

4 代数系

第 1 回・第 2 回ではグラフを, 第 3 回では計算のモデルを扱った. 本回では, 集合に演算という構造を加えた **代数系** (algebraic system) を調べる. 整数の加法, 有理数の乗法, 置換の合成といった一見異なる対象が, 結合法則・単位元・逆元といった同じ規則を共有していることに着目し, それらを統一的にとらえる枠組みとして **群・環・体** を導入する. 演算を一つもつものが群, 加法と乗法の二つをもつものが環, さらに零でない元による除法まで許すものが体であり, これらは代数学の骨格をなすとともに, 符号理論や暗号など情報科学の応用でも基礎となる.

● 4-1 : 二項演算と群

定義 4.1. 集合 X に対して, 写像 $*$: $X \times X \rightarrow X$ を X 上の **二項演算** (binary operation) という. $*(a, b)$ を通常 $a * b$ と書く.

$*$ が写像 $X \times X \rightarrow X$ であること自体に, 「任意の $a, b \in X$ に対し $a * b$ がふたたび X の元である」という要請 (**閉じている**, closure) が含まれていることに注意する.

定義 4.2. 集合 G と, その上の二項演算 $*$ の組 $(G, *)$ が **群** (group) であるとは, 次の 3 条件をみたすことをいう.

(G1) (結合法則) 任意の $a, b, c \in G$ に対し $(a * b) * c = a * (b * c)$.

(G2) (単位元の存在) ある $e \in G$ が存在して, 任意の $a \in G$ に対し $e * a = a * e = a$. この e を G の **単位元** (identity) という.

(G3) (逆元の存在) 任意の $a \in G$ に対し, ある $b \in G$ が存在して $a * b = b * a = e$. この b を a の **逆元** (inverse) という.

さらに, 任意の $a, b \in G$ に対し $a * b = b * a$ が成り立つとき, G を **可換群** または **アーベル群** (abelian group) という.

演算 $*$ を積のように書いて $a * b$ を ab と略記し, 単位元を 1 (または e), a の逆元を a^{-1} と書くことが多い. 一方, 演算が加法の性質をもつ場合には, $*$ を $+$, 単位元を 0 , 逆元を $-a$ と書く. 以下では文脈に応じて両方の記法を用いる.

例 4-1 (1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ はいずれも加法に関するアーベル群である (単位元 0 , a の逆元 $-a$).

(2) $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ は乗法に関するアーベル群である (単位元 1 , a の逆元 $1/a$). 同様に $\mathbb{R}^\times, \mathbb{C}^\times$ もアーベル群である. 一方 $(\mathbb{Z}, \times)$ は群でない (たとえば 2 の乗法逆元 $1/2$ が $\mathbb{Z}$ に属さない).

(3) $\{1, -1\}$ は乗法に関するアーベル群である. また 1 元集合 $\{e\}$ は $e * e = e$ により群になる (**自明群**).

例 4-2 (剰余類のなす加法群) n を正の整数とする. 整数 a, b に対し $n \mid a - b$ のとき $a \equiv b \pmod{n}$ と書く. これは $\mathbb{Z}$ 上の同値関係であり, a を含む同値類を **剰余類** $\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$ という. 相異なる剰余類は $\bar{0}, \bar{1}, \dots, \overline{n-1}$ の n 個で, その全体を $\mathbb{Z}/n\mathbb{Z}$ と書く. ここに加法を

$$\bar{a} + \bar{b} := \overline{a + b}$$

で定める. これは代表元の取り方によらず定まる (**well-defined**). 実際, $a \equiv a', b \equiv b' \pmod{n}$ ならば

$n \mid (a - a')$ かつ $n \mid (b - b')$ より $n \mid ((a + b) - (a' + b'))$ となる. こうして $(\mathbb{Z}/n\mathbb{Z}, +)$ は n 個の元からなるアーベル群になる (単位元 $\bar{0}$, $\bar{a}$ の逆元 $-\bar{a} = \overline{n-a}$). たとえば $n = 4$ のときの加法は次の演算表 (Cayley 表) で与えられる.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

命題 4.3. 群 G について, 次が成り立つ.

