

4 代数系の基礎 (2) – 群 –

● 4-1 : 代数系

整数全体の集合 $\mathbb{Z}$ は、**通常**の和に関して次の性質をもつ。

$$(O) \quad \forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x + y \in \mathbb{Z}.$$

$$(I) \quad \forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, (x + y) + z = x + (y + z).$$

$$(II) \quad \text{特別な数 } 0 \in \mathbb{Z} \text{ は, } \forall x \in \mathbb{Z}, x + 0 = x = 0 + x \text{ を満たす.}$$

$$(III) \quad \forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, (\text{s.t.}) x + y = 0 = y + x.$$

また、実数の成分をもつ n 次の正則行列全体

$$\text{GL}_n(\mathbb{R}) := \{A \mid A \text{ は実数の成分をもつ } n \text{ 次の正則行列}\}$$

は、**行列の積**に関して次の性質をもつ、

$$(O') \quad \forall A \in \text{GL}_n(\mathbb{R}), \forall B \in \text{GL}_n(\mathbb{R}), AB \in \text{GL}_n(\mathbb{R}).$$

$$(I') \quad \forall A \in \text{GL}_n(\mathbb{R}), \forall B \in \text{GL}_n(\mathbb{R}), \forall C \in \text{GL}_n(\mathbb{R}), (AB)C = A(BC).$$

$$(II') \quad \text{単位行列 } E \in \text{GL}_n(\mathbb{R}) \text{ は, } \forall A \in \text{GL}_n(\mathbb{R}), AE = A = EA \text{ を満たす.}$$

$$(III') \quad \forall A \in \text{GL}_n(\mathbb{R}), \exists B \in \text{GL}_n(\mathbb{R}), (\text{s.t.}) AB = E = BA.$$

このように、「通常

(O), (O') : 任意の 2 つの元に演算を施した結果は、**再びもとの集合に属している**。

定義 4.1. 空でない集合 G に対して、写像 $*$: $G \times G \rightarrow G$ を G の **二項演算** という。 $(a, b) \in G \times G$ のこの写像による像を $a * b$ 、あるいは単に ab とかく。このとき、組 $(G, *)$ を **代数系** という。

代数系 $(G, *)$ において、行列の積のように、いつでも $x * y = y * x$ が成り立つとは限らないことに注意しよう。

例 4-1 (1) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ は代数系である。また、 $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ も代数系である。一方、差に関しては $(\mathbb{N}, -)$ は $2 - 3 = -1 \notin \mathbb{N}$ であるから代数系ではない。

(2) $m \in \mathbb{N}$ とする。このとき、 $(\mathbb{Z}/m\mathbb{Z}, +)$ と $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ は代数系である。

(3) k を $\mathbb{R}$ または $\mathbb{C}$ とする。 $\text{Mat}_n(k)$ を成分が k の要素であるような n 次正方行列全体とする。このとき、行列の和と積に関して $(\text{Mat}_n(k), +)$, $(\text{Mat}_n(k), \cdot)$ は代数系である。また、 $(\text{GL}_n(k), \cdot)$ は代数系である。一方、 $(\text{GL}_n(k), +)$ は、 $A \in \text{GL}_n(k)$ に対して、 $A + (-A) = O \notin \text{GL}_n(k)$ だから代数系ではない。

● 4-2 : 結合法則

例えば、 $(3 + 4) + 5 = 12 = 3 + (4 + 5)$ の様に、数や行列の和、積はどの順序で計算しても同じ結果になる。

(I), (I') : 演算を施すとき、**演算の順序によらず結果は同じ** になる。

これは、任意の 3 つの要素 x, y, z に対して、「 x と y を演算したものに、 z との演算を計算した結果」と「 x に、 y と z を演算したものの演算を計算した結果」が等しいことを述べている。

定義 4.2. $(G, *)$ を代数系とする. 二項演算 $*$ が [結合法則](#) を満たすとは, 任意の $x, y, z \in G$ に対して,

$$(x * y) * z = x * (y * z)$$

を満たすときをいう.

● 4-3 : 単位元の存在

数の和では 0 を足しても値を変えない. 行列の演算においても, (演算が可能な範囲において) 単位行列 E を乗じてももとの行列に変化はない.

(II), (II') : 左右のどちらから演算を施しても **もとの値を変えない特別な要素が存在する**.

定義 4.3. $(G, *)$ を代数系とする. G の特別な元 $e \in G$ が, 任意の $x \in G$ に対して $e * x = x = x * e$ を満たすとき, e を G の [単位元](#) という.

単位元は, 「土台の集合が何か」「演算は何か」に依存して存在したり存在しなかったりする.

例 4-2 $\mathbb{N}$ では, $0 \notin \mathbb{N}$ なので和の単位元は存在しないが, $1 \in \mathbb{N}$ なので積の単位元は存在する.

しかし, 次の命題が示すように, 単位元は存在すれば一意的に定まる.

