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.

SPONTANEOUS SYMMETRY BREAKING 1

- The solution does not have the symmetry manifest in the equation.
- Example: particle in a left-right symmetric potential V(x)

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

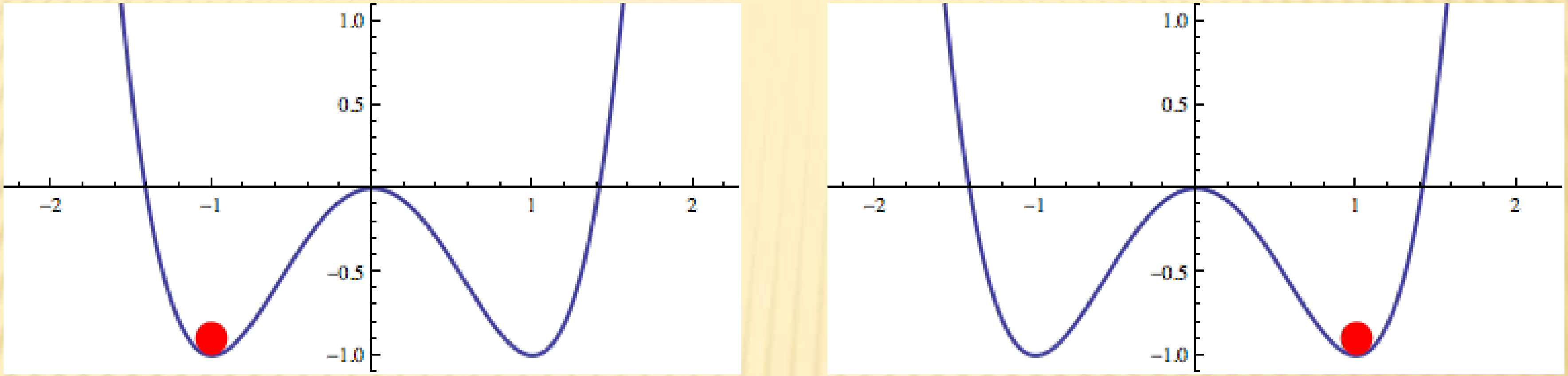
Equation is invariant under the parity transformation $x \leftrightarrow -x$

but the solution may not be.

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

$$\frac{dV(x)}{dx} = 4x(x^2-1) = 0 \quad \rightarrow \quad x^2 = 1 \quad \rightarrow \quad x = \pm 1$$

SPONTANEOUS SYMMETRY BREAKING 2



- 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?

- Born Oct. 25, 1811 in a suburb of Paris.
- 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 (□) 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.
  cf. "Les Misérables" by Victor Hugo, musical by Claude-Michel Schönberg, movie coming in 2012.

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?

BRIEF HISTORY OF ALGEBRAIC EQUATIONS

$$\begin{aligned} \text{Linear} &: ax+b=0 \\ \text{Quadratic} &: ax^2+bx+c=0 \\ \text{Cubic} &: ax^3+bx^2+cx+d=0 \\ \text{Quartic} &: ax^4+bx^3+cx^2+dx+e=0 \\ \text{Quintic} &: ax^5+bx^4+cx^3+dx^2+ex+f=0 \end{aligned}$$

- The solution formula for the quadratic equation was known worldwide since ancient times. (Can be found on mesopotamian cuniform tablets.)
- Solution formulae to the cubic and the quartic were discovered during the 16th century in Italy.
- The formula for the quintic could not be found. Proved that it did not exist independently by Neils Henrik Abel (Norwegian, 1802-1829) and 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)

