アソシエーション・スキームとその表現

花木 章秀

信州大学 理学部

JMO 夏季セミナー (清里高原)
August 28, 2014

代数的組合せ論

代数的組合せ論

- 誤り訂正符号
  情報通信の際の雑音 (ノイズ) を除去するための理論
  純粋数学としての研究も盛んに行われている
- デザイン (配置)
  構造をもった母集団から良い部分集合を得るための理論

$\longrightarrow$ アソシエーション・スキーム (Delsart 理論)

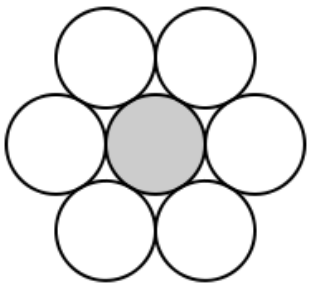
球面上の組合せ論

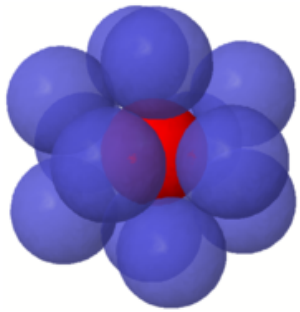
球面上に良い性質をもった有限個の点をとる。

Kissing number problem

kissing number $=$ n 次元球面に接する同じ大きさの球面の個数の最大値
(接点が球面上の有限個の点となる。ケプラー予想と密接に関係する。)

$n = 1$ のとき 2
$n = 2$ のとき 6
$n = 3$ のとき 12 (ニュートンとグレゴリーの論争 1694,
シュッテ-ヴェルデン 1953)
$n = 4$ のとき 24 (Musin 2003)





球面上の組合せ論

Kissing number

n	1	2	3	4	5	6	7	8	9	10	$\cdots$	24	$\cdots$
$\sharp$	2	6	12	24	40	72	126	240	306	500	$\cdots$	196560	$\cdots$
					44	78	134		364	554	$\cdots$		$\cdots$

類似の問題

辺の長さが x, y の長方形に辺の長さが 1 の正方形を何個詰め込むことができるか？

(x, y を整数としていないことに注意)

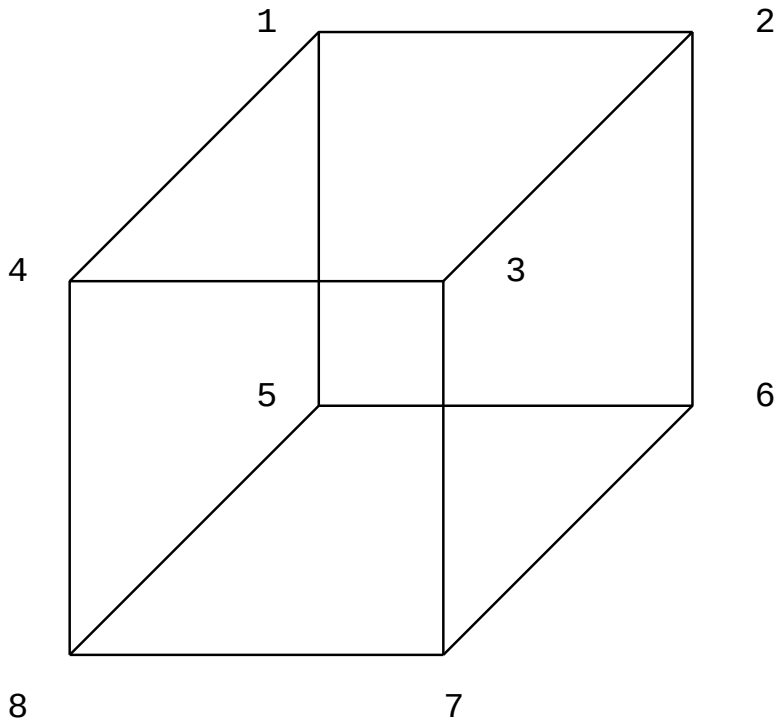
$$\lfloor x \rfloor \lfloor y \rfloor \leq n \leq xy$$

x, y が共に整数ならば、上限と下限が一致し、値が確定する。

(一般には難しく、未解決問題の一つである。)

正多面体の頂点

5 つの 3 次元正多面体 (正 n 面体, $n = 4, 6, 8, 12, 20$) は色々な意味で “美しい” 図形である。
正 6 面体 (立方体) を例として、その頂点の集合がどのような性質をもつかを考える



頂点間の距離を成分とする行列を考える。

正多面体の頂点

$$R = \left(\begin{array}{cccc|cccc} 0 & 1 & 2 & 1 & 1 & 2 & 3 & 2 \\ 1 & 0 & 1 & 2 & 2 & 1 & 2 & 3 \\ 2 & 1 & 0 & 1 & 3 & 2 & 1 & 2 \\ 1 & 2 & 1 & 0 & 2 & 3 & 2 & 1 \\ \hline 1 & 2 & 3 & 2 & 0 & 1 & 2 & 1 \\ 2 & 1 & 2 & 3 & 1 & 0 & 1 & 2 \\ 3 & 2 & 1 & 2 & 2 & 1 & 0 & 1 \\ 2 & 3 & 2 & 1 & 1 & 2 & 1 & 0 \end{array}\right)$$

成分に注目して、4 つの行列を作る。

$$A_0 = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right), \quad A_1 = \left(\begin{array}{cccc|cccc} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right),$$

$$A_2 = \cdots, A_3 = \cdots$$

正多面体の頂点

得られた行列 A_0, A_1, A_2, A_3 をかけてみると面白いことが分かる。

	A_0	A_1	A_2	A_3
A_0	A_0	A_1	A_2	A_3
A_1	A_1	$3A_0 + 2A_2$	$2A_1 + 3A_3$	A_2
A_2	A_2	$2A_1 + 3A_3$	$3A_0 + 2A_2$	A_1
A_3	A_3	A_2	A_1	A_0

A_iA_j は必ず A_k たちの一次結合で書けるのである。

$$A_iA_j = \sum_{k=0}^{3} p_{ij}^k A_k$$

これは他の正多面体に対しても成り立つことが確認できる。
これを一般化してアソシエーション・スキームを定義する。

アソシエーション・スキーム

$A_0, \cdots, A_d$ を 0 と 1 のみを成分とする n 次正方行列とする。
$\{A_0, \cdots, A_d\}$ がアソシエーション・スキームであるとは、次の条件をみたすこととする。

1. $\sum_{i=0}^{d} A_i$ はすべての成分が 1 の行列である
2. A_0 は単位行列である
3. A_i の転置行列はまたある $A_{i'}$ である
4. ある整数 p_{ij}^k があって $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$ となる

行列のサイズ n をアソシエーション・スキームの位数という。

$A_i A_{i'}$ の対角成分には A_i の各行にある 1 の個数が並ぶ。これが A_k たちの一次結合で表されるということから、その個数が一定であることが分かる。この個数を A_i の valency といい n_i で表す。A_i の各列にも n_i 個の 1 があることが分かる。

