math

Joey Yu Hsu, MD

June 12, 2024

since 2024/06/11

Contents

list of definition

list of theorem

list of example

List of Figures

Part I

LaTeX & math languages

Chapter 1

LyX

1.1 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 設定爲 English, 如果檔案語言設定爲 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啓此檔，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

1.2 LyZ: linking Zotero and LyX

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

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

1.3 list of theorems module

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

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

1.3.1 list of equations

https://tex.stackexchange.com/questions/173102/table-of-equations-like-list-of-figures

https://stackoverflow.com/questions/61517319/vertical-spacing-adjustment-between-different-chapters-labels-in-the-list-of-eq

1.4 multiple bibliography

error keeps occurring, thus do it in the final step

1.4.1 bibtopic: per chapter

bibtopic.sty

pass options to package in LyX before usepackage

Document >Settings... >Local layout.

Add ‘PackageOptions <package> <option1,option2,...>‘

Chapter 2

$\LaTeX$3

2.1 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

2.1.1 single coloring

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

also can be put into "preamble"

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

2.1.2 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
ρ_0	ρ_0	ρ_1	ρ_2	π_0	π_1	π_2
ρ_1	ρ_1	ρ_2	ρ_0	π_1	π_2	π_0
ρ_2	ρ_2	ρ_0	ρ_1	π_2	π_0	π_1
π_0	π_0	π_2	π_1	ρ_0	ρ_2	ρ_1
π_1	π_1	π_0	π_2	ρ_1	ρ_0	ρ_2
π_2	π_2	π_1	π_0	ρ_2	ρ_1	ρ_0
$\cdot_{S_3}$	e	(123)	(132)	(3) (12)	(1) (23)	(2) (31)
e	e	(123)	(132)	(3) (12)	(1) (23)	(2) (31)
(123)	(123)	(132)	e	(1) (23)	(2) (31)	(3) (12)
(132)	(132)	e	(123)	(2) (31)	(3) (12)	(1) (23)
(3) (12)	(3) (12)	(2) (31)	(1) (23)	e	(132)	(123)
(1) (23)	(1) (23)	(3) (12)	(2) (31)	(123)	e	(132)
(2) (31)	(2) (31)	(1) (23)	(3) (12)	(132)	(123)	e

$\cdot_{S_3}$	[123]	[231]	[312]	[213]	[132]	[321]
[123]	[123]	[231]	[312]	[213]	[132]	[321]
[231]	[231]	[312]	[123]	[132]	[321]	[213]
[312]	[312]	[123]	[231]	[321]	[213]	[132]
[213]	[213]	[321]	[132]	[123]	[312]	[231]
[132]	[132]	[213]	[321]	[231]	[123]	[312]
[321]	[321]	[132]	[213]	[312]	[231]	[123]
$\cdot_{S_3}$	()	(123)	(132)	(12)	(23)	(31)
()	()	(123)	(132)	(12)	(23)	(31)
(123)	(123)	(132)	()	(23)	(31)	(12)
(132)	(132)	()	(123)	(31)	(12)	(23)
(12)	(12)	(31)	(23)	()	(132)	(123)
(23)	(23)	(12)	(31)	(123)	()	(132)
(31)	(31)	(23)	(12)	(132)	(123)	()