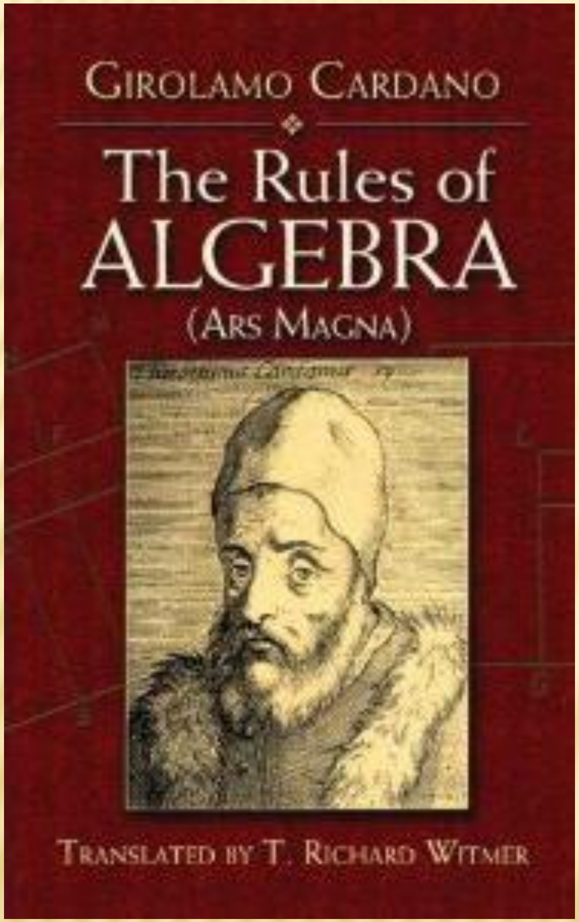
Geralomo Cardano
(1501-1576)

?

Lodovico Ferrari
(1522-1565)

- Del Ferro discovers solution to the special case $x^3+px=q, \quad p>0, \quad q>0$.
- 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.

READ ALL ABOUT IT IN…



First published in 1545

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:

$$x^3 + px = q$$
$$x^3 = px + q$$
$$x^3 + q = px$$
$$x^3 + px^2 = q$$
$$x^3 = px^2 + q$$
$$x^3 + q = px^2$$
$$x^3 + px^2 + qx = r$$
$$x^3 + px^2 = qx + r$$
$$x^3 = px^2 + qx + r$$
$$x^3 + qx = px^2 + r$$
$$x^3 + r = px^2 + qx$$
$$x^3 + qx + r = px^2$$
$$x^3 + px^2 + r = qx$$

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

$$0 = ax^2 + bx + c$$

$$\downarrow$$

Divide both sides by *a*,
then complete the square:

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

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

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

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

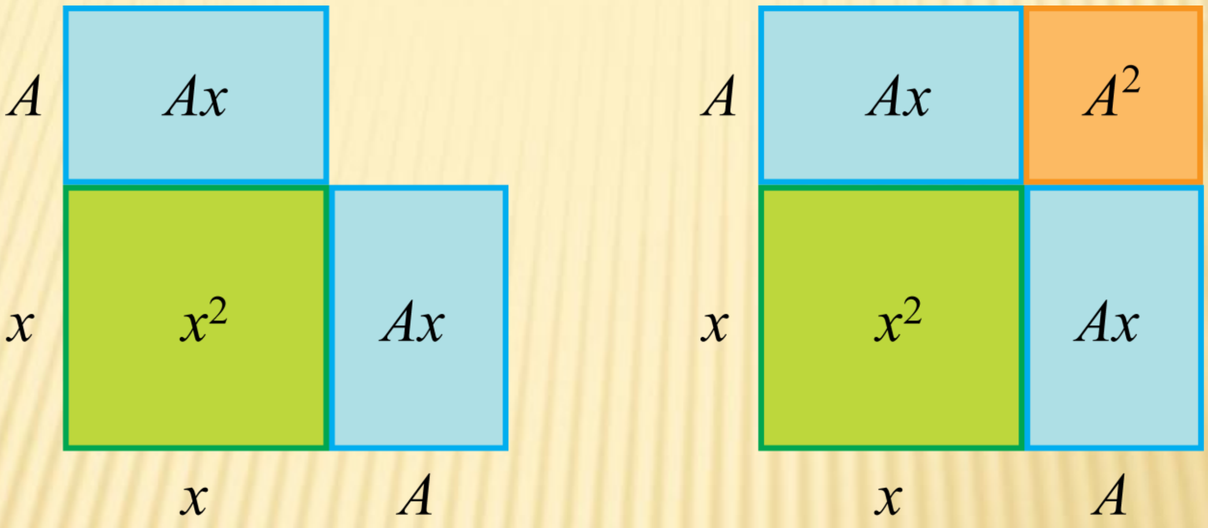
$$\downarrow$$

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

$$\downarrow$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

COMPLETING THE SQUARE:



$$x^2 + 2Ax \quad \rightarrow \quad x^2 + 2Ax + A^2 = (x + A)^2$$

RELATION BETWEEN COEFFICIENTS AND ROOTS

$$x^2 - s_1 x + s_2 = (x - \alpha_1)(x - \alpha_2)$$

$$\downarrow$$

$$s_1 = \alpha_1 + \alpha_2$$

$$s_2 = \alpha_1 \alpha_2$$

- 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:

