代数学入門

花木 章秀

2012 年前期
(2012/04/06)

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。

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 $\emptyset$ 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 $A_\lambda \cap A_{\lambda'} = \emptyset$ 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 (有理整数環)
- $\mathbb{Q}$: 有理数全体の集合 (有理数体)
- $\mathbb{R}$: 実数全体の集合 (実数体)
- $\mathbb{C}$: 複素数全体の集合 (複素数体)

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 $f^{-1}(b) = \emptyset$ 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 $C_a \cap C_b = \emptyset$ 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

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

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。異なる同値類全体の集合を、集合 A を同値関係 $\sim$ で**割った集合**といい $A/\sim$ と書く。

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。$S' = \{X \in P(A) \mid X \neq \emptyset\}$ 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

空でない集合 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。

Chapter 2

群

2.1 群の定義と例

すべての元が正則元であるモノイドを**群** (group) という。すなわち、演算の定義された集合 G で

(G1) [**結合法則**] 任意の $a, b, c \in G$ について $a(bc) = (ab)c$ である。

(G2) [**単位元の存在**] ある $e \in G$ が存在して、任意の $a \in G$ に対して $ea = ae = a$ である。(このとき e を 1_G とも書く。)

(G3) [**逆元の存在**] 任意の $a \in G$ に対して、ある $b \in G$ が存在して $ab = ba = e$ である。(このときの b を a^{-1} と書く。)

がすべて成り立つとき G を群という。群は半群やモノイドの特別なものであるから、それらに対して成り立つことはすべて成り立つ。群 G において、更に

(G4) [**交換法則**] 任意の $a, b \in G$ について $ab = ba$ である。

が成り立つとき G を**アーベル群** (abelian group)、または**可換群** (commutative group) という。

命題 2.1.1. 群 G について次が成り立つ。

(1) [**簡約法則**] $ax = ay$ ならば $x = y$ である。また $xa = ya$ ならば $x = y$ である。

(2) $f : G \to G$ $(x \mapsto x^{-1})$ は全単射である。

(3) $a \in G$ を一つ固定するとき

$$\begin{aligned} g_a &: G \to G \quad (x \mapsto xa) \\ h_a &: G \to G \quad (x \mapsto ax) \\ k_a &: G \to G \quad (x \mapsto a^{-1}xa) \end{aligned}$$

はすべて全単射である。

証明. (1) $ax = ay$ とすると、両辺に左から a^{-1} をかけて $x = y$ となる。逆も同様である。(2) $(x^{-1})^{-1} = x$ より $f^2 = \mathrm{id}_G$ となり f は全単射である。(3) $g_a \circ g_{a^{-1}} = g_{a^{-1}} \circ g_a = \mathrm{id}_G$ となり g_a は全単射である。他も同様である。 □

命題 2.1.2. 群 G において、任意の $x \in G$ が $x^2 = 1$ を満たすならば、G はアーベル群である。

証明. 任意の $x \in G$ に対して $x^2 = 1$ より $x^{-1} = x$ である。よって任意の $a, b \in G$ に対して $(ab)^{-1} = ab$ である。一方 $(ab)^{-1} = b^{-1}a^{-1} = ba$ であるから $ab = ba$ となる。 □

例 2.1.3. $\mathbb{Q}^\sharp = \mathbb{Q} - \{0\}$ とおく。このとき $\mathbb{Q}^\sharp$ は乗法に関してアーベル群で、単位元は 1、$a \in \mathbb{Q}^\sharp$ の逆元は $1/a$ である。$\mathbb{R}^\sharp = \mathbb{R} - \{0\}$, $\mathbb{C}^\sharp = \mathbb{C} - \{0\}$ でも同様である。

例 2.1.4. (1) $\mathbb{Q}$ は乗法に関してモノイドではあるが群ではない。なぜならば 0 に逆元がないからである。

(2) $\mathbb{Z}^\sharp = \mathbb{Z} - \{0\}$ は乗法に関してモノイドではあるが群ではない。なぜならば 2 に逆元がないからである。

命題 2.1.5. M をモノイドとし U を M の正則元全体の集合とする。このとき U は M の演算で群になる。

証明. $a, b \in U$ ならば $ab \in U$ なので演算は U で定義される。また $1 \in U$ より U はモノイドである。$a \in U$ ならば $a^{-1} \in U$ も成り立ち U は群である。 □

この命題の U を $U(M)$ と書いて M の**単数群** (unit group) という。

例 2.1.6. (1) $\mathbb{Q}$ は乗法に関してモノイドである。その単数群は $U(\mathbb{Q}) = \mathbb{Q}^\sharp = \mathbb{Q} - \{0\}$ である。

(2) $\mathbb{Z}$ は乗法に関してモノイドである。その単数群は $U(\mathbb{Z}) = \{-1, 1\}$ である。

例 2.1.7 (対称群)**.** モノイド X^X (例 1.7.5) について、その単数群 $U(X^X)$ を X 上の**対称群** (symmetric group) といい、これを $S(X)$ と書くことにする。$S(X)$ の元は X から X への全単射で、それを X 上の**置換** (permutation) という。置換を具体的に書くには

$$S(X) \ni \sigma = \begin{pmatrix} x \\ \sigma(x) \end{pmatrix}$$

のように書く。特に $|X| = n$ のとき、$X = \{1, 2, \cdots, n\}$ と考えても本質的には同じである。このとき $S(X)$ を S_n とも書き、これを n **次対称群**という。S_n の元を n 次の置換という。

例 2.1.8. 3 次対称群 S_3 の元をすべて書くと以下のようになる。

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

元の積は以下のようになる。

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

右の置換を先に行い、例えば 1 については $1 \mapsto 1 \mapsto 3$ となる。逆元は上の行と下の行を入れ替えて

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

と計算できる。置換を表す列の並びは元の対応を表しているだけなので、列を並び替えても構わない。

問 2.1.9. S_3 の演算表を書け。

問 2.1.10. $n \geq 3$ のとき S_n はアーベル群ではないことを、具体的に $\sigma\tau \neq \tau\sigma$ なる $\sigma, \tau \in S_n$ を見つけることによって示せ。

群 G について、$|G| < \infty$ のとき G を**有限群** (finite group) という。また $|G| = \infty$ のとき G を**無限群** (infinite group) という。$|G| < \infty$ のとき $|G|$ を G の**位数** (order) という。

問 2.1.11. n 次対称群 S_n の位数は $n!$ であることを示せ。

例 2.1.12 (一般線形群)**.** $\mathbb{R}$ を成分とする n 次正方行列の全体を $M(n, \mathbb{R})$ と書く。$M(n, \mathbb{R})$ が行列の積によって単位行列を単位元とするモノイドである。その単数群を $\mathbb{R}$ 上 n 次の**一般線形群** (general linear group) といい $GL(n, \mathbb{R})$ と書く。$M(n, \mathbb{R})$ の単数は正則行列のことであるから $GL(n, \mathbb{R})$ は正則行列全体の集合である。$GL(n, \mathbb{R})$ は無限群である。

$GL(n, \mathbb{Q})$, $GL(n, \mathbb{C})$ も同様である。

(これらは $M_n(\mathbb{R})$, $GL_n(\mathbb{R})$ などとも書かれる。)

問 2.1.13. $n \geq 2$ のとき $GL(n, \mathbb{R})$ はアーベル群ではないことを示せ。

問 2.1.14. A をモノイドで、集合として有限集合であるとする。右簡約法則「$x, y, z \in A$ に対して $xz = yz$ ならば $x = y$ である」が成り立つとすると A は群になる。これを示せ。また A が有限集合ではないとき、これは正しくない。そのような例を具体的に一つ示せ。

2.2 加群

群 G がアーベル群であるとき、その演算を加法の形で書くことが多い。このとき G を**加群** (additive group)、または**加法群**という。加群の単位元を**零元**といい 0 または 0_G と書く。また a の逆元は $-a$ と書く。群の定義を加法の形で書き直すと以下のようになる。

(A1) [**結合法則**] 任意の $a, b, c \in G$ について $a + (b + c) = (a + b) + c$ である。

(A2) [**零元の存在**] ある $0 \in G$ が存在して、任意の $a \in G$ に対して $0+a = a+0 = a$ である。

(A3) [**逆元の存在**] 任意の $a \in G$ に対して、ある $b \in G$ が存在して $a+b = b+a = 0$ である。(このときの b を $-a$ と書く。)

(A4) [**交換法則**] 任意の $a, b \in G$ について $a+b = b+a$ である。

加群 G において $a+(-b)$ を $a-b$ と書く。

例 2.2.1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は (通常の加法によって) すべて加群である。$\mathbb{N}$ は加群ではない。