アソシエーション・スキームの例 - 正 6 面体

例 2.1 (立方体の定めるアソシエーション・スキーム)

$$R = \left(\begin{array}{cccc|cccc} 0 & 1 & 2 & 1 & 1 & 2 & 3 & 2 \\ 1 & 0 & 1 & 2 & 2 & 1 & 2 & 3 \\ 2 & 1 & 0 & 1 & 3 & 2 & 1 & 2 \\ 1 & 2 & 1 & 0 & 2 & 3 & 2 & 1 \\ \hline 1 & 2 & 3 & 2 & 0 & 1 & 2 & 1 \\ 2 & 1 & 2 & 3 & 1 & 0 & 1 & 2 \\ 3 & 2 & 1 & 2 & 2 & 1 & 0 & 1 \\ 2 & 3 & 2 & 1 & 1 & 2 & 1 & 0 \end{array}\right)$$

位数は 8

valency は $n_0 = 1$, $n_1 = 3$, $n_2 = 3$, $n_3 = 1$

(有限) 集合 X の置換全体の集合 $\mathrm{Sym}(X)$ を考える。

例 2.2 (3 次対称群)

$X = \{1, 2, 3\}$ のとき

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$\mathrm{Sym}(X)$ は写像の合成を演算として群となる。これを X 上の対称群という。特に $X = \{1, 2, \cdots, n\}$ であるとき $\mathrm{Sym}(X)$ を n 次対称群といい S_n と表す。S_n は $n!$ 個の元をもつ。

群と置換表現、正則表現

二項演算 $(a,b) \mapsto ab$ が定められた集合 G が群であるとは次の条件をみたすことである。

- 結合法則 $a(bc) = (ab)c$ が成り立つ。
- 単位元 e が存在する：すべての $a \in G$ に対して $ae = ea = a$
- すべての $a \in G$ に逆元 a^{-1} が存在する：$aa^{-1} = a^{-1}a = e$

任意の $a, b \in G$ に対して $ab = ba$ となるとき G をアーベル群という。

G の部分集合 H が G の演算で、また群になるとき、H を G の部分群という。これは、次の条件が成り立つことと同値である。

- $a, b \in H$ ならば $ab \in H$
- $a \in H$ ならば $a^{-1} \in H$

G が有限集合ならば、一つ目の条件だけから二つ目の条件は得られる。

例 2.3

3 次対称群 S_3 の部分集合

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

は S_3 の部分群である。(H は $S_2 = \mathrm{Sym}(\{1,2\})$ と同じものと見ることもできる。)

対称群 S_n の部分群を n 次置換群という。

定理 2.4 (Cayley)

任意の有限群はある対称群の部分群と同型である。

G を有限群とするとき、$g \in G$ を右からかけることによって G の置換が引き起こされる。この対応によって G は $|G|$ 次の置換群と同型になる。これを G の正則置換表現という。

群と置換表現、正則表現

置換を行列で表すことを考える。例えば $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ を考えよう。これを 3 次の行列で表す。その 1 行には、$1^\sigma = 2$ なので 2 列目に 1 を置き、他の成分は 0 とする。同様に 2, 3 行目も定めると

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

となる。これを置換の行列表現という。置換の積と行列の積が対応することに注意しておく。

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

群と置換表現、正則表現

有限群 G に対して、正則置換表現と行列表現をあわせて正則置換行列表現が得られる。

例 2.5

位数 3 の群の正則置換行列表現は以下の通りである。

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

命題 2.6

任意の有限群は、その正則置換行列表現を考えることによって、アソシエーション・スキームと見ることができる。

この意味で、アソシエーション・スキームは有限群の概念の一般化であるということができる。

部分群と群の剰余

有限群の正則置換行列表現を考え、その行列を一つの行列で表そう。次の二つ例のように、部分群は対角線上に並ぶ小行列のみに現れる要素に対応する。(行列の行と列は適当に並べ替えることができるので、常にこのように見えるわけではない。)

$$\left(\begin{array}{cc|cc|cc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ \hline 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 4 & 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 2 & 5 & 4 & 1 & 0 \end{array}\right), \qquad \left(\begin{array}{cc|cc|cc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 4 & 5 & 2 & 3 \\ \hline 2 & 3 & 0 & 1 & 5 & 4 \\ 4 & 5 & 1 & 0 & 3 & 2 \\ \hline 3 & 2 & 5 & 4 & 0 & 1 \\ 5 & 4 & 3 & 2 & 1 & 0 \end{array}\right)$$

各ブロックを一つの要素と見て、同じ数を含むものを同じと見なす。

$$\left(\begin{array}{c|c|c} a & b & c \\ \hline c & a & b \\ \hline b & c & a \end{array}\right), \qquad \left(\begin{array}{c|c|c} a & b & b \\ \hline b & a & b \\ \hline b & b & a \end{array}\right)$$

部分群と群の剰余

$$\left(\begin{array}{c|c|c} a & b & c \\ \hline c & a & b \\ \hline b & c & a \end{array}\right), \qquad \left(\begin{array}{c|c|c} a & b & b \\ \hline b & a & b \\ \hline b & b & a \end{array}\right)$$

これを群の部分群による剰余という。一つ目の例では剰余もまた群となっているが、二つ目の例では群ではない。剰余が群となるような部分群は正規部分群とよばれる。

一般に群の部分群による剰余はアソシエーション・スキームになる。

アソシエーション・スキームはこのように群からも自然に得られる概念でもあるのである。

アダマール行列

H を 1 と -1 だけを成分にもつ n 次正方行列とする。

$$H^t H = nI$$

(I は単位行列) となるとき H をアダマール行列という。この条件は H の各行が互いに直交する (内積が 0 である) ということである。

例 2.7

次の行列はアダマール行列である。

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

アダマール行列

定理 2.8

n 次のアダマール行列が存在すれば $n = 1, 2$ または $n \equiv 0 \pmod 4$ である。

Proof.

$n = 1, 2$ のときは存在するので、$n > 2$ と仮定する。
アダマール行列のある行、または列を -1 倍しても、それはまたアダマール行列であることに注意する。これによって、第 1 行の成分はすべて 1 であると仮定してよい。第 2 行は、第 1 行と直交するので、成分には 1 と -1 が等しい数だけある。また、アダマール行列の行や列を入れ替えても、それはまたアダマール行列である。よって、第 2 行のはじめの半分 (m 個としよう) が 1 で残りが -1 であるとしてよい。第 3 行を考える。はじめの m 個のうち a 個が 1 だったとしよう。はじめの m 個のうち -1 は $m - a$ 個ある。第 3 行も第 1 行と直交するから、後ろの m 個のうち 1 は $m - a$ 個、-1 は a 個となる。第 2 行と第 3 行が直交するから $m = 2a$ となる。したがって、行列のサイズ $2m = 4a$ は 4 で割り切れる。 □

アダマール行列

アダマール行列について有名な予想がある。

予想 2.9

$n \equiv 0 \pmod 4$ ならば n 次のアダマール行列が存在する。

2004 年に H. Kharaghani がサイズ 428 のアダマール行列を構成した。現在、存在が分かっていない最小のサイズは 668 である (らしい)。

${}^tH + H = 2I$ となるアダマール行列を歪対称アダマール行列という (対角成分がすべて 1 で、他の部分は対角線で折り返すと -1 倍)。

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

サイズ n の歪対称行列からはある性質をもつ位数 $n-1$ のアソシエーション・スキームが得られ、その存在は同値である。歪対称アダマール行列に対しても、上記の予想は未解決である。

