

『離散構造』 3章演習問題 (亀山)

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

問 1 (関数の個数) $f^{m,n} : \mathcal{N}_m \rightarrow \mathcal{N}_n$ となる関数 f について考える。ただし $m, n > 0$ とする。

(a) $f^{3,5}$ で単射になるものが何個あるか。

解答: 60 個。単射ということは、 $f(0), f(1), f(2)$ が相異なるということであり、コドメインの要素数は 5 なので、 $5 \times 4 \times 3 = 60$ 個となる。

(b) $f^{5,3}$ で単射になるものが何個あるか。

解答: 0 個。定義域の方が要素数が多いので、単射にはなり得ない。

(c) (難問) 一般に、 $f^{m,n}$ で単射になるものが何個あるか、 m と n の式で表しなさい。

解答: $m > n$ のときは、単射にならないので、0 個である。

$m \leq n$ のときは、 $n \times (n-1) \times \dots \times (n-m+1)$ 個ある。これは、 $n!/(n-m)!$ とも書くことができる。

(ところで、この問題は、「難問」という印をつけるほどでもなかったと思う。)

(d) $f^{3,3} \circ f^{3,3}$ が $\mathcal{N}_3$ の上の恒等写像となる $f^{3,3}$ が何個あるか。

解答: 4 個。

具体的に考えればよい。 $f^{3,3}(0), f^{3,3}(1), f^{3,3}(2)$ の値を (a, b, c) の形で書いて、関数をあらわすことにすると、 $f^{3,3} \circ f^{3,3} = id_{\mathcal{N}_3}$ となるものは、 $(0, 1, 2), (1, 0, 2), (0, 2, 1), (2, 1, 0)$ の 4 個である。

問 2 (関数の性質)

関数 $f_a : \mathcal{N}_{17} \rightarrow \mathcal{N}_{17}$ と $g_b : \mathcal{N}_{17} \rightarrow \mathcal{N}_{17}$ を、 $f_a(x) = (x+a) \bmod 17$ 、 $g_b(x) = b \cdot x \bmod 17$ と定める。ただし、 $\bmod$ は、割算の余りを求める演算で、 $a, b \in \mathcal{N}_{17}$ とする。

(a) $a = 7$ のとき、 f_a は全射か、また、単射か。

解答: f_7 は全射である。なぜなら、任意の $y \in \mathcal{N}_{17}$ に対して、 $f_7(x) = y$ となる $x \in \mathcal{N}_{17}$ が存在するので。(具体的には $y < 7$ のとき $x = y + 10$ とし、 $7 \leq y < 17$ のとき、 $x = y - 7$ とすれば、 $x \in \mathcal{N}_{17}$ かつ、 $f_7(x) = y$ となるので。)

f_7 は単射である。なぜなら、 $f_7(y) = f_7(z)$ と仮定すると、 $(y+7) \bmod 17 = (z+7) \bmod 17$ となり、 y と z は 17 で割った余りが等しい。 $y, z \in \mathcal{N}_{17}$ なので、 $y = z$ である。

(補足) 全射である理由として、「 $f_7(0), f_7(1), \dots, f_7(16)$ の値が 0 以上 17 未満だから」という解答は正しくない。なぜなら、「 $f_7(0), f_7(1), \dots, f_7(16)$ の値が $\mathcal{N}_{17}$ の要素である」というのは、 f_7 が $\mathcal{N}_{17} \rightarrow \mathcal{N}_{17}$ の関数であれば必ず成立することであり、全射であることを意味しないからである。

正しい理由としては、「 $f_7(0), f_7(1), \dots, f_7(16)$ の値を並べると、0 以上 17 未満の**全ての値からなる列**となるから」と言ってほしい。

いいかえれば、

$$\{f_7(0), f_7(1), \dots, f_7(16)\} \subset \mathcal{N}_{17}$$

が成立するのは (f_7 が $\mathcal{N}_{17} \rightarrow \mathcal{N}_{17}$ の関数であれば) 当然であり、

$$\{f_7(0), f_7(1), \dots, f_7(16)\} = \mathcal{N}_{17}$$

が成立するかどうか、 f_7 が全射かどうかの分かれ目である。

- (b) $b = 5$ のとき, g_b は全射か, また, 単射か.

