代数位相

酒匂貴市

平成 27 年 4 月 4 日

目 次

第 I 部
代数

1　基本的事項

1.1　写像

定義 1.1　（単射）集合 A から集合 B への写像 T について、$T(a) = T(a')\ (\in B)$ ならば $a = a'\ (a, a' \in A)$ が成り立つとき、T を**単射**という。◂

定義 1.2　（像・全射）集合 A から集合 B への写像 T について、A の元の T によって写像されたものの全体 $\mathbf{T(A)} = \{\mathbf{T(a)}|\mathbf{a} \in \mathbf{A}\}$ を、***A* の *T* による像 (像集合)*** という。また、一般には $T(A) \subset B$ だが、$\underline{T(A) = B}$ が成り立つとき、T を A から B の**全射**という。◂

定義 1.3　（全単射）集合 A から集合 B への写像 T が、単射かつ全射であるとき、T を**全単射**という。◂

定義 1.4　（逆写像）集合 A から集合 B への写像 T があるとき、E_A, E_B をそれぞれ集合 A, B における恒等写像として、写像 $T^{-1} : B \to A$ が $T^{-1} \circ T = E_A,\ T \circ T^{-1} = E_B$ を満たすならば、T^{-1} を**逆写像**という。◂

全射によって二つの集合を写像を通じて結びつけて理解することが可能となる。さらに単射であれば、写像を通じて二つの集合が一対一に対応させられる。このことは、逆写像の存在という形で明確にあらわれる。

定理 1.1　集合 A から集合 B への写像 T が、全単射であるとき、任意の $b \in B$ に対して $T(a) = b$ となる A の元 a がただひとつ存在し、T は逆写像 T^{-1} を持つ。

(proof)
全射の定義により、$T(A) = B$ なので、任意の $b \in B$ に対して $b \in T(A) = B$ となる。従って、$T(a) = b$ となる A の元 a が必ず存在する。ここで、$T(a) = b$ となる A の元 a が複数存在したとする。すなわち、$T(a) = T(a') = b \quad (a \neq a')$ となったとすると、これは T が単射であることに矛盾する。従って、$T(a) = b$ となる A の元 a はただひとつだけである。

このとき、$T^{-1} : b \mapsto a$ とおくと T^{-1} は写像となるが、E_A, E_B をそれぞれ A, B における恒等写像とすると、上の議論より任意の $b \in B$ に対して $T(a) = b$ となる $a \in A$ が唯一必ず存在して $a = T^{-1}(b)$ と表されるので

$$T \circ T^{-1}(b) = T(a) = b$$

であり、したがって $T \circ T^{-1} = E_B$ である。また、任意の $a \in A$ に対して $T(a) \in B$ であり、上の議論より $T(a') = T(a)$ となる $a' \in A$ が唯一存在して $a' = T^{-1}(T(a))$ と表される。ところが、単射であることより $T(a') = T(a)$ ならば $a' = a$ であり、従って

$$a = T^{-1}(T(a))$$

が任意の $a \in A$ について成立する、つまり $T^{-1} \circ T = E_A$ である。よって、T^{-1} は T の逆写像である。 証明終

定理 1.2　集合 A から集合 B への写像 T が、逆写像 T^{-1} を持つとき、T, T^{-1} は全単射である。

(proof)
$T(a) = T(a')$ であるとき、$a = T^{-1}(T(a)) = T^{-1}(T(a')) = a'$ であり、T は単射である。また、像を考えると一般には $T^{-1}(B) \subset A$ であり、従って

$$T \circ T^{-1}(B) \subset T(A) \subset B$$

である。ところが $T \circ T^{-1} = E_B$ なので、$T \circ T^{-1}(B) = B$ であり、従って

$$T \circ T^{-1}(B) = T(A) = B$$

である。よって、$T(A) = B$ より T は全射であり、あわせて、T は全単射である。T^{-1} についても同様である。 証明終

1.2 同値関係と同値類

定義 1.5 （**二項関係**）集合 S について、その積集合 $S \times S$ の部分集合 R を**二項関係**という。逆に $(x, y) \in R$ のとき、x と y は関係 R で結ばれているとか R 関係があるという。◂

定義 1.6 （**同値関係**）X を集合とし、R を X 上の二項関係とする。二項関係 R が次の *3* 条件を満たすとき、R を X 上の**同値関係**という。

1. 任意の $a \in X$ に対して $(a, a) \in R$ （反射律）
2. 任意の $a, b \in X$ に対して $(a, b) \in R$ ならば $(b, a) \in R$ （対称律）
3. 任意の $a, b, c \in X$ に対して $(a, b) \in R$ かつ $(b, c) \in R$ ならば $(a, c) \in R$ （推移律）

同値関係 $(a, b) \in R$ のことを $a \sim b$ のようにも表す。◂

定義 1.7 （**同値類**）集合 A の空でない部分集合の族 $\mathfrak{F} = \{A_i | i \in I\}$ が次の *2* 条件を満たすとき、$\mathfrak{F}$ を A の**類別**または**分割**という。

1. $A = \cup_{i \in I} A_i$
2. $i, j \in I, i \neq j$ なら $A_i \cap A_j = \emptyset$

このとき、各 A_i を類別 $\mathfrak{F}$ による**類**という。特に集合 X 上に同値関係 R が定義されているとき、ある X の元 a に対して a に同値である元を全て集めた集合は類となる。これを同値関係 R の**同値類**といい、a ををこの同値類の**代表元**という。◂

定義 1.8 （**商集合**）$\sim$ を X 上の同値関係とするとき、$\sim$ の同値類全体からなる集合を、X の $\sim$ による**商集合**といい、$X/\sim$ とかく。すなわち、$S/\sim = \{[a] | a \in S\}$。◂

同値関係は、「ある観点から等しい」ことを表すものと捉えられる。その観点から同一視したものが同値類であり、同値類を構成要素として集合を解釈しなおしたものが商集合であるといえよう。

例 1.9 $\boldsymbol{N}$ を *0* と自然数の全体とし、$\boldsymbol{N} \ni m (\neq 0)$ を固定するとき、$a \sim b \Leftrightarrow a \equiv b \pmod{m}$ と定義すると $\boldsymbol{N}$ を m 割った余りによって同値類に類別できる。これは、余りが等しいものを同一視したことに相当する。

1.3 半順序・順序

定義 1.10 （**擬順序**）X を集合とし、R を X 上の二項関係とする。二項関係 R が次の条件を満たすとき、R を X 上の**擬順序**という。

1. 任意の $a \in X$ に対して $(a, a) \in R$ （反射律）
2. 任意の $a, b, c \in X$ に対して $(a, b) \in R$ かつ $(b, c) \in R$ ならば $(a, c) \in R$ （推移律）

擬順序 $(a, b) \in R$ のことを $a \prec b$ などのようにも表す。◂

定義 1.11（半順序）X を集合とし、R を X 上の二項関係とする。二項関係 R が次の条件を満たすとき、R を X 上の**半順序**という。

1. 任意の $a \in X$ に対して $(a,a) \in R$ （反射律）
2. 任意の $a,b \in X$ に対して $(a,b) \in R$ かつ $(b,a) \in R$ ならば $a = b$ （反対称律）
3. 任意の $a,b,c \in X$ に対して $(a,b) \in R$ かつ $(b,c) \in R$ ならば $(a,c) \in R$ （推移律）

半順序 $(a,b) \in R$ のことを $a \leq b$ などのようにも表す。このとき $(X, \leq)$ を**半順序集合**という。さらに、任意の $a,b \in X$ について $a \leq b$ または $b \leq a$ が成立するときは、二項関係 $\leq$ は**全順序**であるといい、$(X, \leq)$ を**全順序集合**という。◂

定義 1.12（順序同型）$(X, \leq), (Y \leq)$ を半順序集合とする。写像 $f : X \to Y$ が全単射であり

$$x \leq y \Leftrightarrow f(x) \leq f(y)$$

が成立する場合、f を**順序同型写像**という。順序同型写像が存在する場合、X と Y は順序同型であるという。順序同型を集合同士の二項関係として捉えた場合、順序同型は同値関係である。◂

定義 1.13（最大元・最小元）$(X, \leq)$ を半順序集合とし、A を X の部分集合とする。$a \in A$ が $\forall x \in A, x \leq a$ を満たすとき、a を A の最大元といい、$\max A$ と表す。また、$a \in A$ が $\forall x \in A, a \leq x$ を満たすとき、a を A の最小元といい、$\min A$ と表す。最大元もしくは最小元は存在するとは限らないが、反対称律より存在すれば一意である。◂

定義 1.14（極大元・極小元）$(X, \leq)$ を半順序集合とし、A を X の部分集合とする。$a \in A$ が $\forall x \in A$ について「$a \leq x \Rightarrow x = a$」を満たすとき、$a$ を A の極大元という。また、$\forall x \in A$ について「$x \leq a \Rightarrow x = a$」を満たすとき、$a$ を A の極小元という。極大元もしくは極小元は存在するとは限らず、たくさん存在することもある。◂

定義 1.15（強連結成分分解）X を集合とし、$\prec$ を X 上の擬順序とする。二項関係 $a \sim b$ を

$$a \sim b \Leftrightarrow a \prec b \text{ かつ } b \prec a$$

によって定義すると、$\sim$ は同値関係となる。このとき $\sim$ による商集合 $X/\sim$ を**強連結成分分解**といい、同値類を**強連結成分**という。◂

$a \prec b$ のとき、それぞれを代表元とする強連結成分 $[a], [b]$ とその任意の元 $x \in [a], y \in [b]$ について

$$x \prec a, a \prec b, b \prec y \ \therefore x \prec y$$

が成立しており、強連結成分に対して $[a] \leq [b] \Leftrightarrow a \prec b$ によって二項関係 $\leq$ を定義できる。$\leq$ は明らかに擬順序であり、さらに $[a] \leq [b]$ かつ $[b] \leq [a]$ ならば $a \sim b$ つまり $[a] = [b]$ であり、反対称律を満たすことから $\leq$ は半順序である。

2 代数系

2.1 代数系

数学的な演算（算法）の枠組みとして、代数系を定義する。

定義 2.1（代数系）X を集合とする。$A(\subset X \times X)$ から X への写像 f を上の**二項算法**または、**内算法**という。$A = X \times X$ ならば、内算法は**全域で定義されている**という。また、Ω を適当な別の集合として、$\Omega \times X$ から X への写像を Ω を**作用域**とする**外算法**といい、内算法と外算法をあわせて**算法**という。X の元 x, y について、$f(x,y)$ を $x + y$ と書くとき、この算法を**加法**といい、xy と書くとき**乗法**という。また、何種類かの算法を備えた集合を**代数系**といい、例えば集合 X に算法 $\circ$ が定義されているとき、$(X, \circ)$ と書く。◂

代数系における同値類を考える場合には、算法を同値類に対するものとして再解釈できることが重要である。このことは、次のようにまとめられる。

定義 2.2 （**商構造**）E を集合、$\circ, \sim$ をそれぞれ E 上で定義された内算法と同値関係とするとき、任意の E の元 a, b, c に対し

$$c = a \circ b, a' \in [a], b' \in [b] \Longrightarrow a' \circ b' \in [c] \tag{1}$$

が成り立つ時、内算法 $\circ$ と同値関係 $\sim$ が**両立する**という。また、E の外算法 $\diamond$ について

$$a \sim b \Longrightarrow \alpha \diamond a \sim \alpha \diamond b \tag{2}$$

が成り立つとき、外算法 $\diamond$ と同値関係 $\sim$ が**両立する**という。$E(\circ, \sim), E(\diamond, \sim)$ においてそれぞれ $\circ, \diamond$ と $\sim$ が両立するとき、$(E/\sim, \bullet), (E/\sim, \blacklozenge)$ という新たな代数系を

$$[a] \bullet [b] = [a \circ b] \tag{3}$$

$$\alpha \blacklozenge [a] = [\alpha \diamond a] \tag{4}$$

となるように定義することができる。このような代数系を**商構造** [1] という。◂

2.2 準同型・同型

定義 2.3 （**準同系·同型**）*2* つの代数系 $(E, \circ_1, \cdots, \circ_m, \diamond_1, \cdots, \diamond_n), (E', \circ'_1, \cdots, \circ'_m, \diamond'_1, \cdots, \diamond'_n)$ について、$\circ_1, \cdots, \circ_m, \circ'_1, \cdots, \circ'_m$ は内算法、$\diamond_1, \cdots, \diamond_n, \diamond'_1, \cdots, \diamond'_n$ は $\diamond_i, \diamond'_i$ の作用域 Ω_i が等しい外算法とする。このとき、ある E_1 から E_2 の写像 f が存在して、任意の E_1 の元 a, b と $\alpha_j \in \Omega_j$ について

$$f(a \circ_i b) = f(a) \circ'_i f(b) \qquad i = 1, \cdots, m \tag{5}$$

$$f(\alpha_j \diamond_j b) = \alpha_j \diamond'_j f(b) \qquad j = 1, \cdots, n \tag{6}$$

が成り立つ時 f は**準同型写像**であるという。特に全単射である準同型写像を**同型写像**という。また、同型写像を持つとき、*2* つの代数系は**同型**であるといい、$(E_1, \circ_1) \simeq (E_2, \circ_2)$ と書く。◂

2.2.1 同型

定理 2.1 二つの代数系 E, E' が同型であるという関係を $E \cong E'$ で表せば、$\cong$ は同値関係である。

(proof)

(反射律) 恒等写像は同型写像であり、これを以て $E \cong E$ である。

(対称律)$E \cong E'$ であるとき、E から E' の間に同型写像 f が存在する。f は全単射なので、定理 1.1 より、E' から E への逆写像 f^{-1} が存在する。f^{-1} は逆写像 $(f^{-1})^{-1} = f$ を持つので全単射である。また、$f^{-1}(a') = a, f^{-1}(b') = b$ であるとき $f(a) = a', f(b) = b'$ なので、f が準同型であることにより、任意の内算法 $\circ$ について $a' \circ b' = f(a) \circ f(b) = f(a \circ b)$ つまり

$$f^{-1}(a \circ b) = a' \circ b' = f^{-1}(a) \circ f^{-1}(b)$$

[1] この定義では、一般には $\{x \circ y; x \in [a],\ y \in [b]\} \subset [a] \bullet [b]$ であり、$\{k \diamond x; x \in [a]\} \subset k \blacklozenge [a]$ であることに注意せよ。ここでいう両立は、算法が写像になっていることを保証しているだけである。これらの集合が一致するためには、両立の定義において、必要条件が必要十分条件になっていなければならない。

であり、また、任意の外算法 $\diamond$ について、k を作用域の元として $k \diamond a' = k \diamond f(a) = f(k \diamond b)$ つまり

$$f^{-1}(k \diamond a) = k \diamond a' = k \diamond f^{-1}(a)$$

であるので、f^{-1} は準同型写像である。まとめると、T^{-1} は E' から E への同型写像ということになり、$E' \cong E$ となる。

(推移律)$E \cong E', E' \cong E''$ であるとき、それぞれの間に同型写像 f, g が存在する。この時、任意の $x \in E$ に対して $g(f(x)) \equiv (g \circ f)(x)$ は E'' の元を与えており、$(g \circ f)$ は E から E'' への写像である。しかも写像 $(g \circ f)$ は、簡単な考察により、全単射で準同型であることがわかる。つまり E から E'' に同型写像 $(g \circ f)$ が存在するということであり、$E \cong E''$ である。 証明終

二つの代数系 E, E' が**同型**であることは、その代数系で定義されている算法の上では、**二つの代数系を同一視していい**ということを表している。まず、同型写像は全単射であるため、E, E' は同型写像を通じて一対一に対応させられる。さらに、同型写像は準同型であるため、算法の適用結果が同型写像を通じて一致する。例えば、内算法について考えると、E の元 a, b に内算法 $\circ$ を適用した結果（$a \circ b$）と、E' の対応する元 $a' \equiv f(a), b' \equiv f(b)$ に、対応する E' の内算法 $\circ'$ を適用した結果（$a' \circ' b'$）が、f を通して一致する

$$f(a \circ b) = a' \circ' b'$$

のであるから、f で移りあえるものを同一視すれば、E で $a \circ b$ を考えることと、E' で $a' \circ' b$ を考えることは同じこととみなせる。

(代数系 E)		(代数系 E')
a, b	$\leftrightarrow_{f, f^{-1}}$	a', b'
$\downarrow$		$\downarrow$
$a \circ b$	$\leftrightarrow_{f, f^{-1}}$	$a' \circ b'$

外算法についても同様である。

2.2.2 準同型

定義 2.4 f を E から F への準同型写像とするとき、$a \sim b \Leftrightarrow f(a) = f(b)$ とすると

1. $f(a) = f(a)$
2. $f(a) = f(b) \Leftrightarrow f(b) = f(a)$
3. $f(a) = f(b), f(b) = f(c) \Rightarrow f(a) = f(c)$

なので同値関係を定めることができるため、代数系 E/f を定義することができる[2]。◂

これはつまり、準同型写像 f を適用すると等しくなるものを同一視することにあたる。像 $f(E)$ の元一つに対して同値類がひとつ対応しており、明らかに次のことが言える。

定理 2.2 （準同型定理）E を全ての算法が全域で定義された代数系とするとき、準同型写像 $f : E \to F$ によって生成される同値関係 $\sim$ による商集合 E/f は、像 $f(E)$ と同型である。

定理 2.3 準同型写像 $f : E \to F$ によって生成される同値関係 $\sim$ による商集合 E/f について、E の算法は全て同値関係 $\sim$ と両立しており、商集合 E/f 上に商構造を定義できる。

[2]たとえば剰余について、$a \to [a]$ を準同型写像 f とみなすことができるので、$(E/\sim, \bullet)$ を E/f と書くことができる。

3　内算法と可逆化

3.1　内算法についての定義

定義 3.1（結合的）集合 X に内算法 $\circ$ が定義されているものとする。このとき

$$\forall a,b,c \in X : (a \circ b) \circ c = a \circ (b \circ c) \tag{7}$$

が成り立つことを、内算法 $\circ$ は**結合的**であるという。◂

以下、結合的な内算法を考える。結合的であることにより、内算法については計算順序を考えなくてよい（括弧をつけなくてよい）。

定義 3.2（半群）集合 X に内算法 $\circ$ が全域で定義されており、内算法 $\circ$ が結合的であるとき、代数系 $(X,\circ)$ は**半群**であるという。◂

定義 3.3（単位元）集合 X に内算法 $\circ$ が定義されているものとする。このとき、ある特別な元 e が存在して、

$$\forall x \in X : x \circ e = e \circ x = x \tag{8}$$

となるとき、e を**単位元**という。◂

定理 3.1 単位元が存在するならば、それは一意である。

(proof)
e, e' がともに単位元であると仮定する。すると仮定より $e = e \circ e' = e'$。 証明終

定義 3.4（逆元）集合 X に内算法 $\circ$ が定義されており、単位元 e が存在するとする。X の各元 x に対し

$$x \circ y = y \circ x = e \tag{9}$$

となる X の元 y を x の**逆元**といい、x^{-1} で表す。◂

定理 3.2 x に対応する逆元が存在するならば、それは一意である。

(proof)
a, b がともに x の逆元だと仮定すると $a = a \circ e = a \circ x \circ b = e \circ b = b$ である。 証明終

定義 3.5（可換）集合 X に内算法 $\circ$ が定義されているものとする。このとき X の任意の元 x,y について

$$x \circ y = y \circ x$$

が成立するとき、$\circ$ は可換であるという。◂

定義 3.6（正則元）集合 X に結合的で可換な内算法 $\circ$ が定義されており、$a \circ x = a \circ y$ ならば $x = y$ が成立するとき（写像 $f_a(x) = a \circ x$ が単射であるとき）、a を**正則元**という。◂

例 3.7 自然数と加算を考えた場合、自然数すべてが正則元である。整数と乗算を考えた場合、0 以外の整数が正則元である。

a, b が正則元であるとき $a \circ b$ も正則元であることに留意する。

3.2 可逆化の手続き

3.2.1 商構造の構成

内算法が可換な半群 $(X, \circ)$ に対し、X の正則元の全体を X^* とし、積集合 $X \times X^*$ を考える。また、積集合 $X \times X^*$ における内算法 $\bullet'$ を次のように定義する。

$$(x, x^*) \bullet' (y, y^*) \equiv (x \circ y, x^* \circ y^*)$$

補題 3.3 積集合 $X \times X^*$ 上の関係 $\sim$ を

$$(x, x^*) \sim (y, y^*) \Leftrightarrow x \circ y^* = y \circ x^*$$

と定義すると、$\sim$ は同値関係である。

(proof)
反射律・対象律は自明である。推移律については、可換性を使って

$$\begin{aligned} y^* \circ (x \circ z^*) &= (y^* \circ x) \circ z^* \\ &= (x^* \circ y) \circ z^* \\ &= x^* \circ (y \circ z^*) \\ &= x^* \circ (y^* \circ z) \\ &= y^* \circ (z \circ x^*) \end{aligned}$$

であり、y^* は正則元であるので

$$x \circ z^* = z \circ x^*$$

が成立する。よって示された。 証明終

補題 3.4 積集合 $X \times X^*$ 上の次の同値関係 $\sim$

$$(x, x^*) \sim (y, y^*) \Leftrightarrow x \circ y^* = y \circ x^*$$

は、内算法 $\bullet'$ と両立する。

(proof)
$c \equiv (x, x^*) \bullet' (y, y^*) = (x \circ y, x^* \circ y^*)$ とするとき、任意の $(a, a^*) \in [(x, x^*)], (b, b^*) \in [(y, y^*)]$ に対して

$$(a, a^*) \bullet' (b, b^*) \in [c]$$

となることを示せばよい。

$$\begin{aligned} a \circ x^* &= x \circ a^* \\ b \circ y^* &= y \circ b^* \end{aligned}$$

より

$$\begin{aligned} (a \circ x^*) \circ (b \circ y^*) &= (x \circ a^*) \circ (y \circ b^*) \\ (a \circ b) \circ (x^* \circ y^*) &= (x \circ y) \circ (a^* \circ b^*) \end{aligned}$$

が成立する。つまり

$$(a, a^*) \bullet' (b, b^*) = (a \circ b, a^* \circ b^*) \sim (x \circ y, x^* \circ y^*) = c$$

である。よって示された。 証明終

積集合 $X \times X^*$ 上で $\sim$ による同値類を考え、商集合を $C \equiv (X \times X^*)/\sim$ とおくと、上の補題より C 上の商構造を定義できる。つまり、このときの C における内算法を $\bullet$ によって表すと $[a], [b] \in C$ について

$$[a] \bullet [b] = [a \bullet' b] \tag{10}$$

となるよう同値類に対する内算法を定めることができる。この内算法もやはり可換かつ結合的である。したがって、得られる商構造も半群を成す。

3.2.2 もとの半群との対応

積集合 $X \times X^*$ のうち $x \in X, x^* \in X^*$ によって $(x \circ x^*, x^*)$ の形で表されるものを考える。$F(x) = \{(x \circ x^*, x^*) : x^* \in X^*\}$ とする。$y \in X, y^* \in X^*$ について

$$\begin{aligned}
&(y, y^*) \in [(x \circ x^*, x^*)] \\
\Leftrightarrow\ &(x \circ x^*, x^*) \sim (y, y^*) \\
\Leftrightarrow\ &(x \circ x^*) \circ y^* = y \circ x^* \\
\Leftrightarrow\ &x^* \circ (x \circ y^*) = x^* \circ y \\
\Leftrightarrow\ &x \circ y^* = y \\
\Leftrightarrow\ &(y, y^*) \in F(x)
\end{aligned}$$

なので、$F(x) = [(x \circ x^*, x^*)] \in C$ つまり、$F(x)$ は商構造 C の元である。また、任意の $x, y \in X$ に対して

$$F(x) \bullet F(y) = [(x \circ x^*, x^*) \bullet' (y \circ y^*, y^*)] = [((x \circ y) \circ (x^* \circ y^*), x^* \circ y^*)] = F(x \circ y)$$

なので、$F : X \to C$ は準同型写像であり、また単射であることも容易に分かる。よって、X と像 $F(X)(\subset C)$ は同型である。このことは、C はその一部として X と同一視できる部分をもっており、C が X の拡張として捉えられることを意味している。

3.2.3 単位元

補題 3.5 任意の $x \in X, x^* \in X^*, u \in X^*$ に対して

$$(x, x^*) \sim (u, u) \ \Leftrightarrow\ x = x^*$$

(proof)
u が正則元であることより容易に示される。 証明終

これより $\{(u, u) : u \in X^*\}$ が C の元（同値類）であることが分かる。実は、これは C における単位元である。

補題 3.6 任意の $x \in X, x^* \in X^*, u \in X^*$ に対して

$$(x, x^*) \bullet' (u, u) \sim (u, u) \bullet' (x, x^*) \sim (x, x^*)$$

(proof)
可換性より容易に示される。 証明終

系 3.7 任意の $a \in C$ と $e \equiv \{(u,u) : u \in X^*\}$ について

$$a \bullet e = e \bullet a = a$$

つまり e は C の単位元である。

系 3.8 もとの半群 $(X, \circ)$ が単位元 e を持つ場合、対応する商構造の元 $F(e)$ は商構造の単位元である。

3.2.4 逆元の構成

C の部分集合 $R \equiv \{c \in C : \exists (x, x^*) \in c, x \in X^*, x^* \in X^*\}$ を考える。$a \in R$ ならば、ある $x, x^* \in X^*$ が存在して $a = [(x, x^*)]$ と表される。このとき、$[(x^*, x)] \in R$ が a の逆元となる。

$$\begin{aligned} a \bullet [(x^*, x)] &= [(x, x^*)] \bullet [(x^*, x)] \\ &= [(x, x^*) \bullet' (x^*, x)] \\ &= [(x \circ x^*, x^* \circ x)] \\ &= [(x \circ x^*, x \circ x^*)] \\ &= e \end{aligned}$$

$[(x^*, x)] \bullet a$ についても可換性より示される。

もとの半群の正則元 $x \in X^*$ に対して $F(x) = \{(x, x^*) : x^* \in X\} \in R$ である。これは重要な意味を持ち、半群 $(X, \circ)$ を $(C, \bullet)$ に拡大したとき、もとの半群の正則元に相当する C の要素は逆元を必ず持つ。そのため、この拡大の操作は**可逆化**と呼ばれるのである。また、次のことも言える。

系 3.9 もとの半群のすべての要素が正則元であれば、可逆化後のすべての要素が逆元を持つ。

3.2.5 整数・有理数の例

例 3.8 X を自然数の集合とし、内算法は加算を考える。このとき、同値関係は $x+y^* = x^*+y \Leftrightarrow x-x^* = y-y^*$ であり、(x, x^*) で $x-x^*$ が同じであるものを同一視していることに相当する。ただし、定義は加算のみで行われていることに注意せよ。自然数 n に対して、拡張された商構造で n に対応するのは同値類 $\{(n+x^*, x^*) : x^*$ は自然数 $\}$ である。単位元に対応するのは同値類 $\{(x^*, x^*) : x^*$ は自然数 $\}$ であり、まさにこれが 0（ゼロ）なのである。自然数はすべて正則元であり、かならず逆元 $\{(x^*, n+x^*) : x^*$ は自然数 $\}$ をもつ。$\{(n+x^*, x^*) : x^*$ は自然数 $\}$ を n と表し、$\{(x^*, x^*) : x^*$ は自然数 $\}$ を 0 と表し、$\{(x^*, n+x^*) : x^*$ は自然数 $\}$ を $-n$ と表すことで、可逆化により自然数から整数が生み出される。また、逆元を用いて $n-m = n+(-m)$ と定義することで、減算を定義することができる。

例 3.9 X を整数の集合とし、内算法は乗算を考える。このとき、同値関係は $xy^* = x^*y \Leftrightarrow \frac{x}{x^*} = \frac{y}{y^*}$ であり、分数で約分したものが同じであるものを同一視していることに相当する。つまり、この場合の可逆化は分数を考えていることに他ならない。整数において正則元は 0 以外の整数であり、分母が 0 になることは認められていない。また、分子が 0 でない場合には逆元（ここでは逆数）が存在する。こうして、整数から可逆化により有理数が生み出される。

4 束

4.1 定義

定義 4.1 （束）代数系 $(X, \wedge, \vee)$ について、$\wedge, \vee$ が全域で定義された結合的で可換な内算法であり、**吸収則**と呼ばれる次の性質

$$(x \vee y) \wedge x = x,\ (x \wedge y) \vee x = x$$

を満たすとき、代数系 $(X, \wedge, \vee)$ は**束**であるという。束の部分集合が内算法について閉じており束をなしている場合、その部分集合は部分束という。◂

束に対しては、半順序が定義できる。

定理 4.1 束 $(X, \wedge, \vee)$ について、$a \leq b \Leftrightarrow b = a \vee b$ と定義すると、$\leq$ は半順序である。

(proof)
吸収則より $a = (a \wedge c) \vee a$ であり $c = a \vee b$ とすると $a = (a \wedge (a \vee b)) \vee a = (a) \vee a \Leftrightarrow a \leq a$ である。（反射律）
$a \leq b, b \leq a$ のとき $a = a \vee b = b$ である。（反対称律）
$a \leq b, b \leq c$ のとき $c = b \vee c = (b \vee a) \vee c = (b \vee c) \vee a = c \vee a$ より $a \leq c$ である。（推移律） 証明終

定義 4.2 （束から導かれる半順序）束 $(X, \wedge, \vee)$ について、$a \leq b \Leftrightarrow b = a \vee b$ による半順序 $\leq$ を束から導かれる半順序という。束においては、以下この半順序のみを考えることとする。◂

定理 4.2 $a \leq b \Leftrightarrow a = a \wedge b$

(proof)
$a \leq b$ のとき $b = a \vee b$ である。このとき吸収則より $a \wedge b = a \wedge (a \vee b) = a$ である。逆に、$a = a \wedge b$ のとき、吸収則より $a \vee b = (a \wedge b) \vee b = b \Leftrightarrow a \leq b$ である。 証明終

定理 4.3 $a = a \wedge a = a \vee a$

(proof)
反射律 $a \leq a$ なので半順序の定義および前の定理より示される。 証明終

これと定義より、吸収則そのものがもっとも基本的な半順序を形成する。

定理 4.4 $a \wedge b \leq a \leq a \vee b, \quad a \wedge b \leq b \leq a \vee b$

定理 4.5 $a \leq b$ のとき $a \wedge x \leq b \wedge x, \quad a \vee x \leq b \vee x$

(proof)
$(a \wedge x) \wedge (b \wedge x) = (a \wedge b) \wedge (x \wedge x) = a \wedge x$ より $a \wedge x \leq b \wedge x$ である。また、$(a \vee x) \vee (b \vee x) = (a \vee b) \vee (x \vee x) = b \vee x$ より $a \vee x \leq b \vee x$ である。 証明終

4.2 区間

束 $(X, \wedge, \vee)$ について $a \leq b$ のとき $[a, b] \equiv \{x \in X : a \leq x \leq b\}$ を考えると、$x, y \in [a, b]$ について $x \wedge y = (x \wedge a) \wedge y = (x \wedge y) \wedge a$ より $a \leq x \wedge y$ であり、$x \vee y = (x \vee b) \vee y = (x \vee y) \vee b$ より $x \vee y \leq b$ である。よって

$$a \leq x \wedge y \leq x \vee y \leq b$$

であり、内算法 $\wedge, \vee$ は $[a, b]$ で閉じていることから $([a, b], \wedge, \vee)$ は部分束である。

定義 4.3 （区間）束 $(X, \wedge, \vee)$ について $a \leq b$ のとき、部分束 $[a, b] \equiv \{x \in X : a \leq x \leq b\}$ を**区間**もしくは商束という。◂

定義 4.4 （転置的）束 $(X, \wedge, \vee)$ について、二つの区間 $[a, b], [A, B]$ が $a = b \wedge A, B = b \vee A$ を満たす場合、二つの区間は**転置的**であるという。◂

定義 4.5 （モジュラ束）束 $(X, \wedge, \vee)$ が $x \leq z$ のとき $(x \vee y) \wedge z = x \vee (y \wedge z)$ を満たす場合、モジュラ束であるという。◂

定理 4.6 モジュラ束 $(X, \wedge, \vee)$ の転置的な区間 $[a, b], [A, B]$ において $f : [a, b] \to [A, B]$ を $f(x) = x \vee A$ と定義すると、f は同型写像かつ順序同型写像である。

(proof)
まず $f(a) = a \vee A = (b \wedge A) \vee A = A$ であり、$f(b) = b \vee A = B$ である。また、$g(x) = x \wedge b$ とすると $g(f(x)) = f(x) \wedge b = (x \vee A) \wedge b$ であり、$x \in [a, b]$ なら $X \leq b$ なので、モジュラ束の性質と $a \leq x$ より

$$g(f(x)) = (x \vee A) \wedge b = x \vee (A \wedge b) = x \vee a = x$$

であり、g は f の逆関数である。逆関数を持つことから f は全単射である。さらに $a = g(A) = A \wedge b, b = g(B) = B \wedge b$ も成立している。

f が準同型写像であることを示そう。$x, y \in [a, b]$ に対して

$$\begin{aligned} g(f(x) \wedge f(y)) &= (x \vee A) \wedge (y \vee A) \wedge b \\ &= (x \vee A) \wedge (y \vee A) \wedge (b \wedge b) \\ &= ((x \vee A) \wedge b) \wedge ((y \vee A) \wedge b) \\ &= x \wedge y \end{aligned}$$

より $f(x) \wedge f(y) = f(x \wedge y)$ である。また

$$\begin{aligned} f(x) \vee f(y) &= (x \vee A) \vee (y \vee A) \\ &= (x \vee y) \vee A \\ &= f(x \vee y) \end{aligned}$$

であることから、f は準同型写像であり、すでに全単射であると示していることから f が同型写像であると分かる。f が順序同型写像であることは、f が同型写像であることからすぐに示せる。 証明終

系 4.7 モジュラ束の転置的な区間は同型であり、かつ順序同型である。

したがって、ある区間から転置的な区間とっていったときにたどり着ける区間はすべて同型かつ順序同型である。そこで次の定義を置く。

定義 4.6 （射影的）束 $(X, \wedge, \vee)$ の二つの区間 $[a, b], [A, B]$ について、区間の列 $[a_1, b_1], \cdots, [a_{n-1}, b_{n-1}]$ が存在して、$[a_0, b_0] = [a, b], [a_n, b_n] = [A, B]$ としたとき、$[a_k, b_k]$ と $[a_{k+1}, b_{k+1}]$ が $k = 0, \cdots, n-1$ について転置的であるとき、二つの区間は**射影的**であるという。モジュラ束の射影的な区間は同型であり、かつ順序同型となっている。◂

定理 4.8 モジュラ束において $a_1 \leq a_2, b_1 \leq b_2$ のとき、区間 $[(a_2 \wedge b_1) \vee a_1, (a_2 \wedge b_2) \vee a_1]$ と $[(a_1 \wedge b_2) \vee b_1, (a_2 \wedge b_2) \vee b_1]$ は射影的である。

(proof)
$(a_2 \wedge b_1) \vee a_1$ と $a_2 \wedge b_2$ から転置的な区間を構成する。$b_1 \leq b_2$ より $a_2 \wedge b_1 \leq a_2 \wedge b_2$ である。

$$\begin{aligned}((a_2 \wedge b_1) \vee a_1) \wedge (a_2 \wedge b_2) &= (a_2 \wedge b_1) \vee (a_1 \wedge (a_2 \wedge b_2)) \quad \because \text{モジュラ束の性質} \\ &= (a_2 \wedge b_1) \vee (a_1 \wedge a_2 \wedge b_2) \\ &= (a_2 \wedge b_1) \vee (a_1 \wedge b_2) \quad \because a_1 \leq a_2\end{aligned}$$

であり

$$\begin{aligned}((a_2 \wedge b_1) \vee a_1) \vee (a_2 \wedge b_2) &= (a_2 \wedge b_1) \vee (a_2 \wedge b_2) \vee a_1 \\ &= (a_2 \wedge b_2) \vee a_1\end{aligned}$$

なので、区間 $[(a_2 \wedge b_1) \vee a_1, (a_2 \wedge b_2) \vee a_1]$ と $[a_2 \wedge b_2, (a_2 \wedge b_1) \vee (a_1 \wedge b_2)]$ は転置的である。どうようにして a と b を入れ替えると、区間 $[(a_1 \wedge b_2) \vee b_1, (a_2 \wedge b_2) \vee b_1]$ と $[a_2 \wedge b_2, (a_2 \wedge b_1) \vee (a_1 \wedge b_2)]$ は転置的である。よって示された。 証明終

4.3 組成列

定義 4.7 （組成列）束 $(X, \wedge, \vee)$ の元 $a \leq b$ に対して

$$a = u_0 < u_1 \cdots < u_n = b$$

となっており、$u_k < v < u_{k+1}$ を満たす元 v が存在しないとき、$\{u_0, \cdots, u_n\}$ を**組成列**という。ただし、「$x < y \Leftrightarrow x \leq y$ かつ $x \neq y$」とする。◂

