by Dr. Taro

"余り"の数学

review　$n \in \mathbb{N}$, $n \geq 2$

$\exists k \in \mathbb{Z}$ s.t. $x, y \in \mathbb{Z}$,　$x - y = n \cdot k \Leftrightarrow x \sim y$

定理　～は同値関係である

(0) $x \sim y \wedge x \not\sim y$

(1) $x \sim x$

(2) $x \sim y \Rightarrow y \sim x$

(3) $x \sim y \wedge y \sim z$
$\Rightarrow x \sim z$

(0) 明らか，(1) $x - x = 0$ より成立.

(2) $x \sim y \Rightarrow x - y = n \cdot k \Rightarrow y - x = -n \cdot k$

$\therefore y \sim x$　($\exists (-m) \in \mathbb{Z}$ s.t. $x, y \in \mathbb{Z}$, $y - x = -n \cdot k$)

(3) $\exists m \in \mathbb{Z}$ s.t. $x \sim y \Rightarrow x - y = nk$

$\exists m \in \mathbb{Z}$ s.t.

$y \sim z = y - z = mk$

$x - y + y - z = (n + m)k$

$\Rightarrow x - z = (n+m)k$

$\therefore x \sim z$

$x, y \in \mathbb{Z}$,　$x \sim y$ のとき

x と y は $n \in \mathbb{N}$ を法として合同といい，$x \equiv y \pmod{n}$ と書く

$x \in \mathbb{Z}$

$y \equiv x \pmod{n} \Leftrightarrow y - x = nk$　$(n \in \mathbb{N}, k \in \mathbb{Z})$

$\Leftrightarrow y = x + n \cdot k$ となる $\exists k \in \mathbb{Z}$

$[x] = \{ y \in \mathbb{Z} \mid y = n \cdot k + x$ となる $k \in \mathbb{Z}$ が存在する $\}$

一方，$x \in \mathbb{Z}$ に対し，$x = n \cdot k + r$,　$k, r \in \mathbb{Z}$, $0 \leq r < n$

$\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$

$0 \leq r, r' < n$ かつ $r \neq r' \Rightarrow [r] \cap [r'] = \phi$

従って $\mathbb{Z}/\sim \; = \{ [0], [1], \cdots, [n-1] \}$

$\mathbb{Z}/\sim$ を $\mathbb{Z}/n\mathbb{Z}$,　$\mathbb{Z}/n$,　$\mathbb{Z}_n$ のようにも書いたりする

つまり $\forall x \in \mathbb{Z}$,

$[x] = [r]$

$x \equiv r \pmod{n}$

となる $0 \leq r < n$

一方で $0 \leq r, r' < n$ が

$r \neq r'$ のとき

$r \not\equiv r' \pmod{n}$

$\Rightarrow [r] \cap [r'] = \phi$

~ $\mathbb{Z}/n\mathbb{Z}$ ~

$\mathbb{Z}$ 上の演算に関する性質

和, 積 に関して次をみたす.

(R1) $x, y \in \mathbb{Z}$ に対して和 $x+y \in \mathbb{Z}$ が定まり次をみたす.

$x, y, z \in \mathbb{Z}$

(R1-1) $x+y = y+x$

(R1-2) $x+(y+z) = (x+y)+z$

(R1-3) $\exists\, 0 \in \mathbb{Z}$ $\forall x \in \mathbb{Z}$, $0+x = x+0 = x$

(R1-4) $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$ s.t. $y+x = x+y = 0$

(この $y = -x$ とかかれる)

このとき, $x, y \in \mathbb{Z}$ に対して $x-y = x+(-y)$ として引き算を def. する.

(R2) $x, y \in \mathbb{Z}$, 積 $x \cdot y \in \mathbb{Z}$ が定まり次をみたす.