Chapter 3

Ti*k*Z

3.1 Ti*k*Z-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 corneres, 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}
```

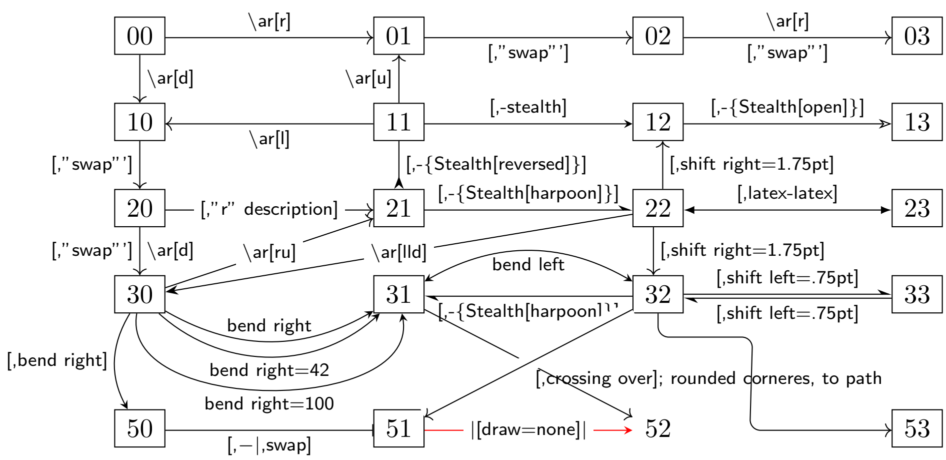

Figure 3.1: learn TikZ-CD = tikz-cd in one picture 2

Chapter 4

PGFplots

Chapter 5

LEAN

5.1 MathLib

https://leanprover-community.github.io/mathlib-overview.html

Part II

mathematics

Chapter 6

logic & computation

6.1 set theory

6.2 computability

6.3 model theory

Chapter 7

algebra

7.1 group theory

定義 7.1.1 (group). 群

$$
\begin{aligned}
&G \text{ is a group}\\
&\Updownarrow \text{def.}\\
G=(G,\cdot)=(G,\cdot_G)=&\left\{ g \left| \begin{array}{lll} g_1\cdot g_2 = g_1g_2\in G & \forall g_1,g_2\in G & (c)\ \cdot_G \text{ closure}\\ g_1(g_2g_3)=(g_1g_2)g_3=g_1g_2g_3 & \forall g_1,g_2,g_3\in G & (a)\ \cdot_G \text{ associativity}\\ e\cdot g=eg=g=ge=g\cdot e & \exists e=e_G\in G,\forall g\in G & (id)\ \text{identity element}\\ \overline{g}\cdot g=\bar{g}g=e=g\bar{g}=g\cdot\overline{g} & \forall g\in G,\exists\overline{g}\in G & (in)\ \text{inverse element} \end{array}\right.\right\}
\end{aligned}
$$

定理 7.1.1.

$$\begin{array}{r}\forall g\in G\\ g\neq e\in G\end{array}\Rightarrow \forall\widetilde{g}\in G\left[g\widetilde{g}\neq\widetilde{g}\right]$$

定理 7.1.2.

$$\begin{array}{r}\forall g_1,g_2\in G\\ g_1\neq g_2\end{array}\Rightarrow \forall g\in G\left[g_1g\neq g_2g\right]$$

定理 7.1.3 (rearrangement theorem).

$$\forall g\in G\left[\{g\widetilde{g}|\widetilde{g}\in G\}=G\right]$$

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

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

□

定理 7.1.4 ($C_3 = \mathbb{Z}_3 \trianglelefteq S_3 = D_3$).

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

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

定義 7.1.2 (homomorphism).

定理 7.1.5 (kernel of homomorphism).

7.2 field theory

7.2.1 Galois theory

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

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

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

$$
\begin{aligned}
0 =& (x - \alpha) && x = \alpha \Leftrightarrow x \in \{\alpha\} \\
=& x - \alpha \\
0 =& (x - \alpha)(x - \beta) && x = \alpha, \beta \Leftrightarrow x \in \{\alpha, \beta\} \\
=& x^2 - (\alpha + \beta) x + \alpha\beta \\
0 =& (x - \alpha)(x - \beta)(x - \gamma) && x = \alpha, \beta, \gamma \Leftrightarrow x \in \{\alpha, \beta, \gamma\} \\
=& x^3 - (\alpha + \beta + \gamma) x^2 + (\alpha\beta + \beta\gamma + \gamma\alpha) x - \alpha\beta\gamma \\
0 =& (x - \alpha)(x - \beta)(x - \gamma)(x - \delta) && x = \alpha, \beta, \gamma, \delta \Leftrightarrow x \in \{\alpha, \beta, \gamma, \delta\} \\
=& x^4 - (\alpha + \beta + \gamma + \delta) x^3 + \cdots + \alpha\beta\gamma\delta \\
0 =& (x - \alpha)(x - \beta)(x - \gamma)(x - \delta)(x - \varepsilon) && x = \alpha, \beta, \gamma, \delta, \varepsilon \Leftrightarrow x \in \{\alpha, \beta, \gamma, \delta, \varepsilon\} \\
=& x^5 - (\alpha + \beta + \gamma + \delta + \varepsilon) x^4 + \cdots - \alpha\beta\gamma\delta\varepsilon
\end{aligned}
$$

$$
\begin{aligned}
0 =& (x-\alpha_1) & x=\alpha_1 \Leftrightarrow x\in\{\alpha_1\}\\
=& x-\alpha_1 & \\
0 =& (x-\alpha_1)(x-\alpha_2) & x=\alpha_1,\alpha_2 \Leftrightarrow x\in\{\alpha_1,\alpha_2\}\\
=& x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2 & \\
0 =& (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) & x=\alpha_1,\alpha_2,\alpha_3 \Leftrightarrow x\in\{\alpha_1,\alpha_2,\alpha_3\}\\
=& x^3-(\alpha_1+\alpha_2+\alpha_3)x^2+(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)x-\alpha_1\alpha_2\alpha_3 & \\
