On the solvability of irreducible polynomials and its relation to orbit graphs

福井大学医学部　藤田亮介 (Ryousuke Fujita)
School of Medical Sciences, University of Fukui
福井大学大学院教育学研究科　野尻定幸 (Sadayuki Nojiri)
Graduate School of Education, University of Fukui

1 Introduction

Let F be a field of characteristic 0. Let $f(x) \in F[x]$ be a polynomial of degree n and $\alpha_1, \cdots, \alpha_n$ be roots of $f(x)$. Then the automorphism group $\mathrm{Aut}\,(F(\alpha_1, \cdots, \alpha_n)/F)$ over F is said to be the *Galois group* of $f(x)$ which is denoted by $Gal_F(f)$. According to Galois Theory, an algebraic equation $f(x) = 0$ is solvable if and only if the Galois group of $f(x)$ is algebraically solvable. We set $\Omega := \{\alpha_1, \cdots, \alpha_n\}$. Then $Gal_F(f) < S^{\Omega}$. In particular, if $f(x)$ is irreducible, $Gal_F(f)$ acts transitively on Ω. Let us give the following two examples:

(1) The case where $f(x) = x^3 - 2$,

  (i) $Gal_{\mathbb{Q}}(f) \cong S_3$,
  (ii) S_3 is solvable, and
  (iii) $f(x) = 0$ is algebraically solvable.

(2) The case where $f(x) = x^5 - 6x + 3$,

  (i) $Gal_{\mathbb{Q}}(f) \cong S_5$,
  (ii) S_5 is not solvable, and
  (iii) $f(x) = 0$ is not algebraically solvable.

In general, it is hard to get the Galois gourp of a polynomial and just as hard to determine the solvability of the Galois group. A lot of precedent studies have found the algorithms to determine a Galois group. We also discovered the way to decide the solvability of the Galois group. The purpose of this note is to state the relationship between the solvability of irreducible polynomials and orbit graphs.

2 Preliminaries

In this section, we present some fundamental definitios and properties of graphs and groups. First, we would like to emphasize that the graphs we will be dealing with are directed graphs. A *directed* graph consists of a finite set of vertices $V(\mathfrak{G})$ and a set of edges $A(\mathfrak{G})$ consisting of ordered pairs of vertices. Remark that $V(\mathfrak{G})$ is not an emptyset. If $(v_1, v_2) \in A(\mathfrak{G})$, then we often write $v_1 \to v_2$. A *non-paired* directed graph is the directed graph such that $(v_2, v_1) \notin A(\mathfrak{G})$ for all $(v_1, v_2) \in A(\mathfrak{G})$. On the other hand, a *paired* directed graph is the directed graph such that $(v_2, v_1) \in A(\mathfrak{G})$ for all $(v_1, v_2) \in A(\mathfrak{G})$. A *diagonal* graph is the directed graph such that $A(\mathfrak{G}) = D := \{(v, v) \mid v \in V(\mathfrak{G})\}$.

Let $\mathfrak{G} = (V(\mathfrak{G}), A(\mathfrak{G}))$ be a directed graph. Let $a \in V(\mathfrak{G})$. We set $\Delta(a) = \{b \in V(\mathfrak{G}) \mid (a, b) \in A(\mathfrak{G})\}$ and $\delta(a) = \{b \in V(\mathfrak{G}) \mid (b, a) \in A(\mathfrak{G})\}$. Then

$$\deg(a) := |\Delta(a)| + |\delta(a)|$$

is called the *degree* of a. Moreover $\mathfrak{G}$ is said to be *regular* when any vertex has the same degree. Let $\mathfrak{G} = (V(\mathfrak{G}), A(\mathfrak{G}))$ be a directed graph. Let $a, b\,(\neq a) \in V(\mathfrak{G})$. A sequence

$$a_0 e_1 a_1 e_2 a_2 \cdots e_k a_k, \quad (a_0 = a,\ a_k = b, e_i := (a_{i-1}, a_i)\ or\ (a_i, a_{i-1}) \in A(\mathfrak{G}))$$

is called a *path* joining a and b. Both a and b are *connected* when there is a path joining a and b. Remark that $a \in V(\mathfrak{G})$ is self-connected with a. A graph $\mathfrak{G} = (V(\mathfrak{G}), A(\mathfrak{G}))$ is *connected* if every two vertices of $\mathfrak{G}$ are connected.

