BCM I : Take-Home Midterm

Due May 26, 2010

Division: **ID#:** **Name:**

1. X を 4 個の元からなる集合、Y を 3 個の元からなる集合とする。そのとき、それぞれの写像がいくつあるかを下の表に書き込め。

	$X \longrightarrow Y$	$Y \longrightarrow X$	$X \longrightarrow X$	$Y \longrightarrow Y$
写像 (mapping)				
単射 (injection)				
全射 (surjectivon)				
全単射 (bijection)				

2. (a) P, Q, R を命題とするとき、$(P \vee Q) \wedge (\sim R) \equiv (P \wedge (\sim R)) \vee (Q \wedge (\sim R))$ が正しければ証明し、正しくなければ、そのことを示せ。

   (b) A, B. C を集合とするとき、$(A \cup B) - C = (A - C) \cup (B - C)$ を 正しければ <u>(a) を用いて</u> 証明し、正しくなければ、<u>(a) との関連性から</u> 反例を示せ。

Division: **ID#:** **Name:**

3. m を正の整数とする。$a, b \in \boldsymbol{Z}$ に対して、$a \equiv b \Leftrightarrow m \mid b-a$ ($\Leftrightarrow \exists c \in \boldsymbol{Z}$ such that $b-a = cm$) とすると、$\equiv$ は、$\boldsymbol{Z}$ 上の同値関係となる。m を明記するため、$a \equiv b \pmod m$ と書くこともある。$a \in \boldsymbol{Z}$ を含む同値類を $[a] = [a]_{\equiv} = \{x \in \boldsymbol{Z} \mid x \equiv a\}$ と書き、この同値類全体を、$\boldsymbol{Z}_m = \{[a] \mid a \in \boldsymbol{Z}\}$ とする。また、$a \in \boldsymbol{Z}$ に対し写像 μ_a を、$\mu_a : \boldsymbol{Z}_m \to \boldsymbol{Z}_m$ ($[x] \mapsto [a \cdot x]$) で定義する。

   (a) $a, b, c, d \in \boldsymbol{Z}$ とするとき、$a \equiv c$ かつ $b \equiv d$ ならば $ab \equiv cd$ であることを示せ。

   (b) $m = 12$ としたとき、$\mu_5 : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{12}$ は全単射であることを示せ。

   (c) $m = 12$ としたとき、$\mu_{10} : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{12}$ は単射ではないことを示せ。

Division: **ID#:** **Name:**

(d) 正の整数 m について $\gcd\{m, a\} = d > 1$ ならば μ_a は全射ではないことを示せ。

(e) 正の整数 m について $\gcd\{m, a\} = 1$ ならば μ_a は全単射となることを示せ。

Division: **ID#:** **Name:**

4. X, Y を集合、$f : X \to Y$、$g : Y \to X$ を写像とする。$A \subset X$、$B \subset Y$ とするとき以下の問いに答えよ。

   (a) 合成写像 $g \circ f$ が全射であるとき、g も全射であることを示せ。

   (b) $A \subset f^{-1}(f(A) \cap B)$ が正しければ証明し、正しくなけれ反例をあげよ。

Message : (a) これまでの数学通論 I (BCM I) について。
(b) 改善点など何でも書いて下さい。

Solutions to Midterm 2010 *May 26, 2010*

1. X を 4 個の元からなる集合、Y を 3 個の元からなる集合とする。そのとき、それぞれの写像がいくつあるかを下の表に書き込め。[1]

	$X \longrightarrow Y$	$Y \longrightarrow X$	$X \longrightarrow X$	$Y \longrightarrow Y$
写像 (mapping)	$3^4 = 81$	$4^3 = 64$	$4^4 = 256$	$3^3 = 27$
単射 (injection)	0	$\binom{4}{3}3! = 24$	$4! = 24$	$3! = 6$
全射 (surjectivon)	$3 \cdot \binom{4}{2} \cdot 2 = 36$	0	24	6
全単射 (bijection)	0	0	24	6

式を書いておいたので、どのように考えるのかも理解して下さい。たとえば、$|X| = 10$, $|Y| = 7$ のときはどうでしょうか。全射の数以外は、この表に対応するものを埋めることができると思います。一応、単射の数だけ説明しておくと、単射の像の取り方が二項係数で書いてあり、その像が決まると、全単射の数と同じなので、階乗が出てきます。さて、$|X| = n$, $|Y| = m$ のときの、X から Y への全射の数を $s(n, m)$ と書くことにしましょう。$n < m$ のときは $s(n, m) = 0$ です。$s(n, n) = n!$ はおそらく良いでしょう。n に関する帰納法とし、$X = I(n+1)$ とします。(一般に、$I(n) = \{1, 2, \ldots, n\}$。) $f(I(n)) = Y$ となる f の数は、$s(n, m)$ でその一つ一つについて、$f(n+1)$ は Y のどの要素でもよいので、$f(I(n)) = Y$ となる、$X = I(n+1)$ から Y への全射の数は、$m \cdot s(n, m)$. さて、$f : X \to Y$ は全射だが、$f(I(n)) \neq Y$ となるときは、$Y \setminus f(I(n)) = \{f(n+1)\}$ ですから、そのようなものは、$m \cdot s(n, m-1)$ となります。最初の m は $Y \setminus f(I(n))$ の取り方をあらわしますが、それが決まれば、$f(n+1)$ は一通りに決まりますから、このようになります。すると、全体では、