0 =& (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) & x=\alpha_1,\alpha_2,\alpha_3,\alpha_4 \Leftrightarrow x\in\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}\\
=& x^4-(\alpha_1+\alpha_2+\alpha_3+\alpha_4)x^3+\cdots+\alpha_1\alpha_2\alpha_3\alpha_4 & \\
0 =& (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5) & x=\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5 \Leftrightarrow x\in\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5\}\\
=& x^5-(\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5)x^4+\cdots-\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5 &
\end{aligned}
$$

定理 7.2.1 (Abel-Ruffini theorem)**.** *There is no general formula for solving a polynomial of degree 5 or higher.*

定義 7.2.1 (field)**.** körper $\mathbb{K}=\mathbb{F}$ field

定義 7.2.2 (reducible polynomial vs. irreducible polynomial)**.** [1, p.357]

$$
\begin{aligned}
f(x) =& p_n x^n + p_{n-1}x^{n-1}+\cdots+p_1x+p_0 & \Leftrightarrow f(x)\in\mathbb{K}[x]\\
& & p_n\neq 0 \Rightarrow \deg f(x)=n\in\mathbb{N}\\
=& p_jx^j=\sum_{j=1}^{n}p_jx^j & j\in\mathbb{Z}_{[0,n]}\\
& & p_j\in\mathbb{K}=\mathbb{F}\\
=& p_n(x-x_1)(x-x_2)\cdots(x-x_n) & \{x_1,x_2,\cdots,x_n\}\subseteq\mathbb{K}(x_1,x_2,\cdots,x_n)\\
=& p_n(x-x_1)\cdots(x-x_n) & \{x_1,\cdots,x_n\}\subseteq\mathbb{K}(x_1,\cdots,x_n)\\
& \Updownarrow & \\
f(x) & \text{ is reducible over } \mathbb{K}(x_1,\cdots,x_n) &
\end{aligned}
$$

引理 7.2.1 (irreducible polynomial factor lemma)**.** *[1, p.362]*
factor theorem https://en.wikipedia.org/wiki/Factor_theorem

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

備註 7.2.1 (polynomial cf. integer). [1, p.363]

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

引理 7.2.2 (variable represented by roots)**.** *[1, p.366]*

$$
\begin{aligned}
f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m) & \quad \in\mathbb{K}(\alpha_1,\cdots,\alpha_m)[x]\\
& (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)\cdots(\alpha_{m-1}-\alpha_m)(\alpha_m-\alpha_1)\neq 0
\end{aligned}
$$

$$\Downarrow \textit{ variable represented by roots}$$

$$
\begin{aligned}
\varphi(\boldsymbol{x}) =& \varphi(x_1,\cdots,x_m) & \varphi(\boldsymbol{x})=\frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{array}{r}P(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}]\\ 0\neq Q(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}]\end{array}\\
V=\varphi(\boldsymbol{\alpha}) =& \varphi(\alpha_1,\cdots,\alpha_m) & \forall\sigma_1,\sigma_2\in S_m[\sigma_1\neq\sigma_2\Leftrightarrow\sigma_1(V)\neq\sigma_2(V)]\\
V_i=\varphi(\sigma_i\boldsymbol{\alpha}) =& \varphi(\sigma_i\alpha_1,\cdots,\sigma_i\alpha_m) & \\
& \Updownarrow & \\
\exists\varphi(\boldsymbol{x})=\varphi(x_1,\cdots,x_m) =& \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{array}{r}P(\boldsymbol{x})\in\mathbb{K}[x]\\ 0\neq Q(\boldsymbol{x})\in\mathbb{K}[x]\end{array} & \begin{bmatrix} V=\varphi(\boldsymbol{\alpha})=\varphi(\alpha_1,\cdots,\alpha_m)\\ \forall\sigma_1,\sigma_2\in S_m[\sigma_1\neq\sigma_2\Leftrightarrow\sigma_1(V)\neq\sigma_2(V)]\end{bmatrix}
\end{aligned}
$$

引理 7.2.3 (roots represented by variable). *[1, p.368]*

$$
\begin{aligned}
f(x) &= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m) && \in \mathbb{K}(\alpha_1,\cdots,\alpha_m)[x] \\
& && (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)\cdots(\alpha_{m-1}-\alpha_m)(\alpha_m-\alpha_1)\neq 0 \\
&\Downarrow lemma\ 7.2.2 \\
\varphi(\boldsymbol{x}) &= \varphi(x_1,\cdots,x_m) && \varphi(\boldsymbol{x}) = \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{matrix} P(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}] \\ 0\neq Q(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}]\end{matrix} \\
