } { {\c{color}{red}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { \c{rho}\^{\2\} } { {\c{color}{Green}{\0}} }
} \l_tmpa_tl

  % rho
  %% \rho_\d
  \regex_replace_all:nnN { \c{rho}_{\c{scriptscriptstyle} 0}} {
{ {\c{color}{red}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { \c{rho}_{\c{scriptscriptstyle} 1}} {
{ {\c{color}{blue}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { \c{rho}_{\c{scriptscriptstyle} 2}} {
{ {\c{color}{Green}{\0}} }
} \l_tmpa_tl

  %% \d_\rho
  \regex_replace_all:nnN { 0_{\c{scriptscriptstyle} \c{rho}}} {
{ {\c{color}{red}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { 1_{\c{scriptscriptstyle} \c{rho}}} {
{ {\c{color}{blue}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { 2_{\c{scriptscriptstyle} \c{rho}}} {
{ {\c{color}{Green}{\0}} }
} \l_tmpa_tl

  % pi
  %% \pi_\d
  \regex_replace_all:nnN { \c{pi}_{\c{scriptscriptstyle} 0}} {
{ {\c{color}{magenta}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { \c{pi}_{\c{scriptscriptstyle} 1}} {
{ {\c{color}{cyan}{\0}} }
} \l_tmpa_tl
  \regex_replace_all:nnN { \c{pi}_{\c{scriptscriptstyle} 2}} {
```

```

{ {\c{color}{orange}}{\0}}
} \l_tmpa_tl

%% \d_\pi
\regex_replace_all:nnN { 0_{{\c{scriptscriptstyle} \c{pi}}}} }
{ {\c{color}{magenta}}{\0}}
} \l_tmpa_tl
\regex_replace_all:nnN { 1_{{\c{scriptscriptstyle} \c{pi}}}} }
{ {\c{color}{cyan}}{\0}}
} \l_tmpa_tl
\regex_replace_all:nnN { 2_{{\c{scriptscriptstyle} \c{pi}}}} }
{ {\c{color}{orange}}{\0}}
} \l_tmpa_tl

% \d{3}
%% \[\d{3}\]
\regex_replace_all:nnN { \c{left}\[(123)\c{right}\] }
{ \c{left}\[{\c{color}{red}}{\1}}\c{right}\]
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\[(231)\c{right}\] }
{ \c{left}\[{\c{color}{blue}}{\1}}\c{right}\]
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\[(312)\c{right}\] }
{ \c{left}\[{\c{color}{Green}}{\1}}\c{right}\]
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\[(213)\c{right}\] }
{ \c{left}\[{\c{color}{magenta}}{\1}}\c{right}\]
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\[(132)\c{right}\] }
{ \c{left}\[{\c{color}{cyan}}{\1}}\c{right}\]
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\[(321)\c{right}\] }
{ \c{left}\[{\c{color}{orange}}{\1}}\c{right}\]
} \l_tmpa_tl

%% \(\d{3}\)
\regex_replace_all:nnN { \c{left}\(\c{right}\) }
{ {\c{color}{red}}{\0}}
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\((123)\c{right}\) }
{ \c{left}\( {\c{color}{blue}}{\1} \c{right}\) }
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\((132)\c{right}\) }
{ \c{left}\( {\c{color}{Green}}{\1} \c{right}\) }
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\((12)\c{right}\) }
{ \c{left}\( {\c{color}{magenta}}{\1} \c{right}\) }
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\((23)\c{right}\) }
{ \c{left}\( {\c{color}{cyan}}{\1} \c{right}\) }
} \l_tmpa_tl
\regex_replace_all:nnN { \c{left}\((31)\c{right}\) }
{ \c{left}\( {\c{color}{orange}}{\1} \c{right}\) }
} \l_tmpa_tl

\tl_use:N \l_tmpa_tl
}
\ExplSyntaxOff

```

\cdot_{D_3}	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2	\cdot_{S_3}	[123]	[231]	[312]	[213]	[132]	[321]
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2	[123]	[123]	[231]	[312]	[213]	[132]	[321]
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0	[231]	[231]	[312]	[123]	[132]	[321]	[213]
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1	[312]	[312]	[123]	[231]	[321]	[213]	[132]
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1	[213]	[213]	[321]	[132]	[123]	[312]	[231]
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2	[132]	[132]	[213]	[321]	[231]	[123]	[312]
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0	[321]	[321]	[132]	[213]	[312]	[231]	[123]
\cdot_{S_3}	e	(123)	(132)	(3)(12)	(1)(23)	(2)(31)	\cdot_{S_3}	()	(123)	(132)	(12)	(23)	(31)
e	e	(123)	(132)	(3)(12)	(1)(23)	(2)(31)	()	()	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	e	(1)(23)	(2)(31)	(3)(12)	(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	e	(123)	(2)(31)	(3)(12)	(1)(23)	(132)	(132)	()	(123)	(31)	(12)	(23)
(3)(12)	(3)(12)	(2)(31)	(1)(23)	e	(132)	(123)	(12)	(12)	(31)	(23)	()	(132)	(123)
(1)(23)	(1)(23)	(3)(12)	(2)(31)	(123)	e	(132)	(23)	(23)	(12)	(31)	(123)	()	(132)