Hamming スキーム

n, q を自然数とする。$\Omega = \{0, 1, \cdots, q-1\}$ とし

$$X = \Omega^n = \{(a_1, \cdots, a_n) \mid a_i \in \Omega\}$$

とおく。$a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n) \in X$ に対して

$$d(a, b) = (a_i \neq b_i \text{ となる } i \text{ の数})$$

とする。このとき d を距離と思って行列を作れば、それはアソシエーション・スキームを定める。これを Hamming スキームといい $H(n, q)$ と表す。

Hamming スキームは符号理論と関係している。立方体は $H(3, 2)$ である。

Johnson スキーム

v, k を自然数とする。$k \leq v/2$ と仮定する。$\Omega = \{1, 2, \cdots, v\}$ とし、X を Ω の k 点部分集合の全体とする。$a, b \in X$ に対して

$$d(a, b) = k - |a \cap b|$$

とおく。このとき d を距離と思って行列を作れば、それはアソシエーション・スキームを定める。これを Johnson スキームといい $J(v, k)$ と表す。

Johnson スキームはデザイン理論と関係している。$k > v/2$ でも同様の定義は可能であるが、$J(v, k)$ と $J(v, v-k)$ は “同じ” アソシエーション・スキームを定めるので、$k \leq v/2$ という仮定は本質的ではない。

アソシエーション・スキームの分類

アソシエーション・スキームは有限群と同じように、数学の色々な所に現れる。必要とされる場面によって、様々な特殊な性質をもったアソシエーション・スキームが考えられている。しかし、その一方で、一般論 (すべてのアソシエーション・スキームに対して成り立つ理論) を考えておけば、その利用価値は高い。

特に、どのようなアソシエーション・スキームがどのくらい存在するかを知ること (アソシエーション・スキームの分類) は、この分野における大きな問題の一つである。

アソシエーション・スキームの分類

有限群の分類

有限群はその位数が 2000 程度まで分類が済んでいるようである。有限群 G が、自明でない正規部分群 N をもつとき、G は N と剰余群 G/N を重ねて出来ていると考えることができる。自明でない正規部分群をもたない有限群を有限単純群という。したがって、有限群を分類するには

- 有限単純群の分類
- 二つの有限群の重ね合わせの理論 (拡大理論)

を知れば良いことになる。

アソシエーション・スキームの分類

有限単純群の分類

有限単純群の分類は 1980 年代に完成した (ことになっている)。

- 素数位数巡回群
- 交代群 A_n $(n \geq 5)$
- リー型の群 (16 種類の系列)
- 26 個の散在型単純群

一方で、拡大の理論は十分ではなく (十分な結果が存在するのかどうかも怪しい)、すべての有限群を分類することは現時点では不可能と思われる。しかし、有限群に関する多くの問題が、帰納法によって有限単純群の場合に帰着され、その分類を用いて解決されている。

アソシエーション・スキームの分類

アソシエーション・スキームに対しても部分スキームと剰余スキームが考えられる。

$$\left(\begin{array}{cc|cc|cc} 0 & 1 & 2 & 2 & 3 & 3 \\ 1 & 0 & 2 & 2 & 3 & 3 \\ \hline 3 & 3 & 0 & 1 & 2 & 2 \\ 3 & 3 & 1 & 0 & 2 & 2 \\ \hline 2 & 2 & 3 & 3 & 0 & 1 \\ 2 & 2 & 3 & 3 & 1 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right), \left(\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}\right)$$

自明でない部分スキームをもたないものを原始的アソシエーション・スキームという。アソシエーション・スキームの分類を考えるには、有限群の場合と同じように、

- 原始的スキームの分類
- 拡大理論

が必要になると思われる。

アソシエーション・スキームの分類

拡大理論

二つのアソシエーション・スキーム $\mathfrak{X}, \mathfrak{Y}$ を与え、$\mathfrak{X}$ を部分スキームに含み、$\mathfrak{X}$ による剰余スキームが $\mathfrak{Y}$ になるものを考えることである。有限群に対しても、特別な場合を除いて難しく、アソシエーション・スキームに対しては、有効な方法は知られていない。

もっとも簡単なアソシエーション・スキームに、二つの行列だけで定義されるもの K_n がある。

$$K_3 : \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

K_n の K_2 による拡大は対称デザインに対応しており、このように簡単な場合であってもその分類は難しい。

アソシエーション・スキームの分類

例 3.1 (対称デザイン (Fano 平面) から得られるアソシエーション・スキーム)

対称デザインの一つである Fano 平面によって定まるアソシエーション・スキームは以下の通りである。

$$\left(\begin{array}{ccccccc|cccccccc}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 2 & 2 & 2 & 3 & 3 \\
1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 3 & 3 & 3 & 2 & 2 & 3 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 2 & 3 & 3 & 2 & 3 & 3 & 2 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 3 & 2 & 3 & 3 & 2 & 3 & 2 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 3 & 3 & 2 & 3 & 3 & 2 & 2 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 3 & 2 & 3 & 2 & 3 & 2 & 3 \\
\hline
2 & 3 & 2 & 2 & 3 & 3 & 3 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 3 & 3 & 3 & 2 & 3 & 2 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
2 & 2 & 3 & 3 & 3 & 2 & 3 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
3 & 2 & 3 & 2 & 3 & 3 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
3 & 2 & 2 & 3 & 2 & 3 & 3 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
3 & 3 & 2 & 3 & 3 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
3 & 3 & 3 & 2 & 2 & 2 & 3 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{array}\right)$$

部分スキームに K_7 を含み、剰余スキームは K_2 である。

対称デザインの存在と、このタイプのアソシエーション・スキームの存在は同値である。

アソシエーション・スキームの分類

原始的スキームの分類

次のような組合せ論的な対象から原始的スキームが得られる。(これらから得られないものも多くある。)

- (ほとんどの) 強正則グラフ
- 歪対称アダマール行列
- 有限単純群

すべてが、それ自身で研究対象となるものであり、現時点では分類は無理であると思われる。特に行列のサイズが素数ならば、アソシエーション・スキームは原始的となるが、その場合でさえ分類は出来ていない。

坂内英一先生の夢

原始的アソシエーション・スキームを分類することによって、
有限単純群の分類定理を見直したい。

アソシエーション・スキームの分類

$\lvert X\rvert$	♯ a.s.	by	$\lvert X\rvert$	♯ a.s.	by	$\lvert X\rvert$	♯ a.s.
1	1	Nomiyama (1995)	16	222	Miyamoto -Hanaki (1998–) with computers	31	? $\geq 100,000$
2	1		17	5		32	18,210
3	2		18	95		33	27
4	4		19	7		34	20
5	3		20	95		35	?
6	8		21	32		36	?
7	4		22	16		37	?
8	21		23	22		38	33
9	12		24	750		39	?
10	13		25	45		40	?
11	4	Hirasaka (1997)	26	34		41	?
12	59		27	502		42	?
13	6	Hirasaka -Suga (1996)	28	185		43	?
14	16		29	26		44	?
15	25		30	243		45	?