V = \varphi(\boldsymbol{\alpha}) &= \varphi(\alpha_1,\cdots,\alpha_m) && \forall\sigma_1,\sigma_2\in S_m\left[\sigma_1\neq\sigma_2\Leftrightarrow\sigma_1(V)\neq\sigma_2(V)\right] \\
V_i = \varphi(\sigma_i\boldsymbol{\alpha}) &= \varphi(\sigma_i\alpha_1,\cdots,\sigma_i\alpha_m) \\
&\Updownarrow \\
\exists\varphi(\boldsymbol{x}) = \varphi(x_1,\cdots,x_m) &= \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{matrix} P(\boldsymbol{x})\in\mathbb{K}[x] \\ 0\neq Q(\boldsymbol{x})\in\mathbb{K}[x]\end{matrix} && \begin{bmatrix} V = \varphi(\boldsymbol{\alpha}) = \varphi(\alpha_1,\cdots,\alpha_m) \\ \forall\sigma_1,\sigma_2\in S_m\left[\sigma_1\neq\sigma_2\Leftrightarrow\sigma_1(V)\neq\sigma_2(V)\right]\end{bmatrix} \\
&\Downarrow \textit{ roots represented by variable} \\
\alpha_1 &= \alpha_1(V) = \varphi_1(V) && i\in\mathbb{N}_{\leq m} \\
&\vdots && \varphi_i(\boldsymbol{x}) = \frac{P_i(\boldsymbol{x})}{Q_i(\boldsymbol{x})}, \begin{matrix} P_i(\boldsymbol{x})\in\mathbb{K}[x] \\ 0\neq Q_i(\boldsymbol{x})\in\mathbb{K}[x]\end{matrix} \\
\alpha_m &= \alpha_m(V) = \varphi_m(V) \\
&\Updownarrow \\
\exists\varphi_i(\boldsymbol{x}) &= \varphi_i(x_1,\cdots,x_m) = \frac{P_i(\boldsymbol{x})}{Q_i(\boldsymbol{x})}, \begin{matrix} P_i(\boldsymbol{x})\in\mathbb{K}[x] \\ 0\neq Q_i(\boldsymbol{x})\in\mathbb{K}[x]\end{matrix} && \begin{bmatrix} \alpha_1 = \alpha_1(V) = \varphi_1(V) \\ \vdots \\ \alpha_m = \alpha_m(V) = \varphi_m(V)\end{bmatrix}
\end{aligned}
$$

引理 7.2.4 (root rearrangement by variable conjugate). *[1, p.370]*

$$
\begin{aligned}
f(x) &= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m) && \in \mathbb{K}(\alpha_1,\cdots,\alpha_m)[x] \\
& && (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)\cdots(\alpha_{m-1}-\alpha_m)(\alpha_m-\alpha_1)\neq 0 \\
&\Downarrow lemma\ 7.2.2 \\
\varphi(\boldsymbol{x}) &= \varphi(x_1,\cdots,x_m) && \varphi(\boldsymbol{x}) = \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{matrix} P(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}] \\ 0\neq Q(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}]\end{matrix} \\
V = \varphi(\boldsymbol{\alpha}) &= \varphi(\alpha_1,\cdots,\alpha_m) && \forall\sigma_1,\sigma_2\in S_m\left[\sigma_1\neq\sigma_2\Leftrightarrow\sigma_1(V)\neq\sigma_2(V)\right] \\
V_i = \varphi(\sigma_i\boldsymbol{\alpha}) &= \varphi(\sigma_i\alpha_1,\cdots,\sigma_i\alpha_m) \\
&\wedge \\
f_V(x) &= (x-V_1)\cdots(x-V_n) && \textit{is a minimal polynomial } \in\mathbb{K}[x] \\
& && n = \deg f_V(x) \\
&\Downarrow lemma\ 7.2.3 \\
\alpha_1 &= \alpha_1(V) = \varphi_1(V) && i\in\mathbb{N}_{\leq m} \\
&\vdots && \varphi_i(\boldsymbol{x}) = \frac{P_i(\boldsymbol{x})}{Q_i(\boldsymbol{x})}, \begin{matrix} P_i(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}] \\ 0\neq Q_i(\boldsymbol{x})\in\mathbb{K}[\boldsymbol{x}]\end{matrix} \\
\alpha_m &= \alpha_m(V) = \varphi_m(V) \\
&\Downarrow \textit{ root rearrangement by variable conjugate} \\
\{\alpha_1,\cdots,\alpha_m\} &\in \{\varphi_1(V_1),\cdots,\varphi_m(V_1)\} && = \{\varphi_1(V),\cdots,\varphi_m(V)\}, \quad V = V_1 \\
&\vdots \\
\{\alpha_1,\cdots,\alpha_m\} &\in \{\varphi_1(V_n),\cdots,\varphi_m(V_n)\} && = \{\varphi_1(V),\cdots,\varphi_m(V)\}, \quad V = V_n
\end{aligned}
$$

範例 7.2.1 (Galois group of $x^2+1=0$). [1, p.367～372]

$$
\begin{aligned}
f(x) &= x^2+1 && \in\mathbb{Q}[x] \\
&= (x+\mathrm{i})(x-\mathrm{i}) && \in\mathbb{Q}(\mathrm{i})[x]\subset\mathbb{C}[x] \\
&= (x-\mathrm{i})(x+\mathrm{i}) \\
&= (x-\mathrm{i})(x-(-\mathrm{i})) \\
&= (x-\alpha)(x-\beta) && \{\alpha,\beta\} = \{+\mathrm{i},-\mathrm{i}\} \\
&= (x-\alpha_1)(x-\alpha_2) && \{\alpha_1,\alpha_2\} = \{\mathrm{i},-\mathrm{i}\}
\end{aligned}
$$

