Galois Theory for Physicists

Spontaneous Symmetry Breaking and the Solution to the Quintic

Tatsu Takeuchi
@Kyoto Sangyo University, Maskawa-Juku
January 12, 2012
DISCLAIMER:

- Start with the complex number field $\mathbb{C}$.
- Fundamental theorem of algebra is assumed.
- Do not claim any mathematical rigour.
The solution does not have the symmetry manifest in the equation.

Example: particle in a left-right symmetric potential $V(x)$

$$m \frac{d^2 x}{dt^2} = -\frac{dV(x)}{dx}, \quad V(x) = V(-x)$$

Equation is invariant under the parity transformation $x \leftrightarrow -x$ but the solution may not be.

$$V(x) = x^4 - 2x^2$$

$$\frac{dV(x)}{dx} = 4x(x^2 - 1) = 0 \quad \rightarrow \quad x^2 = 1 \quad \rightarrow \quad x = \pm 1$$
The equation has left-right symmetry, but the solution does not. The mass is forced to choose between two possible ground states.

The two ground states transform into each other under the broken (hidden) symmetry transformation \( \rightarrow \) non-trivial representation of the symmetry group.
WHO WAS ÉVARISTE GALOIS?

- Mathematical prodigy, but failed entrance exam to École Polytechnic. Entered École Normale instead but expelled.
- Political radical (Republican). Jailed many times.
- Died May 31, 1832 from a bullet wound suffered during a duel on May 30. He was 20 years old. Circumstances of the duel are unknown.
- Wrote papers during the night before the duel outlining his mathematical ideas → Proof that the quintic cannot be solved by radicals (\( \sqrt[5] \)) using Group Theory.
WHO KILLED ÉVARISTE GALOIS?

- Was Galois murdered by his political enemies? Note that the duel was just a week before the failed Paris Uprising of 1832 (June 5~6, 1832) by his Republican friends.

Students at the barricade in Les Misérables. Would have Galois been killed at the uprising had he not died a week earlier?

Marius and Cosette in Les Misérables. Did Evariste and Stephanie enjoy a similar relationship or was she the reason for the duel?
Linear :  \( ax + b = 0 \)

Quadratic :  \( ax^2 + bx + c = 0 \)

Cubic :  \( ax^3 + bx^2 + cx + d = 0 \)

Quartic :  \( ax^4 + bx^3 + cx^2 + dx + e = 0 \)

Quintic :  \( ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0 \)

- The solution formula for the \textbf{quadratic} equation was known worldwide since ancient times. (Can be found on mesopotamian cuniform tablets.)
- Solution formulae to the \textbf{cubic} and the \textbf{quartic} were discovered during the 16\textsuperscript{th} century in Italy.
- The formula for the \textbf{quintic} could not be found. Proved that it did not exist independently by \textbf{Neils Henrik Abel} (Norwegian, 1802-1829) and \textbf{Galois} (1811-1832).
**THE CUBIC & THE QUARTIC**
**THE BATTLE OF THE ITALIAN MATH-MAGICIANS:**

- **Scipione del Ferro** (1465-1526)
- **Niccolo Fontana (Tartaglia)** (1499/1500?-1557)
- **Geralomo Cardano** (1501-1576)
- **Lodovico Ferrari** (1522-1565)

- **Del Ferro** discovers solution to the special case $x^3+px=q$, $p>0$, $q>0$.
- Del Ferro’s student **Antonio Maria Fiore**, who had inherited the magic formula from del Ferro, challenges **Tartaglia** to a math duel in 1535 and is defeated, Tartaglia having discovered the solution overnight.
- **Cardano** bugs Tartaglia until he divulges his secret. Cardano supposedly promised that he will not tell anyone.
- Cardano generalizes the result, learns that del Ferro had the result before Tartaglia, and publishes "**Ars Magna**" in 1545.
- Infuriated Tartaglia challenges Cardano to a math duel but is defeated by Cardano’s student **Ferrari** who figured out the solution to the quartic.
Still in print after more than four and a half centuries. (Perhaps not as impressive as Euclid’s Elements.)

The cubic is separated into 13 cases (to avoid the use of negative numbers) and discussed in gory detail:

\[
\begin{align*}
    x^3 + px &= q \\
    x^3 &= px + q \\
    x^3 + q &= px \\
    x^3 + px^2 &= q \\
    x^3 &= px^2 + q \\
    x^3 + q &= px^2 \\
    x^3 + px^2 + qx &= r \\
    x^3 + px^2 &= qx + r \\
    x^3 + px^2 &= qx + r \\
    x^3 + px^2 &= qx + r \\
    x^3 + r &= px^2 + qx \\
    x^3 + qx + r &= px^2 \\
    x^3 + px^2 + r &= qx
\end{align*}
\]

Ferrari’s result for the quartic is only mentioned in passing. Cardano didn’t think it was important because the space we live in is 3-dimensional. (Huh?)
QUADRATIC EQUATION

