

Regular Permutation Group と

Strongly Connected Automaton の Automorphism Group
について

早大 理工 植村 憲治

§ 1 序

strongly connected automaton の automorphism group は regular permutation group になる事が知られている。筆者はまず regular permutation group に関する 1 つの定理 ([定理 2.1]) を得た。さらにまた semigroup の idempotents の partial order を使って [補助定理 3.2] と [定理 3.2] を示した。それらを使って次の [定理 4.3] を得た。[定理 4.3]: automaton $A = (S, I, M)$ が strongly connected で、 $\bar{I}$ をその characteristic semigroup とし、 e を $\bar{I}$ の minimal idempotent とした時、 A の automorphism group $G(A)$ は group $e\bar{I}e$ の subgroup の homomorphic image である。これは Fleck によって得られた結果 (5) の拡張であり、それを別の方法によって導いたことにもなっている。

§ 2 Regular Permutation Group

[定義 2.1] X 上の permutation group G が "regular (permutation group)" であるとは、ある $x_0 \in X$ に対して $x_0 g = x_0$ ($g \in G$) ならば g は identity mapping であるような permutation group をいう。

G を X 上の permutation group として X 上に relation $\sim$ を $x \sim y \Leftrightarrow \exists g \in G \quad x = yg$ で定義するとこれは equivalence relation となる。

[定義 2.2] 上の $\sim$ によって得られた X 上の分割を G による transitive class (可遷域) と呼ぶ。特に transitive class が 1 つだけの permutation group を transitive な permutation group という。

[補助定理 2.1] G を finite set X 上の regular permutation group とし、 G による X の transitive classes を $\{X_1, X_2, \dots, X_r\}$ とすると $\#G = \#X_i$ である。

(証明) $x_0 \in X_i$ を fixed する

$\varphi: G \rightarrow X_i$ を $g \mapsto x_0 g$ で定義する。

i) $x_0 g \sim x_0$ 即ち $x_0 g \in X_i$ によって well-defined

ii) $x \in X_i$ とすると $x \sim x_0$ より $x = x_0 g$ となる g が存在。即ち onto.

iii) $\varphi(g) = \varphi(g')$ とする。即ち $x_0 g = x_0 g' \Rightarrow x_0 = x_0 g' g^{-1}$

G が regular より $g' g^{-1} = id \quad \therefore g' = g$

よって φ は one-to-one $\therefore \#G = \#X_i \quad Q.E.D.$

[系 2.1] 上の条件で $\#G$ は $\#X$ の約数である。

[定理 2.1] G を finite set X 上の regular permutation group とする。その時 X 上の permutation group H が存在して

i) H の transitive class は G の transitive class と同じである、

ii) H は regular であり、

iii) H の elements は G の elements と可換であり、($hg = gh$ for any $g \in G, h \in H$)

iv) $H \cong G$ であり

v) 特に G が transitive ならば H は unique である。

(証明)

第 0 段 $X = \{1, 2, \dots, m, m+1, \dots, 2m, \dots, \alpha m+1, \dots, (\alpha+1)m\}$ とし、

G による transitive class を $\{1, \dots, m\}, \{m+1, \dots, 2m\}, \dots, \{\alpha m+1, \dots, (\alpha+1)m\}$

とする。 $X_\lambda = \{\lambda m+1, \dots, (\lambda+1)m\} \quad 0 \leq \lambda \leq \alpha$ とおく。

$G = \{g_1, \dots, g_m\}, g_1 = id$ としておく。(これは [補助定理

2.1] による。) 各 class より 1 つずつ element をとってき

てそれらを $\lambda m+1$ とする。その他の elements を改ためて

$\lambda m+k = (\lambda m+1)g_k \quad (1 \leq k \leq m)$ で定める。

$$\text{すると } (\lambda m + 1)g_k = \lambda m + k = \lambda m + 1 \cdot g_k$$

$$\begin{aligned} (\lambda m + i)g_k &= \{(\lambda m + 1)g_i\}g_k = (\lambda m + 1)g_i g_k = \lambda m + 1 \cdot g_i g_k \\ &= \lambda m + i \cdot g_k \quad 1 \leq i, k \leq m. \end{aligned}$$

第1段. permutations の set $H = \{h_1, \dots, h_m\}$ を次の様に定める.