$$(\alpha_1, \alpha_2) = (\mathrm{i}, -\mathrm{i}) \Rightarrow \begin{cases} \alpha_1 = & +\mathrm{i} \\ \alpha_2 = & -\mathrm{i} \end{cases}$$

$$\varphi(\boldsymbol{x}) = \varphi(x_1, x_2) \in \mathbb{Q}(\mathbb{K})$$

$$\varphi(\boldsymbol{x}) = \varphi(x_1, x_2) \in \mathbb{Q}(\mathbb{Z}) \Rightarrow \varphi(\boldsymbol{x}) = \varphi(x_1, x_2) \in \{x_1 + x_2, x_1 - x_2, x_1 x_2, \cdots\}$$

$$\varphi(\boldsymbol{x}) = \varphi(x_1, x_2) = x_1 - x_2$$

$$V = \varphi(\boldsymbol{\alpha}) = \varphi(\alpha_1, \alpha_2) = \alpha_1 - \alpha_2$$

$$\forall \sigma, \tau \in S_2 [\sigma \neq \tau \Leftrightarrow \sigma V \neq \tau V]$$

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

$$\sigma_1(V) = [12](\alpha_1 - \alpha_2) = \alpha_1 - \alpha_2 = (+\mathrm{i}) - (-\mathrm{i}) = +2\mathrm{i} = +V$$

$$\sigma_2(V) = [21](\alpha_1 - \alpha_2) = \alpha_2 - \alpha_1 = (-\mathrm{i}) - (+\mathrm{i}) = -2\mathrm{i} = -V$$

$$\sigma_1(V) = +2\mathrm{i} \neq -2\mathrm{i} = \sigma_2(V)$$

$$\sigma_1(V) \neq \sigma_2(V)$$

$$\sigma_1(V) = [12](\alpha_1 - \alpha_2) = \alpha_1 - \alpha_2 = (+\mathrm{i}) - (-\mathrm{i}) = +2\mathrm{i} = +V \qquad +\mathrm{i} = +\frac{V}{2}$$

$$\sigma_2(V) = [21](\alpha_1 - \alpha_2) = \alpha_2 - \alpha_1 = (-\mathrm{i}) - (+\mathrm{i}) = -2\mathrm{i} = -V \qquad -\mathrm{i} = -\frac{V}{2}$$

$$\begin{cases} \alpha_1 = & +\mathrm{i} = +\frac{V}{2} = \varphi_1(V) = \alpha_1(V) \\ \alpha_2 = & -\mathrm{i} = -\frac{V}{2} = \varphi_2(V) = \alpha_2(V) \end{cases} \qquad \begin{cases} \varphi_1(x) = & +\frac{x}{2} \\ \varphi_2(x) = & -\frac{x}{2} \end{cases}$$

$$\mathbb{K}(V) = \mathbb{K}(\alpha_1(V), \alpha_2(V)) = \mathbb{K}(\alpha_1, \alpha_2)$$

$$V = 2\mathrm{i}$$

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

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

$$f(x) = x^2 + 1 = (x - (+\mathrm{i}))(x - (-\mathrm{i})) = (x - \alpha_1)(x - \alpha_2) \qquad f(x) = 0 \Rightarrow x \in \{\alpha_1, \alpha_2\} = \{+\mathrm{i}, -\mathrm{i}\}$$

$$\begin{aligned} \varphi(\boldsymbol{x}) =& \varphi(x_1, x_2) = x_1 - x_2 \\ V = \varphi(\boldsymbol{\alpha}) =& \varphi(\alpha_1, \alpha_2) = \alpha_1 - \alpha_2 = +2\mathrm{i} \\ \varphi(\alpha_1, \alpha_2) =& \alpha_1 - \alpha_2 = (+\mathrm{i}) - (-\mathrm{i}) = +2\mathrm{i} = V_1 \\ \varphi(\alpha_2, \alpha_1) =& \alpha_2 - \alpha_1 = (-\mathrm{i}) - (+\mathrm{i}) = -2\mathrm{i} = V_2 \end{aligned}$$

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2) = (\varphi_1(V), \varphi_2(V)) = \left(+\frac{V}{2}, -\frac{V}{2}\right)$$

$$f_V(x) = (x - V)\left(x - \overline{V}\right) = (x - (+2\mathrm{i}))(x - (-2\mathrm{i})) = x^2 + 4 \quad f_V(x) = 0 \Rightarrow x \in \{V_1, V_2\} = \{+2\mathrm{i}, -2\mathrm{i}\}$$

$$n = \deg f_V(x) = 2$$

$$\{\alpha_1, \alpha_2\} = \{\varphi_1(V_1), \varphi_2(V_1)\} = \left\{+\frac{V_1}{2}, -\frac{V_1}{2}\right\} = \{+\mathrm{i}, -\mathrm{i}\}$$

$$\{\alpha_2, \alpha_1\} = \{\varphi_1(V_2), \varphi_2(V_2)\} = \left\{+\frac{V_2}{2}, -\frac{V_2}{2}\right\} = \{-\mathrm{i}, +\mathrm{i}\}$$

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

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

定義 7.2.3 (Galois group). [1, p.374～375,382～385]

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

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

$$\Downarrow lemma\ 7.2.2$$

$$\varphi(\boldsymbol{x}) = \varphi(x_1,\cdots,x_m) \qquad \varphi(\boldsymbol{x}) = \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{array}{r} P(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0 \neq Q(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \end{array}$$

$$V = \varphi(\boldsymbol{\alpha}) = \varphi(\alpha_1,\cdots,\alpha_m) \qquad \forall \sigma_1,\sigma_2 \in S_m [\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)]$$

