数理解析研究所講究録 1228 巻 2001 年 22-27

Sylow's Theorem for Association Schemes

平坂　貢 (Mitsugu Hirasaka),* Mikhail Muzychuk,
Paul-Hermann Zieschang

2001 年 2 月 19 日

本講演の内容はシローの定理のアソシエーションスキームへの拡張についての議論であり、M.Muzychuk と P.-H.Zieschang との共同研究である。

1　序

アソシエーションスキーム（以下ＡＳと略す）は有限集合 X に可移に作用する置換群の $X \times X$ 上での軌道全体の満たすいくつかの性質によって定義されたものである。従って有限群の正則置換もＡＳの一例であり、これは即ち有限群全体がＡＳ全体の中に埋め込まれていることを意味している。本研究は「埋め込まれた有限群全体で成り立つシローの定理をＡＳ全体でどこまで拡張できるのか？」という方針をもとにして進められている。

まずは学部生に戻ったつもりで群の定義および諸性質を復習してみよう。

群とは結合法則を満たす二項演算が定義された集合で、その二項演算に関する単位元と各逆元を有するものである。有限群の部分集合がその二項演算に関して閉じているときに部分群という。部分群は群をその剰余類に分割し、もし部分群が正規であれば商群が自然に定義される。

この道筋のＡＳ版を次節で辿ってみよう。その前にＡＳの定義を正確に述べる。なお記号に関しては P.-H.Zieschang 著の「An Algebraic Approach to Association Schemes」で与えられているものを使用する。

定義 1.1. X を有限集合として、R を $X \times X$ の分割とする。通常 R の元は relation と呼ばれる。(X, R) は次の三つの条件を満たすときにアソシ

*発表者。浦項工科大学計算数学科 (POSTECH, Com^{2}MaC) 所属、ポストドクター。

エーションスキームと呼ばれる。
(i) $1_X := \{(x,x) \mid x \in X\} \in R$;
(ii) $\forall r \in R,\ r^* \in R$;
(iii) $\forall d,\ e \in R,\ A_d A_e = \sum_{f \in R} a_{def} A_f$.
ただし A_r は $r \in R$ に関する隣接行列であり、$\{a_{def}\}$ は $\{A_r\}$ を基底とする全行列環の部分環の構造定数である。

ここで R の部分集合全体 $\mathcal{P}(R)$ 上で複合積と呼ばれる二項演算を次のように定義する。
$\mathcal{P}(R) \times \mathcal{P}(R) \to \mathcal{P}(R)$,
$(D,E) \mapsto DE := \{f \in R \mid \sum_{d \in D} \sum_{e \in E} a_{def} \neq 0\}$
この複合積は結合法則を満たすが、この積に関して群論と類似の議論を展開して行くことが基本方針である。

2 積閉集合と商スキーム

有限群の部分集合で二項演算で閉じているものを部分群というが、このことを複合積について考えてみよう。

(X,R) をＡＳとする。このとき R の部分集合 F が複合積に関して閉じているときに積閉集合と言う。すなわち、$FF \subseteq F$。

任意の積閉集合 F は X の同値関係を導くことが知られており、R も「$r \sim s \iff a \in FsF$」の同値関係によって分解される。これは群論で言うところの両側分解の一般化である。
$X/F := \{xF \mid x \in X\}$, $R/\!\!/F := \{r^F \mid r \in R\}$
ただし $r^F := \{(xF, yF) \mid y \in x(FrF)\}$.
そのとき $(X/F, R/\!\!/F)$ はＡＳになることが知られていて F による商ＡＳと呼ばれる。

ここで留意したいのがＡＳの場合は任意の積閉集合がその商ＡＳを導くと言うことである。これは、群の部分群の場合はその剰余類が必ずしも自然な商群を導かないことと比較して、ＡＳに関する命題の帰納法を用いる際に重宝する性質である。

群論におけるラグランジェの定理のＡＳ版も成り立つ。それを紹介する前に「位数」に対応する valency という数を定義する。ＡＳの各 relation の隣接行列はコンスタントな行和をもつが、この数を valency と言う。そして R の部分集合 E の valency（n_E と記す）は E の元の valency の和として定義される。すなわち、$n_E = \sum_{e \in E} n_e$ ただし $n_e := a_{ee^*1}$。次の式が

