

環と ideal

Def 環とは以下の7つの公理を満たす5つ組 $(R, +, \cdot, 0_R, 1_R)$ のことである。

ここで R : 集合

$+, \cdot : R \times R \rightarrow R$: 写像 (2項演算)

$0_R, 1_R \in R$: 元 (0項演算) である。

① $\forall a \in R \forall b \in R \forall c \in R, (a+b)+c = a+(b+c)$ 結合

② $\forall a \in R \forall b \in R, a+b = b+a$ 交換

③ $\forall a \in R, 0_R + a = a = a + 0_R$ 単位元

④ $\forall a \in R \exists b \in R, a+b = 0_R = b+a$ 逆元

⑤ $\forall a \in R \forall b \in R \forall c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ 結合

⑥ $\forall a \in R, 1_R \cdot a = a = a \cdot 1_R$ 単位元

⑦ $\forall a \in R \forall b \in R \forall c \in R, a(b+c) = ab+ac, (a+b)c = ac+bc$

例 $(\mathbb{Z}, +, \cdot, 0, 1)$ は環である

例 $M_n(\mathbb{C}) := \{n \times n \text{ 複素行列}\} (= \{(a_{ij})_{1 \leq i, j \leq n} \in \mathbb{C}^{n^2}\})$

に $(M_n(\mathbb{C}), +, \cdot, 0_n, E_n)$ は環である

用語 環 $(R, +, \cdot, 0_R, 1_R)$ が以下を満たすとき, 可換環という

⑧ $\forall a \in R \forall b \in R, ab = ba$

例 $\mathbb{Z}$ は可換環

$M_n(\mathbb{C})$ は $n \geq 2$ のとき可換環ではない

例 $\mathbb{C}[x] := \{\text{複素係数多項式}\} (= \{ \sum_{i \geq 0} a_i x^i \mid \#\{i \geq 0 \mid a_i \neq 0\} < \infty \})$
 について $(\mathbb{C}[x], +, \cdot, 0, 1)$ は可換環

用語 可換環 $(R, +, \cdot, 0_R, 1_R)$ かつ以下をみたすとき、体 という

⑨ $0_R \neq 1_R$ かつ $\forall a \in R, a \neq 0_R \Rightarrow \exists b \in R \quad ab = 1_R = ba$

例 $\mathbb{Z}$ は体ではない

$\mathbb{Q}$ は体 (他、 $\mathbb{R}, \mathbb{C}$ は体)

例 $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ には $ij = k = -ji, i^2 = -1$
 $jk = i = -kj, j^2 = -1$
 $ki = j = -ik, k^2 = -1$
 2"積を入れたもの"を4元数環という。

• $\mathbb{H}$ は環だが可換環ではない。

• $\mathbb{H}$ は ⑧ 以外の公理 (①~⑦ + ⑨) をみたす (斜体)

skew field

domain

用語 可換環 $(R, +, \cdot, 0_R, 1_R)$ かつ以下をみたすとき、整域という

⑨' $0_R \neq 1_R$ かつ $\forall a \in R \forall b \in R \quad a \neq 0_R, b \neq 0_R \Rightarrow ab \neq 0_R$

例 $\mathbb{Z}$ は整域

$M_2(\mathbb{C})$ 2" $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ だが、そもそも $M_2(\mathbb{C})$ は可換環でない

常識的事実(一部)

prop $(R, +, \cdot, 0_R, 1_R)$: 環

(A) $x \in R$ が ③ をみたす (i.e., $\forall a \in R, a+x=a=x+a$) $\Rightarrow x=0_R$

(B) $y \in R$ が ⑥ をみたす (i.e., $\forall a \in R, ya=a=ay$) $\Rightarrow y=1_R$

proof (A) $a=0_R$ とすると, $0_R+x=0_R$ - ③ より $0_R+x=x$

(B) 同様 //

prop R : 環, $a \in R$ に対し $b, b' \in R$ が 以下をみたす $\Rightarrow b=b'$

$$a+b=0_R=b+a \quad \text{かつ} \quad a+b'=0_R=b'+a$$

④ 元の一意的性

$$\textcircled{!} (b'+a)+b \stackrel{\textcircled{1}}{=} b'+(a+b)$$

$$\stackrel{\textcircled{3}}{=} b \stackrel{\textcircled{3}}{=} 0_R + b \quad \parallel \quad b' + 0_R \stackrel{\textcircled{3}}{=} b' //$$

記法 ④ 上の prop より ④ の b は一意的である。これを $-a$ と書く。

prop R : 環 $\forall a \in R, (-1_R) \cdot a = -a$ (③) $-(-a) = a$ である

$$0_R \cdot a = 0_R$$

$$\textcircled{!} 0_R \stackrel{\textcircled{3}}{=} 0_R + 0_R \text{ より } \textcircled{7} \text{ から } 0_R \cdot a = 0_R \cdot a + 0_R \cdot a$$

$$-(0_R \cdot a) \text{ を両方に加える } 0_R \cdot a + (- (0_R \cdot a)) = ((0_R \cdot a + 0_R \cdot a) + (- (0_R \cdot a)))$$

$$\parallel$$

$$0_R$$

$$\parallel \textcircled{4}$$

$$0_R \cdot a + (0_R \cdot a + (- (0_R \cdot a)))$$

$$\parallel$$

$$0_R \cdot a + 0_R = 0_R \cdot a$$

$(-1_R) \cdot a = -a$ を言うには $a + (-1_R) \cdot a = 0_R$ を言えばよい。

$$\begin{aligned} a + (-1_R) \cdot a &= 1_R \cdot a + (-1_R) \cdot a \\ &= (1_R + (-1_R)) \cdot a = 0_R \cdot a = 0_R // \end{aligned}$$

