

抽象代数

anko

2023 年 5 月 29 日

目次

1	群論	2
2	環論	2
3	加群	6
4	体論	6

1 群論

Definition 1.1 (群). 空集合でない集合 G 上で単位元, 逆元のある結合的な演算が定義されているとき G を群という.

Definition 1.2 (群の位数). 群 G の濃度 $|G|$ を群 G の位数という.
また G について $|G| < \infty$ のとき有限群, $|G| \geq \infty$ のとき無限群という.

Definition 1.3 (部分群). 群 G の部分集合 H が群となるときの H は G の部分群であるという.

2 環論

Definition 2.1 (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.

Proposition 2.2. $\forall a \in A \ 0a = a0 = 0$

Proof. $0a = (0 + 0)a = 0a + 0a$ より $0a = 0$. 逆も同様. ■

Proposition 2.3. $1 = 0$ となる環 \iff 0 以外の元のない自明な環.

Proof. $a = 1a = 0a = 0$ 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.

Definition 2.4 (準同型・同型). A, B を環, $\phi: A \rightarrow B$ 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 $\text{Aut}^{\text{al}} A$ と書く.

Proposition 2.5. $\phi: A \rightarrow B$ が環の準同型なら $\phi(0_A) = 0_B$ である.

Proof. $\phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) + \phi(0_A)$ より $\phi(0_A) = 0_B$ となる. ■

Proposition 2.6. 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 ϕ, ψ が同型なら, $\phi \circ \psi$ も同型である.

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

Proposition 2.7. $\phi : A \rightarrow B$ が環の準同型ならば, 単射 $\iff \text{Ker } \phi = \{0\}$

Proof. (\implies) ϕ 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 ϕ 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

$$1 = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \quad (2.1)$$

$$1 = xy^{-1} \quad (2.2)$$

より $x = y$ となるから ϕ は単射である. ■

Definition 2.8 (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.

Definition 2.9 (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.

Definition 2.10 (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.

Definition 2.11 (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.

$$(f \pm g)(x) = \sum_{i_1, \dots, i_n} (a_{i_1, \dots, i_n} \pm b_{i_1, \dots, i_n}) x_1^{i_1} \cdots x_n^{i_n} \quad (2.3)$$

$$f(x)g(x) = \sum_{i_1, \dots, j_n} a_{i_1, \dots, i_n} b_{j_1, \dots, j_n} x_1^{i_1+j_1} \cdots x_n^{i_n+j_n} \quad (2.4)$$

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.

Definition 2.12 (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 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、

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

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.

Lemma 2.13.

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

Proof.

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

■

Definition 2.14 (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.

Theorem 2.15 (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

Proof. (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 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 \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)

■

Proposition 2.16. 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.

Proof. 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.

■

Proposition 2.17 (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.

Proposition 2.18 (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.

Proof.

■

Proposition 2.19. 体の多項式環はユークリッド環である.

Proof. $d = \deg$ とすると成り立つ.

■

Proposition 2.20 (正規環). $f(x) = a_n x^n + \cdots + a_0 \in A[x]$ で $a_0, a_n \neq 0, \alpha \in K$

Definition 2.21. 1. ネーター環

2. アルティン環

3 加群

Definition 3.1. 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 $SL_n(R)$.

4 体論

Definition 4.1. 体 K について自然な環準同型 $\phi: \mathbb{Z} \ni n \mapsto n \cdot 1 \in K$ の核 $\text{Ker}(\phi) \subset \mathbb{Z}$ は準同型定理 $\mathbb{Z}/\text{Ker}(\phi) \cong \text{Im}(\phi)$ と $\text{Im}(\phi)$ は整域であることから素イデアルである. \mathbb{Z} の素イデアルは (0) または素数 p があり (p) であるから $\text{Ker}(\phi)$ も (0) または (p) である. このとき標数 $\text{ch } K$ はそれぞれ $0, p$ であるという.

Theorem 4.2. 標数に対応する体の性質

1. 標数 0 の体なら, \mathbb{Q} を含む.
2. 標数 $p > 0$ の体なら, \mathbb{F}_p を含む.

Proof. ■

Definition 4.3. K が標数 $p > 0$ の体, n が正の整数で $q = p^n$ とおくと $\text{Frob}_q: K \ni x \mapsto x^q \in K$ をフロベニウス準同型という.

Theorem 4.4. フロベニウス準同型は体の準同型である.

