ラテン方陣の代数的構造と数独パズル解の構成

東邦大学理学部情報科学科 足立智子
Tomoko Adachi
Department of Information Science, Toho University

東邦大学大学院理学研究科 桑嶋大地
Daichi Kuwajima
Toho University, graduate student

1. はじめに

正整数 n に対して, $n \times n$ の正方格子に n 種類の文字（シンボル）を入れ, どの縦の列，横の行にもすべてのシンボルがちょうど 1 個ずつ出現するように配置したものを, 位数 n のラテン方陣 (Latin square) と呼ぶ. シンボルの集合全体を A ($|A| = n$) とし, A 上のラテン方陣と呼ぶこともある. $A = \{1, 2, ..., n\}$ とすることが多い.

正整数 n に対して, $n^2 \times n^2$ の正方格子に $1, 2, \cdots, n^2$ の数字を入れ, どの縦の列，横の行にもすべての数字がちょうど 1 回ずつ出現し, $n \times n$ の n^2 個の小正方格子（ブロックと呼ぶ）に $1, 2, \cdots, n^2$ の数字がちょうど 1 回ずつ出現するように配置したものを, 位数 n^2 の数独解 (Sudoku solution) と呼ぶ. 前半の条件は, 位数 n^2 のラテン方陣になることである. 後半の条件を, ブロック条件と呼ぶことにする. $n = 3$ の場合は, 通常の数独パズルの解 (完成形) である.

ラテン方陣に関しては様々な研究がなされており, 文献 [2, 3] に詳しい. 本稿では, ラテン方陣の代数的構造や諸性質を調査し, シンボルの集合 A が有限群や有限体となる場合のラテン方陣の性質を述べる. さらに, これらの性質を用いて, 素数 p に対し, 位数 p^2 の数独解を構成する方法を紹介する.

2. ラテン方陣の代数的構造

基数 n の集合 A において二項演算 $\cdot$ を考える. 本稿では集合 A が空集合でない有限集合の場合のみを扱うので, $card(A) = n$ は正整数となる.

この n を有限集合 A の位数 ($|A| = n$) と呼び, $A = \{1, 2, ..., n\}$ とすることが多い. また, 本稿の後半で A が有限体である場合を扱う際には, 加法単位元 0 と乗法単位元 1 を同時に扱いたいので, $A = \{0, 1, 2, ..., n-1\}$ とする.

二項演算 $\cdot$ が集合 A で閉じているとき, すなわち, 任意の $a, b \in A$ に対して $a \cdot b \in A$ が成り立つとき, $(A, \cdot)$ は全域性 (Totality) を持つという.

任意の $a, b \in A$ に対して連立方程式 $a \cdot x = b, y \cdot a = b$ が一意の解 $x, y \in A$ を持つとき, $(A, \cdot)$ は可除性 (Divisibility) を持つという. 全域性と可除性を持つ $(A, \cdot)$ を準群 (Quasi-group) と呼ぶ.

準群 $(A, \cdot)$ において $a \cdot b = c$ の演算が成り立つとき, a 行 b 列のセルに c を配置した演算表をケイリー表 (Cayley Table) と呼ぶ. ケイリー表は、行を $a \in A$ で表し, 列を $b \in A$ で表し, 演算結果 $a \cdot b = c$ を $|A| \times |A| = n \times n$ の行列に配置している. 全域性と可除性により, ケイリー表の $n \times n$ の演算結果部分 (ケイリー表から行番号 a と列番号 b の縁取りを取り除いた部分) は, どの横の行, 縦の列にもすべての A の要素がちょうど 1 回ずつ出現する. よって, 準群 $(A, \cdot)$ のケイリー表は位数 n のラテン方陣になる. 逆に, 位数 n のラテン方陣 L が与えられると, L をケイリー表の演算結果部分に持つような準群 $(A, \cdot)$ が定まる. この演算結果部分（ラテン方陣）に行番号 a の項目 (縁) と列番号 b の項目 (縁) を追加したものを縁取りラテン方陣 (bordered Latin square) と呼ぶ.

定理 2.1 *([2]),* 準群の各演算表はラテン方陣になる. 逆に, 任意の縁取りラテン方陣は準群の演算表になる.

