

# Quiz 1

Due at 10:00 a.m. on April 20, 2007

Division:

ID#:

Name:

1.  $P, Q, R$  を命題とする。このとき、 $(P \wedge Q) \Rightarrow R \equiv Q \Rightarrow (P \Rightarrow R)$  (論理同値) であることを真理表を完成することにより証明せよ。

$P$	$Q$	$R$	$(P \wedge Q) \Rightarrow R$	$Q \Rightarrow (P \Rightarrow R)$	$X$
$T$	$T$	$T$			$T$
$T$	$T$	$F$			$T$
$T$	$F$	$T$			$T$
$T$	$F$	$F$			$T$
$F$	$T$	$T$			$T$
$F$	$T$	$F$			$T$
$F$	$F$	$T$			$T$
$F$	$F$	$F$			$T$

2. 上の論理同値を基本性質 (命題 1.1 (1)–(7) または 教科書 p.44 (1)–(4) と  $P \Rightarrow Q \equiv (\sim P) \vee Q$ ) のみを用いて示せ。どの基本性質を用いたかその番号も記せ。

3.  $Q \Rightarrow (P \Rightarrow R)$  と論理同値な命題の一つを  $\sim$  と  $\vee$  および括弧 ( ) のみを用いてあらわせ。 $\wedge, \Rightarrow, \Leftrightarrow$  は用いないこと。

4. 真理値がすべて  $T$  となるような論理式  $X$  で  $P, Q, R$  をすべて含んだものを一つ与え、その真理値がすべて  $T$  となることを、ことばで説明せよ。

Message 欄 (裏にもどうぞ): この授業に期待すること。要望。自分にとって数学とは。

# Solutions to Quiz 1

(April 20, 2007)

1.  $P, Q, R$  を命題とする。このとき、 $(P \wedge Q) \Rightarrow R \equiv Q \Rightarrow (P \Rightarrow R)$  (論理同値) であることを真理表を完成することにより証明せよ。

$P$	$Q$	$R$	$(P \wedge Q) \Rightarrow R$	$Q \Rightarrow (P \Rightarrow R)$	$X$
$T$	$T$	$T$	$T$	$T$	$T$
$T$	$T$	$F$	$T$	$F$	$T$
$T$	$F$	$T$	$F$	$T$	$T$
$T$	$F$	$F$	$F$	$T$	$T$
$F$	$T$	$T$	$F$	$T$	$T$
$F$	$T$	$F$	$F$	$T$	$T$
$F$	$F$	$T$	$F$	$T$	$T$
$F$	$F$	$F$	$F$	$T$	$T$

2. 上の論理同値を基本性質 (命題 1.1 (1)-(7) または 教科書 p.44 (1)-(4) と  $P \Rightarrow Q \equiv (\sim P) \vee Q$ ) のみを用いて示せ。どの基本性質を用いたかその番号も記せ。

解. (NetCommons に Note も公開しているので、クラスで述べた命題 1.1 の番号に従います。)

$$\begin{aligned}
 (P \wedge Q) \Rightarrow R &\stackrel{(7)}{\equiv} \sim (P \wedge Q) \vee R \stackrel{(3)}{\equiv} \sim (Q \wedge P) \vee R \stackrel{(6)}{\equiv} (\sim Q \vee \sim P) \vee R \\
 &\stackrel{(4)}{\equiv} \sim Q \vee (\sim P \vee R) \stackrel{(7)}{\equiv} Q \Rightarrow (\sim P \vee R) \stackrel{(7)}{\equiv} Q \Rightarrow (P \Rightarrow R) \quad \blacksquare
 \end{aligned}$$

3.  $Q \Rightarrow (P \Rightarrow R)$  と論理同値な命題の一つを  $\sim$  と  $\vee$  および括弧 ( ) のみを用いてあらわせ。 $\wedge, \Rightarrow, \Leftrightarrow$  は用いないこと。

解. 前問より

$$Q \Rightarrow (P \Rightarrow R) \equiv (\sim Q \vee \sim P) \vee R. \quad \blacksquare$$

形からも明らかなように、 $P$  と  $Q$  は入れ替えても同じです。また、 $\vee$  の結合法則から、最後の論理式は、括弧の付け方によらないので、 $\sim Q \vee \sim P \vee R$ 。ただし、 $\sim$  (否定) は先にするという約束で、括弧を付けてありません。次には注意して下さい。下のものが論理同値ではないことはどのように示すことができますか。

$$P \wedge (Q \vee R) \neq (P \wedge Q) \vee R, \quad P \vee (Q \wedge R) \neq (P \vee Q) \wedge R.$$

4. 真理値がすべて  $T$  となるような論理式  $X$  で  $P, Q, R$  をすべて含んだものを一つ与え、その真理値がすべて  $T$  となることを、ことばで説明せよ。

解.  $(P \wedge Q) \Rightarrow R$  と  $Q \Rightarrow (P \Rightarrow R)$  が論理同値であることから、

$$(P \wedge Q) \Rightarrow R \Leftrightarrow Q \Rightarrow (P \Rightarrow R)$$

はトートロジー。すなわち、すべての真理値が  $T$  になります。  $\blacksquare$

実際には真ん中の  $\Leftrightarrow$  を  $\Rightarrow$  に変えても構いませんし、他にも様々なものを構成することができます。たとえば  $P \vee \sim P$  はトートロジーですから、 $(P \vee \sim P) \vee Q \vee R$  もトートロジーです。

# Quiz 2

(Due at 10:00 a.m. on Fri. April 27, 2007)

Division:            ID#:                            Name:

$A, B, C$  を集合とする。以下の証明においては、Venn 図を用いないこと。

1.  $A \cap B \subseteq A \cap (B \cup C)$  であることを証明せよ。
2.  $A \cap B = A \cap (B \cup C)$  であるが、 $B \neq B \cup C$  である例を挙げよ。
3.  $A \cap C \subseteq A \cap B \Rightarrow A \cap B = A \cap (B \cup C)$  であることを証明せよ。
4.  $A \cap B = A \cap (B \cup C) \Rightarrow A \cap C \subseteq A \cap B$  であることを背理法を用いず証明せよ。
5.  $A \cap B = A \cap (B \cup C) \Rightarrow A \cap C \subseteq A \cap B$  を背理法を用いて証明せよ。

Message 欄 (裏にもどうぞ): 数学と論理の関係について、その違いについて。(HP 掲載不可は明記のこと)

# Solutions to Quiz 2

(April 27, 2007)

