

## §4. 整数の合同に関する剰余集合

2 以上の自然数  $m$  を固定する。 $m$  で割ったときに余りが  $r$  ( $r \in \{0, 1, \dots, m-1\}$ ) となる整数をすべて集めてきて得られる  $\mathbb{Z}$  の部分集合を  $m$  による  $r$  の剰余類と呼ぶ。 $m$  による剰余類をすべて集めた集合— $m$  を法とする剰余集合—には和と積が定義され、 $\mathbb{Z}$  における和と積と類似の性質を持つ。ここでは、このような剰余集合の性質を考察する。

### ● 4-1 : 整数の $m$ を法とする剰余集合

2 以上の自然数  $m$  と  $a \in \mathbb{Z}$  に対して、 $\mathbb{Z}$  の部分集合

$$[a]_m = \{ x \in \mathbb{Z} \mid x \equiv a \pmod{m} \}$$

を  $m$  による  $a$  の剰余類 (residue class) という。 $m$  による剰余類をすべて集めてきた集合を  $\mathbb{Z}/m\mathbb{Z}$  と書き、 $\mathbb{Z}$  の  $m$  を法とする剰余集合と呼ぶ：

$$\mathbb{Z}/m\mathbb{Z} = \{ [a]_m \mid a \in \mathbb{Z} \}.$$

#### 補題 4-1-1

$m$  を 2 以上の整数とする。 $a, b \in \mathbb{Z}$  に対して次が成り立つ。

- (1)  $[a]_m = [b]_m \iff a \equiv b \pmod{m}$ .  
 (2)  $\mathbb{Z}/m\mathbb{Z} = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$ .

(証明)

(1) 「 $\implies$ 」の証明：[補題 3-2-1(i)] より  $a \in [a]_m = [b]_m$  であるから、 $a \equiv b \pmod{m}$  となる。

「 $\impliedby$ 」の証明：任意に  $x \in [a]_m$  をとると、 $x \equiv a \pmod{m}$  である。これと  $a \equiv b \pmod{m}$  から  $x \equiv b \pmod{m}$  を得る ([補題 3-2-1(iii)]). したがって、 $x \in [b]_m$  であり、 $[a]_m \subset [b]_m$  が示された。 $[a]_m \supset [b]_m$  は [補題 3-2-1(ii),(iii)] を用いて示されるので、 $[a]_m = [b]_m$  を得る。

(2)  $Q = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$  とおくと、剰余集合の定義から、 $Q \subset \mathbb{Z}/m\mathbb{Z}$  である。 $\mathbb{Z}/m\mathbb{Z} \subset Q$  を示す。 $C \in \mathbb{Z}/m\mathbb{Z}$  を任意にとる。 $C = [a]_m$  ( $a \in \mathbb{Z}$ ) と書くことができる。除法の原理から、 $a = qm + r$  ( $0 \leq r < m$ ) を満たす  $q, r \in \mathbb{Z}$  が存在する。このとき、 $a \equiv r \pmod{m}$  となる。よって、(1) により、 $C = [a]_m = [r]_m \in Q$  である。□

**例 4-1-2**  $m = 2$  のとき、 $[0]_2 = \{ 2n \mid n \in \mathbb{Z} \}$ ,  $[1]_2 = \{ 2n+1 \mid n \in \mathbb{Z} \}$  であり、 $[0]_2 = [2]_2$ ,  $[1]_2 = [-1]_2$  である。また、 $\mathbb{Z}/2\mathbb{Z} = \{ [0]_2, [1]_2 \}$  である。

### ● 4-2 : 整数の剰余集合における和と積

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  に和と積が定義されるように、剰余集合  $\mathbb{Z}/m\mathbb{Z} = \{ [a]_m \mid a \in \mathbb{Z} \}$  にも和と積を定めることができる。ここでは、その定義の仕方を説明しよう。

任意の  $C, D \in \mathbb{Z}/m\mathbb{Z}$  に対して、 $C = [a]_m$ ,  $D = [b]_m$  となる代表元  $a, b \in \mathbb{Z}$  をとり、

$$C + D := [a + b]_m, \quad CD := [ab]_m$$

によって定める。 $C + D$  と  $CD$  は  $C, D$  の代表元の選び方によらない。実際、 $C = [a']_m$ ,  $D = [b']_m$  でもあったとすると、[補題 4-1-1] により  $a \equiv a' \pmod{m}$ ,  $b \equiv b' \pmod{m}$  となる。[補題 3-2-2] から

$$a + b \equiv a' + b' \pmod{m}, \quad ab \equiv a'b' \pmod{m}$$

がわかるので、再び [補題 4-1-1] により、 $[a + b]_m = [a' + b']_m$ ,  $[ab]_m = [a'b']_m$  が従う。こうして、任意の  $C, D \in \mathbb{Z}/m\mathbb{Z}$  に対して、 $C + D, CD \in \mathbb{Z}/m\mathbb{Z}$  が矛盾なく定義されている (well-defined) ことがわかる。 $C + D, CD$  をそれぞれ  $C$  と  $D$  の和、積という。