0 = ax^2 + bx + c

Divide both sides by \( a \), then complete the square:

\[ 0 = x^2 + \frac{b}{a}x + \frac{c}{a} \]

\[ = \left( x + \frac{b}{2a} \right)^2 - \left( \frac{b^2}{4a^2} - \frac{c}{a} \right) \]

\[ = \left( x + \frac{b}{2a} \right)^2 - \left( \frac{b^2}{4a^2} - \frac{c}{a} \right) \]

\[ \downarrow \]

\[ \left( x + \frac{b}{2a} \right)^2 = \left( \frac{b^2}{4a^2} - \frac{c}{a} \right) \]

\[ \downarrow \]

\[ x + \frac{b}{2a} = \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = \pm \frac{\sqrt{b^2 - 4ac}}{2a} \]

\[ \downarrow \]

\[ x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \]
COMPLETING THE SQUARE:

\[ x^2 + 2Ax \rightarrow x^2 + 2Ax + A^2 = (x + A)^2 \]
RELATION BETWEEN COEFFICIENTS AND ROOTS

\[ x^2 - s_1x + s_2 = (x - \alpha_1)(x - \alpha_2) \]

\[ \downarrow \]

\[ s_1 = \alpha_1 + \alpha_2 \]

\[ s_2 = \alpha_1\alpha_2 \]

- Solving the quadratic is equivalent to finding the two numbers for which their sum and product are given.
- Note that the coefficients are symmetric polynomials of the roots. They are invariant under \( \alpha_1 \leftrightarrow \alpha_2 \), that is, their symmetry group is \( S_2 \).
CUBIC EQUATION – STEP 1

Divide both sides by $a$, then complete the cube:

$$0 = ax^3 + bx^2 + cx + d$$

$$\downarrow$$

$$0 = x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a}$$

$$= \left( x^3 + \frac{b}{a}x^2 + \frac{b^2}{3a^2}x + \frac{b^3}{27a^3} \right) - \left( \frac{b^2}{3a^2}x + \frac{b^3}{27a^3} \right) + \frac{c}{a}x + \frac{d}{a}$$

$$= \left( x + \frac{b}{3a} \right)^3 + \left( \frac{c}{a} - \frac{b^2}{3a^2} \right) \left( x + \frac{b}{3a} \right) + \left( \frac{d}{a} - \frac{bc}{3a^2} + \frac{2b^3}{27a^3} \right)$$

$$= y^3 + py + q$$
Let $y = u + v$:

\[ 0 = y^3 + py + q \]

\[ = (u + v)^3 + p(u + v) + q \]

\[ = (u^3 + v^3 + q) + (3uv + p)(u + v) \]

\[ \downarrow \]

\[ uv = -\frac{p}{3}, \quad u^3 + v^3 = -q \]

\[ \downarrow \]

\[ u^3 v^3 = -\frac{p^3}{27} \]

$u^3$ and $v^3$ are solutions to:

\[ 0 = z^2 + qz - \frac{p^3}{27} \]

\[ \downarrow \]

\[ z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \equiv z_\pm \]

\[ \downarrow \]

\[ u = \sqrt[3]{z_+}, \quad v = \sqrt[3]{z_-}, \quad \sqrt[3]{z_+} \sqrt[3]{z_-} = -\frac{p}{3} \]

\[ \downarrow \]

\[ y = \begin{cases} u + v \\ u \omega + v \omega^2 \\ u \omega^2 + v \omega \end{cases} \quad \text{where } \omega^3 = 1. \]
RELATION BETWEEN COEFFICIENTS AND ROOTS

\[ x^3 - s_1x^2 + s_2x - s_3 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \]

\[ s_1 = \alpha_1 + \alpha_2 + \alpha_3 \]
\[ s_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 \]
\[ s_3 = \alpha_1\alpha_2\alpha_3 \]

- Solving the cubic is equivalent to finding the three numbers for which their sum, product, and the sum of products of all pairs are given.
- The coefficients are **symmetric polynomials** of the roots. They are invariant under all permutations of the three roots, i.e. their symmetry group is \( S_3 \).
Complete the 4D-hypercube to eliminate the $x^3$ term:

\[ 0 = ax^4 + bx^3 + cx^2 + dx + e \]

\[ \downarrow \]

\[ 0 = x^4 + \frac{b}{a}x^3 + \frac{c}{a}x^2 + \frac{d}{a}x + \frac{e}{a} \]

\[ = \left(x + \frac{b}{4a}\right)^4 + \left(c - \frac{3b^2}{8a^2}\right)\left(x + \frac{b}{4a}\right)^2 + \left(d - \frac{bc}{2a^2} + \frac{b^3}{8a^3}\right)\left(x + \frac{b}{4a}\right) \]

\[ + \left(e - \frac{bd}{a} + \frac{b^2c}{4a^2} - \frac{3b^4}{16a^3}\right) \]

\[ = y^4 + py^2 + qy + r \]
QUARTIC EQUATION – STEP 2 – FERRARI

\[-py^2 - qy - r = y^4\]

\[(2t - p)y^2 - qy + (t^2 - r) = y^4 + (2t y^2 + t^2) = (y^2 + t)^2\]

Choose the constant \( t \) so that the left hand side is a complete square:

\[\Delta_2 = (-q)^2 - 4(2t - p)(t^2 - r) = -8 \left[ t^3 - \frac{p}{2} t^2 - rt + \left( \frac{4pr - q^2}{8} \right) \right] = 0\]

