Solutions and Permutations (2008)

I studied the formulas for the solutions of quadratic equation in the third year of junior high school and the Cardan's formulas and Ferarri's method in a freshman year of college. At the last stage of the theory of equations, I studied Galois theory in a sophomore year. I would like to briefly state the theory of equations and let it be a data on my consideration.

1. Formulas for the solutions of equation

We can find the formulas by using the following factorization.

1) $a^2-b^2 = (a + b)(a-b)$

2) $a^3 + b^3 + c^3-3abc = (a + b + c)(a^2 + b^2 + c^2-ab-ac-bc)$

3) $a^4 + b^4 + c^4 + d^4-2(a^2b^2 + a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + c^2d^2)-8abcd$

$= - (- a + b + c + d)(a-b + c + d)(a + b-c + d)(a + b + c-d)$

(1) For the general quadratic equation $x^2-bx + c = 0$,

setting $x = y + \frac{b}{2}$, ……(A)

we find an adjoint equation $y^2-p^2 = 0$ where $p = \frac{\sqrt{D}}{2}$, $D = b^2-4c$.

By 1)

$$y = \pm p = \pm \frac{\sqrt{D}}{2}$$

By (A)

$$x = \frac{b \pm \sqrt{D}}{2}$$

(2) For the general cubic equation $x^3-bx^2 + cx-d = 0$,

setting $x = y + \frac{b}{3}$, ……(B)

we find $y^3 + py-q = 0$ where $p = c-\frac{b^2}{3}$, $q = d-\frac{bc}{3} + \frac{2b^3}{27}$.

Setting $p = - 3uv$, $q = u^3 + v^3$, we find

$u^3 + v^3 = q$, $u^3v^3 = (- \frac{p}{3})^3$.

Because u^3, v^3 are solutions of the adjoint equation $t^2-qt + (- \frac{p}{3})^3 = 0$,

$$t = \frac{q}{2} \pm \sqrt{R} \quad \text{where} \quad R = (\frac{q}{2})^2 + (\frac{p}{3})^3.$$

$$\therefore u = \sqrt[3]{\frac{q}{2} + \sqrt{R}}, \quad v = \sqrt[3]{\frac{q}{2}-\sqrt{R}}.$$

By 2) $y^3 + u^3 + v^3 - 3uvy = (y + u + v)(y^2 + u^2 + v^2 - yu - yv - uv)$

$= (y + u + v)(y + uy + vy^2)(y + vy + uy^2).$

$\therefore\ y = -u - v,\ -uy - vy^2,\ -vy - uy^2.$

By (B)

$$x = \frac{b}{3} - u - v,\quad \frac{b}{3} - uy - vy^2,\quad \frac{b}{3} - vy - uy^2.$$

R*emark*: y : *a* primitive cubic root of unity, $y^3 = 1,\ 1 + y + y^2 = 0.$

(3) For the general biquadratic equation $x^4 - bx^3 + cx^2 - dx + e = 0,$

setting $x = y + \frac{b}{4},$ ……(C)

we find $y^4 + py^2 - qy + r = 0$

where $p = c - \frac{3b^2}{8},\ q = d - \frac{bc}{2} + \frac{b^3}{8},\ r = e - \frac{bd}{4} + \frac{b^2c}{16} - \frac{3b^4}{256}.$

Setting $p = -2(u^2 + v^2 + w^2),$

$q = 8uvw,\ r = u^4 + v^4 + w^4 - 2(u^2v^2 + u^2w^2 + v^2w^2),$ ……(D)

the given equation is factorized by 3) as follows;

$y^4 - 2(u^2 + v^2 + w^2)y - 8uvwy + \{u^4 + v^4 + w^4 - 2(u^2v^2 + u^2w^2 + v^2w^2)\}$

$= -(-y + u + v + w)(y - u + v + w)(y + u - v + w)(y + u + v - w)$

By (D)

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

$u^2v^2w^2 = (\frac{q}{8})^2$

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

Because $u^2,\ v^2,\ w^2$ are the solutions for cubic equation $(t - u^2)(t - v^2)(t - w^2) = 0,$

we find

$t^3 - (u^2 + v^2 + w^2)t^2 + (u^2v^2 + u^2w^2 + v^2w^2)t - u^2v^2w^2 = 0.$

$\therefore\ t^3 + \frac{p}{2}t^2 + (\frac{p^2}{16} - \frac{r}{4})t - (\frac{q}{8})^2 = 0$ (Adjoint equation)

This reduces to (2).