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

$$\downarrow$$

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

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

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

$$= y^3 + py + q$$

Cubic Equation – Step 2

Let $y = u + v$:

$$\begin{aligned} 0 &= y^3 + py + q \\ &= (u+v)^3 + p(u+v) + q \\ &= (u^3 + v^3 + q) + (3uv + p)(u+v) \end{aligned}$$

$\downarrow$

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

$\downarrow$

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

u^3 and v^3 are solutions to:

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

$\downarrow$

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

$\downarrow$

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

$\downarrow$

$$y = \begin{cases} u + v \\ u\omega + v\omega^2 \\ u\omega^2 + v\omega \end{cases} \qquad \text{where } \omega^3 = 1.$$

RELATION BETWEEN COEFFICIENTS AND ROOTS

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

$$\downarrow$$

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3$$

$$s_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1$$

$$s_3 = \alpha_1\alpha_2\alpha_3$$

- 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.

QUARTIC EQUATION – STEP 1

Complete the 4D-hypercube to eliminate the x^3 term:

$$0 = ax^4 + bx^3 + cx^2 + dx + e$$

$$\downarrow$$

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

$$= \left(x + \frac{b}{4a}\right)^4 + \underbrace{\left(\frac{c}{a} - \frac{3b^2}{8a^2}\right)}_{p}\left(x + \frac{b}{4a}\right)^2 + \underbrace{\left(\frac{d}{a} - \frac{bc}{2a^2} + \frac{b^3}{8a^3}\right)}_{q}\left(x + \frac{b}{4a}\right)$$

$$+ \underbrace{\left(\frac{e}{a} - \frac{bd}{4a^2} + \frac{b^2c}{16a^3} - \frac{3b^4}{256a^4}\right)}_{r}$$

$$= y^4 + py^2 + qy + r$$

QUARTIC EQUATION – STEP 2 – FERRARI

$$-py^2 - qy - r = y^4$$

$$(2t - p)y^2 - qy + (t^2 - r) = y^4 + (2ty^2 + t^2) = (y^2 + t)^2$$

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:

$$(2t - p)y^2 - qy + (t^2 - r) = (Ay + B)^2 = (y^2 + t)^2$$

$$\downarrow$$

$$\pm(Ay + B) = y^2 + t$$

QUARTIC EQUATION – STEP 2 – EULER

Let $y = u + v + w$:

$$\begin{aligned}
0 &= y^4 + py^2 + qy + r \\
&= (u+v+w)^4 + p(u+v+w)^2 + q(u+v+w) + r \\
&= \left[(u^2+v^2+w^2)^2 + p(u^2+v^2+w^2) + 4(u^2v^2+v^2w^2+w^2u^2) + r\right] \\
&\quad + \left[4(u^2+v^2+w^2) + 2p\right](uv+vw+wu) + \left[8uvw + q\right](u+v+w)
\end{aligned}$$

$$\downarrow$$

$$-\frac{q}{8} = uvw \qquad \rightarrow \qquad \frac{q^2}{64} = u^2v^2w^2$$

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

$$\frac{p^2 - 4r}{16} = u^2v^2 + v^2w^2 + w^2u^2$$

QUARTIC EQUATION – STEP 3 – EULER

u^2, v^2, and w^2 are solutions to:

$$0 = z^3 + \frac{p}{2}z^2 + \frac{p^2-4r}{16}z - \frac{q^2}{64} \qquad \left(z = \frac{2t-p}{4}\right)$$

$$\downarrow$$

$$z = z_1, z_2, z_3$$

$$\downarrow$$

$$u = \sqrt{z_1}, \quad v = \sqrt{z_2}, \quad w = \sqrt{z_3}, \quad \sqrt{z_1}\sqrt{z_2}\sqrt{z_3} = -\frac{q}{8}$$

$$\downarrow$$

$$y = \begin{cases} u+v+w \\ u-v-w \\ -u+v-w \\ -u-v+w \end{cases}$$

FERRARI–EULER COMPARISON

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

Euler $\quad z = u^2 \quad \leftrightarrow \quad t = u^2 - v^2 - w^2 \quad$ Ferrari

$$\underbrace{(2t-p)}_{4u^2}y^2 - \underbrace{q}_{8uvw}\, y + \underbrace{(t^2 - r)}_{4v^2w^2} = (y^2 + \underbrace{t}_{u^2 - v^2 - w^2})^2$$

$$\downarrow$$

$$\pm 2(uy + vw) = y^2 + \left(u^2 - v^2 - w^2\right)$$

$$\downarrow$$

$$y^2 \mp 2uy + \left[u^2 - (v \pm w)^2\right] = 0$$

$$\downarrow$$

$$\left[y - (u + v + w)\right]\left[y - (u - v - w)\right] = 0 \quad \to \quad y = u + v + w, \quad u - v - w$$

$$\left[y + (u + v - w)\right]\left[y + (u - v + w)\right] = 0 \quad \to \quad y = -u - v + w, \quad -u + v - w$$

