

1 環 R と R のイデアル \mathfrak{a} と \mathfrak{b} の和 $\mathfrak{a} + \mathfrak{b}$ と積 $\mathfrak{a}\mathfrak{b}$ を

$$\begin{aligned}\mathfrak{a} + \mathfrak{b} &= \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}, \\ \mathfrak{a} \cdot \mathfrak{b} &= \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}\end{aligned}$$

によって定義する. $R = \mathbb{Z}$ のとき, 以下の \mathfrak{a} と \mathfrak{b} に対し, $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a} \cap \mathfrak{b}$ を求めよ.

- (1) $\mathfrak{a} = (2)$, $\mathfrak{b} = (3)$
- (2) $\mathfrak{a} = (4)$, $\mathfrak{b} = (6)$
- (3) $\mathfrak{a} = (x)$, $\mathfrak{b} = (y)$, $(x, y \in \mathbb{Z}_{>0}, x, y \text{ は互いに素})$
- (4) $\mathfrak{a} = (x)$, $\mathfrak{b} = (y)$, $(x, y \in \mathbb{Z}_{\geq 0})$

(解答)

- (1) $\mathfrak{a} + \mathfrak{b} = (2) + (3) = \{2x + 3y \mid x, y \in \mathbb{Z}\}$ が成り立つ. $2 \cdot 2 + 3 \cdot (-1) = 1$ より $1 \in \mathfrak{a} + \mathfrak{b}$. したがって $\mathfrak{a} + \mathfrak{b} = (1) = \mathbb{Z}$ となる. 一方, $\mathfrak{a}\mathfrak{b} = (2)(3) = (6)$ であり,

$$\begin{aligned}\mathfrak{a} \cap \mathfrak{b} &= \{x \in \mathbb{Z} \mid x \text{ は } 2 \text{ の倍数かつ } 3 \text{ の倍数}\} \\ &= \{x \in \mathbb{Z} \mid x \text{ は } 6 \text{ の倍数}\} \\ &= (6)\end{aligned}$$

- (2) $\mathfrak{a} + \mathfrak{b} = (4) + (6) = (2)$, $\mathfrak{a}\mathfrak{b} = (4)(6) = (24)$, $\mathfrak{a} \cap \mathfrak{b} = (4) \cap (6) = (12)$.
 (3) $\mathfrak{a} + \mathfrak{b} = (x) + (y) = (1)$, $\mathfrak{a}\mathfrak{b} = (x)(y) = (xy)$, $\mathfrak{a} \cap \mathfrak{b} = (x) \cap (y) = (xy)$.
 (4) $\mathfrak{a} + \mathfrak{b} = (x) + (y) = (\gcd\{x, y\})$, $\mathfrak{a}\mathfrak{b} = (x)(y) = (xy)$, $\mathfrak{a} \cap \mathfrak{b} = (x) \cap (y) = (\text{lcm}\{x, y\})$. (ただし $\gcd\{x, y\}$ および $\text{lcm}\{x, y\}$ は x, y のそれぞれ最大公約数と最小公倍数を表す.)

2 環 R とそのイデアル $\mathfrak{a}, \mathfrak{b}$ に対し, $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ が成り立つことを示せ.

(解答) $z \in \mathfrak{a}\mathfrak{b}$ とすると, $z = x_1 y_1 + \cdots + x_n y_n$ を満たす $x_i \in \mathfrak{a}$, $y_i \in \mathfrak{b}$ ($i = 1, 2, \dots, n$) が存在する. 任意の i に対し, $x_i \in \mathfrak{a}$ より $x_i y_i \in \mathfrak{a}$, 同様に $y_i \in \mathfrak{b}$ より $x_i y_i \in \mathfrak{b}$. したがって $x_i y_i \in \mathfrak{a} \cap \mathfrak{b}$ を得る. $\mathfrak{a} \cap \mathfrak{b}$ はイデアルであるので, R の和について閉じており, $z \in \mathfrak{a} \cap \mathfrak{b}$ となる.

3 環 R とそのイデアル \mathfrak{p} に対し, 次が成り立つことを示せ.

(1) \mathfrak{p} は R の素イデアル \iff 剰余環 R/\mathfrak{p} は整域

(2) (0) は R の素イデアル \iff 環 R は整域

(解答)

(1) \mathfrak{p} を R の素イデアルとする. $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p}$ と $c \in R$ に対し $c + \mathfrak{p} = \mathfrak{p} \iff c \in \mathfrak{p}$ が成り立つことから,

$$a + \mathfrak{p} \neq \mathfrak{p} \text{ かつ } b + \mathfrak{p} \neq \mathfrak{p} \text{ ならば } (a + \mathfrak{p})(b + \mathfrak{p}) \neq \mathfrak{p}$$

が成り立ち, R/\mathfrak{p} は整域となる.

逆に R/\mathfrak{p} が整域とする. $a, b \in R$ に対し, $ab \in \mathfrak{p}$ ならば $(a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p}$ となり, $a + \mathfrak{p} = \mathfrak{p}$ または $b + \mathfrak{p} = \mathfrak{p}$ が成り立つ. したがって, このとき $a \in \mathfrak{p}$ または $b \in \mathfrak{p}$ が成り立ち, \mathfrak{p} は素イデアルである.

(2) $\mathfrak{p} = (0)$ とおき, 前の問題で示した同値性を用いると主張を得る.

4 $R = \mathbb{Z}$ とし, $x \in \mathbb{Z}$, $\mathfrak{a} = (x)$ とする. x が素数のとき \mathfrak{a} は極大イデアルであることを示せ. また $x = 0$ のとき \mathfrak{a} は極大イデアルではないが, 素イデアルであることを示せ.

(解答) $x = p$ (p は素数) のとき, $R/\mathfrak{a} = \mathbb{Z}/p\mathbb{Z}$ は体である. したがって \mathfrak{a} は極大イデアルである. 一方 $x = 0$ のとき, $R/\mathfrak{a} \simeq R = \mathbb{Z}$ となる. \mathbb{Z} は整域であるが, 体ではないため, \mathfrak{a} は素イデアルであって, 極大イデアルでない.

5 体のイデアルは零イデアル (0) と R のみであることを示せ. また環 R が単位元 1 をもつとき, R のイデアルが (0) と R のみならば, R は体であることを示せ.

(解答) R を体とし, \mathfrak{a} を R のイデアルとする. $\mathfrak{a} \neq 0$ ならば, $x \neq 0$ となる $x \in \mathfrak{a}$ が存在する. R は体なので a には乗法逆元 $a^{-1} \in F^\times$ が存在し, $1 \in a^{-1} \cdot \mathfrak{a} \subseteq \mathfrak{a}$ つまり $\mathfrak{a} = (1) = R$ となる.

逆に R のイデアル \mathfrak{a} が (0) と (1) のみであるとする. R の任意の元 $a \in R$ に対し, a で生成されるイデアル $\mathfrak{a} = (a)$ を考える. R のイデアルは (0) と (1) のみなので, $\mathfrak{a} = (0)$ または $\mathfrak{a} = (1)$ が成り立つ. 前者は $a = 0$, 後者は a が単元であることを意味するため, $a \in R \setminus \{0\}$ ならば, a は単元であることがわかる.