1.  $A \cap B \subseteq A \cap (B \cup C)$ であることを証明せよ。

解.  $x \in A \cap B$  とする。 $A \cap B$  の定義より  $x \in A$  かつ  $x \in B$ 。 $x \in B$  だから、 $B \cup C$  の定義より、 $x \in B \cup C$ 。 $x \in A$  だったから  $x \in A \cap (B \cup C)$ 。したがって、 $A \cap B \subseteq A \cap (B \cup C)$  である。 ■

集合  $X, Y$  において、 $X \subseteq Y$  を示すには、その定義である、 $x \in X \Rightarrow x \in Y$  がすべての  $x$  について成立することを言う。しかし、ここでは、 $B \subseteq B \cup C$  だから、 $A \cap B \subseteq A \cap (B \cup C)$  としても良い。ただ、その場合は、 $X \subseteq X \cup Y$  および  $Y \subseteq Z$  ならば  $X \cap Y \subseteq X \cap Z$  という基本性質を利用していることを確認すること。

2.  $A \cap B = A \cap (B \cup C)$  であるが、 $B \neq B \cup C$  である例を挙げよ。

解.  $A = \emptyset, B = \emptyset, C = \{\emptyset\} (= \mathcal{P}(\emptyset))$ . ■

例はたくさんありますが、大切なのは、具体的な例をあげること。これは、 $A \cap B = A \cap (B \cup C) \Rightarrow B = B \cup C$  が一般には成立しない「反例」といいます。成り立たない条件を見つけるのではありません。一般には成り立たないことを示すには、非常に特殊な例であっても、一つ成り立たない例があれば良いのです。たくさん例がある場合も、一つしか例が無い場合もありますが、どちらであっても一つ示せば、成り立たないことを示すことができます。 $\sim (\forall x P(x)) \equiv \exists x (\sim P(x))$ 。

3.  $A \cap C \subseteq A \cap B \Rightarrow A \cap B = A \cap (B \cup C)$  であることを証明せよ。

解.  $A \cap B = A \cap (B \cup C)$  を示すには、 $A \cap B \subseteq A \cap (B \cup C)$  と  $A \cap B \supseteq A \cap (B \cup C)$  を示せばよい。前者は問題1で示しているので、後者を示せば十分である。 $x \in A \cap (B \cup C)$  とする。すると、 $x \in A$  かつ  $x \in B \cup C$ 。したがって、 $x \in B$  または  $x \in C$  である。 $x \in B$  とすると、 $x \in A$  だから  $x \in A \cap B$ 。一方、 $x \in C$  とすると、 $x \in A \cap C$  である。仮定より  $A \cap C \subseteq A \cap B$  だから  $x \in A \cap B$  したがっていずれの場合も、 $x \in A \cap B$  となるので、 $A \cap B \supseteq A \cap (B \cup C)$  すなわち、 $A \cap B = A \cap (B \cup C)$  を示すことができた。 ■

どこで仮定を利用するかを明確にしないとイケません。また  $P \Rightarrow Q$  型の命題は、 $P$  が真で  $Q$  が偽のときのみ偽ですから、この命題を示すときは、 $Q$  が真であることを証明すればよいのです。その途中で、どこかで  $P$  が真であること（仮定という。 $P$  が偽のときは  $P \Rightarrow Q$  は真。）を使うわけですが、 $P$  が真であることは常に必要でないことを理解して下さい。

4.  $A \cap B = A \cap (B \cup C) \Rightarrow A \cap C \subseteq A \cap B$  であることを背理法を用いず証明せよ。

解.  $C \subseteq B \cup C$  に注意すると、 $A \cap C \subseteq A \cap (B \cup C)$ 。仮定から、 $A \cap B = A \cap (B \cup C)$  だから、 $A \cap C \subseteq A \cap B$  である。 ■

むろん、 $x \in A \cap C$  として仮定を用いて、 $x \in A \cap B$  を示すのが一番正当です。上では少し基本性質を使って、証明を短くしました。どんな基本性質を使ったかわかりますか。

5.  $A \cap B = A \cap (B \cup C) \Rightarrow A \cap C \subseteq A \cap B$  を背理法を用いて証明せよ。

解.  $A \cap C \not\subseteq A \cap B$  とする。すると、 $x \in A \cap C$  かつ  $x \notin A \cap B$  なる元  $x$  が存在する。 $C \subseteq B \cup C$  だから  $x \in A \cap (B \cup C)$  である。仮定から、 $A \cap B = A \cap (B \cup C)$  であるが、 $x \notin A \cap B$  でこれは、 $x \in A \cap (B \cup C)$  に反する。したがって  $A \cap C \subseteq A \cap B$  でなければならない。 ■

# Quiz 3

(Due: 7:00 p.m. May 7, 2007)

Division:

ID#:

Name:

$a, b \in \mathbf{Z}$  に対して  $b = ca$  となる  $c \in \mathbf{Z}$  が存在するとき  $a \mid b$  と書くことにする。 $n$  を正の整数とし  $n \mid b - a$  のとき  $a \equiv b$  と書く。また  $[a] = \{x \in \mathbf{Z} \mid x \equiv a\}$  とする。

1.  $a \equiv b$  は整数の集合  $\mathbf{Z}$  に同値関係を定義すること、すなわち以下を示せ。

For all  $a, b, c \in \mathbf{Z}$ , (i)  $a \equiv a$ , (ii)  $a \equiv b \Rightarrow b \equiv a$ , (iii)  $a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$ .

2.  $a, b, c, d \in \mathbf{Z}$  に対して  $a \equiv b$  かつ  $c \equiv d$  ならば  $ac \equiv bd$  であることを示せ。

3. 整数  $a, p, r$  が  $a = pn + r$  を満たすとする。すると  $[a] = \{mn + r \mid m \in \mathbf{Z}\}$  であることを示せ。

4. 整数  $x, y, z$  で  $x^2 + y^2 = 3z^2$  を満たすものを考える。 $n = 3$  として  $\equiv$  を用いる。

(a)  $x \equiv y \equiv 0$  であることを示せ。(ヒント： $z$  を整数とすると  $z^2 \equiv 0$  または  $1$  であることをまず示せ。)

(b)  $x = y = z = 0$  であることを示せ。(ヒント：まず  $x, y, z$  の最大公約数は  $1$  として良いことを示せ。)

Message 欄 (裏にもどうぞ)：ICU の教学改革について。(HP 掲載不可は明記のこと)

# Solutions to Quiz 3

(May 7, 2007)

$a, b \in \mathbf{Z}$  に対して  $b = ca$  となる  $c \in \mathbf{Z}$  が存在するとき  $a | b$  と書くことにする。 $n$  を正の整数とし  $n | b - a$  のとき  $a \equiv b$  と書く。また  $[a] = \{x \in \mathbf{Z} \mid x \equiv a\}$  とする。

1.  $a \equiv b$  は整数の集合  $\mathbf{Z}$  に同値関係を定義すること、すなわち以下を示せ。

For all  $a, b, c \in \mathbf{Z}$ , (i)  $a \equiv a$ , (ii)  $a \equiv b \Rightarrow b \equiv a$ , (iii)  $a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$ .