- (1) 単位元はただ一つである.
- (2) 各元 $a \in G$ の逆元はただ一つである.
- (3) (簡約法則) $a, x, y \in G$ に対し, $ax = ay$ ならば $x = y$ であり, また $xa = ya$ ならば $x = y$ である.

証明. (1) e, e' をともに単位元とすると, $e = e * e' = e'$ である (第 1 の等号は e' が, 第 2 の等号は e が単位元であることによる).

(2) b, b' をともに a の逆元とすると, 結合法則より

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$$

である.

(3) $ax = ay$ とする. a の逆元 a^{-1} を左から掛けると, 結合法則により $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = y$ を得る. $xa = ya$ の場合は a^{-1} を右から掛ければよい. $\square$

● 4-2 : 部分群と対称群

定義 4.4. 群 G の元の個数 $|G|$ を G の **位数** (order) という. $|G|$ が有限のとき, G を **有限群** という.

定義 4.5. 群 G の空でない部分集合 H が, G の単位元を含み, G の演算のもとで積と逆元について閉じているとき, すなわち

- (i) $e \in H$, (ii) 任意の $a, b \in H$ に対し $ab \in H$, (iii) 任意の $a \in H$ に対し $a^{-1} \in H$

をみたすとき, H を G の **部分群** (subgroup) といい, $H \leq G$ と書く. このとき H 自身も G の演算によって群になる.

命題 4.6 (部分群の判定). 群 G の空でない部分集合 H が部分群であるための必要十分条件は, 任意の $a, b \in H$ に対し $ab^{-1} \in H$ が成り立つことである.

証明. (必要性) H が部分群ならば, (iii) より $b^{-1} \in H$, (ii) より $ab^{-1} \in H$ である.

(十分性) 条件を仮定する. $H \neq \emptyset$ ゆえ元 $a \in H$ がとれ, これに条件を適用すると $e = aa^{-1} \in H$ となり (i) が成り立つ. 次に任意の $a \in H$ に対し, $e, a \in H$ に条件を適用して $a^{-1} = ea^{-1} \in H$ となり (iii) が成り立つ. 最後に任意の $a, b \in H$ に対し, いま示した (iii) より $b^{-1} \in H$ だから, $a, b^{-1} \in H$ に条件を適用して $ab = a(b^{-1})^{-1} \in H$ となり (ii) が成り立つ. ゆえに H は部分群である. $\square$

例 4-3 正の整数 n に対し, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ は $(\mathbb{Z}, +)$ の部分群である. 実際 $n\mathbb{Z} \ni 0$ で空でなく, $nk, nl \in n\mathbb{Z}$ に対し $nk - nl = n(k - l) \in n\mathbb{Z}$ だから, 命題 4.6 (加法なので条件は $a - b \in n\mathbb{Z}$) より部分群である. 逆に $(\mathbb{Z}, +)$ の部分群はすべてこの形であることが知られている.

置換の合成がつくる群は, 有限群の最も基本的な例である.

定義 4.7. 集合 $\{1, 2, \dots, n\}$ からそれ自身への全単射を **置換** (permutation) という. 置換全体の集合を S_n とし, 写像の合成 $\circ$ を演算とする組 $(S_n, \circ)$ を n 次の **対称群** (symmetric group) という.

S_n は群である. 実際, 写像の合成は結合的であり, 恒等写像 id が単位元, 全単射の逆写像が逆元を与える. その位数は $|S_n| = n!$ である. 置換 σ を, i の下に $\sigma(i)$ を並べた二行の記法で表す.

例 4-4 S_3 は位数 6 の群である. 合成 $\sigma \circ \tau$ は「先に τ , 次に σ を施す」ことと約束する.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

とすると,

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

であり, $\sigma \circ \tau \neq \tau \circ \sigma$ となる. ゆえに S_3 はアーベル群ではない. 一般に $n \geq 3$ のとき S_n は非可換である.

