For Tutors

MeBio　数学テキスト

東進数学コンクール６月

—問題と解答—

Edited by kamei

第 1 章

問題

§ 1　問題

東京出版発行の「大学への数学」の裏表紙内側に，毎月「東進数学コンクール」が掲載されています．高校生向けの超難問ですが，数学的にも深い意味を持つものばかりで，出題者の能力に感心するばかりです．2016 年 6 月号の問題は次の通りでした．解いてみるとこれまた奥の深い問題であることがわかってきました．そこで私の追加問題を加えて紹介します．

東進の問題 1–1–1

S を有限個の元からなる集合とする．S の二つの元からなる組に対して定義され，S に値を取る関数 f が

$$f(f(f(a,\ b),\ f(c,\ b)),\ f(c,\ a)) = b \cdots (\mathrm{A})$$

を満たすとする．このとき , S の任意の元 $a,\ b$ に対し $f(a,\ b) = f(b,\ a)$ が成り立つことを示せ.

亀井の追加問題 1–1–2

この問題の場合 S の要素数は 3^m $(m = 0,\ 1,\ 2,\ \cdots)$ に限られることを示せ，また $|S| = 3^m$ のときこの関数は実際に実現可能で，その構造は同型を除いて一通りに決まることを示せ.

$\boxed{\text{未解決}}$

第 2 章

解答

§ 1　東進の問題の解答

$\#(S) = n$ とする．$S = \{s_1,\ s_2,\ \cdots,\ s_n\}$ とおく．

命題 2–1–1　$f : S \times S \to S$ は全射である．
証明　任意の $z \in S$ に対し $f(x,\ y) = z$ となる $x,\ y$ の存在をいえばよいが，

$$f(f(f(a,\ z),\ f(c,\ z)),\ f(c,\ a)) = z$$

が成り立つので $x = f(f(a,\ z),\ f(c,\ z)),\ y = f(c,\ a)$ としてやればよい．□

命題 2–1–2　任意の $y \in S$ に対し S から S への写像 $x \mapsto f(x,\ y)$ は全射である．
証明　任意の $y,\ z \in S$ に対し $f(x,\ y) = z$ となる x の存在をいえばよい．命題 1–2–1 より f は全射なので，$f(c,\ a) = y$ となる $a,\ c$ が存在する．そのとき

$$f(f(f(a,\ z),\ f(c,\ z)),\ f(c,\ a)) = z \Longrightarrow f(f(f(a,\ z),\ f(c,\ z)),\ y) = z$$

が成り立つので $x = f(f(a,\ z),\ f(c,\ z))$ としてやればよい．□

系 2–1–3　任意の $y \in S$ に対し S から S への写像 $x \mapsto f(x,\ y)$ は全単射である．
これより $f(x,\ y) = f(x',\ y) \iff x = x'$ が従う．
証明　S が有限集合なので全射なら全単射である．□

命題 2–1–4　任意の $y \in S$ に対し S から S への写像 $x \mapsto f(y,\ x)$ は全射である．
証明　任意の $y,\ z \in S$ に対し $f(y,\ x) = z$ となる x の存在をいえばよい．まず (A) 式で $c = a$ とおくと

$$f(f(f(a,\ b),\ f(a,\ b)),\ f(a,\ a)) = b$$

この式で a を固定し b を s_1〜s_n まで動かすと，右辺は n 通りの値を取る，従って左辺の $f(a,\ b)$ も n 通りの値を取らないといけない．これは題意を表している．□
（実はこの式からは $f(s_1, s_1)$〜$f(s_n,\ s_n)$ がすべて異なることも導かれるのだが，以下では使わなかった．）

系 2–1–5　任意の $y \in S$ に対し S から S への写像 $x \mapsto f(y,\ x)$ は全単射である．
これより $f(x,\ y) = f(x,\ y') \iff y = y'$ が従う．
証明　S が有限集合なので全射なら全単射である．□

命題 2–1–6　任意の $p \in S$ に対し $f(p,\ p) = p$ である．
証明　まず (A) 式で $a = b = c = p$ としてみよう．

$$f(f(f(p,\ p),\ f(p,\ p)),\ f(p,\ p)) = p$$

$f(p,\ p) = q\ \cdots$ ① と表記すれば，この式は $f(f(q,\ q),\ q) = p$ となる．さらに $f(q,\ q) = r\ \cdots$ ② と表記することにより，この式を $f(r,\ q) = p\ \cdots$ ③ と表しておく．

