

# 同値関係

桂田 祐史

2013年7月18日, 2023年4月3日

(同値関係とは、何かと何かを「同じ」と見なし、クラス分けして議論するための数学的な枠組みである。)

この文書の内容を講義するのに2回の講義が必要である。

この節の原稿の最初のバージョンは佐藤篤之先生による。数学科後藤四郎先生の「代数学3」のテキスト等も参考にした。

(約束)  $(\forall x \in X) (\forall y \in X)$  を短く  $(\forall x, y \in X)$  と書くことがある。同様にして  $(\forall x \in X) (\forall y \in X) (\forall z \in X)$  を  $(\forall x, y, z \in X)$  と書く。  $\forall$  のかわりに  $\exists$  でも同様の省略を行なう。

## 1 二項関係

**例 1.1 ( $\mathbb{R}$  上の順序関係)** 任意の  $x, y \in \mathbb{R}$  に対し、 $x < y$  であるかどうか、定まっている。

**例 1.2 (相等関係)**  $A$  を集合とすると、任意の  $a, a' \in A$  に対し  $a = a'$  であるかどうか、定まっている。■

**例 1.3 (包含関係)** 集合  $A$  のべき集合  $2^A = \text{Pow}(A)$  の任意の2元  $B, C$  に対し、 $B \subset C$  であるかどうか、定まっている。■

**例 1.4 (整除)** 2つの整数  $a, b$  に対して、 $b = na$  を満たす整数  $n$  が存在するとき、 $b$  は  $a$  の倍数である、あるいは  $a$  は  $b$  の約数であるといい、 $a \mid b$  で表す。整数全体の集合  $\mathbb{Z}$  の2元  $a, b$  に対して、 $a \mid b$  であるかどうか、定まっている。■

このように、空でない集合  $X$  の任意の2元  $x, x'$  に対し、 $x \sim x'$  であるかどうか定まっているとき、 $\sim$  は  $X$  上の**二項関係** (binary relation) である、という。

例1.1では  $<$  は  $\mathbb{R}$  上の、例1.2では  $=$  は  $A$  上の、例1.3では  $\subset$  は  $2^A = \text{Pow}(A)$  上の、二項関係である。

**余談 1.5 (二項関係の集合の言葉を用いた定義)** 空でない集合  $X$  上の二項関係とは、 $X \times X$  の部分集合  $R$  のことである、と定義する。確かに  $R \subset X \times X$  とするとき、 $x \sim y \stackrel{\text{def.}}{\iff} (x, y) \in R$  とすると、(上で説明した意味での)  $X$  上の二項関係  $\sim$  が得られる。 $(x, y) \in R$  のことを  $x R y$  と表す場合もある:

$$x \sim y \iff (x, y) \in R \iff x R y.$$

集合  $R$  を二項関係  $\sim$  のグラフと呼ぶ。

例えば  $X = \{a, b, c\}$  ( $a, b, c$  はどの二つも相異なる),  $R = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$  とすると、

$$a R a, \quad b R b, \quad c R c, \quad b R c, \quad c R b$$

だけが成り立ち、他 (例えば  $a R b$ ) が成り立たない。■

## 2 同値関係

**定義 2.1 (同値関係)** 空でない集合  $X$  上の二項関係  $\sim$  が次の (1), (2), (3) をみたすとき、 $\sim$  を  $X$  上の同値関係 (equivalence relation) と呼ぶ。

(1)  $\forall x \in X$  に対し  $x \sim x$ . (反射律, reflexivity)

(2)  $\forall x, y \in X$  に対し  $x \sim y \Rightarrow y \sim x$ . (対称律, symmetry)

(3)  $\forall x, y, z \in X$  に対し  $x \sim y$  かつ  $y \sim z \Rightarrow x \sim z$ . (推移律, transitivity)

