

GRIESS による MONSTER の構成について

オハイオ州立大学 原田耕一郎

ミシガン大学の Griess は 1980 年 3 月 難問とされて
いた MONSTER の計算機を使わずに構成に成功したと発表
した。それは非結合的ではあるが可換な代数 (Algebra)
を使うもので 群論の新しい研究方向を示唆しているよう
に思える。ここでは Griess による MONSTER の構成の概
略と 多重可移群と可換代数の関係について述べる。

議論の大まかの理解のためには小さい群がよいので、先ず
5 次の交代群 A_5 を例にとる。 A_5 の指標表は次のようなもの
である。

元	1	2	3	5_1	5_2
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

$$2 = (12)(34)$$

$$3 = (123)$$

$$5_1 = (12345)$$

$$5_2 = (13524)$$

M を指標 χ の表現空間とするとき $M \otimes M$ は一般に次のように分解する.

$$M \otimes M = S^2(M) \oplus A^2(M)$$

ここで $S^2(M)$, $A^2(M)$ はそれぞれ 2 次の対称積, 交代積と呼ばれているもので, どちらも既約とはかぎらない。

$S^2(M)$ の元 g における指標の値が

$$\frac{\chi(g)^2 + \chi(g^2)}{2}$$

であることに注意して A_5 の $S^2(\chi)$ の分解の表をつくってみると次のようになる。

	χ_1	χ_2	χ_3	χ_4	χ_5
$S^2(\chi_1)$	1	0	0	0	0
$S^2(\chi_2)$	1	0	0	0	1
$S^2(\chi_3)$	1	0	0	0	1
$S^2(\chi_4)$	1	0	0	1	1
$S^2(\chi_5)$	1	0	0	1	2

さて M を χ_4 の表現空間とすると $\dim M = 4$ であって, $S^2(M)$ は M を唯一回既約成分として含む. そこで

$$f: M \otimes M \xrightarrow{\text{proj}} S^2(M) \xrightarrow{\text{proj}} M$$

なる写像を考えれば f は nontrivial である。しかも A_5 不変である。おまわち

$$f(a, b)^g = f(a^g, b^g) \quad a, b \in M, g \in A_5$$

が成立している。 f が $S^2(M)$ を経て M 上へ写すのであるから さらに

$$f(a, b) = f(b, a), \quad a, b \in M$$

も成立している。ここで次の定義をおく。

定義 $ab = f(a, b), \quad a, b \in M.$

上に述べた事実によって M に可換で A_5 -不変な代数構造が入ったわけである。これは一般には非結合的な代数構造である。 $S^2(M)$ の中には M が唯一回入っているわけであるから上記のように定義される構造は unique に定まる。 A_5 の 4 次の表現に対して 代数構造を実際に求めてみよう。

オーの方法

λ を A_5 の order 5 の元とせよ。 $\chi(\lambda) = -1$ であることにより λ の M 上の eigenvalue は $\lambda, \lambda^2, \lambda^3, \lambda^4, \lambda = e^{2\pi i/5}$ となる。 e_1, e_2, e_3, e_4 を対応する eigenvector とする。すべての積 $e_i e_j$ を決めればよい。 λ の $e_i e_j$ に対する作用を調べると $e_i e_j \in \mathbb{C} e_{i+j}$ となっていることは自明である。ただし $i+j$ は mod 5 で考え $e_0 = 0$ と定義しておく。

$$e_i e_j = a_{ij} e_{i+j}, \quad a_{ij} \in \mathbb{C}$$

とあって すべての a_{ij} を決めることに帰着する。 $a_{23} = a_{14} = 0$ であるが その他の a_{ij} を求めるためには さらに大きい群 $N = N_{A_5}(\langle x \rangle)$ が必要である。 N の中には τ という involution があって $x^\tau = x^{-1}$ となっている。適当に scalar 倍をとることにより $e_1^\tau = e_4, e_2^\tau = e_3$ としよう。これによって $a_{11} = a_{44}$ 等の情報が得られる。さらに考えている部分群を大きくしてやうか、少しちがうもの等も考えることにより 結局

$$e_i e_j = e_{i+j} \quad 1 \leq i, j \leq 4$$

という簡明な式が得られる。これで M の代数構造が決まったわけである。

次の方法

M_0 を A_5 の自然な 5 次の表現の表現空間とせよ。

$$M_0 = \langle x_1, x_2, x_3, x_4, x_5 \rangle$$

このとき M は次のようにみえる。

$$M = \frac{M_0}{\langle x_1 + x_2 + x_3 + x_4 + x_5 \rangle}$$

$\bar{x}_i$ 等が M の元をあらわせば、知りたりのは $\bar{x}_i^2$ と $\bar{x}_i \bar{x}_j$ の値である。 A_5 の多重可移性により

$$\bar{x}_1 \bar{x}_3 = a_1 \bar{x}_1 + a_2 \bar{x}_2 + a_3 \bar{x}_3 + a_4 \bar{x}_4$$

$$\bar{x}_1 \bar{x}_2 = b_1 \bar{x}_1 + b_2 \bar{x}_2 + b_3 \bar{x}_3 + b_4 \bar{x}_4$$