Let Ω be a finite set. Given a permutation group G on Ω, then $(G,\ \Omega)$ becomes an action by $x^\sigma := \sigma(x)$, and $x^{\sigma\tau} := \tau(\sigma(x))$ for $x \in \Omega,\ \sigma,\ \tau \in G$. Reversely, given a permutation group action $(G,\ \Omega)$, then G becomes a permutation group on Ω by $\sigma(x) := x^\sigma$, and $\tau(\sigma(x)) := x^{\sigma\tau}$ for $x \in \Omega,\ \sigma,\ \tau \in G$. Consequently, a permutation group G on Ω has one to one correspondence with a permutation group action $(G,\ \Omega)$. Hence, we identify a permutation group G on Ω with a permutation group action $(G,\ \Omega)$. An action is said to be *transitive* if there is only one orbit. We say a permutation group G on Ω is transitive when a permutation group action $(G,\ \Omega)$ is transitive. Hereafter we also denote a permutation group G on Ω by $(G,\ \Omega)$. Furthermore (G, Ω) is said to be a 2-*transitive permutation group* if G acts transitively on the subset of $\Omega \times \Omega$ consisting of the 2-tuples all of whose entries are distinct.

Let (G, Ω) be a transitive permutation group. For $\sigma \in G$, we consider a map

$$\sigma : \Omega \times \Omega \longrightarrow \Omega \times \Omega\ ;\ (a, b) \longmapsto (a, b)^\sigma := (a^\sigma, b^\sigma).$$

Therefore $(G, \Omega \times \Omega)$ is a permutation group. Let Δ be a G-orbit of $\Omega \times \Omega$. A graph (Ω, Δ) is called a *orbit graph* of the G-orbt Δ. Note that (Ω, Δ) is a non-paired directed regular graph or a paired directed regular graph. It is also verified that the degree of (Ω, Δ) is $\dfrac{2|\Delta|}{|\Omega|}$.

Example 2.1 Let $\Omega = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $G = \langle(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4)\rangle \cong C_4 < S_4$ (Note that the symbol $H < G$ means that H is a subgroup of G). Then there are four G-orbits on $\Omega \times \Omega$ as follows:

$$\begin{aligned}
\Omega \times \Omega &= \Delta_1 \coprod \Delta_2 \coprod \Delta_3 \coprod \Delta_4 \\
\Delta_1 &:= D \\
\Delta_2 &:= \{(\alpha_1, \alpha_2), (\alpha_2, \alpha_3), (\alpha_3, \alpha_4), (\alpha_4, \alpha_1)\} \\
\Delta_3 &:= \{(\alpha_1, \alpha_3), (\alpha_2, \alpha_4), (\alpha_3, \alpha_1), (\alpha_4, \alpha_2)\} \\
\Delta_4 &:= \{(\alpha_1, \alpha_4), (\alpha_2, \alpha_1), (\alpha_3, \alpha_2), (\alpha_4, \alpha_3)\}
\end{aligned}$$

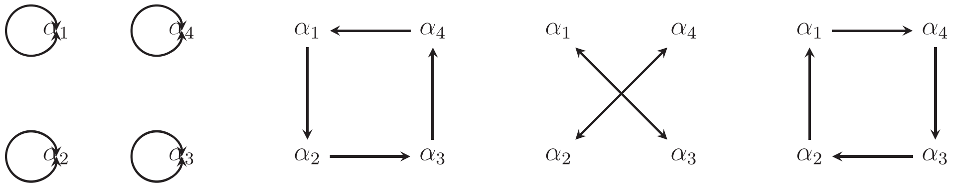

Figure 1: (Ω, Δ_i) (Form left, $i = 1,\ i = 2,\ i = 3,\ i = 4$)