Then, we can take the square-root of both sides:

\[(2t - p)y^2 - qy + (t^2 - r) = (Ay + B)^2 = (y^2 + t)^2\]

\[\pm(Ay + B) = y^2 + t\]
Let \( y = u + v + w \):

\[
0 = y^4 + py^2 + qy + r
= (u + v + w)^4 + p(u + v + w)^2 + q(u + v + w) + r
= (u^2 + v^2 + w^2)^2 + p(u^2 + v^2 + w^2) + 4(u^2v^2 + v^2w^2 + w^2u^2) + r
\]
\[+ [4(u^2 + v^2 + w^2) + 2p](uv + vw + wu) + [8uvw + q](u + v + w) \]

\[
\downarrow
\]

\[
-\frac{q}{8} = uvw \quad \rightarrow \quad \frac{q^2}{64} = u^2v^2w^2
\]

\[
-\frac{p}{2} = u^2 + v^2 + w^2,
\]

\[
\frac{p^2 - 4r}{16} = u^2v^2 + v^2w^2 + w^2u^2
\]
\[ u^2, v^2, \text{ and } w^2 \text{ are solutions to:} \]
\[ 0 = z^3 + \frac{p}{2} z^2 + \frac{p^2 - 4r}{16} z - \frac{q^2}{64} \]
\[ z = z_1, z_2, z_3 \]
\[ u = \sqrt{z_1}, \quad v = \sqrt{z_2}, \quad w = \sqrt{z_3}, \quad \sqrt{z_1} \sqrt{z_2} \sqrt{z_3} = -\frac{q}{8} \]
\[ y = \begin{cases} 
  u + v + w \\
  u - v - w \\
  -u + v - w \\
  -u - v + w 
\end{cases} \]
**FERRARI–EULER COMPARISON**

\[
0 = z^3 + \frac{p}{2} z^2 + \frac{p^2 - 4r}{16} z - \frac{q^2}{64} \quad \leftrightarrow \quad 0 = t^3 - \frac{p}{2} t^2 - rt + \left(\frac{4pr - q^2}{8}\right)
\]

Euler \quad z = u^2 \quad \leftrightarrow \quad t = u^2 - v^2 - w^2 \quad \text{Ferrari}

\[
\left(\frac{2t - p}{4}\right)y^2 \quad \text{Ferrari} \quad y + \left(\frac{2t - p}{4}\right) = (y^2 + \frac{12}{3})^2
\]

\[
\pm 2(uy + vw) = y^2 + (u^2 - v^2 - w^2)
\]

\[
y^2 \ m2u y + [u^2 - (v \pm w)] = 0
\]

\[
[y - (u + v + w)][y - (u - v - w)] = 0 \quad \rightarrow \quad y = u + v + w, \quad u - v - w
\]

\[
[y + (u + v - w)][y + (u - v + w)] = 0 \quad \rightarrow \quad y = -u - v + w, \quad -u + v - w
\]
The coefficients are symmetric polynomials of the roots. They are invariant under all permutations of the four roots, i.e. their symmetry group is $S_4$. 
ORDER N ALGEBRAIC EQUATION:

\[ 0 = x^N - s_1 x^{N-1} + s_2 x^{N-2} + \ldots + (-1)^{N-1} s_{N-1} x + (-1)^N s_N \]

\[ = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \ldots (x - \alpha_{N-1})(x - \alpha_N) \]

\[ s_1 = \alpha_1 + \alpha_2 + \alpha_3 + \ldots + \alpha_{N-1} + \alpha_N \]

\[ s_2 = \sum_{i<j} \alpha_i \alpha_j \]

\[ s_3 = \sum_{i<j<k} \alpha_i \alpha_j \alpha_k \]

\[ s_N = \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_{N-1} \alpha_N \]

The coefficients are **symmetric polynomials** of the roots. They are invariant under any permutation of the roots, i.e. their symmetry group is \( S_N \).
SOLUTION FORMULA:

\[ s_1 = \alpha_1 + \alpha_2 + \alpha_3 + \ldots + \alpha_{N-1} + \alpha_N \]
\[ s_2 = \sum_{i<j} \alpha_i \alpha_j \]
\[ s_3 = \sum_{i<j<k} \alpha_i \alpha_j \alpha_k \] \[ \Rightarrow \]
\[ M \]
\[ s_N = \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_{N-1} \alpha_N \]

\[ \alpha_1 = f_1( s_1, s_2, s_3, \ldots, s_{N-1}, s_N ) \]
\[ \alpha_2 = f_2( s_1, s_2, s_3, \ldots, s_{N-1}, s_N ) \]
\[ \alpha_3 = f_3( s_1, s_2, s_3, \ldots, s_{N-1}, s_N ) \]
\[ \alpha_{N-1} = f_{N-1}( s_1, s_2, s_3, \ldots, s_{N-1}, s_N ) \]
\[ \alpha_N = f_N( s_1, s_2, s_3, \ldots, s_{N-1}, s_N ) \]