$(\lambda m + i)h_k = \lambda m + k g_i$. すると h_k はたしかに X 上の permutation となっており, さらに $X_\lambda h_k = X_\lambda$ ($0 \leq \lambda \leq \alpha, 1 \leq k \leq m$) である. よって H が group であることと, H が X_λ 上 transitive な事が示されれば, H の transitive class と G の transitive class は等しくなる.

$$(\lambda m + i)h_j h_k = (\lambda m + j g_i)h_k = \lambda m + k g_{j g_i} \quad *$$

ここで $1 \cdot g_j g_i = j g_i = 1 \cdot g_i \cdot g_i$. G が regular である事が

$$\text{よって } g_j g_i = g_i g_i \quad (g_i g = g_i \cdot g \quad g \in G) \quad \dots (1)$$

$$\text{よって } * = \lambda m + k g_j g_i = \lambda m + (k g_j) g_i$$

$$= (\lambda m + i)h_k g_j \quad (0 \leq \lambda \leq \alpha, 1 \leq i \leq m)$$

$$\text{即ち } h_j h_k = h_k g_j \quad (1 \leq j, k \leq m) \quad \dots (2)$$

よって H は permutation としての演算に関して閉じているから group である.

$$\lambda m + i, \lambda m + j \in X_\lambda \text{ として } \lambda m + j = \lambda m + k g_i \text{ とす}$$

$$\text{る. } \lambda m + j = \lambda m + k g_i = (\lambda m + i)h_k. \text{ よって } H \text{ は } X_\lambda \text{ 上}$$

transitive. よって H の transitive classes は $\{X_0, X_1, \dots$

$\dots X_\alpha\}$ である

第2段 $(\lambda m + i)h_k = \lambda m + i$ とする。 $\lambda m + i = (\lambda m + 1)g_i$.

又 $(\lambda m + i)h_k = \lambda m + k g_i = (\lambda m + k)g_i \quad \therefore (\lambda m + 1)g_i = (\lambda m + k)g_i$
 g_i^{-1} をかけ $\lambda m + 1 = \lambda m + k \quad \therefore k = 1 \quad \therefore h_k = h_1 = id.$ よって
 H は regular である。

第3段 $h_j \in H, g \in G$ とする。 $(\lambda m + i)h_j g = (\lambda m + j g_i)g$

$$= \lambda m + j g_i g = \lambda m + j g_i g \quad (1)より$$

$$= (\lambda m + i g)h_j = (\lambda m + i)g h_j \quad (0 \leq \lambda \leq \alpha, 1 \leq i \leq m)$$

$$よって h_j g = g h_j$$

第4段 $\varphi: G \rightarrow H$ by $g_i \mapsto h_i^{-1} (= g_i \mapsto h_i \mapsto h_i^{-1})$ を考える

と = φ は well-defined, surjective, injective.

$$\begin{aligned} \varphi(g_i \cdot g_j) &= \varphi(g_i \cdot g_j) \quad (1)より = (h_i \cdot g_j)^{-1} = (h_j \cdot h_i)^{-1} \quad (2)より \\ &= (h_i)^{-1} \cdot (h_j)^{-1} = \varphi(g_i) \varphi(g_j). \quad \text{よって } G \cong H \end{aligned}$$

第5段 $G = \{g_1, \dots, g_m\} \quad X = \{1, \dots, m\}$ とする H を G の全ての elements と可換な elements よりなる group で transitive とする。
 $h \in H, 1 \cdot h = h \quad (h \in X)$ とすると, $i \cdot h = 1 \cdot g_i h = 1 h g_i = h g_i \quad (i=1, \dots, m)$ となって G の全ての element と可換で
 1 を h に動かす permutation はただ一つしか存在しない
 事がわかる。即ち H は unique である。 Q.E.D.

[系2.2] G を finite set X 上の transitive regular permutation group とする。 G の全ての elements と可換な mapping の全体は結局は第5段の H にとどまる。証明は第5段と同様。

§ 3. Semigroup.