ラグランジェの定理のＡＳ版である。ただしFは積閉集合である。

$$n_R = n_{R/\!/F} n_F.$$

そして商ＡＳの各 vlency も次の式で計算される。

$$\forall F \le R,\ r \in R,\ n_{r^F} = n_{FrF}/n_F.$$

次節で具体的な例を考えよう。

3　ＡＳの例、p-valeced 条件

第一節にて有限群がアソシエーションスキームに埋め込まれると書いたが、その埋め込み方を示す。Gを有限群とする。そのとき$(G, \tilde{G})$はＡＳになる。ただし

$$\forall g \in G,\ \tilde{g} := \{(a,b) \mid ba^{-1} = g\}, \tilde{G} := \{\tilde{g} \mid g \in G\}.$$

ここで任意の$g \in G$に対して$n_{\tilde{g}} = 1$となることに注意しよう。この性質は複合積を通常の群の演算と同一視可能ということを導く。すなわち「$\forall g, h \in G,\ \tilde{g}\tilde{h} = \{\tilde{gh}\}$」である。逆に valency が全て 1 のＡＳはある有限群から上記のように導かれるものと同型であることはよく知られている。

この埋め込まれた有限群の商ＡＳを考えてみよう。HをGの部分群とする。このとき明らかに$\tilde{H}$は$\tilde{G}$の積閉集合であり、その商ＡＳの頂点集合はHの剰余類になり、relation set はHによるGの両側分解と自然に対応している。言葉を変えると、$\tilde{G}$はGのG/Hへの自然な作用によって定義される group case と呼ばれるもＡＳと同型である。

シローの定理は学部の教科書に出てくるほど身近で有名な有限群論の定義である。シローの定理のＡＳ版は一体どのような命題になるのだろうか？群の二項演算を複合積で位数を valency で置き換えて類似な命題を作ることはできるが、一般のＡＳではその命題は偽になってしまう。しかしながら次に述べるp-valenced 条件が全てを成功に導く。

素数pを固定する。すべての valency がpのベキであるＡＳはp-valenced 条件を満たすという。

p-valenced ＡＳの例を挙げて見よう。Gを有限群としてPをGのp-部分群とする。そのときの商ＡＳ$(G/P, \tilde{G}/\!/\tilde{P})$は$p$-valenced 条件を満たす。これは両側分解したときの位数がpベキになることから明かある。特に$(G, \tilde{G})$もp-valenced になる。

もっとわかりやすい例を挙げると$(p+1)$点からなる完全グラフからできるＡＳもp-valencedになる。

これらの例は全てgroup caseであるが、次にgroup case以外の例を挙げよう。Hanaki, MiyamotoによってI頂点数が28以下のＡＳは完全に分類されているのだが[1]その中でNo.176と番号付けられているものは2-valencedであり、group caseではないこともわかっている。

4 主定理とその証明の概略

定理 4.1. pを素数として、(X,R)を*p-valenced*なＡＳとする。このとき$|X| = p^i m$、ただし$i \in \mathbb{Z}_{\geq 0}$, $(m,p) = 1$と表せる。$\mathrm{Syl}_p(R) := \{P \leq R \mid n_P = p^i\}$と記そう。このとき次が成り立つ。
(i) $\mathrm{Syl}_p(R) \neq \emptyset$
(ii) $\forall P,\ S \in \mathrm{Syl}_p(R),\ \exists g \in R\ s.t.\ g^* P g = S.$
(iii) $|\mathrm{Syl}_p(R)| \equiv 1 \pmod{p}.$

（注意）(X,R)をp-valencedと仮定する。そのとき、Xの位数がpで割り切れることとvalency$p$の積閉集合があることは同値になる。これはXの位数が各valencyの和になっていることとvalency1のrelation達は群構造をもつことから導かれる。つまり、もしpが$|X|$の約数ならば$\mathbf{O}_\theta(R) := \{r \in R \mid n_r = 1\}$のvalencyも$p$で割り切れて、ということは$\mathbf{O}_\theta(R)$の中にvalency pの部分群があることになる。逆にこのような積閉集合があるならラグランジェの定理のＡＳ版によりXの位数がpで割り切れることがわかる。

次は一般のＡＳに関するよく知られた補題である。証明は

$$A_E A_F = \sum_{g \in EF} \lambda_g A_g$$

という式を考えれば一目瞭然なので割愛する。

補題 4.2. 任意のRの部分集合$E,\ F$に関して$n_E \leq n_{EF} \leq n_E n_F$が成り立つ。

次も一般のＡＳに関する補題である。

[1] `http://kissme.shinshu-u.ac.jp/as/data/as28` を参照

補題 4.3. H, K を R の積閉集合として、 g を R の元とする。このとき次が成り立つ。
(i) $n_{gK} = n_K \iff g^*g \subseteq K$.
(ii) $n_K = n_{HgK} \iff g^*Hg \subseteq K$
(iii) n_{HgK} は $n_H n_g n_K$ の約数である.