$x \sim y$  のとき、 $x$  と  $y$  は同値である、 $x$  は  $y$  に同値である、という。

**注意 2.2** 1 つの集合上にも複数の同値関係が存在しうる。次の 2 つの極端な同値関係が例となる。

**例 2.3 (自明な同値関係 (何とでも同値))** 任意の 2 元  $a, b \in A$  に対し  $a \sim b$  と定めると、この  $\sim$  は  $A$  上の同値関係である。■

**例 2.4 (相等関係 (自分だけと同値))** 任意の集合上で相等関係  $=$  は同値関係である。■

数学では非常に多くの同値関係が登場するが、ここでは簡単なものをいくつか紹介 (思い出し?) する。

**例 2.5 (図形の合同)** 2 つの平面図形  $A$  と  $B$  が合同  $A \cong B$  ( $A$  is congruent to  $B$ ,  $A$  を平行移動・回転・裏返しなどして  $B$  に“重ねられる”) という関係は同値関係である。(図形の合同を表す記号には世界標準がなく、日本の学校数学では  $A \equiv B$  と書くのが普通ですが、英語文化圏では  $A \cong B$  と書くのだそうです) ■

**例 2.6 (図形の相似)** 2 つの平面図形  $A$  と  $B$  が相似  $A \sim B$  ( $A$  is similar to  $B$ ,  $A$  をスケールアップ (拡大, 縮小)・平行移動・回転・裏返しなどして  $B$  に“重ねられる”) という関係は同値関係である。(図形の相似を表す記号には世界標準がなく、日本の学校数学では  $A \sim B$  と書くのが普通ですが、英語文化圏では  $A \sim B$  や  $A \parallel B$  と書くのだそうです。) ■

**例 2.7 (自然数  $n$  を法として合同)**  $n$  は自然数とする。整数全体の集合  $\mathbb{Z}$  上の同値関係  $\sim$  を次のように定める。

$$a, b \in \mathbb{Z} \text{ に対し、} a \sim b \stackrel{\text{def}}{\iff} a - b \text{ は } n \text{ の倍数.}$$

$a \sim b$  はしばしば  $a \equiv b \pmod{n}$  と書かれ、 $a$  と  $b$  は  $n$  を法として合同である ( $a$  and  $b$  are congruent modulo  $n$ ,  $a$  is congruent to  $b$  modulo  $n$ )、という。要するに、 $a$  と  $b$  は  $n$  で割った余りが等しいとき、そのときに限り  $a \sim b$ 。

この  $\sim$  が同値関係の 3 条件をみたすことを示す。

**証明**  $\forall a \in \mathbb{Z}$  に対して、 $a - a = 0 \cdot n$ ,  $0 \in \mathbb{Z}$  なので  $a \sim a$ 。ゆえに反射律が成り立つ。

$a \sim b$  とすると、 $(\exists j \in \mathbb{Z}) a - b = jn$ 。このとき  $b - a = (-j)n$ ,  $-j \in \mathbb{Z}$  であるから  $b \sim a$ 。ゆえに対称律が成り立つ。

$a \sim b$ ,  $b \sim c$  が成り立つ。 $(\exists j, j' \in \mathbb{Z}) a - b = jn$ ,  $b - c = j'n$ 。このとき  $a - c = (a - b) + (b - c) = (j + j')n$ ,  $j + j' \in \mathbb{Z}$  なので  $a \sim c$ 。ゆえに推移律が成り立つ。■

$a \equiv b \pmod{n}$ ,  $c \equiv d \pmod{n}$  とするとき、

$$a + c \equiv b + d \pmod{n}, \quad ac \equiv bd \pmod{n}$$

が成り立つ。実際  $(\exists k, \ell \in \mathbb{Z}) a - b = km, c - d = \ell m$  ならば、

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) = (k + \ell)m, \\ ac - bd &= ac - bc + bc - bd = (a - b)c + b(c - d) = kmc + b\ell m = (kc + b\ell)m, \\ k + \ell &\in \mathbb{Z}, \quad kc + b\ell \in \mathbb{Z}\end{aligned}$$