Proof.

$$\text{Frob}_q(x + y) = (x + y)^q = x^q + y^q = \text{Frob}_q(x) + \text{Frob}_q(y) \quad (4.1)$$

$$\text{Frob}_q(xy) = (xy)^q = x^q y^q = \text{Frob}_q(x) \text{Frob}_q(y) \quad (4.2)$$

$$\text{Frob}_q(0) = 0 \quad (4.3)$$

$$\text{Frob}_q(1) = 1 \quad (4.4)$$

■

Definition 4.5. 体の拡大の定義

1. L/K が体の拡大とする. L の K 上のベクトル空間としての次元を $[L : K]$ と書く. 拡大次数 $[L : K]$ が有限なら L/K を有限次拡大, そうでなければ無限次拡大という.
2. n 変数有理式. $\alpha \in L$ により $K(\alpha)$ となるとき, L を K の単拡大という. 有限個の元 $\alpha_1, \dots, \alpha_n \in L$ により $L = K(\alpha_1, \dots, \alpha_n)$ となるとき, L は K 上有限生成であるという.
3. L/K が体の拡大とする. L のすべての元が K 上代数的なら L/K は代数拡大という. そうでなければ, 超越拡大という.

4. K を任意の定数でない 1 変数多項式 $f(x) \in K[x]$ に対し $\alpha \in K$ があり, $f(\alpha) = 0$ となるとき, K を代数閉体という. L/K が代数拡大であり L が代数閉体であるとき, L を K の代数閉包という.
5. L/K が代数拡大とする. L のすべての元が K 上分離的なら L/K を分離拡大という.
6. L/K が代数拡大とする. $\alpha \in L$ なら α の K 上の最小多項式が L 上では 1 次式の積になるとき, L/K を正規拡大という.
7. L/K が分離拡大かつ正規拡大ならガロア拡大という.

Proposition 4.6. $L/M, M/K$ が有限次拡大なら L/K も有限次拡大で $[L : K] = [L : M][M : K]$ となる.

Proof. $l = [L : M], m = [M : K], \{x_1, \dots, x_l\}$ を L の M 上の基底, $\{y_1, \dots, y_m\}$ を M の K 上の基底とする.

このとき $z \in L$ なら $a_i \in M$ があり, $z = \sum_i a_i x_i$ となる. また $b_{ij} \in K$ があり $z = \sum_{i,j} b_{ij} x_i y_j$ となる. よって, $B = \{x_i y_j \mid i = 1, \dots, l, j = 1, \dots, m\}$ は K 加群として L を生成する. ■

Proposition 4.7. 既約な最小多項式

1. $L = K[x]/(f(x))$ は体で $[L : K] = \deg f(x)$ である.

Proof. ■

Theorem 4.8. 以下は互いに同値である.

1. L/K が有限生成かつ代数拡大である.
2. L/K が有限個の代数的な元から生成している.
3. L/K が有限次拡大である.

Proof. $(1 \implies 2)$

代数的でない元から生成すれば超越拡大となることから代数的な元から生成している.

$(2 \implies 3)$

代数的な元から生成するとその最小多項式の次数が拡大次数となることから n に関する帰納法を用いて L/K は有限次拡大である.

$(3 \implies 1)$

$n = [L : K]$ として $x \in L$ なら $1, x, \dots, x^n$ は一次従属である. よって, $a_0 + \dots + a_n x^n = 0$ となる a_0, \dots, a_n が存在する. つまり, x は代数的な元である. これより L/K は代数拡大である.

また, 無限生成ならば無限次拡大であるから有限生成である. ■

Proposition 4.9. L/K が代数拡大, $\alpha \in L$ で, $L \supset M \supset K$ を中間体とする. α が K 上分離的なら M 上でも分離的である.

Proof. $\alpha \in \bar{K}$ の K 上の最小多項式 $f(x)$ が分離多項式であり, $\bar{K} = \bar{M}$ かつ M 上の最小多項式は $f(x)$ を割り切るから分離多項式となり, M 上でも分離的である. ■

Proposition 4.10. $f(x) \in K[x]$ を K 上既約な多項式とする. このとき以下は互いに同値である.

1. $f(x)$ は \bar{K} 上で重根を持つ

$$2. f'(x) = 0$$

3. $\text{ch } K = p > 0$ であり, K 上既約な分離多項式 $g(x)$ と $n > 0$ があり, $f(x) = g(x^{p^n})$ となる.

Proof. $(1 \iff 2)$

$f'(x) = 0$ ならば

$(2 \iff 3)$ ■

Theorem 4.11. Steinitz の定理

1. K の代数拡大 L で, 代数閉体であるものが存在する.

2. $L_1 \supseteq M_1 \supseteq K, L_2 \supseteq M_2 \supseteq K$

Proof. ■

Definition 4.12. 数論に用いられる用語の定義

1. \mathbb{Q} の有限次拡大体を代数体という.

2. $x \in \mathbb{C}$ が \mathbb{Z} 上整なら代数的整数であるという.

3. \mathbb{C} の代数的整数の集合を Ω と書き, 代数的整数環という.

4. L を代数体, Ω を代数的整数環とすると, $L \cap \Omega$ を L の整数環という.