可換環論

Anko

2023 年 8 月 11 日

目次

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。 $\diamond$

証明
任意の元 $x \in A$ について次が成り立つ。

$$x = x1 = x0 = 0 \tag{1}$$

$\square$

定義 (環準同型写像 (ring homomorphism)).
環 A, B に関して写像 $f : A \to B$ 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.
$f : A \to B,\ g : B \to C$ が環準同型写像ならば合成写像 $g \circ f : A \to C$ も環準同型写像である。 $\diamond$

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 $\phi : A \to A\mathfrak{a}$ 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.
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。

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

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。

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

□

命題 5.

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

$$f\text{ が単元である} \iff a_0\text{が単元かつ } a_1,\ldots,a_n\text{はベキ零元である} \tag{4}$$

$$f\text{ がベキ零元である} \iff a_0,a_1,\ldots,a_n\text{がベキ零元である} \tag{5}$$

$$f\text{ が零因子である} \iff A\text{ のある元 } a \neq 0\text{ が存在して } af = 0\text{ を満たす} \tag{6}$$

◇

証明

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

$$\begin{aligned} ff^{-1} &= (a_0+a_1x+\cdots+a_nx^n)(b_0+b_1x+\cdots+b_mx^m) && (7)\\ &= a_0b_0 + (a_0b_1+a_1b_0)x + \cdots + a_nb_mx^{n+m} && (8)\\ &= 1 && (9)\\ \iff a_0b_0 &= 1, \sum_{i+j=k} a_ib_j = 0 \qquad (k>0) && (10) \end{aligned}$$

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。

$$\begin{aligned} a_n^{r+1}b_{m-r} &= a_n^r(a_nb_{m-r}) && (11)\\ &= a_n^r(-a_{n-1}b_{m-r+1} - a_{n-2}b_{m-r+2} - \cdots - a_{n-r}b_m) && (12)\\ &= -a_{n-1}(a_n^rb_{m-r+1}) + a_na_{n-2}(a_n^{r-1}b_{m-r+2}) + \cdots + a_n^{r-1}a_{n-r}(a_nb_m) && (13)\\ &= 0 && (14) \end{aligned}$$

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 $a_1,\ldots,a_n$ はベキ零元である。

($\Longleftarrow$) $g = b_0 + b_1 x + \cdots + b_m x^m$ とおき $fg = 1$ となるように g を決定する。

$$
\begin{aligned}
fg &= (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) && (15)\\
&= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m} = 1 && (16)\\
\iff\ & a_0 b_0 = 1, \sum_i a_i b_{k-i} = 0 \qquad (k > 0) && (17)\\
\iff\ & b_0 = a_0^{-1}, b_k = -a_0^{-1}\left(\sum_{i=1}^{k} a_i b_{k-i}\right) && (18)
\end{aligned}
$$

これより f は単元となる。

2. ($\Longrightarrow$) $1 + f$ は単元であるから (1) より $a_1, \ldots, a_n$ 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。

   ($\Longleftarrow$) 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. ($\Longrightarrow$) $g = b_0 + b_1 x + \cdots + b_m x^m$ 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 $a_n b_m = 0$ であるから $a_n g$ について

$$
\begin{aligned}
f a_n g &= 0 && (19)\\
\deg a_n g &< m && (20)
\end{aligned}
$$

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。

$$
\begin{aligned}
a_n g = a_{n-1} g = \cdots = a_0 g = 0 && (21)\\
b_0 f = 0 && (22)
\end{aligned}
$$

($\Longleftarrow$) 自明。

□

定義 (準同型・同型)**.**
A, B を環, $\phi : A \to B$ を写像とする.

1. ϕ が準同型で逆写像が存在し, 逆写像も準同型であるとき, ϕ 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 $\mathrm{Aut}^{\mathrm{al}} A$ と書く.

命題 6.