解.  $a | b$  の定義から、(I)  $a | 0$  はすべての整数について成立し ( $0 = 0a$ )、(II)  $a | b$  ( $b = ca$  となる  $c$  がある) ならば  $a | -b$  ( $-b = (-c)a$ ) も常に成り立ち、(III)  $a | b$  ( $b = b'a$  となる  $b'$  があり) かつ  $a | c$  ( $c = c'a$  となる  $c'$  がある) ならばすべての整数  $x, y$  について  $a | xb + yc$  ( $xb + yc = (xb' + yc')a$ ) となっていることを確認する。

(i) 性質 (I) より  $n | a - a$  だから  $a \equiv a$ 。(ii) 性質 (II) より  $a \equiv b$  すなわち  $n | b - a$  ならば  $n | a - b$  だから  $b \equiv a$ 。(iii)  $a \equiv b$  かつ  $b \equiv c$  すなわち  $n | b - a$  かつ  $n | c - b$  とすると 性質 (III) より  $n | (c - b) + (b - a)$ 。したがって  $a \equiv c$  となる。(定理 7.6 (p.153) 参照) ■

2.  $a, b, c, d \in \mathbf{Z}$  に対して  $a \equiv b$  かつ  $c \equiv d$  ならば  $ac \equiv bd$  であることを示せ。

解.  $a \equiv b$  かつ  $c \equiv d$  とする、定理より  $n | b - a$  かつ  $n | d - c$  である。ここで

$$bd - ac = (bd - bc) + (bc - ac) = b(d - c) + c(b - a).$$

問題 1 の解答の性質 (III) で  $a \rightarrow n, x \rightarrow b, y \rightarrow c, b \rightarrow d - c, c \rightarrow b - a$  とすれば上の式で  $n | (bd - ac)$  を得るから、 $ac \equiv bd$  となる。(結果 4.10 (p.84) 参照) ■

3. 整数  $a, p, r$  が  $a = pn + r$  を満たすとすると  $[a] = \{mn + r \mid m \in \mathbf{Z}\}$  であることを示せ。

解.  $A = \{mn + r \mid m \in \mathbf{Z}\}$  とし、 $[a] \subseteq A$  かつ  $A \subseteq [a]$  を示す。

まず  $x \in [a]$  とする。 $[a]$  の定義より  $n | a - x$ 、仮定より  $a = pn + r$  だから  $x \equiv a \equiv r$ 。問題 1 (iii) (ii) より  $x \equiv r$  すなわち  $r \equiv x$ 。したがって  $n | x - r$  だから  $x = mn + r$  となる  $m \in \mathbf{Z}$  が存在する。これは、 $x \in A$  を意味する。

$x \in A$  とする。すると  $m \in \mathbf{Z}$  で  $x = mn + r$  となるものがある。したがって

$$x \equiv mn + r \equiv r \equiv pn + r \equiv a$$

これより 問題 1 (iii) を用いて、 $x \equiv a$  すなわち  $x \in [a]$  となる。 ■

4. 整数  $x, y, z$  で  $x^2 + y^2 = 3z^2$  を満たすものを考える。 $n = 3$  として  $\equiv$  を用いる。

- (a)  $x \equiv y \equiv 0$  であることを示せ。(ヒント： $z$  を整数とすると  $z^2 \equiv 0$  または  $1$  であることをまず示せ。)

解.  $n = 3$  として  $\equiv$  を用いる。 $z$  を 3 で割ったあまりを  $r$  とすると  $z = 3q + r$ 、 $r = 0, 1, 2$  だから、 $z \equiv 0, 1$  or  $2$ 。したがって問題 2 より  $z^2 \equiv 0, 1$  または  $4$  であるが  $4 \equiv 1$  だから  $z^2 \equiv 0$  または  $1$ 。したがって  $x^2, y^2$  についても同じ事が言えるが、 $x^2 + y^2 = 3z^2 \equiv 0$  だから  $x^2$  または  $y^2$  の少なくとも一方が  $1$  と  $3$  を法として合同だとこの式は成立しない。したがって  $x^2 \equiv y^2 \equiv 0$ 。また上の考察からこうなるのは、 $x \equiv y \equiv z \equiv 0$  のときに限る。 ■

- (b)  $x = y = z = 0$ であることを示せ。(ヒント：まず  $x, y, z$  の最大公約数は 1 として良いことを示せ。)

解.  $x, y, z$  のすべては零ではないとする。 $x, y, z$  の最大公約数を  $d$  とする。 $x = dx', y = dy', z = dz'$  で、 $x', y', z'$  の最大公約数は 1 である。また、 $x^2 + y^2 = 3z^2$  より  $x'^2 + y'^2 = 3z'^2$  となる。また  $x', y', z'$  のすべては零ではない。したがって、 $x^2 + y^2 = 3z^2$  を満たす互いに素な整数  $x, y, z$  ですべては零でないものが存在しないことを示せばよい。(a) より  $x \equiv y \equiv 0$ 。すると  $9 \mid x^2, 9 \mid y^2$  となり  $9 \mid 3z^2$ 。したがって  $3 \mid z^2$  だから (a) で見たように、 $3 \mid z$  を得る。しかし、これは 3 が  $x, y, z$  の公約数であることとなり、矛盾である。すなわち  $x = y = z = 0$  である。 ■

上で最大公約数が出てきました。 $x, y, z$  がすべて零のときの最大公約数は定義せず避けました。一般的には、どんな整数も、零の約数になりますから、いくらでも大きな約数が存在し、最大な公約数は、すべてが零の場合には、決められなくなってしまいます。このことを回避する一つの方法は、最大公約数は、すべてが零ではないときに、定めることです。一つでも零でなければ、その数を  $a$  としましょう、の約数は  $|a|$  以下ですから、最大の公約数も  $|a|$  以下となり、最大の公約数を定めることができます。しかし、ほかの代数系に拡張するなど、一般化を考えるときには、通常的大小関係以外の方法で最大公約数を決めたほうが便利なので、もう少し一般的に扱えるように、定義し直してみたいと思います。次の定義で定められる数がみなさんが知っている、最大公約数と同じになること、さらに、すべてが零の場合も、最大公約数はある数になることを確かめて下さい。

最大公約数  $a_1, a_2, \dots, a_n \in \mathbf{Z}$  とする。次の性質を満たす  $d \in \mathbf{Z}$  を  $a_1, a_2, \dots, a_n$  の最大公約数 (the greatest common divisor) といい  $d = \gcd\{a_1, a_2, \dots, a_n\}$  と書く。

$\gcd\{a_1, a_2, \dots, a_n\} = 1$  であるとき  $a_1, a_2, \dots, a_n$  は互いに素である (relatively prime) という。

(i)  $d \geq 0$ .

