ガロワ理論

福島洋平

大阪府立大学工学域電気電子系学類一年

2017 年 3 月 4 日

マイブーム

マイブーム $\longrightarrow$ 不可能の証明 (がんばりゃなんとかなるんじゃね!?)

フェルマーの最終定理

n≧3 で

$$X^n + Y^n = Z^n$$

を満たす自然数 X,Y,Z は存在しない.

円積問題

与えられた長さの半径を持つ円に対し、定規とコンパスによる有限回の操作でそれと面積の等しい正方形を作図することはできない.

マイブーム

根の公式の存在

5 次以上の方程式に根の公式はない.

初等関数であらわせない関数

$$\int x^x dx$$

は初等関数であらわせない.

これらに共通する理論がある. それが今回のテーマである.

本日講義する内容は

群の姿になった体の問題たちが繰り広げる大理論！

を「根の公式の存在条件」を通して説明することである.

を「根の公式の存在条件」を通して説明することである.

論文がダメになったフランスの問題児が繰り広げる大理論！

ガロワりろん

Galois Theory

講演内容

1. 方程式とその根の存在
   - 分解体, 代数学の基本定理.
2. 根の公式
   - ラグランジュ・リゾルベント
   - べき根
3. 体論
   - 「根の公式が存在すること」の体での表現
4. 群論
5. ガロワ理論

方程式とその根の存在

1 変数代数方程式 (以下方程式)

1 つの変数を含んだ多項式どうしを等号で結んだもの.
一般に変数を x として

$$\sum_{k=0}^{n} a_k x^k = 0 (a_n = 1)$$

で表すことができる.
このとき a_k は係数,n を次数, その方程式を n 次方程式ともいう.
また 方程式に代入して成り立つ定数 をその方程式の解, 根という.

解 (solutions)→ 下線部全体の集合の要素. 同じものを区別しない.
根 (roots)→ 因数分解したときの (x-ココ) 全体. 同じものを区別.

1 つ目の疑問

さてまずここで

Question-1

Q. すべての方程式は根をもつか?あとその個数は?

→ 方程式の根の存在, 個数は変数の属する集合による.

1 つ目の疑問

さてまずここで

Question-1

Q. すべての方程式は根をもつか?あとその個数は?

$\longrightarrow$ 方程式の根の存在, 個数は変数の属する集合による.

方程式の根の存在とその個数

「$3x - 1 = 0$」は

- $x \in \mathbb{N}, \mathbb{Z}$ で根なし.
- $x \in \mathbb{Q}, \mathbb{R}, \mathbb{C}$ で「$1/3$」が根.

方程式の根の存在とその個数

「$3x - 1 = 0$」は

- $x \in \mathbb{N}, \mathbb{Z}$ で根なし.
- $x \in \mathbb{Q}, \mathbb{R}, \mathbb{C}$ で「$1/3$」が根.

方程式の根の存在とその個数

「$3x - 1 = 0$」は

- $x \in \mathbb{N}, \mathbb{Z}$ で根なし.
- $x \in \mathbb{Q}, \mathbb{R}, \mathbb{C}$ で「$1/3$」が根.

方程式の根の存在とその個数

「$x^3+1=0$」は

- $x \in \mathbb{N}$ で根なし.
- $x \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ で「-1」が根.
- $x \in \mathbb{C}$ で「$-1, -\omega_3, -\omega_3^2$」が根. ただし $\omega_3 = \dfrac{-1+\sqrt{3}i}{2}$.

このように変数の属する集合ごとに大きく異なる.
ただ根の存在とその個数に関しては次のような定理が存在する.

方程式の根の存在とその個数

「$x^3 + 1 = 0$」は

- $x \in \mathbb{N}$ で根なし.
- $x \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ で「-1」が根.
- $x \in \mathbb{C}$ で「$-1, -\omega_3, -\omega_3^2$」が根. ただし $\omega_3 = \dfrac{-1 \pm \sqrt{3}i}{2}$.

このように変数の属する集合ごとに大きく異なる.
ただ根の存在とその個数に関しては次のような定理が存在する.

方程式の根の存在とその個数

「$x^3 + 1 = 0$」は

- $x \in \mathbb{N}$ で根なし.
- $x \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ で「-1」が根.
- $x \in \mathbb{C}$ で「$-1, -\omega_3, -\omega_3^2$」が根. ただし $\omega_3 = \dfrac{-1 \pm \sqrt{3}i}{2}$.

このように変数の属する集合ごとに大きく異なる.
ただ根の存在とその個数に関しては次のような定理が存在する.

方程式の根の存在とその個数

「$x^3 + 1 = 0$」は

- $x \in \mathbb{N}$ で根なし.
- $x \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ で「-1」が根.
- $x \in \mathbb{C}$ で「$-1, -\omega_3, -\omega_3^2$」が根. ただし $\omega_3 = \dfrac{-1 \pm \sqrt{3}i}{2}$.

このように変数の属する集合ごとに大きく異なる.
ただ根の存在とその個数に関しては次のような定理が存在する.

分解体, 代数学の基本定理.

分解体

F 係数方程式にはその根を含む $L \supseteq F$ な分解体 L がある.

代数学の基本定理

$\mathbb{C}$ 係数 n 次方程式は $\mathbb{C}$ の範囲に重複含め n 個の根を持つ.

1 つ目の疑問の解答

Question-1

Q. すべての方程式は根をもつか?あとその個数は?

Answer-1

方程式の根の存在, 個数は変数の属する集合による.
分根体, 代数学の基本定理.

今回は係数, 変数ともに $\mathbb{C}$ の範囲の場合を考える.

根の公式

2 つ目の疑問

前項より任意の方程式に根があることがわかった.
では方程式から具体的に根を得られる方法は存在するのか?
方程式は係数を定めれば根が決まる.⟶ 材料は係数.
係数はなにができるか?⟶ 四則演算.

2 つ目の疑問

前項より任意の方程式に根があることがわかった.
では方程式から具体的に根を得られる方法は存在するのか?
方程式は係数を定めれば根が決まる.⟶ 材料は係数.
係数はなにができるか?⟶ 四則演算.

2 つ目の疑問

前項より任意の方程式に根があることがわかった.
では方程式から具体的に根を得られる方法は存在するのか?
方程式は係数を定めれば根が決まる.→ 材料は係数.
係数はなにができるか?→ 四則演算.

2 つ目の疑問

前項より任意の方程式に根があることがわかった.
では方程式から具体的に根を得られる方法は存在するのか?
方程式は係数を定めれば根が決まる.⟶ 材料は係数.
係数はなにができるか?⟶ 四則演算.

2 つ目の疑問

前項より任意の方程式に根があることがわかった.
では方程式から具体的に根を得られる方法は存在するのか?
方程式は係数を定めれば根が決まる.$\longrightarrow$ 材料は係数.
係数はなにができるか?$\longrightarrow$ 四則演算.

2つ目の疑問

前項より任意の方程式に根があることがわかった.
では方程式から具体的に根を得られる方法は存在するのか?
方程式は係数を定めれば根が決まる.$\longrightarrow$ 材料は係数.
係数はなにができるか?$\longrightarrow$ 四則演算.

2 つ目の疑問

Question-2

Q. 与えられた方程式から根をもれなく, 係数の四則で表せないか?

1 次方程式においてこれは容易に実現される.
つまり 1 次方程式「$x + a = 0$」において根は「$-a$」.
次に 2 次方程式を考える.

2 次方程式の根の公式～根と係数の関係～

任意の 2 次方程式に次の定理が成り立つ.

根と係数の関係 (2 次)

2 次方程式 $x^2 + ax + b = 0$ においてその根を α, β とすると

$$a = -(\alpha + \beta)$$
$$b = \alpha\beta$$

このとき右辺はの α, β のすべての入れ替えで不変である.
このように文字の入れ替えにたいして不変な式を対称式という.

つきまとう対称性

対称式

ある有理式がある n 個の文字のすべての入れ替えに対して不変のとき, その多項式を (n 次) 対称式という.

そして対称式どうしの四則演算には次の定理が成り立つ.

対称式どうしの四則演算

対称式どうしの四則演算の結果もまた対称式である.

しつこいさすが対称性しつこい

「根と係数の関係」から係数は根 α, β の対称式

$\longrightarrow$ さっきの定理から係数の四則演算の結果は根 α, β の対称式.

$\longrightarrow$ 対称式でない「α」「β」は表せない!

これは 2 次以降の方程式一般にいえる.

しつこいさすが対称性しつこい

「根と係数の関係」から係数は根 α, β の対称式
$\longrightarrow$ さっきの定理から係数の四則演算の結果は根 α, β の対称式.
$\longrightarrow$ 対称式でない「α」「β」は表せない!
これは 2 次以降の方程式一般にいえる.

しつこいさすが対称性しつこい

「根と係数の関係」から係数は根 α, β の対称式
$\longrightarrow$ さっきの定理から係数の四則演算の結果は根 α, β の対称式.
$\longrightarrow$ 対称式でない「α」「β」は表せない!
これは 2 次以降の方程式一般にいえる.

対称性には勝てなかったよ

Question-2

Q. 与えられた方程式から根をもれなく, 係数の四則で表せないか?

Answer-2

2 次以降は一般には無理.

これでは我々は方程式に対してあまりにも貧弱である.
より一般に根を得るには四則演算以外に「新たな操作」が必要.
現状把握のために係数の四則演算で何が表せるかを考える.

対称式の基本定理

実は根と係数の関係に現れる対称式「$\alpha+\beta$」「$\alpha\beta$」は
(2 次の) 基本対称式とよばれ次の強力な定理が成り立つ.

対称式の基本定理

任意の対称式は基本対称式の四則で表される.

よって係数の四則で「α」「β」の対称式ならなんでも表せる.
$\rightarrow$「ある操作をすれば対称式でなくなる」対称式が欲しい
$\rightarrow$「ラグランジュ・リゾルベント」

対称式の基本定理

実は根と係数の関係に現れる対称式「$\alpha+\beta$」「$\alpha\beta$」は
(2 次の) 基本対称式とよばれ次の強力な定理が成り立つ.

対称式の基本定理

任意の対称式は基本対称式の四則で表される.

よって係数の四則で「α」「β」の対称式ならなんでも表せる.
$\rightarrow$「ある操作をすれば対称式でなくなる」対称式が欲しい
$\rightarrow$「ラグランジュ・リゾルベント」

対称式の基本定理

実は根と係数の関係に現れる対称式「$\alpha+\beta$」「$\alpha\beta$」は
(2 次の) 基本対称式とよばれ次の強力な定理が成り立つ.

対称式の基本定理

任意の対称式は基本対称式の四則で表される.

よって係数の四則で「α」「β」の対称式ならなんでも表せる.
$\longrightarrow$「ある操作をすれば対称式でなくなる」対称式が欲しい
$\longrightarrow$「ラグランジュ・リゾルベント」

ラグランジュ・リゾルベント

2 次のラグランジュ・リゾルベント (以下リゾルベント)

$$\alpha - \beta$$

これは 1 次の対称性と 2 次の対称性をつなぐものになっている.
というのもリゾルベント自身は対称式ではないが 2 乗した

$$(\alpha - \beta)^2$$

は対称式になっている. 対称式であれば係数で表せる. 実際
$(\alpha - \beta)^2 = \{-(\alpha + \beta)\}^2 - 4\alpha\beta = a^2 - 4b$

式の対称性を下げるのが得意なフレンズ

あとは x^2 から x を与える操作 を認めれば四則では到達できなった
対称でない式の世界へと踏み出せるのだ. この 操作 を**べき根**という.

対称性を落とす「べき根」

べき根

与えられた x から n 乗すると x になる y のうち 1 つを与える写像.

$$f(x) = \sqrt[n]{x}$$

で表す.n=2 のとき 2 を省略して $\sqrt{x}$ とも表す.

これを操作に認めると

$$\sqrt{a^2 - 4b} = \sqrt{(\alpha - \beta)^2} = \alpha - \beta$$

と係数から対称式でない式を生み出せる.

2 次方程式の根の公式

前ページの結果を用いて

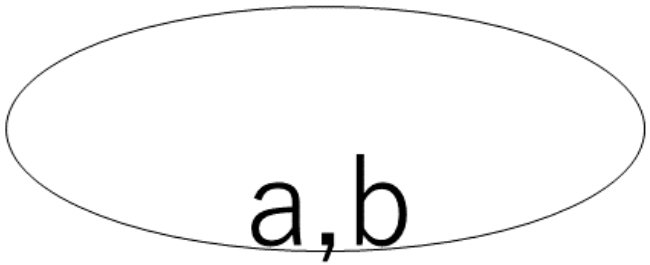
$$\alpha = \frac{\alpha+\beta}{2} + \frac{\alpha-\beta}{2} = \frac{-a}{2} + \frac{\sqrt{a^2-4b}}{2}$$
$$\beta = \frac{\alpha+\beta}{2} - \frac{\alpha-\beta}{2} = \frac{-a}{2} - \frac{\sqrt{a^2-4b}}{2}$$

根を係数の四則演算とべき根であらわしたものを根の公式という.

