環と加群の基礎

大阿久 俊則

目 次

0 集合と写像

最初に，講義で用いる集合と写像に関する基本的な概念と記号をまとめておくので，必要に応じて参照してください．

0.1 集合と写像

集合 (set) とは，いくつかの（有限個または無限個の）要素の集まりである．要素の個数が 0 であるような集合を**空集合** (empty set) といい $\emptyset$ と表す．自然数全体の集合を $\mathbb{N} = \{1, 2, 3, \dots\}$, 整数全体の集合を $\mathbb{Z}$，有理数全体の集合を $\mathbb{Q}$，実数全体の集合を $\mathbb{R}$，複素数全体の集合を $\mathbb{C}$ で表す．要素の数が有限であるような集合を**有限集合**，要素の数が無限であるような集合を**無限集合**という．集合 X に対して $\sharp X$ または $|X|$ で X の要素の個数を表す．X が無限集合の場合は $\sharp X = |X| = \infty$ と書く．

X を集合とする．Y が X の**部分集合** (subset) であるとは，Y の任意の要素は X の要素でもあることである．このとき $Y \subset X$ と表す．$\emptyset$ と X 自身も X の部分集合である．従って $X \subset X$ も真であることに注意する．$Y \subset X$ かつ $Y \neq X$ であるとき，$Y \subsetneqq X$ と表し Y は X の**真部分集合** (proper subset) であるという．A, B を集合 X の部分集合とするとき，A と B の**共通部分** (intersection) $A \cap B$ と**和集合** (union) $A \cup B$ は，

$$A \cap B := \{x \in X \mid x \in A \text{ かつ } x \in B\}, \quad A \cup B := \{x \in X \mid x \in A \text{ または } x \in B\}$$

で定義される．ここで記号 $:=$ は右辺が左辺の記号の定義であることを示す．(単に $=$ で表すことも多い．) さらに一般に，ある集合 Λ （大文字のラムダ）があって，Λ の各々の元 λ （小文字のラムダ）に対して X の部分集合 A_λ が定義されているとする．このとき，

$$\bigcap_{\lambda \in \Lambda} A_\lambda := \{x \in X \mid x \in A_\lambda \ (\forall \lambda \in \Lambda)\}, \quad \bigcup_{\lambda \in \Lambda} A_\lambda := \{x \in X \mid x \in A_\lambda \ (\exists \lambda \in \Lambda)\}$$

と定義する．

集合 X から集合 Y への**写像** (map) $f : X \to Y$ とは，X の各々の元 x に対して Y の元 y を対応させる規則のことである．このとき $y = f(x)$ と表す．この対応関係を明確にするため $f : X \ni x \mapsto y \in Y$ と表すこともある．X を f の**定義域**という．

A を X の部分集合とするとき，f の A への**制限** $f|_A$ とは，A の各々の元 a に対して $a \in X$ とみなして $f(a)$ を対応させる写像 $f|_A : A \to Y$ のことである．すなわち $f|_A$ は f の定義域を X から A に制限して得られる写像のことである．

集合 X の**恒等写像** (identity map) $\mathrm{id}_X : X \to X$ とは，任意の $x \in X$ について $\mathrm{id}_X(x) = x$ で定義される写像のことである．

$f : X \to Y$ と $g : Y \to Z$ を写像とするとき，**合成写像** $g \circ f : X \to Z$ を $(g \circ f)(x) = g(f(x))$ $(\forall x \in X)$ で定義する．

写像 $f : X \to Y$ が**単射** (injective) または **1 対 1**(one to one) とは，$x, y \in X$ かつ $x \neq y$ ならば $f(x) \neq f(y)$ であることである．

写像 $f : X \to Y$ が**全射** (surjective) または**上への写像** (onto) とは，任意の $y \in Y$ に対して $f(x) = y$ をみたす $x \in X$ が (少なくとも 1 つ) 存在することである．

写像 $f : X \to Y$ が**全単射** (bijective) とは，f が全射かつ単射であることである．このとき，任意の $y \in Y$ に対して $f(x) = y$ を満たす $x \in X$ がただ 1 つ定まる．この x を $x = f^{-1}(y)$ と表す．これによって，f の**逆写像** (inverse map) $f^{-1} : Y \to X$ が定まり，$f^{-1} \circ f = \mathrm{id}_X$, $f \circ f^{-1} = \mathrm{id}_Y$ が成立する．

集合 X から自然数全体の集合 $\mathbb{N}$ への全単射が存在するとき X は**可算集合**であるという．$\mathbb{Z}$ と $\mathbb{Q}$ は可算集合であるが，$\mathbb{R}$ と $\mathbb{C}$ は可算集合ではない．

$f : X \to Y$ を写像として，A を X の部分集合とするとき，

$$f(A) := \{f(x) \mid x \in A\} \subset Y$$

のことを A の f による**像** (image) という．写像 $f : X \to Y$ を X から $f(X)$ への写像 $f : X \to f(X)$ とみなすこともできる．（これを同じ記号 f で表すのは正確には記号の濫用である．）そうすると $f : X \to f(X)$ は全射になる．

Y の部分集合 B に対して

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\} \subset X$$

を B の f による**逆像** (inverse image) という．（逆写像 f^{-1} との違いに注意せよ．逆写像は f が全単射のときのみ定義される．f が全単射ならば $f^{-1}(B)$ は B の写像 f^{-1} による像とみなすこともできる．）

$f : X \to Y$ を写像，A, B を X の部分集合，C, D を Y の部分集合とするとき，

$$f(A \cup B) = f(A) \cup f(B), \quad f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D), \quad f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$$

が成立する．しかし，$f(A \cap B) = f(A) \cap f(B)$ は一般に成立しない．

集合 X と Y の**直積集合** (direct product) とは，X の元と Y の元の組全体からなる集合

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}$$

のことである．（$x \neq y$ のとき $(x, y) \neq (y, x)$ であることに注意する．）ある集合 Λ があって，Λ の各々の元 λ に対して集合 X_λ が定義されているとする．このとき，任意の λ に対して X_λ の 1 つの元 x_λ を選んで並べたものを $(x_\lambda)_{\lambda \in \Lambda}$ と表し，それらの全体

$$\prod_{\lambda \in \Lambda} X_\lambda := \{(x_\lambda)_{\lambda \in \Lambda} \mid x_\lambda \in X_\lambda \quad (\forall \lambda \in \Lambda)\}$$

を X_λ $(\lambda \in \Lambda)$ の直積集合という．特に n を自然数として $\Lambda = \{1, 2, \ldots, n\}$ の場合は

$$\prod_{i=1}^{n} X_i = X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i \quad (i = 1, \ldots, n)\}$$

と表す．

0.2 同値関係と商集合

集合 X における**関係** (relation) とは，直積集合 $X \times X$ の部分集合 R のことである．$x, y \in X$ が $(x, y) \in R$ を満たすとき $x \sim y$ と表す．これを関係 $\sim$ とも書く．

集合 X における**同値関係** (equivalence relation) とは，X における関係 $\sim$ であって，任意の $x, y, z \in X$ について

(1) $x \sim x$

(2) $x \sim y$ ならば $y \sim x$

(3) $x \sim y$ かつ $y \sim z$ ならば $x \sim z$

を満たすもののことである．$x \sim y$ のとき x と y は同値であるという．

集合 X における同値関係 $\sim$ があるとき，$x \in X$ に対して x と同値な元の全体

$$[x] = \overline{x} = \{y \in X \mid x \sim y\} \subset X$$

のことを x を含む（または x の）**同値類**という．$x, y \in X$ のとき，$[x] = [y]$ または $[x] \cap [y] = \emptyset$ のどちらか一方のみが成立することが同値関係の定義からわかる．X の相異なる同値類全体からなる集合

$$X/\sim := \{[x] \mid x \in X\}$$

のことを X の $\sim$ による**商集合** (quotient set) または**類別**という．写像

$$p : X \ni x \longmapsto [x] \in X/\sim$$

は全射であり，この同値関係による**自然な全射**または**標準射影**という．

X の部分集合 S が，

(1) 任意の $x \in X$ に対してある $s \in S$ があって $x \sim s$

(2) $s, t \in S$ に対して，$s \sim t$ と $s = t$ は同値

の 2 つの条件を満たすとき，S のことを同値関係 $\sim$ についての**完全代表系**という．

たとえば，X を東京女子大学の学生全体の集合として，x と y が同じ専攻に属するとき $x \sim y$ と定義すれば，$\sim$ は同値関係であり，$X/\sim$ は（12 の）専攻全体の集合とみなすことができる．（専攻とその専攻に属する学生全体の集合とを同一視する．）自然な全射 $p : X \to X/\sim$ は各学生に対して所属する専攻を対応させる写像である．たとえば各専攻の 1 年生から学生番号が最小の学生を一人ずつ選べば，それらの 12 人の学生達はこの同値関係についての完全代表系である．

1 環

環とは，和と積という 2 つの演算が定義され，結合法則，交換法則，分配法則などの計算規則が成り立つような集合である．整数全体，多項式全体，正方行列全体，連続関数の全体などが環の代表的な例である．このことからもわかるように，群，環，体などの代数系と呼ばれるもののうち特になじみ深くかつ応用の広い概念であり，代数学だけでなく解析学や幾何学においても重要である．ここでは，環の定義，例，基本的な性質から始めて，環準同型とイデアルの概念を導入する．特に環の中で最も基本的な単項イデアル整域 (PID) と呼ばれる環について詳しく述べる．たとえば整数全体や 1 変数多項式の全体は単項イデアル整域である．整数の素因数分解や多項式の因数分解の概念を単項イデアル整域において一般的に考察する．なお，表題の最後に*の付いた節はこの講義録の後半や「ガロア理論入門」を読むためには不要である．

1.1 環の定義と例

定義 1.1 集合 R が**環** (ring) であるとは，2 つの 2 項演算（加法と乗法）

$$R \times R \ni (a,b) \longmapsto a+b \in R, \qquad R \times R \ni (a,b) \longmapsto ab \in R$$

が定義され以下の性質 (1)–(7) を満たすことである．

(1) 任意の $a,b,c \in R$ に対して $(a+b)+c = a+(b+c)$ が成立する．（加法の結合法則）

(2) 任意の $a,b \in R$ に対して $a+b = b+a$ が成立する．（加法の交換法則）

(3) R の元 0_R が存在して，任意の $a \in R$ に対して $a+0_R = a$ が成立する．（0_R を加法についての単位元といい，通常は単に 0 で表す．）

(4) R の任意の元 a に対してある $b \in R$ が存在して $a+b = 0$ が成立する．このとき $b = -a$ と表し a の加法についての逆元という．

(5) 任意の $a,b,c \in R$ に対して $(ab)c = a(bc)$ が成立する．（乗法の結合法則）

(6) R のある元 1_R が存在して，任意の $a \in R$ に対して $a1_R = 1_R a = a$ が成立する．（1_R を乗法についての単位元といい，通常は 1 で表す．）

(7) 任意の $a,b,c \in R$ に対して $a(b+c) = ab+ac$, $(a+b)c = ac+bc$ が成立する．（分配法則）

$a,b \in R$ に対して，$a-b = a+(-b)$ と定義する．さらに

(8) 任意の $a,b \in R$ に対して $ab = ba$ が成立する（乗法の交換法則）

とき，R は**可換環** (commutative ring) であるという．可換環でない環のことを非可換環という．

定義 1.2 環 R の元 a が R の**可逆元** (invertible element) または**単元** (unit) であるとは，$ab = ba = 1$ を満たすような $b \in R$ が存在することである．このとき b を a の（乗法に関する）**逆元**といい $b = a^{-1}$ と表す．

K が可換環であって，K の 0 と異なる任意の元が可逆元であるとき，K は**体** (field) であるという．

補題 1.1 R を環とする．

(1) 加法に関する単位元 0 はただ一つである．

(2) $a \in R$ に対して $a + b = 0$ をみたす $b \in R$ はただ一つである．

(3) 乗法に関する単位元 1 はただ一つである．

(4) a が R の単元（可逆元）であれば $ab = ba = 1$ をみたす $b \in R$ はただ一つである．

証明: (1) R の 2 つの元 0 と $0'$ があって，任意の $a \in R$ について $a+0 = a$ かつ $a+0' = a$ が成立すると仮定する．$a + 0 = a$ より $0' + 0 = 0'$, $a + 0' = a$ より $0 + 0' = 0$ となるが，$0' + 0 = 0 + 0'$ であるから $0' = 0$ が従う．

(2) $a + b = a + b' = 0$ とすると，

$$b' = b' + 0 = b' + (a + b) = (b' + a) + b = (a + b') + b = 0 + b = b$$

(3) R の 2 つの元 1 と $1'$ があって，任意の $a \in R$ について $a1 = 1a = a$ かつ $a1' = 1'a = a'$ が成立すると仮定すると $1' = 11' = 1$.

(4) b と b' が共に乗法に関する a の逆元，すなわち $ab = ba = ab' = b'a = 1$ とすると，

$$b' = b'1 = b'(ab) = (b'a)b = 1b = b$$

□

補題 1.2 R を環とすると任意の $a, b \in R$ について次が成立する．

(1) $a0 = 0a = 0$.

(2) $(-a)b = a(-b) = -(ab)$ ($-(ab)$ を単に $-ab$ と書く．)　特に，$(-1)a = a(-1) = -a$.

証明: (1) $a0 = a(0 + 0) = a0 + a0$ の両辺に $-(a0)$ を加えて

$$0 = a0 + (-(a0)) = (a0 + a0) + (-(a0)) = a0 + (a0 + (-(a0))) = a0$$

$0a$ についても同様.

(2) $(-a)b + ab = ((-a) + a)b = 0b = 0$ より $(-a)b$ は ab の加法に関する逆元であるから，$(-a)b = -(ab)$ である．$a(-b)$ についても同様．□

環 R において，もし $1_R = 0_R$ ならば，任意の $a \in R$ に対して $a = a1_R = a0_R = 0_R$ となるから，$R = \{0_R\}$ である．これを自明な環または零環という．逆に言えば，R が 0_R 以外の元を含めば $1_R \neq 0_R$ である．

環 R の元 a と非負整数 n に対して，

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n} & (n > 0) \\ 1 & (n = 0) \end{cases}$$

と定義して a の n 乗という．n, m が非負整数のとき $a^n a^m = a^{n+m}$ が成立する．

定義 1.3 R を環とする．R の部分集合 S が，R の単位元 0_R と 1_R を含み，R の演算について環になっているとき，S を R の**部分環** (subring) という．

補題 1.3 R を環とする．R の部分集合 S が R の部分環であるための必要十分条件は

(1) $a, b \in S$ ならば $a + b, -a, ab$ はすべて S に属する．

(2) 0_R と 1_R は S に属する．

が成立することである．

証明: (1),(2) が S が部分環であるための必要条件であることは明らかだから，十分条件であることを示す．(1),(2) より R における加法と乗法の演算は S における 2 項演算を定義する．環の定義 (1)–(7) は，R が環であることと条件 (1),(2) から明らかに成立する．□

例 1.1 整数全体 $\mathbb{Z}$, 有理数全体 $\mathbb{Q}$, 実数全体 $\mathbb{R}$，複素数全体 $\mathbb{C}$ は通常の和と積によって可換環となる．加法の単位元は整数 0，乗法の単位元は整数 1 である．さらに $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体となる．これらをそれぞれ，有理整数環，有理数体，実数体，複素数体という．更に，各々の環は，それを含む環の部分環である．

$\mathbb{Z}$ の単元は 1 と -1 である．実際 $1^2 = (-1)^2 = 1$ より 1 と -1 は単元である．$n \in \mathbb{Z}$ を単元とすると，$nm = 1$ をみたす $m \in \mathbb{Z}$ が存在するが，$|n||m| = 1$ より $|n| = 1$，すなわち $n = 1$ または $n = -1$ でなければならない．

例 1.2 整数 n は平方数（ある整数の 2 乗）ではないとすると，$\mathbb{Z}[\sqrt{n}] := \mathbb{Z} + \mathbb{Z}\sqrt{n} = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ は複素数体 $\mathbb{C}$ の部分環である．($n < 0$ のときは i を虚数単位として $\sqrt{n} = \sqrt{-n}i$ と定義する．）実際，$a, b, c, d \in \mathbb{Z}$ とすると，

$$(a + b\sqrt{n}) + (c + d\sqrt{n}) = (a + c) + (b + d)\sqrt{n} \in \mathbb{Z}[\sqrt{n}],$$
$$(a + b\sqrt{n})(c + d\sqrt{n}) = ac + bdn + (ad + bc)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$$

であり，$-(a + b\sqrt{n}) = -a + (-b)\sqrt{n}$, $0 = 0 + 0\sqrt{n}$, $1 = 1 + 0\sqrt{n}$ も $\mathbb{Z}[\sqrt{n}]$ に含まれるから補題 1.3 により $\mathbb{Z}[\sqrt{n}]$ は $\mathbb{C}$ の部分環である．

例 1.3 K を体（たとえば $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$）とする．K の元を成分とする $n \times n$ 行列の全体 $M_n(K)$ は，行列の和と積により環となる．加法の単位元は 0 行列 $O = O_n$，乗法の単位元は単位行列 $I = I_n$ (E_n と表すこともある）である．$n \geq 2$ ならば $M_n(K)$ は非可換環である．$M_n(K)$ の可逆元とは正則行列のことである．

例 1.4 X を空でない集合，R を環とする．X から R への写像の全体を $\mathrm{Map}(X,R)$ で表す．$f,g\in\mathrm{Map}(X,R)$ に対して $f+g, fg\in\mathrm{Map}(X,R)$ を

$$(f+g)(x)=f(x)+g(x),\qquad (fg)(x)=f(x)g(x)\qquad (\forall x\in X)$$

で定義すると，$\mathrm{Map}(X,R)$ は環となる．加法の単位元は $0(x)=0_R$ $(\forall x\in X)$ で定義される写像 0 であり，乗法の単位元は $1(x)=1_R$ $(\forall x\in X)$ で定義される写像 1 である．R が可換環ならば $\mathrm{Map}(X,R)$ も可換環である．$f\in\mathrm{Map}(X,R)$ が可逆元であるための必要十分条件は，任意の $x\in X$ に対して $f(x)$ が R の可逆元であることである．このとき $g(x)=f(x)^{-1}$ $(x\in R)$ で定義される $g\in\mathrm{Map}(X,R)$ が f の逆元となる．

例 1.5 I を $\mathbb{R}$ の区間とする．I で定義された実数値連続関数の全体を $C(I)$ で表す．$C(I)$ は $\mathrm{Map}(I,\mathbb{R})$ の部分環であり，可換環となる（「連続と極限」を参照）．$f\in C(I)$ が可逆元であるための必要十分条件は，任意の $x\in I$ について $f(x)\neq 0$ であることである．

例 1.6 I を $\mathbb{R}$ の開区間とする．m を自然数または ∞ とする．I で C^m 級（m 回微分可能で m 次導関数が連続）であるような実数値関数の全体を $C^m(I)$ で表す．$C^m(I)$ は $C(I)$ の部分環であり，可換環となる．さらに，$0\leq k<m$ のとき $C^k(I)$ は $C^m(I)$ の部分環である．$(C^0(I)=C(I)$ と定義する．$)$ $f\in C^k(I)$ が可逆元であるための必要十分条件は，任意の $x\in I$ について $f(x)\neq 0$ であることである．

定義 1.4 R を $\{0\}$ でない可換環とする．$a,b\in R$ について $a\neq 0$ かつ $b\neq 0$ ならば $ab\neq 0$ が成り立つとき，R を**整域** (integral domain) という．

たとえば $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ は整域である．K が体ならば K は整域である．実際，a,b を K の 0 と異なる 2 つの元とする．もし $ab=0$ ならば，$0=a^{-1}(ab)=(a^{-1}a)b=b$ となり仮定に反する．

一方，R が可換環であって，集合 X が 2 つ以上の元を含むとき，$\mathrm{Map}(X,R)$ は整域ではない．実際，X の異なる元 a,b を固定して，

$$f(x)=\begin{cases}1_R & (x=a)\\ 0_R & (x\neq a)\end{cases}\qquad g(x)=\begin{cases}1_R & (x=b)\\ 0_R & (x\neq b)\end{cases}$$

により $f,g\in\mathrm{Map}(X,R)$ を定義すると，任意の $x\in X$ について $(fg)(x)=f(x)g(x)=0_R$ となるから，$fg=0$ である．

1.2　環準同型

定義 1.5 R と R' を環とする．写像 $f:R\to R'$ が**環準同型** (ring homomorphism) とは，

(1) $f(a+b)=f(a)+f(b)\quad(\forall a,b\in R)$

(2) $f(ab)=f(a)f(b)\quad(\forall a,b\in R)$

(3) $f(1_R) = 1_{R'}$ ($1_R, 1_{R'}$ はそれぞれ R, R' における乗法の単位元)

を満たすことである．さらに f が全単射であるとき，f を**環同型** (ring isomorphism) という．f が同型写像であることを明記したい場合は $f : R \xrightarrow{\sim} R'$ と表すことにする．このとき R と R' は同型であるといい，写像を明示せずに簡単に $R \cong R'$ と表すこともある．f が環同型ならば逆写像 f^{-1} は R' から R への環同型である．

補題 1.4 $f : R \to R'$ が環準同型ならば，$f(0_R) = 0_{R'}$ および，任意の $a \in R$ について $f(-a) = -f(a)$ が成立する．

証明: $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$ より $f(0_R) = 0_{R'}$ が従う．また，$0 = f(0) = f(a + (-a)) = f(a) + f(-a)$ より $f(-a)$ は R' における $f(a)$ の加法に関する逆元であるから，$f(-a) = -f(a)$ が成立する．□

補題 1.5 $f : R \longrightarrow R'$ と $g : R' \longrightarrow R''$ が共に環準同型であれば $g \circ f : R \longrightarrow R''$ も環準同型である．

証明: $a, b \in R$ とすると

$$(g \circ f)(a + b) = g(f(a + b)) = g(f(a) + f(b)) = g(f(a)) + g(f(b)) = (g \circ f)(a) + (g \circ f)(b),$$
$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$$

および $(g \circ f)(1_R) = g(f(1_R)) = g(1_{R'}) = 1_{R''}$ が成立するから $g \circ f$ は環準同型である．□

例 1.7 写像 $\iota : \mathbb{Z} \longrightarrow \mathbb{C}$ を $\iota(n) = n$ $(\forall n \in \mathbb{Z})$ で定義すれば，ι は環準同型である．

例 1.8 X を空でない集合，R を環とする．X の元 a を固定して，写像 $\rho : \mathrm{Map}(X, R) \to R$ を

$$\mathrm{Map}(R, X) \ni f \longmapsto \rho(f) := f(a) \in R$$

で定義すると ρ は環準同型である．

例 1.9 K を $\mathbb{R}$ または $\mathbb{C}$ とする．I_n を n 次単位行列とするとき，写像

$$\iota : K \ni a \longmapsto aI_n \in M_n(K)$$

は環準同型である．

- ここまでは非可換の場合も含めて一般の環を考えたが，以下では可換環のみを扱う．

1.3 多項式環

R を可換環，x を不定元（文字）とする．n を 0 以上の整数，$a_0, a_1, \ldots, a_n \in R$ として

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

という形に表される式のことを x についての R 係数**多項式** (polynomial) という．$a_n \neq 0$ のとき，f の**次数** (degree) は n であるといい $\deg f = n$ と書く．特に R の元 a は次数 0 の多項式とみなすことができる．これを定数多項式という．0 でない定数多項式の次数は 0 である．ただし，定数多項式 0 だけは特別扱いし，次数が $-\infty$ であると便宜上定義する．また $a_n = 1$ であるとき f は**モニック** (monic) であるという．

x についての R 係数多項式の全体を $R[x]$ と表す．

$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum_{i=0}^{m} b_i x^i$$

をもう 1 つの多項式とするとき, f と g の和と積を

$$f + g = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i$$

$$fg = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + a_0 b_0 = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i$$

により定義する．ただし，$i > n$ のときは $a_i = 0$, $j > m$ のときは $b_j = 0$ と解釈する．

$R[x]$ はこの和と積によって可換環になる．加法と乗法についての単位元はそれぞれ定数多項式 0 と 1 である．これを R 上の (1 変数) **多項式環**という．

実際，$R[x]$ が環の定義の (1),(2),(3) を満たすことは多項式の和の定義から明らかである．(4) は

$$-f = (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots + (-a_1)x + (-a_0)$$

とすればよい．乗法の結合法則 (5) を示すために，

$$h = c_l x^l + c_{l-1}x^{l-1} + \cdots + c_1 x + c_0 \qquad (c_0, c_1, \ldots, c_l \in R)$$

とする．

$$fg = d_{n+m}x^{n+m} + d_{n+m-1}x^{n+m-1} + \cdots + d_1 x + d_0,$$
$$d_k = \sum_{i=0}^{k} a_i b_{k-i} \qquad (0 \leq k \leq n+m)$$

より

$$(fg)h = e_{n+m+l}x^{n+m+l} + e_{n+m+l-1}x^{n+m+l-1} + \cdots + e_1 x + e_0,$$
$$e_k = \sum_{i=0}^{k} d_i c_{k-i} = \sum_{i=0}^{k} \sum_{j=0}^{i} (a_j b_{i-j}) c_{k-i} \qquad (0 \leq k \leq n+m+l)$$

であり，$e_k = \sum_{i=0}^{k}\sum_{j=0}^{i}(a_j b_{i-j})c_{k-i}$ は $i+j+l=k$ となるような非負整数 i,j,l をすべて動かしたときの $(a_i b_j)c_l$ の和に等しい．同様にして，

$$f(gh) = e'_{n+m+l}x^{n+m+l} + e'_{n+m+l-1}x^{n+m+l-1} + \cdots + e'_1 x + e'_0$$

とすると，e'_k は $i+j+l=k$ となるような非負整数 i,j,l をすべて動かしたときの $a_i(b_j c_l)$ の和であることがわかる．$(a_i b_j)c_l = a_i(b_j c_l)$ であるから $e_k = e'_k$ であることがわかる．以上により $(fg)h = f(gh)$ が示された．可換環の定義の (6),(7),(8) は容易に確かめられる．

$a \in R$ に対して a を定数多項式 a として $R[x]$ の元とみなしたものを $\iota(a)$ で表すと，

$$\iota : R \longrightarrow R[x]$$

は単射な環準同型である．そこで以降では，$\iota(a)$ を単に a と表して，R を $R[x]$ の部分環とみなす．

補題 1.6 R が整域ならば $R[x]$ も整域であり，$f, g \in R[x]$ に対して $\deg(fg) = \deg f + \deg g$ が成立する．ただし，整数 n に対して $-\infty + n = -\infty$, $-\infty + (-\infty) = -\infty$ と定義する．

証明: $f = a_n x^n + \cdots + a_0$, $g = b_m x^m + \cdots + b_0$ のとき $fg = a_n b_m x^{n+m} + \cdots + a_0 b_0$ である．$a_n \neq 0$，$b_m \neq 0$ ならば $a_n b_m \neq 0$ であるから，

$$\deg(fg) = n + m = \deg f + \deg g$$

が成立する．$f = 0$ のときは，$fg = 0$ であるから，$\deg(fg) = -\infty = \deg f + \deg g$ が成立する．□

命題 1.1 R を整域とすると，多項式環 $R[x]$ の単元全体は R の単元（を定数多項式とみなしたもの）の全体である．

証明: a を R の単元とすると，$ab = 1$ を満たす $b \in R$ が存在する．これを $R[x]$ における等式とみなすことができるから，定数多項式 a は $R[x]$ の単元である．逆に $f \in R[x]$ を $R[x]$ の単元とすると $fg = 1$ を満たす $g \in R[x]$ が存在する．このとき補題 1.6 により $\deg f + \deg g = \deg 1 = 0$ であるから $\deg f = \deg g = 0$，すなわち f も g も定数多項式でなければならない．$f = a$, $g = b$ $(a, b \in R)$ とすれば $ab = 1$ であるから $f = a$ は R の単元である．□