$$V_i = \varphi(\sigma_i\boldsymbol{\alpha}) = \varphi(\sigma_i\alpha_1,\cdots,\sigma_i\alpha_m)$$

$$\wedge$$

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

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

$$\Downarrow lemma\ 7.2.3$$

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

$$\vdots \qquad \varphi_i(\boldsymbol{x}) = \frac{P_i(\boldsymbol{x})}{Q_i(\boldsymbol{x})}, \begin{array}{r} P_i(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0 \neq Q_i(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \end{array}$$

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

$$\wedge lemma\ 7.2.4$$

$$\{\alpha_1,\cdots,\alpha_m\} \in \{\varphi_1(V_1),\cdots,\varphi_m(V_1)\} = \{\varphi_1(V),\cdots,\varphi_m(V)\}, \qquad V = V_1$$

$$\vdots$$

$$\{\alpha_1,\cdots,\alpha_m\} \in \{\varphi_1(V_n),\cdots,\varphi_m(V_n)\} = \{\varphi_1(V),\cdots,\varphi_m(V)\}, \qquad V = V_n$$

$$\Downarrow$$

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

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

定理 7.2.2 (Galois group).

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

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

$$F(\boldsymbol{\alpha}) = F(\alpha_1,\cdots,\alpha_m) = F(\varphi_1(V),\cdots,\varphi_m(V)) = \widehat{F}(V)$$

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

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

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

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

$$= x^n + k_1x^{n-1} + \cdots + k_n \qquad k_1,\cdots,k_n \in \mathbb{K}$$

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

$$k_i \text{ are known}$$

$$F(\boldsymbol{\alpha}) = F(\alpha_1,\cdots,\alpha_m) = F(\varphi_1(V),\cdots,\varphi_m(V))$$

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

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

$$= \sum_{i=1}^{m} c_i[k_1,\cdots,k_n] = \sum_{i=1}^{m} c_i[k_1(\boldsymbol{V}),\cdots,k_n(\boldsymbol{V})] \qquad c_i \in \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{array}{r} P(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0 \neq Q(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \end{array}$$

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

$$k_i \text{ are known}$$

$$\Downarrow$$

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

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

$$
\begin{aligned}
F(\boldsymbol{\alpha}) =& F(\alpha_1,\cdots,\alpha_m) = F(\varphi_1(V),\cdots,\varphi_m(V)) = k && \text{known } k \in \mathbb{K} \\
\dot{F}(V) =& F(\varphi_1(V),\cdots,\varphi_m(V)) - k && F \in \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{array}{r} P(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0 \neq Q(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \end{array} \\
\dot{F}(x) =& 0 \\
& \Downarrow \\
x =& V && \because F(\varphi_1(V),\cdots,\varphi_m(V)) = k \\
\dot{F}(x) =& (x - x_1)\cdots(x - x_{m-n})\ddot{F}(x) && \{x_1,\cdots,x_{m-n}\} \subseteq \mathbb{K} \\
\ddot{F}(x) =& \frac{\dot{F}(x)}{(x - x_1)\cdots(x - x_{m-n})} && \in \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{array}{r} P(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0 \neq Q(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \end{array} \\
\ddot{F}(V) =& \frac{\dot{F}(V)}{(V - x_1)\cdots(V - x_{m-n})} = \frac{0}{(V - x_1)\cdots(V - x_{m-n})} && \Rightarrow \ddot{F}(V) = 0 \\
& \Downarrow lemma\ 7.2.1 && f_V(x) \text{ is irreducible polynomial} \in \mathbb{K}[x] \\
0 = \ddot{F}(V) =& \ddot{F}(V_1) = \cdots = \ddot{F}(V_n) \\
& \Downarrow \\