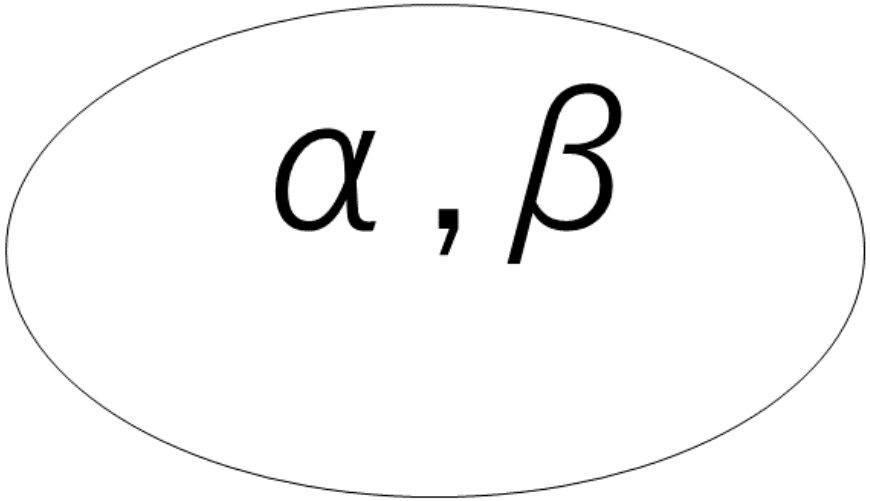
Question-2 改

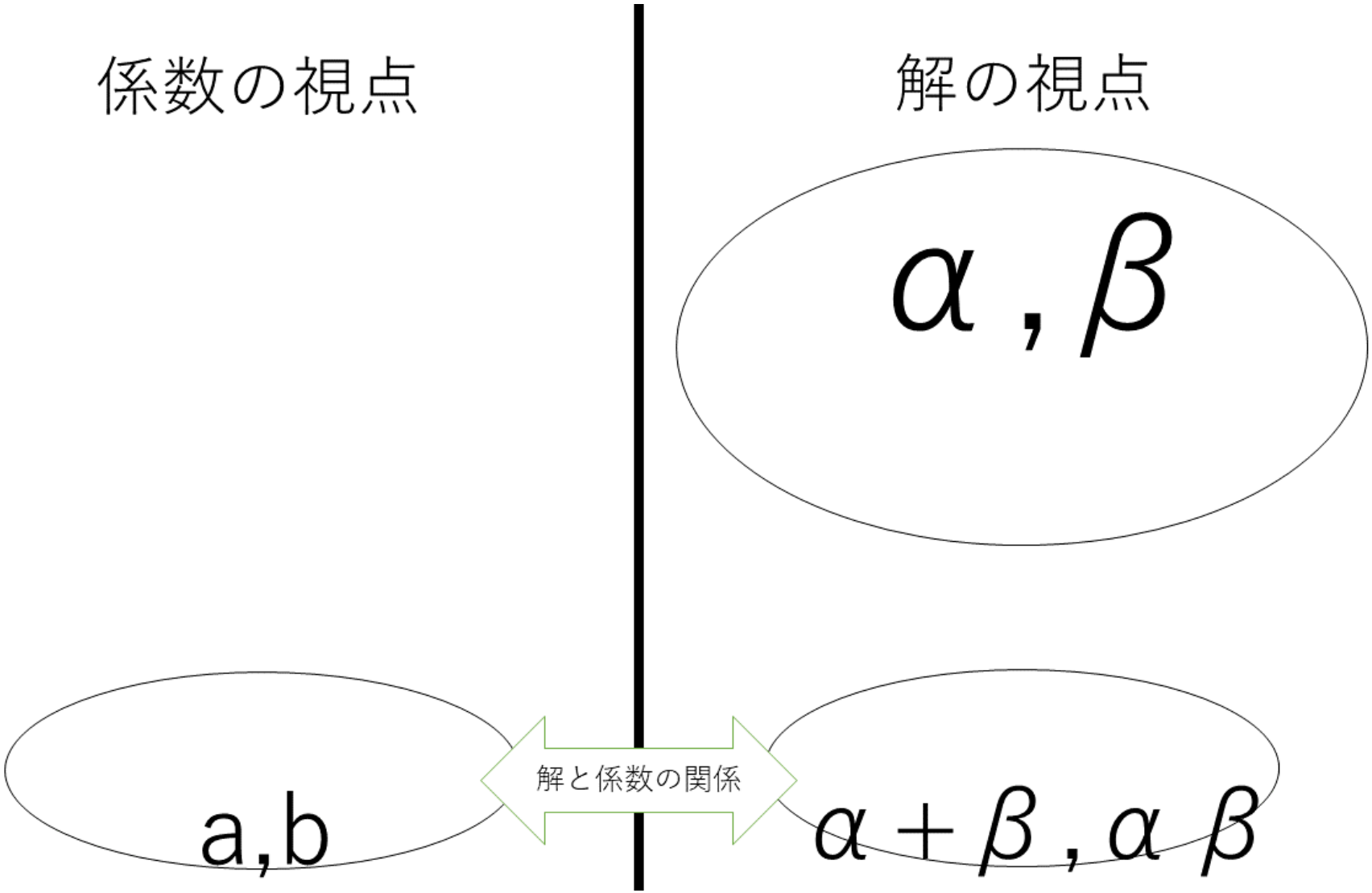
Q. 与えられた方程式に根の公式は存在するか?

