7　環準同型写像, 素イデアルと極大イデアル

• 7-1 : 環準同型写像

2 つの群を比較するときに, 群準同型写像を考えたように, ここでは 2 つの環を比較するために「環準同型写像」を考えよう.

定義 7.1. 2 つの環 R_1 と R_2 を考える. 写像 $f : R_1 \to R_2$ が **環準同型写像** であるとは, 以下の 3 条件を満たすときをいう.

(RH1) 任意の $x, y \in R_1$ に対して, $f(x+y) = f(x) + f(y)$ を満たす.
(RH2) 任意の $x, y \in R_1$ に対して, $f(xy) = f(x)f(y)$ を満たす.
(RH3) $f(1_{R_1}) = 1_{R_2}$ を満たす.

を満たすときをいう. 環準同型写像 f が全単射であるとき, f は **環同型写像** と呼ばれる. R_1 から R_2 への環同型写像があるとき, R_1 と R_2 は **同型** であるといい記号で $R_1 \simeq R_2$ で表す.

例 7-1　(1) **例 6-3** で考えた写像 $f : \mathbb{R}[X] \longrightarrow \mathbb{C}$ を

$$f(a_0 + a_1X + a_2X^2 + \cdots a_nX^n) := a_0 + a_1i + a_2i^2 + \cdots + a_ni^n$$

で定義すると, これは環準同型写像である.

(2) $m > 1$ とする. 自然な射影 $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ は環準同型写像である. 実際, 任意の $x, y \in \mathbb{Z}$ に対して,

$$\pi(x+y) = \overline{x+y} = x\overline{x} + \overline{y} = \pi(x) + \pi(y)$$
$$\pi(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \pi(x)\pi(y)$$
$$\pi(1) = \overline{1}$$

が成り立つからである.

• 7-2 : 環準同型写像の核と像

群準同型写像のときと同様に, 環準同型写像に対して核や像を定義することができる.

定義 7.2. 2 つの環 R_1 と R_2 と環準同型写像 $f : R_1 \to R_2$ を考える.

$$\mathsf{ker}(f) := \{x \in R_1 \mid f(x) = 0\}$$

を f の **核** と呼ぶ. また,

$$\mathsf{im}(f) := \{f(x) \in R_2 \mid x \in R_1\}$$

を f の **像** と呼ぶ.

命題 7.3. 2 つの環 R_1 と R_2 と環準同型写像 $f : R_1 \to R_2$ に対して, 核 $\mathsf{ker}(f)$ は R_1 のイデアルとなる.

証明. まず, $\mathsf{ker}(f)$ が R_1 の部分群であることは**命題 5.4** によってわかる. そこで, 任意の $x \in \mathsf{ker}(f)$ と任意の $r \in R_1$ に対して $rx \in \mathsf{ker}(f)$ を示せば良い. f は環準同型写像であることと, **命題 7.4**(1) により

$$f(rx) = f(r)f(x) = f(r)0 = 0$$

である. よって, $rx \in \mathsf{ker}(f)$ がわかったので $\mathsf{ker}(f)$ は R_1 のイデアルとなる. □

命題 7.4. 2 つの環 R_1 と R_2 と環準同型写像 $f : R_1 \to R_2$ に対して, 像 $\mathsf{im}(f)$ は R_2 の演算によって環となる.

証明. 以下では, $\mathsf{im}(f)$ が環の定義を満たすことを確認しよう. はじめに, $\mathsf{im}(f)$ が R_2 の積について閉じていることを確認する. 任意に $y, y' \in \mathsf{im}(f)$ をとると, 像の定義からある $x, x' \in R_1$ が存在して $y = f(x)$, $y' = f(x')$ を満たす. このとき, f は環準同型写像であるから $yy' = f(x)f(x') = f(xx')$ となるので $yy' \in \mathsf{im}(f)$ である.

(R1) $\mathsf{im}(f)$ が R_2 の和に関して部分群であることは**命題 5.4** によってわかる.
(R2) R_2 の積は結合法則を満たしているので, $\mathsf{im}(f)$ でも結合法則を満たしている.
(R3) 環準同型写像の定義から $1_{R_2} = f(1_{R_1})$ だから $1_{R_2} \in \mathsf{im}(f)$ である.
(R4) R_2 の和 $+$ と積 $\cdot$ に関して分配法則を満たしているので, $\mathsf{im}(f)$ でも和と積に関して分配法則を満たしている.

以上より, 像 $\mathsf{im}(f)$ は R_2 の演算によって環となる. □

さて, 群の場合における準同型定理が環の場合にも成り立つ. (証明は群の場合と同様であるから省略する. 各自で証明を完成させよ.)

定理 7.5 (環準同型定理)**.** 2 つの環 R_1 と R_2 と環準同型写像 $f : R_1 \to R_2$ に対して, 写像

$$\begin{array}{rccc} \overline{f}: & R_1/\mathsf{ker}(f) & \longrightarrow & \mathsf{im}(f) \\ & \overline{x} & \longmapsto & f(x) \end{array}$$

は環の同型写像である. つまり, 環の同型 $R_1/\mathsf{ker}(f) \simeq \mathsf{im}(f)$ が成り立つ.

