

12

木村：“位数 $4n(n-1)$ の
 n 次の 2 重可遷群”について

名大大学院 岩崎 史郎

よく知られているように，多くの単純群が 2 重可遷群として表わされるが，2 点の *stabilizer* によって 2 重可遷群はどの程度特徴づけられるだろうか？ $\mathcal{G}$ を 2 重可遷群とし，その 2 点の *stabilizer* $\mathcal{H}$ を色々変えてみよう。

$|\mathcal{H}| = 1 \Rightarrow \mathcal{G} : \text{Frobenius 群}$

$|\mathcal{H}| = \text{odd} \Rightarrow$ i) $\mathcal{G}$ は *regular normal subgroup* を含む
 か又は

ii) $\mathcal{G}$ は単純群 $L_2(q)$, $S_2(q)$, $U_3(q)$

($q = 2^n \geq 4$) のどれかに同型な正規部分群を含む。(Bender)

$|\mathcal{H}| = \text{even}$ のときは，

$|\mathcal{H}| = 2 \Rightarrow \mathcal{G} \cong \text{PSL}(2, 5) \text{ 或 } S_4$. (S は $\text{SL}(2, 8)$
 の 3 次の拡大で *degree* 28)

という伊藤氏の結果が出ているが， $|\mathcal{H}| = 4$ のとき， $\mathcal{G}$ は何

か? 木村さんの論文はこの自然な向に答えたものである。

即ち,

$\mathcal{G}$ を $\Omega = \{1, 2, \dots, n\}$ 上の 2 重可遷群で regular normal subgroup を含まないとし, 1, 2 の stabilizer $\mathcal{K} = \mathcal{G}_{1,2}$ はその共役と独立 i.e. $\forall G \in \mathcal{G}, \mathcal{K} \cap \mathcal{K}^G = 1$ 或 $\mathcal{K}$ とする.

(I) $\mathcal{K}$: cyclic $\implies \mathcal{G} \cong \text{PGL}(2, 5)$ or $\text{PSL}(2, 9)$

(II) $\mathcal{K}$: (2, 2) 型 abelian $\implies \mathcal{G} \cong \text{PSL}(2, 7) \cong \text{PSL}(3, 2)$

$\mathcal{K}$ の fixed point の集合 $\mathcal{J}(\mathcal{K}) = \{\alpha \in \Omega \mid \alpha^G = \alpha \text{ for } \forall G \in \mathcal{K}\}$ を $\{1, 2, \dots, i\}$ ($i \geq 2$) とすると, $\mathcal{K}$ の独立性は次のことを意味する; $\mathcal{K}$ が cyclic, $\mathcal{K} = \langle K \rangle$ のときは $K = (1)(2) \cdots (i)$

$\underbrace{(\underbrace{1, 2, \dots, i}_{4})}_{4} \cdots \underbrace{(\underbrace{1, 2, \dots, i}_{4})}_{4}$ (i.e. K は 2-cycle $\underbrace{(\underbrace{1, 2}_{2})}_{2}$ を含まない) であり, $N_{\mathcal{K}} \mathcal{K} = C(K^2)$ である. (K がこのような形にかけることは、定理の証明で矛盾を出すとき最後のとどめとして使われる.)

$\mathcal{K}$ が (2, 2) 型 abelian のときは $\mathcal{K}$ のすべての元 $\neq 1$ は $(1)(2) \cdots (i) \underbrace{(\underbrace{1, 2}_{2})}_{2} \cdots \underbrace{(\underbrace{1, 2}_{2})}_{2}$ の形をしている.

証明は伊藤氏にならって $\mathcal{G}$ が 2 重可遷群であるから, 1 の stabilizer $\mathcal{G}_1 = \mathcal{f}$ によって $\mathcal{G}$ を分解し ($\mathcal{G} = \mathcal{f} + \mathcal{f} I \mathcal{f}$, ここに I は $I = (1, 2) \cdots$ なる形の involution), $\mathcal{G}$ の involution の個数と $\mathcal{f}$ の involution の個数との関係を調べることから始める. その際, $\mathcal{G}$ 又は $\mathcal{f}$ の involution を fixed

* Ω を $\mathcal{G}$ の部分集合とすると, $N_{\mathcal{G}} \Omega$, $C_{\mathcal{G}} \Omega$ はそれぞれ Ω における $\mathcal{G}$ の normalizer, $\mathcal{G}$ の centralizer を表わす.