[定義 3.1] S を semigroup とする。 $e \in S$ が idempotent であるとは $e^2 = e$ を満たすことをいう。 E で S の idempotents 全体の set をあらわす。

[注意] e_1, e_2 が idempotents であっても e_1, e_2 が idempotent とはかぎらない。即ち E は S の subsemigroup とはならない。

[定義 3.2] E の partial order の定義。 $e_i, e_j \in E$ に対して relation $e_i \leq e_j \Leftrightarrow e_i e_j = e_j e_i = e_i$ を定めるとこれは partial order の条件 i) $a \leq a$ for any a , ii) $a \leq b, b \leq a \Rightarrow a = b$, iii) $a \leq b, b \leq c \Rightarrow a \leq c$ を満たす事が容易に確かめられる。

[定義 3.3] E に minimal element の存在する時それを minimal (又は primitive) idempotent と呼ぶ。即ち e が minimal $\Leftrightarrow e e' = e' e = e$, かつ $e' \in E \Rightarrow e' = e$ 。

[補助定理 3.1] S を finite semigroup とし, $a \in S$ とする。この時自然数 n が存在して a^n は idempotent である。

(証明) S が finite だから $a^{m+r} = a^m$ となる自然数 m, r が存在する。 ($0 < m < r$) よって $m \leq sr < m+r$ となる自然数 s がただ一つ存在する。 $a^{sr+r} = a^{m+r+(sr-m)} \quad (0 \leq sr-m < r)$
 $= a^{m+sr-m} = a^{sr} \quad \therefore (a^{sr})^2 = a^{sr+sr} = a^{sr+r+(s-1)r}$
 $= a^{sr+(s-1)r} = \dots = a^{sr}$ よって a^{sr} は idempotent である。 Q.E.D.

(定理 3.1]. S を finite semigroup, e をその idempotent とする。
 eSe が group である必要十分条件は e が minimal であること。

(証明) 必要性. eSe が group であって $e' \leq e$ とする。
 $ee' = e'e = e'$ より $ee'e = (ee')e = e'e = e' \therefore e' \in eSe$. group
 の idempotent は identity だけだから $e' = e$. よって e は minimal.
 十分性. $e(eSe) = (eSe)e = eSe$. よって e は eSe の identity.
 今 $(eSe)^t$ が idempotent とする. (補助定理 3.1)) $e(eSe)^t$
 $= (eSe)^te = (eSe)^t$. 即ち $(eSe)^t \leq e$. e が minimal より
 $(eSe)^t = e$ である. よって $t = 1$ ならば $eSe = e$ となって e
 が逆元になり, $t \geq 2$ ならば $(eSe)^{t-1}$ が逆元となる. 即ち
 eSe は group である. Q.E.D.

[補助定理 3.2] S を finite semigroup とし, e_1, e_2 をその
 minimal idempotents とする. $(e_1 e_2 e_1)^m = e_1, (e_2 e_1 e_2)^n = e_2$.
 m, n をその様な最小の正の整数とする. その時 $m = n$ である.

(証明) $(e_1 e_2 e_1)^m$ が idempotent であれば, e_1 が minimal より,
 $(e_1 e_2 e_1)^m = e_1$ となる. $(e_2 e_1 e_2)^n$ についても同様である.
 $m > n$ とする. $e_1 = (e_1 e_2 e_1)^m = e_1 e_2 (e_2 e_1 e_2)^{m-1} e_1$
 $= e_1 e_2 (e_2 e_1 e_2)^{n+(m-n-1)} e_1 = e_1 e_2 (e_2 e_1 e_2)^{m-n-1} e_1$
 $(m-n-1 \geq 0)$
 $= (e_1 e_2 e_1)^{m-n}$ となって m がその様な最小の正の整数という
 仮定に反する. 即ち $m \leq n$ である. $m, n; e_1, e_2$ の対称性より
 $n \leq m$ がいえて, $m = n$ である. Q.E.D.

