

# 可換環論

Anko

2023 年 7 月 20 日

## 目次

1	環論 .....	2
2	加群 .....	11

# 1 環論

定義 (環 (ring)).

集合  $A$  が次の条件を満たす 2 つの二項演算をもつとき  $A$  を環という。

1.  $A$  は加法に関してアーベル群である。
2. 乗法は結合的であり、加法に対して分配的である。
3. すべての  $x \in A$  に対して、 $x1 = 1x = x$  を満たす元  $1 \in A$  が存在する。

命題 1.

$0 = 1$  のとき  $A$  は唯一の元  $0$  からなる。このとき  $A$  は零環 (zero ring) といい、 $0$  で表される。◇

証明

任意の元  $x \in A$  について次が成り立つ。

$$x = x1 = x0 = 0 \quad (1)$$

□

定義 (環準同型写像 (ring homomorphism)).

環  $A, B$  に関して写像  $f : A \rightarrow B$  が次の条件を満たすとき環準同型写像 (ring homomorphism) という。

1.  $f(x + y) = f(x) + f(y)$
2.  $f(xy) = f(x)f(y)$
3.  $f(1) = 1$

命題 2.

$f : A \rightarrow B, g : B \rightarrow C$  が環準同型写像ならば合成写像  $g \circ f : A \rightarrow C$  も環準同型写像である。◇

具体例

1.  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$  の和積は可換環となる。

2. 行列  $M_n(\mathbb{R})$  は非可換環となる.
3. 関数  $C^\infty(\mathbb{R})$  の和積は可換環となる.
4. 群環 (有限群から可換環への写像の像の総和) の和積は環となる.
5. 2 次の環  $\mathbb{Z}[\sqrt{d}]$  は環になる.

**定義** (部分環 (subring)).

環  $A$  の部分集合  $S$  は、加法乗法に関して閉じていて  $A$  の単位元を含んでいるとき  $A$  の部分環 (subring) であるという。

**定義** (イデアル).

$\mathfrak{a}$  を環  $A$  の部分集合とする。 $\mathfrak{a}$  が  $A$  の加法部分群でかつ  $A\mathfrak{a} \subseteq \mathfrak{a}$  を満たすとき、 $\mathfrak{a}$  を  $A$  のイデアル (ideal) という。剰余群  $A/\mathfrak{a}$  は環  $A$  の乗法から一意的に乗法が定義され、環となる。これを剰余環 (quotient ring, residue-class ring)  $A/\mathfrak{a}$  という。 $A/\mathfrak{a}$  の元は  $A$  における  $\mathfrak{a}$  の剰余類であり、任意の  $x \in A$  に対して剰余類  $x + \mathfrak{a}$  を対応させる写像  $\phi: A \rightarrow A/\mathfrak{a}$  は全射的環準同型写像である。

**命題 3.**

$\mathfrak{a}$  を含んでいる  $A$  のすべてのイデアル  $\mathfrak{b}$  の集合と、剰余環  $A/\mathfrak{a}$  のすべてのイデアル  $\mathfrak{b}$  の集合との間には、 $\mathfrak{b} = \phi^{-1}(\mathfrak{b})$  ◇

**定義.**

環  $A$  の零因子 (zero divisor) とは、「0 を割り切る」元  $x$  のことである。すなわち  $A$  のある元  $y \neq 0$  が存在して  $xy = 0$  となる元  $x \in A$  のことである。零元と異なる零因子をもたない環を整域 (integral domain) という ( $0 \neq 1$  としている)。

元  $x \in A$  はある  $n > 0$  に対して  $x^n = 0$  となるとき、ベキ零元 (nilpotent) であるという。 $x \in A$  が 1 を割り切るとき、すなわちある元  $y \in A$  が存在して  $xy = 1$  となるとき  $x$  を  $A$  の単元 (unit) という。このとき  $y$  は  $x$  に対して一意に定まり、 $x^{-1}$  によって表す。 $A$  におけるすべての単元の集合はアーベル群をつくる。

**命題 4.**

$A \neq 0$  を環とする。このとき次は同値である。

1.  $A$  は体である。
2.  $A$  のイデアルは  $0$  と  $(1)$  のみである。
3.  $A$  から零でない環  $B$  へのすべての環準同型は単射である。