**例 4-2-1**  $\bar{0} = [0]_2, \bar{1} = [1]_2$  とおき、和の表と積の表を作ると次のようになる。

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

×	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

但し、左の表は、 $\bar{a}, \bar{b}$  をそれぞれ各表の縦、横に並ぶ  $\mathbb{Z}/2\mathbb{Z}$  の元とすると、縦と横の交わる部分に  $\bar{a} + \bar{b}, \bar{a}\bar{b}$  を書き入れて作られている。

**演習 4-1\***  $\bar{a} = [a]_4$  ( $a = 0, 1, 2, 3$ ) とおき、 $\mathbb{Z}/4\mathbb{Z}$  における和と積の表を作成せよ。

● **4-3 :  $\mathbb{Z}/m\mathbb{Z}$  の和と積の性質**

$\mathbb{Z}/m\mathbb{Z}$  の和 (加法)、積 (乗法) は、以下のように、 $\mathbb{Z}$  の和、積と類似の性質を持っている。

- (a) 任意の  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/m\mathbb{Z}$  に対して、
  - (i) **結合法則** :  $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c}), (\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$ .
  - (ii) **交換法則** :  $\bar{a} + \bar{b} = \bar{b} + \bar{a}, \bar{a}\bar{b} = \bar{b}\bar{a}$ .
  - (iii) **分配法則** :  $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}, (\bar{a} + \bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c}$ .
- (b) **0 の存在** :  $\bar{0} := [0]_m$  と定めると、任意の  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  に対して、
 
$$\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}.$$
- (c) **1 の存在** :  $\bar{1} = [1]_m$  と定めると、 $\bar{1} \neq \bar{0}$  であって、任意の  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  に対して、
 
$$\bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1}.$$
- (d) **マイナス元** の存在 : 任意の  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  に対して、その代表元  $a \in \mathbb{Z}$  を1つとり、 $-\bar{a} = [-a]_m \in \mathbb{Z}/m\mathbb{Z}$  と定めると、
 
$$\bar{a} + (-\bar{a}) = (-\bar{a}) + \bar{a} = \bar{0}.$$

**注意 1** : (d) において、 $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  のマイナス元  $-\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  を、 $\bar{a}$  の代表元  $a$  を1つとって、 $-\bar{a} = [-a]_m$  として定めた。この  $-\bar{a}$  は、[補題 3-2-2] により、 $\bar{a}$  の代表元  $a$  の選び方に関係なく定まっている。

**注意 2** :  $\mathbb{Z}/m\mathbb{Z}$  の和は、上記のように、 $\mathbb{Z}$  の和と同じ性質を持つ。しかし、積に関しては  $\mathbb{Z}/m\mathbb{Z}$  と  $\mathbb{Z}$  とで次の点で異なる。それは、 $\mathbb{Z}$  における積は、**簡約法則** 「 $c \neq 0, ac = bc \Rightarrow a = b$ 」を満たす一方、 $\mathbb{Z}/m\mathbb{Z}$  における積はこれを満たすとは限らない (演習 4-1) という点である。実は、

$$\mathbb{Z}/m\mathbb{Z} \text{ における積が簡約法則を満たす} \iff m \text{ は素数}$$

が成立する (下の [命題 4-4-1] を参照)。

● **4-4 :  $\mathbb{Z}/m\mathbb{Z}$  の可逆元**

$\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  に対して、 $\bar{a}\bar{x} = \bar{1}$  となる  $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$  が存在するとき、 $\bar{a}$  は ( $\mathbb{Z}/m\mathbb{Z}$  の乗法に関する) **可逆元** (invertible element)、あるいは、**単元** (unit) であるという。また、この  $\bar{x}$  を  $\bar{a}$  の (乗法に関する) **逆元** (inverse element) という。 $\mathbb{Z}/m\mathbb{Z}$  のどのような元が可逆元になるのかは、次の命題により簡単に知ることができる。

**命題 4-4-1**

$m$  を 2 以上の整数とする。 $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  とし、 $a \in \mathbb{Z}$  をその代表元 (すなわち、 $\bar{a} = [a]_m$ ) とするとき、次が成り立つ :

$$\bar{a}\bar{x} = \bar{1} \text{ となる } \bar{x} \in \mathbb{Z}/m\mathbb{Z} \text{ が存在する} \iff \gcd(a, m) = 1.$$

