代数学入門

花木 章秀

2007 年前期
(2007/11/06)

目次

Chapter 1

記号と準備

この講義では現代代数学の基礎となる「群」、「環」、「体」の定義、および基本的な性質や例を理解することを目標とする。これらは、更に進んだ代数学を学ぶ際だけでなく、幾何学、解析学、情報科学、物理学などの広い分野で応用される基本的、かつ重要なものである。

代数学、あるいはより広く数学、においては、ある対象のもつ基本的な性質のみに注目し、その性質だけを考えた理論を構築し、そこで得られた理論を元の問題に応用するといった手法がとられる。まったく違う対象が、類似の性質をもつ場合に、その共通の性質だけに注目して得られた結果は、そのどちらにも適用できる。したがって多くの対象がもつ性質を考え、それに関する一般論を構築しておけば、その適用範囲は広くなり、その重要性は増すことになる。このような考えから定義され、研究されてきたものに前述の「群」、「環」、「体」などがあるのである。

簡単な例を考えよう。例えば n 次元ベクトル全体の集合 V を考える。V には加法や減法が定義される。しかし乗法、除法は定義されない。そこで “加法と減法が定義されている集合” についての一般論を構築しておけば、同様の性質をもつもの全てに適用できる。これが「群」である。(この定義は正確ではないが、詳しくは後で学ぶ。)

次に n 次の正方行列全体の集合 R を考えよう。R には加法と減法が定まっているので、これは群である。しかし R には乗法も定まっている。R を単に加法に関する群と見ているだけでは、その乗法に関する情報は得られない。そこで加法、減法、乗法の定まっているものを「環」と定める。

n 次正方行列には、一般に逆行列が存在するわけではないので、R に除法を定めることはできない。しかしながら有理数全体、実数全体、複素数全体などのように除法も考えられるものも少なくはない。そこでこのように四則演算が行える対象を「体」と定めるのである。

この講義ノートは主に「代数学, 永尾汎, 朝倉書店」[1] の第一章を参考にして作成したが、記号などはなるべく「代数学入門、石田信、実教出版」[2] に合わせた。

1.1 集合

A を**集合** (set) とする。a が A の**要素** (element)、あるいは**元**、であることを $a \in A$ または $A \ni a$ と書く。a が A の要素でないことは $a \notin A$ と書く。B が A の**部分集合**

(subset) であるとき $B \subset A$ と書く。このとき $B = A$ も許すことに注意しておく。特に $B \subset A$ かつ $B \neq A$ であるとき B は A の**真部分集合** (proper subset) であるといい $B \subsetneq A$ と書く。また **空集合** (empty set) は ϕ で表す。

$B \subset A$ のとき $A - B = \{a \in A \mid a \notin B\}$ とする。

A が**有限集合** (finite set) であるとき、$|A|$ または $\sharp A$ でその要素の個数を表す。A が**無限集合** (infinite set) であるときには $|A| = \infty$ と書く。$|A| < \infty$ は A が有限集合であると言うことを意味するものとする。

注意. 有限集合は、適当な非負整数 n と、適当な番号付けによって $\{a_1, a_2, \cdots, a_n\}$ と書き表すことができる。しかし一般の無限集合を $\{a_1, a_2, \cdots\}$ と書くのは誤りである。

$A \cap B$, $A \cup B$ はそれぞれ**共通部分** (intersection)、**和集合** (union) である。一般に集合 A_i $(i = 1, 2, \cdots, n)$ に対して

$$\bigcap_{i=1}^{n} A_i, \quad \bigcup_{i=1}^{n} A_i$$

で、それぞれ共通部分、和集合を表す。加算無限個の集合 A_i $(i = 1, 2, \cdots)$ については $\bigcap_{i=1}^{\infty} A_i, \bigcup_{i=1}^{\infty} A_i$ などの記号を用いるが、一般の無限集合については、適当な添字集合 Λ を用いて、集合を A_λ $(\lambda \in \Lambda)$ と表し、

$$\bigcap_{\lambda \in \Lambda} A_\lambda, \quad \bigcup_{\lambda \in \Lambda} A_\lambda$$

などと書く。この書きかたは Λ が有限集合でも用いることができるため、最も汎用的な記述である。

添字の動く範囲を適当に省略することも多い。例えば、全ての正の実数 a について、閉区間 $[-a, a]$ の共通部分を表すには、上記の規則に従えば $\bigcap_{a \in \{b \in \mathbb{R} \mid b > 0\}} [-a, a]$ と書くべきであるが、実際には省略して $\bigcap_{a>0} [-a, a]$ などと書くことが多い。

