このテキストは「代数学3・同演習」のために準備した。最終稿には遠いが,**予習と復習を心がける学生にとっては**，少しは勉学上の参考になるかもしれない。演習問題を追加し，使いながら完成させる計画である。

2007年春　後藤四郎

目 次

1　集合と写像

1.1　集合

現代数学は「集合」と「写像」の言葉で記述される。

ものの「あつまり」を「全体として一つのもの」と考えるとき，これを「集合」という。集合に対し，集められた一つ一つのものはその集合の要素（または，元）であるという。例えば，整数の全体を一つのものと考え，この集合を $\mathbb{Z}$ で表せば，$-3, -2, -3, 0, 1, 100, 2002$ といった一つ一つの整数は集合 $\mathbb{Z}$ の要素である。

集合はふつう $A, B, C, \cdots$ などの大文字で表し，集合の要素の方は $a, b, c, \cdots$ などの小文字で表す。小文字 a で表されるあるものが，集合 A の要素であることを $a \in A$ と書く。a が集合 A の要素ではないことは $a \notin A$ と書く。即ち，$4 \in \mathbb{Z}$ であるが，$\frac{1}{2}, \sqrt{2} \notin \mathbb{Z}$ である。

特に，$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$ によって，それぞれ，有理数の全体からなる集合，実数の全体からなる集合，複素数の全体からなる集合を表すのが普通である。

要素が一つもない集合を空集合といい，記号 $\emptyset$ で表す。

問題 1.1. 次の主張は正しいか？

(1) $100 \in \emptyset$

(2) $100 \notin \mathbb{Z}$

(3) $5 \in \mathbb{Q}$

(4) $-2 \notin \mathbb{Z}$

(5) $1 + \sqrt{2} \in \mathbb{Q}$

(6) $i = \sqrt{-1} \notin \mathbb{R}$

1.2　集合の表し方

集合を表すには，二通りの方法がある。一つは，集合の要素をすべて具体的に書いてしまうというやり方である。例えば，

$$A = \{0, 1, 2, 3, 4, 5, 6\}$$

と書けば，A は $0, 1, 2, 3, 4, 5, 6$ を全部あつめて得られる集合を表している。したがって，集合 A の要素は全部で 7 個あり，$4, 6 \in A$ であるが，$-2, -1 \notin A$ である。このやり方には，要素がすぐに目に見える形で分かるという長所があるが，例えば，要素が 10,000 個あったりするような場合でも，なお便利な表記法であるかどうかは疑わしいし，要素が無限個あるような集合を記述するには適当と思えない。もう一つの記述法は，集めようとする一つ一つのものが満たすべき条件を述べ，その条件を満たすもの全体を一つの集合と考えようとする立場であって，次のような書き方である。

$$A = \{x \mid x \text{ は条件 } P(x) \text{ を満たす}\}$$

ここで $P(x)$ は，集めようとしているもの x が満たすべき，何らかの条件を表している。例えば，この記述法を使うと，整数の全体からなる集合 $\mathbb{Z}$ は

$$\mathbb{Z} = \{x \mid x \text{ は整数である}\}$$

となる。この例では,「整数である」が，条件 $P(x)$ に相当している。

$$C = \{(a, b) \mid a, b \in \mathbb{R} \text{ であって } a^2 + b^2 = 1 \text{ が成り立つ}\}$$

とおけば，C は，実数 a, b の組であって等式 $a^2 + b^2 = 1$ を満たすもの (a, b) の全体からなる集合であり，座標平面上で原点を中心とする半径 1 の円周にほかならない。例えば，$(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}) \in C$ であるが，$(1, 1) \notin C$ である。

問題 1.2. 2 番目の記述法で，集合の形に書け。

(1) 1 以上 100 以下の実数の全体からなる集合

(2) 集合 $A = \{0, 1, 2, 3, 4, 5, 6\}$

(3) 座標平面上で点 $(0, 1)$ を通り傾き 2 の直線上の点の全体よりなる集合

(4) 有理数 a, b を用いて $a + b\sqrt{2}$ の形に表される実数の全体よりなる集合

(5) 複素平面上で座標が整数であるような点の全体よりなる集合

1.3 部分集合

A, B は集合とする。集合 A のいかなる要素も集合 B の要素であるとき，A は B の部分集合であるといい，A が B の部分集合であることを $A \subseteq B$ と書く。例えば，$a \in \mathbb{Z}$ なら，a は整数であるから必ず有理数であって，$a \in \mathbb{Q}$ となる。故に $\mathbb{Z} \subseteq \mathbb{Q}$ である。即ち，$A \subseteq B$ とは,「$a \in A$ ならば $a \in B$」という命題が真であることを意味する。空集合 $\emptyset$ はどんな集合 A に対しても部分集合であると考える。即ち $\emptyset \subseteq A$ が正しい。

集合 A が集合 B の部分集合でないことを，$A \not\subseteq B$ と書く。$A \not\subseteq B$ であるための必要十分条件は，$a \notin B$ であるような $a \in A$ が少なくとも一つは存在することである。

問題 1.3. 次の主張は正しいか。正しければ証明を，正しくなければその理由を述べよ。

(1) $\mathbb{Q} \not\subseteq \mathbb{Z}$

(2) $\mathbb{R} \subseteq \mathbb{C}$

(3) $A = \{0, 3, 5\}, B = \{0, 1, 3, 4, 6\}$ のとき，$A \not\subseteq B$ である。

(4) 有理数 a, b を用いて $a + b\sqrt{2}$ の形に表される実数の全体よりなる集合を A とし，有理数 a, b を用いて $a + b\sqrt{3}$ の形に表される実数の全体よりなる集合を B とすれば，$A \not\subseteq B$ である。

要素を完全に共有するとき，2 つの集合 A, B は互いに等しいといい，$A = B$ と書く。

定理 1.4. A, B を集合とする。$A = B$ であるための必要十分条件は，$A \subseteq B$ と $B \subseteq A$ が成り立つことである。

証明. $A = B$ と仮定せよ。すると集合 A, B は要素を完全に共有するので，$x \in A$ ならば必ず $x \in B$ であり，$x \in B$ ならば必ず $x \in A$ である。故に $A \subseteq B$ であってかつ $B \subseteq A$ が成り立つ。逆に $A \subseteq B$ であってかつ $B \subseteq A$ ならば，$x \in A$ であることと $x \in B$ とは同値であるから，A, B は完全に要素を共有し，等式 $A = B$ が成り立つ。 □

定義 1.5. A, B は集合とする。

(1) $A \cup B = \{x \mid x \in A$ であるかまたは $x \in B$ である $\}$,

(2) $A \cap B = \{x \mid x \in A$ かつ $x \in B$ である $\}$,

(3) $A \setminus B = \{x \mid x \in A$ であるが $x \notin B\}$

と定め，$A \cup B$ を A, B の和集合，$A \cap B$ を A, B の共通部分，$A \setminus B$ を A, B の差集合という。

問題 1.6. A, B, C は集合とする。次の主張を証明せよ。

(1) $A \subseteq A \cup B$

(2) $A \cap B \subseteq A$

(3) $[A \cap B] \cup [A \setminus B] = A$

(4) $B \cap (A \setminus B) = \emptyset$

(5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(6) $A \cap B = A$ であるための必要十分条件は，$A \subseteq B$ である。

(7) $A \cup B = A$ であるための必要十分条件は，$B \subseteq A$ である。

証明. (1) $x \in A$ であれば,「$x \in A$ であるかまたは $x \in B$ である」という条件の前半が満たされるので，定義によって $x \in A \cup B$ である。いかなる $x \in A$ も $x \in A \cup B$ であるから，$A \subseteq A \cup B$ である。

(4) もしも $B \cap (A \setminus B) \neq \emptyset$ であったならば，集合 $B \cap (A \setminus B)$ は空でないので，少なくとも一つの要素 x を含む。定義により $x \in B$ であってかつ $x \in A \setminus B$ が成り立つ。しかしなが

ら $x \in A \setminus B$ ならば，これも定義によって必ず $x \notin B$ であるから，$x \in B$ は不可能であってあり得ない。故に $B \cap (A \setminus B) = \emptyset$ であることがわかる。

(5) $x \in A \cap (B \cup C)$ とせよ。すると $x \in A$ である。故に，もしも $x \notin (A \cap B) \cup (A \cap C)$ ならば，$x \notin A \cap B$ であってかつ $x \notin A \cap C$ であるから，$x \notin B$ であって $x \notin C$ であることが従う。しかしながら $x \in B \cup C$ でもあったので，これは不可能である。故に，$x \in (A \cap B) \cup (A \cap C)$ であり，$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ であることがわかる。$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ であることを確かめよう。$x \in (A \cap B) \cup (A \cap C)$ とせよ。すると $x \in A \cap B$ であるかまたは $x \in A \cap C$ であるから，いずれにしても $x \in A$ であり，その他に，$x \in B$ かまたは $x \in C$ が成り立つ。即ち，$x \in A$ であってかつ $x \in B \cup C$ が成り立つ。故に，定義によって $x \in A \cap (B \cup C)$ である。したがって，$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ が成り立ち，等式 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ が得られる。

□

問題 1.7. 次の等式を証明せよ。

$$\{\begin{pmatrix} a \\ b \\ c \end{pmatrix} \mid a, b, c \in \mathbb{R} \text{ であって } a + b + c = 0\} = \{a \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \mid a, b \in \mathbb{R}\}$$

但し，$\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ は 3 次の列ベクトルを表す。

2 同値関係と類別

2.1 直積

A, B は空でない集合とする。$A \times B$ によって，A の元 a と B の元 b の組 (a, b) の全体よりなる集合を表す。即ち

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

である。但し，２つの組 (a_1, b_1) と (a_2, b_2) は，$a_1 = a_2$ であってかつ $b_1 = b_2$ であるとき，等しいと考えている。集合 $A \times B$ を A, B の直積という。

例えば，$A = \{-1, 0, 1\}$, $B = \{1, 2, 3, 4\}$ なら，集合 $A \times B$ は 12 個の元よりなり

$$A \times B = \{(-1,1), (-1,2), (-1,3), (-1,4), (0,1), (0,2), (0,3), (0,4), (1,1), (1,2), (1,3), (1,4)\}$$

である。同様に

$$A \times A = \{(-1,-1), (-1,0), (-1,1), (0,-1), (0,0), (0,1), (1,-1), (1,0), (1,1)\}$$

である。

2.2 同値関係

空でない集合 A に対し，直積 $A \times A$ の部分集合を A 上の関係という。R が A 上の関係であれば，元 $a, b \in A$ に対し，組 (a, b) は集合 $A \times A$ の元であるから，$(a, b) \in R$ かまたは $(a, b) \notin R$ のどちらか一方だけが成り立つ。$(a, b) \in R$ であることを aRb と書く。

例えば，集合 $A = \{-1, 0, 1\}$ に対し

$$R_1 = \{(-1,-1), (0,-1), (1,1)\},$$
$$R_2 = \{(-1,1), (0,-1), (0,1), (1,-1), (1,0)\},$$
$$R_3 = \{(-1,-1), (1,1), (0,0)\}$$

とおけば，R_1, R_2, R_3 はどれも $A \times A$ の部分集合であるから，すべて集合 A の上の関係である。$1R_11$ であるが，$1R_10$ ではない。同様に $-1R_21$ であるが，$1R_21$ ではない。

定義 2.1. R は集合 A 上の関係とせよ。次の 3 条件が満たされるとき，R は A 上の同値関係であるという。

(1) いかなる $a \in A$ に対しても，aRa が成り立つ。

(2) $a, b \in A$ のとき，aRb なら bRa である。

(3) $a, b, c \in A$ のとき，aRb かつ bRc ならば aRc である。

問題 2.2. $A=\{1,2,3,4\}$ とし $R=\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1)\}$ とおけば，R は A 上の同値関係であることを確かめよ。

例 2.3. $R=\{(a,b)\mid a,b\in\mathbb{Z}$ であって $a-b$ は 7 の倍数である $\}$ とおけば，R は集合 $\mathbb{Z}$ 上の同値関係である。