であるから。■

豆知識: TeX では、 $(\text{mod } n)$  を  $\backslash\text{pmod } n$  と入力する。

**例 2.8** (九去法)  $10 \equiv 1 \pmod{9}$  であるから、自然数  $n$  に対して、 $10^n \equiv 1 \pmod{9}$ .

$$\begin{aligned}123456789 &= 1 \times 10^8 + 2 \times 10^7 + 3 \times 10^6 + 4 \times 10^5 + 5 \times 10^4 + 6 \times 10^3 + 7 \times 10^2 + 8 \times 10 + 9 \\ &= 1 \times 1 + 2 \times 1 + 3 \times 1 + 4 \times 1 + 5 \times 1 + 6 \times 1 + 7 \times 1 + 8 \times 1 + 9 \\ &\equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 \equiv (1 + 8) + (2 + 7) + (3 + 6) + (4 + 5) + 9 \\ &\equiv 0 + 0 + 0 + 0 + 0 \equiv 0 \pmod{9}.\end{aligned}$$

これから 123456789 は 9 の倍数であることが分かる。同様に 987654321 も 9 の倍数である (数字をどう入れ替えても同じだ)。電卓のない時代、等式の両辺を 9 で割った余りを計算して比較することで、検算することがあった ( $a = b$  ならば  $a \equiv b \pmod{9}$  のはず)。9 で割った余りを求めるには、各桁の数字を足せばよいが、その際に 9 が現れたら、除去すればよい。その検算法を九去法と呼ぶ (らしい)。■

**例 2.9** “一般角” を考えたとき、 $2\pi$  の整数倍だけ違うものは同一視するのが便利なおことがある。  $x, y \in \mathbb{R}$  に対して

$$x \sim y \stackrel{\text{def.}}{\iff} (\exists n \in \mathbb{Z}) x - y = 2n\pi.$$

これが  $\mathbb{R}$  上の同値関係になることの証明は、例 2.7 と同様なので省略する。

例えば  $-\pi \sim \pi$ ,  $\frac{9\pi}{4} \sim \frac{\pi}{4}$ . また  $x \sim y$  ならば  $\cos x = \cos y$ ,  $\sin x = \sin y$ ,  $e^{ix} = e^{iy}$ . ■

**例 2.10** 写像  $f: X \rightarrow Y$  が与えられたとき、 $x \sim y \iff f(x) = f(y)$  により  $\sim$  を定める。この  $\sim$  は  $X$  上の同値関係である。

**証明**  $\forall x \in X$  に対して、 $f(x) = f(x)$  より  $x \sim x$ .

$x, y \in X$  に対して、 $x \sim y$  が成り立つとする。  $f(x) = f(y)$  であるから、 $f(y) = f(x)$  なので、 $y \sim x$ . ゆえに対称律が成り立つ。

$x, y, z \in X$  に対して、 $x \sim y$  かつ  $y \sim z$  とする。  $f(x) = f(y)$  かつ  $f(y) = f(z)$  であるから、 $f(x) = f(z)$ . ゆえに  $x \sim z$ . ゆえに推移律が成り立つ。■

**問 1** ある人が「対称律があれば、 $x \sim y$  とするとき、 $y \sim x$ . ここで推移律を用いると  $x \sim x$  が導かれる。だから同値関係の定義で反射律は実は余分である。」と言った。正しいだろうか？

### 3 同値類と商集合

**定義 3.1 (同値類)**  $\sim$  を集合  $X$  上の同値関係とする。 $x \in X$  に対して

$$C(x) := \{y \in X \mid y \sim x\}$$

を  $x$  の (属する) **同値類** (the equivalence class to which  $x$  belongs, the equivalence class of  $x$ ) と呼ぶ。