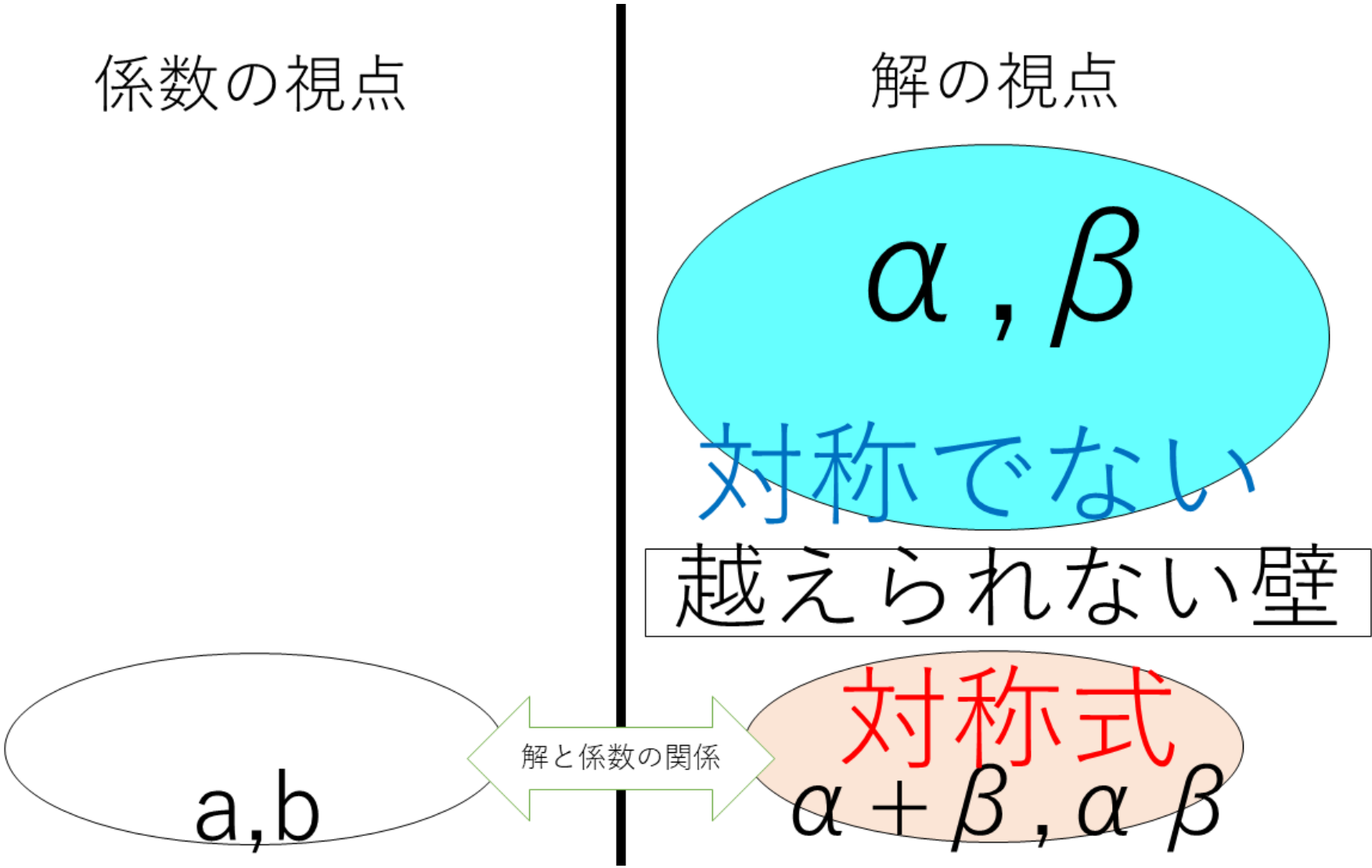
係数の視点

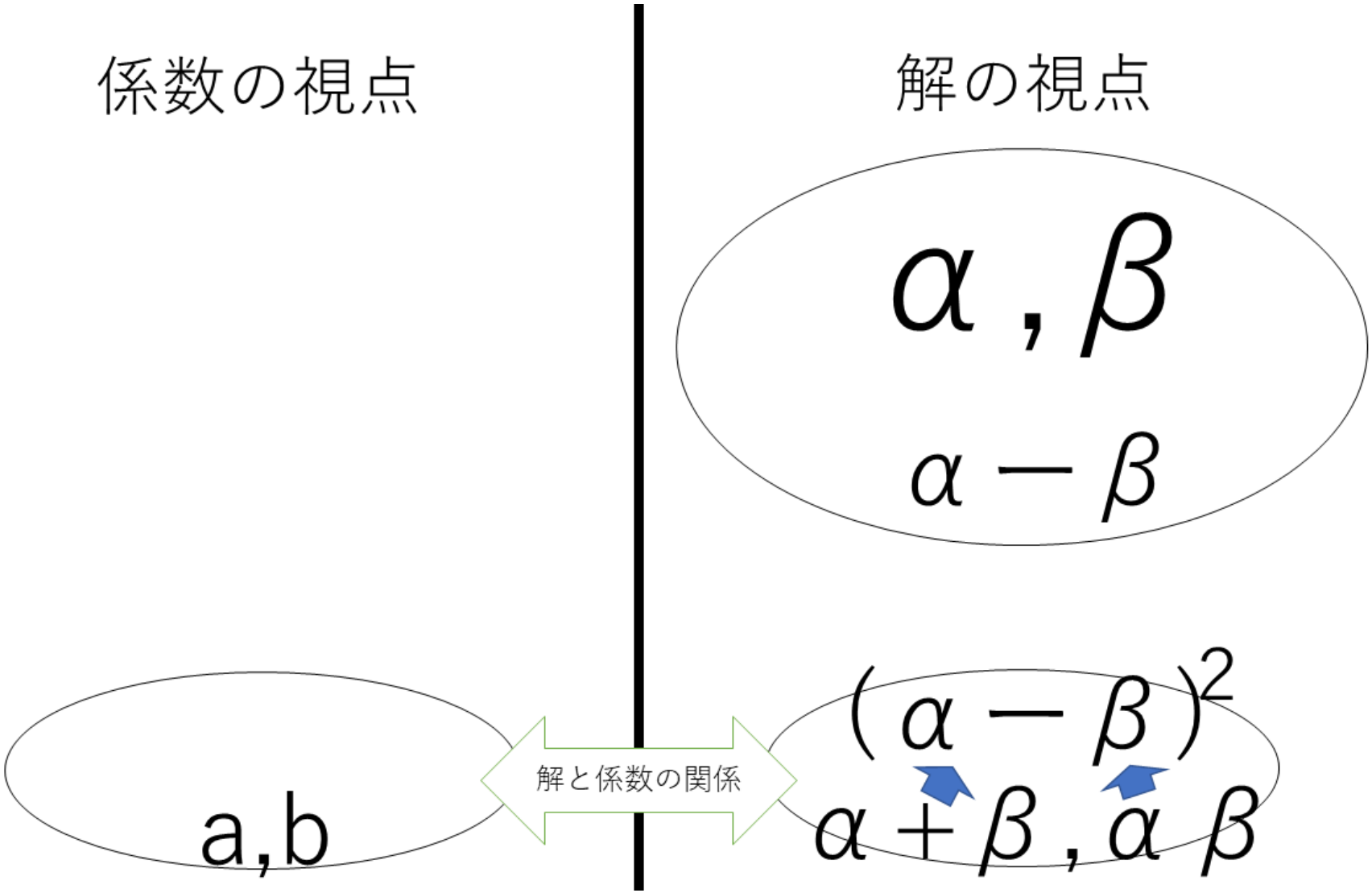


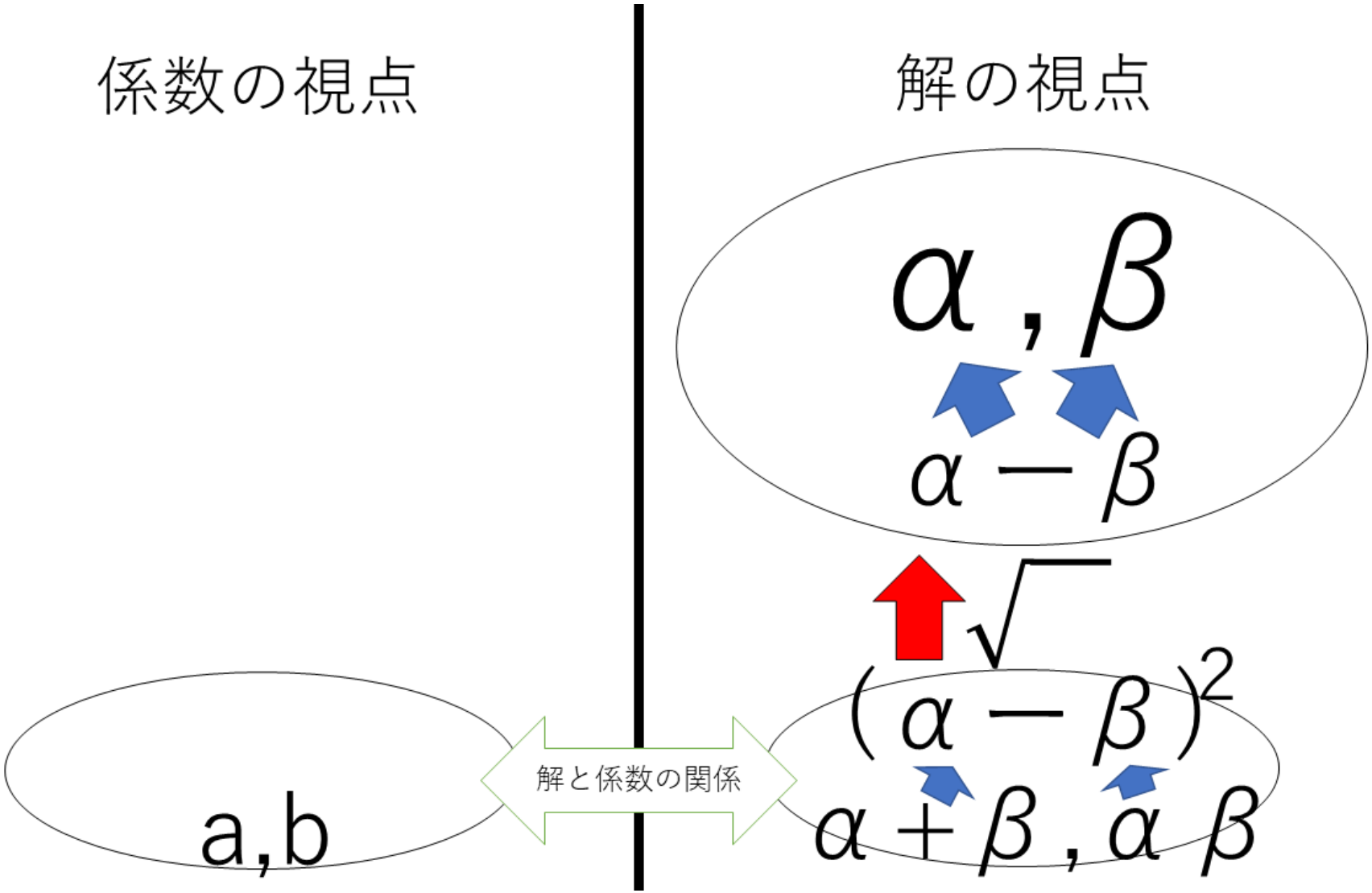
解の視点

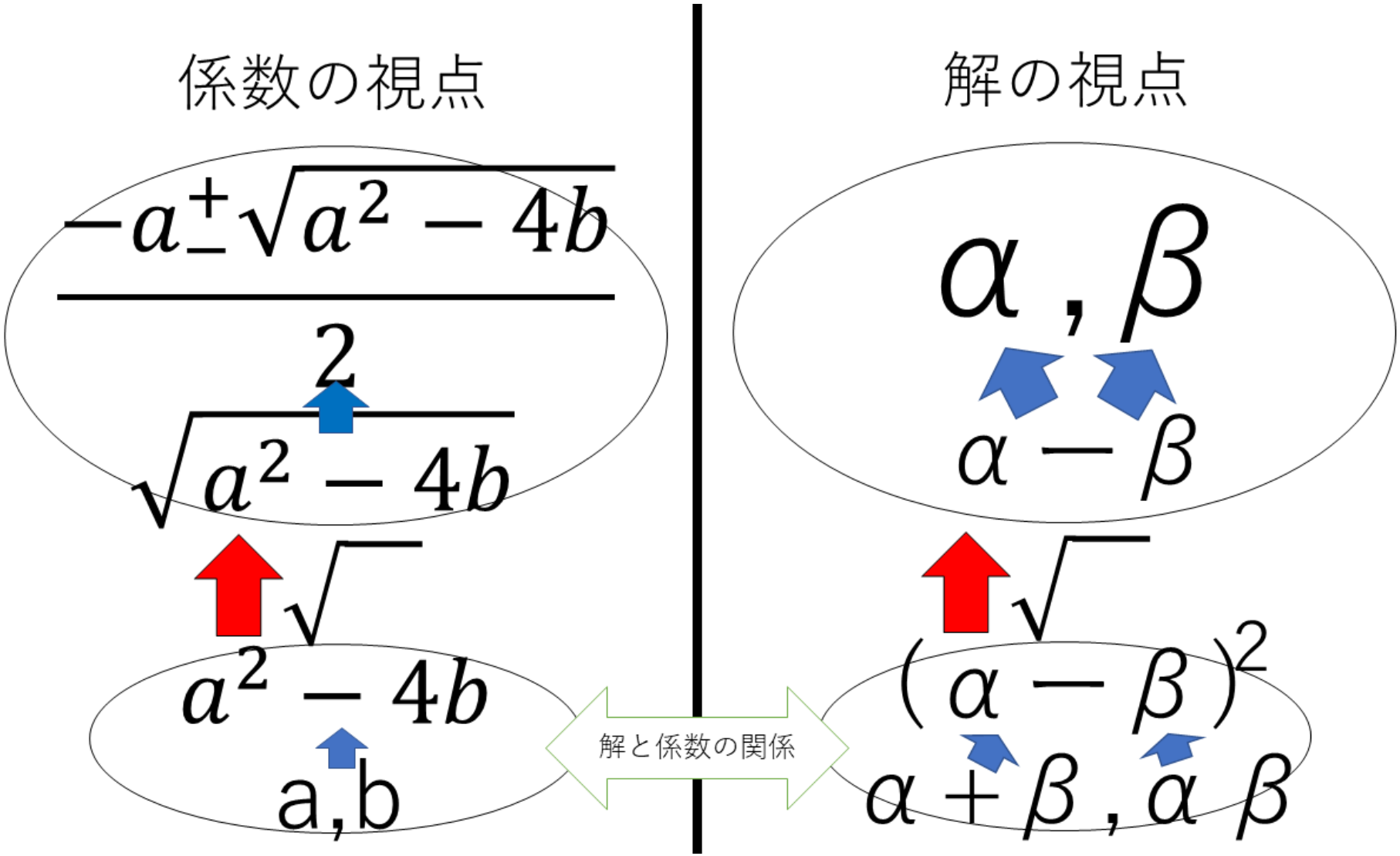



係数の視点
解の視点
α , β
a,b
解と係数の関係
α + β , α β


係数の視点
解の視点
α , β
対称でない
越えられない壁
a,b
解と係数の関係
対称式
α + β , α β


係数の視点
解の視点
α , β
α − β
a,b
解と係数の関係
(α − β)²
α + β , α β


係数の視点
解の視点
α , β
α − β
√
(α − β)²
α + β , α β
a,b
解と係数の関係


係数の視点
$\frac{-a \pm \sqrt{a^2-4b}}{2}$
$\sqrt{a^2-4b}$
a^2-4b
a,b
解と係数の関係
解の視点
α, β
$\alpha-\beta$
$(\alpha-\beta)^2$
$\alpha+\beta, \alpha\beta$

3 次方程式の根の公式

まずは基本となる根と係数の関係を思いだそう.

根と係数の関係 (3 次)

3 次方程式 $x^3 + ax^2 + bx + c = 0$ においてその根を α, β, γ とすると

$$
\begin{aligned}
a &= -(\alpha + \beta + \gamma) \\
b &= \alpha\beta + \beta\gamma + \gamma\alpha \\
c &= -\alpha\beta\gamma
\end{aligned}
$$

右辺は 3 次の基本対称式になっている.

3 次のラグランジュ・リゾルベント

今回のリゾルベントを与えよう.

3 次のラグランジュ・リゾルベント

$$L_1 = \alpha + \omega_3\beta + \omega_3^2\gamma$$
$$L_2 = \alpha + \omega_3^2\beta + \omega_3\gamma$$

こいつらの 3 乗の対称性を調べてみる.

L_1^3, L_2^3 の対称性

$$
\begin{aligned}
L_1^3 &= (\alpha+\omega_3\beta+\omega_3^2\gamma)^3 \\
&\to (\alpha+\omega_3\beta+\omega_3^2\gamma)^3 \to L_1^3 \\
&\to (\beta+\omega_3\gamma+\omega_3^2\alpha)^3 \to L_1^3 \\
&\to (\gamma+\omega_3\alpha+\omega_3^2\beta)^3 \to L_1^3 \\
&\to (\alpha+\omega_3\gamma+\omega_3^2\beta)^3 \to L_2^3 \\
&\to (\gamma+\omega_3\beta+\omega_3^2\alpha)^3 \to L_2^3 \\
&\to (\beta+\omega_3\alpha+\omega_3^2\gamma)^3 \to L_2^3
\end{aligned}
$$

$$
\begin{aligned}
L_2^3 &= (\alpha+\omega_3^2\beta+\omega_3\gamma)^3 \\
&\to (\alpha+\omega_3^2\beta+\omega_3\gamma)^3 \to L_2^3 \\
&\to (\beta+\omega_3^2\gamma+\omega_3\alpha)^3 \to L_2^3 \\
&\to (\gamma+\omega_3^2\alpha+\omega_3\beta)^3 \to L_2^3 \\
&\to (\alpha+\omega_3^2\gamma+\omega_3\beta)^3 \to L_1^3 \\
&\to (\gamma+\omega_3^2\beta+\omega_3\alpha)^3 \to L_1^3 \\
&\to (\beta+\omega_3^2\alpha+\omega_3\gamma)^3 \to L_1^3
\end{aligned}
$$

対称式ではないが, 確かに対称性は下がっている. すなわち α, β, γ の３次の対称性が L_1^3, L_2^3 の２次の対称性に落とし込まれている.

$(L_1^3 - L_2^3)^2$ 対称性

1 次の対称性と 2 次の対称性をつなぐものは 2 次のリゾルベント, すなわちその 2 数の差であった. 実際

$$(L_1^3 - L_2^3)^2$$

$$= 9(\omega_3^2 + \omega_3 - 2)\{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)\}^2$$

$$= -27\{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)\}^2 \leftarrow \text{対称式!!}$$

$(L_1^3 - L_2^3)^2$ は対称式なので係数 a, b, c で表せる.

$(L_1^3 - L_2^3)^2$ 対称性

1 次の対称性と 2 次の対称性をつなぐものは 2 次のリゾルベント, すなわちその 2 数の差であった. 実際

$$(L_1^3 - L_2^3)^2$$

$$= 9(\omega_3^2 + \omega_3 - 2)\{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)\}^2$$

$$= -27\{(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)\}^2 \leftarrow \text{対称式!!}$$

$(L_1^3 - L_2^3)^2$ は対称式なので係数 a, b, c で表せる.