解答: g_5 は全射である。なぜなら、任意の $y \in \mathcal{N}_{17}$ に対して、 $g_5(x) = y$ となる $x \in \mathcal{N}_{17}$ が存在するので。

(この場合、 y から x を計算する式を見つけるのは簡単ではないが、具体的に、 $x = 0, 1, 2, \dots, 16$ に対して、 $g_5(x)$ を計算して、 $g_5(\mathcal{N}_{17}) = \mathcal{N}_{17}$ となることをいえばよい。実際、 $x = 0, 1, 2, \dots, 16$ に対して、 $g_5(x)$ は、 $0, 5, 10, 15, 3, 8, 13, 1, 6, 11, 16, 4, 9, 14, 2, 7, 12$ となり、たしかに、 $g_5(\mathcal{N}_{17}) = \mathcal{N}_{17}$ である。)

g_5 は単射である。なぜなら、全射かどうかの判定で、 $g_5(x)$ の値をすべて計算しているのだから、それをつかって、「 $x \neq y$ ならば $g_5(x) \neq g_5(y)$ 」が成立することがわかるから。

(別解: $g_5(y) = g_5(z)$ と仮定すると、 $(5y) \bmod 17 = (5z) \bmod 17$ となり、 $5(y - z)$ が 17 の倍数である。5 と 17 は互いに素なので、 $y - z$ が 17 の倍数となるが、 $y, z \in \mathcal{N}_{17}$ なので $y = z$ である。)

- (c) 合成関数 $g_5 \circ f_7$ による集合 $\{1, 2, 3\}$ の像を求めよ。

解答: これは、具体的に計算するだけである。(合成の順番を間違えないように。)

$$(g_5 \circ f_7)(1) = g_5(f_7(1)) = 40 \bmod 17 = 6$$

$$(g_5 \circ f_7)(2) = g_5(f_7(2)) = 45 \bmod 17 = 11$$

$$(g_5 \circ f_7)(3) = g_5(f_7(3)) = 50 \bmod 17 = 16$$

であるので、 $(g_5 \circ f_7)(\{1, 2, 3\}) = \{6, 11, 16\}$ である。

- (d) $f_{12} \circ f_5$ が恒等写像となることを示せ。

解答: 任意の $x \in \mathcal{N}_{17}$ に対して、

$$(f_{12} \circ f_5)(x) = f_{12}(f_5(x)) = (((x + 5) \bmod 17) + 12) \bmod 17 = (x + 17) \bmod 17 = x \bmod 17$$

となり、 $x \in \mathcal{N}_{17}$ なので $x \bmod 17 = x$ である。

よって、任意の $x \in \mathcal{N}_{17}$ に対して $(f_{12} \circ f_5)(x) = x$ となり、 $f_{12} \circ f_5 = id_{\mathcal{N}_{17}}$ が言えた。

- (e) $g_7 \circ g_b$ が恒等写像となるときがあるか、ある場合はその b の値をすべて求めよ。

解答: ある。 $b = 5$ のとき。

$b = 0, 1, 2, \dots, 16$ を順番に調べればよく、 $g_7 \circ g_5$ が恒等写像となる。(それ以外では恒等写像になることはない。)

これをチェックすると、任意の $x \in \mathcal{N}_{17}$ に対して、

$$(g_7 \circ g_5)(x) = g_7(g_5(x)) = 7(5x \bmod 17) \bmod 17 = (2 \cdot 17 \cdot x + x) \bmod 17 = x \bmod 17$$

となり、 $x \in \mathcal{N}_{17}$ なので $x \bmod 17 = x$ である。

補足: 上記より g_7 と g_5 は互いに逆関数となっている。実は、「17 で割った余り」の世界では、 $a \neq 0$ に対して、 g_a の逆関数が必ず存在し、それは、ある $b \in \mathcal{N}_{17}$ に対して g_b の形である。 $(g_1$ の逆関数はそれ自身、 g_2 の逆関数は g_9 など)。

問 3 (関数の性質)

授業の中で関数の性質の証明をやる暇がなかったので、まず、例題として、以下のものを証明する。(ウェブにある 3 章の例題も参考にしたい。)

(例題 1) 関数 $f: S \rightarrow T$ と $g: T \rightarrow U$ に対して、 f と g が全射であれば、 $g \circ f$ も全射であることを証明しなさい。

(例題1の解答) 全射であることを証明するためには、「任意の $y \in U$ に対して、ある $x \in S$ があって、 $(g \circ f)(x) = y$ となる」ことを言えばよい。

そこで任意の $y \in U$ を取る。 g は全射であるので、ある $z \in T$ が存在して、 $g(z) = y$ となる。さらに、 f は全射であるので、ある $x \in S$ が存在して、 $f(x) = z$ となる。この x に対して、 $(g \circ f)(x) = g(f(x)) = g(z) = y$ となるので、任意の $y \in U$ に対して、 $(g \circ f)(x) = y$ となる $x \in S$ が存在することが言えた。