- Solution formulae must invert the relations between the coefficients and the roots and express the roots in terms of the coefficients.
IMPOSSIBILITY OF SOLUTION FORMULAE:

\[ \alpha_i = f_i( s_1, s_2, s_3, \ldots, s_{N-1}, s_N ) \]

- Right-hand side is manifestly invariant under any permutation of the roots.
- Left-hand side is not.
- Therefore, such a relation is impossible!??
- But formulae for the quadratic, cubic, and the quartic exist!
- So what is wrong with this argument?
THE LANGUAGE OF SYMMETRIES: GROUP THEORY

Definition of a Group $G$:

+ Closed under group multiplication
  \[ a, b \in G \rightarrow a \circ b \in G \]

+ Group multiplication is associative
  \[ (a \circ b) \circ c = a \circ (b \circ c) \]

+ Unit element exists
  \[ \exists e \in G \text{ such that } e \circ a = a \circ e = a \quad \forall a \in G \]

+ Inverse element exists for every element
  \[ \forall a \in G, \exists a^{-1} \in G \text{ such that } a \circ a^{-1} = a^{-1} \circ a = e \]
“Symmetry” refers to invariance under some set of transformations.

Define the “product” of two symmetry transformations as the transformation obtained by performing the two symmetry transformations in succession. Then, the set of all symmetry transformations forms a group.

The unit element is the transformation which does nothing.

The inverse element is the inverse transformation.
The symmetric group $S_N$ is the group formed by all possible permutations of $N$ objects and denoted $S_N$. It has $N!$ elements.

Examples:

$S_2 = \{e, (12)\}$

$S_3 = \{e, (12), (13), (23), (123), (132)\}$

$S_4 = \{e, (12), (13), (14), (23), (24), (34),$

$(12)(34), (13)(24), (14)(23),$

$(123), (132), (124), (142), (134), (143), (234), (243),$

$(1234), (1243), (1324), (1342), (1423), (1432)\}$
NOTATION:

\[ e : \text{do nothing} \]
\[ (12) : 1 \rightarrow 2 \rightarrow 1 \]
\[ (123) : 1 \rightarrow 2 \rightarrow 3 \rightarrow 1 \]
\[ (1234) : 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1 \]
\[ (123)(45) : 1 \rightarrow 2 \rightarrow 3 \rightarrow 1, \ 4 \rightarrow 5 \rightarrow 4 \quad \text{etc.} \]

\[
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (142), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (15342) \]
A Group $H$ contained inside another Group $G$ is called a subgroup of $G$, e.g.:

Group : $S_3 = \{e, (12), (13), (23), (123), (132)\}$

Subgroups : $\{e\}, S_2 = \{e, (12)\}, S'_2 = \{e, (13)\}, S''_2 = \{e, (23)\}, C_3 = \{e, (123), (132)\}$

The number of elements in a subgroup is always a divisor of the number of element in the parent group. (Lagrange’s theorem.)
Let $H$ be a subgroup of $G$. The elements of $G$ can be classified into equivalence classes using $a^{-1}b \in H$ as an equivalence relation. That is, $a$ and $b$ are equivalent if $\exists h \in H$ such that $b = ah$. These classes are called cosets.

Group : $S_3 = \{e, (12), (13), (23), (123), (132)\}$
Subgroup : $S_2 = \{e, (12)\}$
Cosets: $eS_2 = \{e, (12)\}$, $(13)S_2 = \{(13), (123)\}$, $(23)S_2 = \{(23), (132)\}$

Group : $S_3 = \{e, (12), (13), (23), (123), (132)\}$
Subgroup : $C_3 = \{e, (123), (132)\}$
Cosets: $eC_3 = \{e, (123), (132)\}$, $(13)C_3 = \{(13), (12), (23)\}$
Two elements $a$ and $b$ of a group $G$ are said to be conjugate to each other if $\exists g \in G$ such that $gag^{-1} = b$. What this means is that $a$ and $b$ are the “same kind” of transformation which can be transformed into each other by $g$.

$$ (12)(23)(12) = (13) $$
$$ (12)(123)(12) = (132) $$
$$ (123)(12)(132) = (23) $$

Conjugacy is an equivalence relation which can be used to classify the elements of $G$ into conjugacy classes.

$S_3 : \{e\}, \{(12),(13),(23)\}, \{(123),(132)\}$

$S_4 : \{e\}, \{(12),(13),(14),(23),(24),(34)\}, \{(12)(34),(13)(24),(14)(23)\}, \{(123),(132),(124),(142),(134),(143),(234),(243)\}, \{(1234),(1243),(1324),(1342),(1423),(1432)\}$
Let $H$ be a subgroup of $G$. If for all $h \in H$ and all $g \in G$, we have the relation $ghg^{-1} \in H$, then the subgroup $H$ is said to be an invariant subgroup. It is a subgroup consisting of complete conjugate classes.

Group : $S_3 = \{e, (12), (13), (23), (123), (132)\}$

Invariant Subgroups : $\{e\}, \quad C_3 = \{e, (123), (132)\}$

$ghg^{-1}$ is the transformation of $h$ by $g$. Since all elements of $H$ stay in $H$ under all transformations in $G$, we can write: $gHg^{-1} = H$.

