環と ideal

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

ここで R：集合

$+,\cdot : R\times R \to R$ ：写像（2項演算）

$0_R, 1_R \in R$ ：元（0項演算）　である。

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

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

③ $\forall a\in R,\ 0_R+a=a=a+0_R$

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

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

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

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

について $(M_n(\mathbb{C}),+,\cdot,O_n,E_n)$ は環である。

用語 環 $(R,+,\cdot,0_R,1_R)$ が以下をみたすとき，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 $\mathbb{C}[x] := \{\text{複素係数多項式}\} \left(= \left\{ \sum_{i \geq 0} a_i x^i \;\middle|\; \#\{i \geq 0 \mid a_i \neq 0\} < \infty \right\}\right)$

について $(\mathbb{C}[x], +, \cdot, 0, 1)$ は可換環

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

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

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 $ij = k = -ji$, $i^2 = -1$
$jk = i = -kj$, $j^2 = -1$
$ki = j = -ik$, $k^2 = -1$
で"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)

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

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

例 $\mathbb{Z}$ は整域

$M_2(\mathbb{C})$ で $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 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) $a=0_R$ ととると, $0_R+x=0_R$ 一方 ③ より $0_R+x=x$

(B) 同様 //

prop R : 環, $a \in R$ について $b, b' \in R$ が以下をみたす $\Rightarrow b=b'$

$a+b=0_R=b+a$ かつ $a+b'=0_R=b'+a$

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

$b \overset{③}{=} 0_R+b$ ‖ $b'+0_R \overset{③}{=} b'$ ‖ //

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

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

$0_R \cdot a = 0_R$

(!) $0_R \overset{③}{=} 0_R+0_R$ より ⑦ から $0_R \cdot a = 0_R \cdot a + 0_R \cdot a$

$-(0_R \cdot a)$ を両辺加えると $0_R \cdot a + (-(0_R \cdot a)) = ((0_R \cdot a + 0_R \cdot a) + (-(0_R a)))$

‖ ‖ ①

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

‖

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

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

$$a+(-1_R)\cdot a = 1_R\cdot a + (-1_R)\cdot a$$
$$= (1_R+(-1_R))\cdot a = 0_R\cdot a = 0_R \quad //$$

Cor R：環, $(-1_R)(-1_R)=1_R$

☺ $(-1_R)\cdot(-1_R) = -(-1_R) = 1_R$ //
(↑ prop)

以下、このような常識的な変形は断りなく用いる。

prop R：有限整域 $\Rightarrow$ Rは体

☺ $a\neq 0_R$ in Rについて,

$f_a : R \longrightarrow R$ は単射である。
$x \longmapsto ax$

(実際 $ax=ax' \overset{①}{\Rightarrow} a(x-x')=0_R \overset{①'}{\Rightarrow} x-x'=0_R \Rightarrow x=x'$)

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。

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 $ab=1_R\ (=ba)$ が言えた //

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。

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

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

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)′ $0_R \in I$

(☺ (I1),(I2),(I3) $\Rightarrow$ (I1)′ を言えばよい。
$I \neq \emptyset$ より $z_0 \in I$ がとれる。このとき $0_R \cdot z_0 = 0_R \in I$ である。)

例 $I=\{0\}$ および $I=R$ は R の ideal

Remark $I \subseteq R$：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
$\forall a \in R \quad a \cdot 1_R = a \in I$)

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

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

☺ $I = \{0\}$ なら $d = 0$ とする。

以下 $I \neq \{0\}$ とし、$x_0 \in I$ ($x_0 \neq 0$) をとる。$(-1)\cdot x_0 \in I$ を考えることで

$x_0 > 0$ としてよい。

つまり $\sum := \{x \in I \mid x > 0\} \neq \emptyset$ なので最小元 d がとれる。

以下 $I = d\mathbb{Z}$ を示す。

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

$I \subseteq d\mathbb{Z}$ であること : $\forall x \in I$ について d で"割り算"すると

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

s.t. $0 \leq r < d$

$r = x - dq \in I$ なので d の最小性より

$r = 0$ でなければならない //

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

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

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

$a, b \in I$ なので d は a と b を割り切る。よって $d = 1$ //