K が体であるとき $K[x]$ の単元は 0 でない定数多項式の全体である．$\mathbb{Z}[x]$ の単元は定数多項式 ± 1 の 2 つのみである．

命題 1.2 (多項式の割り算) 整域 R の元を係数とする多項式

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \qquad (m \geq 0,\ b_0, \ldots, b_m \in R)$$

において b_m が R の単元であると仮定する（特に g がモニックならよい）．このとき，任意の多項式 $f \in R[x]$ に対して

$$f = qg + r, \qquad \deg r < m = \deg g$$

を満たす多項式 $q, r \in R[x]$ が一意的に存在する．f を上のように表すことを，f の g による**割り算**といい，q を**商**, r を**余り**または**剰余**という．

証明: $m = 0$ のときは $g = b_0$ は R の単元であるから，$q = b_0^{-1} f, r = 0$ とすればよい．そこで $m = \deg g \geq 1$ と仮定して，$n := \deg f$ についての帰納法で示す．$n < m$ のときは $q = 0, r = f$ とすればよい．$n \geq m$ のときは，

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

と表すとき

$$f - a_n b_m^{-1} x^{n-m} g = (a_{n-1} - a_n b_m^{-1} b_{m-1}) x^{n-1} + \cdots$$

の次数は $n - 1$ 以下であるから，帰納法の仮定により

$$f - a_n b_m^{-1} x^{n-m} g = q_1 g + r, \qquad \deg r < m$$

を満たす $q_1, r \in R[x]$ が存在する．このとき

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

が成立するから $q = a_n b_m^{-1} x^{n-m} + q_1$ とおけば割り算の式が成立する．

最後に割り算の一意性を示そう．

$$f = qg + r = q'g + r', \qquad \deg r < m,\ \deg r' < m$$

を満たす $q, q', r, r' \in R[x]$ が存在したとすると，

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

となる．補題 1.6 により，この左辺は 0 でなければ次数 m 以上であり，右辺の次数は m より小なので矛盾である．従って両辺は 0 でなければならない．$g \neq 0$ であり $R[x]$ は整域であるから $q - q' = 0$ かつ $r' - r = 0$ である．従って割り算の商 q と余り r は一意的である．□

特に R が体ならば，g は 0 多項式でなければよい．

例 1.10 $\mathbb{Z}$ 係数の多項式環 $\mathbb{Z}[x]$ において，

$$f = 3x^3 - x^2 + 4x - 5, \qquad g = x^2 - x + 1$$

として f を g で割り算すると (g はモニックであることに注意)，

$$f = (3x + 2)g + 3x - 7$$

すなわち商は $3x+2$, 余りは $3x-7$ である．$\mathbb{Z}[x]$ において，f をたとえば $2g=2x^2-2x+2$ で割り算することはできない．$\mathbb{Q}[x]$ ならば可能であり，

$$f=\Big(\frac{3}{2}x+1\Big)2g+3x-7$$

となる．

定義 1.6 (代入) R 係数の多項式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ $(a_i\in R)$ と $c\in R$ に対して，R の元

$$f(c):=a_nc^n+a_{n-1}c^{n-1}+\cdots+a_1c+a_0$$

を $f(x)$ に $x=c$ を代入した値という．

命題 1.3 定義 1.6 において写像 $\rho_c:R[x]\ni f\mapsto f(c)\in R$ は $R[x]$ から R への環準同型であり全射である．

証明: f を上のような多項式として

$$g=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$$

とおく．定義より $\rho_c(1)=1$ が成立する．

$$\rho_c(f+g)=(f+g)(c)=\sum_{i=0}^{\max\{n,m\}}(a_i+b_i)c^i=\sum_{i=0}^{n}a_ic^i+\sum_{i=0}^{m}b_ic^i=f(c)+g(c)$$
$$=\rho_c(f)+\rho_c(g),$$

$fg=d_{n+m}x^{n+m}+d_{n+m-1}x^{n+m-1}+\cdots+d_1x+d_0$ とおくと，

$$\rho_c(fg)=(fg)(c)=\sum_{i=0}^{n+m}d_ic^i=\sum_{i=0}^{n+m}\sum_{j=0}^{i}a_jb_{i-j}c^i=\sum_{i=0}^{n+m}\sum_{j=0}^{i}a_jc^jb_{i-j}c^{i-j}$$
$$=\sum_{j=0}^{n}a_jc^j\sum_{k=0}^{m}b_kc^k=f(c)g(c)=\rho_c(f)\rho_c(g)$$

が成立する．以上により ρ_c は環準同型である．任意の $a\in R$ に対して a を定数多項式とみなせば $\rho_c(a)=a$ となるから ρ_c は全射である．□

補題 1.7 (剰余定理) R を整域とする．$f(x)\in R[x]$ を 1 次式 $x-a$ $(a\in R)$ で割った余りは定数多項式 $f(a)$ である．

証明: $f(x)$ を $x-\alpha$ で割った余りは 0 次式であるから定数 $c\in R$ である．商を $q(x)$ とすれば $R[x]$ において

$$f(x)=q(x)(x-a)+c$$

が成立するから，ρ_c が環準同型であることを用いると，$x=a$ を代入して
$f(a)=q(a)(a-a)+c=c$ を得る．□

1.4 イデアル

定義 1.7 可換環 R の空でない部分集合 I が R の**イデアル** (ideal) であるとは，

$$a, b \in I \Rightarrow a + b \in I, \qquad a \in I, c \in R \Rightarrow ca \in I$$

が成立することである．特に $a \in I$ ならば $0 = 0a \in I$ であるから，I は 0 を含む．$\{0\}$ と R は R のイデアルである．R と異なるイデアルを**真のイデアル** (proper ideal) という．

例 1.11 可換環 R の元 a に対して，

$$Ra = aR = \{ca \mid c \in R\}$$

は R のイデアルである．特に整数 n に対して $\mathbb{Z}n = \mathbb{Z}n$ (n の倍数全体) は $\mathbb{Z}$ のイデアルである．

補題 1.8 環 R のイデアル I について，$I = R$ であることと，$1 \in I$ は同値である．

証明: $I = R$ ならば $1 \in I$ であることは明らかである．逆に $1 \in I$ を仮定すると，任意の $c \in R$ について, $c = c1$ は I に属するから，$I = R$ となる．□

補題 1.9 $Ra = R$ であることと a が単元であることは同値である．

証明: a が単元ならば，任意の $c \in R$ について $c = c1 = (ca^{-1})a$ は R に属するから $Ra = R$ である．逆に $Ra = R$ と仮定すると，1 は Ra に属するから，ある $b \in R$ があって $1 = ba$ が成立する．よって a は単元である．□

I と J を可換環 R のイデアルとするとき，その和

$$I + J := \{a + b \mid a \in I, b \in J\}$$

は R のイデアルである．また共通部分 $I \cap J$ もイデアルである．さらに一般に，$I_1, \ldots, I_n$ が R のイデアルであるとき，

$$I_1 + I_2 + \cdots + I_n := \{a_1 + a_2 + \cdots + a_n \mid a_k \in I_k \ (k = 1, \ldots, n)\},$$
$$I_1 \cap I_2 \cap \cdots \cap I_n$$

も R のイデアルである．特に $a_1, \ldots, a_n \in R$ に対して $Ra_1 + \cdots + Ra_n$ を $a_1, \ldots, a_n$ の**生成するイデアル**という．

例 1.12 m と n を整数とすると，$\mathbb{Z}m + \mathbb{Z}n = \{am + bn \mid a, b \in \mathbb{Z}\}$ と $\mathbb{Z}m \cap \mathbb{Z}n$ は $\mathbb{Z}$ のイデアルである．たとえば，$\mathbb{Z}3 + \mathbb{Z}2 = \mathbb{Z}$ （$3 - 2 = 1$ より），$\mathbb{Z}3 \cap \mathbb{Z}2 = \mathbb{Z}6$ となる（整数 n が 2 の倍数かつ 3 の倍数であることと 6 の倍数であることは同値だから）．

定義 1.8 可換環 R から可換環 R' への環準同型 f に対して，その**核** (kernel) と**像** (image) を

$$\mathrm{Ker}\, f = \{a \in R \mid f(a) = 0_{R'}\}, \qquad \mathrm{Im}\, f = f(R) = \{f(a) \mid a \in R\}$$

で定義する．

命題 1.4 $f : R \to R'$ を可換環 R から可換環 R' への環準同型とすると，$\mathrm{Ker}\, f$ は R のイデアルであり，$\mathrm{Im}\, f$ は R' の部分環である．

証明: $f(0_R) = 0_{R'}$ より $0_R \in \mathrm{Ker}\, f$ である．$a, b \in \mathrm{Ker}\, f$ とする．$f(a+b) = f(a)+f(b) = 0_{R'} + 0_{R'} = 0_{R'}$ であるから，$a + b \in \mathrm{Ker}\, f$ が成立する．また，任意の $c \in R$ に対して $f(ca) = f(c)f(a) = f(c)0_{R'} = 0_{R'}$ となる．従って $\mathrm{Ker}\, f$ は R のイデアルである．

次に $a', b' \in \mathrm{Im}\, f$ とすると，$f(a) = a'$, $f(b) = b'$ となる $a, b \in R$ が存在する．このとき，

$$a' + b' = f(a) + f(b) = f(a + b) \in \mathrm{Im}\, f, \quad a'b' = f(a)f(b) = f(ab) \in \mathrm{Im}\, f,$$
$$-a' = -f(a) = f(-a) \in \mathrm{Im}\, f, \quad 0_{R'} = f(0_R) \in \mathrm{Im}\, f, \quad 1_{R'} = f(1_R) \in \mathrm{Im}\, f$$

と補題 1.3 より $\mathrm{Im}\, f$ は R' の部分環である．□

例 1.13 R を可換環，$c \in R$ とすると，

$$\rho_c : R[x] \ni f(x) \longmapsto f(c) \in R$$

は全射環準同型であった（命題 1.3）．剰余定理により，$f(c) = 0$ と $f(x)$ が $x - c$ の倍元であることとは同値であるから，$\mathrm{Ker}\, \rho_c = R[x](x - c)$ である．

1.5 剰余環と環準同型定理

R を可換環，I を R のイデアルとする．R における同値関係 $\sim$ を

$$a \sim b \quad \Leftrightarrow \quad a - b \in I$$

により定義する．これが同値関係であることを示そう．$a, b, c \in R$ とする．$a - a = 0 \in I$ より $a \sim a$ である．$a \sim b$ ならば $a - b \in I$ であり，$b - a = -(a - b)$ も I に属するから $b \sim a$ である．$a \sim b$ かつ $b \sim c$ とすると，$a - c = (a - b) + (b - c) \in I$ であるから $a \sim c$ が成立する．以上により $\sim$ は R における同値関係である．

この同値関係による商集合 $R/\sim$ を R/I と表す．$a \in R$ に対して，a を含む同値類を $[a]$ または $\overline{a}$ で表す．すなわち

$$\overline{a} = [a] = \{x \in R \mid x - a \in I\}$$

である．$a, b \in R$ に対して和 $\overline{a} + \overline{b} \in R/I$ と積 $\overline{a}\overline{b} \in R/I$ を

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a}\,\overline{b} = \overline{ab}$$

により「定義」する．この「定義」は同値類の代表元 a, b の取り方に依存しないことを確かめる必要がある．$a \sim a'$, $b \sim b'$ とすると，I がイデアルであることから，

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I, \qquad ab - a'b' = (a - a')b + a'(b - b') \in I$$

となるので $\overline{a+b} = \overline{a'+b'}$, $\overline{ab} = \overline{a'b'}$ であり，上の定義は同値類の選び方によらない (well-defined である) ことがわかった．

この和と積により R/I は可換環になる．加法の単位元は $\overline{0}$, 乗法の単位元は $\overline{1}$ である．実際，任意の $a \in R$ に対して R/I における和と積の定義より

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}, \qquad \overline{a}\overline{1} = \overline{a1} = \overline{a}$$

が成立する．また $a, b, c \in R$ に対して

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c})$$

が成立する．同様にして $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$ も示される．$\overline{a} + \overline{(-a)} = \overline{a+(-a)} = \overline{0}$ より $\overline{a}$ の加法に関する逆元は $-\overline{a} = \overline{-a}$ である．可換環の定義（定義 1.1）の (2), (7), (8) も容易に確かめられる．

この R/I のことを R の I による**剰余環** (quotient ring, factor ring, residue class ring) という．

写像 $\pi : R \longrightarrow R/I$ を $\pi(a) = \overline{a}$ により定義しよう．このとき π は全射な環準同型である．実際，$a, b \in R$ に対して $\pi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b)$ と $\pi(ab) = \overline{ab} = \overline{a}\overline{b} = \pi(a)\pi(b)$ が成立し，$\pi(1) = \overline{1}$ は R/I における乗法の単位元である．また R/I の任意の元はある $a \in R$ によって $\overline{a} = \pi(a)$ と表される．π のことを自然な全射環準同型ということもある．

例 1.14 $n \in \mathbb{Z}$ に対して $\mathbb{Z}n = n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$ は $\mathbb{Z}$ のイデアルであるから，剰余環 $\mathbb{Z}/\mathbb{Z}n$ が定義される．$n = 0$ のときは $\mathbb{Z}n = \{0\}$ であるから，$a, b \in \mathbb{Z}$ に対して $a \sim b$ と $a = b$ は同値である．従って $\mathbb{Z}/\mathbb{Z}n = \mathbb{Z}/\{0\}$ は $\mathbb{Z}$ と同一視できる．

$n \neq 0$ の場合は $\mathbb{Z}n = \mathbb{Z}(-n)$ であるから $n > 0$ としてよい．a を任意の整数とするとき，a を n で割り算して，

$$a = qn + r \qquad (0 \leq r < n)$$

を満たす整数 q （商）と r（剰余）が一意的に存在する．このとき $a - r = qn \in \mathbb{Z}n$ であるから，$a \sim r$ すなわち $\mathbb{Z}/\mathbb{Z}n$ において $\overline{a} = \overline{r}$ が成立する．従って $\mathbb{Z}/\mathbb{Z}n$ の元（$\mathbb{Z}$ における同値関係 $\sim$ による同値類）は $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ のいずれかである．また j, k を $0 \leq j < k \leq n-1$ を満たす整数とするとき， $k - j$ は n の倍数ではないから，$\overline{j} \neq \overline{k}$ である．以上により，n が自然数のときは集合として

$$\mathbb{Z}/\mathbb{Z}n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

であることがわかった．$\mathbb{Z}/\mathbb{Z}n$ は上で定義した演算によって環となる．加法の単位元は $\overline{0}$, 乗法の単位元は $\overline{1}$ である．$0 \leq a \leq n-1$ かつ $0 \leq b \leq n-1$ のとき $a+b$ を n で割った余りを c, ab を n で割った余りを d とすれば $\overline{a} + \overline{b} = \overline{c}$, $\overline{a}\overline{b} = \overline{d}$ である．n が素数でなければ $n = jk$ を満たす $j, k \in \{2, \ldots, n-1\}$ が存在するから $\overline{j}\overline{k} = \overline{0}$ となり，$\mathbb{Z}/\mathbb{Z}n$ は整域でない．たとえば $\mathbb{Z}/3\mathbb{Z}$ と $\mathbb{Z}/4\mathbb{Z}$ の加法と乗法の演算表は次のようになる．

$\mathbb{Z}/3\mathbb{Z}$

和	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

積	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/4\mathbb{Z}$

和	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

積	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

定義 1.9 R を可換環とする．0 と異なる R の元 a について，0 と異なるある $b \in R$ があって $ab = 0$ となるとき，a を R の**零因子** (zero divisor) という．定義より，R が整域であることと R の零因子が存在しないこととは同値である．

例 1.15 上の演算表からわかるように，$\mathbb{Z}/3\mathbb{Z}$ は整域であり零因子を持たない．一方 $\mathbb{Z}/4\mathbb{Z}$ の零因子は $\overline{2}$ である．また $\mathbb{Z}/6\mathbb{Z}$ の零因子は $\overline{2}, \overline{3}, \overline{4}$ である．

例 1.16 K を体とする．K 係数の n 次多項式 f を 1 つ決めて，多項式環 $K[x]$ のイデアル $K[x]f$ による剰余環 $R := K[x]/K[x]f$ を考察しよう．任意の $g \in K[x]$ に対して g を f で割り算して

$$g = qf + r \qquad (q, r \in K[x],\ \deg r < n)$$

と書く．g の R における剰余類を $[g]$ で表すと，$g - r = qf \in K[x]f$ より $[g] = [r]$ である．従って，R の任意の元はある $n-1$ 次以下の多項式の同値類である．また $r, r' \in K[x]$ かつ $\deg r < n$, $\deg r' < n$ とすると，

$$[r] = [r'] \quad \Leftrightarrow \quad r - r' \in K[x]f \quad \Leftrightarrow \quad r - r' = qf \quad (\exists q \in K[x])$$

であるが，$r - r'$ の次数は $n = \deg f$ より小さいから，これが成立するのは $r - r' = 0$ すなわち $r = r'$ の場合のみである．以上により，集合としては

$$R = \{[g] \mid g \in K[x],\ \deg g \leq n - 1\}$$

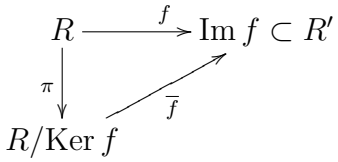
すなわち次数 $n-1$ 以下の多項式の全体と同一視できる．たとえば

$$S := \mathbb{Q}[x]/\mathbb{Q}[x](x^2 - 2) = \{[ax + b] \mid a, b \in \mathbb{Q}\}$$

であり，$[x^2] = [2]$ に注意すると $a, b, c, d \in \mathbb{Q}$ のとき S において

$$[ax + b][cx + d] = [acx^2 + (ad + bc)x + bd] = [(ad + bc)x + (2ac + bd)]$$

定理 1.1 (環準同型定理) R と R' を可換環とし，$f : R \longrightarrow R'$ を環準同型とする．$\pi : R \longrightarrow R/\mathrm{Ker}\, f$ を自然な全射準同型，すなわち $\pi(a) = \overline{a}$ を $a \in R$ の $R/\mathrm{Ker}\, f$ における同値類とする．このとき環同型 $\overline{f} : R/\mathrm{Ker}\, f \xrightarrow{\sim} \mathrm{Im}\, f$ であって，$\overline{f} \circ \pi = f$ すなわち $\overline{f}(\overline{a}) = f(a)$ $(\forall a \in R)$ をみたす $\overline{f}$ がただ一つ存在する．



証明: $\overline{f}(\overline{a}) = f(a)$ であるから，このような $\overline{f}$ は存在すれば一通りしかない．まず，$\overline{f}(\overline{a}) = f(a)$ によって写像 $\overline{f} : R/\mathrm{Ker}\, f \to R'$ が定まる (well-defined) ことを示そう．$\overline{a} = \overline{b}$ すなわち $a - b \in \mathrm{Ker}\, f$ とすると，$f(a) - f(b) = f(a - b) = 0$ であるから，$\overline{f}(\overline{a}) = \overline{f}(\overline{b})$ となる．よって $\overline{f}$ は well-defined である．$a, b \in R$ に対して，

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

同様に $\overline{f}(\overline{a}\overline{b}) = \overline{f}(\overline{a})\overline{f}(\overline{b})$ も成立する．従って $\overline{f}$ は環準同型である．

$$\overline{f}(\overline{a}) = f(a) = 0 \;\Leftrightarrow\; a \in \mathrm{Ker}\, f \;\Leftrightarrow\; \overline{a} = 0$$

であるから $\overline{f}$ は単射である．$\overline{f}$ の像は f の像 $\mathrm{Im}\, f$ と一致するから，$\overline{f}$ は $R/\mathrm{Ker}\, f$ から $\mathrm{Im}\, f$ への全射である．□

例 1.17 R を整域とする．$c \in R$ を固定するとき，写像

$$\rho_c : R[x] \ni f(x) \longmapsto f(c) \in R$$

は全射環準同型であり，準同型定理により環同型

$$\overline{\rho_c} : R[x]/\mathrm{Ker}\, \rho_c \longrightarrow R$$

であって $\overline{\rho_c}([f]) = \rho_c(f) = f(c)$ が任意の $f \in R[x]$ について成り立つようなものが存在する．ここで $[f]$ は f の $R[x]/\mathrm{Ker}\, \rho_c$ における剰余類を表す．剰余定理により $\mathrm{Ker}\, \rho_c = R[x](x - c)$ が成立するから，剰余環 $R[x]/R[x](x - c)$ と R は同型である．

1.6 ユークリッド整域と単項イデアル整域

R を整域とする．R の元 a, b $(a \neq 0)$ について，$b = ac$ となる $c \in R$ が存在するとき，a を b の**約数** (divisor) または**約元**，b を a の**倍数** (multiple) または**倍元**という．このとき a は b を割り切るといい，記号 $a|b$ で表す．$a|b$ と $Rb \subset Ra$ は同値である．実際 $a|b$ ならば $b \in Ra$ であるから $Rb \subset Ra$ となる．逆に $Rb \subset Ra$ ならば $b \in Ra$ であるから，$a|b$ となる．

定義 1.10 可換環 R のイデアル I が**単項イデアル** (principal ideal) であるとは，R の元 a が存在して I が a の倍元全体，すなわち

$$I = Ra = \{ca \mid c \in R\}$$

となることである．Ra のことを a の生成するイデアルといい，aR または (a) と表すこともある．

定義 1.11 整域 R が**単項イデアル整域** (principal ideal domain, PID) であるとは，R の任意のイデアルが単項イデアルであることである．

定義 1.12 整域 R が**ユークリッド整域** (Euclidean domain) であるとは，写像

$$N : R \ni a \longmapsto N(a) \in \mathbb{N} \cup \{0, -1\}$$

が存在して次を満たすことである．

(1) $a \neq 0$ ならば $N(a) > N(0)$

(2) $a \neq 0$ ならば，任意の $b \in R$ に対してある $q \in R$ とある $r \in R$ が存在して

$$b = qa + r, \quad N(r) < N(a) \qquad (b \text{ の } a \text{ による割り算})$$

例 1.18 整数環 $\mathbb{Z}$ はユークリッド整域である．実際，整数 n に対して $N(n) := |n|$ を n の絶対値とすれば，これは $\mathbb{Z}$ から $\mathbb{N} \cup \{0, -1\}$ への写像である．$n \neq 0$ のとき $N(n) = |n| \geq 1 > 0 = N(0)$ であるから，定義の (1) は成り立つ．$n \neq 0$ のとき，任意の整数 m を $|n|$ で割った余りを r, 商を q とすれば，

$$m = q|n| + r, \quad 0 \leq r < |n|$$

が成立する．よって $N(r) = r < |n| = N(n)$ であり，$n > 0$ ならば $m = qn + r$, $n < 0$ ならば $m = (-q)n + r$ となるのでユークリッド整域の定義が満たされる．

命題 1.5 K を体とするとき多項式環 $K[x]$ はユークリッド整域である．

証明: $f \in K[x]$ に対して，$f \neq 0$ ならば $N(f) = \deg f$, $f = 0$ ならば $N(f) = N(0) = -1$ により写像 $N : K[x] \to \mathbb{N} \cup \{0, -1\}$ を定義する．$f \in K[x]$ が 0 多項式でなければ $\deg f \geq 0$ である．また，割り算により，任意の $g \in K[x]$ に対して

$$g = qf + r, \quad \deg r < \deg f$$

をみたす $q, r \in K[x]$ が存在する．このとき $r \neq 0$ ならば $N(r) = \deg r < \deg f = N(f)$, $r = 0$ ならば $N(r) = -1 < 0 \leq \deg f = N(f)$ が成立するから $K[x]$ はユークリッド整域である．□

定理 1.2 ユークリッド整域は単項イデアル整域 (PID) である．

証明: R をユークリッド整域，N を R から $\mathbb{N} \cup \{0, -1\}$ への写像でユークリッド整域の条件をみたすものとする．I を R の任意のイデアルとする．$I = \{0\}$ の場合は，$I = R0$ であるから I は単項イデアルである．よって以下では，I は 0 以外の元を含むと仮定してよい．$\mathbb{N} \cup \{0, -1\}$ の部分集合 $\{N(a) \mid a \in I \setminus \{0\}\}$ は最小元を持つ．すなわち，ある $a \in I \setminus \{0\}$ があって，任意の 0 でない I の元 b に対して，$N(a) \leq N(b)$ が成立する．このとき， $I = Ra = \{ca \mid c \in R\}$ となることを示そう．まず，$a \in I$ と I がイデアルであることより $Ra \subset I$ が従う．逆の包含関係を示そう．b を I の任意の元とすると，

$$b = qa + r, \quad N(r) < N(a)$$

をみたす $q, r \in R$ が存在する．このとき，I がイデアルであることから，$r = b - qa$ は I に属する．いま $r \neq 0$ と仮定すると，$N(a)$ の最小性から $N(r) \geq N(a)$ でなければならないが，これは割り算の性質に反する．よって $r = 0$ でなければならない．すると，$b = qa \in Ra$ であるから，$I \subset Ra$ が示された．故に $I = Ra$ であり I は単項イデアルである．□

この定理によって整数環 $\mathbb{Z}$ と体 K 上の多項式環 $K[x]$ はともに単項イデアル整域であることがわかる．

補題 1.10 a, b を整域 R の 0 と異なる 2 つの元とする．このとき $Ra \subset Rb$ と a が b の倍元であることとは同値である．

証明: $Ra \subset Rb$ と仮定すると $a \in Ra \subset Rb$ であるから a は Rb に属する．よって $a = qb$ を満たす $q \in R$ が存在する．逆に $a = qb$ を満たす $q \in R$ が存在すれば，任意の $c \in R$ について $ca = cqb \in Rb$ であるから $Ra \subset Rb$ が成立する．□

補題 1.11 整域 R の 2 つの単項イデアル Ra と Rb $(a, b \in R)$ が一致するための条件は，ある単元 $u \in R$ があって $b = ua$ が成立することである．

証明: $a \in Ra$ より，$Ra = \{0\}$ と $a = 0$ は同値である．よって a と b は 0 と異なるとしてよい．上の補題によって $Ra = Rb$ となるための条件は $b|a$ かつ $a|b$ である．このとき $b = ua$ かつ $a = vb$ を満たす $u, v \in R$ が存在する．$a = vb = uva$ より $(1 - uv)a = 0$ となるが，R は整域であり $a \neq 0$ だから $1 - uv = 0$ すなわち $uv = 1$ である．よって u, v は単元である．逆に，ある単元 u が存在して $b = ua$ であれば $a = u^{-1}b$ より $a|b$ かつ $b|a$ であるから，上の補題により $Ra = Rb$ である．□

例 1.19 $\mathbb{Z}$ のイデアルは，0 以上の整数（非負整数）n を用いて $I = \mathbb{Z}n$ と表される．この対応によって，非負整数の全体と $\mathbb{Z}$ のイデアル全体が 1 対 1 に対応する．