証明. 実際，確かに R は $\mathbb{Z}\times\mathbb{Z}$ の部分集合であり，いかなる $a\in\mathbb{Z}$ に対しても，$a-a=0$ は 7 の倍数であるから，aRa が成り立つ。$a,b\in\mathbb{Z}$ のとき，aRb なら，$a-b$ は 7 の倍数であるから，$b-a$ も 7 の倍数であり，bRa が成り立つ。$a,b,c\in\mathbb{Z}$ のとき，aRb かつ bRc ならば，$a-b$ と $b-c$ は 7 の倍数であるから，$a-c=(a-b)+(b-c)$ も 7 の倍数であり，aRc が成り立つ。故に，R は集合 $\mathbb{Z}$ 上の同値関係である。 □

問題 2.4. $A=\mathbb{R}^3\setminus\{0\}$ とし，集合 A 上に関係 R を

$$R=\{(a,b)\mid a,b\in A\text{であり，ある }0\neq\lambda\in\mathbb{R}\text{があって等式 }a=\lambda b\text{が成り立つ}\}$$

と定める。R は集合 A 上の同値関係であることを確かめよ。但し

$$\mathbb{R}^3=\{\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}\mid a_1,a_2,a_3\in\mathbb{R}\}$$

である。

2.3 類別と商集合

R は空でない集合 A 上の同値関係とする。

定義 2.5. 元 $a\in A$ に対し

$$C(a)=\{x\mid x\in A\text{であって }xRa\text{が成り立つ}\}$$

とおき，集合 $C(a)$ を元 a を含むクラス（または，類）という。明らかに $C(a)\subseteq A$ であり，$a\in C(a)$ である。したがって $C(a)\neq\emptyset$ である。（$C(a)$ の代りに，$\overline{a}$ と書くことも多い。）

例えば，問題 2.2 の例では，$C(1) = C(2) = \{1, 2\}$，$C(3) = \{3\}$，$C(4) = \{4\}$ である。

定理 2.6. $a, b \in A$ とせよ。a, b に関する次の 3 条件は，互いに同値である。

(1) aRb

(2) $C(a) \cap C(b) \neq \emptyset$

(3) $C(a) = C(b)$

証明. (1) $\Rightarrow$ (3) $x \in C(a)$ とすれば，$x \in A$ であって xRa である。仮定により aRb であるので，xRb が成り立ち，$x \in C(b)$ が得られる。故に $C(a) \subseteq C(b)$ である。さて，aRb であるので bRa でもあり，故に a, b の役割をひっくり返すことによって，$C(b) \subseteq C(a)$ であることが従い，等式 $C(a) = C(b)$ が得られる。

(3) $\Rightarrow$ (2) $C(a) = C(b)$ であるから $C(a) \cap C(b) = C(a)$ である。勿論 $C(a) \neq \emptyset$ であるから，$C(a) \cap C(b) \neq \emptyset$ となる。

(2) $\Rightarrow$ (1) 集合 $C(a) \cap C(b)$ は空でないので，少なくとも一つの元 $c \in C(a) \cap C(b)$ を取ることができる。すると $c \in C(a)$ であるから，$c \in A$ であって cRa である。故に aRc でもある。同様に，$c \in C(b)$ であるから，cRb が成り立つ。即ち aRc かつ cRb であるから，aRb である。 □

$A/R = \{C(a) \mid a \in A\}$ とおき，集合 A の R による商集合と呼ぶ。

系 2.7. 次の主張が正しい。

(1) いかなる $X \in A/R$ も，A の空でない部分集合である。

(2) $X, Y \in A/R$ とすると，$X \neq Y$ ならば必ず $X \cap Y = \emptyset$ である。

(3) いかなる $a \in A$ に対しても，ある $X \in A/R$ が存在して $a \in X$ が成り立つ。

即ち，A/R は集合 A の「クラス分け」なのである。実際，集合 A 上に「同値関係を一つ定める」ことと，集合 A を「クラスに分ける」ことは，互いに同等であることが知られている。

例えば，カレンダー

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

とは何かを考えよう。$A = \{1, 2, 3, \ldots, 29, 30, 31\}$ とし

$$R = \{(a, b) \mid a, b \in A \text{ であって } a - b \text{ は } 7 \text{ の倍数である } \}$$

とおけば，R はこの集合 A 上の同値関係であって

$$\begin{aligned} C(1) &= \{1, 8, 15, 22, 29\}, \\ C(2) &= \{2, 9, 16, 23, 30\}, \\ C(3) &= \{3, 10, 17, 24, 31\}, \\ C(4) &= \{4, 11, 18, 25\}, \\ C(5) &= \{5, 12, 19, 26\}, \\ C(6) &= \{6, 13, 20, 27\}, \\ C(7) &= \{7, 14, 21, 28\} \end{aligned}$$

となる。（例えば，$1, 8, 15, 22, 29$ は，1 との差が 7 の倍数であるから，$1, 8, 15, 22, 29 \in C(1)$ である。$a \in C(1)$ なら，$a \in A$ であって $a-1$ は 7 の倍数であるので，$a - 1 = 7n$ $(n \in \mathbb{Z})$ と表される。$1 \leq a \leq 31$ であって $a = 7n+1$ という形をした整数を求めれば，$a = 1, 8, 15, 22$ または 29 である。故に，$a \in \{1, 8, 15, 22, 29\}$ となり，等式 $C(1) = \{1, 8, 15, 22, 29\}$ が得られる。）集合 $C(i)$ $(1 \leq i \leq 7)$ 達の元を見比べれば一目瞭然ではあるが，$1, 2, 3, 4, 5, 6, 7$ はどの異なる 2 つの差も 7 の倍数ではないので，$1 \leq i, j \leq 7$ のとき，$i \neq j$ である限り $C(i) \cap C(j) = \emptyset$ となる。ここで，集合 A の元はどれも，必ずどこかの $C(i)$ に含まれていることに注意しよう。即ち，$A/R = \{C(i) \mid 1 \leq i \leq 7\}$ は，まさしく 1 から 31 までの整数を「クラスに分けている」のである。この意味では,「曜日」とは類に付けられた名前であり，類 $C(1)$ に含まれる日を日曜日，類 $C(2)$ に含まれる日を月曜日，類 $C(3)$ に含まれる日を火曜日，$\ldots$ と名付けたものがカレンダーに他ならないと考えられる。

$C(1)$	$C(2)$	$C(3)$	$C(4)$	$C(5)$	$C(6)$	$C(7)$
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

問題 2.8. $R = \{(a,b) \mid a,b \in \mathbb{Z}$ であって $a-b$ は 10 の倍数である $\}$ とする。いかなる $a \in \mathbb{Z}$ に対しても，等式 $C(a) = \{10n + a \mid n \in \mathbb{Z}\}$ が成り立つことを確かめよ。商集合 $\mathbb{Z}/R$ は丁度 10 個の要素よりなることを示せ。

問題 2.9. まず，集合 $A = \{1,2,3,4,5\}$ をクラスに分け，そのクラス分けを用いて，集合 A 上に同値関係を定めよ。例えば，$C_1 = \{1,3\}$，$C_2 = \{2,4\}$，$C_3 = \{5\}$ というクラス分けに対しては，$R = \{(a,b) \mid a,b \in A$ であり，a,b は同じクラスに属する，即ち，ある $1 \leq i \leq 3$ が存在して $a,b \in C_i$ である $\}$ と定めれば，R は集合 A 上の同値関係であって，等式 $A/R = \{C_1, C_2, C_3\}$ が成り立つ。この考え方を，一般の空でない集合 A に対し拡張せよ。

問題 2.10. A が無限集合ならば，集合 A 上には無限に多くの異なる同値関係を定義できることを証明せよ。

3 写像

3.1 公式的定義

A, B は空でない集合とする。

定義 3.1. f が A から B への写像であるとは

(1) $f \subseteq A \times B$ であって，

(2) どんな $a \in A$ に対しても，$(a,b) \in f$ を満たすような元 $b \in B$ が少なくとも一つは存在し，

(3) $a \in A$, $b, b' \in B$ のとき，もしも $(a,b), (a,b') \in f$ ならば，必ず等式 $b = b'$ が成り立つ

ことをいう。

この定義は「写像とは，集合 A の各々の元 a に対し，集合 B の元 b を一つずつ定める規則のことである」という使いやすく分かりやすい定義を，堅苦しくしかし数学的には厳密に述べたものである。

f が A から B への写像であることを，$f : A \to B$ と書く。$f : A \to B$ であれば，$(a, b) \in f$ となる元 $b \in B$ は，与えられた元 $a \in A$ に対し唯一つ定まる。この $b \in B$ を $b = f(a)$ と書き，a の f による像という。$b = f(a)$ であることを $f : a \mapsto b$ と書くこともある。

例 3.2. $f(a) = a^2 - 1$ と定めれば，写像 $f : \mathbb{R} \to \mathbb{R}$ が得られる。上の書き方を使えば，$f = \{(a, a^2 - 1) \mid a \in \mathbb{R}\}$ となる。

例えば $A = \{1, 2, 3\}$ としよう。集合 A から集合 B への写像 f を定めることと，$A \times B$ の部分集合で $f = \{(1, x), (2, y), (3, z)\}$ (ここで x, y, z はなにか B の元である) という形をしているものを定めることは同じであって，行列

$$\begin{pmatrix} 1 & 2 & 3 \\ x & y & z \end{pmatrix}$$

の x, y, z を，B の元で置き換えることとも同等である。$B = \{4, 5, 6, 7\}$ のとき，このような行列の書き方で説明すると

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 5 & 5 \end{pmatrix}$$

などは，勿論 $f : A \to B$, $g : A \to B$ であって，$f : 1 \mapsto 4$, $f : 2 \mapsto 5$, $f : 3 \mapsto 6$, $g(1) = 6$, $g(2) = g(3) = 5$ である。A から B への写像は，全部で $4^3 = 64$ 個ある。

定義 3.3. 2つの写像 $f : A \to B$, $g : C \to D$ は，$A = C$ かつ $B = D$ であって，さらに，いかなる $a \in A$ に対しても等式 $f(a) = g(a)$ が成り立つとき，等しいと言い，$f = g$ と書く。

$f, g : A \to B$ のときは，$f = g$ であるための必要十分条件は，任意の $a \in A$ に対し等式 $f(a) = g(a)$ が成り立つことである。

3.2 像と原像

A, B は空でない集合とし $f : A \to B$ は写像とせよ。$X \subseteq A$，$Y \subseteq B$ に対し

$$f(X) = \{b \in B \mid \text{ある } a \in X \text{ があって } b = f(a) \text{ と表される }\},$$

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

とおき，$f(X)$ を f による X の像，$f^{-1}(Y)$ を f による Y の原像と呼ぶ。$f(X) \subseteq B$ であって，$f^{-1}(Y) \subseteq A$ である。特に $f(A)$ を写像 f の像という。

例えば，$A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ とし，$f : A \to B$ を $f(1) = 5, f(2) = 7, f(3) = 4$ とする。このとき，$X = \{2, 3\}$，$Y_1 = \{6\}$，$Y_2 = \{4, 5\}$ に対し，$f(X) = \{4, 7\}$ であって，$f^{-1}(Y_1) = \emptyset$，$f^{-1}(Y_2) = \{1, 3\}$ である。f の像は $f(A) = \{4, 5, 7\}$ となる。

問題 3.4. いかなる写像 $f : A \to B$ についても，等式 $f(\emptyset) = \emptyset$, $f^{-1}(\emptyset) = \emptyset$，$f^{-1}(B) = A$ が成り立つことを確かめよ。

証明. $a \in A$ とすれば，$f(a) \in B$ であるから，$a \in f^{-1}(B)$ が成り立ち，$A \subseteq f^{-1}(B)$ であることがわかる。定義により $f^{-1}(B) \subseteq A$ であるから，等式 $f^{-1}(B) = A$ が成り立つ。 □

問題 3.5. 写像 $f : \mathbb{R} \to \mathbb{R}$ を $f(a) = a^2 - 1$ と定め，$X = \{a \in \mathbb{R} \mid a \geq 2\}$，$Y = \{a \in \mathbb{R} \mid a \geq 3\}$ とすれば，等式 $f(X) = Y$ が成り立つことを確かめよ。また，$f^{-1}(\{0\}) = \{-1, 1\}$ であることを示せ。

