

6 代数系の基礎 (4) – 環と体 –

● 6-1: 環の定義

代数系 $(G, *)$ は演算 $*$ に関して **群** であるとは、次の 3 条件を満たすことであった。

$$(G1) \quad \forall x \in G, \forall y \in G, \forall z \in G, (x * y) * z = x * (y * z).$$

$$(G2) \quad \exists e \in G \text{ (s.t.) } \forall x \in G, e * x = x * e = x.$$

$$(G3) \quad \forall x \in G, \exists y \in G \text{ (s.t.) }, x * y = y * x = e.$$

定義 6.1. 群 $(G, *)$ が **アーベル群** であるとは、任意の $x, y \in G$ に対して、

$$x * y = y * x$$

が成り立つときをいう。

例 6-1 $\mathbb{Z}$ や $\mathbb{Z}/m\mathbb{Z}$ は和についてアーベル群となる。一方、 $\text{GL}(\mathbb{R})$ は行列の積について群であるが、アーベル群ではない。また、対称群 S_n もその積についてアーベル群ではない。

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 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、2 つの二項演算をもつような集合を考えよう。

定義 6.2. 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) 代数系 $(R, +)$ は**アーベル群**である。

(R2) 代数系 $(R, \cdot)$ 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) 代数系 $(R, \cdot)$ は**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、

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

を満たす。

環の積 $x \cdot y$ は簡単のため xy と書かれる。環 R の積について、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 は **和と積の 2 つの二項演算をもつ**。このとき、**和に関しては群** であるが、**積に関しては、結合法則と単位元の存在のみ要求している**。

- 和に関する単位元を 0_R で表し、これを R の **零元** と呼ぶ。
- 和に関する x の逆元を $-x$ で表す。
- **もし仮に** $x \in R$ が積に関する逆元をもつ、すなわち、ある $y \in R$ で

$$xy = 1_R = yx$$

を満たすものが存在する**ならば**, x は **可逆元** と呼ばれ, x の逆元 y を x^{-1} で表し, これを x インバースと呼ぶ.

例 6-2 (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, これらは可換環である.

(2) $m > 1$ とする. $\mathbb{Z}/m\mathbb{Z}$ は第 3 章で定義した和と積

$$[x] + [y] := [x + y], \quad [x] \cdot [y] := [xy]$$

に関して可換環となる.

(3) k を $\mathbb{R}$ もしくは $\mathbb{C}$ とする. このとき, $\text{Mat}_n(k)$ は行列の和と積に関して環となる. $\text{Mat}_n(k)$ を **全行列環** と呼ぶ. これは可換環ではない

(4) k を $\mathbb{R}$ もしくは $\mathbb{C}$ とする. このとき, $k[X]$ を変数 X に関する多項式全体のなす集合とする. つまり,

$$k[X] := \{f(X) = a_0 + a_1X + \cdots + a_nX^n \mid a_0, a_1, \dots, a_n \in k, n \geq 0\}$$

で表される集合とする, 2 つの多項式 $f(X) = \sum_{i=0}^n a_iX^i, g(X) = \sum_{j=0}^m b_jX^j \in k[X]$ 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 $k[X]$ は可換環となる. $k[X]$ を k 上の **多項式環** と呼ぶ.

• 6-2: 「マイナス × マイナス」と「0 による割り算」

中学 1 年生の数学で初めて負の数や文字式を学ぶと, 次の疑問を抱く人は多い.

なぜ, $(-1) \times (-1) = 1$ なのだろうか? なぜ, 数は 0 では割ってはいけないのか?

これらには様々な説明がなされるが, ここでは「環」の言葉から機械的な説明を与えよう.

命題 6.3. 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) $(-a) \cdot (-b) = a \cdot b$.

証明. (1) 0_R は零元であることと, 分配則 (R4) により

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

である. このとき, 等式 $a \cdot 0_R = a \cdot 0_R + a \cdot 0_R$ の両辺に $a \cdot 0_R$ の和に関する逆元 $-(a \cdot 0_R)$ を加えれば $0_R = a \cdot 0_R$ を得る. 同様に $0_R \cdot a = 0_R$ も示せる.