一般に整域 R の 0 でない 2 つの元 a, b に対して，$d \in R \setminus \{0\}$ が a と b の**最大公約元** (greatest common divisor, GCD) とは，$d|a$ かつ $d|b$ であって，さらに R の 0 でない任意の元 e が $e|a$ かつ $e|b$ をみたせば $e|d$ となることである．a と b の最大公約元を $\mathrm{GCD}(a, b)$ で表そう．a と b の最大公約元が単元であるとき，a と b は**互いに素** (relatively prime) であるという．

命題 1.6 a, b を単項イデアル整域 R の 0 でない元とすると，$d \in R$ が a と b の最大公約元であるための必要十分条件は $Ra + Rb = Rd$ が成立することである．特に，a と b の最大公約元は存在して，単元倍を除いて一意的である．

証明: $Ra + Rb = Rd$ を仮定する．$a \in Ra \subset Rd$ であるから $d|a$ である．同様に $d|b$ も成立する．$e|a$ かつ $e|b$ とすると，$Ra \subset Re$ かつ $Rb \subset Re$ より $Rd = Ra + Rb \subset Re$ となるから $e|d$ である．よって d は a と b の最大公約元である．

逆に d を a と b の最大公約元とする．R は単項イデアル整域であるから，$Ra + Rb = Re$ となるような $e \in R$ が存在する．このとき前半の議論により e は a と b の最大公約元

である．最大公約元の定義から $e|d$ かつ $d|e$ が成立するから，e は d の単元倍であり，$Ra+Rb=Re=Rd$ となる．以上と補題 1.11 より，最大公約元 d は単元倍を除いて一意的であることがわかる．□

R が単項イデアル整域であるとき, R の零でない元 a と b が互いに素であるための必要十分条件は，上の命題により $Ra+Rb=R$ が成立することである．このとき $Ra\cap Rb=Rab$ が成立する．実際，$Rab\subset Ra\cap Rb$ は明らかであるから，$x\in Ra\cap Rb$ とする．a と b は互いに素だから $sa+tb=1$ を満たす $s,t\in R$ が存在する．このとき $x=x(sa+tb)=sax+tbx$ であり ax と bx は共に ab の倍元であるから x は Rab に属する．

R がユークリッド整域の場合には，最大公約元は以下の**ユークリッドの互除法** (Euclidean algorithm) により計算することができる．

R の 0 と異なる元 a,b に対して，次のように R の元 $q_1,q_2,\dots$ と $r_1,r_2,\dots$ を順番に割り算して決める:

$$\begin{aligned} a&=q_1b+r_1, && N(r_1)<N(g),\\ b&=q_2r_1+r_2, && N(r_2)<N(r_1),\\ r_1&=q_3r_2+r_3, && N(r_3)<N(r_2)\\ &\cdots \end{aligned}$$

ただし，ある自然数 k に対して $r_k=0$ となったら終了する．もしこの操作が終了しなかったとすると，$N(r_1)>N(r_2)>N(r_3)>\cdots$ となるが，一方任意の自然数 k について $N(r_k)\geq -1$ であるから，この不等式が無限に続くことはあり得ない．従ってこの手続き（アルゴリズム）は有限回で終了する．そこで $r_n\neq 0$ かつ $r_{n+1}=0$ とすると

$$r_{j-1}=q_{j+1}r_j+r_{j+1}\quad (0\leq j\leq n) \tag{1}$$

が成立する． ただし $r_{-1}:=a$, $r_0:=b$ とおいた．このとき $r_n=\mathrm{GCD}(a,b)$ であることを示そう．そのために (1) において

$$\mathrm{GCD}(r_{j-1},r_j)=\mathrm{GCD}(r_j,r_{j+1}) \tag{2}$$

が成立することに注意する． 実際，$c\in R$ が r_{j-1} と r_j を割り切るとすると，(1) から c は $r_{j+1}=r_{j-1}-q_{j+1}r_j$ も割り切る．逆に c が r_j と r_{j+1} を割り切るとすると，(1) から c は r_{j-1} も割り切る．従って r_{j-1} と r_j の公約元全体と r_j と r_{j+1} の公約元全体は一致するから (2) が成立する．(2) を次々に用いれば

$$\mathrm{GCD}(a,b)=\mathrm{GCD}(r_{-1},r_0)=\mathrm{GCD}(r_0,r_1)=\cdots=\mathrm{GCD}(r_{n-1},r_n)$$

であり，r_n は r_{n-1} を割り切るから，$\mathrm{GCD}(r_{n-1},r_n)=r_n$ である．

この過程を逆にたどれば $d=\mathrm{GCD}(a,b)$ のとき $d=sa+tb$ を満たす $s,t\in R$ を一組求めることができる（以下の例を参照）．

例 1.20 $\mathbb{Z}$ において 855 と 2014 の最大公約数を求めよう．

$$\begin{aligned} &2014=2\times 855+304, && 855=2\times 304+247, && 304=1\times 247+57,\\ &247=4\times 57+19, && 57=3\times 19+0 \end{aligned}$$

よって $\mathrm{GCD}(855, 2014) = 19$ である．この計算を逆にたどると，

$$\begin{aligned} 19 &= 247 - 4 \times 57 = 247 - 4 \times (304 - 1 \times 247) = -4 \times 304 + 5 \times 247 \\ &= -4 \times 304 + 5 \times (855 - 2 \times 304) = 5 \times 855 - 14 \times 304 \\ &= 5 \times 855 - 14 \times (2014 - 2 \times 855) = -14 \times 2014 + 33 \times 855 \end{aligned}$$

例 1.21 多項式環 $\mathbb{Q}[x]$ において $f = x^4 - 1$ と $g = x^3 - x^2 + 2x - 2$ の最大公約元は,

$$\begin{aligned} f &= (x+1)g + (-x^2+1), \\ g &= -(x-1)(-x^2+1) + (3x-3), \\ -x^2+1 &= \left(-\frac{1}{3}x - \frac{1}{3}\right)(3x-3) \end{aligned}$$

より $3x - 3 = 3(x - 1)$ である． 3 は $\mathbb{Q}[x]$ における単元だから f と g の最大公約元は $x - 1$ としてよい．なお，f, g の係数は整数であるが，途中の計算で有理数係数の多項式が現れている．$\mathbb{Z}[x]$ はユークリッド整域ではないのでユークリッド整域である $\mathbb{Q}[x]$ で計算を実行する必要があるからである．この計算を逆にたどると

$$\begin{aligned} x - 1 &= \frac{1}{3}(3x-3) = \frac{1}{3}g + \frac{1}{3}(x-1)(-x^2+1) = \frac{1}{3}g + \frac{1}{3}(x-1)\{f - (x+1)g\} \\ &= \frac{1}{3}(x-1)f + \frac{1}{3}(-x^2+2)g \end{aligned}$$

命題 1.7 R を単項イデアル整域，$I_1, I_2, I_3, \ldots$ を R のイデアルの無限増大列，すなわち

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

をみたすイデアルの列とする．このとき，ある自然数 n が存在して，$k \geq n$ のとき $I_k = I_n$ が成り立つ．すなわち n 番目以降のイデアルはすべて同一となる．

証明: $I = \bigcup_{k \geq 1} I_k$ とおく．I は R のイデアルである．実際，$a, b \in I$ とすると，ある自然数 j と k があって $a \in I_j$, $b \in I_k$ となる．たとえば $j \geq k$ とすると $a, b \in I_j$ であるから，$a + b \in I_j \subset I$ である．また，任意の $c \in R$ に対して，$ca \in I_j \subset I$ となる．よって I は R のイデアルである．R は単項イデアル整域であるから，ある $a \in I$ があって $I = Ra$ と表される． I の定義により，ある n があって $a \in I_n$ となる．任意の $c \in R$ に対して $ac \in I_n$ であるから，$I = Ra \subset I_n$ である．定義より $I_n \subset I$ であるから，$I = I_n$ でなければならない．このとき，任意の $k \geq n$ について， $I = I_n \subset I_k \subset I$ より $I_k = I_n$ が成立する．□

1.7 素イデアルと極大イデアル

定義 1.13 可換環 R の真のイデアル $I \subsetneq R$ が**素イデアル** (prime ideal) とは，$a, b \in R$ について，$ab \in I$ ならば $a \in I$ または $b \in I$ となることである．

定義 1.14 可換環 R の真のイデアル $I \subsetneqq R$ が**極大イデアル** (maximal ideal) とは，$I \subsetneqq J \subsetneqq R$ をみたすイデアル J が存在しないことである．

命題 1.8 R を可換環，I を R の真のイデアルとする．

(1) I が素イデアルであることと R/I が整域であることは同値である．

(2) I が極大イデアルであることと R/I が体であることは同値である．

証明: (1) I を素イデアルとする．$a, b \in R$ に対してそれらの R/I における剰余類を $\overline{a}, \overline{b}$ で表す．$\overline{a}\overline{b} = \overline{0}$ とすると，$ab \in I$ であるから，$a \in I$ または $b \in I$, すなわち $\overline{a} = \overline{0}$ または $\overline{b} = \overline{0}$ となる．よって R/I は整域である．逆に R/I が整域ならば $ab \in I$ のとき $\overline{a}\overline{b} = \overline{0}$ より $\overline{a} = \overline{0}$ または $\overline{b} = \overline{0}$，すなわち $a \in I$ または $b \in I$ となるので，I は素イデアルである．

(2) I を極大イデアルとする．$a \in R \setminus I$ すなわち $\overline{a} \neq \overline{0}$ とすると，$a \notin I$ より $I \subsetneqq I + Ra$ であるから $I + Ra = R$ でなければならない．よって $x + ca = 1$ となる $x \in I$ と $c \in R$ が存在する．このとき $\overline{x} = \overline{0}$ であるから

$$\overline{1} = \overline{x} + \overline{c}\,\overline{a} = \overline{c}\,\overline{a}$$

よって $\overline{a}$ は R/I の可逆元だから R/I は体である．

逆に R/I が体であると仮定して I が極大イデアルであることを示そう．$I \subsetneqq J$ をみたすイデアル J があったとして，$a \in J \setminus I$ をとる．$\overline{a} \neq \overline{0}$ であるから，$\overline{a}\overline{b} = \overline{1}$ となる $b \in R$ が存在する．このとき $ab - 1 \in I$ である．$I \subset J$ と $a \in J$ より $1 = (1 - ab) + ab \in J$ であるから，$J = R$ となる．よって I は極大イデアルである．□

系 1.1 可換環 R の極大イデアルは素イデアルである．

証明: 体は整域であるから，上の命題から直ちに従う．□

例 1.22 p を素数とすると $\mathbb{Z}p$ は $\mathbb{Z}$ の極大イデアルである．実際，$\mathbb{Z}p$ が極大イデアルでないと仮定すると，$\mathbb{Z}p \subsetneqq J \subsetneqq \mathbb{Z}$ を満たす $\mathbb{Z}$ のイデアル J が存在する．J は $\{0\}$ とは異なる単項イデアルであるから，ある自然数 n があって $J = \mathbb{Z}n$ となる．$J \neq \mathbb{Z}$ より $1 \notin J$ であるから $n \geq 2$ である．このとき $p \in \mathbb{Z}p \subset J = \mathbb{Z}n$ より p は n の倍数である．p は素数であるから $n = p$ でなければならない．すると $\mathbb{Z}p = J$ となり仮定に反する．よって $\mathbb{Z}p$ は極大イデアルである．従って素イデアルでもある．

p が素数でない 2 以上の自然数ならば $p = qr$ をみたす 2 以上の整数 q, r が存在する．このとき q も r も p の倍数ではないから，$q \notin \mathbb{Z}p, r \notin \mathbb{Z}p$ かつ $qr \in \mathbb{Z}p$ となる．従って $\mathbb{Z}p$ は素イデアルではない．以上により自然数 p について次の同値性が示された：

$$p \text{ は素数} \quad \Leftrightarrow \quad \mathbb{Z}p \text{ は } \mathbb{Z} \text{ の極大イデアル} \quad \Leftrightarrow \quad \mathbb{Z}p \text{ は } \mathbb{Z} \text{ の素イデアル}$$

ただし $\{0\}$ は $\mathbb{Z}$ の素イデアルであるが極大イデアルではない（たとえば $\{0\} \subsetneqq 2\mathbb{Z}$）．

例 1.23 $I = \mathbb{Z}[x]x$ は $\mathbb{Z}[x]$ の素イデアルであるが極大イデアルではない．実際，

$$\rho_0 : \mathbb{Z}[x] \ni f(x) \longmapsto f(0) \in \mathbb{Z}$$

は $\mathbb{Z}[x]$ から $\mathbb{Z}$ への全射環準同型であり，$\mathrm{Ker}\,\rho_0$ は定数項が 0 の多項式全体であるから $\mathbb{Z}[x]x = I$ と一致する．従って環準同型定理より，$\mathbb{Z}[x]/I$ から $\mathbb{Z}$ への環同型が存在する．$\mathbb{Z}$ は整域であるから I は素イデアルである．しかし $\mathbb{Z}$ は体ではないから I は極大イデアルではない．

命題 1.9 単項イデアル整域 R の $\{0\}$ と異なる素イデアルは極大イデアルである．

証明: I を単項イデアル整域 R の $\{0\}$ と異なる素イデアルとする．ある $p \in R \setminus \{0\}$ があって $I = Rp$ となる．J を $I \subsetneqq J$ をみたす R のイデアルとする．ある $a \in R \setminus \{0\}$ があって $J = Ra$ となる．このとき，$Rp \subset Ra$ より $a|p$ であり，ある $b \in R$ によって $p = ab$ と書ける．Rp は素イデアルで $ab = p \in Rp$ であるから，$a \in Rp$ または $b \in Rp$ が成立する．もし $a \in Rp$ ならば $J = Ra \subset Rp = I$ となり J の取り方に反する．よって $b \in Rp$ でなければならない．従ってある $u \in R$ が存在して $b = up$ と書ける．$p = ab = aup$ より $(au - 1)p = 0$ となるが，$I \neq \{0\}$ より $p \neq 0$ であり R は整域であるから $au = 1$ を得る．従って a は単元であり，$J = Ra = R$ となる．よって I は極大イデアルである．□

命題 1.10 R を単項イデアル整域，I を R の真のイデアルとすると，R の極大イデアル J であって $I \subset J$ を満たすものが存在する．

証明: I が極大イデアルならば $J = I$ とすればよい．I が極大イデアルでなければ $I \subsetneqq I_1 \subsetneqq R$ をみたすイデアル I_1 が存在する．I_1 が極大イデアルならば $J = I_1$ とすればよい．I_1 が極大イデアルでなければ $I_1 \subsetneqq I_2 \subsetneqq R$ を満たすイデアル I_2 が存在する．以下同様にして，I_k が極大イデアルでなければ $I_k \subsetneqq I_{k+1} \subsetneqq R$ を満たすイデアル I_{k+1} が存在する．この操作が終了しなければ，すなわち $I_1, I_2, \ldots$ が極大イデアルでなければ，イデアルの真の増大列 $I_1 \subsetneqq I_2 \subsetneqq \cdots$ ができることになり命題 1.7 に矛盾する．従ってある自然数 n があって I_n は極大イデアルとなる．$I \subset I_n$ であるから主張が示された．□

たとえば $\mathbb{Z}$ においてイデアル $\mathbb{Z}6$ は 2 つの極大イデアル $\mathbb{Z}2$ と $\mathbb{Z}3$ に含まれる．

1.8 素元分解整域

定義 1.15 R を整域とし，p を R の零でも単元でもない元とする．

(1) p が**素元** (prime element) とは，イデアル Rp が素イデアルとなることである．(すなわち $a, b \in R$ について ab が p の倍元ならば a または b が p の倍元であること.)

(2) p が**既約元** (irreducible element) または既約であるとは，$p = ab$ $(a, b \in R)$ ならば a または b が R の単元となることである．(すなわち，単元でない 2 つの元の積に分解されないこと.)

p が素元（または既約元）であって，u が単元ならば，up も素元（または既約元）であることは容易にわかる．

例 1.24 0 でない整数 n について n が既約元であることと $|n|$ が素数であることは（素数の定義より）同値である．また，例 1.22 より n が素元であることと $|n|$ が素数であることも同値である．従って $\mathbb{Z}$ においては既約元と素元は一致する．

例 1.25 K を体として $f \in K[x]$ を 0 でない多項式とする．f が $K[x]$ の既約元であるための必要十分条件は，$f = gh$ かつ $\deg g \geq 1, \deg h \geq 1$ を満たす $g, h \in K[x]$ が存在しないことである．実際，$K[x]$ の単元は 0 でない定数多項式であるから，$f = gh$ かつ g, h が単元でなければ g, h の次数は 1 以上である．特に f の次数が 3 以下であれば，f が既約元であるための必要十分条件は，$f(a) = 0$ を満たす $a \in R$ が存在することである．実際，f が既約でなければ，f は次数 1 の約元 $x - a$ を持たなければならない．このとき剰余定理から $f(a) = 0$ である．$K[x]$ の既約元のことを**既約多項式**という．

例 1.26 $f = 2(x^2 + 1)$ は $\mathbb{Q}[x]$ における既約元である（$f(a) = 0$ を満たす $a \in \mathbb{Q}$ が存在しないから）が，$\mathbb{Z}[x]$ においては既約元でない（2 は $\mathbb{Z}[x]$ の単元でないから）．また，$\mathbb{C}[x]$ においては $f = 2(x - i)(x + i)$ と分解されるから，f は既約元でない．

例 1.27 $R := \mathbb{Z}[\sqrt{-5}]$ において

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$$

が成立する．$1 \pm \sqrt{-5}$ は 2 の倍元でない（実部 1 が 2 の倍数でないので）がそれらの積は 6 で 2 の倍元であるから 2 は R の素元ではない．同様にして，3 と $1 \pm \sqrt{-5}$ も R の素元ではないことがわかる．しかし，$2, 3, 1 \pm \sqrt{-5}$ は R の既約元である．

命題 1.11 R を整域とするとき，$p \in R$ が素元ならば p は既約元である．

証明: まず，p は単元でないことを示す．p が単元とすると，$1 = p^{-1}p \in Rp$ となるから $Rp = I$ であり，Rp が素イデアル，従って真のイデアルであることに反する．次に，R の元 a, b があって $p = ab$ と表されたする．$ab = p \in Rp$ であり，Rp は素イデアルだから，$a \in Rp$ または $b \in Rp$ である．たとえば $a \in Rp$ とすると，ある $c \in R$ があって，$a = cp$ と書ける．このとき，$p = ab = cbp$ すなわち $(cb - 1)p = 0$ である．$p \neq 0$ で R は整域だから，$cb = 1$，よって b は単元である．以上により p は既約元であることが示された．□

整域 R において，0 でなく単元でもない a が有限個の素元 $p_1, \ldots, p_r$ の積として $a = p_1 \cdots p_r$ と表されるとき，これを a の**素元分解**という．R の 0 でなく単元でもない任意の元が素元分解を持つとき，R を**素元分解整域** あるいは **一意分解整域** (unique factorization domain, UFD) という．「一意」（一通り）という形容詞は次の命題で正当化される．

命題 1.12 整域 R の 0 でなく単元でもない a の素元分解が存在すれば，それは単元倍を除いて一意的（一通り）である．すなわち，もし

$$a = p_1 \cdots p_r = q_1 \cdots q_s \qquad (p_i, q_j \text{ は } R \text{ の素元})$$

と 2 通りに素元分解されれば，$r = s$ であり，集合 $\{1, \ldots, r\}$ のある置換 σ が存在して，$i = 1, \ldots, r$ について，$q_{\sigma(i)}$ は p_i の単元倍となる．

証明: $q_1(q_2\cdots q_s)$ は p_1 の倍元だから，素イデアル Rp_1 に属する．従って q_1 または $q_2\cdots q_s$ は Rp_1 に属する．もし $q_1 \notin Rp_1$ ならば $q_2(q_3\cdots q_s) \in Rp_1$ より，$q_2 \in Rp_1$ または $q_3\cdots q_s \in Rp_1$ となる．この議論を続ければ，結局ある q_i が Rp_1 に属することがわかる．$q_1,\dots,q_s$ を並べ変えて $q_1 \in Rp_1$ としてよい．このとき，ある $u_1 \in R$ によって $q_1 = u_1p_1$ と書ける．q_1 は素元であるから，命題 1.11 により既約元である．p_1 は単元でないから，u_1 が単元でなければならない．$q_1 = u_1p_1$ を最初の素元分解の式に代入すると，

$$p_1p_2\cdots p_r = u_1p_1q_2\cdots q_s \quad \text{すなわち} \quad p_2\cdots p_r = u_1q_2\cdots q_s$$

を得る．次に $q_2\cdots q_s = u_1^{-1}p_2\cdots p_r$ は Rp_2 に属するから，上と同様の議論により，適当に順番を入れ替えれば，q_2 が Rp_2 に属し，ある単元 u_2 によって $q_2 = u_2p_2$ と表されることがわかる．以上の議論を繰り返せば，適当に順番を入れ替えることにより，$i = 1,\dots,r$ について，単元 u_i が存在して $q_i = u_ip_i$ が成立する．特に $r \le s$ である．$r < s$ とすると

$$p_1\cdots p_r = q_1\cdots q_s = (u_1p_1)\cdots(u_rp_r)q_{r+1}\cdots q_s = u_1\cdots u_rp_1\cdots p_rq_{r+1}\cdots q_s$$

が成立する．これと R が整域であることから，$1 = u_1\cdots u_rq_{r+1}\cdots q_s$ となるが，$q_{r+1},\dots,q_s$ は単元ではないから矛盾である．従って $r = s$ であり命題の主張が示された．□

命題 1.13 R を一意分解整域とすると，R の 0 でない元 a について，a が素元であることと a が既約元であることは同値である．

証明: 命題 1.11 より素元は既約元であるから，既約元が素元であることを示せばよい．そこで a を既約元として，$a = p_1\cdots p_r$ を素元分解とする．$p_1,\dots,p_r$ は素元だから既約元であり，特に単元ではない．よって $r \ge 2$ ならば a が既約元であることに反するから $r = 1$ でなければならない．従って $a = p_1$ は素元である．□

定理 1.3 単項イデアル整域 (PID) は一意分解整域 (UFD) である．

証明: 単項イデアル整域 R の 0 でも単元でもない任意の元 a が素元分解を持つことを示せばよい．命題 1.10 により $Ra \subset I_1$ を満たす極大イデアル I_1 が存在する．R は単項イデアル整域だから，$I_1 = Rp_1$ となる $p_1 \in R$ が存在する．Rp_1 は極大イデアルだから素イデアルであり，p_1 は素元である．$a \in Ra \subset I_1 = Rp_1$ より $a = p_1a_1$ となる $a_1 \in R$ が存在する．a_1 が単元でなければ，Ra_1 は真のイデアルであるから，上の議論を a の代わりに a_1 に対して適用することにより，$a_1 = p_2a_2$ となるような素元 p_2 と $a_2 \in R$ が存在する．この操作を続けると，$a_i = p_{i+1}a_{i+1}$ $(i = 1,2,3,\dots)$ をみたす R の素元 p_{i+1} と $a_{i+1} \in R$ が順に決まる．ただし，ある $i = n$ について a_n が単元になれば，この操作は終了して，$a = p_1\cdots p_{n-1}(a_np_n)$ は a の素元分解である．もしこの操作が終了しなければイデアルの無限増大列

$$Ra \subset Ra_1 \subset Ra_2 \subset$$

ができる．命題 1.7 により，ある自然数 n があって $Ra_n = Ra_{n+1}$ となる．よって a_{n+1} は Ra_n に属するから，$a_{n+1} = ua_n$ となる $u \in R$ が存在する．一方 $a_n = p_{n+1}a_{n+1}$ であったから，$a_n = p_{n+1}ua_n$ すなわち $up_{n+1} = 1$ となり，p_{n+1} は単元でなければならない．これ

は p_{n+1} が素元であることに反する．故に以上の操作は有限回で終了し a の素元分解が得られる．□

この定理により，有理整数環 $\mathbb{Z}$ と体 K 上の多項式環 $K[x]$ は一意分解整域である．a が $\mathbb{Z}$ の素元 (= 既約元) であるための必要十分条件は 素数 p があって $a = \pm p$ と表されることである．従って任意の自然数は素数の積として一通りに表わされる（素因数分解とその一意性）．たとえば $2015 = 5 \cdot 13 \cdot 31$.