$$s(n+1, m) = m \cdot s(n, m) + m \cdot s(n, m-1) = m(s(n, m) + s(n, m-1)),$$

ただし、 $s(n, n) = n!$, $s(n, 1) = 1$。したがって、$s(4, 3) = 3 \cdot (s(3, 3) + s(3, 2)) = 3(3! + 2(s(2, 2) + s(2, 1)) = 3(6 + 2(2 + 1)) = 36.$

コンピュータではどうしたらよいでしょうか。プログラムがしっかり書ければ、おそらく、この程度の数の問題であれば、手でも計算できるでしょう。しかし、数が大きくなると、上のように漸化式をもとめるか、または、何らかのことをしないと求まりません。代数学専門の Magma Calculator というのが web 上にありますが、それでの計算例を別紙としておきました。

http://magma.maths.usyd.edu.au/calc/

Free software では、sage (http://www.sagemath.org/) というのがオススメです。まずは、そのようなソフトを使って計算し、それから一般的な性質を考えることも、重要です。最後は数学ですが。

[1] 以下において $\binom{n}{m} = {}_nC_m$。

2. (a) P, Q, R を命題とするとき、$(P \vee Q) \wedge (\sim R) \equiv (P \wedge (\sim R)) \vee (Q \wedge (\sim R))$ が正しければ証明し、正しくなければ、そのことを示せ。

解. $(P \vee Q) \wedge (\sim R) \equiv (P \wedge (\sim R)) \vee (Q \wedge (\sim R))$ は分配法則によって成立する。

Note. もちろん、真理表を書いて示すのが一番基本的です。

(b) $A, B. C$ を集合とするとき、$(A \cup B) - C = (A - C) \cup (B - C)$ を 正しければ (a) を用いて 証明し、正しくなければ、(a) との関連性から 反例を示せ。

解. 命題 x に関する命題 $P(x), Q(x), R(x)$ をそれぞれ、$x \in A, x \in B, x \in C$ とする。すると、

$$(A \cup B) - C = \{x \mid (P(x) \vee Q(x)) \wedge (\sim R(x))\},$$

$$(A - C) \cup (B - C) = \{x \mid (P(x) \wedge (\sim R(x))) \vee (Q(x) \wedge (\sim R(x))).$$

ここで、(a) より $(P(x) \vee Q(x)) \wedge (\sim R(x))$ が真であることと、$(P(x) \wedge (\sim R(x))) \vee (Q(x) \wedge (\sim R(x))$ が真であることとは、同値であるから、$(A \cup B) - C = (A - C) \cup (B - C)$ は正しい。

3. m を正の整数とする。$a, b \in \boldsymbol{Z}$ に対して、$a \equiv b \Leftrightarrow m \mid b - a$ ($\Leftrightarrow \exists c \in \boldsymbol{Z}$ such that $b - a = cm$) とすると、$\equiv$ は、$\boldsymbol{Z}$ 上の同値関係となる。m を明記するため、$a \equiv b \pmod m$ と書くこともある。$a \in \boldsymbol{Z}$ を含む同値類を $[a] = [a]_\equiv = \{x \in \boldsymbol{Z} \mid x \equiv a\}$ と書き、この同値類全体を、$\boldsymbol{Z}_m = \{[a] \mid a \in \boldsymbol{Z}\}$ とする。また、$a \in \boldsymbol{Z}$ に対し写像 μ_a を、$\mu_a : \boldsymbol{Z}_m \to \boldsymbol{Z}_m$ $([x] \mapsto [a \cdot x])$ で定義する。[2]

(a) $a, b, c, d \in \boldsymbol{Z}$ とするとき、$a \equiv c$ かつ $b \equiv d$ ならば $ab \equiv cd$ であることを示せ。

解. $a \equiv c$ より、$m \mid c - a$ だから $c - a = em$ となる整数 $e \in \boldsymbol{Z}$ が存在する。同様にして、$b \equiv d$ より、$d - b = fm$ となる整数 $f \in \boldsymbol{Z}$ が存在する。従って

$$cd - ab = cd - ad + ad - ab = (c - a)d + a(d - b) = (ed + af)m.$$

これより $m \mid cd - ab$ すなわち、$ab \equiv cd$ を得る。 ■

(b) $m = 12$ としたとき、$\mu_5 : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{12}$ は全単射であることを示せ。

解. 下の対応より明か。

$$\begin{pmatrix} [x] \\ \mu_5([x]) \end{pmatrix} = \begin{pmatrix} [0] & [1] & [2] & [3] & [4] & [5] & [6] & [7] & [8] & [9] & [10] & [11] \\ [0] & [5] & [10] & [3] & [8] & [1] & [6] & [11] & [4] & [9] & [2] & [7] \end{pmatrix}$$