$n \in \mathbb{N}$ に対して、加群 G の元 a を n 個加えたものを na と書く。また $-a$ を n 個加えたものを $-na$ と書く。また $0a = 0$ と定める。これによって任意の $m \in \mathbb{Z}$ に対して ma が定義され、以下が成り立つ。$a, b \in G$, $m, n \in \mathbb{Z}$ とする。

(1) $(-m)a = m(-a) = -(ma)$ である。特に $(-1)a = -a$ である。

(2) $(m+n)a = ma + na$

(3) $m(na) = (mn)a$

(4) $m(a+b) = ma + mb$

ここで (2), (3), (4) は通常の意味の分配法則、結合法則ではないことに注意する。

2.3 部分群

群 G の空でない部分集合 H が

(B1) $a, b \in H$ ならば $ab \in H$ である。

(B2) $a \in H$ ならば $a^{-1} \in H$ である。

を満たすとき、H を G の**部分群** (subgroup) という。

命題 2.3.1. 群 G の空でない部分集合 H について以下は同値である。

(1) H は G の部分群である。

(2) H は G の演算によって群である。

(3) $a, b \in H$ ならば $ab^{-1} \in H$ である。

証明. (1) $\Longrightarrow$ (2) H を G の部分群とする。(B1) より $a, b \in H$ ならば $ab \in H$ であるから G の演算は H の演算を定義する。結合法則は G で成り立つので H でも成り立つ。また H は空でないからある元 a を含む。このとき (B2) より $a^{-1} \in H$ でもある。よって $1_G = aa^{-1} \in H$ であり 1_G は H においても単位元である。(B2) により任意の元の逆元も存在する。

(2) $\Longrightarrow$ (3) 群の定義より明らかである。

(3) $\Longrightarrow$ (1) H は空でないから $a \in H$ をとると $1 = aa^{-1} \in H$ である。任意に $a \in H$ をとる。このとき $1 \in H$ より $a^{-1} = 1a^{-1} \in H$ である。よって (B2) が成り立つ。最後に任意に $a, b \in H$ をとる。(B2) より $b^{-1} \in H$ である。したがって $ab = a(b^{-1})^{-1} \in H$ となり (B1) が成り立つ。 □

命題 2.3.2. H, K が共に G の部分群であるとき $H \cap K$ も G の部分群である。

証明. $a, b \in H \cap K$ とする。$ab^{-1} \in H \cap K$ を示せばよい。$a \in H$, $b \in H$ であるから H が部分群であることにより $ab^{-1} \in H$ である。同様に K が部分群であることにより $ab^{-1} \in K$ である。よって $ab^{-1} \in H \cap K$ である。 □

群 G の部分集合 A, B に対して

$$\begin{aligned} AB &= \{ab \mid a \in A,\ b \in B\} \\ A^{-1} &= \{a^{-1} \mid a \in A\} \end{aligned}$$

と定める。特に $B = \{b\}$ のときには $A\{b\}$ を Ab とも書く。bA も同様である。

$$Ab = \{ab \mid a \in A\}, \quad bA = \{ba \mid a \in A\}$$

問 2.3.3. 群 G と、その部分集合 A, B, C に対して、次が成り立つことを示せ。

(1) $A(BC) = (AB)C$

(2) $(A^{-1})^{-1} = A$

(3) $(AB)^{-1} = B^{-1}A^{-1}$

問 2.3.4. 群 G と、その空でない部分集合 H に対して、以下は同値であることを示せ。

(1) H は G の部分群である。

(2) $HH \subset H$ かつ $H^{-1} \subset H$

(3) $HH^{-1} \subset H$

問 2.3.5. H が群 G の部分群であるとき

$$HH = HH^{-1} = H^{-1} = H$$

が成り立つ。これを示せ。

注意. 上記の計算を群の元の計算と混同してはいけない。例えば $HH^{-1} = 1$ は一般に正しくない。(なぜ正しくないのかを考えよ。)

命題 2.3.6. 群 G と、その空でない部分集合 H に対して、$|H| < \infty$ かつ $HH \subset H$ ならば H は G の部分群である。

証明. $h \in H$ に対して $h^{-1} \in H$ を示せばよい。$HH \subset H$ より $h^2 \in H$ であり、同様にに繰り返せば、任意の $n \in \mathbb{N}$ に対して $h^n \in H$ である。H は有限集合であるから、すべての h^n が異なることはできず、したがってある $m, n \in \mathbb{N}$, $m < n$ が存在して $h^m = h^n$ となる。このとき簡約法則によって $h^{n-m} = 1$ である。$n - m = 1$ ならば $1 = h \in H$ であり、$h^{-1} = 1 \in H$ である。$n - m > 0$ のとき $n - m - 1 \leq 0$ であって、よって $h^{-1} = h^{n-m-1} \in H$ となる。 □

命題 2.3.7. H, K が群 G の部分群であるとき次が成り立つ。

(1) HK が G の部分群であるための必要十分条件は $HK = KH$ である。

(2) L が H を含む G の部分群であるならば $(HK) \cap L = H(K \cap L)$ である。

証明. (1) HK が G の部分群であるとする。このとき $(HK)^{-1} = HK$ である。一方 $H^{-1} = H$, $K^{-1} = K$ なので $(HK)^{-1} = K^{-1}H^{-1} = KH$ となるので $HK = KH$ となる。

次に $HK = KH$ であるとする。このとき $(HK)(HK)^{-1} = HKK^{-1}H^{-1} = HKKH = HHKK = HK$ であるから HK は G の部分群である。

(2) $x \in HK \cap L$ とする。$x \in HK$ より $h \in H$ と $k \in K$ が存在して $x = hk$ である。$x \in L$ であって $h \in H \subset L$ であるから $k = h^{-1}x \in L$ である。よって $k \in K \cap L$ となり $x = hk \in H(K \cap L)$ である。以上より $(HK) \cap L \subset H(K \cap L)$ となる。

$y \in H(K \cap L)$ とする。ある $h \in H$ と $k \in K \cap L$ が存在して $y = hk$ である。このとき $y = hk \in HK$ であり、$h \in H \subset L$ であるから $y = hk \in L$ も成り立つ。よって $y \in HK \cap L$ であり $H(K \cap L) \subset HK \cap L$ である。

以上により $(HK) \cap L = H(K \cap L)$ が成り立つ。 □

群 G において G 自身と $\{1\}$ は G の部分群である。$\{1\}$ を G の**自明な部分群** (trivial subgroup) という。自明な部分群を単に 1 と書くことも多い。また G と異なる部分群を**真部分群** (proper subgroup) という。

S を群 G の部分集合とする。

$$a_1{}^{n_1} a_2{}^{n_2} \cdots a_r{}^{n_r} \quad (a_i \in S, n_i \in \mathbb{Z}, r \in \mathbb{N})$$

の形の元すべての集合は G の部分群である。これを $\langle S \rangle$ と書き、S **で生成される部分群** (subgroup generated by S) という。S が有限集合 $\{s_1, \cdots, s_\ell\}$ であるとき $\langle S \rangle$ を $\langle s_1 \cdots, s_\ell \rangle$ とも書く。

特に $S = \{a\}$ のとき

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots\}$$

である。これを a で生成される**巡回群** (cyclic group) といい a をその**生成元** (generater) という。部分群 $\langle a \rangle$ の位数を元 a の**位数** (order) といい $o(a)$ と書く。

問 2.3.8. $\langle S \rangle$ が部分群であることを示せ。

命題 2.3.9. 巡回群 $\langle a \rangle$ について次が成り立つ。

(1) $a^m = 1$ となる $m \in \mathbb{N}$ が存在することと $\langle a \rangle$ が有限巡回群であることは同値である。

(2) $\langle a \rangle$ が有限巡回群であるとする。$a^m = 1$ となる $m \in \mathbb{N}$ のうち最小のものを n をすれば $n = o(a)$ であって次が成り立つ。

(i) $a^m = 1 \iff n \mid m$

(ii) $\langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ であって、これらの元はすべて相異なる。

(3) $\langle a \rangle$ が無限巡回群ならば

$$\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots$$

はすべて相異なり $\langle a \rangle$ はこれらの元からなる。

証明. (1) $a^m = 1$ なる $m \in \mathbb{N}$ が存在するとする。このとき、任意の $\ell \in \mathbb{Z}$ について $\ell = nq + r$, $0 \leq r < m$ なる $q, r \in \mathbb{Z}$ が存在する。このとき $a^\ell = (a^m)^q a^r = a^r$ であるから、$\langle a \rangle \subset \{1, a, a^2, \cdots, a^{m-1}\}$ であって、これは有限である。

逆に $\langle a \rangle$ が有限群であるとすれば、ある $0 < s < t$ に対して $a^s = a^t$ であり、このとき $a^{t-s} = 1$, $t - s \in \mathbb{N}$ である。

