

『離散構造』 3 章 (関数)
演習問題の解答 (2009/3/3 訂正)
亀山

問題 1 (関数の定義と単射・全射)

以下に示す対応付けが、 $\mathcal{R}$ から $\mathcal{R}$ への関数、部分関数、単射、全射であるか答えよ。

- (a) $x \mapsto x^3 - x$: 関数である、従って部分関数でもある、単射でない ($0 \mapsto 0$ かつ $1 \mapsto 0$ となる) が、全射である ($x \in \mathcal{R}$ の範囲で、 $x^3 - x$ も $\mathcal{R}$ 全体を渡る)。
- (b) $x \mapsto (x = y^3 \text{ となる } y)$: 関数であり、部分関数でもあり、単射、全射である。
- (c) $x \mapsto \sqrt{x^3}$: (2009/3/3 大越君の指摘により訂正) 以前に「関数であり、部分関数でもあり、単射、全射である。」と書いていたのは誤りです。これは、 $x \geq 0$ の場合でないと、対応する値がないので、関数にはなりません。部分関数です。失礼しました。
- (d) $x \mapsto (x = \tan y \text{ となる } y)$: 関数でも部分関数でもない (x に対応する y が複数ある。たとえば、 $x = 0$ のとき $y = 0, 2\pi$ などが対応する)。

問題 2 (像、合成、全射、単射)

$f(x) = \sin x$, $g(x) = x^3 - 1$, $A = \{x \in \mathcal{R} \mid 0 \leq x \leq \pi\}$ とする。

- (a) $0 \leq x \leq \pi$ の範囲で $0 \leq \sin x \leq 1$ であるので、 $f(A) = \{x \in \mathcal{R} \mid 0 \leq x \leq 1\}$ となる。
 $g'(x) = 3x^2$ となり、 $g'(x) \geq 0$ なので、 g は (広義の) 単調増加である。よって、 $0 \leq x \leq \pi$ の範囲で、 $g(0) \leq g(x) \leq g(\pi)$ となり、 $g(A) = \{x \in \mathcal{R} \mid -1 \leq x \leq \pi^3 - 1\}$ となる。
- (b) 合成関数 $f \circ g$ が定義されるのは、 g のコドメインと f の定義域 (ドメイン) が一致するときであるが、このケースではこれらは両方とも $\mathcal{R}$ なので、一致する。よって、 $f \circ g$ は定義される。また、 $(f \circ g)(x) = f(g(x)) = \sin(x^3 - 1)$ である。

同様に、 $g \circ f$ も定義され、 $(g \circ f)(x) = g(f(x)) = \sin^3 x - 1$ である。

- (c) (問題文では、求める集合の名前が A であったが、これでは上の方で与えられた集合 A とだぶってしまうので、ここでは C と書く。)

$C \subset \mathcal{R}$ のとき、 $f: \mathcal{R} \rightarrow C$ が全射となる C を 1 つ求めよ。

まず f が関数となるためには、 $f(\mathcal{R}) \subset C$ でなければいけない。(そうでなければ、 $f(x) \notin C$ となる $x \in \mathcal{R}$ が存在することになり、 f は $\mathcal{R}$ から C への関数とはならない。)

また、 f が全射となるためには、 $f(\mathcal{R}) \supset C$ でなければいけない。(そうでなければ、 $f(x) = y$ となる x が存在しない $y \in C$ が存在することになり、 f は全射にならない。)

以上より、 $C = f(\mathcal{R})$ となる。つまり、 $C = \{x \in \mathcal{R} \mid 0 \leq x \leq 1\}$ となる。このとき、実際に f は $\mathcal{R}$ から C への関数となり、また、全射となる。

- (d) $B \subset \mathcal{R}$ のとき、 $g: B \rightarrow \mathcal{R}$ が単射となる B を 1 つ求めよ。

これは問題が不備であった。もともと g は ($B = \mathcal{R}$ のときに既に) 単射であったので、 $B \subset \mathcal{R}$ となる、どんな B をとっても g は単射である。

そこで、問題を少し変更して、 $g(x) = x^3 - x$ だったとする。($g: \mathcal{R} \rightarrow \mathcal{R}$ は単射ではないので、問題として意味がある。) この場合、 B としては、たとえば、 $\{x \in \mathcal{R} \mid x \geq \frac{1}{\sqrt{3}}\}$ とすれば、この範囲で g は (狭義の) 単調増加なので、 $g: B \rightarrow \mathcal{R}$ は単射となる。(これ以外にも、いろいろな取りかたがある。たとえば、 $B = \{0\}$ など。)

(e) $f \circ h = h \circ g$ となる関数 $h: \mathcal{R} \rightarrow \mathcal{R}$ を1つ求めよ。

答: $f \circ h = h \circ g$ というのは、関数の等しさの定義により、「すべての実数 x に対して、 $(f \circ h)(x) = (h \circ g)(x)$ となる」ということである。

従って、 $(f \circ h)(x) = f(h(x)) = \sin(h(x))$ と、 $(h \circ g)(x) = h(g(x)) = h(x^3 - 1)$ という式が、すべての実数 x に対して等しい値になる。

これは、三角関数と多項式が絡みあっており、真面目に考えると、却って解けなくなる。

発想を変えて、特殊なケースに帰着させて解いてみよう。 $h(x) = c$ という定数関数 ($c \in \mathcal{R}$ とする) であると仮定してみると、 $(f \circ h)(x) = \sin c$ となり、 $(h \circ g)(x) = c$ となる。よって $\sin c = c$ となる実数 c を見つければよいことになり、 $c = 0$ とすればよい。つまり、 $h(x) = 0$ という関数にすれば、 $f \circ h = h \circ g$ となる。