アソシエーション・スキームの分類

アソシエーション・スキームの分類は今の所、有効な手段がなくこれ以上は困難である。

$\Longrightarrow$ 何らかの別の方針が必要

- 粗い分類
- 代数的な考察
- 表現論

環、体、ベクトル空間、代数

代数学の基本概念として環、体、ベクトル空間、および代数を定義する。群とは、一つの演算が定義されていて (1) 結合法則 (2) 単位元の存在 (3) 逆元の存在、の 3 条件をみたすものであった。

環

R が環であるとは、加法と乗法の 2 つの演算が定義されていて、

- 加法についてアーベル群
- 乗法について結合法則をみたし、単位元をもつ
- 分配法則が成り立つ

$$a(b+c) = ab + ac, \quad (a+b)c = ac + bc$$

の 3 条件をみたすものである。

整数全体の集合 (有理整数環 $\mathbb{Z}$)、n 変数多項式全体の集合 (多項式環 $K[x_1, \cdots, x_n]$)、n 次正方行列全体の集合 (全行列環 $M_n(K)$) などが環の典型的な例である。

環、体、ベクトル空間、代数

体
K が体であるとは、可換環であって、0 以外のすべての元が乗法に関する逆元をもつことをいう。

有理数全体の集合 (有理数体 $\mathbb{Q}$)、実数全体の集合 (実数体 $\mathbb{R}$)、複素数全体の集合 (複素数体 $\mathbb{C}$) などが典型的な体の例である。

2 以上の自然数 n を固定する。整数の n で割った余りだけに注目して考えるとき、"数" は $0, 1, \cdots, n-1$ だけと見ることができる。この全体の集合を $\mathbb{Z}/n\mathbb{Z}$ と表す。$\mathbb{Z}/n\mathbb{Z}$ は自然に可換環の構造をもつ。特に $n = p$ が素数であるならば $\mathbb{Z}/p\mathbb{Z}$ は体となる。
(一般に要素の数が有限である体は、この例のように、ある 1 つの素数 p と関係している。このとき、その体の標数は p であるという。$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ などに対しては、その標数は 0 であるという。)

ベクトル空間

K を体とする。(分かりにくければ、例えば実数体 $\mathbb{R}$ と思っていてよい。) 加法群 V にスカラー倍 (K の元をかけること) が定義されていて、いくつかの簡単な性質をみたすとき、V を K-ベクトル空間という。

K 上の n 次元ベクトルの全体

$$K^n = \{(a_1, \cdots, a_n) \mid a_i \in K \ (i = 1, \cdots, n)\}$$

は自然な演算によって K-ベクトル空間である。

多項式環 $K[x_1, \cdots, x_n]$ や $m \times n$ 行列の全体 $M_{m,n}(K)$ も、自然な演算によって K-ベクトル空間である。

ベクトル空間の基底

K を体とし、K-ベクトル空間 K^n を考える。$\boldsymbol{e}_1 = (1, 0, \cdots, 0)$, $\boldsymbol{e}_2 = (0, 1, 0, \cdots, 0)$, $\cdots$, $\boldsymbol{e}_n = (0, \cdots, 0, 1)$ と、1 つの成分だけが 1 のベクトルをとる。このとき、任意のベクトル $\boldsymbol{a} = (a_1, \cdots, a_n)$ は

$$\boldsymbol{a} = a_1\boldsymbol{e}_1 + \cdots + a_n\boldsymbol{e}_n$$

と一意的に表される。この性質をもつベクトルの集まりを、ベクトル空間の基底という。基底の個数をベクトル空間の次元という。

例えば $\mathbb{R}^2$ において、

- $\boldsymbol{e}_1 = (1, 0)$, $\boldsymbol{e}_2 = (0, 1)$
- $\boldsymbol{v}_1 = (1, 0)$, $\boldsymbol{v}_2 = (1, 1)$
- $\boldsymbol{w}_1 = (1, 2)$, $\boldsymbol{w}_2 = (-1, 1)$

などはすべて基底である。基底をとるということは、座標平面 (空間) に座標軸を決めるようなものであり、基底のとり方はたくさんある。

線形写像と行列

ベクトル空間 V から W への写像 f で、和とスカラー倍を保存するものを線形写像という。一般に、数学では、その構造を定める基本的な “もの” を定め、それを保存する写像を考えることが多く (圏論的な議論)、これもその一例である。$\boldsymbol{x} = \sum_{i=1}^{n} x_i \boldsymbol{v}_i$ と基底 $\{\boldsymbol{v}_i\}$ を用いて表されるとき、

$$f(\boldsymbol{x}) = \sum_{i=1}^{n} x_i f(\boldsymbol{v}_i)$$

となり、線形写像は基底の行き先のみで決まる。$\{\boldsymbol{w}_1, \cdots, \boldsymbol{w}_m\}$ を W の基底として $f(\boldsymbol{v}_i) = \sum_{j=1}^{m} a_{ji} \boldsymbol{w}_j$ と表し、A をその (i, j)-成分が a_{ij} である $m \times n$ 行列と定める。

$\sum_{i=1}^{n} x_i \boldsymbol{v}_i$ を $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ と表わせば、上記のことは

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

と表される。すなわち線形写像は基底を定めることによって、適当な行列で表される。この行列を f の表現行列という。逆に行列は線形写像を定める。

$\{\boldsymbol{v}'_i\}, \{\boldsymbol{w}'_i\}$ を V, W の別の基底とする。このとき

$$(\boldsymbol{v}'_1, \cdots, \boldsymbol{v}'_n) = (\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n)P, \quad (\boldsymbol{w}'_1, \cdots, \boldsymbol{w}'_m) = (\boldsymbol{w}_1, \cdots, \boldsymbol{w}_m)Q$$

となる正則行列 P, Q がある。

$$(\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\boldsymbol{v}'_1, \cdots, \boldsymbol{v}'_n) P^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$ だから、

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = P^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$ と置き直して

$$f \quad : \quad (\boldsymbol{v}'_1, \cdots, \boldsymbol{v}'_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\mapsto (\boldsymbol{w}_1, \cdots, \boldsymbol{w}_m) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\boldsymbol{w}'_1, \cdots, \boldsymbol{w}'_m) Q^{-1} A P \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

すなわち、基底を取りかえることによって表現行列は $Q^{-1}AP$ に変わる。特に $V = W$ としたとき、表現行列は $P^{-1}AP$ になる。

正方行列 A を、適当な正則行列 P によって $P^{-1}AP$ に変形することは、基底の取り換えを行うことに過ぎず、ある意味で A と $P^{-1}AP$ は同じものであると見ることができる。このような二つの行列は相似であると言われる。

相似な行列のうち、もっとも簡単な形のものを求める、という問題が「行列の標準化」と呼ばれる問題である。軸に対して傾いた放物線や楕円は、行列の標準化を用いて軸 (基底) を取りかえることによって、通常のものとして扱うことができる。

環、体、ベクトル空間、代数

K を体とする。環であって、K-ベクトル空間の構造をもつものを K-代数、または K-多元環という。K 上の多項式環や全行列環が K-代数の典型的な例である。

群代数 (群環)
G を乗法を演算とする (有限) 群とする。G の元を形式的な基底とする K-ベクトル空間 $KG = \{\sum_{g\in G} a_g g \mid a_g \in K\}$ を考え、積を群の積で定義する。これによって KG は K-代数となり、これを群代数、または群環という。

代数の表現

前に群の置換表現と行列表現を見た。群や代数は抽象的なものであるが、それを具体的なものを用いて表すことを表現という。

一般に二つの群 G と H に対して、群の構造を保つ写像 $f : G \to H$ を群準同型という。群は一つの演算 (乗法) で定められるものであるから、準同型であるための条件は

$$f(ab) = f(a)f(b)$$

が成り立つということである。

n 次の置換全体の集合は n 次対称群 S_n であった。有限群 G から S_n への群準同型を群の置換表現というのである。

代数の表現

K を体とし、有限次元 K-代数 A を考える。A から全行列環 $M_n(K)$ への K-代数準同型を A の行列表現という。ここで、代数は、加法、乗法、スカラー倍で定まるものであったから、$a, b \in A$, $k \in K$ に対して