■

(c) $m = 12$ としたとき、$\mu_{10} : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{12}$ は単射ではないことを示せ。

解. 以下のように $\mu_{10}([0]) = \mu_{10}(6)$ だから単射ではない。

$$\begin{pmatrix} [x] \\ \mu_{10}([x]) \end{pmatrix} = \begin{pmatrix} [0] & [1] & [2] & [3] & [4] & [5] & [6] & [7] & [8] & [9] & [10] & [11] \\ [0] & [10] & [8] & [6] & [4] & [2] & [0] & [10] & [8] & [6] & [4] & [2] \end{pmatrix}$$

どの要素も二つの要素の像になっています。 ■

ここでは、すべて書きましたが、特に単射は、$\mu_{10}([0]) = \mu_{10}([6])$ と $[0] \neq [6]$ を示すだけで十分ですね。

[2] μ_a が実際写像となることを示すには、(a) が必要である。すなわち、$[x] = [y] \Rightarrow [ax] = [ay]$ でなければいけない g、$[x] = [y]$ より $x \equiv y$ だから、$ax \equiv ay$ となり、これより $[ax] = [ay]$ を得る。

(d) 正の整数 m について $\gcd\{m,a\} = d > 1$ ならば μ_a は全射ではないことを示せ。

解. 全射とすると、$\mu_a([x]) = [1]$ となる $x \in \boldsymbol{Z}$ が存在する。すると、$ax \equiv 1$ だから $ax - 1 = my$ となる整数 m が存在する。よって、$ax - my = 1$。$d \mid m$ かつ $d \mid a$ だから $ax - my = 1$ より $d \mid 1$ これは、$d > 1$ に矛盾。したがって、全射ではない。

別解. 仮定より、$m = dx,\ a = dy$ となる自然数 x, y が存在する。ここで、$x < m$ である。すると、任意の整数 z について $z = xq+r$ ただし、$0 \le r \le x-1$ とすると、

$$\begin{aligned}\mu_a([z]) &= [az] = [a(xq+r)] = [axq+ar] = [dyxq+ar] = [ar+myq] \\ &= [ar] \in \{[0],[a],[2a],\ldots,[(x-1)a]\}.\end{aligned}$$

これより、$x < m$ 個の値しかとらないので、全射ではない。

Note. $\mu_a([x]) = [ax] = [ydx] = [ym] = [0] = \mu_a([0])$ で、$[x] \neq [0]$ だから、単射でないことを言い、有限集合だから、単射でないなら、全射でないと言ってもよい。上ではより直接的な方法で示した。

(e) 正の整数 m について $\gcd\{m,a\} = 1$ ならば μ_a は全単射となることを示せ。

解. 仮定より $ax + my = 1$ となる整数 $x.y$ が存在する。（例 5.2, 定理 6.3 参照）任意の整数 z について

$$[z] = [(ax+my)z] = [axz+myz] = [axz] = \mu_a([xz])$$

だから全射。$\mu_a([b]) = \mu_a([c])$ とすると、$[ab] = [ac]$ 従って、

$$[b] = [b-myb] = [(1-my)b] = [xab] = [xac] = [(1-my)c] = [c-myc] = [c].$$

よって、単射。

4. X, Y を集合、$f : X \to Y$、$g : Y \to X$ を写像とする。$A \subset X$、$B \subset Y$ とするとき以下の問いに答えよ。

(a) 合成写像 $g \circ f$ が全射であるとき、g も全射であることを示せ。

解. 合成写像 $g \circ f$ は X から X への写像で、全射だから、$a \in X$ に対して $g \circ f(b) = a$ となる $b \in X$ が存在する。ここで $f(b) = c \in Y$ とおくと、$g(c) = g(f(b)) = (g \circ f)(b) = a$。したがって 任意の $a \in X$ に対して、$g(c) = a$ となる $c \in Y$ が存在したから、g は全射である。 ■

(b) $A \subset f^{-1}(f(A) \cap B)$ が正しければ証明し、正しくなけれ反例をあげよ。

解. 正しくない。$X = A = \{1\}$, $Y = \{1,2\}$, $B = \{2\}$ とし、$f(1) = 1$ とすると、$f(A) = \{1\}$ よって、$f(A) \cap B = \emptyset$ だから $f^{-1}(f(A) \cap B) = \emptyset$. $A \neq \emptyset$ だから、$A \not\subset f^{-1}(f(A) \cap B)$. ■

反例は、具体的に、かつ、写像の例をあげるときは、必ず、定義域、終域と、対応方法が必要です。考えるときは絵を描くのも助けとなりますが、絵だけでは反例とはなりません。定義が曖昧となりやすいからです。

正解だった問題についても、解答をしっかり確認しておいてください。

鈴木寛 (hsuzuki@icu.ac.jp)