定理 4.9 （ジョルダン・ヘルダーの定理）モジュラ束 $(X, \wedge, \vee)$ の元 $a \leq b$ に対して、二つの組成列

$$a = u_0 < u_1 \cdots < u_n = b$$
$$a = s_0 < s_1 \cdots < s_m = b$$

が存在するとき、$n = m$ であり、区間の列 $[u_0, u_1], \cdots, [u_n, u_n]$ に対して、$[s_0, s_1], \cdots, [s_n, s_n]$ を並び替えた区間の列 $[s_{\sigma(0)}, s_{\sigma(0)+1}], \cdots, [s_{\sigma(n)}, s_{\sigma(n)+1}]$ で、$[u_k, u_{k+1}]$ と $[s_{\sigma(k)}, s_{\sigma(k)+1}]$ が射影的であるものが存在する。

(proof)
$u_{-1} = s_{-1} = a$ と拡張しておく。$c_{ij} \equiv (u_i \wedge s_j) \vee u_{i-1} = (u_{i-1} \vee s_j) \wedge u_i$ とする。

$$c_{ij} \vee u_i = (u_{i-1} \vee s_j) \wedge u_i \wedge u_i = (u_{i-1} \vee s_j) \wedge u_i = c_{ij}$$

より $c_{ij} \leq u_i$ であり

$$c_{ij} \wedge u_{i-1} = (u_{i-1} \vee (s_j \wedge u_i)) \wedge u_{i-1} = u_{i-1}$$

より $u_{i-1} \leq c_{ij}$ である。つまり $u_{i-1} \leq c_{ij} \leq u_i$ である。i を固定すると $s_{j-1} < s_j$ より $c_{i(j-1)} \leq c_{ij}$ である。よって

$$a = c_{00} \leq \cdots \leq c_{0m} \leq c_{10} \leq \cdots \leq c_{(n-1)m} \leq c_{n0} \cdots \leq c_{nm} = b$$

である。同様に $d_{ji} \equiv (u_i \wedge s_j) \vee s_{j-1}$ と定義すると、

$$a = d_{00} \leq \cdots \leq d_{0n} \leq d_{10} \leq \cdots \leq d_{(m-1)n} \leq d_{m0} \cdots \leq d_{mn} = b$$

定理 4.8 より区間 $[c_{i(j-1)}, c_{ij}]$ と $[d_{j(i-1)}, d_{ji}]$ は射影的である。この結果、射影的であることがまだ分かっていない区間は、$[c_{(i-1)m}, c_{i0}]$ の形で表される区間、$[c_{0(j-1)}, c_{0j}]$ の形で表される区間、$[d_{(j-1)n}, d_{j0}]$ の形で表される区間、$[d_{0(i-1)}, d_{0i}]$ の形で表される区間となる。

$[c_{0(j-1)}, c_{0j}]$ の形で表される区間、$[d_{0(i-1)}, d_{0i}]$ の形で表される区間は実は $[a, a]$ である。$[c_{(i-1)m}, c_{i0}]$ の形で表される区間は $[u_{i-1}, u_{i-1}]$ であり、$[d_{(j-1)n}, d_{j0}]$ の形で表される区間は $[s_{j-1}, s_{j-1}]$ である。これらはすべて転置的であり、したがって射影的でもある。$\{c_{ij}\}$ の区間と $\{d_{ji}\}$ の区間は並び替えるとすべて射影的にすることができる。また、区間の数はいずれも $(n+1)(m+1)$ 個で等しい。

$\{c_{ij}\}$ の列と $\{d_{ji}\}$ の列から区間が $[x, x]$ の形になっているものを取り除く操作を繰り返すと、それぞれがもとの組成列となる。このとき、片方の列で $[x, x]$ の形になっているものに対しては、対応する射影的なもう片方の列における区間も、同型でなければならないため、$[x, x]$ の形になっており、取り除かれる区間の数は等しい。もとの区間の数が $(n+1)(m+1)$ で等しく、そこから除かれる区間の数も等しいため、組成列の要素数は等しい（$n = m$）。 証明終

5 群

5.1 群

定義 5.1 （群）半群 $(X, \circ)$ について、単位元が存在し、すべての元が逆元を持つとき、代数系 $(X, \circ)$ は**群**であるという。また、さらに内算法 $\circ$ が可換であるとき、**可換群**または**アーベル群**という。◂

整数は加法に関して可換群である。有理数はやはり加法に関して可換群であるが、0 に逆元がないため乗法に関しては群ではない。

群では、逆元が常に存在するため、**すべての元が正則元**であることがいえる。

5.1.1 準同型・同型関係

群の準同型写像による像もまた群となる。

定理 5.1 G を群とし、f を G を定義域とする準同型写像とするとき、像 $f(G)$ は単位元 $f(e)$、逆元 $f(x^{-1})$ をもって群となる。

(proof)
証明略。 証明終

これより直ちに、このことがいえる。

定理 5.2 群 G, G' が同型写像 $f : G \to G'$ を以て同型であるとき、それぞれの単位元を e, e' とすると

$$f(e) = e', \quad f^{-1}(e') = e, \quad f(x^{-1}) = f(x)^{-1}, \quad f^{-1}(x^{-1}) = f^{-1}(x)^{-1}$$

である。

5.1.2 半群の可逆化との関係

すでに述べたとおり、可換な内算法を持つ半群は、可逆化の手続きにより、単位元とその一部の元に対して逆元をもつものに拡張できる。また、系 3.9 は次のように言い換えられる。

定理 5.3 すべての元が正則元である可換な内算法を持つ半群は、可逆化すると可換群となる。

5.2 部分群・剰余群

定義 5.2 （部分群）$(G, \circ)$ を群とし、$G \supset H, (H, \circ)$ が群となる [3] とき、$(H, \circ)$ を $(G, \circ)$ の**部分群**という。◂

定義 5.3 （正規部分群）$(G, \circ)$ を群、H をその部分群とする。$\forall x \in G$ に対して $\{x \circ h : h \in H\} = \{h \circ x : h \in H\}$ が成立するとき、H を**正規部分群**という。◂

明らかに、可換群の部分群はすべて正規部分群である。

定理 5.4 $(G, \circ)$ を群、$H \subset G$ とするとき、H が群になるための必要十分条件は任意の $x, y \in H$ に対して $x^{-1} \circ y \in H$ となることである。

[3] 内算法が H の中で閉じている、すなわち $\forall a, b \in H$ に対して $a \circ b \in H$ であることを意味に含んでいる。

(proof)
必要性は自明である。十分性については次のとおり。
$\underbrace{x^{-1} \circ x}_{e} \in H$ より単位元をもつ。
$x^{-1} \circ e = x^{-1} \in H$ より逆元をもつ。
$x^{-1} \in H$ より $\underbrace{(x^{-1})^{-1} \circ y}_{x \circ y} \in H$ なので、閉じている。 証明終

定理 5.5 $(G, \circ)$ を群、H を G の部分群とするとき、H が正規部分群になるための必要十分条件は任意の $x \in G$ に対して $\{x \circ h \circ x^{-1} : h \in H\} = H$ となることである。

(proof)
必要性は容易に示せる。十分性については次のとおり。
$\forall x \in G$ に対して $\{x \circ h \circ x^{-1} : h \in H\} = H$ が成立するとき、$\exists h_2 \in H$ によって任意の $h \in H$ について $\forall x \in G, x \circ h = h_2 \circ x$ と表せる。つまり $\{x \circ h : h \in H\} \subset \{h \circ x : h \in H\}$ が成立する。
ところで、$\forall x \in G$ に対して $\{x \circ h \circ x^{-1} : h \in H\} = H$ が成立するので $\forall x, \{x^{-1} \circ h \circ x : h \in H\} = H$ も成立する。よって $\{x \circ h : h \in H\} \supset \{h \circ x : h \in H\}$ も成立し、結局 $\{x \circ h : h \in H\} = \{h \circ x : h \in H\}$ が成立する。 証明終

定理 5.6 $(G, \circ)$ を群、H を G の部分群とし、$x, y \in G$ に対して $x^{-1} \circ y \in H$ のとき、$x \sim y$ と書くとすれば、$\sim$ は同値関係である。

(proof)
$x^{-1} \circ x = e \in H$ より反射律が成立する。
$x^{-1} \circ y \in H$ ならば $(x^{-1} \circ y)^{-1} \in H$ より対称律が成立する。
$x^{-1} \circ y, y^{-1} \circ z \in H$ ならば $x^{-1} \circ y \circ y^{-1} \circ z = x^{-1} \circ z \in H$ より推移律が成立する。 証明終

定理 5.7 $(G, \circ)$ を群、H を G の正規部分群とし、$x, y \in G$ に対して同値関係 $\sim$ を $x \sim y \Leftrightarrow x^{-1} \circ y \in H$ によって定めるとき、$x \sim y \Leftrightarrow y \circ x^{-1} \in H$ も成立する[4]。

(proof)
$x \circ y$ とする。$y = x \circ (x^{-1} \circ y) \in \{x \circ h : h \in H\} = \{h \circ x : h \in H\}$ なので $h \in H$ によって $y = h \circ x$ と表せる。よって $y \circ x^{-1} = h \in H$ である。

逆に、$y \circ x^{-1} \in H$ のとき、$y = (y \circ x^{-1}) \circ x \in \{h \circ x : h \in H\} = \{x \circ h : h \in H\}$ なので $h \in H$ によって $y = x \circ h$ と表せる。よって $x^{-1} \circ y = h \in H \Leftrightarrow x \sim y$ である。 証明終

定理 5.8 $(G, \circ)$ を群、H を G の正規部分群とし、$x, y \in G$ に対して同値関係 $\sim$ を $x \sim y \Leftrightarrow x^{-1} \circ y \in H$ によって定めるとき、同値関係 $\sim$ と内算法 $\circ$ は両立し、得られる商構造は群となる。（この商構造を**剰余群**という。）

(proof)
まず、両立することを示す。$a, b \in G, a' \in [a], b' \in [b]$ とする。このとき $a^{-1} \circ a' \in H, b' \circ b^{-1} \in H$ である。よって

$$a^{-1} \circ a' \circ b' \circ b^{-1} \in H$$

[4]正規部分群の場合は、同値関係 $\sim$ において $x^{-1} \circ y$ と $y \circ x^{-1}$ の順序を気にしなくてよいということである。

であり

$$a' \circ b' \circ b^{-1} = a \circ (a^{-1} \circ a' \circ b' \circ b^{-1}) \in \{a \circ h : h \in H\} = \{h \circ a : h \in H\}$$

が成立することから $h \in H$ によって $a' \circ b' \circ b^{-1} = h \circ a$ と表される。これより

$$(a' \circ b') \circ (a \circ b)^{-1} = a' \circ b' \circ b^{-1} \circ a^{-1} = h \in H$$

つまり $a' \circ b' \sim a \circ b \Leftrightarrow a' \circ b' \in [a \circ b]$ であり、内算法 $\circ$ と同値関係 $\sim$ は両立する。そこで、商構造を $[a \circ b] = [a] \circ [b]$ となるよう定義できる。このときの商集合を G/H とする。このとき、$a \in G$ を同値類 $[a] \in G/H$ に割り当てる写像は準同型写像[5] である。この写像は全射でもあるので、定理 5.1 より G/H は群である。 証明終

ここで、単位元が含まれる同値類 $[e]$ について考えると

$$x \in [e] \Leftrightarrow x \circ e^{-1} \in H \ \Leftrightarrow x \in H$$

であるので $H = [e]$ に他ならない。定理 5.1 を踏まえると、正規部分群 H は、それから作られる剰余群の単位元そのものであるとわかる。

また、代表元が $a \in G$ である同値類 $[a] \in G/H$ について考えると $\forall x \in [a] \Leftrightarrow x \circ a^{-1} \in H$ より

$$x = (x \circ a^{-1}) \circ a \in \{h \circ a : h \in H\} = \{a \circ h : h \in H\}$$

なので $[a] \subset \{h \circ a : h \in H\} = \{a \circ h : h \in H\}$ である。逆に $\forall x \in \{h \circ a : h \in H\} = \{a \circ h : h \in H\}$ について、$h \in H$ によって $x = h \circ a$ と表されるので

$$x \circ a^{-1} = h \in H \Leftrightarrow x \in [a]$$

となる。よって $[a] = \{h \circ a : h \in H\} = \{a \circ h : h \in H\}$ である。ここで、写像 $f_a : H \to [a], f_a(h) = a \circ h$ を考えると、群が逆元を必ず持つことより逆写像が $f_a^{-1}(x) = a^{-1} \circ x$ と定まるため、f_a は全単射である。つまり、剰余群のそれぞれの元（同値類）はすべて正規部分群 H と同じ大きさを持っている。

定理 5.9 （群の第一同型定理）G, G' を群、$f : G \to G'$ を全射な準同型写像、H' を G' の正規部分群とする。このとき、

$$H \equiv f^{-1}(H') \equiv \{x \in G | f(x) \in H'\}$$

が G の正規部分群となり、G/H と G'/H' が同型である。

(proof)
写像 $g : G \to G'/H'$ を $g(x) = [f(x)]$ によって定めると、g もまた全射であり、$x, y \in G$ に対して

$$g(x) \circ g(y) = [f(x)] \circ [f(y)] = [f(x) \circ f(y)] = [f(x \circ y)] = g(x \circ y)$$

であるため、準同型である。よって準同型定理 2.2 より g によって生成される商集合 G/g は $g(G) = G'/H'$ と同型である。したがって定理 5.2 より G/g も群であり、G'/H' の単位元 H' に対応する G/g の元が G/g の単位元である。つまり G/g の単位元は $H \equiv f^{-1}(H') \equiv \{x \in G | f(x) \in H'\}$ である。

H が正規部分群であることを示す。定理 5.5 を用いる。$\forall x \in G$ に対して

$$\begin{aligned} f\left(\{x \circ h \circ x^{-1} : h \in H\}\right) &= \{f(x) \circ f(h) \circ f(x^{-1}) : h \in H\} \\ &= \{f(x) \circ h' \circ f(x)^{-1} : h' \in H'\} \quad \because f(H) = H' \\ &= H' \end{aligned}$$

[5] この写像を**標準的準同型写像**という。

であるため $\{x \circ h \circ x^{-1} : h \in H\} \subset f^{-1}(H') = H$ が成立する。x は任意なので、特に $\{x^{-1} \circ h \circ x : h \in H\} \subset H$ も成立する。よって任意の $h \in H$ について $\exists h_2 \in H, h = x \circ h_2 \circ x^{-1}$ となる。つまり $H \subset \{x \circ h \circ x^{-1} : h \in H\}$ であり

$$\{x \circ h \circ x^{-1} : h \in H\} = H$$

が成立する。よって H は正規部分群である。

ここで、商集合 G/g における同値関係について

$$\begin{aligned} & g(x) = g(y) \\ \Leftrightarrow\ & [f(x)] = [f(y)] \\ \Leftrightarrow\ & f(x)^{-1} \circ f(y) \in H' \\ \Leftrightarrow\ & f(x^{-1} \circ y) \in H' \\ \Leftrightarrow\ & x^{-1} \circ y \in H \end{aligned}$$

であるため、g から生成される商集合 G/g は、正規部分群 H による剰余群 G/H に等しい。よって示された。 証明終

5.3 核

定義 5.4 （核）$f : G \to G'$ を準同型写像とするとき、$f(x) = e'$(単位元) となるような G の元全部の集合を f の**核**といい、$\ker f$ と書く。◂

$\ker f$ は、準同型写像 f を適用した結果が等しいものを同一視する（定義 2.4）商集合 G/f の同値類のひとつである。また、ここでは群の内算法を $\circ$ で表すとする。

定理 5.10 （群の準同型定理）G, G' が群で $f : G \to G'$ を準同型写像とするとき、$\ker f$ は G の正規部分群であり、剰余群 $G/\ker f$ は像 $f(G) \equiv \{f(x) | x \in G\}$ と同型になる。

(proof)
剰余群 $G/\ker f$ は、以下に定義される同値関係 $\sim$

$$\begin{aligned} a \sim b \quad & \Leftrightarrow \quad a^{-1} \circ b \in \ker f \\ & \Leftrightarrow \quad f(a^{-1} \circ b) = f(a)^{-1} \circ f(b) = e' \quad \because \text{定理 5.1} \\ & \Leftrightarrow \quad f(a) = f(b) \end{aligned}$$

による商集合であり、準同型写像 f によって生成される同値関係による商集合 G/f（定義 2.4）に等しく、したがって、準同型定理 2.2 より、像 $f(G)$ と $G/\ker f = G/f$ は同型である。 証明終

5.4 直積

$(G_1, \circ), (G_2, \circ)$ を群とする。直積 $G_1 \times G_2$ に対して、内算法を $(g_1, g_2) \circ (g_1', g_2') \equiv= (g_1 \circ g_1', g_2 \circ g_2')$ により定義する。これは全域で定義された内算法となる。このとき、G_1, G_2 の単位元を e_1, e_2 とすると

$$(g_1, g_2) \circ (e_1, e_2) = (e_1, e_2) \circ (g_1, g_2) = (g_1, g_2)$$

より、(e_1, e_2) が単位元となる。また

$$(g_1, g_2) \circ (g_1^{-1}, g_2^{-1}) = (g_1^{-1}, g_2^{-1}) \circ (g_1, g_2) = (e_1, e_2)$$

より、任意の $(g_1, g_2) \in G_1 \times G_2$ に対して逆元 (g_1^{-1}, g_2^{-1}) が存在する。よって、直積 $G_1 \times G_2$ も群となる。これは**直積群**などとも呼ばれる。

定理 5.11 $(G,\circ)$ を群、H_1, H_2 をその部分群とするとき、次が成立する。

$$H_1 \cap H_2 = \{e\} \text{ かつ } G = \{h_1 \circ h_2 : h_1 \in H_1, h_2 \in H_2\} \tag{11}$$
$$\Leftrightarrow \text{任意の } x \in G \text{ が } x = h_1 \circ h_2 \, , h_1 \in H_1, h_2 \in H_2 \text{と一意に表現できる} \tag{12}$$

さらに H_1, H_2 が正規部分群であれば

$$x = h_1 \circ h_2 = h_2 \circ h_1 \, , h_1 \in H_1, h_2 \in H_2$$

が成立し、G は直積群 $H_1 \times H_2$ と同型である。

(proof)
(11) が成立するとき。任意の $x \in G$ は $x = h_1 \circ h_2 \, , h_1 \in H_1, h_2 \in H_2$ と表せる。

$$x = h_1 \circ h_2 = j_1 \circ j_2 \, , j_1 \in H_1, j_2 \in H_2$$

と 2 通りに表せたとする。このとき $j_1^{-1} \circ h_1 = j_2 \circ h_2^{-1} \in H_1 \cap H_2$ より

$$j_1^{-1} \circ h_1 = j_2 \circ h_2^{-1} = e$$

である。したがって $h_1 = j_1, h_2 = j_2$ であり、一意に表現される。

(12) が成立するとき。$G = \{h_1 \circ h_2 : h_1 \in H_1, h_2 \in H_2\}$ は自明である。$\forall x \in H_1 \cap H_2$ について $x = x \circ e = e \circ x$ が成立しており、この表現は一意であるため $x = e$ でなければならない。よって $H_1 \cap H_2 = \{e\}$ である。

H_1, H_2 が正規部分群であるとき。$a \equiv h_1 \circ h_2 \circ h_1^{-1} \circ h_2^{-1}$ とすると $h_1 \circ h_2 \circ h_1^{-1}, h_2 \in H_2$ より $a \in H_2$ である。また、$h_1, h_2 \circ h_1^{-1} \circ h_2^{-1} \in H_1$ でもある。よって $a \in H_1 \cap H_2$ つまり $a = e$ である。したがって $h_1 \circ h_2 = h_2 \circ h_1$ が成立する。

ここで、写像 $f : H_1 \times H_2 \to G$ を $f((h_1, h_2)) = h_1 \circ H_2$ として定める。(12) より f は全単射である。さらに $x = (x_1, x_2), y = (y_1, y_2) \in H_1 \times H_2$ について

$$\begin{aligned} f(x \circ y) &= f((x_1 \circ y_1, x_2 \circ y_2)) \\ &= x_1 \circ y_1 \circ x_2 \circ y_2 \\ &= x_1 \circ x_2 \circ y_1 \circ y_2 \\ &= f(x) \circ f(y) \end{aligned}$$

なので、f は同型写像である。 証明終

直積群は、群を単純に 2 つ組み合わせたものに過ぎない。上の定理が成立するような群は、直積群と同型であり、実は 2 つの群が重複せずに重なっているだけである。

6 環体

6.1 定義

定義 6.1 （分配的）集合 X に算法 $\circ_1, \circ_2$ が定義されているものとする。このとき、X の任意の元 a, b, c に対し

$$(a \circ_1 b) \circ_2 c = (a \circ_1 c) \circ_2 (b \circ_1 c)$$
$$a \circ_2 (b \circ_1 c) = (a \circ_1 b) \circ_2 (a \circ_1 c)$$

が成り立つ時、**分配的**であるという。上の *2* 式を**分配則**という。◂

定義 6.2 （環）代数系 $(X, +, \cdot)$ について

1. $(X, +)$ が可換群である。
2. $(X, \cdot)$ が半群である。
3. $(X, +, \cdot)$ は分配的である。

が成立するとき、代数系 $(X, +, \cdot)$ は**環**であるという。さらに、$\cdot$ が可換である場合は**可換環**であるという。◂

環においては、$+$ を加法、$\cdot$ を乗法という。加法の単位元は 0、乗法の単位元は 1 と表す。また、環の元 x の加法についての逆元は $-x$ と表すとする。可換群に、もうひとつの結合的な内算法（乗法）を導入し、可換群の内算法との関係として分配則を仮定したものが環である。典型的な環としては整数がある。

以後、環の乗法については、記号を省略することも可能とする。

定義 6.3 （体）環 $(X, +, \cdot)$ について $(X - \{0\}, \cdot)$ が群であるとき、代数系 $(X, +, \cdot)$ は**斜体**であるという。さらに、$\cdot$ が可換である場合は**体**であるという。◂

典型的な体としては、有理数、実数、複素数がある。

6.2 環の基本的性質

6.2.1 逆元

環は加法については必ず逆元を持つ。よって環 $(X, +, \cdot)$、$x, y \in X$ について $x - y \equiv x + (-y)$ によって常に**減算**を定義できる。$x \cdot y$ の逆元については、分配則と逆元の一意性より、次が成立する。

定理 6.1 環 $(X, +, \cdot)$ とその元 $x, y \in X$ について $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$

6.2.2 加法単位元

加法の単位元 0 は、分配則により乗法においても次の特別な性質がある。

定理 6.2 環 $(X, +, \cdot)$ とその元 $x \in X$ について $x \cdot 0 = 0 \cdot x = 0$

ただし、$x \cdot y = 0$ のとき $x = 0$ もしくは $y = 0$ は一般には成立しない。

定義 6.4 （零因子）可換環 $(X, +, \cdot)$ において、$x \neq 0, y \neq 0$ で $x \cdot y = 0$ となるとき x, y は**零因子**という。◂

可換環において零因子がなければ $x \cdot y = 0$ のとき $x = 0$ もしくは $y = 0$ となる。したがって、次が成立する。

定理 6.3 零因子を持たない可換環においては、0 以外は乗法についても正則元となる。

(proof)
$a \neq 0$ とする。$a \cdot x = a \cdot y$ のとき、$a \cdot (x + (-y)) = 0$ であり、$a \neq 0$ なので $x + (-y) = 0$ つまり $x = y$ となる。
証明終

6.3 可逆化

零因子を持たない可換環 $(X,+,\cdot)$ は、$X\times(X-\{0\})$ 上の商集合において、乗法について可逆化をおこなうことができる。可換環を可逆化し、加法を適切に導入すれば体にすることができる。こうして可逆化された体を、**商体**という。

例 6.5 整数は零因子を持たない可換環である。すでに見たように乗法についての可逆化は、分数を考えることに他ならない。これについて、加法を

$$\frac{n_1}{m_1}+\frac{n_2}{m_2}=\frac{n_1m_2+n_2m_1}{m_1m_2}$$

と導入することで、商体として有理数体が得られる。

6.3.1 商体の加法

商体に導入すべき加法は一概には決められない。しかしながら、最低限満たしておく性質がある。まず、明らかなように加法について可換群をなし、乗法との関係において分配的であることが求められる。

さらに、もとの環の拡張として捉えられるようにすべきである。商体 $(M,+,\cdot)$ 上でもとの可換環の元 $x\in X$ に対応するのは $\{x\}\equiv\{(x\cdot x^*,x^*):x^*\in X-\{0\}\}\in M$ である。$\{X\}\equiv\{\{x\}:x\in X\}\subset M$ とする。もとの環の拡張として捉えられるためには、$(\{X\},+,\cdot)$ が $(X,+,\cdot)$ と同型となるべきである。可逆化において、$(\{X\},\cdot)$ が $(X,\cdot)$ と同型であることは保証されているが、加法を加えたときに同型となるとは限らない。つまり、加法について、$x,y\in X$ として、次が成立すべきである。

$$\{x\}+\{y\}=\{x+y\} \tag{13}$$

ここに述べた条件を満たす商体は、次の例に示すように、少なくともひとつは常に存在しており、以後、商体についてはこれらの性質を満たしているものとする。

例 6.6 （**分数体**）可逆化の途中にあらわれる代数系 $(X\times(X-\{0\}),\cdot)$ に対して

$$(x,x^*)+(y,y^*)\equiv(x\cdot y^*+y\cdot x^*,x^*\cdot y^*)$$

によって内算法を定義する[6]。これは可換で結合的な内算法となる。ここで、商構造を作るための同値関係を $\sim$ とする。$(f,f^*)\sim(x,x^*)$, $(g,g^*)\sim(y,y^*)$ なる $(f,f^*),(g,g^*)\in X\times(X-\{0\})$ を考えると、$f\cdot x^*=x\cdot f^*$, $g\cdot y^*=y\cdot g^*$ である。このとき

$$\begin{aligned}(x\cdot y^*+y\cdot x^*)\cdot f^*\cdot g^* &= x\cdot y^*\cdot f^*\cdot g^*+y\cdot x^*\cdot f^*\cdot g^*\\ &= x^*\cdot y^*\cdot f\cdot g^*+y^*\cdot x^*\cdot f^*\cdot g\\ &= (f\cdot g^*+f^*\cdot g)\cdot x^*\cdot y^*\end{aligned}$$

より

$$\begin{aligned}&(x\cdot y^*+y\cdot x^*,\cdot x^*\cdot y^*)\sim(f\cdot g^*+f^*\cdot g,f^*\cdot g^*)\\ \Leftrightarrow\ &(x,x^*)+(y,y^*)\sim(f,f^*)+(g,g^*)\end{aligned}$$

である。つまり $X\times(X-\{0\})$ 上の内算法 $+$ と同値関係 $\sim$ が両立している。したがって、商構造 $X\times(X-\{0\})/\sim$ の内算法 $+$ を

$$[(x,x^*)]+[(y,y^*)]=[(x,x^*)+(y,y^*)]$$

[6]整数を有理数にする場合の、分数の和と同様の定義である。

となるように定義できる。こうして、商構造 $X\times(X-\{0\})/\sim$ には 2 つの内算法 $+,\cdot$ が導入されたことになる。$M\equiv X\times(X-\{0\})/\sim$ と表すことにする。可逆化の手続きにより、$(M,\cdot)$ は半群であることは保証されている。今回定義した内算法 $+$ は全域で定義されており、やはり可換で結合的である。よって $(M,+)$ が可換な半群であることはわかった。

このとき、もとの環の元 $x,y\in X$ に対して、$x^*,y^*\in X-\{0\}$ とすると

$$\begin{aligned}(x\cdot x^*,x^*)+(y\cdot y^*,y^*)&=(x\cdot x^*\cdot y^*+y\cdot y^*\cdot x^*,x^*\cdot y^*)\\&=((x+y)\cdot(x^*\cdot y^*),x^*\cdot y^*)\end{aligned}$$

となるので、このように定義された内算法 $+$ については、上に述べた商体における望ましい性質

$$\begin{aligned}\{x\}+\{y\}&=[(x\cdot x^*,x^*)]+[(y\cdot y^*,y^*)]=[(x\cdot x^*,x^*)+(y\cdot y^*,y^*)]=[((x+y)\cdot(x^*\cdot y^*),x^*\cdot y^*)]\\&=\{x+y\}\end{aligned}$$

が成立している。

もとの環の加法単位元 0 に対応する M の元 $\{0\}=[(0,u)],u\in X-\{0\}$ を考えると、$\forall(x,x^*)\in X\times(X-\{0\})$ について

$$\{0\}+[(x,x^*)]=[(0,u)]+[(x,x^*)]=[(0,u)+(x,x^*)]=[(x\cdot u,x^*\cdot u)]=[(x,x^*)]$$

が成立するので、$\{0\}$ は M の加法の単位元である。

任意の M の元 $[(x,x^*)]$ に対して $[(-x,x^*)]$ を考えると

$$[(x,x^*)]+[(-x,x^*)]=[x\cdot x^*+x^*\cdot(-x),x^*\cdot x^*]=[(x+(-x))\cdot x^*,x^*\cdot x^*]=[0,x^*\cdot x^*]=\{0\}$$

が成立するので、すべての M の元に対して逆元が存在する。したがって、これまでの示したことにより $(M,+)$ は可換群であることがわかる。

分配則については、$\forall(x,x^*),(y,y^*),(z,z^*)\in X\times(X-\{0\})$ について

$$\begin{aligned}([(x,x^*)]+[(y,y^*)])\cdot[(z,z^*)]&=[(x\cdot y^*+y\cdot x^*,x^*\cdot y^*)]\cdot[(z,z^*)]\\&=[((x\cdot y^*+y\cdot x^*)\cdot z,x^*\cdot y^*\cdot z^*)]\\&=[((x\cdot y^*\cdot z+y\cdot x^*\cdot z,x^*\cdot y^*\cdot z^*)]\\&=[((x\cdot y^*\cdot z\cdot z^*+y\cdot x^*\cdot z\cdot z^*,x^*\cdot y^*\cdot z^*\cdot z^*)]\\&=[(x\cdot z,x^*\cdot z^*)+(y\cdot z,y^*\cdot z^*)]\\&=[(x\cdot z,x^*\cdot z^*)]+[(y\cdot z,y^*\cdot z^*)]\\&=[(x,x^*)\cdot(z,z^*)]+[(y,y^*)\cdot(z,z^*)]\\&=[(x,x^*)]\cdot[(z,z^*)]+[(y,y^*)]\cdot[(z,z^*)]\end{aligned}$$

であることより成立している。したがって、$(M,+,\cdot)$ は可換環である。

さらに乗法について可逆化を行っており、乗法単位元は $e\equiv\{(u,u):u\in X-\{0\}\}$ である。$\forall[(x,x^*)]\in M-\{\{0\}\}$ について $x,x^*\in X-\{0\}$ であることから

$$[(x,x^*)]\cdot[(x^*,x)]=[(x,x^*)\cdot(x^*,x)]=[(x\cdot x^*,x\cdot x^*)]=e$$

であり、$(M-\{\{0\}\},\cdot)$ は可換群である。したがって、$(M,+,\cdot)$ は体である。このように構成された商体は、いわゆる分数の計算規則を導入したものであり**分数体**とよぶものとする。

6.3.2 商体の基本的な性質

上で述べたことをまとめると、商体の基本的な性質は、次のようにあらわされるだろう。

定理 6.4 商体は体であり、その部分集合がもとの（零因子を持たない）可換環と同型となっている。

再度記号を整理する。もとの可換環を $(X, +, \cdot)$ とし、商体を $(M, +, \cdot)$、もとの可換環と商体を対応させる写像を $x(\in X) \mapsto \{x\}$ とする。定理の内容より $\{X\} \equiv \{\{x\} : x \in X\} \subset M$ について、同型写像 $\{\ \}$ によって $(\{X\}, +, \cdot)$ と可換環 $(X, +, \cdot)$ は同型である。

商体の中でも、まず $(\{X\}, +, \cdot)$ が重要である。加法についてのみ考えた場合、$(\{X\}, +)$ は可換群 $(X, +)$ と同型であることから、定理 5.2 より $(\{X\}, +)$ は単位元 $\{0\}$ と $\forall\{x\} \in \{X\}$ に対して逆元 $\{-x\}$ をもって群となる。加法は可換であるため、$(\{X\}, +)$ は $(M, +)$ の正規部分群である。単位元は一意であるため、商体 $(M, +, \cdot)$ の加法単位元は $\{0\}$ そのものである。

定理 6.5 商体の加法の単位元は $\{0\}$ である。

可逆化により、$(\{X\}, +)$ では、もとの可換環とことなり乗法の単位元 1 と逆元を考えることができる。これらは、もとの可換環をつかって次のように表現できる。

定理 6.6 $x \neq 0\ (\in X)$ とすると $1 = \{x\} \cdot \{x\}^{-1}$

(proof)
$x \neq 0$ であるため $\{x\} \in M - \{\{0\}\}$ であり、乗法の逆元 $\{x\}^{-1}$ が存在して $1 = \{x\} \cdot \{x\}^{-1}$ が成立する。 証明終

定理 6.7 $x \neq 0\ (\in X)$ とすると $-1 = \{-x\} \cdot \{x\}^{-1}$

(proof)

$$\begin{aligned} 1 + \{-x\} \cdot \{x\}^{-1} &= \{x\} \cdot \{x\}^{-1} + \{-x\} \cdot \{x\}^{-1} \\ &= (\{x\} + \{-x\}) \cdot \{x\}^{-1} \\ &= \{0\} \cdot \{x\}^{-1} = \{0\} \end{aligned}$$

なので、$-1 = \{-x\} \cdot \{x\}^{-1}$ である。 証明終

6.3.3 演算子法

非負実数上で定義された複素連続関数の空間 C を考える。加法は、単純な関数の足し算とし、乗法としては次の合成積を考える。

$$(a * b)(t) \equiv \int_0^t a(t-s)b(s)ds$$

合成積 $*$ は全域で定義され、可換かつ結合的である。よって $(C, +, *)$ は可換環であることが分かる。また、この環は零因子を持たないことが知られている [7]。したがって、$(C, +, *)$ は可逆化することができる。可逆化された商体 $(M, +, *)$ をミクシンスキーの演算子という。

合成積に関する単位元 $\delta \equiv \{(g, g) : g \in (C - \{0\})\} \in M$ は、いわゆるディラックのデルタ関数に対応するものであり、もとの C には属さないものである。$f \in C$ に対して $\{f\} \equiv \{(f * g, g) : g \in (C - \{0\})\} \in M$ が

[7] Titchmarsh の定理

商体上でもとの f に対応する。C 上では、$(1*f)(t)=\int_0^t f(s)ds$ である。$l\equiv\{1\}\in M$ を積分演算子という。$l^2=\{1\}*\{1\}=\{1*1\}=\{t\}, l^3=\left\{\frac{t^2}{2!}\right\},\cdots,l^n=\left\{\frac{t^{(n-1)}}{(n-1)!}\right\}$ である。また、複素数 c に対して $c\equiv\{c\}*l^{-1}\in M$ と定義する。このとき

$$c*\{f\}=\{c\}*l^{-1}*\{f\}=l^{-1}*\{c\}*\{f\}=l^{-1}*\{1\}*\{(cf)\}=l^{-1}*\{1\}*\{(cf)\}=\{(cf)\}$$

であり、M 上で定数を表現する。加法の逆元は $(-c)$ であることが容易に分かる。

乗法（合成積）の逆元に関連して、$\frac{a}{b}=a*b^{-1}$ と表記することにする。このとき

$$\frac{a}{b}*\frac{c}{d}=a*b^{-1}*c*d^{-1}=a*c*(b*d)^{-1}=\frac{a*c}{b*d}$$

であり、また

$$\begin{aligned}\frac{a}{b}+\frac{c}{d}&=a*b^{-1}+c*d^{-1}\\&=a*d*(b*d)^{-1}+c*b*(b*d)^{-1}\\&=(a*d+c*b)*(b*d)^{-1}\\&=\frac{a*d+c*b}{b*d}\end{aligned}$$

であるので、通常の分数のように取り扱うことが可能である。

積分演算子の逆元 $s\equiv l^{-1}$ は微分演算子といわれる。$\int_0^t 1\cdot f'(s)ds=f(s)-f(0)$ なので、M 上では

$$\begin{aligned}l*\{f'\}&=\{f\}+\{-f(0)\}\\\{f'\}&=s*\{f\}+(-f(0))\end{aligned}$$