Example 2.2 Let $\Omega = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $G = S_4$. Then there are two G-orbits on $\Omega \times \Omega$ as follows:

$$\begin{aligned} \Omega \times \Omega &= \Delta_1 \coprod \Delta_2 \\ \Delta_1 &:= D \\ \Delta_2 &:= (\Omega \times \Omega) \backslash D \end{aligned}$$

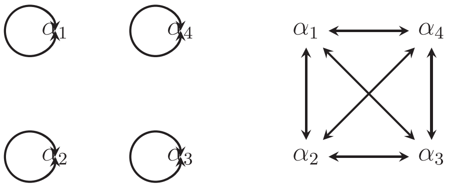

Figure 2: (Ω, Δ_i) (From left, $i = 1,\ i = 2$)

The next proposition is the key of this note.

Proposition 2.3 Let (G, Ω) be a transitive permutation group. Let Δ be a G-orbit of $\Omega \times \Omega$. Then the following is equivalent:

(1) (G, Ω) is primitive, and

(2) Each orbit graph (Ω, Δ_i) $(i = 2, 3, \cdots, r)$ is connected.

Let $(G,\ \Omega)$ be a transitive permutation group. A subset $\Delta \subset \Omega$ is called a *non-primitive block* of $(G,\ \Omega)$ if

$$\Delta^\sigma = \Delta \text{ or } \Delta^\sigma \cap \Delta = \emptyset \quad (\forall \sigma \in G).$$

Clearly, Ω and $\Delta = \{a\}$(= one point set) are non-primitive blocks of $(G,\ \Omega)$. Each of them is called a *trivial non-primitive block.* When $(G,\ \Omega)$ has only trivial non-primitive blocks, we say $(G,\ \Omega)$ is *primitive.* In case not so, $(G,\ \Omega)$ is said to be *non-primitive.* In particular, if Ω is a finite set with prime number elements, then (G, Ω) is primitive. Moreover (G, Ω) is primitive if and only if G_x is a maximal subgroup of G $(\forall x \in \Omega)$, where G_x is the *isotropy group* at x. In group theory, this is also called the *stablizer* at x.

We will show two easy examples.

Example 2.4 Let $\Omega = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$， $\sigma := (\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4)$， $G = \langle \sigma \rangle \cong C_4$， and $\Delta := \{\alpha_1, \alpha_3\} \subseteq \Omega$. Then

(i) $\Delta^e = \{{\alpha_1}^e, {\alpha_3}^e\} = \{\alpha_1, \alpha_3\} \implies \Delta^e = \Delta$

(ii) $\Delta^\sigma = \{{\alpha_1}^\sigma, {\alpha_3}^\sigma\} = \{\alpha_2, \alpha_4\} \implies \Delta^\sigma \cap \Delta = \emptyset$

(iii) $\Delta^{\sigma^2} = \{{\alpha_1}^{\sigma^2}, {\alpha_3}^{\sigma^2}\} = \{\alpha_3, \alpha_1\} \implies \Delta^{\sigma^2} = \Delta$

(iv) $\Delta^{\sigma^3} = \{{\alpha_1}^{\sigma^3}, {\alpha_3}^{\sigma^3}\} = \{\alpha_4, \alpha_2\} \implies \Delta^{\sigma^3} \cap \Delta = \emptyset$

By (i)， (ii)， (iii)， (iv), (G, Ω) is a non-primitive permutation group.

Example 2.5 Let $\Omega = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $G = S_4$, we have $G_{\alpha_i} = \langle (\alpha_j\ \alpha_k\ \alpha_l), (\alpha_j\ \alpha_k) \rangle \cong S_3$ $(\forall \alpha_i \in \Omega)$, where $\alpha_i \in \Omega \backslash \{\alpha_j, \alpha_k, \alpha_l\}$. Since G_{α_i} contains an odd permutaion, it follows that $G_{\alpha_i} \not< A_4$. Hence (G, Ω) is a primitive permutation group.