証明. $b \in f(X)$ なら，$b \in \mathbb{R}$ であり，何かある $a \in X$ によって $b = a^2 - 1$ と表される。$a \geq 2$ であるから，$b \in \mathbb{R}, b \geq 3$ となり，$b \in Y$ が得られる。故に $f(X) \subseteq Y$ である。逆に，$b \in Y$ とすれば，$b \geq 3$ であるから，$b + 1 \geq 4$ となり，$a = \sqrt{b+1}$ とおけば，$a \in \mathbb{R}$ であって，$a \geq 2, f(a) = a^2 - 1 = b$ が成り立つ。$a \in X$ であるから，$b \in f(X)$ となり，$Y \subseteq f(X)$ であることが従う。故に $f(X) = Y$ である。 $a \in f^{-1}(\{0\})$ ならば，$a \in \mathbb{R}$ であって $f(a) = a^2 - 1 \in \{0\}$ が成り立つ。故に，$a^2 = 1$ であるから，$a = -1$ または $a = 1$ であっ

て，$a \in \{-1, 1\}$ となる。逆に，$a \in \{-1, 1\}$ なら，$a = -1$ であるか $a = 1$ であるから，$a^2 = 1$ であって $f(a) = 0$ となる。即ち，$a \in f^{-1}(\{0\})$ である。故に，等式 $f^{-1}(\{0\}) = \{-1, 1\}$ が成り立つ。 □

問題 3.6. 写像 $f : \mathbb{R}^3 \to \mathbb{R}$ を $f(\begin{pmatrix} a \\ b \\ c \end{pmatrix}) = a + b + c$ と定めるとき，次の問に答えよ。

(1) 等式

$$f^{-1}(\{0\}) = \{\lambda \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \mid \lambda, \mu \in \mathbb{R}\}$$

が成り立つことを確かめよ。

(2) $X = \{\begin{pmatrix} a \\ b \\ 0 \end{pmatrix} \mid a, b \in \mathbb{R}\}$ とおけば，等式 $f(X) = \mathbb{R}$ が成り立つことを確かめよ。

(3) $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 6 \\ -2 \end{pmatrix} \in f^{-1}(\{1\})$ であることを確かめよ。

(4) 等式

$$f^{-1}(\{1\}) = \{\lambda \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mid \lambda, \mu \in \mathbb{R}\}$$

が成り立つことを確かめよ。

定理 3.7. $f : A \to B$ を写像とし，$X, X_1, X_2 \subseteq A$, $Y, Y_1, Y_2 \subseteq B$ とすれば，次の主張が正しい。

(1) $X_1 \subseteq X_2$ ならば $f(X_1) \subseteq f(X_2)$ である。

(2) $Y_1 \subseteq Y_2$ ならば $f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$ である。

(3) $f(f^{-1}(Y)) \subseteq Y$ である。

(4) $X \subseteq f^{-1}(f(X))$ である。

(5) 等式 $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$ が成り立つ。

(6) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$ である。

証明. (1) $b \in f(X_1)$ とし $b = f(a)$ $(a \in X_1)$ と表せば，$X_1 \subseteq X_2$ であるから，$a \in X_2$ となり，$b \in f(X_2)$ であることが従う。故に $f(X_1) \subseteq f(X_2)$ である。

(2) $a \in f^{-1}(Y_1)$ なら，$a \in A$ であって $f(a) \in Y_1$ が成り立つ。$Y_1 \subseteq Y_2$ であるから，$f(a) \in Y_2$ となり，$a \in f^{-1}(Y_2)$ である。故に $f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$ である。

(3) $b \in f(f^{-1}(Y))$ なら，$b = f(a)$ $(a \in f^{-1}(Y)$ と表すと，$a \in A$ であって $f(a) \in Y$ であるので，$b = f(a) \in Y$ が成り立つ。故に，$f(f^{-1}(Y)) \subseteq Y$ である。

(4) $a \in X$ ならば，$f(a) \in f(X)$ である。故に，$a \in f^{-1}(f(X))$ であるので，$X \subseteq f^{-1}(f(X))$ となる。

(5) $b \in f(X_1 \cup X_2)$ なら，$b = f(a)$ $(a \in X_1 \cup X_2)$ と表せば，$a \in X_1$ であるかまたは $a \in X_2$ が成り立つ。$a \in X_1$ であれば，$b = f(a) \in f(X_1)$ であり，$a \in X_2$ であれば，$b = f(a) \in f(X_2)$ であるので，$b = f(a) \in f(X_1) \cup f(X_2)$ が成り立つ。故に $f(X_1 \cup X_2) \subseteq f(X_1) \cup f(X_2)$ である。$X_1 \subseteq X_1 \cup X_2$ であるから，(1) によって $f(X_1) \subseteq f(X_1 \cup X_2)$ となる。同様に，(1) より $f(X_2) \subseteq f(X_1 \cup X_2)$ であるので，$f(X_1) \cup f(X_2) \subseteq f(X_1 \cup X_2)$ が成り立ち，等式 $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$ が得られる。

(6) (2) より $f^{-1}(Y_1) \cup f^{-1}(Y_2) \subseteq f^{-1}(Y_1 \cup Y_2)$ である。$a \in f^{-1}(Y_1 \cup Y_2)$ とすれば，$f(a) \in Y_1$ か $f(a) \in Y_2$ が成り立つので，$a \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$ となり，等式 $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$ が得られる。 □

問題 3.8. $f : A \to B$ を写像とし，$X, X_1, X_2 \subseteq A$, $Y, Y_1, Y_2 \subseteq B$ とする。次の主張は正しいか。正しければ証明を，正しくなければ反例（正しくないという明確な理由）を述べよ。

(1) $f(f^{-1}(Y)) = Y$ である。

(2) $X = f^{-1}(f(X))$ である。

(3) $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ である。

(4) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$ である。

証明. (4) だけが正しい。他のものについては，例えば，$A = \{1,2,3\}$, $B = \{4,5,6,7\}$ とし，$f : A \to B$ を $f(1) = 5, f(2) = 7, f(3) = 5$ とする。このとき，

(1) $Y = B$ とすれば，$f^{-1}(B) = A$ であるが，$f(A) = \{5,7\} \neq B$ である。

(2) $X = \{2,3\}$ とすれば，$f(X) = \{5,7\}$ であるから，$f^{-1}(f(X)) = \{1,2,3\}$ である。

(3) $X_1 = \{1\}$, $X_2 = \{3\}$ とすれば $X_1 \cap X_2 = \emptyset$ であるから，$f(X_1 \cap X_2) = f(\emptyset) = \emptyset$ である。しかしながら，$f(X_1) = f(X_2) = \{5\}$ であるから $f(X_1) \cap f(X_2) = \{5\}$ である。 □

3.3 特殊な写像・単射と全射

A, B は空でない集合とし，$f : A \to B$ は写像とする。

定義 3.9. (1) 等式 $f(A) = B$ が成り立つとき，f は全射であるという。

(2) $a_1, a_2 \in A$ とする。$f(a_1) = f(a_2)$ なら必ず $a_1 = a_2$ が成り立つとき，f は単射であるという。

(3) f が単射であってかつ全射であるとき，f は全単射であるという。

条件 (1) は，如何なる $b \in B$ も，何かある $a \in A$ によって $b = f(a)$ という形に表されることを意味している。条件 (2) は，$a_1, a_2 \in A$ であって，$a_1 \neq a_2$ なら，必ず $f(a_1) \neq f(a_2)$ であることを意味している。

例えば，$A = \{1,2,3\}$, $B = \{4,5,6,7\}$ のとき，写像 $f : A \to B$ を単射となるように定めることは，行列

$$\begin{pmatrix} 1 & 2 & 3 \\ x & y & z \end{pmatrix}$$

の中の x, y, z を異なる B の元 3 つで埋めることと同等である。実際，$f(1) = 5, f(2) = 6, f(3) = 4$ は単射であり，$g(1) = 7, g(2) = 6, g(3) = 5$ も単射であるが，$h(1) = 4, h(2) = 7, h(3) = 4$ は単射でない。いかなる写像 $f : A \to B$ についても $f(A)$ は高々3 個の元しか含まないので，この例ではどんな $f : A \to B$ も全射にはなり得ない。

問題 3.10. $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7\}$ とする。

(1) 全射 $f : A \to B$ を 2 つ作れ。

(2) どんな写像 $f : A \to B$ も単射ではないことを証明せよ。

問題 3.11. $\mathrm{M}_2(\mathbb{R})$ によって 2 次実正方行列の全体よりなる集合を表す。即ち

$$\mathrm{M}_2(\mathbb{R}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \}$$

とし，写像 $f : \mathbb{R} \to \mathrm{M}_2(\mathbb{R})$ を $f(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ によって定める。次の問に答えよ。

(1) 任意の $a, b \in \mathbb{R}$ に対して，等式 $f(a+b) = f(a)f(b)$ が成り立つことを確かめよ。但し $a+b$ は数の和を表し，$f(a)f(b)$ は 2 つの行列 $f(a), f(b)$ の積を表す。

(2) f は単射であることを確かめよ。

(3) f は全射であるか。正しければ証明を，正しくないならばその理由を述べよ。

問題 3.12. $f : \mathbb{R} \to \mathbb{R}$ を $f(a) = a^2 + 1$ と定めると，写像 f は単射でも全射でもないことを確かめよ。

問題 3.13. $\mathbb{N} = \{n \mid n$ は正の整数である $\}$ とし，$f, g : \mathbb{N} \to \mathbb{N}$ を

$$f(n) = \begin{cases} 1 & (n = 1 \text{ のとき}) \\ n - 1 & (n \geq 2 \text{ のとき}), \end{cases}$$

$g(n) = n + 1$ と定める。

(1) 写像 f は全射であるが，単射ではないことを確かめよ。

(2) 写像 g は単射であるが，全射ではないことを確かめよ。

定理 3.14. X は空ではない有限集合（元が有限個しかない集合）とし，$f : X \to X$ は写像とする。このとき f に関する次の 3 条件は，互いに同値である。

(1) f は単射である。

(2) f は全射である。

(3) f は全単射である。

証明. (1) $\Rightarrow$ (2) 集合 X の元の個数を n とし，$X = \{a_1, a_2, \cdots, a_n\}$ とすると，

$$f(X) = \{f(a_1), f(a_2), \cdots, f(a_n)\}$$

である。写像 f は単射であるから，元 $f(a_1), f(a_2), \cdots, f(a_n)$ は互いに異なり，集合 $f(X)$ は n 個の要素よりなる。$f(X) \subseteq X$ であるから，等式 $f(X) = X$ が成り立ち，f は全射であることが従う。

(2) $\Rightarrow$ (1) $f(X) = X$ であるから，$\{f(a_1), f(a_2), \cdots, f(a_n)\} = X$ が成り立つ。X の元の個数は n であるので，$i \neq j$ なら $f(a_i) \neq f(a_j)$ であり，f は単射である。 □

$n \geq 1$ を整数とし $X = \{1, 2, 3, \cdots, n\}$，$S_n = \{f \mid f : X \to X$ は全単射である $\}$ とおく。行列の書き方をしたとき，写像 $f : X \to X$ を一つ定めるには

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$$

の空白である $i_1, i_2, i_3, \cdots, i_n$ を，1 から n までの整数で埋めればよい。写像 f を単射にしたければ，$i_1, i_2, i_3, \cdots, i_n$ を $1, 2, 3, \cdots, n$ の順列にすれば十分であって，このとき f は自動的に全射となる。$1, 2, 3, \cdots, n$ の順列の個数は丁度 $n!$ 個あるので，集合 S_n は $n!$ 個の要素よりなる。即ち

系 3.15. $n \geq 1$ を整数とし $X = \{1, 2, 3, \cdots, n\}$，$S_n = \{f \mid f : X \to X$ は全単射である $\}$ とおくと，集合 S_n は $n!$ 個の要素よりなる。

3.4 写像の合成

定義 3.16. (1) A, B, C は空でない集合とし，$f : A \to B$, $g : B \to C$ は写像とする。集合 A の各元 a に $g(f(a))$ を対応させることによって定まる集合 A から集合 C への写像を，f と g

の合成といい，$g{\cdot}f$ と書く。 即ち，$g{\cdot}f : A \to C$ であり，$(g{\cdot}f)(a) = g(f(a))$ が全ての $a \in A$ について成り立つ。

(2) A は空でない集合とする。集合 A の各元 $a \in A$ に対し a 自身を対応させることによって定まる集合 A から集合 A への写像を，A 上の恒等写像といい，1_A と書く。即ち，$1_A : A \to A$ であり，$1_A(a) = a$ が全ての $a \in A$ について成り立つ。

1_A は全単射である。

例えば，$A = \{1, 2, 3\}$，$B = \{4, 5, 6, 7\}$，$C = \{8, 9, 10\}$ とし，写像 $f : A \to B$, $g : B \to C$ を

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 6 & 7 \end{pmatrix}, \quad g = \begin{pmatrix} 4 & 5 & 6 & 7 \\ 8 & 8 & 10 & 9 \end{pmatrix}$$

とすれば，写像 $g{\cdot}f : A \to C$ は

$$g{\cdot}f = \begin{pmatrix} 1 & 2 & 3 \\ 8 & 10 & 9 \end{pmatrix}$$

となる。このような行列の形に書けば,

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

である。

写像 $f, g : \mathbb{R} \to \mathbb{R}$ をそれぞれ $f(a) = a^2 - 1$, $g(a) = 2a + 5$ とすれば，合成写像 $g{\cdot}f : \mathbb{R} \to \mathbb{R}$ は $(g{\cdot}f)(a) = g(f(a)) = 2(a^2 - 1) + 5 = 2a^2 + 3$ となる。

問題 3.17. $A = \{1, 2, 3, 4, 5\}$ とする。A から A への写像 f, g, h を次のように定める。

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}, h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

合成 $fg, fh, (fg)h, f(gh)$ を求めよ。

証明.

