6　環・体・イデアル

• 6-1 : 環と体の定義

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ には和に関して群となっていたが, これらは積という演算を同時にもつ. このように, 複数の二項演算をもつような集合を考えよう.

定義 6.1. 集合 R が **環** であるとは, R に和 $+$, 積 $\cdot$ の 2 つの二項演算をもち, 以下の条件を満たすときをいう.

(R1) R は和 $+$ に関してアーベル群である. 和に関する単位元を 0_R で表し, これを R の **零元** と呼ぶ.
(R2) R の積 $\cdot$ は結合法則をみたす. すなわち, 任意の $x, y, z \in R$ に対して, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ を満たす.
(R3) R の積 $\cdot$ に関する単位元 1_R をもつ. すなわち, 任意の $x \in R$ に対して, $x \cdot 1_R = x = 1_R \cdot x$ を満たす 1_R が存在する.
(R4) R の和 $+$ と積 $\cdot$ に関して分配法則を満たす. すなわち, 任意の $x, y, z \in R$ に対して, $x \cdot (y+z) = x \cdot y + x \cdot z$, および $(x+y) \cdot z = x \cdot z + y \cdot z$ を満たす.

環 R の積が可換, すなわち任意の $x, y \in R$ に対して $x \cdot y = y \cdot x$ を満たすならば, R は **可換環** と呼ばれる. 環 R が **斜体** であるとは, 以下の条件を満たすときをいう.

(F) 0_R 以外の任意の元 $x \in R$ は積に関する逆元をもつ. すなわち, ある $y \in R$ で $x \cdot y = 1_R = y \cdot x$ を満たすものが存在する.

可換環 R が斜体であるとき, R を **体** と呼ぶ. 位数が有限であるような体を **有限体** と呼ぶ.

環の積 $x \cdot y$ は簡単のため xy と書かれる.

例 6-1　(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は通常の和と積に関して環となる. 特に, これらは積に関して可換であるから可換環である. また, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ の 0 以外には積に関する逆元をもつので体である. 一方, $\mathbb{Z}$ は $2 \in \mathbb{Z}$ に対して, 積に関する逆元をもたないので体ではない.

(2) $\mathsf{k} = \mathbb{R}$ または $\mathbb{C}$ であるとする. このとき, $\mathsf{Mat}_n(\mathsf{k})$ は行列の和と積に関して環となる. 行列の積は可換ではないので可換環ではない. $\mathsf{Mat}_n(\mathsf{k})$ を **全行列環** と呼ぶ.

(3) $\mathsf{k} = \mathbb{R}$ または $\mathbb{C}$ であるとする. このとき, $\mathsf{k}[X]$ を変数 X に関する多項式全体のなす集合とする. このとき, $f(X) = \sum_{i=0}^{n} a_i X$, $g(X) = \sum_{j=0}^{m} b_j X \in \mathsf{k}[X]$ に対して, 和と積を以下で定義する. $n \leq m$ として, $a_{n+1} = a_{n+2} = \cdots = a_m = 0$ とおき,

$$f(x) + g(x) := \sum_{i=0}^{m} (a_i + b_i) X^i, \quad f(X)g(X) := \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^k$$

と定義する. 多項式の和と積に関して $\mathsf{k}[X]$ は可換環となる. $\mathsf{k}[X]$ を k 上の **多項式環** と呼ぶ.

(4) $m > 1$ とする. $\mathbb{Z}/m\mathbb{Z}$ は次の和と積に関して可換環となる.

$$\overline{x} + \overline{y} := \overline{x+y}, \quad \overline{x} \cdot \overline{y} := \overline{xy}$$

命題 6.2. R を環とする. R の任意の元 $a, b, c \in R$ について, 以下が成り立つ.

(1) $a \cdot 0_R = 0_R = 0_R \cdot a$.
(2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.
(3) $(-a) \cdot (-b) = a \cdot b$.

担当：茨城大学 情報科学領域　宮本 賢伍

証明. (1) $a\cdot 0_R = a\cdot(0_R+0_R) = a\cdot 0_R + a\cdot 0_R$ である. このとき, 等式 $a\cdot 0_R = a\cdot 0_R + a\cdot 0_R$ 両辺に $a\cdot 0_R$ の和に関する逆元 $-a\cdot 0_R$ を加えれば $0_R = a\cdot 0_R$ が示された. 同様にして $0_R\cdot a = 0_R$ も得られる.