Remark: We can find the roots of equation from which coefficients by algebraic operations and radical extensions. Since the coefficients of equation are symmetric expressions, the coefficients do not change by permutation on the solutions. That is why the Galois extensions begin with an isomorphism.

2. The solutions of adjoint equation and permutation

The solutions of adjoint equation do not change by permutation on the solutions.

(1) We can replace the quadratic equation $x^2 + px - q = 0$ by the following adjoint equation.

$$y^2 - p^2 = 0 \quad \text{where} \quad p = \frac{\sqrt{D}}{2}$$

Let x_1, *and* x_2 be the solutions of the given equation,

$$D = (x_1 - x_2)^2$$

$$\therefore\ y^2 = \frac{1}{4}(x_1 - x_2)^2$$

$$y = \frac{1}{2}(x_1 - x_2), \quad \frac{1}{2}(x_2 - x_1)$$

Therefore the solutions of adjoint equation are not changed by the permutation on x_1 *and* x_2.

(2) We can replace the following cubic equation,

$$t^2 - qt + (-\frac{p}{3})^3 = 0$$

$$\text{where} \quad p = c - \frac{b^2}{3}, \quad q = d - \frac{bc}{3} + \frac{2b^3}{27}.$$

Let x_1, x_2 and x_3, be the solutions of the given equation and u and v be the solutions of the adjoint equation.

$$x_1 = -\frac{b}{3a} + u + v, \quad x_2 = -\frac{b}{3a} + uy + vy^2, \quad x_3 = -\frac{b}{3a} + uy^2 + vy$$

Since $y^3 = 1$, $y^2 + y + 1 = 0$,

$$u = \frac{1}{3}(x_1 + yx_3 + y^2x_2), \quad v = \frac{1}{3}(x_1 + yx_2 + y^2x_3)$$

$$uy = \frac{1}{3}(x_2 + yx_1 + y^2x_3), \quad vy = \frac{1}{3}(x_3 + yx_1 + y^2x_2)$$

$$uy^2 = \frac{1}{3}(x_3 + yx_2 + y^2x_1), \quad vy^2 = \frac{1}{3}(x_2 + yx_3 + y^2x_1)$$

Since the adjoint equation is a rational equation of x_1, x_2 and x_3, we can find the other solutions by the permutations on x_1, x_2 and x_3 from $x_1 + yx_2 + y^2x_3$.

(3) We can replace the following biquadratic equation by the following equation, which has solutions u^2, v^2 and w^2.

$$t^3 + \frac{p}{2}t^2 + (\frac{p^2}{16} - \frac{r}{4})t - (\frac{q}{8})^2 = 0$$

Let x_1, x_2, x_3 and x_4 be the solutions of the given equation and t_1, t_2 *and* t_3 be the solutions of the adjoint equation,

$$u = \pm\sqrt{t_1},\ v = \pm\sqrt{t_2},\ w = \pm\sqrt{t_3}.$$

Under the condition $uvw = -8/q$ (constant) we consider the sign of three letters u, v and w if the signs of two letters out of three letters are determined, the sign of another letter is necessarily determined. So it is all right to fix $\sqrt{t_1}$, $\sqrt{t_2}$ and $\sqrt{t_3}$ as one of the combination of the three solutions u, v and w.

$$y_1 = \sqrt{t_1} + \sqrt{t_2} + \sqrt{t_3},\ y_2 = \sqrt{t_1} - \sqrt{t_2} - \sqrt{t_3},$$
$$y_3 = -\sqrt{t_1} + \sqrt{t_2} - \sqrt{t_3},\ y_4 = -\sqrt{t_1} - \sqrt{t_2} + \sqrt{t_3}$$

$$\therefore\quad y_1 + y_2 - y_3 - y_4 = 4\sqrt{t_1},\quad y_1 - y_2 + y_3 - y_4 = 4\sqrt{t_2},$$
$$y_1 - y_2 - y_3 + y_4 = 4\sqrt{t_3}$$

$$\therefore\quad u^2 = \frac{1}{16}(y_1 + y_2 - y_3 - y_4)^2,\quad v^2 = \frac{1}{16}(y_1 - y_2 + y_3 - y_4)^2,$$
$$w^2 = \frac{1}{16}(y_1 - y_2 - y_3 + y_4)^2$$

By $y = x + \frac{b}{4a}$,

$$u^2 = \frac{1}{16}(x_1 + x_2 - x_3 - x_4)^2,\quad v^2 = \frac{1}{16}(x_1 - x_2 + x_3 - x_4)^2,$$
$$w^2 = \frac{1}{16}(x_1 - x_2 - x_3 + x_4)^2$$

Let x_1, x_2, x_3 and x_4 be the solutions of the given equation, the solutions of the adjoint equation are the polynomial of x_1, x_2, x_3 and x_4. One of them is $x_1 + lx_2 + l^2x_3 + l^3x_4$ ($l = -1$), and we can find other solutions by the permutations on the solutions x_1, x_2, x_3 and x_4.