問題 3 集合 $A = \{x \in \mathcal{N} \mid 0 \leq x \leq 12\}$ と、整数 i に対して、 $g_i: A \rightarrow A$ となる関数と、 $h_i: A \rightarrow A$ となる関数とを、 $g_i(x) = (x+i) \bmod 13$ で定義する。 $h_i(x) = (x \times i) \bmod 13$ で定義する。ただし、 $\bmod$ は整数上の割り算を行い、余りを返す関数とする。

(a) g_3 が関数になっていることを確かめよ。 g_3 は全射か、また、単射か。

答. g_3 の定義域は有限集合なので、 $0, 1, \dots, 12$ に対する g_3 の値を列挙できる。列挙すると、 $3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 0, 1$ となり、確かに、関数となっており、さらに、全単射になっていることがわかる。

(b) h_5 が関数になっていることを確かめよ。 h_5 は全射か、また、単射か。

答. $0, 1, \dots, 12$ に対する h_5 の値を列挙すると、 $0, 5, 10, 2, 7, 12, 4, 9, 1, 6, 11, 3, 8$ となり、関数で、かつ、全単射になっていることがわかる。

(c) $h_i = h_j$ となるのは、 i と j がどのような条件を満たすときか。

答. $h_i = h_j$ となるのは、すべての $x \in A$ に対して、 $h_i(x) = h_j(x)$ ということである。従って、特に $h_i(1) = h_j(1)$ である。すなわち $i \bmod 13 = j \bmod 13$ である。(i と j を 13 で割った余りが一致するとき。)

逆に、 $i \bmod 13 = j \bmod 13$ であるとき、 $h_i = h_j$ となることはすぐわかる。

(d) h_i が h_j の逆関数となるのは、 i と j がどのような条件を満たすときか。

答. h_i が h_j の逆関数となるというのは、任意の $x \in A$ に対して、 $h_i(h_j(x)) = x$ かつ $h_j(h_i(x)) = x$ となるときである。(ちなみに、このとき h_j は h_i の逆関数になっている。)

よって、 $(xij) \bmod 13 = x$ となるので、 $(x(ij-1)) \bmod 13 = 0$ である。これが任意の $x \in A$ に対して成立するためには、 $(ij-1) \bmod 13 = 0$ でなければいけない。すなわち、 ij を 13 で割ると 1 余る場合である。

逆に、「 ij を 13 で割ると 1 余る場合」には、 h_i は h_j の逆関数となっていることは容易にわかる。

よって、「 ij を 13 で割ると 1 余る」ことが、 h_i が h_j の逆関数となる必要十分条件である。

[補足] 問題の答としては、ここまでで OK だが、「 ij を 13 で割ると 1 余る」という条件を、もっとかみくだいてみよう。 $i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ に対して、それぞれ、 $j = 1, 7, 9, 10, 8, 11, 2, 5, 3, 4, 6, 12$ とすれば、 ij が 13 で割って 1 余る。つまり、 $1 \leq i \leq 12$ となる任意の i に対して、 h_i の逆関数は h_j の形をしていることになる。

たとえば、 $(3 \times 9) \bmod 13 = 1$ なので、 h_3 の逆関数は h_9 となる。これは、「3 をかける」演算の逆 (意味的には「3 で割る」演算) が、「9 をかける」という演算で実現できる (分数は必要ない) ことを意味している。0 以外の全ての要素でのかけ算に逆関数が存在すること等から、「13 で割った余りの世界」は、代数学の言葉で「体」(たい, field) であることがわかる。このように、かけ算の逆演算が存在する体は非常に便利であり、暗号理論などで活躍する。

なお、上記の話は、素数である 13 で割った余りの世界だったからうまく行ったのであり、素数でないとうまく行かない (たとえば、6 で割った余りの世界では、 h_2 が全単射でなく、逆関数が存在しない。)

(e) $g_i = h_j$ となることがあるか。

答. ある. $i \bmod 13 = 1$ で $j \bmod 13 = 0$ のとき. (これ以外の場合は $g_i = h_j$ とはならない。)

問題 4 f と g が単射で、合成関数 $g \circ f$ が定義されるとき、 $g \circ f$ も単射であることを証明せよ。

答. $f: A \rightarrow B, g: B \rightarrow C$ とする. $g \circ f$ が単射であるというのは、

$$\forall x \in A. \forall y \in A. (x \neq y \Rightarrow (g \circ f)(x) \neq (g \circ f)(y))$$

ということである. そこでこれを証明する. なお、 f と g が単射であるので、以下の 2 つが成立する。

$$\forall x \in A. \forall y \in A. (x \neq y \Rightarrow f(x) \neq f(y))$$

$$\forall z \in B. \forall w \in B. (z \neq w \Rightarrow g(z) \neq g(w))$$

$x \in A$ かつ $y \in A$ とし、さらに $x \neq y$ と仮定する。

f が単射であるという条件 (上記の 1 つ目の式) と $x \neq y$ ということから、 $f(x) \neq f(y)$ である. なお、当然ながら、 $f(x) \in B$ で $f(y) \in B$ である。

次に、 g が単射であるという条件における z と w を、それぞれ、 $f(x)$ と $f(y)$ とおくと、 $f(x) \neq f(y) \Rightarrow g(f(x)) \neq g(f(y))$ となり、先ほど $f(x) \neq f(y)$ を示したので、 $g(f(x)) \neq g(f(y))$ が導けた。よって、 $(g \circ f)(x) \neq (g \circ f)(y)$ となる。

以上から、 $g \circ f$ が単射であることが証明された。

[補足] 単射であることの定義を以下のようにして証明してもよい。

$$\forall x \in A. \forall y \in A. ((g \circ f)(x) = (g \circ f)(y)) \Rightarrow (x = y)$$

この場合の証明はここには書かないので、各自チャレンジしてほしい。