(2) 示すことは $(-a)\cdot b$ が $a\cdot b$ の和に関する逆元であることである. ここで

$$(-a)\cdot b + a\cdot b = (-a+a)\cdot b = 0_R\cdot b = 0_R$$

を得る. よって, $(-a)\cdot b = -(a\cdot b)$ である. 同様にして, $a\cdot(-b) = -(a\cdot b)$ である.

(3) $(-a)\cdot(-b) + a\cdot(-b) = (-a+a)\cdot(-b) = 0_R\cdot(-b) = 0_R$ なので, $-a)\cdot(-b)$ は $a\cdot(-b)$ の和に関する逆元である. 逆元の一意性から $(-a)\cdot(-b) = a\cdot b$ である. □

特に, $R=\mathbb{Z}$ で $a=b=1$ とすれば, $(-1)\cdot(-1)=1$ を得る.

レポート 6-1　$i=\sqrt{-1}$ を虚数単位として, 行列 E, I, J, K を以下で定める.

$$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad I=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\quad J=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad K=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$$

このとき, 以下を示せ.

(1) $I^2=J^2=K^2=-E$ を示せ.
(2) $IJ=-JI=K$, $JK=-KJ=I$, $KI=-IK=J$ を示せ.
(3) $R:=\{aE+bI+cJ+dK \mid a,b,c,d\in\mathbb{R}\}$ は環でであることを示せ.
(4) $A=aE+bI+cJ+dK$ を零行列でないとする. A の逆元が

$$\frac{1}{a^2+b^2+c^2+d^2}(aE-bI-cJ-dK)$$

で与えられることを示せ. 従って, R は斜体となるが, これを **Hamilton の四元数体** と呼ぶ.

次の主張はエルガマル暗号の基礎部分を支えている主張である.

定理 6.3. $p>1$ であるとする. $\mathbb{Z}/p\mathbb{Z}$ が体であるための必要十分条件は p が素数となることである.

証明. **（必要条件）**対偶を示す. つまり, p が素数でないとき, $\mathbb{Z}/p\mathbb{Z}$ が体ではないことを示す. p が素数ではないとすれば, p は合成数である. つまり, $1<x,y<p$ なる整数 $x,y\in\mathbb{Z}$ で $p=xy$ とかける. このとき, $\overline{xy}=\overline{p}=\overline{0}$ である. さて, 背理法によって $\mathbb{Z}/p\mathbb{Z}$ が体でないことを示そう. $\mathbb{Z}/p\mathbb{Z}$ が体であるとすれば, $\overline{x}$ に逆元 $\overline{x}^{-1}$ が存在する. $\overline{xy}=\overline{0}$ の左から $\overline{x^{-1}}$ をかけると $\overline{y}=\overline{0}$ を得るが, これは矛盾である. 以上で $\mathbb{Z}/p\mathbb{Z}$ が体ではない.

（十分条件）p を素数とする. $0<m<p$ であるような $m\in\mathbb{Z}$ に対して $\overline{m}\in\mathbb{Z}/m\mathbb{Z}$ が逆元を持つことを示せばよい. m と p は互いに素なので, Euclid の互除法によって

$$xm+yp=1$$

となるような整数 $x,y\in\mathbb{Z}$ が取れる. 従って, $\overline{1}=\overline{xm+yp}=\overline{xm}$ となる. よって $\overline{x}$ は逆元をもったので $\mathbb{Z}/m\mathbb{Z}$ は体である. □

• 6-2 : 可換環のイデアル

環 $\mathbb{Z}$ の部分群 $m\mathbb{Z}$ は正規部分群であって, 剰余群 $\mathbb{Z}/m\mathbb{Z}$ が構成された. さらに, $\mathbb{Z}/m\mathbb{Z}$ は環という数学的構造をもった, そこでこれを一般化して, 環 R の何かしらの部分群 I をもって新しく環 R/I を作ることを考えよう.

定義 6.4. 可換環 R のアーベル群としての部分群 I が R の **イデアル** とは, 次の条件を満たすときをいう.

