『離散構造』 演習問題 No.4 解答例 (亀山)

この問題では、$\mathcal{N}_n = \{x \in \mathcal{N} \mid 0 \le x < n\}$ とする。(つまり、$\mathcal{N}_n = \{0, 1, 2, \cdots, n-1\}$ である。$n \notin \mathcal{N}_n$ であることに注意せよ。)

問 1 (像、全射、単射、合成、逆関数)

$a \in \mathcal{N}_{13}$ に対して、関数 $f_a : \mathcal{N}_{13} \to \mathcal{N}_{13}$ を，$f_a(x) = (a \cdot x) \mod 13$ と定める．ただし， mod は，自然数上の割算の余りを求める演算とする。たとえば、$7 \mod 3 = 1$ である。

(a) $S = \{1, 3, 5\}$ とし、f_7 による S の像 $f_7(S)$ と、f_8 による $f_7(S)$ の像 $f_8(f_7(S))$ を計算しなさい。

答え: $f_7(S) = \{f_7(1), f_7(3), f_7(5)\} = \{7, 8, 9\}$ である。

$f_8(f_7(S)) = \{f_8(7), f_8(8), f_8(9)\} = \{4, 12, 7\}$ である。

(b) 関数 f_5 が単射になることを示しなさい。

答え: 以下のどちらでもよい。

(その 1): $x = 0, 1, \cdots, 12$ に対して $f_5(x)$ の値は、$0, 5, 10, 2, 7, 12, 4, 9, 1, 6, 11, 3, 8$ となり、異なる x に対して、$f(x)$ の値は異なるので、単射である。

(その 2): $x, y \in \mathcal{N}_{13}$ となる x, y に対して $f_5(x) = f_5(y)$ と仮定する。f_5 の定義から、$(5x - 5y) \mod 13 = 0$ である。5 と 13 は互いに素なので、$(x - y) \mod 13 = 0$ であるが、$0 \le x, y < 13$ なので、$x = y$ である。

(c) 「すべての $a \in \mathcal{N}_{13}$ に対して、関数 f_a は全射である」という命題は成立するか判定しなさい。

答え: 成立しない。$a = 0$ のとき $f_a(\mathcal{N}_{13}) = \{0\} \neq \mathcal{N}_{13}$ であるので、全射でない。(参考: $a \neq 0$ であれば、f_a は全射である。)

(d) 合成関数に関して、任意の $a, b \in \mathcal{N}_{13}$ に対して、$f_a \circ f_b = f_b \circ f_a$ が成立するか判定しなさい。(成立すれば根拠を述べ、成立しないなら反例を示しなさい。)

答え: 成立する。

任意の $x \in \mathcal{N}_{13}$ を取る。

$(f_a \circ f_b)(x) = f_a(f_b(x)) = (a(bx \mod 13)) \mod 13 = abx \mod 13.$

$(f_b \circ f_a)(x) = f_b(f_a(x)) = (b(ax \mod 13)) \mod 13 = abx \mod 13.$

この 2 つから、$(f_a \circ f_b)(x) = (f_b \circ f_a)(x)$ であることが言えたので、$f_a \circ f_b = f_b \circ f_a$ である。

(e) (発展課題) 一般に関数 $f : S \to S$ を n 回合成した関数 f^n は、$f^0 = id_S$ (恒等関数), $f^{n+1} = f \circ f^n$ $(n \ge 0)$ と定義される。

$x \in \mathcal{N}_{13}$ に対して、$f_2^n(x) = 1$ となる $n \in \mathcal{N}_{13}$ が存在するとき、その最小の n を $g(x) = n$ とする。そのような $n \in \mathcal{N}_{13}$ が存在しないとき、$g(x) = 0$ とする。このような $g : \mathcal{N}_{13} \to \mathcal{N}_{13}$ が関数であるかどうか、また、単射であるかどうか調べなさい。

答え: g の値を具体的に計算すればよい。$f_2^n(0) = 0$ なので、$g(0) = 0$ である。$f_2^0(1) = 1$ なので、$g(1) = 0$ である。

初項が 2 で、f_2 を繰返し適用してできる数列 $2, f_2(2), f_2^2(2), \cdots$ は、$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$ なので、$g(2) = 11$ である。また、この数列を見ることにより、$g(3) = 8$, $g(4) = 10$ 等と定まる。

これらより、$g(x)$ の値は、$x = 0, 1, 2, \cdots, 12$ に対して、$0, 0, 11, 8, 10, 3, 7, 1, 9, 4, 2, 5, 6$ である。よって、g は $\mathcal{N}_{13} \to \mathcal{N}_{13}$ という関数であり、単射ではない、全射でもない。

補足: 仮に、g の定義を少し修正して、「最小の n に対して $g(x) = n+1$」と定義していれば、g は全単射となるところであった。

(f) 本問題の f_a は $a = 1$ のとき恒等関数となり、全単射であり、よって、逆関数を持つ。他の $a \in \mathcal{N}_{13}$ の値について、f_a が全単射になるものを 1 つ以上あげて、その場合の逆関数を示しなさい。