αとき, $a_i, b_i, 1 \leq i \leq 4$ がわかればよい. A_5 の適当な元で上の式を変換して代数構造が A_5 不変なることを使えば容易なる計算で

$$\bar{x}_i \bar{x}_i = -3b_i \bar{x}_i$$

$$\bar{x}_i \bar{x}_j = b_i (\bar{x}_i + \bar{x}_j) \quad i \neq j$$

なる式を得る. $-\frac{1}{b_i} \bar{x}_i$ を再び $\bar{x}_i$ と書けば,

$$\bar{x}_i \bar{x}_i = 3\bar{x}_i \quad 1 \leq i \leq 5$$

$$\bar{x}_i \bar{x}_j = -\bar{x}_i - \bar{x}_j \quad 1 \leq i < j \leq 5$$

を得る. これで α の方法によっても代数構造が唯一に決まったわけである。

上の考察では 簡単のために 11 元群 A_5 をとったが実は任意の 3 重可移群から同様な代数が得られる. すなわち G を $\Omega = \{1, 2, 3, \dots, n+1\}$ 上の 3 重可移群とするとき M を n 次の既約置換表現とすれば A_5 α ときと同じ記号を使うことにすれば

$$\bar{x}_i \bar{x}_i = (n-1) \bar{x}_i \quad 1 \leq i \leq n+1$$

$$\bar{x}_i \bar{x}_j = -\bar{x}_i - \bar{x}_j \quad 1 \leq i < j \leq n+1$$

となることが証明できる.

次に上のようにつくられた可換代数の自己同型群は何かなるものがあるのか. 代数を作るにあたって使用した群 A_5 を

どが自己同型群の中に含まれることは自明だが一般にはそれよりも大きくなる。3重可移群から作られた代数の場合は次の定理が得られる。

定理 A を体 F 上の可換 (非結合的) 代数で次の条件を満たすものとせよ。

(1) A は $\alpha_1, \alpha_2, \dots, \alpha_n$ を basis に持つベクトル空間である。

(2) $\alpha_i \alpha_i = (n-1)\alpha_i, \quad 1 \leq i \leq n$

$\alpha_i \alpha_j = -\alpha_j - \alpha_i, \quad 1 \leq i < j \leq n.$

このとき、もし体の標数が $n+1$ より大きいならば A の自己同型群は $n+1$ 次の対称群 S_{n+1} となる。

自己同型群の元で $\det$ が 1 になるものの全体が交代群 A_{n+1} になることは明白である。この定理の証明にあたっては、 $\alpha_{n+1} = -\alpha_1 - \alpha_2 - \dots - \alpha_n$ とおくと $\{\alpha_1, \alpha_2, \dots, \alpha_{n+1}\}$ が 均質 となり自己同型群がその上に働くことになる。

さて表題にあるモンスターの話に移るわけであるが、モンスターは位数が大きいだけで目的は同じである。もちろん A_5 とモンスターでは、鉛筆大のロケットを打ち上げるのと、巨大なロケットを木星や土星にまで導びくのと、の差ぐらい。

技術的なちがいがあろう。後者の方をやりとげた Griess の仕事は正に画期的なものである。

A_5 において 4次元の空間と det であったものが モンスター においては 196883次元の空間と associative form と Griess が呼ぶところのある形式とを不変にするようなものの全体としてとらえられる。

単純群 G であってその一つの involution σ の中心化群 $C_G(\sigma)$ が位数 2^{25} の extra special group の $\cdot 1$ による拡大となっているものは存在すべし unique に定まる。

$C = C_G(\sigma)$ とおけば C は実在する群である。 M を C の既約表現で次数が 299, 98280 と 98304 の直和とせよ。 M は、故に、 C 空間としては確かに実在する。 M の上に可換代数の構造を定めて その自己同型群 (の一部) として モンスターをとらえようとするのが目的である。 先ず M に C 不変な代数を入れる。 M が 3つの空間の直和であることなどによりその構造は unique には定まらない。 Griess によれば 6つのパラメーターによって書けるということである。

次に $\langle C, \sigma \rangle = \text{"モンスター"}$ となるような自己同型 σ を定義してやる必要がある。 モンスターは存在証明以外はなんでもわかっていいるわけだから群論的には都合のよい σ を見つけることはできる。 その σ の C に対する性質を利用して σ の M

における作用を定めて、 σ の自己同型としての存在を確定させる。その過程において先の6つのパラメーターのうち5つの線型独立な関係式が得られるので M の可換代数の構造は殆んど unique に定まる。ただし構造が unique であるかどうか自体は モンスターの存在とは直接関係はない。都合のよい構造がひとつあって、その自己同型群の中に求めるモンスターが入っていることだけが問題をなすのである。

さて上のごとくして存在の確定した $G = \langle C, \sigma \rangle$ なる M の自己同型群の部分群が実際有限群となって、もとめる群モンスターになることは証明の必要なことである。そのための C および σ をマトリックスとして実際に書いたものを使う。そのマトリックス表現 (196883次元) を見れば $p=2, 3$ 以外の素数では good reduction があることがわかる。言い換えると表現は有理数体上で書けているのである。 $G(p)$ をその良い素数 p に対する reduction とせよ。 $G(p)$ はもちろん有限群であって有限群の諸定理が使える。それらを使えば $G(p)$ の中で $\mathbb{F}(p)$ の中に化群がもとの C に同型なることがわかる。よってモンスターの特徴づけにより $G(p)$ はモンスターに同型なることがわかる。これでモンスター自体の存在は確定するわけだが、 $G(p)$ が $p=2, 3$ 以外の素数全部についてモンスターとなるのであるから G 自体がモンスター

一となっていることも同時にわかるのである。これで主目的
 となっている存在証明は終るわけである。 Griess はさらに
~~議論~~をすすめて、ある associative form というものを導入
 すれば、それを含めた意味での M の自己同型群が $G = \langle C, \sigma \rangle$
 となることも証明しているようである。

モンスター存在証明の概要は以上のようなものであるが、くわし
 くは Griess の論文を見ていただくより他はない。計算につぐ
 計算の長い論文である。