(ii)  $d \mid a_1, d \mid a_2, \dots, d \mid a_n$ .

(iii)  $c \mid a_1, c \mid a_2, \dots, c \mid a_n$  ならば  $c \mid d$ .

実は、 $a_1, a_2, \dots, a_n \in \mathbf{Z}$  としたとき、最大公約数  $d = \gcd\{a_1, a_2, \dots, a_n\}$  がただ一つ存在し、このとき、 $d = a_1x_1 + a_2x_2 + \dots + a_nx_n$  となる  $x_1, x_2, \dots, x_n \in \mathbf{Z}$  が存在します。 $d$  と  $d'$  が共に、 $\gcd\{a_1, a_2, \dots, a_n\}$  の条件を満たすとすると、 $d$  が (ii) を、 $d'$  が (iii) を満たすことより、 $d \mid d'$ 。同様にして、 $d' \mid d$ 。(i) の条件から  $d = d'$  となります。従って、上の条件を満たす数は一意性に決まります。また、

$a_1, a_2, \dots, a_n, a_{n+1} \in \mathbf{Z}$  とする。この時、次が成立する。

$$\gcd\{a_1, a_2, \dots, a_n, a_{n+1}\} = \gcd\{\gcd\{a_1, a_2, \dots, a_n\}, a_{n+1}\}.$$

これを用いれば、最大公約数の存在も、 $n = 2$  の場合に証明することができればよいことが分かります。この部分の証明そして、 $d = a_1x_1 + a_2x_2 + \dots + a_nx_n$  と書けることの証明は演習問題とします。

$a = 132, b = -36$  の場合の例を書きます。

$$132 = (-36)(-3) + 24, \quad -36 = 24(-2) + 12, \quad 24 = 12 \cdot 2 + 0$$

であるから、最後の 0 でない剰余 12 が 132 と  $-36$  の最大公約数である。さらに

$$12 = -36 + 24 \cdot 2 = -36 + (132 + (-36)3) \cdot 2 = 132 \cdot 2 + (-36)7.$$

# Quiz 4

(Due at 10:00 a.m. on Friday May 11, 2007)

Division:

ID#:

Name:

1.  $(\mathbf{Z} \times \mathbf{Z}^*, Q)$ :  $\mathbf{Z}^* = \mathbf{Z} - \{0\}$  は 0 以外の整数全体を表すとする。  $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}^*$  に対して、  $0 \mid ad - bc$  すなわち  $ad = bc$  のとき、  $(a, b)Q(c, d)$  と定義する。

(a)  $Q$  は集合  $\mathbf{Z} \times \mathbf{Z}^*$  の同値関係であることを示せ。

(b)  $(1, 2)$  の属する同値類を決定せよ。

(c)  $(a, b)Q(a', b')$  かつ  $(c, d)Q(c', d')$  ならば、  $(ad + bc, bd)Q(a'd' + b'c', b'd')$  であることを示せ。

(d) (a), (b) は有理数の和がその表し方によらないことを示していることを説明せよ。

2.  $(\mathbf{Z} \times \mathbf{Z}, \tilde{Q})$ :  $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}$  に対して、  $0 \mid ad - bc$  すなわち  $ad = bc$  のとき、  $(a, b)\tilde{Q}(c, d)$  と定義する。 このとき  $\tilde{Q}$  は集合  $\mathbf{Z} \times \mathbf{Z}$  の同値関係になるかどうか判定せよ。理由も述べよ。

Message 欄：将来の夢、目標、25年後の自分について、世界について。

# Solutions to Quiz 4

(May 11, 2007)

1.  $(\mathbf{Z} \times \mathbf{Z}^*, Q)$ :  $\mathbf{Z}^* = \mathbf{Z} - \{0\}$  は 0 以外の整数全体を表すとする。  $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}^*$  に対して、  $0 \mid ad - bc$  すなわち  $ad = bc$  のとき、  $(a, b)Q(c, d)$  と定義する。

(a)  $Q$  は集合  $\mathbf{Z} \times \mathbf{Z}^*$  の同値関係であることを示せ。

解.  $(a, b) \in \mathbf{Z} \times \mathbf{Z}^*$  とする。  $ab = ba$  だから  $Q$  の定義より  $(a, b)Q(a, b)$ 。 反射律が成立。  $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}^*$  において  $(a, b)Q(c, d)$  とする。  $Q$  の定義より  $ad = bc$  だから  $cb = da$ 。 したがって  $Q$  の定義より  $(c, d)Q(a, b)$ 。 対称律が成立。  $(a, b), (c, d), (e, f) \in \mathbf{Z} \times \mathbf{Z}^*$  において  $(a, b)Q(c, d)$  かつ  $(c, d)Q(e, f)$  とする。  $Q$  の定義より  $ad = bc$  かつ  $cf = de$  である。 よって  $(af - be)d = adf - bde = bcf - bcf = 0$ 。 ここで  $d \neq 0$  だから  $af = be$  となり  $Q$  の定義より  $(a, b)Q(e, f)$  が成り立つ。 推移律が成立。

(b) (1, 2) の属する同値類を決定せよ。

解.  $(a, b) \in \mathbf{Z} \times \mathbf{Z}^*$ ,  $(a, b)Q(1, 2)$  とする。  $Q$  の定義より  $2a = b$  ただし  $b \in \mathbf{Z}^*$ 。 逆に  $(a, 2a) \in \mathbf{Z} \times \mathbf{Z}^*$  とすると  $(1, 2)Q(a, 2a)$ 。 したがって (1, 2) の属する同値類  $[(1, 2)]$  は

$$[(1, 2)] = \{(a, 2a) \mid a \in \mathbf{Z}^*\} = \left\{ (a, b) \in \mathbf{Z} \times \mathbf{Z}^* \mid \frac{a}{b} = \frac{1}{2} \right\}.$$