Now, we want to state the solvability of irreducible polynomials and its relation to orbit graphs. Let F be a field of characteristic 0. Let $f(x) \in F[x]$ be a irreducible polynomial of degree 6 and Ω be the set of roots of $f(x)$. Let G be a Galois group of $f(x)$. Let $\Delta_1 (= D), \Delta_2, \cdots, \Delta_r$ を $\Omega \times \Omega$ be G-orbits of $\Omega \times \Omega$. Then the following are equivalent:

(1) G is solvable,

(2) $f(x)$ is algebraically solvable,

(3) (G, Ω) is a non-primitive permutation group, and

(4) ${}^{\exists}i \in \{2, \cdots, r\}$ *s.t.* (Ω, Δ_i) is a non-connected graph.

We can see that the solvability of an irreducible polynomial has one to one correspondence with the connectivity of the orbit graph. However, this is very rare. In general, it does not hold for the degree of composition number.

Let p be a prime. Let $\mathbb{F}_p$ be a field with p elements. We put

$$AGL(1, \mathbb{F}_p) := \left\{ \begin{pmatrix} 1 & 2 & \dots & p \\ a+b & 2a+b & \dots & pa+b \end{pmatrix} \mid a \in \mathbb{F}_p \backslash \{0\}, b \in \mathbb{F}_p \right\}.$$

Let q be a prime power. $GL_d(\mathbb{F}_q)$ is known as a group of linear transformations of a vector space of dimension d over $\mathbb{F}_q$. Its subgroup consisting of matrices of determinant 1 is denoted by $SL_d(\mathbb{F}_q)$. Moreover $PGL_d(\mathbb{F}_q)$ is the factor group by the center of $GL_d(\mathbb{F}_q)$ and $PSL_d(\mathbb{F}_q)$ is the image of $SL_d(\mathbb{F}_q)$ in $PGL_d(\mathbb{F}_q)$.

Let $G (< S_p)$ be a transitive permutation groups. Then it is well known that G is one of the following group. A solvable group is a group satisfying the following (2).

(1) $G = S_p$ *or* A_p,

(2) ${}^{\exists}\sigma \in S_p$ *s.t.* $G < \sigma^{-1} AGL(1, \mathbb{F}_p) \sigma$,

(3) $G \cong PSL_2(\mathbb{F}_{11})$,

(4) $G \cong M_{11}$ *or* M_{23}, and

(5) $PSL_d(\mathbb{F}_q) < G < P\Gamma L_d(\mathbb{F}_q)$ *s.t.* $p = \dfrac{q^d - 1}{q - 1}$, $d \geq 2$, $q = l^m$ (l is prime number).
Here $P\Gamma L_d(\mathbb{F}_q) \rhd PGL_d(\mathbb{F}_q)$ and $P\Gamma L_d(\mathbb{F}_q)/PGL_d(\mathbb{F}_q) \cong C_m$.

Note that M_{11}(resp.M_{23}) is a subgroup of S_{11}(resp.S_{23}) which is called the *Mathieu group* of degree 11(resp.23). These are a kind of sporadic simple groups.

3 Main Results

Let Ω be a finite set with prime elements. Let (G, Ω) is a transitive permutation group. Let $\Delta_1(= D), \Delta_2, \cdots, \Delta_r$ be G-orbits of $\Omega \times \Omega$. Then (Ω, Δ_i) $(2 \leq i \leq r)$ is a connected graph. Our results are proved by using GAP adequately.

