『離散構造』 3章演習問題 (亀山)

この問題では、$\mathcal{N}_n = \{x \in \mathcal{N} \mid 0 \le x < n\}$ 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)

$a \in \mathcal{N}_{19}$ に対して、2 つの関数 $f_a : \mathcal{N}_{19} \to \mathcal{N}_{19}$ と $g_a : \mathcal{N}_{19} \to \mathcal{N}_{19}$ を，$f_a(x) = (x+a) \mod 19$、$g_a(x) = (a \cdot x) \mod 19$ 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、g_7 による $f_7(S)$ の像 $g_7(f_7(S))$ を計算しなさい。

解答.

$f_7(S) = \{f(1), f(3), f(5)\} = \{8, 10, 12\}$ である。

$g_7(f_7(S)) = \{g(8), g(10), g(12)\} = \{18, 13, 8\}$ である。

(b) 前問にひき続き、合成関数 $g_7 \circ f_7$ による S の像と、合成関数 $f_7 \circ g_7$ による S の像を計算しなさい。前問と本問で計算した 4 つの像のうち一致するものがあるか？

解答.

$(g_7 \circ f_7)(S) = \{(g_7 \circ f_7)(1), (g_7 \circ f_7)(3), (g_7 \circ f_7)(5)\} = \{g_7(f_7(1)), g_7(f_7(3)), g_7(f_7(5))\} = \{18, 13, 8\}$ である。

$(f_7 \circ g_7)(S) = \{(f_7 \circ g_7)(1), (f_7 \circ g_7)(3), (f_7 \circ g_7)(5)\} = \{f_7(g_7(1)), f_7(g_7(3)), f_7(g_7(5))\} = \{14, 9, 4\}$ である。

よって、$(g_7 \circ f_7)(S) = g_7(f_7(S))$ である。

(c) (難しい) 一般に、集合 $S \subset \mathcal{N}_{19}$ に対して、(1) g による「f による S の像」の像 (f による S の像を T とするとき、$g(T)$ と書けるもの) と、(2) 合成関数 $g \circ f$ による S の像の 2 つは一致するか？

解答. 一致する。つまり $(g \circ f)(S) = g(f(S))$ である。(注。 これは、合成関数の定義そのものではないかと思った人もいるだろうが、厳密にいうと、そうではない。つまり、f の定義域にはいる任意の x に対して、$(g \circ f)(x) = g(f(x))$ は、合成関数の定義そのものであるが、「像」に関して同じ形の式が成立することは、証明を要する。

証明: 両辺とも集合であるので、「左辺⊂右辺」とその逆を証明する。 (ここで、「f による S の像」を T と書くことにする。)

「左辺⊂右辺」について：任意の $x \in (g \circ f)(S)$ を取る。像の定義により、ある $y \in S$ に対して、$x = (g \circ f)(y)$ となる。合成関数の定義より、$x = g(f(y))$ である。ところで、像の定義より $f(y) \in T$ である。よって、$x \in g(T)$ である。(「左辺⊂右辺」の証明終了。)

「右辺⊂左辺」について：任意の $x \in g(T)$ を取る。像の定義により、ある $z \in T$ に対して、$x = g(z)$ となる。ところで、$z \in T = f(S)$ なので、像の定義により、ある $w \in S$ に対して、$z = f(w)$ となる。よって、ある $w \in S$ に対して、$x = g(z) = g(f(w)) = (g \circ f)(w)$ である。よって、$x \in (g \circ f)(S)$ である。(「右辺⊂左辺」の証明終了。)

(d) $a = 7$ のとき，f_a は全射か，また，単射か.

解答. $f_7(0), f_7(1), f_7(2), \cdots, f_7(18)$ をすべて計算すると、$7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 0, 1, 2, 3, 4, 5, 6$ となる。

よって、f_7 は全射かつ単射 (全単射) である。

(e) $a = 7$ のとき，g_a は全射か，また，単射か.

$g_7(0), g_7(1), g_7(2), \cdots, g_7(18)$ をすべて計算すると、$0, 7, 14, 2, 9, 16, 4, 1, 18, 6, 13, 1, 8, 15, 3, 10, 17, 5, 12$ となる。

よって、g_7 は全射かつ単射 (全単射) である。

(f) f_3 は全単射である。同様に、f_a が全単射になる $a \in \mathcal{N}_{19}$ を全て求めなさい。

解答. すべての $a \in \mathcal{N}_{19}$ に対して f_a は全単射になる。

[理由の一例 (いろいろな理由があり得る)]

f_a は、有限集合から同じ要素数の有限集合への関数であるので、単射であれば全射である。(単射であるのに全射でないとすると、コドメインが定義域より大きな集合となる。) よって、f_a が単射であることを示せばよい。

そこで、任意の $x, y \in \mathcal{N}_{19}$ を取る。そして、$f_a(x) = f_a(y)$ と仮定しよう。(目標は $x = y$ を示すことである。) $f_a(x) = (a + x) \mod 19 = f_a(y) = (a + y) \mod 19$ である。よって、$(x - y) \mod 19 = 0$ である。$x, y \in \mathcal{N}_{19}$ なので、差が 19 で割り切れる 2 つの数は等しいものしかない。よって $x = y$ である。