(2)(31)	(2)(31)	(1)(23)	(3)(12)	(132)	(123)	e	(31)	(31)	(23)	(12)	(132)	(123)	()

0.5 TikZ

0.5.1 TikZ-CD = tikz-cd: commutative diagram

```

\usepackage{tikz}
\usepackage{pgfplots}

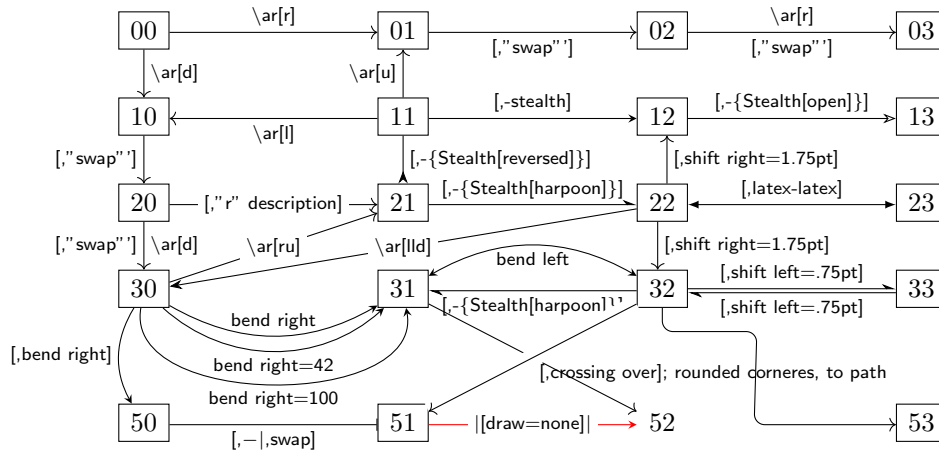
\usetikzlibrary{cd,arrows.meta}
\begin{tikzcd}[column sep=2.75cm, %small,large,huge
               cells={nodes={draw}}
]
00
\ar[r,"\backslash \text{ar[r]}"]
\ar[d,"\backslash \text{ar[d]}"]
&
01
\ar[r,"\text{[,\"swap\"'}]"]
&
02
\ar[r,"\backslash \text{ar[r]}","\text{[,\"swap\"'}]"]
&
03
\\
10
\ar[d,"\text{[,\"swap\"'}]"]
&
11
\ar[u,"\backslash \text{ar[u]}"]
\ar[l,"\backslash \text{ar[l]}"]
\ar[r,-stealth,"\text{[,-\text{stealth}\text{[]}]"}]
\ar[d,-\{Stealth[reversed]\},"\text{[,-\{\text{Stealth[reversed]\}\}\text{[]}]"}]
&
12
\ar[r,-\{Stealth[open]\},"\text{[,-\{\text{Stealth[open]\}\}\text{[]}]"}]
&
13
\\
20
\ar[r,"\text{[,\"r\" description}]" description]
\ar[d,"\backslash \text{ar[d]}","\text{[,\"swap\"'}]"]
&
21
\ar[r,-\{Stealth[harpoon]\},"\text{[,-\{\text{Stealth[harpoon]\}\}\text{[]}]"}]
&
22
\ar[u,shift right=1.75pt,"\text{[,shift right=1.75pt]}"]

```

```

\ar[lld,-Stealth,"\backslash \text{ar[lld]}" description]
\ar[r,latex-latex,"\text{[,latex-latex]}"]
\ar[d,shift right=1.75pt,"\text{[,shift right=1.75pt]}"]
&
23
\\
30
\ar[ru,"\backslash \text{ar[ru]}" description]
\ar[r,bend right,-stealth,"\text{bend right}"]
\ar[r,bend right=42,-stealth,"\text{bend right=42}"']
\ar[r,bend right=100,-stealth,"\text{bend right=100}"']
\ar[dd,bend right,-stealth,"\text{[,bend right]}"']
&
31
\ar[r,bend left,stealth-stealth,"\text{bend left}"']
\ar[ddr]
&
32
\ar[l,-{Stealth[harpoon]},"\text{[,}-|\text{Stealth[harpoon]}}\text{]}"]
\ar[r,-{Stealth[harpoon]},shift left=.75pt,"\text{[,shift left=.75pt]}"]
\ar[ddl,crossing over,"\text{[,crossing over]; rounded corners, to path}"]
\ar[ddr,
    rounded corners,
    to path={--([yshift=-2ex]\tikztostart.south)
        --([yshift=-2ex,xshift=+2ex]\tikztostart.south)
        --([yshift=-2ex,xshift=+8ex]\tikztostart.south)
        --([xshift=-12ex]\tikztotarget.west)
        --(\tikztotarget)
    },
]
&
33
\ar[l,-{Stealth[harpoon]},shift left=.75pt,"\text{[,shift left=.75pt]}"]
\\
&
&
&
\\
50
\ar[r,-|,"\text{[,}-|\text{[,swap]}",swap]
&
51
\ar[r,-stealth,red,text=black,"\text{[draw=none]}|" description]
&
|[draw=none]|52
&
53
\end{tikzcd}

```



Chapter 1

group theory

定義 1.0.1 (group). 群

$$G \text{ is a group} \\ \Updownarrow \text{def.} \\ G = (G, \cdot) = (G, \cdot_G) = \left\{ g \left| \begin{array}{ll} g_1 \cdot g_2 = g_1 g_2 \in G & \forall g_1, g_2 \in G \quad (c) \cdot_G \text{ closure} \\ g_1 (g_2 g_3) = (g_1 g_2) g_3 = g_1 g_2 g_3 & \forall g_1, g_2, g_3 \in G \quad (a) \cdot_G \text{ associativity} \\ e \cdot g = eg = g = ge = g \cdot e & \exists e = e_G \in G, \forall g \in G \quad (id) \text{ identity element} \\ \bar{g} \cdot g = \bar{g}g = e = g\bar{g} = g \cdot \bar{g} & \forall g \in G, \exists \bar{g} \in G \quad (in) \text{ inverse element} \end{array} \right. \right\}$$

定理 1.0.1.

$$\begin{array}{l} \forall g \in G \\ g \neq e \in G \end{array} \Rightarrow \forall \tilde{g} \in G [g\tilde{g} \neq \tilde{g}]$$

定理 1.0.2.

$$\begin{array}{l} \forall g_1, g_2 \in G \\ g_1 \neq g_2 \end{array} \Rightarrow \forall g \in G [g_1 g \neq g_2 g]$$

定理 1.0.3 (rearrangement theorem).

$$\forall g \in G [\{g\tilde{g} | \tilde{g} \in G\} = G]$$

Proof. proof idea: $f = g(\bar{g}f) = gg^{-1}f = ef = f$

$$\begin{array}{l} \forall g \in G, \exists \bar{g} \in G \left[\bar{g}g = e = g\bar{g} \right] \\ \Downarrow \\ \forall f \in G \left[f = ef \stackrel{e=\bar{g}\bar{g}}{=} (g\bar{g})f \stackrel{(a)}{=} g(\bar{g}f) \right] \Rightarrow \forall f \in G [f = g(\bar{g}f)] \stackrel{(c)\bar{g}f \in G}{\Rightarrow} f \in \{g\tilde{g} | \tilde{g} \in G\} \\ \Downarrow \\ \forall f \in G [f \in \{g\tilde{g} | \tilde{g} \in G\}] \\ \Downarrow \\ G \subseteq \{g\tilde{g} | \tilde{g} \in G\} \\ \{g\tilde{g} | \forall \tilde{g} \in G\} \subseteq G \because (c) \cdot_G \text{ closure} \\ \Downarrow \\ G = \{g\tilde{g} | \tilde{g} \in G\} \end{array}$$

□

定理 1.0.4 ($C_3 = \mathbb{Z}_3 \leq S_3 = D_3$).