であり、$s*\{f\}=\{f'\}+f(0)$ となる。

例 6.7 f を指数関数 $f(t)=Ae^{\alpha t}$ とすれば $f'(t)=\alpha f(t),\ f(0)=A$ である。M 上に表現すれば

$$\begin{aligned}\{f'\}&=\{\alpha f\}\\s*\{f\}&=\alpha*\{f\}+A\\(s-\alpha)*\{f\}&=A\\\{f\}&=\frac{A}{s-\alpha}\end{aligned}$$

である。

例 6.8 f を正弦関数 $f(t)=\sin\alpha t$ とすれば $f''(t)=-\alpha^2 f(t),\ f'(0)=\alpha,\ f(0)=0$ である。M 上に表現すれば

$$\begin{aligned}\{f''\}&=-\alpha^2\{f\}\\s*\{f'\}&=-\alpha^2\{f\}+\alpha\\s^2*\{f\}&=-\alpha^2\{f\}+\alpha+s*0\\(s^2+\alpha^2)*\{f\}&=\alpha\\\{f\}&=\frac{\alpha}{s^2+\alpha^2}\end{aligned}$$

である。

例 6.9 f を余弦関数 $f(t) = \cos \alpha t$ とすれば $f(t) = \frac{(\sin t)'}{\alpha}$ である。M 上に表現すれば

$$\begin{aligned} \{f\} &= s * \{\sin t\} * \frac{1}{\alpha} \\ &= \frac{s}{s^2 + \alpha^2} \end{aligned}$$

である。

ミクシンスキーの演算子は、微分方程式を解くのに用いることができる。この微分方程式の解法を演算子法などという。

例 6.10 $f''(t) - 3f'(t) + 2f(t) = 0$ を解く。M 上に表現すると

$$\begin{aligned} \{f''\} - 3 * \{f'\} + 2 * \{f\} &= \{0\} \\ s * \{f'\} - 3 * \{f'\} + 2 * \{f\} &= \{0\} + f'(0) \\ (s-3) * \{f'\} + 2 * \{f\} &= f'(0) \\ s * (s-3) * \{f\} + 2 * \{f\} &= f'(0) + (s-3) * f(0) \\ (s^2 - 3 * s + 2) * \{f\} &= (f'(0) - 3f(0)) + s * f(0) \\ \{f\} &= \frac{(f'(0) - 3f(0)) + s * f(0)}{(s-2) * (s-1)} \\ &= \frac{f'(0) - f(0)}{s-2} + \frac{2f(0) - f'(0)}{s-1} \\ &= \{(f'(0) - f(0))e^{2t}\} + \{(2f(0) - f'(0))e^{t}\} \\ &= \{(f'(0) - f(0))e^{2t} + (2f(0) - f'(0))e^{t}\} \end{aligned}$$

となるので

$$f(t) = (f'(0) - f(0))e^{2t} + (2f(0) - f'(0))e^{t}$$

である。

演算子法で微分方程式を解くことについては、次のようにまとめられる。

1. 関数空間に、積分を内包する内算法（合成積）を定義する。
2. 合成積について、関数空間が合成積について可逆化可能である。
3. 合成積について可逆化した商体を考える。
4. 積分演算子の逆元が商体上の微分演算子となる。
5. 微分方程式を関数空間から商体へ同型写像を使ってうつす。
6. もとめるべき関数、微分演算子、定数が商体の元であり、逆元の存在が 0 を除き保証される。
7. 代数的な変形により、商体上でのもとめるべき関数の表現を得る。
8. 商体から関数空間への変換表（同型写像）をつかって関数空間での表現を得る。

ラプラス変換による微分方程式の解法と部分的に同じであるが、純粋に代数的に構成しているため、収束を考えなくてよい点でラプラス変換とは異なる。応用上の代数の有用性を感じることのできる例である。

6.4 イデアル

定義 6.11 （部分環）$(R,+,\cdot)$ を環とする。$I \subset R$ について $(I,+,\cdot)$ が環となるとき、I は部分環という。◂

$(I,+)$ と $(I,\cdot)$ が可換な半群であり、分配則が成り立つのは明らかである。$(I,+)$ が部分群であることが求められるため、任意の $x,y \in I$ について $x-y \in I$ となるという性質を持つ必要がある。さらに、$x\cdot y \in I$ が成立すれば、乗法について閉じており、I は部分環となる。部分環は加法について正規部分群であることにも留意する。

定理 6.8 $(R,+,\cdot)$ を環とする。$I(\subset R)$ が部分環であることと、$\forall x,y \in I \Rightarrow x-y, x\cdot y \in I$ が成立することは同値である。

定義 6.12 （イデアル）$(R,+,\cdot)$ を環とし、I を部分環とする。$x \in R, a \in I \Rightarrow x\cdot a, a\cdot x \in I$ が成り立つとき、I を**イデアル**という。◂

定理 6.9 $(R,+,\cdot)$ を環とし、I をイデアルとする。同値関係 $x \sim y \Leftrightarrow x-y \in I$ は加法および乗法と両立する。

(proof)
$x \sim f, y \sim g$ とする。$x-f, y-g \in I$ である。I は加法について正規部分群であるため、$(x-f)+(y-g) = (x+y)-(f+g) \in I$ つまり $x+y \sim f+g$ であり、同値関係 $\sim$ は加法と両立する。また、I がイデアルであることより $(x-f)\cdot y, f\cdot(y-g) \in I$ である。よって $(x-f)\cdot y + f\cdot(y-g) = x\cdot y - f\cdot g \in I$ つまり $x\cdot y \sim f\cdot g$ であり、同値関係 $\sim$ は乗法と両立する。 証明終

定義 6.13 （剰余環）$(R,+,\cdot)$ を環とし、I をイデアルとする。I は正規部分群でもあり、剰余群 $(R/I,+)$ を考えることができる。さらに、同じ同値関係は乗法とも両立しているため、乗法も含んだ商構造 $(R/I,+,\cdot)$ を考えることができる。剰余群 $(R/I,+)$ は可換群であり、$(R/I,\cdot)$ は半群である。また、もとの加法・乗法が分配的であることから、そこから得られた商構造においても分配則が成り立つ。したがって、$(R/I,+,\cdot)$ は環となる。これを**剰余環**という。◂

定義 6.14 （核）$(R,+,\cdot),(R',+,\cdot)$ を環とし、$f: R \to R'$ を準同型写像とする。環においては、加法の群としての核を環の核という。すなわち、$\ker f = \{x \in R : f(x) = 0\}$ である。◂

定理 6.10 $(R,+,\cdot),(R',+,\cdot)$ を環とし、$f: R \to R'$ を準同型写像とする。核 $\ker f$ はイデアルである。

(proof)
核は加法についてまず正規部分群である。さらに $x,y \in \ker f$ について $f(x\cdot y) = f(x)\cdot f(y) = 0$ より $x\cdot y \in \ker f$ である。よって核は部分環である。また、$a \in R$ について $f(x\cdot a) = f(x)\cdot f(a) = 0, f(a\cdot x) = f(a)\cdot f(x) = 0$ より I はイデアルである。 証明終

定理 6.11 （環の準同型定理）$(R,+,\cdot),(R',+,\cdot)$ を環とし、$f: R \to R'$ を準同型写像とする。剰余環 $R/\ker f$ は像 $f(R)$ と同型になる。

(proof)
剰余環 $R/\ker f$ は、以下に定義される同値関係 $\sim$

$$\begin{aligned} a \sim b &\Leftrightarrow a-b \in \ker f \\ &\Leftrightarrow f(a-b) = f(a) - f(b) = 0 \\ &\Leftrightarrow f(a) = f(b) \end{aligned}$$

による商集合であり、準同型写像 f によって生成される同値関係による商集合 R/f（定義 2.4）に等しく、したがって、準同型定理 2.2 より、像 $f(R)$ と $R/\ker f = R/f$ は同型である。 証明終

定義 6.15（極大イデアル）$(R,+,\cdot)$ を環とし、I をそのイデアルとする。R のイデアル J について

$$I \subset J \subset R, I \neq J \ \Rightarrow\ J = R$$

が成立するとき、R を**極大イデアル**という。◂

定理 6.12 $(R,+,\cdot)$ を乗法単位元を持つ可換環とし、I をその極大イデアルとする。このとき剰余環 R/I は体である。

(proof)
剰余環 R/I を構成するための同値関係は R の加法･乗法と両立しており、$[1] \in R/I$ が剰余環における乗法単位元である。ここで剰余環の加法単位元 $[0] = I$ でない元の代表元 $a \neq I$ をとる。このとき $J \equiv \{r \cdot a + h : r \in R, h \in I\}$ と定義すると、$x, y \in J$ について $x - y \in J, x \cdot y \in J$ が成立しており J は定理 6.9 よりイデアルである。定義より $I \neq J$ が成立しており、$a \in J$ について $a \neq I$ が成立しており $J \neq I$ である。よって I が極大イデアルなので $J = R$ である。よって $1 \in J$ であり $1 = r' \cdot a + h'$ を満たす $r' \in R, h' \in I$ が存在する。このとき剰余環 R/I において

$$[r'] \cdot [a] = [r' \cdot a] = [1 - h'] = [1]$$

であるため $[a] \neq [0]$ について逆元 $[r']$ が存在しており、$R/I - \{[0]\}$ が乗法について可換群であるので、R/I は体である。 証明終

6.4.1 生成されるイデアル

$(R,+,\cdot)$ を乗法単位元をもつ可換環とする。$a_1, \cdots, a_n \in R$ に対して $(a_1, \cdots, a_n) \equiv \{a_1 \cdot x_1 \cdots a_m \cdot x_n : x_1, \cdot, x_n \in R\}$ を考える。これが部分環であることは、定理 6.8 よりわかる。さらにこれはイデアルでもある。

定義 6.16（生成されるイデアル）$(R,+,\cdot)$ を乗法単位元をもつ可換環とする。$a_1, \cdots, a_n \in R$ に対して $(a_1, \cdots, a_n) \equiv \{a_1 \cdot x_1 \cdots a_m \cdot x_n : x_1, \cdot, x_n \in R\}$ を $a_1, \cdots, a_n \in R$ で**生成されるイデアル**という。特に、ひとつの元 a により生成されるイデアル (a) を**単項イデアル**という。$(R,+,\cdot)$ のすべてのイデアルが単項イデアルとして表されるとき、$(R,+,\cdot)$ は**単項イデアル環**という。◂

生成されるイデアルは、典型的なイデアルのイメージを与えるものである。

6.5 整域

定義 6.17（整域）乗法の単位元 1 を持ち、零因子を持たない可換環を**整域**という。単項イデアル環が整域であるとき、**単項イデアル整域**という。◂

整域は、乗法についても 0 以外の元が正則元となり、乗法について可逆化した商体を構成可能である。整域の乗法単位元は商体の乗法単位元に対応している（系 3.8）。整数は、典型的な整域である。

定義 6.18（ユークリッド整域）整域 $(R,+,\cdot)$ について、$x \in R, x \neq 0$ に対して非負整数 $g(x)$ が定義されていて

$$a, b \in R, a \neq 0, b \neq 0 \Rightarrow g(a) \leq g(ab) \tag{14}$$

$$a, b \in R, b \neq 0 \Rightarrow \exists q, r \in R, a = qb + r, r = 0 \text{ または } g(r) < g(b) \tag{15}$$

を満たすとき、$(R,+,\cdot), g$ はユークリッド整域という。◂

例えば、整数は $g(x) = |a|$ によってユークリッド整域となる。式 (15) は、整数の割り算の余りについての性質に対応している。

定理 6.13 ユークリッド整域の $\{0\}$ でないイデアル I は、$m \in \{x \in I - \{0\} : \forall y \in I - \{0\}, g(x) \leq g(y)\}$ によって $I = (m)$ と表される単項イデアルである。

(proof)
$(R, +, \cdot), g$ をユークリッド整域とする。イデアルが $\{0\}$ だけであれば、明らかに単項イデアル整域である。I を $I \neq \{0\}$ なる $(R, +, \cdot)$ の任意のイデアルとする。$b \in \{x \in I - \{0\} : \forall y \in I - \{0\}, g(x) \leq g(y)\}$ とする。ユークリッド整域の性質により、任意の $a \in I$ について、$a = qb + r$ を満たす $q, r \in R$ が存在して、$r = 0$ もしくは $g(r) < g(b)$ である。しかし、イデアルの性質により $r = a - qb \in I$ であるため、$g(b) \leq g(r)$ とならなければならない。よって $r = 0$ であり $a = qb$ となる。 証明終

系 6.14 ユークリッド整域は単項イデアル整域である。

6.6 倍元・約元

定義 6.19 （倍元・約元）整域 $(R, +, \cdot)$、$a, b \in R$ について、$b = ac$ なる c が存在するとき、$a|b$ と表し、a を b の約元、b を a の倍元という。$a|b$ かつ $b|a$ のとき、a と b は同伴であるという。◂

$a|b$ は $b \in (a), (a) \supset (b)$ と同値である。また、同伴であることは、$b = ac$ なる乗法可逆元 c が存在すること、$(a) = (b)$ と同値である。

倍元・約元の関係 $|$ を二項関係と考えたとき、次のとおり推移律が成り立っている。

定理 6.15 $a|b, b|c$ ならば $a|c$

反射律を満たすことは明らかであるため、$|$ は擬順序である。このとき、同伴は同値関係となり、強連結成分分解（商集合）[8] を考え、$|$ からその上に半順序を定義することができる。この半順序も $|$ で表すこととしよう。このとき、$a|b$ ならば強連結成分について $[a]|[b]$ である。$[a]|[b]$ かつ $[a] \neq [b]$ のときは $[a] < [b]$ と表すものとする。

例 6.20 整数の場合、同伴となるのは n に対しては $-n$ だけである。強連結成分分解は非負整数を考えることに相当し、半順序は約数・倍数の関係に対応する。

補題 6.16 整域 $(R, +, \cdot)$ について、同伴による強連結成分分解を考える。このとき、同伴と乗法は両立している。

(proof)
$a, b \in R$ とし、$x \in [a], y \in [b]$ とする。このとき乗法可逆元 u_1, u_2 によって $x = au_1, y = bu_2$ と表される。よって $xy = (ab)(u_1u_2)$ であり $xy \in [ab]$ である。 証明終

そのため、強連結成分分解に対して乗法を $[a][b] = [ab]$ となるよう定義できる。$|$ も強連結成分分解上で約元・倍元の関係に対応するものとなる。

補題 6.17 整域 $(R, +, \cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。$\alpha, \beta \in \Gamma(R)$ について $\alpha|\beta \Leftrightarrow \exists \gamma \in \Gamma(R), \beta = \alpha\gamma$ である。

[8] ここで用いている倍元・約元に関する強連結成分分解の記号は、一般的なものでないことに留意する。

(proof)
$\alpha|\beta$ のとき、$a \in \alpha, b \in \beta$ とする。$[a]|[b]$ となるので $a|b$ である。よって $\exists c \in R, b = ac$ であり、$\beta = [b] = [ac] = [a][c] = \alpha[c]$ と表される。逆に、$\exists \gamma \in \Gamma(R), \beta = \alpha\gamma$ のとき、$a \in \alpha, b \in \beta, c \in \gamma$ とする。$[b] = [a][c] = [ac]$ より $ac|b$ が成立する。$a|ac$ なので $a|b$ であり従って $[a]|[b]$ つまり $\alpha|\beta$ である。 証明終

系 6.18 整域 $(R, +, \cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。任意の $\beta \in \Gamma(R)$ について $[1]|\beta$ が成立する。

系 6.19 整域 $(R, +, \cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。任意の $\alpha \in \Gamma(R)$ について $\alpha|[0]$ が成立する。

強連結成分分解に対しては、$|$ が半順序であり、$[1]$ は任意の元と半順序を定義できて、強連結成分分解の最小元である。また、$[0]$ は任意の元と半順序を定義できて、強連結成分分解の最大元である。最大限や最小元は一意であることから、$\forall \alpha \neq [1]$ に対して $[1] < \alpha$ であり、$\forall \beta \neq [0]$ に対して $\beta < [0]$ である。なお、$[1]$ は乗法可逆元の全体である。

補題 6.20 整域 $(R, +, \cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。$[1] \in \Gamma(R)$ は R の乗法可逆元の全体である。

(proof)
乗法可逆元 u は $1 = uu^{-1}$ より $u|1$ であり $1|u$ は常に成立するため、1 と同伴である。つまり、乗法可逆元はすべて $[1]$ に属している。逆に $u \in [1]$ について $u|1, 1|u$ である。よって $1 = us$ となる s が存在するが、このとき s は逆元であり、u は乗法可逆元である。 証明終

このため、整域が**体**であると、強連結成分分解は $\{[0], [1]\}$ の 2 要素しかもたないことになり、**倍元・約元に関する議論がほとんど意味の無い**ものになる。数に関しては、一般的に整数に対する約数・倍数しか考えないのは、こういったことも背景にある。

補題 6.21 整域 $(R, +, \cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。$\alpha(\neq [0]), \beta \in \Gamma(R)$ に対して $\beta = \alpha\gamma$ を満たす $\gamma \in \Gamma(R)$ は一意である。

(proof)
$\beta = \alpha\gamma = \alpha\gamma'$ と二通りに表されたとする。$a, a' \in \alpha, c \in \gamma, c' \in \gamma'$ とする。$u, s \in [1]$ によって $a = a'u, ac = a'c's$ である。よって $a(c - c'us) = 0$ である。$\alpha \neq [0]$ より $a \neq 0$ なので $c = c'(us)$ より c と c' は同伴である。つまり $\gamma = \gamma'$ である。 証明終

補題 6.22 $m \in R$ とし、$\Gamma(R)$ を同伴による R の強連結成分分解とすると、次が成立する。

$$(m) = \bigcup_{\gamma \in \Gamma(R)} [m]\gamma$$

(proof)
任意の $x \in (m)$ について、$x = mc, c \in R$ であるため、強連結成分に対応させると $[x] = [mc] = [m][c]$ であり $x \in [x] = [m][c] \subset \bigcup_{\gamma \in \Gamma(R)} [m]\gamma$ である。よって $(m) \subset \bigcup_{\gamma \in \Gamma(R)} [m]\gamma$ である。逆に任意の $x \in \bigcup_{\gamma \in \Gamma(R)} [m]\gamma$ について、ある γ' が存在して $x \in [m]\gamma'$ である。$c \in \gamma'$ をとると、$x \in [m][c] = [mc]$ より $mc|x$ であり $m|mc$ なので、$m|x$ つまり $x \in (m)$ である。よって $(m) \supset \bigcup_{\gamma \in \Gamma(R)} [m]\gamma$ であり、示される。 証明終

単項イデアル (m) に対して、強連結成分分解上では $([m]) \equiv \{[m]\gamma : \gamma \in \Gamma(R)\}$ が対応しており、$(m) = \bigcup_{\gamma \in ([m])} \gamma$ である。$([m])$ の最小元は $[m]$ となっている。

補題 6.23 整域 $(R,+,\cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。$\alpha,\beta,\gamma \in \Gamma(R), \beta \neq [0]$ について $\beta = \alpha\gamma$ のとき $\gamma \neq [1]$ ならば $\alpha < \beta$ である。

(proof)
$\alpha|\beta$ は成立しているので、$\gamma \neq [1] \Rightarrow \alpha \neq \beta$ を示せばよい。そのためには、$\alpha = \beta \Rightarrow \gamma = [1]$ を示せばよい。そこで、$\alpha = \beta$ の場合を考える。$a \in \alpha, b \in \beta, c \in \gamma$ について ac と b が同伴なので、乗法可逆元 $u \in [1]$ が存在して $ac = bu$ と表せる。また、a と b も同伴なので、$s \in [1]$ が存在して $a = bs$ と表せる。このとき、$bu = ac = bsc$ より $bc = b(us^{-1})$ である。定理 6.3 より $b \neq 0$ ならば $c = us^{-1} \in [1]$ である。よってこのとき $\gamma = [1]$ である。 証明終

定義 6.21 （既約元）整域 $(R,+,\cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。このとき、$\alpha,\beta,\gamma \in \Gamma(R)$ について $\alpha = \beta\gamma$ ならば $\beta = [1]$ または $\gamma = [1]$ が成り立つとき、$\alpha \neq [1]$ を既約強連結成分とよぶことにする。また、既約強連結成分の元を**既約元**という。◂

任意の $\beta \in \Gamma(R)$ に対して $\beta = \alpha\gamma$ の形に分解することは、少なくとも $\alpha = 1, \gamma = \beta$ によって可能である。この形にしか分解できないのが既約強連結成分であり、逆に既約強連結成分以外の強連結成分（[1] でない）は $\alpha \neq [1], \beta \neq [1]$ を満たす強連結成分に分解できる。

6.6.1 単項イデアル整域における約元・倍元

定義 6.22 単項イデアル整域においては、任意のイデアル I が単項イデアル (m) として表すことができる。このとき、イデアル I に対して同伴による強連結成分分解上の最小元 $[m]$ を $\mathrm{imin} I$ とする。◂

定義 6.23 （最大公約元）単項イデアル整域 $(R,+,\cdot)$ において、$a_1,\cdots,a_n \in R$ に対して $\mathrm{imin}(a_1,\cdots,a_n)$ を最大公約強連結成分と呼ぶものとする。また、最大公約強連結成分の元を**最大公約元**といい $gcd(a_1,\cdots,a_n)$ で表す。◂

定理 6.24 $gcd(a_1,\cdots,a_n)|a_1,\cdots,gcd(a_1,\cdots,a_n)|a_n$

(proof)
任意の $y \in (a_1,\cdots,a_n)$ について $gcd(a_1,\cdots,a_n)|y$ である。$a_1,\cdots,a_n \in (a_1,\cdots,a_n)$ なので、示される。 証明終

定理 6.25 $gcd(a_1,\cdots,a_n) = a_1x_1 + \cdots + a_nx_n$ となる $x_1,\cdots,x_n$ が存在する。

(proof)
定義より $gcd(a_1,\cdots,a_n) \in (a_1,\cdots,a_n)$ であり、$(a_1,\cdots,a_n)$ の定義より示される。 証明終

定理 6.26 $gcd(a,b) \in [1]$ のとき $gcd(b,ac)$ と $gcd(b,c)$ は同伴である。

(proof)
まず、$(b,ac) \subset (b,c)$ より $gcd(b,c)|gcd(b,ac)$ である。直前の定理より $ax' + by' = u, u \in [1]$ なる x', y' が存在する。このとき $x_0 = x'u^{-1}, y_0 = y'u^{-1}$ によって $ax_0 + by_0 = 1$ となる。また、直前の定理より $gcd(b,c) = bx_1 + cy_1$ なる x_1, y_1 が存在する。このとき

$$gcd(b,c) = (bx_1 + cy_1) = (bx_1 + cy_1)(ax_0 + by_0) = ac(y_1x_0) + b(x_1(ax_0 + by_0) + y_1by_0) \in (ac,b)$$

より $gcd(b,ac)|gcd(b,c)$ である。よって示された。 証明終

定理 6.27 単項イデアル整域 $(R,+,\cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とする。$\alpha_1,\cdots,\alpha_n \in \Gamma(R)$ と、任意の $a_k, b_k \in \alpha_k$ について $gcd(a_1,\cdots,a_n)$ と $gcd(b_1,\cdots,b_n)$ は同伴である。

(proof)
$gcd(a_1,\cdots,a_n) = a_1x_1+\cdots+a_nx_n$ となる $x_1,\cdots,x_n$ が存在する。また $a_k, b_k \in \alpha_k$ より $a_k = b_ku_k, u_k \in [1]$ と表せる。このとき $gcd(a_1,\cdots,a_n) = b_1(u_1x_1)+\cdots+b_n(u_nx_n) \in (b_1,\cdots,b_n)$ なので $gcd(b_1,\cdots,b_n)|gcd(a_1,\cdots,a_n)$ である。同様に $gcd(a_1,\cdots,a_n)|gcd(b_1,\cdots,b_n)$ を示すことができる。 証明終

定義 6.24 上の定理により、強連結成分 $\alpha_1,\cdots,\alpha_n \in \Gamma(R)$ に対して、その元による最大公約強連結成分は等しい。そこで、これについても最大公約強連結成分を定義できるので、$\mathrm{imin}(\alpha_1,\cdots,\alpha_n)$ と表すものとする。
◂

これについての基本的な性質として次のようなものがある。

補題 6.28 $\mathrm{imin}(\alpha_1,\cdots,\alpha_n)|\alpha_1,\cdots,\mathrm{imin}(\alpha_1,\cdots,\alpha_n)|\alpha_n$

補題 6.29 $\mathrm{imin}(\alpha\beta,\alpha) = \alpha$

(proof)
まず $\mathrm{imin}(\alpha\beta,\alpha)|\alpha$ である。また、$a \in \alpha, b \in \beta$ について、(ab,a) の任意の元は $abx+ay = a(bx+y)$ と表せるので $a|gcd(ab,a)$ つまり $\alpha|\mathrm{imin}(\alpha\beta,\alpha)$ であり、強連結成分分解上の $|$ は反対称則を満たすので $\alpha = \mathrm{imin}(\alpha\beta,\alpha)$ である。 証明終

補題 6.30 $\mathrm{imin}(\alpha\beta,\alpha\gamma) = \alpha\ \mathrm{imin}(\beta,\gamma)$

(proof)
$a \in \alpha, b \in \beta, c \in \gamma$ について、(ab,ac) の任意の元は $abx+acy = a(bx+cy) = a\ gcd(b,c)\ z$ と表せる。つまり $(ab,ac) = (agcd(b,c))$ であり、これがなすイデアルの強連結成分分解上の最小元は一致する。よって $\mathrm{imin}(\alpha\beta,\alpha\gamma) = [agcd(b,c)] = \alpha\ \mathrm{imin}(\beta,\gamma)$ である。 証明終

次の性質も、単項イデアル整域の重要な性質である。

補題 6.31 単項イデアル整域の任意の強連結成分について、有限の既約強連結成分の積で表せる。

(proof)
単項イデアル整域 $(R,+,\cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とし、$\alpha_0 \in \Gamma(R)$ が有限の既約強連結成分の積で表せないと仮定する。このとき α_0 が既約強連結成分であると仮定に反するため、$\alpha_1 \neq [1], \beta_1 \neq [1]$ によって $\alpha_0 = \alpha_1\beta_1$ と表せる。補題 6.23 より $\alpha_0 > \alpha_1, \alpha_0 > \beta_1$ である。少なくとも片方は有限の既約強連結成分の積では表せないため、一般性を失わず α_1 が有限の既約強連結成分の積では表せないとする。α_1 に対して同様の処理を行うことで $\alpha_1 > \alpha_2$ なる α_2 が得られ、繰り返していくと点列 $\alpha_0 > \alpha_1 > \alpha_2\cdots$ が得られる。このときそれぞれの元 $a_k \in \alpha_k$ をとり $I \equiv \bigcup_{k=0}^{\infty}(a_k)$ とする。$\forall x,y \in I$ について $\exists l,m, x \in (a_l) \subset (a_{\min(l,m)}), y \in (a_m) \subset (a_{\min(l,m)})$ となる。よって $x-y \in I$ である。また $\forall x \in I, \forall y \in R$ について明らかに $xy \in I$ である。よって I はイデアルである。単項イデアル整域の性質により、$I = (m), m \in R$ と表せる。$m \in I$ でもあるので $\exists K, m \in (a_K) = \bigcup_{\gamma\in\Gamma}[a_k]\gamma$ である。よって $\exists\gamma', [m] = [a_K]\gamma'$ つまり $\alpha_K|[m]$ である。このとき $\alpha_{K+1} < [m]$ である。しかし、$I = (m) \subset (a_{K+1})$ より $m|a_{K+1}$ つまり $[m]|\alpha_{K+1}$ であり、矛盾する。よっ

て、有限の既約強連結成分の積で表せる。 証明終

単項イデアル整域においては、有限の既約強連結成分の積に分解できることがわかった。その分解の仕方にどのような構造があるかに興味がある。

6.6.2 同伴による強連結成分分解の束構造

単項イデアル整域 $(R,+,\cdot)$ について、$\Gamma(R)$ を同伴による R の強連結成分分解とし、強連結成分 $\alpha,\beta,\gamma\in\Gamma(R)$ を考える。このとき、最大公約強連結成分をつかって、内算法 $\wedge$ を $\alpha\wedge\beta\equiv \mathrm{imin}(\alpha,\beta)$ と定義すると、全域で定義された可換な内算法である。さらに、次のとおり結合的でもある。

補題 6.32 内算法 $\wedge$ は結合的である。

(proof)
$a\in\alpha, b\in\beta, c\in\gamma$ とする。(a,b,c) の任意の元 $ax_1+bx_2+cx_3$ について、強連結成分分解上の最小元は $\mathrm{imin}(a,b,c)$ である。また、ax_1+bx_2 は $ax_1+bx_2=gcd(a,b)y$ の形で表せる。よって (a,b,c) の任意の元は $gcd(a,b)y+cx_3$ と表せる。この強連結成分分解上の最小元は $\mathrm{imin}(gcd(a,b),c)$ である。最小元は一意であるため $\mathrm{imin}(gcd(a,b),c)=\mathrm{imin}(a,b,c)$ であり、$gcd(a,b)\in\alpha\wedge\beta$ なので $(\alpha\wedge\beta)\wedge\gamma=\mathrm{imin}(gcd(a,b),c)=\mathrm{imin}(a,b,c)$ である。同様にして $\alpha\wedge(\beta\wedge\gamma)=\mathrm{imin}(a,b,c)$ なので $(\alpha\wedge\beta)\wedge\gamma=\alpha\wedge(\beta\wedge\gamma)$ である。 証明終

$\alpha',\beta'\in\Gamma(R)$ として、$\alpha=(\alpha\wedge\beta)\alpha',\beta=(\alpha\wedge\beta)\beta'$ と表したとき、補題 6.21 より α',β' は一意に定まる。これをつかって、$\alpha\vee\beta\equiv(\alpha\wedge\beta)\alpha'\beta'$ と定義すると、$\vee$ は全域で定義された結合的で可換な内算法となる。さらに、次のとおり吸収則を満たしている。

補題 6.33 $(\alpha\vee\beta)\wedge\alpha=\alpha,\ (\alpha\wedge\beta)\vee\alpha=\alpha$

(proof)
$(\alpha\vee\beta)=(\alpha\wedge\beta)\alpha\beta'=\alpha\beta'$ なので補題 6.29 より $(\alpha\vee\beta)\wedge\alpha=(\alpha\beta')\wedge\alpha=\alpha$ である。また、$\alpha\wedge\beta=(\alpha\wedge\beta)[1],\alpha=(\alpha\wedge\beta)\alpha'$ であるので $(\alpha\wedge\beta)\vee\alpha=(\alpha\wedge\beta)[1]\alpha'=(\alpha\wedge\beta)\alpha'=\alpha$ である。 証明終

したがって、代数系 $(\Gamma(R),\wedge,\vee)$ は束である。さらに $\Gamma(R)$ 上には乗法と半順序 $|$ が定義されている。このとき、半順序 $|$ は、次のとおり束から定義する半順序と同じものである。

補題 6.34 $\alpha|\beta\Leftrightarrow\beta=\alpha\vee\beta$

(proof)
$\alpha|\beta$ のとき $\alpha\wedge\beta=\alpha$ であり、$\alpha\vee\beta=(\alpha)[1]\beta'=\beta$ となる。逆に、$\beta=\alpha\vee\beta$ のとき。$\alpha\vee\beta=\beta\alpha$ なので $\beta=\beta\alpha$ である。$b\in\beta, c\in\alpha'$ とする。このとき $bu=bc, u\in[1]$ が成立している。変形して $b(u-c)=0$ である。$b=0$ ならば明らかに $\alpha|\beta$ が成立している。$b\neq0$ ならば整域の性質より $c=u$ である。よって $\alpha'=[1]$ であり $\alpha=\alpha\wedge\beta$ が成立して $\alpha|\beta$ である。 証明終

補題 6.35 $\alpha,\beta,\alpha',\beta'\in\Gamma(R)$ として、$\alpha=(\alpha\wedge\beta)\alpha',\beta=(\alpha\wedge\beta)\beta'$ と表したとき、$\alpha'\wedge\beta'=[1]$ である。

(proof)
$a\in\alpha, b\in\beta, a'\in\alpha', b'\in\beta'$ とする。$a=gcd(a,b)\,a', b=gcd(a,b)\,b'$ である。任意の $c\in\alpha'\wedge\beta'$ について $a'=cx, b'=cy$ と表せる。このとき $a=gcd(a,b)\,cx, b=gcd(a,b)\,cy$ となるため $(a,b)\subset(gcd(a,b)\,c)$ であり $gcd(a,b)\,c|gcd(a,b)$ となる。よって、最小公倍強連結成分の最小性より $gcd(a,b)\,c\in\mathrm{imin}(a,b)$ である。これを満たすには $c\in[1]$ が必要十分条件である。つまり $\alpha'\wedge\beta'=[1]$ である。 証明終

補題 6.36 $\alpha,\beta,\gamma \in \Gamma(R)$ について、$\alpha \wedge \beta = [1]$ ならば $\beta \wedge (\alpha\gamma) = \beta \wedge \gamma$ である。

(proof)
$a \in \alpha, b \in \beta, c \in \gamma$ とする。$\alpha \wedge \beta = [1]$ なので $gcd(a,b) \in [1]$ である。よって定理 6.26 より $gcd(b,c)$ と $gcd(b,ac)$ が同伴である。つまり、$(b,c) = (b,ac)$ であり $\mathrm{imin}(b,c) = \mathrm{imin}(b,ac)$ が成立している。このとき、$ac \in \alpha\gamma$ なので

$$\beta \wedge \gamma = \mathrm{imin}(\beta,\gamma) = \mathrm{imin}(b,c) = \mathrm{imin}(b,ac) = \mathrm{imin}(\beta,\alpha\gamma) = \beta \wedge (\alpha\gamma)$$

である。 証明終

ほかにも束の性質に加えて、つぎのような性質がある。

$$(\alpha\beta) \wedge (\alpha\gamma) = \alpha(\beta \wedge \gamma)$$
$$(\alpha\beta) \vee (\alpha\gamma) = \alpha(\beta \vee \gamma)$$
$$(\alpha \wedge \beta)(\alpha \vee \beta) = \alpha\beta$$

補題 6.37 代数系 $(\Gamma(R), \wedge, \vee)$ はモジュラ束である。

(proof)
束であることは分かっている。$\alpha|\gamma$ とする。このとき、$\alpha = (\alpha \wedge \beta)\alpha', \beta = (\alpha \wedge \beta)\beta', \gamma = (\alpha \wedge \beta)\alpha'\gamma'$ と表すことができ、$\alpha' \wedge \beta' = [1]$ が成立している。これらにより

$$\begin{aligned}(\alpha \vee \beta) \wedge \gamma &= (\alpha\beta') \wedge (\alpha\gamma') \\ &= \alpha(\beta' \wedge \gamma')\end{aligned}$$

であり

$$\begin{aligned}\alpha \vee (\beta \wedge \gamma) &= \alpha \vee (\alpha \wedge \beta)(\beta' \wedge \alpha'\gamma') \\ &= \alpha \vee (\alpha \wedge \beta)(\beta' \wedge \gamma') \quad \because \text{補題 6.36} \\ &= \alpha(\beta' \wedge \gamma') \quad \because \alpha' \wedge \beta' \wedge \gamma' | \beta' \wedge \gamma' = [1] \text{ より} \alpha' \wedge \beta' \wedge \gamma' = [1]\end{aligned}$$

である。よって $(\alpha \vee \beta) \wedge \gamma = \alpha \vee (\beta \wedge \gamma)$ であり、モジュラ束である。 証明終

これによって、モジュラ束の性質が使用できることとなった。

単項イデアル整域の任意の強連結成分 $\alpha \neq 0$ に対して、補題 6.31 より有限の既約強連結成分の積で表せる。この表現の一つを

$$\alpha = \beta_1 \cdots \beta_n$$

とする。このとき、$\gamma_k \equiv \beta_1 \cdots \beta_k, \gamma_0 \equiv [1]$ とすると

$$[1] = \gamma_0 < \gamma_1 < \cdots < \gamma_n = \alpha$$

は組成列となる。今考えている強連結成分分解はモジュラ束であるため、ジョルダン・ヘルダーの定理 4.9 より、任意の組成列の長さは等しく、組成列の区間を並び替えると対応する区間が射影的になるようにできる。

ここで、$[r, rp]$ の形で表される区間と射影的な区間について考える。まず $[r, rp]$ と $[A, B]$ が転置的だったとする。ひとつのパターンは $r = A \wedge rp, B = A \vee rp$ となる場合である。このとき、$A = rA', rp = rp$ と表されて $B = A \vee rp = rA'p = Ap$ となる。つまり $[A, B] = [A, Ap]$ である。もうひとつのパターンは

$A = r \wedge B, rp = r \vee B$ となる場合である。このとき、$r = Ar', B = AB'$ と表されて $rp = Ar'B' = rB'$ である。よって $p = B'$ であり $[A, B] = [A, Ap]$ となる。つまり、$[r, rp]$ と転置的な区間は $[A, Ap]$ という形をしており、繰り返しても同じなので、$[r, rp]$ と射影的な区間は $[A, Ap]$ という形をしている。

