Splitting Fields of Association Schemes

大阪教育大学
宗政昭弘

定義 d-class association scheme $(X, \{R_i\}_{i=0}^d)$ とは、有限集合 X と $X \times X$ の分割 $\{R_i\}_{i=0}^d$ で、

(i) $R_0 = \{(x,x) \mid x \in X\}$

(ii) $\forall i, \exists i'$ s.t. $\{(x,y) \mid (y,x) \in R_i\} = R_{i'}$

(iii) $\forall i, j, k \quad \forall (x,y) \in R_k,$

$p_{ij}^k = \#\{z \in X \mid (x,z) \in R_i, (z,y) \in R_j\}$ は (x,y) によらず一定

(iv) $p_{ij}^k = p_{ji}^k \quad \forall i, j, k.$

adjacency matrix A_i を次のように定義する

$$(A_i)_{xy} = \begin{cases} 1 & (x,y) \in R_i \\ 0 & (x,y) \notin R_i \end{cases}$$

$\mathfrak{A}$ を $A_0, A_1, \cdots, A_d$ で $\mathbb{C}$ 上生成される線形空間と

すると、$\mathfrak{A}$は可換な$\mathbb{C}$代数になる。$\mathfrak{A}$を adjacency algebra と呼ぶ。$\mathfrak{A}$は$M_n(\mathbb{C})$ $(n=|X|)$ の subalgebra と考えると自然に$\mathbb{C}^n$に作用する。$\mathfrak{A}$の極大共通固有空間は丁度 $d+1$ 個あることがわかり、そのうちのひとつは$(1,1,\cdots,1)$で生成される1次元空間である：$\mathbb{C}^n=V_0\oplus V_1\oplus\cdots\oplus V_d$, $V_0=(1,1,\cdots,1)$. $\mathbb{C}^n$からV_iへの射影をE_iとおく。特に$E_0=\frac{1}{n}J$, Jは all 1 matrix である。すると

$$A_j=\sum_{i=0}^{d}P_j(i)E_i \tag{1}$$

と書ける。ただし$P_j(i)$はA_jのV_i上での固有値である。$P=(P_j(i))$を character table と呼び$K=\mathbb{Q}(P_j(i),\ 0\leq i,j\leq d)\subset\mathbb{C}$ を splitting field と呼ぶ。

問題　Kは円分体に含まれるか。

つまり、association scheme の character table が 1 の巾根で書けるかということだが、この問題は未解決である。association scheme の代表的な例として、有限群の等質空間があるが、この場合には、その置換表現に現れる指標の値を使って$P_j(i)$を表せるので、確かに円分体に含まれている。

さて、(1)式は $\{E_i\}_{i=0}^d$ について解くことができて、

$$\mathfrak{A}=\langle A_0, A_1, \cdots, A_d\rangle=\langle E_0, E_1, \cdots, E_d\rangle$$

となる。従って、$\mathfrak{A}$は行列の乗法だけでなく、行列の成分ごとの乗法（Hadamard積）についても閉じていることがわかる。

$$E_i \circ E_j=\frac{1}{n}\sum_{k=0}^{d} q_{ij}^{k} E_k$$

と書いたとき（$\circ$ は Hadamard積）q_{ij}^k をKrein parameterと呼ぶ。$L=\mathbb{Q}(q_{ij}^k,\ 0\le i,j,k\le d)$ とおくと $L\subset K$ である。さらに次のことがわかる。

定理 $\quad Gal(K/L)\subset Z(Gal(K/\mathbb{Q}))$

証明の概略を述べよう。$\sigma\in Gal(K/\mathbb{Q})$ とすると、σは$\mathfrak{A}$の自己同型を引き起こし、primitive idempotents $\{E_i\}_{i=0}^d$ を置換する。$\tau\in Gal(K/L)$ とすると τは Krein parameter を fix するので、Hadamard積に関する primitive idempotents $\{A_j\}_{j=0}^d$ を置換する。これより、

$$\begin{aligned}P_j(i)^{\sigma\tau}&=P_j(i^{\varphi(\sigma)})^{\tau}=P_{j^{\psi(\tau)}}(i^{\varphi(\sigma)})\\&=P_{j^{\psi(\tau)}}(i)^{\sigma}=P_j(i)^{\tau\sigma}\end{aligned}$$

（ただし $\varphi(\sigma)$, $\psi(\tau)$ は $\{0,1,\cdots,d\}$ の置換）となり、$\sigma\tau=\tau\sigma$

が成り立つ。すなわち $\tau \in Z(Gal(K/\mathbb{Q}))$.

系 Krein parameter が有理数ならば、Kは円分体に含まれる。

実際、定理から、$L=\mathbb{Q}$ なら $Gal(K/\mathbb{Q})$ が abelian であることがわかり、Kronecker-Weber の定理により、Kが円分体に入ることがわかる。

$L=\mathbb{Q}$ でない association scheme は、等質空間の場合にもあり得るが、筆者の知る限り、Lは2次体か4次体である。Krein parameter は、character table の成分から計算する公式があるので、character table が与えられれば Krein parameter が有理数かどうか判定できる。定理の証明に使われている議論を応用すると、この判定が容易にできる。この方法を示す例をあげよう。$PGL(3,2)$ は、$X=\{(x,\ell) \mid x$ は射影空間 $PG(2,2)$ の点, ℓ は直線, $x \notin \ell\}$ の上に可移に作用し、Coxeter graph と呼ばれる distance-transitive graph (従って association scheme) ができる。その character table は

$$P=\begin{pmatrix} 1 & 3 & 6 & 12 & 6 \\ 1 & -1+\sqrt{2} & -2\sqrt{2} & -2 & 2+\sqrt{2} \\ 1 & -1-\sqrt{2} & 2\sqrt{2} & -2 & 2-\sqrt{2} \\ 1 & 2 & 1 & -2 & -2 \\ 1 & -1 & -2 & 4 & -2 \end{pmatrix}$$