二項演算 $\cdot$ に関して集合 A が単位元 e を持つとき, すなわち, 任意の $a \in A$ に対して $a \cdot e = e \cdot a = a$ となるようなある $e \in A$ が存在するとき, $(A, \cdot)$ は単位律 (Identity) を持つという. 単位律を満たす準群をループ (Loop) と呼ぶ。単位元 e は 1 と表記することが多い.

二項演算 $\cdot$ に関して集合 A が結合法則 (Associative law) を満たすとき, すなわち, 任意の $a, b, c \in A$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成立するとき, $(A, \cdot)$ は結合律 (Associativity) を持つという. 結合律を持つループを群 (Group) と呼ぶ.

$A = \{1, 2, ..., n\}$ の場合に, ケーリー表の縁取り部分を $1, 2, ..., n$ のように自然に小さい順に並べたときに得られるラテン方陣を, standard form または reduced と呼ぶ.

ラテン方陣 L に対し, 行番号の置換, 列番号の置換, シンボルの置換を施した方陣もまたラテン方陣となり, L と本質的に同じである. これらのラテン方陣は, L と isotopic であると呼ばれる. isotopic なラテン方陣の代表元として, standard form を選ぶことが多い.

3. 有限群上のラテン方陣

A 上のラテン方陣 L が群であるとは, A が群で L がそのケイリー表であることを指す. 群のケイリー表については, 次の定理が知られている. 二つ目の性質は quadrangle criterion と呼ばれる.

定理 3.1 *([2]),* 有限群 G の任意のケイリー表 M は次の二つの性質を持つ. 逆に, この二つの性質を持つ行列 M は群のケイリー表になる.

1. M はラテン方陣である. 言い換えれば, $M = (a_{i,j})$ は, 各行および各列に G の元の置換を並べた正方行列である.
2. *(quadrangle criterion)* 任意の $i, j, k, \ell, i', j', k', \ell'$ に対し, $a_{j,\ell} = a_{j',\ell'}$ を満たすように三本の方程式 $a_{i,k} = a_{i',k'}$, $a_{i,\ell} = a_{i',\ell'}$, $a_{j,k} = a_{j',k'}$ を形成する.

これより, ラテン方陣 M の 2 行 (行番号 a, b)2 列 (列番号 x, y) にまたがる小方陣

$$\begin{bmatrix} a\cdot x & a\cdot y \\ b\cdot x & b\cdot y \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

で, r, s, t, u の内の 3 個の元が定まれば, 残る 1 個は, その小方陣の位置に関わらず, 決まってしまう. quadrangle criterion は, 文献 [6] では, Brant の法則に相当する. 立方体の 8 頂点にある 8 個の符号語とは,

$$(a, x, r), (a, y, s), (b, x, r), (b, y, u), (a', x', r), (a', y', s), (b', x', t), (b', y', u)$$

を指す.

定理 3.2 *([6], Brant* の法則*),* 符号 L が立方体の 8 頂点にある 8 個の符号語のうちの 7 個を含むならば, 残る 1 個も符号 L に含まれる.

群上のラテン方陣は少なく, その個数は次の定理で知られている.

定理 3.3 *([6]),* 位数 n の有限群 G のケイリー表と同値なラテン方陣の *standard form* の個数は, $\frac{(n-1)!}{\varphi}$ で与えられる. ここで, φ は群 G の自己同型群の位数である.

4. 有限体上のラテン方陣と数独解の構成

A 上のラテン方陣 L が体であるとは, A が体で L がそのケイリー表 (加法演算表) であることを指す. 有限体の位数は素数または素数べきであり, 位数 q の有限体を $GF(q)$ と表記する. 素数 p に対し, 位数 p の有限体 $GF(p)$ は, 剰余環 Z_p と同型であり, $GF(p) = Z_p = \{0, 1, 2, \cdots, p-1\}$ と表記することが多い.

素数 p に対し, 位数 p^2 の数独解は, 有限体 $K = GF(p^2)$ を用いて構成することができる.