● 4-3 : 環

群は演算を一つもつ代数系であった. 整数のように, 加法と乗法の二つの演算をあわせもつ代数系が環である.

定義 4.8. 集合 R と, その上の二つの二項演算 $+$ (加法), $\cdot$ (乗法) の組 $(R, +, \cdot)$ が **環** (ring) であるとは, 次をみたすことをいう.

(R1) $(R, +)$ はアーベル群である (単位元を 0 , a の加法逆元を $-a$ と書く).

(R2) 乗法 $\cdot$ は結合的であり, 乗法単位元 1 をもつ (任意の $a \in R$ に対し $1 \cdot a = a \cdot 1 = a$).

(R3) (分配法則) 任意の $a, b, c \in R$ に対し $a(b+c) = ab+ac$ かつ $(a+b)c = ac+bc$.

さらに乗法が可換, すなわち任意の a, b に対し $ab = ba$ であるとき, R を **可換環** (commutative ring) という.

本講義では乗法単位元 1 の存在を仮定する流儀を採る. なお $1 = 0$ となるのは $R = \{0\}$ (零環) のときに限る (このとき任意の a に対し $a = 1 \cdot a = 0 \cdot a = 0$ となるからである. ただし下の命題 4.9 を用いた).

命題 4.9. 環 R の任意の元 a, b に対し, 次が成り立つ.

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

(2) $(-a)b = a(-b) = -(ab)$. とくに $(-1)a = -a$ である.

(3) $(-a)(-b) = ab$. とくに $(-1)(-1) = 1$ である.

証明. (1) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$ である. 両辺に $0 \cdot a$ の加法逆元を加えると $0 = 0 \cdot a$ を得る. $a \cdot 0 = 0$ も同様である.

(2) 分配法則と (1) より $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$ だから, $(-a)b$ は ab の加法逆元, すなわち $(-a)b = -(ab)$ である. $a(-b) = -(ab)$ も同様である. とくに $a = 1$ とおけば $(-1)b = -(1 \cdot b) = -b$ を得る.

(3) (2) を二度用いると

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

である (最後の等号は, 加法群において $-(-x) = x$ が成り立つことによる). とくに $a = b = 1$ とおけば $(-1)(-1) = 1$ を得る. $\square$

命題 4.9 の (2), (3) は, 「 -1 を掛けると符号が変わる」「負の数どうしの積は正になる」といったなじみ深い規則が, 環の公理 (とりわけ分配法則) だけから導かれることを示している. たとえば整数環 $\mathbb{Z}$ における

$(-1)(-1) = 1$ や $(-3)(-5) = 15$ は, この一般的な事実の特別な場合にすぎない.

例 4-5 (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は通常の加法・乗法により可換環である.

(2) $\mathbb{Z}/n\mathbb{Z}$ に乗法を $\bar{a} \cdot \bar{b} := \overline{ab}$ で定めると, これも well-defined であり ($a \equiv a', b \equiv b'$ のとき $ab - a'b' = a(b - b') + (a - a')b'$ が n で割り切れる), $\mathbb{Z}/n\mathbb{Z}$ は乗法単位元 $\bar{1}$ をもつ可換環になる.

(3) n 次実正方形行列全体 $M_n(\mathbb{R})$ は, 行列の和と積により環である. 単位元は単位行列 I であり, $n \geq 2$ では非可換である (一般に $AB \neq BA$).

(4) 実数係数の多項式全体 $\mathbb{R}[x]$ は可換環である.

定義 4.10. 環 R の元 a が **単元** (unit) であるとは, ある $b \in R$ が存在して $ab = ba = 1$ となることをいう. また, $a \neq 0$ であって, ある $b \neq 0$ に対し $ab = 0$ となる元 a を **零因子** (zero divisor) という.

例 4-6 $\mathbb{Z}$ の単元は ± 1 のみである. 環 $\mathbb{Z}/6\mathbb{Z}$ では, $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$ でありながら $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ となる. ゆえに $\bar{2}, \bar{3}$ は零因子である.