(2) (i) $a^m = 1$ とすると $m = nq + r$, $0 \leq r < n$ なる $q, r \in \mathbb{Z}$ が存在する。このとき

$$1 = a^m = (a^n)^q a^r = a^r$$

となるが n の最小性から $r = 0$ である。よって $n \mid m$ である。$n \mid m$ と仮定すれば、明らかに $a^m = (a^n)^{m/n} = 1$ である。

(i) より $\langle a \rangle = \{1, a, a^2, \cdots, a^{n-1}\}$ となることはすぐに分かる。これらがすべて異なることを示す。$0 \leq i < j < n$ に対して $a^i = a^j$ とすると $a^{j-i} = 1$, $0 < j - i < n$ となり n の最小性に反する。よってこれらはすべて異なり $o(a) = |\langle a \rangle| = n$ である。

(2) $\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots$ がすべて異なることを示せばよい。$i < j$ $(i, j \in \mathbb{Z})$ に対して $a^i = a^j$ と仮定すると、前と同様に $a^{j-i} = 1$, $0 < j - i$ となり $\langle a \rangle$ は有限巡回群になる。よって、これらの元はすべて異なる。 □

2.4 剰余類

H を群 G の部分群とする。G 上の関係 $\sim$ を「$aH = bH$ のとき $a \sim b$」で定める。このとき $\sim$ は G 上の同値関係であることを示そう。

まず、任意の $a \in G$ に対して $aH = aH$ であるから $a \sim a$ である。次に $a \sim b$ と仮定する。このとき $aH = bH$ であるから $bH = aH$ で $b \sim a$ が成り立つ。$a \sim b$ かつ $b \sim c$ と仮定すれば $aH = bH = cH$ であるから $a \sim c$ である。以上より $\sim$ は同値関係である。

命題 2.4.1. H を群 G の部分群 H とする。$a, b \in G$ について次の条件は同値である。

(1) $a \sim b$ (すなわち $aH = bH$)

(2) $b \in aH$

(3) $a \in bH$

(4) $a^{-1}b \in H$

証明. (1) $\Longrightarrow$ (2) $b = b1 \in bH = aH$ である。

(2) $\Longrightarrow$ (3) $b \in aH$ とすると、ある $h \in H$ が存在して $b = ah$ である。このとき $h^{-1} \in H$ であるから $a = bh^{-1} \in bH$ である。

(3) $\Longrightarrow$ (4) $a \in bH$ とすると、ある $h \in H$ が存在して $a = bh$ である。このとき $a^{-1}b = h^{-1} \in H$ である。

(4) $\Longrightarrow$ (1) ある $h \in H$ が存在して $a^{-1}b = h$ である。このとき $a = bh^{-1}$, $b = ah$ に注意しておく。

任意の $h_1 \in H$ に対して $ah_1 = bh^{-1}h_1 \in bH$ であるから $aH \subset bH$ が成り立つ。任意の $h_2 \in H$ に対して $bh_2 = ahh_2 \in aH$ であるから $bH \subset aH$ が成り立つ。以上より $aH = bH$ である。 □

以上のことは関係 $\sim$ を $Ha = Hb$ で定義しても同様に成り立つ。

aH を H の**左剰余類** (left coset) といい、左剰余類全体の集合を G/H と書く。同様に Ha を H の**右剰余類** (right coset) といい、右剰余類全体の集合を $H \setminus G$ と書く。

$\sim$ は同値関係で左剰余類はその同値類となるので、左剰余類に関する類別

$$G = \bigcup_{i \in I} a_i H$$

が得られる。

問 2.4.2. $G = \bigcup_{i \in I} a_i H$ が左剰余類に関する類別であることと、$G = \bigcup_{i \in I} H a_i^{-1}$ が右剰余類に関する類別であることは同値であることを示せ。

例 2.4.3. 3 次対称群 S_3 を考える。S_3 の元は

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$g_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad g_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

である。

$H = \langle g_2 \rangle = \{g_1, g_2\}$ として左剰余類を考えてみると

$$\begin{aligned} g_1 H &= g_2 H = \{g_1, g_2\} \\ g_3 H &= g_4 H = \{g_3, g_4\} \\ g_5 H &= g_6 H = \{g_5, g_6\} \end{aligned}$$

である。一方、右剰余類は

$$\begin{aligned} H g_1 &= H g_2 = \{g_1, g_2\} \\ H g_3 &= H g_5 = \{g_3, g_5\} \\ H g_4 &= H g_6 = \{g_4, g_6\} \end{aligned}$$

である。よってこの場合、左剰余類による類別と右剰余類による類別は異なっている。

$K = \langle g_4 \rangle = \{g_1, g_4, g_5\}$ として左剰余類を考えてみると

$$\begin{aligned} g_1K &= g_4K = g_5K = \{g_1, g_4, g_5\} \\ g_2K &= g_3K = g_6K = \{g_2, g_3, g_6\} \end{aligned}$$

であり、右剰余類も

$$\begin{aligned} Kg_1 &= Kg_4 = Kg_5 = \{g_1, g_4, g_5\} \\ Kg_2 &= Kg_3 = Kg_6 = \{g_2, g_3, g_6\} \end{aligned}$$

となる。よってこの場合、左剰余類による類別と右剰余類による類別は一致している。

上の例のように、部分群 H による左剰余類による類別と右剰余類による類別が一致するとき、言い換えれば $aH = Ha$ が任意の $a \in G$ について成り立つとき、H を G の**正規部分群** (normal subgroup) という。特に G がアーベル群ならば任意の部分群は正規部分群である。

問 2.4.4. G を有限群とし H をその部分群とする。任意の $a \in G$ に対して $|aH| = |H|$ であることを示せ。また、異なる左剰余類の数を $|G : H|$ と書くとき $|G| = |G : H||H|$ であることを示せ。(これを **Lagrange の定理**という。また $|G : H|$ を G における H の**指数** (index) という。右剰余類についても同様のことが成り立つ。)

問 2.4.5. G を有限群とする。$x \in G$ に対して x の位数は $|G|$ の約数であることを示せ。これによって、 G の任意の元 x について $x^{|G|} = 1$ が成り立つことが分かる。

2.5 剰余群

G を群とし N をその正規部分群とする。このとき、任意の $a \in G$ について $aN = Na$ である。よって剰余類は右、左の区別をする必要がない。剰余類全体の集合 G/N に以下のような演算を考える。

$$(aN)(bN) = (ab)N$$

まずこれが矛盾なく定義されることを示す。

> この場合 $aN = a'N$ となる $a' \in G$ が存在するかもしれない。違う a' を使うと結果が変わってしまうというのでは演算 (写像) が定義されているとはいえない。したがって、演算が矛盾なく定義されるためには $aN = a'N$ かつ $bN = b'N$ と仮定したとき $(ab)N = (a'b')N$ が成り立たなければならない。

$aN = a'N$ かつ $bN = b'N$ と仮定する。ある $n_1, n_2 \in N$ が存在して $a' = an_1$, $b' = bn_2$ である。また $bN = Nb$ なので、ある $n_3 \in N$ が存在して $n_1b = bn_3$ である。よってこのとき

$$a'b' = an_1bn_2 = abn_3n_2 \in (ab)N$$

となり $(a'b')N = (ab)N$ である。よってこの演算は矛盾なく定義される。

この演算に関して、結合法則が成り立つことは明らかで、更に

$$(1N)(aN) = (aN)(1N) = aN, \quad (aN)(a^{-1}N) = (a^{-1}N)(aN) = 1N$$

が成り立つ。よって G/N はこの演算によって $1N$ を単位元とする群になる。aN の逆元は $a^{-1}N$ である。この群を G の N による**剰余群** (factor group) といい、剰余類全体の集合と同じ記号を使って G/N とかく。

例 2.5.1. $\mathbb{Z}$ を加群と見る。$n \in \mathbb{N}$ を一つ固定する。n で生成される部分群 $\langle n \rangle$ は n の倍数全体の集合で、これを $n\mathbb{Z}$ と書く。$a \in \mathbb{Z}$ を含む $n\mathbb{Z}$ による剰余類は

$$a + n\mathbb{Z} = \{a + n\ell \mid \ell \in \mathbb{Z}\}$$

である。また $\{0, 1, \cdots, n-1\}$ は剰余類による類別の完全代表系である。よって

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z},\ 1 + n\mathbb{Z}, \cdots,\ (n-1) + n\mathbb{Z}\}$$

である。演算は、例えば

$$(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$$

のようになる。

Chapter 3

環と体

3.1 定義と例

集合 R 上に加法と乗法が定義されているとする。R が**環** (ring) であるとは

(R1) R は加法に関して加群である。

(R2) R は乗法に関して半群である。

(R3) [**分配法則**] 任意の $a, b, c \in R$ について $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ が成り立つ。