(定理 3.2) S を finite semigroup とし, e_1, e_2 を S の minimal idempotents とする. $e_1 S e_1 \cong e_2 S e_2$ である。

(証明) $(e_1 e_2 e_1)^m = e_1, (e_2 e_1 e_2)^m = e_2$ とする m が存在する。

(補助定理 3.2) $\varphi: e_1 S e_1 \rightarrow e_2 S e_2$ を次の様に定義する。

$$\varphi: e_1 S e_1 \mapsto (e_2 e_1)^m e_1 S e_1, (e_1 e_2) = (e_2 e_1)^m S e_1 e_2$$

i) well-defined はあきらか。

$$ii) e_2 S e_2 = (e_2 e_1)^m e_2 S e_2 (e_1 e_2)^m = (e_2 e_1)^m \{ e_2 S e_2 (e_1 e_2)^m \} e_1 e_2$$

$\therefore \varphi(e_1 e_2 S e_2 (e_1 e_2)^{m-1} e_1) = e_2 S e_2$. よって φ は surjective

$$iii) \varphi(e_1 S e_1) \varphi(e_1 S_2 e_1) = \{ (e_2 e_1)^m S_1 e_1 e_2 \} \{ (e_2 e_1)^m S_2 e_1 e_2 \}$$

$$= \{ (e_2 e_1)^m S_1 (e_1 e_2 e_1)^m S_2 e_1 e_2 = (e_2 e_1)^m S_1 e_1 S_2 e_1 e_2$$

$$= \varphi((e_1 S_1 e_1) (e_1 S_2 e_1)). \text{ よって } \varphi \text{ は homomorphism.}$$

$$iv) (e_2 e_1)^m S e_1 e_2 = e_2 \text{ とすると, } e_1 (e_2 e_1)^m S e_1 e_2 = e_1 e_2$$

$$\therefore e_1 S e_1 e_2 = e_1 e_2 \quad \therefore e_1 S (e_1 e_2)^m e_1 = (e_1 e_2)^m e_1$$

$$\therefore e_1 S e_1 = e_1 \quad \text{よって } \varphi \text{ は isomorphism である。 Q.E.D.}$$

(補助定理 3.3) S を finite set X 上の mapping のつくる semi-group とする。 G を S の subgroup として e を G の identity とする。 $X_0 = Xe$ とする時, G を X_0 に制限したものは X_0 の permutation group であり, G と isomorphic である。

(証明) $x \in X_0$ とする。 $x = ye$ ($y \in X$) $xe = ye^2 = ye = x$
 $\therefore xe = x$ ---- (i). よって e は X_0 上の identity mapping である。
 $g \in G$ に対して $g_0 = g|_{X_0}$ とする。 $x \in X$ の時 $xg = xge \in X_0$

$\therefore xg \in X_0$. 特に $x_0g \in X_0 \therefore x_0g_0 \in X_0$. $xg = yg$ $x, y \in X_0$ とすると
 まず $xe = ye$ より (i) より $x = y$ ゆえに $x_0g = x_0 \therefore x_0g_0 = x_0$. 即
 ち g_0 は x_0 の permutation である. 対応 $\varphi: g \mapsto g_0$ を考えると,

i) well-defined

ii) 定義より surjective

iii) $g_0 = g'_0$ とすると, $x \in X$ に対して $xg = x(eg) = (xe)g = (xe)g_0$
 $= (xe)g'_0 = xeg' = xg'$. よって $g = g'$, ゆえに injective.

iv) $x \in X_0$ に対して $xg_0g'_0 = xeg_0g'_0 = xegg' = x(gg')$.

$\therefore g_0g'_0 = (gg')_0$.

よって φ は isomorphism である.

[定理 3.3] $\mathcal{S}$ を finite set X 上の mapping の semigroup とする
 e を minimal idempotent とすると $e\mathcal{S}e$ は Xe 上の permutation
 group である ([補助定理 3.3]) 特に $\mathcal{S}$ が X 上 transitive ならば
 (i.e. $\forall x, y \in X, \exists s \in \mathcal{S}, y = xs$) $e\mathcal{S}e$ は transitive になる.

(証明) $xe, ye \in Xe$ とする. $\mathcal{S}$ が transitive より s が存在し
 $(xe)s = ye \therefore (xe)se = ye \cdot e = ye \therefore xe(ese) = ye$.

よって $e\mathcal{S}e$ は transitive である.

Q.E.D.