レポート 7-1　実数係数の多項式環 $\mathbb{R}[X]$ を考える. 写像

$$\begin{array}{rccc} \varphi: & \mathbb{R}[X] & \longrightarrow & \mathbb{R} \\ & a_0 + a_1X + \cdots + a_nX^n & \longmapsto & a_0 \end{array}$$

で定める. このとき, φ は環準同型写像であることを示せ. また, $\mathsf{ker}(\varphi) = (X)$ であることを示せ. (ただし, (X) は X によって生成されたイデアルである.)

命題 7.6. 2 つの環 R_1 と R_2 と環準同型写像 $f : R_1 \to R_2$ に対して, f が単射であることと $\mathsf{ker}(f) = \{0\}$ であることは同値である.

証明. **(必要条件)** $f : R_1 \to R_2$ が単射であるとする. 任意に $x \in \mathsf{ker}(f)$ をとる. このとき, $f(x) = 0$ である. 一方, $f(0) = 0$ であるが, f は単射なので $x = 0$ である. 従って $\mathsf{ker}(f) = \{0\}$ がわかった.
(十分条件) $\mathsf{ker}(f) = \{0\}$ を仮定する. $x, x' \in R_1$ が $f(x) = f(x')$ であると仮定しよう. このとき,

$$0 = f(x) - f(x') = f(x - x')$$

だから $x - x' \in \mathsf{ker}(f)$ である. 仮定より, $x - x' = 0$ だから $x = x'$ が示された. □

- **7-3 : 整域**

まず, 具体例として可換環 $\mathbb{Z}/6\mathbb{Z}$ を考えよう. このとき, $\overline{2}, \overline{3} \in \mathbb{Z}/6\mathbb{Z}$ をとれば, これは両方とも零元 $\overline{0}$ ではない. しかし, これらの積を考えれば,

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$$

である. このように, 一般には可換環 R において, R の元 a, b で $ab = 0$ だからといって, $a = 0$ または $b = 0$ とは限らない. 一方で, $\mathbb{Z}$ のように, $ab = 0$ であれば $a = 0$ または $b = 0$ が成り立つこともある. このような可換環には名前がついているので, それをきちんと定義しよう.

定義 7.7. 可換環 R が, $a, b \in R$ について $ab = 0$ ならば $a = 0$ または $b = 0$ が成り立つとき, R は **整域** と呼ばれる. 対偶をとれば, $a \neq 0$, $b \neq 0$ ならば $ab \neq 0$ であるときをいう.

例 7-2　(1) 整数環 $\mathbb{Z}$ は整域である.

(2) 体は整域である. 実際, F を体として $a, b \in F$ が $ab = 0$ と仮定する. もし, $a \neq 0$ であれば, F は体なので a の逆元 $a^{-1} \in F$ が存在するが. これを $ab = 0$ にかければ $b = 0$ を得る. よって体は整域である.

(3) 体 K 上の多項式環 $K[X]$ は整域である. 実際, $f(X) = a_0 + a_1X + \cdots + a_mX^m$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$ が $f(X) \neq 0$, $g(X) \neq 0$ を満たすとする. ここで, $a_m \neq 0$, $a_n \neq 0$ であるとしよう. このとき,

$$f(X)g(X) = a_0b_0 + (a_1b_0 + a_0b_1)X + \cdots + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + \cdots + a_mb_nX^{m+n}$$

であるが, K は体なので整域であるため $a_mb_n \neq 0$ である. つまり, $f(X)g(X)$ の最高次の係数は 0 ではないので, $f(X)g(X) \neq 0$ である. 以上で $K[X]$ は整域である.

命題 7.8. $m > 1$ とする. $\mathbb{Z}/m\mathbb{Z}$ が整域であるための必要十分条件は m が素数となることである.

証明. **（必要条件）** 対偶を示す. m が素数でないとすると, ある 1 より大きい整数 $m, k \in \mathbb{Z}$ がとれて $n = mk$ とできる. このとき, $1 < m, k < n$ であるから, $\overline{m}$, $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ は零元 $\overline{0}$ ではない. しかし,

$$\overline{m} \cdot \overline{k} = \overline{mk} = \overline{n} = \overline{0}$$

であるから $\mathbb{Z}/m\mathbb{Z}$ は整域ではない.

（十分条件） m が素数であるとき, **命題 6.3** から $\mathbb{Z}/m\mathbb{Z}$ は体であり, 特に整域である. □

• 7-4 : 素イデアル, 極大イデアル

p を素数とする. p によって生成される単項イデアル $p\mathbb{Z}$ を考えよう. もし, $x, y\mathbb{Z}$ であり, $xy \in p\mathbb{Z}$ であったとする. このとき, ある $k \in \mathbb{Z}$ がとれて

$$xy = pk$$

とできる. p は素数であるから素因数分解を考えれば x または y は p の倍数でなければならない. つまり, $x \in p\mathbb{Z}$ または $y \in p\mathbb{Z}$ が成り立つ. このようなイデアルを素数が生成するイデアルということで「素イデアル」というが, これを一般化して定義を与えておこう.