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(ka) = kf(a)$$

であるものを代数準同型という。多くの場合、更に

$$f(1) = 1$$

を要求するので、ここでもこの条件を仮定しておく。

A と B の間に、準同型であり、かつ全単射であるものが存在するとき、A と B は同型であるといい $A \cong B$ と表す。

代数の表現

$f : A \to M_n(K)$ を A の表現とする。$M_n(K)$ は左からかけることによって、自然に n 次元ベクトル空間 $V = K^n$ に作用する。このとき V を左 K-加群という。

左 K-加群 V の部分空間 W で、A の作用で閉じているもの、すなわち $v \in W$ と $a \in A$ に対して $av \in W$ となるもの、を V の A-部分加群という。このとき、群などの場合と同様に剰余加群 V/W も考えられ、V は W と V/W を “重ねて” できていると考えることができる。

K-加群 V が自明でない (0 でも V でもない) 部分加群をもたないとき既約であるという。既約でないとき可約であるという。

代数の表現

表現が既約、可約であることを行列の形を用いて説明しよう。V を A-加群、W を V の部分加群とする。対応する表現を $T : A \to M_n(K)$ とする。V の基底 $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n$ を $\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m$ が W の基底になるようにとる。このとき W が A の作用で閉じていることから、$a \in A$ のこの基底に関する表現行列 $T(a)$ は

$$\left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1m} & a_{1,m+1} & \cdots & a_{1n} \\ & \cdots & & & \cdots & \\ a_{m1} & \cdots & a_{mm} & a_{m,m+1} & \cdots & a_{m,n} \\ \hline 0 & \cdots & 0 & a_{m+1,m+1} & \cdots & a_{m+1,n} \\ & \cdots & & & \cdots & \\ 0 & \cdots & 0 & a_{n,m+1} & \cdots & a_{nn} \end{array}\right)$$

となる。逆に、ある正則行列 P に対して $P^{-1}T(a)P$ がすべての $a \in A$ に対してこの形になれば表現は可約である。

左上の部分が部分加群 W に対応する表現で、右下の部分が剰余加群 V/W に対応する表現となる。

代数の表現

このように、表現 $T : a \mapsto T(a)$ と $T^P : a \mapsto P^{-1}T(a)P$ は基底の取り方が違うだけで、ある意味では同じものと考えられる。

表現 $T : A \to M_n(K)$ が既約であるときを考えよう。一般の場合は簡単には説明できないので、考える体 K は十分大きいものとする。

> 任意の多項式がその体に根をもつような体を代数閉体という。
> ここでは K が代数閉体であることを仮定しよう。例えば、有理数体 $\mathbb{Q}$ や実数体 $\mathbb{R}$ は代数閉体ではないが、複素数体 $\mathbb{C}$ は代数閉体である。

K が代数閉体であるとき、表現 $T : A \to M_n(K)$ が既約であるための必要十分条件は、T が全射であることである。すなわち、任意の行列 $M \in M_n(K)$ に対して $T(a) = M$ となる $a \in A$ が存在することである。

可約ならば全射にならないことは明らかであるが、逆は K が代数閉体であることを用いなければならず、やや難しい。

行列の標準形

代数の表現をよく理解するために、行列の標準形について簡単に説明する。

M を n 次複素正方行列とする。ある正則行列 P があって、$P^{-1}MP$ が対角行列になるとき、M は対角化可能であるという。例えば、実対称行列は対角化可能であることが知られている。

もちろん対角化可能でない行列も存在する。例えば

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

は対角化可能ではない。

行列の標準形

$\lambda \in \mathbb{C}$ と自然数 n に対して

$$J(\lambda, n) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

とおくと、任意の正方行列はこの形の行列を対角線上に並べたものと相似になることが知られている (Jordan 標準形)。

この形を代数の表現の時のように考えれば、1 次元の部分加群が積み重なっていることが分かる。右上の 1 がなければ、順番を入れ替えることができるので、加群は実質的には重なっていないことになるが、1 があると本当に重なっているのである。

半単純代数

K-代数 A の任意の表現が既約表現の直和になるとき (分解したときの右上を 0 にできるとき)、A は半単純であるといわれる。

代数閉体 K 上の半単純代数 A は

$$A \cong M_{n_1}(K) \oplus \cdots \oplus M_{n_r}(K)$$

となることが知られている (Wedderburn の構造定理)。このとき、各成分 $M_{n_i}(K)$ への射影が既約表現の同値類の代表系を与える。そして、任意の表現はこれらをいくつかずつ並べたものになっている。したがって成分の重複度だけで表現の同値類が決定される。

代数が半単純でないときには、表現の構造を知ることは難しい。行列の Jordan 標準形は、半単純でなくてもその様子が分かる例となっている。

指標

ここでは $K = \mathbb{C}$ としよう (標数 0 の代数閉体ならばよい)。A を半単純 $\mathbb{C}$-代数とする。

$$A \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$$

であり、各成分への射影 $T_i : A \to M_{n_i}(\mathbb{C})$ が既約表現の同値類の代表である。

任意の表現 $T : A \to M_n(\mathbb{C})$ に対して、そのトレース (対角成分の和) を T の指標という。

既約表現の指標を既約指標という。T_i の指標を χ_i と表す。一般に M と $P^{-1}MP$ のトレースは等しいから、同値な表現は同じ指標を与える。

A の元で、$M_{n_i}(\mathbb{C})$ の $(1,1)$ 成分だけが 1 で、他の成分がすべて 0 であるようなものに対応するものを e_i で表す。このとき

$$\chi_i(e_i) = 1, \quad \chi_j(e_i) = 0 \ (j \neq i)$$

である。

指標

T を表現とし、その既約分解を $T = \sum_{j=1}^{r} m_j T_j$ とする。このとき T の指標 χ に対しても $\chi = \sum_{j=1}^{r} m_j \chi_j$ である。ここで e_i の値を考えれば

$$\chi(e_i) = \sum_{j=1}^{r} m_j \chi_j(e_i) = m_i$$

である。表現が同値であるための必要十分条件は、すべての m_i が一致することなので、次のことが分かる。

命題 4.1

$\mathbb{C}$ 上の半単純代数 A について、二つの表現が同値であるための必要十分条件は、それらの指標が一致することである。

表現は行列に値をとる写像であり、また見かけが違っても同値なものがあるが、指標は複素数値関数であり、扱いやすい。

アソシエーション・スキームの隣接代数

アソシエーション・スキームの話に戻ろう。定義の確認をし、前とはやや違った記号を用いる。

X を有限集合とする。$s \subset X \times X = \{(x, y) \mid x, y \in X\}$ に対して、その隣接行列 $\sigma_s \in M_X(\mathbb{C})$ を、その (x, y) 成分は $(x, y) \in s$ のとき 1、そうでないとき 0 として定める。

S を $X \times X$ の分割とする。すなわち、

- 任意の $s \in S$ は空集合でない
- $X \times X = \bigcup_{s \in S} s$
- $s, t \in S$, $s \neq t$ ならば $s \cap t = \emptyset$