ここで二つめの集合は、有理数として  $1/2$  と等しいものという意味である。 ■

(c)  $(a, b)Q(a', b')$  かつ  $(c, d)Q(c', d')$  ならば、  $(ad + bc, bd)Q(a'd' + b'c', b'd')$  であることを示せ。

解. まず  $b, d, b', d' \in \mathbf{Z}^*$  だから  $(ad + bc, bd), (a'd' + b'c', b'd') \in \mathbf{Z} \times \mathbf{Z}^*$  である。 また  $(a, b)Q(a', b')$ 、  $(c, d)Q(c', d')$  より  $ab' = ba'$ 、  $cd' = dc'$  だから

$$\begin{aligned} (ad + bc)b'd' - bd(a'd' + b'c') &= adb'd' - bcb'd' - bda'd' - bdb'c' \\ &= ba'dd' - bb'dc' - ba'dd' - bb'dc' = 0. \end{aligned}$$

したがって、  $(ad + bc, bd)Q(a'd' + b'c', b'd')$  である。 ■

(d) (a), (b) は有理数の和がその表し方によらないことを示していることを説明せよ。

解.  $Q$  の定義から  $(a, b)Q(a', b')$ 、  $(c, d)Q(c', d')$  は、  $ab' = ba'$ 、  $cd' = dc'$  であるが、これは、有理数として  $a/b = a'/b'$ 、  $c/d = c'/d'$  と同値である。 また、  $(ad + bc, bd)Q(a'd' + b'c', b'd')$  は  $(ad + bc)/bd = (a'd' + b'c')/b'd'$  と同値である。 つまり有理数  $a/b$ 、  $c/d$  が他の分数で表せたとしても、和の計算結果は、  $a/b$  の分子分母を用いても、  $a'/b'$  の分子分母をもちいても、  $c/d$  の分子分母のかわりに、  $c'/d'$  の分子分母を用いても、

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'}$$

で等しいことを表している。 ■

2.  $(\mathbf{Z} \times \mathbf{Z}, \tilde{Q})$ :  $(a, b), (c, d) \in \mathbf{Z} \times \mathbf{Z}$  に対して、  $0 \mid ad - bc$  すなわち  $ad = bc$  のとき、  $(a, b)\tilde{Q}(c, d)$  と定義する。 このとき  $\tilde{Q}$  は集合  $\mathbf{Z} \times \mathbf{Z}$  の同値関係になるかどうか判定せよ。 理由も述べよ。

解.  $(0, 1)\tilde{Q}(0, 0)$  かつ  $(0, 0)\tilde{Q}(1, 0)$  であるが  $(0, 1)\tilde{Q}(1, 0)$  は成立しない。 したがって推移律は成り立たないので、同値関係ではない。 ■

# Quiz 5

Due at 10:00 a.m. on May 18, 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、 $X - Y = X \cap \bar{Y} = \{x \mid (x \in X) \wedge (x \notin Y)\}$  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。

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

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.  $a, b \in \mathbf{Z}$  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  $\mathbf{Z}$  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、 $h = g \circ f : A \rightarrow C$  ( $a \mapsto g(f(a))$ ) 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 : Midterm Exam について。[裏にもどうぞ。掲載不可の場合は明記のこと。]

# Solutions to Quiz 5

May 18, 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。

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

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、 $X - Y = X \cap \bar{Y} = \{x \mid (x \in X) \wedge (x \notin Y)\}$  である。

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

解. ( $\subseteq$ )  $x \in A$  は  $x \in C$ ,  $x \notin C$  のいずれかだから、 $A \subseteq (A - C) \cup (A \cap C)$ 。また、 $A \subseteq A \cup B$  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  $A \cap C \subseteq A \cup (B - C)$ 。また、 $x \in (A \cup B) - C$  とすると、 $x \in A$  または  $x \in B$  であつ、 $x \notin C$  である。もし  $x \in A$  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  $x \in B - C$ 。よつて常に、 $x \in A \cup (B - C)$  である。したがつて、 $A \cup (B - C) \supseteq ((A \cup B) - C) \cup (A \cap C)$ 。

よつて、 $A \cup (B - C) = ((A \cup B) - C) \cup (A \cap C)$  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。したがつて、

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

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。

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

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.  $a, b \in \mathbf{Z}$  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  $\mathbf{Z}$  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、 $[a] = \{x \in \mathbf{Z} \mid x \equiv a \pmod{7}\}$  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、 $h = g \circ f : A \rightarrow C$  ( $a \mapsto g(f(a))$ ) 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。 ■

# Quiz 6

(Due at 10:00 a.m. on Fri. May. 25, 2007)

Division:

ID#:

Name:

1.  $X = \{1, 2, 3\}$ ,  $Y = \{a, b, c, d\}$  とする。以下の解答においては、理由も書くこと。

(a)  $X$  から  $Y$  への単射はいくつあるか。

(b)  $Y$  から  $X$  への全射はいくつあるか。

2.  $f$  を集合  $X$  から  $Y$  への写像、 $g$  を集合  $Y$  から  $Z$  への写像とする。

(a)  $g \circ f : X \rightarrow Z$  が全射ならば、 $g$  は全射であることを証明せよ。

(b)  $g$  が全射であるとき、 $g \circ f : X \rightarrow Z$  は全射であるか。証明または、反証を与えよ。

Message 欄 (裏にもどうぞ): 中学・高等学校などで、数学がきらいまたはとても苦手だと思っている生徒が多いようですが、原因は何でしょうか。改善方法はありますか。(HP 掲載不可は明記のこと)

# Solutions to Quiz 6

(May 25, 2007)

1.  $X = \{1, 2, 3\}$ ,  $Y = \{a, b, c, d\}$  とする。以下の解答においては、理由も書くこと。

(a)  $X$  から  $Y$  への単射はいくつあるか。

解.  $f: X \rightarrow Y$  を単射とすると、 $f(X)$  は 3 個の元からなる  $Y$  の部分集合である。 $f(X)$  の取り方が 4 通りあり、それぞれについて、 $f(X)$  の元の順列だけ  $f$  の取り方があるから (一般に、 $n$  個の元からなる集合からそれ自身への全単射の数は、 $n!$  個)、単射の数は、 $4 \cdot 3! = 24$ . ■

