数理解析研究所講究録
第424巻 1981年 13-21

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の計算機を使わない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も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。

議論の大すじ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

$2=(12)(34)$
$3=(123)$
$5_1=(12345)$
$5_2=(13524)$

14

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。すなわち

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

が成立している。f が $S^2(M)$ を経て M の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．

<u>定義</u>． $ab = f(a,b)$ ，$a, b \in M$.

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。

<u>オ一の方法</u>．

x を A_5 の order 5 の元とせよ．$\chi(x) = -1$ であることにより x 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_ie_j を決めればよい。 x の e_ie_j に対する作用を調べると $e_ie_j \in \mathbb{C}e_{i+j}$ 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。

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

とおいて 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 t という involution があって $x^t=x^{-1}$ となっている. 適当に scalar 倍をとることにより $e_1^t=e_4$, $e_2^t=e_3$ とればよい。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ゆくか, 少しちがうもの等を考えることにより 結局

$$e_ie_j=e_{i+j} \qquad 1\le i,j\le 4$$

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。

<u>オニの方法</u>

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は次のようにみなせる.

$$M=M_0/\langle x_1+x_2+x_3+x_4+x_5\rangle$$

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

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

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

のとき, a_i, b_i, $1\le i\le 4$ 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

$$\bar{x}_i\bar{x}_i = -3b_1\bar{x}_i$$

$$\bar{x}_i\bar{x}_j = b_1(\bar{x}_i+\bar{x}_j) \qquad i\neq j$$

なる式を得る。 $-\frac{1}{b_1}x_i$ を 再び x_i と書けば,

$$\bar{x}_i\bar{x}_i = 3\bar{x}_i \qquad 1\le i\le 5$$

$$\bar{x}_i\bar{x}_j = -\bar{x}_i-\bar{x}_j \qquad 1\le i<j\le 5$$

を得る. これで 第二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 簡単のために小さい群 A_5 をとったが実は任意の3重可移群からも同様な代数が得られる. すなわち G を $\Omega=\{1,2,3,\cdots,n+1\}$ 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 のときと同じ記号を使うことにすれば

$$\bar{x}_i\bar{x}_i = (n-1)\bar{x}_i \qquad 1\le i\le n+1$$

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

となることが証明できる.

次に上のように与えられた可換代数の自己同型群はいかなるものであろうか. 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ろう. 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。

<u>定理</u> Aを体k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 $x_1, x_2, \quad, x_n$ を basis にもつベクトル空間である。

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

$x_i x_j = -x_i - x_j \quad , \qquad 1 \leq i < j \leq n$.

このとき. もし体k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 Σ_{n+1} となる。

自己同型群の元で det が 1 になるもの全体が交代群 A_{n+1} になることは明白であろう。上の定理の証明にあたっては. $x_{n+1} = -x_1 - x_2 - \cdots - x_n$ とおくと $\{x_1, x_2, \cdots, x_{n+1}\}$ が<u>均質</u>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全体としてとらえられる。

単純群Gであってそのひとつのinvolution zの中心化群 $C_G(z)$が 位数 2^{25}の extra special group の ·1 による拡大となっているものは存在すれば unique に定まる。$C = C_G(z)$ 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つのパラメターによって書けるということである。

次に $\langle C, \sigma \rangle$ = "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つのパラメターのうちに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 それ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なのである。

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。言いおくれたが 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 $z(p)$の中心化群がもとの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

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た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。

モンスターの存在証明の概要は以上のようであるが，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。