を満たすことをいう。更に

(R4) [**単位元の存在**] 乗法に関する単位元 $1_R (\neq 0)$ が存在する。

が成り立つとき、R を**単位元をもつ環**という。
(R1), (R2), (R3) が成り立ち、かつ

(R5) [**交換法則**] 任意の $a, b \in R$ に対して $ab = ba$ が成り立つ。

が満たされるとき R を**可換環** (commutative ring) という。

環 R の加法に関する単位元を**零元**といい 0 または 0_R と書く。R が単位元をもつ環であるとき、乗法に関する単位元を単に**単位元**といい 1 または 1_R と書く。

問 3.1.1. 環 R の任意の元 x について $0x = x0 = 0$ であることを示せ。(この 0 は R の加群としての単位元 0_R のことで、$0_{\mathbb{Z}} \in \mathbb{Z}$ とは違う意味である。しかしこの問題によって $0_R x$ と $0_{\mathbb{Z}} x$ を区別する必要はなくなる。)

R が単位元をもつ環のとき、R は乗法についてモノイドであるから、その単数群 $U(R)$ が考えられる。$U(R)$ を環 R の**単数群** (unit group) といい、その元を R の**正則元**、または**単数** (unit) という。(正則元を扱うときには常に、考える環が単位元をもつと仮定する。)

単位元をもつ環 R において、0 以外のすべての元が正則元であるとき R を**斜体** (skew field, division ring) という。特に可換な斜体を**体** (field)、または**可換体** (commutative field) という。

例 3.1.2 (零環)**.** ただ一つの元 a をもつ集合に $a+a=a$, $aa=a$ で演算を定めれば、これは環になる。これを**零環**という。零環は単位元をもたない。

例 3.1.3 (有理整数環)**.** $\mathbb{Z}$ は通常の加法と乗法で単位元をもつ可換環である。これを**有理整数環** (rational integer ring) という。

例 3.1.4 (有理数体、実数体、複素数体)**.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は通常の加法と乗法で体である。これをそれぞれ**有理数体** (rational number field)、**実数体** (real number field)、**複素数体** (complex number field) という。

例 3.1.5 (全行列環)**.** R を (可換とは限らない) 環とする。R の元を成分とする n 次正方行列の全体は通常の演算で環になる。これを R 上 n 次の**全行列環** (full matrix ring) といい $M(n,R)$、または $M_n(R)$ と書く。R が単位元をもてば $M(n,R)$ も単位元をもつ。

R を環とする。$0\neq a\in R$ が R の**左零因子** (left zero divisor) であるとは、ある $0\neq b\in R$ が存在して $ab=0$ となることである。同様に $0\neq a\in R$ が R の**右零因子** (right zero divisor) であるとは、ある $0\neq b\in R$ が存在して $ba=0$ となることである。0 は左 (右) 零因子とはいわないことにする。

命題 3.1.6. 単位元をもつ環 R の正則元は左 (右) 零因子ではない。特に R が斜体ならば R に左 (右) 零因子は存在しない。

証明. a を正則元であり、かつ左零因子であるとする。ある $0\neq b\in R$ が存在して $ab=0$ である。このとき

$$b=1b=a^{-1}ab=a^{-1}0=0$$

となり $b\neq 0$ に矛盾する。 □

R が可換環であるときには a が左零因子であることと、右零因子であることは同値であり、左右の区別をする必要がない。このとき a を単に**零因子** (zero divisor) という。

単位元をもつ可換環 R が**整域** (integral domain) であるとは、R に零因子が存在しないことである。

例 3.1.7. 体は整域である。また有理整数環 $\mathbb{Z}$ は体ではないが整域である。

問 3.1.8. A を整域とし、集合として有限集合であるとする。このとき A は体になることを示せ。

問 3.1.9. 有理整数環 $\mathbb{Z}$ 上の全行列環 $M(n,\mathbb{Z})$ の単数はどの様なものか決定せよ。

群では簡約法則「$ax=ay$ ならば $x=y$」が成り立つが、一般の環ではこれは正しくない。しかし整域では、以下のように $a\neq 0$ という仮定の下で簡約法則が成り立つ。

命題 3.1.10. R を整域とする。$0\neq a\in R$, $x,y\in R$ に対して $ax=ay$ ならば $x=y$ である。

証明. $ax=ay$ とする。$a(x-y)=0$ となる。$a\neq 0$ なので、整域には零因子がないことから $x-y=0$ である。よって $x=y$ である。 □

問 3.1.11. 複素数体 $\mathbb{C}$ 上の全行列環 $M(2,\mathbb{C})$ で、$ax=ay$ であるが $x\neq y$ となるような例を示せ。

3.2 整数の合同によって定義される環

$n \in \mathbb{N}$, $n \geq 2$ を一つ固定する。前と同じように $a, b \in \mathbb{Z}$ に対して、ある $\ell \in \mathbb{Z}$ が存在して $a - b = n\ell$ となるとき $a \equiv b \pmod{n}$ と書くことにする (問 1.2.1)。このときこの関係は同値関係である。その a を含む同値類は

$$a + n\mathbb{Z} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + n\ell \mid \ell \in \mathbb{Z}\}$$

であった。異なる同値類全体の集合は

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z},\ 1 + n\mathbb{Z},\ \cdots,\ (n-1) + n\mathbb{Z}\}$$

である。例 2.5.1 で $\mathbb{Z}/n\mathbb{Z}$ は加群 $\mathbb{Z}$ の部分加群 $n\mathbb{Z}$ による剰余群で

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

で加法が矛盾なく定義できることを見た。同じように

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}$$

で $\mathbb{Z}/n\mathbb{Z}$ に乗法が矛盾なく定義できることを確認する。

$a + n\mathbb{Z} = a' + n\mathbb{Z}$, $b + n\mathbb{Z} = b' + n\mathbb{Z}$ とする。ある $\ell, \ell' \in \mathbb{Z}$ が存在して $a' = a + n\ell$, $b' = b + n\ell'$ である。このとき

$$a'b' = (a + n\ell)(b + n\ell') = ab + n(a\ell' + b\ell + n\ell\ell') \in ab + n\mathbb{Z}$$

であるから $a'b' + n\mathbb{Z} = ab + n\mathbb{Z}$ であり、乗法は矛盾なく定義される。

$\mathbb{Z}/n\mathbb{Z}$ は加群であり、乗法については $1 + n\mathbb{Z}$ を単位元とするモノイドである。また分配法則、交換法則が成り立つことは容易に確かめられ、したがって $\mathbb{Z}/n\mathbb{Z}$ は可換環の構造を持つ。以下では文脈から n が明らかなときには $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ を $\bar{a}$ とも書くことにする。$\mathbb{Z}/n\mathbb{Z}$ の単数、および零因子を考える。

例 3.2.1. $\mathbb{Z}/9\mathbb{Z}$ を考える。乗法に関する演算表は以下のようになる。

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

行に 1 を含むものが単数で、0 との積以外に 0 を含むものが零因子である。したがって単数群は $U(\mathbb{Z}/9\mathbb{Z}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ であり、零因子は $\bar{3}, \bar{6}$ である。単数同士の積は、また単数であることも確認しておこう。

一般の場合を扱うために以下の定理を用意する。

定理 3.2.2. $a, b \in \mathbb{N}$ とする。$\gcd(a,b) = d$ であるならば、ある $x, y \in \mathbb{Z}$ が存在して

$$ax + by = d$$

となる。

証明. $a > b$ と仮定してかまわない。このとき b に関する帰納法で示す。$b = 1$ ならば $\gcd(a,b) = 1$ で $x = 0$, $y = 1$ とすればよい。$b > 1$ とする。

$$a = bq + r, \quad 0 \leq r < b$$

なる $q, r \in \mathbb{Z}$ が存在する。

$\gcd(a,b) = \gcd(b,r)$ であることを示す。$d \mid b$ とする。このとき $d \mid a$ ならば $d \mid a - bq = r$ である。また $d \mid r$ ならば $d \mid bq + r = a$ である。よって d が a, b の公約数であることと b, r の公約数であることは同値である。したがって $\gcd(a,b) = \gcd(b,r)$ が成り立つ。

$r = 0$ ならば $\gcd(a,b) = \gcd(b,0) = b$ で $x = 0$, $y = 1$ とすればよい。

$d = \gcd(a,b)$ とおく。$0 < r$ とすれば $b > r$ なので b, r に帰納法の仮定を適用することができ、ある $x', y' \in \mathbb{Z}$ が存在して $bx' + ry' = d$ となる。このとき

$$d = bx' + ry' = bx' + (a - bq)y' = ay' + b(x' - qy')$$

となるから $x = y'$, $y = x' - qy'$ とおけばよい。 □

この定理を用いて、一般の $\mathbb{Z}/n\mathbb{Z}$ の単数を決定することができる。

定理 3.2.3. $a + n\mathbb{Z}$ が $\mathbb{Z}/n\mathbb{Z}$ の単数であるための必要十分条件は $\gcd(a,n) = 1$ となることである。すなわち

$$U(\mathbb{Z}/n\mathbb{Z}) = \{a + n\mathbb{Z} \mid \gcd(a,n) = 1\}$$

である。

証明. $\gcd(a,n) = 1$ とする。このとき定理 3.2.2 より、ある $x, y \in \mathbb{Z}$ が存在して $ax + ny = 1$ である。この両辺を n を法として考えれば $\bar{a}\,\bar{x} = \bar{1}$ となり $\bar{a}$ は単数である。