(b)  $Y$  から  $X$  への全射はいくつあるか。

解.  $\text{epi}(n, m)$  で  $n$  点集合から、 $m$  点集合への全射の数を表すとする。 $A = \{1, 2, \dots, n, n+1\}$ ,  $C = \{1, 2, \dots, n\}$ ,  $B = \{1, 2, \dots, m\}$  とする。全射  $f: A \rightarrow B$  において、 $f(n+1) \in f(C)$  の場合と、 $f(n+1) \notin f(C)$  の場合を分けて考えると、前者の場合は、 $f|_C: C \rightarrow B$  は全射。後者の場合は、 $f|_C: C \rightarrow D$ ,  $D = B - \{f(n+1)\}$  が全射だから、 $f(n+1)$  の取り方が  $m$  個あることから、

$$\text{epi}(n+1, m) = m(\text{epi}(n, m) + \text{epi}(n, m-1))$$

が成立する。 $\text{epi}(\ell, \ell)$  は全単射の数だから  $\ell!$  また  $\text{epi}(\ell, 1) = 1$ 。従って、

$$\begin{aligned} \text{epi}(4, 3) &= 3(\text{epi}(3, 3) + \text{epi}(3, 2)) = 3(3! + 2(\text{epi}(2, 2) + \text{epi}(2, 1))) \\ &= 3(6 + 2(2 + 1)) = 36. \quad \blacksquare \end{aligned}$$

全射の数は少し難しいですね。他の考え方もあります。

2.  $f$  を集合  $X$  から  $Y$  への写像、 $g$  を集合  $Y$  から  $Z$  への写像とする。

(a)  $g \circ f: X \rightarrow Z$  が全射ならば、 $g$  は全射であることを証明せよ。

解.  $z \in Z$  とする。 $g \circ f$  は全射だから  $x \in X$  で  $(g \circ f)(x) = z$  となるものがある。ここで、 $f(x) = y$  とおくと、 $g(y) = g(f(x)) = (g \circ f)(x) = z$  となる。すなわち、任意の  $z \in Z$  に対して、 $g(y) = z$  となる  $y \in Y$  が存在したので、 $g$  は全射である。 ■

(b)  $g$  が全射であるとき、 $g \circ f: X \rightarrow Z$  は全射であるか。証明または、反証を与えよ。

解. 成立しない。反例を示す。 $X = \{1\}$ ,  $Y = Z = \{1, 2\}$ ,  $f(1) = 1$ ,  $g(1) = 1$ ,  $g(2) = 2$  とすると、 $g \circ f(X) = \{1\}$  だから  $g \circ f(x) = 2$  となる  $x \in X$  は存在しないので、 $g \circ f$  は全射ではない。 ■

# Quiz 7

(Due at 10:00 a.m. on Fri. June 1, 2007)

Division:            ID#:            Name:

1.  $A = \{x \in \mathbf{Q} \mid x \geq 1\}$  は通常的大小関係について、整列集合でないことを示せ。すなわち  $A$  の空でない部分集合  $S$  で最小元の存在しないものをあげ、実際に最小元がないことを証明せよ。
  
2.  $a_{n+2} = (\alpha + \beta)a_{n+1} - \alpha \cdot \beta a_n$  を満たす数列  $a_0, a_1, a_2, \dots$  を考える。ただし、 $\alpha, \beta$  は相異なる実数の定数とする。
  - (a)  $a, b$  が  $a_0 = a + b, a_1 = a\alpha + b\beta$  を満たすとする。このとき、 $a_n = a\alpha^n + b\beta^n$  であることを数学的帰納法で証明せよ。
  
  - (b)  $a_{n+2} = a_{n+1} + 2a_n$  ( $n = 0, 1, \dots$ ) で、 $a_0 = 1, a_1 = 5$  であるとき、一般項  $a_n$  を求めよ。

Message 欄：数学で（または他のことを勉強していて）感激したこと、面白いと思ったことがあったら、そのことについて教えて下さい。（HP 掲載不可は明記のこと）

# Solutions to Quiz 7

(June 1, 2007)

1.  $A = \{x \in \mathbf{Q} \mid x \geq 1\}$  は通常的大小関係について、整列集合でないことを示せ。すなわち  $A$  の空でない部分集合  $S$  で最小元の存在しないものをあげ、実際に最小元がないことを証明せよ。

解.  $S = \{1 + \frac{1}{n} \mid n \in \mathbf{N}\}$  とする。自然数  $n$  について  $1 < 1 + \frac{1}{n} = \frac{n+1}{n} \in \mathbf{Q}$  だから  $S$  は  $A$  の空でない部分集合である。 $S$  に最小元  $a$  が存在したとすると、最小元の定義から、 $a \in S$  だから  $a = 1 + \frac{1}{m}$ ,  $m \in \mathbf{N}$  と書くことができる。しかし、

$$1 + \frac{1}{m+1} < 1 + \frac{1}{m} = a, \quad 1 + \frac{1}{m+1} \in S$$

だから、 $a$  の  $S$  での最小性に反する。従って、 $S$  の最小元は存在せず、 $A$  は整列集合ではない。 ■

2.  $a_{n+2} = (\alpha + \beta)a_{n+1} - \alpha \cdot \beta a_n$  を満たす数列  $a_0, a_1, a_2, \dots$  を考える。ただし、 $\alpha, \beta$  は相異なる実数の定数とする。

- (a)  $a, b$  が  $a_0 = a + b, a_1 = a\alpha + b\beta$  を満たすとする。このとき、 $a_n = a\alpha^n + b\beta^n$  であることを数学的帰納法で証明せよ。

解. 仮定より、 $n = 0, 1$  のとき、 $a_n = a\alpha^n + b\beta^n$  は成立する。そこで、 $k \geq 1$  とし、 $n = 0, 1, \dots, k$  の時に  $a_n = a\alpha^n + b\beta^n$  が成り立つとして、 $n = k+1$  の時に成立することを示す。仮定から、特に、 $a_{k-1} = a\alpha^{k-1} + b\beta^{k-1}$ ,  $a_k = a\alpha^k + b\beta^k$  であるから、

$$\begin{aligned} a_{k+1} &= (\alpha + \beta)a_k - \alpha \cdot \beta a_{k-1} \\ &= (\alpha + \beta)(a\alpha^k + b\beta^k) - \alpha \cdot \beta(a\alpha^{k-1} + b\beta^{k-1}) \\ &= a\alpha^{k+1} + b\beta^{k+1} + \alpha \cdot \beta(a\alpha^{k-1} + b\beta^{k-1}) - \alpha \cdot \beta(a\alpha^{k-1} + b\beta^{k-1}) \\ &= a\alpha^{k+1} + b\beta^{k+1}. \end{aligned}$$