◇

### 証明

(1  $\implies$  2)  $\mathfrak{a} \neq 0$  を  $A$  のイデアルとする。 $\mathfrak{a}$  は零でない元  $x$  を含む。 $x$  は単元であるから  $\mathfrak{a} \supseteq (x) = (1)$  となり  $\mathfrak{a} = (1)$  を得る。

(2  $\implies$  3)  $\phi: A \rightarrow B$  を環準同型とする。このとき  $\text{Ker}(\phi)$  は (1) と異なるイデアルであるから  $\text{Ker}(\phi) = 0$  である。よって  $\phi$  は単射である。

(3  $\implies$  1)  $x$  を単元でない  $A$  の元とする。すると  $(x) \neq (1)$  であるから  $B = A/(x)$  は零環ではない。 $\phi: A \rightarrow B$  を自然な準同型とすると  $\text{Ker}(\phi) = (x)$  である。仮定より  $\phi$  は単射であるから  $(x) = 0$ 。したがって  $x = 0$  となる。□

### 命題 5.

$x$  を環  $A$  のベキ零元とする。 $1+x$  は  $A$  の単元であることを示せ。これよりベキ零元と単元の和は単元であることを示せ。◇

### 証明

$x$  がベキ零元であるから  $x^n = 0$  となる  $n > 0$  が存在する。

$$(1+x)(1+(-x)+\cdots+(-x)^{n-1}) = 1+(-x)^n = 1 \quad (2)$$

単元  $a$  を用いると  $a^{-1}x$  もベキ零元となるから  $a+x$  も単元となる。

$$(a+x)a^{-1} = 1+a^{-1}x \quad (3)$$

□

### 命題 6.

$f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$  について

1.  $f$  が単元である  $\iff a_0$  が単元で、かつ  $a_1, \dots, a_n$  はベキ零元である。
2.  $f$  がベキ零元である  $\iff a_0, a_1, \dots, a_n$  がベキ零元である。
3.  $f$  が零因子である  $\iff A$  のある元  $a \neq 0$  が存在して  $af = 0$  を満たす。

◇

### 証明

1. ( $\implies$ )  $f^{-1} = b_0 + b_1x + \cdots + b_mx^m$  とおくと

$$ff^{-1} = (a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) \quad (4)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m} \quad (5)$$

$$= 1 \quad (6)$$

$$\iff a_0b_0 = 1, \sum_{i+j=k} a_ib_j = 0 \quad (k > 0) \quad (7)$$

より  $a_0, b_0$  は単元である。ここで  $a_n^{r+1}b_{m-r} = 0$  について帰納法を用いて示す。まず  $a_nb_m = 0$  である。 $r-1$  までが成り立ち  $r$  のときを考える。

$$a_n^{r+1}b_{m-r} = a_n^r(a_nb_{m-r}) \quad (8)$$

$$= a_n^r(-a_{n-1}b_{m-r+1} - a_{n-2}b_{m-r+2} - \cdots - a_{n-r}b_m) \quad (9)$$

$$= -a_{n-1}(a_n^rb_{m-r+1}) + a_na_{n-2}(a_n^{r-1}b_{m-r+2}) + \cdots + a_n^{r-1}a_{n-r}(a_nb_m) \quad (10)$$

$$= 0 \quad (11)$$

これより帰納法から  $a_n^{r+1}b_{m-r} = 0$  が成り立つ。これより  $r = m$  とすると  $b_0$  は単元であるから  $a_n^{m+1} = 0$  より  $a_nx^n$  はベキ零元である。これより  $f - a_nx^n$  は単元である。よって帰納法から  $a_1, \dots, a_n$  はベキ零元である。

( $\Leftarrow$ )  $g = b_0 + b_1x + \cdots + b_mx^m$  とおき  $fg = 1$  となるように  $g$  を決定する。

$$fg = (a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) \quad (12)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m} = 1 \quad (13)$$

$$\iff a_0b_0 = 1, \sum_i a_ib_{k-i} = 0 \quad (k > 0) \quad (14)$$

$$\iff b_0 = a_0^{-1}, b_k = -a_0^{-1} \left( \sum_{i=1}^k a_ib_{k-i} \right) \quad (15)$$

これより  $f$  は単元となる。

2. ( $\implies$ )  $1 + f$  は単元であるから (1) より  $a_1, \dots, a_n$  はベキ零元である。また  $f^m = 0$  となる  $m > 0$  があり、その定数項は  $a_0^m = 0$  であるから  $a_0$  もベキ零元である。