$(L_1^3 - L_2^3)^2$ 対称性

べき根をとって $L_1^3 - L_2^3$ を得られれば 2 次方程式のときにならって

$$L_1^3 = \frac{L_1^3 + L_2^3}{2} + \frac{L_1^3 - L_2^3}{2}$$
$$L_2^3 = \frac{L_1^3 + L_2^3}{2} - \frac{L_1^3 - L_2^3}{2}$$

で L_1^3, L_2^3 を得る. これらのべき根をとれば L_1, L_2 が得られ,

3 次方程式の根の公式

$$\begin{aligned}\alpha &= \frac{\alpha+\beta+\gamma}{3}+\frac{\alpha+\omega_3\beta+\omega_3^2\gamma}{3}+\frac{\alpha+\omega_3^2\beta+\omega_3\gamma}{3}\\ &= \frac{-a}{3}+\frac{L_1}{3}+\frac{L_2}{3}\end{aligned}$$

同様に

$$\beta = \frac{-a}{3}+\frac{\omega_3^2 L_1}{3}+\frac{\omega_3 L_2}{3}$$

$$\gamma = \frac{-a}{3}+\frac{\omega_3 L_1}{3}+\frac{\omega_3^2 L_2}{3}$$

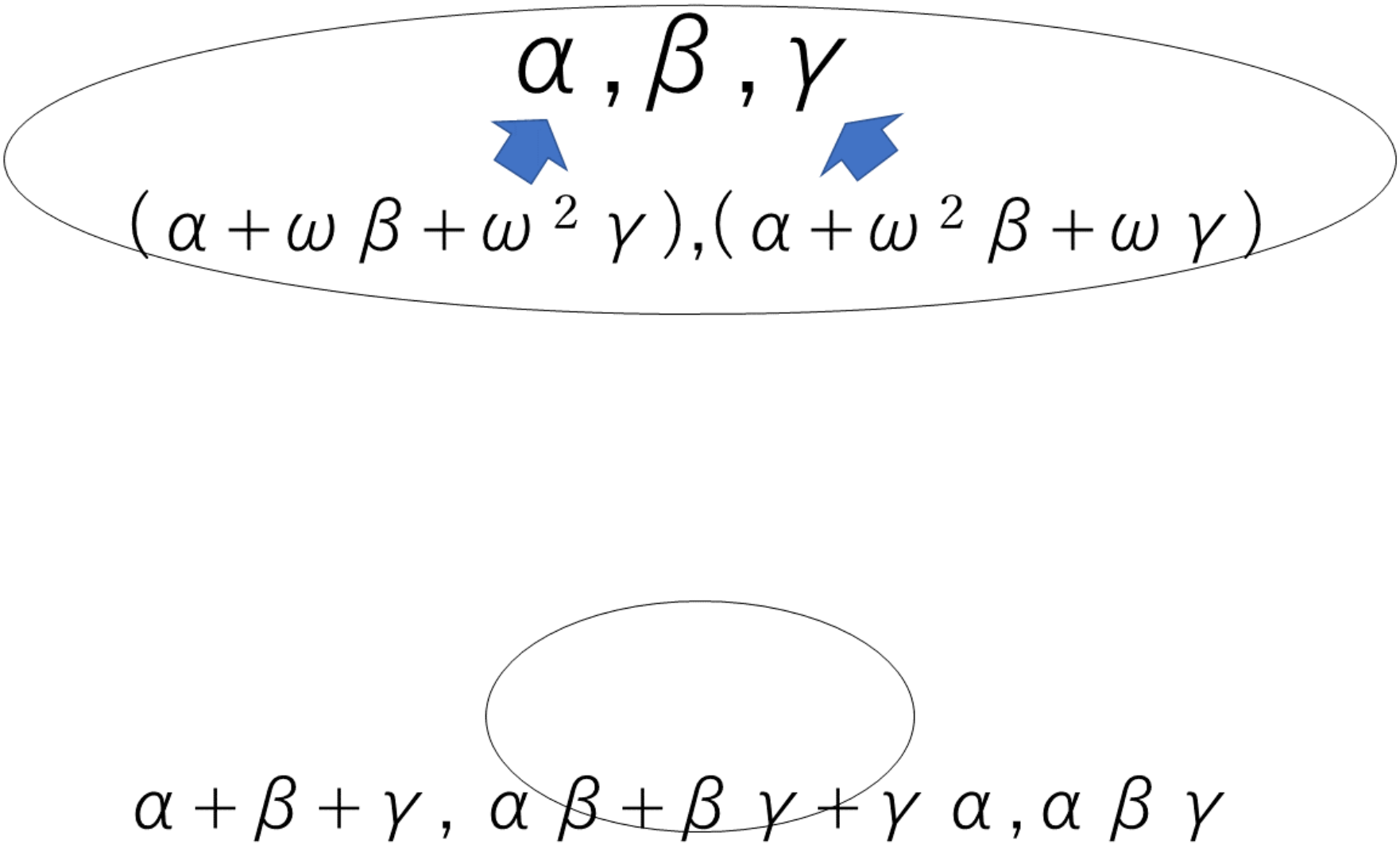
で根の公式が得られた.

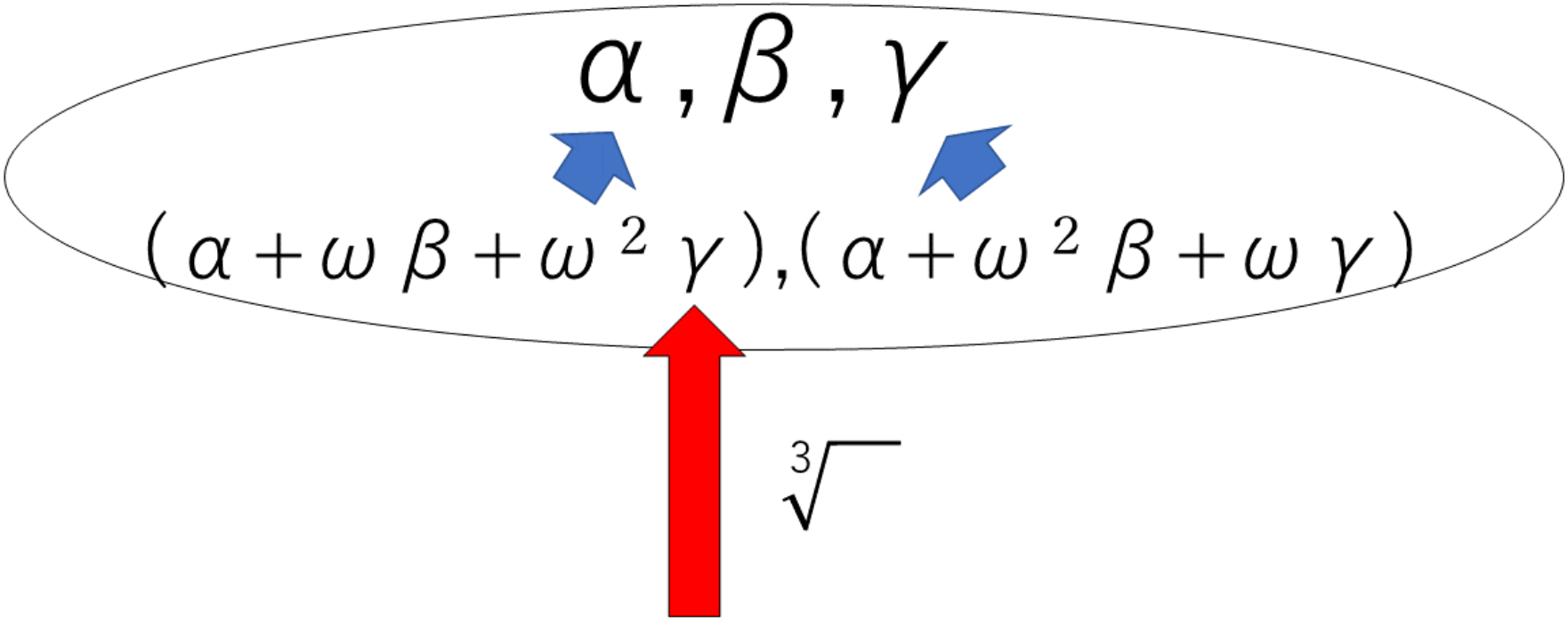
3 次方程式の根の公式

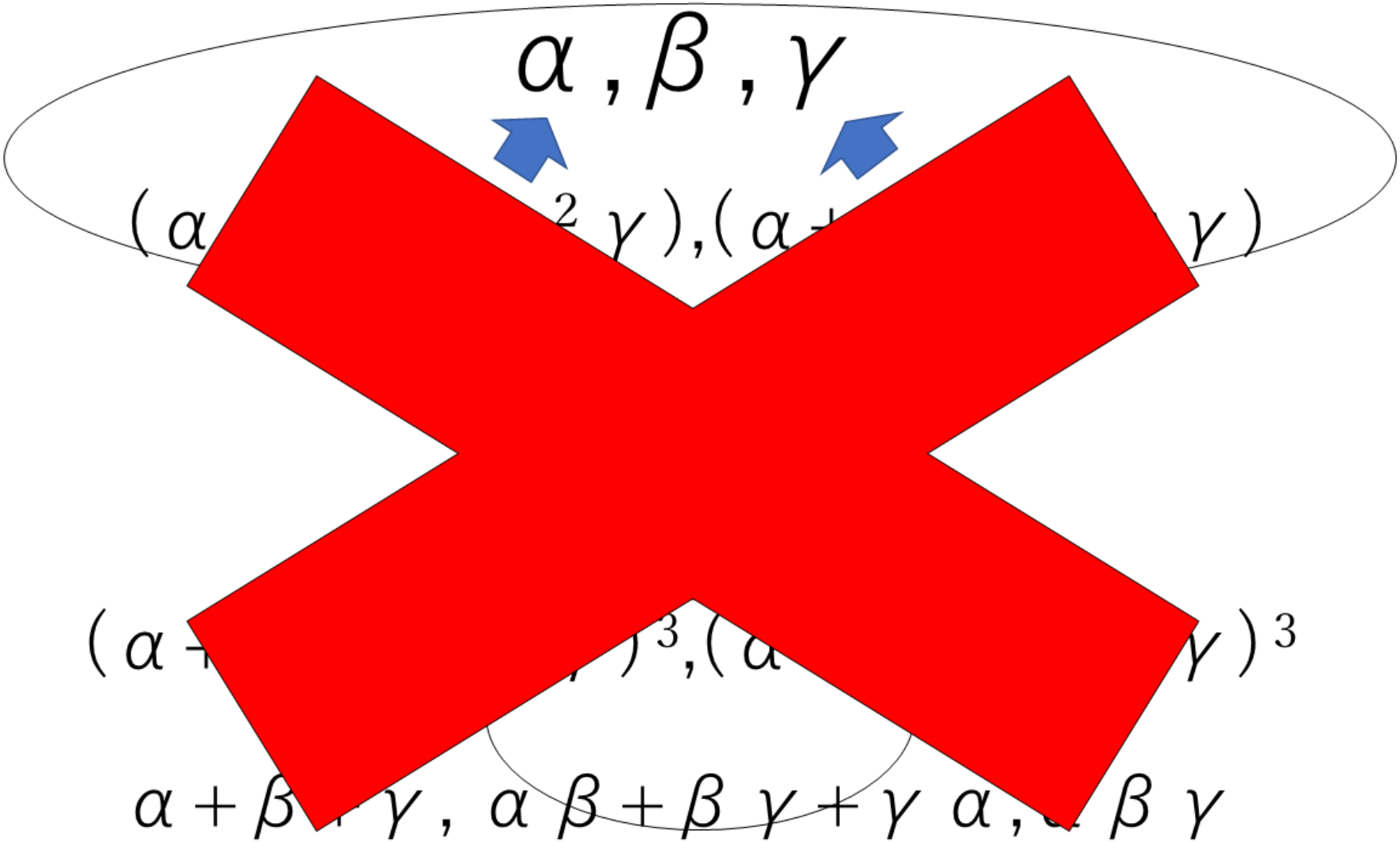
$$x = -\frac{a}{3} - \frac{\sqrt[3]{2}(-a^2+3b)}{3\sqrt[3]{-2a^3+9ab-27c+3\sqrt{3}\sqrt{-a^2b^2+4b^3+4a^3c-18abc+27c^2}}} + \frac{\sqrt[3]{-2a^3+9ab-27c+3\sqrt{3}\sqrt{-a^2b^2+4b^3+4a^3c-18abc+27c^2}})}{3\sqrt[3]{2}},$$

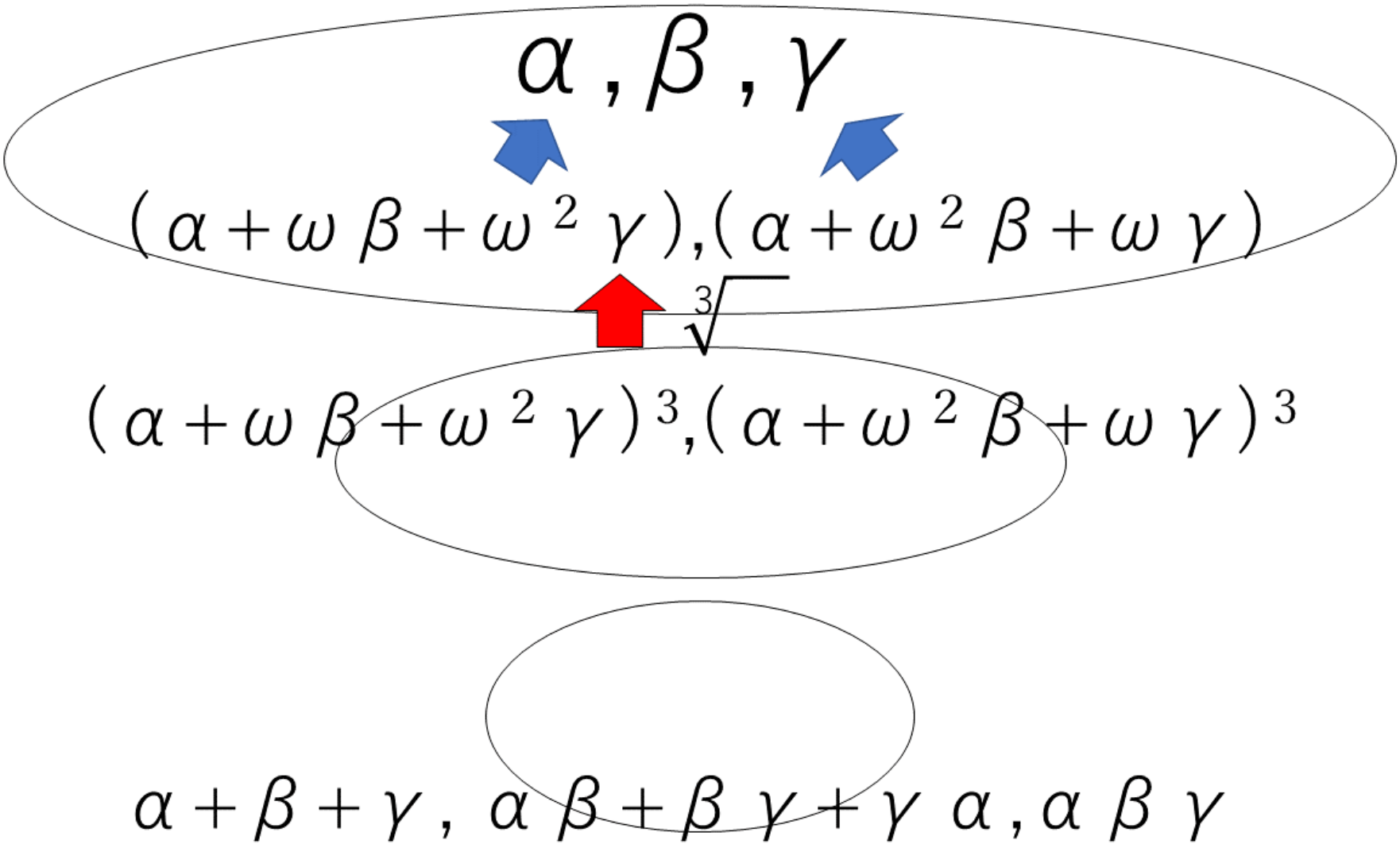
$$-\frac{a}{3} + \frac{(1+i\sqrt{3})(-a^2+3b)}{3\sqrt[3]{4}\sqrt[3]{-2a^3+9ab-27c+3\sqrt{3}\sqrt{-a^2b^2+4b^3+4a^3c-18abc+27c^2}}} - \frac{(1-i\sqrt{3})\sqrt[3]{-2a^3+9ab-27c+3\sqrt{3}\sqrt{-a^2b^2+4b^3+4a^3c-18abc+27c^2}}}{6\sqrt[3]{2}},$$