同値関係を明示して、 $x$  の同値関係  $\sim$  についての同値類 (the equivalence class of  $x$  with respect to the equivalence relation  $\sim$ )、 $x$  の  $\sim$  同値類 (the  $\sim$  equivalence class of  $x$ ) と呼ぶこともある。

$C(x)$  のことを  $[x]$  や  $[x]_{\sim}$  で表すことも多い。

$C(x)$  は  $X$  の部分集合である ( $C(x) \subset X$ ,  $C(x) \in 2^X$ )。

**例 3.2 (3 を法として合同という同値関係の同値類)** (後でもっときちんとやるけれど、先走って例を)  $\mathbb{Z}$  上の同値関係  $\sim$  を  $a \sim b \Leftrightarrow a \equiv b \pmod{3}$  で定めるとき、 $C(0) = \{3m \mid m \in \mathbb{Z}\}$  (3 の倍数全体),  $C(1) = \{3m + 1 \mid m \in \mathbb{Z}\}$  (3 で割って 1 余る数の全体),  $C(2) = \{3m + 2 \mid m \in \mathbb{Z}\}$  (3 で割って 2 余る数の全体),  $C(3) = C(0)$ ,  $C(4) = C(1)$ , 逆方向に  $C(-1) = C(2)$ ,  $C(-2) = C(1)$  ( $C(x)$  は  $x$  との差が 3 の倍数であるもの全体と考えると良い)。結局、相異なる同値類は  $C(0)$ ,  $C(1)$ ,  $C(2)$  の 3 つだけである。■

**例 3.3 (平面のベクトル)** 平面上の線分があるとき、どちらかの端点を「始点」と呼び、もう一方 (「終点」と呼ぶ) と区別したものを**有向線分**という。A を始点、B を終点とする有向線分を「有向線分 AB」と呼び、 $\overrightarrow{AB}$  と表す。X を平面上の有向線分の全体として、X 上の二項関係  $\sim$  を

$$\overrightarrow{AB} \sim \overrightarrow{CD} \quad \text{def} \quad \text{“}\overrightarrow{AB} \text{ を平行移動すると } \overrightarrow{CD} \text{ に重なる”}$$

で定めたとき、 $\sim$  は同値関係になる。この同値関係に関する同値類のことを**平面のベクトル**と呼ぶ。■

—— 高校数学の教科書 (数研出版) から ——

有向線分は位置と、向きおよび大きさで定まる。その位置を問題にしないで、向きと大きさだけで定まる量を**ベクトル**という。

**補題 3.4**  $X$  は集合で、 $\sim$  は  $X$  上の同値関係とする。

(1)  $\forall x \in X$  に対して、 $x \in C(x)$ . (ゆえに  $C(x) \neq \emptyset$  である。)

(2)  $\forall x, y \in X$  に対して、次の3条件は互いに同値である。

(i)  $x \sim y$ .

(ii)  $C(x) = C(y)$ .

(iii)  $C(x) \cap C(y) \neq \emptyset$ .

(3)  $\forall x, y \in X$  に対して、次の3条件は互いに同値である。

(i)  $x \not\sim y$ .

(ii)  $C(x) \neq C(y)$ .

(iii)  $C(x) \cap C(y) = \emptyset$ .

**証明** まず、 $\forall x, y \in X$  に対して、 $y \in C(x) \Leftrightarrow y \sim x$  を注意しておく。

(1) 反射律  $x \sim x$  より  $x \in C(x)$ .

(2) (i)  $\Rightarrow$  (ii) を示す。 $x \sim y$  と仮定する。 $C(x) \subset C(y)$  を示そう。 $z \in C(x)$  とすれば  $z \sim x$ , それと  $x \sim y$  より  $z \sim y$ . ゆえに  $z \in C(y)$ . よって  $C(x) \subset C(y)$ . 対称律により  $y \sim x$  が成り立つので (まったく同様に)  $C(y) \subset C(x)$ . よって  $C(x) = C(y)$ .

