数理解析研究所講究録
第 123 巻 1971 年 68-80

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 $\{X_1, X_2, \cdots, X_r\}$ とすると $\# G = \# X_i$ である

(証明) $x_0 \in X_i$ を fixed する

$\varphi : G \to X_i$ を $g \mapsto x_0 g$ で定義する．

i) $x_0 g \sim x_0$ 即ち $x_0 g \in X_i$ 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 $g'g^{-1} = id$ $\therefore g' = g$

よって φ は one-to-one $\therefore \# G = \# X_i$ 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 と同じであり，

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 $X=\{1,2,\cdots,m,m+1,\cdots,2m,\cdots,\alpha m+1,\cdots,(\alpha+1)m\}$ として，G による transitive class を $\{1,\cdots,m\},\{m+1,\cdots,2m\},\cdots\{\alpha m+1,\cdots(\alpha+1)m\}$ とする。$X_\lambda=\{\lambda m+1,\cdots,(\lambda+1)m\}$ $0\leqq\lambda\leqq\alpha$ とおく.

$G=\{g_1,\cdots,g_m\}$, $g_1=id$ としておく，(これらは〔補助定理2.1〕による.) 各 class より1つづつ 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 $\lambda m+k=(\lambda m+1)g_k$ $(1\leqq k\leqq m)$ で定める，

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

$$(\lambda m+i)g_k=\{(\lambda m+1)g_i\}g_k=(\lambda m+1)g_i g_k=\lambda m+1\cdot g_i g_k$$
$$=\lambda m+i\cdot g_k \qquad 1\leqq i,k\leqq m.$$

第1段. permutationsの set $H=\{h_1,\cdots,h_m\}$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 $X_\lambda h_k=X_\lambda$ $(0\leqq\lambda\leqq\alpha, 1\leqq k\leqq m)$ 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。

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

ここで $1\cdot g_{jg_i}=j g_i=1\cdot g_j\cdot g_i$。Gが regular である事から, $g_{jg_i}=g_j g_i$ $\qquad (g_{i\cdot g}=g_i\cdot g \quad g\in G)$ ‥‥(1)

よって $*=\lambda m+k\, g_j\cdot g_i=\lambda m+(k g_j)g_i$

$=(\lambda m+i)h_{kg_j}$ $\quad (0\leqq\lambda\leqq\alpha, 1\leqq i\leqq m)$

即ち $h_j\cdot h_k=h_{kg_j}$ $\qquad (1\leqq j,k\leqq m)$ ‥‥(2)

よってHは permutationとしての演算に閉じているから group である。

$\lambda m+i, \lambda m+j\in X_\lambda$ として $\lambda m+j=\lambda m+k g_i$ とする。$\lambda m+j=\lambda m+k g_i=(\lambda m+i)h_k$. よってHは$X_\lambda$上transitive. よってHの transitive classes は $\{X_0, X_1,\cdots\cdots X_\alpha\}$ 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 $(\lambda m+i)h_k=\lambda m+k\,g_i=(\lambda m+k)g_i$ $\therefore (\lambda m+1)g_i=(\lambda m+k)g_i$

g_i^{-1} をかけて $\lambda m+1=\lambda m+k$ $\therefore k=1$ $\therefore h_k=h_1=id$. よって

Hは regular である。

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

$=\lambda m+j\,g_i g=\lambda m+j\,g_{ig}$ (1)より

$=(\lambda m+ig)h_j=(\lambda m+i)g\,h_j$ $(0\leqq\lambda\leqq\alpha,\ 1\leqq i\leqq m)$

よって $h_j g=g\,h_j$

第4段 $\varphi: G\rightarrow H$; by $g_i\longmapsto h_i^{-1}$ $(=g_i\mapsto h_i\mapsto h_i^{-1})$ を考えるとこれは well-defined, surjective, injective。

$\varphi(g_i\cdot g_j)=\varphi(g_{i}\cdot g_j)\underset{(1)より}{=}(h_{i}\cdot g_j)^{-1}=(h_j\cdot h_i)^{-1}{}_{(2)より}$

$=(h_i)^{-1}\cdot(h_j)^{-1}=\varphi(g_i)\,\varphi(g_j)$ よって $G\cong H$

第5段 $G=\{g_1,\cdots,g_m\}$ $X=\{1,\cdots,m\}$ 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.