答え: 実は、$1 \leq a < 13$ となるすべての a の値に対して、f_a は全単射となるので、($a \neq 0$ であるかぎり) どの値を a としてもよい。$a = 5$ のときは、上記の (b) で値を計算したので、その逆関数をあげると、$x = 0, 1, 2, \cdots, 12$ に対して $f_5^{-1}(x) = 0, 8, 3, 11, 6, 1, 9, 4, 12, 7, 2, 10, 5$ である。

ちなみに、$f_5^{-1} = f_8$ である。これは $f_5 \circ f_8 = f_{40} = f_1 = id$ および $f_8 \circ f_5 = id$ となることからわかる。

補足: $a \neq 0$ であれば、関数 f_a たちにはすべて逆関数が存在して f_b の形となる。つまり、「13 で割った余りの世界」は、$a = 0$ のケースを除いて、「a 倍する」(乗算) 操作の逆演算 (「a で割る」(除算) に相当する演算) が必ず存在する体系となる。(代数系の言葉では「体 (field)」である。)

問 2 (関数や集合の性質)

(a) 2 の倍数 (負の数を含む) の集合と、3 で割ると 1 余る整数 (負の数を含む) の集合の間に、全単射が存在することを示しなさい。

答え：$S = \{x \in \mathcal{Z} \mid \exists y \in \mathcal{Z} \land x = 2y\}$ および $T = \{x \in \mathcal{Z} \mid \exists y \in \mathcal{Z} \land x = 3y+1\}$ とすると、$f : S \to T$ を $f(x) = 3x/2 + 1$ とおくと、f は全単射である。

単射であること: $f(x) = f(y)$ と仮定すると $3x/2 + 1 = 3y/2 + 1$ となり、$x = y$ である。

全射であること: T の任意の要素を z とすると、$z = 3y + 1$ となる $y \in \mathcal{Z}$ が存在する。$2y \in S$ および $f(2y) = z$ であるので、$z \in f(S)$ である。よって f は全射である。

(b) 集合 S, T に対して、$f : S \to T$ となる単射 f があれば、$g : T \to S$ となる全射 g が存在することを示しなさい。

答え: この問題は $S \neq \{\}$ (S は空集合ではない) という条件がなければ不成立であった。この点をお詫びする。以下では、このことを仮定して上記問題を証明する。

$S \neq \{\}$ であるので、S には要素が 1 つ以上あり、このうちのどれかを a とする。(どれでもよい。)

関数 $g : T \to S$ を 以下のように定める。

$$g(y) = \begin{cases} x & \text{もし } f(x) = y \text{ となる } x \text{ が存在したら} \\ a & \text{otherwise} \end{cases}$$

ここで、f は単射であるので、「$f(x) = y$ となる x が存在したら、その x はただ 1 つである」ことが言える。よって、上記の最初のケースで、x は一意的に定まる。2 つ目のケースでももちろん一意的に定まり、よって、g は関数になる。

さらに、g は $T \to S$ の全射である。なぜなら、任意の $x \in S$ に対して、$f(x) = y$ とすると $y \in T$ であり $g(y) = x$ であるので、$x \in g(T)$ であるから。

(c) 集合 S, T の要素数をそれぞれ n, m とする。$f : S \to T$ となる関数の個数、および、$g : S \to T$ となる単射の個数を m と n の式で表しなさい。

答え: $S \to T$ となる関数は、S のそれぞれの要素に対して、m 通りの値の割り当て方があるので、m を n 回かけたもの、つまり、m^n 個ある。

$S \to T$ となる単射は、S の最初の要素に対して、m 通りの値の割り当て方があり、次の要素に対しては $m-1$ 通り、etc. となり、S の最後の要素に対して、$m-n+1$ 通りある。ただし $n > m$ であれば、単射は存在しないので、0 個である。よって、

$n \le m$ のとき、$m(m-1)(m-2)\cdots(m-n+1)$ 個 (これは $m!/(m-n)!$ とも書ける) であり、$n > m$ のとき 0 個である。

(d) (発展課題) S を集合とするとき、$f : 2^S \to S$ となる関数 f が単射にならないことを示しなさい。(ヒント: $T = \{y \in S \mid y = f(x) \wedge f(x) \notin x\}$ と置き、$f(T) \in T$ かどうかを考えなさい。)

答え: f が単射であると仮定する。

$f(T) \in T$ と仮定すると、T の定義から、ある $x \in 2^S$ に対して、$f(T) = f(x) \wedge f(x) \notin x$ となる。f は単射なので、$f(T) = f(x)$ か $T = x$ が導ける。よって、$f(T) \notin T$ となる。これは、最初の仮定である $f(T) \in T$ に矛盾するので、結局、$f(T) \in T$ でないことが言えた。

よって、$f(T) \notin T$ である。そうすると、T の定義から、$f(T) \in T$ である。しかし、これは $f(T) \notin T$ と矛盾する。

結局、f が単射であるというだけの仮定から矛盾が導けたので、f は単射でない。

補足: 「2^S から S への単射が存在しない」ということは、集合 2^S が、集合 S よりも「要素数が多い」ということを意味している。(有限集合のときは、これは自明だが、無限集合のときもこのことが成立する点が重要である。たとえば、「整数の集合のべき集合は、整数の集合よりも要素数が多い」ということが導ける。なお、無限集合については、通常は、「要素数」でなく「濃度 (cardinality)」という言葉を使う。)