3. Formation of symmetric group

$S_2 = 1,\ (1\ 2)$

$S_3 =$

1	(1 3)	(2 3)
(1 2)	(1 2 3)	(1 3 2)

$S_4 =$

1	(1 4)	(2 4)	(3 4)
(1 2)	(1 2 4)	(1 4 2)	(1 2)(3 4)
(1 3)	(1 3 4)	(1 3)(2 4)	(1 4 3)
(2 3)	(1 4)(2 3)	(2 3 4)	(2 4 3)
(1 2 3)	(1 2 3 4)	(1 4 2 3)	(1 2 4 3)
(1 3 2)	(1 3 2 4)	(1 3 4 2)	(1 4 3 2)

$$S_5 = S_4 + S_4\ (1\ 5) + S_4\ (2\ 5) + S_4\ (3\ 5) + S_4\ (4\ 5)$$

In general, $S_n = S_{n-1} + S_{n-2}\ t_1 + S_{n-3}\ t_2 + \cdots + S_{n-1}\ t_{n-1}$

where $t_1 = (1\ n)$, $t_2 = (2\ n)$, $\cdots$, $t_{n-1} = (n\text{-}1\ n)$

4. Normal subgroup of permutation grouop

1) All the permutation is generated by the transpositions $(1\ n)$.

(1) Cyclic group

$$(i\ j\ k) = (1\ i)(1\ j)(1\ k)$$

(2) Transposition

$$(i\ j) = (1\ i)(1\ j)(1\ i)$$

2) Permutation group G is generated by transposition $(1\ n)$ of $x_1 \to x_n$.

Let $H : 1, s_2, s_3, \cdots, s_r$

As H contains 1, $H : x_1 \to x_1$

When $t_2 = (1\ 2)$,

$Ht_2 : t_2, s_2t_2, \cdots, s_rt_2 : x_1 \to x_2$

.....

When $t_n = (1\ n)$

$Ht_n : t_n, s_2t_n, \cdots, s_rt_n : x_1 \to x_n$

$G = H + Ht_2 + Ht_3 + \cdots + Ht_n$

3) If H is invariant group, then $t_i^{-1}Ht_i$ is invariant permutation.

$\because$ t_i^{-1} is $x_i \to x_1$

H is $x_1 \to x_1$

t_i is $x_1 \to x_i$

$\therefore$ $t_i^{-1}\ H\ t_i$ is $x_i \to x_i$

Remark: $(x_i\ x_j)$ is denoted by $(i\ j)$.

5. Alternating group

$A_2 = 1$

$A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$

$A_4 =$

1	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2 3)	(2 3 4)	(1 4 2)	(1 3 4)
(1 3 2)	(1 4 3)	(2 3 4)	(1 2 4)

$A_5 = A_4 + A_4\ (1\ 2)\ (3\ 4\ 5) + A_4\ (1\ 3)(2\ 4\ 5) + A_4\ (1\ 4)(2\ 3\ 5) + A_4\ (1\ 5)(2\ 3\ 4)$

Remark: (1 2) (3 4 5), (1 3)(2 4 5), (1 4)(2 3 5), (1 5)(2 3 4) : even permutation

1) Alternating group is generated by cyclic group $(i\ j\ k)$.

$\because$ $(i\ j\ k) = (i\ j)(i\ k)$ ·····even permutation

2) Commutator subgroup of S_n is alternating group A_n.

$\because$ $(i\ j\ k) = (i\ j\ m)(i\ k\ l)(m\ j\ i)(l\ k\ i)$

$= (i\ j\ m)\ (i\ k\ l)(i\ j\ m)^{-1}(i\ k\ l)^{-1}$

3) $(i\ j\ k)^{-1} = (k\ j\ i)$

6. Symmetric group and Alternating group

1) $[\, S_n : A_n \,] = 2$

$\because$ If $s\ (\in S_n)$ is odd permutation then sA_n is odd permutation.