$gHg^{-1} = H$ implies $gH = Hg$. So $H$ as a whole commutes with $G$. 
SOLUTION TO THE QUADRATIC REVISITED:

\[ x^2 - s_1x + s_2 = 0 \quad \rightarrow \quad x_\pm = \frac{s_1 \pm \sqrt{\Delta_2}}{2} \]

- The square-root is double-valued \( \rightarrow \) We are forced to chose between two possible square-roots whenever the discriminant is non-zero!
  \[ \sqrt{\Delta_2} = \alpha_1 - \alpha_2 \quad \text{or} \quad \alpha_2 - \alpha_1 \]

- Symmetry breaks from \( S_2 \) to the trivial invariant subgroup \{e\}.
  \[ \sqrt{\Delta_2} \quad \leftrightarrow^{(12)} \quad -\sqrt{\Delta_2} \]

- The square-root of the discriminant serves as a basis for a 1x1 representation of \( S_2 \):
  \[ e \rightarrow \begin{bmatrix} 1 \end{bmatrix}, \quad (12) \rightarrow \begin{bmatrix} -1 \end{bmatrix} \]
SOLUTION TO THE CUBIC REVISITED 1:

\[ x^3 - s_1x^2 + s_2x - s_3 = 0 \rightarrow y^3 + py + q = 0 \]

where \( y = x - \frac{s_1}{3}, \quad p = -\frac{s_1^2}{3} + s_2, \quad q = -\frac{2s_1^3}{27} + \frac{s_1s_2}{3} - s_3. \)

\[ z^2 + qz - \frac{p^3}{27} = 0 \rightarrow z_{\pm} = -\frac{q}{2} \pm \frac{i}{6} \sqrt{\Delta_3} \]

discriminant \( \Delta_3 = -27q^2 - 4p^3 \)

\[ = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_3 + 18s_1s_2s_3 - 27s_3^2 \]

\[ = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 \]

\( \sqrt{\Delta_3} = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \) or \( -(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \)
SOLUTION TO THE CUBIC REVISITED 2:

- Symmetry breaks from $S_3$ to the invariant subgroup $C_3=\{e,(123),(132)\}$.

\[
\sqrt{\Delta_3} \quad \overset{(12)(13)(23)}{\leftrightarrow} \quad -\sqrt{\Delta_3}
\]

- The three transpositions $(12)$, $(13)$, and $(23)$ are actually equivalent since:

  \[
  (12) = (12)e = e(12) \\
  (13) = (12)(132) = (123)(12) \\
  (23) = (12)(123) = (132)(12)
  \]

- The three permutations $e$, $(123)$, and $(132)$ are of course equivalent since they keep the discriminant invariant. So the actions of all the permutations of $S_3$ are equivalent to that of $\{e,(12)\}=S_3/C_3$. This is known as the Quotient Group.

\[
eC_3 = \{e,(123),(132)\} \rightarrow [1] \quad \text{and} \quad (12)C_3 = \{(12),(13),(23)\} \rightarrow [-1]
\]
Let $H$ be a subgroup of $G$. Each coset with respect to $H$ can be expressed collectively as $aH$ for some $a \in G$.

When $H$ is an invariant subgroup of $G$, then “multiplication” between cosets can be defined as $aH \cdot bH = a(Hb)H = a(bH)H = (ab)H$. The group formed by this group multiplication is called the quotient group $G/H$.
Taking the cubic roots of \( z_\pm \) breaks \( C_3 = \{e, (123), (132)\} \) down to the trivial invariant subgroup \( \{e\} \).

\[
\begin{align*}
z_+ &= \left( \frac{\alpha_1 + \omega^2 \alpha_2 + \omega \alpha_3}{3} \right)^3, \\
z_- &= \left( \frac{\alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3}{3} \right)^3
\end{align*}
\]

\[
\begin{align*}
\sqrt[3]{z_+} &= \frac{\alpha_1 + \omega^2 \alpha_2 + \omega \alpha_3}{3}, \\
\sqrt[3]{z_-} &= \frac{\alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3}{3}
\end{align*}
\]

\[
\begin{align*}
\sqrt[3]{z_+} \xrightarrow{(123)} \omega \sqrt[3]{z_+} & \xrightarrow{(123)} \omega^2 \sqrt[3]{z_+} \\
\sqrt[3]{z_-} \xrightarrow{(132)} \omega \sqrt[3]{z_-} & \xrightarrow{(132)} \omega^2 \sqrt[3]{z_-}
\end{align*}
\]
The cubic roots of $z_{\pm}$ provide a basis for a 1x1 representation of $S_3 = \{e, (123), (132)\}$:

\[
\begin{align*}
\sqrt[3]{z_+} & : \quad e \rightarrow [1], \quad (123) \rightarrow [\omega], \quad (132) \rightarrow [\omega^2] \\
\sqrt[3]{z_-} & : \quad e \rightarrow [1], \quad (123) \rightarrow [\omega^2], \quad (132) \rightarrow [\omega]
\end{align*}
\]