RELATION BETWEEN COEFFICIENTS AND ROOTS

$$x^4 - s_1 x^3 + s_2 x^2 - s_3 x + s_4 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$$

$$\downarrow$$

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$$

$$s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4$$

$$s_3 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4$$

$$s_4 = \alpha_1\alpha_2\alpha_3\alpha_4$$

- 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:

$$0 = x^N - s_1 x^{N-1} + s_2 x^{N-2} + \cdots + (-1)^{N-1} s_{N-1} x + (-1)^N s_N$$
$$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_{N-1})(x-\alpha_N)$$

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_{N-1} + \alpha_N$$
$$s_2 = \sum_{i<j} \alpha_i \alpha_j$$
$$s_3 = \sum_{i<j<k} \alpha_i \alpha_j \alpha_k$$
$$\vdots$$
$$s_N = \alpha_1 \alpha_2 \alpha_3 \cdots \alpha_{N-1} \alpha_N$$

- 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:

$$
\begin{aligned}
s_1 &= \alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_{N-1} + \alpha_N \\
s_2 &= \sum_{i<j} \alpha_i \alpha_j \\
s_3 &= \sum_{i<j<k} \alpha_i \alpha_j \alpha_k \\
&\vdots \\
s_N &= \alpha_1 \alpha_2 \alpha_3 \cdots \alpha_{N-1} \alpha_N
\end{aligned}
\quad \Rightarrow \quad
\begin{aligned}
\alpha_1 &= f_1(s_1, s_2, s_3, \cdots s_{N-1}, s_N) \\
\alpha_2 &= f_2(s_1, s_2, s_3, \cdots s_{N-1}, s_N) \\
\alpha_3 &= f_3(s_1, s_2, s_3, \cdots s_{N-1}, s_N) \\
&\vdots \\
\alpha_{N-1} &= f_{N-1}(s_1, s_2, s_3, \cdots s_{N-1}, s_N) \\
\alpha_N &= f_N(s_1, s_2, s_3, \cdots s_{N-1}, s_N)
\end{aligned}
$$

- Solution formulae must invert the relations between the coefficients and the roots and express the roots in terms of the coefficients.

IMPOSSIBLITY OF SOLUTION FORMULAE:

$$\alpha_i = f_i(s_1, s_2, s_3, \cdots s_{N-1}, s_N)$$

- 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

$$a, b \in G \quad \rightarrow \quad a \circ b \in G$$

  - Group multiplication is associative

$$(a \circ b) \circ c = a \circ (b \circ c)$$

  - Unit element exists

$$\exists e \in G \text{ such that} \qquad e \circ a = a \circ e = a \qquad \forall a \in G$$

  - Inverse element exists for every element

$$\forall a \in G, \quad \exists a^{-1} \in G \text{ such that} \qquad a \circ a^{-1} = a^{-1} \circ a = e$$

GROUP OF SYMMETRY TRANSFORMATIONS

- "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

- The group formed by all possible permutations of N objects is called the symmetric group and denoted S_N. It has N! elements.
- Examples:

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

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

$$\begin{aligned} S_4 = \{e, &(12), (13), (14), (23), (24), (34), \\ &(12)(34), (13)(24), (14)(23), \\ &(123), (132), (124), (142), (134), (143), (234), (243), \\ &(1234), (1243), (1324), (1342), (1423), (1432)\} \end{aligned}$$

NOTATION:

$$\begin{aligned} e &: \text{ do nothing} \\ (12) &: 1 \to 2 \to 1 \\ (123) &: 1 \to 2 \to 3 \to 1 \\ (1234) &: 1 \to 2 \to 3 \to 4 \to 1 \\ (123)(45) &: 1 \to 2 \to 3 \to 1, \quad 4 \to 5 \to 4 \qquad \text{etc.} \end{aligned}$$

$$\begin{pmatrix} 1\,2\,3\,4 \\ \downarrow\downarrow\downarrow\downarrow \\ 4\,1\,3\,2 \end{pmatrix} = (142), \qquad \begin{pmatrix} 1\,2\,3\,4\,5 \\ \downarrow\downarrow\downarrow\downarrow\downarrow \\ 5\,1\,4\,2\,3 \end{pmatrix} = (15342)$$