$\therefore\ S_n = A_n + sA_n$

2) A_n is a Normal subgroup of S_n.

7. Compositio series

$S_2 \rhd E$ where $E = \{1\}$

$[S_2 : E] = 2$ (prime)

$S_3 \rhd A_3 \rhd E$

$[S_3 : A_3] = 2$ (prime), $[A_3 : E] = 3$ (prime)

$S_4 \rhd A_4 \rhd V_4 \rhd K \rhd E$

$V_4 = \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$

$K = \{1,\ (1\ 3)(2\ 4)\}$

$[S_3 : A_3] = 2$ (prime), $[A_3 : E] = 3$ (prime)

$S_5 \rhd A_5 \rhd E$

$[S_5 : A_5] = 20$ (non-prime), $[A_5 : E] = 60$ (non-prime)

Remark: V_4: Klein four group (Vierengruppe)

8. Minimal polynomial

Definition

If E / F be an extension field, then there is a monic polynomial whose coefficients belong to F, and having a root a on E. When the dimension of the polynomial is minimal, we call this polynomial minimal polynomial of a over F.

9. Simple extension field

1) Definition

Let E / F be an extension field, and let S be a subset of E. Then the smallest subfield of L containing F and S is called the field obtained by adjoining S to F and is denoted by F(S).

2) Theorem

Let F be the number field, then the field $F(a, b, c, \cdots, d)$ which is obtained by adjoining algebraic number $a, b, c, \cdots, d$ is a simple extension field.

$$F(a, b, c, \cdots, d) = F(t)$$

$\because$ It suffices to prove $F(a, b) = F(t)$.

Let $f(x)$ be a minimal polynomial of a and $g(x)$ be of b. Let $a = a_1, a_2, \cdots, a_i$ be a root of $f(x)$ and $b = b_1, b_2, \cdots, b_j$ be of $g(x)$, where $\dfrac{a_i - a}{b - b_j} \neq c$.

Setting $t = a + cx$, $f_1(x) = f(t-cx)$ where $f_1(x) \in F(t)[x]$

$f_1(b) = f(t-cb) = f(a) = 0$

$f_1(b_j) = f(t-cb_j) \neq f(a_i) = 0$

$\because\ t-cb_j = t-cb + c(b-b_j)$

$= a + c(b-b_j)$

$\neq a_i \quad \because \dfrac{a_i-a}{b-b_j} \neq c$

$\therefore\ f_1(b_j) \neq 0$

Since $f_1(x)$ and $g(x)$ have a common root b, $f_1(x) = x-b$

$\therefore\ b \in F(t)$

Similary,

since $g_1(x)$ and $f(x)$ have only one common root a, $g_1(x) = x-a$

$\therefore\ a \in F(t)$

$\therefore\ F(a, b) \subset F(t)$ ·····(1)

$t = a + cb \in F(a, b)$

$\therefore\ F(t) \subset F(a, b)$ ·····(2)

By (1) (2), $F(a, b) = F(t)$

Example $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$ Q: R*ational number field*

Example The field of rational numbers has no automorphism except the identity.

Theorem (Extension Theorem)

Let E / F be an extension field and s be an isomorphism over F, we can extend s over E. And the number of extension is n. $[E : F] = n$

$\because$

$$\begin{array}{ccc} E & \xrightarrow{s} & s(E) \\ \cup & & \cap \\ F & \xrightarrow[s]{} & s(F) \end{array}$$

It suffices to prove this theorem in case E is an extension field of F.

(i) Let $f(x)$ be irreducible over F, then $s(f(x))$ be irreducible over $s(F)$.

$\because$ If $s(f(x))$ is not irreducible,

$s(f(x)) = g(x)h(x)$.

Since s is isomorphism and there exists s^{-1},

$s^{-1}\ s(f(x)) = s^{-1}(g(x))\ s^{-1}\ (h(x))$

$\therefore\ f(x) = s^{-1}(g(x))\ s^{-1}\ (h(x))$

This contradicts the fact that $f(x)$ is irreducible.

$\therefore$ $s(f(x))$ is irreducible.

(ii) E is closed under algebraic operation $\circ$.

