環論 (第 1 回)

1. 環の定義と性質

加法と乗法が定義され, いくつかの条件を満たす集合を環と言う. 例えば, 整数全体の集合や複素係数多項式全体の集合などが環になる. 今回は環の定義と基本的な性質について解説する.

定義 1-1.
集合 A に演算 $+$ と $\cdot$ が定義され, 次の (1) から (4) を満たすとき, A を**環**といい, さらに (5) も満たすとき**可換環**という.

(1) A は $+$ に関して可換群になる. つまり,

(1-1) $a+(b+c)=(a+b)+c\ \ (\forall a,b,c\in A)$. (加法の結合法則).

(1-2) $+$ について次を満たす元 0_A がある.

$$a+0_A=0_A+a=a\ \ (\forall a\in A).$$

0_A を A の**零元**という.

(1-3) 任意の $a\in A$ に対して,

$$a+b=b+a=0_A$$

を満たす $b\in A$ が存在する. このような元 b を a の**加法的逆元**といい, $(-a)$ で表す.

(1-4) $a+b=b+a\ \ (\forall a,b\in A)$. (加法の可換性)

(2) $a\cdot(b\cdot c)=(a\cdot b)\cdot c\ \ (\forall a,b,c\in A)$ (乗法の結合法則).

(3) 分配法則が成り立つ. つまり,

(3-1) $a\cdot(b+c)=a\cdot b+a\cdot c\ \ (\forall a,b,c\in A)$.

(3-2) $(b+c)\cdot a=b\cdot a+c\cdot a\ \ (\forall a,b,c\in A)$.

(4) $\cdot$ に関して次を満たす $1_A\in A$ が存在する.

$$a\cdot 1_A=1_A\cdot a=a\ \ \ (\forall a\in A).$$

1_A を A の**単位元**という.

(5) $a\cdot b=b\cdot a\ \ (\forall a,b\in A)$. (乗法の可換性)

(補足)

(1) 0_A, 1_A, $a \cdot b$ はそれぞれ, 0, 1, ab と略することもある.

(2) 定義 1-1 の 0_A, 1_A は A の中にただ一つだけである. また各 $a \in A$ に対して, a の加法的逆元もただ一つだけである.

(3) 引き算 $a-b$ は $a+(-b)$ として定める.

(4) $a \in A$, $n \in \mathbb{Z}$ に対して, na を次で定める.

$$na = \begin{cases} \underbrace{a+a+\cdots+a}_{n\ \text{個}} & n \geq 1 \text{ のとき}, \\ 0_A & n = 0 \text{ のとき}, \\ \underbrace{(-a)+(-a)+\cdots+(-a)}_{|n|\ \text{個}} & n \leq -1 \text{ のとき}. \end{cases}$$

(4) $a \in A$, $n \in \mathbb{Z}$ $(n \geq 0)$ に対して, a^n を次で定める.

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\ \text{個}} & n \geq 1 \text{ のとき}, \\ 1_A & n = 0 \text{ のとき}. \end{cases}$$

問題 1-1 定義 1-1 の条件 (4) を満たす 1_A は A の中にただ一つだけであることを示せ.

まず, 馴染みのある例をいくつか挙げる.

例 1-1

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は通常の足し算と掛け算で可換環である.

(2) 複素係数多項式全体 $A = \mathbb{C}[x]$ は通常の足し算と掛け算で可換環となる. A の零元 0_A はゼロ多項式 (=全ての係数が 0 の多項式) であり, 単位元 1_A は定数多項式 1 である.

☆ 一般的な多項式環については, 後々の資料で詳しく解説する.

次に可換環でない例もみておく.

例 1-2
　複素 2 次正方行列全体

$$M_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{C} \right\}$$

は行列の足し算と掛け算で環となる. このとき, 零元と単位元は

$$0_A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad 1_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

である. また,

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

なので, $M_2(\mathbb{C})$ は可換環ではない.

　次は少し変わった例を紹介する. この例を用いて, 「環のであること」の証明の仕方を説明する.

