BCMM I : Midterm Exam

May 15, 2007

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

1. P, Q, R を命題とする。二つの論理式 $(P \vee \sim Q) \Rightarrow (Q \wedge \sim R)$, $Q \wedge (R \Rightarrow \sim P)$ が論理同値であることを以下の二つの方法で証明せよ。

   (a) 真理表を書くことによって。

P	Q	R	$(P \vee \sim Q) \Rightarrow (Q \wedge \sim R)$	$Q \wedge (R \Rightarrow \sim P)$
T	T	T		
T	T	F		
T	F	T		
T	F	F		
F	T	T		
F	T	F		
F	F	T		
F	F	F		

   (b) 式の変形によって。(詳しく途中式を書くこと。)

2. 集合 A, B, C について、Venn 図を使わずに次を証明せよ。ただし、X, Y を集合としたとき、$X - Y = X \cap \overline{Y} = \{x \mid (x \in X) \wedge (x \notin Y)\}$ である。

$$A \cup (B - C) = ((A \cup B) - C) \cup (A \cap C)$$

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

3. R を集合 A に定義された関係とする。任意の $a, b, c \in A$ について関係 R が 次の条件 (a), (b), (c) を満たすとき R は同値関係というのであった。

   (a) aRa, (b) $aRb \Rightarrow bRa$, (c) $(aRb \wedge bRc) \Rightarrow aRc$.

   ここで $a \in A$ に対して、$[a] = \{x \in A \mid xRa\}$ と定義したとき、次が成立することを示せ。一つ一つのステップで、上の (a), (b), (c) のどの性質を使ったか明記せよ。

   $$[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset.$$

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

4. $a, b \in \boldsymbol{Z}$ に対して $2a^2 + 5b^2 \equiv 0 \pmod 7$ のとき aRb と定める。

   (a) R が 整数の集合 $\boldsymbol{Z}$ 全体の上の同値関係であることを示せ。

   (b) 相異なる同値類はいくつあるか。同値類を決定せよ。

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

5. f を集合 A から集合 B への写像（関数）、g を集合 B から集合 C への写像とする。この時、$h = g \circ f : A \to C$ $(a \mapsto g(f(a)))$ によって 集合 A から C への写像 $h = g \circ f$ を定義する。以下を証明または反証せよ。

   (a) g が全射であるとき $h = g \circ f$ も全射である。

   (b) f は単射ではないが $h = g \circ f$ は単射であるような例が存在する。

Message : (a) これまでの数学通論 I (BCMM I) について。
(b) 改善点など何でも書いて下さい。[裏にもどうぞ。掲載不可の場合は明記のこと。]

Solutions to Midterm 2007 *May 15, 2007*

1. P, Q, R を命題とする。二つの論理式 $(P \vee \sim Q) \Rightarrow (Q \wedge \sim R)$, $Q \wedge (R \Rightarrow \sim P)$ が論理同値であることを以下の二つの方法で証明せよ。

   (a) 真理表を書くことによって。

P	Q	R	$(P$	$\vee$	$\sim Q)$	$\Rightarrow$	$(Q$	$\wedge$	$\sim R)$	Q	$\wedge$	$(R$	$\Rightarrow$	$\sim P)$
T	T	T	T	T	F	**F**	T	F	F	T	**F**	T	F	F
T	T	F	T	T	F	**T**	T	T	T	T	**T**	F	T	F
T	F	T	T	T	T	**F**	F	F	F	F	**F**	T	F	F
T	F	F	T	T	T	**F**	F	F	T	F	**F**	F	T	F
F	T	T	F	F	F	**T**	T	F	F	T	**T**	T	T	T
F	T	F	F	F	F	**T**	T	T	T	T	**T**	F	T	T
F	F	T	F	T	T	**F**	F	F	F	F	**F**	T	T	T
F	F	F	F	T	T	**F**	F	F	T	F	**F**	F	T	T

   (b) 式の変形によって。(詳しく途中式を書くこと。)

   解. 以下の変形においては、それぞれ 「$\Rightarrow$ の書きかえ」、「ド・モルガン」、「分配法則」、「$\Rightarrow$ の書きかえ」を用いた。それ以外にも、$\sim(\sim Q) \equiv Q$ や、$\wedge$ や $\vee$ の可換性と呼ばれる、$P \wedge Q \equiv Q \wedge P$ や $P \vee Q \equiv Q \vee P$ を用いた。

$$
\begin{aligned}
&(P \vee \sim Q) \Rightarrow (Q \wedge \sim R) \equiv \sim(P \vee \sim Q) \vee (Q \wedge \sim R) \\
&\quad \equiv \quad (\sim P \wedge Q) \vee (Q \wedge \sim R) \equiv Q \wedge (\sim R \vee \sim P) \equiv Q \wedge (R \Rightarrow \sim P). \blacksquare
\end{aligned}
$$

2. 集合 A, B, C について、Venn 図を使わずに次を証明せよ。ただし、X, Y を集合としたとき、$X - Y = X \cap \overline{Y} = \{x \mid (x \in X) \wedge (x \notin Y)\}$ である。

$$A \cup (B - C) = ((A \cup B) - C) \cup (A \cap C)$$

解. $(\subseteq)$ $x \in A$ は $x \in C$、$a \notin C$ のいずれかだから、$A \subseteq (A - C) \cup (A \cap C)$。$A \subseteq A \cup B$ だから、$A = (A - C) \cup (A \cap C) \subseteq ((A \cup B) - C) \cup (A \cap C)$。また、$B - C \subseteq (A \cup B) - C$ だから、$A \cup (B - C) \subseteq ((A \cup B) - C) \cup (A \cap C)$ を得る。