$\bar{a}$ が単数であるとする。ある $b \in \mathbb{Z}$ が存在して $\bar{a}\,\bar{b} = \bar{1}$ である。したがって $\ell \in \mathbb{Z}$ が存在して $ab - 1 = n\ell$ である。変形して $1 = ab - n\ell$ を得る。この式の右辺は $\gcd(a,n)$ で割り切れるので、左辺の 1 も $\gcd(a,n)$ で割り切れ $\gcd(a,n) = 1$ となる。 □

次に $\mathbb{Z}/n\mathbb{Z}$ の零因子を決定しよう。

定理 3.2.4. $\bar{0} \neq \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ について以下の条件は同値である。

(1) $\bar{a}$ は零因子である。

(2) $\bar{a}$ は単数ではない。

(3) $\gcd(a,n)>1$ である。

証明. (2) $\Longleftrightarrow$ (3) は定理 3.2.3 で示されている。零因子は単数ではないので (1) $\Longrightarrow$ (2) も成り立つ。

(3) $\Longrightarrow$ (1) $\gcd(a,n)=d>1$ とする。このとき $n=d\ell$ とすれば $1<\ell<n$ となる。$a=da'$ とすれば $\bar{\ell}\neq\bar{0}$ であって $\bar{a}\,\bar{\ell}=\bar{a'}\,\bar{n}=\bar{0}$ となる。よって $\bar{a}$ は零因子である。 □

定理 3.2.5. $\mathbb{Z}/n\mathbb{Z}$ について以下の条件は同値である。

(1) $\mathbb{Z}/n\mathbb{Z}$ は体である。

(2) $\mathbb{Z}/n\mathbb{Z}$ は整域である。

(3) n は素数である。

証明. 前の定理より (1) $\Longleftrightarrow$ (2) が成り立つ。

(3) $\Longrightarrow$ (1) n が素数ならば、任意の $1\leq a<n$ に対して $\gcd(a,n)=1$ であるから $\bar{a}$ は単数であり $\mathbb{Z}/n\mathbb{Z}$ は体である。

(1) $\Longrightarrow$ (3) $\mathbb{Z}/n\mathbb{Z}$ が体ならば、任意の $1\leq a<n$ に対して $\gcd(a,n)=1$ でなくてはならず n は素数である。 □

問 3.2.6. $128x+405y=1$ をみたす整数の組 (x,y) を一つ求めよ。

問 3.2.7. 全行列環 $M_2(\mathbb{Z}/2\mathbb{Z})$ の元をすべて書け。またその単数群を決定せよ。

3.3 部分環

R を環とする。R の空でない部分集合 S が R の**部分環** (subring) であるとは

- $a,b\in S$ ならば $a-b\in S$, $ab\in S$ である。

を満たすこととする。S が R の部分環であるとき S 自身は 環である。

例 3.3.1. $\mathbb{Z}$ は $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ の部分環である。

例 3.3.2. $R=M(n,\mathbb{R})$ とする。

$$S=\{(a_{ij})\in R\mid i>j \text{ ならば } a_{ij}=0\}=\left\{\left.\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ & a_{22} & \cdots & a_{2n}\\ & & \ddots & \vdots\\ 0 & & & a_{nn}\end{pmatrix}\right| a_{ij}\in\mathbb{R}\right\}$$

とおけば S は R の部分環であることを確認する。

$A=(a_{ij}),B=(b_{ij})\in S$ とする。$A-B\in S$ は明らかであるから $AB\in S$ を示せばよい。$AB=(c_{ij})$ とおくと

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$$

である。$i>j$ とする。$i>k$ ならば $a_{ik}=0$ で $k>j$ ならば $b_{kj}=0$ である。よって $i\leq k\leq j$ のときのみ $a_{ik}b_{kj}\neq 0$ となり得るが $i>j$ であるから、すべての k に対して $a_{ik}b_{kj}=0$ であり $c_{ij}=0$ となる。よって $AB\in S$ である。

この例の S が環になることを定義から直接示すのは、いろいろな条件を満たすことを確かめなければならず、なかなか大変である。しかし R の部分集合で、その演算も R の演算を用いて定義されているため、部分環であることを示しさえすれば S 自身が環であることを示すことができる。一般の場合にも、ある集合がある演算で環になることを示したいときには、それが良く知られた環の部分集合として得られていないかどうかを考えることが有効であることが多い。

例 3.3.3. 可換環 $\mathbb{Z}/6\mathbb{Z}$ とその部分集合 $S = \{\bar{0}, \bar{2}, \bar{4}\}$ を考える。このとき S は部分環になる。$\mathbb{Z}/6\mathbb{Z}$ は単位元 $\bar{1}$ をもち、S は単位元 $\bar{4}$ をもつ。このように部分環と元の環の単位元は必ずしも一致しない。

問 3.3.4. $R = M(2, \mathbb{R})$ の部分集合

$$S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

は R の部分環であることを示せ。

3.4 イデアルと剰余環

R を環とする。R の空でない部分集合 I が R の**イデアル** (ideal) であるとは、

(I1) $i, j \in I$ ならば $i - j \in I$ である。

(I2) $a \in R, i \in I$ ならば $ai \in I$ である。

(I3) $a \in R, i \in I$ ならば $ia \in I$ である。

をみたすことである。(I1), (I2) を満たす集合 I は**左イデアル** (left ideal) とよばれ、(I1), (I3) を満たす集合 I は**右イデアル** (right ideal) とよばれる。イデアルを左 (右) イデアルと区別するために**両側イデアル** (two-sided ideal) ともいう。

可換環においては、右イデアル、左イデアル、両側イデアルを区別する必要はなく、単にイデアルという。

I を環 R のイデアルであるとする。$a, b \in R$ に対して $a \equiv b \pmod{I}$ を $a - b \in I$ であることで定める。このとき、この関係は R 上の同値関係となる。$a \in R$ を含む同値類は

$$a + I = \{a + i \mid i \in I\}$$

である。同値類の全体の集合を R/I と表す。$a+I, b+I \in R/I$ に対して、加法と乗法を

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I$$

で定めれば、これらの演算は矛盾なく定義される。

乗法についてのみ定義に矛盾がないことを確認する。$a+I=a'+I, b+I=b'+I$ とする。$a'=a+i, b'=b+j$ となる $i,j\in I$ が存在する。このとき

$$a'b'-ab=(a+i)(b+j)-ab=ib+aj+ij$$

である。(I3) より $ib\in I$、(I2) より $aj\in I$、(I2) より $ij\in I$ であり、(I1) より $ab=ib+aj+ij\in I$ である。よって $a'b'+I=ab+I$ となり、乗法は定義される。

加法に関する結合法則はすぐに分かる。$0+I$ が単位元、$a+I$ の逆元は $-a+I$ となり、R/I は加法群である。

乗法に関する結合法則もすぐに分かる。また分配法則も確かめられ R/I は環となる。これを R の I による**剰余環** (factor ring) という。

- R が可換環ならば R/I も可換環である。
- R が単位元 1 をもち $I\subsetneq R$ であるならば R/I も単位元 $1+I$ をもつ。

問 3.4.1. $n\in\mathbb{N}$ に対して $n\mathbb{Z}=\{n\ell\mid\ell\in\mathbb{Z}\}$ は $\mathbb{Z}$ のイデアルであることを示せ。(このときの剰余環が $\mathbb{Z}/n\mathbb{Z}$ である。)

問 3.4.2.

$$R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\,\middle|\,a,b,c\in\mathbb{R}\right\},\quad I=\left\{\begin{pmatrix}0&b\\0&0\end{pmatrix}\,\middle|\,b\in\mathbb{R}\right\}$$

とおくと I は R のイデアルであることを示せ。

環 R において、R 自身と $\{0_R\}$ は R のイデアルである。これを R の**自明なイデアル** (trivial ideal) という。

問 3.4.3. 単位元を持つ環 R とそのイデアル I について、$I=R$ であることと $1_R\in I$ であることは同値である。これを示せ。

問 3.4.4. R を可換環とし $a\in R$ とする。$aR=\{ar\mid r\in R\}$ は R のイデアルであることを示せ。(この aR を a で生成される**単項イデアル** (principal ideal) という。)

問 3.4.5. R を可換でない環とし $a\in R$ とする。$\{r_1ar_2\mid r_1,r_2\in R\}$ は R のイデアルとは限らないことを示せ。また a を含むイデアルのうち、最小のものは何かを考えよ。