( $\Leftarrow$ ) 各  $a_i$  に対して  $m_i$  を  $a_i^{m_i} = 0$  となる最小の数とする。 $M = \max m_i$  とおくと鳩の巣原理より  $f^{nM} = 0$  となる。よって  $f$  はベキ零元である。

3. ( $\implies$ )  $g = b_0 + b_1x + \cdots + b_mx^m$  を  $fg = 0$  を満たす最小の次数の多項式  $g \in A[x]$  とする。ここで  $a_nb_m = 0$  であるから  $a_ng$  について

$$fa_ng = 0 \quad (16)$$

$$\deg a_ng < m \quad (17)$$

より次数の最小性から  $a_n g = 0$  となる。これより  $fg = (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1})g = 0$  であるから  $a_{n-1} b_m = 0$  が成り立ち、 $a_{n-1} g = 0$  となる。よって同様に考えて一次の係数を比較することで分かる。

$$a_n g = a_{n-1} g = \cdots = a_0 g = 0 \quad (18)$$

$$b_0 f = 0 \quad (19)$$

( $\Leftarrow$ ) 自明。

□

**定義 (準同型・同型).**

$A, B$  を環,  $\phi: A \rightarrow B$  を写像とする.

1.  $\phi$  が準同型で逆写像が存在し、逆写像も準同型であるとき、 $\phi$  は同型であるという。  
また、このとき、 $A, B$  は同型であるといい、 $A \cong B$  と書く。
2.  $A = B$  なら準同型・同型を自己準同型・自己同型という。環  $A$  の自己同型全体の集合を  $\text{Aut}^{\text{al}} A$  と書く。

**命題 7.**

$\phi: A \rightarrow B$  が環の準同型なら  $\phi(0_A) = 0_B$  である。

◇

**証明**

$\phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) + \phi(0_A)$  より  $\phi(0_A) = 0_B$  となる。

□

**命題 8.**

$A, B, C$  を環,  $\phi: A \rightarrow B, \psi: B \rightarrow C$  を準同型とすると、その合成  $\phi \circ \psi: A \rightarrow C$  も準同型である。同様に  $\phi, \psi$  が同型なら、 $\phi \circ \psi$  も同型である。

◇

**証明**

$\psi \circ \phi(x + y) = \psi(\phi(x + y)) = \psi(\phi(x) + \phi(y)) = \psi(\phi(x)) + \psi(\phi(y)) = \psi \circ \phi(x) + \psi \circ \phi(y)$  となり、 $\psi \circ \phi(xy) = \psi \circ \phi(x)\psi \circ \phi(y)$  や  $\psi \circ \phi(1_A) = 1_C$  も同様に示せるから  $\psi \circ \phi$  は準同型である。同型も同様。

□

**命題 9.**

$\phi: A \rightarrow B$  が環の準同型ならば、単射  $\iff \text{Ker } \phi = \{0\}$

◇

**証明**

( $\implies$ )  $\phi$  が環の準同型であるから  $\phi(0_A) = 0_B$  より  $0_A \in \text{Ker } \phi$ . また元  $\forall x, y \in \text{Ker } \phi$  について  $\phi$  の単射性より  $\phi(x) = \phi(y) \implies x = y$  となり,  $\text{Ker } \phi$  には 0 以外の元は存在しない.

( $\impliedby$ )  $\phi(x) = \phi(y)$  となる  $x, y$  について

$$1 = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \quad (20)$$

$$1 = xy^{-1} \quad (21)$$

より  $x = y$  となるから  $\phi$  は単射である.  $\square$

**定義 ( $n$  変数多項式).**

$A$  係数あるいは  $A$  上の  $n$  変数  $x = (x_1, \dots, x_n)$  の多項式とは,  $\mathbb{N}^n$  から  $A$  への写像で有限個の  $(i_1, \dots, i_n) \in \mathbb{N}^n$  を除いて値が 0 になるものと, 変数  $x = (x_1, \dots, x_n)$  の組のことである. この写像の  $(i_1, \dots, i_n) \in \mathbb{N}^n$  での値が  $a_{i_1, \dots, i_n}$  なら, この多項式を

$$f(x) = f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

などを書く. すべての  $a_{i_1, \dots, i_n}$  が 0 である多項式を 0 と書く. 各  $a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$  を  $f(x)$  の項,  $a_{i_1, \dots, i_n}$  を係数という. 特に  $a_{0, \dots, 0}$  を  $f(x)$  の定数項という.