$K[x]$ の素元 (= 既約元) は体 K によって異なる．たとえば $x^2 - 2$ は $\mathbb{Q}[x]$ においては既約であるが，$\mathbb{R}[x]$ においては $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ と分解できるので既約ではない．$\mathbb{C}[x]$ の素元の全体は 1 次式の全体である．すなわち $\mathbb{C}[x]$ において 1 次以上の任意の多項式は 1 次式の積に分解できる．これは代数学の基本定理と呼ばれる（「複素関数論 II」で証明する）．

1.9 環の直積と中国剰余定理*

環 $R_1, \ldots, R_n$ の**直積** (direct product) R は，集合としては直積集合

$$R = R_1 \times R_2 \times \cdots \times R_n$$

であり，$(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in R$ に対して

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n), \quad (a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

により定義される和と積により環となる．加法の単位元は $0_R = (0_{R_1}, \ldots, 0_{R_n})$，乗法の単位元は $1_R = (1_{R_1}, \ldots, 1_{R_n})$ である．

可換環 R の 2 つのイデアル I と J が $I + J = R$ を満たすとき**互いに素**であるという．特に R が単項イデアル整域で $I = Ra$, $J = Rb$ のときは，a と b の最大公約元が単元であること，すなわち a と b が互いに素であることと同値である．

定理 1.4 (中国剰余定理 (Chinese remainder theorem)) $I_1, \ldots, I_n$ は可換環 R のイデアルであり，どの 2 つも互いに素，すなわち $1 \leq i < j \leq n$ のとき $I_i + I_j = R$ とする．このとき環同型写像

$$f : R/\bigcap_{j=1}^{n} I_j \xrightarrow{\sim} R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

が存在する．

証明: n に関する帰納法で示そう．まず $n = 2$ のときに示す．R から R/I_j への自然な全射準同型を π_j とする．すなわち $\pi_j(a)$ は $a \in R$ の R/I_j における同値類である．$g : R \longrightarrow R/I_1 \times R/I_2$ を $g(a) = (\pi_1(a), \pi_2(a))$ で定義すると，g は環準同型である．$\operatorname{Ker} g = I_1 \cap I_2$ であることは定義から容易にわかる．g が全射であることを示そう．$I_1 + I_2 = R$ よりあ

る $a_j \in I_j$ $(j = 1, 2)$ があって，$a_1 + a_2 = 1$ が成立する．任意の $x_1, x_2 \in R$ に対して，$x = x_1a_2 + x_2a_1$ とおくと，$a_1 + a_2 = 1$ より

$$x - x_1 = x_1(a_2 - 1) + x_2a_1 = -x_1a_1 + x_2a_1 = (x_2 - x_1)a_1 \in I_1,$$
$$x - x_2 = x_1a_2 + x_2(a_1 - 1) = x_1a_2 - x_2a_2 = (x_1 - x_2)a_2 \in I_2$$

となるから，$\pi_1(x) = \pi_1(x_1)$, $\pi_2(x) = \pi_1(x_2)$，すなわち $g(x) = (\pi(x_1), \pi(x_2))$ が成立する．よって，g は全射である．従って環準同型定理によって環同型 $f : R/(I_1 \cap I_2) \longrightarrow R/I_1 \times R/I_2$ であって $a \in R$ の $R/(I_1 \cap I_2)$ における同値類を $(\pi_1(a), \pi_2(a))$ に写すものが存在する．

$n \geq 3$ のときは，まず

$$(I_1 \cap I_2) + I_j = R \qquad (3 \leq \forall j \leq n) \tag{3}$$

が成立することを示そう．$I_1 + I_j = R$, $I_2 + I_j = R$ より，$x_1 + x_j = 1$, $y_2 + y_j = 1$ をみたす $x_1 \in I_1$, $y_2 \in I_2$, $x_j, y_j \in I_j$ が存在する．このとき

$$1 = (x_1 + x_j)(y_2 + y_j) = x_1y_2 + (x_1y_j + x_jy_2 + y_jy_j)$$

であり，x_1y_2 は $I_1 \cap I_2$ に属し，$x_1y_j + x_jy_2 + y_jy_j$ は I_j に属すから，(3) が示された．よって帰納法の仮定により環同型

$$f' : R/(I_1 \cap I_2 \cap I_3 \cdots \cap I_n) \longrightarrow R/(I_1 \cap I_2) \times R/I_3 \times \cdots \times R/I_n$$

が存在する．一方，前半の議論より，環同型

$$f_2 : R/(I_1 \cap I_2) \longrightarrow R/I_1 \times R/I_2$$

が存在するから，この 2 つの環同型の合成により求める環同型を得る．□

1.10 整域の商体

整数から有理数を構成する方法を一般化して，整域から「分数」を用いて体を構成することができる．

R を整域として，直積集合 $R \times (R \setminus \{0\})$ における関係 $\sim$ を

$$(a, b) \sim (a', b') \quad \Leftrightarrow \quad ab' = a'b \qquad (a, a' \in R,\ b, b' \in R \setminus \{0\})$$

で定義する．この関係 $\sim$ は同値関係になる．実際，$(a, b) \sim (a, b)$ と $(a, b) \sim (a', b') \Leftrightarrow (a', b') \sim (a, b)$ は明らかである．$(a, b) \sim (a', b')$ かつ $(a', b') \sim (a'', b'')$ とすると，$ab' = a'b$, $a'b'' = a''b'$ であるから，

$$b'(ab'') = (b'a)b'' = (a'b)b'' = b(a'b'') = b(a''b') = b'(a''b)$$

より R が整域であることと $b' \neq 0$ に注意して $ab'' = a''b$ を得る．よって $\sim$ は同値関係である．この同値関係による $R \times (R \setminus \{0\})$ の商集合を K とする．(a, b) の K における同値

類を $\dfrac{a}{b}$ と表す．c を R の 0 でない元とすると，$a(bc)=(ac)b$ であるから，$(a,b)\sim(ac,bc)$ であり，$\dfrac{a}{b}=\dfrac{ac}{bc}$ が成立する．K における加法と乗法を

$$\frac{a}{b}+\frac{a'}{b'}=\frac{ab'+a'b}{bb'},\qquad \frac{a}{b}\frac{a'}{b'}=\frac{aa'}{bb'}$$

により定義する．この定義は代表元の選び方によらず well-defined であることが確かめられる．この演算により K は可換環となる．加法の単位元は $\dfrac{0}{1}$, 乗法の単位元は $\dfrac{1}{1}$ である．さらに，$a\neq 0$ のとき $\dfrac{a}{b}\dfrac{b}{a}=\dfrac{1}{1}$ であるから，K は体である．

R から K への写像 h を $h(a)=\dfrac{a}{1}$ により定義すると，h は環準同型である．

$$h(a)=0 \;\Leftrightarrow\; \frac{a}{1}=\frac{0}{1} \;\Leftrightarrow\; a=0$$

であるから，h は単射である．よって R を K の部分環とみなすことができる．特に a と $h(a)=\dfrac{a}{1}$ を同一視して $\dfrac{a}{1}=a$ と表す．K のことを R の**商体** (quotient field) という．

たとえば，有理整数環 $\mathbb{Z}$ の商体は有理数体 $\mathbb{Q}$ であり，体 K 上の多項式環 $K[x]$ の商体は K 係数の有理関数（分数式）の全体 $K(x)$ である．$K(x)$ は K 係数の**有理関数体**と呼ばれる．

1.11 素元分解整域と多項式環*

以下では R を素元（一意）分解整域 (UFD) とする．（R は一般には PID ではない.）R の零でも単元でもない任意の元 a に対して，単元倍しても相異なるような R の素元 $p_1,\dots p_r$ と自然数 $n_1,\dots,n_r$，および R の単元 u が存在して

$$a=up_1^{n_1}\cdots p_r^{n_r}$$

と表すことができる．（a の素元分解において単元倍すれば等しくなるような素元を 1 つにまとめればよい.）R の零とも単元とも異なる元 b の素元分解を

$$b=vq_1^{m_1}\cdots q_s^{m_s}$$

とする．ここで $q_1,\dots q_s$ は単元倍しても互いに異なるような R の素元，$m_1,\dots,m_s$ は自然数，v は単元である．順番を入れ替えれば，ある非負整数 $t\le\min\{r,s\}$ と単元 $u_1,\dots,u_t$ が存在して

$$q_i=u_ip_i\quad(1\le i\le t),\qquad i>t \text{ または } j>t \text{ ならば } p_i \text{ と } q_j \text{ は単元倍しても異なる}$$

と仮定できる．

補題 1.12 以上の条件の下で，$1 \le i \le t$ のとき $l_i = \min\{n_i, m_i\}$ とおけば，a と b の最大公約元 $\mathrm{GCD}(a,b)$ は $d := p_1^{l_1} \cdots p_t^{l_t}$ である．ただし $t = 0$ のときは $d = 1$ とする．

証明: d が a と b の約元であることは定義から明らか．e を a と b の約元として，

$$e = w r_1^{\nu_1} \cdots r_k^{\nu_k}$$

を素元分解とする．ここで $r_1, \ldots, r_k$ は単元倍しても互いに異なるような R の素元であり w は単元である．

$r_1^{\nu_1}$ は a と b の約元である．よってある $a' \in R$ があって $a = r_1^{\nu_1} a'$ と書ける．a' の素元分解に $r_1^{\nu_1}$ を掛けたものが a の素元分解になるから，素元分解の一意性により r_1 は $p_1, \ldots, p_s$ のいずれか p_i の単元倍であり $\nu_1 \le n_i$ となる．$r_1^{\nu_1}$ は b の約元でもあるから，r_i はある q_j の単元倍であり $\nu_j \le m_j$ でなければならない．すると q_j は p_i の単元倍であるから，$i = j \le t$ である．よって $\nu_1 \le l_i = \min\{m_i, n_i\}$ が従う．$r_2^{\nu_2}, \ldots, r_k^{\nu_k}$ についても同様の議論により，$r_1, \ldots, r_k$ を適当に入れ替えれば, $k \le t$ であり，ある単元 u' があって

$$e = w r_1^{\nu_1} \cdots r_k^{\nu_k} = u' p_1^{\nu_1} \cdots p_k^{\nu_k}, \qquad \nu_i \le l_i \quad (1 \le i \le k)$$

が成立することがわかる．従って e は d の約元である．以上により d は a と b の最大公約元であることが示された．□

３つ以上の元の最大公約元も素元分解を用いて上の補題と同様に与えられる．

注意: R が単項イデアル整域 (PID) でなければ，$d = \mathrm{GCD}(a,b)$ であるとき $Rd = Ra + Rb$ は一般には成立しない．(そもそも $Ra + Rb$ は一般には単項イデアルにならない．)

以下では，一意分解整域 R 上の多項式環 $R[x]$ を考察する．0 と異なる R 係数の多項式，すなわち $R[x]$ の元

$$f = f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad (a_0, a_1, \ldots, a_n \in R,\ a_n \ne 0) \tag{4}$$

に対して，$a_0, a_1, \ldots, a_n$ のうち 0 と異なる元の最大公約元を f の**内容** (content) といい，$\mathrm{cont}(f)$ で表す．$\mathrm{cont}(f)$ は単元倍を除いて f から一意的に定まる．たとえば $f = 6x^2 - 4x + 8 \in \mathbb{Z}[x]$ の内容は $\mathrm{cont}(f) = 2$ （または -2）である．内容 $\mathrm{cont}(f)$ が R の単元であるとき f を $R[x]$ の**原始多項式** (primitive polynomial) と呼ぶ．たとえば $3x^2 - 4$ は $\mathbb{Z}[x]$ の原始多項式である．

(4) の多項式 f の内容が $a = \mathrm{cont}(f)$ であるとき，$a_i = a a_i'$ をみたす $a_i' \in R$ が一意的に定まり，$f_0 := a_n' x^n + \cdots + a_1' x + a_0'$ は原始多項式であり $f = a f_0$ が成立する．逆に原始多項式 f_0 と $a \in R \setminus \{0\}$ に対して $f = a f_0$ の内容は a である．

補題 1.13 (Gauss の補題) R を一意分解整域として，f, g を $R[x]$ の零でない元とすると，$\mathrm{cont}(fg)$ は $\mathrm{cont}(f)\mathrm{cont}(g)$ の単元倍である．特に，f と g が原始多項式ならば fg も原始多項式である．

証明: $a = \mathrm{cont}(f)$, $b = \mathrm{cont}(g)$ とおけば原始多項式 $f_0, g_0 \in R[x]$ が存在して $f = a f_0$, $g = b g_0$ と表せる．このとき $f_0 g_0$ が原始多項式であれば，$fg = ab f_0 g_0$ より $\mathrm{cont}(fg) = ab$

となる．よって最初から f, g は原始多項式と仮定して，fg が原始多項式であることを示せばよい．

$$f = a_n x^n + \cdots + a_1 x + a_0 \quad (a_n \neq 0), \qquad g = b_m x^m + \cdots + b_1 x + b_0 \quad (b_m \neq 0)$$

とする．fg が原始多項式でないと仮定すると $d := \mathrm{cont}(fg)$ は単元でない．従って d はいくつかの R の素元の積で表される．その素元の 1 つを p とする．f と g は原始多項式だから，f と g 各々の係数で p の倍元ではないものが存在する．すなわち，非負整数 k と l が存在して，

$$p \not| a_k \text{ かつ } (j > k \Rightarrow p | a_j), \qquad p \not| b_l \text{ かつ } (j > l \Rightarrow p | b_j),$$

が成立する．このとき fg の x^{k+l} の係数 c_{k+l} は

$$c_{k+l} = a_k b_l + a_{k+1} b_{l-1} + a_{k+2} b_{l-2} + \cdots + a_{k-1} b_{l+1} + a_{k-2} b_{l+2} + \cdots$$

となり，右辺の第 1 項以外はすべて p の倍元である．一方 a_k も b_l も p の倍元ではなく，p は素元だから $a_k b_l$ は p の倍元ではない．よって c_{k+l} は p の倍元ではない．一方 p は $d = \mathrm{cont}(fg)$ の約元であるから c_{k+l} の約元でもある．これは矛盾であるから fg は原始多項式である．□

一般に R を整域として K をその商体とすると，R は K の部分環であるから，多項式環 $R[x]$ を多項式環 $K[x]$ の部分環とみなすことができる．

補題 1.14 零でない多項式 $f \in K[x]$ に対してある $c \in K$ と原始多項式 $f_0 \in R[x]$ が存在して $f = cf_0$ と表される．

証明: K は R の商体であるから，定義によりある $a_i, b_i \in R$ $(b_i \neq 0)$ が存在して

$$f = \frac{a_n}{b_n} x^n + \cdots + \frac{a_1}{b_1} x + \frac{a_0}{b_0}$$

と表される．$g := b_0 b_1 \cdots b_n f$ は $R[x]$ に属するから，原始多項式 $g_0 \in R[x]$ と R の元 a があって $g = a g_0$ と表される．従って $K[x]$ において

$$f = \frac{a}{b_0 b_1 \cdots b_n} g_0$$

が成立する．□

命題 1.14 R を素元分解整域として K を R の商体とする．$f \in R[x]$ を原始多項式とする．$g \in R[x]$ が $K[x]$ において f の倍元であれば g は $R[x]$ においても f の倍元である．

証明: g が $K[x]$ において f の倍元であれば，$g = hf$ を満たす $h \in K[x]$ が存在する．原始多項式 $h_0 \in R[x]$ と $a, b \in R$ $(b \neq 0)$ が存在して $h = (a/b) h_0$ と表せる．このとき $R[x]$ において $bg = a h_0 f$ が成立する．両辺の内容を比較して $b\,\mathrm{cont}(g) = a$ を得る．特に a は b の倍元であるから $c := a/b$ は R に属する．従って $h = c h_0$ は $R[x]$ に属するから g は $R[x]$ においても f の倍元である．□

例 1.28 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ $(a_i \in \mathbb{Z},\ n \in \mathbb{N},\ a_n \neq 0,\ a_0 \neq 0)$ を $\mathbb{Z}[x]$ の原始多項式とする．もし有理数 r が $f(r) = 0$ を満たせば，$r = a/b$ かつ $a|a_0,\ b|a_n$ を満たす整数 a, b が存在する．実際，互いに素な整数 a, b によって $r = a/b$ と表すと，$b(x - r) = bx - a$ は $\mathbb{Q}[x]$ において $f(x)$ の約元であり，$\mathbb{Z}[x]$ における原始多項式でもあるから，上の命題によって $bx - a$ は $\mathbb{Z}[x]$ において $f(x)$ の約元である．従ってある $n-1$ 次多項式 $q(x) \in \mathbb{Z}[x]$ が存在して $f(x) = (bx - a)q(x)$ と表せる．両辺の x^n の係数と定数項を比較して結論を得る．

命題 1.15 R を素元分解整域として K を R の商体とする．$f \in R[x]$ が次数 1 以上の原始多項式ならば，f が $R[x]$ の既約元であることと f が $K[x]$ の元として既約元であることとは同値である．

証明: f が $K[x]$ の元として既約であると仮定する．f は 1 次以上の K 係数多項式の積で表すことはできない．従って，もし f が $R[x]$ の既約元でなければ，単元ではない R の元 a と $R[x]$ の元 g が存在して $f = ag$ と表される．よって $\mathrm{cont}(f) = a\,\mathrm{cont}(g)$ は a の倍元である．これは $\mathrm{cont}(f)$ が単元であることに反する．よって f は $R[x]$ の既約元である．

逆に，f が $K[x]$ の既約元ではないと仮定すると，次数が 1 以上の K 係数多項式 $g, h \in K[x]$ が存在して $f = gh$ と表される．原始多項式 $g_0, h_0 \in R[x]$ と K の元 c, d が存在して $g = cg_0,\ h = dh_0$ と表せる．R の元 c_1, c_2, d_1, d_2 が存在して $c = c_1/c_2,\ d = d_1/d_2$ と表されるから

$$f = \frac{c_1 d_1}{c_2 d_2} g_0 h_0 \quad \text{すなわち} \quad c_2 d_2 f = c_1 d_1 g_0 h_0 \in R[x]$$

となる．よって Gauss の補題により $c_2 d_2 \mathrm{cont}(f) = c_1 d_1 \mathrm{cont}(g_0)\mathrm{cont}(h_0)$ であり，$\mathrm{cont}(f)$, $\mathrm{cont}(g_0)$, $\mathrm{cont}(h_0)$ はすべて R の単元であるから，R の単元 u が存在して $c_1 d_1 = u c_2 d_2$ となる．これから $c_2 d_2 f = u c_2 d_2 g_0 h_0$ すなわち $f = u g_0 h_0$ を得る．よって f は $R[x]$ の既約元ではない．□

命題 1.16 $R[x]$ の既約元は $R[x]$ の素元である．

証明: f を $R[x]$ の既約元とする．f が定数多項式 $f = c$ $(c \in R \setminus \{0\})$ ならば，c は R の既約元であるから R の素元である．従って $R[x]$ の素元でもある．

$a = \mathrm{cont}(f)$ とすると $f = af_0$ をみたす原始多項式 $f_0 \in R[x]$ が存在するから a は単元でなければならない．よって f は原始多項式である．f は $K[x]$ の元としても既約であり $K[x]$ は PID だから，f は $K[x]$ の素元である．f が $R[x]$ の素元であることを示そう．$g, h \in R[x]$ かつ gh が f の倍元であると仮定する．f は $K[x]$ の素元だから g または h は $K[x]$ において f の倍元である．f は原始多項式だから命題 1.14 によって g または h は $R[x]$ において f の倍元である．故に f は $R[x]$ の素元である．□

定理 1.5 R が素元分解整域ならば，多項式環 $R[x]$ も素元分解整域である．

証明: $f(x) \in R[x]$ の内容を c とすると原始多項式 $f_0(x) \in R[x]$ が存在して $f(x) = cf_0(x)$ と表される．$K[x]$ は素元分解整域であるから，$K[x]$ の既約元 $g_1(x), \ldots, g_r(x)$ が存在して $f_0(x) = g_1(x) \cdots g_r(x)$ と表される．□

例 1.29 整数係数の多項式環 $\mathbb{Z}[x]$ は素元分解整域である．

1.12 多変数多項式環*

n を自然数として，$x_1, \ldots, x_n$ を n 個の不定元（変数または文字）とする．R を可換環とするとき，ある非負整数 $N_1, \ldots, N_n$ によって

$$f = f(x_1, \ldots, x_n) = \sum_{\alpha_1=0}^{N_1} \cdots \sum_{\alpha_n=0}^{N_n} c_{\alpha_1 \cdots \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \qquad (c_{\alpha_1 \cdots \alpha_n} \in R) \tag{5}$$

と表される「式」のことを不定元 $x_1, \ldots, x_n$ についての R 係数多項式という．R 係数多項式の全体を $R[x_1, \ldots, x_n]$ と表す．(5) を書き直すと

$$f(x_1, \ldots, x_{n-1}, x_n) = \sum_{\alpha_n=0}^{N_n} g_{\alpha_n}(x_1, \ldots, x_{n-1}) x_n^{\alpha_n},$$

$$g_{\alpha_n}(x_1, \ldots, x_{n-1}) := \sum_{\alpha_1=0}^{N_1} \cdots \sum_{\alpha_{n-1}=0}^{N_{n-1}} c_{\alpha_1 \cdots \alpha_n} x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} \in R[x_1, \ldots, x_{n-1}]$$

と表されるから，f は不定元 x_n についての $R[x_1, \ldots, x_{n^1}]$ 係数多項式とみなすことができる．この対応によって集合として

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

とみなすことができる．$R[x_1]$ は環であるから，$R[x_1, x_2] = R[x_1][x_2]$ も環となる．以下同様にして（n についての帰納法により）$R[x_1, \ldots, x_n]$ は環であることがわかる．これを R 係数の n 変数多項式環という．

例 1.30 たとえば $f = x^4 + 4x^3y - 2y^2 + 3xy + 5x$ は不定元 x, y についての $\mathbb{Z}$ 係数多項式である．y について整理すれば $f = -2y^2 + (4x^3 + 3x)y + (x^4 + 5x) \in \mathbb{Z}[x][y]$ とみなせる．また，x について整理すれば $f = x^4 + 4yx^3 + (3y + 5)x - 2y^2 \in \mathbb{Z}[y][x]$ とみなせる．

補題 1.15 R が整域ならば $R[x_1, \ldots, x_n]$ も整域である．

証明: n についての帰納法で示す．$n = 1$ のときは補題 1.6 により $R[x_1]$ は整域である．$R[x_1, \ldots, x_{n-1}]$ が整域であると仮定すると，補題 1.6 により $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ も整域である．□

定理 1.6 R が一意分解整域 (UFD) ならば $R[x_1, \ldots, x_n]$ も一意分解整域である．

証明: 定理 1.5 と n に関する帰納法を用いればよい．□

2 加群

環の上の加群とは，ベクトル空間の概念の一般化であり，代数学だけでなく，解析学や幾何学でも重要な概念である．ここでは特に単項イデアル整域（またはユークリッド整域）上の有限生成加群の構造を調べ，応用としてアーベル群の基本定理と正方行列の Jordan 標準形を導く．

2.1 加群の定義と例

M が**アーベル群** (abelian group, 加法群，可換群）であるとは，加法と呼ばれる演算 $M \times M \ni (u, v) \longmapsto u + v \in M$ が定義され，次の (1)–(4) を満たすことである．

(1) 任意の $u, v, w \in M$ に対して $(u + v) + w = u + (v + w)$ が成立する．（加法の結合法則）

(2) 任意の $u, v \in M$ に対して $u + v = v + u$ が成立する．（加法の交換法則）

(3) M の元 0_M が存在して，任意の $u \in M$ に対して $u + 0_M = u$ が成立する．（0_M を加法についての単位元といい，通常は単に 0 で表す．）

(4) M の任意の元 u に対してある $v \in M$ が存在して $u + v = 0_M$ が成立する．このとき $v = -u$ と表し u の加法についての逆元という．

$u, v \in M$ に対して $u - v = u + (-v)$ と定義する．

補題 2.1 M をアーベル群とすると，加法についての単位元 0_M はただ 1 つである．また，$u \in M$ の加法についての逆元はただ 1 つである．

証明: $0'_M$ を M の加法についての別の単位元とすると，$0'_M = 0'_M + 0_M = 0_M$. また $u, v, w \in M$ が $u + v = u + w = 0_M$ を満たせば，

$$v = 0_M + v = (u + w) + v = (w + u) + v = w + (u + v) = w + 0_M = w$$

□

アーベル群 M が可換環 R 上の**加群**または R **加群** (R-module) であるとは，R の M への作用

$$R \times M \ni (a, u) \longmapsto au \in M$$

が定義されていて次の (5)–(8) を満たすことである．

(5) $1_R u = u \quad (\forall u \in M)$

(6) $(ab)u = a(bu) \quad (\forall a, b \in R,\ \forall u \in M)$

(7) $(a + b)u = au + bu \quad (\forall a, b \in R,\ \forall u \in M)$

(8) $a(u + v) = au + av \quad (\forall a \in R,\ \forall u, v \in M)$

特に，加法の単位元 0 のみからなる加群 $\{0\}$ は R 加群である．これを 0 加群といい，単に 0 と表すこともある．

補題 2.2 環 R 上の加群 M の任意の元 u に対して $0_R u = 0_M$, $(-1_R)u = -u$ が成立する．

証明: 性質 (7) より $0_R u = (0_R + 0_R)u = 0_R u + 0_R u$. よって

$$0_M = 0_R u + (-(0_R u)) = (0_R u + 0_R u) + (-(0_R u)) = 0_R u + (0_R u + (-(0_R u))) = 0_R u + 0_M = 0_R u.$$

これで $0_R u = 0_M$ が示された.

$$0_M = 0_R u = (1_R + (-1_R))u = 1_R u + (-1_R)u = u + (-1_R)u$$

より $(-1_R)u$ は u の加法に関する逆元，すなわち $(-1_R)u = -u$ である．□

例 2.1 有理整数環 $\mathbb{Z}$ 上の加群とはアーベル（可換）群のことである．実際，M をアーベル群として，$u \in M$ に対する整数 n の作用を

$$nu = \begin{cases} \underbrace{u + \cdots + u}_{n} & (n > 0) \\ 0 & (n = 0) \\ -(\underbrace{u + \cdots + u}_{-n}) & (n < 0) \end{cases}$$

で定義すると，M が $\mathbb{Z}$ 加群となることが容易にわかる．逆に M が $\mathbb{Z}$ 加群ならば，加群の定義によって M はアーベル群である.

例 2.2 体 K 上の加群とは，K 上のベクトル空間のことである.

例 2.3 R を可換環とすると，環の積 $R \times R \ni (a, b) \mapsto ab \in R$ を R の R への作用とみなすことにより R は R 加群となる．すなわち $u \in R$ を加群の元, $a \in R$ を環の元とみなして au を加群の元とみなしている.

R を可換環，M を R 加群とする，M の空でない部分集合 N が M の**部分 R 加群** (R-submodule) であるとは,

$$u, v \in N \;\Rightarrow\; u \pm v \in N, \qquad (u \in N, a \in R) \;\Rightarrow\; au \in N$$

が成立することである．N の元 u をとると，$u + (-u) = 0_M$ も N に属するから，部分加群 N は 0_M を含む.

K が体のときは N が M の部分空間であることと同値である．環 R を R 加群とみなしたとき，R の部分 R 加群とは，R のイデアルのことである.

N_1 と N_2 を M の部分 R 加群とすると，$N_1 + N_2 := \{u_1 + u_2 \mid u_1 \in N_1, u_2 \in N_2\}$ と $N_1 \cap N_2$ は M の部分 R 加群である.