これを既約強連結成分の積への分解における組成列に当てはめると、組成列に現れる区間 $[\gamma_{k-1}, \gamma_k] = [\gamma_{k-1}, \gamma_{k-1}\beta_k]$ と射影的な区間は $[A, A\beta_k]$ という形をしており、既約強連結成分の 1 回の積に対応している。したがって、ジョルダン・ヘルダーの定理の結果は、既約強連結積分の積の形による表現のひとつが

$$\alpha = \beta_1 \cdots \beta_n$$

ならば、ほかに

$$\alpha = \beta'_1 \cdots \beta'_m$$

という形で表現できたときその組成列を $\gamma'_k \equiv \beta'_1 \cdots \beta'_k, \gamma'_0 \equiv [1]$ によって

$$[1] = \gamma'_0 < \gamma'_1 < \cdots < \gamma'_m = \alpha$$

と構成しておくと、$n = m$ となっており、組成列の区間 $[\gamma'_0, \gamma'_0\beta'_1], \cdots, [\gamma'_{n-1}, \gamma'_{n-1}\beta'_n]$ を並び替えたもの

$$[\gamma'_{\sigma(1)-1}, \gamma'_{\sigma(1)-1}\beta'_{\sigma(1)}], \cdots, [\gamma'_{\sigma(n)-1}, \gamma'_{\sigma(n)-1}\beta'_{\sigma(n)}]$$

について、$[\gamma'_{\sigma(k)-1}, \gamma'_{\sigma(k)-1}\beta'_{\sigma(k)}]$ と $[\gamma_{k-1}, \gamma_{k-1}\beta_k]$ が射影的になっている。これはつまり $\beta'_{\sigma(k)} = \beta_k$ を意味しており、既約強連結積分への分解は積の順序を無視すると一意である。

定理 6.38 単項イデアル整域において、同伴による強連結成分分解を考えたとき、任意の強連結成分は既約強連結成分分解の有限の積に表され、その表現は、積の順序を別として、一意である。

6.6.3 素元分解

定義 6.25 （素元）整域 $(R, +, \cdot)$ において、非可逆元 $p \neq 0$ が

$$p|ab \Rightarrow p|a \text{ もしくは } p|b$$

を満たすとき、p は**素元**であるという。◂

定理 6.39 素元は既約元である。

(proof)
整域 $(R, +, \cdot)$ において、p を素元とする。同伴による強連結成分を $\Gamma(R)$ とする。非可逆元なので $[p] \neq [1]$ である。ここで、$\alpha, \beta \in \Gamma(R)$ によって $[p] = \alpha\beta$ と表されるとする。少なくとも $\alpha = [p], \beta = [1]$ によって常にこの形に表すことはできる。$a \in \alpha, b \in \beta$ とすると $p|ab, ab|p$ が成立している。このとき、素元の定義より $p|a$ もしくは $p|b$ が成立している。一般性を失わず $p|a$ とする。$a|ab, ab|p$ より $a|p$ でもあることから $p|a, a|p$ つまり $[p] = \alpha$ である。このとき $p = pub, u \in [1]$ の形で表される。$p \neq 0$ なので $1 = ub, b = u^{-1} \in [1]$ であり $\beta = [1]$ である。よって示された。 証明終

定理 6.40 単項イデアル整域において、既約元は素元である。

(proof)
単項イデアル整域 $(R, +, \cdot)$ において、p を既約元とする。同伴による強連結成分を $\Gamma(R)$ とする。まず既約

元は明らかに 0 ではない。ここで $p|ab$ とする。$[a], [b]$ を定理 6.38 によって一意に既約強連結成分に分解したものを

$$[a] = \alpha_1 \cdots \alpha_n, \quad [b] = \beta_1 \cdots \beta_m$$

とすると、やはり同じ定理により $[ab] = [a][b]$ を分解したものは

$$[ab] = \alpha_1 \cdots \alpha_n \beta_1 \cdots \beta_m$$

である。$p|ab$ なので $[ab] = [p]\gamma, \gamma \in \Gamma(R)$ と表せる。既約強連結成分への分解は一意であるため、$\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m$ のいずれかは $[p]$ と一致しなければならない。よってこのとき $[p]|[a]$ または $[p]|[b]$ が成立している。つまり $p|a$ または $p|b$ である。 証明終

定義 6.26 （**一意分解整域**）整域の 0 でない元が、積の順序と可逆元の積を別とすれば、有限個の素元の積に一意に表されるとき、整域は**一意分解整域**という。このときの素元による分解を**素元分解**という。◂

単項イデアル整域においては、素元と既約元は同じものであることから、定理 6.38 は次のように言い換えられる。

定理 6.41 単項イデアル整域は一意分解整域である。

一意分解整域は、整域であるため、やはり同伴による強連結成分分解を考えることができる。素元は既約強連結成分の代表元であり、一意分解整域では、その [0] でない任意の強連結成分が、有限個の既約強連結成分の積に積の順序を別として一意に表される。このとき、異なる既約強連結成分に添字をつけて $\beta_1 \cdots \beta_n$ とすると [0] でない強連結成分は、非負整数 $m_1, \cdots, m_n$ をつかって

$$\beta_1^{m_1} \cdots \beta_n^{m_n}$$

という形に一意に表せることになる。

定理 6.42 単項イデアル整域 $(R, +, \cdot)$ の素元 p について、イデアル (p) は極大イデアルである。

(proof)
$(p) \subset J$ なるイデアル J を考える。単項イデアル整域なので $J = (m)$ と表される。$p \in (m)$ なので、$m|p$ が満たされる。ところで、p は一意に素元分解されるので $p = mu, u \in [1]$ と表される。このとき $m = pu^{-1} \in (p)$ なので $(m) \subset (p)$ つまり $J = (m) = (p)$ である。 証明終

定理 6.12 より即座に次が得られる。

系 6.43 単項イデアル整域 $(R, +, \cdot)$ の素元 p について、剰余環 $(R/(p), +, \cdot)$ は体である。

定義 6.27 （**一意分解整域の最大公約元・最小公倍元**）一意分解整域 $(R, +, \cdot)$ において、同伴による強連結成分を $\Gamma(R)$ とする。0 でない $a_1, \cdots, a_M \in R$ に対して、異なる既約強連結成分 $\beta_1, \cdots, \beta_M$ によって

$$\begin{aligned} [a_1] &= \beta_1^{m_1(1)} \cdots \beta_n^{m_M(1)} \\ &\vdots \\ [a_n] &= \beta_1^{m_1(n)} \cdots \beta_n^{m_M(n)} \end{aligned}$$

と表したとき

$$\beta_1^{\min(m_1(1), \cdots, m_1(n))} \cdots \beta_n^{\min(m_M(1), \cdots, m_M(n))}$$

を $a_1, \cdots, a_n$ の最大公約強連結成分とよぶこととする。ただし、$\beta_k^0 = [1]$ とする。最大公約強連結成分の元を**最大公約元**といい、$gcd(a_1, \cdots, a_n)$ で表す。また

$$\beta_1^{\max(m_1(1),\cdots,m_1(n))} \cdots \beta_n^{\max(m_M(1),\cdots,m_M(n))}$$

を $a_1, \cdots, a_n$ の最小公倍連結成分とよぶこととする。最小公倍連結成分の元を**最小公倍元**といい、$lcm(a_1, \cdots, a_n)$ で表す。◂

この最大公約元が、単項イデアル整域においては、すでに定義した最大公約元と同じであることを確認しておく。これを示すには $\mathrm{imin}(a_1, \cdots, a_n) = \beta_1^{\min(m_1(1),\cdots,m_M(n))} \cdots \beta_n^{\min(m_M(n),\cdots,m_M(n))}$ を示せばよい。$\gamma \equiv \beta_1^{\min(m_1(1),\cdots,m_M(n))} \cdots \beta_n^{\min(m_M(n),\cdots,m_M(n))}$ とおく。明らかに $\gamma|[a_1], \cdots, \gamma|[a_n]$ なので、$c \in \gamma$ によって

$$a_1 = cd_1, \cdots, a_n = cd_n$$

と表せる。よってイデアル $(a_1, \cdots, a_n)$ の任意の元は c の倍元として表される。これにより $[c]|\mathrm{imin}(a_1, \cdots, a_n)$ であるが、$\mathrm{imin}(a_1, \cdots, a_n)$ はイデアル $(a_1, \cdots, a_n)$ の最小元であるため

$$\beta_1^{\min(m_1(1),\cdots,m_M(n))} \cdots \beta_n^{\min(m_M(n),\cdots,m_M(n))} = \gamma = [c] = \mathrm{imin}(a_1, \cdots, a_n)$$

が成立しなければならない。

基本的な性質としては次のようなものが挙げられる。

定理 6.44

$$gcd(a_1, \cdots, a_n)|a_1, \cdots, gcd(a_1, \cdots, a_n)|a_n$$

定理 6.45

$$gcd(ha_1, \cdots, ha_n) = h\, gcd(a_1, \cdots, a_n)$$

定理 6.46

$$a_1|lcm(a_1, \cdots, a_n), \cdots, a_n|lcm(a_1, \cdots, a_n)$$

定理 6.47

$$ab = gcd(a, b)lcm(a, b)$$

また、定義より、$gcd(a, b) \in [1]$ のときは、a と b には共通する素元がない。これより次の定義を置く。

定義 6.28 （**互いに素**）一意分解整域 $(R, +, \cdot)$ の 0 でない元 $a_1, \cdots, a_n \in R$ が、どの二つをとっても $gcd(a_i, a_j) \in [1], i \neq j$ となるとき、$a_1, \cdots, a_n$ は**互いに素**であるという。◂

互いに素な元はどれをとっても共通する素元がない。よって、例えば次のような性質が成り立つ。

定理 6.48 a, b が互いに素であるとき $gcd(b, ac)$ と $gcd(b, c)$ は同伴である。

6.7 体

体は、その定義から明らかに乗法単位元をもつ可換環である。また、次も成り立っている。

定理 6.49 体は零因子を持たない。つまり体は整域である。

(proof)
体 $(K,+,\cdot)$ の任意の元 $x\neq 0, y\neq 0$ を考える。体の定義より x,y は乗法逆元 x^{-1},y^{-1} を有する。このとき $xy=0$ だったとすると

$$1=(xy)x^{-1}y^{-1}=0$$

が成立する。このとき $x=x1=x0=0$ となって矛盾する。よって $xy\neq 0$ でなければならない。 証明終

整域である体において、同伴による強連結成分分解を考えると、すでに述べたとおり、0 以外の元はすべて可逆であるため、強連結成分が [0] と [1] しかないことになる。そのため、強連結成分分解を考える意味はほとんど無いが、次が自明に成立している。

定理 6.50 体は一意分解整域である。

7 形式的べき級数環・多項式環

7.1 定義

定義 7.1 （形式的べき級数環）$(R,+,\cdot)$ を乗法単位元 1 を持つ可換環とする。R 上の点列の集合 $R[[x]]$ を考える。点列 $\{a_i\},\{b_i\}$ に対して（ただし、i は非負整数とする。）、加法を

$$\{a_i\}+\{b_i\}\equiv\{a_i+b_i\}$$

によって定義し、乗法を

$$\{a_i\}\cdot\{b_i\}\equiv\left\{\sum_{j+k=i}a_j\cdot b_k\right\}$$

によって定義する。

このとき、環の性質より加法は全域で定義された結合的で可換な内算法である。さらに、$\forall i, o_i=0$ なる点列 $\{o_i\}$ が、任意の R 上の点列 $\{a_i\}$ に対して $\{a_i\}+\{o_i\}=\{a_i+0\}=\{a_i\}$ となるため、$\{o_i\}$ が加法単位元となる。これを再び 0 で表す。さらに、任意の R 上の点列 $\{a_i\}$ に対して $\{-a_i\}$ が逆元となる。よって、$(R[[x]],+)$ は可換群である。

乗法については、全域で定義されており

$$\begin{aligned}(\{a_i\}\cdot\{b_i\})\cdot\{c_i\}&=\left\{\sum_{j+k=i}a_j\cdot b_k\right\}\cdot\{c_i\}\\&=\left\{\sum_{l+m=i}\sum_{j+k=m}a_j\cdot b_k\cdot c_l\right\}\\&=\left\{\sum_{k+l+m=i}a_j\cdot b_k\cdot c_l\right\}\\&=\{a_i\}\cdot(\{b_i\}\cdot\{c_i\})\end{aligned}$$

より、結合的である。よって、$(R[[x]],\cdot)$ は半群である。さらに

$$
\begin{aligned}
(\{a_i\}+\{b_i\})\cdot\{c_i\} &= \{a_i+b_i\}\cdot\{c_i\} \\
&= \left\{\sum_{j+k=i}(a_j+b_j)\cdot c_k\right\} \\
&= \left\{\sum_{j+k=i} a_j\cdot c_k + b_j\cdot c_k\right\} \\
&= \left\{\sum_{j+k=i} a_j\cdot c_k\right\} + \left\{\sum_{j+k=i} b_j\cdot c_k\right\} \\
&= \{a_i\}\cdot\{c_i\} + \{b_i\}\cdot\{c_i\}
\end{aligned}
$$

であり、逆から乗法を適用しても同様に成り立つため、分配則が成り立つ。乗法が可換であることも容易に分かる。よって $(R[[x]],+,\cdot)$ は可換環となる。これを**形式的べき級数環**という。形式的べき級数環 $(R[[x]],+,\cdot)$ の元は、$\{a_i\}$ を R の点列として $\sum_i a_i x^i$ のように表される。乗法 $\cdot$ は省略可能とする。各 $a_i x^i$ は項と呼ばれる。$a_i = 0$ なる項は省略可能とする。また、x^0 は省略する。上記の加法と乗法の定義は、普通のべき級数の和と積に対応している。◂

形式的べき級数環は、収束（位相）の議論なしに定義することができる。ただし、環の上では無限和が定義されていないため、x への代入操作は直接的に定義することはできない。それでも、純粋に代数的に形式的べき級数は議論することができる。

ここで、$e_0 = 1, e_i = 0 (i \geq 1)$ なる点列 $\{e_i\}$ を考えれば $\left(\sum_i e_i x^i\right)\left(\sum_i a_i x^i\right) = \sum_i \left(\sum_{j+k=i} e_j \cdot a_k\right) x^i = \sum_i a_i x^i$ より、$\sum_i e_i x^i$ は $R[[x]]$ における乗法単位元である。これは、表記の省略ルールに従い 1 と表される。

定義 7.2 （多項式環）$(R,+,\cdot)$ を可換環とする。$R[x] \equiv \left\{\sum_i a_i x^i : a_i \in R, \exists M, k \geq M, a_k = 0\right\} \subset R[[x]]$ を考えると、定理 *6.8* の条件を満たすため、$(R[[x]],+,\cdot)$ の部分環であるとわかる。これを**多項式環**といい、多項式環の元を**多項式**という。多項式 $f(x) \in R[x]$ は、$f(x) \neq 0$ であるとき、その定義より $a_k \neq 0$ を満たす最大の整数が存在する。これを**次数**といい、$\deg f(x)$ と表す。◂

次数が 0 の多項式の集合は、明らかに部分環をなしており、可換環 $(R,+,\cdot)$ と同型である。加法単位元 0 と乗法単位元 1 はここに属しており、多項式環はもとの可換環を部分環として持っているといえる。これは**定数**と呼ばれる。そこで、形式的べき級数環・多項式環の議論では、もとの可換環は次数が 0 の多項式として扱うものとする。これにより、可換環 R とその形式的べき級数環 $R[[x]]$・多項式環 $R[x]$ との加法・乗法が定義できる。

7.2 形式的べき級数環

定理 7.1 整域の形式的べき級数環は整域である。

(proof)
すでに乗法単位元を持つ可換環の形式的べき級数環が、可換環であり乗法単位元を持つことは示している。もとの可換環が零因子を持たない場合に形式的べき級数環も零因子を持たないことを示せればよい。ここで

$$
\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) = 0
$$

とする。このとき $i = 0, 1, 2, \cdots$ に対して $\sum_{j=0}^{i} a_j b_{i-j} = 0$ が成立している。特に $i = 0$ に対して $a_0 b_0 = 0$ である。零因子を持たないため、$a_0 = 0$ または $b_0 = 0$ は成立している。

まず $a_0 = 0, b_0 \neq 0$ の場合を考える。このとき $i = 1, 2, \cdots$ に対して $\sum_{j=1}^{i} a_j b_{i-j} = 0$ が成立している。特に $i = 1$ に対して $a_1 b_0 = 0$ なので $a_1 = 0$ である。このとき $i = 2, \cdots$ に対して $\sum_{j=2}^{i} a_j b_{i-j} = 0$ が成立している。特に $i = 2$ に対して $a_2 b_0 = 0$ なので $a_2 = 0$ である。以下、同様に繰り返すことにより $\sum_i a_i x^i = 0$ であることがわかる。$a_0 \neq 0, b_0 = 0$ の場合は、上と同様にして $\sum_i b_i x^i = 0$ であることがわかる。

$a_0 = 0, b_0 = 0$ の場合を考えると、$i = 1, 2, \cdots$ に対して $\sum_{j=1}^{i-1} a_j b_{i-j} = 0$ が成立している。これは $\left(\sum_i a_{i+1} x^i\right)\left(\sum_i b_{i+1} x^i\right) = 0$ を意味しており、同じ議論を繰り返すことができる。もし、任意の非負整数 i に対して $a_i = b_i = 0$ ならば、$\sum_i a_i x^i = \sum_i b_i x^i = 0$ である。$a_i \neq 0$ もしくは $b_i \neq 0$ となる元が存在すれば、上の議論に帰結して $\sum_i a_i x^i = 0$ もしくは $\sum_i b_i x^i = 0$ である。よって、もとの可換環が零因子を持たないとき、形式的べき級数環は零因子を持たない。 証明終

系 7.2 整域の多項式環は整域である。

定理 7.3 形式的べき級数 $\sum_i a_i x^i$ が可逆である必要十分条件は a_0 が可逆であることである。

(proof)
$\sum_i a_i x^i$ が可逆であるとする。逆元を $\sum_i b_i x^i$ とすると

$$\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) = 1$$

なので $a_0 b_0 = 1$ が成立している。このとき、b_0 は a_0 の逆元であることから、a_0 は可逆である。

逆に、a_0 が可逆であるとする。このとき、形式的べき級数 $\sum_i b_i x^i$ を

$$b_0 = a_0^{-1}$$
$$b_i = -a_0^{-1} \sum_{k=1}^{i} a_k b_{i-k} \quad i = 2, 3, \cdots$$

と漸化式によって順に定めていくと $\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) = 1$ であり、確かに可逆である。 証明終

形式的べき級数環の中では、逆元は見つけやすい。ただし、この性質は多項式環においては必ずしも成立していない。多項式の逆元が一般には多項式であるとは限らないためである。

定義 7.3 （形式的微分）形式的べき級数 $f(x) = \sum_i a_i x^i$ に対して $f'(x) = \sum_i (i+1) a_{i+1} x^i$ を形式的微分という。ただし、$(i+1) = \sum_{k=1}^{i+1} 1$ とする。◂

形式的微分については、$f(x) = \sum_i a_i x^i,\ g(x) = \sum_i b_i x^i$ に対して

$$\begin{aligned}(f(x)+g(x))' &= \left(\sum_i (a_i + b_i)x^i\right)' \\ &= \sum_i (i+1)(a_{i+1}+b_{i+1})x^i \\ &= \sum_i (i+1)a_{i+1}x^i + \sum_i (i+1)b_{i+1}x^i \\ &= f'(x) + g'(x)\end{aligned}$$

$$\begin{aligned}(f(x)g(x))' &= \left(\sum_i \left(\sum_{j'+k=i} a_{j'}b_k\right)x^i\right)' \\ &= \sum_i \left((i+1)\sum_{j'+k=i+1} a_{j'}b_k\right)x^i \\ &= \sum_i \left((k+j+1)\sum_{j+k=i} a_{j+1}b_k\right)x^i \\ &= \sum_i \left(k\sum_{j+k=i} a_{j+1}b_k\right)x^i + \sum_i \left((j+1)\sum_{j+k=i} a_{j+1}b_k\right)x^i \\ &= \sum_i \left((k+1)\sum_{j+k=i} a_j b_{k+1}\right)x^i + \sum_i \left((j+1)\sum_{j+k=i} a_{j+1}b_k\right)x^i \\ &= f(x)g'(x) + f'(x)g(x)\end{aligned}$$

が成り立っている。

7.3 多項式の基本的性質

多項式は形式的べき級数環の元であるため、形式的べき級数環の性質は基本的には利用できる。さらに多項式については、多項式のみで成立する性質がある。

7.3.1 多項式への代入

多項式に対しては代数的に代入操作が定義できる。

定義 7.4 （代入）$(R,+,\cdot)$ を可換環とする。多項式 $f(x) = \sum_i a_i x^i \in R[x]$ と $\alpha \in R$ について、変数 x を α に置き換えたもの $\sum_i a_i \alpha^i$ は R の元である。これを $f(\alpha)$ で表す。写像 $f(x) \mapsto f(\alpha)$ を適用することを代入するという。◂

代入は、実はもう少し拡張することができる。

定義 7.5 （環の代入）$(R,+,\cdot)$ を乗法単位元を持つ可換環、$(X,+,\cdot)$ を乗法単位元 E をもつ環とする。X に対しては算法 $*: R \times X \to X$ が定義されており、R の加法単位元 0 と $T \in X$ について $0 * T = 0$ が成立するとする。以下、算法 $\cdot, *$ は省略して表記できることとする。このとき、多項式 $f(x) = \sum_i a_i x^i \in R[x]$ と $T \in X$ について、$T^0 = E$ と決めておくと、項 $a_i T^i = a_i * T^i \in X$ であり、$f(x)$ の変数 x を T に置き換えたもの $\sum_i a_i T^i$ は、算法 $*$ の性質により X における有限和であることから X の元である。これを $f(T)$ で表す。写像 $f(x) \mapsto f(T)$ を適用することを代入するという。◂

上の定義において、$(X,+,\cdot)$ 自身が環であることから、$f(T)$ には代数系 $(f(X),+,\cdot,*)$ としての加法と乗法がすでに定義されている。多項式に基づいて議論するためには、代入操作が準同型写像であるべきである。

定理 7.4 $(R,+,\cdot)$ を乗法単位元を持つ可換環、$(X,+,\cdot)$ を乗法単位元 E をもつ環とする。X に対しては算法 $*:R\times X\to X$ が定義されており、次を満たすとする。

1. $x,y\in R$ と $T,S\in X$ について $(x*T)(y*S)=(xy)*(TS)$ が成立する。
2. $x,y\in R$ と $T\in X$ について $(x*T)+(y*T)=(x+y)*T$ が成立する。

このとき、代入を行う写像は準同型写像である。

(proof)
$f(x)\in R[x]$ に $T\in X$ を代入する写像を ϕ で表す。$\sum_i a_i x^i, \sum_i b_i x^i \in R[x]$ とする。

$$\begin{aligned}\phi\left(\sum_i a_i x^i\right)+\phi\left(\sum_i b_i x^i\right)&=\left(\sum_i a_i T^i\right)+\left(\sum_i b_i T^i\right)\\&=\sum_i\left(a_i T^i+b_i T^i\right)\\&=\sum_i\left(a_i+b_i\right)T^i\\&=\phi\left(\sum_i\left(a_i+b_i\right)x^i\right)\end{aligned}$$

であり、また

$$\begin{aligned}\phi\left(\sum_i a_i x^i\right)\phi\left(\sum_j b_j x^j\right)&=\left(\sum_i a_i T^i\right)\left(\sum_j b_j T^j\right)\\&=\sum_i\left(a_i T^i\right)\sum_j\left(b_j T^j\right)\\&=\sum_i\sum_j\left(a_i T^i\right)\left(b_j T^j\right)\quad\because\text{分配則}\\&=\sum_i\sum_j\left(a_i b_j T^{i+j}\right)=\sum_k\sum_{i+j=k}\left(a_i b_j T^k\right)\\&=\sum_k\left(\sum_{i+j=k}a_i b_j\right)T^k\\&=\phi\left(\sum_k\left(\sum_{i+j=k}a_i b_j\right)x^k\right)\end{aligned}$$

となることから、ϕ は準同型写像である。 証明終

$X=R$ であれば、$0*T=0$ および上の定理を満たすことは明らかである。

$X=R[x]$ を考えることもできる。このとき、算法 $*:R\times R[x]\to R[x]$ は、R を $R[x]$ の次数が 0 の多項式とみなすことにより、乗法から定義すればよい。この場合も、$0*T=0$ および上の定理が満たされる。

7.3.2 次数

多項式においては、次数が定義でき、つぎのような性質を持っている。

定理 7.5

$$\deg(f(x)+g(x)) \leq \max(\deg f(x), \deg g(x))$$

定理 7.6

$$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$$

定義 7.6 多項式 $f(x) = \sum_{i=0}^{\deg f(x)} a_i x^i$ について、a_0 を**定数項**といい、$a_{\deg f(x)}$ を**最高次の係数**という。最高次の係数が乗法単位元のとき、**モニック**な多項式であるという。◂

7.3.3 整除

まず、容易に次が分かる。

補題 7.7 $\deg f(x) \geq \deg g(x)$ で $g(x)$ がモニックな多項式であるとき、$f(x)$ の最高次の係数を a とすると

$$F(x) = f(x) - ax^{(\deg f(x) - \deg g(x))} g(x), \quad \deg F(x) \leq \deg f(x) - 1$$

なる多項式 $F(x)$ が存在する。

$f(x)$ に上の補題を適用したものを $f_1(x)$ とし、以下 $f_k(x)$ に上の補題を適用したものを $f_{k+1}(x)$ とすると、$\deg f_n(x) < \deg g(x)$ となるまで繰り返し適用が可能であり

$$f_n(x) = f_{n-1}(x) - b_0 g(x) = f_{n-2}(x) - (b_0 + b_1 x)g(x) = f(x) - q(x)g(x)$$

のような形で表せる。このような操作は**整除**と呼ばれている。$q(x)$ は商、$f_n(x)$ は剰余（余り）などといわれる。この場合、操作の方法により商と剰余は一意に定まる。

補題 7.8 多項式 $f(x), g(x)$ について $g(x)$ がモニックな多項式であるとき

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x) \text{ もしくは } r(x) = 0$$

となる多項式 $q(x), r(x)$ が一意に存在する。

(proof)
$\deg f(x) \geq \deg g(x)$ の場合については、うえに記したとおりである。$\deg f(x) < \deg g(x)$ の場合は、多項式の範囲では何を乗じても $f(x)$ にならないため、一意に $q(x) = 0, r(x) = f(x)$ によって条件が満たされる。 証明終

ただちに、これは次のように拡張できる。

定理 7.9 多項式 $f(x), g(x)$ について $g(x)$ の最高次の係数が可逆であるとき

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x) \text{ もしくは } r(x) = 0$$

となる多項式 $q(x), r(x)$ が一意に存在する。

これから、次が成立する。

定理 7.10 体の多項式はユークリッド整域である。

(proof)
体は整域でもあるので、体の多項式環は整域である。また、定理 7.5 および直前の定理より次数 deg を持ってユークリッド整域の条件を満たしている。 証明終

したがって、体の多項式環は単項イデアル整域・一意分解整域でもある。

整除に関しては次のような基本的な性質が成り立つ。

定理 7.11 （剰余定理）$(R,+,\cdot)$ を乗法単位元を持つ可換環とし、$a \in R$ とする。このとき、R の多項式 $f(x)$ を $x-a$ で整除した剰余は $f(a)$ に等しい。

(proof)
$f(x) = q(x)(x-a) + r(x)$ と表されているが、$r(x) = 0$ もしくは $\deg r(x) < \deg(x-1) = 0$ なので $r(x)$ は定数である。この定数を r' とすると $f(x) = q(x)(x-a) + r'$ である。$x = a$ を代入すると $f(a) = r'$ が成立する。つまり $r(x) = f(a)$ である。 証明終

系 7.12 （因数定理）$(R,+,\cdot)$ を乗法単位元を持つ可換環とし、$a \in R$ とする。このとき、R の多項式 $f(x)$ が $x-a$ の倍元であるための必要十分条件は $f(a) = 0$ である。

7.4 整域の多項式

零因子を持たないという条件を追加した整域の多項式を考える。すでに見たとおり整域の多項式環は整域である。また、乗法における次数の不等式が等号で成り立つ。

定理 7.13

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$

系 7.14 整域の多項式環において、可逆元は可逆な定数項である。

整域の多項式では、いわゆる多項式の解について重要な性質が成り立つ。

定義 7.7 （解）整域 $(R,+,\cdot)$ とその多項式 $f(x)$ について、$f(a) = 0$ なる $a \in R$ を多項式の**解**という。また、$f(x) = (x-a)^2 g(x)$ と表されるとき、a は $f(x)$ の**重解**であるという。◂

定理 7.15 整域の多項式の異なる解の個数はその多項式の次数以下である。

(proof)
$(R,+,\cdot)$ を整域とし $f(x)$ をその多項式、$a_1, \cdots, a_m$ をその異なる解とする。因数定理より $f(x)$ は $(x-a_1)$ の倍元であるから $f(x) = (x-a_1)g_1(x)$ と表せる。このとき $f(a_2) = (a_2-a_1)g_1(a_2) = 0$ より $g_1(a_2) = 0$ である。よって $g_1(x) = (x-a_2)g_2(x)$ と表せる。これを繰り返すと

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_m)g_m(x)$$

と表せる。このとき、整域なので次数に関して

$$\deg f(x) = m + \deg g_m(x) \geq m$$

であり、確かに異なる解の個数 m は多項式の次数以下である。 証明終

定理 7.16 整域の多項式 $f(x)$ が重解 a を持つ必要十分条件は $f(a) = f'(a) = 0$ である。

(proof)
$f(x)$ が重解 a を持つとする。このとき $f(x) = (x-a)^2 g(x)$ と表される。このとき $f(a) = 0$ は明らかに成り立っている。$f'(x) = (2x-2a)g(x) + (x-a)^2 g'(x)$ であるため、$f'(a) = 0$ も成立する。逆に、$f(a) = f'(a) = 0$ とする。因数定理より $f(x) = (x-a)h(x)$ と表せる。このとき $f'(x) = h(x) + (x-a)h'(x)$ なので $f'(a) = 0$ より $f'(a) = h(a) = 0$ であり、因数定理より $h(a) = (x-a)g(x)$ と表せる。よって $f(x) = (x-a)^2 g(x)$ と表せ、重解 a を持っている。 証明終

7.4.1 一意分解整域の多項式

定義 7.8 （**原始多項式**）一意分解整域 $(R, +, \cdot)$ の多項式 $\sum_{i=0}^{D} a_i x^i$ に対して、$gcd(a_0, \cdots, a_D)$ を**容量**という。容量が $[1]$ に属する多項式を**原始多項式**という。◂

一意分解整域の任意の多項式 $f(x)$ について、容量 d と原始多項式 $h(x)$ によって $f(x) = dh(x)$ と表せる。

定理 7.17 一意分解整域 $(R, +, \cdot)$ の原始多項式 $f(x), g(x)$ について $af(x) = b\,g(x), a, b \in R$ が成り立つならば a と b は同伴である。

(proof)
$f(x) = \sum_{i=0}^{D} F_i x^i,\ g(x) = \sum_{i=0}^{D} G_i x^i$ とすると $\sum_{i=0}^{D} aF_i x^i = \sum_{i=0}^{D} bG_i x^i$ が成立している。このとき

$$\begin{aligned} a\ gcd(F_1, \cdots, F_D) &= gcd(aF_1, \cdots, aF_D) = gcd(bG_1, \cdots, bG_D) \\ &= b\ gcd(G_1, \cdots, G_D) \end{aligned}$$

であり、原始多項式であることより $gcd(F_1, \cdots, F_D), gcd(G_1, \cdots, G_D) \in [1]$ なので a と b は同伴である。 証明終

定理 7.18 一意分解整域の原始多項式の積は原始多項式である。

(proof)
原始多項式 $f(x), g(x)$ の積 $f(x)g(x)$ が原始多項式で無いとすると、ある素元 p が存在して $f(x)g(x)$ のすべての係数が p の倍元である。しかし、$f(x), g(x)$ は原始多項式なので、それぞれの係数のすべてが p の倍元ということはない。このとき、$f(x), g(x)$ において係数が p の倍元でない最小の次数を r, s とする。$f(x) = \sum_{i=0}^{D} a_i x^i, g(x) = \sum_{i=0}^{D} b_i x^i$ と表されるならば $f(x)g(x)$ の x^{r+s} の項の係数は

$$a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_r b_r + \cdots + a_{r+s} b_0$$

であり、これも p の倍元である。$a_r b_r$ 以外はすべて p の倍元なので、$a_r b_r$ も p の倍元となり、矛盾する。よって $f(x)g(x)$ は原始多項式である。 証明終

一意分解整域 $(R, +, \cdot)$ の多項式については、R 可逆化した分数体（商体）K を考えることが有効である。分数体 K の中で R に相当する部分を再び $R(\subset K)$ で表すとする。

補題 7.19 一意分解整域 $(R, +, \cdot)$ の分数体を K とする。このとき任意の $f(x) \in K[x]$ に対してある $r \in R$ によって $r(x) \in R[x]$ と表せる。

(proof)

$f(x)=0$ なら明らかである。$f(x)=\sum_{i=0}^{D} c_i x^i, D\geq 0$ とする。$c_i\in K$ は $a_i\in R, b_i\in R-\{0\}$ により $c_i=\frac{a_i}{b_i}$ と表せる。ここで、$r=lcm(b_0,\cdots,b_D)$ とすると $r=b_i d_i, d_i\in R$ の形で表すことができ

$$rf(x)=\sum_{i=0}^{D}(a_i d_i)x^i$$

となる。このとき $a_i, d_i\in R$ なので $a_i d_i\in R$ であり $rf(x)\in R[x]$ である。 証明終

すでに見たとおり、体の多項式は一意分解整域である。そこで、$f(x)\in R[x]$ に対して $K[x]$ の中では、積の順序と K の定数倍を別として一意に分解することができる。このときの分解の表現において、それぞれの素元は K の定数倍についてはどれをとってもよいため、上の補題を満たす $R(\subset K)$ の定数倍をしておくことによって

$$f(x)=d\,g_1(x)\cdots g_m(x),\ d\in R, g_i(x)\in R[x], \deg g_i(x)\geq 1$$

という形に、R の定数倍と積の順序を別として一意に分解することができる。さらに、容量を d に集約することにより、各 $g_i(x)$ を原始多項式に限定することもできる。このとき、上の補題より $g_1(x)\cdots g_m(x)$ の部分は積の順序と可逆元の積を別として一意である。

また $g_i(x)$ は $K[x]$ の素元であり、非可逆元 $a(x), b(x)\in K[x]$ に対して「$g_i(x)|a(x), b(x)\ \Rightarrow\ p|a(x)$ もしくは $p|b(x)$」が成り立っている。$K[x]$ においては、定数項 $(\neq 0)$ が可逆元のすべてである。よって次数が 1 以上の $a(x), b(x)\in R[x]\subset K[x]$ に対しては「$g_i(x)|a(x), b(x)\Rightarrow p|a(x)$ もしくは $p|b(x)$」が成立する。$R[x]$ においては、定数項にも非可逆元があるため、$a(x)$ か $b(x)$ の片方が非可逆な定数項の場合に $g_i(x)|a(x)b(x)$ が成立することがある。一般性を失わず $a\in R$ が非可逆な定数項であるとする。このとき $ab(x)=g_i(x)c(x), c(x)\in R[x]$ となっている。$b(x), c(x)$ の容量を b', c' とすると、$B(x), C(x)$ を原始多項式として $(ab')B(x)=(c')(g_i(x)C(x))$ と表せる。$g_i(x), C(x)$ が原始多項式なので $g_i(x)C(x)$ も原始多項式である。よって上の定理 7.17 より ab' と c' が同伴であり、$c'=ab'u, u\in[1]$ と表せる。このとき $B(x)=ug_i(x)C(x)$ であり $b(x)=b'ug_i(x)C(x)$ より $g_i(x)|b(x)$ が成立している。以上より、$g_i(x)\in R[x]$ は素元である。まとめると、$g_1(x)\cdots g_m(x)$ の部分は積の順序と可逆元の積を別として素元により一意に分解されている。

残りは $d\in R$ の部分である。R は一意分解整域を考えているので、d も当然素元の積に積の順序と可逆元の積を別として一意に分解できる。よって、$f(x)=d\,g_1(x)\cdots g_m(x)$ がすべて積の順序と可逆元の積を別として素元により一意に分解されることになる。