$$\begin{array}{l} \rho_{k+3} = \rho_k \\ \pi_{k+3} = \pi_k \\ \rho_i \rho_j = \rho_{i+j} \\ \rho_i \pi_j = \pi_{i+j} \\ \pi_i \rho_j = \pi_{i-j} \\ \pi_i \pi_j = \rho_{i-j} \end{array}$$

$$\begin{aligned}
 C_3 = \mathbb{Z}_3 &= \{0, 1, 2\} \\
 &= \{0_\rho, 1_\rho, 2_\rho\} = \{[123], [231], [312]\} = \{(), (123), (132)\} && \leq S_3 \\
 &= \left\{e^{i\frac{2\pi}{3}0}, e^{i\frac{2\pi}{3}1}, e^{i\frac{2\pi}{3}2}, \dots, e^{i\frac{2\pi}{3}(n-1)}\right\} \stackrel{n=3}{=} \left\{e^{i\frac{2\pi}{3}0}, e^{i\frac{2\pi}{3}1}, e^{i\frac{2\pi}{3}2}\right\} \\
 &= \{e, g, g^2, \dots, g^{n-1}\} = \{g^0, g^1, g^2\} = \{e, g, g^2\}, g^n = e \\
 &= \{e, \rho, \rho^2\} = \{\rho_0, \rho_1, \rho_2\} = \{\rho_j | j \in \{0, 1, 2\}\} && \leq D_3 = \{\rho_k, \pi_k\} = \{\rho_{k,3}, \pi_{k,3}\} \\
 \rho_i \mathbb{Z}_3 &= \{\rho_i \rho_j | j \in \{0, 1, 2\}\} \\
 &= \{\rho_{i+j} | j \in \{0, 1, 2\}\} \stackrel{i+j \equiv j+i}{=} \{\rho_{j+i} | j \in \{0, 1, 2\}\} \\
 &= \{\rho_j \rho_i | j \in \{0, 1, 2\}\} = \mathbb{Z}_3 \rho_i && \Rightarrow \rho_i \mathbb{Z}_3 = \mathbb{Z}_3 \rho_i \\
 \pi_i \mathbb{Z}_3 &= \{\pi_i \rho_j | j \in \{0, 1, 2\}\} \\
 &= \{\pi_{i-j} | j \in \{0, 1, 2\}\} \stackrel{\pi_{k+3} = \pi_k}{=} \{\pi_{3+i-j} | j \in \{0, 1, 2\}\} \\
 &= \{\pi_{i+(3-j)} | 3-j \in \{3, 2, 1\}\} = \{\pi_{(3-j)+i} | 3-j \in \{3, 2, 1\}\} && i + (3-j) = (3-j) + i \\
 &= \{\rho_{3-j} \pi_i | 3-j \in \{3, 2, 1\}\} = \{\rho_{3-j} | 3-j \in \{3, 2, 1\}\} \pi_i && \rho_i \pi_j = \pi_{i+j} \\
 &= \{\rho_j | j \in \{0, 1, 2\}\} \pi_i = \mathbb{Z}_3 \pi_i && \Rightarrow \pi_i \mathbb{Z}_3 = \mathbb{Z}_3 \pi_i \\
 &\Downarrow \\
 \rho_i \mathbb{Z}_3 &= \mathbb{Z}_3 \rho_i \\
 \pi_i \mathbb{Z}_3 &= \mathbb{Z}_3 \pi_i && \Rightarrow g \mathbb{Z}_3 = \mathbb{Z}_3 g \quad \forall g \in D_3 \\
 &\Downarrow \\
 \mathbb{Z}_3 &\leq D_3 = S_3 \\
 g \mathbb{Z}_3 &= \mathbb{Z}_3 g \quad \forall g \in D_3 && \Rightarrow \mathbb{Z}_3 \trianglelefteq D_3 = S_3 \\
 &&& \Updownarrow \\
 &&& \mathbb{Z}_3 \trianglelefteq S_3 = D_3
 \end{aligned}$$

定義 1.0.2 (homomorphism).

定理 1.0.5 (kernel of homomorphism).

Chapter 2

Galois theory

$$x - \alpha = (x - \alpha) = 0 \Rightarrow x = \alpha \Leftrightarrow x \in \{\alpha\}$$

$$x^2 - (\alpha + \beta)x + \alpha\beta = (x - \alpha)(x - \beta) = 0 \Rightarrow x = \alpha, \beta \Leftrightarrow x \in \{\alpha, \beta\}$$

$$x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)x - \alpha\beta\gamma = (x - \alpha)(x - \beta)(x - \gamma) = 0 \Rightarrow x = \alpha, \beta, \gamma \Leftrightarrow x \in \{\alpha, \beta, \gamma\}$$

$$\begin{aligned} 0 &= (x - \alpha) & x &= \alpha \Leftrightarrow x \in \{\alpha\} \\ &= x - \alpha \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha)(x - \beta) & x &= \alpha, \beta \Leftrightarrow x \in \{\alpha, \beta\} \\ &= x^2 - (\alpha + \beta)x + \alpha\beta \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha)(x - \beta)(x - \gamma) & x &= \alpha, \beta, \gamma \Leftrightarrow x \in \{\alpha, \beta, \gamma\} \\ &= x^3 - (\alpha + \beta + \gamma)x^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)x - \alpha\beta\gamma \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha)(x - \beta)(x - \gamma)(x - \delta) & x &= \alpha, \beta, \gamma, \delta \Leftrightarrow x \in \{\alpha, \beta, \gamma, \delta\} \\ &= x^4 - (\alpha + \beta + \gamma + \delta)x^3 + \cdots + \alpha\beta\gamma\delta \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha)(x - \beta)(x - \gamma)(x - \delta)(x - \varepsilon) & x &= \alpha, \beta, \gamma, \delta, \varepsilon \Leftrightarrow x \in \{\alpha, \beta, \gamma, \delta, \varepsilon\} \\ &= x^5 - (\alpha + \beta + \gamma + \delta + \varepsilon)x^4 + \cdots - \alpha\beta\gamma\delta\varepsilon \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha_1) & x &= \alpha_1 \Leftrightarrow x \in \{\alpha_1\} \\ &= x - \alpha_1 \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha_1)(x - \alpha_2) & x &= \alpha_1, \alpha_2 \Leftrightarrow x \in \{\alpha_1, \alpha_2\} \\ &= x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) & x &= \alpha_1, \alpha_2, \alpha_3 \Leftrightarrow x \in \{\alpha_1, \alpha_2, \alpha_3\} \\ &= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)x - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) & x &= \alpha_1, \alpha_2, \alpha_3, \alpha_4 \Leftrightarrow x \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \\ &= x^4 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)x^3 + \cdots + \alpha_1\alpha_2\alpha_3\alpha_4 \end{aligned}$$

$$\begin{aligned} 0 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)(x - \alpha_5) & x &= \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \Leftrightarrow x \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\} \\ &= x^5 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5)x^4 + \cdots - \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5 \end{aligned}$$