問 3.4.6. 有理整数環 $\mathbb{Z}$ の任意のイデアルは単項イデアルであることを示せ。(このように任意のイデアルが単項イデアルであるような環を**単項イデアル環**という。特に整域である単項イデアル環を**単項イデアル整域** (principal ideal domain) という。)

3.5 多項式環

R を可換環とする。R の元を係数とする文字 x の整式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \quad (a_i \in R)$$

を x に関する R 上の**多項式** (polynomial) という。$f(x)$ を単に f とも書く。x を**不定元** (indeterminate) または**変数**という。不定元 x に関する R 上の多項式全体の集合を $R[x]$ と書く。

$R[x]$ における加法と乗法を通常の場合と同じように定義する。すなわち、加法は

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_mx^m$$

に対して

$$f(x) + g(x) = \sum_{i=0}^{\ell}(a_i + b_i)x^i$$

である。ただし $\ell = \max(n, m)$ で、定義されていない係数は 0 とする。また乗法は

$$f(x)g(x) = \sum_{k=0}^{n+m} c_kx^k, \quad c_k = \sum_{i+j=k} a_ib_j$$

とする。これによって $R[x]$ は可換環となる。これを x に関する R 上の**多項式環** (polynomial ring) という。

$f(x) = a_0 + a_1x + \cdots + a_nx^n$ において $a_n \neq 0$ のとき、n を $f(x)$ の**次数** (degree) といい $\deg f(x)$ または $\deg f$ と書く。$f(x) = 0$ のときには、形式的に $\deg 0 = -\infty$ とする。非負整数 d、または $d = -\infty$ に対して $-\infty \leq d$, $-\infty + d = -\infty$ とする。

以下では R を整域とする。

命題 3.5.1. R を整域とする。$f(x),\ g(x) \in R[x]$ に対して

$$\begin{aligned} \deg(f+g) &\leq \max(\deg f,\ \deg g) \\ \deg(fg) &= \deg f + \deg g \end{aligned}$$

が成り立つ。

証明. 一つ目の式は明らかである。

$f(x) \neq 0$, $g(x) \neq 0$ とする。$f(x) = \sum_{i=0}^{m} a_ix^i$ $(a_m \neq 0)$, $g(x) = \sum_{j=0}^{n} b_jx^j$ $(b_n \neq 0)$ とすると $f(x)g(x) = \sum_{k=0}^{m+n}\sum_{i=0}^{m} a_ib_{k-i}x^k$ である。x^{m+n} の係数は a_mb_n で、$a_m \neq 0$ と $b_n \neq 0$ であることと R が整域であることから $a_mb_n \neq 0$ である。よって、このとき二つ目の式が成り立つ。

$f(x) = 0$ または $g(x) = 0$ のときは、任意の $n \in \{-\infty, 0\} \cup \mathbb{N}$ に対して $-\infty + n = -\infty$ より明らかである。 □

定理 3.5.2. 整域 R 上の一変数多項式環 $R[x]$ はまた整域である。

証明. $R[x]$ が単位元をもつ可換環であることは明らかであるから、$R[x]$ に零因子がないことを示せばよい。

$f(x), g(x) \in R[x]$, $f(x) \neq 0$, $g(x) \neq 0$ とする。このとき $\deg(f) \neq \infty$, $\deg(g) \neq -\infty$ で、命題 3.5.1 より、$\deg(fg) \neq -\infty$、すなわち $f(x)g(x) \neq 0$ である。 □

$\deg f(x) = 0$ である $f(x)$、または $f(x) = 0$ は R の元と思うことができ、これによって $R \subset R[x]$ とみなす。

問 3.5.3. 整域でない R と $\deg(fg) < \deg f + \deg g$ となるような $f(x), g(x) \in R[x]$ の例を具体的にあげよ。

定理 3.5.4. R を整域とする。$f(x),\ g(x) \in R[x]$ に対して $g(x)$ の最高次の係数が R の正則元であるならば、ある $q(x),\ r(x) \in R[x]$ が存在して

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg g$$

と一意的に表される。

証明. $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_mx^m$ とする。まず $q(x)$, $r(x)$ の存在を $n = \deg f$ に関する帰納法で示す。$g(x) \neq 0$ であるから $\deg g \geq 0$ である。$n = -\infty$、または $n < m$ のときは $q(x) = 0$, $r(x) = g(x)$ とすればよい。$n \geq m$ とする。$h(x) = f(x) - a_n{b_m}^{-1}x^{n-m}g(x)$ とおくと $\deg h < n$ で、帰納法の仮定より

$$h(x) = g(x)q_1(x) + r(x), \quad \deg r < \deg g$$

なる $q_1(x), r(x) \in R[x]$ が存在する。このとき

$$f(x) = h(x) + a_n{b_m}^{-1}x^{n-m}g(x) = g(x)(q_1(x) + a_n{b_m}^{-1}x^{n-m}) + r(x)$$

となり、これは求める式である。

次に一意性を示す。

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x), \quad \deg r, \deg r' < \deg g$$

と仮定する。このとき

$$g(x)(q(x) - q'(x)) = r'(x) - r(x)$$

である。$q(x) \neq q'(x)$ であるならば、左辺の次数は $\deg g$ 以上であり、右辺の次数は $\deg g$ 未満である。これは矛盾なので $q(x) = q'(x)$、よって $r(x) = r'(x)$ も成り立ち記述の一意性が示される。 □

この定理は特に

- R が体であるとき、
- $g(x)$ の最高次係数が 1 であるとき、

に適用できる。最高次係数が 1 である多項式を**モニック** (monic) な多項式という。

定理 3.5.4 の $q(x), r(x)$ を、それぞれ $f(x)$ を $g(x)$ で割ったときの**商、余り**という。特に $r(x) = 0$ のとき $f(x)$ は $g(x)$ で**割り切れる**といい $g(x) \mid f(x)$ と書く。

$f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ と $\alpha \in R$ に対して

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R$$

を $f(x)$ に α を**代入した値**という。$f(\alpha) = 0$ であるとき α は $f(x)$ の**根** (root) であるという。

定理 3.5.5. R を整域とし $f(x) \in R[x], \alpha \in R$ とするとき以下が成り立つ。

(1) [**剰余定理**] ある $q(x) \in R[x]$ が存在して $f(x) = (x - \alpha)q(x) + f(\alpha)$ となる。

(2) [**因数定理**] $f(\alpha) = 0$ であるための必要十分条件は $x - \alpha \mid f(x)$ となることである。

証明. $f(x)$ と $g(x) = x - \alpha$ に定理 3.5.4 を適用すれば、ある $q(x),\ r(x) \in R[x]$ が存在して

$$f(x) = (x - \alpha)q(x) + r(x), \quad \deg r < \deg(x - \alpha) = 1$$

である。よって $r(x) = r \in R$ である。この両辺に α を代入すれば $f(\alpha) = r$ である。よって剰余定理が成り立つ。

因数定理は剰余定理からすぐに分かる。 □

問 3.5.6. 体 K 上の一変数多項式環 $K[x]$ は単項イデアル整域であることを示せ。

命題 3.5.7. R を整域とし $0 \neq f(x) \in R[x], \deg f = n$ とする。このとき $f(x)$ の相異なる根は n 個以下である。

証明. n に関する帰納法で示す。$n = 0$ のときは $f(x) = r \neq 0$ で、根は 0 個である。よって命題は成り立つ。

$n \geq 1$ とする。$f(x)$ に根が存在しなければ命題は成立する。よって $f(x)$ に根が存在すると仮定してよく、α を一つの根とする。このとき

$$f(x) = (x - \alpha)g(x)$$

となる $g(x) \in R[x]$ が存在し $\deg g = n - 1$ である。帰納法の仮定より $g(x)$ の根は高々 $n - 1$ である。β を $f(x)$ の根とすれば

$$0 = f(\beta) = (\beta - \alpha)g(\beta)$$

であり、R が整域であることから $\beta - \alpha = 0$ または $g(\beta) = 0$ である。これは $f(x)$ の根が α であるか、または $g(x)$ の根であることを意味し、よって $f(x)$ の根は高々 n 個である。 □

$f(x) \in R[x]$ とする。このとき写像 $f^* : R \to R\ (\alpha \mapsto f(\alpha))$ が得られる。

命題 3.5.8. $f(x), g(x) \in R[x]$ とする。R が無限個の元を含む整域であるとき $f(x) = g(x)$ と $f^* = g^*$ は同値である。

証明. $f(x)=g(x)$ ならば $f^*=g^*$ であることは明らかである。

$f(x)\neq g(x)$ とする。$h(x)=f(x)-g(x)$ とおく。$h(x)\neq 0$ なので $h(x)$ は高々 $\deg h$ 個の根をもつ。よって R が無限個の元を含むならば $h(\alpha)\neq 0$ となる $\alpha\in R$ が存在する。よって $0\neq h(\alpha)=f^*(\alpha)-g^*(\alpha)$ であり $f^*\neq g^*$ である。 □