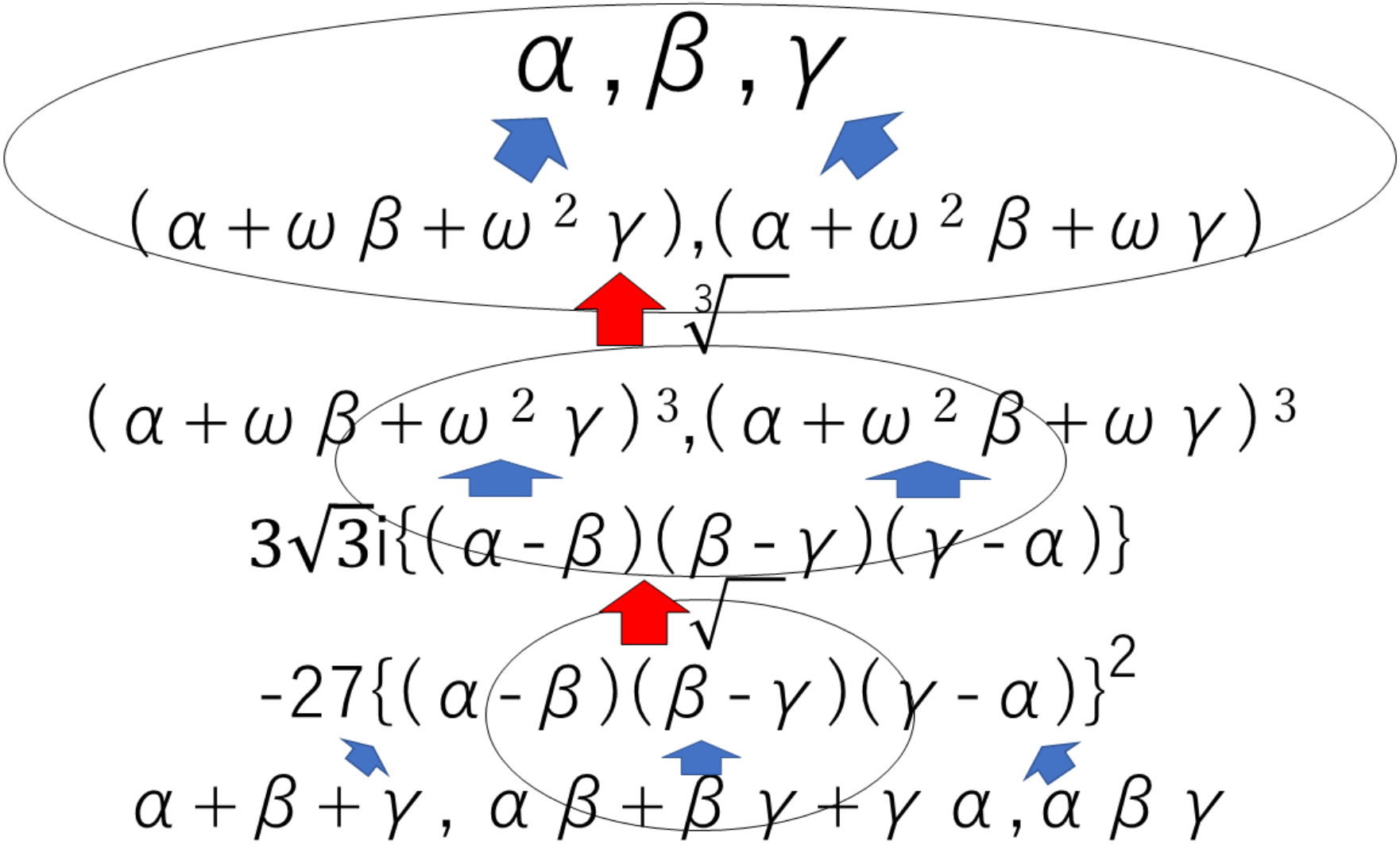
$$-\frac{a}{3} + \frac{(1-i\sqrt{3})(-a^2+3b)}{3\sqrt[3]{4}\sqrt[3]{-2a^3+9ab-27c+3\sqrt{3}\sqrt{-a^2b^2+4b^3+4a^3c-18abc+27c^2}}} - \frac{(1+i\sqrt{3})\sqrt[3]{-2a^3+9ab-27c+3\sqrt{3}\sqrt{-a^2b^2+4b^3+4a^3c-18abc+27c^2}}}{6\sqrt[3]{2}}$$


α, β, γ
$(\alpha + \omega\,\beta + \omega^2\,\gamma), (\alpha + \omega^2\,\beta + \omega\,\gamma)$
$\alpha + \beta + \gamma,\ \alpha\,\beta + \beta\,\gamma + \gamma\,\alpha,\ \alpha\,\beta\,\gamma$


α, β, γ
$(\alpha + \omega\beta + \omega^2\gamma), (\alpha + \omega^2\beta + \omega\gamma)$
$\sqrt[3]{}$
$(\alpha + \omega\beta + \omega^2\gamma)^3, (\alpha + \omega^2\beta + \omega\gamma)^3$
$\alpha + \beta + \gamma,\ \alpha\beta + \beta\gamma + \gamma\alpha,\ \alpha\beta\gamma$


α , β , γ


α, β, γ
$(\alpha+\omega\beta+\omega^2\gamma), (\alpha+\omega^2\beta+\omega\gamma)$
$\sqrt[3]{}$
$(\alpha+\omega\beta+\omega^2\gamma)^3, (\alpha+\omega^2\beta+\omega\gamma)^3$
$\alpha+\beta+\gamma,\ \alpha\beta+\beta\gamma+\gamma\alpha, \alpha\beta\gamma$


α , β , γ
(α + ω β + ω 2 γ),(α + ω 2 β + ω γ)
3
√
(α + ω β + ω 2 γ) 3,(α + ω 2 β + ω γ) 3
3√3i{(α - β)(β - γ)(γ - α)}
√
-27{(α - β)(β - γ)(γ - α)}2
α + β + γ , α β + β γ + γ α , α β γ

4 次方程式,5 次方程式の根の公式

4 次方程式 $\longrightarrow$ 一般にリゾルベントが存在し, 根の公式が存在する.
5 次以上の方程式 $\longrightarrow$ 一般にはリゾルベントが存在せず根の公式も存在しない.

4 次方程式の根の公式

$$x = -\frac{a}{4}$$
$$-\frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{\sqrt[3]{2}(b^2 - 3ac + 12d)}{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}} + \frac{3\sqrt[3]{2}}{\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}}}$$
$$-\frac{1}{2}\sqrt{\frac{a^2/2 - 4b/3 - \sqrt[3]{2}(b^2 - 3ac + 12d)}{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}} - \frac{3\sqrt[3]{2}}{\sqrt[3]{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}}}$$
$$-\frac{}{4\sqrt{a^2/4 - 2b/3 + \{\sqrt[3]{2}(b^2 - 3ac + 12d)\}/\{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc +}}}}$$

みたいなのが 4 つ.

2 つ目の疑問改の解答 (仮)

Question-2 改

Q. 与えられた方程式に根の公式は存在するか?

Answer-2 改 (仮)

4 次までなら一般に存在する.5 次以上なら一般には存在しない.
存在するかどうかはリゾルベントが鍵を握ってるぽい.

今回は根の公式の存在条件をガロア理論を使って説明する.
そのためにはまず「根の公式の存在条件」をより正確に記述する必要がある.
その記述する言語は四則演算で閉じた集合をあらわす「体」である.
以下「体」の用語を紹介し,「根の公式の存在条件」をより正確に記述する.

体論

「体」と書いて「タイ」と読む.

体

四則演算で閉じた集合を体という.

例:数体 ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$ など), 素体 ($\mathbb{Q}, \mathbb{Z}/p^*$), 対称式全体.

部分体

体の部分集合で体であるものを部分体という.

四則ではもう大きくなれない体を大きくすることを考える.

よそからスカウトしてくるイメージ

単拡大体

体 F と a を含む最小の体を F に a を添加した単拡大体 F(a) という.

- 一般には a の有理式全体で表される.
- a が F 係数方程式の根のとき F 係数 a の線形結合で表せる.

同様に $F(a_1, a_2, \cdots, a_n)$ も定義される.

例:$\mathbb{Q}(\sqrt{2}) = \{q_1 + q_2\sqrt{2}; q_1, q_2 \in \mathbb{Q}\}$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{q_1 + q_2\sqrt{2} + q_3\sqrt{3} + q_4\sqrt{6}; q_1, \cdots, q_4 \in \mathbb{Q}\}$

$$\mathbb{Q}(\pi) = \left\{ \frac{\sum_{j=0}^{m} q_j \pi^j}{\sum_{i=0}^{n} p_i \pi^i}; p_1, \cdots, p_n, q_1, \cdots, q_m \in \mathbb{Q}, n, m \in \mathbb{N} \right\}$$

べき根拡大

単拡大の特別な例としてべき根拡大がある.

$x^n = a$ の根

$x^n = a$ の根の 1 つ $\sqrt[n]{a}$ とすると残りの根は

$$\sqrt[n]{a}\omega_n^k (k = 1, 2, \cdots, n-1)$$

ただし $\omega_n = cos(2\pi/n) + isin(2\pi/n) = exp(2\pi i/n)$.

べき根拡大

F が 1 の n 乗根 ω_n を含むとする. このとき $x^n = a$ の根の 1 つ $\sqrt[n]{a}$ とすると $F(\sqrt[n]{a})$ は $x^n = a$ の根をすべて含む (ガロワ拡大). このような拡大をべき根拡大という.

肉体言語ではありません

「根の公式が存在する」ことを体の言葉で表現すると

「根の公式が存在すること」の体での表現

方程式の係数を $a_1, \cdots, a_n$ として $F = \mathbb{Q}(a_1, \cdots, a_n)$ とする.
そして F に方程式の根を全て添加した体を K(ガロワ拡大体) とする.
このとき部分体の列

$$E = F_k \supset F_{k-1} \supset \cdots \supset F_0 = F$$

で
(i)$E \supset K$
(ii)F_i にある元 f_i があり,$F_{i+1} = F_i(\sqrt[k]{f_i})$
を満たすものがある.

この f_i はラグランジュリゾルベントにあたるものである.

「根の公式が存在すること」の体での表現を得られた訳だが, このままでは曖昧である.
ガロワ理論ではこの「体の問題」を「群の問題」に落とし込んで非常にスマートな形で「根の公式が存在すること」を表現する. 以下必要な群論の用語を説明する.

群論

群の定義

群

ある集合 G が性質 (i)(ii)(iii) を持つ二項演算 $\circ : G \times G \to G$ を供えているとき, その集合を群という.
(i) 結合則:$\forall x, y, z[x \circ (y \circ z) = (x \circ y) \circ z]$
(ii) 単位元の存在:$\exists e \forall x[x \circ e = x]$
(iii) 逆元の存在:$\forall x \exists x^{-1}[x \circ x^{-1} = e]$

3 次の対称群

n 個のものの入れ替えを表す写像全体を n 次の対称群 S_n という.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right.$$

$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$= \{e, s, s^2, t, s^2t, st\}$$

3 次対称群の乗積表

右 \ 左	e	s	s^2	t	s^2t	st
e	e	s	s^2	t	s^2t	st
s	s	s^2	e	s^2t	st	t
s^2	s^2	e	s	st	t	s^2t
t	t	st	s^2t	e	s^2	s
s^2t	s^2t	t	st	s	e	s^2
st	st	s^2t	t	s^2	s	e

可換じゃない

部分群, 巡回群

部分群

群の部分集合で群であるものを部分群という.