(ii)  $\Rightarrow$  (iii) を示す。 $C(x) = C(y)$  と仮定すると、 $C(x) = C(x) \cap C(y)$ . (1) より  $C(x) \neq \emptyset$  であるから、 $C(x) \cap C(y) \neq \emptyset$ .

(iii)  $\Rightarrow$  (i) を示す。 $C(x) \cap C(y) \neq \emptyset$  と仮定すると、 $z \in C(x) \cap C(y)$  を満たす  $z$  が存在する。このとき  $z \sim x$  かつ  $z \sim y$  なので、(対称律と推移律を用いて)  $x \sim y$ .

(3) これは (2) の対偶である。■

**命題 3.5 (部屋分け, 類別)** 集合  $X$  上の同値関係  $\sim$  に対し

$$X = \bigcup_{x \in X} C(x),$$

また

$$(\forall x \in X)(\forall y \in X) \quad (C(x) = C(y)) \vee (C(x) \cap C(y) = \emptyset)$$

が成り立つ。

授業では、集合  $X$  を分割した図を板書すること。各クラスは同じ大きさであるとは限らない。 $x$  と同じクラスに  $y$  があり、違うクラスに  $y'$  があり、 $C(x) = C(y)$ ,  $C(x) \neq C(y')$ ,  $C(x) \cap C(y') = \emptyset$  と書いておく。

**証明**  $\forall x \in X$  に対して、 $C(x) \subset X$  であるから、 $\bigcup_{x \in X} C(x) \subset X$ . 一方、 $\forall x' \in X$  に対して、

$x' \in C(x')$  であるから、 $x' \in \bigcup_{x \in X} C(x)$ . ゆえに  $X \subset \bigcup_{x \in X} C(x)$ .

後半は、まず明らかに「 $(C(x) = C(y) \text{ または } C(x) \neq C(y))$ 」で、前命題 (3) の (ii)  $\Leftrightarrow$  (iii) により、 $C(x) \neq C(y) \Leftrightarrow C(x) \cap C(y) = \emptyset$ . ■

**定義 3.6 (商集合)** 集合  $X$  と、 $X$  上の同値関係  $\sim$  があるとき、同値類全体の集合

$$X/\sim := \{C(x) \mid x \in X\}$$

を  $X$  の  $\sim$  による**商集合** (the quotient set of  $X$  by  $\sim$ ) と呼ぶ。

各  $x \in X$  に  $C(x) \in X/\sim$  を対応させることで定まる写像

$$q: X \rightarrow X/\sim, \quad q(x) = C(x) \quad (x \in X)$$

を**商写像** (quotient map) あるいは**標準的全射** (canonical surjection) と呼ぶ。  $q$  を  $X/\sim$  への**標準的射影** (the canonical projection map to  $X/\sim$ ) と呼び、  $\pi$  と書くことも多い。

$C \in X/\sim$  に対して、  $C = C(x)$  を満たすような  $x$  を  $C$  の**代表元** (a representative of  $C$ ) と呼ぶ。

$\forall x \in X$  に対して、  $C(x) \subset X$  すなわち  $C(x) \in 2^X$  であるから、  $X/\sim \subset 2^X$  である。

$C$  の「代表元」 $x$  というと、何か特別なニュアンスを感じる人がいるかもしれないが、  $C = C(x)$  さえ満たすならば、  $x$  は  $C$  の代表元と呼ばれる (何でも構わない)。英語では the representative でなくて a representative であることに注意。