(証明)

[系 3-5-2] により、 $\gcd(a, m) = 1$  であることと  $ax \equiv 1 \pmod{m}$  となる  $x \in \mathbb{Z}$  が存在することとは同値である。 $ax \equiv 1 \pmod{m}$  となる  $x \in \mathbb{Z}$  が存在することと  $[a]_m[x]_m = \bar{1}$  となる  $x \in \mathbb{Z}$  が存在することとは同値であるから、命題の主張が成立する。□

演習 4-2\*  $\mathbb{Z}/10\mathbb{Z}$  における可逆元をすべて求めよ。また、各可逆元の逆元を求めよ。

上の命題から、直ちに次の結果が従う。

系 4-4-2

$p$  を素数とする。このとき、 $\bar{0}$  でない任意の  $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$  は  $\mathbb{Z}/p\mathbb{Z}$  において逆元を持つ。

● 4-5 : 体

$\mathbb{Z}/m\mathbb{Z}$  が持っている性質 (a)–(d) と [系 4-4-2] を合わせると、素数  $p$  に対し、 $\mathbb{Z}/p\mathbb{Z}$  は  $\mathbb{R}, \mathbb{C}$  が持つ四則演算に関する性質と全く同じ性質を持つことがわかる。つまり、 $\mathbb{Z}/p\mathbb{Z}$  は体と呼ばれる、 $0$  で割ることを除いて加減乗除を自由に行うことができる、和と積を伴った集合になっている。体は次のように定義される。

定義 4-5-1

集合  $\mathbb{K} (\neq \emptyset)$  上に、和 (または加法) と呼ばれる二項演算  $+$  と、積 (または乗法) と呼ばれる二項演算  $\cdot$  が定義されていて、以下の条件を満たすとき、 $\mathbb{K}$  を体 (field) という。

- (a) 任意の  $a, b, c \in \mathbb{K}$  に対して、
  - (i) 結合法則 :  $(a + b) + c = a + (b + c)$ ,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
  - (ii) 交換法則 :  $a + b = b + a$ ,  $a \cdot b = b \cdot a$ .
  - (iii) 分配法則 :  $a \cdot (b + c) = a \cdot b + a \cdot c$   $(a + b) \cdot c = a \cdot c + b \cdot c$ .
- (b) 零元の存在 : 次の条件を満たす元  $0_{\mathbb{K}} \in \mathbb{K}$  が存在する : 任意の  $a \in \mathbb{K}$  に対して  $a + 0_{\mathbb{K}} = a = 0_{\mathbb{K}} + a$ .
- (c) 単位元の存在 : 次の条件を満たす元 ( $0_{\mathbb{K}} \neq$ )  $1_{\mathbb{K}} \in \mathbb{K}$  が存在する : 任意の  $a \in \mathbb{K}$  に対して、 $a \cdot 1_{\mathbb{K}} = a = 1_{\mathbb{K}} \cdot a$ .
- (d) マイナス元の存在 : 任意の  $a \in \mathbb{K}$  に対して、次の条件を満たす元  $x \in \mathbb{K}$  が存在する :  $a + x = x + a = 0_{\mathbb{K}}$ . (但し、 $0_{\mathbb{K}}$  は (b) と同じ  $\mathbb{K}$  の元である。)
- (e) 逆元の存在 : 任意の ( $0_{\mathbb{K}} \neq$ )  $a \in \mathbb{K}$  に対して、次の条件を満たす元  $x \in \mathbb{K}$  が存在する :  $a \cdot x = x \cdot a = 1_{\mathbb{K}}$ . (但し、 $1_{\mathbb{K}}$  は (c) と同じ  $\mathbb{K}$  の元である。)

注意 1 : 体とは、正確には、組  $(\mathbb{K}, +, \cdot)$  のことを指す。“ $\mathbb{K}$  を体とする” という言い方をすることがあるが、この場合には、集合  $\mathbb{K}$  上に、上の条件を満たす和  $+$  と積  $\cdot$  が 1 組指定されていると考える。

注意 2 : 積  $a \cdot b$  を通常  $ab$  で表わす。

注意 3 : 加法の結合法則から、 $n$  個の元  $a_1, a_2, \dots, a_n \in \mathbb{K}$  に対して、 $\mathbb{K}$  の元  $a_1 + a_2 + \dots + a_n$  が括弧の付け方によらずに定まる。同様に、乗法の結合法則から、 $\mathbb{K}$  の元  $a_1 \cdot a_2 \cdot \dots \cdot a_n$  が括弧の付け方によらずに定まる。特に、 $a_1 = \dots = a_n = a$  のとき、 $a_1 + a_2 + \dots + a_n$  を  $na$  と書き、 $a_1 a_2 \cdot \dots \cdot a_n$  を  $a^n$  と書く。