**定義 ( $n$  変数多項式の代入).**

$c = (c_1, \dots, c_n) \in A^n$  とするとき

$$f(c) = f(c_1, \dots, c_n) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} c_1^{i_1} \cdots c_n^{i_n}$$

とする. この値を考えることを代入という.

**定義 ( $n$  変数多項式の次数).**

$f(x)$  の次数  $\deg f(x)$  を

$$\deg f(x) = \begin{cases} \max\{i_1 + \cdots + i_n \mid a_{i_1, \dots, i_n} \neq 0\} & (f(x) \neq 0) \\ -\infty & (f(x) = 0) \end{cases}$$

と定義する.

定義 ( $A$  係数あるいは  $A$  上の  $n$  変数多項式環).

2 つの  $n$  変数多項式

$$f(x) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}, \quad g(x) = \sum_{i_1, \dots, i_n} b_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

は,  $a_{i_1, \dots, i_n} = b_{i_1, \dots, i_n}$  がすべての  $i_1, \dots, i_n$  に対して成り立つとき多項式の同値関係  $f(x) = g(x)$  であると定義する. また次のように多項式の和差積を定義する.

$$(f \pm g)(x) = \sum_{i_1, \dots, i_n} (a_{i_1, \dots, i_n} \pm b_{i_1, \dots, i_n}) x_1^{i_1} \cdots x_n^{i_n} \quad (22)$$

$$f(x)g(x) = \sum_{i_1, \dots, j_n} a_{i_1, \dots, i_n} b_{j_1, \dots, j_n} x_1^{i_1+j_1} \cdots x_n^{i_n+j_n} \quad (23)$$

すると多項式全体の集合  $A[x]$  は環となり,  $A$  係数あるいは  $A$  上の  $n$  変数多項式環という.

定義 (無限変数多項式環).

無限変数多項式環  $A[x_i]_{i \in I}$  とは  $n > 0$  を整数とすると,  $X_n$  を  $\mathbb{N}^n$  から  $A$  への写像  $a$  で有限個の  $(i_1, \dots, i_n) \in \mathbb{N}^n$  を除いて値が 0 であるものと  $\{1, \dots, n\}$  から  $I$  への単射写像  $\phi$  の組全体の集合とする.  $X_n$  には  $\mathfrak{S}_n$  が作用し, その軌道の集合を  $Y_n$  とする.  $(a, \phi) \in X_n$  で代表される  $Y_n$  の元に対し,

$$\sum_{i_1, \dots, i_n \in \mathbb{N}} a(i_1, \dots, i_n) x_{\phi(1)}^{i_1} \cdots x_{\phi(n)}^{i_n}$$

と書く. これは代表元のとりかたによらず定まる.  $\{Y_n\}_n$  は集合族となり,  $n \leq m$  なら  $Y_n \subseteq Y_m$  とみなせる.  $A[x_i]_{i \in I} = \bigcup_n Y_n$  と定義すればよい.  $A[x_i]_{i \in I}$  が集合として存在するときそれを無限変数多項式環という.

定理 10.

$$A[x_1, \dots, x_n] \cong A[x_1, \dots, x_{n-1}][x_n]$$

◇

証明



$$f(x_1, \dots, x_n) = \sum_{i_n} \left( \sum_{i_1, \dots, i_{n-1}} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} \right) x_n^{i_n}$$

□

定義 (環の鎖).

a

1. 環: 加法が可換群, 乗法がモノイドであり, また分配法則を満たす.
2. 可換環: 環について乗法が可換である.
3. 整域: 可換環  $A$  について任意の  $a, b \in A \setminus \{0\}$  に対し,  $ab \neq 0$  となる.
4. 正規環: 整域  $A$  について商体  $K$  の元が  $A$  上整なら  $A$  の元となる.
5. 一意分解環 (UFD): 整域について任意の元は素元分解できる.
6. 単項イデアル整域 (PID): 整域について任意のイデアルが単項イデアルである.
7. ユークリッド環: 整域  $A$  について写像  $d: A \setminus \{0\} \rightarrow \mathbb{N}$  があり,  $a, b \in A$  で  $b \neq 0$  なら,  $q, r \in A$  があり,  $a = qb + r$  で  $r = 0$  または  $d(r) < d(b)$  となる.
8. 体: 可換環  $A$  の乗法が  $A \setminus \{0\}$  において可換群となる.