point 0, 1個, 2個以上のものにわけて考える (fixed point が2個以上の involution は $\bar{K}$ の involution に共役だから、その $\mathcal{G}$ における個数 a は $[\mathcal{G} : N\bar{K}]$ を使って表わされる; $\bar{K}$ が cyclic, $\bar{K} = \langle K \rangle$ のときは K^2 が $\bar{K}$ の唯一の involution で、 $N\bar{K} = C(K^2)$ より $a = [\mathcal{G} : N\bar{K}]$. $\bar{K}$ が (2, 2) 型 abelian のときは $\bar{K}$ が丁度3個の involution をもつから $a = 3[\mathcal{G} : N\bar{K}]$). Witt の定理によって $N\bar{K}/\bar{K}$ は $\{1, 2, \dots, i\}$ 上2重可遷で Frobenius 群 ($|N\bar{K}/\bar{K}| = i(i-1)$) となることから、 i はある素数 p の巾乗 ($i = p^m$) になることがわかる. involution の個数の関係式から、 $n = \text{odd}$ (どんな involution も1個以上 fix する), $n = \text{even}$ (どんな involution も1個だけ fix することはない, つまり fixed point 0 か2個以上) のそれぞれの場合に n が i によって表わされ、従って $\mathcal{G}$ の order が i 従って p で表わされる. n の i による表わし方は $I (\in N\bar{K})$ の $\bar{K}$ への作用のしかたを反映して $n = \text{odd}$, $n = \text{even}$ の場合それぞれに4通りあり、計8通りあることがわかる. この8通りの場合を吟味し、次々に矛盾を導き、残るのは定理で言ったようなものだけであると話をすすめていく. 8通りにわけられた場合を矛盾に追いやって消していくときに使われるのは、 $N\bar{K}/\bar{K}$ が $\{1, 2, \dots, i\}$ 上2重可遷な Frobenius 群であること, normal complement の存在を保証する Burnside

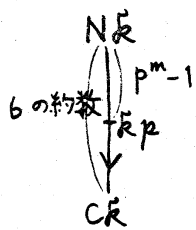
や Schur-Zassenhaus の定理, automorphism の働き方からその働きを受ける群の性質を明らかにする定理, そしていつもいつもお世話になる Sylow の定理などである。

場合の消し方の概略を見てみよう。

$n = \text{odd}$ のとき (このとき $p = \text{odd prime}$)

p を $N\bar{K}$ ($i = p^m, |N\bar{K}| = 4i(i-1) = 4p^m(p^m-1)$) の p -Sylow 群とすると, $N\bar{K}/\bar{K}$ が $\{1, 2, \dots, i\}$ 上 Frobenius 群であることから p は elementary abelian で $p \triangleleft N\bar{K}$.

$\bar{K}p/\bar{K}$ は Frobenius 群 $N\bar{K}/\bar{K}$ の Frobenius kernel だから $\bar{K}p$ と $C\bar{K}$ は含む, 含まれるの関係にある。 $\bar{K}$ が cyclic のときは $[N\bar{K} : C\bar{K}] = 1$ 或 2 だから $p \subset C\bar{K}$, 従って $\bar{K}p \subset C\bar{K}$.



$\bar{K}$ が $(2,2)$ 型 abelian のときは $C\bar{K} < \bar{K}p \leq N\bar{K}$ ならば, 左図より p, m が決まり ($p = 3, m = 1$) が決定する (そのような $\bar{K}$ はないか, 定理で主張したようなもの)。

$\bar{K}$ が cyclic でも, $\bar{K}$ が $(2,2)$ 型 abelian でも $\bar{K}p \subset C\bar{K}$ (このとき, p が elementary abelian より $p \subset C_p$, よって $\bar{K}p \subset C_p$) のときは次のようにする。まず $\bar{K}p$ と C_p とのずれを調べる。 p が $\bar{K}$ の p -Sylow 群にもなっているときは, Sylow, Burnside, Schur-Zassenhaus の定理を使って, $\bar{K}p$ は C_p において normal complement をもつことがいえる (