Theorem 3.1 Let $p\,(\geq 5)$ be a prime. Let $\Omega := \{\alpha_1, \cdots, \alpha_p\}$. Let (G, Ω) is a transitive permutation group. Let $\Delta_1(= D), \Delta_2, \cdots, \Delta_r$ be G-orbits of $\Omega \times \Omega$. Then we have

(1) $G = S^{\Omega}$ *or* $A^{\Omega} \Longrightarrow r = 2$ and (Ω, Δ_2) is a paired directed regular graph of degree $2(p - 1)$.

(2) $^{\exists}\sigma \in S_p$ *s.t.* $G < \sigma^{-1}AGL(1, \mathbb{F}_p)\sigma$,
(i) $|G|$ is odd, then (Ω, Δ_i) $(2 \leq i \leq r)$ is a non-paired directed regular graph of degree $\dfrac{2|G|}{|\Omega|}$.
(ii) $|G|$ is even, then (Ω, Δ_i) $(2 \leq i \leq r)$ is a paired directed regular graph of degree $\dfrac{2|G|}{|\Omega|}$.
In particular, if $G = \sigma^{-1}AGL(1, \mathbb{F}_p)\sigma$, it means that $r = 2$ and (Ω, Δ_2) is a paired directed regular graph of degree $2(p - 1)$.

(3) $G \cong PSL_2(\mathbb{F}_{11}) \Longrightarrow r = 2$ and (Ω, Δ_2) is a paired directed regular graph of degree $2(p - 1)$.

(4) $G \cong M_{11}$ *or* $M_{23} \Longrightarrow r = 2$ and (Ω, Δ_2) is a paired directed regular graph of degree $2(p - 1)$.

(5) $PSL_d(\mathbb{F}_q) < G < P\Gamma L_d(\mathbb{F}_q)$ *s.t.* $p = \dfrac{q^d - 1}{q - 1} \Longrightarrow r = 2$ and (Ω, Δ_2) is a paired directed regular graph of degree $2(p - 1)$.

Let $\Omega := \{\alpha_1, \cdots, \alpha_n\}$ $(n \in \mathbb{N})$. Let (G, Ω) is a 2-transitive permutation group and $\Omega' := \{\{\alpha_i, \alpha_j\} \mid i, j(\neq i) \in \{1, \cdots, n\}\}$. For $\sigma \in G$, we consider a map

$$\sigma : \Omega' \longrightarrow \Omega' \ ; \ \{a, b\} \longmapsto \{a, b\}^{\sigma}.$$

Then (G, Ω') is a transitive permutation group. For $\sigma \in G$, a map

$$\sigma : \Omega' \times \Omega' \longrightarrow \Omega' \times \Omega' \ ; \ (\{\alpha_i, \alpha_j\}, \{\alpha_k, \alpha_l\}) \longmapsto (\{\alpha_i, \alpha_j\}, \{\alpha_k, \alpha_l\})^{\sigma}$$

is a bijection. Hence $(G, \Omega' \times \Omega')$ is a permutation group. Let Δ' be a G-orbit of $\Omega' \times \Omega'$. Immediately, we get an orbit graph (Ω', Δ'). Remark that $D'(= \{(\{\alpha_i, \alpha_j\}, \{\alpha_i, \alpha_j\}) \mid \{\alpha_i, \alpha_j\} \in \Omega'\})$ is a G-orbit of $\Omega' \times \Omega'$. Since (G, Ω') is a transitive permutation group, it is either primitive or non-primitive.

Theorem 3.2 Let p be a prime (≥ 5). Let $\Omega := \{\alpha_1, \cdots, \alpha_p\}$ and $\Omega' := \{\{\alpha_i, \alpha_j\} \mid i, j(\neq i) \in \{1, \cdots, p\}\}$. Let (G, Ω) is a transitive permutation group.. Le ${\Delta_1}'(= D'), \cdots, {\Delta_t}'$ be G-orbits of $\Omega' \times \Omega'$. Then

(1) $G = S^{\Omega}$ *or* $A^{\Omega} \Longrightarrow (\Omega', {\Delta_i}')$ $(i = 2, \cdots, t)$ is connected.