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix},$$

$$fh = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$$

である。 □

問題 3.18. S_3 の元をすべて書きだし，それらを合成せよ。

証明. $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$ である。$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ とおき，合成の表

左下 × 右上	e	a	b	c	f	g
e						
a			g		c	
b						
c						
f						e
g					e	f

を作る。$ab = g$, $af = c$ であるので，升目を g, c で埋める。以下同様である。 □

問題 3.19. A, B, C は空でない集合とし，$f : A \to B$, $g : B \to C$ を写像とする。次の主張が正しいことを確かめよ。

(1) 任意の $X \subseteq A$ に対し，$(gf)(X) = g(f(X))$ が成り立つ。

(2) 任意の $Y \subseteq C$ に対し，$(gf)^{-1}(Y) = f^{-1}(g^{-1}(Y))$ が成り立つ。

(3) f が単射なら，任意の $X_1, X_2 \subseteq A$ に対し，等式 $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ が成り立つ。

定理 3.20. A, B, C は空でない集合とし，$f : A \to B$, $g : B \to C$ を写像とすると，次の主張が正しい。

(1) f, g がどちらも単射なら，合成 gf も単射である。

(2) f, g がどちらも全射なら，合成 gf も全射である。

(3) 合成 gf が単射なら，f は単射である。

(4) 合成 gf が全射なら，g は全射である。

証明. (1) $a_1, a_2 \in A$ が等式 $(gf)(a_1) = (gf)(a_2)$ を満たすなら，$g(f(a_1)) = g(f(a_2))$ である。写像 g は単射であるから，$f(a_1) = f(a_2)$ となり，f も単射であるので $a_1 = a_2$ となって，合成写像 gf も単射であることが従う。

(2) $(gf)(A) = g(f(A)) = g(B) = C$ による。次のように考えてもよい。任意に $c \in C$ を取れ。すると，写像 g は全射であるから，ある $b \in B$ が存在し等式 $c = g(b)$ が成り立つ。写像 f は全射であるから，この $b \in B$ に対し，何かある $a \in A$ が存在して等式 $b = f(a)$ が成り立つ。故に

$$c = g(b) = g(f(a)) = (gf)(a)$$

であるから，いかなる $c \in C$ に対しても，何かある $a \in A$ が存在して等式 $c = (gf)(a)$ が成り立つ。即ち合成写像 gf は全射である。

(3) $a_1, a_2 \in A$ が等式 $f(a_1) = f(a_2)$ を満たすとせよ。すると，$g(f(a_1)) = g(f(a_2))$ であるので，$(gf)(a_1) = (gf)(a_2)$ が成り立つ。写像 gf は単射であるから $a_1 = a_2$ となり，故に，写像 f は単射である。

(4) $C = (gf)(A) = g(f(A)) \subseteq g(B) \subseteq C$ による。次のように考えてもよい。任意に $c \in C$ を取れ。すると，写像 gf は全射であるから，ある $a \in A$ が存在し等式 $c = (gf)(a)$ が成り立つ。$b = f(a)$ とおけば，$c = (gf)(a) = g(f(a)) = g(b)$ であるから，いかなる $c \in C$ に対しても，何かある $b \in B$ が存在して等式 $c = g(b)$ が成り立つ。即ち写像 g は全射である。 □

系 3.21. A, B は空でない集合とし，$f : A \to B$, $g : B \to A$ は写像とする。もし $gf = 1_A, fg = 1_B$ ならば，f も g も必ず全単射である。

問題 3.22. (1) 合成 gf は単射であるが，g は単射ではないという例を作れ。

(2) 合成 gf は全射であるが，f は全射ではないという例を作れ。

命題 3.23. A, B, C, D は空でない集合とし，$f : A \to B$, $g : B \to C$, $h : C \to D$ は写像とする。次の等式が成り立つ。

(1) $(hg)f = h(gf)$

(2) $1_B \cdot f = f$

(3) $f \cdot 1_A = f$

証明. (1) $(hg)f, h(gf)$ はどちらも集合 A から集合 C への写像である。$a \in A$ をとれば，$(hg)(f(a)) = h(g(f(a))), (h(gf))(a) = h((gf)(a)) = h(g(f(a)))$ であるので，等式 $((hg)f)(a) = (h(gf))(a)$ が成り立つ。故に $(hg)f = h(gf)$ である。

(2) $1_B \cdot f, f$ はどちらも A から B への写像である。$a \in A$ とせよ。$(1_B \cdot f)(a) = 1_B(f(a)) = f(a)$ であるから，等式 $1_B \cdot f = f$ が成り立つ。

(3) (2) と同様である。

□

3.5 逆写像

定理 3.24. A, B は空でない集合とし，$f : A \to B$ は写像とする。このとき，写像 f に関する次の条件は，互いに同値である。

(1) f は全単射である。

(2) ある写像 $g : B \to A$ が存在し，等式 $gf = 1_A, fg = 1_B$ が成り立つ。

写像 f が全単射であるならば，この定理の条件 (2) に現れる写像 $g : B \to A$ は，f に対し一意的に定まる。この g を f の逆写像といい，$g = f^{-1}$ と書く（f-inverse と読む）。即ち，逆写像 f^{-1} は B から A への写像であって，等式 $ff^{-1} = 1_B$, $f^{-1}f = 1_A$ を満たす。

証明. (1) $\Rightarrow$ (2) $b \in B$ を取る。写像 f は全射であるから，$a \in A$ であって $b = f(a)$ となるものが，少なくとも一つは存在する。$a_1, a_2 \in A$ が等式 $b = f(a_1)$, $b = f(a_2)$ を満たすなら，

$f(a_1) = f(a_2)$ であり，写像 f は単射であるので，等式 $a_1 = a_2$ が得られる。即ち，$b \in B$ を与えたとき，$b = f(a)$ となる $a \in A$ は，元 b に対して唯一通りに定まる。故に写像 $g : B \to A$ を $g(b) = a$ と定めれば，$g(f(a)) = a$ が全ての $a \in A$ に対して成り立ち，また，いかなる $b \in B$ に対しても $f(g(b)) = b$ であるので，等式 $fg = 1_B$, $gf = 1_A$ が成り立つ。

(2) $\Rightarrow$ (1) 系 3.21 に従う。

さて，$g, g' : B \to A$ であって $gf = g'f = 1_A$, $fg = fg' = 1_B$ が成り立つと仮定せよ。すると，$g = g1_B = g(fg') = (gf)g' = 1_A g' = g'$ であるから，等式 $g = g'$ が得られる。故に，条件 (2) を満たす写像 $g : B \to A$ は f に対し唯一つ定まる。 □

$n \geq 1$ を整数とし，$X = \{1, 2, \cdots, n\}$，$f \in S_n$ とせよ。$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$ とすれば，$i_1, i_2, \cdots, i_n$ は $1, 2, \cdots, n$ の順列である。f^{-1} は i_1 を 1 に，i_2 を 2 に，$\cdots$, i_n を n に対応させるような，X から X への写像である。従って，行列の形で書くと，$f^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$，即ち

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

となる。例えば $n = 5$ で $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$ なら

$$f^{-1} = \begin{pmatrix} 5 & 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

である。実際に確かめれば

$$f^{-1}f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1_X$$

であることが，納得される。

問題 3.25. S_3 の元に対し，その逆写像を求め，それらがすべて S_3 の元であることを確かめよ。

証明. 表 3.18 を用いてもよいが，例えば $f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = g$ である。$e^{-1} = e$, $a^{-1} = a$ で，他も同様である。 □

系 3.26. A, B は空でない集合とし，$f : A \to B$ は写像とする。次の主張が正しい。

(1) $1_A^{-1} = 1_A$ である。

(2) f が全単射であれば，その逆写像 f^{-1} も全単射であり，等式 $(f^{-1})^{-1} = f$ が成り立つ。

証明. 等式 $1_A 1_A = 1_A$ と $ff^{-1} = 1_B$, $f^{-1}f = 1_A$ が成り立つからである。 □

系 3.27. A, B, C は空でない集合とし，$f : A \to B$, $g : B \to C$ を写像とする。f, g が全単射ならば，合成写像 $gf : A \to C$ も全単射であって，等式 $(gf)^{-1} = f^{-1}g^{-1}$ が成り立つ。

証明. 写像 gf が全単射であることは，定理 3.20 に従う。$f^{-1} : B \to A$, $g^{-1} : C \to B$ であるので，合成 $f^{-1}g^{-1}$ は C から A への写像である。写像の合成に関する結合法則 3.23(1) によれば

$$(gf)(f^{-1}g^{-1}) = ((gf)f^{-1})g^{-1} = (g(ff^{-1}))g^{-1} = (g1_B)g^{-1} = gg^{-1} = 1_C$$

であって

$$(f^{-1}g^{-1})(gf) = ((f^{-1}g^{-1})g)f = (f^{-1}(g^{-1}g))f = (f^{-1}1_B)f = f^{-1}f = 1_A$$

であるから，定理 3.24 によって，等式 $(gf)^{-1} = f^{-1}g^{-1}$ が得られる。 □

4 群のモデルとしての対称群 S_n

4.1 置換

X は空でない集合とし，$S_X = \{f \mid f : X \to X$ は全単射である $\}$ とおくと，S_X は写像の合成を演算に群をなす。ここでは X が有限集合の場合を解析し，群のモデルとしての対称群 S_n の構造を述べたいと思う。

$n \geq 1$ を整数とし，$X = \{1, 2, \cdots, n\}$ とし，$S_n = \{f \mid f : X \to X$ は全単射である $\}$ とおく。集合 S_n は $n!$ 個の元よりなる。

S_n の元は $1, 2, \cdots, n$ の順列に対応するので，S_n の元を n 文字の置換といい，S_n を n 次の対称群と呼ぶことが多い。置換は σ, τ, ρ のようなギリシャ文字で表すのが普通である。$\sigma, \tau \in S_n$ としたとき，合成写像 $\sigma\tau$ を σ と τ の積と呼ぶ。$\sigma\tau \in S_n$ であるから，集合 S_n 内では「かけ算」ができるのである。

次の主張が正しい。

命題 4.1. $\sigma, \tau, \rho \in S_n$ とする。

(1) 等式 $(\sigma\tau)\rho = \sigma(\tau\rho)$ が成り立つ。

(2) $e = 1_X$ とおくと，$e \in S_n$ であって，等式 $\sigma e = e\sigma = \sigma$ が成り立つ。

(3) $\sigma^{-1} \in S_n$ であって，等式 $\sigma\sigma^{-1} = \sigma\sigma^{-1} = e$ が成り立つ。