(g) g_3 を n 回合成した関数を h_n とする。つまり、$h_0(x) = x$, $h_1(x) = g_3(x)$, $h_2(x) = g_3(g_3(x))$ 等である。$n \in \mathcal{N}_{19}$ に対して、h_n が恒等関数になる場合があるかこたえなさい。

解答. h_{18} は $\mathcal{N}_{19} \to \mathcal{N}_{19}$ の恒等関数である。

なぜなら、任意の $x \in \mathcal{N}_{19}$ に対して、$h_{18}(x) = g_3(\cdots g_3(g_3(g_3(x)))) = (3(3x \mod 19) \mod 19) \cdots = 3^{18}x \mod 19 = (1 \cdot x) \mod 19 = x$ であるから。

演習後の補足. 指摘があったように、これは問題が若干不備であり、h_0 も (自明に) 恒等関数であった。正しい問題文は、「$a \in \mathcal{N}_{19} - \{0\}$ となる a に対して、h_a が恒等関数となることがあるか」とすべきであった。

補足. これは問題としては成立しているが、計算が大変すぎて、多くの人が困惑したかもしれない。実は、g_3 ではなく g_7 を n 回合成した関数を考えてもらう予定であり、これならば、$7^3 \mod 19 = 1$ なので、3 回だけ合成すれば恒等関数になるところであった。g_3 は、恒等関数になるまでの合成回数が最も多い (皆さんにとっては、最悪の) 選択肢となってしまった。

(h) g_3 の逆関数は存在するが、それを f_a や g_b の形の関数の合成で書くことができるか、答えなさい。

解答. 前問の結果から、g_3 を 18 回合成すると恒等関数になるので、g_3 の逆関数は、「g_3 を 17 回合成した関数」、つまり、h_{17} である。

そして、$3^{17} \mod 19 = 13$ なので、$h_{17} = g_{13}$ である。

(i) (難しい) 各 $a \in \mathcal{N}_{19}$ に対して、g_a の逆関数が存在するか、また、それが、f_a や g_b (および、必要ならば、それらの合成関数) で表すことができるか答えなさい。

解答. 前問の結果から g_a が g_b の逆関数になる組み合わさせがたくさんありそうと推測できる。そこで、そのような (a, b) の組を探そう。$g_b(g_a(1)) = 1$ が必要だから、$ab \mod 19 = 1$ でなければならない。そのような $(a, b) \in \mathcal{N}_{19} \times \mathcal{N}_{19}$ は、$(1, 1)$, $(2, 10)$, $(3, 13)$, $(4, 5)$, $(6, 16)$, $(7, 11)$, $(8, 12)$, $(9, 17)$ $(14, 15)$ $(18, 18)$ がある。実は、これらすべての場合に、g_a と g_b は互いに逆関数となる。一方、$a = 0$ のときは、g_a が単射でないので、明らかに逆関数は存在しない。

よって、$a \in \mathcal{N}_{19} - \{0\}$ となるすべての a に対して g_a の逆関数が存在し、その逆関数を g_b とすると、(a, b) の組は上記のように与えられる。

補足. g_3 の逆関数がある、ということは、この世界 (19 の余りの世界) では、「3 をかける」の逆が存在する、つまり、実質的に「3 で割る」を意味する操作が存在する、ということである。このように、足し算、引き算、かけ算、わり算がすべてそろっていて、それらの間に一定の関係が成立する構造を、代数学では、「体 (たい、field)」と呼び、逆演算が自由自在にできることから、非常に有用である。なお、ここで 19(素数) で割った余りの世界にしたから、「体」になったのであって、たとえば、「6 で割った余りの世界」にしてしまうと、「2 倍する」演算の逆演算がない (2 倍する、という操作が全単射にならない) ので、困ってしまう。この話の発展した先に暗号理論があり、将来、情報セキュリティの授業で勉強してほしい。

問 2 (関数の性質)

(a) 「関数 $f : S \to T$ と $g : T \to U$ に対して，$g \circ f$ が単射であれば、f は単射である」は常に成立するか。常に成立するなら証明し、常には成立しないなら反例を与えよ。

解答。成立する。

[証明 (の一例)] $g \circ f$ が単射であると仮定する。任意の $x, y \in S$ を取り、$f(x) = f(y)$ と仮定する。(目標は $x = y$ を導くことである。)

g を、$f(x) = f(y)$ の両辺に適用して、$g(f(x)) = g(f(y))$ を得る。合成関数の定義より、$(g \circ f)(x) = (g \circ f)(y)$ である。$g \circ f$ は単射なので、$x = y$ である。よって、$x = y$ が言えたので、f は単射である。

(b) 「関数 $f : S \to T$ と $g : T \to U$ に対して，$g \circ f$ が単射であれば、g は単射である」は常に成立するか。常に成立するなら証明し、常には成立しないなら反例を与えよ。

解答。成立しない。

[反例 (の一例)] $f : \mathcal{N} \to \mathcal{N}$ を $f(x) = x + 1$, $g : \mathcal{N} \to \mathcal{N}$ を $g(x) = max(x - 1, 0)$ とする。ここで max は最大値を取る関数で、要するに $g(0) = 0$ で、$x \neq 0$ ならば $g(x) = x - 1$ ということである。

このとき、g は単射でない。($g(0) = g(1) = 0$ なので。) $g \circ f$ は恒等関数なので、単射である。

これは、「すべての f, g に対して、$g \circ f$ が単射であれば、g は単射である」の反例となっている。