例 2.4 V を体 K 上の有限次元ベクトル空間とし，$T : V \longrightarrow V$ を線形写像とする．K 係数の多項式

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \qquad (a_0, \ldots, a_n \in K)$$

に対して, $P(x)$ の $\mathbf{v} \in V$ への作用を

$$P(x)\mathbf{v} = P(T)\mathbf{v} = a_n T^n \mathbf{v} + a_{n-1} T^{n-1} \mathbf{v} + \cdots + a_1 T\mathbf{v} + a_0 \mathbf{v}$$

で定義する．この作用によって V は $K[x]$ 加群になる．V の部分集合 W が V の部分 $K[x]$ 加群であるための必要十分条件は，W が V の部分ベクトル空間であって，かつ任意の $\mathbf{v} \in W$ に対して $T\mathbf{v} \in W$ が成立することである．このとき W を T **不変部分空間**ともいう．

M と N を環 R 上の加群とする．写像 $f : M \to N$ が R **準同型** (R-homomorphism) または R **線形** (R-linear) であるとは，

$$f(u+v) = f(u) + f(v), \qquad f(au) = af(u) \qquad (\forall u, v \in M,\ \forall a \in R)$$

が成立することである．特に M のすべての元を N の単位元 0_N にうつす写像は R 準同型である．これを零写像と呼ぶ．

$f : M \to N$ が R 準同型であるとき，f の**核** (kernel) $\operatorname{Ker} f := \{u \in M \mid f(u) = 0_N\}$ は M の R 部分加群である．また f の**像** (image) $\operatorname{Im} f = f(M)$ は N の R 部分加群である．

R 準同型 $f : M \longrightarrow N$ が全単射であるとき，f は R **同型** (R-isomorphism) であるといい，f が同型写像であることを明記したい場合は $f : M \xrightarrow{\sim} N$ と表すことにする．また M と N は R 加群として同型であるともいい，単に $M \cong N$ と表すこともある．このとき，f^{-1} は N から M への R 同型である．

補題 2.3 f を可換環 R 上の加群 M から N への R 準同型とすると，$f(0_M) = 0_N$ および，任意の $u \in M$ について $f(-u) = -f(u)$ が成立する．

証明: $f(0_M) = f(0_M + 0_M) = f(0_M) + f(0_M)$ の両辺に $-f(0_M)$ を加えて $f(0_M) = 0_N$ を得る．$f(u) + f(-u) = f(u-u) = f(0_M) = 0_N$ より $f(-u) = -f(u)$ を得る．□

補題 2.4 M と N をアーベル群，$f : M \to N$ を写像とする．このとき f が群準同型，すなわち $f(u+v) = f(u) + f(v)$ が任意の $u, v \in M$ について成り立つことと，f が M と N を $\mathbb{Z}$ 加群とみなしたとき $\mathbb{Z}$ 準同型であることは同値である．

証明: $\mathbb{Z}$ 準同型ならば群準同型であることは明らかだから，f が群準同型であると仮定する．このとき，任意の $n \in \mathbb{Z}$ と $u \in M$ について $f(nu) = nf(u)$ が成立することを示せばよい．$n = 0$ のときは両辺が 0 になるので成立する．$n > 0$ のときは n 倍の定義により

$$f(nu) = f(\underbrace{u + \cdots + u}_{n}) = \underbrace{f(u) + \cdots + f(u)}_{n} = nf(u)$$

$n < 0$ のときは

$$f(nu) = f(\underbrace{-(u + \cdots + u)}_{-n}) = -f(\underbrace{u + \cdots + u}_{-n}) = -(\underbrace{f(u) + \cdots + f(u)}_{-n}) = nf(u)$$

□

例 2.5 M を R 加群とすると，任意の $a \in R$ に対して写像 $M \ni u \mapsto au \in M$ は M から M への R 準同型である．

2.2 自由加群と有限生成加群

以下では R を可換環とする．一般に，$M_1, M_2, \ldots, M_n$ を R 上の加群とするとき，それらの**直和** (direct sum)

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$$

を次のように定義する．まず集合としては M は $M_1, \ldots, M_n$ の直積集合，すなわち

$$M = M_1 \times M_2 \times \cdots \times M_n = \{(u_1, u_2, \ldots, u_n) \mid u_1 \in M_1,\ u_2 \in M_2, \ldots, u_n \in M_n\}$$

である．$(u_1, u_2, \ldots, u_n), (v_1, v_2, \ldots, v_n) \in M$ の和を

$$(u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$$

で定義し，$a \in R$ の作用を

$$a(u_1, u_2, \ldots, u_n) = (au_1, au_2, \ldots, au_n)$$

で定義すると，M は R 加群となる．このとき，各々の M_i のことを M の**直和因子** (direct summand) という．このとき M から M_i への自然な全射準同型 $\pi_i : M \ni (u_1, \ldots, u_n) \mapsto u_i \in M_i$ $(i = 1, \ldots, n)$ が定まる．

特に，R を R 加群と見て，$M_i = R$ $(i = 1, \ldots, n)$ の直和を

$$\underbrace{R \oplus \cdots \oplus R}_{n} = R^n$$

と表す．R が体のときは R^n は n 次元の数ベクトル空間のことである．

R 加群 M の元 $u_1, \ldots, u_r$ が与えられたとき，

$$N = Ru_1 + Ru_2 + \cdots + Ru_r := \{a_1u_1 + a_2u_2 + \cdots + a_ru_r \mid a_1, a_2, \ldots, a_r \in R\}$$

は M の R 部分加群であることは容易にわかる．これを $u_1, u_2, \ldots, u_r$ の**生成する** R 部分加群，$\{u_1, u_2, \ldots, u_r\}$ を N の**生成系** (set of generators) という．または，$u_1, \ldots, u_r$ が N を（R 加群として）**生成する**ともいう．

定義 2.1 M を可換環 R 上の加群とする．M の有限個の元 $u_1, \ldots, u_r$ が存在して，M が $u_1, \ldots, u_r$ で生成される R 加群であるとき，M は R 上**有限生成** (finitely generated over R) であるという．

R 加群 M の有限個の元 $u_1, \ldots, u_r$ が R 上 **1 次独立** (linearly independent) であるとは，$a_1, \ldots, a_r \in R$ かつ $a_1u_1 + a_2u_2 + \cdots + a_ru_r = 0$ ならば，$a_1 = a_2 = \cdots = a_r = 0$ となることである．1 次独立でないとき，1 次従属という．

定義 2.2 可換環 R 上の加群 M の有限個の元 $u_1, \ldots, u_r$ が M の**基底** (basis) であるとは，M が $u_1, \ldots, u_r$ の生成する R 加群であり，かつ $u_1, \ldots, u_r$ が R 上 1 次独立であることである．M が有限個（r 個）の元からなる基底を持つとき，M を**有限階数**（または階数 r の）**自由加群** (free modole of finite rank) という．（R が体のときは，有限次元ベクトル空間という．）

特に R^n は $(1,0,\ldots,0),\ \ldots,\ (0,\ldots,0,1) \in R^n$ を基底（標準基底と呼ばれる）とする階数 n の自由加群である．

一般に R 加群は有限生成であっても基底を持つとは限らない．整域 R 上の加群が有限個の元からなる基底を持てば，その個数は一定であること，すなわち R 自由加群の階数は基底の選び方によらないことは，次節で証明する．

例 2.6 n を 2 以上の自然数とするとき $\mathbb{Z}$ 加群 $M := \mathbb{Z}/\mathbb{Z}n$ は $\overline{1}$ で生成されるが $n\overline{1} = \overline{n} = \overline{0}$ であるから，$\overline{1}$ は 1 次独立ではない．M は自由加群ではない．実際，M の任意の元は n 倍すると 0 になるから M のどの元も 1 次独立でない．

例 2.7 $N = \{(u,v) \in \mathbb{Z}^2 \mid u+v=0\}$ とおくと，N は $\mathbb{Z}^2$ の部分加群である．N の基底として $(1,-1)$ がとれる．実際 $(u,v) \in N$ とすると $v=-u$ であり $(u,v) = u(1,-1)$ と一意的に表される．従って N は階数 1 の自由加群である．

以下では，線形代数での習慣に従って，自由加群 R^n の元を横ではなく縦に並べて

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = {}^t(a_1, a_2, \ldots, a_n) \ \in R^n \qquad\qquad (a_1,\ldots,a_n \in R)$$

と表すことにする．（スペースの節約のため横ベクトルの前に転置行列の記号 ^{t} を付けて縦ベクトルにする．）

さて，R 加群 M が基底 $u_1,\ldots,u_m$ を持つとする．このとき，R 加群 R^m から M への R 同型 $\Phi_M : R^m \longrightarrow M$ を

$$\Phi_M({}^t(x_1,x_2,\ldots,x_m)) = x_1u_1 + x_2u_2 + \cdots + x_mu_m \qquad (x_1,\ldots,x_m \in R)$$

により定義する．実際，Φ_M が R 準同型であることは容易にわかる．さらに，Φ_M が全単射であることと $u_1,\ldots,u_m$ が基底であることは同値である．（なお，$\Phi_M : R^m \to M$ は R 同型であるから，逆写像 $\Psi_M : M \to R^m$ も R 同型である．線形代数では Φ_M でなく Ψ_M を用いることが多いが，Φ_M の方が定義が簡明である．）

M を基底 $u_1,\ldots,u_m$ を持つ R 自由加群，N を基底 $v_1,\ldots,v_n$ を持つ R 自由加群として，$f : M \longrightarrow N$ を R 準同型とする．このとき，

$$f(u_i) = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{ni}v_n = \sum_{j=1}^{n} a_{ji}v_j \qquad (1 \le i \le m)$$

を満たす $a_{ij} \in R$ がただ一通り存在する．a_{ij} を第 (i,j) 成分とする $n \times m$ 行列 A のことを，写像 f の基底 $u_1,\ldots,u_m$ と $v_1,\ldots,v_n$ に関する**行列表示**または**表現行列**という．（$N = M$ のときは通常は M と N で同じ基底を用いる．）$x_1,\ldots,x_m,y_1,\ldots,y_n \in R$ に対して，

$$f(x_1u_1 + \cdots + x_mu_m) = \sum_{i=1}^{m} x_i f(u_i) = \sum_{i=1}^{m} x_i \sum_{j=1}^{n} a_{ji}v_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ji}x_i \right) v_j$$

であるから，

$$f(x_1u_1+\cdots+x_mu_m)=y_1v_1+\cdots+y_nv_n \quad\Longleftrightarrow\quad \begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}=A\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix} \tag{6}$$

となる．逆に R の元を成分とする $n\times m$ 行列 $A=(a_{ij})$ を与えれば，(6) によって R 準同型 $f:M\to N$ が定まる．

R 同型 $\Phi_N:R^n\to N$ を

$$\Phi_N({}^t(y_1,\ldots,y_n))=y_1v_1+\cdots+y_nv_n \qquad (y_1,\ldots,y_n\in R)$$

により定義する．このとき (6) より，任意の R^m の元 $\mathbf{v}$ に対して $f(\Phi_M(\mathbf{v}))=\Phi_N(A\mathbf{v})$ が成立する．すなわち，R 準同型の図式

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\Phi_M}\uparrow & & \uparrow{\scriptstyle\Phi_N} \\ R^m & \xrightarrow{A} & R^n \end{array}$$

は**可換図式** (commutative diagram)（矢印の 2 通りのたどり方による写像の合成が一致すること）である．

さらに，L を基底 $w_1,\ldots,w_l$ を持つ R 自由加群として，$g:N\longrightarrow L$ を R 準同型とする．このとき，

$$g(v_i)=b_{1i}w_1+\cdots+b_{li}w_l=\sum_{j=1}^{l}b_{ji}w_j \qquad (1\le i\le n)$$

により $b_{ij}\in R$ を定め，$l\times n$ 行列 $B=(b_{ij})$ を作る．このとき R 準同型 $g\circ f:M\longrightarrow L$ の M の基底 $u_1,\ldots,u_m$ と L の基底 $w_1,\ldots,w_l$ に関する行列表示は BA である．実際

$$\begin{aligned}(g\circ f)(u_i)=g(f(u_i))&=g(a_{1i}v_1+\cdots+a_{ni}v_n)=\sum_{k=1}^{n}a_{ki}g(v_k)\\ &=\sum_{k=1}^{n}a_{ki}\sum_{j=1}^{l}b_{jk}w_j=\sum_{j=1}^{l}\left(\sum_{k=1}^{n}b_{jk}a_{ki}\right)w_j \qquad (i=1,\ldots,m)\end{aligned}$$

が成立する．これは次の図式が可換であることからも従う．

$$\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & L \\ {\scriptstyle\Phi_M}\uparrow & & \uparrow{\scriptstyle\Phi_N} & & \uparrow{\scriptstyle\Phi_L} \\ R^m & \xrightarrow{A} & R^n & \xrightarrow{B} & R^l \end{array}$$

例 2.8 整数係数の 2 次以下の多項式の全体 $M=\{a_2x^2+a_1x+a_0\mid a_0,a_1,a_2\in\mathbb{Z}\}$ を考える．M はアーベル群，従って $\mathbb{Z}$ 加群であり，基底として $1,x,x^2$ をとれる．写像 $T:M\to M$

を $T(f(x)) = f(x+1)$ $(\forall f(x) \in \mathbb{Z}[x])$ によって定義すると，T は $\mathbb{Z}$ 準同型であることが容易にわかる．

$$T(1) = 1, \quad T(x) = x+1, \quad T(x^2) = (x+1)^2 = x^2 + 2x + 1$$

であるから，T の基底 $1, x, x^2$ に関する行列表示は $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ である．

2.3 可換環の元を成分とする行列と行列式

R を可換環とする．n を自然数として，R の元を成分とする n 次正方行列の全体を $M_n(R)$ で表そう．$M_n(R)$ は $n \geq 2$ のとき一般に非可換環である．$a \in R$ に対して aI_n のことを**スカラー行列**という．スカラー行列は任意の $A \in M_n(R)$ と可換，すなわち $(aI_n)A = A(aI_n)$ が成立する．この行列を単に aA と表す．この作用により $M_n(R)$ は R 加群ともみなせる．

$M_n(R)$ の元 $A = (a_{ij})$ に対して，その**行列式** (determinant) $\det A$ とは，線形代数で学んだ R が体（たとえば実数体や複素数体）の場合と同様に

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \, a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

で定義される R の元のことである．ここで S_n は集合 $\{1, 2, \ldots, n\}$ の置換の全体，$\operatorname{sgn}\sigma$ は置換 σ の符号（偶置換ならば 1，奇置換ならば -1) を表す．行列式については，R が体の場合の性質がほとんどそのまま成立する．

命題 2.1 $A, B \in M_n(R)$ に対して $\det {}^tA = \det A$ が成立する．

証明: $\sigma \in S_n$ の逆置換（逆写像）を σ^{-1} とすると，

$$\det {}^tA = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \, a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \, a_{1\sigma^{-1}(1)} a_{2\sigma^{-1}(2)} \cdots a_{n\sigma^{-1}(n)}$$

であり，σ が S_n 全体を動くとき σ^{-1} も S_n の全体を動き，$\operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\sigma$ であるから，これは $\det A$ に等しい．□

命題 2.2 行列式は各行および各列について R 線形である．すなわち，$\mathbf{a}_1, \ldots, \mathbf{a}_n$, $\mathbf{b}_j$ を R の元を成分とする n 次元横ベクトル，$\lambda, \mu \in R$，$1 \leq j \leq n$ とするとき，

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \lambda\mathbf{a}_j + \mu\mathbf{b}_j \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \lambda \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_j \\ \vdots \\ \mathbf{a}_n \end{pmatrix} + \mu \det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{b}_j \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

が成立する．列についても同様である．

証明: $\mathbf{a}_i$ の第 j 成分を a_{ij}, $\mathbf{b}_j$ の第 k 成分を b_{jk} とすると，

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \lambda\mathbf{a}_j + \mu\mathbf{b}_j \\ \vdots \\ \mathbf{a}_n \end{pmatrix} = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma\, a_{1\sigma(1)}\cdots(\lambda a_{j\sigma(j)} + \mu b_{j\sigma(j)})\cdots a_{n\sigma(n)}$$
$$= \lambda \sum_{\sigma\in S_n} \operatorname{sgn}\sigma\, a_{1\sigma(1)}\cdots a_{j\sigma(j)}\cdots a_{n\sigma(n)} + \mu \sum_{\sigma\in S_n} \operatorname{sgn}\sigma\, a_{1\sigma(1)}\cdots b_{j\sigma(j)}\cdots a_{n\sigma(n)}$$

より行ベクトルについては成立する．転置行列をとれば，列ベクトルについても成立することがわかる．□

命題 2.3 $A \in M_n(R)$ の行列式は行と列について交代的である．すなわち A の 2 つの行，あるいは 2 つの列を入れ替えた行列を B とすると，$\det B = -\det A$ が成立する．特に A の 2 つの行（または 2 つの列）が同一ならば，$\det A = 0$ である．

証明: $A = (a_{ij})$ の第 i 行と第 j 行 $(1 \le i < j \le n)$ を入れ替えた行列を B とすると

$$\begin{aligned} \det B &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma\, a_{1\sigma(1)}\cdots a_{j\sigma(i)}\cdots a_{i\sigma(j)}\cdots a_{n\sigma(n)} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma\, a_{1\sigma(1)}\cdots a_{i\sigma(j)}\cdots a_{i\sigma(i)}\cdots a_{n\sigma(n)} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}\sigma\, a_{1\tau(1)}\cdots a_{i\tau(i)}\cdots a_{i\tau(j)}\cdots a_{n\tau(n)} \end{aligned}$$

ここで，$\tau = \sigma\cdot(i,j)$ である．このとき，$\operatorname{sgn}\tau = -\operatorname{sgn}\sigma$ であり，σ が S_n 全体を動くとき τ も S_n 全体を動くから，この最後の式は $-\det A$ に等しい．A の第 i 行と第 j 行が等しいときは $B = A$ であるから，$\det A = -\det B = -\det A$ より $\det A = 0$ となる．□

命題 2.4 R^n の n 個の元を変数とする写像 $F : (R^n)^n \longrightarrow R$ が R 多重線形かつ交代的，すなわち

$$F(\mathbf{a}_1,\ldots,\lambda\mathbf{a}_j+\mu\mathbf{b}_j,\ldots,\mathbf{a}_n) = \lambda F(\mathbf{a}_1,\ldots,\mathbf{a}_j,\ldots,\mathbf{a}_n) + \mu F(\mathbf{a}_1,\ldots,\mathbf{b}_j,\ldots,\mathbf{a}_n)$$
$$F(\mathbf{a}_1,\ldots,\mathbf{a}_j,\ldots,\mathbf{a}_i,\ldots,\mathbf{a}_n) = -F(\mathbf{a}_1,\ldots,\mathbf{a}_i,\ldots,\mathbf{a}_j,\ldots,\mathbf{a}_n)$$

が任意の $1 \le i < j \le n$，任意の $\mathbf{a}_1,\ldots,\mathbf{a}_n,\mathbf{b}_j \in R^n$ と任意の $\lambda,\mu \in R$ について成立すれば，

$$F(\mathbf{a}_1,\ldots,\mathbf{a}_n) = F(\mathbf{e}_1,\ldots,\mathbf{e}_n)\det \begin{pmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_j \\ \vdots \\ \mathbf{a}_n \end{pmatrix}$$

となる．ここで $\mathbf{e}_1 = (1,0,\ldots,0),\ldots,\mathbf{e}_n = (0,\ldots,0,1) \in R^n$ は R^n の標準基底である．

証明: $\mathbf{a}_i$ の第 j 成分を a_{ij} とすると，F の多重線形性から

$$\begin{aligned} F(\mathbf{a}_1,\dots,\mathbf{a}_2) &= F(a_{11}\mathbf{e}_1+\cdots+a_{1n}\mathbf{e}_n,\mathbf{a}_2,\dots,\mathbf{a}_n) \\ &= \sum_{k_1=1}^{n} a_{1,k_1}F(\mathbf{e}_{k_1},\mathbf{a}_2,\dots,\mathbf{a}_n) = \sum_{k_1=1}^{n} a_{1,k_1}\sum_{k_2=1}^{n} a_{2,k_2}F(\mathbf{e}_{k_1},\mathbf{e}_{k_2},\mathbf{a}_3,\dots,\mathbf{a}_n) \\ &= \cdots \\ &= \sum_{k_1=1}^{n}\cdots\sum_{k_n=1}^{n} a_{1,k_1}\cdots a_{n,k_n}F(\mathbf{e}_{k_1},\dots,\mathbf{e}_{k_n}) \end{aligned}$$

ここで F の交代性を用いると，$k_1,\dots,k_n$ に重複がある（同じ数字が現れる）ときは $F(\mathbf{e}_{k_1},\dots,\mathbf{e}_{k_n})=0$ となり，$k_1,\dots,k_n$ が相異なるときは，

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

とすれば，$F(\mathbf{e}_{k_1},\dots,\mathbf{e}_{k_n}) = \operatorname{sgn}\sigma\, F(\mathbf{e}_1,\dots,\mathbf{e}_n)$ となることがわかる．よって

$$F(\mathbf{a}_1,\mathbf{a}_2,\dots,\mathbf{a}_n) = \sum_{\sigma\in S_n}\operatorname{sgn}\sigma\, a_{1\sigma(1)}\cdots a_{n\sigma(n)}F(\mathbf{e}_1,\mathbf{e}_2,\dots,\mathbf{e}_n) = F(\mathbf{e}_1,\mathbf{e}_2,\dots,\mathbf{e}_n)\det A$$

を得る．□

命題 2.5 任意の $A,B\in M_n(R)$ に対して $\det(AB)=\det A\det B$ が成立する．

証明: A の行を $\mathbf{a}_1,\dots,\mathbf{a}_n$ として，

$$F(\mathbf{a}_1,\dots,\mathbf{a}_n) = \det(AB) = \det\begin{pmatrix}\mathbf{a}_1B\\ \vdots \\ \mathbf{a}_nB\end{pmatrix}$$

を考えると，$F(\mathbf{a}_1,\dots,\mathbf{a}_n)$ は R 多重線形かつ交代的であることが容易にわかる．よって命題 2.4 により

$$F(\mathbf{a}_1,\dots,\mathbf{a}_n) = F(\mathbf{e}_1,\dots,\mathbf{e}_n)\det A = \det(I_nB)\det A = \det B\det A$$

が成立する．ここで I_n は n 次単位行列である．□

命題 2.6 n_1,n_2 を自然数，A_{ij} $(1\le i,j\le 2)$ を R の元を成分とする $n_i\times n_j$ 行列として，

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22}\end{pmatrix}$$

とおく．もし A_{21} または A_{12} が 0 行列ならば，$\det A = \det A_{11}\det A_{22}$ が成立する．

証明: $n = n_1 + n_2$ とおき A の第 (i,j) 成分を a_{ij} とする．$A_{21} = O$ と仮定しよう．すると，$n_1 < i \leq n$ かつ $1 \leq j \leq n_1$ のとき $a_{ij} = 0$ である．行列式の定義により

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \, a_{1\sigma(1)} \cdots a_{n_1\sigma(n_1)} a_{n_1+1,\sigma(n_1+1)} \cdots a_{n\sigma(n)}$$

である．もし $\sigma(n_1+1), \ldots, \sigma(n)$ の中に n_1 以下のものがあれば $a_{n_1+1,\sigma(n_1+1)} \cdots a_{n\sigma(n)} = 0$ となるから，σ は集合 $\{n_1+1, \ldots, n\}$ をそれ自身に写すとしてよい．このとき σ は集合 $\{1, \ldots, n_1\}$ をそれ自身に写す．そこで，σ の $\{1, \ldots, n_1\}$ への制限を $\sigma_1 \in S_{n_1}$, σ の $\{n_1, \ldots, n\}$ への制限を $\sigma_2 \in S_{n_2}$ とすれば，$\sigma = \sigma_1\sigma_2$ である．よって，上記の和において，σ_1 を S_{n_1} 全体を動かし，σ_2 を S_{n_2} (集合 $\{n_1+1, \ldots, n\}$ の置換の全体をみなす）全体を動かして $\sigma = \sigma_1\sigma_2$ とすればよい．従って，

$$\begin{aligned}
\det A &= \sum_{\sigma_1 \in S_{n_1}} \sum_{\sigma_2 \in S_{n_2}} \operatorname{sgn}(\sigma_1\sigma_2) \, a_{1\sigma_1(1)} \cdots a_{n_1\sigma_1(n_1)} a_{n_1+1,\sigma_2(n_1+1)} \cdots a_{n\sigma_2(n)} \\
&= \left(\sum_{\sigma_1 \in S_{n_1}} \operatorname{sgn}\sigma_1 \, a_{1\sigma_1(1)} \cdots a_{n_1\sigma_1(n_1)} \right) \left(\sum_{\sigma_2 \in S_{n_2}} \operatorname{sgn}\sigma_2 \, a_{n_1+1,\sigma_2(n_1+1)} \cdots a_{n\sigma_2(n)} \right) \\
&= \det A_{11} \det A_{22}
\end{aligned}$$

となることがわかる．$A_{12} = O$ の場合は転置行列を考えればよい．□

$A = (a_{ij}) \in M_n(R)$ の第 (i,j) **余因子** (cofactor) とは，A の第 i 行と第 j 列を除いてできる $n-1$ 次正方行列の行列式に $(-1)^{i+j}$ を掛けて得られる R の元のことである．

命題 2.7 $A = (a_{ij}) \in M_n(R)$ の第 (i,j) 余因子を $\tilde{a}_{ij}$ とすると，

$$\begin{aligned}
\det A &= a_{i1}\tilde{a}_{i1} + a_{i2}\tilde{a}_{i2} + \cdots + a_{in}\tilde{a}_{in} \qquad (1 \leq i \leq n) \\
\det A &= a_{1j}\tilde{a}_{1j} + a_{2j}\tilde{a}_{2j} + \cdots + a_{nj}\tilde{a}_{nj} \qquad (1 \leq j \leq n)
\end{aligned}$$

証明: まず $i = 1$ の場合に最初の等式を示そう．行列式の多重線形性と交代性，および命題 2.6 を用いると，

$$\det A = \begin{vmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} 0 & a_{12} & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \cdots + \begin{vmatrix} 0 & 0 & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} - \begin{vmatrix} a_{12} & 0 & 0 & \cdots & 0 \\ a_{22} & a_{21} & a_{23} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n2} & a_{n1} & a_{n3} & \cdots & a_{nn} \end{vmatrix} + \cdots + (-1)^{n-1} \begin{vmatrix} a_{1n} & 0 & \cdots & 0 \\ a_{2n} & a_{21} & \cdots & a_{2,n-1} \\ \vdots & \vdots & & \vdots \\ a_{nn} & a_{n1} & \cdots & a_{n,n-1} \end{vmatrix}$$

$$= a_{11}\tilde{a}_{11} + a_{12}\tilde{a}_{12} + \cdots + a_{1n}\tilde{a}_{1n}$$

となり証明できた.（最後の行で命題 2.6 と $(-1)^{i+1} = (-1)^{i-1}$ を用いた.）$2 \leq j \leq n$ のときは，まず A の第 j 行を第 1 行に移動し，第 2 行から第 $j-1$ 行は 1 つ下に移動する．すなわち，A の行に対して巡回置換 $(1, 2, \ldots, j)$ を施す．この置換の符号は $(-1)^{j+1}$ であるから，行列式は $(-1)^{j+1}$ 倍される．その後 $j = 1$ の場合の結果を用いれば，最初の等式が証明される．2 番目の等式は転置行列を考えればよい．□

$A = (a_{ij}) \in M_n(R)$ に対して，$\tilde{a}_{ji}$ を第 (i, j) 成分とする n 次正方行列 $(\tilde{a}_{ji})$ を A の**余因子行列** (adjugate matrix) という．

命題 2.8 $A = (a_{ij}) \in M_n(R)$ の余因子行列を $\tilde{A}$ とすると，$A\tilde{A} = \tilde{A}A = (\det A)I_n$ が成立する．

証明: $A\tilde{A}$ の第 (i, j) 成分 b_{ij} は $a_{i1}\tilde{a}_{j1} + \cdots + a_{in}\tilde{a}_{jn}$ であるから，$i = j$ のときは，命題 2.7 により，$b_{ii} = \det A$ となる．$i \neq j$ のときは，b_{ij} は，A の第 i 行を A の第 j 行で置き換えて第 j 行はそのままとした行列の行列式である.（余因子 $\tilde{a}_{i1}, \ldots, \tilde{a}_{in}$ は A の第 i 行の成分には無関係なのでこの操作で変化しないことに注意.）よって $b_{ij} = 0$ である．以上により $A\tilde{A} = (\det A)I_n$ であることが示された．$\tilde{A}A$ は，列についての展開を用いればよい．□

定理 2.1 $A \in M_n(R)$ が可逆元（単元）であるための必要十分条件は，$\det A$ が R の単元であることである．

証明: A が可逆元であれば $AB = I_n$ を満たす $B \in M_n(R)$ が存在する．このとき $\det A \det B = \det(AB) = \det I_n = 1$ であるから，$\det A$ は R の単元である．逆に $\det A$ が R の単元であれば，$u \det A = 1$ となるような R の単元 u が存在する．これと $A\tilde{A} = \tilde{A}A = (\det A)I_n$ より，

$$A(u\tilde{A}) = u(A\tilde{A}) = (u \det A)I_n = I_n, \quad (u\tilde{A})A = u(\tilde{A}A) = (u \det A)I_n = I_n$$

を得る．よって A は逆元 $A^{-1} = u\tilde{A} = (\det A)^{-1}\tilde{A} \in M_n(R)$ を持つから，$M_n(R)$ の可逆元である．□

$M_n(R)$ の可逆元の全体を $GL(n, R)$ で表す．特に $A \in M_n(\mathbb{Z})$ が可逆元，すなわち $A \in GL(n, \mathbb{Z})$ であるための必要十分条件は $\det A = \pm 1$ となることである．このような整数行列 A のことを**ユニモジュラー (unimodular) 行列**という．

命題 2.9 R を整域とし，R 加群 M が基底 $u_1, \ldots, u_n$ を持つとする．このとき，M の任意の $n+1$ 個の元は R 上 1 次従属である．