$\mathcal{G}$ は C_p の Hall subgroup であることから $\mathcal{G} \triangleleft N_p$ もわかる。
 従って $N_{\bar{K}} \subset N_p$ は $\mathcal{G}$ に働く)。 $N_{\bar{K}}$ における p の complement $\mathcal{H} = \mathcal{G} \cap N_{\bar{K}}$ の $\mathcal{G}$ への働き方を調べる ($\mathcal{G}$ は fixed point をもたないことや $|\mathcal{G}| \mid n$ などを使って) と, $\mathcal{H}$ のどの元 $\neq 1$ も $\mathcal{G}$ の元 $\neq 1$ と可換にならず, 従って $|\mathcal{G}| \geq |\mathcal{H}| + 1 = 4(p^m - 1) + 1 = 4p^m - 3$ となる。ところが, 一方では $|\mathcal{G}| \mid n$ (n は p によって表わされている) だから, いま出た $\mathcal{G}$ の order のとりうる値と比較して矛盾を出す。これでもまだ矛盾が出ない場合 ($|\mathcal{G}| = 4p^m - 3$ ($p \neq 3$) で $\mathcal{H}$ は $\mathcal{G}^\# = \mathcal{G} - \{1\}$ に transitive に働く場合, $\mathcal{G}$ は elementary abelian q -group (q は p でない素数)) は, $\mathcal{G}$ が $\mathcal{G}$ の q -Sylow 群であること, p の normalizer N_p と $\mathcal{G}$ の normalizer $N_{\mathcal{G}}$ の関係を調べ, それが Sylow の定理に反することをいう。

p が $\mathcal{G}$ の Sylow 群でないとき ($\sqrt[n]{\bar{K}: \text{cyclic}} = i^2 = p^{2m}$ や $n = i(4i-3) = p^m(4p^m-3)$, $p=3$ のときがその場合だが, 後者の場合をごく簡単に述べよう) は, その centralizer C_p は p よりも order の高い p -Sylow 群 p' をもつことになり, $C_p = \bar{K} p'$ (p' は $\mathcal{G}$ の p -Sylow 群にもなっていることが $\mathcal{G}$ の order からわかる) となることがわかる (これは少々面倒だが, p や p'/p の automorphism を調べたりして出す)。そして p , p'/p から p' の性質 (p' が abelian になるとか, $\bar{K}$ の p' への働き方)

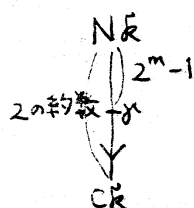
を調べて矛盾を出すのである。

以上に見るように、 $\bar{R}$ が cyclic のときは比較的面倒であるが、 $\bar{R}$ が $(2, 2)$ 型 abelian のときはかなり簡単である。それはひとえに、 n の p による表わされ方によっている。即ち、 $\bar{R}p \subset C\bar{R}$ のときは上記の説明中、 $|p| \geq 4p^m - 3$ と $|p| \mid n$ を比較する所で全部矛盾が出て、話は済んでしまうのである。 $C\bar{R} < \bar{R}p \leq N\bar{R}$ のときにしても、 $p = 3$ (4ページ参照) となることと、 n の p による表わされ方から直ちに話は済む。つまり、 $|p| = 3^m \mid |p|$ であるが、たとえば、 $n = \frac{1}{3}p^m(p^m + 2) = \frac{1}{3} \cdot 3^m(3^m + 2)$ のときは、 $|p| = 4n(n-1) = 4 \cdot \frac{1}{3} \cdot 3^m(3^m + 2) \cdot \frac{1}{3}(3^m - 1)(3^m + 3)$ で $3^m \nmid |p|$ となって矛盾である。

$n = \text{even}$ のとき (このとき $p = 2$ となる)

今度は、上の場合と逆に、 $\bar{R}$ が cyclic のとき簡単で、 $\bar{R}$ が $(2, 2)$ 型 abelian のときが面倒である。 $N\bar{R} (|N\bar{R}| = 2^{m+2}(2^m - 1))$ の 2-sylow 群を $\mathfrak{p}$ としよう。 $\mathfrak{p}/\bar{R}$ は Frobenius 群 $N\bar{R}/\bar{R}$ の Frobenius kernel だから、 $\mathfrak{p}$ と $C\bar{R}$ は含む、含まれるの関係にある。($\mathfrak{p}$ は $n = \text{odd}$ のときの $N\bar{R}$ の p -sylow 群 $\mathfrak{p}$ と比べて、 $\bar{R}$ とのかかわりあいなどが全く異なる; $\bar{R} \subset \mathfrak{p}$ であるが $\bar{R} \cap \mathfrak{p} = 1$)。

$\bar{R}$ が cyclic のとき、 I の $\bar{R}$ への作用のしかたは 2通り ($K^I = K^{-1} \sim K$) あり、 $K^I = K^{-1}$ のときは $I \not\subset C\bar{R}$, $I \subset \mathfrak{p}$



から, 左図のようになって $m=1$, 従って $i=2$ となり, 定理で主張しているような φ が出てくる. $K^I = K$ i.e. I が R に trivial に働くときは, $K \in C(I)$ で (従って $C(I)$ は order 4 の元 K をもつ), $I \sim K^2$ ($\sim$ は共役を表わす. φ が 2 重可遷だからこのように仮定してよい.) から $C(I) \sim C(K^2) = NR$. また, φ/R は degree $i=2^m$ の 2 重可遷な Frobenius 群 NR/R の 2-sylow 群だから elementary abelian であるが, このことから $C(I)$ の order 4 の元は 2 乗するとすべて I になり, $K^2 = I$ ($K^2 = (1)(2)\dots$, $I = (12)\dots$) となって矛盾が出る.