例 3.5.9. p を素数とし $R=\mathbb{Z}/p\mathbb{Z}$ とすれば R は整域である。このとき $f(x)=x^p-x$ とすれば任意の $\alpha\in R$ に対して $f(\alpha)=0$ であり、よって $f^*=0^*$ である。これは次のように示される。まず $f(0)=0$ である。$\alpha\neq 0$ に対しては $\alpha\in U(\mathbb{Z}/p\mathbb{Z})$ で $U(\mathbb{Z}/p\mathbb{Z})$ は位数 $p-1$ の群だから問 2.4.5 より $\alpha^{p-1}=1$ である。よって $f(\alpha)=\alpha^p-\alpha=0$ となる。

多変数の多項式環 $R[x_1,x_2,\cdots,x_n]$ は帰納的に

$$R[x_1,x_2,\cdots,x_n]=R[x_1,x_2,\cdots,x_{n-1}][x_n]$$

($R[x_1,\cdots,x_{n-1}]$ 上の変数 x_n に関する多項式環) として定義される。その元は

$$f(x_1,x_2,\cdots,x_n)=\sum a_{i_1i_2\cdots i_n}{x_1}^{i_1}{x_2}^{i_2}\cdots{x_n}^{i_n},\quad (a_{i_1i_2\cdots i_n}\in R)$$

と表される。これを $x_1,x_2,\cdots,x_n$ に関する R 上の**多項式** (polynomial) という。$a_{i_1i_2\cdots i_n}\neq 0$ のとき $a_{i_1i_2\cdots i_n}{x_1}^{i_1}{x_2}^{i_2}\cdots{x_n}^{i_n}$ を f の **項** (term) といい $i_1+i_2+\cdots+i_n$ をその**次数** (degree) という。

命題 3.5.10. R が整域のとき $R[x_1,x_2,\cdots,x_n]$ も整域である。また、その単数群は R の単数群と一致する。

証明. R が整域だから $R[x_1]$ は整域、よって $R[x_1,x_2]=R[x_1][x_2]$ も整域、これを繰り返して $R[x_1,x_2,\cdots,x_n]$ も整域である。

$U(R)=U(R[x])$ を示せば、上と同じような議論で $R[x_1,x_2,\cdots,x_n]$ の単数は R の単数と一致する。$f(x)\in R[x]$ を単数とする。ある $g(x)\in R[x]$ が存在して $f(x)g(x)=1$ である。次数を比べると $\deg f+\deg g=0$ であるから $\deg f=\deg g=0$、すなわち $f(x),g(x)\in R$ である。よって $f(x)$ は R の単数であり $U(R[x])\subset U(R)$ である。$U(R)\subset U(R[x])$ は明らかであり $U(R)=U(R[x])$ である。 □

$f(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$ に対して、写像 $f^*:R\times R\times\cdots\times R\to R$ が定義される。

命題 3.5.11. R は無限個の元を含む整域とする。$f(x_1,x_2,\cdots,x_n),g(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$ とする。このとき $f\neq g$ と $f^*\neq g^*$ は同値である。

証明. $f=g$ ならば $f^*=g^*$ は明らかである。

$f-g$ を考えれば、$f\neq 0$ のときに $f^*\neq 0^*$ であることを示せばよいことになる。これを n に関する帰納法で示す。$n=1$ のときは既に示した。f を $R[x_1,\cdots,x_{n-1}]$ を係数とする x_n の多項式と見て

$$f(x_1,\cdots,x_n)=\sum_{i=0}^{m}g_i(x_1,\cdots,x_{n-1}){x_n}^i$$

と書く。$f \neq 0$ だから、ある i について $g_i \neq 0$ である。帰納法の仮定より $g_i(\alpha_1, \cdots, \alpha_{n-1}) \neq 0$ となる $(\alpha_1, \cdots, \alpha_{n-1}) \in R \times \cdots \times R$ が存在する。このとき $0 \neq f(\alpha_1, \cdots, \alpha_{n-1}, x_n) \in R[x_n]$ であるから、ある $\alpha_n \in R$ が存在して $f(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n) \neq 0$ である。よって $f^* \neq 0$ である。 □

3.6 色々な体

K を体とする。$1 \in K$ に対して

$$1,\ 1+1,\ 1+1+1, \cdots$$

を考え、それぞれ単に $1,\ 2,\ 3, \cdots$ と書く。$0,\ -1,\ -2 = (-1) + (-1), \cdots$ も考えて

$$F = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

を考えれば F は K の部分環となる。K には零因子がないので F にも零因子はなく F は整域である。F は加群として 1 で生成される巡回群で、したがって $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N})$、または $\mathbb{Z}$ と本質的に同じものである (命題 2.3.9)。これを同一視する。$F = \mathbb{Z}/n\mathbb{Z}$ であるとき F が整域であることにより n は素数になる (定理 3.2.5)。この素数を K の**標数** (characteristic) という。$F = \mathbb{Z}$ のときには K の標数は 0 であるという。標数 p $(\neq 0)$ の体において $p = 0$ である。標数が 0 でない体を**正標数**の体ともいう。

例 3.6.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は標数 0 の体である。$\mathbb{Z}/p\mathbb{Z}$ (p は素数) は標数 p の体である。

命題 3.6.2. K を標数 p $(\neq 0)$ の体とする。$a, b \in K$ に対して

$$(a+b)^p = a^p + b^p$$

が成り立つ。

証明. 二項定理により $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ である。ここで $0 < i < p$ とすると

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

であり、分子に p が現れるが分母には p は現れない。よって、これは p の倍数であり K において 0 である。 □

問 3.6.3. $F = \mathbb{Z}/5\mathbb{Z}$ とする。$n \in \mathbb{N}$ に対して、写像 $f_n : F \to F$ を $f(a) = a^n$ で定める。$n = 2, 3, 4, 5$ について、f_n は単射 (全射) であるか、それぞれ決定せよ。

問 3.6.4. p を素数とし $F = \mathbb{Z}/p\mathbb{Z}$ とする。任意の $a \in F$ に対して $a^p = a$ であることを示せ。

例 3.6.5 (有理数体 $\mathbb{Q}$ の構成)**.** 有理整数環 $\mathbb{Z}$ から有理数体 $\mathbb{Q}$ を構成しよう。$\mathbb{Z}^* = \mathbb{Z} - \{0\}$ (非零因子全体の集合) とする。直積集合 $\mathbb{Z} \times \mathbb{Z}^*$ に関係 $\sim$ を「$at = bs$ のとき $(a, s) \sim (b, t)$」として定める。この関係は同値関係である。(a, s) を含む同値類を a/s と書くことにする。同値類全体の集合 $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$ を R と書くことにする。R に加法と乗法を

$$\begin{aligned} a/s + b/t &= (at + bs)/st \\ (a/s)(b/t) &= (ab)/(st) \end{aligned}$$

で定めれば、この演算は矛盾なく定義され、結合法則、分配法則などが成り立つ。これによって R は可換環となる。単位元は $1/1$、零元は $0/1$、a/s $(a \neq 0)$ の逆元は s/a である。これにより R は体となる。この体を**有理数体**といい $\mathbb{Q}$ と書く。

問 3.6.6. 例 3.6.5 において以下のことを確認せよ。

(1) $\sim$ が同値関係であること。

(2) 加法と乗法が矛盾なく定義されること。

(3) 加法の結合法則、乗法の結合法則、乗法の交換法則、分配法則、が成り立つこと。

例 3.6.5 の構成は $\mathbb{Z}$ でなくても、一般の整域 D に対して行うことができる。このようにして作った体を整域 D の**商体** (quotient field) という。

例 3.6.7. R を整域とすると、R 上の多項式環 $R[x]$ は整域である。$R[x]$ の商体は

$$\left\{ \frac{f(x)}{g(x)} \;\middle|\; g(x) \neq 0 \right\}$$

である。これを R 上の**有理関数体**といい $R(x)$ と書く。

R の商体を K とすると、適当な同一視によって $K(x) = R(x)$ である。

$m \in \mathbb{Z}$ が**平方数**であるとは、$m = a^2$ となる $a \in \mathbb{Z}$ が存在することである。$m \in \mathbb{Z}$ が**平方自由** (square free) であるとは、$m \neq 0, 1$ であって m を割り切る 1 以外の平方数が存在しないことである。m が平方自由であるということは、簡単に言えば $\sqrt{m}$ がより簡単な形に変形できないということである。

例 3.6.8. 3, 15, -6, -105 などは平方自由である。0, 1, -4, 9, 12 などは平方自由ではない。

m を平方自由な整数とし

$$\begin{aligned} \mathbb{Q}[\sqrt{m}] &= \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} \\ \mathbb{Q}(\sqrt{m}) &= \left\{ \frac{a + b\sqrt{m}}{c + d\sqrt{m}} \;\middle|\; a, b, c, d \in \mathbb{Q},\ c^2 + d^2 \neq 0 \right\} \end{aligned}$$