証明: M の $n+1$ 個の元 $v_1, \ldots, v_{n+1}$ を任意にとる．$u_1, \ldots, u_n$ が基底であることから，

$$v_i = \sum_{j=1}^{n} a_{ji}u_j \qquad (1 \leq i \leq n+1)$$

を満たす $a_{ij} \in R$ が存在する． a_{ij} を (i,j) 成分とする $n \times (n+1)$ 行列を A とする．R の商体を K として，$a_{ij} \in K$ とみなす．A の階数（ランク）は n 以下であるから，A に行基本変形を施すことにより，

$$A \begin{pmatrix} c_1 \\ \vdots \\ c_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} c_1 \\ \vdots \\ c_{n+1} \end{pmatrix} \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

をみたす $c_1, \ldots, c_{n+1} \in K$ を求めることができる．各 c_i は R の商体の元であるから $c_i = \dfrac{a_i}{b_i}$ $(a_i, b_i \in R,\ b_i \neq 0)$ と表すことができる．そこで，$d_i = (b_1 \cdots b_{n+1})c_i$ とおけば $d_i \in R$ かつ $(d_1, \ldots, d_{n+1}) \neq (0, \ldots, 0)$ である．このとき，

$$\sum_{i=1}^{n+1} d_i v_i = \sum_{i=1}^{n+1} \sum_{j=1}^{n} d_i a_{ji} u_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n+1} a_{ji} d_i \right) u_j = b_1 \cdots b_{n+1} \sum_{j=1}^{n} \left(\sum_{i=1}^{n+1} a_{ji} c_i \right) u_j = 0$$

となるから，$v_1, \ldots, v_{n+1}$ は 1 次従属である．□

定理 2.2 整域上の有限階数自由加群の階数は，基底の選び方によらず一定である．

証明: 整域 R 上の加群 M が基底 $u_1, \ldots, u_n$ を持つとする．このとき M の $n+1$ 個以上の元は上の命題により R 上 1 次従属となるから，基底にはなり得ない．よって $v_1, \ldots, v_m$ が M の別の基底ならば，$m \leq n$ でなければならない．この両者の基底の立場を入れ替えれば $n \leq m$ であることもわかるから，$m = n$ を得る．□

命題 2.10 整域 R 上の加群 M が基底 $u_1, \ldots, u_m$ を持つとする．$a_{ij} \in R$ として

$$v_i = \sum_{j=1}^{m} a_{ji} u_j \qquad (1 \leq i \leq m)$$

とおく．このとき $v_1, \ldots, v_m$ が M の基底となるための必要十分条件は，行列 $A = (a_{ij})$ が $M_m(R)$ の可逆元であることである．このとき A を**基底変換の行列**という．

証明: $v_1, \ldots, v_m$ が M の基底であるとすると，$b_{ij} \in R$ が存在して

$$u_i = \sum_{j=1}^{m} b_{ji} v_j \qquad (1 \leq i \leq m)$$

と表される．このとき，

$$u_i = \sum_{j=1}^{m} b_{ji} \sum_{k=1}^{m} a_{kj} u_k = \sum_{k=1}^{m} \left(\sum_{j=1}^{m} a_{kj} b_{ji} \right) u_k \qquad (1 \leq i \leq m)$$

と $u_1, \ldots, u_m$ が 1 次独立なことから，$B = (b_{ij})$ とおくと，$AB = I_m$ が成立する．$u_1, \ldots, u_m$ と $v_1, \ldots, v_m$ の役割を入れ替えれば $BA = I_m$ が成立することもわかるから，A は $M_m(R)$ における可逆元である．

逆に A が可逆元であると仮定して $B=(b_{ij})=A^{-1}$ とおくと，

$$\sum_{i=1}^{m} b_{ij}v_i = \sum_{i=1}^{m}\sum_{k=1}^{m} b_{ij}a_{ki}u_k = \sum_{k=1}^{m}\left(\sum_{i=1}^{m} a_{ki}b_{ij}\right)u_k = \sum_{k=1}^{m}\delta_{kj}v_k = u_j$$

が成立する．$u_1,\dots,u_m$ は基底だから，任意の $u\in M$ に対して，$u=c_1u_1+\cdots+c_mu_m$ となるような $c_1,\dots,c_m\in R$ が存在する．このとき

$$u=\sum_{j=1}^{m} c_ju_j = \sum_{j=1}^{m} c_j\sum_{i=1}^{m} b_{ij}v_i = \sum_{i=1}^{m}\left(\sum_{j=1}^{m} b_{ij}c_j\right)v_i$$

であるから，$v_1,\dots,v_m$ は M を生成する．$v_1,\dots,v_m$ が 1 次独立であることを示そう．$c_i\in R$, $c_1v_1+\cdots+c_mv_m=0$ と仮定すると，

$$0=\sum_{i=1}^{m} c_iv_i = \sum_{i=1}^{m} c_i\left(\sum_{j=1}^{m} a_{ji}u_j\right) = \sum_{j=1}^{m}\left(\sum_{i=1}^{m} a_{ji}c_i\right)u_j$$

と $u_1,\dots,u_m$ が 1 次独立なことから，

$$\sum_{i=1}^{m} a_{ji}c_i = 0 \qquad (1\le i\le m)$$

$A=(a_{ij})$ は可逆だから左から A^{-1} を掛けて $c_1=\cdots=c_m=0$ を得る．□

2.4 基底変換と行列表示

M を基底 $u_1,\dots,u_m$ を持つ自由 R 加群とする．$u'_1,\dots,u'_m$ を M の別の基底とすると，

$$u'_i=\sum_{j=1}^{m} p_{ji}u_j = p_{1i}u_1+\cdots+p_{mi}u_m \qquad (i=1,\dots,m)$$

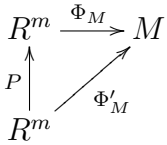
をみたす $p_{ji}\in R$ が定まり，基底変換の行列 $P=(p_{ij})$ は命題 2.10 によって $M_m(R)$ の可逆元である．2 組の基底によって 2 つの R 同型写像

$$\Phi_M : R^m\ni\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}\longmapsto\sum_{i=1}^{m}x_iu_i\in M, \qquad \Phi'_M : R^m\ni\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}\longmapsto\sum_{i=1}^{m}x_iu'_i\in M$$

が定まる．このとき任意の $\mathbf{v}\in R^m$ に対して $\Phi'_M(\mathbf{v})=\Phi_M(P\mathbf{v})$ が成立する．実際，$\mathbf{v}={}^t(x_1,\dots,x_m)$ とすると，

$$\Phi'_M(\mathbf{v})=\sum_{i=1}^{m}x_iu'_i=\sum_{i=1}^{m}\sum_{j=1}^{m}x_ip_{ji}u_j=\sum_{j=1}^{m}\Big(\sum_{i=1}^{m}p_{ji}x_i\Big)u_j=\Phi_M(P\mathbf{v})$$

が成立する．これは次の図式が可換であることを意味している．

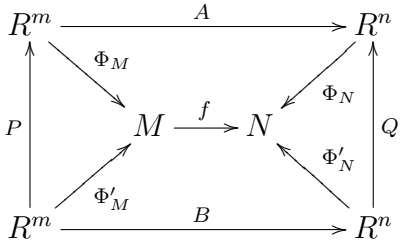


N を基底 $v_1, \ldots, v_n$ を持つ R 自由加群として，$f : M \longrightarrow N$ を R 準同型とする．A を f のこれらの基底に関する行列表示とする．

$u'_1, \ldots, u'_m$ を M の別の基底，$v'_1, \ldots, v'_n$ を N の別の基底として，基底変換の行列を $P = (p_{ij})$, $Q = (q_{ij})$，すなわち

$$u'_i = \sum_{j=1}^{m} p_{ji} u_j \qquad (i = 1, \ldots, m), \qquad v'_i = \sum_{j=1}^{n} q_{ji} v_j \qquad (i = 1, \ldots, n)$$

とおく．P は m 次の可逆行列，Q は n 次の可逆行列である．基底 $u'_1, \ldots, u'_m$ と $v'_1, \ldots, v'_n$ に関する f の行列表示を B とする．このとき次の可換図式ができる．



この可換図式より $AP = QB$ すなわち $B = Q^{-1}AP$ が成立することがわかる．特に $M = N$ の場合は M と N で同じ基底を用いるのが自然であり，このとき $\Phi_M = \Phi_N$, $\Phi'_M = \Phi'_N$, $P = Q$ となるから，$B = P^{-1}AP$ を得る．

2.5 単因子

R をユークリッド整域とする.（実は，R が単項イデアル整域の場合でも以下で述べる事項は成立するが，より抽象的な議論が必要となる.）R の元を成分とする行列を基本変形と呼ばれる操作によってある標準形に変形できることを示すのがこの節の目標である．

加群の言葉で言い換えれば，R 上の有限階数自由加群 M, N と R 準同型 $f : M \to N$ に対して，f の行列表示がなるべく簡単な形になるような M と N の基底を選ぶことに相当する．

定理 2.3 (単因子論の基本定理) R をユークリッド整域として，A を R の元を成分とする $n \times m$ 行列であって 0 行列ではないものとすると，可逆な行列 $P \in GL(n, R)$, $Q \in GL(m, R)$ と R の 0 でない元 $d_1, \ldots, d_r$ $(1 \leq r \leq \min\{n, m\})$ が存在して

$$PAQ = B = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_r \\ & & & \end{pmatrix}$$

かつ $i=2,\dots,r$ について d_i は d_{i-1} の倍元となる．ここで右辺の行列の $d_1,\dots,d_r$ 以外の成分はすべて 0 である．行列 B のことを行列 A の**標準形**と呼ぶ．$d_1,\dots,d_r$ を行列 A の**単因子** (elementary divisor) という．d_i は単元倍してもよい．特に，d_i が R の単元ならば $d_i=1$ としてよい．

証明: R の元を成分とする $n\times m$ 行列 A に対して，次の 6 つの操作を環 R 上の行または列**基本変形**と呼ぶことにする．

(1) A のある行または列を α 倍する．ただしα は R の単元とする．

(2) $i\neq j$ として，A の第 i 行に第 j 行の β 倍を加える．または，A の第 i 列に第 j 列の β 倍を加える．ただし β は R の任意の元とする．

(3) $i\neq j$ として，A の第 i 行と第 j 行，または A の第 i 列と第 j 列を入れ替える．

(1) の操作は，$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$ という n 次または m 次正方行列を左または右から A に掛けることに相当する．

(2) の操作は

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & \cdots & \beta & \\ & & & \ddots & \vdots & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix} \quad \text{または} \quad \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & \vdots & \ddots & & \\ & & \beta & \cdots & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

という n 次または m 次正方行列を左または右から A に掛けることに相当する．

(3) の操作は

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & \cdots & 1 & \\ & & \vdots & \ddots & \vdots & \\ & & 1 & \cdots & 0 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

という n 次または m 次正方行列を左または右から A に掛けることに相当する．

(1) に対応する行列の行列式は R の単元 α，(2) に対応する行列の行列式は 1，(3) に対応する行列の行列式は -1 であるから，いずれも可逆な行列である．

従って，A に対して左右の基本変形を有限回行うことにより，定理の右辺の形の行列に変形できることを示せばよい．以下ではユークリッド整域の定義における写像 $N : R \to \mathbb{N} \cup \{0, -1\}$ を用いて，$N(a_{ij})$ を仮に a_{ij} の**大きさ**（$R = \mathbb{Z}$ の場合は絶対値，$R = K[x]$ の場合は次数）と呼ぶことにする．次の手続き（アルゴリズム）を実行する．(以下では行列のサイズ n, m は最初の n, m より小さくなる可能性があることに注意.)

(1) A が 0 行列ならば終了．A が 0 行列でなく A のサイズが 1×1 ならばその $(1,1)$ 成分を最後の単因子 d_r として終了．A が 0 行列でも 1×1 行列でもなければ，A の成分のうち大きさが最小のものの 1 つを a_{ij} とするとき，第 1 行と第 i 行の交換，第 1 列と第 j 列の交換を行って a_{ij} が $(1,1)$ 成分になるようにする．この行列をあらためて A として (2) に進む

(2) A の要素のうち a_{11} が大きさが最小であるとする．

(i) もし a_{1j} $(j \geq 2)$ および a_{i1} $(i \geq 2)$ がすべて a_{11} で割り切れれば，第 j 列 $(\forall j \geq 2)$ に第 1 列の $-a_{1j}/a_{11}$ 倍を加え，第 i 行 $(\forall i \geq 2)$ に第 1 行の $-a_{i1}/a_{11}$ 倍を加えることにより，第 1 行と第 1 列の要素は a_{11} 以外はすべて 0 にできる．この行列を A として (3) に進む．

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} \longrightarrow \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a'_{22} & \cdots & a'_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n2} & \cdots & a'_{nm} \end{pmatrix}$$

(ii) もし，a_{1j} $(j \geq 2)$ および a_{i1} $(i \geq 2)$ の中に a_{11} で割り切れないもの，たとえば a_{1j} があれば，a_{1j} を a_{11} で割り算して $a_{1j} = qa_{11} + r$ $(q, r \in R, N(r) < N(a_{11}))$ とする．このとき，第 j 列に第 1 列の $-q$ 倍を加えれば，$(1, j)$ 成分は r となる．この行列をあらためて A として (1) に戻る．

$$\begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ a_{21} & \cdots & a_{2j} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nm} \end{pmatrix} \longrightarrow \begin{pmatrix} a_{11} & \cdots & r & \cdots & a_{1m} \\ a_{21} & \cdots & a'_{2j} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a'_{nj} & \cdots & a_{nm} \end{pmatrix}$$

(3) A の第 1 行と第 1 列の要素は $(1,1)$ 成分を除いてすべて 0 であるとする．A の行または列の数が 1 ならば $(1,1)$ 成分を最後の単因子 d_r として終了．そうでなければ次の (i) または (ii) へ．

(i) a_{ij} $(i \geq 2, j \geq 2)$ がすべて a_{11} で割り切れれば，a_{11} は単因子である．これが第 k 番目に得られた単因子であれば $d_k = a_{11}$ とする．A の行または列の数が

1 ならば終了．そうでなければ，A から第 1 行と第 1 列を除いてできる行列をあらためて A として (1) に戻る．

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n2} & \cdots & a_{nm} \end{pmatrix} \longrightarrow \begin{pmatrix} a_{22} & \cdots & a_{2m} \\ \vdots & & \vdots \\ a_{n2} & \cdots & a_{nm} \end{pmatrix}, \qquad d_k = a_{11}$$

(ii) a_{ij} $(i \geq 2, j \geq 2)$ のうち a_{11} で割り切れないものがあれば，その 1 つを a_{ij} として d を a_{11} と a_{ij} の最大公約元とする．(d の大きさが最小になるような a_{ij} を選ぶとよい．) このとき $d = sa_{11} + ta_{ij}$ を満たす $s, t \in R$ が存在する．第 i 行の t 倍を第 1 行に加えて，第 1 列の s 倍を第 j 列に加えれば $(1, j)$ 成分が d になる．ここで，a_{ij} は a_{11} で割り切れないからその余り r_1 は 0 ではない．a_{ij} と a_{11} にユークリッドの互除法を適用したときの余りを順に $r_1, r_2, \ldots$ とすると，$N(a_{11}) > N(r_1) > N(r_2) > \cdots$ が成立する．a_{ij} と a_{11} の最大公約元 d は $r_1, r_2, \ldots$ のどれかであるから $N(d) < N(a_{11})$ が成立する．この行列をあらためて A として (1) に戻る．

$$\begin{pmatrix} a_{11} & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{nj} & \cdots & a_{nm} \end{pmatrix} \longrightarrow \begin{pmatrix} a_{11} & \cdots & d & \cdots & a'_{1m} \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{nj} & \cdots & a_{nm} \end{pmatrix}$$

以上の手続きは有限回で終了する．実際，ステップ (2) の (ii), (3) の (i)，(3) の (ii) からステップ (1) に戻ると，$(1, 1)$ 成分の大きさまたは行列 A のサイズはその 1 つ前の段階のときより真に小さくなる．従って以上の操作（ループ）が無限に続くことはない．

行列のサイズが小さくなるのはステップ (3) の (i) のみである．そこで A の第 1 行と第 1 列を除いた行列を A' とする．A' に対する基本変形は，A に対する第 1 行と第 1 列を変えない基本変形とみなすことができる．さらに，A' の各成分は $d_k = a_{11}$ の倍元である．A' に基本変形を施してもこのことは変わらないから，A' が零行列でなければ A' の最初の単因子 d_{k+1} も d_k の倍元である．A' が零行列ならば，d_k が A の最後の単因子である．

計算が終了するのは (1) の (i) でサイズが 1×1 になったとき，または (3) の (i) でサイズが $1 \times m$ または $n \times 1$ になったときであり，そのとき $(1, 1)$ 成分以外は 0 となっているから，以上の計算を総合すれば，A が標準形に変形できたことになる．□

単因子が基本変形の選び方によらず行列から（単元倍を除いて）一意的に定まることは後で証明する．

例 2.9 整数係数の 1×3 行列 $A = \begin{pmatrix} 6 & -21 & 15 \end{pmatrix}$ の単因子は 3 である．

$$A = \begin{pmatrix} 6 & -21 & 15 \end{pmatrix} \overset{(2)(ii)}{\longrightarrow} \begin{pmatrix} 6 & 3 & 15 \end{pmatrix} \overset{(1)}{\longrightarrow} \begin{pmatrix} 3 & 6 & 15 \end{pmatrix} \overset{(2)(i)}{\longrightarrow} \begin{pmatrix} \underline{3} & 0 & 0 \end{pmatrix} = B, \quad d_1 = 3$$

例 2.10 次の整数行列 A の単因子は 2 と 26 である．

$$A=\begin{pmatrix}22&-10\\30&-16\end{pmatrix}\overset{(1)}{\longrightarrow}\begin{pmatrix}-10&22\\-16&30\end{pmatrix}\overset{(2)(ii)}{\longrightarrow}\begin{pmatrix}-10&2\\-16&-2\end{pmatrix}\overset{(1)}{\longrightarrow}\begin{pmatrix}2&-10\\-2&-16\end{pmatrix}\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}2&0\\-2&-26\end{pmatrix}$$
$$\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}\underline{2}&0\\0&-26\end{pmatrix}\overset{(3)(i)}{\longrightarrow}(-26)\longrightarrow(\underline{26}),\qquad B=\begin{pmatrix}\underline{2}&0\\0&26\end{pmatrix}\quad d_1=2,\,d_2=26$$

例 2.11 次の整数行列の単因子は 1 と 6 である．

$$A=\begin{pmatrix}3&-6&9\\6&10&-20\end{pmatrix}\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}3&0&0\\0&22&-38\end{pmatrix}\overset{(3)(ii)}{\longrightarrow}\begin{pmatrix}3&1&-38\\0&22&-38\end{pmatrix}$$
$$\overset{(1)}{\longrightarrow}\begin{pmatrix}1&3&-38\\22&0&-38\end{pmatrix}\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}\underline{1}&0&0\\0&-66&798\end{pmatrix}\overset{(3)(i)}{\longrightarrow}\begin{pmatrix}-66&798\end{pmatrix}\overset{(2)(ii)}{\longrightarrow}\begin{pmatrix}-66&6\end{pmatrix}$$
$$\overset{(1)}{\longrightarrow}\begin{pmatrix}6&-66\end{pmatrix}\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}\underline{6}&0\end{pmatrix}$$

よって標準形は $\begin{pmatrix}1&0&0\\0&6&0\end{pmatrix}$, 単因子は $1,6$ である．

例 2.12 $\mathbb{Q}[x]$ の元を成分とする次の行列の単因子は 1 と $(x-2)^2$ である．

$$A=\begin{pmatrix}x-8&4\\-9&x+4\end{pmatrix}\overset{(1)}{\longrightarrow}\begin{pmatrix}4&x-8\\x+4&-9\end{pmatrix}\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}4&0\\x+4&-\frac{1}{4}x^2+x-1\end{pmatrix}$$
$$\overset{(2)(i)}{\longrightarrow}\begin{pmatrix}4&0\\0&-\frac{1}{4}x^2+x-1\end{pmatrix}\to\begin{pmatrix}1&0\\0&(x-2)^2\end{pmatrix}=B$$

最後の変形では第 1 行に $\mathbb{Q}[x]$ の単元 $\dfrac{1}{4}$ を掛け，第 2 行に $\mathbb{Q}[x]$ の単元 -4 を掛けた．（この変形を行う前の行列も既に標準形になっている．）

2.6　剰余加群と準同型定理

M を環 R 上の加群，N をその部分加群とする．M における同値関係 $\sim$ を

$$u\sim v\quad\Leftrightarrow\quad u-v\in N$$

により定義する．これが同値関係であることは，N が部分加群であることから容易にわかる．この同値関係による商集合 $M/\sim$ を M/N と表す．$u\in M$ に対して，u を含む同値類を $[u]$ または $\overline{u}$ で表す．すなわち

$$\overline{u}=[u]=\{v\in M\mid u-v\in N\}$$

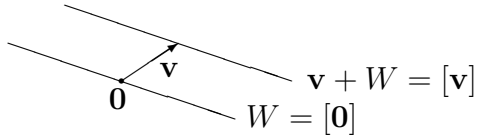
である．$u,v\in M$ に対して和 $\overline{u}+\overline{v}\in M/N$ と $a\in R$ の作用 $a\overline{u}\in M/N$ を

$$\overline{u}+\overline{v}=\overline{u+v},\qquad a\,\overline{u}=\overline{au}$$

により「定義」する．この定義が well-defined であることは容易に確かめられる．これによって M/N は R 加群となる．M/N のことを M の N による**剰余加群** (quotient module) という．

例 2.13 R を可換環，I を R のイデアルとする．R を R 加群とみなしたとき，I は R の部分 R 加群であるから，剰余加群 R/I が定義される．同値関係は剰余環のときと同じだから，剰余加群 R/I と剰余環 R/I は加法群としては同じである．しかし，剰余加群では $a \in R$ と $u \in R$ に対して $a\overline{u} \in R/I$ が定義されるの対して，剰余環では $u, v \in R$ に対して $\overline{uv} \in R/I$ が定義される．

例 2.14 (商ベクトル空間) V を体 K 上の有限次元ベクトル空間，W を V の部分ベクトル空間とすると，剰余加群 V/W は K 加群，すなわち K 上のベクトル空間である．これを商ベクトル空間という．$\mathbf{v} \in V$ の V/W における同値類 $[\mathbf{v}]$ は W を $\mathbf{v}$ だけ平行移動してできる V の部分集合 (アフィン部分空間と呼ばれる) $\mathbf{v} + W = \{\mathbf{v} + \mathbf{w} \mid \mathbf{w} \in W\}$ である．V/W はアフィン部分空間 $\mathbf{v} + W$ $(\mathbf{v} \in V)$ のうち相異なるものの全体である．



V と W のベクトル空間としての次元を $\dim V = n$, $\dim W = m$ とすると，V の基底 $\{\mathbf{e}_1, \ldots, \mathbf{e}_m, \mathbf{e}_{m+1}, \ldots, \mathbf{e}_n\}$ を $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ が W の基底になるようにとれる．このとき定義から $c_1, \ldots, c_n \in K$ に対して

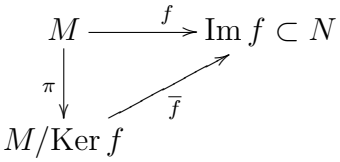
$$[c_1\mathbf{e}_1 + \cdots + c_n\mathbf{e}_n] = [c_{m+1}\mathbf{e}_{m+1} + \cdots + c_n\mathbf{e}_n] = c_{m+1}[\mathbf{e}_{m+1}] + \cdots + c_n[\mathbf{e}_n],$$
$$c_{m+1}[\mathbf{e}_{m+1}] + \cdots + c_n[\mathbf{e}_n] = [\mathbf{0}] \Leftrightarrow c_{m+1}\mathbf{e}_{m+1} + \cdots + c_n\mathbf{e}_n \in W \Leftrightarrow c_{m+1} = \cdots = c_n = 0$$

が成立する．実際，$c_{m+1}\mathbf{e}_{m+1} + \cdots + c_n\mathbf{e}_n \in W$ ならば，ある $c_1, \ldots, c_m \in K$ があって

$$c_{m+1}\mathbf{e}_{m+1} + \cdots + c_n\mathbf{e}_n = c_1\mathbf{e}_1 + \cdots + c_m\mathbf{e}_m$$

と表される．$\mathbf{e}_1, \ldots, \mathbf{e}_m, \ldots, \mathbf{e}_n$ は 1 次独立だから $c_1 = \cdots = c_n = 0$ となる．以上により $[\mathbf{e}_{m+1}], \cdots, [\mathbf{e}_n]$ が V/W の基底になっていることがわかった． 特に次元の公式 $\dim(V/W) = \dim V - \dim W$ が成立する．

定理 2.4 (加群の準同型定理) R を可換環，M と N を R 加群，$f : M \longrightarrow N$ を R 準同型とする．$\pi : M \longrightarrow M/\mathrm{Ker}\, f$ を自然な全射準同型，すなわち $\pi(u) = \overline{u}$ は $u \in M$ の $M/\mathrm{Ker}\, f$ における同値類とする．このとき R 同型 $\overline{f} : M/\mathrm{Ker}\, f \xrightarrow{\sim} \mathrm{Im}\, f$ であって，$\overline{f} \circ \pi = f$ すなわち $\overline{f}(\overline{u}) = f(u)$ $(\forall u \in M)$ をみたす $\overline{f}$ がただ一つ存在する．



証明: $\overline{f}(\overline{u}) = f(u)$ であるから，このような $\overline{f}$ は存在すれば一通りしかない．まず，$\overline{f}(\overline{u}) = f(u)$ によって写像 $\overline{f} : M/\mathrm{Ker}\, f \to N$ が定まる (well-defined) ことを示そう．$\overline{u} = \overline{v}$ すなわち $u - v \in \mathrm{Ker}\, f$ とすると，$f(u) - f(v) = f(u - v) = 0$ であるから，$\overline{f}(\overline{u}) = \overline{f}(\overline{v})$ となる．よって $\overline{f}$ は well-defined である．$\overline{f}$ が R 準同型であることは，f が R 準同型であることから容易にわかる．

$$\overline{f}(\overline{u}) = f(u) = 0 \;\Leftrightarrow\; u \in \mathrm{Ker}\, f \;\Leftrightarrow\; \overline{u} = \overline{0}$$

であるから $\overline{f}$ は単射である．$\overline{f}$ の像は f の像 $\mathrm{Im}\, f$ と一致するから，$\overline{f}$ は $M/\mathrm{Ker}\, f$ から $\mathrm{Im}\, f$ への全単射である．□

例 2.15 V と W を体 K 上のベクトル空間，$T : V \to W$ を K 線形写像とする．このとき K 同型写像 $\overline{T} : V/\mathrm{Ker}\, T \to \mathrm{Im}\, T$ であって，任意の $\mathbf{v} \in V$ に対して $\overline{T}([\mathbf{v}]) = T\mathbf{v}$ を満たすものが存在する．特に $V/\mathrm{Ker}\, T$ と $\mathrm{Im}\, T$ の次元は等しいから

$$\dim V - \dim \mathrm{Ker}\, T = \dim(V/\mathrm{Ker}\, T) = \dim \mathrm{Im}\, T$$