$\phi : A \to B$ が環の準同型なら $\phi(0_A) = 0_B$ である. A, B, C を環, $\phi : A \to B$, $\psi : B \to C$ を準同型とするとき, その合成 $\phi \circ \psi : A \to C$ も準同型である. 同様に ϕ, ψ が同型なら, $\phi \circ \psi$ も同型である. $\diamond$

証明

$$\phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) + \phi(0_A) = 0_B \tag{23}$$

$$\begin{aligned} \psi \circ \phi(x+y) &= \psi(\phi(x+y)) = \psi(\phi(x) + \phi(y)) = \psi(\phi(x)) + \psi(\phi(y)) && (24) \\ &= \psi \circ \phi(x) + \psi \circ \phi(y) && (25) \\ \psi \circ \phi(xy) &= \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) && (26) \\ &= \psi \circ \phi(x) \cdot \psi \circ \phi(y) && (27) \\ \psi \circ \phi(1_A) &= \psi(\phi(1_A)) = \psi(1_B) = 1_C && (28) \end{aligned}$$

$\psi \circ \phi$ は準同型である。同型も同様。 $\square$

命題 7.

$\phi : A \to B$ が環の準同型ならば, 単射 $\iff$ $\mathrm{Ker}\,\phi = \{0\}$ $\diamond$

証明

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

$$\begin{aligned} 1 &= \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) && (29) \\ 1 &= xy^{-1} && (30) \end{aligned}$$

より $x = y$ となるから ϕ は単射である. $\square$

命題 8.

$A \neq 0$ 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。

$\diamond$

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。

$(2 \implies 3)$ $\phi : A \to B$ を環準同型とする。このとき $\mathrm{Ker}(\phi)$ は (1) と異なるイデアルであるから $\mathrm{Ker}(\phi) = 0$ である。よって ϕ 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。$\phi : A \to B$ を自然な準同型とすると $\mathrm{Ker}(\phi) = (x)$ である。仮定より ϕ は単射であるから $(x) = 0$。したがって $x = 0$ となる。 $\square$

定義.
A のイデアル $\mathfrak{p}$ は $\mathfrak{p} \neq (1)$ かつ $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ または $y \in \mathfrak{p}$ という条件を満たすとき A の素イデアル (prime ideal) であるという。
A のイデアル $\mathfrak{m}$ は $\mathfrak{m} \neq (1)$ かつ $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq (1)$ を満たすいかなる A のイデアル $\mathfrak{a}$ も存在しないとき A の極大イデアル (maximal ideal) であるという。

定理 9.

$$\mathfrak{p}\text{ が素イデアルである} \iff A/\mathfrak{p}\text{ は整域である} \tag{31}$$
$$\mathfrak{m}\text{ が極大イデアルである} \iff A/\mathfrak{m}\text{ は体である} \tag{32}$$

$\diamond$

証明

$\square$

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

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

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

定義 (n 変数多項式の代入)**.**
$c = (c_1, \cdots, c_n) \in A^n$ とするとき

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

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

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

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

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

は, $a_{i_1,\cdots,i_n} = b_{i_1,\cdots,i_n}$ がすべての $i_1, \cdots, i_n$ 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.

$$(f \pm g)(x) = \sum_{i_1,\cdots,i_n} (a_{i_1,\cdots,i_n} \pm b_{i_1,\cdots,i_n}) x_1^{i_1} \cdots x_n^{i_n} \tag{33}$$

$$f(x)g(x) = \sum_{i_1,\cdots,j_n} a_{i_1,\cdots,i_n} b_{j_1,\cdots,j_n} x_1^{i_1+j_1} \cdots x_n^{i_n+j_n} \tag{34}$$

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 $n > 0$ を整数とするとき, X_n を $\mathbb{N}^n$ から A への写像 a で有限個の $(i_1, \cdots, i_n) \in \mathbb{N}^n$ を除いて値が 0 であるものと $\{1, \cdots, n\}$ から I への単射写像 ϕ 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,

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

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.

命題 10 (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 11 (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 12.

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 13 (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 $SL_n(R)$.