従って $K=\mathbb{Q}(\sqrt{2})$ である。$\sigma:\sqrt{2}\mapsto-\sqrt{2}\in Gal(K/\mathbb{Q})$ は、Pの行の置換を引き起こす（$\{E_i\}_{i=0}^{d}$の置換）が、列の置換は引き起こさない。つまり Hadamard 積を保存しない、Krein parameter を fix しない、ということがわかる。このようにして、Pの形を見ただけで Krein parameter が有理数かどうかが判定できるのである。

一方、もしKが円分体に含まれないような association scheme があったとすれば、どのような形をしているであろうか。$Gal(K/\mathbb{Q})$は非可換でなければならない。手初めとして、$Gal(K/\mathbb{Q})=S_3$ となる例はあるだろうか。A_j の最小多項式は $\prod_{i=0}^{d}(X-P_j(i))$ で $P_j(0)$は整数だから、3次の既約成分を持つためには $d\geqq3$ でなくてはならない。$d=3$ の時を考えると $\dim V_1=\dim V_2=\dim V_3$

となり P_{ij}^{k} は次の形になる

$$B_1=\begin{pmatrix} 0 & 1 & 0 & 0 \\ a+b+c & a-1 & b & c \\ 0 & b & c & a \\ 0 & c & a & b \end{pmatrix} \quad B_2=\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & b & c & a \\ a+b+c & c & a-1 & b \\ 0 & a & b & c \end{pmatrix}$$

$$B_3=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & c & a & b \\ 0 & a & b & c \\ a+b+c & b & c & a-1 \end{pmatrix}$$

ただし $P_{ij}^{k}=(B_i)_{jk}$, a,b,c は $a^2+b^2+c^2-ab-bc-ca=a$ をみたす整数. character table P は

$$P=\begin{pmatrix} 1 & m & m & m \\ 1 & \theta_1 & \theta_2 & \theta_3 \\ 1 & \theta_2 & \theta_3 & \theta_1 \\ 1 & \theta_3 & \theta_1 & \theta_2 \end{pmatrix}$$

ただし $m=a+b+c$, $\{\theta_1,\theta_2,\theta_3\}$ は 3次方程式 $x^3+x^2-mx+bc-a^2=0$ の3根である。(cf. Brouwer-Cohen-Neumaier, "Distance-regular graphs", Lemma 12.7.4 on P.389)。実は上の3次方程式の判別式は平方であることがわかって、Galois群は S_3 でないことがわかる。

ところで、上にあげた本には、この3次方程式が可約

となる必要十分条件は $b=c$ である、と書かれているが、これは間違いである。実際、

$$a=343t^2+464t+157$$
$$b=343t^2+463t+156$$
$$c=343t^2+445t+144$$

とおくと

$$(x+7t+5)(x+28t+19)(x-35t-23)$$

と因数分解される。$t=-1$ のとき association scheme は実在し、それは $GF(7^3)$ の3乗剰余からつくられる cyclotomic scheme と呼ばれるものである。

一般に $GF(q)$ 上の e-class cyclotomic scheme とは association scheme $(X, \{R_i\}_{i=0}^{e})$ で、$X=GF(q)$, $GF(q)^*=\langle\theta\rangle$, $C_i=\langle\theta^e\rangle\theta_i$ (e乗剰余), $R_i=\{(x,y)\mid x-y\in C_i\}$ $(i=1,2,\cdots,e)$ で定義される。cyclotomic scheme の splitting field が $\mathbb{Q}$ になるのはどのような時かという質問を提示したところ、畔村良雄氏（神戸大）、山本幸一氏（東京女子大）から回答があり、それらを一般化して次の結果が得られた。

定理　$GF(p^r)$ 上の e-class cyclotomic scheme（p は素数，$p^r-1=ef$, $e>1$, $f>1$）の splitting field は $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ の次数 $(p-1)/(p-1,f)$ の中間体である。

特に $GF(7^3)$ 上 3-class のときは $7^3-1=3\cdot 114$ で $(p-1)/(p-1,f)=6/(6,114)=1$ より splitting field は $\mathbb{Q}$ である。一般に cyclotomic scheme の character table は次のように書ける

$$P=\begin{pmatrix} 1 & f & f & & f \\ 1 & \chi(\underline{C_1}) & \chi(\underline{C_2}) & \cdots & \chi(\underline{C_e}) \\ 1 & \chi(\underline{C_e}) & \chi(\underline{C_1}) & \cdots & \chi(\underline{C_{e-1}}) \\ \vdots & \vdots & & & \vdots \\ 1 & \chi(\underline{C_2}) & \chi(\underline{C_3}) & \cdots & \chi(\underline{C_1}) \end{pmatrix}$$

ここで，χ は nontrivial な $GF(q)$ の加法的指標，

$$\chi(\underline{C_i})=\sum_{a\in C_i}\chi(a)$$

で，これは Gauss の周期と呼ばれるものである。