Together, they provide a basis for a 2x2 representation of $S_3$:

\[
\begin{align*}
e & \rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (123) \rightarrow \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \quad (132) \rightarrow \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega \end{bmatrix} \\
(23) & \rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (12) \rightarrow \begin{bmatrix} 0 & \omega \\ \omega^2 & 0 \end{bmatrix}, \quad (13) \rightarrow \begin{bmatrix} 0 & \omega^2 \\ \omega & 0 \end{bmatrix}
\end{align*}
\]
SOLUTION TO THE QUARTIC – OUTLINE 1:

\[ x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 = 0 \quad \rightarrow \quad y^4 + py^2 + qy + r = 0 \]

where \( y = x - \frac{s_1}{4}, \quad p = -\frac{3s_1^2}{8} + s_2, \quad q = -\frac{s_1^3}{8} + \frac{s_1s_2}{2} - s_3, \quad r = \frac{-3s_1^4}{256} + \frac{s_1^2s_2}{16} - \frac{s_1s_3}{4} + s_4. \)

\[ z^3 + \frac{p}{2}z^2 + \frac{p^2 - 4r}{16}z - \frac{q^2}{64} = 0 \quad \rightarrow \quad \zeta^3 + P\zeta + Q = 0 \]

where \( \zeta = z + \frac{p}{6}, \quad P = -\frac{p^3}{48} - \frac{r}{4}, \quad Q = -\frac{p^3}{864} - \frac{q^2}{64} + \frac{pr}{24}. \)

\[ \xi^2 + Q\xi - \frac{p^3}{27} = 0 \quad \rightarrow \quad \xi_{\pm} = -\frac{Q}{2} \pm \frac{i}{384} \sqrt{\frac{\Delta_4}{3}} \]

\[ \Delta_4 = s_1^2s_2^3s_3^2 - 4s_2^3s_3^2 - 4s_1s_3^3s_3 - 27s_3^4 - 4s_1s_2s_3^3s_4 + 16s_2^4s_4 + 18s_1s_2s_3s_4 - 80s_1s_2s_3s_4 - 6s_1s_2^3s_4 + 144s_2s_3^2s_4 - 27s_1s_4^2 + 144s_1^2s_2^2s_4 - 128s_1^2s_2^2s_4 - 192s_1s_3s_4^2 + 256s_4^3 \]

\[ = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_1 - \alpha_4)^2(\alpha_2 - \alpha_3)^2(\alpha_2 - \alpha_4)^2(\alpha_3 - \alpha_4)^2 \]
SOLUTION TO THE QUARTIC – OUTLINE 2:

\[ \sqrt{\Delta_4} = + (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4) \]

or

\[ = - (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4) \]

\[ \sqrt{\Delta_4} \quad \leftrightarrow \quad \text{odd permutations} \quad \rightarrow \quad - \sqrt{\Delta_4} \]

Symmetry breaks from \( S_4 \) to the invariant subgroup \( A_4 = \{ \text{all even permutations} \} \).

\[ eA_4 = \{ \text{all even permutations} \} \rightarrow \begin{bmatrix} 1 \end{bmatrix} \]

\[ (12)A_4 = \{ \text{all odd permutations} \} \rightarrow \begin{bmatrix} -1 \end{bmatrix} \]

\[ S_4 / A_4 = \{ e, (12) \} \]
**SOLUTION TO THE QUARTIC – OUTLINE 3:**

\[ 3\sqrt{\xi} \quad \overset{(132)(234)(124)(143)}{\longrightarrow} \quad \omega \ 3\sqrt{\xi} \quad \overset{(132)(234)(124)(143)}{\longrightarrow} \quad \omega^2 \ 3\sqrt{\xi} \]

\[ 3\sqrt{\xi} \quad \overset{(123)(134)(243)(142)}{\longrightarrow} \quad \omega \ 3\sqrt{\xi} \quad \overset{(123)(134)(243)(142)}{\longrightarrow} \quad \omega^2 \ 3\sqrt{\xi} \]

- Symmetry breaks from \( A_4 \) to its invariant subgroup \( V = \{ e, (12)(34), (13)(24), (14)(23) \} \), known as the *four-group*

\[
\begin{align*}
  eV &= \{ e, (12)(34), (13)(24), (14)(23) \} \\
  (123)V &= \{ (123), (134), (243), (142) \} \\
  (132)V &= \{ (132), (234), (124), (143) \} \\
  A_4 / V &= \{ e, (123), (132) \}
\end{align*}
\]

\[
\begin{pmatrix}
  3\sqrt{\xi} \\
  3\sqrt{\xi}
\end{pmatrix} \quad \overset{\begin{pmatrix}
  1 \\
  1
\end{pmatrix}}{\longrightarrow} \quad \begin{pmatrix}
  \omega^2 \\
  \omega
\end{pmatrix} \quad \overset{\begin{pmatrix}
  \omega \\
  \omega^2
\end{pmatrix}}{\longrightarrow} \quad \begin{pmatrix}
  1 \\
  1
\end{pmatrix}
\]

\[
\begin{pmatrix}
  3\sqrt{\xi} \\
  3\sqrt{\xi}
\end{pmatrix} \quad \overset{\begin{pmatrix}
  1 \\
  1
\end{pmatrix}}{\longrightarrow} \quad \begin{pmatrix}
  \omega^2 \\
  \omega
\end{pmatrix} \quad \overset{\begin{pmatrix}
  \omega \\
  \omega^2
\end{pmatrix}}{\longrightarrow} \quad \begin{pmatrix}
  1 \\
  1
\end{pmatrix}
\]
SOLUTION TO THE QUARTIC – OUTLINE 4:

\[ \sqrt{z_1} \leftrightarrow (13)(24), (14)(23) \quad - \sqrt{z_1} \]
\[ \sqrt{z_2} \leftrightarrow (12)(34), (14)(23) \quad - \sqrt{z_2} \]
\[ \sqrt{z_3} \leftrightarrow (12)(34), (13)(24) \quad - \sqrt{z_3} \]