定理 7.20 一意分解整域の多項式環は一意分解整域である。

8 多変数の多項式

8.1 多変数多項式環

定義 8.1 （多変数多項式環）多項式環 $R[x]$ に対して、その多項式環 $(R[x])[y]$ を考えることができる。これを $R[x,y]$ と表す。同様に繰り返すことにより、多変数多項式環 $R[x_1,\cdots,x_n]$ を定義できる。◂

整域の多項式環は整域なので、整域の多変数多項式環も整域である。また、一意分解整域の多項式環は一意分解整域なので、一意分解整域の多変数多項式環も一意分解整域である。しかし、体の多項式環はユークリッド整域であるが体ではないため、体の多変数多項式環は一意分解整域であるということまでしかいえない。（単項イデアル整域であるとも限らない。）

定義 8.2 （**単項式**）多変数多項式において、変数の積 $x_1^{a_1}\cdots x_n^{a_n}$ を**単項式**という。単項式の変数の数 $a_1+\cdots+a_n$ を**次数**という。多変数多項式の次数もやはり有限である。一般に、多変数多項式は、単項式にもとの環（係数）を乗じたものの和の形をしている。次数が 0 の項はやはり定数項と呼ばれる。◂

定理 8.1 （***Dickson* の補題**）整域の多項式において、約元・倍元の関係に基づく半順序を考えるとき、単項式の集合 $M\neq\emptyset$ の極小元は有限個である。

(proof)
まず 1 変数の場合を考える。このとき、単項式のすべては $1, x, x^2, x^3, \cdots$ と非負整数に対応しており、1 変数単項式から非負整数への写像 $\phi(x^n)=n$ は順序同型写像である。よって $\phi(M)$ は非負整数の集合であり、最小元がひとつ存在する。このとき、最小元に対応する単項式を考えると、M の最小元であり、唯一の極小元である。

n 変数までは定理が証明されているとする。多項式環 $R[x_1,\cdots,x_n,y]$ を考える。$x_1,\cdots,x_n$ の単項式の集合 $N\equiv\{u : uy^b\in M\}$ をとると、仮定より N の極小元は有限である。これを $s_1,\cdots,s_k$ とする。N の任意の元 u について少なくとも $u|u$ は成立しているため、$s_1|u,\cdots,s_k|u$ のいずれかは成立している。また、s_i に対して $s_iy^b\in M$ を満たすある非負整数 b が存在する。このうちのひとつを b_i とし、$B\equiv\max(b_1,\cdots,b_k)$ とする。任意の M の元は $uy^m, u\in N$ と表される。$B\leq m$ の場合は $y^{b_1}|y^m,\cdots,y^{b_k}|y^m$ が成立しているため、$uy^m\in M$ は $s_1y^{b_1},\cdots,s_ky^{b_k}$ のいずれかの倍元である。$m<B$ の場合を考える。$N_m\equiv\{u : uy^m\in M\}\subset N$ を考えると、仮定より極小元が有限であるのでこれを $v_1(m),\cdots,v_{K(m)}(m)$ とする。このとき $uy^m\in M$ は $v_1(m)y^m,\cdots,v_{K(m)}(m)y^m$ のいずれかの倍元である。以上より、任意の M の元 $uy^m, u\in N$ について、

$$
\begin{gathered}
s_1y^{b_1},\cdots,s_ky^{b_k}\\
v_1(0),\cdots,v_{K(0)}(0)\\
v_1(1)y,\cdots,v_{K(1)}(0)y\\
\vdots\\
v_1(B-1)y^{B-1},\cdots,v_{K(B-1)}(B-1)y^{B-1}
\end{gathered}
$$

のいずれかの倍元である。M の極小元はこの部分集合である必要があるため、M の極小元は有限個である。よって、数学的帰納法より定理が示される。 証明終

定理 8.2 （***Hilbert* 基底定理**）整域の多変数多項式環 $R[x_1,\cdots,x_n]$ のイデアル I について、有限の単項式 $u_1,\cdots,u_N$ が存在して

$$I=(u_1,\cdots,u_N)$$

である。

(proof)
イデアル I に含まれる単項式すべての集合を M とすると、Dickson の補題より M の極小元は有限個である。それらを $\{u_1,\cdots,u_N\}$ とすると、任意の $x\in M$ について $\exists u_k, u_k|x$ が成立する。つまり、$x=u_ky, y\in M$ と表せる。多変数多項式は、単項式に係数（環）を乗じたものの有限和の形をしており、任意の多変数多項式は有限和 $c_1e_1+\cdots+c_me_m,\ c_i\in R, e_j\in M$ の形に表せることから、単項式に生成されるイデアルによって $I=(u_1,\cdots,u_N)$ の形に表せる。 証明終

系 8.3 多変数多項式環 $R[x_1,\cdots,x_n]$ について、有限の単項式 $u_1,\cdots,u_N$ が存在して

$$R[x_1,\cdots,x_n]=(u_1,\cdots,u_N)$$

である。

8.2 グレブナー基底

定義 8.3 （**単項式順序**）n 変数の単項式の集合 $\mathcal{M}_n$ に対して全順序 $\leq$ が

$$u \in \mathcal{M}_n,\ 1 \leq u \text{ 等号条件は } u = 1$$
$$u \leq v \in \mathcal{M}_n \ \Rightarrow\ \forall w \in \mathcal{M}_n, uw \leq vw \text{ 等号条件は } u = v$$

を満たすとき、全順序 $\leq$ を**単項式順序**という。

変数に適当な順序をつけてその順に $x_1, \cdots, x_n$ のように添字を割り当てておく。単項式を $x_1^{a_1} \cdots x_n^{a_n}$ の形に表したとき、まず次数 a_1 の大小で順序を決め、次数 a_1 が等しい場合は次数 a_2 の大小で順序を決め、以下次数 a_k が等しい場合は次数 a_{k+1} の大小で順序を決めるという規則で定める順序を**辞書式順序**という。辞書式順序は単項式順序である。◂

明らかに次が成立する。

定理 8.4 単項式順序 $\leq$ について、$u|v$ ならば $u \leq v$ である。

次は単項式順序について重要な性質である。

定理 8.5 単項式順序についての減少列

$$f_0 > f_1 > \cdots$$

は高々有限個である。

(proof)
$M \equiv \{f_0, f_1, \cdots\}$ とする。Dickson の補題（定理 8.1）より M は有限個の極小元 $e_0, \cdots, e_s$ をもつ。M の任意の元 x は少なくとも自分自身によって $x|x$ となることから、ある極小元 e_k が存在して $e_k|x$ が成立する。このとき、上の定理より $e_k \leq x$ である。したがって、$e_0, \cdots, e_s$ の単項式順序による最小元 e' をとると任意の $x \in M$ について $e' \leq x$ が成立する。したがって、$f_0 > f_1 > \cdots$ が無限列であるとすると、$e' > y$ なる y が存在することになり矛盾する。よって M は高々有限個である。 証明終

定義 8.4 （**主項**）多項式のそれぞれの単項式のうち、単項式順序が最大の項を**主項**といい、多項式 f の主項を $\mathrm{in}_<(f)$ であらわす。主項の次元を多項式の次元といい、$\deg f$ で表す。◂

定義 8.5 （**イニシャルイデアル**）多項式環 $R[x_1, \cdots, x_n]$ のイデアル $I \neq \{0\}$ において、その主項の集合 $\{\mathrm{in}_<(f) : f \in I\}$ の有限和がなすイデアル $\mathrm{in}_<(I) \equiv \left\{ \sum_j g_j(x) f_j(x) : f_j(x) \in \{\mathrm{in}_<(f) : f \in I\}, g_j(x) \in R[x_1, \cdots, x_n] \right\}$ をイニシャルイデアルという。◂

定理 8.6 $\mathrm{in}_<(fg) = \mathrm{in}_<(f)\mathrm{in}_<(g)$ 特に g が単項式なら $\mathrm{in}_<(fg) = \mathrm{in}_<(f)g$

定義 8.6 （**グレブナー基底**）体の多項式環 $K[x_1, \cdots, x_n]$ のイデアル $I \neq \{0\}$ において、有限個の多項式の集合 $\{g_1, \cdots, g_s\} \subset I$ が

$$\mathrm{in}_<(I) = (\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$$

を満たすとき、$\{g_1, \cdots, g_s\}$ は**グレブナー基底**という。◂

定理 8.7 体の多項式環 $K[x_1,\cdots,x_n]$ において、$\{g_1,\cdots,g_s\}$ がイデアル $I\neq\{0\}$ のグレブナー基底である場合、$I=(g_1,\cdots,g_s)$ である。つまり、グレブナー基底からもとのイデアルが生成される。

(proof)

$\forall f\in I$ について。$f=0$ ならば $f\in(g_1,\cdots,g_s)$ は自明である。$f\neq 0$ のときは、$\mathrm{in}_<(f)\in\mathrm{in}_<(I)=(\mathrm{in}_<(g_1),\cdots,\mathrm{in}_<(g_s))$ である。$\mathrm{in}_<(f)$ は単項式であるので、単項式 w が存在して $\mathrm{in}_<(f)=w\,\mathrm{in}_<(g_k)$ が成立しなければならない。このとき $\mathrm{in}_<(f)=w\,\mathrm{in}_<(g_k)=\mathrm{in}_<(w\,g_k)$ である。f,g_k の主項の係数を c,d_k とし、$f_1\equiv d_k\,f-cg_k$ とすると、$f_1=0$ もしくは $f>f_1$ が成立する。$f_1=0$ のときは $f=(d_k^{-1}c)g_k\in(g_1,\cdots,g_s)$ である。$f_1\neq 0$ のときは $f>f_1$ となっている。f_1 について同様の処理を行うことができ、繰り返したものを $f_2,f_3,\cdots$ とする。どこがで $f_k=0$ となれば、$f_1,\cdots,f_k$ の構成法より $f\in(g_1,\cdots,g_s)$ であることがわかる。$f_k=0$ となる f_k が存在しない場合は

$$f>f_1>f_2>\cdots$$

という狭義減少する無限列が構成できる。しかし、定理 8.5 よりこのような無限列は構成できない。よって、かならず $f_k=0$ となる f_k が存在し、$f\in(g_1,\cdots,g_s)$ が成立する。よって $I\subset(g_1,\cdots,g_s)$ である。$g_1,\cdots,g_s\in I$ なので $I\supset(g_1,\cdots,g_s)$ も成立しているので、$I=(g_1,\cdots,g_s)$ である。 証明終

定義 8.7 （**標準表示**）多変数多項式環を考える。多項式 f と多項式 $g_1,\cdots,g_s$ に対して

$$f=f_1g_1+\cdots+f_sg_s+r$$
$$r=0\ or\ r\text{ を構成する任意の単項式がイデアル }(\mathrm{in}_<(g_1),\cdots,\mathrm{in}_<(g_s))\text{ に属さない}$$

を満たす $f_1,\cdots,f_s,r$ が存在する。これを f の $g_1,\cdots,g_s$ に関する**標準表示**という。また、このとき r を f の $g_1,\cdots,g_s$ に関する**余り**という。◂

標準表示については、次のように考えることができる。まず $r_0=f$ から始める。r_0 を構成する単項式のすべてがイデアル $J\equiv(\mathrm{in}_<(g_1),\cdots,\mathrm{in}_<(g_s))$ に属さなければ、$r=r_0=f$ と $f_1=\cdots=f_s=0$ によって標準表示が得られる。ここで、r_0 を構成する単項式のうちイデアル J に属するものの集合を R_0 とし、R_0 における単項式順序についての最大元を u_0 とする。このとき u_0 は多項式 h_0 によって $u_0=h_0\mathrm{in}_<(g_{\sigma(0)})$ という形に表せる。u_0 の係数を c_0 とすると、$r_1\equiv r_0-c_0h_0g_{\sigma(0)}$ は単項式 u_0 を含まない。ここで、r_1 を構成する単項式のうちイデアル J に属するものの集合を R_1 とし、R_1 における単項式順序についての最大元を u_1 とする。$h_0g_{\sigma(0)}$ に属する単項式 $z\neq\mathrm{in}_<(g_{\sigma(0)})$ は単項式順序を $\leq$ とすると、$z<h_0\mathrm{in}_<(g_{\sigma(0)})=u_0$ を満たしており

$$R_1=(R_0-\{u_0\})\cup\{z\neq\mathrm{in}_<(g_{\sigma(0)}):z\text{ は }h_0g_{\sigma(0)}\text{に属する単項式}\}$$

なので、R_1 の最大元たる u_1 については $u_1<u_0$ を満たしている。同様の処理を繰り返していくと、単項式の列 $u_0>u_1>\cdots$ を構成することができる。Dickson の補題より、これには有限個の極小元が存在する。したがって、$u_0>u_1>\cdots$ が無限の列であるとすると、定理 8.5 に矛盾するため、どこがで R_s が空集合となる。このとき、r_s について $r_s=0$ または r_s を構成する任意の単項式がイデアル J に属していない。また、$f=r_0=\sum_j c_jh_jg_{\sigma(j)}+r_s$ であることから、標準表示が得られていることになる。一般的には余りは一意には定まらないことが知られている。しかし、グレブナー基底による余りは一意に定まる。

定理 8.8 体の多項式のグレブナー基底に関する余りは一意に定まる。

(proof)

多項式 f がイデアル I のグレブナー基底 $g_1,\cdots,g_s$ によって次のとおり 2 通りの標準表示に表されたとする。

$$
\begin{aligned}
f &= f_1 g_1 + \cdots + f_s g_s + r \\
&= f'_1 g_1 + \cdots + f'_s g_s + r'
\end{aligned}
$$

このとき、$r - r' \in (g_1, \cdots, g_s) = I$ である。標準表示の定義より、r, r' を構成する任意の単項式がイデアル $(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ に属さないので、$r - r'$ の主項 $\mathrm{in}_<(r - r')$ もイデアル $(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s)) = \mathrm{in}_<(I)$ には属さない。しかし $r - r'$ はイデアル I に属しているので、その主項 $\mathrm{in}_<(r - r')$ はイニシャルイデアル $\mathrm{in}_<(I)$ に属さなければならない。したがって、$\mathrm{in}_<(r - r') = 0$ つまり $r - r' = 0$ でなければ矛盾する。つまり余りは一意である。 証明終

このことから、イデアルに属するかどうかはグレブナー基底による余りを求めればよい。

系 8.9 多項式がイデアル I に属することと、多項式の I のグレブナー基底による余りが 0 であることは同値である。

8.2.1 Buchberger アルゴリズム

ここでは、多項式は体の多変数多項式を考える。Hilbert 基底定理より、任意のイデアル I が有限の単項式 $u_1, \cdots, u_s$ によって、$I = (u_1, \cdots, u_s)$ と表現できる。このとき $u_1, \cdots, u_s$ をイデアルの生成系といい、生成系が有限個であることを有限生成であるなどという。Buchberger アルゴリズムは、イデアルの生成系からグレブナー基底を構成するアルゴリズムである。

定義 8.8 （***S* 多項式**）多項式 f, g の主項 $\mathrm{in}_<(f), \mathrm{in}_<(g)$ を、最小公約多項式 $gcd(\mathrm{in}_<(f), \mathrm{in}_<(g))$ によって $\mathrm{in}_<(f) = F\ gcd(\mathrm{in}_<(f), \mathrm{in}_<(g)),\ \mathrm{in}_<(g) = G\ gcd(\mathrm{in}_<(f), \mathrm{in}_<(g))$ と互いに素な単項式 F, G によって表しておくとき、f, g のおける $\mathrm{in}_<(f), \mathrm{in}_<(g)$ の係数を a, b とすると

$$
S(f, g) \equiv a^{-1} G f - b^{-1} F g
$$

を **S 多項式**という。◂

S 多項式は、互いの主項を打ち消した多項式である。上において、$lcm(\mathrm{in}_<(f), \mathrm{in}_<(g)) = FG\ gcd(\mathrm{in}_<(f), \mathrm{in}_<(g))$ なので

$$
F = \frac{lcm(\mathrm{in}_<(f), \mathrm{in}_<(g))}{\mathrm{in}_<(g)}, \quad G = \frac{lcm(\mathrm{in}_<(f), \mathrm{in}_<(g))}{\mathrm{in}_<(f)}
$$

と表記することにすれば、次のようにも表せる [9]。

$$
S(f, g) \equiv \frac{lcm(\mathrm{in}_<(f), \mathrm{in}_<(g))}{\mathrm{in}_<(f)} a^{-1} f - \frac{lcm(\mathrm{in}_<(f), \mathrm{in}_<(g))}{\mathrm{in}_<(g)} b^{-1} g
$$

主項が等しい場合は次のようになる。

$$
S(f, g) \equiv a^{-1} f - b^{-1} g
$$

補題 8.10 体 K の多項式 $f_1, \cdots, f_s$ の主項がすべて単項式 w であり $g = \sum_{i=1}^{s} b_i f_i$ が $\mathrm{in}_<(g) < w$ を満たすならば

$$
g = \sum_{i,j}^{s} c_{ij} S(f_i, f_j), \quad c_{ij} \in K
$$

という表現が可能である。

[9] 商体（分数体）を考えていることに相当する。

(proof)

f_i の主項の係数を c_i とすると、$\sum_{i=1}^{s} b_i c_i = 0$ が必要である。また、$f_1, \cdots, f_s$ の主項がすべて等しいので、$g_i \equiv c_i^{-1} f_i$ とおくと

$$S(f_i, f_j) = g_i - g_j$$

である。これより

$$\begin{aligned} g &= \sum_{i=1}^{s} b_i f_i \\ &= \sum_{i=1}^{s} b_i c_i g_i \\ &= (b_1 c_1)(g_1 - g_2) + (b_1 c_1 + b_2 c_2)(g_2 - g_3) + \cdots + (b_1 c_1 + \cdots + b_{s-1} c_{s-1})(g_{s-1} - g_s) + (b_1 c_1 + \cdots + b_s c_s) g_s \\ &= (b_1 c_1) S(f_1, f_2) + (b_1 c_1 + b_2 c_2) S(f_2, f_3) + \cdots + (b_1 c_1 + \cdots + b_{s-1} c_{s-1}) S(f_{s-1}, f_s) \end{aligned}$$

となり、示される。 証明終

定理 8.11 （***Buchberger*** **判定法**）体の多変数多項式環のイデアル I について $I = (g_1, \cdots, g_s)$ であるとする。$g_1, \cdots, g_s$ がグレブナー基底であることと、任意の $i \neq j$ について $S(g_i, g_j)$ の $g_1, \cdots, g_s$ に関する余りを 0 にできることは、同値である。

(proof)

$g_1, \cdots, g_s$ がグレブナー基底であるとき、$S(g_i, g_j) \in I$ なので、$S(g_i, g_j)$ の $g_1, \cdots, g_s$ に関する余りは 0 となり、必要性は証明される。

十分性を考える。任意の $f(\neq 0) \in I = (g_1, \cdots, g_s)$ は $f = \sum_{i=1}^{s} h_i g_i$ と表すことができる。このとき、各 $i = 1, \cdots, s$ について $h_i g_i$ の主項 $\mathrm{in}_<(h_i g_i)$ のうち、単項式順序による最大元を $\delta(h_1, \cdots, h_s)$ とすると、f の主項と一致するか、係数の合計が 0 となって $\delta(h_1, \cdots, h_s)$ が消去されるかなので、単項式順序に関して $\mathrm{in}_<(f) \leq \delta(h_1, \cdots, h_s)$ が成立している。ここで、可能な $h_1, \cdots, h_s$ による $\delta(h_1, \cdots, h_s)$ のなす集合 M を考えると、M は単項式のなす集合なので Dickson の補題より M は有限の極小元を有する。この有限の極小元のうち単項式順序についての最小元 δ_f をとると、δ_f は M の最小元である。また、$\mathrm{in}_<(f) \leq \delta_f$ が成立している。以下では δ_f に対応する $h_1, \cdots, h_s$ を考えるものとする。h_i を主項とそれ以外に $h_i = c_i \mathrm{in}_<(h_i) + h_j'$ と分解しておく。

$$\begin{aligned} f &= \sum_{i=1}^{s} h_i g_i \\ &= \sum_{\mathrm{in}_<(h_i g_i) < \delta_f} h_i g_i + \sum_{\mathrm{in}_<(h_i g_i) = \delta_f} h_i g_i \\ &= \sum_{\mathrm{in}_<(h_i g_i) < \delta_f} h_i g_i + \sum_{\mathrm{in}_<(h_i g_i) = \delta_f} \mathrm{in}_<(h_i) g_i + \sum_{\mathrm{in}_<(h_i g_i) = \delta_f} h_i' g_i \end{aligned}$$

$$f - \sum_{\mathrm{in}_<(h_i g_i) < \delta_f} h_i g_i - \sum_{\mathrm{in}_<(h_i g_i) = \delta_f} h_i' g_i = \sum_{\mathrm{in}_<(h_i g_i) = \delta_f} \mathrm{in}_<(h_i) g_i$$

と変形しておく。

ここで $\mathrm{in}_<(f) < \delta_f$ を仮定する。このとき (左辺の主項) $< \delta_f$ が成立しており、右辺の主項はすべて δ_f なので、直前の補題より

$$f - \sum_{\mathrm{in}_<(h_ig_i)<\delta_f} h_ig_i - \sum_{\mathrm{in}_<(h_ig_i)=\delta_f} h'_ig_i = \sum_{\mathrm{in}_<(h_ig_i)=\delta_f} \mathrm{in}_<(h_i)g_i = \sum_{\mathrm{in}_<(h_ig_i)=\mathrm{in}_<(h_jg_j)=\delta_f} c_{ij}S(\mathrm{in}_<(h_i)g_i, \mathrm{in}_<(h_j)g_j)$$

と表せる。g_i の主項の係数を b_i とする。最右辺においては主項は δ_f で共通しているため $S(\mathrm{in}_<(h_i)g_i, \mathrm{in}_<(h_j)g_j) = b_i^{-1}\mathrm{in}_<(h_i)g_i - b_j^{-1}\mathrm{in}_<(h_j)g_j$ である。また、各 $\mathrm{in}_<(g_i)$ について $\mathrm{in}_<(g_i)|\delta_f$ であるので、$\delta_f = u_{ij}lcm(\mathrm{in}_<(g_i), \mathrm{in}_<(g_j))$ と表せる。このとき、$\mathrm{in}_<(h_ig_i) = \mathrm{in}_<(h_jg_j) = \delta_f$ が成り立つ $i \neq j$ について

$$\begin{aligned}
u_{ij}S(g_i, g_j) &= \frac{u_{ij}\ lcm(\mathrm{in}_<(g_i), \mathrm{in}_<(g_j))}{\mathrm{in}_<(g_i)}b_i^{-1}g_i - \frac{u_{ij}\ lcm(\mathrm{in}_<(g_i), \mathrm{in}_<(g_j))}{\mathrm{in}_<(g_j)}b_j^{-1}g_j \\
&= \frac{\delta_f}{\mathrm{in}_<(g_i)}b_i^{-1}g_i - \frac{\delta_f}{\mathrm{in}_<(g_j)}b_j^{-1}g_j \\
&= \frac{\mathrm{in}_<(h_ig_i)}{\mathrm{in}_<(g_i)}b_i^{-1}g_i - \frac{\mathrm{in}_<(h_jg_j)}{\mathrm{in}_<(g_j)}b_j^{-1}g_j \\
&= \frac{\mathrm{in}_<(h_i)\mathrm{in}_<(g_i)}{\mathrm{in}_<(g_i)}b_i^{-1}g_i - \frac{\mathrm{in}_<(h_j)\mathrm{in}_<(g_j)}{\mathrm{in}_<(g_j)}b_j^{-1}g_j \\
&= \mathrm{in}_<(h_i)b_i^{-1}g_i - \mathrm{in}_<(h_j)b_j^{-1}g_j \\
&= S(\mathrm{in}_<(h_i)g_i, \mathrm{in}_<(h_j)g_j)
\end{aligned}$$

が成立するため

$$\begin{aligned}
\sum_{\mathrm{in}_<(h_ig_i)=\delta_f} \mathrm{in}_<(h_i)g_i &= \sum_{\mathrm{in}_<(h_ig_i)=\mathrm{in}_<(h_jg_j)=\delta_f} c_{ij}S(\mathrm{in}_<(h_i)g_i, \mathrm{in}_<(h_j)g_j) \\
&= \sum_{\mathrm{in}_<(h_ig_i)=\mathrm{in}_<(h_jg_j)=\delta_f} c_{ij}u_{ij}S(g_i, g_j)
\end{aligned}$$

である。任意の $i \neq j$ について $S(g_i, g_j)$ の $g_1, \cdots, g_s$ に関する余りを 0 にできる場合は

$$S(g_i, g_j) = \sum_{k=1}^{s} Q(i, j, k)g_k$$

と表せる。よって

$$\begin{aligned}
\sum_{\mathrm{in}_<(h_ig_i)=\delta_f} \mathrm{in}_<(h_i)g_i &= \sum_{\mathrm{in}_<(h_ig_i)=\mathrm{in}_<(h_jg_j)=\delta_f} c_{ij}u_{ij}S(g_i, g_j) \\
&= \sum_{\mathrm{in}_<(h_ig_i)=\mathrm{in}_<(h_jg_j)=\delta_f} c_{ij}u_{ij}\sum_{k=1}^{s} Q(i, j, k)g_k \\
&= \sum_{k=1}^{s}\left(\sum_{\mathrm{in}_<(h_ig_i)=\mathrm{in}_<(h_jg_j)=\delta_f} c_{ij}u_{ij}Q(i, j, k)\right)g_k \\
&= \sum_{k=1}^{s} H_kg_k
\end{aligned}$$

という形に表せる。また、S 多項式は主項を消去したものなので $\mathrm{in}_<(S(g_i, g_j)) < \delta_f$ であり、したがって、そこから求めた H_kg_k についても $\mathrm{in}_<(H_kg_k) < \delta_f$ となる。このとき

$$\begin{aligned}
f - \sum_{\mathrm{in}_<(h_ig_i)<\delta_f} h_ig_i - \sum_{\mathrm{in}_<(h_ig_i)=\delta_f} h'_ig_i &= \sum_{k=1}^{s} H_kg_k \\
f &= \sum_{\mathrm{in}_<(h_ig_i)<\delta_f} h_ig_i + \sum_{\mathrm{in}_<(h_ig_i)=\delta_f} h'_ig_i + \sum_{k=1}^{s} H_kg_k \\
&= \sum_{k=1}^{s} H'_kg_k
\end{aligned}$$

という形で表すことができ、$\mathrm{in}_<(H'_k g_k) < \delta_f$ が成立している。このとき $\delta(H'_1, \cdots, H'_s) < \delta_f$ が成立することになるが、これは δ_f の定義に矛盾する。よって $\mathrm{in}_<(f) = \delta_f$ が成立する。すなわち、任意の $f(\neq 0) \in I$ について $\mathrm{in}_<(f) = \mathrm{in}_<(h_i g_i)$ なる $h_i g_i$ が存在する。つまり、$\mathrm{in}_<(f) \in (\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ であり、イニシャルイデアルの元はすべて $(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ に属する。つまり $\mathrm{in}_<(I) \subset (\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ である。また $\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s) \in \mathrm{in}_<(I)$ なので $(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s)) \subset \mathrm{in}_<(I)$ である。つまり $\mathrm{in}_<(I) = (\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ が成立しており、$g_1, \cdots, g_s$ はグレブナー基底である。 証明終

これから、Buchberger アルゴリズムを次のように構成できる。

1. イデアルの生成系 $g_1, \cdots, g_s$ からスタートする。
2. $g_1, \cdots, g_s$ に対して Buchberger 判定法を適用し、グレブナー基底であれば終了する。
3. $S(g_i, g_j)$ の $g_1, \cdots, g_s$ に関する余り $(\neq 0)$ を g_{s+1} とする。
4. 余りの定義より g_{s+1} を構成する単項式はイデアル $(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ に属さない。
5. $g_1, \cdots, g_s, g_{s+1}$ は明らかにイデアルの生成系であり、これに対して 1. に戻って適用する。

このアルゴリズムを適用するとき、生成系の主項について

$$\mathrm{in}_<(g_{s+1}) \neq \mathrm{in}_<(g_j) \quad (j = 1, \cdots, s)$$

が成立している。また、g_{s+1} は $S(g_i, g_j)$ から作られていることから、単項式順序による最小元について $\min(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s)) > \min(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s), \mathrm{in}_<(g_{s+1}))$ が成立している。$m_s \equiv \min(\mathrm{in}_<(g_1), \cdots, \mathrm{in}_<(g_s))$ とすると

$$m_s > m_{s+1} > m_{s+2} > \cdots$$

なる単項式による減少列が構成できる。定理 8.5 より、この列は有限でなければならない。つまり、Buchberger アルゴリズムは有限回で終了し、イデアルの生成系から必ずグレブナー基底を得ることができる。

定理 8.12 体の多変数多項式環のイデアルには必ずグレブナー基底が存在する。

(proof)
Hilbert 基底定理により有限の生成系が必ず得られ、Buchberger アルゴリズムによりそこから必ずグレブナー基底が得られる。 証明終

第 II 部

数と位相

9　数の代数

すでに、数については基本的に既知として取り扱ってきているが、改めて代数的な整理をしておく。

9.1　順序環・順序体

定義 9.1　（順序環・順序体）環 $(X,+,\cdot)$ に全順序 $\leq$ が定義されており、$x,y,z \in X$ について

$$x<y \ \Rightarrow\ x+z<y+z$$
$$x<y, z>0 \ \Rightarrow\ xz<yz, zx<zy$$

が成立するとき、$(X,+,\cdot,\leq)$ は**順序環**であるという。順序環が体であるときは特に**順序体**であるという。◂

順序環に対しては正負の概念を導入できる。

定義 9.2　（正負）順序環 $(X,+,\cdot,\leq)$ の全順序について、加法単位元 0 より大きい元を**正**の元、加法単位元 0 より小さい元を**負**の元という。また、$x \in X$ に対して

$$|x| = \begin{cases} x & (x \leq 0) \\ -x & (x<0) \end{cases}$$

を**絶対値**という。◂

定理 9.1　順序環は零因子を持たない。

(proof)
$x \neq 0$ と $|x|>0$ が同値であるため、$y \neq 0$ に対して $|x|,|y|>0$ に対して $0=0|x|<|x||y|=|xy|$ より $xy \neq 0$ である。 証明終

定理 9.2　順序環の元 a,b に対して $|a+b| \leq |a|+|b|$ が成立する。

(proof)
a,b のいずれかが 0 であれば明らかに成立している。$a \neq 0, b \neq 0$ のときについて場合分けする。

$a>0, b>0$ のときは $a+b>0+b>0$ であり $|a+b|=a+b=|a|+|b|$ より定理が成立している。

$a>0, b<0$ のとき、$|a|+|b|=a-b$ である。$0 \leq a+b$ であれば $|a+b|=a+b<a+0=a-b+b<a-b=|a|+|b|$ であり定理が成立している。$a+b<0$ であれば $|a+b|=-a-b<-a-b+a=-b=0-b<a-b=|a|+|b|$ であり定理が成立している。$a<0, b>0$ のときについても同様である。

$a<0, b<0$ のときは $a+b<0+b<0$ であり $|a+b|=-a-b=|a|+|b|$ より定理が成立している。よって示された。 証明終

これより即座に、三角不等式と呼ばれるつぎの性質が成り立つことが分かる。

定理 9.3　（三角不等式）順序環の元 x,y,z について $|x-y| \leq |x-z|+|z-y|$

9.2 自然数

定義 9.3 （整列順序）半順序集合 $(X, \leq)$ の任意の空集合でない部分集合が常に最小元を持つとき、$\leq$ は**整列順序**であるといい、その場合の半順序集合を**整列順序集合**という。◂

定理 9.4 整列順序は全順序である。

(proof)
整列順序集合 $(X, \leq)$ について、任意の $x, y \in X$ をとると、部分集合 $\{x, y\}$ は必ず最小元 z をもつ。このとき $z = x$ もしくは $z = y$ が成立している。一般性を失わず $z = x$ とする。このとき、$z \leq y$ も成立しているので $x \leq y$ である。よって示された。 証明終

整列順序 $\leq$ をもつ可換な半群 $(\boldsymbol{N}, +)$ からスタートしよう。ここで $+$ は全域で定義された可換で結合的な内算法である。整列順序であるため、$\boldsymbol{N}$ は最小元をもつ。これを一旦 i と表示することにする。次の条件も成り立つとする。

1. $+$ の単位元は $\boldsymbol{N}$ には存在しない。
2. $\forall n \in X$ に対して集合 $\{x \in \boldsymbol{N} : n < x\}$ が常に空集合でない。
3. $\forall n \in X$ に対して $\min(\{x \in \boldsymbol{N} : n < x\}) = n + i$ が成立する。
4. $\forall n (\neq i) \in X$ に対して $n^- + i = n$ となる $n^- \in X$ が存在する。

このとき、$\boldsymbol{N}$ は最大元を持たないことは明らかである。また、整列順序であることと 2. より $\min(\{x \in \boldsymbol{N} : n < x\})$ は常に存在する。さらに n に対して n^- は一意である。仮に一意性を失わず $n^- + i = n, n' + i = n, n^- < n'$ とすると、$n' \in \{x \in \boldsymbol{N} : n^- < x\}$ より $n = \min(\{x \in \boldsymbol{N} : n^- < x\}) \leq n'$ となって矛盾する。

$\forall n \in \boldsymbol{N}$ に対して $n^- + i = n$ なる $n^- \in \boldsymbol{N}$ は $n \neq i$ である限り存在する。そこでこの操作を繰り返した集合 A を考えると最小元 $\min A$ が存在する。$A \subset \boldsymbol{N}$ なので $i \leq \min A$ である。ここで $i < \min A$ だとすると $(\min A)^- + 1 = \min A$ なる元 $(\min A)^-$ が存在して $(\min A)^- < (\min A)$ となり矛盾する。よって $i = \min A$ である。つまり、任意の $\boldsymbol{N}$ の元は i に i の加法を繰り返したものである。

こうした定義された $\boldsymbol{N}$ については、数学的帰納法が使える。

定理 9.5 （数学的帰納法）$\boldsymbol{N}$ についてのある命題が

1. i について成立する。

2. $n \in \boldsymbol{N}$ について成立すれば $n + i$ についても成立する。

を満たすならば、その命題は $\boldsymbol{N}$ 全体について成立する。

(proof)
ある命題を満たさない集合 $A \subset \boldsymbol{N}$ を考える。これが空集合で無いと仮定する。整列順序であることより $\min A$ を考えることができる。i について命題は成り立っているので $\min A \neq i$ である。したがって $z + i = \min A$ なる z をとることができ、z については命題が成立している。このとき、$z + i = \min A$ についても命題が成立しなくてはならないので矛盾する。つまり A は空集合であり、その命題は $\boldsymbol{N}$ 全体について成立する。 証明終

順序と加法については次が成り立つ。

定理 9.6 $n < m, z \in \boldsymbol{N}$ について

$$n < m \ \Rightarrow \ n + z < m + z$$

(proof)
$n+i = \min(\{x \in \boldsymbol{N} : n < x\})$ より $n+i \leq m$ が成立する。よって $n+i \leq m < m+i$ である。つまり $n < m \Rightarrow n+i < m+i$ が示された。定理は $z = i$ について成立している。また、任意の $z \in \boldsymbol{N}$ に対しても n, m をそれぞれ $n+z, m+z$ に置き換えて結合則を用いることにより

$$n+z < m+z \Rightarrow n+(z+i) < m+(z+i)$$

も成立する。よって数学的帰納法より定理が示される。 証明終

さらにこの上に乗法 $\cdot$（$\cdot$ は省略可能とする）も定義する。乗法は全域で定義された可換で結合的な内算法であるとする。さらに次のような条件を満たすとする。

1. 乗法単位元は i である。
2. 乗法と加法は分配則を満たす。

乗法については次が成立しており、乗法が加法の繰り返しに等しいことが分かる。

$$\begin{aligned} n \cdot i &= n \\ n \cdot (m+i) &= n \cdot m + n \cdot i \\ &= n \cdot m + n \end{aligned}$$

また、順序に関して次も成立する。

定理 9.7 $n < m, z \in \boldsymbol{N}$ について

$$n < m \Rightarrow nz < mz$$

(proof)
$z = i$ のときは自明である。$z > i$ のとき成立しているとする。つまり $nz < mz$ である。このとき $n(z+i) = nz+n, \quad m(z+i) = mz+n$ であり、上の定理より $nz+n < mz+n$ であることから、$z+i$ のときも成立している。よって数学的帰納法より定理が示される。 証明終

このようにして構成した $\boldsymbol{N}$ と、同じ性質を持つ $\boldsymbol{N}'$ が存在するとすると、それぞれの乗法単位元 i, i' に対して $i' = \phi(i)$ とし、$\phi(n+i) = \phi(n) + \phi(i) = \phi(n) + i'$ によって写像 $\phi : \boldsymbol{N} \to \boldsymbol{N}'$ を定義すると、詳細には述べないものの、ϕ は順序同型写像かつ同型写像となる。その意味でこのように構成された $\boldsymbol{N}$ は一意性をもっており、$\boldsymbol{N}$ と同じ性質を持つものは**自然数系** [10] といわれ、その元は**自然数**と呼ばれる。