定理 11 (環の鎖).

環  $\Leftarrow$  可換環  $\Leftarrow$  整域  $\Leftarrow$  正規環  $\Leftarrow$  UFD  $\Leftarrow$  PID  $\Leftarrow$  ユークリッド環  $\Leftarrow$  体 ◇

証明

(可換環  $\Rightarrow$  環) 自明.

(整域  $\Rightarrow$  可換環) 自明.

(正規環  $\Rightarrow$  整域) 自明.

(UFD  $\Rightarrow$  正規環)  $\alpha \in K$  を解に持つモニック多項式  $f(x) = x^n + \cdots + a_1x + a_0$  について  $a_0 \neq 0$  とすると,  $\alpha \neq 0$  である. ここで  $\alpha$  を既約分数として  $\alpha = \beta/\gamma$  と表すと,  $\gamma^n f(\alpha) = \beta^n + a_{n-1}\gamma\beta^{n-1} + \cdots + a_0\gamma^n = 0$  より  $\beta^n = -\gamma(a_1\beta^{n-1} + \cdots + a_n\gamma^{n-1})$  なので,  $\gamma \in A^\times$  となる. よって  $\alpha \in A$  である.

(PID  $\Rightarrow$  UFD)

(ユークリッド環  $\Rightarrow$  PID) あるイデアル  $I \subseteq A$  に対し,  $x = \min\{d(y) \mid I \ni y \neq 0\}$  とおくと  $I = (x)$  となることを示す. イデアル  $I$  の元  $\forall z = qx + r \in I$  について  $r = 0 \vee d(r) < d(x)$  であり,  $0 = d(r) < d(x)$  より  $r = 0$  となる. よって  $z = qx \in (x)$  となるので  $I = (x)$  である.

(体  $\Rightarrow$  ユークリッド環) □

**命題 12.**

部分環に性質が引き継がれる.

1. 環の部分環は環である.
2. 可換環の部分環は可換環である.
3. 整域の部分環は整域である.
4. 正規環の部分環は正規環である.
5. UFD の部分環は UFD である.
6. PID の部分環は PID ではない?
7. ユークリッド環の部分環はユークリッド環ではない?
8. 体の部分環は体ではない.

◇

**証明**

それぞれ証明する. 反例を挙げる.

1. 定義から自明.
2. 任意の元  $a, b \in A$  について可換ならばその部分集合も成り立つ.
- 3.
- 4.
- 5.
- 6.
- 7.
8. 有理数体  $\mathbb{Q}$  の部分環  $\mathbb{Z}$  は体ではない.

□

**命題 13 (素イデアルと極大イデアルの関係).**

素イデアル

1.  $A$  が環なら,  $A$  の任意の極大イデアルは素イデアルである.
2.  $A$  が単項イデアル整域なら,  $(0)$  でない任意の素イデアルは極大イデアルである. したがって,  $p$  が素元なら,  $A/(p)$  は体である.

◇

**命題 14 (素元と既約元の関係).**

素元

1.  $A$  が整域なら,  $A$  の素元は既約元である.
2.  $A$  が一意分解環なら,  $A$  の既約元は素元である.

◇

証明

□

命題 15.

体の多項式環はユークリッド環である.

◇

証明

$d = \deg$  とすると成り立つ.

□

命題 16 (正規環).

$f(x) = a_n x^n + \cdots + a_0 \in A[x]$  で  $a_0, a_n \neq 0, \alpha \in K$

◇

定義.

1. ネーター環
2. アルティン環

## 2 加群

定義.

環  $R$  上の行列の集合について定義する.

1.  $m \times n$  行列の集合を  $M_{m,n}(R)$ .
2.  $n$  次正方行の集合を  $M_n(R)$ .
3.  $M_n(R)$  の乗法群 (正則行列の集合) を一般線形群  $GL_n(R)$ .
4.  $GL_n(R)$  の  $\det$  の核 (行列式の値が単位元) を特殊線形群  $SL_n(R)$ .