問 1.1.1. $\bigcap_{a>0} [-a, a]$ と $\bigcup_{a>0} [-a, a]$ は何か。

和集合 $\bigcup_{\lambda \in \Lambda} A_\lambda$ において $\lambda \neq \lambda'$ ならば $A_\lambda \cap A_{\lambda'} = \phi$ が成り立つとき、この和を**共通部分をもたない和** (disjoint union) という。共通部分をもたない和 $\bigcup_{\lambda \in \Lambda} A_\lambda$ において $\left| \bigcup_{\lambda \in \Lambda} A_\lambda \right| < \infty$ ならば、すべての $\lambda \in \Lambda$ について $|A_\lambda| < \infty$ であり $\left| \bigcup_{\lambda \in \Lambda} A_\lambda \right| = \sum_{\lambda \in \Lambda} |A_\lambda|$ である。

A と B を集合とする。A の元と B の元の順序対 (a, b) の全体からなる集合を $A \times B$ と書いて A と B の**直積集合** (direct product, cartesian product)、または単に**直積**という。

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

集合の族 A_λ $(\lambda \in \Lambda)$ に対しても、各集合から一つずつ元を選び、それを元とする集合を定義し、これを直積集合という。このとき直積集合を $\prod_{\lambda\in\Lambda} A_\lambda$ と書く。(Λ が無限集合の場合には、直積集合が空でないことを保証するために**選択公理** (Zermelo's axiom of choice) を必要とする。)

1.2 整数

この講義では以下の記号を用いる。

- $\mathbb{N}$: 自然数全体の集合
- $\mathbb{Z}$: 整数全体の集合
- $\mathbb{R}$: 実数全体の集合
- $\mathbb{C}$: 複素数全体の集合

自然数全体の集合 $\mathbb{N}$ に 0 を含める場合もあるが、この講義では含めないものとする。この節では特に整数に関する基本的な性質と記号を説明する。

$a, b \in \mathbb{Z}$ に対して、ある $\ell \in \mathbb{Z}$ が存在して $b = a\ell$ となるとき b は a で**割り切れる**、または a は b を**割り切る**といい $a \mid b$ と書く。このとき、a は b の**約数** (divisor) である、b は a の**倍数** (multiple) である、ともいう。0 はどんな数でも割り切れ、1 はどんな数も割り切る。また負の数も考えることができる。

有限個、または無限個の、少なくとも一つは 0 でない整数 a_λ $(\lambda \in \Lambda)$ が与えられたとき、任意の $\lambda \in \Lambda$ に対して $c \mid a_\lambda$ が成り立つ $c \in \mathbb{Z}$ を a_λ $(\lambda \in \Lambda)$ の**公約数** (common divisor) という。公約数のうち最大のものを**最大公約数** (greatest common divisor) という。公約数は最大公約数の約数である。特に $a_1, a_2, \cdots$ の最大公約数を $(a_1, a_2, \cdots)$ または $\gcd(a_1, a_2, \cdots)$ と書く。$\gcd(a, b) = 1$ であるとき a と b は**互いに素である**という。

$p \in \mathbb{N}$, $p > 1$ に対して p が**素数** (prime number) であるとは、p の正の約数が 1 と p しかないこととする。これは「$p \mid ab$ ならば、 $p \mid a$ または $p \mid b$」が成り立つことと同値である。

$n \in \mathbb{N}$ を固定する。$a, b \in \mathbb{Z}$ に対して $n \mid a - b$ が成り立つとき a と b は n **を法として合同** (congruent modulo n) であるといい $a \equiv b \pmod{n}$ と書く。

問 1.2.1. 次を示せ。

(1) 任意の $a \in \mathbb{Z}$ に対して $a \equiv a \pmod{n}$

(2) $a \equiv b \pmod{n}$ ならば $b \equiv a \pmod{n}$

(3) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$、ならば $a \equiv c \pmod{n}$

(これにより "n を法として合同である" という $\mathbb{Z}$ 上の関係は同値関係になる。)