(ID) 任意の $r\in R$ と任意の $x\in I$ に対して $rx\in I$ である.

例 6-2　(1) 整数全体のなす環 $\mathbb{Z}$ の部分群 $m\mathbb{Z}$ はイデアルとなる.

(2) 環 R に対して, $\{0\}$ および R 自身は R のイデアルとなる. これを R の **自明なイデアル** という.

(3) 多項式環 $\mathsf{k}[X]$ と $f(X) \in \mathsf{k}[X]$ に対して,

$$(f(X)) := \{f(X)g(X) \mid g(X) \in \mathsf{k}[X]\}$$

(4) 可換環 R の任意の元 a に対して,

$$aR = \{ax \mid x \in R\}$$

とおいたものを, **a によって生成される単項イデアル** と呼ぶ. これを (a) で表す. (3) にあった $(f(X))$ は $f(X)$ によって生成される単項イデアルである.

命題 6.5. 環 $\mathbb{Z}$ のイデアルはすべて単項イデアルとなる. つまり, $\mathbb{Z}$ の任意のイデアル I に対して, ある $n \in \mathbb{Z}$ が存在して, $I = (n)$ とできる.

証明. 環 $\mathbb{Z}$ の任意のイデアル I をとる. $I = \{0\}$ ならば, **命題 6.2** より $I = (0)$ であり, これは単項イデアルである. そこで, 以下, $I \neq (0)$ と仮定する. 任意にゼロでない $a \in I$ をとれば, $-a = (-1)a \in I$ なので $a > 0$ と仮定しても良い.

まず, $a_0 \in I$ を, I に含まれる整数の中で最小の整数であるものをとる. すると, $I = (a_0)$ となる. これを証明しよう. イデアルの定義より, $a_0 \in I$ だから任意の整数 $k \in \mathbb{Z}$ に対して $ka_0 \in I$ である. 従って $(a_0) \subset I$ である. 逆に, 任意に $x \in I$ をとると, ある整数 $q, r \in \mathbb{Z}$ が存在して

$$x = qa_0 + r \quad (0 \leq r \leq a_0 - 1)$$

とできる. このとき, $r = x - qa_0$ であって, $x, a_0 \in I$ だから $r \in I$ である. ところで, $r \neq 0$ ならば, a_0 の最小性に矛盾する. よって $r = 0$ となり, $x = ka_0 \in (a_0)$ である. 以上で, $\mathbb{Z}$ の任意のイデアルは単項イデアルとなることがわかった. □

命題 6.6. 可換環 R が体である必要十分条件は, R のイデアルが自明なイデアルのみであることである.

証明. **（必要条件）**：R を体として, I を R のイデアルとする. $I = \{0\}$ でないと仮定しよう. このとき, $I = R$ であることを示す. $I \subset R$ は自明なので, $R \subset I$ を示せば良い. 零元でないような任意の元 $a \in I$ をとる. R は体なので, a の逆元 $a^{-1} \in R$ がとれる. I はイデアルなので, $aa^{-1} = 1 \in I$ である. ここで, 任意に $r \in R$ をとれば, I はイデアルなので, $r = r \cdot 1 \in I$ となり $R = I$ が示された. 以上で R には自明なイデアルしか存在しない.

（十分条件）：R の零元でないような任意の元 $r \in R$ をとり、これに逆元があることを示す. $r \neq 0$ であるから, r によって生成される単項イデアル $\langle r \rangle \neq \{0\}$ である. R は自明なイデアルしかもたないので, $\langle r \rangle = R$ である. よって, $1 \in \langle r \rangle$ だから, ある元 $s \in R$ が存在して $rs = 1$ とできる. よって r が逆元をもったので, R は体である. □

- **6-3 : 剰余環**

可換環 R とそのイデアル I を考える. このとき, R 上の同値関係 $\sim$ を

$$x \sim y \quad \overset{\text{def}}{\iff} \quad x - y \in I$$

で定める. （これが同値関係になることは, 各自で確かめよ. ）この同値関係による商集合を R/I とかく. $x \in R$ の同値類を $\overline{x}$ とかくことにする. 商集合 R/I に和と積を以下で定義しよう.

$$\overline{x} + \overline{y} := \overline{x + y}, \quad \overline{x} \cdot \overline{y} = \overline{xy}$$