(R2-1) $x \cdot y = y \cdot x$

(R2-2) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(R2-3) 0とは異なる $\exists\, 1 \in \mathbb{Z}$ s.t. $1 \cdot x = x \cdot 1 = x$

(R3) $x, y, z \in \mathbb{Z}$

$x \cdot (y+z) = x \cdot y + x \cdot z$

$(x+y) \cdot z = x \cdot z + y \cdot z$

$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ も環 (R1)〜(R3) をみたすことを確認せよ.}}$

function space

これらの性質 (R1)−(R3) は $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathrm{Map}(A, \mathbb{R})$

$\mathrm{Map}(A, \mathbb{R}) = \{ f \mid f : A \to \mathbb{R} \}$

$f, g \in \mathrm{Map}(A, \mathbb{R})$

$(f+g)(x) := f(x) + g(x) \quad (x \in A)$

$(fg)(x) := f(x) \cdot g(x) \quad (x \in A)$

(R2-1) ↓ とくに

$\Leftrightarrow$ R1〜R3 をみたす集合 R 環 cR 可換環

— 環であること —

$[a], [b] \in \mathbb{Z}/n\mathbb{Z}$

$[a]+[b] = [a+b]$

$[a]\cdot[b] = [a\cdot b]$ と def. したい。

well-defined であること。

$[a]=[c]$, $[b]=[d]$ のときを

・ $[a+b] = [c+d]$

・ $[a\cdot b] = [c\cdot d]$ を確かめる必要がある。

$a \equiv c \pmod{n} \land b \equiv d \pmod{n}$

$[a+b] = [c+d]$, つまり $a+b \equiv c+d \pmod{n}$

$[a\cdot b] = [c\cdot d]$, $a\cdot b \equiv c\cdot d \pmod{n}$

(1) $a \equiv c \pmod{n} \land b \equiv d \pmod{n}$

$\Leftrightarrow$ $a-c = n\cdot k \land b-d = n\cdot l$

$(k, l \in \mathbb{Z})$

$(a+b)-(c+d) = n(k+l) \Rightarrow [a+b]=[c+d]$

(2) $a\cdot b - c\cdot d = (a\cdot b - a\cdot d) + (a\cdot d - c\cdot d)$

$= a(b-d) + (a-c)d$

$= a\cdot n\cdot l + n\cdot k\cdot d$

$= n(a\cdot l + k\cdot d)$ (nの整数)

$\therefore [a \cdot b] = [c \cdot d]$ // (well-defined)

(R1-1) $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$

$$[a]+[b] = [a+b]$$
$$= [b+a] \quad (\mathbb{Z}\text{の性質})$$
(R1-1) に対する
$$= [b]+[a]$$

(R2-1)も同様!

$[a],[b],[c] \in \mathbb{Z}/n\mathbb{Z}$

$$[a]+([b]+[c]) = [a]+([b+c])$$
$$= [a+(b+c)]$$
$$= [(a+b)+c]$$
$\mathbb{Z}$に対する結合律 (R1-2)
$$= [a+b]+[c]$$
(R2-2)
$$= ([a]+[b])+[c]$$
(R2-2)も同様.

(R3) $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$

$$[a]\cdot([b]+[c])$$
$$= [a]\cdot[b+c]$$
$$= [a(b+c)]$$
$$= [ab+ac]$$
$\mathbb{Z}$に関する(R3)
$$= [ab]+[ac]$$
後半は (R2-1) より わかる.
$$= [a][b]+[a][c]$$

和の単位 $[0]$ の存在.

(R1-3) $[0] \in \mathbb{Z}/n\mathbb{Z}$ $(0 \in \mathbb{Z})$

$$[a] + [0] = [a+0] \underset{\mathbb{Z}\text{の}0\text{のdef}}{=} [a]$$

(R1-4) $[a] \in \mathbb{Z}/n\mathbb{Z}$ $(a \in \mathbb{Z})$

$\mathbb{Z}$ に対する (R1-4) より $\exists (-a) \in \mathbb{Z}$

$[-a] \in \mathbb{Z}/n\mathbb{Z}$ を考える.

$$[a] + [-a] = [a + (-a)] \underset{\mathbb{Z}\text{の演算}}{=} [0]$$

$$[-a] + [a] = [-a+a] = [0]$$

(これより $-[a] = [-a]$)

乗法単位の存在.