命題 4.4. $(G, *)$ を代数系とする. このとき, G に単位元 e が存在すれば, それはただ一つに定まる.

証明. $e, e' \in G$ を共に G の単位元であるとする. e' は単位元であるから $e = e * e'$ である. 一方, e も単位元なので $e * e' = e'$ である. 従って $e = e'$ となる. □

● 4-4 : 逆元の存在

どんな数 x に対しても, $-x$ を足せば単位元 0 になる. また, 正則行列 A に, その逆行列 A^{-1} を乗ずれば, 単位行列 E になる.

(III), (III') : どんな要素に対しても, **ある要素が存在して, 演算を左右どちらから施しても結果が単位元となるものがある**.

定義 4.5. $(G, *)$ を代数系で, e は G の単位元であるとする. 任意の $x \in G$ に対して, ある $y \in G$ が存在して $x * y = e = y * x$ を満たすとき, y を x の [逆元](#) という.

逆元は, **G の各々の元に対して定まる概念であり**, やはり「土台の集合が何か」「演算は何か」に依存して存在したり存在しなかったりする.

例 4-3 $\mathbb{N}$ では, どんな自然数 x に対しても $-x$ は自然数ではないので和に関する逆元をもつような x は存在しない. 一方, $\mathbb{Z}$ では, どんな整数 x に対しても $-x$ は再び整数であり, $x + (-x) = 0$ なので和に関する逆元はいつでも存在する. しかし, 整数 x に対して $\frac{1}{x}$ が整数となるのは, $x = \pm 1$ の場合のみであるからこのときのみ積に関する逆元が存在して, それ以外の場合は存在しない.

行列の場合も考えてみると, $\text{Mat}_n(\mathbb{R})$ ではどんな正方行列 $A \in \text{Mat}_n(\mathbb{R})$ に対しても $-A \in \text{Mat}_n(\mathbb{R})$ であるから和に関する逆元はいつでも存在する. しかし, 行列の積について考えれば, $AB = E = BA$ となるような $B \in \text{Mat}_n(\mathbb{R})$ が存在するのは A が正則行列の場合のみである.

単位元のときと同様に, $x \in G$ の逆元が存在すれば一意的に定まる.

命題 4.6. $(G, *)$ を代数系で, e は G の単位元であるとする. このとき, $x \in G$ に逆元 y が存在すれば, それはただ一つに定まる.

証明. $x \in G$ に対して, $y, y' \in G$ が共に x の逆元であるとする. e は G の単位元であるから,

$$y = y * e = y * x * y' = e * y' = y'$$

であるので, $y = y'$ となる. □

● 4-5 : 群

代数系 $(\mathbb{Z}, +)$ や $(GL_n(\mathbb{R}), \cdot)$ は性質 0, 1, 2, 3 をすべて満足している. これらの性質を公理化することで, 2 つの概念を一つにまとめ上げよう.

定義 4.7. 代数系 $(G, *)$ が次の 3 つの条件を満たすとき, G は演算 $*$ に関して **群** であるという.

(G1) 二項演算 $*$ は **結合法則** を満たす. すなわち, 任意の $x, y, z \in G$ に対して,

$$(x * y) * z = x * (y * z)$$

を満たす.

(G2) G には二項演算 $*$ に関する単位元 $e \in G$ が存在する. すなわち, $e \in G$ が存在して, 任意の $x \in G$ に対して $e * x = x = x * e$ を満たす.

(G3) 二項演算 $*$ に関して, 任意の $x \in G$ に対して, x には逆元 $y \in G$ が存在する. すなわち, 任意の $x \in G$ に対して, ある $y \in G$ が存在して $x * y = e = y * x$ を満たす.

例 4-4 (1) 通常の和に関して, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は群をなす. ただし, $\mathbb{N}$ は和に関して群をなさない. 実際, $2 \in \mathbb{N}$ の逆元は自然数ではないからである. また, 通常の積に関しては $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ のいずれも群をなさない. なぜならば, 単位元は 1 であるが, 0 に逆元が存在しないからである.

(2) $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ はいずれも積に関して群となる. この $\mathbb{C}^*$ は **トーラス** とも呼ばれる.

(3) k を $\mathbb{R}$ または $\mathbb{C}$ とする. $\text{Mat}_n(k)$ を成分が k の要素であるような n 次正方行列全体とする. このとき, 行列の和に関して $\text{Mat}_n(k)$ は群をなす. 実際, 行列の和は結合法則を満たすので, (G1) を満たす. 単位元は零行列 O をとればよいので (G2) を満たす. 任意の $X \in \text{Mat}_n(k)$ に対して, X は逆元 $-X$ をもつから (G3) も満たす.

また, $\text{Mat}_n(k)$ は行列の積に関しては, 逆行列をいつでも持つとは限らないから (G3) を満たさず, 従って群ではない.