定理 2.0.1 (Abel-Ruffini theorem). *There is no general formula for solving a polynomial of degree 5 or higher.*

定義 2.0.1 (reducible polynomial vs. irreducible polynomial). [1, p.357]

körper $\mathbb{K} = \mathbb{F}$ field

$$f(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0 \Leftrightarrow f(x) \in \mathbb{K}[x]$$

$$p_n \neq 0 \Rightarrow \deg f(x) = n \in \mathbb{N}$$

$$= p_j x^j = \sum_{j=1}^n p_j x^j \quad j \in \mathbb{Z}_{[0, n]}$$

$$p_j \in \mathbb{K} = \mathbb{F}$$

$$= p_n (x - x_1)(x - x_2) \cdots (x - x_n) \quad \{x_1, x_2, \dots, x_n\} \subseteq \mathbb{K}(x_1, x_2, \dots, x_n)$$

$$= p_n (x - x_1) \cdots (x - x_n) \quad \{x_1, \dots, x_n\} \subseteq \mathbb{K}(x_1, \dots, x_n)$$

$$\Updownarrow$$

$$f(x) \text{ is reducible over } \mathbb{K}(x_1, \dots, x_n)$$

引理 2.0.1 (irreducible polynomial factor lemma). [1, p.362]
 factor theorem https://en.wikipedia.org/wiki/Factor_theorem

$$\begin{array}{ll}
 f(x) \in \mathbb{K}[x] & \mathbb{K} \text{ is a field} \\
 p(x) \text{ is irreducible over } \mathbb{K} & \\
 f(x_0) = 0 = p(x_0) & \exists x_0 \in \mathbb{K} \\
 \Downarrow & \\
 p(x) \mid f(x) & \Leftrightarrow p(x) \text{ is a factor of } f(x)
 \end{array}$$

備註 2.0.1 (polynomial cf. integer). [1, p.363]

$$\begin{array}{ll}
 \text{polynomial} & \Leftrightarrow \text{integer} \\
 P[x] \in \mathbb{K}[x] & \Leftrightarrow \text{natural number } \mathbb{N} \subset \mathbb{Z} \\
 \text{irreducible polynomial} & \Leftrightarrow \text{prime [number]} \mathbb{P} \\
 \text{reducible polynomial} & \Leftrightarrow \text{composite number} \\
 f(x_0) = 0 = p(x_0) \quad \exists x_0 \in \mathbb{K} & \Leftrightarrow \gcd(m, n) = m = p_1^{k_1} \cdots p_\ell^{k_\ell} \quad p_i \in \mathbb{P} \\
 \Downarrow & \Leftrightarrow \Downarrow \quad k_i \in \mathbb{N} \\
 p(x) \mid f(x) & \Leftrightarrow m \mid n
 \end{array}$$

引理 2.0.2 (variable represented by roots). [1, p.366]

$$\begin{array}{ll}
 f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) & \in \mathbb{K}(\alpha_1, \dots, \alpha_m)[x] \\
 & (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3) \cdots (\alpha_{m-1} - \alpha_m)(\alpha_m - \alpha_1) \neq 0 \\
 \Downarrow \text{variable represented by roots} & \\
 \varphi(\mathbf{x}) = \varphi(x_1, \dots, x_m) & \varphi(\mathbf{x}) = \frac{P(\mathbf{x})}{Q(\mathbf{x})}, \quad P(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 & \quad 0 \neq Q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 V = \varphi(\alpha) = \varphi(\alpha_1, \dots, \alpha_m) & \forall \sigma_1, \sigma_2 \in S_m [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)] \\
 V_i = \varphi(\sigma_i \alpha) = \varphi(\sigma_i \alpha_1, \dots, \sigma_i \alpha_m) & \\
 \Updownarrow & \\
 \exists \varphi(\mathbf{x}) = \varphi(x_1, \dots, x_m) = \frac{P(\mathbf{x})}{Q(\mathbf{x})}, \quad P(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] & \quad 0 \neq Q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 & \left[V = \varphi(\alpha) = \varphi(\alpha_1, \dots, \alpha_m) \right. \\
 & \quad \left. \forall \sigma_1, \sigma_2 \in S_m [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)] \right]
 \end{array}$$

引理 2.0.3 (roots represented by variable). [1, p.368]

$$\begin{array}{ll}
 f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) & \in \mathbb{K}(\alpha_1, \dots, \alpha_m)[x] \\
 & (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3) \cdots (\alpha_{m-1} - \alpha_m)(\alpha_m - \alpha_1) \neq 0 \\
 \Downarrow \text{lemma 2.0.2} & \\
 \varphi(\mathbf{x}) = \varphi(x_1, \dots, x_m) & \varphi(\mathbf{x}) = \frac{P(\mathbf{x})}{Q(\mathbf{x})}, \quad P(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 & \quad 0 \neq Q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 V = \varphi(\alpha) = \varphi(\alpha_1, \dots, \alpha_m) & \forall \sigma_1, \sigma_2 \in S_m [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)] \\
 V_i = \varphi(\sigma_i \alpha) = \varphi(\sigma_i \alpha_1, \dots, \sigma_i \alpha_m) & \\
 \Updownarrow & \\
 \exists \varphi(\mathbf{x}) = \varphi(x_1, \dots, x_m) = \frac{P(\mathbf{x})}{Q(\mathbf{x})}, \quad P(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] & \quad 0 \neq Q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 \Downarrow \text{roots represented by variable} & \\
 \alpha_1 = \alpha_1(V) = \varphi_1(V) & i \in \mathbb{N}_{\leq m} \\
 \vdots & \\
 \alpha_m = \alpha_m(V) = \varphi_m(V) & \\
 \Updownarrow & \\
 \exists \varphi_i(\mathbf{x}) = \varphi_i(x_1, \dots, x_m) = \frac{P_i(\mathbf{x})}{Q_i(\mathbf{x})} & \quad P_i(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 & \quad 0 \neq Q_i(\mathbf{x}) \in \mathbb{K}[\mathbf{x}] \\
