可換環論

Anko

2023 年 7 月 17 日

目次

1 環論

定義 (環)**.**
集合 A に 2 つの演算 $+, \times$ が定義されていて加法, 乗法に関してそれぞれ可換群, モノイドになるかつ分配法則を満たすとき A を環という.

命題 1.
$\forall a \in A \ 0a = a0 = 0$ ◇

証明
$0a = (0+0)a = 0a + 0a$ より $0a = 0$. 逆も同様. □

命題 2.
$1 = 0$ となる環 $\iff$ 0 以外の元のない自明な環. ◇

証明
$a = 1a = 0a = 0$ より任意の元は 0 となり自明な環となる. 逆は自明. □

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

1. 任意の $x, y \in A$ に対し $\phi(x+y) = \phi(x) + \phi(y)$, $\phi(xy) = \phi(x)\phi(y)$ が成り立ち, $\phi(1_A) = 1_B$ であるとき, ϕ を準同型という.
2. 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.
3. $A = B$ 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 3.

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

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. $\square$

命題 4.

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

$\psi \circ \phi(x + y) = \psi(\phi(x + y)) = \psi(\phi(x) + \phi(y)) = \psi(\phi(x)) + \psi(\phi(y)) = \psi \circ \phi(x) + \psi \circ \phi(y)$ 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. $\square$

命題 5.

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

証明

($\Longrightarrow$) ϕ が環の準同型であるから $\phi(0_A) = 0_B$ より $0_A \in \operatorname{Ker}\phi$. また元 $\forall x, y \in \operatorname{Ker}\phi$ について ϕ の単射性より $\phi(x) = \phi(y) \implies x = y$ となり, $\operatorname{Ker}\phi$ 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

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

$$1 = xy^{-1} \tag{2}$$

より $x = y$ となるから ϕ 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 $x = (x_1, \cdots, x_n)$ 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.

$$(f \pm g)(x) = \sum_{i_1, \cdots, i_n} (a_{i_1, \cdots, i_n} \pm b_{i_1, \cdots, i_n}) x_1^{i_1} \cdots x_n^{i_n} \tag{3}$$

$$f(x)g(x) = \sum_{i_1, \cdots, j_n} a_{i_1, \cdots, i_n} b_{j_1, \cdots, j_n} x_1^{i_1 + j_1} \cdots x_n^{i_n + j_n} \tag{4}$$

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.

定理 6.

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

$\diamond$

証明

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

$\square$

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 $a, b \in A\backslash\{0\}$ 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 $d : A\backslash\{0\} \to \mathbb{N}$ 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 $A\backslash\{0\}$ において可換群となる.

定理 7 (環の鎖)**.**

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

証明

(可換環 $\Longrightarrow$ 環) 自明.
(整域 $\Longrightarrow$ 可換環) 自明.
(正規環 $\Longrightarrow$ 整域) 自明.
(UFD $\Longrightarrow$ 正規環) $\alpha \in K$ を解に持つモニック多項式 $f(x) = x^n + \cdots + a_1 x + a_0$ について $a_0 \neq 0$ とすると, $\alpha \neq 0$ である. ここで α 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 $\Longrightarrow$ UFD)
(ユークリッド環 $\Longrightarrow$ 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 $\Longrightarrow$ ユークリッド環) $\square$

命題 8.

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 9 (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 10 (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 11.

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 12 (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 $SL_n(R)$.