Let $k, l \in E$

Because $E = F(h)$, $[E : F] = n$,

$$k = f_0 + f_1 h + \cdots + f_{n-1} h^{n-1} \quad f_i \in F$$

$$l = g_0 + g_1 h + \cdots + g_{n-1} h^{n-1} \quad g_i \in F$$

$$s(k) = s(f_0) + s(f_1)s(h) + \cdots + s(f_{n-1})s(h)^{n-1}$$

$$= s(f_0) + s(f_1)s(h) + \cdots + s(f_{n-1})s(h)^{n-1}$$

Simiraly,

$$s(l) = s(g_0) + s(g_1)s(h) + \cdots + s(g_{n-1})s(h)^{n-1}$$

$$\therefore \quad s(k \circ l) = s(f_0 \circ g_0) + s(f_1 \circ g_1)s(h) + \cdots + s(f_{n-1} \circ g_{n-1})s(h)^{n-1}$$

$$= s(k) \circ s(l)$$

(iii) The number of s is n.

Because E is a simple extension field of F, $E = F(h)$.

Let the minimal polynomial be $f(h) = h^n + a_1 h + \cdots + a_n \quad a_i \in F$

$$f(h) = h^n + a_1 h + \cdots + a_n = 0$$

$$\therefore \quad s(f(h)) = s(h)^n + s(a_1)\, s(h)^{n-1} + \cdots + s(a_n) = 0$$

Because $s(h)$ is root of the equation above, the number of s is n.

Definition

Let E / F be a field extension. The Galois group is the set of automorphism of E that fix F pointwise. This is denoted by Gal (E/F).

Theorem (Normality theorem)

Let $F \subset B \subset E$ be a tower of fields, B / F be the splitting field of $f(x) \in F(x)$ and E / F be the splitting field of $g(x) \in F(x)$.

Then Gal(E / B) is a normalsubgroup of Gal(E / F),

$$Gal(E / F) / Gal(E / B) \cong Gal(B / F).$$

$\because$

$$\begin{array}{ccc} E & \cdots\cdots\cdots\cdots> & G(E) = Gal\ (B / F) \\ \cup & & \cap \\ B & \cdots\cdots\cdots\cdots> & G(B) = Gal\ (E / B) \\ \cup & & \cap \\ F & \cdots\cdots\cdots\cdots> & G = Gal\ (E / F) \end{array}$$

Let $s \in G$, it suffices to prove $s\, G\, s^{-1} \subset G(B)$.

B is a Galois extension of F.

Let $s\ g\ s^{-1} \in sG(B)s^{-1}$ and $x \in B$

$$s\ g\ s^{-1}(c) = s(gs^{-1})(c)$$
$$= ss^{-1}(c)$$
$$= c$$

$\therefore\ s\ G(B)\ s^{-1} \in G(B)$

$\therefore$ G*al* (E / B) is a normalsubgroup of G*al* (E / F).

By the First Isomorphism Theorem, we find

G*al*(E / F) / G*al*(E / B) $\cong$ G*al*(B / F).

Theorem Galois group G of $f(x)$ over F is symmetric group S_n.

Let $n \geqq 5$, S_n is not solable group.

$\because$ (i) $K = F(a_1, a_2, \cdots, a_n)$ is a splitting field of $f(x)$ and a_k is a root of $f(x)$.

Because S_n is a subgroup of Galois group of K over F,

$[K : F]$= degree of G $\geqq$ degree of $S_n = n!$·····①

$F \subset F(a_1) \subset F(a_1, a_2) \subset \cdots \subset F(a_1, a_2, \cdots, a_n) = K$

$\therefore [K : F] = [F(a_1) : F] \cdots [K : F(a_1, a_2, \cdots, a_n)] \leqq n!$·····②

By ①②, $G = S_n$

(ii) $S_n \rhd A_n \rhd E$

Let N be a normal subgroup of A_n $(n \geqq 5)$ since alternating group A_n is genarated by $(i\ J\ k)$, then N contains commutators.

$\therefore\ N = A_n$

We can not have the series of residue class groups. Therefor S_n is not solvable. $(n \geqq 5)$

Remark: Cyclic group is commutative and its order is primitive number.

References

1. Joseph Rotman, Galois Theory, Springer-Verlag, 1998
2. Edgar Dehn, Algebraic Equations — An Introduction to the Theories of Lagrange and Galois, Dover, 1960
3. Toshikuni Kusaba, Galois and Equations, Asakura Shoten, 2002
4. Hiroshi Nagao, Algebra, Asakura Shoten, 1992