が成立する．

命題 2.11 R を可換環，M と N を R 加群，$f : M \longrightarrow N$ を R 準同型とする．M' は M の部分 R 加群，N' は N の部分 R 加群であり $f(M') \subset N'$ が成立すると仮定する．このとき R 準同型 $\overline{f} : M/M' \longrightarrow N/N'$ であって $\overline{f}([u]) = [f(u)]$ $(\forall u \in M)$ を満たすものがただ 1 つ存在する．ここで $[u]$ は M/M' における剰余類，$[f(u)]$ は N/N' における剰余類を表す．

証明: $u, v \in M$ が $[u] = [v]$ すなわち $u - v \in M'$ を満たせば $f(u) - f(v) = f(u - v) \in N'$ であるから $[f(u)] = [f(v)]$ が成立する．よって $\overline{f}$ は well-defined である．$\overline{f}$ が R 準同型であることは定義から明らかである．また $\overline{f}([u]) = [f(u)]$ より $\overline{f}$ は f から一意的に定まる．□

M と N を可換環 R 上の加群として，$f : M \to N$ を R 準同型とする．このとき剰余加群 $N/\mathrm{Im}\, f$ のことを準同型 f の**余核** (cokernel) といい，$\mathrm{Coker}\, f$ で表す．f が全射であることと $\mathrm{Coker}\, f$ が零加群 $\{0\}$ であることは同値である．

R がユークリッド整域で M と N が有限階数自由 R 加群のときは，単因子の計算によって f の核，像，余核（と同型な加群）を求めることができる．

M を基底 $u_1, \ldots, u_m$ を持つ自由 R 加群，N を基底 $v_1, \ldots, v_n$ を持つ自由 R 加群として，$f : M \longrightarrow N$ を R 準同型とする．A を f のこれらの基底に関する行列表示とする．単因子論の基本定理によって $P \in GL(m, R)$ と $Q \in GL(n, R)$ が存在して $B = Q^{-1}AP$ が標準形となる．(定理 2.3 における Q を P, P を Q^{-1} とすればよい.) このとき，P と Q をそれぞれ基底変換の行列とするような M の基底 $u'_1, \ldots, u'_m$ と N の基底 $v'_1, \ldots, v'_n$ をとれば，B はこれらの基底に関する f の行列表示である．このとき R 準同型の可換図式

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \Phi'_M}\uparrow & & \uparrow{\scriptstyle \Phi'_N} \\ R^m & \xrightarrow{B} & R^n \end{array} \qquad \Phi'_M\left(\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}\right) = \sum_{i=1}^{m} x_i u'_i, \quad \Phi'_N\left(\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right) = \sum_{j=1}^{n} y_j v'_j$$

ができる（B は行列 B を左から掛ける写像を表す）．すなわち $f\circ\Phi'_M=\Phi'_N\circ B$ が成立する．

命題 2.12 以上の仮定のもとで B を定理 2.3 の標準形とすると，R 加群としての同型

$$\begin{aligned}&\operatorname{Ker} f\cong\operatorname{Ker} B=R^{m-r},\qquad \operatorname{Im} f\cong\operatorname{Im} B=Rd_1\oplus\cdots\oplus Rd_r\cong R^r,\\&\operatorname{Coker} f\cong\operatorname{Coker} B=(R/Rd_1)\oplus\cdots\oplus(R/Rd_r)\oplus R^{n-r}\end{aligned}$$

が成立する．特に $\operatorname{Ker} f$ と $\operatorname{Im} f$ は自由 R 加群である．

証明: Φ'_N が単射であることから，$\mathbf{v}={}^t(x_1,\dots,x_m)\in R^m$ に対して

$$B\mathbf{v}=\mathbf{0}\quad\Leftrightarrow\quad\Phi'_N(B\mathbf{v})=\Phi'_N(\mathbf{0})=0_N\quad\Leftrightarrow\quad f(\Phi'_M(\mathbf{v}))=0_N$$

Φ'_M は全射だから M の任意の元はある $\mathbf{v}\in R^m$ によって $\Phi'_M(\mathbf{v})$ と表せるので $\Phi'_M(\operatorname{Ker} B)=\operatorname{Ker} f$ が示された．Φ'_M は R 同型写像だから $\operatorname{Ker} B$ と $\operatorname{Ker} f$ は R 同型である．次に，Φ'_M が全射であることから

$$\operatorname{Im} f=\operatorname{Im}(f\circ\Phi'_M)=\operatorname{Im}(\Phi'_N\circ B)=\Phi'_N(\operatorname{Im} B)$$

Φ'_N は R 同型写像だから $\operatorname{Im} f$ と $\operatorname{Im} B$ は R 同型である．さらにこの同型と命題 2.11 により R 準同型

$$\overline{\Phi'_N}\ :\ \operatorname{Coker} B=R^n/\operatorname{Im} B\longrightarrow\operatorname{Coker} f=N/\operatorname{Im} f$$

が定まる．Φ'_N が全射であることから $\overline{\Phi'_N}$ も全射であることがわかる．$\mathbf{w}\in R^n$ に対して

$$\begin{aligned}&\Phi'_N([\mathbf{w}])=[\Phi'_N(\mathbf{w})]=[0_N]\in\operatorname{Coker} f\\\Leftrightarrow\quad&\Phi'_N(\mathbf{w})=f(u)=\Phi'_N(B(\Phi'_M)^{-1}(u))\quad(\exists u\in M)\\\Leftrightarrow\quad&\mathbf{w}=B(\Phi'_M)^{-1}(u)\quad(\exists u\in M)\\\Leftrightarrow\quad&\mathbf{w}\in\operatorname{Im} B\quad\Leftrightarrow\quad[\mathbf{w}]=[\mathbf{0}]\in\operatorname{Coker} B\end{aligned}$$

であるから $\overline{\Phi'}$ は単射である．以上により f の核，像，余核は B の核，像，余核と同型であることが示された．

$$B\,{}^t(x_1,\dots,x_m)={}^t(d_1x_1,\dots,d_rx_r,\underbrace{0,\dots,0}_{n-r})\in R^n\qquad(x_1,\dots,x_m\in R)$$

より

$$\begin{aligned}\operatorname{Ker} B&=\{{}^t(\underbrace{0,\dots,0}_{r},x_{r+1},\dots,x_m)\mid x_{r+1},\dots,x_m\in R\}=R^{m-r},\\\operatorname{Im} B&=\{{}^t(d_1x_1,\dots,d_rx_r,\underbrace{0,\dots,0}_{n-r})\mid x_1,\dots,x_r\in R\}=Rd_1\oplus\cdots\oplus Rd_r\cong R^r,\\\operatorname{Coker} B&=(R/Rd_1)\oplus\cdots\oplus(R/Rd_r)\oplus\underbrace{R\oplus\cdots\oplus R}_{n-r}=(R/Rd_1)\oplus\cdots\oplus(R/Rd_r)\oplus R^{n-r}\end{aligned}$$

を得る．ここで $R^r\in{}^t(x_1,\dots,x_r)\mapsto(d_1x_1,\dots,d_rx_r)\in Rd_1\oplus\cdots\oplus Rd_r$ が R 同型であること（容易に確かめられる）を用いた．□

例 2.16 例 2.11 の行列 A を $\mathbb{Z}^3$ から $\mathbb{Z}^2$ への $\mathbb{Z}$ 準同型とみなすと $\operatorname{Ker} A \cong \mathbb{Z}$, $\operatorname{Im} A \cong \mathbb{Z} \oplus 6\mathbb{Z} \cong \mathbb{Z}^2$, $\operatorname{Coker} A \cong (\mathbb{Z}/\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$.

例 2.17 次の行列 A の定める $\mathbb{Z}^2$ から $\mathbb{Z}^3$ への $\mathbb{Z}$ 準同型を考える．

$$A := \begin{pmatrix} 2 & -6 \\ 8 & -2 \\ -4 & 6 \end{pmatrix} \overset{(2)(i)}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 8 & 22 \\ -4 & -6 \end{pmatrix} \overset{(2)(i)}{\longrightarrow} \begin{pmatrix} \underline{2} & 0 \\ 0 & 22 \\ 0 & -6 \end{pmatrix} \overset{(2)(i)}{\longrightarrow} \begin{pmatrix} 22 \\ -6 \end{pmatrix} \overset{(1)}{\longrightarrow} \begin{pmatrix} -6 \\ 22 \end{pmatrix} \overset{(2)(ii)}{\longrightarrow} \begin{pmatrix} -6 \\ 4 \end{pmatrix}$$

$$\overset{(1)}{\longrightarrow} \begin{pmatrix} 4 \\ -6 \end{pmatrix} \overset{(2)(ii)}{\longrightarrow} \begin{pmatrix} 4 \\ 2 \end{pmatrix} \overset{(1)}{\longrightarrow} \begin{pmatrix} 2 \\ 4 \end{pmatrix} \overset{(2)(i)}{\longrightarrow} \begin{pmatrix} \underline{2} \\ 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}$$

より単因子は $2, 2$ であるから，

$$\operatorname{Ker} A = \{0\}, \quad \operatorname{Im} A \cong 2\mathbb{Z} \oplus 2\mathbb{Z} = \mathbb{Z}^2, \quad \operatorname{Coker} A \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}$$

定理 2.5 (中国剰余定理) R を単項イデアル整域とし，R の 0 でない元 $q_1, \ldots, q_k$ はどの 2 つも互いに素であるとすると，R 同型写像

$$\overline{\varphi} \ : \ R/R(q_1 \cdots q_k) \ \overset{\sim}{\longrightarrow} \ (R/Rq_1) \oplus \cdots \oplus (R/Rq_k)$$

が存在する．（この両辺は環の構造も持ち，$\overline{\varphi}$ は環同型でもある．）

証明: k についての帰納法で証明する．まず $k = 2$ のときに示そう．$\pi_i : R \longrightarrow R/Rq_i$ を自然な全射 R 準同型（R の元に R/Rq_i における同値類を対応させる）として，写像 $\varphi : R \longrightarrow (R/Rq_1) \oplus (R/Rq_2)$ を $a \in R$ に対して $\varphi(a) = (\pi_1(a), \pi_2(a))$ で定義する．φ が R 準同型（かつ環準同型）であることは容易に確かめられる．

$$\varphi(a) = 0 \quad \Leftrightarrow \quad a \in Rq_1 \text{ かつ } a \in Rq_2 \quad \Leftrightarrow \quad a \in R(q_1 q_2)$$

が成立する．実際，$a \neq 0$ が q_1 と q_2 の倍元であるとすると，q_1 の素元分解と q_2 の素元分解は共通の素元を含まないから，素元分解の一意性により，a は q_1 と q_2 の両方の倍元でなければならない．よって，$\operatorname{Ker} \varphi = R(q_1 q_2)$ である．

次に φ が全射であることを示そう．仮定より $Rq_1 + Rq_2 = R$ であるから，ある $a_1, a_2 \in R$ が存在して $a_1 q_1 + a_2 q_2 = 1$ が成り立つ．任意の $c_1, c_2 \in R$ に対して $c = c_1 a_2 q_2 + c_2 a_1 q_1$ とおくと，$\pi_1(q_1) = \overline{0} \in R/Rq_1$, $\pi_2(q_2) = \overline{0} \in R/Rq_2$ より

$$\pi_1(c) = \pi_1(c_1 a_2 q_2) = \pi_1(c_1(1 - a_1 q_1)) = \pi_1(c_1),$$
$$\pi_2(c) = \pi_2(c_2 a_1 q_1) = \pi_2(c_2(1 - a_2 q_2)) = \pi_2(c_2)$$

が成立するから，φ は全射である．従って加群（または環）の準同型定理によって，R 同型（または環同型）

$$\overline{\varphi} \ : \ R/R(q_1 q_2) \ \overset{\sim}{\longrightarrow} \ (R/Rq_1) \oplus (R/Rq_2)$$

であって，$\varphi = \overline{\varphi} \circ \pi$ をみたすものがただ 1 つ存在する．ここで $\pi : R \longrightarrow R/R(q_1q_2)$ は自然な全射準同型である．

$k \geq 3$ のときは q_1 と $q_2 \cdots q_k$ が互いに素なこと（素元分解の一意性から従う）と前半の結果より R 同型

$$R/R(q_1q_2 \cdots q_k) \xrightarrow{\sim} (R/Rq_1) \oplus (R/R(q_2 \cdots q_k))$$

が存在する．帰納法の仮定により R 同型

$$R/R(q_2 \cdots q_n) \xrightarrow{\sim} (R/Rq_2) \oplus \cdots \oplus (R/Rq_k)$$

が存在するから，この 2 つの R 同型を合成すれば求める R 同型を得る．□

例 2.18 $60 = 2^2 \cdot 3 \cdot 5$ より $\mathbb{Z}$ 加群（アーベル群）として $\mathbb{Z}/60\mathbb{Z} \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})$ となる．$\mathbb{Z}/4\mathbb{Z}$ と $(\mathbb{Z}/2\mathbb{Z})^2 = (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ は同型でないことに注意する．実際，後者のすべての元は 2 倍すると 0 になるが，$\mathbb{Z}/4\mathbb{Z}$ においては $2 \cdot \overline{1} = \overline{2} \neq \overline{0}$ である．

例 2.19 例 2.10 の行列 A の定める $\mathbb{Z}$ 準同型 $A : \mathbb{Z}^2 \to \mathbb{Z}^2$ の余核は

$$\operatorname{Coker} A \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/26\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/13\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/13\mathbb{Z})$$

である．また例 2.11 の行列 A の定める $\mathbb{Z}$ 準同型の余核は $\operatorname{Coker} A = \mathbb{Z}/6\mathbb{Z}$
$= (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})$ である．

2.7　ユークリッド整域上の有限生成加群

命題 2.13 R を単項イデアル整域とする．このとき，階数 n の自由 R 加群の任意の部分加群は R 上有限生成であり，高々 n 個の元で生成される．

証明: R^n の任意の部分加群が有限生成であることを n に関する帰納法で証明する．$n = 1$ のときは，R の部分加群 N は R のイデアルであり，R は単項イデアル整域であるから，ある $a \in R$ があって $N = Ra$ となる．よって N は有限生成である．次に $n \geq 2$ として，$n-1$ のときは主張が正しいと仮定する．N を R^n の部分加群とする．R^n から R^{n-1} への写像 f を

$$f({}^t(a_1, \ldots, a_{n-1}, a_n)) = {}^t(a_1, \ldots, a_{n-1}) \in R^{n-1} \qquad (a_1, \ldots, a_{n-1}, a_n \in R)$$

により定義すると f は R 準同型である．$f(N)$ は R^{n-1} の部分加群だから帰納法の仮定により有限生成であり，ある $\mathbf{b}_1, \ldots, \mathbf{b}_r \in R^{n-1}$ $(1 \leq \exists r \leq n-1)$ があって，

$$f(N) = R\mathbf{b}_1 + \cdots + R\mathbf{b}_r \subset R^{n-1}$$

となる．一方

$$I = \{a \in R \mid {}^t(\underbrace{0, \ldots, 0}_{n-1}, a) \in N\}$$

とおくと，I は R のイデアルである．よって，ある $a_0 \in R$ によって $I = Ra_0$ となる．$\mathbf{a}_0 = {}^t(0, \dots, 0, a_0) \in R^n$ とおく．$1 \leq i \leq r$ のとき，$\mathbf{b}_i \in f(N)$ より，$\mathbf{a}_i := \begin{pmatrix} \mathbf{b}_i \\ a_i \end{pmatrix} \in N$ となるような $a_i \in R$ が存在する．$\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_r$ が N を生成することを示そう．$\mathbf{v}$ を N の任意の元とすると，

$$f(\mathbf{v}) = c_1\mathbf{b}_1 + \cdots + c_r\mathbf{b}_r$$

となるような $c_1, \dots, c_r \in R$ が存在する．このとき，$\mathbf{v}$ と $c_1\mathbf{a}_1 + \cdots + c_r\mathbf{a}_r$ は第 n 成分を除いて一致するから，

$$\mathbf{v} = c_1\mathbf{a}_1 + \cdots + c_r\mathbf{a}_r + {}^t(0, \dots, 0, \lambda) \qquad (\exists \lambda \in R)$$

と表される．$\mathbf{v}, \mathbf{a}_1, \dots, \mathbf{a}_r$ はすべて N に属すから，λ は I に属する．よってある $c_0 \in R$ があって $\lambda = c_0a_0$ となり

$$\mathbf{v} = c_1\mathbf{a}_1 + \cdots + c_r\mathbf{a}_r + c_0\mathbf{a}_0$$

であるから，$r + 1 \leq n$ 個の元 $\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_r$ が N を生成する．□

R を単項イデアル整域，M を R 上の有限生成加群として，$u_1, \dots, u_n$ をその生成系とする．

$$N = \{{}^t(a_1, \dots, a_n) \in R^n \mid a_1u_1 + \cdots + a_nu_n = 0\}$$

は R^n の R 部分加群である．よって命題 2.13 により，N は有限個の生成系 $\mathbf{v}_1, \dots, \mathbf{v}_m$ で生成される．さて，2 つの R 準同型

$$f : R^m \ni {}^t(y_1, \dots, y_m) \longmapsto y_1\mathbf{v}_1 + \cdots + y_m\mathbf{v}_m \in R^n$$
$$g : R^n \ni {}^t(x_1, \dots, x_n) \longmapsto x_1u_1 + \cdots + x_nu_n \in M$$

を考えよう．

$\mathbf{v}_1, \dots, \mathbf{v}_m$ が N を生成することから $\operatorname{Im} f = f(R^m) = N = \operatorname{Ker} g$ が成立する．さらに，$u_1, \dots, u_n$ が M を生成することから，g は全射である．このとき

$$R^m \xrightarrow{f} R^n \xrightarrow{g} M \longrightarrow 0$$

は**完全系列** (exact sequence) であるという．一番右側の写像は M から 0 加群 $\{0\}$（これを 0 と略記している）への 0 写像であり，その核は M であって $\operatorname{Im} g$ と一致している．この完全系列のことを R 加群 M の**有限表示** (finite presentation) という．g は全射であるから，加群の準同型定理により，R 同型

$$\overline{g} : \operatorname{Coker} f = R^n/\operatorname{Im} f = R^n/\operatorname{Ker} g \xrightarrow{\sim} M$$

が存在する．よって M は $\operatorname{Coker} f$ に同型である．逆に $f : R^m \to R^n$ を R 準同型とすれば，$\operatorname{Coker} f$ は R 加群であり，

$$R^m \xrightarrow{f} R^n \xrightarrow{\pi} \operatorname{Coker} f \longrightarrow 0$$

が完全系列となる．ここで π は R^n の元に対して $\operatorname{Coker} f = R^n/\operatorname{Im} f$ における同値類を対応させる写像である．

さて f は $\mathbf{v}_1,\dots,\mathbf{v}_m$ を並べた $n\times m$ 行列 A を左から掛ける写像である．従って命題 2.12 により A の単因子を $d_1,\dots,d_r$ として $l=n-r$ とおけば，R 加群としての同型写像

$$\overline{\varphi}:\ M\ \xrightarrow{\sim}\ (R/Rd_1)\oplus(R/Rd_2)\oplus\cdots\oplus(R/Rd_r)\oplus R^l \tag{7}$$

が存在する．もし d_i が単元であれば $R/Rd_i=\{0\}$ であるから，(7) の右辺において d_i が単元である（すなわち $d_i=1$ とできる）ような直和因子は省略してよいことに注意する．

定理 2.6 同型 (7) において，l と単因子 $d_1,\dots,d_r$ は（単元倍を除いて）R 加群 M のみから（すなわち M の有限表示と，有限表示から定まる行列の基本変形の仕方によらず）一意的に定まる．

証明: まず，l が M から一意的に定まることを示す．加群 M の**ねじれ部分** (torsion part) を

$$TM=\{u\in M\mid au=0\ \text{かつ}\ a\neq 0\ \text{をみたす}\ a\in R\ \text{が存在する}\}$$

と定義する．TM は M の部分加群である．実際，$u,v\in TM$ とすると，$au=bv=0$ をみたすような 0 でない $a,b\in R$ が存在する．このとき $(ab)(u+v)=b(au)+a(bv)=0$ であり，さらに $a(cu)=c(au)=0$ が任意の $c\in R$ について成立する．一方，(7) の右辺のねじれ部分は

$$T((R/Rd_1)\oplus(R/Rd_2)\oplus\cdots\oplus(R/Rd_r)\oplus R^l)=(R/Rd_1)\oplus(R/Rd_2)\oplus\cdots\oplus(R/Rd_r)$$

となるから，剰余加群 M/TM と R^l は R 加群として同型である．定理 2.2 により，整域 R 上の自由加群 M/TM の階数は一意的だから，(7) の右辺の l は M から一意的に定まることが証明された．

次に単因子 $d_1,\dots,d_r$ が M から（R の単元倍を除いて）一意的に定まることを示そう．単因子のうち単元でないものについて示せばよい．そのために R 同型

$$(R/Rd_1)\oplus(R/Rd_2)\oplus\cdots\oplus(R/Rd_r)\ \cong\ (R/Rd'_1)\oplus(R/Rd'_2)\oplus\cdots\oplus(R/Rd'_s) \tag{8}$$

が存在して $d_1|d_2|\cdots|d_r$ かつ $d'_1|d'_2|\cdots|d'_s$ であり，d_1 も d'_1 も単元ではないと仮定する．このとき，$r=s$ であり各 d'_i は d_i の単元倍となることを示せばよい．一般に R 加群 N に対して，その**零化イデアル** (annihilating ideal) を

$$\mathrm{Ann}_R N=\{a\in R\mid au=0\quad(\forall u\in N)\}$$

で定義する．I は R のイデアルであることは容易にわかる．さて，同型な加群の零化イデアルは等しいから，同型 (8) より

$$\begin{aligned}Rd_r&=\mathrm{Ann}_R((R/Rd_1)\oplus(R/Rd_2)\oplus\cdots\oplus(R/Rd_r))\\&=\mathrm{Ann}_R((R/Rd'_1)\oplus(R/Rd'_2)\oplus\cdots\oplus(R/Rd'_s))=Rd'_s\end{aligned}$$

を得る。よって d'_s は d_r の単元倍であるから，$d'_s=d_r$ としてよい．次に (8) から両辺の最後の共通の直和因子を除くと

$$\begin{aligned}Rd_{r-1}&=\mathrm{Ann}_R((R/Rd_1)\oplus(R/Rd_2)\oplus\cdots\oplus(R/Rd_{r-1}))\\&=\mathrm{Ann}_R((R/Rd'_1)\oplus(R/Rd'_2)\oplus\cdots\oplus(R/Rd'_{s-1}))=Rd'_{s-1}\end{aligned}$$

を得る．以下同様にして結論を得る．□

系 2.1 ユークリッド整域の元を成分とする行列の単因子は基本変形の取り方によらず単元倍を除いて一意的である．

証明: A をユークリッド整域 R の元を成分とする $n \times m$ 行列として，$f : R^m \to R^n$ を A の定める R 準同型とする．A の単因子を $d_1, \ldots, d_r$ として $l = n - r$ とおくと，$\operatorname{Coker} f$ は R 加群として (7) の右辺に同型である．$d_1, \ldots, d_r$ のうち $d_1, \ldots, d_s$ が単元であるとすると，定理 2.6 により $d_{s+1}, \ldots, d_r$ は（単元倍を除いて）一意的に定まる．特に $r - s$ と $n - r$ は一意的であるから，$s = n - (n - r) - (r - s)$ も一意的である．以上により $d_1, \ldots, d_r$ の一意性が示された．□

さて，R 加群 M の構造の話に戻ろう．R は素元分解整域であるから，d_r の素元分解に現れる素元のうち互いに単元倍にならないようなものを $p_1, p_2, \ldots, p_s$ とすると，非負整数 m_{ij} によって

$$d_i = p_1^{m_{i1}} p_2^{m_{i2}} \cdots p_s^{m_{is}} \qquad (1 \le i \le r)$$

と表され，$1 \le j \le s$ を満たす各々の j について，$m_{1j} \le m_{2j} \le \cdots \le m_{rj}$ が成立する．（これは $d_1 | d_2 | \cdots | d_{r-1} | d_r$ と素元分解の一意性からわかる．）加群に対する中国剰余定理により R 同型

$$R/Rd_i \xrightarrow{\sim} (R/Rp_1^{m_{i1}}) \oplus \cdots \oplus (R/Rp_s^{m_{is}}) \qquad (1 \le i \le r)$$

が存在する．これと同型 (7) を合わせて，R 同型

$$M \cong \underbrace{\bigoplus_{j=1}^{s} \left((R/Rp_j^{m_{1j}}) \oplus \cdots \oplus (R/Rp_j^{m_{rj}}) \right)}_{\text{ねじれ部分}} \oplus \underbrace{R^l}_{\text{自由部分}} \tag{9}$$

を得る．このうち $m_{ij} = 0$ に対応する直和因子は 0 になるので省略してよい．この同型の右辺の直和因子のうち自由加群 R^l を M の**自由部分** (free part)，その他の因子の直和を M の**ねじれ部分** (torsion part) という．(9) の右辺が M から一意的に定まることは，(9) の右辺から単因子 $d_1, \ldots, d_r$ が一意的に復元できることと定理 2.6 からわかる．たとえば

$$(\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/9\mathbb{Z})^2 \oplus (\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/18\mathbb{Z}) \oplus (\mathbb{Z}/90\mathbb{Z})$$

であるから，対応する単因子は $2, 18, 90$ である．

以上により次の定理が得られた．（ただし R がユークリッド整域の場合についてのみ証明した．）

定理 2.7 (PID 上の有限生成加群の構造定理) M を単項イデアル整域 R 上の有限生成加群とすると，単元倍しても相異なるような R の素元 $p_1, \ldots, p_s$ と自然数 m_{ij}，および非負整数 l が存在して，R 同型

$$M \cong \bigoplus_{j=1}^{s} \left((R/Rp_j^{m_{1j}}) \oplus \cdots \oplus (R/Rp_j^{m_{rj}}) \right) \oplus R^l$$

が成立する．さらに s と l は一意的であり，素元 $p_1, \ldots, p_s$ は単元倍を除いて一意的である．m_{ij} は $m_{1j} \le m_{2j} \le \cdots \le m_{rj}$ を満たすようにとれば一意的である．(そうでなければ，m_{ij} を i について適当に置換すれば一意的となる．)

特に $R=\mathbb{Z}$ とすると，

系 2.2 (有限生成アーベル群の基本定理) M を有限生成アーベル群，すなわち，M の有限個の元 $v_1,\ldots,v_r$ が存在して，任意の M の元 u は，ある整数 $n_1,\ldots,n_r$ によって

$$u=n_1v_1+\cdots+n_rv_r$$

と表されるとする．このとき，相異なる素数 $p_1,\ldots,p_s$ と自然数 m_{ij}，および非負整数 l が存在して，群同型

$$M\ \cong\ \bigoplus_{j=1}^{s}\left((\mathbb{Z}/\mathbb{Z}p_j^{m_{1j}})\oplus\cdots\oplus(\mathbb{Z}/\mathbb{Z}p_j^{m_{rj}})\right)\oplus\mathbb{Z}^l$$

が成立する．さらに s,l と素数 $p_1,\ldots,p_s$ は一意的である．m_{ij} は $m_{1j}\le m_{2j}\le\cdots\le m_{rj}$ を満たすようにとれば一意的である．(そうでなければ，m_{ij} を i について適当に置換すれば一意的となる．)