(例題2) 関数 $f: S \rightarrow T$ と $g: T \rightarrow S$ および $h: T \rightarrow S$ に対して、 g が f の逆関数で、 h も f の逆関数であれば、 $g = h$ であることを証明しなさい。

(例題2の解答) 逆関数の定義により、 $f \circ h = \text{id}_T$ および $g \circ f = \text{id}_S$ が成立する。これを使って、

$$g = g \circ \text{id}_T = g \circ (f \circ h) = (g \circ f) \circ h = \text{id}_S \circ h = h$$

となり、 $g = h$ が言えた。なお、途中で、合成関数に関する性質 $g \circ (f \circ h) = (g \circ f) \circ h$ を使った。これは、任意の $x \in T$ に対して、

$$(g \circ (f \circ h))(x) = g((f \circ h)(x)) = g(f(h(x))) = (g \circ f)(h(x)) = ((g \circ f) \circ h)(x)$$

となることから言える。

以上を参考に、以下の性質を証明しなさい。

(a) 関数 $f: S \rightarrow T$ と $g: T \rightarrow U$ に対して、 $g \circ f$ が全射であれば、 g が全射であることを証明しなさい。

解答 (の一例):

$g \circ f$ が全射と仮定する。任意の $z \in U$ を取る。 $g \circ f$ が全射なので、ある $x \in S$ に対して、 $(g \circ f)(x) = z$ となる。よって、 $g(f(x)) = z$ である。 $f(x) = y \in T$ とおくと、ある $y \in T$ に対して、 $g(y) = z$ となっている。よって、 g は全射である。

(b) 関数 $f: S \rightarrow T$ と $g: T \rightarrow U$ に対して、 f が逆関数 f^{-1} を持ち、 g が逆関数 g^{-1} を持つとする。このときは、 $g \circ f$ も逆関数 $(g \circ f)^{-1}$ を持つこと、また、 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ であることを証明しなさい。

ヒント: $f^{-1} \circ g^{-1}$ が $g \circ f$ の逆関数であることを証明すればよい。

解答 (の一例): f が逆関数 f^{-1} を持ち、 g が逆関数 g^{-1} を持つと仮定する。このとき、 $f^{-1} \circ g^{-1}$ が $g \circ f$ の逆関数であることを証明すれば、(上記の「例題2」で、逆関数は存在すれば唯一つであることを証明済みなので) $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$ となる。

つまり、以下の2つを証明すればよい。

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \text{id}_S$$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = \text{id}_U$$

(補足: ここで、 $g \circ f: S \rightarrow U$ であるので、1つ目は S 上の恒等関数、2つ目は U 上の恒等関数であることに注意せよ。)

上記の2つは、以下のように証明できる。(証明の中で、合成関数の性質 $h \circ (g \circ f) = (h \circ g) \circ f$ と、恒等関数の性質 $f \circ \text{id} = f$, $\text{id} \circ g = g$ を使う。)

$$\begin{aligned} (f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ (g \circ f)) \\ &= f^{-1} \circ ((g^{-1} \circ g) \circ f) \\ &= f^{-1} \circ (\text{id}_T \circ f) \\ &= f^{-1} \circ f \\ &= \text{id}_S \end{aligned}$$

また、

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ (f^{-1} \circ g^{-1})) \\ &= g \circ ((f \circ f^{-1}) \circ g^{-1}) \\ &= g \circ (id_T \circ g^{-1}) \\ &= g \circ g^{-1} \\ &= id_U\end{aligned}$$

以上で証明できた。

更に補足: 上記の解答は計算の部分だけを証明したが、どんな関数 h と h' に対しても、いつでも、合成関数 $h' \circ h$ が定義されるわけではないので、数学的に厳密にやるならば、 $(f^{-1} \circ g^{-1}) \circ (g \circ f)$ と $(g \circ f) \circ (f^{-1} \circ g^{-1})$ が定義されること (合成関数が作れる条件を満たしていること) を示す必要がある。これは、以下のように簡単に示せる。

$f^{-1} : T \rightarrow S$ と $g^{-1} : U \rightarrow T$ ということから、合成関数 $f^{-1} \circ g^{-1} : U \rightarrow S$ が定義され、これと、 $g \circ f : S \rightarrow U$ ということから、 $(f^{-1} \circ g^{-1}) \circ (g \circ f) : S \rightarrow S$ と $(g \circ f) \circ (f^{-1} \circ g^{-1}) : U \rightarrow U$ が定義される。