- Symmetry breaks from \( V \) to the trivial invariant subgroup \{e\} via the invariant subgroups \{e,(12)(34)\}, or \{e,(13)(24)\}, or \{e,(14)(23)\}, depending on the order in which the square-roots are introduced.

\[ e \{e, (12)(34)\} = \{e, (12)(34)\} \]
\[ (13)(24) \{e, (12)(34)\} = \{(13)(24), (14)(23)\} \]
\[ V / \{e, (12)(34)\} = \{e, (13)(24)\} \]
The symmetry breaking pattern:

- The unbroken subgroup is an invariant subgroup of the parent group at each step.
- When $p$-th roots are used to break the symmetry down from $G$ to $H$, the quotient group $G/H$ is isomorphic to $C_p$.
- For the quintic to be solvable by radicals, $S_5$ must have a sequence of invariant subgroups such that the quotient group of the successive groups in the sequence is always cyclic.

\[
\frac{\sqrt{\Delta_2}}{S_2} \rightarrow \frac{\sqrt{\Delta_3}}{C_3} \rightarrow \frac{\sqrt{z}}{S_3} \rightarrow \frac{\sqrt{z_3}}{S_4} \rightarrow \frac{\sqrt{z_1}}{A_4} \rightarrow \frac{\sqrt{z_2}}{V} \rightarrow \{e,(12)(34)\} \rightarrow \{e\}
\]
5! = 120 elements, 60 odd and 60 even, 7 conjugacy classes:

\[
\begin{align*}
    e & : 1 \text{ element} \\
    (**)(**) & : 15 \text{ elements} \\
    (***) & : 20 \text{ elements} \\
    (***) & : 24 \text{ elements} \\
    (**) & : 10 \text{ elements} \\
    (**)(**) & : 20 \text{ elements} \\
    (****) & : 30 \text{ elements}
\end{align*}
\]

- \(A_5\) is an invariant subgroup of \(S_5\) and \(S_5/A_5 = \{e, (12)\}\).
By taking the square-root of this discriminant, it is indeed possible to break $S_5$ down to $A_5$. 

- 59 terms!
THE ALTERNATING GROUP $A_5$

- 60 elements, 5 conjugacy classes:
  
  $e$ : 1 element
  
  (**)(**): 15 elements
  
  (***) : 20 elements
  
  (****) : 12 elements
  
  (*****): 12 elements

- Lagrange’s theorem tells us that the number of elements in a proper subgroup of $A_5$ must be 30, 20, 15, 12, 10, 6, 5, 4, 3, 2, or 1.
- For it to be an invariant subgroup, it must contain complete conjugacy classes, including {e}.
- Simple counting shows that it is impossible $\rightarrow A_5$ does not have any invariant subgroups.
PROOF FOR $S_n$ ($n \geq 5$)

- Let $G$ be a group of permutations of five objects or more that include all cyclic permutations of three elements.

\[
(124)(142) = e \\
(135)(153) = e \\
(123) = (124)(135)(142)(153)
\]

- Let $H$ be an invariant subgroup of $G$ such that $G/H$ is cyclic (Abelian).

- Consider the homomorphism $\varphi: G \rightarrow G/H$

\[
f[(124)] \equiv x, \\
f[(135)] \equiv y, \\
f[(123)] = f[(124)(135)(142)(153)] = xyx^{-1}y^{-1} = e
\]

Therefore $(123) \in H$. This is true for any cyclic permutation of three elements. Therefore, $G$ is not solvable.
PHYSICIST VERSION OF GALOIS THEORY:

- The $N$ coefficients of an order $N$ algebraic equation are symmetric polynomials of the $N$ roots. They are invariant under all $N!$ permutations of the $N$ roots. The solution formula must break this $S_N$ symmetry down to $\{e\}$.

- Radicals (p-th roots) break the symmetry by their multi-valuedness, forcing us a choice among $p$ different “vacua.” Transformations from one “vacuum” to another are represented by the $p$-th roots of one. The symmetry must break to an invariant subgroup of the parent group such that the quotient group of the two is isomorphic to $C_p$.