1.3 写像

A と B を集合とする。A の元を一つを定めると B の元が一つ定まるとする。このときこの対応を**写像** (map) といい $A \to B$ などと書く。写像に名前、例えば f、を付けたいときには $f : A \to B$ などと書く。f によって $a \in A$ に対応する B の元を f **による** a **の像**といい $f(a)$ と書く。どの様な写像であるかを明記したい場合には

$$f : A \to B \quad (a \mapsto f(a))$$

などと書くこともある。写像 $f : A \to B$ について、A を f の**定義域** (domain)、B を f の**値域** (range) という。

二つの写像 $f : A \to B$ と $g : C \to D$ が**等しい**とは、$A = C$、$B = D$ であって、任意の $a \in A$ に対して $f(a) = g(a)$ となることとする。また、このとき $f = g$ と書く。

写像 $f : A \to B$ に対して

$$f(A) = \mathrm{Im} f = \{f(a) \mid a \in A\}$$

とおいて、これを f **の像** (image) という。$C \subset A$ についても $f(C) = \{f(a) \mid a \in C\}$ とおいて、これを f **による** C **の像**という。

写像 $f : A \to B$ と $C \subset B$ に対して

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

とおいて、これを f **による** C **の逆像** (inverse image) という。$C = \{b\}$ のときには $f^{-1}(\{b\})$ の代わりに $f^{-1}(b)$ とも書く。すなわち

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

である。$b \notin f(A)$ ならば明らかに $f^{-1}(b) = \phi$ である。ここで $f^{-1}(b)$ という記号を用いているが、一般にこの f^{-1} は B から A への写像ではない。

写像 $f : A \to B$ が**単射** (injection) であるとは、「$a \neq a'$ ならば $f(a) \neq f(a')$ 」が成り立つこととする。写像 $f : A \to B$ が**全射** (surjection) であるとは、$f(A) = B$ となることである。写像 $f : A \to B$ が**全単射** (bijection) であるとは、f が単射、かつ全射であることである。

命題 1.3.1. 写像 $f : A \to B$ について次の条件は同値である。

(1) f は単射である。($a \neq a'$ ならば $f(a) \neq f(a')$ である。)

(2) $f(a) = f(a')$ ならば $a = a'$ である。

(3) 任意の $b \in f(A)$ に対して $|f^{-1}(b)| = 1$ である。

(4) 任意の $b \in B$ に対して $|f^{-1}(b)| \leq 1$ である。

命題 1.3.2. 写像 $f : A \to B$ について次の条件は同値である。

(1) f は全射である。($f(A) = B$ である。)

(2) 任意の $b \in B$ に対して $f(a) = b$ となる $a \in A$ が存在する。

(3) 任意の $b \in B$ に対して $|f^{-1}(b)| \geq 1$ である。

$B \subset A$ であるとき、写像 $\iota : B \to A$ $(b \mapsto b)$ が定義される。これを B **の** A **への埋め込み**、または**包含写像** (inclusion) という。特に $B = A$ のとき、埋め込み $\iota : A \to A$ $(a \mapsto a)$ を A の**恒等写像** (identity map) といい id_A などと書く。

写像 $f : A \to B$ と $g : B \to C$ に対して、写像 $A \to C$ $(a \mapsto g(f(a)))$ が定義できる。これを f と g の**合成写像** (composite map) といい $g \circ f$、または単に gf と書く。

写像 $f : A \to B$ が全単射であるとき、任意の $b \in B$ に対して $f(a) = b$ となる $a \in A$ が唯一つ存在する。言い換えれば $f^{-1}(b) = \{a\}$ である。このとき $f^{-1}(b)$ を $a \in A$ と同一視すれば、写像 $B \to A$ $(b \mapsto f^{-1}(b))$ が得られる。これを f **の逆写像** (inverse map) といい f^{-1} で表す。このとき、明らかに f^{-1} も全単射で

$$f \circ f^{-1} = \mathrm{id}_B, \quad f^{-1} \circ f = \mathrm{id}_A, \quad (f^{-1})^{-1} = f$$

である。

$f : A \to B$ を写像とし $C \subset A$ とする。このとき定義域を C に制限して、写像 $g : C \to B$ $(c \mapsto f(c))$ が得られる。これを f **の** C **への制限** (restriction) といい $f|_C$ などと書く。これは、正確には、包含写像 $\iota : C \to A$ と $f : A \to B$ の合成写像 $f \circ \iota$ である。