巡回群

全ての元をある 1 つの元のべき乗で表すことができる群を巡回群という.

$$H_e = \{e\}, H_s = \{s, s^2, s^3 = e\}, H_t = \{t, t^2 = e\},$$
$$H_{st} = \{st, (st)^2 = e\}, H_{s^2t} = \{s^2t, (s^2t)^2 = e\}$$

部分群に元を左からかましてみた件

$$H_s = \{e, s, s^2\}$$
$$eH_s = \{ee, es, es^2\} = \{e, s, s^2\}$$
$$sH_s = \{se, ss, ss^2\} = \{s, s^2, s^3\} = \{s, s^2, e\}$$
$$s^2H_s = \{s^2e, s^2s, s^2s^2\} = \{s^2, s^3, s^4\} = \{s^2, e, s\}$$
$$tH_s = \{te, ts, ts^2\} = \{t, s^2t, st\}$$
$$s^2tH_s = \{s^2te, s^2ts, s^2ts^2\} = \{s^2t, st, t\}$$
$$stH_s = \{ste, sts, sts^2\} = \{st, t, s^2t\}$$

これらを (左) 剰余類という.

かましてみたら群が分割された件

$H_s = \{e, s, s^2\}$

$eH_s = \{e, s, s^2\}$ $\quad tH_s = \{t, s^2t, st\}$

$sH_s = \{s, s^2, e\}$ $\quad s^2tH_s = \{s^2t, st, t\}$

$s^2H_s = \{s^2, e, s\}$ $\quad stH_s = \{st, t, s^2t\}$

$$S_3 = \{e, s, s^2, t, s^2t, st\}$$

$$S_3 = eH_s + tH_s$$

$$S_3/H_s = \{eH_s, tH_s\}$$

剰余類

剰余類

G を群,H をその部分群とすると g∈G に対し

$$gH=\{gh;h\in H\}$$

を g を含む H の左剰余類という.

同様に右剰余類も定義される.

剰余類による分割

2 つの左剰余類 g_1H, g_2H には「一致」か「共通部分が空」しかない.
そして任意の元 g は gH に属するので剰余類は G を分割する.

剰余類は群を分割する.

群 G は部分群 H ごとに次のように分割される.(+ は直和)

$$\begin{aligned} G &= g_1H + g_2H + \cdots + g_nH \\ &= Hg_1' + Hg_2' + \cdots + Hg_n' \end{aligned}$$

このとき G を分割する左右の剰余類全体それぞれを

$$\begin{aligned} G/H &= \{g_1H, g_2H, \cdots, g_nH\} \\ H\backslash G &= \{Hg_1', Hg_2', \cdots, Hg_n'\} \end{aligned}$$

で定義する.

逆に右からかましてみた件

$H_s = \{e, s, s^2\}$

$H_s e = \{e, s, s^2\}$ $\quad H_s t = \{t, st, s^2 t\}$

$H_s s = \{s, s^2, e\}$ $\quad H_s s^2 t = \{s^2 t, t, st\}$

$H_s s^2 = \{s^2, e, s\}$ $\quad H_s st = \{st, s^2 t, t\}$

$$S_3 = \{e, s, s^2, t, s^2 t, st\}$$

$$S_3 = H_s e + H_s t$$

$$H_s \backslash S_3 = \{H_s e, H_s t\}$$

左右の剰余類を見比べる.

左右の剰余類が完全に一致

$$
\begin{aligned}
eH_s &= \{e, s, s^2\} \\
sH_s &= \{s, s^2, e\} \\
s^2H_s &= \{s^2, e, s\} \\
tH_s &= \{t, s^2t, st\} \\
s^2tH_s &= \{s^2t, st, t\} \\
stH_s &= \{st, t, s^2t\}
\end{aligned}
\quad = \quad
\begin{aligned}
H_se &= \{e, s, s^2\} \\
H_ss &= \{s, s^2, e\} \\
H_ss^2 &= \{s^2, e, s\} \\
H_st &= \{t, st, s^2t\} \\
H_ss^2t &= \{s^2t, t, st\} \\
H_sst &= \{st, s^2t, t\}
\end{aligned}
$$

$$\sigma H_s = H_s\sigma$$

このような部分群を正規部分群という.

正規部分群じゃない例

$$eH_t = \{e, t\}$$
$$sH_t = \{s, st\}$$
$$s^2H_t = \{s^2, s^2t\}$$
$$tH_= \{t, e\}$$
$$s^2tH_t = \{s^2t, s^2\}$$
$$stH_t = \{st, s\}$$

$$\neq$$

$$H_te = \{e, t\}$$
$$H_ts = \{s, s^2t\}$$
$$H_ts^2 = \{s^2, st\}$$
$$H_tt = \{t, e\}$$
$$H_ts^2t = \{s^2t, s\}$$
$$H_tst = \{st, s^2\}$$

$$\sigma H_s \neq H_s\sigma$$

正規部分群

正規部分群

全ての元で左右の剰余類が一致する部分群を正規部分群という.

正規部分群 H において G/H は群となる. これを商群という.

$$\begin{aligned}(g_1H)(g_2H) &= g_1(Hg_2)H \\ &= g_1(g_2H)H \\ &= (g_1g_2)(HH) \\ &= g_1g_2H\end{aligned}$$

で演算を定義すると, 単位元は eH,gH の逆元は $g^{-1}H$.

G が可換なら部分群はすべて正規部分群になる.

商群

$S_3/H_s = \{eH_s, tH_s\}$
$(eH_s)(eH_s) = eH_s$
$(eH_s)(tH_s) = (tH_s)(eH_s) = tH_s$
$(tH_s)(tH_s) = t^2H_s = eH_s$

右 \ 左	eH_s	tH_s
eH_s	eH_s	tH_s
tH_s	tH_s	eH_s

S_3/H_s は巡回群になっている.

群のまとめ

- 群 $\longrightarrow$ イイ感じの 2 項演算を持っている.
- 部分群 $\longrightarrow$ 群の部分集合で群なもの.
- 巡回群 $\longrightarrow$ 全ての元がある 1 つの元のべき乗な群.
- 正規部分群 $\longrightarrow$ その割り算が群になっている.

群のまとめ

- 群 $\longrightarrow$ イイ感じの 2 項演算を持っている.
- 部分群 $\longrightarrow$ 群の部分集合で群なもの.
- 巡回群 $\longrightarrow$ 全ての元がある 1 つの元のべき乗な群.
- 正規部分群 $\longrightarrow$ その割り算が群になっている.

群のまとめ

- 群 $\longrightarrow$ イイ感じの 2 項演算を持っている.
- 部分群 $\longrightarrow$ 群の部分集合で群なもの.
- 巡回群 $\longrightarrow$ 全ての元がある 1 つの元のべき乗な群.
- 正規部分群 $\longrightarrow$ その割り算が群になっている.

群のまとめ

- 群 $\longrightarrow$ イイ感じの 2 項演算を持っている.
- 部分群 $\longrightarrow$ 群の部分集合で群なもの.
- 巡回群 $\longrightarrow$ 全ての元がある 1 つの元のべき乗な群.
- 正規部分群 $\longrightarrow$ その割り算が群になっている.

ガロワ理論

「どうがた」じゃなくて「どうけい」

同型

2 つの体 K,E 間の全射な写像 $\sigma : K \to E$ が (i)(ii)(iii) を満たすとき σ を同型という.
(i)$\sigma(0) = 0 \Leftrightarrow$ 単射である.
(ii)$\sigma(x+y) = \sigma(x) + \sigma(y)$
(iii)$\sigma(xy) = \sigma(x)\sigma(y)$
特に K=E のときは自己同型という. また自己同型で K の部分体 F の元すべてを変えないものを F 上の自己同型という.

任意の同型が持つ性質として例えば

- 有理数を不変にする.

がある.

$\mathbb{Q}(\sqrt{2})$ の自己同型

$\mathbb{Q}(\sqrt{2}) = \{q_1 + q_2\sqrt{2}; q_1, q_2 \in \mathbb{Q}\}$ の自己同型を考える.

とりあえず「$q_1 + q_2\sqrt{2}$」に σ を作用させると

$$\sigma(q_1 + q_2\sqrt{2}) = q_1 + q_2\sigma(\sqrt{2})$$

ここで「$\sqrt{2}^2 - 2 = 0$」に σ を作用させると

$\{\sigma(\sqrt{2})\}^2 - 2 = 0 \Leftrightarrow \sigma(\sqrt{2})$ は $x^2 - 2 = 0$ の根.

$\Rightarrow \mathbb{Q}(\sqrt{2})$ の自己同型は恒等写像 e と「$\sigma(\sqrt{2}) = -\sqrt{2}$」な σ.

代数的な数とその最小方程式

代数的な数とその最小多項式

体 F 係数方程式の根である数 a を F 上代数的な数という.
このとき a が根となる F 係数多項式のうち次数が最小であるものを a の F 上の最小多項式という.

例:$\sqrt{2}$ は $\mathbb{Q}$ 上代数的な数で最小多項式は $x^2 - 2$.
$1 + i$ は $\mathbb{Q}$ 上代数的な数で最小多項式は $x^2 - 2x + 2$.

共役数

代数的な数 a の最小多項式の a 以外の根を F 上の共役数という.

例:$\sqrt{2}$ の $\mathbb{Q}$ 上共役数は $-\sqrt{2}$. $1 + i$ の $\mathbb{Q}$ 上共役数は $1 - i$.

同型写像の性質

F 上の自己同型は F 上代数的数を自身かその共役数へ移す.

F 上代数的数 a の最小多項式を $\sum_{k=1}^{n} f_k x^k$ とすると

$$\sigma\left(\sum_{k=1}^{n} f_k a^k\right) = \sum_{k=1}^{n} f_k \{\sigma(a)\}^k = \sigma(0) = 0$$

つまり $\sigma(a)$ は a の最小多項式 $\sum_{k=1}^{n} f_k x^k$ の根.

ガロワ群

F のガロワ拡大体の F 上自己同型全体はその合成で群になる.
この群をガロワ群という.

ガロワ群

K を F のガロワ拡大体とする. このとき K の F 上の自己同型全体を K の F 上のガロワ群 Gal(K/F) という.

例:$\mathbb{Q}(\sqrt{2})$ は $x^2 - 2 = 0$ の根を全て含むので $\mathbb{Q}$ のガロワ拡大体.
($-1 \in \mathbb{Q}$ よりべき根拡大でもある.)
このとき Gal($\mathbb{Q}(\sqrt{2})/\mathbb{Q}$)=$\{e, \sigma\}(\cong S_2)$

例:一般の 3 次方程式のガロワ群

一般の 3 次方程式 $x^3 + ax^2 + bx + c = 0$ のガロワ群を考える.
方程式の根を α, β, γ とする. このとき

$$F = \mathbb{Q}(a, b, c), K = F(\alpha, \beta, \gamma)$$

で K は F 係数 α, β, γ の多項式全体となる. つまり F 上自己同型は

$$\sigma(\alpha), \sigma(\beta), \sigma(\gamma)$$

の行き先を決定すれば定まる. そして α, β, γ は F 上代数的なので,
結局「α, β, γ の入れ替え」に帰着され

$$\mathrm{Gal}(K/F) \cong S_3$$

となる.

ガロワ対応

ガロワ対応

ガロワ拡大体の部分体とガロワ群の部分群は 1:1 に対応する.
すなわち F のガロワ拡大体を K,G=Gal(K/F) として
(i)K の部分体 E に対し,K の E 上自己同型全体は G の部分群.
(ii)G の部分群 H に対し,H の元で不変となる元全体は K の部分体.

$$\begin{cases} K \supset E \supset F \\ \{e\} \subset H \subset G \end{cases}$$

正規性定理

正規性定理

F のガロワ拡大体を K,G=Gal(K/F) として

K の中間体 E が F のガロワ拡大.
⇔E に対応する G の部分群 H が正規.

このとき Gal(E/F)≅G/H=Gal(K/F)/Gal(K/E).

$$\begin{cases} K \leftarrow E \xleftarrow{Galois} F \\ \{e\} \subset H \subset G \end{cases}$$

べき根拡大のガロワ群

べき根拡大のガロワ群

べき根拡大のガロワ群は巡回群.

ガロワ群が巡回群

1 の n 乗根を含んだ F のガロワ群 Gal(K/F) が位数 n の巡回群ならそれはべき根拡大. すなわちある f が存在し K=F($\sqrt[n]{f}$)

例:$\mathbb{Q}(\sqrt{2})$ は $-1 \in \mathbb{Q}$ よりべき根拡大.
このとき Gal($\mathbb{Q}(\sqrt{2})/\mathbb{Q}$) $= \{e, \sigma\} = \{\sigma^2, \sigma\}$

「体」での表現を「群」での表現へ

「根の公式が存在すること」の体での表現

方程式の係数を $a_1, \cdots, a_n$ として $F = \mathbb{Q}(a_1, \cdots, a_n)$, その方程式における F のガロワ拡大体を K とする. このとき部分体の列

$$E = F_k \supset F_{k-1} \supset \cdots \supset F_0 = F$$

で
(i)$E \supset K$
(ii)F_i にある元 f_i があり,$F_{i+1} = F_i(\sqrt[j]{f_i})$(べき根拡大)
を満たすものがある.

これをガロワ理論で「群の言葉」に翻訳する. 今回は省略するが得られる結果は実は必要十分条件になっている.