 & \left[\begin{array}{l} \alpha_1 = \alpha_1(V) = \varphi_1(V) \\ \vdots \\ \alpha_m = \alpha_m(V) = \varphi_m(V) \end{array} \right]
 \end{array}$$

引理 2.0.4 (root rearrangement by variable conjugate). [1, p.370]

$$\begin{aligned}
 f(x) &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) && \in \mathbb{K}(\alpha_1, \dots, \alpha_m)[x] \\
 &&& (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3) \cdots (\alpha_{m-1} - \alpha_m)(\alpha_m - \alpha_1) \neq 0 \\
 &\Downarrow \text{lemma 2.0.2} \\
 \varphi(x) &= \varphi(x_1, \dots, x_m) && \varphi(x) = \frac{P(x)}{Q(x)}, \quad P(x) \in \mathbb{K}[x] \\
 &&& 0 \neq Q(x) \in \mathbb{K}[x] \\
 V &= \varphi(\alpha) = \varphi(\alpha_1, \dots, \alpha_m) && \forall \sigma_1, \sigma_2 \in S_m [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)] \\
 V_i &= \varphi(\sigma_i \alpha) = \varphi(\sigma_i \alpha_1, \dots, \sigma_i \alpha_m) \\
 &\wedge \\
 f_V(x) &= (x - V_1) \cdots (x - V_n) && \text{is a minimal polynomial} \in \mathbb{K}[x] \\
 &&& n = \deg f_V(x) \\
 &\Downarrow \text{lemma 2.0.3} \\
 \alpha_1 &= \alpha_1(V) = \varphi_1(V) && i \in \mathbb{N}_{\leq m} \\
 &\vdots && \varphi_i(x) = \frac{P_i(x)}{Q_i(x)}, \quad P_i(x) \in \mathbb{K}[x] \\
 &&& 0 \neq Q_i(x) \in \mathbb{K}[x] \\
 \alpha_m &= \alpha_m(V) = \varphi_m(V) \\
 &\Downarrow \text{root rearrangement by variable conjugate} \\
 \{\alpha_1, \dots, \alpha_m\} &\in \{\varphi_1(V_1), \dots, \varphi_m(V_1)\} && = \{\varphi_1(V), \dots, \varphi_m(V)\}, \quad V = V_1 \\
 &\vdots && \\
 \{\alpha_1, \dots, \alpha_m\} &\in \{\varphi_1(V_n), \dots, \varphi_m(V_n)\} && = \{\varphi_1(V), \dots, \varphi_m(V)\}, \quad V = V_n
 \end{aligned}$$

範例 2.0.1 (Galois group of $x^2 + 1 = 0$). [1, p.367~372]

$$\begin{aligned}
 f(x) &= x^2 + 1 && \in \mathbb{Q}[x] \\
 &= (x + i)(x - i) && \in \mathbb{Q}(i)[x] \subset \mathbb{C}[x] \\
 &= (x - i)(x + i) \\
 &= (x - i)(x - (-i)) \\
 &= (x - \alpha)(x - \beta) && \{\alpha, \beta\} = \{+i, -i\} \\
 &= (x - \alpha_1)(x - \alpha_2) && \{\alpha_1, \alpha_2\} = \{i, -i\} \\
 (\alpha_1, \alpha_2) &= (i, -i) \Rightarrow \begin{cases} \alpha_1 = +i \\ \alpha_2 = -i \end{cases} \\
 \varphi(x) &= \varphi(x_1, x_2) \in \mathbb{Q}(\mathbb{K}) \\
 \varphi(x) &= \varphi(x_1, x_2) \in \mathbb{Q}(\mathbb{Z}) \Rightarrow \varphi(x) = \varphi(x_1, x_2) \in \{x_1 + x_2, x_1 - x_2, x_1 x_2, \dots\} \\
 \varphi(x) &= \varphi(x_1, x_2) = x_1 - x_2 \\
 V &= \varphi(\alpha) = \varphi(\alpha_1, \alpha_2) = \alpha_1 - \alpha_2 \\
 \forall \sigma, \tau \in S_2 &[\sigma \neq \tau \Leftrightarrow \sigma V \neq \tau V] \\
 \Leftrightarrow \forall \sigma_1, \sigma_2 \in S_2 &[\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)] \\
 \sigma_1(V) &= [12](\alpha_1 - \alpha_2) = \alpha_1 - \alpha_2 = (+i) - (-i) = +2i = +V \\
 \sigma_2(V) &= [21](\alpha_1 - \alpha_2) = \alpha_2 - \alpha_1 = (-i) - (+i) = -2i = -V \\
 \sigma_1(V) &= +2i \neq -2i = \sigma_2(V) \\
 \sigma_1(V) &\neq \sigma_2(V) \\
 \sigma_1(V) &= [12](\alpha_1 - \alpha_2) = \alpha_1 - \alpha_2 = (+i) - (-i) = +2i = +V && +i = +\frac{V}{2} \\
 \sigma_2(V) &= [21](\alpha_1 - \alpha_2) = \alpha_2 - \alpha_1 = (-i) - (+i) = -2i = -V && -i = -\frac{V}{2} \\
 \begin{cases} \alpha_1 = +i = +\frac{V}{2} = \varphi_1(V) = \alpha_1(V) \\ \alpha_2 = -i = -\frac{V}{2} = \varphi_2(V) = \alpha_2(V) \end{cases} && \begin{cases} \varphi_1(x) = +\frac{x}{2} \\ \varphi_2(x) = -\frac{x}{2} \end{cases} \\
 \mathbb{K}(V) &= \mathbb{K}(\alpha_1(V), \alpha_2(V)) = \mathbb{K}(\alpha_1, \alpha_2)
 \end{aligned}$$

$$V = 2i$$

$$\begin{aligned}\mathbb{K}(V) &= \mathbb{K}(\alpha_1(V), \alpha_2(V)) = \mathbb{K}(\alpha_1, \alpha_2) \\ &= \mathbb{Q}(2i) = \mathbb{Q}(\alpha_1(2i), \alpha_2(2i)) = \mathbb{Q}(+i, -i) = \mathbb{Q}(i)\end{aligned}$$

$$\begin{aligned}(x - V)(x - \bar{V}) &= (x - V)(x - V^*) \\ &= (x - 2i)(x - \bar{2i}) \\ &= (x - 2i)(x - (-2i)) \\ &= (x - 2i)(x + 2i) \\ &= x^2 + 4 \\ &= f_V(x) \in \mathbb{Q}[x] \\ &= (x - V_1)(x - V_2)\end{aligned}$$

$$\begin{aligned}f(x) &= x^2 + 1 = (x - (+i))(x - (-i)) = (x - \alpha_1)(x - \alpha_2) & f(x) = 0 \Rightarrow x \in \{\alpha_1, \alpha_2\} = \{+i, -i\} \\ \varphi(\mathbf{x}) &= \varphi(x_1, x_2) = x_1 - x_2 \\ V = \varphi(\alpha) &= \varphi(\alpha_1, \alpha_2) = \alpha_1 - \alpha_2 = +2i \\ \varphi(\alpha_1, \alpha_2) &= \alpha_1 - \alpha_2 = (+i) - (-i) = +2i = V_1 \\ \varphi(\alpha_2, \alpha_1) &= \alpha_2 - \alpha_1 = (-i) - (+i) = -2i = V_2 \\ \alpha &= (\alpha_1, \alpha_2) = (\varphi_1(V), \varphi_2(V)) = \left(+\frac{V}{2}, -\frac{V}{2}\right) \\ f_V(x) &= (x - V)(x - \bar{V}) = (x - (+2i))(x - (-2i)) = x^2 + 4 & f_V(x) = 0 \Rightarrow x \in \{V_1, V_2\} = \{+2i, -2i\} \\ & & n = \deg f_V(x) = 2\end{aligned}$$