とする。

アソシエーション・スキームの隣接代数

組 (X, S) がアソシエーション・スキームであるとは

- $1 = \{(x, x) \mid x \in X\} \in S$
- $s \in S$ ならば $s^* = \{(y, x) \mid (x, y) \in s\} \in S$
- $s, t, u \in S$ に対して非負整数 p^u_{st} があって、$(x, y) \in u$ ならば $\sharp\{z \in X \mid (x, z) \in s, (z, y) \in t\} = p^u_{st}$

が成り立つことである。

前の定義と比べてみる。

- S が分割であることは $\sum_{i=0}^{d} A_i$ のすべての成分が 1 であること
- 一つ目の条件は単位行列があること
- 二つ目の条件は転置行列があること
- 三つ目の条件は (やや分かりにくいが) $A_i A_j = \sum_{k=0}^{d} p^k_{ij} A_k$

という条件に対応している。最後の条件を隣接行列を用いて表わせば $\sigma_s \sigma_t = \sum_{u \in S} p^u_{st} \sigma_u$ となる。

アソシエーション・スキームの隣接代数

三つ目の条件 $\sigma_s\sigma_t = \sum_{u\in S} p_{st}^u \sigma_u$ から、

$$\mathbb{C}S = \left\{ \sum_{s\in S} a_s\sigma_s \;\middle|\; a_s \in \mathbb{C} \right\}$$

は $M_X(\mathbb{C})$ の部分環となる。これを (X, S) の $\mathbb{C}$ 上の隣接代数という (0 と 1 のみを成分にもつ行列で定義されるので、隣接代数は任意の係数体上で定義される)。この講義では隣接代数の表現をアソシエーション・スキームの表現ということにする。

隣接代数は代数としては積を定める定数 (構造定数) p_{st}^u のみで決まる。構造定数が同じでも組合せ論的に異なるアソシエーション・スキームはたくさんあるので、この意味での表現論ではそれらを区別することは出来ない。したがって表現を考えるということは、アソシエーション・スキームを “粗く” 見ているということになる。

アソシエーション・スキームの隣接代数

複素数体上の隣接代数 $\mathbb{C}S$ について、次の定理は基本的である。

定理 5.1

アソシエーション・スキームの複素数体上の隣接代数 $\mathbb{C}S$ は半単純である。

これによって、アソシエーション・スキームの複素数体上の表現を考えるには、指標を考えることが有効であることが分かる。

正標数の体上の隣接代数の半単純性判定条件は [花木, 2000] によって与えられているが、やや難しい。

アソシエーション・スキームの隣接代数

$\mathbb{C}S$ は半単純なので

$$\mathbb{C}S \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_r}(\mathbb{C})$$

と表すことができる。$|S| = \sum_{i=1}^{r} {n_i}^2$ にも注意しておこう。

隣接代数が可換環になるとき、すなわち $\sigma_s\sigma_t = \sigma_t\sigma_s$ が任意の $s, t \in S$ に対して成り立つとき、アソシエーション・スキームは可換であるという。これは、上の分解に現れる全行列環のサイズ n_i がすべて 1 であることと同値である。

この講義の目標は以下の定理の証明の概略を述べることである。

定理 5.2 (花木-宇野, 2006)

(X, S) をアソシエーション・スキームとする。$|X|$ が素数であれば (X, S) は可換である。

自明な指標と標準指標

(X, S) をアソシエーション・スキームとする。$s \in S$ に対して、その隣接行列を σ_s、valency (σ_s の各行、各列にある 1 の個数) を n_s で表す。写像

$$\mathbb{C}S \to \mathbb{C}, \quad \sigma_s \mapsto n_s$$

が表現である、すなわち代数準同型になる、ことはすぐに分かる。表現の次数が 1 なので、これは表現であると同時に指標でもある。これを自明な指標といい 1_S と表す。

また $\mathbb{C}S \subset M_X(\mathbb{C})$ なので、自然な埋め込み

$$\mathbb{C}S \to M_X(\mathbb{C}), \quad \sigma_s \mapsto \sigma_s$$

が考えられ、これもまた表現となる。これを標準表現といい Γ_S と表す。またその指標を標準指標といい γ_S と表す。

自明な指標と標準指標

自明な指標 1_S はその定義から

$$1_S(\sigma_s) = n_s$$

であった。標準指標については、$1 \neq s \in S$ の対角成分はすべて 0 なので

$$\gamma_S(\sigma_s) = \begin{cases} |X|, & \text{if } s = 1 \\ 0, & \text{otherwise} \end{cases}$$

となる。自明な指標と標準指標はその値が組合せ論的に理解できるため扱いやすい。

指標の重複度

一般に指標が与えられたとき、それを既約指標の和に分解することによって、その指標の様子を調べる。

φ を指標とする。$\mathrm{Irr}(S)$ で既約指標全体の集合を表す。φ は既約指標の和で表すことができるから

$$\varphi = \sum_{\chi \in \mathrm{Irr}(S)} a_\chi \chi$$

となる非負整数 a_χ が定まる。この a_χ を φ における χ の重複度という。

特に標準指標 γ_S の分解

$$\gamma_S = \sum_{\chi \in \mathrm{Irr}(S)} m_\chi \chi$$

の m_χ を χ の重複度という。標準指標は常に与えられているので m_χ は χ に対して定まる定数と見ることができる。

指標の直交関係

隣接代数について

$$\mathbb{C}S \cong \bigoplus_{\chi \in \mathrm{Irr}(S)} M_{\chi(1)}(\mathbb{C})$$

が成り立っていて、直和因子 $M_{\chi(1)}(\mathbb{C})$ への射影が χ を与える既約表現であった。この式の左辺はアソシエーション・スキームの定義に従った組合せ論的な性質によって定義されるもので、右辺は完全に環論的な記述である。右辺の元として分かりやすいものが左辺の元として分かりやすいものとは限らない。逆も同様である。

右辺の元と見て性質の良いものとして、直和因子 $M_{\chi(1)}(\mathbb{C})$ の単位行列を考え、これに対応する左辺の元を e_χ と表す。e_χ を左辺の元として表すこと、すなわち $e_\chi = \sum_{s \in S} a_s \sigma_s$ と表すことを考える。

指標の直交関係

簡単な補題を用意する。まず、次の補題は行列の形から簡単に分かる。

補題 6.1

$\gamma_S(\sigma_s\sigma_{s^*}) = n_s|X|$ であり、$t \neq s^*$ のとき $\gamma_S(\sigma_s\sigma_t) = 0$ である。

補題 6.2 (反転公式)

$a = \sum_{s\in S} a_s\sigma_s \in \mathbb{C}S$ に対して

$$a_s = \frac{1}{n_s|X|} \sum_{\chi\in \mathrm{Irr}(S)} m_\chi \chi(a\sigma_{s^*}).$$

Proof.

$\gamma_S(a\sigma_{t^*}) = \sum_{s\in S} a_s\gamma_S(\sigma_s\sigma_{t^*}) = a_t n_t|X|$ である。一方、
$\gamma_S(a\sigma_{t^*}) = \sum_{\chi\in \mathrm{Irr}(S)} m_\chi\chi(a\sigma_{t^*})$ なので、結果を得る。 □

指標の直交関係

定理 6.3

$\chi \in \mathrm{Irr}(S)$ に対して

$$e_\chi = \frac{m_\chi}{|X|} \sum_{s \in S} \frac{1}{n_s} \chi(\sigma_{s^*}) \sigma_s.$$

Proof.