例題 1-1
　集合

$$A = \{(a,b) \mid a,b \in \mathbb{R}\}$$

を考える. また, A に次で演算を定義する.

$$\begin{aligned} (a,b)+(c,d) &\overset{\text{def}}{=} (a+c, b+d), \\ (a,b)\cdot(c,d) &\overset{\text{def}}{=} (ac, ad+bc). \end{aligned}$$

このとき, A は可換環で $0_A = (0,0), \quad 1_A = (1,0)$ である.

(証明) A が可換環であることを示すためには, 定義 1-1 の (1) から (5) の条件を確認すればよい. ここでは, (2), (4) のみを確認する.

(2) $p=(a,b), q=(c,d), r=(e,f) \in A$ とする. このとき,

$$(p\cdot q)\cdot r = p\cdot(q\cdot r) \qquad \text{(eq1)}$$

を示せばよい. 左辺と右辺の式をそれぞれ計算すると,

$$\begin{aligned} (p \cdot q) \cdot r &= (ac, ad + bc) \cdot (e, f) \\ &= (ace, acf + (ad + bc)e) \\ &= (ace, acf + ade + bce). \\ p \cdot (q \cdot r) &= (a, b) \cdot (ce, cf + de) \\ &= (ace, a(cf + de) + bce) \\ &= (ace, acf + ade + bce). \end{aligned}$$

よって (eq1) が成立する.

(4) $(1, 0)$ が単位元であること . つまり,

$$(1, 0) \cdot p = p \cdot (1, 0) = p \quad (\forall p \in A) \qquad \text{(eq2)}$$

を示せばよい. $p = (a, b)$ とすると,

$$\begin{aligned} (1, 0) \cdot p = (1, 0) \cdot (a, b) = (a, 1 \cdot b + 0 \cdot a) = (a, b) = p, \\ p \cdot (1, 0) = (a, b) \cdot (1, 0) = (a, a \cdot 0 + 1 \cdot b) = (a, b) = p. \end{aligned}$$

よって (eq2) が成立する.

□

問題 1-2 例題 1-1 の環において定義 1-1 の (3-1) が成り立つことを確認せよ.

問題 1-3 例題 1-1 の環 A で考える.

(1) $((2, 1) + (1, 1)) \cdot (-1, 2)$ を計算せよ.

(2) 自然数 n に対して $(0, 1)^n$ を求めよ.

環の基本的な性質を紹介する. 複素数において $(-1) \times (-1) = 1$ が成り立つが, これは一般の環上で成立する性質である.

定理 1-1

A を環, $a, b, c \in A$ とする.

(1) $a \cdot 0_A = 0_A \cdot a = 0_A$.

(2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

(3) $(-a) \cdot (-b) = a \cdot b$.

☆ (3) および 1_A の定義から

$$(-1_A) \cdot (-1_A) = 1_A \cdot 1_A = 1_A.$$

[証明]
(1) $a \cdot 0_A = 0_A$ のみ示す. 0_A の定義から $0_A + 0_A = 0_A$. よって

$$a \cdot (0_A + 0_A) = a \cdot 0_A.$$

分配法則より,

$$a \cdot 0_A + a \cdot 0_A = a \cdot 0_A.$$

この両辺に $-(a \cdot 0_A)$ を足せば, $a \cdot 0_A = 0_A$.

(2) $(-a) \cdot b = -(a \cdot b)$ のみ示す. 分配法則と (1) より,

$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0_A \cdot b = 0_A.$$

両辺に $-(a \cdot b)$ を足せば $(-a) \cdot b = -(ab)$.

(3) $a \cdot b + (-a \cdot b) = 0_A$ より $a \cdot b = -(-a \cdot b)$ を得る. 従って, (2) から

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

□

問題 1-4 A を環とする. $1_A = 0_A$ のとき, $A = \{0_A\}$ を示せ.

問題 1-5 A を可換環とする. $a, b \in A$ に対して, $(a + b) \cdot (a - b) = a^2 - b^2$ を示せ.