$(\supseteq)$ $A \cap C \subseteq A$ だから $A \cap C \subseteq A \cup (B - C)$。$x \in (A \cup B) - C$ とすると、$x \in A$ または $x \in B$ でかつ、$x \notin C$ である。$x \in A$ ならば $x \in A \cup (B - C)$ だから、$x \in B$ とすると、$x \notin C$ だから $x \in B - C$. よって常に、$x \in A \cup (B - C)$ である。したがって、$A \cup (B - C) \supseteq ((A \cup B) - C) \cup (A \cap C)$。

よって、$A \cup (B - C) = ((A \cup B) - C) \cup (A \cap C)$ が証明された。 $\blacksquare$

別解. $A = (A - C) \cup (A \cap C)$ である。上では、$\subseteq$ のみ示したが、右辺は A の部分集合だから等号が成り立つ。したがって、

$$
\begin{aligned}
((A \cup B) - C) \cup (A \cap C) &= ((A \cup B) \cap \overline{C}) \cup (A \cap C) \\
&= (A \cap \overline{C}) \cup (B \cap \overline{C}) \cup (A \cap C) \\
&= (A - C) \cup (A \cap C) \cup (B - C) \\
&= A \cup (B - C).
\end{aligned}
$$

3. R を集合 A に定義された関係とする。任意の $a, b, c \in A$ について関係 R が 次の条件 (a), (b), (c) を満たすとき R は同値関係というのであった。

$$\text{(a) } aRa, \quad \text{(b) } aRb \Rightarrow bRa, \quad \text{(c) } (aRb \wedge bRc) \Rightarrow aRc.$$

ここで $a \in A$ に対して、$[a] = \{x \in A \mid xRa\}$ と定義したとき、次が成立することを示せ。一つ一つのステップで、上の (a), (b), (c) のどの性質を使ったか明記せよ。

$$[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset.$$

解. 対偶 $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$ を示す。$[a] \cap [b] \neq \emptyset \Rightarrow [a] \subseteq [b]$ を示せば、a と b の役目を入れ替えて、$[a] \cap [b] \neq \emptyset \Rightarrow [b] \subseteq [a]$ を得るので、$[a] = [b]$ となる。仮定より、$[a] \cap [b] \neq \emptyset$ だから、$c \in [a] \cap [b]$ とする。$[a]$, $[b]$ の定義より、cRa かつ cRb である。(b) より aRc でもある。ここで、$x \in [a]$ とすると、xRa。aRc と (c) を用いて、xRc。さらに、cRb と (c) を用いると、xRb を得る。したがって、$x \in [b]$ である。$x \in [a]$ は任意だったから、$[a] \subseteq [b]$ を得る。これで証明された。 ■

4. $a, b \in \boldsymbol{Z}$ に対して $2a^2 + 5b^2 \equiv 0 \pmod 7$ のとき aRb と定める。

(a) R が 整数の集合 $\boldsymbol{Z}$ 全体の上の同値関係であることを示せ。

解. $2a^2 + 5b^2 \equiv 0 \pmod 7$ の両辺に $2b^2$ を加え、$7b^2 \equiv 0 \pmod 7$ を用いると、$2a^2 \equiv 2b^2 \pmod 7$ となる。さらに、両辺に 4 をかけると $a^2 \equiv b^2 \pmod 7$ となる。逆に、$a^2 \equiv b^2 \pmod 7$ とすると、両辺に 2 をかけることにより、$2a^2 \equiv 2b^2 \pmod 7$ を得、さらに、$5b^2$ を両辺に加えることにより、最初の式を得る。したがって、aRb は、$a^2 \equiv b^2 \pmod 7$ と同値である。前問における同値関係になる条件 (a) (b) (c) を調べる。しかし、$\equiv$ は同値関係だったから、条件は明らかに成立する。 ■

(b) 相異なる同値類はいくつあるか。同値類を決定せよ。

解. $a \equiv b \pmod 7$ ならば $a^2 \equiv b^2$ だから、$\equiv$ に関する同値類に関して調べればよい。$1^2 \equiv 6^2 \pmod 7$, $2^2 \equiv 5^2 \pmod 7$、$3^2 \equiv 4^2 \pmod 7$ で、0, 1, 4, 2 は 7 を法として異なるので、同値類は 4 個でそれぞれは、$[a] = \{x \in \boldsymbol{Z} \mid x \equiv a \pmod 7\}$ とすると、$[0]$, $[1] \cup [6]$, $[2] \cup [5]$, $[3] \cup [4]$ となる。 ■

5. f を集合 A から集合 B への写像（関数）、g を集合 B から集合 C への写像とする。この時、$h = g \circ f : A \to C$ $(a \mapsto g(f(a)))$ によって 集合 A から C への写像 $h = g \circ f$ を定義する。以下を証明または反証せよ。

(a) g が全射であるとき $h = g \circ f$ も全射である。

解. 成り立たない。反例を示す。$A = \{1\}$, $B = C = \{1, 2\}$, $f(1) = 1$, $g(1) = 1$, $g(2) = 2$ とする。$h(1) = 1$ で、$A = \{1\}$ だから、$h(a) = 2$ となる $a \in A$ は存在しない。したがって、g は全射であるが h は全射ではない。 ■

(b) f は単射ではないが $h = g \circ f$ は単射であるような例が存在する。

解. 存在しない。つまり、h が単射なら f は単射。

$f(a) = f(a')$ とする。すると $h(a) = g(f(a)) = g(f(a')) = h(a')$ となる。h は仮定より単射であるから、$a = a'$ となる。$f(a) = f(a')$ を仮定して、$a = a'$ を得たので、f は単射である。 ■

鈴木寛 (hsuzuki@icu.ac.jp)