$$\begin{aligned}\{\alpha_1, \alpha_2\} &= \{\varphi_1(V_1), \varphi_2(V_1)\} = \left\{+\frac{V_1}{2}, -\frac{V_1}{2}\right\} = \{+i, -i\} \\ \{\alpha_2, \alpha_1\} &= \{\varphi_1(V_2), \varphi_2(V_2)\} = \left\{+\frac{V_2}{2}, -\frac{V_2}{2}\right\} = \{-i, +i\}\end{aligned}$$

$$\mathcal{G} = \mathcal{G}(f) = \text{Gal}(f) = \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V_1) & \varphi_2(V_1) \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V_2) & \varphi_2(V_2) \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \{[12], [21]\}$$

$$\begin{aligned}\mathcal{G} = \mathcal{G}(f) = \text{Gal}(f) &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V) & \varphi_2(V) \end{pmatrix} \middle| V \in \{V_1, V_2\} \right\} \\ &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V_1) & \varphi_2(V_1) \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V_2) & \varphi_2(V_2) \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1 & \alpha_2 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} +i & -i \\ +i & -i \end{pmatrix}, \begin{pmatrix} +i & -i \\ -i & +i \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \{[12], [21]\}\end{aligned}$$

定義 2.0.2 (Galois group). [1, p.374~375, 382~385]

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) \in \mathbb{K}(\alpha_1, \dots, \alpha_m)[x]$$

$$(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3) \cdots (\alpha_{m-1} - \alpha_m)(\alpha_m - \alpha_1) \neq 0$$

lemma 2.0.2

$$\varphi(x) = \varphi(x_1, \dots, x_m) \quad \varphi(x) = \frac{P(x)}{Q(x)}, 0 \neq Q(x) \in \mathbb{K}[x]$$

$$V = \varphi(\alpha) = \varphi(\alpha_1, \dots, \alpha_m) \quad \forall \sigma_1, \sigma_2 \in S_m [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)]$$

$$V_i = \varphi(\sigma_i \alpha) = \varphi(\sigma_i \alpha_1, \dots, \sigma_i \alpha_m)$$

$$\wedge$$

$$f_V(x) = (x - V_1) \cdots (x - V_n) \quad \text{is a minimal polynomial} \in \mathbb{K}[x]$$

$$n = \deg f_V(x)$$

lemma 2.0.3

$$\alpha_1 = \alpha_1(V) = \varphi_1(V) \quad i \in \mathbb{N}_{\leq m}$$

$$\vdots$$

$$\varphi_i(x) = \frac{P_i(x)}{Q_i(x)}, 0 \neq Q_i(x) \in \mathbb{K}[x]$$

$$\alpha_m = \alpha_m(V) = \varphi_m(V)$$

lemma 2.0.4

$$\{\alpha_1, \dots, \alpha_m\} \in \{\varphi_1(V_1), \dots, \varphi_m(V_1)\} \quad = \{\varphi_1(V), \dots, \varphi_m(V)\}, \quad V = V_1$$

$$\vdots$$

$$\{\alpha_1, \dots, \alpha_m\} \in \{\varphi_1(V_n), \dots, \varphi_m(V_n)\} \quad = \{\varphi_1(V), \dots, \varphi_m(V)\}, \quad V = V_n$$

$$\Downarrow$$

$$\mathcal{G} = \mathcal{G}(f) = \text{Gal}(f) = \left\{ \begin{pmatrix} \alpha_1 & \cdots & \alpha_m \\ \varphi_1(V) & \cdots & \varphi_m(V) \end{pmatrix} \right\} \quad \text{is the Galois group of } f(x) \text{ over } \mathbb{K}[x] \quad V \in \{V_1, \dots, V_n\}$$

$$\mathcal{G} = \mathcal{G}(f) = \text{Gal}(f) = \left\{ \begin{pmatrix} \alpha_1 & \cdots & \alpha_m \\ \varphi_1(V) & \cdots & \varphi_m(V) \end{pmatrix} \middle| V \in \{V_1, \dots, V_n\} \right\}$$

1. 不變則已知: $F(\alpha)$ invariant $\Rightarrow F(\alpha)$ known

$$\text{if } \exists F(\alpha) \in \mathbb{K}[x], \forall \sigma_1, \sigma_2 \in S_m [F(\sigma_1(\alpha)) = F(\sigma_2(\alpha))] \Leftrightarrow F(\alpha) \text{ invariant}$$

$$F(\alpha) = F(\alpha_1, \dots, \alpha_m) = F(\varphi_1(V), \dots, \varphi_m(V)) = \hat{F}(V)$$

$$F(\sigma_1(\alpha)) = F(\sigma_2(\alpha)) \Rightarrow \hat{F}(V) = \hat{F}(V_1) = \cdots = \hat{F}(V_n)$$

$$= \frac{\hat{F}(V_1) + \cdots + \hat{F}(V_n)}{n} \quad \text{is a symmetric polynomial}$$

$$f_V(x) = (x - V_1) \cdots (x - V_n) \quad \text{is a minimal polynomial} \in \mathbb{K}[x]$$

$$= x^n - (V_1 + \cdots + V_n)x^{n-1} + \cdots + (-1)^n (V_1 \cdots V_n) \quad n = \deg f_V(x)$$

$$= x^n + k_1 x^{n-1} + \cdots + k_n \quad k_1, \dots, k_n \in \mathbb{K}$$

$$k_i(V_1, \dots, V_n) = k_i(V) \quad \text{is an elementary symmetric polynomial of } V = (V_1, \dots, V_n)$$

$$k_i \text{ are known}$$

$$F(\alpha) = F(\alpha_1, \dots, \alpha_m) = F(\varphi_1(V), \dots, \varphi_m(V))$$

$$= \hat{F}(V_1) = \cdots = \hat{F}(V_n)$$

$$= \hat{F}(V) = \frac{\hat{F}(V_1) + \cdots + \hat{F}(V_n)}{n} \quad \text{is a symmetric polynomial}$$

$$= \sum_{i=1}^m c_i [k_1, \dots, k_n] = \sum_{i=1}^m c_i [k_1(V), \dots, k_n(V)] \quad c_i \in \frac{P(x)}{Q(x)}, 0 \neq Q(x) \in \mathbb{K}[x]$$

$$= \sum_{i=1}^m c_i [k_i(V_1, \dots, V_n)] \quad \text{is a rational polynomial of elementary symmetric polynomials}$$

$$k_i \text{ are known}$$

\Downarrow

$$F(\alpha) \text{ is known}$$

2. 已知則不變： $F(\alpha)$ known $\Rightarrow F(\alpha)$ invariant

$$F(\alpha) = F(\alpha_1, \dots, \alpha_m) = F(\varphi_1(V), \dots, \varphi_m(V)) = k$$

known $k \in \mathbb{K}$