§4. Strongly Connected Automaton の Automorphism Group

[定義 4.1] automaton とは $A = (\mathcal{S}, I, M)$ である. $\mathcal{S}$ は states
 の finite set. I は finite inputs より生成される free semi-
 group である. empty word は必ずしも I に入っていない。

M は $S \times I \rightarrow S$ の mapping で $M(s, xy) = M(M(s, x), y)$ for any $s \in S$, $x, y \in I$ とする。

I 上の relation $\sim$ を $x \sim y \Leftrightarrow M(s, x) = M(s, y)$ for any $s \in S$ とする。これは equivalence relation となる。 x のふくまれる class を $\bar{x}$ である。ゆえにこれは S 上の 1 つの mapping を与えて $s\bar{x} = M(s, x)$ である。よって class の全体 $\bar{I} = \bigcup_{x \in I} \bar{x}$ は S 上の mapping の semigroup となり、 $\bar{x} \cdot \bar{y} = \overline{xy}$ である。 $\bar{I}$ を A の characteristic semigroup と呼ぶ。

[定義 4.2] automaton $A = (S, I, M)$ が strongly connected とは任意の $s_1, s_2 \in S$ に対して $x \in I$ が存在して $s_2 = M(s_1, x)$ が成り立つ事。

[定義 4.3] automaton $A = (S, I, M)$ の S 上の permutation g が automorphism とあるとは、 $M(sg, x) = M(s, x)g$ for any s, x を満たす事である。

[定理 4.1] automaton $A = (S, I, M)$ の automorphism の全体は group をなす。その group を $G(A)$ である。

(証明) g, h ; automorphisms とする。 $M(sgh, x) = M((sg)h, x) = M(sg, x)h = M(s, x)gh$ 。よって gh は automorphism である。よって group となる。 Q.E.D.

[定理 4.2] automaton $A = (S, I, M)$ が strongly connected の時 $G(A)$ は S 上の regular permutation group である。

(証明) $g \in G(A)$, $sg = s$ とする。 $x = M(s, x)$ として,
 $xg = M(s, x)g = M(sg, x) = M(s, x) = x$ よって g は identity
 である。 Q.E.D.

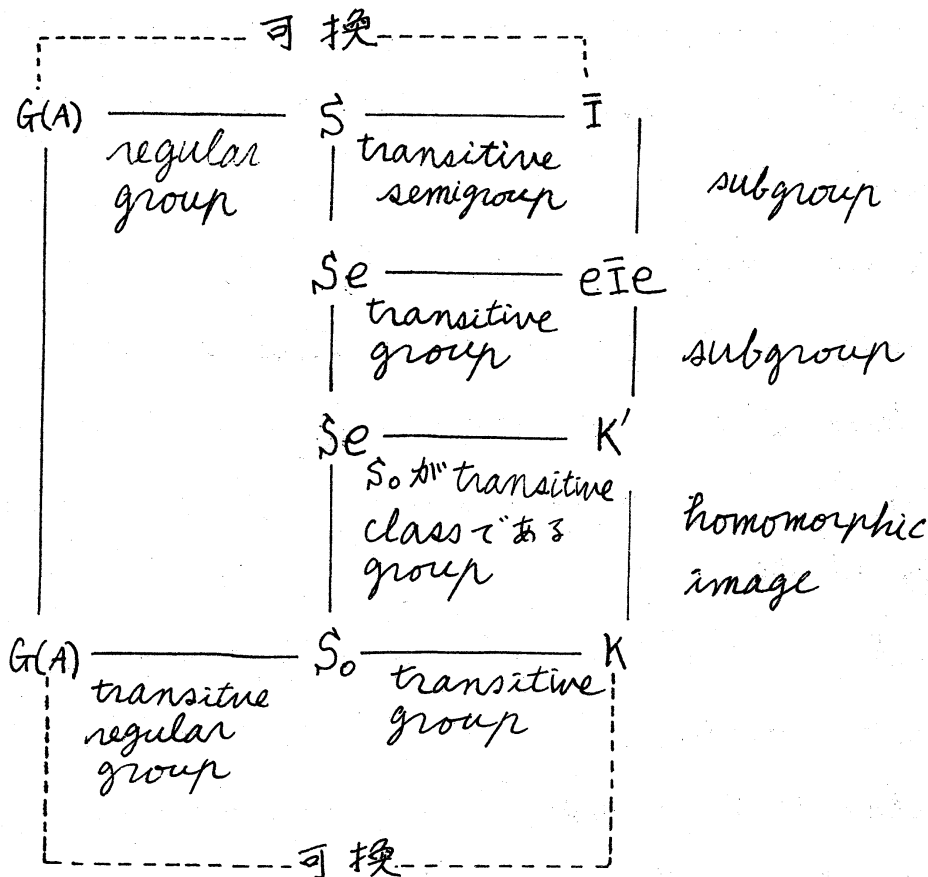
(系 4.1] automaton $A = (S, I, M)$ が strongly connected の時,
 $\# G(A)$ は $\# S$ の約数である。 [系 2.1] による。