- For an order $N$ algebraic equation to be solvable by radicals, the group $S_N$ must have a sequence of invariant subgroups for which the quotient group of successive groups is always cyclic. This is not the case when $N \in 5$. 
COLLORARY AND CAVEATS:

- Not all algebraic numbers can be expressed algebraically!
- The generic quintic can be solved if you allow for an infinite number of rational operations and/or radicals.
- Solution formulas exist which use elliptic functions.
Complete the 5D-hypercube to eliminate the $x^4$ term:

$$0 = x^5 - s_1 x^4 + s_2 x^3 - s_3 x^2 + s_4 x - s_5$$

$$= \left(x - \frac{s_1}{5}\right)^5 + \left(s_2 - \frac{2s_1^2}{5}\right) \left(x - \frac{s_1}{5}\right)^3 - \left(s_3 - \frac{3s_1 s_2}{5} + \frac{4s_1^3}{25}\right) \left(x - \frac{s_1}{5}\right)^2$$

$$+ \left(s_4 - \frac{2s_1 s_3}{5} + \frac{3s_1^2 s_2}{4} - \frac{3s_1^4}{43}\right) \left(x - \frac{s_1}{5}\right)$$

$$+ \left(s_5 - \frac{s_1 s_4}{5} + \frac{s_1^2 s_3}{4} - \frac{s_1^3 s_2}{4} + \frac{4s_1^5}{3125}\right)$$

$$= y^5 + t_2 y^3 - t_3 y^2 + t_4 y - t_5$$

$$y = x - \frac{s_1}{5}$$
Let the five roots of \( 0 = x^5 - s_1 x^4 + s_2 x^3 - s_3 x^2 + s_4 x - s_5 \) be \( x = \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \).

Note that \( \sum_{i=1}^{5} \alpha_i = s_1 \).

Let \( \beta_i = \alpha_i + a \) and choose \( a \) so that \( \sum_{i=1}^{5} \beta_i = 0 \) \( \Rightarrow \) \( a = -\frac{s_1}{5} \).

Then, \( y = \beta_1, \beta_2, \beta_3, \beta_4, \beta_5 \) will be the roots of a quintic equation in \( y \) without the \( y^4 \) term:

\[ 0 = y^5 + t_2 y^3 - t_3 y^2 + t_4 y - t_5 \]
Let the five roots of $0 = y^5 + t_2y^3 - t_3y^2 + t_4y - t_5$ be $y = \beta_1, \beta_2, \beta_3, \beta_4, \beta_5$.

Note that $\sum_{i=1}^{5} \beta_i = 0$, $\sum_{i<j} \beta_i \beta_j = t_2$.

Let $\gamma_i = \beta_i^2 + a\beta_i + b$ and choose $a$ and $b$ so that $\sum_{i=1}^{5} \gamma_i = 0$, $\sum_{i<j} \gamma_i \gamma_j = 0$

$\rightarrow \quad a = \frac{3t_3}{2t_2} \pm \sqrt{\frac{3t_2}{5} - \frac{2t_4}{t_2} + \frac{9t_3^2}{4t_2^2}}, \quad b = \frac{2t_2}{5}$

Then, $z = \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$ will be the roots of a quintic equation in $z$ without the $z^4$ and $z^3$ terms:

$0 = z^5 - u_3z^3 + u_4z - u_5$ (principal quintic form)

where $u_3, u_4, u_5$ are complicated functions of $t_2, t_3, t_4$, and $t_5$. 
Let the five roots of $0 = z^5 - u_3z^2 + u_4z - u_5$ be $y = \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$.

Note that $\sum_{i=1}^{5} \gamma_i = 0$, $\sum_{i<j} \gamma_i \gamma_j = 0$, $\sum_{i<j<k} \gamma_i \gamma_j \gamma_k = u_3$.

Let $\delta_i = \gamma_i^4 + a\gamma_i^3 + b\gamma_i^2 + c\gamma_i + d$ and choose $a, b, c$ and $d$ so that

\[
\sum_{i=1}^{5} \delta_i = 0, \quad \sum_{i<j} \delta_i \delta_j = 0, \quad \sum_{i<j<k} \delta_i \delta_j \delta_k = 0
\]

\[d = \frac{4u_4 - 3u_3a}{5}, \quad b = -\frac{5u_5 - 4u_4a}{3u_3}, \quad a = \text{solution to a quadratic, } c = \text{solution to a cubic}\]

Then, $\zeta = \delta_1, \delta_2, \delta_3, \delta_4, \delta_5$ will be the roots of a quintic equation in $\zeta$ without the $\zeta^4, \zeta^3$ and $\zeta^2$ terms:

$0 = \zeta^5 + v_4\zeta^4 - v_5$ \hspace{1cm} (Bring - Jerrard normal form)

where $v_4, v_5$ are very complicated functions of $u_3, u_4,$ and $u_5$. 
0 = \zeta^5 + v_4 \zeta - v_5

\downarrow

0 = \frac{\zeta^5}{(v_4)^{5/4}} + \frac{\zeta}{(v_2)^{1/4}} - \frac{v_5}{(v_2)^{5/4}}

\downarrow

0 = \xi^5 + \xi - a

\downarrow

\xi^5 + \xi = a
\[ \xi^5 + \xi = a \]
\[ \downarrow \]
\[ \xi = \sum_{k=0}^{\infty} \left( \frac{5k}{k} \right) \frac{(-1)^k a^{4k+1}}{4k+1} = a - a^5 + 5 a^9 - 35 a^{13} + \text{L} \]