$h\in H$, $1\cdot h=k$ $(k\in X)$ とすると, $i\cdot h=1\cdot g_i h=1\,h\,g_i$

$=k\cdot g_i$ $(i=1,\cdots,m)$ となってGの全ての elementと可換で

1をkに動かす permutation はただ1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) $a \leq b$, $b \leq c \Rightarrow a \leq c$を満す事が容易に確められる．

〔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 $\Leftrightarrow$ $ee' = e'e = e'$, かつ$e' \in E \Rightarrow e' = e$

〔補助定理3.1〕 Sをfinite semigroupとし, $s \in S$とする．その時自然数nが存在してs^nはidempotentである．

(証明) Sがfiniteだから$s^{m+r} = s^m$となる自然数m, rが存在する．$(0 < m < r)$ よって$m \leqq gr < m+r$となる自然数gがただ1つ存在する．$s^{gr+r} = s^{m+r+(gr-m)}$ $(0 \leqq gr - m < r)$ $= s^{m+gr-m} = s^{gr}$ $\therefore (s^{gr})^2 = s^{gr+gr} = s^{gr+r+(g-1)r}$ $= s^{gr+(g-1)r} = \cdots = s^{gr}$ よってs^{gr}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。$ee' = e'e = e'$ ゆえ $ee'e = (ee')e = e'e = e'$ ∴ $e' \in eSe$. 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 $(ese)^r$ が idempotent とする. (〔補助定理3.1〕) $e(ese)^r = (ese)^r e = (ese)^r$. 即ち $(ese)^r \leq e$。e が minimal より $(ese)^r = e$ である。よって $r = 1$ ならば $ese = e$ となって e が逆元になり, $r \geq 2$ ならば $(ese)^{r-1}$ 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. $(e_1e_2e_1)^m = e_1$, $(e_2e_1e_2)^n = e_2$ 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) $(e_1e_2e_1)^m$ が idempotent であれば, e_1 が minimal より, $(e_1e_2e_1)^m = e_1$ となる. $(e_2e_1e_2)^n$ についても同様である.

$m > n$ とする. $e_1 = (e_1e_2e_1)^m = e_1e_2(e_2e_1e_2)^{m-1}e_1$

$= e_1e_2(e_2e_1e_2)^{n+(m-n-1)}e_1 = e_1e_2(e_2e_1e_2)^{m-n-1}e_1$
$(m-n-1 \geq 0)$

$= (e_1e_2e_1)^{m-n}$ 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 $m \leqq n$ である。m, n ; e_1, e_2 の対称性より $n \leqq m$ 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 をその minimal idempotents とする。 $e_1Se_1 \cong e_2Se_2$ である。

(証明) $(e_1e_2e_1)^m = e_1$, $(e_2e_1e_2)^m = e_2$ となる m が存在する。
(〔補助定理3.2〕) $\varphi: e_1Se_1 \to e_2Se_2$ を次の様に定義する。

$\varphi: e_1se_1 \mapsto (e_2e_1)^m e_1se_1(e_1e_2) = (e_2e_1)^m s e_1e_2$

i) well-defined はあきらか.

ii) $e_2se_2 = (e_2e_1)^m e_2se_2(e_1e_2)^m = (e_2e_1)^m\{e_2se_2(e_1e_2)^{m-1}\}e_1e_2$

$\therefore \varphi(e_1e_2se_2(e_1e_2)^{m-1}e_1) = e_2se_2$。よって φ は surjective

iii) $\varphi(e_1s_1e_1)\cdot\varphi(e_1s_2e_1) = \{(e_2e_1)^m s_1e_1e_2\}\{(e_2e_1)^m s_2e_1e_2\}$

$= \{(e_2e_1)^m s_1(e_1e_2e_1)^m s_2e_1e_2 = (e_2e_1)^m s_1e_1s_2e_1e_2$

$= \varphi((e_1s_1e_1)\cdot(e_1s_2e_1))$。よって φ は homomorphism.

iv) $(e_2e_1)^m se_1e_2 = e_2$ とすると, $e_1(e_2e_1)^m se_1e_2 = e_1e_2$

$\therefore e_1se_1e_2 = e_1e_2 \quad \therefore e_1s(e_1e_2)^m e_1 = (e_1e_2)^m e_1$

$\therefore e_1se_1 = e_1$ よって φ 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 semigroup 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。 $x = ye \ (y \in X)$ $xe = ye^2 = ye = x$
$\therefore xe = x$ ---- (1). 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 $xg = xge \in X_0$

$\therefore Xg \subset X_0$。特に $X_0 g \subset X_0$ $\therefore X_0 g_0 \subset X_0$ $xg = yg$ $x, y \in X_0$ とすると まず $xe = ye$ よって(1)より $x = y$ ゆえに $X_0 g = X_0$ $\therefore X_0 g_0 = X_0$ 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 $xg_0 g_0' = xeg_0 g_0' = xegg' = x(gg')_0$

$\therefore g_0 g_0' = (gg')_0$

よって φ は isomorphism である。

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

（証明） $xe, ye \in Xe$ とする．S が transitive より s が存在して $(xe)s = ye$ $\therefore (xe)se = ye \cdot e = ye$ $\therefore xe(ese) = ye$．よって eSe は transitive である。 Q.E.D.