問 1.3.3. 写像 $f : \mathbb{Z} \to \mathbb{Z}$ で次の性質を持つものを具体的に、それぞれ一つ構成せよ。

(1) f は全射ではあるが単射ではない。

(2) f は単射ではあるが全射ではない。

(3) f は全単射で $f(0) = -1$ かつ $f(1) = 1$ である。

問 1.3.4. $|A| < \infty$ とするとき、写像 $f : A \to A$ について次の条件は同値であることを示せ。

(1) f は全単射である。

(2) f は単射である。

(3) f は全射である。

問 1.3.5. $f : A \to B$ と $g : B \to C$ について次を示せ。

(1) $g \circ f$ が全射であるならば g は全射である。

(2) $g \circ f$ が単射であるならば f は単射である。

問 1.3.6. $f : A \to B$ と $g : B \to A$ に対して $g \circ f$ と $f \circ g$ が共に全単射であるとする。このとき f も全単射であることを示せ。

問 1.3.7. $f : A \to B$ と $g : B \to C$ が共に全単射であるとする。このとき $g \circ f$ も全単射であり $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ であることを示せ。

問 1.3.8. $f : A \to B$ を写像とし $C \subset A$ とする。$f|_C$ が全射ならば f も全射であることを示せ。また f が単射ならば $f|_C$ も単射であることを示せ。

写像 $f : A \to B$ を具体的に記述するためには、任意の $a \in A$ に対して $f(a) \in B$ を特定すればよい。特に $|A| < \infty$ ならば、すべての $a \in A$ に対して $f(a)$ を定めればよい。例えば $A = \{1, 2, 3\}$, $B = \{a, b\}$ のとき

1	2	3
a	a	b

のように書き、$f(1) = a$, $f(2) = a$, $f(3) = b$ と読むことにすれば、これは写像 $f : A \to B$ を定めている。

問 1.3.9. $|A| = m < \infty$, $|B| = n < \infty$ のとき A から B への写像は何個存在するか。また、その中で単射はいくつあるか。

1.4 同値関係と同値類

A を集合とし $\sim$ を直積集合 $A \times A$ の部分集合とする。このとき $\sim$ を A **上の (二項) 関係** (binary relation) という。$(a, b) \in \sim$ であることを $a \sim b$ と書くことにする。

A 上の関係 $\sim$ が

(E1) [**反射律**] 任意の $a \in A$ について $a \sim a$ である。

(E2) [**対称律**] $a \sim b$ ならば $b \sim a$ である。

(E3) [**推移律**] $a \sim b$ かつ $b \sim c$、ならば $a \sim c$ である。

をすべて満たすとき、$\sim$ は**同値律** (equivalence row) を満たすといい、$\sim$ は**同値関係** (equivalence relation) であるという。$a \sim b$ であるとき a と b は ($\sim$ に関して) **同値である**という。

A 上の同値関係 $\sim$ と $a \in A$ に対して

$$C_a = \{b \in A \mid b \sim a\}$$

とおいて、これを a を含む**同値類** (equivalence class) という。

命題 1.4.1. A 上の同値関係 $\sim$ の同値類について以下が成り立つ。

(1) $a \in C_a$ である。

(2) $b \in C_a$ ならば $a \in C_b$ である。

(3) $C_a \neq C_b$ ならば $C_a \cap C_b = \phi$ である。

同値関係 $\sim$ において、相異なる同値類全体の集合を $\{C_\lambda \mid \lambda \in \Lambda\}$ とする。このとき

$$A = \bigcup_{\lambda\in\Lambda} C_\lambda, \quad (\lambda \neq \mu \text{ ならば } C_\lambda \cap C_\mu = \phi)$$

となる。これを A の $\sim$ による**類別**という。各 C_λ から一つずつ元 a_λ を選ぶとき、a_λ を C_λ の**代表元**といい、$\{a_\lambda \mid \lambda \in \Lambda\}$ を類別 $A = \bigcup_{\lambda\in\Lambda} C_\lambda$ の**完全代表系**という。完全代表系は代表元の選び方により変わるもので、一意的に定まるものではない。

問 1.4.2. 問 1.2.1 は $a \equiv b \pmod n$ で定まる関係が $\mathbb{Z}$ 上の同値関係であることを示している。このときの類別、及び完全代表系を求めよ。

問 1.4.3. 実数を成分とする n 次正方行列全体の集合を $M_n(\mathbb{R})$ と書くことにする。$A, B \in M_n(\mathbb{R})$ に対して、ある正則行列 P が存在して $B = P^{-1}AP$ となるとき $A \sim B$ であると定める。このとき $M_n(\mathbb{R})$ 上の関係 $\sim$ は同値関係であることを示せ。