問題 4.2. $\sigma, \tau, \rho \in S_n$ とする。次の主張を証明せよ。

(1) $\sigma\tau = \sigma\rho$ なら，$\tau = \rho$ である。

(2) $\tau\sigma = \rho\sigma$ なら，$\tau = \rho$ である。

(3) $\sigma\tau = e$ なら，$\tau = \sigma^{-1}, \sigma = \tau^{-1}$ である。

証明. $\sigma^{-1}(\sigma\tau) = (\sigma^{-1}\sigma)\tau = e\tau = \tau$, $(\tau\sigma)\sigma^{-1} = \tau(\sigma\sigma^{-1}) = \tau e = \tau$ を用いよ。 □

$\sigma \in S_n$ とし，σ を行列

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

の形に書くとき，$\sigma(i) = i$ となる文字 i は省略する。例えば

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 5 & 2 & 4 \end{pmatrix}$$

であれば，$1, 3$ を省き，単に

$$\sigma = \begin{pmatrix} 2 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 \end{pmatrix}$$

と書く。更に

$$\sigma = \begin{pmatrix} 2 & 6 & 4 & 5 \\ 6 & 4 & 5 & 2 \end{pmatrix}$$

であって，この σ は $2 \mapsto 6 \mapsto 4 \mapsto 5 \mapsto 2$ と動かしているのであるから，この順序だけ書いてあれば σ が何であるかが分るので，単に $\sigma = (2, 6, 4, 5)$ と書くことにする。従って $n = 10$ のとき $\sigma = (9, 2, 5, 7, 10, 8)$ とおけば

$$\sigma = \begin{pmatrix} 9 & 2 & 5 & 7 & 10 & 8 \\ 2 & 5 & 7 & 10 & 8 & 9 \end{pmatrix}$$

のことであり，省略されている文字も書けば

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 5 & 3 & 4 & 7 & 6 & 10 & 9 & 2 & 8 \end{pmatrix}$$

となる。より一般に $\sigma = (a_1, a_2, \cdots, a_r)$ と書けば

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_{r-1} & a_r \\ a_2 & a_3 & \cdots & a_r & a_1 \end{pmatrix}$$

のことであって，この表現の中に現れていない文字は，σ によって動かされていない。(勿論，$r \geq 1$ であり，$a_1, a_2, \cdots, a_r$ は1から n までの異なる文字とする。特に $(1) = (2) = \cdots = (n) = e$ である。) このような置換 $(a_1, a_2, \cdots, a_r)$ を長さ r の巡回置換といい，$(2, 6) = \begin{pmatrix} 2 & 6 \\ 6 & 2 \end{pmatrix}$ のように，長さ 2 の巡回置換 (a, b) $(1 \leq a, b \leq n, a \neq b)$ を互換と呼ぶ。

$\sigma_1, \sigma_2, \cdots, \sigma_\ell \in S_n$ に対し

$$\sigma_1\sigma_2\cdots\sigma_\ell = (\cdots((\sigma_1\sigma_2)\sigma_3)\cdots)\sigma_\ell$$

と定める。即ち $\sigma_1\sigma_2\sigma_3 = (\sigma_1\sigma_2)\sigma_2$，$\sigma_1\sigma_2\sigma_3\sigma_4 = (\sigma_1\sigma_2\sigma_3)\sigma_4$ であって，$\ell \geq 2$ なら等式 $\sigma_1\sigma_2\cdots\sigma_\ell = (\sigma_1\sigma_2\cdots\sigma_{\ell-1})\sigma_\ell$ が成り立つ。

問題 4.3. $\sigma_1, \sigma_2, \cdots, \sigma_\ell, \tau_1, \tau_2, \cdots, \tau_m \in S_n$ とすれば等式

$$(\sigma_1\sigma_2\cdots\sigma_\ell)(\tau_1\tau_2\cdots\tau_m) = \sigma_1\sigma_2\cdots\sigma_\ell\tau_1\tau_2\cdots\tau_m$$

が成り立つ。

証明. m に関する数学的帰納法による。定義により $\sigma_1\sigma_2\cdots\sigma_\ell\tau_1 = (\sigma_1\sigma_2\cdots\sigma_\ell)\tau_1$ であることに注意せよ。 □

$\sigma \in S_n$ とせよ。$\sigma^0 = e$ と定め, σ を ℓ 回掛けて得られる S_n の元を σ^ℓ と書く。即ち，$\sigma^1 = \sigma$, $\sigma^2 = \sigma\sigma$, $\sigma^3 = \sigma^2\sigma$ であって，$\sigma^\ell = \sigma^{\ell-1}\sigma$ $(\ell \geq 1)$ が成り立つ。負の整数 $\ell < 0$ に対しては, $\sigma^\ell = (\sigma^{-1})^{-\ell}$ と定める。

問題 4.4. $\sigma \in S_n$ とする。次の主張が正しいことを確かめよ。

(1) 等式 $\sigma^{-1}\sigma^\ell = \sigma^{\ell-1}$ $(\ell \geq 1)$ が成り立つ。

(2) 任意の整数 ℓ, m に対し等式 $\sigma^\ell\sigma^m = \sigma^{\ell+m}$, $(\sigma^m)^\ell = \sigma^{\ell m}$ が成り立つ。

証明. (1) ℓ に関する数学的帰納法による。$\ell \geq 2$ であって $\ell - 1$ までこの等式が正しいと仮定してよいので,

$$\sigma^{-1}\sigma^\ell = \sigma^{-1}(\sigma^{\ell-1}\sigma) = (\sigma^{-1}\sigma^{\ell-1})\sigma = \sigma^{\ell-2}\sigma = \sigma^{\ell-1}$$

が成り立つ。

(2) 難しくはないが，かなり面倒くさい。 □

補題 4.5. $\sigma \in S_n$, $i \in X$ とせよ。このとき，必ずある整数 $\ell \geq 1$ が存在して，等式 $\sigma^\ell(i) = i$ が成り立つ。

証明. $X_\sigma = \{\sigma^\ell(i) \mid 1 \leq \ell \in \mathbb{Z}\}$ とおくと，$X_\sigma \subseteq X$ であるから，X_σ は有限集合である。故に，整数 $1 \leq k < m$ を取って，等式 $\sigma^k(i) = \sigma^m(i)$ が成り立つようにできる。従って $\sigma^{-1}(\sigma^k(i)) = \sigma^{-1}(\sigma^m(i))$ であるが, $\sigma^{-1}(\sigma^k(i)) = (\sigma^{-1}\sigma^k)(i) = \sigma^{k-1}(i)$ であって $\sigma^{-1}(\sigma^m(i)) = (\sigma^{-1}\sigma^m)(i) = \sigma^{m-1}(i)$ であるから，k, m を両方とも 1 づつ減らしながら，等式 $\sigma^{m-k}(i) = i$ が得られる。$\ell = m - k$ が求める整数である。 □

問題 4.6. $\sigma \in S_n$ とせよ。このとき，必ずある整数 $\ell \geq 1$ が存在して，等式 $\sigma^\ell = e$ が成り立つことを確かめよ。

証明. 補題 4.5 の議論を用いよ。 □

命題 4.7. 全ての置換は幾つかの巡回置換の積として表される。即ち，$\sigma \in S_n$ とすれば，σ は必ず

$$\sigma = (a_1, a_2, \cdots, a_r)(b_1, b_2, \cdots, b_s)\cdots(c_1, c_2, \cdots, c_t)$$

のような形に表される。

証明. $\sigma \in S_n$ に対し $I(\sigma) = \{i \mid i \in X$ であって$\sigma(i) \neq i\}$ とおく。即ち，$I(\sigma)$ は，置換 σ によって動いてしまうような文字 i の全体からなる集合である。さて，この命題 4.5 が正しくないと仮定せよ。すると，上のような形には決して表されないような $\sigma \in S_n$ が存在する筈である。このような σ の中から集合 $I(\sigma)$ の要素の個数が最小のものを選び，あらためてそれを σ とする。すると，$e = (1)$ であるから，$\sigma \neq e$ である。故に $I(\sigma) \neq \emptyset$ である。$i \in I(\sigma)$ を一つ取って固定し，整数 $\ell \geq 1$ を $\sigma^\ell(i) = i$ が成り立つように取る (補題 4.5 参照)。このような等式 $\sigma^\ell(i) = i$ を成り立たせるような整数 $\ell \geq 1$ を，文字 i に対し最小に選べば，$\sigma(i) \neq i$ であるから $\ell \geq 2$ であって，しかも文字の列 $i = \sigma^0(i), \sigma(i), \sigma^2(i), \cdots, \sigma^{\ell-1}(i)$ はどの 2 つも異なる。実際, $\sigma^m(i) = \sigma^k(i)$ $(0 \leq m < k \leq \ell - 1)$ であったならば，補題 4.5 の証明と全く同じ理由で，等式 $\sigma^{k-m}(i) = i$ が導かれるが，$1 \leq k - m < \ell$ であるので，この等式 $\sigma^{k-m}(i) = i$ は整数 ℓ の取り方に反するからである。$\tau = (i, \sigma(i), \sigma^2(i), \cdots, \sigma^{\ell-1}(i))$ とおき，$\rho = \sigma\tau^{-1}$ とせよ。すると，$\rho(i) = i$ であるから，$i \notin X(\rho)$ である。一方で，$j \notin X(\sigma)$ ならば，$\sigma(j) = j$ であるので，$j \neq i, \sigma(i), \sigma^2(i), \cdots, \sigma^{\ell-1}(i)$ である。故に $\tau(j) = j$ であるので，$\tau^{-1}(j) = j$ が成り立つ。従って $\rho(j) = (\sigma\tau^{-1})(j) = \sigma(\tau^{-1}(j)) = \sigma(j) = j$ が得られる。即ち，$X(\rho) \subseteq X(\sigma)$ であって，かつ $i \notin X(\rho)$ であるから，集合 $X(\rho)$ の要素の個数は集合 $X(\sigma)$ の要素の個数より真に小さい。故に σ の選び方によって，置換 ρ は

$$\rho = (a_1, a_2, \cdots, a_r)(b_1, b_2, \cdots, b_s)\cdots(c_1, c_2, \cdots, c_t)$$

のような形に表されるはずである。しかしながら $\sigma = \rho\tau$ であるので，等式

$$\sigma = (a_1, a_2, \cdots, a_r)(b_1, b_2, \cdots, b_s)\cdots(c_1, c_2, \cdots, c_t)(i, \sigma(i), \sigma^2(i), \cdots, \sigma^{\ell-1}(i))$$

が得られ，σ も正しい形に表されることになる。これは σ がそのような表現を持たないという仮定に反する。故に命題 4.5 は正しい主張である。 □

問題 4.8. 全ての置換は幾つかの共通文字のない巡回置換の積として表されることを証明せよ。即ち，$\sigma \in S_n$ とすれば，σ は必ず

$$\sigma = (a_1, a_2, \cdots, a_r)(b_1, b_2, \cdots, b_s) \cdots (c_1, c_2, \cdots, c_t)$$

のような形に表されるが，このとき巡回置換 $(a_1, a_2, \cdots, a_r), (b_1, b_2, \cdots, b_s), \cdots, (c_1, c_2, \cdots, c_t)$ は，どの 2 つも共通文字を含まないように選べぶことができる。

証明. 命題 4.7 の証明の記号で，巡回置換 $(a_1, a_2, \cdots, a_r), (b_1, b_2, \cdots, b_s), \cdots, (c_1, c_2, \cdots, c_t)$ と $(i, \sigma(i), \sigma^2(i), \cdots, \sigma^{\ell-1}(i))$ は，共通文字を含まないことを示す。 □

補題 4.9. $a_1, a_2, \cdots, a_r \in X$ $(r \geq 2)$ であって，異なる文字とすれば，等式

$$(a_1, a_2, \cdots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \cdots (a_1, a_2)$$

が成り立つ。

証明. $\sigma = (a_1, a_2, \cdots, a_r)$, $\tau = (a_1, a_r)(a_1, a_{r-1}) \cdots (a_1, a_2)$ とおく。$a_1, a_2, \cdots, a_r$ 以外の文字は，σ でも τ でも動かないので，両者による $a_1, a_2, \cdots, a_r$ の像がすべて一致すれば，等式 $\sigma = \tau$ が得られる。a_1 の像は

$$\tau(a_1) = [(a_1, a_r)(a_1, a_{r-1}) \cdots (a_1, a_3)]\,((a_1, a_2)(a_1)) = [(a_1, a_r)(a_1, a_{r-1}) \cdots (a_1, a_3)]\,(a_2) = a_2$$