有限体 $K = GF(p^2)$ は, 基礎体 $F = GF(p)$ の二次拡大である. 基礎体 F 上の二次既約多項式 $f(x)$ を用いて, 拡大体 K を構成する. 原始根 α を F に付加した体 $F(\alpha) = \{c_0 + c_1\alpha | c_0, c_1 \in F\}$ が K である. 拡大体 K は, p 個の coset $F, \alpha + F, 2\alpha + F, \cdots, (p-1)\alpha + F$ に分割できる. このとき, $f(\alpha) = 0$ より, 拡大体 K の任意の非零元 $c_0 + c_1\alpha, (c_0, c_1) \neq (0, 0)$ は, 原始根 α のべき乗 $\alpha^i, (0 \leq i \leq p^2 - 2)$ で表示できる. 乗法群 K^* は, α を生成元とする位数 $p^2 - 1$ の巡回群になる. 拡大体 K から基礎体 F の元を除いた集合を $K - F$ と表記すると, $K - F = \{c_0 + c_1\alpha | c_0, c_1 \in F, c_1 \neq 0\}$ となる.

定理 4.1 *([1]),* 素数 p とし, 基礎体 $F = GF(p)$ の二次拡大体 $K = GF(p^2)$ とする. 拡大体 K の同じ *coset* の相異なる任意の二元 c, d に対し, $K - F$ の元 x を乗じた cx と dx は, 異なる *coset* の元になる.

定理 4.2 *([1]),* 素数 p とし, 基礎体 $F = GF(p)$ の二次拡大体 $K = GF(p^2)$ とする. 拡大体 K の加法に関する演算表を L_0 とする. ここで, この演算表 L_0 において, 行および列の縁取りは, 拡大体 K の *coset* $F, \alpha + F, \cdots, (p-1)\alpha + F$ の順序に並べる. この演算表 L_0 の行の縁取りに, $K - F$ の元 α^i を掛けて, 行の縁取りの順序を並び替える. 列の縁取りの順序は変更しない. この縁取りにおける加法の演算表を L_i とする. このとき, 演算表から縁取りを除いた方陣 L_i は, 位数 p^2 の数独解になる.

ここで, 上の定理で得られた演算表 L_i は数独解になるが, 最初の演算表 L_0 は数独解ではないことに注意しよう.

例えば, $p=3$ の場合に, 基礎体 $F=\{0,1,2\}$, 原始既約多項式 $f(x)=x^2+x+2$ とする. 拡大体 $K=GF(9)$ の元を, coset $F=\{0,1,2\}=\{0,\alpha^0,\alpha^4\}$, $\alpha+F=\{\alpha,\alpha+1,\alpha+2\}=\{\alpha^1,\alpha^7,\alpha^6\}$, $2\alpha+F=\{2\alpha,2\alpha+1,2\alpha+2\}=\{\alpha^5,\alpha^2,\alpha^3\}$ の順に演算表 L_0 の縁取りに配置し, K における加法演算表 L_0 を作る. 下図の L_0 を見てすぐわかるように, ブロック条件を満たさないので, L_0 は数独解ではない.

このとき $\alpha^4=2$ となることに注意すると, $K-F$ の元 α^i であるような i は $i=1,2,3,5,6,7$ となる.

$i=1$ の場合には, 列の縁取り (方陣の上端の縁取り) の順序はそのままで, 行の縁取り (方陣の左端の縁取り) を, $\alpha F=\{0,\alpha,2\alpha^5\}=\{0,\alpha,2\alpha\}$, $\alpha(\alpha+F)=\{\alpha^2,\alpha^8,\alpha^7\}=\{2\alpha+1,1,\alpha+1\}$, $\alpha(2\alpha+F)=\{\alpha^6,\alpha^3,\alpha^4\}=\{\alpha+2,2\alpha+2,2\}$ の順に並び替えて, 加法演算表 L_1 を作成する. 下図の L_1 を見てすぐわかるように, 位数 9 のラテン方陣でありかつブロック条件を満たすので, L_1 は数独解である.