これは、 $a_n = a\alpha^n + b\beta^n$  の  $n$  に  $k+1$  を入れた式であるから、数学的帰納法により、すべての  $0$  以上の整数  $n$  について、 $a_n = a\alpha^n + b\beta^n$  が成立する。 ■

- (b)  $a_{n+2} = a_{n+1} + 2a_n$  ( $n = 0, 1, \dots$ ) で、 $a_0 = 1, a_1 = 5$  であるとき、一般項  $a_n$  を求めよ。

解. 最初の式で、 $\alpha = 2, \beta = -1$  とおけば、 $\alpha + \beta = 1, \alpha \cdot \beta = -2$  だから、 $a_{n+2} = (\alpha + \beta)a_{n+1} - \alpha \cdot \beta a_n$  が成立する。また、 $a + b = 1, 2a - b = 5$  を解くと、 $a = 2, b = -1$  を得るから、上の考察より  $a_n = 2 \cdot 2^n - (-1)^n$  となる。(一意的に決まることはどのようにして示しますか。) ■

注:  $a_{n+2} = pa_{n+1} - qa_n$  を満たす数列において、二次方程式  $x^2 - px + q = 0$  を考える。上ではこの方程式が二実根を持つ場合を考えたが、二つの複素解を持つ場合も全く同様である。では、重根を持つ場合は、どうなるでしょうか。すなわち、 $a_{n+2} = 2pa_{n+1} - p^2a_n$  たとえば、 $a_{n+2} = 2a_{n+1} - a_n$  というような場合です。考えてみて下さい。これができれば、 $a_{n+2} = pa_{n+1} - qa_n$  の形の漸化式で定義されている数列の一般解が得られることとなります。

# Quiz 8

(Due at 10:00 a.m. on Fri. June 8, 2007)

Division:

ID#:

Name:

以下において、 $a, b$  を  $a < b$  である実数とする。問題 3, 4, 5 においては問題 1 の定義にもどってていねいに証明せよ。

1. 集合  $A$  と 集合  $B$  が対等 (個数同値) であることの定義を述べよ。

2.  $f : (-1, 1) \rightarrow \mathbf{R} \left( x \mapsto \frac{x}{1-x^2} \right)$  は全単射であることを示せ。

3. 开区間  $(-1, 1)$  と  $(a, b)$  は対等 (個数同値) であることを示せ。

4. 开区間  $(a, b)$  と  $\mathbf{R}$  は対等 (個数同値) であることを示せ。

5. 直積  $(-1, 1) \times (-1, 1)$  と 直積  $(a, b) \times \mathbf{R}$  は対等 (個数同値) であることを示せ。

Message 欄：あなたが尊敬する、または、魅力的だと思う人は、どのような人ですか。  
そのほか何でもどうぞ。(HP 掲載不可は明記のこと)

# Solutions to Quiz 8

(June 8, 2007)

以下において、 $a, b$  を  $a < b$  である実数とする。問題 3, 4, 5 においては問題 1 の定義にもどって  
ていねいに証明せよ。

1. 集合  $A$  と 集合  $B$  が対等 (個数同値) であることの定義を述べよ。

解. 集合  $A$  から  $B$  への全単射  $f: A \rightarrow B$  が存在するとき、集合  $A$  と 集合  $B$  は対等  
(個数同値) である。

2.  $f: (-1, 1) \rightarrow \mathbf{R} \left( x \mapsto \frac{x}{1-x^2} \right)$  は全単射であることを示せ。

解. 単射性:  $f(x) = f(y)$  と仮定して  $x = y$  を示す。仮定から、 $x/(1-x^2) = f(x) = f(y) = y/(1-y^2)$  である。この式から

$$0 = x(1-y^2) - y(1-x^2) = x - xy^2 - y + x^2y = (x-y)(1+xy)$$

となる。 $f$  の定義域より、 $|x| < 1$  かつ  $|y| < 1$  だから  $|xy| < 1$  で  $1+xy > 0$  である。し  
たがって、 $x = y$  を得る。これは、 $f$  が単射であることを意味する。

全射性:  $y \in \mathbf{R}$  として  $f(x) = y$  となる  $x \in (-1, 1)$  が存在する事を示す。 $\phi(x) = yx^2 + x - y$  を  
考えると  $\phi(1) = 1$ ,  $\phi(-1) = -1$  となるから、中間値の定理から  $\phi(x) = 0$  となる  $x \in (-1, 1)$   
が存在する。すると、この  $x$  に関して  $y = x/(1-x^2) = f(x)$  を満たすから、 $f$  は全射と  
なる。(上記の二次方程式を解くときは、解が  $(-1, 1)$  の間に必ずあることを示す必要があ  
る。) ■

全射性別解:  $y \in \mathbf{R}$  とし  $f(x) = y$  となる  $x \in (-1, 1)$  が存在することをしめす。

$$f(x) = \frac{x}{1-x^2} = \frac{1}{2} \left( \frac{1}{1-x} - \frac{1}{1+x} \right)$$

だから、

$$\lim_{x \rightarrow 1-0} f(x) = +\infty, \quad \lim_{x \rightarrow -1+0} f(x) = -\infty$$

となる。 $f(x)$  は、 $(-1, 1)$  で連続だから、中間値の定理によって、 $x \in (-1, 1)$  で  $f(x) = y$   
となるものが存在する。したがって全射である。 ■

3. 开区間  $(-1, 1)$  と  $(a, b)$  は対等 (個数同値) であることを示せ。

解. 一次関数  $g(x) = \frac{b-a}{2}(x+1) + a$  を考える。 $g(-1) = a$ ,  $g(1) = b$  で  $a < b$  だから、  
 $g(x)$  は単調増加、かつ  $g$  を  $(-1, 1)$  に制限した写像も同じ  $g$  であらわすと、 $g: (-1, 1) \rightarrow$   
 $(a, b)$  ( $x \mapsto \frac{b-a}{2}(x+1) + a$ ) でこれは、全単射である。したがって、定義より  $(-1, 1)$  と  
 $(a, b)$  は対等 (個数同値) である。 ■