(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 $a \cdot (-b) = -(a \cdot b)$ である.

(3) 分配則 (R4) によって,

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

なので, $(-a) \cdot (-b)$ は $a \cdot (-b)$ の和に関する逆元である. (2) と逆元の一意性 (**命題 4.6**) から $(-a) \cdot (-b) = a \cdot b$ である. □

命題 6.3 (3) を, $R = \mathbb{Z}$, $a = b = 1$ として適用すれば

$$(-1) \cdot (-1) = 1 \times 1 = 1$$

を得るのである.

また, もし 0 で割る操作を許したとすれば, $\mathbb{C}$ には 0 の逆元 0^{-1} が存在する. 逆元の定義から, $0 \cdot 0^{-1} = 1$ であるが, 命題 6.3 (1) より $0 \cdot 0^{-1} = 0$ なので $1 = 0$ を得る. (既に矛盾だが,) a は任意の複素数とすれば, $a \cdot 1 = a \cdot 0 = 0$ となり, $\mathbb{C} = \{0\}$ を得る. ゆえに, 任意の複素数が 0 となるという結論を得てしまうのである.

• 6-3: 体の定義

定義 6.4. 可換環 R が **体** であるとは, 以下の条件を満たすときをいう.

(F) 0_R を除く任意の $x \in R$ は可逆元である.

R が有限集合であるような体を **有限体** と呼ぶ.

例 6-3 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は通常の和と積に関して可換環であり, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は 0 を除く全ての元に逆数が存在するから体である.

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 6.5. $p > 1$ 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, 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, $[xy] = [p] = [0]$ 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, $[x]$ に逆元 $[x]^{-1}$ が存在する. $[xy] = [0]$ の左から $[x^{-1}]$ をかけると $[y] = [0]$ 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 $[m] \in \mathbb{Z}/m\mathbb{Z}$ 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, m と p の最大公約数は 1 だから

$$xm + yp = 1$$

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

従って, p が素数のとき, $\mathbb{Z}/p\mathbb{Z}$ が有限体と例となる.

^{*1} 6-A 節を参照

小テスト 6-1 次の記述の **太字** で示している下線部のうち、1 箇所だけ誤った記述がある。誤っている箇所と、それを正しく訂正したものの組み合わせとして適切なものを選べ。

- (1) 環 R は **和** に関して群であるから、**任意の** $x \in R$ に対して逆元、つまり、 $\underline{xy = 1_R = yx}$ となるような $y \in R$ が **ただ一つ** 存在する。
- (2) 集合 R が体であるとは、 R が **可換環** であり、**零元** を除くすべての $x \in R$ が **逆元** をもつときをいい、**有理数全体のなす集合** は有限体の例である。
- (3) 集合 R が環であることを示すには、**和に関してアーベル群である** こと、**和に関して結合法則を満たす** こと、**積に関して単位元をもつ** こと、**和と積に関して分配則を満たす** ことを示せば良い。
- (4) 整数全体の集合 $\mathbb{Z}$ は **アーベル群** ではあるが、**環** ではない理由は、例えば **2** の積に関する逆元が **整数ではない** からである。
- (5) 整数 p が **素数** であるとき、**またそのときに限り** $\mathbb{Z}/p\mathbb{Z}$ は体となる。例えば、 **$p = 57$** のとき、 $\mathbb{Z}/p\mathbb{Z}$ は体であり、 **$[0]$ を除く** 任意の元には逆元が存在する。

小テスト 6-2 次のうち、環となるものをすべて選べ。

- (a) 剰余の和と積に関して $\mathbb{Z}/20\mathbb{Z}$.
- (b) 多項式の和と積に関して $\mathbb{C}[X]$.
- (c) 通常のと積に関して $\mathbb{N}$.
- (d) 通常のと積に関して $\mathbb{Z} \setminus \{0\}$.
- (e) 行列の和と積に関して $\text{Mat}_2(\mathbb{Z})$.
- (f) 行列の和と積に関して $\text{GL}_2(\mathbb{R})$.