0 = \dot{F}(V) =& \dot{F}(V_1) = \cdots = \dot{F}(V_n) \\
& \Downarrow \\
0 = \dot{F}(V) =& F(\varphi_1(V),\cdots,\varphi_m(V)) - k \\
=& F(\varphi_1(V_1),\cdots,\varphi_m(V_1)) - k \\
& \vdots \\
=& F(\varphi_1(V_n),\cdots,\varphi_m(V_n)) - k \\
& \Downarrow \\
k =& F(\varphi_1(V_1),\cdots,\varphi_m(V_1)) = \cdots = F(\varphi_1(V_n),\cdots,\varphi_m(V_n)) && \forall \sigma \in S_n, F(\sigma(\boldsymbol{\alpha})) = F(\boldsymbol{\alpha}) \text{ invariant}
\end{aligned}
$$

範例 7.2.2 (Galois group of $ax^2+bx+c=0, a\neq 0$). [1, p.378～382]

$$
\begin{aligned}
f(x) =& ax^2+bx+c && \in \mathbb{Q}[x] \\
=& a(x-\alpha_1)(x-\alpha_2) \\
=& ax^2 - a(\alpha_1+\alpha_2)x + a\alpha_1\alpha_2 && \in \mathbb{Q}(\alpha_1,\alpha_2)[x] \\
& a\neq 0 && (\alpha_1-\alpha_2)\neq 0 \\
& \Downarrow \\
\alpha_1 =& \frac{-b+\sqrt{b^2-4ac}}{2a} \\
\alpha_2 =& \frac{-b-\sqrt{b^2-4ac}}{2a} \\
& \Downarrow lemma\ 7.2.2 \\
\varphi(\boldsymbol{x}) =& \varphi(x_1,x_2) && \varphi(\boldsymbol{x}) = \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{matrix} P(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}] \\ 0\neq Q(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}] \end{matrix} \\
V = \varphi(\boldsymbol{\alpha}) =& \varphi(\alpha_1,\alpha_2) && \forall \sigma_1,\sigma_2 \in S_2 [\sigma_1\neq\sigma_2 \Leftrightarrow \sigma_1(V)\neq\sigma_2(V)] \\
V_i = \varphi(\sigma_i\boldsymbol{\alpha}) =& \varphi(\sigma_i\alpha_1,\sigma_i\alpha_2) \\
& \wedge \\
f_V(x) =& (x-V_1)(x-V_2) && \text{is a minimal polynomial } \in \mathbb{Q}[x] \\
& && n = \deg f_V(x) \\
& \Downarrow lemma\ 7.2.3 \\
\alpha_1 =& \alpha_1(V) = \varphi_1(V) && i\in\mathbb{N}_{\leq 2} \\
& && \varphi_i(\boldsymbol{x}) = \frac{P_i(\boldsymbol{x})}{Q_i(\boldsymbol{x})}, \begin{matrix} P_i(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0\neq Q_i(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \end{matrix} \\
\alpha_2 =& \alpha_2(V) = \varphi_2(V) \\
& \wedge lemma\ 7.2.4 \\
\{\alpha_1,\alpha_2\} \in& \{\varphi_1(V_1),\varphi_2(V_1)\} && = \{\varphi_1(V),\varphi_2(V)\}, \quad V = V_1 \\
& \vdots \\
\{\alpha_1,\alpha_2\} \in& \{\varphi_1(V_n),,\varphi_2(V_n)\} && = \{\varphi_1(V),\varphi_2(V)\}, \quad V = V_2 \\
& \Downarrow
\end{aligned}
$$

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

[1, p.379]

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

elementary symmetric polynomials

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

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

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

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

[1, p.380～381]

範例 7.2.3 (Galois group of $x^3-2x=0$). [1, p.385～388]

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

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

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

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

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

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

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

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

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

範例 7.2.4 (Galois group of $x^4-4x^3-4x^2+8x-2=0$). MathKiwi: But why is there no quintic formula? — Galois Theory

$$
\begin{aligned}
f(x) =& x^4 - 4x^3 - 4x^2 + 8x - 2 \\
f(x) =& 0 \\
&\Downarrow \\
x \in& \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \\
\alpha_1 =& 1 + \sqrt{2} + \sqrt{3 + \sqrt{2}} \\
\alpha_2 =& 1 - \sqrt{2} + \sqrt{3 + \sqrt{2}} \\
\alpha_3 =& 1 + \sqrt{2} - \sqrt{3 + \sqrt{2}} \\
\alpha_4 =& 1 + \sqrt{2} - \sqrt{3 + \sqrt{2}}
\end{aligned}
$$

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