今度は (A) 式で $a = q,\ b = q,\ c = r$ と置いてみよう．

$$f(f(f(q,\ q),\ f(r,\ q)),\ f(r,\ q)) = q \iff f(f(r,\ p),\ p) = q\ \cdots \text{④}$$

が得られるが，①, ④ の比較により $f(r,\ p) = p\ \cdots$ ⑤ がわかる．すると今度は ③, ⑤ の比較により $p = q$ がわかる．従って $f(p,\ p) = p$ が証明された． □

命題 2–1–7　任意の $x,\ y \in S$ に対し $f(x,\ y) = f(y,\ x)$ である．

証明　まず (A) 式で $a = c = x,\ b = y$ としてみよう．

$$f(f(f(x,\ y),\ f(x,\ y)),\ f(x,\ x)) = y$$

命題 2–1–6 を適用すると $f(f(x,\ y),\ x) = y\ \cdots$ ⑥ がわかる．

今度は (A) 式で $a = x,\ b = x,\ c = f(x,\ y)$ と置いてみよう．⑥を代入することにより

$$f(f(f(x,\ x),\ f(f(x,\ y),\ x)),\ f(f(x,\ y),\ x)) = x \Longrightarrow f(f(x,\ y),\ y) = x\ \cdots \text{⑦}$$

が得られる．$x,\ y$ は任意であったので $x,\ y$ を入れ換えると $f(f(y,\ x),\ x) = y\ \cdots$ ⑧ となる．⑥, ⑧ の比較により $f(x,\ y) = f(y,\ x)$ がわかる． □

§ 2　亀井の追加問題の解答

結論から言おう．この問題の条件を満たす S には $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ 上のベクトル空間の構造が入る．$x,\ y \in S$ に対して写像 f は $f(x,\ y) = -x - y$ で与えられる．

実際 f をこのように定義した場合には

$$\begin{aligned}
& f(f(f(a,\ b),\ f(c,\ b)),\ f(c,\ a)) \\
= \ & f(f(-a-b,\ -c-b),\ -c-a)) \\
= \ & f(-(-a-b)-(-c-b),\ -c-a)) \\
= \ & f(a+c+2b,\ -c-a)) \\
= \ & -(a+c+2b)-(-c-a) \\
= \ & -2b \\
= \ & b
\end{aligned}$$

となっており，(A) 式が成り立っている．そしてこの場合可換性はもちろん成り立っている，

これを示すために使用する前節の関係式をもう一度整理しておこう．前節に既に表れている関係式も，式番号をリセットしてつけ直すことにする．

$$\begin{aligned}
& f(a,\ b) = f(b,\ a) && \cdots \text{①} \\
& f(a,\ b) = c \iff f(b,\ c) = a \iff f(c,\ a) = b && \cdots \text{②} \\
& f(a,\ a) = a && \cdots \text{③} \\
& f(f(a,\ b),\ b) = a && \cdots \text{④} \\
& f(f(a,\ b),\ f(c,\ b)) = f(f(a,\ c),\ b) && \cdots \text{⑤}
\end{aligned}$$

補題 2–2–1

$$f(f(c,\ b),\ d) = f(f(c,\ f(b,\ d)),\ b)\ \cdots \text{⑥}$$

証明　$f(a,\ b)=d$ とおくと $a=f(b,\ d)$ である．これらを ⑤ に代入して

$$\begin{aligned} & f(f(a,\ b),\ f(c,\ b))=f(f(a,\ c),\ b) \\ \Longleftrightarrow\quad & f(d,\ f(c,\ b))=f(f(f(b,\ d),\ c),\ b) \\ \Longleftrightarrow\quad & f(f(c,\ b),\ d)=f(f(c,\ f(b,\ d)),\ b) \end{aligned}$$

□

命題 2–2–2　S の元 0 を固定する．S の元 b に対し写像 $g_b : S \to S$ を，$g_b(a)=f(f(a,\ b),\ 0)$ で定義する．

(1)　g_0 は恒等写像 id である．

(2)　$b \neq 0$ のとき，g_b の固定点は存在しない．

(3)　$g_b \circ g_b = g_{f(b,\ 0)}$ である．

(4)　$g_b \circ g_b \circ g_b = id$ である．

証明

(1)　$g_0(a)=f(f(a,\ 0),\ 0)=a$.