SUBGROUPS

- A Group H contained inside another Group G is called a subgroup of G, e.g.:

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

$$\text{Subgroups} \;:\; \{e\}, \quad S_2 = \{e, (12)\}, \quad S_2' = \{e, (13)\}, \quad S_2'' = \{e, (23)\},$$
$$C_3 = \{e, (123), (132)\}$$

- The number of elements in a subgroup is always a divisor of the number of element in the parent group. (Lagrange's theorem.)

COSETS

- 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.

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

$$\text{Subgroup} \ : \ S_2 = \{e, (12)\}$$

$$\text{Cosets}: \ eS_2 = \{e, (12)\}, \quad (13)S_2 = \{(13), (123)\}, \quad (23)S_2 = \{(23), (132)\}$$

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

$$\text{Subgroup} \ : \ C_3 = \{e, (123), (132)\}$$

$$\text{Cosets}: \ eC_3 = \{e, (123), (132)\}, \quad (13)C_3 = \{(13), (12), (23)\}$$

CONJUGACY CLASSES

- 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.

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

$$\begin{aligned} S_4: \quad & \{e\}, \quad \{(12),(13),(14),(23),(24),(34)\}, \quad \{(12)(34),(13)(24),(14)(23)\}, \\ & \{(123),(132),(124),(142),(134),(143),(234),(243)\}, \\ & \{(1234),(1243),(1324),(1342),(1423),(1432)\} \end{aligned}$$

INVARIANT SUBGROUPS

- 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.

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

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

- 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:

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

$$\text{discriminant} \qquad \Delta_2 = s_1^2 - 4s_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (\alpha_1 - \alpha_2)^2$$

- 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}.

$$\sqrt{\Delta_2} \xleftrightarrow{(12)} -\sqrt{\Delta_2}$$

- The square-root of the discriminant serves as a basis for a 1x1 representation of S_2 :

$$e \rightarrow \left[1\right], \quad (12) \rightarrow \left[-1\right]$$

SOLUTION TO THE CUBIC REVISITED 1:

$$x^3 - s_1 x^2 + s_2 x - s_3 = 0 \quad \rightarrow \quad y^3 + py + q = 0$$

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

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

$$\begin{aligned} \text{discriminant} \qquad \Delta_3 &= -27q^2 - 4p^3 \\ &= s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 + 18 s_1 s_2 s_3 - 27 s_3^2 \\ &= (\alpha_1 - \alpha_2)^2 (\alpha_2 - \alpha_3)^2 (\alpha_3 - \alpha_1)^2 \end{aligned}$$

$$\sqrt{\Delta_3} = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \quad \text{or} \quad -(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$$

SOLUTION TO THE CUBIC REVISITED 2:

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

$$\sqrt{\Delta_3} \xleftrightarrow{(12)(13)(23)} -\sqrt{\Delta_3}$$

- 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.

$$eC_3 = \{e,(123),(132)\} \to [1], \qquad (12)C_3 = \{(12),(13),(23)\} \to [-1]$$

THE QUOTIENT GROUP

- 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 $aH\,bH = a(Hb)H = a(bH)H = (ab)HH = (ab)H$.
  The group formed by this group multiplication is call the quotient group G/H.

SOLUTION TO THE CUBIC REVISITED 3:

- Taking the cubic roots of $z_\pm$ breaks C_3={e,(123),(132)} down to the trivial invariant subgroup {e}.

$$z_+ = \left(\frac{\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3}{3}\right)^3, \qquad z_- = \left(\frac{\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3}{3}\right)^3$$

$$\downarrow$$

$$\sqrt[3]{z_+} = \frac{\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3}{3}, \qquad \sqrt[3]{z_-} = \frac{\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3}{3}$$

$$\sqrt[3]{z_+} \xrightarrow{(123)} \omega\sqrt[3]{z_+} \xrightarrow{(123)} \omega^2\sqrt[3]{z_+}$$

$$\sqrt[3]{z_-} \xrightarrow{(132)} \omega\sqrt[3]{z_-} \xrightarrow{(132)} \omega^2\sqrt[3]{z_-}$$