**例 3.7 (クラス分け)**  $X = 2014$  年度明治大学現象数理学科 1 年生全体の集合 とする。2 つの組があって、“1 組” には T.K. 君、K.S. 君、…がいる。“2 組” には T.T. 君、T.F. 君、…がいる。  $x \sim y$  を  $x$  と  $y$  は同じ組に属することと定義する。  $\sim$  は  $X$  上の同値関係である。  $C(\text{T.K. 君}) = C(\text{K.S. 君})$ ,  $C(\text{T.T. 君}) = C(\text{T.F. 君})$  はともに  $X$  の部分集合である。それぞれ 1 組、2 組という名前がついている。組を指定するには、誰でも良いから所属する学生を一人選べば良い。T.F. 君の所属する組と言え、2 組のことであると分かる。

$$1 \text{ 組} \neq 2 \text{ 組}, \quad 1 \text{ 組} \cap 2 \text{ 組} = \emptyset, \quad 1 \text{ 組} \cup 2 \text{ 組} = X.$$

$$X/\sim = \{1 \text{ 組}, 2 \text{ 組}\}. \blacksquare$$

次の例は、その例自体が応用上重要であるだけでなく、代数系 (群、環、 $R$  加群、多元環、線型空間、…) を何かで割って別の代数系を作る、という非常に基本的かつ重要な操作の例としても重要である。

**例 3.8 ( $n$  を法とする剰余系)**  $n$  を自然数とする。  $\mathbb{Z}$  上の同値関係  $a \sim b \Leftrightarrow a - b$  は  $n$  の倍数、を考える。  $\mathbb{Z}$  の  $\sim$  による商集合を  $\mathbb{Z}/n$  と表す。また  $a$  の属する同値類  $C(a)$  を  $[a]$  と表す。  $[a]$  を、  $n$  を法とする**剰余類** (residue class modulo  $n$ ) という。このとき

$$\mathbb{Z}/n = \{[0], [1], \dots, [n-1]\}$$

である。  $\mathbb{Z}/n$  を  $n$  を法とする**剰余系** (complete residue system) あるいは、  $n$  を法とする**剰余類環** (residue class ring modulo  $n$ ) という。

具体的に、  $n = 3$  の場合を書いてみると

$$\mathbb{Z}/3 = \{[0], [1], [2]\},$$

$$[0] = \{x \in \mathbb{Z} \mid x \sim 0\} = \{3j \mid j \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{x \in \mathbb{Z} \mid x \sim 1\} = \{3j + 1 \mid j \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{x \in \mathbb{Z} \mid x \sim 2\} = \{3j + 2 \mid j \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

さらに  $\mathbb{Z}/n$  の任意の 2 元  $A, B$  に対し、それぞれ代表元  $a, b$  を取って (つまり  $A = [a]$ ,  $B = [b]$ ) となるような  $a, b$ 、

- 和 :  $A + B := [a + b]$ ,
- 積 :  $A \cdot B := [ab]$

と定義する。  $A, B$  に対して  $A = [a], B = [b]$  となる  $a, b$  の取り方は (一般には) 複数ありえるので、  $[a + b]$  と  $[ab]$  が取り方によらずに定まることを確認する必要がある。このようなことは非常にしばしば生じるので、「 $A + B, A \cdot B$  は well-defined である」と言うことになっている。

(その証明)  $A = [a] = [a'], B = [b] = [b']$  であるならば

$$[a + b] = [a' + b'], \quad [ab] = [a'b']$$

を示せばよい。  $a - a' = in, b - b' = jn$  とすれば

$$(a + b) - (a' + b') = (i + j)n,$$

また

$$ab - a'b' = (a - a')b + a'(b - b') = ibn + a'jn = (ib + a'j)n$$

であるから、  $a + b \sim a' + b', ab \sim a'b'$ . ゆえに  $[a + b] = [a' + b'], [ab] = [a'b']$ . ■

$\mathbb{Z}/3$  では、

$$\begin{aligned} [0] + [0] &= [0], & [0] + [1] &= [1] + [0] = [1], & [0] + [2] &= [2] + [0] = [2], \\ [1] + [1] &= [2], & [1] + [2] &= [2] + [1] = [0], \\ [2] + [2] &= [1]. \end{aligned}$$

$$\begin{aligned} [0] \cdot [0] &= [0], & [0] \cdot [1] &= [1] \cdot [0] = [0], & [0] \cdot [2] &= [2] \cdot [0] = [0], \\ [1] \cdot [1] &= [1], & [1] \cdot [2] &= [2] \cdot [1] = [2], \\ [2] \cdot [2] &= [1]. \end{aligned}$$