$e_\chi = \sum_{s \in S} a_s \sigma_s$ とおいて反転公式を用いると

$$a_s = \frac{1}{n_s |X|} \sum_{\varphi \in \mathrm{Irr}(S)} m_\varphi \varphi(e_\chi \sigma_{s^*}) = \frac{1}{n_s |X|} m_\chi \chi(\sigma_{s^*})$$

である。 □

指標の直交関係

e_χ の形から指標の直交関係が得られる。

定理 6.4 (指標の直交関係)

$\chi, \varphi \in \mathrm{Irr}(S)$ に対して

$$\frac{m_\chi}{\chi(1)|X|} \sum_{s \in S} \frac{1}{n_s} \chi(\sigma_{s^*}) \varphi(\sigma_s) = \delta_{\chi\varphi}.$$

ここで $\delta_{\chi\varphi}$ はクロネッカーのデルタで、$\chi = \varphi$ のとき 1、そうでないとき 0 である。

Proof.

$\varphi(e_\chi) = \frac{m_\chi}{|X|} \sum_{s \in S} \frac{1}{n_s} \chi(\sigma_{s^*}) \varphi(\sigma_s)$ で、$\chi = \varphi$ のとき $\varphi(e_\chi) = \chi(1)$、$\chi \neq \varphi$ のとき $\varphi(e_\chi) = 0$ となることから分かる。 □

指標の直交関係

直交関係の簡単な例を見てみよう。

$$\frac{m_\chi}{\chi(1)|X|}\sum_{s\in S}\frac{1}{n_s}\chi(\sigma_{s^*})\varphi(\sigma_s)=\delta_{\chi\varphi}.$$

次の表はあるアソシエーション・スキームの指標の値を表にしたもので、指標表と呼ばれる。

				m_χ
χ_1	1	2	3	1
χ_2	1	2	-3	1
χ_3	1	-1	0	4

直交関係の式の意味をよく考えて、確認してみよう。

指標の直交関係

命題 6.5

自明な指標の重複度は 1 である。

Proof.

直交関係より、$\sum_{s\in S} n_s = |X|$ と $n_{s^*} = n_s$ に注意して、

$$1 = \frac{m_{1_S}}{1_S(1)|X|}\sum_{s\in S}\frac{1}{n_s}1_S(\sigma_{s^*})1_S(\sigma_s) = \frac{m_{1_S}}{|X|}\sum_{s\in S}\frac{1}{n_s}n_s n_s = m_{1_S}$$

となることからより分かる。 □

代数的整数と代数共役

有理数係数多項式の根となる複素数を代数的数という。代数的数の和、差、積、商はまた代数的となる。代数的数全体の集合 Ω は $\mathbb{C}$ の部分体となる。

例 7.1

$\sqrt{2}$, $\sqrt{2}+\sqrt[3]{2}$, i などは代数的、e, π などは代数的でない (超越数)。

最高次係数が 1 の有理整数係数多項式の根となる複素数を代数的整数という。代数的整数の和、差、積はまた代数的整数となる。代数的整数全体の集合 Γ は Ω の部分環となる。$\Gamma \cap \mathbb{Q} = \mathbb{Z}$ であることに注意しておく。つまり、有理数であって代数的整数であるものは、有理整数 (通常の整数) であるということである。

ある代数的数 α と有理数に加減乗除を繰り返し得られる数全体の集合 $K = \mathbb{Q}(\alpha)$ を代数体とよぶ。$O_K = K \cap \Gamma$ とおいて、これを K の整数環という。

二次体の整数環

1 以外の平方数で割り切れない整数 m に対して $\mathbb{Q}(\sqrt{m})$ を二次体という。二次体 $K = \mathbb{Q}(\sqrt{m})$ の整数環は以下のようになる。

(1) $m \equiv 1 \pmod 4$ のとき

$$O_K = \left\{ a + \frac{1+\sqrt{m}}{2}\, b \;\middle|\; a, b \in \mathbb{Z} \right\}$$

(2) $m \equiv 2, 3 \pmod 4$ のとき

$$O_K = \left\{ a + b\sqrt{m} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

代数的整数と代数共役

i と $-i$ を考えよう。これらは代数的には、いずれも 2 乗して -1 になるという意味をもち、区別できるものではない。$\sqrt{2}$ と $-\sqrt{2}$ も同様である。

このように、一つの有理数係数既約多項式の根たちは、ある意味で同じものとなる。このような数を代数共役であるという。代数共役は単に元の関係を定めるだけでなく、体の自己同型を引き起こす。例えば、複素共役はすべての複素数に対して定義される。

$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ を有理数係数の既約多項式とし、その根を $\alpha_1, \cdots, \alpha_n$ とする。このとき $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ と表され、

$$\sum_{i=1}^{n} \alpha_i = -a_{n-1}, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n a_0$$

となるから、代数共役の和 (トレース) と積 (ノルム) は有理数となる。特に α_i が代数的整数ならば、和と積は有理整数である。

代数的整数と代数共役

A を有理整数を成分とする正方行列としよう。A の固有多項式 $|xE - A|$ は最高次係数 1 の有理整数係数の多項式となるから、その根、すなわち A の固有値は代数的整数である。

アソシエーション・スキームの話に戻ろう。隣接行列 σ_s は整数成分の行列なので、その固有値は代数的整数である。指標の値は表現行列のトレースで、トレースは固有値の和になるので、やはり代数的整数である。

T を指標 χ を与えるアソシエーション・スキーム (X, S) の表現とする。代数共役 τ に対して $T^\tau(\sigma_s) = T(\sigma_s)^\tau$ で T^τ を定めれば、T^τ も表現となり、その指標は $\chi^\tau(\sigma_s) = \chi(\sigma_s)^\tau$ となる。このようなものを代数共役な表現、指標などという。

モジュラー表現からの結果

さて、$|X| = p$ が素数であるときを考えよう。証明には一部、モジュラー表現からの結果を用いるので、それを説明する。モジュラー表現とは正標数の体上での表現である。

利用したいのは次の結果である。

定理 8.1 (花木, 2002)

(X, S) をアソシエーション・スキームとし $|X| = p$ を素数 *(*素数べき*)* とする。F を標数 p の体とすると、隣接代数 FS は局所環である。

これを説明するには、また準備が必要になるので、この定理から分かることで必要なことだけを考えよう。

系 8.2

(X, S) をアソシエーション・スキームとし $|X| = p$ を素数とする。$f(x)$ を σ_s の固有多項式とすると $f(x) \equiv (x - n_s)^p \pmod{p}$ となる。

モジュラー表現からの結果

$|X| = p$ を素数とし、F を標数 p の十分大きな (σ_s の固有値をすべて含む) 有限体とする。σ_s を F 上の行列と見て、その固有値が n_s のみであることを示せばよい。自明な表現は任意の体上で考えられるので n_s は σ_s の固有値である。

F に対して、ある代数体 K とその整数環 O_K の素イデアル $\mathfrak{P}$ が存在して $F \cong O_K/\mathfrak{P}$ となる。

> 理解しにくければ、正確ではないが $K = \mathbb{Q}$, $O_K = \mathbb{Z}$, $\mathfrak{P} = p\mathbb{Z}$, $F = Z/p\mathbb{Z}$ と思っていてもよい。