SOLUTION TO THE CUBIC REVISITED 4:

- The cubic roots of $z_{\pm}$ provide a basis for a 1x1 representation of C_3={e,(123),(132)}:

$$\sqrt[3]{z_+} \quad : \quad e \to [1], \quad (123) \to [\omega], \quad (132) \to [\omega^2]$$

$$\sqrt[3]{z_-} \quad : \quad e \to [1], \quad (123) \to [\omega^2], \quad (132) \to [\omega]$$

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

$$e \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (123) \to \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}, \quad (132) \to \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega \end{bmatrix}$$

$$(23) \to \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (12) \to \begin{bmatrix} 0 & \omega \\ \omega^2 & 0 \end{bmatrix}, \quad (13) \to \begin{bmatrix} 0 & \omega^2 \\ \omega & 0 \end{bmatrix}$$

SOLUTION TO THE QUARTIC – OUTLINE 1:

$$x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 = 0 \quad \to \quad y^4 + py^2 + qy + r = 0$$

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

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

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

$$\xi^2 + Q\xi - \frac{P^3}{27} = 0 \qquad \to \qquad \xi_\pm = -\frac{Q}{2} \pm \frac{i}{384}\sqrt{\frac{\Delta_4}{3}}$$

$$\begin{aligned}
\Delta_4 &= s_1^2s_2^3s_3^2 - 4s_2^3s_3^2 - 4s_1^3s_3^3 + 18s_1s_2s_3^3 - 27s_3^4 - 4s_1^2s_2^3s_4 + 16s_2^4s_4 \\
&\quad + 18s_1^3s_2s_3s_4 - 80s_1s_2^3s_3s_4 - 6s_1^2s_3^2s_4 + 144s_2s_3^2s_4 - 27s_1^4s_4^2 \\
&\quad + 144s_1^2s_2s_4^2 - 128s_2^2s_4^2 - 192s_1s_3s_4^2 + 256s_4^3 \\
&= (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_3-\alpha_4)^2
\end{aligned}$$

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

$$= -(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)(\alpha_3-\alpha_4)$$

$$\sqrt{\Delta_4} \xleftrightarrow{\text{odd permutations}} -\sqrt{\Delta_4}$$

- Symmetry breaks from S_4 to the invariant subgroup A_4={all even permutations}.

$$eA_4 = \{\text{all even permutations}\} \quad \to \quad [1]$$

$$(12)A_4 = \{\text{all odd permutations}\} \quad \to \quad [-1]$$

$$S_4 / A_4 = \{e, (12)\}$$

SOLUTION TO THE QUARTIC – OUTLINE 3:

$$\sqrt[3]{\xi_+} \xrightarrow{(132)(234)(124)(143)} \omega\sqrt[3]{\xi_+} \xrightarrow{(132)(234)(124)(143)} \omega^2\sqrt[3]{\xi_+}$$

$$\sqrt[3]{\xi_-} \xrightarrow{(123)(134)(243)(142)} \omega\sqrt[3]{\xi_-} \xrightarrow{(123)(134)(243)(142)} \omega^2\sqrt[3]{\xi_-}$$

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

$$\begin{array}{rlccc}
 & & & \sqrt[3]{\xi_+} & \sqrt[3]{\xi_-} \\
eV & = \{e,(12)(34),(13)(24),(14)(23)\} & \to & [1] & [1] \\
(123)V & = \{(123),(134),(243),(142)\} & \to & [\omega^2] & [\omega] \\
(132)V & = \{(132),(234),(124),(143)\} & \to & [\omega] & [\omega^2] \\
A_4/V & = \{e,(123),(132)\} & & &
\end{array}$$

SOLUTION TO THE QUARTIC – OUTLINE 4:

$$\sqrt{z_1} \xleftrightarrow{(13)(24),\,(14)(23)} -\sqrt{z_1}$$

$$\sqrt{z_2} \xleftrightarrow{(12)(34),\,(14)(23)} -\sqrt{z_2}$$

$$\sqrt{z_3} \xleftrightarrow{(12)(34),\,(13)(24)} -\sqrt{z_3}$$

- 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:

$$S_2 \xrightarrow{\sqrt{\Delta_2}} \{e\}$$

$$S_3 \xrightarrow{\sqrt{\Delta_3}} C_3 \xrightarrow{\sqrt[3]{z}} \{e\}$$

$$S_4 \xrightarrow{\sqrt{\Delta_4}} A_4 \xrightarrow{\sqrt[3]{\xi}} V \xrightarrow{\sqrt{z_1}} \{e,(12)(34)\} \xrightarrow{\sqrt{z_2}\sqrt{z_3}} \{e\}$$

- 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.