まとめると、自然数系は次のような性質を持つものだといえる。

1. 加法について可換な半群であり、単位元を持たない。
2. 整列順序集合であり、最小元は i である。
3. i でない任意の元 n に対して $n^- + i = n$ を満たす直前の元 n^- が一意に存在する。
4. 乗法について可換な半群であり、単位元は i である。
5. 分配則を満たす。
6. $n < m$ ならば $n+z < m+z$
7. $n < m$ ならば $nz < mz$

[10] 加法単位元 0 を含める流儀も存在する。

定理 9.8 自然数は加法について正則元である。つまり、自然数 a, x, y について次が成立する。

$$a + x = a + y \ \Rightarrow \ a + x = a + y$$

(proof)
$a = i$ とする。$x+i = y+i$ が成立している。一般性を失わず $x < y$ と仮定すると $y+i = x+i = \min(\{z : x < z\}) \leq y$ より矛盾する。よって $x = y$ である。a が正則元であるとする。つまり $a + x = a + y$ ならば $x = y$ が成立している。このとき、$(a + i) + x = (a + i) + y$ が成立しているとすると結合側より $a + (i + x) = a + (i + y)$ なので $x + i = y + i$ である。よって $x = y$ である。つまり $a + 1$ についても定理が成り立つ。よって数学的帰納法より定理が示される。 証明終

定理 9.9 自然数 n, m について $n < m$ ならば $m = n + z$ なる自然数 z が存在する。

(proof)
$n = i$ のときを考える。$i < m$ ならば $m = i + z$ なる自然数は存在しており、定理が成立している。ある n のときに定理が成立しているとする。このとき、$n + i < m$ なる m を考える。$m \neq i$ なので $m^- + i = m$ なる自然数 m^- が一意に存在し $n + i < m^- + i$ である。このとき $n \geq m^-$ を仮定すると $n + i \geq m^- + i$ とならなければならず矛盾する。よって $n < m^-$ である。よって $m^- = n + z'$ なる自然数が存在する。このとき $m = m^- + i = (n + z') + i = n + (z' + i)$ であるので、やはり定理が成立する。よって数学的帰納法より示される。 証明終

9.3 整数

自然数系は、加法について可換な半群であるため、加法について可逆化を行うことができる。自然数系 $\boldsymbol{N}$ を加法について可逆化した商構造を $(\boldsymbol{Z}, +)$ で表す。自然数はすべて正則元なので、商構造は $\boldsymbol{Z} = \boldsymbol{N} \times \boldsymbol{N} / \sim$ という構造をしている。ただし、同値関係 $\sim$ は $(x, x^*), (y, y^*) \in \boldsymbol{N} \times \boldsymbol{N}$ に対して

$$(x, x^*) \sim (y, y^*) \Leftrightarrow x + y^* = x^* + y$$

と定義されている。加法はすでに自然に定義されており、加法単位元 $0 = [(i, i)] \in \boldsymbol{Z}$ が存在する。また、$z = [(z, z^*)]$ に対して逆元 $-z = [(z^*, z)]$ が常に存在する。

自然数 n に対応するのは $(n + x^*, x^*)$ の形で表される同値類である。ここで $(y, y^*) \in \boldsymbol{N} \times \boldsymbol{N}$ について $y^* < y$ である場合を考えると、上の定理より $y = y^* + z$ なる自然数 z が存在して $(y, y^*) = (z + y^*, y^*)$ となることから自然数に対応している。$y = y^*$ の場合は加法単位元に対応している。$y < y^*$ の場合は逆元が自然数に対応していることになる。場合分けは上の 3 通りで尽くされるので、自然数の拡張として捉えた場合 $\boldsymbol{Z}$ の元は

1. 自然数
2. 加法単位元 0
3. 加法逆元が自然数である元（負整数とよぶ）

のどれかである。このことを用いてまず全順序を定義する。自然数の範囲では自然数の整列順序と等しいとする。3 区分間ではかならず

$$(\text{負整数}) < 0 < (\text{自然数})$$

であるとする。負整数間においては $x < y \Leftrightarrow (-x) > (-y)$ によって順序を定める。これによって全順序が定義できる。このとき、自然数が正の元であり、負整数が負の元である。

乗法を定義しよう。まず、乗法は可換で結合的かつ分配的であるとする。さらに任意の $n \in \boldsymbol{Z}$ に対して $in = n,\ (-i)n = -n$ という条件を加える。このとき、i は再び乗法単位元であり、$(-i)(-i) = i$ である。また

$$0n = (i + (-i))n = n + (-n) = 0$$

が成立する。これを用いれば、任意の $n \in \boldsymbol{Z}$ は

$$n = \mathrm{sgn}(n)|n|,\ \mathrm{sgn}(n) \in \{-i, 0, i\}, |n| \text{ は自然数}$$

という形に表せる。$n, m \in \boldsymbol{Z}$ について

$$nm = (\mathrm{sgn}(n)\mathrm{sgn}(m)) \cdot |n| \cdot |m|$$

である。n, m が自然数のときは

$$nm = (ii) \cdot (nm) = (nm)$$

なので、自然数の乗法と整合的に乗法が定義できる。こうして、$\boldsymbol{Z}$ に加法・乗法・全順序を導入したものについては、詳細な証明は行わないが、次のように言える。

1. 加法について可換群である。
2. 全順序集合である。
3. 任意の元 n に対して $n^- + i = n$ を満たす直前の元 n^- が一意に存在する。
4. 乗法について可換な半群であり、単位元は i である。
5. 分配則を満たす。
6. $n < m$ ならば $n + z < m + z$
7. $n < m, z > 0$ ならば $nz < mz$
8. 正の元の全体が自然数をなす。

このとき $(\boldsymbol{Z}, +, \cdot, \leq)$ は順序環となっている。これを**整数環**という。以降乗法単位元 i は 1 と表す。順序環は零因子を持たないため、整数環は整域である。そのため、0 以外は乗法について正則元である。さらに、絶対値を以てユークリッド整域であることも示すことができる。よって、整数環は単項イデアル整域・一意分解整域でもある。

定理 9.10 整数 n, m について $n < m$ ならば $m = n + z$ なる自然数 z が存在する。

(proof)
n が自然数であれば m も自然数であり、すでに示されている。$n = 0$ のときは $z = m$ によって成立する。n が負整数のときは、順序環の性質により $0 = n + (-n) < m + (-n)$ であり $m + (-n)$ が自然数である。よってこれを z とすると $z + n = m + (-n) + n = m$ であり、定理が成立している。 証明終

定理 9.11 整数環は、乗法単位元をもつ順序環の中で最小である。つまり、乗法単位元をもつ順序環の部分集合が整数環と同型かつ順序同型となっている。

(proof)
$(R, +\cdot, \leq)$ を乗法単位元を持つ順序環とする。このとき、R には乗法単位元 1 と加法単位元 0 が存在していることに注意する。さらに、環の性質により 1 の加法逆元 -1 も必ず存在する。そこで、整数環 $(\boldsymbol{Z}, +\cdot, \leq)$ のうち、自然数に対応する部分については、$g(n) = \sum_{i=1}^{n} 1$ とし、また $g(0) = 0$ とする。負整数に対応する部分

については、$g(n) = \sum_{i=1}^{n}(-1)$ とする。このとき、環の性質により $g(\boldsymbol{Z}) \subset R$ であり、g は $g : \boldsymbol{Z} \to R$ なる写像である。さらに $g(n+m) = g(n) + g(m)$ であることは容易に分かる。$g(nm) = g(n)g(m)$ については $n = 0, 1, -1$ のときは明らかである。n が自然数のとき、ある n について $g(nm) = g(n)g(m)$ が成立しているとする。このとき

$$\begin{aligned} g((n+1)m) &= g(nm + m) \\ &= g(nm) + g(m) \\ &= g(n)g(m) + g(m) \\ &= g(m)(g(n) + 1) \\ &= g(m)g(n+1) \end{aligned}$$

であり、$n+1$ のときも成立する。よって数学的帰納法より自然数に対して成立する。負整数についても同様に示すことができる。つまり、g は準同型写像である。

順序について $n \leq m$ とする。$n = m$ のときは明らかに $g(n) \leq g(m)$ が成立している。$n < m$ のときは、直前の定理より自然数 z が存在して $m = n + z$ となっている。よって

$$\begin{gathered} g(m) = g(n+z) = g(n) + g(z) \\ g(m) + (-g(n)) = g(z) = \sum_{i=1}^{z} 1 > 0 \\ g(m) > g(n) \end{gathered}$$

であり、$n < m \Rightarrow g(n) < g(m)$ を満たしている。したがって、g は順序を保つとともに、$n \neq m \Rightarrow g(n) \neq g(m)$ となっている。つまり g は単射であり、$g(\boldsymbol{Z}) \subset R$ への写像としては全単射である。したがって、$g(\boldsymbol{Z}) \subset R$ は $\boldsymbol{Z}$ と同型かつ順序同型である。 証明終

このことから、乗法単位元をもつ順序環（順序体を含む）は、整数を含むとみなせる。

9.4 有理数

整数環は整域であることから、乗法について可逆化が可能である。整数環を可逆化した分数体を $(\boldsymbol{Q}, +, \cdot)$ とする。分数体の元は、文字通りの分数の形で表されるものを、約分すると同じものを同一視した同値類である。さらに、分数体の任意の 2 つの元について、分母が同じ自然数となるよう代表元をとったとき（公倍数のうち自然数であるものをとればよい）、分子の整数の順序によって分数体における順序を定めると、順序環の性質によりこれは公倍数のとり方によらず決定でき、全順序となる。さらに、順序環の性質も満たすため、$(\boldsymbol{Q}, +, \cdot, \leq)$ は順序体になる。これは**有理数体**と呼ばれており、その元は**有理数**といわれる。

定理 9.12 有理数体は最小の順序体である。つまり、順序体の部分集合が有理数体と同型かつ順序同型となっている。

(proof)
順序体を $(K, +, \cdot, \leq)$ とする。有理数の代表元を整数 n と自然数 m により $\frac{n}{m}$ とあらわしておく。順序体は順序環でもあるので、準同型かつ順序を保つ写像 $f : \boldsymbol{Z} \to K$ が存在して、$f(n), f(m) \in K$ である。よって $f(n)(f(m)^{-1}) \in K$ であり、f が準同型であることより代表元 $\frac{n}{m}$ のとり方によらずこれは同じ結果となる。そこで、写像 $g : \boldsymbol{Q} \to K$ を $g\left(\frac{n}{m}\right) \mapsto f(n)(f(m)^{-1})$ によって定めておくと、$g(\boldsymbol{Q})(\subset K)$ が $\boldsymbol{Q}$ と同系かつ順序同型となる。（詳細略） 証明終

このことから、順序体は有理数を含むとみなせる。当然自然数も含むとみなせる。

定義 9.4 （アルキメデスの公理）順序体 K において、自然数を含むと考える。任意の $x \in K$ に対して $x < n$ なる自然数 n が存在するとき、順序体 K は**アルキメデスの公理**を満たすという。◂

定理 9.13 有理数体はアルキメデスの公理を満たす。

(proof)
有理数は整数 $n, m > 0$ によって $\frac{n}{m}$ の同値類（約分すると同じものを同一視）として表される。このとき $\frac{(|n|+1)m}{m}$ の同値類は $\frac{n}{m} < \frac{(|n|+1)m}{m}$ を満たすとともに、整数環における $|n|+1 > 0$ に相当するもの、つまり自然数である。 証明終

10 完備性と実数

10.1 順序完備性と実数

定義 10.1 （上限）全順序集合 $(X, \leq)$ の部分集合 $A \subset X$ について、$a \in A$ が以下の条件

1. $b \in A$ なら $b \leq a$
2. $c < a$ なら $c < x$ なる $x \in A$ が存在する

を満たせば、a を A の**上限**であるといい、$a = \sup X$ と表す。◂

定義 10.2 （下限）全順序集合 $(X, \leq)$ の部分集合 $A \subset X$ について、$a \in A$ が以下の条件

1. $b \in A$ なら $b \geq a$
2. $a < c$ なら $x < c$ なる $x \in A$ が存在する

を満たせば、a を A の**下限**であるといい、$a = \inf A$ と表す。◂

次が容易に示される。

定理 10.1 上限及び下限は一意である。

上限 $\sup A$ 及び下限 $\inf A$ は、必ずしも A には属さないことには注意が必要である。それに対し、最大値・最小値は存在するとは限らない。上限 $\sup A$ 及び下限 $\inf A$ が A に属せば、それらはそれぞれ最大値・最小値である。上限及び下限は一意なので、最大値・最小値が存在すれば、それらはまた上限・下限に等しい。

定義 10.3 （有界）全順序集合 $(X, \leq)$ の部分集合 $A \subset X$ について、任意の $a \in A$ に対して $a \leq b$ を満たす $b \in X$ が存在するとき、A は**上に有界**であるという。また、任意の $a \in A$ に対して $b \leq a$ を満たす $b \in X$ が存在するとき、A は**下に有界**であるという。上に有界かつ下に有界であるときは、**有界**であるという。◂

上限が存在すれば上に有界であるが、逆は必ずしも真ではない。同様に、下限が存在すれば下に有界であるが、逆は必ずしも真ではない。

定義 10.4 （順序完備）全順序集合 $(X, \leq)$ の任意の部分集合 $A \subset X$ について、上に有界ならば上限を持ち、下に有界ならば下限を持つとき、全順序集合 $(X, \leq)$ は**順序完備**であるという。◂

定義 10.5 （実数）順序完備な順序体を**実数体**といい、$\boldsymbol{R}$ で表す。実数体の元を**実数**という。◂

10.2　順序体の収束概念

定義 10.6　（点列・数列）自然数からの写像 $n \mapsto a_n \in X$ を X の**点列**という。X がいわゆる数（整数環・有理数体など）の場合には、**数列**とも呼ばれる。$n \leq m$ ならば $a_n \leq a_m$ であるとき、点列は**単調増加**であるという。また、像 $\{a_n\}$ は集合であり、集合に対する概念を点列に対して考えることができる。点列によって $\{a_1, \cdots, a_n\}$ の形に表される集合を有限集合という。◂

念のため、次を示しておこう。

定理 10.2 有限集合は最大元・最小元を持つ。

(proof)
有限集合 $\{a_1, \cdots, a_n\}$ に対して

$$b_1 = a_1, \quad b_{k+1} = \max(a_{k+1}, b_k)$$

によって定義すると、b_n が最大元になっている。また

$$c_1 = a_1, \quad c_{k+1} = \min(a_{k+1}, c_k)$$

によって定義すると、c_n が最小元になっている。 証明終

定義 10.7　（極限・収束）順序体 $(K, +, \cdot, \leq)$ の点列 $\{a_n\}$ が $b \in K$ に**収束**するとは、任意の $0 < \epsilon \in K$ に対してある自然数 N が存在し、$N \leq n$ なる任意の自然数 n について

$$|a_n - b| \leq \epsilon$$

が成り立つことをいう。このとき b を $\{a_n\}$ の**極限**という。◂

収束に関する一般的な記号は今後特に断り無く用いる。

定理 10.3 極限は一意である。

(proof)
点列 $\{a_n\}$ の極限が $b \neq c$ であるとする。一意性を失わず $b < c$ とする。このとき、任意の $\epsilon > 0$ に対してある N が存在して、$N \leq n$ なる任意の自然数 n について

$$|a_n - b| \leq \epsilon$$
$$|a_n - c| \leq \epsilon$$

が成立するので、三角不等式より

$$\begin{aligned} c - b = |c - b| &\leq |c - a_n| + |a_n - b| \\ &= |a_n - c| + |a_n - b| \\ &= 2\epsilon \end{aligned}$$

が成立する。ところで、$c - b > 0$ より $\epsilon = \dfrac{c-b}{4} > 0$ についても成立しなければならない。このとき

$$c - b \leq \frac{c-b}{2} \Rightarrow 2 \leq 1$$

であり矛盾する。よって $b = c$ でなければならない。 証明終

定理 10.4 実数体において、上に有界で単調増加な点列は上限に収束する。

(proof)
点列 $\{a_n\}$ を上に有界で単調増加な列とする。順序完備なので、上限 s が存在し $a_n \leq s$ が成立する。任意の $\epsilon > 0$ について、$b - \epsilon \leq b$ なので $b - \epsilon < a_N$ なる a_N が存在する。単調増加列なので $N \leq n$ に対して

$$b - \epsilon < a_N \leq a_n \leq b < b + \epsilon$$

なので $|a_n - b| < \epsilon$ が成立している。 証明終

定義 10.8 （**コーシー列・コーシー完備**）順序体の点列 $\{a_n\}$ が**コーシー列**であるとは、任意の $0 < \epsilon \in K$ に対してある自然数 N が存在し、$N \leq n, N \leq m$ なる任意の自然数 n, m について

$$|a_n - a_m| \leq \epsilon$$

が成り立つことをいう。点列が収束するときはコーシー列であるが、逆は必ずしも真ではない。順序体の任意のコーシー列が収束するとき、順序体は**コーシー完備**であるという。◂

定理 10.5 実数体はコーシー完備である。

(proof)
コーシー列 $\{a_n\}$ を考える。任意の $\epsilon > 0$ に対してある自然数 N が存在して、$|a_n - a_m| \leq \epsilon,\ N \leq n, m$ が成立している。特に、任意の $(N \leq) n$ に対して $a_N - \epsilon \leq a_n \leq a_N + \epsilon$ なので、$\{a_n\}_{N \leq n}$ は有界である。ここで、点列 $\{b_n\}$ を

$$b_n = \begin{cases} a_N & (n = 1) \\ \max(a_{N+n-1}, b_{n-1}) & (1 < n) \end{cases}$$

によって定義すると、$\{b_n\}$ も有界であり、明らかに単調増加であることから収束する。この極限を c とする。構成法より $\{b_n\}$ の元は $\{a_n\}_{N \leq n}$ のいずれかの元に一致している。よって、$N \leq n$ なる n と自然数 m に対して

$$|a_n - b_m| \leq \epsilon$$

が成立している。また、$\{b_n\}$ が収束することにより、ある L が存在して $L \leq m$ に対して

$$|b_m - c| \leq \epsilon$$

が成立している。よって、$N \leq n, L \leq m$ に対して

$$|a_n - c| \leq |a_n - b_m| + |b_m - c| \leq 2\epsilon$$

が成立している。よって示された。 証明終

定理 10.6 実数体はアルキメデスの公理を満たす。

(proof)
アルキメデスの公理を満たさないとすると、ある $x \in \boldsymbol{R}$ が存在して $x < n$ をみたす自然数 n は存在しない。このとき、任意の自然数 n について $x < n$ が成立しないので、全順序であることより $n \leq x$ が成立する。ここで点列 $\{a_n\}$ を $a_n = n$ によって定義すると、上に有界かつ単調増加なので収束する。この極限を b とする。$b = \sup \boldsymbol{N}$ である。このとき、自然数 1 について、ある自然数 L が存在して $|a_L - b| = b - L \leq 1$ が成立する。このとき $b \leq L + 1$ であり、$L + 1$ も自然数であることから矛盾する。よって実数体はアルキメデスの公理を満たす。 証明終

定理 10.7 順序体の任意の上に有界で単調増加な点列が収束するならば、順序体は順序完備である。

(proof)
上に有界な空集合でない任意の部分集合を A とする。A に最大元が存在すれば、それは上限でもあるため、上限が存在する。そこで A に最大元は存在しない場合を考える。$\forall a \in A$ について、$a \leq b$ なる b が存在する。ここで、$\alpha \in A$ をとり自然数 n に対して

$$B_n \equiv \left\{ \alpha, \alpha + \frac{b-\alpha}{2^n}, a + 2\frac{b-\alpha}{2^n}, \cdots, b \right\}$$

は有限集合であり、その部分集合

$$C_n \equiv \{x \in B_n : \forall a \in A, a \leq x\}$$

も有限集合であることから、最小元が存在する。よって $c_n \equiv \min C_n$ と定義する。$C_n \subset C_{n+1}$ より点列 $\{c_n\}$ は単調減少であり、明らかに α をもって有界である。このとき点列 $\{-c_n\}$ は単調増加であり、$-\alpha$ をもって上に有界であるため、定理の条件より収束する。この極限を z とする。構成法より任意の $a \in A$ について $a \leq c_n$ を満たしている。ここで $z < a'$ なる $a' \in A$ が存在するとする。$a' - z > 0$ に対してある N が存在して $N \leq n$, $c_n - z \leq |c_n - z| \leq a' - z$ が成立する。このとき $c_n \leq a'$ なので $c_n = a'$ である。このとき a' も極限となることが明らかなので $z = a'$ であり矛盾する。よって任意の $a \in A$ について $a \leq z$ である。

ここで、$c_n - \frac{b-\alpha}{2^n}$ を考える。これは B_n に属しているが、c_n の最小性より C_n には属していない。よって $\exists a_n'' \in A$ によって $c_n - \frac{b-\alpha}{2^n} < a_n''$ が成立する。$y < z$ なる y に対して、十分大きい n に対しては

$$\epsilon \equiv z - y - \frac{b-\alpha}{2^n} > 0$$

とでき

$$\begin{aligned} |c_n - z| \leq \epsilon = z - y - \frac{b-\alpha}{2^n} \\ -z + y + \frac{b-\alpha}{2^n} \leq c_n - z \\ y \leq c_n - \frac{b-\alpha}{2^n} < a_n'' \end{aligned}$$

が成立する。つまり $y < z$ なる y に対しては $y < a_n''$ なる $a_n'' \in A$ が存在する。よって z は A の上限である。下限についでも同様に示すことができる。 証明終

補題 10.8 順序体がアルキメデスの公理を満たすならば、有界で単調な点列はコーシー列である。

(proof)
順序体の任意の上に有界で単調増加な点列を $\{a_n\}$ とする。上に有界なので、任意の自然数 n に対して $a_n \leq G$ を満たす G が存在する。

ここで、$\{a_n\}$ はコーシー列でないと仮定しよう。このとき、ある $c > 0$ が存在して、任意の自然数 N に対して $a_n - a_N > c$ となる $N < n$ が存在する。$s(0) = 0$ から始めて $a_n - a_{s(0)} > c$ を満たす n を $s(1)$ とし、以下、$a_n - a_{s(i)} > c$ を満たす n を $s(i+1)$ として、部分列 $b_n = a_{s(n)}$ を構成する。$b_{n+1} - b_n > c$ が成立しているため、

$$a_{s(n+1)} = b_{n+1} = b_1 + cn$$

である。アルキメデスの公理より $\frac{G-b_1}{c} < M$ なる自然数 M が存在する。これによって

$$a_{s(M+1)} = b_1 + cM > G$$

となり矛盾する。よって $\{a_n\}$ はコーシー列である。 証明終

定理 10.9 順序体がコーシー完備であり、アルキメデスの公理を満たすならば、順序完備である。

(proof)
アルキメデスの公理を満たす順序体において、任意の上に有界で単調増加な点列はコーシー列である。コーシー完備であれば、それは収束する。よって、直前の定理より順序完備である。 証明終

これらにより順序体について

1. 順序完備である。
2. 上に有界で単調増加な点列が収束する。
3. アルキメデスの公理を満たし、コーシー完備である。

は同値であることがわかった。これらはまとめて**実数の完備性**と呼ばれる。

10.3 順序体の完備化

有理数体を念頭に、アルキメデスの公理を満たす順序体 K から実数体を構成することを考える。基本的には、極限の集合に相当するものを構成すればよいのだが、極限そのものが実数体でなければ存在しない場合があるので、収束自体も議論することができない。そこで、コーシー列を利用する。

K 上のコーシー列の集合 K' に対して、次の二項関係を導入すると、これは容易に同値関係であることが分かる。

$$\{a_n\} \sim \{b_n\} \Leftrightarrow \lim_{n\to\infty} |a_n - b_n| = 0$$

まず K' に加法・乗法を導入しよう。自然に

$$\{a_n\} + \{b_n\} \equiv \{a_n + b_n\}$$
$$\{a_n\} \cdot \{b_n\} \equiv \{a_n \cdot b_n\}$$

と定義しておけば、同値関係 $\sim$ と両立している。よって $\tilde{K} \equiv K'/\sim$ として商構造 $(\tilde{K}, +, \cdot)$ を定義することができる。K の元 k に対しては、k に収束する点列 $\{k_n\}$ の同値類を対応させると、$(\tilde{K}, +, \cdot)$ の部分集合と $(K, +, \cdot)$ が同型となり、商構造 $(\tilde{K}, +, \cdot)$ はもとの順序体 K を含むと考えることができる。

K' 上でまず順序を定義する。任意の $\epsilon > 0$ に対してある N が存在して $N \leq n$ について

$$a_n - b_n \leq \epsilon$$

が成立するとき、$\{a_n\} \leq \{b_n\}$ であると定める。これが反射律・反対称律を満たすことは明らかである。$\{a_n\} \leq \{b_n\}, \{b_n\} \leq \{c_n\}$ が成立するとき、任意の $\epsilon > 0$ に対してある N が存在して $N \leq n$ について

$$a_n - b_n \leq \epsilon, \quad b_n - c_n \leq \epsilon$$

が成立していることから

$$a_n - c_n \leq 2\epsilon$$

が成立する。ϵ は任意なのでこのときやはり $\{a_n\} \leq \{c_n\}$ である。つまり、$\leq$ は半順序である。

さて、ここで任意の K' の元 $\{a_n\}, \{b_n\}$ について $\{a_n\} \leq \{b_n\}$ も $\{b_n\} \leq \{a_n\}$ も成立していないとする。このとき、ある $c > 0$ が存在して、任意の N について $N \leq n, m$ で

$$a_n - b_n > c,\ b_m - a_m > c$$

となるものが存在する。コーシー列であることより、N を十分大きくとると、任意の $\epsilon > 0$ に対して

$$|a_n - a_m| \leq \epsilon,\ |b_n - b_m| \leq \epsilon$$

が成立している。よって

$$\begin{aligned} 2c < a_n - b_n + b_m - a_m &= |a_n - b_n + b_m - a_m| \\ &\leq |a_n - a_m| + |b_m - a_n| \leq 2\epsilon \end{aligned}$$

が成立しなくてはならない。ところが $\epsilon = \dfrac{c}{2} > 0$ について $2c < c \Rightarrow 2 < 1$ となり矛盾する。よって $\{a_n\} \leq \{b_n\}$ か $\{b_n\} \leq \{a_n\}$ のどちらかは成立する。つまり、$\leq$ は全順序である。ここで

$$\{a_n\} \leq \{b_n\},\ \{a_n\} \sim \{a'_n\},\ \{b_n\} \sim \{b'_n\}$$

のとき、任意の $\epsilon > 0$ に対してある N が存在して $N \leq n$ について

$$\begin{aligned} a_n - b_n &\leq \epsilon \\ |a_n - a'_n| &\leq \epsilon \\ |b_n - b'_n| &\leq \epsilon \end{aligned}$$

なので

$$\begin{aligned} a'_n - b'_n &\leq a_n - b_n + 2\epsilon \\ &\leq 3\epsilon \end{aligned}$$

であり $\{a'_n\} \leq \{b'_n\}$ である。つまり、商構造 $(\tilde{K}, +, \cdot)$ 上で、同じ同値類に属していれば代表元のとりかたによらず順序関係が定まっており、これより商構造 $(\tilde{K}, +, \cdot)$ 上で全順序を定義することができる。そしてやはり、商構造の K に対応する元（当該元に収束する点列による同値類）については、K と順序同型となっている。

商構造 $(\tilde{K}, +, \cdot, \leq)$ では、0 に収束する点列の同値類が再び加法単位元 0 となり、1 に収束する点列の同値類が再び乗法単位元 1 となる。加法については、$[\{a_n\}] \in \tilde{K}$ に対して $[\{-a_n\}]$ が逆元となる。乗法については、$[\{a_n\}] \in \tilde{K} - \{0\}$ に対して $[\{(a_n)^{-1}\}]$ が逆元となる。分配則も成り立っていることから、$(\tilde{K}, +, \cdot, \leq)$ は体である。さらに順序環の条件も満たしていることから、$(\tilde{K}, +, \cdot, \leq)$ は順序体である。

こうしてアルキメデスの公理を満たす順序体 K から順序体 $(\tilde{K}, +, \cdot, \leq)$ を得る手続きを**完備化**といい、また $(\tilde{K}, +, \cdot, \leq)$ は K の**完備化**であるというものとする。これを完備化と称すことができることは、以下で見るように完備性をもっているために他ならない。

定理 10.10 アルキメデスの公理を満たす順序体 K の完備化 $(\tilde{K}, +, \cdot, \leq)$ について、任意の上に有界で単調増加な点列は収束する。

(proof)
$(\tilde{K}, +, \cdot, \leq)$ の任意の有界で単調増加な点列 $\{a_n\}$ を考える。各 a_n は K 上のコーシー列の同値類であり、その代表元を $\{a_i^{(n)}\}$ とする。上に有界であることから、$b \in \tilde{K}$ によって $a_n \leq b$ となっている。b の K 上のコーシー列による代表元を $\{b_i\}$ とする。このとき、任意の $\epsilon > 0$ に対して、十分大きい N をとると $N \leq i$ について

$$a_i^{(n)} - b_i \leq \frac{1}{2^n}$$

とすることができ、また単調増加であることから

$$a_i^{(n)} - a_i^{(n+1)} \leq \frac{1}{2^{n+1}}$$

とすることができる。となる。ここで $y_i \equiv a_N^{(i)} - \frac{1}{2^i}$ と定めると

$$y_i \leq b_N, \quad y_i \leq y_{i+1}$$

が成立する。つまり $\{y_i\}$ は K 上の上に有界で単調増加な点列であり、K はアルキメデスの公理を満たすことから、補題 10.8 より $\{y_i\}$ はコーシー列である。よって $\{y_i\}$ の同値類は $\tilde{K}$ の元である。そこで $y \equiv [\{y_i\}] \in \tilde{K}$ と表すことにする。

さて、$\tilde{K}$ 上で、a_n と y の関係を考えると

$$a_N^{(n)} - y_n = \frac{1}{2^n}$$

であり、コーシー列であることから N を大きくとっておくことにより、$N \leq i$ について

$$\left|a_i^{(n)} - a_N^{(n)}\right| \leq \frac{1}{2^n}$$

とすることができる。このとき

$$\begin{aligned} 0 - \frac{1}{2^n} \leq a_i^{(n)} - a_N^{(n)} + a_N^{(n)} - y_n &\leq \frac{1}{2^n} + \frac{1}{2^n} \\ -\frac{1}{2^n} \leq a_i^{(n)} - y_n &\leq \frac{1}{2^{n-1}} \\ -\frac{1}{2^n} - y_i + y_n \leq a_i^{(n)} - y_i &\leq \frac{1}{2^{n-1}} - y_i + y_n \end{aligned}$$

より、任意の $\epsilon > 0$ に対して十分大きい n に対しては、$\{y_i\}$ もコーシー列であるので

$$\begin{aligned} a_i^{(n)} - y_i &\leq \frac{1}{2^{n-1}} - y_i + y_n \leq \epsilon \\ y_i - a_i^{(n)} &\leq \frac{1}{2^n} + y_i - y_n \leq \epsilon \end{aligned}$$

が成立する。つまり十分大きい n に対しては

$$y \leq a_n,\ a_n \leq y \Leftrightarrow\ a_n = y$$

が成立しており、$\{a_n\}$ は y に収束する。 証明終

系 10.11 アルキメデスの公理を満たす順序体 K の完備化 $(\tilde{K}, +, \cdot, \leq)$ は実数体である。

系 10.12 有理数体の完備化は実数体である。

実は、実数体は一意であることが知られている（複数の実数体は同型かつ順序同型）。そのため、任意のアルキメデスの公理を満たす順序体を完備化したものは同じ実数体とみなせる。こうして実数を構成するところまで行き着いた。

1. 自然数系を加法について可逆化し、整数環を得る。

2. 整数環を乗法について可逆化し、有理数体を得る。

3. 有理数体を完備化し、実数体を得る。

ここで注意しておきたいのは、可逆化と完備化の構成法の違いである。可逆化はもとの元の二つの直積だけで構成できていたが、完備化は無限点列を使って構成している。このため、可逆化はデータ容量のことを無視すれば計算機（コンピュータ）で表現しうるが、完備化は本質的に表現不可能であり、純粋な理論的操作である。

11　位相・距離空間

11.1　位相空間と開集合・閉集合

距離空間への足がかりとして、抽象的な位相の概念を導入する。

定義 11.1（**位相空間・開集合**）集合 X に、次の性質を持つ部分集合族 $\mathfrak{O}$**(開集合族)** が与えられたとき

1. $O_\gamma \in \mathfrak{O}(\gamma \in \Gamma)$ のとき　$\bigcup_{\gamma\in\Gamma} O_\gamma \in \mathfrak{O}$　[11]
2. $O_1, O_2 \in \mathfrak{O}(\gamma \in \Gamma)$ のとき　$O_1 \cap O_2 \in \mathfrak{O}$　[12]
3. $X, \phi \in \mathfrak{O}$

$(X, \mathfrak{O})$ を**位相空間**といい、$\mathfrak{O}$ に属す集合を**開集合**という。◂

定義 11.2（**閉集合**）位相空間 $(X, \mathfrak{O})$ において、X の部分集合 F について $F^c \in \mathfrak{O}$ であるとき、F を**閉集合**という。◂

次のことが容易に分かる。

定理 11.1 位相空間 $(X, \mathfrak{O})$ において、閉集合について以下が成り立つ。

1. $\gamma \in \Gamma$ なる F_γ がすべて閉集合のとき　$\bigcap_{\gamma\in\Gamma} O_\gamma$ も閉集合である。
2. F_1, F_2 が閉集合のとき　$O_1 \cup O_2$ も閉集合である。
3. X, ϕ は閉集合である。

直積に対しては、自然に位相を導入できる。

定理 11.2 位相空間 $(X, \mathfrak{O}_X)$,$(Y, \mathfrak{O}_Y)$ について

$$\mathfrak{O}_X \times \mathfrak{O}_Y \equiv \{A \times B | A \in O_X, B \in O_Y\}$$

と定義すると、$\mathfrak{O}_X \times \mathfrak{O}_Y$ は開集合族の条件を満たし、$(X \times Y, \mathfrak{O}_X \times \mathfrak{O}_Y)$ は位相空間となる。

定義 11.3（**積位相空間**）位相空間 $(X, \mathfrak{O}_X)$,$(Y, \mathfrak{O}_Y)$ について、上の定理より位相空間となる $(X \times Y, \mathfrak{O}_X \times \mathfrak{O}_Y)$ を、**積位相空間**または単純に直積と言う。◂

[11]「開集合の和集合は開集合になる」ことを要請している。
[12]「二つの開集合の共通部分は開集合になる」ことを要請している。

11.2 コンパクト

定義 11.4 （開被覆）位相空間 $(X, \mathfrak{O})$ と X の部分集合 Y において、開集合の族 $\{O_\gamma\}_{\gamma\in\Gamma}$ が

$$Y \subset \bigcup_{\gamma\in\Gamma} O_\gamma$$

をみたすとき、$\{O_\gamma\}_{\gamma\in\Gamma}$ を Y の**開被覆**であるという。[13] 特に、有限個の開集合の族 $\{O_n\}$ によって

$$Y \subset \bigcup_{n=1}^{N} O_n$$

と表されるとき、$\{O_n\}$ は**有限開被覆**であるという。◂

定義 11.5 （コンパクト）位相空間 $(X, \mathfrak{O})$ と X の部分集合 Y において、$\{O_\gamma\}_{\gamma\in\Gamma}$ が Y の開被覆ならば、つまり

$$Y \subset \bigcup_{\gamma\in\Gamma} O_\gamma$$

ならば、$\{O_\gamma\}_{\gamma\in\Gamma}$ からとった有限個の部分集合族 $O_1, O_2, \cdots, O_s$ が既に Y の有限開被覆である、つまり

$$Y \subset \bigcup_{n=1}^{s} O_n$$

であるとき、Y は**コンパクト**であるという。◂

コンパクト性は、最大値・最小値の存在と関係しており、非常に重要である。

定理 11.3 コンパクトな位相空間の部分閉集合はコンパクトである。

(proof)
X をコンパクトな位相空間とし、その部分閉集合を F とおく。$\{O_\gamma\}_{\gamma\in\Gamma}$ を F の開被覆とする。

$$X = F \cup F^c \subset \bigcup_{\gamma\in\Gamma} O_\gamma \cup F^c$$

であり F^c は開集合なので、$\{O_\gamma\}_{\gamma\in\Gamma} \cup F^c$ は X の開被覆である。X はコンパクトなので、この中から X の有限部分開被覆 $\{O_1, \cdots, O_s, F^c\}$ をとれる。このとき

$$X \subset \bigcup_{n=1}^{s} O_s \cup F^c$$

となる。これより、X の要素で $\bigcup_{n=1}^{s} O_s$ に含まれない要素は F^c に含まれるということがいえる。この対偶をとれば、F の要素は $\bigcup_{n=1}^{s} O_s$ に含まれるということになり、

$$F \subset \bigcup_{n=1}^{s} O_s$$

であるから、F は開被覆の有限部分開被覆によって覆われることになる。つまり、F はコンパクトである。
証明終

定理 11.4 位相空間 $(X, \mathfrak{O}_X)$,$(Y, \mathfrak{O}_Y)$ がコンパクトである時、積位相空間 $(X\times Y, \mathfrak{O}_X \times \mathfrak{O}_Y)$ もコンパクトである。