$\mathbb{Z}/n$  は和、差、積が定義できるが、商は一般には定義されない。  $n$  が素数であるときは  $[0]$  以外の同値類で割る商も定義され、  $\mathbb{Z}/n$  は体となる。

**命題 3.9**  $p$  を素数、  $m$  は  $p$  の倍数でないとする。このとき  $km + lp = 1$  をみたす整数  $k, l$  が存在する。(実は仮定を「 $m$  と  $p$  が互いに素ならば」と弱く出来る。)

**証明**  $\mathbb{Z}/p$  で  $p$  個の元  $[0], [m], [2m], \dots, [(p-1)m]$  を考えると、これらはすべて相異なる元である。実際、もしある  $0 \leq i < j \leq p-1$  について  $[im] = [jm]$  が成り立つとすると  $(j-i)m = kp$  をみたす  $k \in \mathbb{Z}$  が存在するが、  $j-i \in \{1, \dots, p-1\}$  と  $m$  はともに  $p$  の倍数ではないので矛盾する。

したがって  $[km] = [1]$  となる  $k$  ( $1 \leq k \leq p-1$ ) が存在する。このとき  $km - 1$  が  $p$  の倍数となるので  $km + lp = 1$  をみたす  $l \in \mathbb{Z}$  が存在する。 ■

**注意 3.10** (1)  $p$  が素数でなくても、  $p$  と  $m$  が互いに素 (最大公約数が 1) であれば、  $km + lp = 1$  をみたす整数  $k, l$  は存在する。(以下余談) これは通常はユークリッドの互除法を用いて証明される。高等学校の新課程では数学 A の「整数の性質」で学ぶことになっている。一般に与えられた整数  $m$  と  $p$  に対して、  $m$  と  $p$  の最大公約数  $d$  と、  $km + lp = d$  を満たす整数  $k, l$  を求めることは重要で、Mathemaitca ではそれを計算するための関数 `ExtendedGCD[]` が用意されている。 `ExtendedGCD[m,p]` とすると、  $m$  と  $p$  の公約数  $d$  と  $km + lp = d$  を満たす整数  $k, l$  が  $\{d, \{k, l\}\}$  というリストで返される。

(2) 上の命題により  $p$  が素数のとき  $\mathbb{Z}/p$  の  $[0]$  でない任意の元  $[m]$  は  $[k][m] = [1]$  をみたす元  $[k]$  を持つ (積の逆元) ことが分かった。結局  $[0]$  でない任意の元で割算が出来る。このような代数系を **体** (field) という。すなわち  $\mathbb{Z}/p$  は (有限) 体である。■

**問 2**  $\mathbb{Z}/5$  の  $[0]$  以外の元  $[1], [2], [3], [4]$  について、それぞれ積の逆元を求めよ。

## 解答コーナー

**問 1 の解説** 正しくない。注目している  $x$  に対して、 $x \sim y$  となる  $y$  が存在することは仮定されていない。極端な例として、空でない集合  $X$  の任意の二元  $x, y$  に対して、 $x \sim y$  は成り立たない、として定義される二項関係  $\sim$  は、推移律と対称律を満たすが、反射律は満たさない。あるいは  $X = \{a, b\}$  上の二項関係  $\sim$  を  $b \sim b$  だけ真、他はすべて偽 ( $a \not\sim a, a \not\sim b, b \not\sim a$ ) としても、対称律と推移律は満たされるが、反射律は満たされない。■

## 参考文献



## 索引

商写像, 6

商集合, 6

剰余類, 6

体, 8

代表元, 6

同値関係, 2

同値類, 4

二項関係, 1

標準的全射, 6

べくとるベクトル, 4

有向線分, 4