§4 Strongly Connected Automaton の Automorphism Group

〔定義4.1〕 automaton とは $A = (S, I, M)$ である．S は states の finite set。I は finite inputs より生成される free semigroup である．empty word は必ずしも I に入っていない。

M は $S \times I \to S$ 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 $s \in S$ とすると これは equivalence relation となる. x のふくまれる class を $\bar{x}$ であらわすとこれは 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 であるとは, $M(sg, x) = M(s, x)g$ for any s, x を満す事である。

〔定理 4.1〕 automaton $A = (S, I, M)$ の automorphism の全体は group をなす。その group を $G(A)$ であらわす。

(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 も又 automorphism である。よって group となる。 Q.E.D.

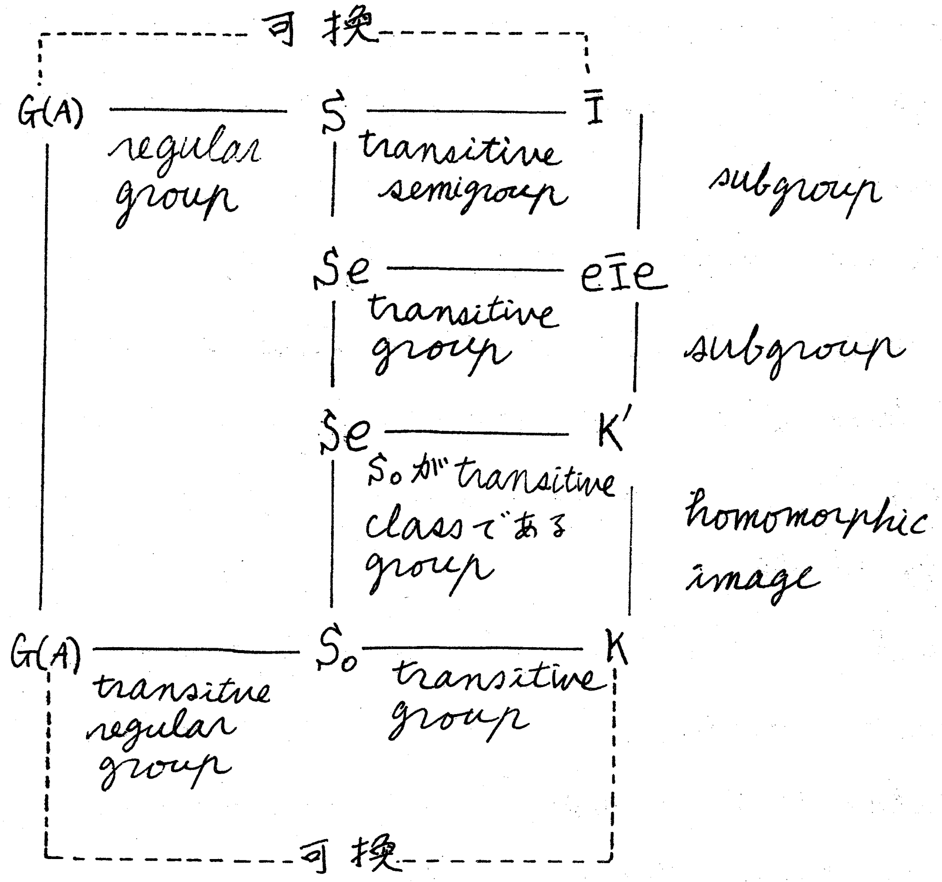
〔定理 4.2〕 automaton $A = (S, I, M)$ が strongly connected の時 $G(A)$ は S 上の regular permutation group である。

【証明】 $g \in G(A)$, $sg = s$ とする。$t = M(s, x)$ として，$tg = M(s, x)g = M(sg, x) = M(s, x) = t$ 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） $s_0 \in Se$ にとる。$s_0 e = s_0$ である。（〔定理 3.3〕）x_e で，$\overline{x_e} = e$ なる I の elements の1つをあらわすこととする。s_0 をふくむ $G(A)$ の transitive class を S_0 で表すと，$S_0 = s_0 \cdot G(A) = s_0 e G(A) = M(s_0, x_e) G(A) = M(s_0 G(A), x_e) = s_0 G(A) e \subset Se$．即ち $S_0 \subset Se$．$s_1, s_2 \in S_0$ として $\overline{y} \in eIe$ があって $s_1 \overline{y} = s_2$（〔定理 3.3〕）とする。この時 $S_0 \overline{y} = s_1 G(A) \overline{y} = M(s_1 G(A), y) = M(s_1, y) G(A) = s_1 \overline{y} G(A) = s_2 G(A) = S_0$ $\therefore S_0 \overline{y} = S_0$ よって $\overline{y}$ は S_0 上の permutation であり，$G(A)$ の定義より $G(A)$ の elements と可換である。よって $K' = \{\overline{y} \mid \overline{y} \in eIe, S_0 \overline{y} = S_0\}$ とすると K' は Se 上 eIe の subgroup で S_0 は K' の transitive class となっている。K' から S_0 上の transitive permutation group K への 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2.1〕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.