THE SYMMETRIC GROUP S_5

- 5!=120 elements, 60 odd and 60 even, 7 conjugacy classes:

$$\left.\begin{array}{rcl} e & : & 1 \text{ element} \\ (**)(**) & : & 15 \text{ elements} \\ (***) & : & 20 \text{ elements} \\ (*****) & : & 24 \text{ elements} \end{array}\right\} \text{even, } A_5$$

$$\left.\begin{array}{rcl} (**) & : & 10 \text{ elements} \\ (***)(**) & : & 20 \text{ elements} \\ (****) & : & 30 \text{ elements} \end{array}\right\} \text{odd}$$

- A_5 is an invariant subgroup of S_5 and S_5/A_5={e,(12)}.

DISCRIMINANT OF THE QUINTIC

$$
\begin{aligned}
\Delta_5 = {} & s_1^2 s_2^2 s_3^2 s_4^2 - 4 s_2^3 s_3^2 s_4^2 - 4 s_1^3 s_3^3 s_4^2 + 18 s_1 s_2 s_3^3 s_4^2 - 27 s_3^4 s_4^2 - 4 s_1^2 s_2^3 s_4^3 + 16 s_2^4 s_4^3 + 18 s_1^3 s_2 s_3 s_4^3 \\
& - 80 s_1 s_2^2 s_3 s_4^3 - 6 s_1^2 s_3^2 s_4^3 + 144 s_2 s_3^2 s_4^3 - 27 s_1^4 s_4^4 + 144 s_1^2 s_2 s_4^4 - 128 s_2^2 s_4^4 - 192 s_1 s_3 s_4^4 + 256 s_4^5 \\
& - 4 s_1^2 s_2^2 s_3^3 s_5 + 16 s_2^3 s_3^3 s_5 + 16 s_1^3 s_3^4 s_5 - 72 s_1 s_2 s_3^4 s_5 + 108 s_3^5 s_5 + 18 s_1^2 s_2^3 s_3 s_4 s_5 - 72 s_2^4 s_3 s_4 s_5 \\
& - 80 s_1^3 s_2 s_3^2 s_4 s_5 + 356 s_1 s_2^2 s_3^2 s_4 s_5 + 24 s_1^2 s_3^3 s_4 s_5 - 630 s_2 s_3^3 s_4 s_5 - 6 s_1^3 s_2^2 s_4^2 s_5 + 24 s_1 s_2^3 s_4^2 s_5 + 144 s_1^4 s_3 s_4^2 s_5 \\
& - 746 s_1^2 s_2 s_3 s_4^2 s_5 + 560 s_2^2 s_3 s_4^2 s_5 + 1020 s_1 s_3^2 s_4^2 s_5 - 36 s_1^3 s_4^3 s_5 + 160 s_1 s_2 s_4^3 s_5 - 1600 s_3 s_4^3 s_5 \\
& - 27 s_1^2 s_2^4 s_5^2 + 108 s_2^5 s_5^2 + 144 s_1^3 s_2^2 s_3 s_5^2 - 630 s_1 s_2^3 s_3 s_5^2 - 128 s_1^4 s_3^2 s_5^2 + 560 s_1^2 s_2 s_3^2 s_5^2 \\
& + 825 s_2^2 s_3^2 s_5^2 - 900 s_1 s_3^3 s_5^2 - 192 s_1^4 s_2 s_4 s_5^2 + 1020 s_1^2 s_2^2 s_4 s_5^2 - 900 s_2^3 s_4 s_5^2 + 160 s_1^3 s_3 s_4 s_5^2 \\
& - 2050 s_1 s_2 s_3 s_4 s_5^2 + 2250 s_3^2 s_4 s_5^2 - 50 s_1^2 s_4^2 s_5^2 + 2000 s_2 s_4^2 s_5^2 \\
& + 256 s_1^5 s_5^3 - 1600 s_1^3 s_2 s_5^3 + 2250 s_1 s_2^2 s_5^3 + 2000 s_1^2 s_3 s_5^3 - 3750 s_2 s_3 s_5^3 - 2500 s_1 s_4 s_5^3 + 3125 s_5^4
\end{aligned}
$$

$$
= (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_1-\alpha_5)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_2-\alpha_5)^2(\alpha_3-\alpha_4)^2(\alpha_3-\alpha_5)^2(\alpha_4-\alpha_5)^2
$$

- 59 terms!
- By taking the square-root of this discriminat, it is indeed possible to break S_5 down to A_5.