● 4-4 : 体

環のうち, 零でない元がつねに乗法逆元をもつ (除法ができる) ものが体である.

定義 4.11. 可換環 F が **体** (field) であるとは, $1 \neq 0$ であり, かつ 0 でない任意の元 $a \in F$ が単元である (乗法逆元 a^{-1} をもつ) ことをいう.

言い換えれば, 体とは $1 \neq 0$ なる可換環であって, $F^\times := F \setminus \{0\}$ が乗法に関してアーベル群をなすものである. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ はいずれも体である. 一方 $\mathbb{Z}$ は体でない (2 が単元でない).

命題 4.12. 体は零因子をもたない. すなわち, 体 F において $ab = 0$ ならば $a = 0$ または $b = 0$ である.

証明. $ab = 0$ かつ $a \neq 0$ とする. a は単元だから逆元 a^{-1} をもち, 命題 4.9 も用いて

$$b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$$

となる. ゆえに $a = 0$ または $b = 0$ である. □

有限体の最も基本的な例は, 素数を法とする剰余類環 $\mathbb{Z}/n\mathbb{Z}$ から得られる. 準備として, $\mathbb{Z}/n\mathbb{Z}$ の単元を特徴づけておく.

命題 4.13. $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ が単元であるための必要十分条件は $\gcd(a, n) = 1$ である.

証明. $\bar{a}$ が単元であることは, ある整数 x について $\bar{a}\bar{x} = \bar{1}$, すなわち $ax \equiv 1 \pmod{n}$ となることと同値である. これはさらに, ある整数 x, y について $ax + ny = 1$ となることと同値であり, Bezout の等式より, これは $\gcd(a, n) = 1$ と同値である. □

定理 4.14. 2 以上の整数 n に対し, $\mathbb{Z}/n\mathbb{Z}$ が体であるための必要十分条件は, n が素数であることである.

証明. $n \geq 2$ より $\bar{1} \neq \bar{0}$ であり, 例 4-5 (2) より $\mathbb{Z}/n\mathbb{Z}$ は可換環である.

(n が素数のとき) $\bar{a} \neq \bar{0}$ とすると $n \nmid a$ である. n は素数だからその正の約数は 1 と n のみで, $n \nmid a$ より $\gcd(a, n) = 1$ となる. ゆえに命題 4.13 より $\bar{a}$ は単元である. こうして 0 でない任意の元が単元となるから, $\mathbb{Z}/n\mathbb{Z}$ は体である.

(n が合成数のとき) $n = ab$ ($1 < a, b < n$) と書ける. このとき $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ でありながら $\bar{a}\bar{b} = \overline{ab} = \bar{n} = \bar{0}$ となるから, $\bar{a}$ は零因子である. 命題 4.12 より体は零因子をもたないので, $\mathbb{Z}/n\mathbb{Z}$ は体でない. □

素数 p に対する体 $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ と書く。これは p 個の元からなる **有限体** (finite field) であり、誤り訂正符号や暗号など情報科学の随所で本質的な役割を果たす。たとえば $\mathbb{F}_5$ では

$$\bar{2}^{-1} = \bar{3} \ (\bar{2} \cdot \bar{3} = \bar{6} = \bar{1}), \quad \bar{3}^{-1} = \bar{2}, \quad \bar{4}^{-1} = \bar{4} \ (\bar{4} \cdot \bar{4} = \bar{16} = \bar{1})$$

のように、0 でないすべての元が逆元をもつ。一方 $\mathbb{Z}/4\mathbb{Z}$ は、定理 4.14 の通り 4 が合成数だから体ではない (実際 $\bar{2} \cdot \bar{2} = \bar{0}$ で $\bar{2}$ は零因子である)。