$$\dot{F}(V) = F(\varphi_1(V), \dots, \varphi_m(V)) - k$$

$$F \in \frac{P(x)}{Q(x)}, 0 \neq Q(x) \in \mathbb{K}[x]$$

$$\dot{F}(x) = 0$$

$$\Downarrow$$

$$x = V$$

$$\because F(\varphi_1(V), \dots, \varphi_m(V)) = k$$

$$\dot{F}(x) = (x - x_1) \cdots (x - x_{m-n}) \ddot{F}(x)$$

$$\{x_1, \dots, x_{m-n}\} \subseteq \mathbb{K}$$

$$\ddot{F}(x) = \frac{\dot{F}(x)}{(x - x_1) \cdots (x - x_{m-n})}$$

$$\in \frac{P(x)}{Q(x)}, 0 \neq Q(x) \in \mathbb{K}[x]$$

$$\ddot{F}(V) = \frac{\dot{F}(V)}{(V - x_1) \cdots (V - x_{m-n})} = \frac{0}{(V - x_1) \cdots (V - x_{m-n})}$$

$$\Rightarrow \ddot{F}(V) = 0$$

$$\Downarrow \text{lemma 2.0.1}$$

$f_V(x)$ is irreducible polynomial $\in \mathbb{K}[x]$

$$0 = \ddot{F}(V) = \ddot{F}(V_1) = \cdots = \ddot{F}(V_n)$$

$$\Downarrow$$

$$0 = \dot{F}(V) = \dot{F}(V_1) = \cdots = \dot{F}(V_n)$$

$$\Downarrow$$

$$0 = \dot{F}(V) = F(\varphi_1(V), \dots, \varphi_m(V)) - k$$

$$= F(\varphi_1(V_1), \dots, \varphi_m(V_1)) - k$$

$$\vdots$$

$$= F(\varphi_1(V_n), \dots, \varphi_m(V_n)) - k$$

$$\Downarrow$$

$$k = F(\varphi_1(V_1), \dots, \varphi_m(V_1)) = \cdots = F(\varphi_1(V_n), \dots, \varphi_m(V_n)) \quad \forall \sigma \in S_n, F(\sigma(\alpha)) = F(\alpha) \text{ invariant}$$

範例 2.0.2 (Galois group of $ax^2 + bx + c = 0, a \neq 0$). [1, p.378~382]

$$\begin{aligned} f(x) &= ax^2 + bx + c && \in \mathbb{Q}[x] \\ &= a(x - \alpha_1)(x - \alpha_2) \\ &= ax^2 - a(\alpha_1 + \alpha_2)x + a\alpha_1\alpha_2 && \in \mathbb{Q}(\alpha_1, \alpha_2)[x] \\ a &\neq 0 && (\alpha_1 - \alpha_2) \neq 0 \end{aligned}$$

$$\begin{aligned} &\Downarrow \\ \alpha_1 &= \frac{-b + \sqrt{b^2 - 4ac}}{2a} \\ \alpha_2 &= \frac{-b - \sqrt{b^2 - 4ac}}{2a} \\ &\Downarrow \text{lemma 2.0.2} \end{aligned}$$

$$\varphi(x) = \varphi(x_1, x_2)$$

$$\varphi(x) = \frac{P(x)}{Q(x)}, \quad \begin{matrix} P(x) \in \mathbb{Q}[x] \\ Q(x) \in \mathbb{Q}[x], 0 \neq Q(x) \end{matrix}$$

$$\begin{aligned} V &= \varphi(\alpha) = \varphi(\alpha_1, \alpha_2) \\ V_i &= \varphi(\sigma_i \alpha) = \varphi(\sigma_i \alpha_1, \sigma_i \alpha_2) \\ &\wedge \end{aligned}$$

$$\forall \sigma_1, \sigma_2 \in S_2 [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)]$$

$$f_V(x) = (x - V_1)(x - V_2)$$

$$\begin{aligned} &\text{is a minimal polynomial} \in \mathbb{Q}[x] \\ &n = \deg f_V(x) \end{aligned}$$

$$\begin{aligned} &\Downarrow \text{lemma 2.0.3} \\ \alpha_1 &= \alpha_1(V) = \varphi_1(V) \end{aligned}$$

$$i \in \mathbb{N}_{\leq 2}$$

$$\varphi_i(x) = \frac{P_i(x)}{Q_i(x)}, \quad \begin{matrix} P_i(x) \in \mathbb{K}[x] \\ Q_i(x) \in \mathbb{K}[x], 0 \neq Q_i(x) \end{matrix}$$

$$\begin{aligned} \alpha_2 &= \alpha_2(V) = \varphi_2(V) \\ &\wedge \text{lemma 2.0.4} \end{aligned}$$

$$\{\alpha_1, \alpha_2\} \in \{\varphi_1(V_1), \varphi_2(V_1)\}$$

$$= \{\varphi_1(V), \varphi_2(V)\}, \quad V = V_1$$

\vdots

$$\{\alpha_1, \alpha_2\} \in \{\varphi_1(V_n), \varphi_2(V_n)\}$$

$$= \{\varphi_1(V), \varphi_2(V)\}, \quad V = V_2$$

\Downarrow

$$\begin{aligned} \mathcal{G} = \mathcal{G}(f) = \text{Gal}(f) &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V) & \varphi_2(V) \end{pmatrix} \middle| V \in \{V_1, V_2\} \right\} = \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V_1) & \varphi_2(V_1) \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V_2) & \varphi_2(V_2) \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_1 & \alpha_2 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \{[12], [21]\} \end{aligned}$$

[1, p.379]

1. 不變則已知: $F(\alpha)$ invariant $\Rightarrow F(\alpha)$ known

elementary symmetric polynomials

$$\begin{aligned} \alpha_1 + \alpha_2 &= \frac{-b}{a} = \frac{-b + \sqrt{b^2 - 4ac}}{2a} + \frac{-b - \sqrt{b^2 - 4ac}}{2a} \\ \alpha_1 \alpha_2 &= \frac{c}{a} = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \cdot \frac{-b - \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

$$\begin{aligned} \alpha_1 + \alpha_2 &\rightarrow \frac{-b}{a} \\ \alpha_1 \alpha_2 &\rightarrow \frac{c}{a} \end{aligned}$$

2. 已知則不變: $F(\alpha)$ known $\Rightarrow F(\alpha)$ invariant

$$\begin{aligned} \frac{-b}{a} &\rightarrow \alpha_1 + \alpha_2 \\ \frac{c}{a} &\rightarrow \alpha_1 \alpha_2 \end{aligned}$$

[1, p.380~381]

範例 2.0.3 (Galois group of $x^3 - 2x = 0$). [1, p.385~388]

$$\begin{aligned}
 f(x) &= x^3 - 2x \\
 &= x(x^2 - 2) && \in \mathbb{Q}[x] \\
 &= x(x - \sqrt{2})(x - (-\sqrt{2})) && \in \mathbb{Q}(\sqrt{2})[x] \subset \mathbb{R}[x] \\
 &= (x - \alpha)(x - \beta)(x - \gamma) && \{\alpha, \beta, \gamma\} = \{0, +\sqrt{2}, -\sqrt{2}\} \\
 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) && \{\alpha_1, \alpha_2, \alpha_3\} = \{0, \sqrt{2}, -\sqrt{2}\}
 \end{aligned}$$

$$\alpha = (\alpha_1, \alpha_2, \alpha_3) = (0, \sqrt{2}, -\sqrt{2}) \Rightarrow \begin{cases} \alpha_1 = 0 \\ \alpha_2 = +\sqrt{2} \\ \alpha_3 = -\sqrt{2} \end{cases}$$