(2)　$g_b(a)=f(f(a,\ b),\ 0)=a$ とすると $f(f(a,\ b),\ a)=0$ つまり $b=0$.　これは矛盾．

(3)

$$\begin{aligned} & g_b \circ g_b(a) \\ = \quad & g_b(f(f(a,\ b),\ 0)) \\ = \quad & f(f(f(f(a,\ b),\ 0),\ b),\ 0) \\ = \quad & f(f(a,\ f(b,\ 0)),\ 0) \\ = \quad & f(f(a,\ 0),\ b) \end{aligned}$$

一方 $g_{f(b,\ 0)}(a)=f(f(a,\ f(b,\ 0)),\ 0)=f(f(a,\ 0),\ b)$ だから一致する．

(4)　(3) より $g_b \circ g_b(a)=f(f(a,\ 0),\ b)$ であるから

$$\begin{aligned} & g_b \circ g_b \circ g_b(a) \\ = \quad & g_b(f(f(a,\ 0),\ b)) \\ = \quad & f(f(f(f(a,\ 0),\ b),\ b),\ 0) \\ = \quad & f(f(a,\ 0),\ 0) \\ = \quad & a \end{aligned}$$

□

系 2–2–3　$|S|>1$ であれば $|S|$ は 3 の倍数である．
証明　単位元 0，および 0 と異なる元 b を選ぶ．S の元を g_b による軌道に分解すると，各軌道は要素数 3 となっている．

□

以下では追加問題を帰納的に示していこう．

まず S の要素数が 1 である場合は何の問題も無い．
要素数が 2 以上の場合，ベクトル空間の単位元にあたる元を**勝手に決めて**それを 0 で表す．S は 0 以外の元を含むので，それを a とする．

補題 2–2–4　$f(0,\ a)$ は 0 とも a とも異なる．
証明　$f(0,\ a)=0$ なら $a=f(0,\ 0)=0$ で矛盾，$f(0,\ a)=a$ なら $0=f(a,\ a)=a$ で矛盾．□

補題 2–2–5　$0,\ a,\ f(0,\ a)$ は f に関して閉じている．
証明　$f(f(0,\ a),\ 0)=a,\ f(a,\ f(0,\ a))=0,\ f(f(0,\ a),\ f(0,\ a))=f(0,\ a)$ だから正しい．□

この結果より $\{0,\ a,\ f(0,\ a)\}$ には $f(a,\ b)=-a-b$ とする $\mathbb{F}_3$ ベクトル空間の構造が入る．その場合 $f(0,\ a)=-a=2a$ である．（$f(0,\ f(0,\ a))=a$ だから $-(-a)=a$ や $-0=0$ も満たされている．）

S の要素数が 3 である場合はこれで構造が決定されている．そこで S の要素数が 4 以上としよう．$\{0,\ a,\ f(0,\ a)\}\subset S$ を a で生成される S の部分集合と呼び $<a>$ で表すことにしよう．$E=<a>$ とし，$b\notin E$ を選ぶ．簡単のため S の要素を自然数で表すことにする．$a=1,\ f(0,\ a)=2,\ b=3$ と表す．S における $f(a,\ b)$ の演算表（の一部）は次のようになっている．

$a \diagdown b$	0	1	2	3
0	0	2	1	
1	2	1	0	
2	1	0	2	
3				3

a を固定したときの $x\mapsto f(a,\ x)$, b を固定したときの $x\mapsto f(x,\ b)$ は全単射なので，$f(0,\ 3),\ f(1,\ 3),\ f(2,\ 3)$ はすべて異なり $0,\ 1,\ 2,\ 3$ とも異なる．そこで $f(0,\ 3)=4,\ f(1,\ 3)=5,\ f(2,\ 3)=6$ と置く．$f(a,\ a)=a$ および $f(a,\ b)=c\iff f(b,\ c)=a\iff f(c,\ a)=b,\ f(f(x,\ 3),\ f(y,\ 3))=f(f(x,\ y),\ 3)$ で値を補うと次のようになる

$a \diagdown b$	0	1	2	3	4	5	6
0	0	2	1	4	3		
1	2	1	0	5		3	
2	1	0	2	6			3
3	4	5	6	3	0	1	2
4	3			0	4	6	5
5		3		1	6	5	4
6			3	2	5	4	6

$f(1,\ 4),\ f(2,\ 4)$ は 0〜6 のどれとも異なるので $f(1,\ 4)=7,\ f(2,\ 4)=8$ とおき，先ほどと同じく空欄を埋める．

$a \diagdown b$	0	1	2	3	4	5	6	7	8
0	0	2	1	4	3				
1	2	1	0	5	7	3		4	
2	1	0	2	6	8		3		4
3	4	5	6	3	0	1	2		
4	3	7	8	0	4	6	5	1	2
5		3		1	6	5	4		
6			3	2	5	4	6		
7		4			1			7	
8			4		2				8