自然な全射 $O_K \to F$ がある。隣接代数についても、全射 $O_K S \to FS$ がある。

モジュラー表現からの結果

$\alpha_1 = n_s, \alpha_2, \cdots, \alpha_\ell$ を σ_s の F 上での異なる固有値とし $\ell > 1$ とする。固有多項式 $f(x)$ も F 係数の多項式と見よう。ある m_i があって

$$f(x) = \prod_{i=1}^{\ell} (x - \alpha_i)^{m_i}$$

と表せる。$g_i(x) = f(x)/(x - \alpha_i)^{m_i}$ $(i = 1, \cdots, \ell)$ とおく。$g_1(x), \cdots, g_\ell(x)$ は共通の因子をもたないので、

$$1 = \sum_{i=1}^{\ell} g_i(x) h_i(x)$$

となる多項式 $h_i(x)$ が存在する。

モジュラー表現からの結果

この式に σ_s を代入すれば

$$I = \sum_{i=1}^{\ell} g_i(\sigma_s)h_i(\sigma_s)$$

である。ここで $E_i = g_i(\sigma_s)h_i(\sigma_s)$ とおく。このとき $E_i \neq O$ で

$$I = \sum_{i=1}^{\ell} E_i, \quad E_iE_j = \delta_{ij}E_i$$

となる。

> $i \neq j$ のとき $g_i(x)h_i(x)g_j(x)h_j(x)$ は $f(x)$ で割り切れ、ケーリー-ハミルトンの定理から $f(\sigma_s) = O$ だから $E_iE_j = O$ である。$i = j$ のとき $E_i = E_iI = \sum_{j=1}^{\ell} E_iE_j = E_i^2$ である。

また E_i は σ_s の多項式で書けているので、隣接代数 FS の元である。

モジュラー表現からの結果

$I = \sum_{i=1}^{\ell} E_i$, $E_i E_j = \delta_{ij} E_i$ という関係から、E_i は $0, 1$ のみを成分にもつ対角行列に相似変形できる。$\ell > 1$ の仮定から E_i のトレースは F で 0 ではない。

一方で、全射 $O_K S \to FS$ で E_i に移る元 $\widetilde{E_i}$ を考えれば、対角成分がすべて等しいことと、行列のサイズが p であることから、そのトレースは F において 0 になる。これは矛盾であり、固有値は n_s のみであることが分かる。

定理の証明

目標とする定理をもう一度書いておこう。

定理 9.1 (花木-宇野, 2006)

(X, S) をアソシエーション・スキームとする。$|X|$ が素数であれば (X, S) は可換である。

これを示すために、次の命題を示す。

定理 9.2

(X, S) をアソシエーション・スキームとする。ある正の整数 m があって、任意の $1_S \neq \chi \in \mathrm{Irr}(S)$ に対して $m_\chi = m$ であるならば (X, S) は可換である。

Proof.

まず、$1 \neq s \in S$ に対して、標準指標を考えれば
$0 = \gamma_S(\sigma_s) = n_s + \sum_{\chi \neq 1_S} m\chi(\sigma_s)$ である。よって

$$-\frac{n_s}{m} = \sum_{\chi \neq 1_S} \chi(\sigma_s)$$

であるが、これは有理数かつ代数的整数なので、有理整数である。すなわち n_s は m で割り切れる。よって

$$\begin{aligned} |X| &= \sum_{s \in S} n_s = 1 + m \sum_{s \neq 1} \frac{n_s}{m} \geq 1 + m(|S| - 1) \\ &= 1 + m \sum_{\chi \neq 1_S} \chi(1)^2 \geq 1 + m \sum_{\chi \neq 1_S} \chi(1) = \gamma_S(\sigma_1) = |X| \end{aligned}$$

となり、すべての $\chi \in \mathrm{Irr}(S)$ に対して $\chi(1) = 1$ であることが分かる。 □

定理の証明

自明でない指標のすべての重複度が等しいことを示せばよいことになったが、そのために次の定理を示す。

定理 9.3 (花木-宇野, 2006)

(X, S) をアソシエーション・スキームとする。$|X|$ が素数であれば、自明でないすべての指標は代数共役である。

この定理を証明する。

$1_S \neq \chi \in \mathrm{Irr}(S)$ とする。χ の代数共役すべての和を Φ とする。χ と代数共役でない既約指標が存在するものとして矛盾を導く。Ψ を $\mathrm{Irr}(S)$ から 1_S と χ の代数共役を除いたものすべての和とする。Φ, Ψ は代数共役で閉じているので、その値は有理整数となる。

定理の証明

σ_s の固有値は標数 p では n_s のみなので、標数 0 では n_s との差が素イデアルに入る。しかし Φ で見ると、その値は有理整数なので、p の倍数となる。したがって、ある $u_s \in \mathbb{Z}$ があって $\Phi(\sigma_s) = \Phi(1)n_s - u_s p$ となる。同様に、ある $v_s \in \mathbb{Z}$ があって $\Psi(\sigma_s) = \Psi(1)n_s - v_s p$ となる。

1_S と Φ に直交関係を用いると

$$\begin{aligned} 0 &= \sum_{s\in S} \frac{1}{n_s} 1_S(\sigma_{s^*})\Phi(\sigma_s) = \sum_{s\in S} \Phi(\sigma_s) \\ &= \sum_{s\in S} (\Phi(1)n_s - u_s p) = p\left(\Phi(1) - \sum_{s\in S} u_s\right) \end{aligned}$$

となる。すなわち $\Phi(1) = \sum_{s\in S} u_s$ である。同様に $\Psi(1) = \sum_{s\in S} v_s$ も得られる。

定理の証明

Φ と Ψ にもう一度直交関係を適用して

$$\begin{aligned}
0 &= \sum_{s\in S}\frac{1}{n_s}\Phi(\sigma_{s^*})\Psi(\sigma_s) = \sum_{s\in S}\frac{1}{n_s}(\Phi(1)n_{s^*} - u_{s^*}p)(\Psi(1)n_s - v_sp) \\
&= \sum_{s\in S}\Phi(1)\Psi(1)n_s - \sum_{s\in S}\Phi(1)v_sp - \sum_{s\in S}\Psi(1)u_{s^*}p + \sum_{s\in S}\frac{1}{n_s}u_{s^*}v_sp^2 \\
&= p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) + \sum_{s\in S}\frac{1}{n_s}u_{s^*}v_sp^2 \\
&= -p\Phi(1)\Psi(1) + \sum_{s\in S}\frac{1}{n_s}u_{s^*}v_sp^2
\end{aligned}$$

となる。

定理の証明

したがって

$$\Phi(1)\Psi(1) = \sum_{s \in S} \frac{1}{n_s} u_{s^*} v_s p$$

となる。ここで $1 \leq \Phi(1) < p$, $1 \leq \Psi(1) < p$, $1 \leq n_s < p$ より、左辺は p で割り切れないが、右辺は p で割り切れ、これは矛盾である。

以上で、素数位数アソシエーション・スキームが可換であることが分かった。

最後に

素数位数アソシエーション・スキームが可換になることは分かったが、その分類が完成しているわけではない。構造定数 p_{st}^{u} の可能性も分からない。(自明なものしか知られていない。) 完全な分類は現状では無理であるように思われるが、構造定数の可能性、特に非自明なものがあるのかどうかを解決したい。(考えてはいるが、有効な手段は見つかっていない。)