[13] 包含関係ではなく"="で定義する流儀もあるが、こちらの方が使いやすい。

(proof)

$X \times Y$ の開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ が与えられた時、そのうちの有限個によって

$$X \times Y \subset \bigcup_{n=1}^{N} O_n$$

となればよいのだが、そのままでは扱いにくいので[14]、開被覆の部分開集合も含めることにより

$$\{O'_\gamma\}_{\gamma\in\Gamma'} = \{O' \in \mathfrak{O}_X \times \mathfrak{O}_Y | O' \subset O_\gamma (\gamma \in \Gamma)\}$$

と拡張した集合族 $\{O'_\gamma\}_{\gamma\in\Gamma'}$ を考える。これは、明らかにもとの開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ を含むので、$\{O'_\gamma\}_{\gamma\in\Gamma'}$ も $X \times Y$ の開被覆である。すなわち

$$X \times Y \subset \bigcup_{\gamma\in\Gamma'} O'_\gamma$$

となる。このとき $O'_\gamma = O'^X_\gamma \times O'^Y_\gamma (O'^X_\gamma \in X, O'^Y_\gamma \in Y)$ と表すことにすると、積位相空間の開集合族 $\mathfrak{O}_X \times \mathfrak{O}_Y$ の定義より O'^X_γ, O'^Y_γ はそれぞれ X, Y の開集合であり

$$X \subset \bigcup_{\gamma\in\Gamma'} O'^X_\gamma \quad Y \subset \bigcup_{\gamma\in\Gamma'} O'^Y_\gamma$$

となる[15]。このとき Y は開被覆 $\{O'^Y_\gamma\}_{\gamma\in\Gamma'}$ によって覆われているので、Y がコンパクトであることより、その中から Y の有限部分開被覆 $\{O'^Y_1, \cdots, O'^Y_s\}$ をとれる。

さて、有限開被覆の各開集合に対し、$O'_\gamma = O'^X_\gamma \times O'^Y_\gamma$ の関係から得られる O'^X_n 全体の成す集合

$$\mathbb{X} \equiv \{A | A \times O'^Y_n (n = 1, \cdots, s) = O'_\gamma (\gamma \in \Gamma')\}$$

を考える。ここで「Y の有限部分開被覆 $\{O'^Y_1, \cdots, O'^Y_s\}$ をどのようにとっても、$\mathbb{X}$ に属するどの集合にも含まれない X の元 x_0 がある」と仮定する。とはいえ、$\{O'_\gamma\}_{\gamma\in\Gamma'} = \{O'^X_\gamma \times O'^Y_\gamma\}_{\gamma\in\Gamma'}$ は $X \times Y$ の開被覆なので、$x_0 \in O'^X_{\gamma 0} (\gamma_0 \in \Gamma')$ となる X の開集合 $O'^X_{\gamma 0}$ が存在する。このとき、対応する $O'^Y_{\gamma 0}$ を Y の有限部分開被覆に加えれば、加えられた Y の有限部分開被覆 $\{O'^Y_1, \cdots, O'^Y_s, O'^Y_{\gamma 0}\}$ に対する $\mathbb{X}$ については、$x_0 \in O'^X_{\gamma 0} \in \mathbb{X}$ となり、仮定に矛盾する。したがって、Y の有限部分開被覆 $\{O'^Y_1, \cdots, O'^Y_s\}$ をうまくとれば、X の任意の元は $\mathbb{X}$ に属する集合のどれかには含まれる。つまり

$$X \subset \bigcup_{A\in\mathbb{X}} A$$

となるということであり、$\mathbb{X}$ は X の開被覆である。

X はコンパクトなので、$\mathbb{X}$ の有限部分被覆 $\{O'^X_1, \cdots, O'^X_t\}$ によって

$$X \subset \bigcup_{n=1}^{t} O'^X_n$$

と覆われる。また、$\{O'^Y_1, \cdots, O'^Y_s\}$ は Y の有限開被覆であったので

$$Y \subset \bigcup_{m=1}^{s} O'^Y_m$$

と覆われる。以上より

$$X \times Y \subset \bigcup_{n=1}^{t} O'^X_n \times \bigcup_{m=1}^{s} O'^Y_m = \bigcup_{n=1}^{t} \bigcup_{m=1}^{s} (O'^X_n \times O'^Y_m)$$

[14] Y の有限開被覆が得られても、$\{O_\gamma\}_{\gamma\in\Gamma}$ で対応する X の集合族が被覆になるとは限らない。
[15] 逆は成立しないのが、直積を扱う上での注意である。これは平面を考えればよくわかる。

である。$\mathbb{X}$ の定義より

$$O'^X_n \times O'^Y_m (n = 1, \cdots, t \quad m = 1, \cdots, s) \quad = \quad O'_\gamma (\gamma \in \Gamma') \quad \subset \quad O_\gamma (\gamma \in \Gamma)$$

である。このとき、上の包含関係で $O'^X_n \times O'^Y_m$ に対応する O_γ を O_{nm} と表すことにすれば、$O'^X_n \times O'^Y_m \subset O_{nm}$ なので

$$X \times Y \subset \bigcup_{n=1}^{t} \bigcup_{m=1}^{s} (O'^X_n \times O'^Y_m) \subset \bigcup_{n=1}^{t} \bigcup_{m=1}^{s} O_{nm}$$

である。よって、もとの開被覆 $\{O_\gamma\}_{\gamma \in \Gamma}$ の有限部分開被覆 $\{O_{11}, O_{12}, \cdots, O_{1s}, \cdots, O_{t1}, \cdots, O_{ts}\}$ によって $X \times Y$ は覆われたので、積位相空間 $(X \times Y, \mathfrak{O}_X \times \mathfrak{O}_Y)$ はコンパクトである。 証明終

11.3 距離空間

定義 11.6 （**距離空間・距離関数**）$\boldsymbol{R}$ を実数体とする。集合 X に

$$\text{関数 } d : X \times X \to \boldsymbol{R}$$

が与えられ、任意の $x, y, z \in X$ について次の性質を満たすとき

1. $d(x,y) \geq 0 \quad d(x,y) = 0$ なら $x = y$
2. $d(x,y) = d(y,x)$
3. $d(x,y) \leq d(x,z) + d(z,y)$ 三角不等式

(X,d) を**距離空間**といい、d を**距離関数**、$d(x,y)$ を x, y の距離という。◂

定義 11.7 距離空間 (X,d) と $x \in X$ について、$V_\epsilon(x) \equiv \{p | d(x,p) < \epsilon\}$ と定義し、これを x の ϵ **近傍**もしくは**開球**という。◂

定義 11.8 距離空間 (X,d) と $x \in X$ について、$\overline{V}_\epsilon(x) \equiv \{p | d(x,p) \leq \epsilon\}$ と定義し、これを x の**閉球**という。◂

補題 11.5 距離空間 (X,d) と、その部分空間 Y について、$y \in Y, x \in Y^c$ ならば $d(x,y) > 0$ となる。

(proof)
$d(x,y) = 0$ ならば距離空間の定義から $x = y$ となり、$x = y \in Y$ となって矛盾する。 証明終

11.3.1 距離空間における収束

距離空間においては、距離関数による実数との対応づけによって、収束の概念を定義できる。

定義 11.9 距離空間 (X,d) において、X の点列 $\{x_n\}$ が

$$\lim_{n \to \infty} d(x_n, a) = 0$$

をみたすとき、点列 $\{x_n\}$ は a に収束するといい

$$\lim_{n \to \infty} x_n = a$$

といったように、数列の収束に準じて表す。◂

三角不等式によって極限の一意性が保証される。

定理 11.6 距離空間 (X,d) において、X の点列 $\{x_n\}$ が、$n \to \infty$ のとき $x_n \to a, x_n \to b$ ならば $a = b$ である。

(proof)
$d(a,b) > 0$ と仮定する。三角不等式から $d(a,b) \leq d(a,x_n) + d(b,x_n)$ であるが、$n \to \infty$ のとき右辺は 0 に収束するので、$d(a,x_n) + d(b,x_n) < d(a,b)$ とすることができ、矛盾する。したがって、$d(a,b) = 0$ であり、距離空間の定義から $a = b$ となる。 証明終

収束に関しては、距離空間においては次のような言いかえが可能である。

補題 11.7 距離空間 (X,d) において、X の点列 $\{x_n\}$ が x に収束することと、任意の $\varepsilon > 0$ に対し、十分大きな n をとれば $x_n \in V_\varepsilon(x)$ となることは同値である。

距離空間に対しては、コーシー列を定義できる。

定義 11.10 （**コーシー列・完備距離空間**）距離空間 (X,d) と X の点列 $\{x_n\}$ について、任意の $\varepsilon > 0$ に対してある自然数 L が存在して

$$\forall n, m \geq L \quad \to \quad d(x_n, x_m) < \epsilon$$

となるとき、点列 $\{x_n\}$ を**コーシー列**という。また、X の任意のコーシー列が収束することを**コーシー完備**であるといい、このとき、X を**完備距離空間**であるという。 ◂

11.3.2 距離空間の開集合・閉集合

定義 11.11 距離空間 (X,d) において、X の部分集合 O が $\forall x \in O$ について、各 x に対し適当な $\epsilon > 0$ をとると $V_\epsilon(x) \subset O$ となるとき、O を**距離空間の意味で開集合**であるという。また、X, ϕ は距離空間の意味の開集合であると定義する。 ◂

定義 11.12 距離空間 (X,d) において、X の部分集合 F について、F^c が距離空間の意味で開集合であるとき、F は**閉集合**であるという。 ◂

定理 11.8 $\gamma \in \Gamma$ なる O_γ がすべて距離空間の意味で開集合であるとき $\bigcup_{\gamma\in\Gamma} O_\gamma$ も距離空間の意味で開集合である。

(proof)
$\forall x \in \bigcup_{\gamma\in\Gamma} O_\gamma$ について、$c \in \Gamma$ のどれかを選べば $x \in O_c$ である。したがって、適当な $\epsilon > 0$ をとれば $V_\epsilon(x) \subset O_c \subset \bigcup_{\gamma\in\Gamma} O_\gamma$ よって、$\bigcup_{\gamma\in\Gamma} O_\gamma$ は距離空間の意味で開集合である。 証明終

定理 11.9 O_1, O_2 が距離空間の意味で開集合のとき $O_1 \cup O_2$ も距離空間の意味で開集合である。

(proof)
$O_1 \cap O_2 = \phi$ のときは、定義よりこれは距離空間の意味で開集合である。$O_1 \cap O_2 \neq \phi$ のとき、$\forall x \in O_1 \cap O_2$ について $x \in O_1$かつ $x \in O_2$ である、O_1, O_2 が距離空間の意味で開集合なので、適当な $\epsilon > 0$ をとれば $V_\epsilon(x) \subset O_1$かつ $V_\epsilon(x) \subset O_2$ よって $V_\epsilon(x) \subset O_1 \cap O_2$ となり、$O_1 \cap O_2$ は開集合である。 証明終

以上の定理と、距離空間の意味での開集合の定義より、次のことが言える。

定理 11.10 距離空間 (X, d) において、距離空間の意味での開集合からなる集合族 $\mathfrak{O}$ をとると、$(X, \mathfrak{O})$ は位相空間になり、距離空間の意味の開集合は位相空間の意味でも開集合となる。

したがって、通常、距離空間においては、距離空間の開集合・閉集合のことを「距離空間の」という序詞を付けずに呼んでも問題ないわけである。

次の定理は、距離空間の閉集合の、最も本質的な性質であり、収束と位相概念を結びつけるものである。加算個の集合族に対する選択公理を用いれば、逆も成り立つことが分かる。

定理 11.11 距離空間 (X, d) において、X の部分集合 F が閉集合であるとき、F の点列 $\{x_n\}$ が x に収束するなら、$x \in F$ である。

(proof)
$x \notin F$ と仮定すると、$x \in F^c$ であるが、F^c は開集合なので適当な正数 ϵ を選べば

$$V_\epsilon(x) \subset F^c$$

となる。点列 $\{x_n\}$ は x に収束しているので、補題 11.7 より十分大きな n に対して

$$x_n \in V_\epsilon(x) \subset F^c$$

となることになるが、これは $\{x_n\}$ が F の点列であることに矛盾する。したがって $x \in F$ である。 証明終

定理 11.12 距離空間 (X, d) において、X の部分集合 F について、F の任意の収束列 $\{x_n\}$ の極限が F に含まれるならば、F は閉集合である。

(proof)
F が閉集合で無いとすると、F^c は開集合でない。従って、ある $\boldsymbol{b} \in F^c$ が存在して、任意の $\epsilon > 0$ に対して $V_\epsilon(\boldsymbol{b}) \not\subset F^c$ すなわち $V_\epsilon(\boldsymbol{b}) \cap F \neq \emptyset$ である。n を自然数とし、$V_{\frac{1}{n}}(\boldsymbol{b}) \cap F$ から選択公理により一要素を選び $\boldsymbol{x}_n$ とすると、点列 $\{\boldsymbol{x}_n\}$ は F 上の点列で、$\boldsymbol{b} \in F^c$ に収束する。つまり、F が閉集合で無いならば、F の収束列で極限が F に含まれないものが存在する。この対偶をとれば示される。 証明終

補題 11.13 開球は開集合である。

(proof)
開球を $V_r(a)$ とする。$\forall b \in V_r(a)$ について、$d(a, b) < r$ である。ここで、$r - d(a, b) > 0$ なので、$V_{r-d(a,b)}(b)$ という b の $r - d(a, b)$ 近傍 を考えることができる。$\forall x \in V_{r-d(a,b)}(b)$ について

$$\begin{aligned} d(b, x) &< r - d(a, b) \\ d(b, x) + d(a, b) &< r \\ d(a, x) &< r \quad \because \text{三角不等式} \end{aligned}$$

であるから、$x \in V_r(a)$ である。つまり、任意の $b \in V_r(a)$ に対し、正数 $r - d(a, b)$ をとることで $V_{r-d(a,b)}(b) \subset V_r(a)$ となるので、開球 $V_r(a)$ は開集合である。 証明終

補題 11.14 閉球は閉集合である。

(proof)
閉球を $\overline{V}_r(a)$ とする。$\forall b \in \overline{V}_r(a)^c$ について、$d(a,b) \geq r$ である。ここで、$d(a,b) - r > 0$ なので、$V_{d(a,b)-r}(b)$ という b の $d(a,b) - r$ 近傍 を考えることができる。$\forall x \in V_{d(a,b)-r}(b)$ について

$$\begin{aligned} d(b,x) &< d(a,b) - r \\ r + d(b,x) &< d(a,b) \\ r + d(b,x) &< d(a,x) + d(b,x) \quad \because \text{三角不等式} \\ r &< d(a,x) \end{aligned}$$

であるから、$x \in \overline{V}_r(a)^c$ である。つまり、任意の $b \in \overline{V}_r(a)^c$ に対し、正数 $d(a,b) - r$ をとることで $V_{d(a,b)-r} \subset \overline{V}_r(a)^c$ となるので、$\overline{V}_r(a)^c$ は開集合である。よって、閉球 $\overline{V}_r(a)$ は閉集合である。 証明終

11.4 近傍

定義 11.13 X を位相空間、$a \in X$ とする。このとき、X の部分集合 A について

$$a \in B \subset A$$

となる開集合 B が存在するとき、A は点 a の**近傍**であるという。◂

定理 11.15 位相空間 X とその部分集合 A について、A が開集合であることと、A の任意の点について $N \subset A$ なる近傍 N が存在することは、同値である。

(proof)
A が開集合であれば、A の任意の点について $N = A$ が $N \subset A$ なる近傍である。逆に、A の任意の点について $N \subset A$ なる近傍 N が存在するとき。そのような、$a \in A$ の近傍を $N(a)$ とすると、$\forall a \in A$ について、近傍の定義より

$$a \in O(a), O(a) \subset N(a)$$

なる開集合 $O(a)$ が存在する。これについて $a \in O(a) \subset \bigcup_{a' \in A} O(a')$ であるから、つまり

$$A \subset \bigcup_{a' \in A} O(a')$$

である。また、$O(a) \subset N(a) \subset A$ であるから

$$\bigcup_{a' \in A} O(a') \subset A$$

である。よって

$$A = \bigcup_{a' \in A} O(a')$$

となる。$O(a')$ はそれぞれ開集合なので、その和集合である A も開集合である。 証明終

距離空間においては、近傍は開球によって表される。

補題 11.16 距離空間では、そのある点 x について、開球 $V_\epsilon(x)$ は、x の近傍である。また、任意の x の近傍 N について

$$\exists \epsilon > 0, V_\epsilon(x) \subset N$$

となる。

11.5　連続写像

定義 11.14 X, Y を位相空間、f を $f : X \to Y$ なる写像、a を X の点とする。$f(a) \in Y$ の任意の近傍 N_Y に対して

$$f(N_X) \subset N_Y$$

となる $a \in X$ の近傍 N_X が存在するとき、f は**点 a で連続**であるという。また、$\forall x \in X$ について f が点 x で連続であるならば、f は**連続**であるという。◂

位相空間での近傍には、全空間も含まれており、近いという感覚はあまりない。連続の定義では、任意の近傍を対象とすることによって、一般の位相空間では表現しづらい「近づく」ということを表現している。

連続写像を通じて、別々の距離空間の収束をリンクさせることができる。

定理 11.17 $(X, d_X), (Y, d_Y)$ を距離空間、f を $f : X \to Y$ なる写像、a を X の点とする。このとき

$$f \text{ が } a \text{ で連続} \quad \leftrightarrow \quad \forall\epsilon, \exists\delta \qquad f(V_\delta(a)) \subset V_\epsilon(f(a))$$

である。

(proof)
f が a で連続であるとき。$f(a)$ の任意の近傍 N_Y に対して $f(N_X) \subset N_Y$ となる a の近傍 N_X が存在する。よって、補題 11.16 より、任意の $\forall\epsilon > 0$ について

$$f(N_X) \subset V_\epsilon(f(a))$$

となる a の近傍 N_X が存在する。このとき、補題 11.16 よりある δ が存在して

$$V_\delta(a) \subset N_X$$

である。よって、任意の ϵ について

$$f(V_\delta(a)) \subset f(N_X) \subset V_\epsilon(f(a))$$

である。

逆に　$\forall\epsilon, \exists\delta, f(V_\delta(a)) \subset V_\epsilon(f(a))$ であるとき。任意の $f(a)$ の近傍 N_Y について、補題 11.16 より、ある $\phi > 0$ が存在して $V_\phi(f(a)) \subset N_Y$ となる。よって、条件よりある δ が存在して

$$f(V_\delta(a)) \subset V_\phi(f(a)) \subset N_Y$$

であり、補題 11.16 から $V_\delta(a)$ は a の近傍である。よって示された。 証明終

定理 11.18 $(X, d_X), (Y, d_Y)$ を距離空間、f を $f : X \to Y$ なる写像、a を X の点とする。このとき

$$f \text{ が } a \text{ で連続} \quad \leftrightarrow \quad \lim_{n\to\infty} x_n = a \text{ なる任意の点列 } \{x_n\} \text{ について } \lim_{x\to\infty} f(x_n) = f(a)$$

である。

(proof)
f が a で連続であるとき。定理 11.17 より

$$\forall \epsilon, \exists \delta \qquad f(V_\delta(a)) \subset V_\epsilon(f(a))$$

である。これを言い換えると

$$\forall d(a,x) < \delta \text{ならば } d(f(a), f(x)) < \epsilon$$

である。$\lim_{n\to\infty} x_n = a$ なので、n を十分大きくとれば $d(a,x) < \delta$ とできる。よってこのとき任意の ϵ について $d(f(a), f(x)) < \epsilon$ となるのだから

$$\lim_{x\to\infty} f(x_n) = f(a)$$

である。

逆に、$\lim_{n\to\infty} x_n = a$ なる任意の点列 $\{x_n\}$ について $\lim_{n\to\infty} f(x_n) = f(a)$ であるとき。f が a で連続でないとすると、定理 11.17 より

$$\forall \delta, \exists \epsilon \quad f(V_\delta(a)) \not\subset V_\epsilon(f(a))$$

である。つまり、任意の δ に対して、ある ϵ が存在して $b \in V_\delta(a)$ かつ $f(b) \notin V_\epsilon(f(a))$ となる $b \in X$ が存在する。よって、$b_n \in V_{\frac{1}{n}}(a)$ かつ $f(b_n) \notin V_\epsilon(f(a))$ であるような点列 $\{b_n\}$ が存在する。これについては $d(b_n, a) < \frac{1}{n}$ であるから、

$$\lim_{n\to\infty} b_n = a$$

よって、条件より

$$\lim_{n\to\infty} f(b_n) = f(a)$$

である。つまり、n を十分大きくとれば

$$d(f(b_n), f(a)) < \epsilon$$

となるということだが、これは $f(b_n) \notin V_\epsilon(f(a))$ に矛盾する。よって f が a で連続である。 証明終

定理 11.19 距離関数は連続である。

(proof)
距離空間を (X,d) とする。$\forall a, b \in X$ について、任意の $x_n \to a, y_n \to b$ なる点列 $\{x_n\}\{y_n\}$ を考えたとき、三角不等式より

$$\begin{aligned} d(x_n, y_n) &\le d(x_n, a) + d(a, y_n) \\ &\le d(x_n, a) + d(y_n, b) + d(a, b) \\ d(x_n, y_n) - d(a, b) &\le d(x_n, a) + d(y_n, b) \end{aligned}$$

であり、また

$$\begin{aligned} d(a, b) &\le d(x_n, a) + d(b, x_n) \\ &\le d(x_n, a) + d(y_n, b) + d(x_n, y_n) \\ -(d(x_n, y_n) - d(a, b)) &\le d(x_n, a) + d(y_n, b) \end{aligned}$$

であるから

$$|d(x_n, y_n) - d(a, b)| \le d(x_n, a) + d(y_n, b)$$

である。したがって、条件より $n \to \infty$ とすると $d(x_n, a) \to 0, d(y_n, b) \to 0$ であるから

$$\lim_{n\to\infty} d(x_n, y_n) = d(a, b)$$

となる。$a, b \in X$ は任意だったので、定理 11.18 より距離関数 d は連続である。 証明終

定理 11.20 写像 $f : X \to Y$ が連続であることと、任意の Y の開集合 O について $f^{-1}(O)$ が X の開集合であることは、同値である。

(proof)
写像 $f : X \to Y$ が連続であるとき。O を Y の任意の開集合とする。$f^{-1}(O)$ が空集合ならば、これは確かに開集合である。$f^{-1}(O) \neq \phi$ であるとき。$\forall x \in f^{-1}(O)$ について、$f(x) \in O$ であり、O は $f(x)$ の近傍であるから、f の連続性より

$$f(N_x) \subset O \to N_x \subset f^{-1}(O)$$

となる x の近傍 N_x が存在する。よって、定理 11.15 より $f^{-1}(O)$ は開集合である。

逆に、任意の Y の開集合 O について $f^{-1}(O)$ が X の開集合であるとき。$\forall x \in X$ について、$f(x)$ の任意の近傍 N_Y を考えると、近傍の定義より $f(x) \in O \subset N_Y$ なる開集合 O が存在する。このとき、$x \in f^{-1}(O)$ であり、条件から $f^{-1}(O)$ は開集合なので $f^{-1}(O)$ は x の近傍である。また、$O \subset N_Y$ より

$$f^{-1}(O) \subset f^{-1}(N_Y)$$

であるから、$f(x)$ の任意の近傍 N_Y に対して、上記の関係を満たす x の近傍 $f^{-1}(O)$ が存在するということであり、任意の $x \in X$ について f は x で連続である。つまり、f は連続である。 証明終

コンパクトな位相空間から連続写像で移ることができる位相空間は再びコンパクトとなる。

定理 11.21 連続写像 $f : X \to Y$ について、X がコンパクトならば $f(X)$ もコンパクトである。

(proof)
$\{O_\gamma\}_{\gamma \in \Gamma}$ を $f(X)$ の開被覆とする。定理 11.20 より、$f^{-1}(O_\gamma)$ は開集合である。また、$\forall x \in X$ について

$$x \in f(X) \subset \bigcup_{\gamma \in \Gamma} O_\gamma$$

であるから

$$\exists \gamma' \in \Gamma \quad f(x) \subset O'_\gamma \leftrightarrow x \in f^{-1}(O'_\gamma)$$

である。$\therefore x \in f^{-1}(O'_\gamma) \subset \bigcup_{\gamma \in \Gamma} f^{-1}(O_\gamma)$ つまり

$$X \subset \bigcup_{\gamma \in \Gamma} f^{-1}(O_\gamma)$$

であり、$\{f^{-1}(O_\gamma)\}_{\gamma \in \Gamma}$ は X の開被覆である。X がコンパクトなので、このうちの有限個の $\{f^{-1}(O_1), \cdots, f^{-1}(O_m)\}$ によって

$$\begin{aligned} X &\subset \bigcup_{n=1}^{m} f^{-1}(O_n) \\ &= f^{-1}\left(\bigcup_{n=1}^{m} O_n\right) \quad \because m < \infty \end{aligned}$$

と覆われる。このとき

$$f(X) \subset f\left(f^{-1}\left(\bigcup_{n=1}^{m} O_n\right)\right) \subset \bigcup_{n=1}^{m} O_n \quad \because f(f^{-1}(A)) \subset A$$

であるから、もとの開被覆から選んだ $\{O_n\}$ は $f(X)$ の有限被覆である。よって、$f(X)$ はコンパクトである。
証明終

11.6 閉包・稠密性

定義 11.15 （閉包）位相空間 X の部分集合 A について、A を含む全ての閉集合の共通部分を A の**閉包**といい

$$\overline{A} = \bigcap_{F \text{ は閉集合}, A \subset F} F$$

で表す。定理 *11.1* より、閉包は閉集合である。明らかに任意の閉集合 $F(\supset A)$ に対して $\overline{A} \subset F$ である。言い換えれば、A の閉包は、A を含む最小の閉集合である。明らかに $A \subset \overline{A}$ は成立している。◂

定義 11.16 （稠密）位相空間 X の部分集合 A が**稠密**であるとは、$\overline{A} = X$ となることをいう。◂

定義 11.17 位相空間が X が**可分**であるとは、加算で稠密な部分集合を持つことを言う。◂

定理 11.22 A が閉集合であることと $A = \overline{A}$ であることは同値である。

(proof)
A が閉集合ならば、A は閉集合で $A \subset A$ なので $\overline{A} = \bigcap_{F \text{ は閉集合}, A \subset F} F \subset A$ であり、また、直前の定理より $A \subset \overline{A}$ なので、あわせて $A = \overline{A}$ である。また、逆に $A = \overline{A}$n ならば、閉包 $\overline{A}$ は閉集合なので当然 A は閉集合である。 証明終

11.6.1 集積点

定義 11.18 （集積点）点 $\boldsymbol{x}$ が距離空間の部分集合 A の**集積点**であるとは、適当な A の点列 $\{\boldsymbol{x}_n\}$ により $\lim_{n\to\infty} \boldsymbol{x}_n = \boldsymbol{x}$ となることをいう。◂

距離空間において、ある集合の集積点とは、その集合上の点列の極限である。閉集合でなければ、ある集合の集積点が再びその集合上の点であるかはわからない。逆に、定理 11.11 より、閉集合の集積点は、再びもとの閉集合に含まれる。

定理 11.23 距離空間において、A の閉包は、A に A の集積点全てを加えた集合である。

(proof)
A に A の集積点全てを加えた集合を S とする。$S = \overline{A}$ を示せばよい。まず、定理 11.11 より、A の閉包は A の集積点全てを含む。$A \subset \overline{A}$ は常に成立するので、$S \subset \overline{A}$ である。また、明らかに、任意の S の収束列の極限（集積点となる）は S に含まれる。したがって、定理 11.12 より S は閉集合である。よって閉包の定義より $\overline{A} \subset S$ である。あわせて $S = \overline{A}$ である。よって示された。 証明終

これを用いれば、稠密性の距離空間における言いかえが示される。

定理 11.24 距離空間 X の部分集合 A について、A が稠密であることは、任意の $\boldsymbol{x} \in X$ が、A の点列 $\{\boldsymbol{x}_n\}$ によって $\boldsymbol{x} = \lim_{n\to\infty} \boldsymbol{x}_n$ となることと同値である。

12 順序体と位相

12.1 距離空間としての順序体

アルキメデスの公理を満たす順序体 K を考える。その完備化は実数体であり、$K \subset \boldsymbol{R}$ とみなせる。そのため、絶対値によって $d(x, y) = |x - y|$ とすると $d : K \times K \to \boldsymbol{R}$ とみなすことができ、距離関数としての性質をすべて満たしている。そのため、アルキメデスの公理を満たす順序体は距離空間としての位相を導入で

きる。

K の点列 $\{x_n\}$ が距離空間として a に収束することは、任意の $\epsilon > 0$ に対してある N が存在して $N \leq n$ について

$$|x_n - a - 0| = |x_n - a| \leq \epsilon$$

が成立することにほかならず、順序体としての収束と同値である。コーシー列の定義も同値となる。距離空間としての完備性はコーシー完備そのものである。

12.2 距離空間としての実数体

実数体も絶対値を以て距離空間であり、距離空間としても完備である。

定理 12.1 実数体上で、有理数体は稠密である。

(proof)
実数体は有理数体の完備化して得ることができた。任意の実数 a に対して、完備化の手続きにおいて a を表現する有理数によるコーシー列のひとつを $\{a_n\}$ とする。実数体はコーシー完備であり、実数体上で $\{a_n\}$ は a に収束している。よって、定理 11.24 より示される。 証明終

系 12.2 任意の実数に対して、それを極限とする収束列が存在する。

12.2.1 実数体とコンパクト性

定義 12.1 実数 $a, b \in \boldsymbol{R}$ について、$[a,b] \equiv \overline{V}_{\frac{b-a}{2}}\left(\frac{a+b}{2}\right) = \{x :\in \boldsymbol{R} : a \leq x \leq b\}$ を**閉区間**といい、$(a,b) \equiv V_{\frac{b-a}{2}}\left(\frac{a+b}{2}\right) = \{x :\in \boldsymbol{R} : a < x < b\}$ を**開区間**という。また $[a,b) \equiv \{x :\in \boldsymbol{R} : a \leq x < b\}$ を**半開区間**という。◂

定理 12.3 実数体 $\boldsymbol{R}$ の有界閉区間はコンパクトである。

(proof)
有界閉区間 $[a,b]$ と、その開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ を考える。

$$A = \{x | [a,x] \text{ が } \{O_\gamma\}_{\gamma\in\Gamma} \text{の有限部分被覆で覆われる }\}$$

とおく。開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ の中には、必ず a を含むものがあるので、それを持ってくることによって $[a,a] = \{a\}$ は有限部分被覆で覆われる。すなわち $a \in A$ であり、A は空集合ではない。また、x が十分大きい時、$[a,x]$ は $[a,b]$ の開被覆では覆えない。よって、A は上に有界である。したがって、$\boldsymbol{R}$ は順序完備なので、上限 $\sup A$ が存在する。

ここで、$\sup A < b$ と仮定する。$a \leq \sup A < b$ なので、$\sup A$ は、開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ のある開集合 O' に含まれる。O' が開集合なので、適当な正数 ϵ をとると、$V_\epsilon(\sup A) \subset O'$ となる。よって、$\sup A < d < \sup A + \epsilon$ となる d を選んでおくと

$$(\sup A, d] \subset (\sup A - \epsilon, \sup A + \epsilon) = V_\epsilon(\sup A) \subset O'$$

である。A の定義より $[a, \sup A]$ は開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ の有限部分被覆 $\{O_1, \cdots, O_s\}$ によって覆われる。このとき、

$$[a,d] = [a, \sup A] + (\sup A, d] \subset O_1 \cup \cdots \cup O_s \cup O'$$

となる。すなわち $[a,d]$ が開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ の有限部分被覆で覆われるということであり、これは $\sup A$ が A の上限であることに矛盾する。したがって、$b \leq \sup A$ である。このとき $[a,b] \subset [a, \sup A]$ であり、$[a, \sup A]$ は $[a,b]$ の開被覆 $\{O_\gamma\}_{\gamma\in\Gamma}$ の有限部分被覆で覆われるので、$[a,b]$ もその有限部分被覆によって覆われる。よって、$[a,b]$ はコンパクトである。 証明終

定理 12.4 実数体 $\boldsymbol{R}$ において、有界閉集合であることと、コンパクト集合であることは同値である。

(proof)
$\boldsymbol{R}$ の有界閉集合を F とする。有界であることより、$F \subset [-a, a]$ となる $a > 0$ が存在する。上述の定理より $[-a, a]$ はコンパクトであり、F はその部分閉集合なので、定理 11.3 より F もコンパクトである。

逆について、$\boldsymbol{R}$ のコンパクト集合を C とする。補題 11.13 より、開区間は開集合なので、$(-a, a) \quad (a = 1, 2, \cdots)$ の全体は A の開被覆であるが、C はコンパクトなのでそのうちの有限個によって覆われる。この有限部分被覆のうち最大のものを $(-N, N)^n$ とすると、$C \subset (-N, N)^n \subset [-N-1, N+1]^n$ であるので、C は有界である。

また、任意の $x \in C^c$ をとり [16]、x を中心とする閉球の補集合による集合族 $\{\overline{V}_{\frac{1}{m}}(x)^c\}_{m \in \boldsymbol{Z}}$ を考える。$\forall y \in C$ について、補題 11.5 より $d(x, y) > 0$ である。よって $d(x, y) > \frac{1}{M} > 0$ なる $M \in \boldsymbol{Z}$ をとれば

$$y \notin \overline{V}_{\frac{1}{M}}(x) \quad \Leftrightarrow \quad y \in \overline{V}_{\frac{1}{M}}(x)^c \quad \therefore C^c \subset \bigcup_{m \in \boldsymbol{Z}} \overline{V}_{\frac{1}{m}}(x)^c$$

となる。さらに、補題 11.14 より $\overline{V}_{\frac{1}{m}}(x)$ は閉集合なので、$\overline{V}_{\frac{1}{m}}(x)^c$ は開集合である。よって、$\{\overline{V}_{\frac{1}{m}}(x)^c\}_{m \in \boldsymbol{Z}}$ は C の開被覆である。C はコンパクトなので、この中から C の有限部分被覆をとることができる。そのうち最大のもの、すなわち m が最小のものを $\overline{V}_{\frac{1}{m'}}(x)^c$ とすれば、これは有限部分被覆の他のどの開集合も含むので

$$C \subset \overline{V}_{\frac{1}{m'}}(x)^c \quad \Leftrightarrow \quad \overline{V}_{\frac{1}{m'}}(x) \subset C^c$$

となる。すなわち、任意の $x \in C^c$ に関して、正数 $\frac{1}{m'}$ をとれば $\overline{V}_{\frac{1}{m'}}(x) \subset C^c$ となるので、C^c は開集合である。よって C は閉集合である。 証明終

実数体 $\boldsymbol{R}$ 上で、有界閉集合は位相の観点からコンパクト性と同値であるという特別な意味が与えられた。さらに、実数体上では最大値・最小値の存在と密接に関連している。

定理 12.5 実数体 $\boldsymbol{R}$ の上に有界な閉集合は、最大値を持ち、下に有界な閉集合は、最小値を持つ。

(proof)
実数体 $\boldsymbol{R}$ の有界閉集合を A とする。最大値について考える。最小値についても同様に証明可能である。上に有界なので、実数の順序完備性より上限 $\sup A$ が存在する。任意の $a \in A$ に対して $a \leq \sup A$ が成立している。$\sup A \neq A$ と仮定する。このとき、任意の $a \in A$ に対して $a < \sup A$ が成立している。$a_k \in A$ をとる。このとき、$a_k < \sup A$ であり $a_k < \dfrac{a_k + \sup A}{2} < \sup A$ が成立している。よって、上限の定義より $\dfrac{a_k + \sup A}{2} < a_{k+1}$ となる $a_{k+1} \in A$ が存在する。このときやはり $\dfrac{a_k + \sup A}{2} < a_{k+1} < \sup A$ である。よって $\dfrac{a_k - \sup A}{2} < a_{k+1} - \sup A < 0$ であり

$$\frac{|a_k - \sup A|}{2} > |a_{k+1} - \sup A|$$

が成立している。よって、$a_0 \in A$ をとって、うえの規則により数列 $\{a_n\}$ をつくると、$|a_n - \sup A|$ がいくらでも小さくなることから $\sup A$ に収束している。このとき、A が閉集合なので定理 11.11 より $\sup A \in A$ となり矛盾する。よって $\sup A \in A$ が成立しており、$\sup A$ が最大値に他ならない。 証明終