$$\varphi(\mathbf{x}) = \varphi(x_1, x_2, x_3) = x_1 + 2x_2 + 4x_3 = 1x_1 + 2x_2 + 4x_3$$

$$\begin{aligned}
 \varphi(\alpha_1, \alpha_2, \alpha_3) &= 1\alpha_1 + 2\alpha_2 + 4\alpha_3 = 1(0) + 2(\sqrt{2}) + 4(-\sqrt{2}) = -2\sqrt{2} = V_1 \\
 \varphi(\alpha_2, \alpha_3, \alpha_1) &= 1\alpha_2 + 2\alpha_3 + 4\alpha_1 = 1(\sqrt{2}) + 2(-\sqrt{2}) + 4(0) = -1\sqrt{2} = V_2 \\
 \varphi(\alpha_3, \alpha_1, \alpha_2) &= 1\alpha_3 + 2\alpha_1 + 4\alpha_2 = 1(-\sqrt{2}) + 2(0) + 4(\sqrt{2}) = +3\sqrt{2} = V_3 \\
 \varphi(\alpha_1, \alpha_3, \alpha_2) &= 1\alpha_1 + 2\alpha_3 + 4\alpha_2 = 1(0) + 2(-\sqrt{2}) + 4(\sqrt{2}) = +2\sqrt{2} = V_4 \\
 \varphi(\alpha_2, \alpha_1, \alpha_3) &= 1\alpha_2 + 2\alpha_1 + 4\alpha_3 = 1(\sqrt{2}) + 2(0) + 4(-\sqrt{2}) = -3\sqrt{2} = V_5 \\
 \varphi(\alpha_3, \alpha_2, \alpha_1) &= 1\alpha_3 + 2\alpha_2 + 4\alpha_1 = 1(-\sqrt{2}) + 2(\sqrt{2}) + 4(0) = +1\sqrt{2} = V_6
 \end{aligned}$$

$$\begin{aligned}
 \mathbb{K}(V) &= \mathbb{K}(\alpha_1(V), \alpha_2(V)) = \mathbb{K}(\alpha_1, \alpha_2) \\
 &= \mathbb{Q}(-2\sqrt{2}) = \mathbb{Q}(\alpha_1(-2\sqrt{2}), \alpha_2(-2\sqrt{2}), \alpha_3(-2\sqrt{2})) \\
 &= \mathbb{Q}(0, +\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})
 \end{aligned}$$

$$\begin{aligned}
 &(x - V_1)(x - (-V_1)) \\
 &= (x - (+V_1))(x - (-V_1)) \\
 &= (x - (-2\sqrt{2}))(x - (+2\sqrt{2})) \\
 &= x^2 - 8 && = f_V(x) \in \mathbb{Q}[x] \\
 &&& n = \deg f_V(x) = 2
 \end{aligned}$$

$$\begin{cases} \varphi_1(x) = 0 \\ \varphi_2(x) = -\frac{x}{2} \\ \varphi_3(x) = +\frac{x}{2} \end{cases} \Rightarrow \begin{cases} \varphi_1(V_1) = 0 \\ \varphi_2(V_1) = -\frac{V_1}{2} = -\frac{-2\sqrt{2}}{2} = +\sqrt{2} \\ \varphi_3(V_1) = +\frac{V_1}{2} = +\frac{-2\sqrt{2}}{2} = -\sqrt{2} \end{cases} \begin{matrix} = \alpha_1 \\ = \alpha_2 \\ = \alpha_3 \end{matrix}$$

$$\begin{cases} \varphi_1(x) = 0 \\ \varphi_2(x) = -\frac{x}{2} \\ \varphi_3(x) = +\frac{x}{2} \end{cases} \Rightarrow \begin{cases} \varphi_1(V_4) = 0 \\ \varphi_2(V_4) = -\frac{V_4}{2} = -\frac{+2\sqrt{2}}{2} = -\sqrt{2} \\ \varphi_3(V_4) = +\frac{V_4}{2} = +\frac{+2\sqrt{2}}{2} = +\sqrt{2} \end{cases} \begin{matrix} = \alpha_1 \\ = \alpha_3 \\ = \alpha_2 \end{matrix}$$

$$\begin{aligned}
 \mathcal{G} = \mathcal{G}(f) = \text{Gal}(f) &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \varphi_1(V_1) & \varphi_2(V_1) & \varphi_3(V_1) \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \varphi_1(V_4) & \varphi_2(V_4) & \varphi_3(V_4) \end{pmatrix} \right\} \\
 &= \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1 & \alpha_3 & \alpha_2 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} = \{[123], [132]\}
 \end{aligned}$$

範例 2.0.4 (Galois group of $x^4 - 4x^3 - 4x^2 + 8x - 2 = 0$). MathKiwi: But why is there no quintic formula? — Galois Theory

$$f(x) = x^4 - 4x^3 - 4x^2 + 8x - 2$$

$$f(x) = 0$$

$$\Downarrow$$

$$x \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$$

$$\alpha_1 = 1 + \sqrt{2} + \sqrt{3 + \sqrt{2}}$$

$$\alpha_2 = 1 - \sqrt{2} + \sqrt{3 + \sqrt{2}}$$

$$\alpha_3 = 1 + \sqrt{2} - \sqrt{3 + \sqrt{2}}$$

$$\alpha_4 = 1 + \sqrt{2} - \sqrt{3 + \sqrt{2}}$$

$$\varphi(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$$

$$\varphi(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4$$

$$\varphi(x_1, x_2, x_3, x_4) = x_1 x_3 + x_2 x_4$$

$$\varphi(x_1, x_2, x_3, x_4) = (x_1 + x_2) - (x_3 + x_4)$$

Chapter 3

probability theory

定理 3.0.1 (Bonferroni inequality). [2, p.77]

$$P(E_1 \cap E_2) \geq 1 - P(E_1) - P(E_2)$$

定義 3.0.1 (exponential family). A family of PDF/PMF is called exponential family if

$$f(x|\boldsymbol{\theta}) = h(x) c(\boldsymbol{\theta}) e^{\sum_{j=1}^k w_j(\boldsymbol{\theta}) t_j(x)} = h(x) c(\boldsymbol{\theta}) \exp \left(\sum_{j=1}^k w_j(\boldsymbol{\theta}) t_j(x) \right)$$

with $\boldsymbol{\theta} = \boldsymbol{\theta}(\theta_1, \dots, \theta_k) = (\theta_1, \dots, \theta_k)$ for some $h(x), c(\boldsymbol{\theta}), w_j(\boldsymbol{\theta}), t_j(x)$, where

$$h(x) c(\boldsymbol{\theta}) \geq 0 \Rightarrow f(x|\boldsymbol{\theta}) \geq 0$$

and parameters $\boldsymbol{\theta}$ and statistic or real number x can be separated.

$$\mathcal{E}^f = \left\{ f \left| f = f(x|\boldsymbol{\theta}) = h(x) c(\boldsymbol{\theta}) e^{\sum_{j=1}^k w_j(\boldsymbol{\theta}) t_j(x)} = h(x) c(\boldsymbol{\theta}) \exp \left(\sum_{j=1}^k w_j(\boldsymbol{\theta}) t_j(x) \right) \right. \right\}$$

Bibliography

- [1] 結城浩. 數學女孩: 數學女孩: 伽羅瓦理論[M/OL]. 世茂, 2014[2024-06-09]. <https://www.books.com.tw/products/0010647846>. 19, 20, 21, 23, 25, 26
- [2] 張翔, 廖崇智. 提綱挈領學統計[M/OL]. 9 版. 大碩教育, 2021[2024-03-24]. <https://www.books.com.tw/products/0010888833>. 29