(R2-3) $[1] \in \mathbb{Z}/n\mathbb{Z}$ $(1 \in \mathbb{Z})$

$$[a] \cdot [1] = [a \cdot 1] \underset{\varphi}{=} [a]$$

$\mathbb{Z}$ 演算 $\mathbb{Z}$ の (R2-3)

$$[1] \cdot [a] = [a]$$

//

$\mathbb{Z}/n\mathbb{Z}$ は可換環 //

整数に無い性質.

例えば 整数 $x, y \in \mathbb{Z}$ について

(a) $x \cdot y = 0 \Rightarrow x = 0 \wedge y = 0$

(b) $x \cdot y = 1 \Rightarrow x = y = 1 \wedge x = y = -1$

一方で, 例えば $n = 10$ のとき $\mathbb{Z}/10\mathbb{Z}$ において

(a) $[2] \neq [0]$, $[5] \neq [0]$

$[2] \cdot [5] = [0]$ $(= [10])$

(b) $[3], [7]$ に対して $[3] \cdot [7] = [21] = [1]$

$n =$ prime でないとき, (a) のようなことが生じる

<u>定理</u>

$\mathbb{Z}/n\mathbb{Z}$ において

$0 < m \leq n$ なる $m \in \mathbb{Z}$ を考える

(1) m と n の最大公約数 d が $d \geq 2$

$\Leftrightarrow$ $[m] \cdot [k] = [0]$ となるような

$[k]$ $(\neq [0]) \in \mathbb{Z}/n\mathbb{Z}$ が存在する

(2) $d = 1$ のとき $[m] \cdot [k] = [1]$ となる $[k] \in \mathbb{Z}/n\mathbb{Z}$

が存在する.

n が 素数 p のとき

$0 < m < p$ なる m に対して

m と p の最大公約数は 1 なので

次が成り立つ.

<u>定理</u> p = prime #.

$[m] \in \mathbb{Z}/p\mathbb{Z}$, $[m] \neq [0]$

このとき, (2) より $\exists \underset{\in \mathbb{Z}/p\mathbb{Z}}{[k]}$ s.t. $[m][k] = 1$

$\mathbb{Q}$, $\mathbb{R}$ と同様に 逆数が $\mathbb{Z}/p\mathbb{Z}$ に
存在する.

in general,

Set K, $\exists$sum, $\exists$prod (R1)~(R3)

$(K, \subset \mathbb{R})$ (R2-4) $0 \in K$ 以外の

すべての $x \in K$ に対して $x \cdot y = y \cdot x = 1$

となる y が存在する. field

K を <u>体</u> という.

著しい性質. $\mathbb{Q}, \mathbb{C}, \mathbb{R}$ ⤳ 無限こ

$\mathbb{Z}/p\mathbb{Z}$ ~ p こしかない

$\mathbb{Z}/p\mathbb{Z}$ は $\mathbb{F}_p$ と書かれる

で「体」を意識したとき.

($d \geq 2 \Rightarrow [m] \cdot [k] = [0]$
となる non-zero $[k]$ が存在.)
$\in \mathbb{Z}/m\mathbb{Z}$

d は m と n の最大公約数

$$m = d \cdot m_1, \quad n = d \cdot n_1 \quad (m_1, n_1 \in \mathbb{N})$$

$$m \cdot n_1 = d\, m_1 \cdot n_1 = m_1\, d\, n_1 = m_1 n$$

$$m \cdot n_1 + (-m_1) \cdot n = 0$$

$$[m][n_1] + [-m_1]\underbrace{[n]}_{[0]} = [0]$$

$$\Rightarrow [m][n_1] = [0] \qquad \boxed{0 < n_1 < n}$$

$$[m] \neq [0], \quad [n_1] \neq [0]$$

// $d \geq 2$ がきいてる