とおく。

命題 3.6.9. $\mathbb{Q}[\sqrt{m}]$ は体である。

証明. まず $R = \mathbb{Q}[\sqrt{m}] \subset \mathbb{C}$ と見て、これが部分環であることを示す。$1 \in R$ である。$\alpha, \beta \in R$ ならば $\alpha - \beta, \alpha\beta \in R$ も明らかで、よって R は可換環である。

$0 \neq a+b\sqrt{m}$ $(a, b \in \mathbb{Q})$ に対して、逆元が存在することを示せばよい。$(a+b\sqrt{m})(a-b\sqrt{m}) = a^b - b^2 m$ は m が平方自由なので 0 にはならない。$a + b\sqrt{m}$ の逆元は $\mathbb{C}$ には存在するので、それが R に含まれることをいえばよい。実際

$$\frac{1}{a+b\sqrt{m}} = \frac{a-b\sqrt{m}}{(a+b\sqrt{m})(a-b\sqrt{m})} = \frac{a}{a^2-b^2m} - \frac{b}{a^2-b^2m}\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$$

である。よって $R = \mathbb{Q}[\sqrt{m}]$ は体である。 □

問 3.6.10. $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}(\sqrt{m})$ であることを示せ。

$\mathbb{Q}[\sqrt{m}]$ を**二次体** (quadratic field) という。これは多項式環 $\mathbb{Q}[x]$ において $(x^2-m)\mathbb{Q}[x]$ というイデアルを考え、それによる剰余環 $\mathbb{Q}[x]/(x^2-m)\mathbb{Q}[x]$ を考えていることと同じである。

同様に $f(x) \in \mathbb{Q}[x]$ を既約多項式 (より小さい次数の多項式の積に分解しない多項式) とするとき、以下で説明するように剰余環 $\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$ は体となる。このような体を**代数体** (algebraic number field) という。

R を整域とする。$f(x) \in R[x]$ が**既約** (irreducible) であるとは、ある $g(x), h(x) \in R[x]$ に対して $f(x) = g(x)h(x)$ であるならば $g(x)$ または $h(x)$ が $R[x]$ の単数 (よって R の単数) となることとする。既約でないときは**可約** (reducible) という。

K を体とする。このとき $f(x) \in K[x]$ は (K の単数による差を除いて) 既約多項式の積に一意的に分解される (証明は省略する)。$f(x), g(x) \in K[x]$ が共通の既約因子をもたないとき、$f(x)$ と $g(x)$ は**互いに素**であるという。

次の定理は証明を省略するが、有理整数環の場合と同じようにユークリッドの互除法を用いて示される。

定理 3.6.11. K を体とする。$f(x)$ と $g(x)$ が互いに素であるならば、

$$f(x)h(x) + g(x)\ell(x) = 1$$

となる $h(x), \ell(x) \in K[x]$ が存在する。

次の定理が示したいことである。

定理 3.6.12. K を体とし $f(x) \in K[x]$ を既約多項式とする。このとき剰余環 $K[x]/f(x)K[x]$ は体である。($K = \mathbb{Q}$, $\deg f(x) = n$ のとき、このような体を n **次体**という。)

証明. $0 \neq \overline{g(x)} \in K[x]/f(x)K[x]$ とし、$\overline{g(x)}$ が単数であることを示せばよい。$\overline{g(x)} \neq 0$ であるから $g(x)$ は $f(x)$ で割り切れず、また $f(x)$ は既約なので、$f(x)$ と $g(x)$ は互いに素である。定理 3.6.11 より

$$f(x)h(x) + g(x)\ell(x) = 1$$

となる $h(x), \ell(x) \in K[x]$ が存在する。このとき、この式を $K[x]/f(x)K[x]$ で考えれば

$$\overline{g(x)}\ \overline{\ell(x)} = 1$$

となり $\overline{g(x)}$ は $K[x]/f(x)K[x]$ で可逆である。 □

この定理によって $\mathbb{Q}$ 上 n 次の既約多項式が存在すれば、それに対して n 次体が得られる。一般に既約多項式を見付けることは容易ではない。以下では、よく知られた多項式の既約判定定理を説明する。

$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ が**原始多項式**であるとは、すべての係数の最大公約数が 1 であることとする。任意の $f(x) \in \mathbb{Z}[x]$ は、ある非負整数 a と原始多項式 $g(x)$ を用いて $f(x) = ag(x)$ と表すことが出来る。

補題 3.6.13. $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ を $\mathbb{Z}[x]$ の原始多項式とする。このとき $f(x)g(x)$ も原始多項式である。

証明. p を素数とする。$f(x)$ と $g(x)$ は原始多項式なので

$$p \mid a_0,\ \ p \mid a_1,\ \ \cdots,\ \ p \mid a_{i-1},\ \ p \nmid a_i,$$
$$p \mid b_0,\ \ p \mid b_1,\ \ \cdots,\ \ p \mid b_{j-1},\ \ p \nmid b_j$$

なる i, j が存在する。このとき $f(x)g(x)$ の x^{i+j} の係数は

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} \cdots + a_{i+j} b_0$$

となり p で割り切れない。したがって $f(x)g(x)$ のすべての係数を割り切る素数はなく、$f(x)g(x)$ は原始多項式である。 □

補題 3.6.14. $f(x) \in \mathbb{Z}[x]$ が $\mathbb{Z}[x]$ で既約であるならば $\mathbb{Q}[x]$ で既約である。

証明. $f(x) \neq 0$ としてよい。$f(x)$ は $\mathbb{Z}[x]$ で既約であるとし、$\mathbb{Q}[x]$ で既約でないとする。$f(x) = g^*(x)h^*(x)$, $\deg g^*(x) \geq 1$, $\deg h^*(x) \geq 1$ である $g^*(x), h^*(x) \in \mathbb{Q}[x]$ が存在する。$\mathbb{Q}$ 上の多項式は、ある有理整数を掛けることによって $\mathbb{Z}$ 上の多項式にすることができるので

$$af(x) = g(x)h(x)$$

なる $a \in \mathbb{Z}$ と $g(x), h(x) \in \mathbb{Z}[x]$ が得られる。このような a として正のものをとることが出来るので、正のもののうち最小のものを a としてとる。$a = 1$ ならば $f(x)$ は可約であり仮定に反する。

$$g(x) = \alpha g_0(x),\ h(x) = \beta h_0(x),\ \alpha, \beta \in \mathbb{Z}$$

で $g_0(x)$ と $h_0(x)$ は原始多項式とする。$a \neq 1$ なので、$p \mid a$ となる素数 p が存在する。p は $af(x) = g(x)h(x) = \alpha\beta g_0(x)h_0(x)$ のすべての係数を割り切る。ここで $g_0(x)h_0(x)$ は原始多項式なので $p \mid \alpha\beta$ である。p は素数なので $p \mid \alpha$ または $p \mid \beta$ である。このとき、例えば $p \mid \alpha$ とすると

$$\frac{a}{p} f(x) = \left(\frac{\alpha}{p} g_0(x)\right)(\beta h_0(x))$$

は $\mathbb{Z}[x]$ における分解で、したがって a の最小性に反する。 □

定理 3.6.15 (アイゼンスタイン (Eisenstein) の既約性判定定理)**.** p を素数とする。$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ について

$$p \mid a_{n-1},\ p \mid a_{n-2},\ \cdots,\ p \mid a_1,\ p \mid a_0,\ p^2 \nmid a_0$$

であるとする。このとき $f(x)$ は $\mathbb{Q}[x]$ で既約である。

証明. $f(x)$ が $\mathbb{Z}[x]$ で既約であることを示せばよい。$f(x) = g(x)h(x)$, $g(x) = \sum_{i=0}^{m} b_ix^i \in \mathbb{Z}[x]$, $h(x) = \sum_{j=0}^{\ell} c_jx^j \in \mathbb{Z}[x]$ とする。$a_0 = b_0c_0$ なので p は b_0 または c_0 の一方のみを割り切る。$p \mid b_0$, $p \nmid c_0$ とする。

$$p \mid b_0,\ p \mid b_1,\ \cdots,\ p \mid b_{i-1},\ p \nmid b_i$$

なる i が存在する。$0 \lneq i \leq m < n$ である。$f(x)$ の x^i の係数は

$$b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0$$

で、これは p で割り切れず、仮定に矛盾する。 □

次はこの定理から直ちに分かる。

系 3.6.16. p を素数とし $n \geq 1$ とする。このとき $x^n - p$ は既約である。よって、任意の $n \geq 1$ に対して n 次代数体は存在する。

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

[3] 代数概論, 森田康夫, 裳華房