担当：茨城大学 情報科学領域　宮本 賢伍

この和と積は well defined である．この和と積に関して R/I は可換環となることが確かめられる．これを R の I による **剰余環** と呼ぶ．

レポート 6-2 R/I における和と積が well-defined であり，この和と積に関して環となることを定義に従って示しなさい．

例 6-3　(1) 環 $\mathbb{Z}$ のイデアルは，ある整数 m で $(m) = m\mathbb{Z}$ の形をしていた．このとき，剰余群 $\mathbb{Z}/m\mathbb{Z}$ は環になっている．

(2) 実数 $\mathbb{R}$ 上の 1 変数多項式環 $\mathbb{R}[X]$ を考える．このとき，$X^2+1 \in \mathbb{R}[X]$ によって生成される単項イデアル (X^2+1) を考えよう．このとき，剰余環 $\mathbb{R}[X]/(X^2+1)$ を考えることができる．すると，

$$\overline{X^2+1} = \overline{0}$$

であるから，$\overline{X}^2 = \overline{-1}$ が得られる．つまり，$\overline{X}$ に関して 2 次以上の項は次数を下げて，1 次以下にすることができるので

$$\mathbb{R}[X]/(X^2+1) = \{\overline{a} + \overline{bX} \mid a, b \in \mathbb{R},\ \ \overline{X}^2 = \overline{-1}\}$$

と表せる．

さて，写像 $f : \mathbb{R}[X] \longrightarrow \mathbb{C}$ を

$$f(a_0 + a_1X + a_2X^2 + \cdots a_nX^n) := a_0 + a_1 i + a_2 i^2 + \cdots + a_n i^n$$

で定義する．つまり，$X = i$ を代入する写像である．このとき，$n \leq m$ として

$$\begin{aligned} f\left(\sum_{k=0}^{n} a_kX^k + \sum_{k=0}^{m} b_kX^k\right) &= f\left(\sum_{k=0}^{n}(a_k+b_k)X^k\right) \\ &= \sum_{k=0}^{n}(a_k+b_k)i^n = \sum_{k=0}^{n} a_k i^k + \sum_{k=0}^{m} b_k i^k = f\left(\sum_{k=0}^{n} a_kX^k\right) + f\left(\sum_{k=0}^{m} b_kX^k\right) \end{aligned}$$

であるので，f は群準同型写像である．任意に $a+bi \in \mathbb{C}$ をとれば，$f(a+bX) = a+bi$ なので，f は全射である．つまり，$\mathsf{im}(f) = \mathbb{C}$ である．従って，準同型定理**定理 5.6** から群の同型

$$\mathbb{R}[X]/\mathsf{ker}(f) \simeq \mathsf{im}(f) = \mathbb{C}$$

である．ここで，$\mathsf{ker}(f) = (X^2+1)$ であることを確認しよう．任意に $g(X) \in \mathsf{ker}(f)$ をとる．$g(X)$ を X^2+1 で割ると，除法の定理から，

$$g(X) = h(X)(X^2+1) + a + bX, \quad h(X) \in \mathbb{R}[X],\ a, b \in \mathbb{R}$$

とできる．このとき，

$$0 = f(g(X)) = g(i) = h(i)(i^2+1) + a + bi = a + bi$$

であるので，$a + bi = 0$．よって，$a = b = 0$ を得るので，$g(X) = h(X)(X^2+1)$ となる．すなわち，$g(X) \in (X^2+1)$ であるので，$\mathsf{ker}(f) \subset (X^2+1)$ である．逆に，任意に $g(X) \in (X^2+1)$ をとれば，$g(X) = h(X)(X^2+1)$ となるような $h(X) \in \mathbb{R}[X]$ が存在する．このとき，

$$f(g(X)) = g(i) = h(i)(i^2+1) = h(i)(-1+1) = 0$$

であるから，$g(X) \in \mathsf{ker}(f)$ となる．よって，$(X^2+1) \subset \mathsf{ker}(f)$ である．以上で $\mathsf{ker}(f) = (X^2+1)$ である．よって，

$$\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$$

を得る．このようにして，複素数 $\mathbb{C}$ は実数上の多項式環の剰余環として実現されるのである．