(2) ${}^{\exists}\sigma \in S_p$ *s.t.* $G = \sigma^{-1} AGL(1, \mathbb{F}_p)\sigma$.
$\Longrightarrow {}^{\exists}i \in \{2, \cdots, t\}$ *s.t.* $(\Omega', {\Delta_i}')$ is disconnected.

(3) $G \cong PSL_2(\mathbb{F}_{11}) \Longrightarrow (\Omega', {\Delta_i}')$ $(i = 2, \cdots, t)$ is connected.

(4) $G \cong M_{11}$ *or* $M_{23} \Longrightarrow (\Omega', {\Delta_i}')$ $(i = 2, \cdots, t)$ is connected.

(5) (i) $PSL_2(\mathbb{F}_q) < G < P\Gamma L_2(\mathbb{F}_q)$ *s.t.* $p = \dfrac{q^2 - 1}{q - 1}(= q + 1) \Longrightarrow (\Omega', {\Delta_i}')$ $(i = 2, \cdots, t)$ is connected.

(5) (ii) $G \cong PSL_d(\mathbb{F}_q)$ *s.t.* $p = \dfrac{q^d - 1}{q - 1}$, $d \geq 3 \Longrightarrow {}^{\exists}i \in \{2, \cdots, t\}$ *s.t.* $(\Omega', {\Delta_i}')$ is disconnected.

By Galois Thery, we get the following.

Theorem 3.3 Let q be a prime power. Let p be a prime (≥ 5) such that $p \neq \dfrac{q^d - 1}{q - 1}$ $(d \geq 3)$. Let F be a field of characteristic 0. Let $f(x) \in F[x]$ be a irreducible polynomial of degree p and Ω be the set of roots of $f(x)$. Let G be the Galois group of $f(x)$. Let ${\Delta_1}'(= D'), \cdots, {\Delta_t}'$ be G-orbits of $\Omega' \times \Omega'$. Then the following are equivalent:

(1) $f(x)$ is not algebraically solvable, and

(2) There are only two G-orbits of $\Omega \times \Omega$ such that (Ω, Δ_2) is the paried directed complete graph and $(\Omega', {\Delta_i}')$ $(2 \leq i \leq t)$ is connected..

Theorem 3.3 holds for $p = 5$. If $5 = \dfrac{q^d - 1}{q - 1}$ $(d \geq 3)$, then $5(q - 1) = q^d - 1 \Longleftrightarrow 5q - q^d = 4 \Longleftrightarrow q(5 - q^{d-1}) = 4$. Since q is a prime power, so that $q = 2,\ 4$. The case where $q = 2$, we just have $5 = 2^d - 1$, and so $2^d = 6$, a contradiction. In the case of $q = 4$ as well, then $15 = 4^d - 1$, so $4^d = 16 \Longleftrightarrow d = 2$. This is also a contradiction because $d \geq 3$. Remark that $F_{20} \cong AGL(1, \mathbb{F}_5)$, where F_{20} is a Frobenuis group of order 20.

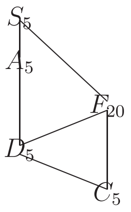

Figure 3: Hasse diagram of transitive permutation groups of degree 5

References

[1] Chartrand, G., *Introductory Graph Theory*, Dover. 1985.

[2] Cox, D.A., *Galois Theory*, John Wiley & Sons, Inc. 2004.

[3] Dixion, J.D. and Mortimer, B., *Permutation Groups*, Springer-Verlag. 1996.

[4] Dummit, D.S., *Solving solvable quintics*, Mathematics of Computation. **1** (1991), 387-401.

[5] Soicher, L. and Mckay, J., *Computing Galois Groups over the Rationals*, Journal of Number Theory. **20** (1985), 273-281.

[6] Wilson, R.A., *The Finite Simple Groups*, Springer-Verlag. 2009.

[7] Wilson, R.J., *Introduction to Graph Theory*, Pearson. 2010.