である。同様に，$\tau(a_i) = a_{i+1}$ $(1 \leq i < r)$ であって，$\tau(a_r) = a_1$ であることが示される。故に $\sigma = \tau$ である。 □

系 4.10. $n \geq 2$ なら，n 文字のいかなる置換も，幾つかの互換の積として表される。

問題 4.11. 置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 5 & 4 & 2 & 7 & 8 & 1 & 9 & 3 & 6 \end{pmatrix}$$

を互換の積として表せ。

4.2　置換の符号

次の主張が正しい。

定理 4.12. $n \geq 2$ とする。与えられた n 文字の置換を幾つかの互換の積として表したとき，偶数個の互換の積として表されるか，それとも奇数個の互換の積として表されるかはその置換のみで定まり，表現の仕方には依存しない。

証明には置換の符号を用いる。

定義 4.13. $\sigma \in S_n$ に対し

$$\varepsilon(\sigma) = \begin{cases} \prod_{i<j} \dfrac{\sigma(j)-\sigma(i)}{j-i} & (n \geq 2 \text{ のとき}) \\ 1 & (n = 1 \text{ のとき}) \end{cases}$$

とおき，置換 σ の符号と呼ぶ。但し $\prod$ は「積」を表す記号である。

命題 4.14. 次の主張が正しい。

(1) $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$

(2) $\varepsilon(\sigma) = 1$ または $\varepsilon(\sigma) = -1$ である。

(3) σ が互換であれば，$\varepsilon(\sigma) = -1$ である。

(4) $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$

証明. $n \geq 2$ としてよいであろう。$\varepsilon(\sigma)^2 = \displaystyle\prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i} \cdot \prod_{j<i} \frac{\sigma(j)-\sigma(i)}{j-i}$ であるから

$$\varepsilon(\sigma)^2 = \frac{\prod_{i<j}(\sigma(j)-\sigma(i)) \cdot \prod_{j<i}(\sigma(j)-\sigma(i))}{\prod_{i<j}(j-i) \cdot \prod_{j<i}(j-i)}$$

となり

$$\varepsilon(\sigma)^2 = \frac{\prod_{i \neq j}(\sigma(j)-\sigma(i))}{\prod_{i \neq j}(j-i)} = 1$$

が得られる。故に $\varepsilon(\sigma) = 1$ または $\varepsilon(\sigma) = -1$ である。

$$\varepsilon(\sigma\tau) = \prod_{i<j} \left[\frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \frac{\tau(j)-\tau(i)}{j-i} \right]$$

であるので

$$\varepsilon(\sigma\tau) = \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma)\varepsilon(\tau)$$

が得られる。$\sigma = (a, b)$ $(1 \leq a < b \leq n)$ ならば，$\varepsilon(\sigma)$ の符号は，1 から n までの整数の組 (i, j) であって，$i < j$ であるにも拘わらず $\sigma(j) < \sigma(i)$ となるものの個数で定まる。このような組 (i, j) は全部で奇数 $2(b-a)-1$ 個あるから，$\varepsilon(\sigma) = -1$ である。(1) より $\varepsilon(\sigma\sigma^{-1}) = \varepsilon(\sigma)\varepsilon(\sigma^{-1})$ であって，$\varepsilon(e) = 1$ であるから，$\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ が成り立つ。以上が (1), (2), (3), (4) の証明である。 □

証明. さて定理 4.12 を証明しよう。与えられた置換 σ を $\sigma = \sigma_1\sigma_2\cdots\sigma_\ell$ (σ_i は互換) という形で表せば，(1) と (3) より，等式 $\varepsilon(\sigma) = \prod_{i=1}^{\ell} \varepsilon(\sigma_i) = (-1)^\ell$ が得られる。故に，互換 σ_i の個数 ℓ が偶数であるか奇数であるかは，$\sigma = \sigma_1\sigma_2\cdots\sigma_\ell$ という表現の仕方には拠らず，σ のみで決まることが分る。 □

問題 4.15. 置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 5 & 4 & 2 & 7 & 8 & 1 & 9 & 3 & 6 \end{pmatrix}$$

の符号を求めよ。

4.3 行列式

n 次の正方行列

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \cdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

に対し

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

とおき，これを A の行列式という。

4.4 偶置換と奇置換

$\varepsilon(\sigma) = 1$ であるとき，置換 σ は偶置換であるといい，$\varepsilon(\sigma) = -1$ であるとき，奇置換であるという。$A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$，$B_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = -1\}$ とおく。$e \in A_n$ である。$B_1 = \emptyset$ であるが，$n \geq 2$ なら，$(1,2) \in B_n$ であるから，$B_n \neq \emptyset$ である。

命題 4.16. 次の主張が正しい。

(1) $\sigma, \tau \in A_n$ なら，$\sigma\tau \in A_n$ である。

(2) $\sigma, \tau \in B_n$ なら，$\sigma\tau \in A_n$ である。

(3) $n \geq 2$ なら，集合 A_n と B_n の要素の個数は，$\frac{n!}{2}$ に等しい。

証明. (3) $\rho = (1,2)$ とせよ。$\rho^2 = e$ であるから，任意の $\sigma \in S_n$ に対し，等式 $(\sigma\rho)\rho = \sigma(\rho\rho) = \sigma e = \sigma$ が成り立つ。故に，$\sigma_1\rho = \sigma_2\rho$ なら，$\sigma_1 = \sigma_2$ である。さて，$\sigma \in A_n$ なら $\sigma\rho \in B_n$ であって，$\tau \in B_n$ なら $\tau\rho \in A_n$ である。写像 $f : A_n \to B_n$, $g : B_n \to A_n$ を，$f(\sigma) = \sigma\rho$, $g(\tau) = \tau\rho$ と定めれば，f, g は単射であるので，集合 A_n と B_n は同じ個数の要素よりなることがわかる。$S_n = A_n \cup B_n$ であって $A_n \cap B_n = \emptyset$ であるから，集合 A_n と B_n の要素の個数は $\frac{n!}{2}$ である。 □

問題 4.17. 集合 A_2, A_3, A_4 の元をすべて書き出せ。

証明. A_4 は次の 12 個の置換よりなる。

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4, & 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$$
$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

□

定理 4.18. $\emptyset \neq H \subseteq S_n$ であり，任意の $\sigma, \tau \in H$ に対し $\sigma\tau \in H$ が成り立つとする。このとき次の主張が正しい。

(1) $e \in H$ である。

(2) $\sigma \in H$ なら，$\sigma^{-1} \in H$ である。

(3) $\sigma, \tau \in H$ なら，$\sigma\tau^{-1} \in H$ である。

(4) $\sigma, \tau \in S_n$ とせよ。$R = \{(\sigma, \tau) \in S_n \times S_n \mid \sigma^{-1}\tau \in H\}$ とおけば，R は集合 S_n 上の同値関係である。

(5) この同値関係 R に関する $\sigma \in S_n$ を含む類を $C(\sigma)$ とすれば，等式 $C(\sigma) = \{\sigma\tau \mid \tau \in H\}$ が成り立つ。

(6) 任意の $\sigma \in S_n$ に対し，集合 $C(\sigma)$ は，集合 H と同じ個数の要素よりなる。

(7) 集合 H の要素の個数を m とすれば，m は $n!$ の約数である。

証明. (1), (2) $\sigma \in H$ とし，写像 $f_\sigma : H \to H$ を $f_\sigma(\tau) = \sigma\tau$ と定めれば，f_σ は単射である。実際，$f_\sigma(\tau_1) = f_\sigma(\tau_2)$ なら，$\sigma\tau_1 = \sigma\tau_2$ であるから，問題 4.2 より，$\tau_1 = \tau_2$ が得られる。故に，H は有限集合で写像 f_σ は単射であるから，f_σ は全射でもあり，$\sigma \in H$ に対して $f_\sigma(\tau) = \sigma$ を満たす $\tau \in H$ が必ず存在する。$\sigma = \sigma\tau$ であるので，両辺に左から σ^{-1} を掛けることによって，$\tau = e$ が得られる。即ち $e \in H$ である。故に，写像 f_σ は全射であるから，$f_\sigma(\rho) = e$ となる $\rho \in H$ が存在するが，このとき $\sigma\rho = e$ であるから，問題 4.2 より $\rho = \sigma^{-1}$ であることがわかる。故に $\sigma^{-1} \in H$ である。

(3) (2) より $\tau^{-1} \in H$ であるから，$\sigma\tau^{-1} \in H$ となる。

(4) $\sigma, \tau, \rho \in S_n$ とせよ。$\sigma^{-1}\sigma = e \in H$ であるから，$\sigma R \sigma$ である。$\sigma R \tau$ なら，$\sigma^{-1}\tau \in H$ であるから，$(\sigma^{-1}\tau)^{-1} \in H$ である。$(\sigma^{-1}\tau)^{-1} = \tau^{-1}(\sigma^{-1})^{-1}$ であって $(\sigma^{-1})^{-1} = \sigma$ であるから，$\tau^{-1}\sigma \in H$ であり，$\tau R \sigma$ が得られる。$\sigma R \tau, \tau R \rho$ なら，$\sigma^{-1}\tau \in H$, $\tau^{-1}\rho \in H$ であるから $\sigma^{-1}\rho = (\sigma^{-1}\tau)(\tau^{-1}\rho) \in H$ となり，$\sigma R \rho$ である。故に，R は S_n 上の同値関係である。

(5) $\sigma H = \{\sigma\tau \mid \tau \in H\}$ とおく。$C(\sigma) = \{x \in S_n \mid \sigma^{-1}x \in H\}$ である。$x \in C(\sigma)$ なら，$\tau = \sigma^{-1}x$ とおけば，$\tau \in H$ であって，しかも両辺に左から σ を掛けることによって，等式 $x = \sigma\tau$ が得られる。故に $x \in \sigma H$ である。逆に，$x \in \sigma H$ を取り，$x = \sigma\tau$ $(\tau \in H)$ と表せば，$\sigma^{-1}x = \tau \in H$ より，$\sigma R x$ となる。R は S_n 上の同値関係であるから，$xR\sigma$ も成り立ち，$x \in C(\sigma)$ が得られる。故に $C(\sigma) = \sigma H$ である。

(6) 写像 $g : H \to C(\sigma) = \sigma H$, $g(\tau) = \sigma\tau$ が，全単射であることによる。

(7) 商集合 S_n/R の元の個数を ℓ とすれば，S_n/R は S_n のクラス分けであって，(6) によってどのクラスも同じ個数 m の元よりなるので，S_n 全体の個数 $n!$ は $m\ell$ に等しい。故に m は，$n!$ の約数である。 □

問題 4.19. S_3 の部分集合 H で，$H \neq \emptyset$ であって，かつ任意の $\sigma, \tau \in H$ に対し $\sigma\tau \in H$ となるものを全て見つけよ。

5 環

5.1 演算

しばらくの間，A は空でない集合とする。

定義 5.1. 直積集合 $A \times A$ から A への写像 $\mu : A \times A \to A$ を集合 A 上の**演算**という。

即ち，集合 A 上の演算とは「A の元の組 (a, b) を与えるごとに，この a, b を材料に A の元 c を新たに一つ作る規則」のことである。集合 A 上の演算 $\mu : A \times A \to A$ を一つ固定してものを考えるときは，簡単のため，A の元の与えられた組 (a, b) から新たに得られる A の元

$c = \mu(a,b)$ を，単に $c = ab$ (或いは $c = a + b,\ c = a * b$ などの記号) で表し，a カケル b と読むことが多い。

ベクトルの和を考えよう。$A = \mathbb{R}^3$ とする。$a, b \in A$ なら，a, b は 3 次の実ベクトルであるから，

$$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

$(a_i, b_i \in \mathbb{R})$ という形に表すことができる。すると $a_1 + b_1, a_2 + b_2, a_3 + b_3 \in \mathbb{R}$ であるから，これらを並べて新しい 3 次の実ベクトル $\begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}$ が得られる。即ち，$a, b \in A$ を与えるごとに，この a, b を材料に新たに A の元を一つ作る規則

$$\mu : A \times A \to A, \quad (\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}) \mapsto \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}$$

が得られる。このベクトル $\begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}$ を $a + b$ と書き，a, b の和と呼ぶ。即ち