（証明）(i) まず $x \in X$ を固定。このとき x の g 近傍のすべての点 z に関する H-近傍の和集合が x の gH-近傍になる。こいつらの和が n_{gK} と一致することと $n_{gK} = n_K$ という条件は同値である。K が積閉集合なので、これらの集合は互いに一致するかまたは排反になるかのどちらかである。それゆえ、$n_{gK} = n_K$ という条件はこれらの集合がすべて一致することを意味しており、g^*g が K が導かれる。逆も明らか。（図を書くと理解しやすい。）

(ii)gK は HgK に含まれる。なぜならば H は積閉集合で 1_X を含むから。それゆえ、$n_K = n_{HgK}$ という条件は等号を意味する。K も積閉集合なので 1_X を含み、それゆえ $Hg \subseteq gK$ が成り立つ。この両辺に左から g^* をかけて、$g^*Hg \subseteq g^*gK$ が導かれる。ひとまずこいつから離れて、$n_K = n_{HgK}$ という条件は更に $n_K = n_{gK}$ という条件を導く。このとき (i) より、$g^*g \subseteq K$ それゆえ、$g^*Hg \subseteq K$ が示された。逆に $g^*Hg \subseteq K$ より、$g^*HgK \subseteq K$ となり、$n_{HgK} \leq n_{g^*HgK} \leq n_K$ となり、$n_K = n_{HgK}$ を導く。

(iii) まず、隣接行列の積、$A_H A_g A_K$ を考える。こいつも隣接行列達の線形結合で表される。すなわち $A_H A_g A_K = \sum_{r \in HgK} \lambda_r A_r$。このとき「$\lambda_g = \lambda_r, \forall r \in HgK$」が次のような組合せ的な数え上げで証明できる。$z$ を x の g-近傍とする。$\lambda_g = |g \cap (xH \cap zK)|$ に注意する。$e \in HgK$ なので $(u, v) \in e$ となる $u \in xH$、$v \in zK$ が存在する。$\lambda_e = |g \cap (uH \cap vK)|$ に注意する。$uH = xH$、$vK = zK$ なので、$\lambda_e = \lambda_g$ である。

最後に $A_H A_g A_K = \sum r \in HgK \lambda_r A_r$ の両辺に成分が全て 1 の行列をかけて「n_{HgK} は $n_H n_g n_K$ の約数である」ことが導かれる。

補題 4.4. (X, R) を *p-valenced* なＡＳとして、P を *valency* が p べきな積閉集合とする。そのとき $(X/P, R/\!\!/P)$ もまた *p-valenced* である。

（証明）まず商ＡＳの valency は $n_{r^P} = n_{PrP}/n_P$ の式で与えられるので、補題 4.3(iii) より、この数は $n_P n_r n_P$ の約数だが、n_P と n_r は p ベキなので n_{PrP} も p べきになり、それゆえ、r^P の valency も p ベキになる。

主定理の証明（ただし (iii) の証明はより多くの準備が必要なので割愛）

(i)F を R の積閉集合で valency が p ベキのものとする。補題 4.4 より、$(X/F, R/\!/F)$ も p-valenced である。もし $n_P < p^i$ ならば $|X/F|$ は p を約数に持つ。これは $R/\!/P$ の積閉集合で valency が p のものが存在するということを主定理後の注意で述べたので、ＡＳにおける対応定理を用いて、R の積閉集合で P を真に含むものがあることがわかる。これを繰り返して $\mathrm{Syl}_p(R) \neq \emptyset$ を導く。

(ii)P と S を $\mathrm{Syl}_p(R)$ の元とする。R は P と S の両側分解で書けることが知られている。すなわち $R = \bigcup_{t\in T} PtS$。このとき $|X| = n_R = \sum_{t\in T} n_{PtS}$ である。n_{PtS} は p^i 以上で補題 4.3(iii) より p ベキである。すると p^i は X の位数を割る最大の p ベキなので、$\{n_{PtS}\}_{t\in T}$ のどれか一つはちょうど p^i になる。すなわち $n_{PtS} = p^i$ となる $g \in T$ が存在する。補題 4.3(ii) より、$g^*Pg \leq S$ となることがわかり valency を比較して等号を得る。

参考文献

[1] A. Hanaki, I. Miyamoto, `http://kissme.shinshu-u.ac.jp/as/data/as28`.

[2] P.-H. Zieschang, An Algebraic Approach to Association Schemes, Lecture Notes in Mathematics 1628, *Springer,* 1996.