「根の公式が存在すること」の群での表現

方程式がべき根で根けるとする. すなわち

$$E = F_k \supset F_{k-1} \supset \cdots \supset F_0 = F$$
$$\text{(i)} E \supset K$$
$$\text{(ii)} F_{i+1} = F(\sqrt[k]{f_i}) \text{(べき根拡大)}$$
$$\text{(iii)} E \text{ は } F \text{ のガロワ拡大}$$

ガロワ対応を以下のように与える.

$$\begin{cases} E = F_k \supset F_{k-1} \supset \cdots \supset F_0 = F \\ \{e\} = H_k \subset H_{k-1} \subset \cdots \subset H_0 = G \end{cases}$$

ここで G=Gal(E/F)

「根の公式が存在すること」の群での表現

部分列をとってきて

$$\begin{cases} E \supset F_{i+1} \supset F_i \\ \{e\} \subset H_{i+1} \subset H_i \end{cases}$$

F_{i+1} は F_i のべき根拡大すなわちガロワ拡大 $\Rightarrow$ H_{i+1} は正規.
$\Rightarrow$ 正規性定理より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$.
$\Rightarrow$ べき根拡大より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$ は巡回群.

$$G = H_0 \supset H_1 \supset \cdots \supset H_k = \{e\}$$
(i)H_{i+1} は H_i の正規部分群.(ii)H_i/H_{i+1} は巡回群.

「根の公式が存在すること」の群での表現

部分列をとってきて

$$\begin{cases} E \supset F_{i+1} \supset F_i \\ \{e\} \subset H_{i+1} \subset H_i \end{cases}$$

F_{i+1} は F_i のべき根拡大すなわちガロワ拡大 $\Rightarrow$ H_{i+1} は正規.

$\Rightarrow$ 正規性定理より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$.

$\Rightarrow$ べき根拡大より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$ は巡回群.

$$G = H_0 \supset H_1 \supset \cdots \supset H_k = \{e\}$$

(i)H_{i+1} は H_i の正規部分群.(ii)H_i/H_{i+1} は巡回群.

「根の公式が存在すること」の群での表現

部分列をとってきて

$$\begin{cases} E \supset F_{i+1} \supset F_i \\ \{e\} \subset H_{i+1} \subset H_i \end{cases}$$

F_{i+1} は F_i のべき根拡大すなわちガロワ拡大 $\Rightarrow$ H_{i+1} は正規.
$\Rightarrow$ 正規性定理より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$.
$\Rightarrow$ べき根拡大より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$ は巡回群.

$$G = H_0 \supset H_1 \supset \cdots \supset H_k = \{e\}$$
(i)H_{i+1} は H_i の正規部分群.(ii)H_i/H_{i+1} は巡回群.

「根の公式が存在すること」の群での表現

部分列をとってきて

$$\begin{cases} E \supset F_{i+1} \supset F_i \\ \{e\} \subset H_{i+1} \subset H_i \end{cases}$$

F_{i+1} は F_i のべき根拡大すなわちガロワ拡大 $\Rightarrow$ H_{i+1} は正規.
$\Rightarrow$ 正規性定理より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$.
$\Rightarrow$ べき根拡大より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$ は巡回群.

$$G = H_0 \supset H_1 \supset \cdots \supset H_k = \{e\}$$
(i)H_{i+1} は H_i の正規部分群.(ii)H_i/H_{i+1} は巡回群.

「根の公式が存在すること」の群での表現

部分列をとってきて

$$\begin{cases} E \supset F_{i+1} \supset F_i \\ \{e\} \subset H_{i+1} \subset H_i \end{cases}$$

F_{i+1} は F_i のべき根拡大すなわちガロワ拡大 $\Rightarrow$ H_{i+1} は正規.
$\Rightarrow$ 正規性定理より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$.
$\Rightarrow$ べき根拡大より $\mathrm{Gal}(F_{i+1}/F_i) \cong H_i/H_{i+1}$ は巡回群.

$$G = H_0 \supset H_1 \supset \cdots \supset H_k = \{e\}$$
(i)H_{i+1} は H_i の正規部分群.(ii)H_i/H_{i+1} は巡回群.

可解群

可解群

群 G が次のような部分群の列を持つとき G を可解群という.

$$G = H_0 \supset H_1 \supset \cdots \supset H_k = \{e\}$$

(i)H_{i+1} は H_i の正規部分群. (ii)H_i/H_{i+1} は巡回群.

可解群の商群

可解群の商群も可解群.

2つ目の疑問改の解答

$$\begin{cases} E \supset K \supset F \\ \{e\} \subset \mathbf{Gal(K/F)} \subset \mathrm{Gal(E/F)} = \mathbf{G} \end{cases}$$

K は F のガロワ拡大 $\Rightarrow$Gal(K/F) は Gal(E/F) の正規部分群.
$\Rightarrow$ 正規性定理より Gal(K/F) $\cong$Gal(E/F)/Gal(E/K).
$\Rightarrow$Gal(E/F) が可解より Gal(K/F) も可解.

根の公式の存在条件

方程式に根の公式が存在する.$\Rightarrow$ その方程式のガロア群が可解.

そして実はこれは必要十分条件になっている.

2つ目の疑問改の解答

$$\begin{cases} E \supset K \supset F \\ \{e\} \subset \mathbf{Gal(K/F)} \subset \mathrm{Gal(E/F)} = \mathbf{G} \end{cases}$$

K は F のガロワ拡大 $\Rightarrow$Gal(K/F) は Gal(E/F) の正規部分群.

$\Rightarrow$ 正規性定理より Gal(K/F) $\cong$Gal(E/F)/Gal(E/K).

$\Rightarrow$Gal(E/F) が可解より Gal(K/F) も可解.

根の公式の存在条件

方程式に根の公式が存在する.$\Rightarrow$ その方程式のガロア群が可解.

そして実はこれは必要十分条件になっている.

2つ目の疑問改の解答

$$\begin{cases} E \supset K \supset F \\ \{e\} \subset \mathbf{Gal(K/F)} \subset \mathrm{Gal(E/F)} = \mathbf{G} \end{cases}$$

K は F のガロワ拡大 $\Rightarrow$Gal(K/F) は Gal(E/F) の正規部分群.
$\Rightarrow$ 正規性定理より Gal(K/F) $\cong$Gal(E/F)/Gal(E/K).
$\Rightarrow$Gal(E/F) が可解より Gal(K/F) も可解.

根の公式の存在条件

方程式に根の公式が存在する.$\Rightarrow$ その方程式のガロア群が可解.

そして実はこれは必要十分条件になっている.

2つ目の疑問改の解答

$$\begin{cases} E \supset K \supset F \\ \{e\} \subset \mathbf{Gal(K/F)} \subset \mathrm{Gal(E/F)} = \mathbf{G} \end{cases}$$

K は F のガロワ拡大 $\Rightarrow$Gal(K/F) は Gal(E/F) の正規部分群.
$\Rightarrow$ 正規性定理より Gal(K/F) $\cong$Gal(E/F)/Gal(E/K).
$\Rightarrow$Gal(E/F) が可解より Gal(K/F) も可解.

根の公式の存在条件

方程式に根の公式が存在する.$\Rightarrow$ その方程式のガロア群が可解.

そして実はこれは必要十分条件になっている.

2つ目の疑問改の解答

$$\begin{cases} E \supset K \supset F \\ \{e\} \subset \mathbf{Gal(K/F)} \subset \mathrm{Gal(E/F)} = \mathbf{G} \end{cases}$$

K は F のガロワ拡大 $\Rightarrow$Gal(K/F) は Gal(E/F) の正規部分群.
$\Rightarrow$ 正規性定理より Gal(K/F) $\cong$Gal(E/F)/Gal(E/K).
$\Rightarrow$Gal(E/F) が可解より Gal(K/F) も可解.

根の公式の存在条件

方程式に根の公式が存在する.$\Rightarrow$ その方程式のガロア群が可解.

そして実はこれは必要十分条件になっている.

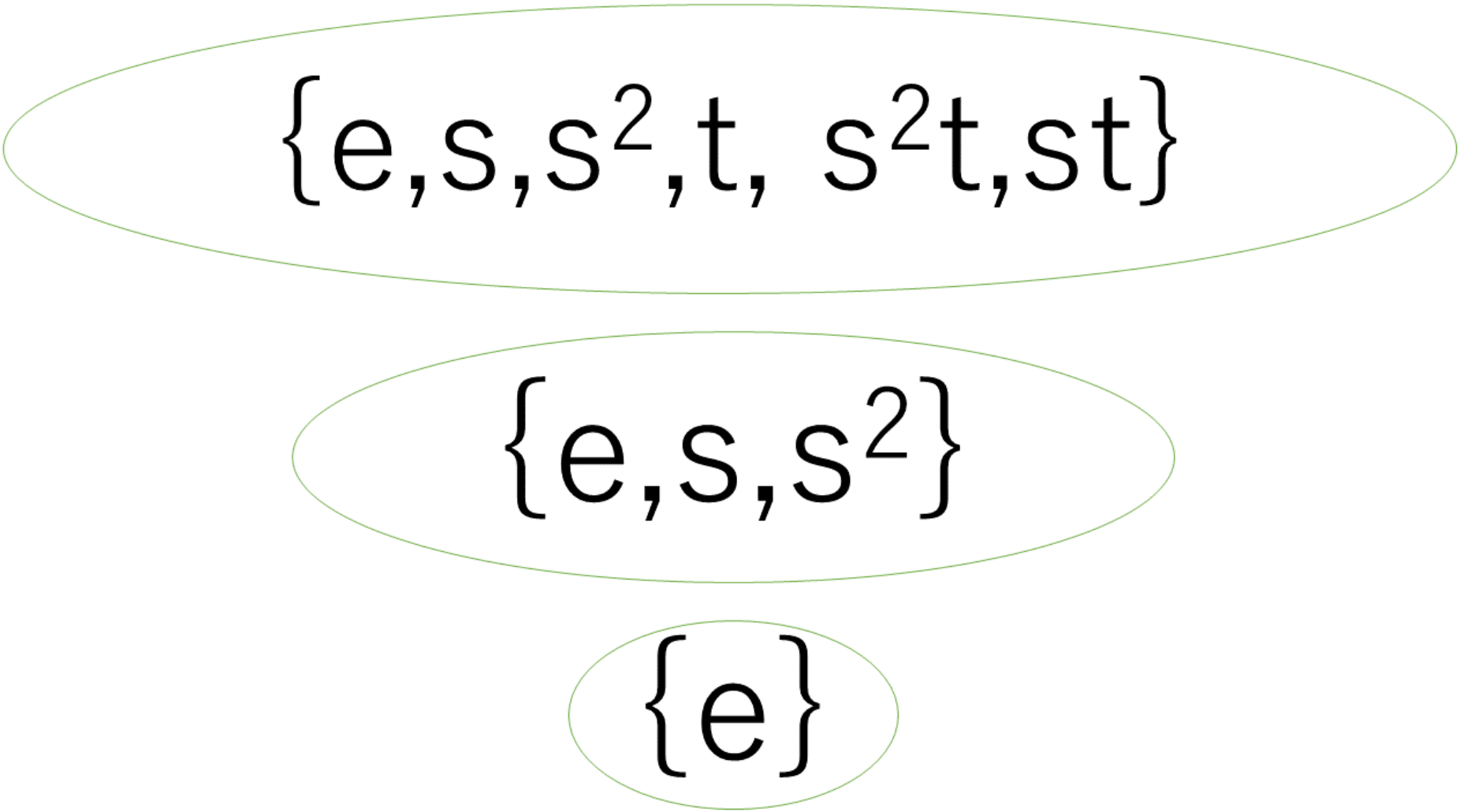
これが根の公式の存在条件だ!!!!