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}$$

である。これがベクトルの和の定義であり，ベクトルの「和」は集合 $A = \mathbb{R}^3$ 上の演算（の一つ）である。

例 5.2. $n \geq 1$ は整数とすると，任意の $\sigma, \tau \in S_n$ に対し合成写像 $\sigma\tau$ は S_n の元であるから，写像の合成は集合 S_n 上に演算を定め，**この演算に関して S_n は群になる**。

「代数学 2」で学んでいるはずであるが，念のために，群の定義を思い出しておこう。

問題 5.3. 上に定めた和 $+$ について集合 $\mathbb{R}^3$ はアーベル群をなすこと，即ち次の主張が正しいことを確かめよ。

(1) （結合法則）$\forall a, b, c \in \mathbb{R}^3$ に対し，等式 $(a + b) + c = a + (b + c)$ が成り立つ。

(2) （交換法則)）$\forall a, b \in \mathbb{R}^3$ に対し，等式 $a + b = b + a$ が成り立つ。

(3) （単位元の存在）等式 $a + 0 = 0 + a = a$ を，$\forall a \in \mathbb{R}^3$ に対して成り立たせるような元 $0 \in \mathbb{R}^3$ が，$\mathbb{R}^3$ 内に少なくとも 1 つ含まれている。

(4) （単位元の一意性）条件 (3) を満たす元 $0 \in \mathbb{R}^3$ は，$\mathbb{R}^3$ 内で一意的に定まり，$\mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ に等しい。

(5) （逆元の存在）$a \in \mathbb{R}^3$ とすれば，$a + x = x + a = 0$ を満たすような元 $x \in \mathbb{R}^3$ が，$\mathbb{R}^3$ 内に少なくとも一つは含まれている。

(6) （逆元の一意性）条件 (5) を満たす $x \in \mathbb{R}^3$ は，元 $a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \in \mathbb{R}^3$ に対し一意的に定まり，$-a = \begin{pmatrix} -a_1 \\ -a_2 \\ -a_3 \end{pmatrix}$ に等しい。

問題 5.4. X は空でない集合とし，$S_X = \{f \mid f : X \to X$ は全単射である $\}$ とおくと，S_X は写像の合成を演算に群をなす。確かめよ。

問題 5.5. $G = \{(a, b) \mid a, b \in \mathbb{R},\ a \neq 0\}$ とおき，$(a, b)(c, d) = (ac, bc + d)$ によって，集合 G 上に演算を定める。

(1) 集合 G はこの演算に関して群をなす，即ち，次の主張が正しいことを確かめよ。

(1.1) $\forall \alpha, \beta, \gamma \in G$ について，等式 $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ が成り立つ。

(1.2) ある $e \in G$ が存在して，$\forall \alpha \in G$ に対し等式 $\alpha e = e\alpha = \alpha$ が成り立つ。

(1.3) (1.2) の条件を満たす $e \in G$ は，集合 G 内に一意的に定まる。

(1.4) $\alpha \in G$ を与えれば，ある $x \in G$ が存在して等式 $\alpha x = x\alpha = e$ が成り立つ。

(1.5) (1.4) の条件を満たす $x \in G$ は，与えられた元 $\alpha \in G$ に対し一意的に定まる。

(2) $\mathrm{Z}(G) = \{\alpha \in G \mid \alpha x = x\alpha, \forall x \in G\}$ とおく。$\mathrm{Z}(G) = \{e\}$ であることを確かめよ。

(3) (問題 8.16 参照)　体 $\mathbb{R}$ 上の一変数多項式環 $\mathbb{R}[X]$ の $\mathbb{R}$-**自己同型**（環の同型写像 $\sigma : \mathbb{R}[X] \to \mathbb{R}[X]$ で $\mathbb{R}$ の元を動かさないもの）全体が，写像の合成を演算になす群を $\mathrm{Aut}_{\mathbb{R}}\,\mathbb{R}[X]$ で表すと

$$G \cong \mathrm{Aut}_{\mathbb{R}}\,\mathbb{R}[X]$$

である。証明せよ。

5.2　環の定義

定義 5.6. R が**環**であるとは，R は空でない集合であって，集合 R 上に 2 つの演算が定められていて，一方を加法 $+$，他方を乗法 $\times$ の記号で表すとき，次の 4 条件が満たされることをいう。

(1) $+$ について集合 R はアーベル群をなす。即ち，次の主張が正しい。

(1.1) $\forall a, b, c \in R$ に対し，等式 $(a+b)+c = a+(b+c)$ が成り立つ。

(1.2) $\forall a, b \in R$ に対し，等式 $a+b = b+a$ が成り立つ。

(1.3) 等式 $a+0 = 0+a = a$ が，$\forall a \in R$ に対して成り立つような元 $0 \in R$ が，R 内に少なくとも一つは含まれている。

(1.4) $a \in R$ とすれば，$a+x = x+a = 0$ を満たすような元 $x \in R$ が，R 内に少なくとも一つは含まれている。

(2) （乗法の結合法則）$\forall a, b, c \in R$ に対し，等式 $(ab)c = a(bc)$ が成り立つ。

(3) （分配法則）$\forall a, b, c \in R$ に対し，等式 $a(b+c) = ab+ac$，$(a+b)c = ac+bc$ が成り立つ。

(4) （乗法に関する単位元の存在）等式 $a1 = 1a = a$ が，$\forall a \in R$ に対して成り立つような元 $1 \in R$ が，R 内に少なくとも一つは含まれている。

命題 5.7. 定義 5.6 に関し，次の主張が正しい。

(1) 条件 (1.3) を満たす $0 \in R$ は，環 R 内で一意的に定まる。

(2) 条件 (1.4) を満たす $x \in R$ は，環 R 内で元 $a \in R$ に対し一意的に定まる。(これを$-\mathbf{a}$ と書く。)

(3) 条件 (4) を満たす $1 \in R$ は，環 R 内で一意的に定まる。(これを環 R の **単位元**と呼ぶ。)

問題 5.8. 命題 8.4 内の主張が正しいことを確かめよ。

乗法について**交換法則**が成り立つような環（即ち，$\forall a, b \in R$ に対し，等式 $ab = ba$ が成り立つような環）を**可換環**という。

問題 5.9. 次の主張が正しいことを証明せよ。

(1) 集合 $\mathbb{R}^3$ は，次の和と積を演算に，可換環をなすことを確かめよ。

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}, \quad \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_2 b_2 \\ a_3 b_3 \end{pmatrix}.$$

(2) $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ とおくと，可換環 $\mathbb{R}^3$ 内では

$$e_i e_j = \delta_{i,j} e_i \quad (1 \leq i, j \leq 3)$$

が成り立つ。

例 5.10. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は，数の加法と乗法を演算に，可換環をなす。

(2) 整数 $n \geq 1$ に対し，n 次の複素正方行列全体のなす集合を $\mathrm{M}_n(\mathbb{C})$ によって表すと，集合 $\mathrm{M}_n(\mathbb{C})$ は行列の和と積を演算に環をなす。$n \geq 2$ のときは，交換法則が成り立たず，$\mathrm{M}_n(\mathbb{C})$ は可換環ではない。

証明. (2) 例えば $n=2$ のときを考え，$a=\begin{pmatrix}0&1\\0&0\end{pmatrix}, b=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ とすれば

$$ab=\begin{pmatrix}0&0\\0&0\end{pmatrix}=\mathbf{0},\ ba=\begin{pmatrix}0&1\\0&0\end{pmatrix}=a\neq\mathbf{0}$$

であるから，$ab\neq ba$ であり，積に関する交換法則は成り立たない。 □

環 R 内では，$a-b=a+(-b)$ によって，減法を定める。

命題 5.11 (環演算の基本的性質). R は環とする。

(1) $a,b\in R$ について，$a+b=0$ なら，等式 $a=-b,\ b=-a$ が成り立つ。故に，$-0=0$ であり，$\forall a\in R$ に対し，$-(-a)=a$ である。

(2) $a\in R$ のとき，$a+a=a$ なら $a=0$ である。

(3) $\forall a,b,c\in R$ に対し，次の等式が成り立つ。

(3.1) $a0=0a=0$

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

(3.3) $-a=(-1)a$，$(-a)(-b)=ab$

(3.4) $a(b-c)=ab-ac$，$(a-b)c=ac-bc$

問題 5.12. 命題 5.11 内の主張が正しいことを確かめよ。

従って，環 R 内で $1=0$ が成り立てば，いかなる元 $a\in R$ に対しても $a=a1=a0=0$ となり，$R=\{0\}$ を得る。このような環を**零環**と呼ぶ。

以下このテキストで，R が環であると言えば，$1\neq 0$，即ち R は零環ではないものとする。

問題 5.13. $A=\mathbb{Z}\times\mathbb{Q}$ とする。

(1) 集合 A は，次の加法と乗法を演算に，可換環をなすことを確かめよ。

$$(a,x)+(b,y)=(a+b,x+y),\ (a,x)(b,y)=(ab,ay+bx)$$

(2) この環 A の中では，$\forall x,y\in\mathbb{Q}\setminus\{0\}$ について，$(0,x)(0,y)=0$ が成り立つことを確かめよ。

この環 A の中では，$1=(1,0)$，$0=(0,0)$ である。この環 A を $\mathbb{Z}$ 上 $\mathbb{Q}$ のイデアル化と呼ぶ。

問題 5.14.

$$A=\left\{\left.\begin{pmatrix}a & b\\ 0 & a\end{pmatrix}\right| a\in\mathbb{Z},b\in\mathbb{Q}\right\}\ \subseteq\ \mathrm{M}_2(\mathbb{Q})$$

とおくと，A は行列の和と積を演算に可換環をなすことを確かめ，単元群 $A^\times$ を決定せよ。

問題 5.15. X は空でない集合とし，$A=\{f\mid f:X\to\mathbb{R}\}$ とおく。すなわち，A は X 上で定義される実関数の全体よりなる集合である。次の問いに答えよ。

(1) 集合 A は，次の加法と乗法を演算に，可換環をなすことを確かめよ。

$$(f+g)(x)=f(x)+g(x),\ (fg)(x)=f(x)g(x)$$

(2) $X=\mathbb{R}$ とする。各 $n\in\mathbb{Z}$ に対し

$$I_n=\{f\in A\mid f(x)=0,n\leq\forall x\in\mathbb{R}\}$$

とおく。集合 I_n は環 A のイデアルであって，$\forall n\in\mathbb{Z}$ について $I_n\subsetneq I_{n+1}$ となることを確かめよ。（イデアルの定義は 6.4 を見よ。）従って，この環 A は Noether 環ではない。（Noether 環の定義は 11.5 を見よ。）

問題 5.16. $i=\sqrt{-1}$ とし，$A=\{a+bi\mid a,b\in\mathbb{Z}\}$ とする。

(1) 集合 A は，数の和と積を演算に，可換環をなすことを確かめよ。

(2) $\alpha\in A$ に対し，元 $\beta\in A$ が存在して等式 $\alpha\beta=1$ が成り立つという。このような $\alpha\in A$ をすべて求めよ，即ち，集合 $A^\times$ の元をすべて求めよ。（単元群 $A^\times$ については，問題 5.48 を見よ。）

5.3　環の準同型写像と部分環

定義 5.17. S は環とする。S の部分集合 R は次の条件を満たすとき，S の**部分環**であるという。

(1) R は環 S の単位元 1 を含む。

(2) $\forall x, y \in R$ に対し，$x+y, -x, xy \in R$ である。

問題 5.18. R が環 S の部分環であれば，R は環 S の和と積を演算に環をなす（S が可換なら，R も可換である）ことを確かめよ。

問題 5.19. $\mathbb{C}$ 内で $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$，$\mathbb{Q}[\omega] = \{a+bw \mid a, b \in \mathbb{Q}\}$ $(w = \frac{-1+\sqrt{3}i}{2})$ とおけば，$\mathbb{Z}[i]$ と $\mathbb{Q}[\omega]$ は環 $\mathbb{C}$ の部分環である。確かめよ。