問 1.4.4. $A, B \in M_n(\mathbb{R})$ に対して、ある正則行列 P が存在して $B = AP$ となるとき $A \sim B$ であると定める。このとき $M_n(\mathbb{R})$ 上の関係 $\sim$ は同値関係であることを示せ。

問 1.4.5. 写像 $f : A \to B$ が与えられているとする。A 上の関係 $\sim$ を $f(a) = f(a')$ のとき $a \sim a'$ であるとして定める。このとき $\sim$ は同値関係であることを示し、その類別を決定せよ。

1.5 順序集合と Zorn の補題

$\leq$ を集合 A 上の関係とする。$\leq$ が

(O1) [**反射律**] 任意の $a \in A$ について $a \leq a$ である。

(O2) [**非対称律**] $a \leq b$ かつ $b \leq a$ ならば $a = b$ である。

(O3) [**推移律**] $a \leq b$ かつ $b \leq c$ ならば $a \leq c$ である。

をすべて満たすとき $\leq$ を**順序** (order) といい、$(A, \leq)$ を**順序集合** (ordered set) という。順序 $\leq$ を明示しないで A を順序集合ということもある。$a \leq b$ を $b \geq a$ とも書く。また $a \leq b$ であって $a \neq b$ のとき、$a \lneq b$ または $a < b$ とも書く。

B が順序集合 A の部分集合であるとき、B は A の順序によって順序集合である。

例 1.5.1. $\mathbb{R}$ は通常の順序で順序集合である。$\mathbb{Q}, \mathbb{Z}$ は $\mathbb{R}$ の部分集合であるから $\mathbb{R}$ における順序によって順序集合である。

順序集合 $(A, \leq)$ において、任意の二元 a, b について $a \leq b$ または $b \leq a$ が成り立つとき、$\leq$ を**全順序** (totally order)、$(A, \leq)$ を**全順序集合** (totally ordered set) という。(単なる順序を**半順序** (partially order) ともいう。)

例 1.5.2. A を集合とし $P(A)$ でその部分集合全体の集合を表す。$P(A)$ を A の**べき集合** (power set) といい 2^A とも書く。このとき $P(A)$ は集合の包含関係 $\subset$ によって順序集合である。A が少なくとも 2 つの元を含むとき、$P(A)$ は全順序集合ではない。

$(A, \leq)$ を順序集合とする。$a \lneq b$ となる $b \in A$ が存在しないとき、すなわち $a \leq b$, $b \in A$ ならば $a = b$ が成り立つとき、$a \in A$ を**極大元** (maximal element) という。$b \lneq a$ となる $b \in A$ が存在しないとき、$a \in A$ を**極小元** (minimal element) という。任意の $b \in A$ に対して $b \leq a$ となるとき、$a \in A$ を**最大元** (largest element) という。任意の $b \in A$ に対して $a \leq b$ となるとき、$a \in A$ を**最小元** (smallest element) という。最大 (小) 元は極大 (小) 元であるが、一般に逆は正しくない。また極大 (小) 元は存在するとは限らない。

例 1.5.3. 開区間 $(0, 1)$ を自然な順序によって順序集合と見る。このとき $(0, 1)$ に極大 (小) 元、最大 (小) 元は存在しない。

例 1.5.4. 二つ以上の元を含む集合 A のべき集合 $P(A)$ の部分集合 $S = \{X \in P(A) \mid X \neq A\}$ を包含関係によって順序集合と見る。このとき、任意の $a \in A$ に対して $A - \{a\}$ は S の極大元であるが最大元ではない。$S' = \{X \in P(A) \mid X \neq \phi\}$ とすると、任意の $a \in A$ に対して $\{a\}$ は S' の極小元であるが最小元ではない。

B を順序集合 A の部分集合とする。$a \in A$ が B の**上界**であるとは、任意の $b \in B$ に対して $b \leq a$ となることである。B の上界が存在するとき B は**上に有界である**という。A が**帰納的**であるとは、A の空でない任意の全順序部分集合が上に有界であることとする。

定理 1.5.5 (Zorn の補題)**.** A が帰納的順序集合であるならば A には極大元が存在する。

Zorn の補題は選択公理、整列可能定理と同値であり、厳密な数学においてはその利用に注意が必要であるが、ここでは深くは扱わないで、それを認める。

順序集合 $(A, \leq)$ が**整列集合** (well ordered set) であるとは、A の空でない任意の部分集合に最小元が存在することである。整列可能定理は、任意の集合が適当な順序によって整列集合にできることを主張する。