さらに上の表の空欄は

$$
\begin{aligned}
f(0,\ 5) &= f((3,\ 4),\ f(6,\ 4)) = f((3,\ 6),\ 4) = f(2,\ 4) = 8\\
f(0,\ 6) &= f((3,\ 4),\ f(5,\ 4)) = f((3,\ 5),\ 4) = f(1,\ 4) = 7\\
f(1,\ 6) &= f((0,\ 2),\ f(3,\ 2)) = f((0,\ 3),\ 2) = f(4,\ 2) = 8\\
f(2,\ 5) &= f((0,\ 1),\ f(3,\ 1)) = f((0,\ 3),\ 1) = f(4,\ 1) = 7\\
f(3,\ 7) &= f((0,\ 4),\ f(1,\ 4)) = f((0,\ 1),\ 4) = f(2,\ 4) = 8\\
f(3,\ 8) &= f((0,\ 4),\ f(2,\ 4)) = f((0,\ 2),\ 4) = f(1,\ 4) = 7
\end{aligned}
$$

によって補完される.

$a \diagdown b$	0	1	2	3	4	5	6	7	8
0	0	2	1	4	3	8	7	6	5
1	2	1	0	5	7	3	8	4	6
2	1	0	2	6	8	7	3	5	4
3	4	5	6	3	0	1	2	8	7
4	3	7	8	0	4	6	5	1	2
5	8	3	7	1	6	5	4	5	0
6	7	8	3	2	5	4	6	0	1
7	6	4	5	8	1	2	0	7	3
8	5	6	4	7	2	0	1	3	8

定理 2–2–6　上の表は関係式 $f(f(f(a,\ b),\ f(c,\ b)),\ f(c,\ a)) = b \cdots$ (A) と矛盾していない.
証明　容易. □

補題 2–2–7　$-b = f(0,\ b)$ は 0 とも b とも異なる. また $-b \notin E$ である.
証明　容易. □

$E - b = f(E,\ b) = \{f(e,\ b) \mid e \in E\}$, $E + b = f(E,\ -b) = \{f(e,\ -b) \mid e \in E\}$ を考える.

命題 2–2–8

(1)　$|E - b| = |E + b| = |E|$

(2)　$(E - b) \cap E = \phi$, $(E + b) \cap E = \phi$

(3)　$(E - b) \cap (E + b) = \phi$

証明

(1)　$e \mapsto f(e,b)$, $e \mapsto f(e,-b)$ は全単射なので明らか.

(2)　$(E-b) \cap E \neq \phi$ として $f(e_1,\ b) = e_2,\ (e_1,\ e_2 \in E)$ とする．この場合 $b = f(e_1,\ e_2)$ となり E は演算 f に関して閉じているので $f(e_1,\ e_2) \in E$ である．これは矛盾．$(E+b) \cap E = \phi$ も同様.

(3)　$(E-b) \cap (E+b) \neq \phi$ として $f(e_1,\ b) = f(e_2,\ -b),\ (e_1,\ e_2 \in E)$ とする．

$$
\begin{aligned}
& f(e_1,\ b) = f(e_2,\ -b) \\
\iff\ & f(e_1,\ b) = f(e_2,\ f(0,\ b)) \\
\iff\ & f(f(e_1,\ b),\ f(0,\ b)) = e_2 \\
\iff\ & f(f(e_1,\ 0),\ b) = e_2 \\
\iff\ & f(f(e_1,\ 0),\ e_2) = b
\end{aligned}
$$

これは $b \in E$ を意味するので矛盾.

□

補題 2–2–9　$E-b,\ E+b$ は f に関して閉じている.
証明　$e_1,\ e_2 \in E$ とすると $f(f(e_1,\ b),\ f(e_2,\ b)) = f(f(e_1,\ e_2),\ b)$ つまり $f(E-b,\ E-b) \subset E-b$.
$f(E+b,\ E+b) \subset E+b$ も同様. □

補題 2–2–10　$f(E,\ E-b) \subset E+b$.
証明　$e_1,\ e_2 \in E$ とすると $f(e_1,\ f(e_2,\ b)) =$
つまり $f(E,\ E-b) \subset E+b$.　$f(E,\ E+b) \subset E-b$ も同様. □

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
1																											
2																											
3																											
4																											
5																											
6																											
7																											
8																											
9																											
10																											
11																											
12																											
13																											
14																											
15																											
16																											
17																											
18																											
19																											
20																											
21																											
22																											
23																											
24																											
25																											
26																											
27																											