4. 开区間  $(a, b)$  と  $\mathbf{R}$  は対等 (個数同値) であることを示せ。

解.  $f \circ g^{-1}: (a, b) \rightarrow \mathbf{R} (x \mapsto f(g^{-1}(x)))$  とする、 $f$  も  $g$  も全単射だから  $g$  の逆写像も、  
 $g$  の逆写像と  $f$  の合成写像も全単射である。したがって、开区間  $(a, b)$  と  $\mathbf{R}$  は対等 (個数  
同値) である。 ■

5. 直積  $(-1, 1) \times (-1, 1)$  と 直積  $(a, b) \times \mathbf{R}$  は対等 (個数同値) であることを示せ。

解.  $h: (-1, 1) \times (-1, 1) \rightarrow (a, b) \times \mathbf{R} ((x_1, x_2) \mapsto (g(x_1), f(x_2)))$  とする。ただし、  
 $f(x), g(x)$  はそれぞれ、問題 2, 3 ので定義されたものである。まず、 $h(x_1, x_2) = h(x_{1'}, x_{2'})$   
とする。 $h$  の定義より、 $h(x_1, x_2) = (g(x_1), f(x_2))$ ,  $h(x_{1'}, x_{2'}) = (g(x_{1'}), f(x_{2'}))$  だから  
 $g(x_1) = g(x_{1'})$  および  $f(x_2) = f(x_{2'})$  を得る。 $g, f$  は共に、単射だから  $x_1 = x_{1'}$  および  
 $x_2 = x_{2'}$  を得る。したがって、 $(x_1, x_2) = (x_{1'}, x_{2'})$  となり、 $h$  は単射である。 $y_1 \in (a, b)$ ,  
 $y_2 \in \mathbf{R}$  とすると  $g, f$  が全射だから  $g(x_1) = y_1$ ,  $f(x_2) = y_2$  となる  $x_1, x_2 \in (-1, 1)$  が存  
在する。このとき、 $h(x_1, x_2) = (g(x_1), f(x_2)) = (y_1, y_2)$  となるから  $h$  は全射である。した  
がって、直積  $(-1, 1) \times (-1, 1)$  と 直積  $(a, b) \times \mathbf{R}$  は対等 (個数同値) である。 ■

# Quiz 9

(Due at 10:00 a.m. on Fri. June 15, 2007)

Division:

ID#:

Name:

以下において、 $a, b$  を  $a < b$  である実数とする。問題 3, 4, 5 においては問題 1 の定義にもどってていねいに証明せよ。

1. 集合  $A$  と  $B$  において  $|A| \leq |B|$  であることの定義を述べよ。

2.  $f : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \rightarrow \mathbf{R} (x \mapsto \tan x)$  は全単射であることを示せ。

3.  $|[a, b]| \leq \left| \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \right|$  であることを示せ。

4.  $\left| \left( -\frac{\pi}{2}, \frac{\pi}{2} \right) \right| \leq |[a, b]|$ であることを示せ。

5.  $|[a, b]| = |\mathbf{R}|$ であることを示せ。定理を用いるときには、定理の主張も明記せよ。

Message 欄：ICU を選んだ理由は何ですか。ICU をより魅力的にするにはどうしたら良いでしょうか。

# Solutions to Quiz 9

(June 15, 2007)

以下において、 $a, b$  を  $a < b$  である実数とする。問題 3, 4, 5 においては問題 1 の定義にもどってていねいに証明せよ。

1. 集合  $A$  と  $B$  において  $|A| \leq |B|$  であることの定義を述べよ。

解. 集合  $A$  から  $B$  への単射  $f: A \rightarrow B$  が存在するとき、 $|A| \leq |B|$  である。 ■

注:  $|A| = |C|$ ,  $|B| = |D|$ ,  $|A| \leq |B|$  ならば  $|C| \leq |D|$  である。実際、 $g: C \rightarrow A$  と  $h: B \rightarrow D$  を全単射とすると、 $h \circ f \circ g: C \rightarrow D$  は単射であることが簡単に確かめられる。各自確かめられたし。

2.  $f: (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbf{R}$  ( $x \mapsto \tan x$ ) は全単射であることを示せ。

解.  $f$  の導関数  $f'(x) = \sec^2 x \geq 0$  だから  $f(x) = \tan x$  は単調増加関数であるから単射である。また、 $\lim_{x \rightarrow -\pi/2+0} f(x) = -\infty$ ,  $\lim_{x \rightarrow \pi/2-0} f(x) = +\infty$  で  $f(x) = \tan x$  は連続だから、中間値の定理により全射である。 ■

3.  $|[a, b]| \leq |(-\frac{\pi}{2}, \frac{\pi}{2})|$  であることを示せ。

解. 以下のように写像  $g$  を定義する。

$$g: [a, b] \rightarrow \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \left(x \mapsto \frac{1}{b-a}(x-a)\right)$$

とすると、 $g([a, b]) = [0, 1] \subseteq (-\pi/2, \pi/2)$ 。また、 $g'(x) = 1/(b-a) > 0$  だから  $g(x)$  は単調増加なので、単射。従って定義より  $|[a, b]| \leq |(-\pi/2, \pi/2)|$ 。 ■

注: Quiz 8 と、 $j: [a, b] \rightarrow (a-1, b+1)$  ( $x \mapsto x$ ) を使えば、 $|[a, b]| \leq |(a-1, b+1)| = |(-\pi/2, \pi/2)|$  が導ける。

4.  $|(-\frac{\pi}{2}, \frac{\pi}{2})| \leq |[a, b]|$  であることを示せ。

解. 以下のように、写像  $h$  を定義する。

$$h: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \rightarrow [a, b] \left(x \mapsto \frac{b-a}{3\pi} \left(x + \frac{\pi}{2}\right) + \frac{2a+b}{3}\right).$$

すると、 $h((-\pi/2, \pi/2)) = ((2a+b)/3, (a+2b)/3) \subseteq [a, b]$  かつ、 $h(x)$  は単調増加だから単射。したがって、 $|(-\pi/2, \pi/2)| \leq |[a, b]|$  である。 ■

5.  $|[a, b]| = |\mathbf{R}|$  であることを示せ。定理を用いるときには、定理の主張も明記せよ。

解. 一般に、 $|X| \leq |Y|$  かつ  $|Y| \leq |X|$  ならば、Cantor-Bernstein の定理によって、 $|X| = |Y|$  である。したがって問題 3, 4 の結果より、 $|[a, b]| = |(-\pi/2, \pi/2)|$  である。問題 2 より  $|(-\pi/2, \pi/2)| = |\mathbf{R}|$  だから、 $|[a, b]| = |\mathbf{R}|$  である。 ■