R が $(2,2)$ 型 abelian のときは, I が R に trivial に作用しても, $C(I)$ は order 4 の元をもつことがいえないから, 上のようにはいかない。それ故に, 今度は面倒になるのである。(因みに, 伊藤氏の扱ったものは, $|R|=2$ だからやはり $C(I)$ が order 4 の元をもつことがいえず, ここから S という変てこな群が飛び出して来たのである。) 木村さんは, ここを次のようにして切り抜けた. $\mathcal{U}$ を NR における φ の complement ($|NR|=2^{m+2}(2^m-1)$, $|\mathcal{U}|=2^m-1$, Schur-Zassenhaus) とすると, $\mathcal{U}$ の φ への働き方から, φ の各元は具体的に

$$\varphi = R + \sum_{v \in \mathcal{U}} I^v R \text{ とかけることを有効に使うのである.}$$

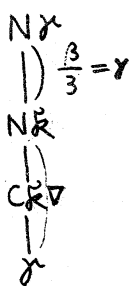
$C_R \lt \varphi$ のときは扱いやすい: 先と同じような図式から,

$m=2$, 従って $\mathcal{M}$ は order $2^{2+2}=16$ の non-abelian となる.

一方, $\mathcal{M}$ の元の形から $\mathcal{M}$ は丁度 9 個の involution をもっていることがわかる. しかし, order 16 の non-abelian group でこのような群は存在しない.

$\mathcal{M} \leq CR$ のときが問題である.

β を丁度 β 個を fix する $\mathcal{M}$ の involution の個数とする (つまり, R の単位元以外の 3 個の元は丁度 β 個だけ fix する involution であるが, このような元と共役な $\mathcal{M}$ の元が β 個あるとする.). $\mathcal{M}$ の中に R と共役な subgroup が γ 個あると



すれば, $[q:NR] = \gamma [q:N\mathcal{M}]$.

R はその共役と独立だから, $\beta = 3\gamma$. よって

左図のような図式がえられる. 一方, 少し前に

言ったように, $\mathcal{M}$ の各元 (単位元以外は fix point

ないか, 丁度 β 個だけ fix する) は具体的にかけている

ことから, β のとりうる値も決まる. $N\mathcal{M}$ の q における in-

dex $[q:NR]$ が β の値を使って表わされるが, これが整数

になるかどうかを調べるのがこの論法の要点である.

以上, 大まかに概略を述べたが, 統一した基本的な考え方がわからないままに書いたので, すっきりしない. 更に

$|R| = \text{odd}$ の場合の Bender の論文も読んでいないので比較

もできず, おもしろくないがお許し願いたい.

なお、最近、木村さんは、上の問題を発展させて、2点の *stabilizer* が order 2 の *cyclic group* のときの2重可遷群をも決定した。結果は予測したような群で、変てこなものは出てこないが、証明はかなり複雑のようである。勿論、 $|K| = 4$ の場合の証明が model になっている ($n = \text{even}$ で、 K が $(2, 2)$ 型 *abelian* の所で述べた論法も使われる)。

大抵、どんな本でも言いたいことは沢山あるけれど、紙数の関係上割愛せざるをえないらしいが、小生、木村さんの論文をよく理解していないこともあって、何も言うことができない。渡された原稿用紙があまってあまって仕方がないので、木村さんや名大での群論ゼミのことを2, 3行書いておこう。木村さんは山育ちのせいもあってか、実に悠々、淡々としておられる。数学の研究も無理なく伸び伸びとやっておられるようで、しかもここぞというときには気魄がこもる。木村さんに接した人が誰でも感ずるように、とても遊び好きで親しみやすく、ときにはゼミの時間をさいて恋愛特殊講義さへして下さる。

都筑先生、木村さん、原田さんの名コンビによるゼミは外野席で見物している僕達には、話している内容はちっともわからなくても、各自が言いたいことを言われ、すこぶる痛快であった。木村さんなどは机の上に足をのせたりして、とて

も行儀がわるい。

けれども、この4月から都筑先生が北大へ行かれてしまい、名コンビの大きな一角がくずれてしまった。そしてまた夏には原田さんが Princeton に行かれることになっている。都筑先生、原田さんに行かれて困るけれど、木村さんに尻をたたかれながらやっていくことにしよう。