系 12.6 実数体 $\boldsymbol{R}$ の有界閉集合は、最大値・最小値をもつ。

[16] C^c は C の補集合を表す。

コンパクト性は連続写像によって保存され、実数体ではコンパクト性が有界閉集合と同値であり、最大値・最小値の存在を保証することから、コンパクトな集合から実数への連続写像については、最大値・最小値の存在が保証される。これは、原理上も応用上も極めて重要な性質である。

定理 12.7 位相空間 X のコンパクトな部分集合 A と連続写像 $f : X \to \boldsymbol{R}$ については、$f(A) \subset \boldsymbol{R}$ に最大値・最小値が存在する。

(proof)
定理 11.21 より、$f(A)$ はコンパクトである。よって、定理 12.4 より $f(A)$ は有界閉集合である。ゆえに、定理 12.6 より、$f(A)$ に最大値・最小値が存在する。 証明終

12.2.2 中間値の定理

連続写像の概念が導入されたことにより、解の存在を保証する中間値の定理を考えることができる。

定理 12.8 実数体の有界閉区間 $[a,b]$ 上で連続な写像 $f : [a,b] \to \boldsymbol{R}$ について $f(a) < 0, f(b) > 0$ が成立しているとする。このとき、$f(c) = 0$ となる $c \in [a,b]$ が存在する。

(proof)
$A \equiv \{x \in [a,b] : f(x) \leq 0\}$ とする。A は上に有界であることから上限が存在する。$c = \sup A$ とする。まず、$a \in A$ なので $a \leq c$ である。また、$A \subset [a,b]$ であり $c = \sup A \leq \sup[a,b] = b$ である。つまり $a \leq c \leq b$ を満たしている。

$f(c) < 0$ と仮定する。f は c で連続であるため、ある $\delta > 0$ が存在して

$$f([c-\delta, c+\delta]) \subset V_{0.5|f(c)|}(f(c)) = (1.5f(c), 0.5f(c))$$

が成立する。このとき特に $f(c+\delta) < 0.5f(c) < 0$ であり、c が上限であることに矛盾する。よって $0 \leq f(c)$ である。

$0 < f(c)$ と仮定する。f は c で連続であるため、ある $\delta > 0$ が存在して

$$f([c-\delta, c+\delta]) \subset V_{f(c)}(f(c)) = (0, 2f(c))$$

が成立する。c は上限なので $c - \delta < a' \leq c \in A$ となる a' が存在する。このとき $0 \leq f(a')$ であるが、これは $f(a') \subset f([c-\delta, c+\delta]) \subset (0, 2f(c))$ に矛盾する。よって $f(c) = 0$ でなければならない。 証明終

12.2.3 実数の多項式

実数の多項式 $f(x) \in \boldsymbol{R}[x]$ は、代入によって $f : \boldsymbol{R} \to \boldsymbol{R}$ なる写像と考えることができる。さらに、これは連続写像である。

定理 12.9 実数の多項式 $f(x) \in \boldsymbol{R}[x]$ は任意の実数において連続である。

(proof)
a を任意の実数とし、$\{a_n\}$ を a に収束する任意の数列とする。$f(x) = \sum_i b_i x^i$ と表しておく。

$$\begin{aligned}\lim_{n\to\infty} f(a_n) &= \lim_{n\to\infty} \sum_i b_i (a_n)^i \\ &= \sum_i \lim_{n\to\infty} b_i (a_n)^i \quad \because \text{和の極限} \\ &= \sum_i b_i a^i \quad \because \text{積の極限} \\ &= f(a)\end{aligned}$$

となるため、定理 11.18 より $f(x)$ は任意の実数において連続である。 証明終

よって、実数の多項式においては、中間値の定理により解の存在を検討することができる。

12.2.4 n 重根

n を自然数とし、実数の多項式 $f(x) = x^n - a$ の解を検討しよう。$a = 0$ ならば $x = 0$ が解である。まず $0 < a < 1$ の場合を検討しよう。$f(0) = -a < 0$ であり $f(1) = 1 - a > 0$ なので中間値の定理 12.8 より $f(c) = 0$ なる $0 \leq c \leq 1$ が存在する。つぎは、$1 \leq a$ の場合を考える。$a = 1$ ならば $x = 1$ が解である。$1 < a$ のときは $a < a^n$ が成立している。よって $f(0) = -a < 0, f(a) = a^n - a > 0$ なので $f(c) = 0$ なる $0 \leq c \leq a$ が存在する。

定義 12.2 （**n 重根**）自然数 n, 実数 a について、実数の多項式 $x^n - a$ の解を **n 重根**という。また、そのうち a と符号が等しいものを $a^{\frac{1}{n}}$ と表す。とくに $\sqrt{a} = a^{\frac{1}{2}}$ と表す。◂

上に見たとおり、$0 \leq a$ については n 重根は存在する。順序の性質により、n 重根が存在するとき、その絶対値は一意である。より詳しい構造は n が偶数か奇数かによって異なる。

n が偶数のとき x^n は $a > 0$ に対して n 重根は正負二つ存在する。一方で、x^n がつねに非負であるため、$a < 0$ に対して n 重根が存在しない。

n が奇数のとき x^n は $a > 0$ に対して n 重根はひとつ存在する。また、$a < 0$ に対しても n 重根がひとつだけ存在する。

13 ユークリッド空間

定義 13.1 $\boldsymbol{R}$ を実数体とする。$\boldsymbol{R^n}$ に

$$\boldsymbol{x} = (x_1, \cdots, x_n), \boldsymbol{y} = (y_1, \cdots, y_n) \in \boldsymbol{R^n} \quad ; \quad d(\boldsymbol{x}, \boldsymbol{y}) = \sqrt{\sum_{k=1}^{n} (x_k - y_k)^2}$$

という距離を導入すると、$(\boldsymbol{R^n}, d)$ は距離空間となる。これを**ユークリッド空間**と言い、d を**標準距離・ユークリッド距離**と称する。◂

距離空間であるので、定義 11.11 及び 11.12 により**開集合・閉集合**を定義できる。他の距離空間・位相空間に関する事項も同様である。

13.1 積位相空間による開集合の定義

$\boldsymbol{R}$ 自身も距離空間なので、$\boldsymbol{R^n}$ の開集合族を $\boldsymbol{R}$ の積位相空間 (p68) から定義することもできる、すなわち

$$O = O_1 \times \cdots \times O_n \subset \boldsymbol{R^n} \text{が開集合} \Leftrightarrow O_1, \cdots, O_n \text{がすべて} \boldsymbol{R} \text{の開集合}$$

と定義すれば、これは定理 11.2 より位相空間の開集合族の条件を満たす。こうして得られた、積位相空間としての開集合は、ユークリッド距離による開集合と一見異なるが、実のところ、この二つは同値である。

定理 13.1 $O = O_1 \times \cdots \times O_n \subset \boldsymbol{R^n}$ が、積位相空間としての $\boldsymbol{R^n}$ の開集合であることと、ユークリッド距離空間としての開集合であることは、同値である。

(proof)
$O = O_1 \times \cdots \times O_n \subset \boldsymbol{R^n}$ が、積位相空間としての $\boldsymbol{R^n}$ の開集合であるとき。まず

$$O_i\text{が } \boldsymbol{R} \text{ の開集合である} \quad \Leftrightarrow \quad \forall a \in O_i\text{に対して適当な正数}\epsilon\text{をとると } V_\epsilon(a) \subset O_i\text{となる}$$

である。ここでは $V_\epsilon(a) = \{x; |x - a| < \epsilon\}$ であるから、O が積位相空間としての $\boldsymbol{R^n}$ の開集合であるとは、

$\forall \boldsymbol{a} = (a_1, \cdots, a_n) \in O$ に対して適当な正数 $\epsilon_1, \cdots, \epsilon_n$ をとると
$\{(x_1, \cdots, x_n); |x_1 - a_1| < \epsilon_1, \cdots, |x_n - a_n| < \epsilon_n\} \subset O$ となる

ことである。

このとき、$\epsilon \equiv min(\epsilon_1, \cdots, \epsilon_n)$ とすると

$$\{(x_1, \cdots, x_n); |x_1 - a_1| < \epsilon, \cdots, |x_n - a_n| < \epsilon\} \subset O$$

である。$\forall \boldsymbol{y} \in V_\epsilon(\boldsymbol{a})$ について

$$|y_i - a_i|^2 \leq \sum_{k=1}^{n} |y_k - a_k|^2 = d(\boldsymbol{y}, \boldsymbol{a})^2 < \epsilon^2$$

よって $\boldsymbol{y} \in \{(x_1, \cdots, x_n); |x_1 - a_1| < \epsilon, \cdots, |x_n - a_n| < \epsilon\}$ であるからつまり

$$\begin{aligned} V_\epsilon(\boldsymbol{a}) &\subset \{(x_1, \cdots, x_n); |x_1 - a_1| < \epsilon, \cdots, |x_n - a_n| < \epsilon\} \\ &\subset O \quad \because (13.1) \end{aligned}$$

であり、任意の $\boldsymbol{a} \in O$ について適当な $\epsilon > 0$ をとると $V_\epsilon(\boldsymbol{a}) \subset O$ が成り立つので、O はユークリッド距離空間の意味でも開集合である。

逆に、O がユークリッド距離空間の意味で開集合であるとき。任意の $\boldsymbol{a} \in O$ について適当な $\epsilon > 0$ をとると $V_{\epsilon\sqrt{n}}(\boldsymbol{a}) \subset O$ が成り立つ。$\forall \boldsymbol{x} \in \{(x_1, \cdots, x_n); |x_1 - a_1| < \epsilon, \cdots, |x_n - a_n| < \epsilon\}$ について

$$\begin{aligned} d(\boldsymbol{x}, \boldsymbol{a})^2 &= \sum_{i=1}^{n} |x_i - a_i|^2 \\ &< \sum_{i=1}^{n} \epsilon^2 = n\epsilon^2 \\ d(\boldsymbol{x}, \boldsymbol{a}) &< \epsilon\sqrt{n} \end{aligned}$$

よって、$\boldsymbol{x} \in V_{\epsilon\sqrt{n}}$ である。つまり

$$\{(y_1, \cdots, y_n); |y_1 - a_1| < \epsilon, \cdots, |y_n - a_n| < \epsilon\} \subset V_{\epsilon\sqrt{n}} \subset O$$

であり、任意の $\boldsymbol{a} \in O$ について適当な $\epsilon > 0$ をとると $\{(y_1, \cdots, y_n); |y_1 - a_1| < \epsilon, \cdots, |y_n - a_n| < \epsilon\} \subset O$ が成り立つので、O は $\boldsymbol{R}$ の積位相空間の意味でも開集合である。 証明終

13.2 半開区間・開区間・閉区間

定義 13.2 $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{R^n}$ について

$$[\boldsymbol{a}, \boldsymbol{b}) \equiv [a_1, b_1) \times \cdots \times [a_n, b_n) = \{(x_1, \cdots, x_n); a_1 \leq x_1 < b_1, \cdots, a_n \leq x_n < b_n\}$$

と定義し、これを**半開区間**という。同様に**閉区間**もしくは $\boldsymbol{n}$ **次元長方形**を

$$[\boldsymbol{a},\boldsymbol{b}] \equiv [a_1,b_1]\times\cdots\times[a_n,b_n] = \{(x_1,\cdots,x_n); a_1 \le x_1 \le b_1,\cdots,a_n \le x_n \le b_n\}$$

と定義し、また**開区間**を

$$(\boldsymbol{a},\boldsymbol{b}) \equiv (a_1,b_1)\times\cdots\times(a_n,b_n) = \{(x_1,\cdots,x_n); a_1 < x_1 < b_1,\cdots,a_n < x_n < b_n\}$$

と定義する。また、これらについて、その大きさを

$$|[\boldsymbol{a},\boldsymbol{b})| \equiv |[\boldsymbol{a},\boldsymbol{b}]| \equiv |(\boldsymbol{a},\boldsymbol{b})| \equiv |a_1-b_1|\cdots|a_n-b_n|$$

と定義する。 ◂

定義 13.3 $\boldsymbol{R^n}$ の部分集合 A が**有界**であるとは、適切な閉区間 I をとったとき $A \subset I$ となることをいう。◂

定理 13.2 半開区間の共通部分は半開区間である。

(proof)
定義を考えると

$$\begin{aligned}&[b_1,a_1)\times\cdots\times[b_n,a_n)\cap[b_1',a_1')\times\cdots\times[b_n',a_n')\\ =&[min(b_1,b_1')-max(a_1,a_1'))\times\cdots\times[min(b_n,b_n')-max(a_n,a_n'))\end{aligned}$$

である。よって示された。 証明終

定理 13.3 半開区間 $I_1 \subset I_2$ について $|I_1| \le |I_2|$

(proof)
各次元について $|b_i - a_i|$ を考えればよい。容易。詳細略。 証明終

補題 13.4 開区間は開集合である。

(proof)
$\boldsymbol{R}$ では、$(a,b) = V_{\frac{|a-b|}{2}}(\frac{a+b}{2})$ なので、補題 11.13 より、開集合である。

$\boldsymbol{R^n}$ の開区間は、$\boldsymbol{R}$ の開区間の直積なので、積位相空間の意味では開集合である。よって、定理 13.1 より、$\boldsymbol{R^n}$ の開区間は開集合である。 証明終

13.3 コンパクト

ユークリッド空間においても、コンパクトであることと有界閉集合であることが同値である。片方づつ示そう。

定理 13.5 $\boldsymbol{R^n}$ の有界閉集合はコンパクトである。

(proof)
$\boldsymbol{R^n}$ の有界閉集合を F とおく。有界なので十分大きな閉区間 $[-\boldsymbol{a},\boldsymbol{a}]$ をとれば $F \subset [-\boldsymbol{a},\boldsymbol{a}] = [-a,a]^n$ となる。定理 12.3 より $[-a,a]$ はコンパクトであり、したがって、定理 11.4 より $[-\boldsymbol{a},\boldsymbol{a}] = [-a,a]^n$ もコンパクトである。F はその部分閉集合なので、定理 11.3 より F もコンパクトである。 証明終

定理 13.6 $\boldsymbol{R^n}$ のコンパクトな集合は、有界閉集合である。

(proof)
C を $\boldsymbol{R^n}$ のコンパクト集合とする。補題 13.4 より、開区間は開集合なので、$(-a,a)^n \quad (a=1,2,\cdots)$ の全体は A の開被覆であるが、C はコンパクトなのでそのうちの有限個によって覆われる。この有限部分被覆のうち最大のものを $(-N,N)^n$ とすると、$C \subset (-N,N)^n \subset [-N-1,N+1]^n$ であるので、C は有界である。

また、任意の $x \in C^c$ をとり、x を中心とする閉球の補集合による集合族 $\{\overline{V}_{\frac{1}{m}}(x)^c\}_{m\in\boldsymbol{Z}}$ を考える。$\forall y \in C$ について、補題 11.5 より $d(x,y)>0$ である。よって $d(x,y) > \frac{1}{M} > 0$ なる $M \in \boldsymbol{Z}$ をとれば

$$y \notin \overline{V}_{\frac{1}{M}}(x) \quad \Leftrightarrow \quad y \in \overline{V}_{\frac{1}{M}}(x)^c \quad \therefore C^c \subset \bigcup_{m\in\boldsymbol{Z}} \overline{V}_{\frac{1}{m}}(x)^c$$

となる。さらに、補題 11.14 より $\overline{V}_{\frac{1}{m}}(x)$ は閉集合なので、$\overline{V}_{\frac{1}{m}}(x)^c$ は開集合である。よって、$\{\overline{V}_{\frac{1}{m}}(x)^c\}_{m\in\boldsymbol{Z}}$ は C の開被覆である。C はコンパクトなので、この中から C の有限部分被覆をとることができる。そのうち最大のもの、すなわち m が最小のものを $\overline{V}_{\frac{1}{m'}}(x)^c$ とすれば、これは有限部分被覆の他のどの開集合も含むので

$$C \subset \overline{V}_{\frac{1}{m'}}(x)^c \quad \Leftrightarrow \quad \overline{V}_{\frac{1}{m'}}(x) \subset C^c$$

となる。すなわち、任意の $x \in C^c$ に関して、正数 $\frac{1}{m'}$ をとれば $\overline{V}_{\frac{1}{m'}}(x) \subset C^c$ となるので、C^c は開集合である。よって C は閉集合である。 証明終

補題 13.7 閉区間はコンパクトであり、有界閉集合である。

(proof)
閉区間を $[a_1,b_1]\times\cdots\times[a_n,b_n]$ とする。定理 12.3 より、各 $[a_1,b_1],\cdots,[a_n,b_n]$ はコンパクトである。よって、定理 11.4 より閉区間 $[a_1,b_1]\times\cdots\times[a_n,b_n]$ はコンパクトである。したがって、定理 13.6 よりこれは有界閉集合である。 証明終

補題 13.8 $\boldsymbol{R^n}$ の閉球はコンパクトである。

(proof)
任意の閉球に対して、それを含む閉区間が存在する。（定理 13.1 と同様。）直前の補題より、閉区間はコンパクトである。閉球は、コンパクト集合である閉区間の部分閉集合なので、定理 11.3 より、閉球はコンパクトである。 証明終

13.4 完備性

定理 13.9 ユークリッド空間 $\boldsymbol{R^n}$ はコーシー完備である。

(proof)
$\boldsymbol{R^n}$ の任意のコーシー列 $\{\boldsymbol{x}_k\}$ について、その i 要素を x_k^i と表示することにする。コーシー列であることより、任意の $\epsilon>0$ に対して、L が存在して $L \le k,m$ について

$$d(\boldsymbol{x}_k,\boldsymbol{x}_m) \le \epsilon$$

が成立する。このとき

$$|x_k^i - x_m^i|^2 \le \sum_i (x_k^i - x_m^i)^2 \le \epsilon^2$$

なので $|x_k^i - x_m^i| \le \epsilon$ が成立しており、各 i について $\{x_k^i\}$ もコーシー列であり、収束する。この極限を c_i とし、$\boldsymbol{c}=(c_1,\cdots,c_n)$ とする。このとき、任意の $\epsilon>0$ について、十分大きい k に対しては

$$|x_k^i - c_i| < \frac{\epsilon}{\sqrt{n}}$$

が成立するので

$$\begin{aligned} d(\boldsymbol{x}_k, \boldsymbol{c}) &= \sqrt{\sum_i |x_k^i - c_i|^2} \\ &\leq \sqrt{\sum_i \frac{\epsilon^2}{n}} \\ &= \sqrt{\epsilon^2} = \epsilon \end{aligned}$$

より、任意のコーシー列 $\{\boldsymbol{x}_k\}$ が収束している。 証明終

14　多項式の解と複素数

体の多項式（多変数でない）は、すでに定理 7.10 で示しているとおり、ユークリッド整域であり、単項イデアル整域・一意分解整域でもある。

14.1　代数的・超越的

$(K, +, \cdots)$ を体とする。K の多項式 $K[x]$ の解がどのようになっているかは興味のあるところである。そこで $a \in K$ を固定し、$K[a] \equiv \{f(a) : f(x) \in K[x]\} \subset K$ と定める。写像 $\phi_a : K[x] \to K[a]$ を

$$\phi_a : f(x) \mapsto f(a)$$

によって定める。ϕ_a は全射かつ準同型写像である。したがって、核 $\ker \phi_a (\subset K[x])$ はイデアルである。環の準同型定理 6.11 より、像 $\phi_a(K[x]) = K[a]$ と剰余環 $K[x]/\ker \phi_a$ が同型である。

核 $\ker \phi_a$ には必ず $0 \in K[x]$ は含まれる。$\ker \phi_a = \{0\}$ のとき、$a \in K$ は**超越的**であるという。$\ker \phi_a \neq \{0\}$ のとき、$a \in K$ は**代数的**であるという。

a が超越的であることは、多項式の解として a が表せないことを意味している。また、a が超越的であるとき、剰余環 $K[x]/\ker \phi_a$ は $K[x]$ そのものなので、$\phi_a(K[x]) = K[a]$ と $K[x]$ が同型であり、ϕ_a は同型写像である。

a が代数的であるとき、$K[x]$ が単項イデアル整域であることより、$\ker \phi_a = (p_a(x))$ を満たす多項式 $p_a(x) \in K[x]$ が存在する。このとき、$p_a(x)$ を a の**最小多項式**という。最小多項式は同伴なもの、すなわち、K の定数倍を除いて一意である。特に断らない限り、最小多項式はモニックなものを選ぶものとする。

多項式 $f(x) \in K[x]$ が解として a を持つ（$f(a) = 0$）ことは、$f(x) \in \ker \phi_a = (p_a(x))$ と同値である。よって

$$f(a) = 0 \ \Leftrightarrow \ p_a(x) | f(x)$$

が成立し、多項式が解として a を持つことと、最小多項式の倍元であることが同値である。また、$p_a(a) = 0$ も当然成立している。

14.2　体の拡大

定義 14.1　（部分体・拡大体）体 $(K, +, \cdot)$ について、$E \subset K$ について $(E, +, \cdots)$ が体であるとき、E を K の**部分体**といい、K を E の**拡大体**という。◂

典型的には、体 $(K, +, \cdot)$ について、多項式環 $K[x]$ はその拡大体である。

さて、ここで体の多項式環 $K[x]$ の剰余環について考える。$K[x]$ は単項イデアル整域であることに注意する。$K[x]$ の任意のイデアルは単項イデアルであるため、多項式 $p(x)$ によって $I = (p(x))$ のように表すことができる。このとき、剰余環 $K[x]/(p(x))$ はどのようなものであろうか。剰余環のそれぞれの元は、代表元のひとつを $g(x)$ とすると $g(x) + h(x),\ h(x) \in (p(x))$ の形で表される元の集合（同値類）である。すなわち

$$g(x) + p(x)Q(x)$$

の形で表される元の集合ということになる。体の多項式では常に整除が行えるため

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

を満たす $r(x), q(x)$ が一意に存在する。したがって

$$\begin{aligned} g(x) + p(x)Q(x) &= p(x)q(x) + r(x) + p(x)Q(x) \\ &= p(x)(q(x) + Q(x)) + r(x) \end{aligned}$$

であり、剰余環 $K[x]/(p(x))$ を構成する同値類に属する多項式は、すべて余りが $r(x)$ に等しい。このとき、同値類 $[r(x)] = [g(x)]$ は

$$r(x) + p(x)f(x)$$

の形に表される多項式の集合であり、剰余環は余りが等しい多項式をひとまとめにしたものといえる。（まさにこれが剰余環の名称の由来でもある。）

ここで $\deg p(x) \geq 1$ であれば、定数 $a \in K$ を $p(x)$ で整除した余りは a そのものである。つまり、剰余環 $K[x]/(p(x))$ は K を含むと考えることができる。さらに $p(x)$ が素元（**既約多項式**と呼ばれる。）であれば、系 6.43 より $K[x]/(p(x))$ は体であり、K の拡大体である。

さて、$p(x)$ は次数が 1 以上の既約多項式であるとし、K から拡大体 $K[x]/(p(x))$ への同値類をとる写像

$$\phi : f(x) \mapsto [f(x)]$$

を考える。この写像は準同型写像である。K の定数 a に対して、$\phi(a)$ は $K[x]/(p(x))$ において K に対応する元であり、$K[x]/(p(x))$ を拡大体と考えることは $\phi(a) = a$ とみなすことに相当する。ここで $\alpha \equiv \phi(x) \in K[x]/(p(x))$ とおく。K の多項式

$$f(x) = \sum_i a_i x^i$$

は、$K[x]/(p(x))$ を K の拡大体と考えているため、$K[x]/(p(x))$ の多項式ともみなすことができ

$$\begin{aligned} \phi(f(x)) = \phi\left(\sum_i a_i x^i\right) &= \sum_i \phi\left(a_i x^i\right) \\ &= \sum_i \phi(a_i)\,\phi(x)^i \\ &= \sum_i a_i \alpha^i \end{aligned}$$

が成立することから、$K[x]/(p(x))$ において、$K[x]/(p(x))$ の多項式 $f(x)$ に α を代入したもの $f(\alpha)$ であると考えることができる。とくに、$p(x)$ について $\phi(p(x)) = p(\alpha) \in K[x]/(p(x))$ であり、また

$$\phi(p(x)) = [p(x)] = [0] = \phi(0) = 0$$

であることから

$$p(\alpha) = 0$$

が成立する。以上のことは、K の既約多項式 $p(x)$ が K において解を持つかどうかにかかわらず、K の拡大体 $E \equiv K[x]/(p(x))$ をつくれば、拡大体 E において多項式 $p(x)$ は必ず解をひとつは持つようにできるということである。

定理 14.1 体 K とその既約多項式 $p(x)$ について、少なくとも $K[x]/(p(x))$ を以て、$p(x)$ が解を持つような K の拡大体が存在する。

14.3 複素数体の構成

すでに見たとおり、実数体 $\boldsymbol{R}$ において、x^2+1 の解 $\sqrt{-1}$ は存在しない。しかし、上に見た方法により x^2+1 が解を持つ拡大体 $\boldsymbol{R}[i]/(i^2+1)$ を構成することができる。これは**複素数体**と呼ばれており、$\boldsymbol{C}$ で表される。複素数体の元は**複素数**といわれる。

複素数は、実数の多項式 $\boldsymbol{R}[i]$ を考え、差がイデアル (i^2+1) に属するものが等しいというルールを付加すればよい。特に、複素数 z に対して $i^2z+z = z(i^2+1) \in (i^2+1)$ より

$$i^2 z = -z$$

という等式が成り立つと考える。

$\boldsymbol{C} = \boldsymbol{R}[i]/(i^2+1)$ は、剰余環としては、多項式を i^2+1 で整除した余りと一対一に対応することから、複素数は一意に $a+bi$ の形に表せる。この形は、多項式を $i^2z = -z$ というルールで整理を繰り返すことでも得られる。そのため、複素数はユークリッド空間 $\boldsymbol{R}^2$ に対応させることができる。具体的には、写像

$$f_{R2C} : \boldsymbol{R^2} \ni (a,b)^T \quad \mapsto \quad a+bi \in \boldsymbol{C}$$

を考える。これは明らかに全単射であり、この写像によって複素数体とユークリッド空間 $\boldsymbol{R}^2$ を対応させ、位相を導入する。複素数体における距離関数は

$$d(x,y) \equiv d\left(f_{R2C}^{-1}(x), f_{R2C}^{-1}(y)\right)$$

と定義する。これによって距離空間としての位相を導入することができる。特に、複素数 z に対して、**絶対値**を $|z| \equiv d(z,0)$ によって定義する。

複素数体における位相は、結局ユークリッド空間 $\boldsymbol{R^2}$ に帰着させているに過ぎないため、ユークリッド空間における性質は基本的にはそのまま通用する。重要なことは f_{R2C} が全単射かつ連続写像であることである。全単射かつ連続である写像は**同相写像**と呼ばれ、同相写像で結ばれる位相空間は**位相同型**であるという。この用語のもと、複素数体とユークリッド空間 $\boldsymbol{R^2}$ は位相同型である。主な性質について、下に述べておこう。

定理 14.2 複素数体 $\boldsymbol{C}$ における閉球はコンパクトである。

(proof)
複素数体 $\boldsymbol{C}$ における半径 r で中心を z_0 とする閉球 $\overline{V}_r(z_0) = \{z \in \boldsymbol{C}; |z-z_0| \le r\}$ について、$z = a+bi, z_0 = a_0+b_0i$ と表わせば

$$|z-z_0| \le r \quad \Longleftrightarrow \quad d((a,b)^T, (a_0.b_0)^T) \le r$$

なので

$$f_{R2C}(\overline{V}_r((a_0,b_0))) = \overline{V}_r(z_0)$$

だから、定理 11.21 より $\overline{V}_r(z_0)$ はコンパクトである。 証明終

定理 14.3 複素数体 $\boldsymbol{C}$ はコーシー完備である。

(proof)
複素数体における距離関数である $d(a_1+b_1i, a_2+b_2i) = |(a_1+b_1i)-(a_2+b_2i)|$ と、これを $\boldsymbol{R^2}$ の元と見たときの（f_{R2C}^{-1} で対応させたときの）$d\left(\begin{pmatrix}a_1\\b_1\end{pmatrix},\begin{pmatrix}a_2\\b_2\end{pmatrix}\right) = \sqrt{(a_1-a_2)^2+(b_1-b_2)^2}$ は等しく、収束は全く同値となる。したがって、定理 13.9 より $\boldsymbol{R^2}$ はコーシー完備なので、複素数体 $\boldsymbol{C}$ もコーシー完備である。 証明終

14.4 複素数の極表示

複素数は $r(\cos\theta + i\sin\theta)$ という形にも表せる。これは**極表示**と呼ばれている。r は**絶対値**と呼ばれ、θ は**偏角**と呼ばれる。極表示の観点では、複素数の乗法が

$$\begin{aligned} r_1(\cos\theta_1 + i\sin\theta_1)\cdot r_2(\cos\theta_2 + i\sin\theta_2) &= r_1r_2\{(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)\} \\ &= r_1r_2\{\cos(\theta_1+\theta_2) + i\cos(\theta_1+\theta_2)\} \end{aligned}$$

というように、絶対値の乗法と偏角の加法（つまり回転）として考えられる。

これを使うと、複素数における n 乗根を検討することができる。複素数 $r(\cos\theta+i\sin\theta)$ の n 乗根を求めよう。まず、非負実数に対しては、非負 n 乗根が 1 つ必ず存在している。そこで、絶対値は $r^{\frac{1}{n}}$ でなければならない。偏角については、n 乗根のひとつは $\dfrac{\theta}{n}$ であることがわかる。さらに、2π 回転した場合は元に戻るため、n 乗した場合、$\dfrac{2\pi}{n}$ の $0, 1, \cdots, n-1$ 倍を乗じたものはすべて n 乗根である。定理としてまとめておく。

定理 14.4 複素数体においては、n 乗根が n 個必ず存在する。

14.5 代数学の基本定理

実数体において x^2+1 が解を持つような拡大体として複素数を構成したが、どこまで拡大すれば常に多項式が解を持つようにすることができるのであろうか。驚くべきことに、実は複素数体までで常に多項式が解を持つ。この事実は代数学の基本定理とも呼ばれている。

定理 14.5 複素数の多項式は連続写像である。

(proof)
z を任意の複素数とし、$\{a_n\}$ を z に収束する任意の数列とする。$f(x) = \sum_i b_i x^i$ と表しておく。

$$\begin{aligned} \lim_{n\to\infty} f(a_n) &= \lim_{n\to\infty}\sum_i b_i(a_n)^i \\ &= \sum_i \lim_{n\to\infty} b_i(a_n)^i \quad \because \text{和の極限} \\ &= \sum_i b_i z^i \quad \because \text{積の極限} \\ &= f(z) \end{aligned}$$

となるため、定理 11.18 より $f(x)$ は任意の複素数数において連続である。 証明終

定理 14.6 （代数学の基本定理）複素数の 1 次以上の任意の多項式は必ず解を持つ。

(proof)

複素数の多項式を $f(z) = \sum_{i=0}^{n} a_i z^i$ とする。定数倍しても解は変わらないため、モニックな多項式（$a_n = 1$）に一意性を失わず限定する。

$$f(z) = 0 \Leftrightarrow |f(z)| = 0$$

であるため、$|f(z)|$ の最小値を検討することによって解の存在を考えることができる。

まず、$|z|$ が十分大きいときの $|f(z)|$ について調べる。

$$|f(z)| = \left|\sum_{i=0}^{n} a_i z^i\right| = |z^n|\left|1 + \sum_{i=0}^{n-1} \frac{a_i}{z^{n-i}}\right|$$

であり

$$\left|\sum_{i=0}^{n-1} \frac{a_i}{z^{n-i}}\right| \leq \sum_{i=0}^{n-1} \frac{|a_i|}{|z|^{n-i}}$$

なので、$\left|\sum_{i=0}^{n-1} \frac{a_i}{z^{n-i}}\right|$ は $|z|$ を大きくすればいくらでも小さくなる。したがって $\left|1 + \sum_{i=0}^{n-1} \frac{a_i}{z^{n-i}}\right|$ はいくらでも 1 に近づけることができる。よって、$|z|$ を十分大きくすれば、例えば

$$\left|1 + \sum_{i=0}^{n-1} \frac{a_i}{z^{n-i}}\right| \geq 0.9$$

とすることができる、このとき

$$|f(z)| = |z^n|\left|1 + \sum_{i=0}^{n-1} \frac{a_i}{z^{n-i}}\right|$$
$$\geq 0.9|z|^n$$

であり、$|z|$ を大きくすれば $|f(z)|$ はいくらでも大きくなる。そこで、ある実数 $M > 0$ をとると $|z| > M$ のとき $|f(z)| \geq |f(0)|$ とすることができる。このとき、$|z| \leq M$ の中に $|f(0)|$ が含まれるため、閉球 $\overline{V}_M(0) = \{z \in \boldsymbol{C} : |z| \leq M\}$ の中で $|f(z)|$ を最小にするものが見つかれば、それは z が複素数体全体にわたる場合における $|f(z)|$ の最小値である。

定理 14.5 より $f(z)$ は連続写像であり、また距離関数も連続写像であることから、複素数体から実数体への写像としての $|f(z)|$ も連続写像である。定理 14.2 より閉球 $\overline{V}_M(0)$ はコンパクトであることから、定理 12.7 より $\{|f(z)| : |z| \leq M\}$ に最小値が存在する。最小値に対応する $\overline{V}_M(0)$ の元を z_0 とする。$|f(z_0)|$ は $|f(z)|$ の最小値である。

$g(z) \equiv f(z + z_0)$ と定義する。$g(0) = f(z_0)$ なので $|g(z)|$ は $z = 0$ において最小値をとる。ここで、$|g(0)| > 0$ であると仮定する。$g(0)$ は $g(z)$ の定数項に相当するため、$g(z)$ は定数項が 0 でない。これを $a = g(0) \neq 0$ とおく。また、$g(z)$ は 1 次以上の多項式であるため、定数項以外に係数が 0 でないものが存在する。そのうち次数の最も小さいものの係数を $b \neq 0$ とし、その次数を K とする。このとき、$g(z)$ は

$$g(z) = a + bz^K + z^{K+1}h(z), \quad h(z) \in \boldsymbol{C}[z]$$

という形に表される。定理 14.4 より、複素数体においては n 乗根がつねに存在するため、$-\frac{a}{b}$ の K 乗根 c が常に存在する。このとき $bc^K = -a$ が成立している。$t > 0$ なる小さい実数 t をとると、多項式 $h(z)$ は定数もしくは連続なので $t|c^{K+1}h(tc)| < |a|$ とすることができる。このとき

$$
\begin{aligned}
|g(tc)| &= |a + b(tc)^K + (tc)^{K+1}h(tc)| \\
&= |a - at^K + t^K tc^{K+1}h(tc)| \\
&\leq |a - at^K| + t^K t|c^{K+1}h(tc)| \\
&< |a|(1 - t^K) + t^K|a| \\
&= |a| = |g(0)|
\end{aligned}
$$

であり、$|g(0)|$ が最小であることに矛盾する。よって $|f(z_0)| = 0$ であり、z_0 が解として存在している。 証明終

ここで、$f(z)$ を複素数の多項式としよう。代数学の基本定理より、$f(z)$ は少なくとも解をひとつもつため、これを α_1 とする。このとき因数定理より $f(z) = (z - \alpha_1)f_1(z)$ と表すことができる。$f_1(z)$ が定数でなければ、やはり解を一つ持つため、それを α_2 とすると $f(z) = (z - \alpha_1)(z - \alpha_2)f_2(z)$ と表すことができる。この操作を定数になるまで繰り返せば

$$f(z) = c(z - \alpha_1)\cdots(z - \alpha_n)$$

という形に表せることになる。これは素元分解のひとつの形であり、体の多項式は定理 7.10 よりユークリッド整域であり、一意分解整域でもあることから、この形への分解は一意である。

定理 14.7 複素数の多項式は

$$c(z - \alpha_1)\cdots(z - \alpha_n)$$

という形に一意に変形できる。

参考文献

[1] 杉原厚吉 工学のための応用代数 共立出版 1999.

[2] JST CREST 日比チーム（編） グレブナー道場 共立出版 2011.

[3] 数学の基礎 集合・数・位相 齋藤正彦著 基礎数学 14 東京大学出版会.

[4] 固有値問題 30 講 志賀浩二著 朝倉書店.

[5] 代数系入門 松坂和夫 岩波書店 1976.

[6] 位相への 30 講 志賀浩二 朝倉書店.