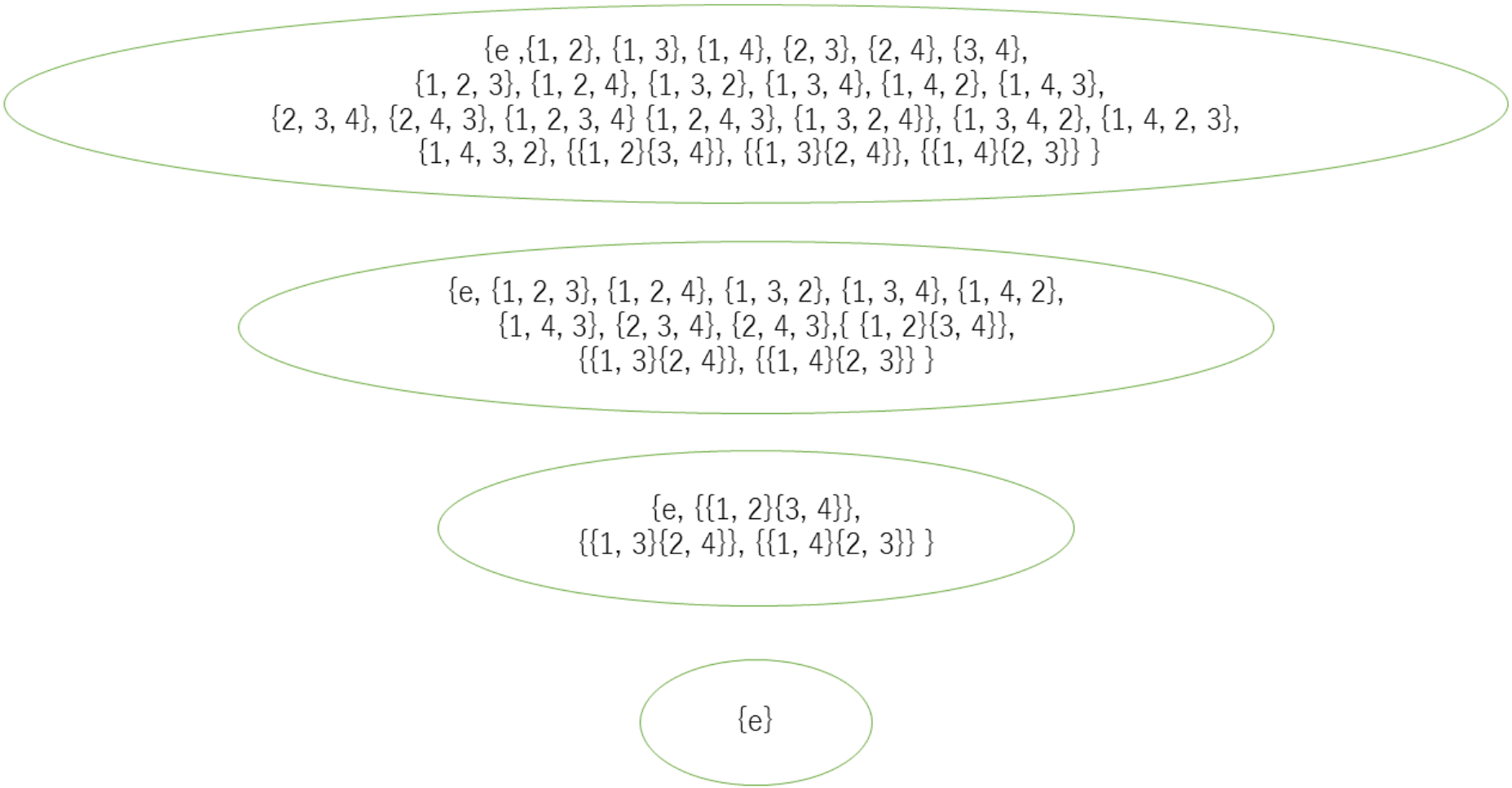
Question-2 改

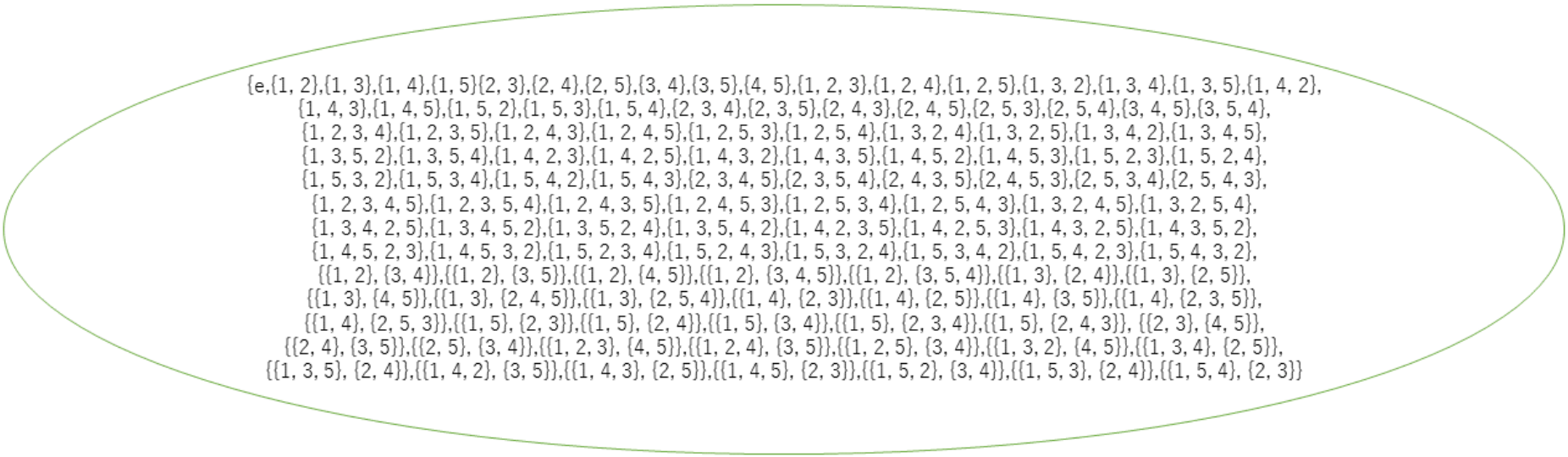
Q. 与えられた方程式に根の公式は存在するか?

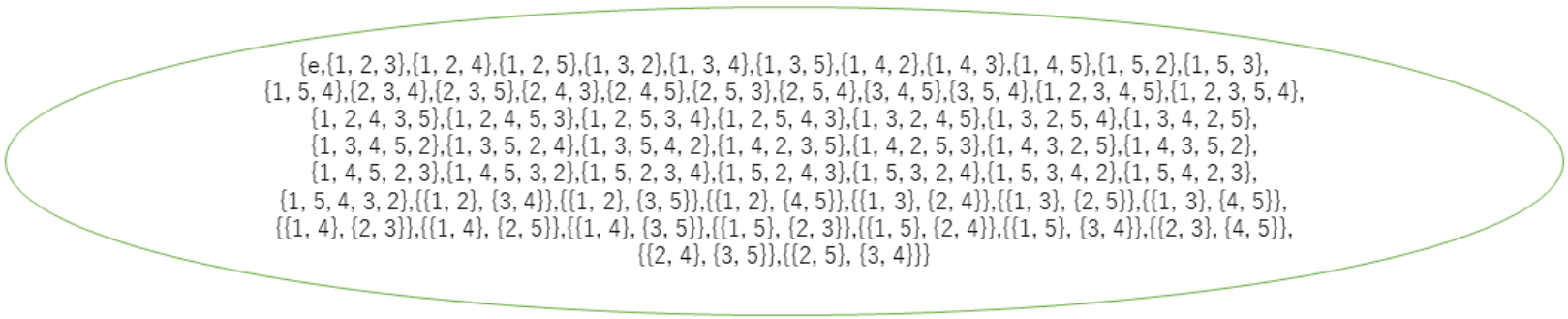
Answer-2 改

そのガロワ群が可解なら存在する.


{e,s,s²,t, s²t,st}
{e,s,s²}
{e}


{e ,{1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4},
{1, 2, 3}, {1, 2, 4}, {1, 3, 2}, {1, 3, 4}, {1, 4, 2}, {1, 4, 3},
{2, 3, 4}, {2, 4, 3}, {1, 2, 3, 4} {1, 2, 4, 3}, {1, 3, 2, 4}}, {1, 3, 4, 2}, {1, 4, 2, 3},
{1, 4, 3, 2}, {{1, 2}{3, 4}}, {{1, 3}{2, 4}}, {{1, 4}{2, 3}} }
{e, {1, 2, 3}, {1, 2, 4}, {1, 3, 2}, {1, 3, 4}, {1, 4, 2},
{1, 4, 3}, {2, 3, 4}, {2, 4, 3},{ {1, 2}{3, 4}},
{{1, 3}{2, 4}}, {{1, 4}{2, 3}} }
{e, {{1, 2}{3, 4}},
{{1, 3}{2, 4}}, {{1, 4}{2, 3}} }
{e}


{e,{1, 2},{1, 3},{1, 4},{1, 5}{2, 3},{2, 4},{2, 5},{3, 4},{3, 5},{4, 5},{1, 2, 3},{1, 2, 4},{1, 2, 5},{1, 3, 2},{1, 3, 4},{1, 3, 5},{1, 4, 2},
{1, 4, 3},{1, 4, 5},{1, 5, 2},{1, 5, 3},{1, 5, 4},{2, 3, 4},{2, 3, 5},{2, 4, 3},{2, 4, 5},{2, 5, 3},{2, 5, 4},{3, 4, 5},{3, 5, 4},
{1, 2, 3, 4},{1, 2, 3, 5},{1, 2, 4, 3},{1, 2, 4, 5},{1, 2, 5, 3},{1, 2, 5, 4},{1, 3, 2, 4},{1, 3, 2, 5},{1, 3, 4, 2},{1, 3, 4, 5},
{1, 3, 5, 2},{1, 3, 5, 4},{1, 4, 2, 3},{1, 4, 2, 5},{1, 4, 3, 2},{1, 4, 3, 5},{1, 4, 5, 2},{1, 4, 5, 3},{1, 5, 2, 3},{1, 5, 2, 4},
{1, 5, 3, 2},{1, 5, 3, 4},{1, 5, 4, 2},{1, 5, 4, 3},{2, 3, 4, 5},{2, 3, 5, 4},{2, 4, 3, 5},{2, 4, 5, 3},{2, 5, 3, 4},{2, 5, 4, 3},
{1, 2, 3, 4, 5},{1, 2, 3, 5, 4},{1, 2, 4, 3, 5},{1, 2, 4, 5, 3},{1, 2, 5, 3, 4},{1, 2, 5, 4, 3},{1, 3, 2, 4, 5},{1, 3, 2, 5, 4},
{1, 3, 4, 2, 5},{1, 3, 4, 5, 2},{1, 3, 5, 2, 4},{1, 3, 5, 4, 2},{1, 4, 2, 3, 5},{1, 4, 2, 5, 3},{1, 4, 3, 2, 5},{1, 4, 3, 5, 2},
{1, 4, 5, 2, 3},{1, 4, 5, 3, 2},{1, 5, 2, 3, 4},{1, 5, 2, 4, 3},{1, 5, 3, 2, 4},{1, 5, 3, 4, 2},{1, 5, 4, 2, 3},{1, 5, 4, 3, 2},
{{1, 2}, {3, 4}},{{1, 2}, {3, 5}},{{1, 2}, {4, 5}},{{1, 2}, {3, 4, 5}},{{1, 2}, {3, 5, 4}},{{1, 3}, {2, 4}},{{1, 3}, {2, 5}},
{{1, 3}, {4, 5}},{{1, 3}, {2, 4, 5}},{{1, 3}, {2, 5, 4}},{{1, 4}, {2, 3}},{{1, 4}, {2, 5}},{{1, 4}, {3, 5}},{{1, 4}, {2, 3, 5}},
{{1, 4}, {2, 5, 3}},{{1, 5}, {2, 3}},{{1, 5}, {2, 4}},{{1, 5}, {3, 4}},{{1, 5}, {2, 3, 4}},{{1, 5}, {2, 4, 3}}, {{2, 3}, {4, 5}},
{{2, 4}, {3, 5}},{{2, 5}, {3, 4}},{{1, 2, 3}, {4, 5}},{{1, 2, 4}, {3, 5}},{{1, 2, 5}, {3, 4}},{{1, 3, 2}, {4, 5}},{{1, 3, 4}, {2, 5}},
{{1, 3, 5}, {2, 4}},{{1, 4, 2}, {3, 5}},{{1, 4, 3}, {2, 5}},{{1, 4, 5}, {2, 3}},{{1, 5, 2}, {3, 4}},{{1, 5, 3}, {2, 4}},{{1, 5, 4}, {2, 3}}


{e,{1, 2, 3},{1, 2, 4},{1, 2, 5},{1, 3, 2},{1, 3, 4},{1, 3, 5},{1, 4, 2},{1, 4, 3},{1, 4, 5},{1, 5, 2},{1, 5, 3},
{1, 5, 4},{2, 3, 4},{2, 3, 5},{2, 4, 3},{2, 4, 5},{2, 5, 3},{2, 5, 4},{3, 4, 5},{3, 5, 4},{1, 2, 3, 4, 5},{1, 2, 3, 5, 4},
{1, 2, 4, 3, 5},{1, 2, 4, 5, 3},{1, 2, 5, 3, 4},{1, 2, 5, 4, 3},{1, 3, 2, 4, 5},{1, 3, 2, 5, 4},{1, 3, 4, 2, 5},
{1, 3, 4, 5, 2},{1, 3, 5, 2, 4},{1, 3, 5, 4, 2},{1, 4, 2, 3, 5},{1, 4, 2, 5, 3},{1, 4, 3, 2, 5},{1, 4, 3, 5, 2},
{1, 4, 5, 2, 3},{1, 4, 5, 3, 2},{1, 5, 2, 3, 4},{1, 5, 2, 4, 3},{1, 5, 3, 2, 4},{1, 5, 3, 4, 2},{1, 5, 4, 2, 3},
{1, 5, 4, 3, 2},{{1, 2}, {3, 4}},{{1, 2}, {3, 5}},{{1, 2}, {4, 5}},{{1, 3}, {2, 4}},{{1, 3}, {2, 5}},{{1, 3}, {4, 5}},
{{1, 4}, {2, 3}},{{1, 4}, {2, 5}},{{1, 4}, {3, 5}},{{1, 5}, {2, 3}},{{1, 5}, {2, 4}},{{1, 5}, {3, 4}},{{2, 3}, {4, 5}},
{{2, 4}, {3, 5}},{{2, 5}, {3, 4}}}


{e}

まとめ

- 根の表現には四則以外の操作が必要である.
- 根の公式の存在条件は体の言葉で与えられる.
- ガロワ理論においてそれを群の問題へ昇華できる.