以上で、演算を一つもつ群、加法と乗法の二つをもつ環、さらに除法まで許す体が出そろった。三者の関係を整理すると次の通りである。

	演算	おもな要請	代表例
群	1 つ	結合律・単位元・逆元をもつ	$(\mathbb{Z}, +)$, S_n , $\mathbb{Z}/n\mathbb{Z}$
環	2 つ	加法についてアーベル群, 乘法について結合律と単位元, および分配律	$\mathbb{Z}$, $M_n(\mathbb{R})$, $\mathbb{R}[x]$
体	2 つ	可換環であって $1 \neq 0$, かつ 0 以外の元が乘法逆元をもつ	$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$

● 4-5 : 準同型と同型

これまで、整数の加法群 $(\mathbb{Z}, +)$ と剰余類の加法群 $(\mathbb{Z}/n\mathbb{Z}, +)$ のように、別々に定義された代数系を見てきた。それらの間の「演算を保つ写像」を考えると、代数系どうしの関係が見えてくる。

定義 4.15. 群 $(G, *)$ から群 $(G', *)$ への写像 $f: G \rightarrow G'$ が **群準同型** (group homomorphism) であるとは、任意の $a, b \in G$ に対し

$$f(a * b) = f(a) *' f(b)$$

が成り立つことをいう。すなわち、 G で先に演算してから写しても、写してから G' で演算しても結果は同じである。さらに f が全単射であるとき、 f を **同型写像** (isomorphism) といい、このとき G と G' は **同型** (isomorphic) であるといって $G \cong G'$ と書く。

命題 4.16. 群準同型 $f: G \rightarrow G'$ は、単位元を単位元に、逆元を逆元に写す。すなわち、 G, G' の単位元をそれぞれ e, e' とすると $f(e) = e'$ であり、また任意の $a \in G$ に対し $f(a^{-1}) = f(a)^{-1}$ である。

証明. $f(e) = f(e * e) = f(e) *' f(e)$ の両辺に $f(e)$ の逆元を掛けると、命題 4.3 の簡約法則より $e' = f(e)$ を得る。また $f(a) *' f(a^{-1}) = f(a * a^{-1}) = f(e) = e'$ だから、 $f(a^{-1})$ は $f(a)$ の逆元、すなわち $f(a^{-1}) = f(a)^{-1}$ である。□

例 4-7 (1) 正の実数全体 $\mathbb{R}_{>0}$ は乘法に関するアーベル群である。指数関数 $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \times)$ は $\exp(x+y) = \exp(x)\exp(y)$ をみたすから群準同型であり、さらに全単射 (逆写像は $\log$) だから同型写像である。ゆえに $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$ であって、加法群と乘法群という一見異なる群が実は同型である。

(2) 剰余をとる写像 $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/n\mathbb{Z}, +)$, $\pi(a) = \bar{a}$ は、 $\pi(a+b) = \overline{a+b} = \bar{a} + \bar{b}$ より群準同型である (全射だが単射でない)。

(3) 行列式 $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ は $\det(AB) = \det(A)\det(B)$ より群準同型である。ここで $GL_n(\mathbb{R})$ は正則な (逆行列をもつ) n 次実行列全体のなす群である。

環に対しても、加法と乗法の両方を保つ写像を考える。

定義 4.17. 環 R から環 R' への写像 $f: R \rightarrow R'$ が **環準同型** (ring homomorphism) であるとは、任意の $a, b \in R$ に対し

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(1_R) = 1_{R'}$$

の三つが成り立つことをいう。全単射な環準同型を (環の) [同型写像](#) といい, このとき $R \cong R'$ と書く。

例 4-8 剰余をとる写像 $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $\pi(a) = \bar{a}$ は環準同型である。実際 $\pi(a+b) = \bar{a} + \bar{b}$, $\pi(ab) = \overline{ab} = \bar{a}\bar{b}$, $\pi(1) = \bar{1}$ が成り立つ。

同型な代数系は, 演算に関するあらゆる性質を共有する。たとえば, 一方がアーベル群ならば他方もアーベル群であり, 一方が体ならば他方も体である。ゆえに代数学では, 同型な対象は表記や名前の違いを超えて「同じもの」とみなして扱う。