令和元年度卒業研究概要

有限体の元を並べてできるある長方形の考察

中等教育教員養成課程　数学専攻　河野 直道

本論文の目標は, 有限体 $\mathbb{F}_p$ の元を並べてできる長方形について考察することである. 有限体の元を長方形の形に並べることができることを保障しているのが, 次に述べる定理である.

定理 1. p を素数とする. $^\forall\overline{a} \in \mathbb{F}_p^\times$ に対して, $\overline{a}$ の位数は $p-1$ の約数である.

$\mathbb{F}_p^\times$ の元 $\overline{a}$ をとり, $\overline{a}$ の位数 n に対し, $\overline{1}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{n-1}$ と n 個の元を並べる. 次に, ここに表れなかった元 $\overline{b_2}$ をとり, $\overline{b_2}, \overline{b_2}\overline{a}, \overline{b_2}\overline{a}^2, \ldots, \overline{b_2}\overline{a}^{n-1}$ を並べる. さらに, 今までに表れなかった元 $\overline{b_3}$ をとり, $\overline{b_3}, \overline{b_3}\overline{a}, \overline{b_3}\overline{a}^2, \ldots, \overline{b_3}\overline{a}^{n-1}$ を並べる. 以下, これを繰り返すと, $\mathbb{F}_p^\times$ の元全体を次のような長方形の形に並べることができる.

$\overline{1}$	$\overline{a}$	$\overline{a}^2$	$\cdots$	$\overline{a}^{n-1}$
$\overline{b_2}$	$\overline{b_2}\overline{a}$	$\overline{b_2}\overline{a}^2$	$\cdots$	$\overline{b_2}\overline{a}^{n-1}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\overline{b_m}$	$\overline{b_m}\overline{a}$	$\overline{b_m}\overline{a}^2$	$\cdots$	$\overline{b_m}\overline{a}^{n-1}$

この長方形について, 特に各行に現れる元の集合に着目して考察を行った結果, 次の定理を得た.

定理 5. $^\forall n \in \mathbb{N}$, $n \mid p-1$ に対して, 位数が n となる $\mathbb{F}_p^\times$ の元が必ず存在する.

定理 6. 定理 5 を満たす $\mathbb{F}_p^\times$ の元の個数は n と互いに素な n 以下の整数の個数に等しい.

これらの定理の証明には, 原始根の概念を必要とした.

また, 数値計算を行った結果, 次の予想が得られた.

予想 1. $g_1, g_2, \ldots, g_r$ を p の原始根すべてとする. 任意の整数 a に対し,

$$\overline{a} = \overline{g_1}^{m_1} = \overline{g_2}^{m_2} = \cdots = \overline{g_r}^{m_r}$$

のとき, $d = (m_1, m_2, \ldots, m_r, p-1)$ とすると, 長方形は d 行となる.

今回の研究で叶わなかった予想 1 の証明は今後の課題とする.