注意 4 : 二項演算  $+$  と  $\cdot$  が、(e) を除くすべての条件を満たすとき、(単位元を持つ) 可換環 (commutative ring) という。また、(e) と積に関する交換法則を除くすべての条件を満たすとき、(単位元を持つ) 環 (ring) という。体は可換環であり、可換環は環である。つまり、「体  $\Rightarrow$  可換環  $\Rightarrow$  環」が成り立つ。

**注意5:** (b)の性質を持つ元  $0_{\mathbb{K}}$  を  $\mathbb{K}$  の**零元** (zero element) といい、(c)の性質を持つ元  $1_{\mathbb{K}}$  を  $\mathbb{K}$  の**単位元** (identity element) という。体  $\mathbb{K}$  において、零元、単位元はそれぞれ1つずつしかない(下の補題を参照)。

**注意6:** 誤解の恐れのないときには、 $\mathbb{K}$  の零元  $0_{\mathbb{K}}$ 、単位元  $1_{\mathbb{K}}$  を、それぞれ、 $0, 1$  と書く。

**例 4-5-2** 整数全体からなる集合  $\mathbb{Z}$  は、いつも使っている和と積に関して可換環である。この可換環を(有理) **整数環** (integer ring) という。 $2 \in \mathbb{Z}$  の逆元が ( $\mathbb{Z}$  の中に) 存在しないので、整数環  $\mathbb{Z}$  は体ではない。一方、有理数全体からなる集合  $\mathbb{Q}$ 、実数全体からなる集合  $\mathbb{R}$ 、複素数全体からなる集合  $\mathbb{C}$  は、いつも使っている和と積に関して体である。これらの体を、順番に、**有理数体** (rational number field)、**実数体** (real number field)、**複素数体** (complex number field) という。

**例 4-5-3**  $p$  が素数のとき、第4-3, 4-4節の結果から、 $\mathbb{Z}/p\mathbb{Z}$  は体になる。この体を  $\mathbb{F}_p$  で表わし、位数  $p$  の**有限体** (finite field) と呼ぶ。

**演習 4-3\*** 実数体  $\mathbb{R}$  の部分集合

$$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$$

に対して和と積を定義し、それらに関して  $\mathbb{Q}(\sqrt{2})$  が体になることを確かめよ。

**補題 4-5-4**

$\mathbb{K}$  を体とする。このとき、

- (1) 体の条件 (b) を満たす  $0_{\mathbb{K}}$  は一意的である。さらに、任意の  $a \in \mathbb{K}$  に対して、 $a + x = x + a = 0_{\mathbb{K}}$  となる  $x \in \mathbb{K}$  は一意的である。この  $x$  を  $-a$  と記す。
- (2) 体の条件 (c) を満たす  $1_{\mathbb{K}}$  は一意的である。さらに、任意の  $a \in \mathbb{K} - \{0_{\mathbb{K}}\}$  に対して、 $ax = xa = 1_{\mathbb{K}}$  となる  $x \in \mathbb{K}$  は一意的である。この  $x$  を  $a^{-1}$  と記す。

**(証明)**

(1)  $0'_{\mathbb{K}}$  も (b) の条件を満たしているとする。任意の  $a \in \mathbb{K}$  に対して  $0'_{\mathbb{K}} + a = a$  であるから、 $a$  として特に、 $0_{\mathbb{K}}$  の場合を考えて、 $0'_{\mathbb{K}} + 0_{\mathbb{K}} = 0_{\mathbb{K}}$  を得る。同様に、任意の  $a \in \mathbb{K}$  に対して  $a + 0_{\mathbb{K}} = a$  であるから、 $a$  として特に  $0'_{\mathbb{K}}$  の場合を考えて、 $0'_{\mathbb{K}} + 0_{\mathbb{K}} = 0'_{\mathbb{K}}$  を得る。よって、 $0'_{\mathbb{K}} = 0'_{\mathbb{K}} + 0_{\mathbb{K}} = 0_{\mathbb{K}}$  である。

次に、 $x, x' \in \mathbb{K}$  を  $a \in \mathbb{K}$  のマイナス元とする。このとき、

$$x' = 0_{\mathbb{K}} + x' = (x + a) + x' = x + (a + x') = x + 0_{\mathbb{K}} = x$$

となる。よって、 $a$  に対してマイナス元は一意的である。

(2) も (1) と同様にして証明される(詳細は演習問題とする)。 □