定義 7.9.　(a) 可換環 R の R とは異なるイデアル I が **素イデアル** であるとは, $x, y \in R$ が $xy \in I$ であるならば $x \in I$ または $y \in I$ を満たすときをいう.

(b) 可換環 R の R とは異なるイデアル I が **極大イデアル** であるとは, I を真に含むようなイデアルは R のみであるときをいう.

補題 7.10. I, J を可換環 R のイデアルとする. このとき,

$$I + J := \Big\{ x + y \mid x \in I,\, y \in J \Big\}$$

は R のイデアルとなる.

証明. $I + J$ が R の部分アーベル群であることは容易に確認できる. 任意に $r \in R$ と $x + y \in I + J$ をとると, R は環なので

$$r(x + y) = rx + ry$$

である. I, J は R のイデアルだから $rx \in I$, $ry \in J$ である. 従って $rx + ry \in I + J$ であるから $I + J$ は R のイデアルとなることがわかった. □

レポート 7-2　R のイデアル I, J に対して,

$$IJ := \left\{ \sum_{i=1}^{n} x_iy_i \mid x_i \in I,\, y_i \in J,\, n \geq 0 \right\}$$

は R のイデアルとなることを示せ.

命題 7.11. R の極大イデアル I は素イデアルである.

証明. I を R の極大イデアルとする. $x, y \in R$ で $xy \in I$ であると仮定する. このとき, $x \notin I$ であると仮定すれば, $I + \langle x \rangle$ は R のイデアルとなる. このとき, $x \notin I$ で $x \in I + \langle x \rangle$ であるから, これは I を真に含んでいる. 仮定より, I は極大イデアルだから $I + \langle x \rangle = R$ となる. すると, ある $z \in I$ と $a \in R$ で

$$z + ax = 1$$

とできる. これの両辺に y をかければ

$$zy + axy = y$$

を得る. ここで, I はイデアルだから $xy, zy \in I$ だから $zy + axt = y \in I$ である. 従って I は素イデアルとなる. □

定理 7.12. 可換環 R のイデアルを I とする.

(a) I が素イデアルであることと剰余環 R/I が整域であることは同値である.
(b) I が極大イデアルであることと剰余環 R/I が体であることは同値である.

証明. (a) **（必要条件）** I を素イデアルと仮定する. $\overline{x}, \overline{y} \in R/I$ が $\overline{x} \cdot \overline{y} = \overline{0}$ であると仮定する. このとき, R/I を構成する同値関係の入れ方から $xy - 0 = xy \in I$ であり, I は素イデアルだから $x \in I$ もしくは $y \in I$ が成り立つ. すなわち, $\overline{x} = \overline{0}$ または $\overline{y} = \overline{0}$ が成り立つ.

（十分条件） R/I が整域であると仮定する. $xy \in I$ と仮定すると, $\overline{x} \cdot \overline{y} = \overline{0}$ である. R/I が整域だから $\overline{x} = \overline{0}$ または $\overline{y} = \overline{0}$ が成り立つ. これは $x \in I$ または $y \in I$ が成り立つ. すなわち I は素イデアルとなることが示された.

(b) **（必要条件）** I を極大イデアルと仮定する. 零元 $\overline{0}$ ではない $\overline{x} \in R/I$ をとる. このとき, $x \notin I$ である. そこで, R のイデアル $I + \langle x \rangle$ を考えれば, これは I を真に含むイデアルとなる. I は極大イデアルだから, $I + \langle x \rangle = R$ となる. すなわち, ある $z \in I$ と $a \in R$ が存在して

$$z + ax = 1$$

とできる. このとき,

$$\overline{1} = \overline{z + ax} = \overline{z} + \overline{ax} = \overline{a} \cdot \overline{x}$$

となる. これは, $\overline{a}$ が $\overline{x}$ の逆元であることを表している. 従って R/I は体である.

（十分条件） R/I が体であると仮定する. I が極大イデアルではないとすれば, I, R とは異なるイデアル $I \subset J$ となるものが存在する. このとき,

$$J/I := \left\{ \overline{x} \in R/I \mid x \in J \right\}$$

とおけば, これは $\{0\}$ とも R/I とも異なる R/I のイデアルとなることが容易にわかる. これは, R/I は自明なイデアルではないようなイデアルをもつということなので**命題 6.6** によって R/I が体であることに矛盾する. よって I は極大イデアルとなることがわかった. □

レポート 7-3　証明中の

$$J/I := \left\{ \overline{x} \in R/I \mid x \in J \right\}$$

とおけば, これは $\{0\}$ とも R/I とも異なる R/I のイデアルとなることをきちんと示せ.