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

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

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

$$
\begin{aligned}
& (x - V_1)(x - (-V_1)) && (7.1) \\
=& (x - (+V_1))(x - (-V_1)) && (7.2) \\
=& \left(x - \left(-2\sqrt{2}\right)\right)\left(x - \left(+2\sqrt{2}\right)\right) && (7.3) \\
=& x^2 - 8 \qquad = f_V(x) \in \mathbb{Q}[x] && (7.4) \\
& n = \deg f_V(x) = 2 && (7.5)
\end{aligned}
$$

$$
\begin{aligned}
f(x) =& ax^2+bx+c && \in \mathbb{Q}[x] && (7.6)\\
=& a(x-\alpha_1)(x-\alpha_2) && && (7.7)\\
=& ax^2 - a(\alpha_1+\alpha_2)x + a\alpha_1\alpha_2 && \in \mathbb{Q}(\alpha_1,\alpha_2)[x] && (7.8)\\
& a \neq 0 && (\alpha_1-\alpha_2)\neq 0 && (7.9)\\
& \Downarrow && && \\
\alpha_1 =& \frac{-b+\sqrt{b^2-4ac}}{2a} && && (7.10)\\
\alpha_2 =& \frac{-b-\sqrt{b^2-4ac}}{2a} && && (7.11)\\
& \Downarrow \textit{lemma } 7.2.2 && && \\
\varphi(\boldsymbol{x}) =& \varphi(x_1,x_2) && \varphi(\boldsymbol{x}) = \frac{P(\boldsymbol{x})}{Q(\boldsymbol{x})}, \begin{matrix} P(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}] \\ 0 \neq Q(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}]\end{matrix} && (7.12)\\
V = \varphi(\boldsymbol{\alpha}) =& \varphi(\alpha_1,\alpha_2) && \forall \sigma_1,\sigma_2 \in S_2\left[\sigma_1 \neq \sigma_2 \Leftrightarrow \sigma_1(V) \neq \sigma_2(V)\right] && (7.13)\\
V_i = \varphi(\sigma_i\boldsymbol{\alpha}) =& \varphi(\sigma_i\alpha_1,\sigma_i\alpha_2) && && (7.14)\\
& \wedge && && (7.15)\\
f_V(x) =& (x-V_1)(x-V_2) && \text{is a minimal polynomial } \in \mathbb{Q}[x] && (7.16)\\
& && n = \deg f_V(x) && (7.17)\\
& \Downarrow \textit{lemma } 7.2.3 && && \\
\alpha_1 =& \alpha_1(V) = \varphi_1(V) && i \in \mathbb{N}_{\leq 2} && (7.18)\\
& && \varphi_i(\boldsymbol{x}) = \frac{P_i(\boldsymbol{x})}{Q_i(\boldsymbol{x})}, \begin{matrix} P_i(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}] \\ 0 \neq Q_i(\boldsymbol{x}) \in \mathbb{K}[\boldsymbol{x}]\end{matrix} && (7.19)\\
\alpha_2 =& \alpha_2(V) = \varphi_2(V) && && (7.20)\\
& \wedge \textit{lemma } 7.2.4 && && \\
\{\alpha_1,\alpha_2\} \in& \{\varphi_1(V_1),\varphi_2(V_1)\} && = \{\varphi_1(V),\varphi_2(V)\}, \quad V = V_1 && (7.21)\\
& \vdots && && \\
\{\alpha_1,\alpha_2\} \in& \{\varphi_1(V_n),,\varphi_2(V_n)\} && = \{\varphi_1(V),\varphi_2(V)\}, \quad V = V_2 && (7.22)\\
& \Downarrow && && \\
\mathcal{G} =& \mathcal{G}(f) = \mathrm{Gal}(f) && && (7.23)\\
=& \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \varphi_1(V) & \varphi_2(V) \end{pmatrix} \middle| V \in \{V_1, V_2\} \right\} && && (7.24)\\
=& \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\} && && (7.25)\\
=& \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\} && && (7.26)\\
=& \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \{[12],[21]\} && && (7.27)
\end{aligned}
$$

Chapter 8

linear algebra

Chapter 9

topology

9.1 metric space

Chapter 10

analysis

10.1 Hilbert space

10.2 complex analysis

10.3 Fourier analysis

Chapter 11

probability theory

定理 11.0.1 (Bonferroni inequality). *[2, p.77]*

$$\mathrm{P}(E_1 \cap E_2) \geq 1 - \mathrm{P}(E_1) - \mathrm{P}(E_2)$$

定義 11.0.1 (exponential family). A family of PDF/PMF is called exponential family if

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

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

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

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

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

Part III

physics

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. 33, 34, 36, 38, 39

[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. 49