1.6 二項演算

A を集合とする。写像 $f : A \times A \to A$ を A の **(二項) 演算**という。f による (a, b) の像 $f(a, b)$ を ab や $a + b$ などで表す。ab と書くとき、この演算を**乗法**といい ab を**積**という。同様に、$a + b$ と書くとき、この演算を**加法**といい $a + b$ を**和**という。

任意の $a, b, c \in A$ に対して $(ab)c = a(bc)$ が成り立つとき、この演算は**結合法則**を満たすという。

$ab = ba$ であるとき a と b は**可換である**といい、任意の二元が可換である演算は**交換法則**を満たすという。一般に演算は交換法則を満たすとは限らないが、交換法則を満たさない演算に対しては加法の表記を用いない。

加法と乗法の両方が定義された集合 A において、任意の $a, b, c \in A$ について

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc$$

が成り立つとき**分配法則**が成り立つという。乗法について交換法則が満たされるとは限らないので、両方の式が必要であることに注意しておく。

例 1.6.1. (1) $\mathbb{Z}$ で通常の加法を演算とすれば結合法則、交換法則が成り立つ。演算を乗法にしても同様である。また $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ などでも加法、乗法、共に同様である。

(2) $\mathbb{Z}$ で通常の減法を演算とすれば結合法則、交換法則、共に成り立たない。

(3) $n \geq 2$ とする。実数体 $\mathbb{R}$ 上の n 次正方行列全体の集合 $M_n(\mathbb{R})$ で通常の行列の乗法を演算とすれば、結合法則は成り立つが、交換法則は成り立たない。また $M_n(\mathbb{R})$ において通常の加法と乗法で分配法則が成り立つ。

A の二項演算は写像 $f : A \times A \to A$ であるから、二項演算を定めるということは、任意の $(a, b) \in A \times A$ に対して $f(a, b) \in A$ を特定することである。特に $|A| < \infty$ のときには、そのすべてを書き表せばよい。これには表を用いるのが効率が良い。例えば $A = \{a, b, c\}$ のとき

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

とし $f(b, a) = c$ のように読むことにすれば、これは二項演算を定めている。このような表を**演算表**という。演算が乗法で書かれているときには**乗法表**、加法で書かれているときには**加法表**ともいう。

問 1.6.2. 上の演算表について、交換法則、結合法則が満たされるかどうかを、それぞれ判定せよ。

1.7 半群とモノイド

集合 A に一つの演算 (以下では乗法とする) が定義されていて、結合法則 $(ab)c = a(bc)$ を満たすとする。このとき A を**半群** (semigroup) という。

半群 A の n 個の元 $a_1, a_2, \cdots, a_n$ に対して $((\cdots((a_1a_2)a_3)\cdots)a_{n-1})a_n$ を $a_1a_2\cdots a_n$ と書く。結合法則は「3 つの元の積はその順番を変えなければどの順序で演算を行っても、その結果は変わらない」ということを意味している。一般に 3 つ以上の場合でもこれは正しい。

定理 1.7.1 (一般化された結合法則)**.** 半群 A の n 個の元の積について、その順番を変えなければどの順序で演算を行っても、その結果は変わらない。

証明. n に関する帰納法で証明する。$n \leq 3$ の場合は正しい。$n \geq 4$ とし $n-1$ 個以下の積については正しいと仮定する。最後の演算が XY となったとし、X は r 個の元の積、Y は $n-r$ 個の元の積であるとする。

$r = n-1$ のとき、帰納法の仮定から $X = a_1a_2\cdots a_{n-1}$ であるから $XY = a_1a_2\cdots a_n$ である。

$r \leq n-2$ とする。帰納法の仮定から $X = a_1a_2\cdots a_r$, $Y = a_{r+1}a_{r+2}\cdots a_n$ である。よって、帰納法の仮定に注意して

$$\begin{aligned} XY &= (a_1a_2\cdots a_r)(a_{r+1}a_{r+2}\cdots a_n) = (a_1a_2\cdots a_r)((a_{r+1}a_{r+2}\cdots a_{n-1})a_n) \\ &= ((a_1a_2\cdots a_r)(a_{r+1}a_{r+2}\cdots a_{n-1}))a_n = (a_1a_2\cdots a_{n-1})a_n \\ &= a_1a_2\cdots a_{n-1}a_n \end{aligned}$$