演習問題 6-1 $\mathbb{Z}/4\mathbb{Z}$ の元のうち、積に関する逆元を持たないものを求めよ。また、 $\mathbb{Z}/5\mathbb{Z}$ の各元の積に関する逆元をすべて求めよ。

演習問題 6-2 $i = \sqrt{-1}$ 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。このような R は **Hamilton の四元数体** と呼ばれる。

演習問題 6-3 $\mathbb{R}[X]$ の部分集合 I を

$$I := \{(X^2 + 1)f(X) \mid f(X) \in \mathbb{R}[X]\}$$

と定める。次の問いに答えよ。

- (1) I は和に関して群であることを示せ。
- (2) 任意の $g(X) \in \mathbb{R}[X]$ と、任意の $h(X) \in I$ に対して、 $g(X)h(X) \in I, h(X)g(X) \in I$ であることを示せ。
- (3) $\mathbb{R}[X]$ 上の二項関係 R を、

$$g(X) \sim h(X) \stackrel{\text{def}}{\iff} g(X) - h(X) \in I$$

と定義すれば、これが $\mathbb{R}[X]$ 上の同値関係となることを示せ。

- (4) (3) で定めた商集合 $\mathbb{R}[X]/\sim$ における $f(X) \in \mathbb{R}[X]$ の像を $[f(X)]$ とおく. $\mathbb{R}[X]/\sim$ 上に和と積を

$$[f(X)] + [g(X)] := [f(X) + g(X)], \quad [f(X)] \cdot [g(X)] := [f(X)g(X)]$$

と定めれば, これが well-defined であることを示せ.

- (5) 商集合 $\mathbb{R}[X]/\sim$ は (4) で定めた和と積について環をなすことを示せ.

- (6) 写像 $f: \mathbb{C} \rightarrow \mathbb{R}[X]/\sim$ を, $a + bi \in \mathbb{C}$ ($a, b \in \mathbb{R}$) に対して

$$f: \mathbb{C} \longrightarrow \mathbb{R}[X]/\sim; \quad a + bi \longmapsto [a + bX]$$

と定義すると, 以下が成り立つことを示せ.

- (i) f は well-defined であることを示せ.
- (ii) 任意の $\alpha, \beta \in \mathbb{C}$ に対して $f(\alpha + \beta) = f(\alpha) + f(\beta)$ である.
- (iii) 任意の $\alpha, \beta \in \mathbb{C}$ に対して $f(\alpha\beta) = f(\alpha)f(\beta)$ である.
- (iv) $f(1) = 1$ である.
- (v) f は全単射である.

• 6-A : $ax + by$ の形をした最小の正の数

定理. $a, b \in \mathbb{N}$ に対して, 集合 L を

$$L := \{ax + by \mid a, b \in \mathbb{Z}\}$$

とおく. このとき, L に属する最小の自然数は a と b の最大公約数である.

証明. a と b の最大公約数を g とおき, L に属する最小の自然数を d とおく. $d \in L$ なので, ある $x_0, y_0 \in \mathbb{Z}$ で

$$d = ax_0 + by_0$$

となるものが存在する. 除法の原理によって, L に属する元 $ax + by$ を d で割ると

$$ax + by = qd + r \quad (q \in \mathbb{Z}, \quad 0 \leq r < d)$$

となるような q と r をとることができる. このとき,

$$r = a(x - qx_0) + b(y - qy_0)$$

であり, $x - qx_0$ と $y - qy_0$ は共に整数なので $r \in L$ であるが, d は L に属する最小の自然数なので $r = 0$ でなければならない. 従って, L の元は d の倍数であることがわかる. 特に, d は $a = a \cdot 1 + b \cdot 0$ と $b = a \cdot 0 + b \cdot 1$ を割り切るので, d は a と b の公約数である. ゆえに, $d \leq g$ がわかった.

一方, g は a と b を割り切るので, 任意の整数 $x, y \in \mathbb{Z}$ に対して, $ax + by$ も割り切る. ゆえに, g は d も割り切るので $g \leq d$ である.

以上で $g = d$ であることが示された. □

これにより, 次の系を得る.

系. $a, b \in \mathbb{N}$ が互いに素であるとすれば, $ax + by = 1$ を満たす整数の組 (x, y) が存在する.