Cor $R: \text{環}, (-1_R)(-1_R) = 1_R$

$$\begin{aligned} \textcircled{!} (-1_R) \cdot (-1_R) &= -(-1_R) = 1_R // \\ &\quad \uparrow \\ &\quad \text{prop} \end{aligned}$$

prop $R: \text{有限整域} \Rightarrow R \text{は体}$

$\textcircled{!} a \neq 0_R \text{ in } R \text{ について,}$

$f_a: R \rightarrow R$ は単射である。
 $x \mapsto ax$

$$\left(\begin{array}{l} \text{実際 } ax = ax' \xrightarrow{\textcircled{1}} a(x - x') = 0_R \\ \xrightarrow{\textcircled{1}'} x - x' = 0_R \\ \Rightarrow x = x' \end{array} \right)$$

R は有限集合なので f_a は全単射になる。

よって $\exists b \in R, f_a(b) = 1_R$ 。つまり $ab = 1_R (= ba)$ がい言えた //

Wedderburnの定理

Remark 少し難しい事実として、「有限斜体は体」であることが知られている。

以下、このような
常識的な変形は
断りなく用いる。

例えば $ab = 1_R = ba$
となる b を a^{-1} とか $\frac{1}{a}$ と
書くなどである

a^{-1} の一意性や、 $(a^{-1})^{-1} = a$
についても同様である。

ideal に ついてDef R : 可換環部分集合 $I \subseteq R$ が ideal とは, 以下の 3 条件をみたすこと

(I1) $I \neq \emptyset$

(I2) $\forall x \in I \forall y \in I, x+y \in I$

$x+y \in R$

(I3) $\forall x \in I \forall a \in R, ax \in I$

$ax \in R$

例 $R = \mathbb{Z}$, $I = 2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\} (= \{\text{偶数}\})$ は R の ideal $I' = \{\text{奇数}\}$ は R の ideal ではないRemark ideal の定義で, (I1), (I2), (I3) を (I1)', (I2), (I3) に変えても同じ

(I1)' $0_R \in I$

($\Rightarrow$) (I1), (I2), (I3) $\Rightarrow$ (I1)' を示すのはよい。

$I \neq \emptyset$ より $z_0 \in I$ がある。 $a = 0$ とし $0_R \cdot z_0 = 0_R \in I$ である。

例 $I = \{0\}$ および $I = R$ は R の ideal $\Rightarrow$ 明らか idealRemark $I \subseteq R$: ideal について $I = R \Leftrightarrow 1_R \in I$

($\Rightarrow$): 明らか

($\Leftarrow$): $I \supseteq R$ を示せばよい

$\forall a \in R \quad a \cdot 1_R = a \in I$

ただ 17 存在

Thm $I \subseteq \mathbb{Z}$: ideal

$$\exists! d \geq 0 \text{ s.t. } I = d\mathbb{Z} (= \{dx \mid x \in \mathbb{Z}\} = \{d \text{ の倍数}\})$$

① $I = \{0\}$ ならば $d = 0$ とする。

以下 $I \neq \{0\}$ とし、 $i_0 \in I$ をとる。 $(-1) \cdot i_0 \in I$ を考えよ。 $i_0 \neq 0$

$i_0 > 0$ としよ。

つまり $\Sigma := \{i \in I \mid i > 0\} \neq \emptyset$ なる $\mathbb{Z}$ 最小元 d がとれる。

以下 $I = d\mathbb{Z}$ を示す。

$I \supseteq d\mathbb{Z}$ であることを : $I \ni d$ と (I3) より明らか

$I \subseteq d\mathbb{Z}$ であることを : $\forall i \in I$ について d で割り算すると

$$i = dq + r \text{ と書ける。 ここで } q, r \in \mathbb{Z}$$

$$\text{s.t. } 0 \leq r < d$$

$$r = i - dq \in I \text{ なる } d \text{ の最小性より}$$

$$r = 0 \text{ とならなければならない}$$

応用 $a, b \in \mathbb{Z}_{\geq 1}$ を互いに素なとき $\exists x \in \mathbb{Z} \exists y \in \mathbb{Z} \text{ s.t. } ax + by = 1$

② $I = \{ax + by \mid x, y \in \mathbb{Z}\}$ は $\mathbb{Z}$ の ideal である。

$$\text{よって } \exists! d \geq 1 \text{ s.t. } I = d\mathbb{Z}$$

$$a, b \in I \text{ なる } d \text{ は } a \text{ と } b \text{ を割り切る。 よって } d = 1 //$$