2.8 行列の Jordan 標準形

V を体 K 上の n 次元ベクトル空間として，$T:V\longrightarrow V$ を K 線形写像とする．$\mathbf{e}_1,\ldots,\mathbf{e}_n$ を V の基底とすると，

$$T(\mathbf{e}_i)=T\mathbf{e}_i=\sum_{j=1}^{n}a_{ji}\mathbf{e}_j\qquad(i=1,\ldots,n)$$

を満たす $a_{ji}\in K$ が一意的に定まる．このとき，n 次正方行列 $A=(a_{ij})$ は，線形写像 T の基底 $\mathbf{e}_1,\ldots,\mathbf{e}_n$ に関する行列表示である．V の基底 $\mathbf{e}_1,\ldots,\mathbf{e}_n$ をうまく選んで，T の行列表示をできるだけ簡単な形にすることが以下の目標である．

変数 x に関する K 係数の多項式 $p(x)=\sum_{i=0}^{k}p_ix^i$ $(p_i\in K)$ の $\mathbf{v}\in V$ への作用を

$$p(x)\mathbf{v}=p(T)\mathbf{v}=\sum_{i=0}^{k}p_iT^i\mathbf{v}$$

で定義する．ただし $T^0=I$ は V から V への恒等写像とする．$p(x)$ が定数多項式 $p_0\in K$ のときは，$p(x)\mathbf{v}$ はスカラー p_0 の作用 $p_0\mathbf{v}$ に等しいことに注意しよう．この作用によって，V を K 係数多項式環 $R:=K[x]$ の上の加群とみなすことができる．K を定数多項式からなる R の部分環と同一視すると，R の V への作用は，スカラー全体 K の作用を拡張したものになっている．V をこのように R 加群とみなしたものを単なる線形空間 V と区別するため V_T と表す．

命題 2.14 T と S を体 K 上のベクトル空間 V から V への 2 つの K 線形写像とする．このとき V_T と V_S が $R=K[x]$ 上の加群として同型になるための必要十分条件は，K 同型写像（全単射な K 線形写像）$\Phi:V\longrightarrow V$ があって，$S=\Phi\circ T\circ\Phi^{-1}$ となることである．

証明: V_T から V_S への R 同型写像 $\Phi : V_T \longrightarrow V_S$ が存在したとする．特に Φ は V から V への K 線形写像である．R の V_T と V_S への作用の定義と Φ が R 準同型であることから，

$$\Phi(T\mathbf{v}) = \Phi(x\mathbf{v}) = x\Phi(\mathbf{v}) = S\Phi(\mathbf{v})$$

が任意の $\mathbf{v} \in V$ について成り立つから，$\Phi \circ T = S \circ \Phi$, すなわち $S = \Phi \circ T \circ \Phi^{-1}$ である．

逆に，$S = \Phi \circ T \circ \Phi^{-1}$ をみたすような K 同型写像 $\Phi : V \longrightarrow V$ が存在したとする．このとき，任意の $\mathbf{v} \in V_T$ に対して

$$\Phi(x\mathbf{v}) = \Phi(T\mathbf{v}) = S\Phi(\mathbf{v}) = x\Phi(\mathbf{v})$$

が成立する．さらに，任意の自然数 j に対して $\Phi \circ T^j = S^j \circ \Phi$ が成立する．実際，$j = 1$ のときは上で示された．$j \geq 2$ のときは，$j-1$ のときは示されたとすると，

$$\Phi \circ T^j = (\Phi \circ T) \circ T^{j-1} = (S \circ \Phi) \circ T^{j-1} = S \circ (\Phi \circ T^{j-1}) = S \circ (S^{j-1} \circ \Phi) = S^j \circ \Phi$$

より j のときも成立する．以上により，任意の $p(x) = \sum_{i=0}^{k} p_i x^i \in K[x]$ に対して

$$\Phi(p(x)\boldsymbol{x}) = \Phi\left(\sum_{i=0}^{k} p_i T^i \mathbf{v}\right) = \sum_{i=0}^{k} p_i \Phi(T^i \mathbf{v}) = \sum_{i=0}^{k} p_i S^i \Phi(\mathbf{v}) = p(x)\Phi(\mathbf{v})$$

が成立するので Φ は V_T から V_S への R 同型である．□

命題 2.15 V を体 K 上の n 次元ベクトル空間，$T : V \to V$ を K 線形写像として，V の基底 $\mathbf{e}_1, \ldots, \mathbf{e}_n$ に関する T の行列表示を $A \in M_n(K)$ とする．$R = K[x]$ として，写像 $f : R^n \to R^n$ と $g : R^n \to V_T$ をそれぞれ

$$\begin{aligned} f({}^t(v_1, \ldots, v_n)) &= (xI_n - A)\,{}^t(v_1, \ldots, v_n) \qquad (v_1, \ldots, v_n \in R), \\ g({}^t(u_1, \ldots, u_n)) &= u_1\mathbf{e}_1 + \cdots + u_n\mathbf{e}_n \qquad (u_1, \ldots, u_n \in R) \end{aligned}$$

により定義すると，

$$R^n \xrightarrow{f} R^n \xrightarrow{g} V_T \longrightarrow 0$$

は R 加群の完全系列である．

この命題の証明のために，次の補題を示そう．

補題 2.5 A を体 K の元を成分とする n 次正方行列，x を不定元（変数）とする．このとき，$R = K[x]$ の元を成分とする任意の縦ベクトル $\mathbf{u} \in R^n$ に対して，ある $\mathbf{q} \in R^n$ と定数ベクトル $\mathbf{r} \in K^n$ が存在して $\mathbf{u} = (xI_n - A)\mathbf{q} + \mathbf{r}$ が成立する．

証明: ある非負整数 m と定数ベクトル $\mathbf{u}_i \in K^n$ があって

$$\mathbf{u} = \mathbf{u}_0 + x\mathbf{u}_1 + \cdots + x^m\mathbf{u}_m$$

と表せる．補題の主張を m についての帰納法で示そう．$m = 0$ の場合は $\mathbf{u} = \mathbf{u}_0 \in K^n$ であるから，$\mathbf{q} = \mathbf{0}$, $\mathbf{r} = \mathbf{u}$ とおけばよい．$m \geq 1$ として $m-1$ の場合には主張は示され

たと仮定する．$\mathbf{u} - x^{m-1}(xI_n - A)\mathbf{u}_m$ の各成分は x について高々 $m-1$ 次であるから，帰納法の仮定により，

$$\mathbf{u} - x^{m-1}(xI_n - A)\mathbf{u}_m = (xI_n - A)\mathbf{q}' + \mathbf{r} \qquad (\exists \mathbf{q}' \in R^n,\ \exists \mathbf{r} \in K^n)$$

が成立する．よって

$$\mathbf{u} = (xI_n - A)(\mathbf{q}' + x^{m-1}\mathbf{u}_m) + \mathbf{r}$$

となるから $\mathbf{q} = \mathbf{q}' + x^{m-1}\mathbf{u}_m$ とおけばよい．□

$\Phi_A(x) := \det(xI_n - A)$ は行列 A の**特性（固有）多項式** (characteristic polynomial) と呼ばれる．

命題 2.15 の証明：$A = (a_{ij})$ として，行列 $xI - A$ の第 i 列を $\mathbf{p}_i$ とおくと，

$$\begin{aligned} g(\mathbf{p}_i) &= g({}^t(-a_{1i}, \dots, x - a_{ii}, \dots, -a_{ni})) = -a_{1i}\mathbf{e}_1 - \cdots + (T - a_{ii})\mathbf{e}_i - \cdots - a_{ni}\mathbf{e}_n \\ &= -\sum_{j=1}^{n} a_{ji}\mathbf{e}_j + T\mathbf{e}_i = -\sum_{j=1}^{n} a_{ji}\mathbf{e}_j + \sum_{j=1}^{n} a_{ji}\mathbf{e}_j = \mathbf{0} \end{aligned}$$

が $1 \le i \le n$ のとき成立する．よって任意の $\mathbf{v} = {}^t(v_1, \dots, v_n) \in R^n$ に対して

$$g(f(\mathbf{v})) = g(v_1\mathbf{p}_1 + \cdots + v_n\mathbf{p}_n) = v_1 g(\mathbf{p}_1) + \cdots + v_n g(\mathbf{p}_n) = \mathbf{0}$$

となるから $g \circ f$ は零写像，よって $\operatorname{Im} f \subset \operatorname{Ker} g$ である．

逆に $\mathbf{u} \in \operatorname{Ker} g$ と仮定する．補題より $\mathbf{u} = (xI_n - A)\mathbf{q} + \mathbf{r} = f(\mathbf{q}) + \mathbf{r}$ をみたす $\mathbf{q} \in R^n$ と $\mathbf{r} = {}^t(r_1, \dots, r_n) \in K^n$ が存在する．このとき

$$\mathbf{0} = g(\mathbf{u}) = g(f(\mathbf{q}) + \mathbf{r}) = g(f(\mathbf{q})) + g(\mathbf{r}) = g(\mathbf{r}) = r_1\mathbf{e}_1 + \cdots + r_n\mathbf{e}_n$$

となるが，$r_1, \dots, r_n \in K$ であり $\mathbf{e}_1, \dots, \mathbf{e}_n$ は K 上 1 次独立であるから，$\mathbf{r} = \mathbf{0}$，従って $\mathbf{u} = f(\mathbf{q})$ は $\operatorname{Im} f$ に属する．よって $\operatorname{Ker} g \subset \operatorname{Im} f$ である．g が全射であることは $\mathbf{e}_1, \dots, \mathbf{e}_n$ が基底であることから従う．□

$R = K[x]$ の元を成分とする行列 $xI_n - A$ の単因子を $d_1(x), \dots, d_r(x)$ とすると，$M_n(R)$ の可逆元 $P(x), Q(x)$ が存在して

$$P(x)(xI_n - A)Q(x) = B(x) := \begin{pmatrix} d_1(x) & & & \\ & d_2(x) & & \\ & & \ddots & \\ & & & d_r(x) \end{pmatrix}$$

が成立する．$a := \det P(x)$ と $b := \det Q(x)$ は R の可逆元，すなわち 0 と異なる K の元（定数多項式）であり，$\Phi_A(x)$ は x のモニック多項式であるから

$$\det B(x) = (\det P(x))(\det Q(x)) \det(xI_n - A) = ab\Phi_A(x)$$

は 0 とは異なる R の元である．よって $r = n$ かつ $\det B(x) = d_1(x) \cdots d_n(x) = ab\Phi_A(x)$ が成立する．特に $d_n(x)$ は $\Phi_A(x)$ の約元であり，

$$\deg d_1(x) + \cdots + \deg d_n(x) = \deg \Phi_A(x) = n$$

が成立することがわかる．

以上と前節の結果より R 加群としての同型写像

$$\varphi : V_T \longrightarrow (R/Rd_1(x)) \oplus \cdots \oplus (R/Rd_n(x)) \tag{10}$$

が存在する．この右辺を更に分解するため，以下ではK が複素数体 $\mathbb{C}$ の場合を考察する．すると代数学の基本定理によって $d_1(x), \ldots, d_n(x)$ は 1 次式の積に分解できて，加群に対する中国剰余定理により，複素数 $\alpha_1, \ldots, \alpha_m$ と自然数 n_i が存在して，$R := \mathbb{C}[x]$ 上の加群としての同型

$$\psi : V_T \longrightarrow (R/R(x-\alpha_1)^{n_1}) \oplus \cdots \oplus (R/R(x-\alpha_m)^{n_m})$$

が存在する．ただし $\alpha_1, \ldots, \alpha_m$ の中には同一のものがあってもよい．

$$(x-\alpha_1)^{n_1} \cdots (x-\alpha_m)^{n_m} = d_1(x) \cdots d_m(x) = (\text{定数}) \times \Phi_A(x)$$

より $n_1 + \cdots + n_m = n$ であることに注意する．

$$V_j := \psi^{-1}(R/R(x-\alpha_j)^{n_j}) \qquad (1 \le j \le r)$$

は V_T の部分 R 加群であるから，ベクトル空間として

$$V = V_1 \oplus \cdots \oplus V_m$$

という直和分解が成り立ち，各 V_j は T 不変部分空間，すなわち $T(V_j) \subset V_j$ が成立する．ψ によって $\overline{1} \in R/(x-\alpha_j)^{n_j}$ に対応する V の元を $\mathbf{v}_j$ (すなわち $\psi(\mathbf{v}_j) = \overline{1}$) として，

$$\mathbf{v}_{ji} := (x-\alpha_j)^{n_j-i}\mathbf{v}_j = (T-\alpha_j I)^{n_j-i}\mathbf{v}_j \qquad (1 \le i \le n_j)$$

とおく．

補題 2.6 $\mathbf{v}_{j1}, \ldots, \mathbf{v}_{j,n_j}$ はベクトル空間 V_j の基底である．

証明: V_j は R 加群として $\mathbf{v}_j$ で生成されるから，V_j の任意の元は，ある多項式 $f(x) \in \mathbb{C}[x]$ によって $f(x)\mathbf{v}_j$ と表される．$f(x)$ を $(x-\alpha_j)^{n_j}$ で割り算すると，ある多項式 $q(x), r(x)$ があって，

$$f(x) = q(x)(x-\alpha_j)^{n_j} + r(x), \quad \deg r(x) < n_j$$

が成り立つ．$r(x) = r(x-\alpha_j+\alpha_j)$ を $x-\alpha_j$ の多項式として

$$r(x) = c_1(x-\alpha_j)^{n_j-1} + c_2(x-\alpha_j)^{n_j-2} + \cdots + c_{n_j-1}(x-\alpha_j) + c_{n_j}$$

と表すことができる．このとき

$$\psi((x-\alpha_j)^{n_j}\mathbf{v}_j) = (x-\alpha_j)^{n_j}\psi(\mathbf{v}_j) = (x-\alpha_j)^{n_j}\overline{1} = \overline{0}$$

より $(x-\alpha_j)^{n_j}\mathbf{v}_j = \mathbf{0}$ となるから，

$$\begin{aligned} f(x)\mathbf{v}_j &= q(x)(x-\alpha_j)^{n_j}\mathbf{v}_j + r(x)\mathbf{v}_j = r(x)\mathbf{v}_j \\ &= c_1(x-\alpha_j)^{n_j-1}\mathbf{v}_j + c_2(x-\alpha_j)^{n_j-2}\mathbf{v}_j + \cdots + c_{n_j-1}(x-\alpha_j)\mathbf{v}_j + c_{n_j}\mathbf{v}_j \\ &= c_1\mathbf{v}_{j1} + c_2\mathbf{v}_{j2} + \cdots + c_{n_j}\mathbf{v}_{j,n_j} \end{aligned}$$

が成立する．従って $\mathbf{v}_{j1},\ldots,\mathbf{v}_{j,n_j}$ は V_j を張る．次にこれらが 1 次独立であることを示そう．

$$c_1\mathbf{v}_{j1} + c_2\mathbf{v}_{j2} + \cdots + c_{n_j}\mathbf{v}_{j,n_j} = \mathbf{0}, \quad c_1,\ldots,c_{n_j} \in \mathbb{C}$$

と仮定して，

$$r(x) = c_1(x-\alpha_j)^{n_j-1} + c_2(x-\alpha_j)^{n_j-2} + \cdots + c_{n_j-1}(x-\alpha_j) + c_{n_j}$$

とおくと，上の変形を逆にたどって $r(x)\mathbf{v}_j = \mathbf{0}$ を得る．

$r(x)\mathbf{v}_j = \mathbf{0} \quad \Leftrightarrow \quad R/R(x-\alpha_j)^{n_j}$ において $r(x)\overline{1} = \overline{0} \quad \Leftrightarrow \quad r(x)$ は $(x-\alpha_j)^{n_j}$ の倍元であり，$r(x)$ の次数は $(x-\alpha_j)^{n_j}$ の次数 n_j より小さいから $r(x) = 0$ でなければならない．従って $\mathbf{v}_{j1},\ldots,\mathbf{v}_{j,n_j}$ は 1 次独立である．□

以上により，$\mathbf{v}_{j1},\ldots,\mathbf{v}_{j,n_j}$ は V_j の基底であり，$j = 1,\ldots,m$ とすれば，全体として V の基底になることがわかった．この基底による線形写像 T の行列表示を求めよう．定義により

$$(T-\alpha_j I)\mathbf{v}_{ji} = (T-\alpha_j I)^{n_j-i+1}\mathbf{v}_j = \mathbf{v}_{j,i-1} \qquad (2 \le i \le n_j)$$

が成立することがわかる．また，

$$(T-\alpha_j I)\mathbf{v}_{j1} = (T-\alpha_j I)^{n_j}\mathbf{v}_j = (x-\alpha_j)^{n_j}\mathbf{v}_j = \mathbf{0}$$

となる．まとめると，

$$\begin{aligned} T\mathbf{v}_{j1} &= \alpha_j\mathbf{v}_{j1} \\ T\mathbf{v}_{ji} &= \alpha_j\mathbf{v}_{ji} + \mathbf{v}_{j,i-1}, \qquad (2 \le i \le n_j) \end{aligned}$$

となる．従って，T の行列表示を J とすると，

$$J = J(\alpha_1,n_1) \oplus \cdots \oplus J(\alpha_m,n_m) := \begin{pmatrix} J(\alpha_1,n_1) & & \\ & \ddots & \\ & & J(\alpha_m,n_m) \end{pmatrix}$$

$$J(\alpha_j,n_j) = \begin{pmatrix} \alpha_j & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \alpha_j \end{pmatrix} \qquad (j = 1,\ldots,m)$$

となる．この J を写像 T の **Jordan（ジョルダン）標準形**, 各々の $J(\alpha_j,n_j)$ を **Jordan ブロック** (または Jordan 細胞）という．

定理 2.8 (Jordan 標準形の一意性) V を $\mathbb{C}$ 上の n 次元ベクトル空間，T と S を V から V への線形写像とする．T の Jordan 標準形と S の Jordan 標準形が Jordan ブロックの順序を除いて一致するための必要十分条件は，V から V への同型写像（全単射の線形写像）Φ があって，$S = \Phi \circ T \circ \Phi^{-1}$ が成立することである．

証明: 以上の議論により，T の Jordan 標準形と (10) の右辺，すなわち $xI_n - A$ の単因子 $d_1(x), \ldots, d_n(x)$ とが 1 対 1 に対応している．定理 2.7 により，(10) の右辺は V_T の $\mathbb{C}[x]$ 加群としての構造から一意的に定まる．これと命題 2.14 から結論を得る．□

系 2.3 A を複素数を成分とする n 次正方行列とすると，ある正則行列 P と複素数 $\alpha_1 \ldots, \alpha_r$，自然数 $n_1, \ldots, n_r$ が存在して，

$$P^{-1}AP = J = J(\alpha_1, n_1) \oplus \cdots \oplus J(\alpha_r, n_r) \tag{11}$$

となる．これを A の Jordan 標準形という．また 2 つの n 次正方行列 A と B が Jordan ブロックの並べ方を除いて同じ Jordan 標準形を持つための必要十分条件は，ある n 次正則行列 P があって，$B = P^{-1}AP$ となることである．

証明: 行列 A によって定まる，数ベクトル空間 $V = \mathbb{C}^n$ から V への線形写像を T とする．V のある基底 $\mathbf{v}_1, \ldots, \mathbf{v}_n$ に関する T の行列表示が Jordan 標準形 J となる．このとき，縦ベクトル $\mathbf{v}_1, \ldots, \mathbf{v}_n$ を並べてできる n 次正方行列を P とすれば，P は正則行列であり，(11) が成立する．最後の主張は定理 2.8 から従う．□

一般に体 K の元を成分とする n 次正方行列 A と多項式 $f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$ $(c_i \in K)$ に対して，変数 x に行列 A を代入してできる行列

$$f(A) = c_m A^m + c_{m-1}A^{m-1} + \cdots + c_1 A_1 + c_1 I_n$$

を考える．$V = K^n$ として，$xI_n - A$ の単因子を $d_1(x), \ldots, d_n(x)$ とすると，

$$\begin{aligned} K[x]d_n(x) = \operatorname{Ann}_{\mathbb{C}[x]} V_T &= \{f(x) \in K[x] \mid f(x)\mathbf{u} = f(A)\mathbf{u} = \mathbf{0}\ (\forall \mathbf{u} \in V)\} \\ &= \{f(x) \in K[x] \mid f(A) = O\} \end{aligned}$$

であるから，$d_n(x)$ は $f(A) = O$ (O は零行列）が成立するような 0 でない多項式のうち次数最小のものである．そこで $d_n(x)$ のことを行列 A の**最小多項式** (minimal polynomial) という．$\Phi_A(x)$ は $d_n(x)$ の倍元であったから次の定理が証明された．

定理 2.9 (Cayley-Hamilton の定理) A を体 K の元を成分とする正方行列として，$\Phi_A(x)$ をその特性多項式とすると，$\Phi_A(A) = O$ （0 行列）が成立する．

例 2.20 複素数を成分とする 2 次正方行列の Jordan 標準形は

$$\text{(i)} \quad \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \qquad \text{(ii)} \quad \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

の 2 種類である．対応する単因子は，(i) で $\alpha \neq \beta$ のときは $1, (x-\alpha)(x-\beta)$, (i) で $\alpha = \beta$ のときは $x-\alpha, x-\alpha$ である．(ii) の場合の単因子は，$1, (x-\alpha)^2$ である．最後の単因子が最小多項式であるから，2 次行列の場合は最小多項式のみから Jordan 標準形が決まることがわかる．

例 2.21 複素数を成分とする 3 次正方行列の Jordan 標準形は

$$\text{(i)}\quad \begin{pmatrix}\alpha&0&0\\0&\beta&0\\0&0&\gamma\end{pmatrix} \qquad \text{(ii)}\quad \begin{pmatrix}\alpha&1&0\\0&\alpha&0\\0&0&\beta\end{pmatrix} \qquad \text{(iii)}\quad \begin{pmatrix}\alpha&1&0\\0&\alpha&1\\0&0&\alpha\end{pmatrix}$$

の 3 種類である．単因子は，(i) で α,β,γ が相異なる場合は $1,\ 1,\ (x-\alpha)(x-\beta)(x-\gamma)$ であり，$\alpha=\beta\neq\gamma$ の場合は $1,\ x-\alpha,\ (x-\alpha)(x-\gamma)$ であり，$\alpha=\beta=\gamma$ の場合は $x-\alpha,\ x-\alpha,\ x-\alpha$ である．(ii) で $\alpha\neq\beta$ の場合は単因子は $1,\ 1,\ (x-\alpha)^2(x-\beta)$ であり，$\alpha=\beta$ の場合は $1,\ x-\alpha,\ (x-\alpha)^2$ である．(iii) の場合の単因子は $1,\ 1,\ (x-\alpha)^3$ である．これより，3 次行列の場合は最小多項式と特性方程式から Jordan 標準形が決まることががわかる．たとえば $\alpha\neq\beta$ のとき，$\begin{pmatrix}\alpha&0&0\\0&\alpha&0\\0&0&\beta\end{pmatrix}$ の最小多項式は $(x-\alpha)(x-\beta)$, 特性多項式は $(x-\alpha)^2(x-\beta)$ であり，$\begin{pmatrix}\alpha&0&0\\0&\beta&0\\0&0&\beta\end{pmatrix}$ の最小多項式は $(x-\alpha)(x-\beta)$, 特性多項式は $(x-\alpha)(x-\beta)^2$ である．

しかし 4 次以上の行列では，たとえば $\begin{pmatrix}\alpha&0&0&0\\0&\alpha&0&0\\0&0&\alpha&1\\0&0&0&\alpha\end{pmatrix}$ と $\begin{pmatrix}\alpha&1&0&0\\0&\alpha&0&0\\0&0&\alpha&1\\0&0&0&\alpha\end{pmatrix}$ の最小多項式は共に $(x-\alpha)^2$, 特性多項式は共に $(x-\alpha)^4$ であり，最小多項式と特性多項式からは区別できない．単因子はそれぞれ $x-\alpha,\ x-\alpha,\ (x-\alpha)^2$ と $1,\ (x-\alpha)^2,\ (x-\alpha)^2$ である．

例 2.22 $A=\begin{pmatrix}0&7&5\\2&4&4\\-3&-3&-4\end{pmatrix}$ の Jordan 標準形を求めよう．

$$xI_3-A=\begin{pmatrix}x&-7&-5\\-2&x-4&-4\\3&3&x+4\end{pmatrix}\to\begin{pmatrix}-2&x-4&-4\\x&-7&-5\\3&3&x+4\end{pmatrix}$$

$$\to\begin{pmatrix}-2&0&0\\0&\frac{1}{2}x^2-2x-7&-2x-5\\0&\frac{3}{2}x-3&x-2\end{pmatrix}\to\begin{pmatrix}\frac{1}{2}x^2-2x-7&-2x-5\\\frac{3}{2}x-3&x-2\end{pmatrix}$$

$$\to\begin{pmatrix}x-2&\frac{3}{2}x-3\\-2x-5&\frac{1}{2}x^2-2x-7\end{pmatrix}\to\begin{pmatrix}x-2&\frac{3}{2}x-3\\-9&\frac{1}{2}x^2+x-13\end{pmatrix}\to\begin{pmatrix}-9&\frac{1}{2}x^2+x-13\\x-2&\frac{3}{2}x-3\end{pmatrix}$$

$$\to\begin{pmatrix}-9&0\\0&\frac{1}{18}x^3-\frac{1}{6}x-\frac{1}{9}\end{pmatrix}\quad d_1(x)=-9,\ d_2(x)=\frac{1}{18}x^3-\frac{1}{6}x-\frac{1}{9}=\frac{1}{18}(x-2)(x+1)^2$$

よって単因子は 1 と $(x-2)(x+1)^2$ であるから A の Jordan 標準形は $\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$.

Jordan 標準形を求めるためには必ずしも単因子の計算を経由する必要はない．行列表示が Jordan 標準形になるような基底を直接求めてもよい．

例 2.23 上の例の行列 A の Jordan 標準形を単因子を計算せずに求めよう．A の特性方程式は $\Phi_A(x) = \det(I_3 - A) = (x-2)(x+1)^2$ である．まず固有値 2 に対する固有ベクトルとして $\mathbf{v}_1 := {}^t(1,1,-1)$ をとれる．次に固有値 -1 に対する固有ベクトルとして $\mathbf{v}_{2,1} := {}^t(1,1,-3)$ がとれ，これと 1 次独立な固有ベクトルはないことがわかる．よって A の Jordan ブロックは $J(2,1)$ と $J(-1,2)$ の 2 つである．これで Jordan 標準形は求まったが，さらに変換行列を求めるために，$A\mathbf{v}_{2,2} = -\mathbf{v}_{2,2} + \mathbf{v}_{2,1}$ を満たすようなベクトル $\mathbf{v}_{2,2} = {}^t(x_1, x_2, x_3)$ を連立 1 次方程式

$$(A + I_2)\mathbf{v}_{2,2} = \begin{pmatrix} 1 & 7 & 5 \\ 2 & 5 & 4 \\ -3 & -3 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$$

を解いて求めると，1 つの解として $\mathbf{v}_{2,2} = {}^t(1,0,0)$ を得る．以上により

$$P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}, \qquad P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ -1 & -3 & 0 \end{pmatrix}$$

ここで，上記の条件を満たすベクトル $\mathbf{v}_{2,1}$ と $\mathbf{v}_{2,2}$ が存在することは，単因子の理論から保証されていることに注意する．単因子を用いずに線形代数のみを用いて Jordan 標準形の存在と一意性を示すことも可能ではあるが議論が極めて煩雑になる．