(4) k を $\mathbb{R}$ または $\mathbb{C}$ とする. n 次正則行列全体をなす集合を $GL_n(k)$ とおく. これは行列の積に関して群をなす. 実際, 行列の積は結合法則を満たすので, (G1) を満たす. 単位元は単位行列 E をとればよいので (G2) を満たす. 任意の $X \in GL_n(k)$ に対して, X は正則なので逆行列 X^{-1} が存在するが, これが X の逆元である. $GL_n(k)$ は **一般線形群** と呼ばれる. これは, 行列の和に関しては群をなさない. 実際, $(GL_n(k), +)$ はそもそも代数系ではない.

命題 4.8. $m \in \mathbb{N}$ とする. このとき, 代数系 $(\mathbb{Z}/m\mathbb{Z}, +)$ について, $\mathbb{Z}/m\mathbb{Z}$ は群である.

証明. (G1) 任意の $[a], [b], [c] \in \mathbb{Z}/m\mathbb{Z}$ に対して, $\mathbb{Z}/m\mathbb{Z}$ の和の定義から

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$$

となり, (G1) が成り立つ.

(G2) 任意の $[a] \in \mathbb{Z}$ に対して,

$$[a] + [0] = [a + 0] = [a], \quad [0] + [a] = [0 + a] = [a]$$

となり, 単位元 $[0]$ が存在するから (G2) が成り立つ.

(G3) 任意の $[a] \in \mathbb{Z}$ に対して, $[-a] \in \mathbb{Z}/m\mathbb{Z}$ を考えれば

$$[a] + [-a] = [a - a] = [0], \quad [-a] + [a] = [-a + a] = [0]$$

となり, 任意の $[a]$ に対する逆元が存在したから (G3) が成り立つ.

以上で, $\mathbb{Z}/m\mathbb{Z}$ は和に関して群である.

□

小テスト 4-1 以下に示す代数系について, (G_1) , (G_2) , (G_3) のうち成り立っているものを全て選べ.

- (1) $(\mathbb{N}, +)$
- (2) $(\mathbb{R}, -)$
- (3) $(\mathbb{Z} \setminus \{0\}, \cdot)$
- (4) $(\mathbb{R}, *)$, ただし, $x, y \in \mathbb{R}$ に対して $x * y := \max(x, y)$.
- (5) $(\mathbb{Z}/7\mathbb{Z}, \cdot)$

小テスト 4-2 次の記述が正しいければ ○, 間違っていれば × を選択せよ.

- (1) $(G, *)$ が代数系であるとは, G が $G \neq \emptyset$ であるような集合であって, $\forall x, y \in G, x * y \in G$ を満たすときをいう.
- (2) 代数系 $(G, *)$ が群であることを示すには, 「 $*$ が結合法則を満たすこと」「 G には $*$ に関する単位元が存在すること」「 G の任意の元に逆元が存在すること」の 3 つを証明すればよい.
- (3) $G = \{a, b, c, d\}$ として, G 上の二項演算 $*$ が次の演算表によって与えられているとき, 単位元は b である.

$*$	a	b	c	d
a	b	a	b	a
b	a	b	c	d
c	b	c	b	c
d	c	d	a	c

- (4) 代数系 $(G, *)$ の演算 $*$ は, 任意の $x, y \in G$ に対して, $x * y = y * x$ を満たすとは限らないが, 結合法則はいつでも満たす.
- (5) 代数系 $(G, +)$ の演算 $+$ は, 任意の $x, y \in G$ に対して, $x + y = y + x$ を満たす.

演習問題 4-1 集合 Z を絶対値が 1 となる複素数全体, すなわち

$$Z = \{z \in \mathbb{C} \mid |z| = 1\}$$

とする. Z は複素数の積に関して群をなすことを示せ.

演習問題 4-2 $G = \{1, 2, 3, 12, 18, 36\}$ とし, G 上の二項演算 $*_1$ と $*_2$ をそれぞれ

$$x *_1 y := x \text{ と } y \text{ の公約数のうち, } G \text{ に属するものの最大値}$$

$$x *_2 y := x \text{ と } y \text{ の公倍数のうち, } G \text{ に属するものの最小値}$$

と定義する. このとき, それぞれの代数系 $(G, *_1)$, $(G, *_2)$ について以下の問に答えよ.

- (1) それぞれの代数系 $(G, *_1)$, $(G, *_2)$ の演算表を構成せよ.
- (2) それぞれの代数系 $(G, *_1)$, $(G, *_2)$ には単位元が存在するか. 存在するならばそれを示し, 存在しないならば理由を述べよ.
- (3) それぞれの代数系 $(G, *_1)$, $(G, *_2)$ について, 各元 $x \in G$ に逆元が存在すれば, それを示せ.

演習問題 4-3 代数系 $(G, *)$ は群をなすとする. $a \in G$ を 1 つとり固定する. 写像 f と g を

$$\begin{aligned} f: G &\longrightarrow G; & g &\longmapsto ag \\ g: G &\longrightarrow G; & g &\longmapsto ga \end{aligned}$$

はそれぞれ全単射であることを示せ.