THE ALTERNATING GROUP A_5

- 60 elements, 5 conjugacy classes:

$$\begin{aligned} e &: \ 1 \text{ element} \\ (**)(**) &: \ 15 \text{ elements} \\ (***) &: \ 20 \text{ elements} \\ (*****) &: \ 12 \text{ elements} \\ (*****) &: \ 12 \text{ elements} \end{aligned}$$

- 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≥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 □: 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 Nε5.

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.

SOLUTION TO THE QUINTIC - STEP 1 COMPLETING THE 5D HYPERCUBE

Complete the 5D-hypercube to eliminate the x^4 term:

$$\begin{aligned}
0 &= x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5 \\
&= \left(x - \frac{s_1}{5}\right)^5 + \underbrace{\left(s_2 - \frac{2s_1^{\,2}}{5}\right)}_{t_2}\left(x - \frac{s_1}{5}\right)^3 - \underbrace{\left(s_3 - \frac{3s_1s_2}{5} + \frac{4s_1^{\,3}}{25}\right)}_{t_3}\left(x - \frac{s_1}{5}\right)^2 \\
&\quad + \underbrace{\left(s_4 - \frac{2s_1s_3}{5} + \frac{3s_1^{\,2}s_2}{25} - \frac{3s_1^{\,4}}{125}\right)}_{t_4}\left(x - \frac{s_1}{5}\right) - \underbrace{\left(s_5 - \frac{s_1s_4}{5} + \frac{s_1^{\,2}s_3}{25} - \frac{s_1^{\,3}s_2}{125} + \frac{4s_1^{\,5}}{3125}\right)}_{t_5} \\
&= y^5 + t_2y^3 - t_3y^2 + t_4y - t_5
\end{aligned}$$

$$y = x - \frac{s_1}{5}$$

SOLUTION TO THE QUINTIC - STEP 1 ALTERNATIVE POINT OF VIEW

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 $\sum_{i=1}^{5} \beta_i = 0 \quad \rightarrow \quad a = -\frac{s_1}{5}$.

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:

$$0 = y^5 + t_2 y^3 - t_3 y^2 + t_4 y - t_5$$

SOLUTION TO THE QUINTIC - STEP 2 TSCHIRNHAUSEN TRANSFORMATION (1683)

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

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

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

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

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:

$0 = z^5 - u_3 z^2 + u_4 z - u_5$ (principal quintic form)

where u_3, u_4, u_5 are complicated functions of t_2, t_3, t_4, and t_5.

SOLUTION TO THE QUINTIC - STEP 3 BRING (1786)-JERRARD (1852)

Let the five roots of $0 = z^5 - u_3 z^2 + u_4 z - u_5$ be $y = \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$.

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

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

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

$$\rightarrow \quad d = \frac{4u_4 - 3u_3 a}{5}, \quad b = -\frac{5u_5 - 4u_4 a}{3u_3},$$

$$a = \text{solution to a quadratic}, \quad c = \text{solution to a cubic}$$

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

$0 = \zeta^5 + v_4 \zeta - v_5$ (Bring - Jerrard normal form)

where v_4, v_5 are very complicated functions of u_3, u_4, and u_5.

SOLUTION TO THE QUINTIC - STEP 4 RESCALE

$$0 = \zeta^5 + v_4 \zeta - v_5$$

$$\downarrow$$

$$0 = \frac{\zeta^5}{(v_4)^{5/4}} + \underbrace{\frac{\zeta}{(v_4)^{1/4}}}_{\xi} - \underbrace{\frac{v_5}{(v_4)^{5/4}}}_{a}$$

$$\downarrow$$

$$0 = \xi^5 + \xi - a$$

$$\downarrow$$

$$\xi^5 + \xi = a$$

SOLUTION TO THE QUINTIC – STEP 5 INVERT RELATION

$$\xi^5 + \xi = a$$

$$\downarrow$$

$$\xi = \sum_{k=0}^{\infty} \binom{5k}{k} \frac{(-1)^k a^{4k+1}}{4k+1} = a - a^5 + 5a^9 - 35a^{13} + \ldots$$