このようにして得られた演算表 $L_i,(i=1,2,3,5,6,7)$ は, 位数 9 の数独解になる. 有限体 $K=GF(9)=\{0,1,2,\alpha,\cdots,2+2\alpha\}$ の元を通常の数独で用いるシンボル $A=\{1,2,\cdots,9\}$ に置き換えると, 通常の数独解 (数独パズルの完成形) になる.

$$
L_0=\left[\begin{array}{ccc|ccc|ccc}
0 & 1 & 2 & \alpha & 1+\alpha & 2+\alpha & 2\alpha & 1+2\alpha & 2+2\alpha \\
1 & 2 & 0 & 1+\alpha & 2+\alpha & \alpha & 1+2\alpha & 2+2\alpha & 2\alpha \\
2 & 0 & 1 & 2+\alpha & \alpha & 1+\alpha & 2+2\alpha & 2\alpha & 1+2\alpha \\
\hline
\alpha & 1+\alpha & 2+\alpha & 2\alpha & 1+2\alpha & 2+2\alpha & 0 & 1 & 2 \\
1+\alpha & 2+\alpha & \alpha & 1+2\alpha & 2+2\alpha & 2\alpha & 1 & 2 & 0 \\
2+\alpha & \alpha & 1+\alpha & 2+2\alpha & 2\alpha & 1+2\alpha & 2 & 0 & 1 \\
\hline
2\alpha & 1+2\alpha & 2+2\alpha & 0 & 1 & 2 & \alpha & 1+\alpha & 2+\alpha \\
1+2\alpha & 2+2\alpha & 2\alpha & 1 & 2 & 0 & 1+\alpha & 2+\alpha & \alpha \\
2+2\alpha & 2\alpha & 1+2\alpha & 2 & 0 & 1 & 2+\alpha & \alpha & 1+\alpha
\end{array}\right],
$$

$$L_1 = \left[\begin{array}{ccc|ccc|ccc} 0 & 1 & 2 & \alpha & 1+\alpha & 2+\alpha & 2\alpha & 1+2\alpha & 2+2\alpha \\ \alpha & 1+\alpha & 2+\alpha & 2\alpha & 1+2\alpha & 2+2\alpha & 0 & 1 & 2 \\ 2\alpha & 1+2\alpha & 2+2\alpha & 0 & 1 & 2 & \alpha & 1+\alpha & 2+\alpha \\ \hline 1+2\alpha & 2+2\alpha & 2\alpha & 1 & 2 & 0 & 1+\alpha & 2+\alpha & \alpha \\ 1 & 2 & 0 & 1+\alpha & 2+\alpha & \alpha & 1+2\alpha & 2+2\alpha & 2\alpha \\ 1+\alpha & 2+\alpha & \alpha & 1+2\alpha & 2+2\alpha & 2\alpha & 1 & 2 & 0 \\ \hline 2+\alpha & \alpha & 1+\alpha & 2+2\alpha & 2\alpha & 1+2\alpha & 2 & 0 & 1 \\ 2+2\alpha & 2\alpha & 1+2\alpha & 2 & 0 & 1 & 2+\alpha & \alpha & 1+\alpha \\ 2 & 0 & 1 & 2+\alpha & \alpha & 1+\alpha & 2+2\alpha & 2\alpha & 1+2\alpha \end{array}\right],$$

5. おわりに

本稿では, 素数 p に対し, 基礎体 $F = GF(p)$ の二次拡大体 $K = GF(p^2)$ 上のラテン方陣を用いて. 位数 p^2 の数独解を構成する方法を紹介した. 同様の手法で, 素数または素数べきの正整数 q に対して, 位数 q の有限体 $F = GF(q)$ を基礎体とする二次拡大体 $K = GF(q^2)$ 上のラテン方陣を考えることにより. 位数 q^2 の数独解を構成することができる.

他にも, 直交する数独解の構成法については, [4, 5] がある.

参考文献

[1] D. Keedwell (2010); Constructions of complete sets of orthogonal diagonal Sudoku squares, *Australasian Journal of Combinatorics*, Vol. 47, pp. 227–238.

[2] D. Keedwell and J. Dénes (2015); *Latin Squares and their applications, (second edition)*, North-Holland publications.

[3] C. F. Laywine and G. L. Mullen (1998); *Discrete Mathematics Using Latin Squares*, John Weiley & Sons, INC.

[4] J. Lorch (2009); Mutually orthogonal families of linear sudoku solutions, *Journal of the Australian Mathematical Society*, Vol. 87, pp. 409–420.

[5] J. Lorch (2010); Orthogonal combings of linear sudoku solutions, *Australasian Journal of Combinatorics*, Vol. 47, pp. 247–264.

[6] 山本幸一 (1989); 新数学講座 *14*　組合せ数学 *[*絶版*]* , 朝倉書店.