[定理 4.3] ([5] Theorem 2.4) $A = (S, I, M)$ が strongly connected
 automaton とする。 e を I の minimal idempotent とすると,
 $G(A)$ は eIe の subgroup の homomorphic image である。

(証明) $s_0 \in Se$ にする。 $s_0 e = s_0$ である。 ([定理 3.3]) x_e で,
 $\bar{x}_e = e$ なる I の elements の 1 つ をあつねふことにする。 s_0 をふ
 くた $G(A)$ の transitive class を S_0 と表すと, $S_0 = s_0 \cdot G(A) = s_0 e G(A)$
 $= M(s_0, x_e) G(A) = M(s_0, G(A), x_e) = s_0 G(A) e \subset Se$. 即ち $S_0 \subset Se$.
 $s_1, s_2 \in S_0$ として $\bar{y} \in eIe$ があつて $s_1 \bar{y} = s_2$ ([定理 3.3]) と
 する。 この時 $S_0 \bar{y} = s_1 G(A) \bar{y} = M(s_1, G(A), \bar{y}) = M(s_1, \bar{y}) G(A)$
 $= s_1 \bar{y} G(A) = s_2 G(A) = S_0$. $\therefore S_0 \bar{y} = S_0$. よって $\bar{y}$ は S_0 上の per-
 mutation であり, $G(A)$ の定義より $G(A)$ の elements と可換である。
 よって $K' = \{ \bar{y} \mid \bar{y} \in eIe, S_0 \bar{y} = S_0 \}$ とすると K' は $Se \cap eIe$
 の subgroup で S_0 は K' の transitive class となっている。 K' が S_0
 上の transitive permutation group K の mapping を $g \mapsto g|_{S_0}$
 で定義するとこれは homomorphism である。 K は S_0 上の transitive
 permutation group で, 同じく S_0 上 transitive な regular

permutation group $G(A)$ と可換である。よって (定理 2.17 より)

K は $G(A)$ と isomorphic, 即ち $G(A)$ は $e\bar{I}e$ の subgroup の homomorphic image である。



よって $G(A) \cong K$

Q.E.D.

注意: Fleck は $A=(S, I, M)$ が strongly connected の時 $G(A)$ が $\bar{I}$ の subgroup の homomorphic image である事を示している。興味ある問題としては $G(A) \cong e\bar{I}e$ となるための必要十分条件を求める事であるが, 筆者はそれについて最近解を得た。いわゆる strongly connected, state-independent automaton においては

成り立っている事が示される。

文献

1. Weeg, G.P. "The structure of an automaton and its operation-preserving transformation group". J.ACM 9 P345 '62
2. Fleck, A.C. "Isomorphism group of automata", J.ACM. 9 P468 '62
3. Oehmke, R.H. "On the structure of an automaton and its input semigroup", J.ACM, 10 P521 '63
4. Barnes, B "Groups of automorphisms and sets of equivalence classes of input for automata", J.ACM, 12 P561 '65
- 5 Fleck, A.C. "On the automorphism group of automata." J.ACM, 12 P566 '65
- 6 Bavel, Z "Structure and transition preserving functions of finite automata", J.ACM, 15 P135 '68
- 7 Wielandt, H. Finite Permutation Groups. Academic Press, New York, '64.