である。 □

半群 A において交換法則 $ab = ba$ が成り立つとき、A を**可換半群**という。可換半群においては、n 個の元の積は、元の順番、演算の順番をどの様に変えても、その結果は変わらない。

半群 A の元 e で、任意の $a \in A$ に対して $ae = ea = a$ となるものが存在するとき、この e を A の**単位元** (identity element) という。単位元が存在する半群を**モノイド** (monoid) という。

例 1.7.2. (1) $\mathbb{N}$ は通常の乗法で (可換) 半群である。また 1 が単位元になるのでモノイドである。

(2) $\mathbb{N} - \{1\}$ は通常の乗法で半群であるが、単位元は存在しない。

(3) $\mathbb{Z}$ は通常の加法で (可換) 半群である。また 0 が単位元になるのでモノイドである。

(4) $\mathbb{N}$ は通常の加法で半群であるが、単位元は存在しない。

命題 1.7.3. モノイドの単位元はただ一つ存在する。

証明. e, e' をともに単位元であるとする。e が単位元だから $e' = ee'$ である。また e' が単位元であるから $e = ee'$ である。よって $e = e'$ であり、単位元はただ一つである。 □

演算が乗法で書かれたモノイド A において、その単位元を 1 または 1_A などと書く。演算が加法で書かれているときには、その単位元を 0 または 0_A と書く。(代数においては、多くの集合の演算を同時に考えることがあり、それぞれが単位元をもつとき、単に 1 と書いたのでは区別が難しい。このとき 1_A などと書き、どの半群の単位元なのかを明らかにするのである。逆に、考えている半群が一つしかないようなときには区別の必要がないので、単に 1 のように表しても問題はない。)

モノイド A の元 a と自然数 n について $a^0 = 1_A$, $a^n = a^{n-1}a$ と定める。a^n を a **の** n **乗** (a to the n-th power) という。

問 1.7.4. モノイド A において指数法則が成り立つことを示せ。すなわち $a \in A$ と $m, n \in \mathbb{N}$ に対して以下を示せ。

(1) $a^m a^n = a^{m+n}$

(2) $(a^m)^n = a^{mn}$

(3) $ab = ba$ ならば $(ab)^m = a^m b^m$

例 1.7.5. 集合 X に対して、X^X で X から X への写像全体の集合を表すことにする。$\sigma, \tau \in X^X$ に対して、その積 $\sigma\tau$ を $(\sigma\tau)(x) = \sigma(\tau(x))$ で定める ($\sigma\tau = \sigma \circ \tau$ である)。このとき X^X はモノイドで、その単位元は恒等写像 id_X である。

A をモノイドとする。$u \in A$ に対して $uu' = u'u = 1$ となる $u' \in A$ が存在するとき u を A の**正則元**、**単元**、または**単数** (unit)、などという。このときの u' を u の**逆元** (inverse element) という。

命題 1.7.6. モノイド A の正則元 u の逆元はただ一つ存在する。

証明. u', u'' を u の逆元とする。このとき

$$u' = u'1 = u'(uu'') = (u'u)u'' = 1u'' = u''$$

である。 □

正則元 u の逆元を u^{-1} と書く。u^{-1} も正則元で $(u^{-1})^{-1} = u$ である。

例 1.7.7. モノイド A において 1_A は正則元で $(1_A)^{-1} = 1_A$ である。

問 1.7.8. $u_1, u_2, \cdots, u_n$ をモノイドの正則元とする。このとき $u_1u_2\cdots u_n$ も正則元で $(u_1u_2\cdots u_n)^{-1} = {u_n}^{-1}\cdots {u_2}^{-1}{u_1}^{-1}$ である。これを示せ。

u をモノイド A の正則元とする。0 と $n \in \mathbb{N}$ に対して

$$u^0 = 1_A, \quad u^{-n} = (u^{-1})^n$$

とすれば、指数法則は任意の $m, n \in \mathbb{Z}$ に対して成り立つ。

問 1.7.9. モノイド X^X (例 1.7.5 参照) において $\sigma \in X^X$ が正則元であることと、σ が全単射であることは同値である。これを示せ。

参考文献

[1] 代数学, 永尾汎, 朝倉書店

[2] 代数学入門, 石田信, 実教出版