以下 R, S は環とする。

定義 5.20. 写像 $f : R \to S$ は次の 2 条件を満たすとき，**環の準同型写像**であるという。

(1) $\forall a, b \in R$ に対し，$f(a+b) = f(a) + f(b)$，$f(ab) = f(a)f(b)$ である。

(2) $f(1) = 1$ である。

環準同型写像の合成は，環準同型写像である。環 R に対し，恒等写像 $1_R : R \to R, a \mapsto a$ は，環準同型写像である。

命題 5.21. $f : R \to S$ が環の準同型写像なら，$\forall a, b \in R$ に対し，等式 $f(-a) = -f(a)$，$f(a-b) = f(a) - f(b)$ と，$f(0) = 0$ が成り立つ。故に，環準同型写像 f の像

$$f(R) = \{f(a) \mid a \in R\}$$

は，S の部分環である。

問題 5.22. 命題 5.21 内の主張が正しいことを確かめよ。

問題 5.23. 次の主張が正しいことを確かめよ。

(1) 写像 $f : \mathbb{C} \to \mathbb{C}$，$f(a+bi) = a - bi$ $(a, b \in \mathbb{R}, i = \sqrt{-1})$ は，環の準同型写像であって，全単射である。

(2) $\mathbb{R}$ から環 $\mathrm{M}_2(\mathbb{R})$ への写像 g を

$$g(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

と定めると，写像 g は環の準同型写像となる。この写像 g は単射であるが，全射ではない。

問題 5.24. $f : \mathbb{R} \to \mathbb{R}$ が環準同型写像なら，等式 $f = 1_{\mathbb{R}}$ が成り立つことを証明せよ。

問題 5.25. $A = \mathbb{Z} \times \mathbb{Q}$，$B = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{Z}, b \in \mathbb{Q} \right\} \subseteq \mathrm{M}_2(\mathbb{Q})$ とし，それぞれ問題 5.13，問題 5.14 のようにして，可換環とみなす。このとき，写像

$$\varphi : A \to B, \quad (a, b) \mapsto \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

$(a \in \mathbb{Z}, b \in \mathbb{Q})$ は，環の準同型写像で全単射であることを確かめよ。

問題 5.26. 問題 5.13 で，$f : R \to \mathbb{Z}$ を $f(a, x) = a$，$g : \mathbb{Z} \to R$ を $g(a) = (a, 0)$ と定めれば，f, g は環の準同型写像であって，$fg = 1_{\mathbb{Z}}$ となることを確かめよ。

問題 5.27. 問題 5.9 のように集合 $\mathbb{R}^3$ を可換環とみなす。このとき各 $1 \leq i \leq 3$ について，写像

$$p_i : \mathbb{R}^3 \to \mathbb{R}, \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \mapsto a_i$$

とおくと，次の主張が正しい。確かめよ。

(1) 各 p_i は環準同型写像で全射である。

(2) $f : \mathbb{R} \to \mathbb{R}^3, x \mapsto \begin{pmatrix} x \\ x \\ x \end{pmatrix}$ も，環準同型写像であって，各 $1 \leq i \leq 3$ について，等式

$$p_i \cdot f = 1_{\mathbb{R}}$$

が成り立つ。

(3) $\operatorname{Ker} p_1 = (e_2, e_3)$ である。但し，$e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ とする。($\operatorname{Ker} p_1$ の定義は定義 5.32 を，イデアルの生成元については問題 5.37 を参照せよ。)

問題 5.28. 環準同型写像 $f : R \to S$ が全単射なら，逆写像 $f^{-1} : S \to R$ も環の準同型写像である。確かめよ。

問題 5.29. R, S を環とする。**環の同型写像** $f : R \to S$，即ち，**環の準同型写像** $f : R \to S$ **で全単射であるもの**が，少なくとも一つ存在するとき，環 R と環 S は互いに**同型である**という。二つの環 R, S が同型であることを，$R \cong S$ とかく。$\cong$ は環の間の同値関係であることを確かめよ。

問題 5.30.

$$\mathbb{D} = \left\{ \left(\begin{array}{cc} a & b \\ -b & a \end{array} \right) \middle| a, b \in \mathbb{R} \right\} \subseteq \mathrm{M}_2(\mathbb{R})$$

とおく。次の主張が正しいことを確かめよ。

(1) $\mathbb{D}$ は行列環 $\mathrm{M}_2(\mathbb{R})$ の可換な部分環である。

(2) 写像 $\varphi : \mathbb{C} \to \mathbb{D}$, $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ $(a, b \in \mathbb{R})$ は，環の同型写像で，従って $\mathbb{C} \cong \mathbb{D}$ である。

問題 5.31. R を環とし

$$\operatorname{Aut} R = \{\sigma \mid \sigma : R \to R \text{ は環の同型写像である } \}$$

とおく。集合 $\operatorname{Aut} R$ は S_R の部分群であり，写像の合成を演算に群をなすことを確かめよ。

定義 5.32. 環の準同型写像 $f : R \to S$ に対し

$$\operatorname{Ker} f = f^{-1}(\{0\}) \ (= \{a \in R \mid f(a) = 0\})$$

と定め，これを f の**核**と呼ぶ。集合 $\operatorname{Ker} f$ は次の性質を持つ。

(1) $0 \in \mathrm{Ker}\, f$

(2) $x, y \in \mathrm{Ker}\, f$，$a \in R$ ならば，$x+y,\ ax,\ xa \in \mathrm{Ker}\, f$ である。

証明. $f(0) = 0$ であるから，$0 \in \mathrm{Ker}\, f$ となる。$x, y \in \mathrm{Ker}\, f$，$a \in R$ ならば，$f(x+y) = f(x) + f(y) = 0 + 0 = 0$, $f(ax) = f(a)f(x) = f(a)\cdot 0 = 0$，$f(xa) = f(x)f(a) = 0\cdot f(a) = 0$ である。故に $x+y,\ ax,\ xa \in \mathrm{Ker}\, f$ である。 □

命題 5.33. 環の準同型写像 $f : R \to S$ が単射であるための必要十分条件は，$\mathrm{Ker}\, f = \{0\}$ が成り立つことである。

証明. f は単射とする。$a \in \mathrm{Ker}\, f$ なら $f(a) = 0 = f(0)$ であるから，$a = 0$ が従う。故に $\mathrm{Ker}\, f = \{0\}$ である。$\mathrm{Ker}\, f = \{0\}$ とせよ。$a, b \in R$ が $f(a) = f(b)$ を満たすなら，$f(a-b) = f(a) - f(b) = f(b) - f(b) = 0$ であるから，$a - b \in \mathrm{Ker}\, f = \{0\}$ である。故に $a - b = 0$ であり，等式 $a = b$ が従う。即ち写像 f は単射である。 □

問題 5.34. $\{R_\lambda\}_{\lambda\in\Lambda}$ は，空ではない集合 Λ を添え字に持つ環の族とする。次の主張が正しいことを証明せよ。

(1) 直積集合 $R = \prod_{\lambda\in\Lambda} R_\lambda = \{\{a_\lambda\}_{\lambda\in\Lambda} \mid \forall\lambda \in \Lambda\text{について}, a_\lambda \in R_\lambda\}$ は，成分ごとの和と積を演算に，環をなす。即ち，$a = \{a_\lambda\}_{\lambda\in\Lambda}, b = \{b_\lambda\}_{\lambda\in\Lambda} \in R$ に対し

$$a + b = \{a_\lambda + b_\lambda\}_{\lambda\in\Lambda}, a\cdot b = \{a_\lambda \cdot b_\lambda\}_{\lambda\in\Lambda}$$

とすると，この和と積に関して，R は環となる。

(2) 各 $\lambda \in \Lambda$ に対し，$p_\lambda : R \to R_\lambda, a = \{a_\lambda\}_{\lambda\in\Lambda} \mapsto a_\lambda$ とすると，p_λ は環の準同型写像で全射である。

(3) R が可換環であるための必要十分条件は，すべての $\lambda \in \Lambda$ について環 R_λ が可換環であることである。

(4) $\forall\lambda \in \Lambda$ について，環 R_λ は可換環とせよ。このとき，$\sharp\Lambda \geq 2$ なら，環 R は決して整域ではない。（整域の定義は，定義 6.49 を見よ。）

5.4 イデアルと剰余類環

R は環とする。

定義 5.35. I が環 R のイデアルであるとは，次の 2 条件が満たされることをいう。

(1) $\emptyset \neq I \subseteq R$ である。

(2) $\forall a \in R, \forall x, y \in I$ に対し，$x+y,\ ax,\ xa \in I$ である。

R が可換環のときは，条件 (2) は「$a \in R,\ x, y \in I$ なら, $x+y,\ ax \in I$」と同値である。

例えば，集合 $\{0\}$ と R 自身は，環 R のイデアルである。与えられた環 R の中に，どのようなイデアルがどのくらい多様に含まれているかは，環 R の構造の複雑さ (豊かさ）を測る指標の一つとなる。

補題 5.36. I が環 R のイデアルであれば，I は加法群 R の部分群である。即ち，$\forall x, y \in I$ に対し，$x - y \in I$ が成り立つ。故に $0 \in I$ である。

証明. $x, y \in I$ なら，$-y = (-1)y \in I$ であるから，$x - y = x + (-y) \in I$ となる。 □

問題 5.37. 次の主張を証明せよ。（問題 12.1 を参照せよ。）

(1) $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ を環 R のイデアルの列（このような列を環 R の**イデアルの昇鎖**という）とすれば，和集合 $I = \bigcup_{i \geq 1} I_i$ も環 R のイデアルである。

(2) I, J を R のイデアルとし，$I + J = \{a + b \mid a \in I, b \in J\}$ とおく。$I + J, I \cap J$ も環 R のイデアルであって，$I \cup J \subseteq I + J$ となる。（$I + J$ を I と J の**和**という。）

(3) 環 R のイデアル I, J に対し，

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid n \geq 1 \text{で}, \text{各} 1 \leq i \leq n \text{について} a_i \in I, b_i \in J\}$$

とおくと，IJ も環 R のイデアルであって，$IJ \subseteq I \cap J$ となる。（IJ を I と J の**積**という。）

問題 5.38. A は可換環とする。$a_1, a_2, \cdots, a_n \in A \ \ (n \geq 1)$ を取って，

$$I = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in A\}$$

とおく。次の主張 (1), (2), (3), (4) を証明せよ。

(1) $1 \leq \forall i \leq n$ について $a_i \in I$ である。

(2) I は A のイデアルである。

(3) J が A のイデアルで，$1 \leq \forall i \leq n$ について $a_i \in J$ なら，$I \subseteq J$ である。

即ち，I は $a_1, a_2, \cdots, a_n$ のすべてを含む最小のイデアルである。この I を $a_1, a_2, \cdots, a_n$ で生成されたイデアルといい，$I = (a_1, a_2, \cdots, a_n)$ または $I = (a_1, a_2, \cdots, a_n)A$ と表す。一つの元 $a \in A$ で生成されたイデアル $I = (a)$ は**単項イデアル**という。

$\mathfrak{a}$ は A のイデアルとする。有限個の元 $a_1, a_2, \cdots, a_n \in A \ (n \geq 1)$ を選んで $\mathfrak{a} = (a_1, a_2, \cdots, a_n)$ と表すことができるとき，イデアル $\mathfrak{a}$ は**有限生成である**という。

(4) I, J は A のイデアルとする。I, J が有限生成なら，$I + J, IJ$ も有限生成である。

問題 5.39. I を環 R のイデアルとするとき，$I = R$ であることと $1 \in I$ とは同値である。確かめよ。

問題 5.40. 自然数 $n \geq 1$ を取り，$\mathrm{M}_n(\mathbb{C})$ によって，n 次の複素正方行列の全体がなす環を表す。（環 $\mathrm{M}_n(\mathbb{C})$ における和と積は，行列の和と積である。）このとき，次の主張が正しいことを証明せよ。

(1) 環 $R = \mathrm{M}_n(\mathbb{C})$ のイデアルは，R と $\{0\}$ だけである。

(2) すべての 環準同型写像$\varphi : R \to S$ は単射である。

定理 5.41. I は環 R のイデアルとする。

(1) 2 元 $a, b \in R$ に対し，$a - b \in I$ であることを $a \sim b$ とかくと，$\sim$ は集合 R 上の同値関係である。

(2) 元 $a \in R$ に対し，$\overline{a}$ によって，元 a を含む同値類 $\mathrm{C}(a) = \{x \in R \mid x \sim a\}$ を表すと，等式

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

が成り立つ。($\overline{a}$ は $a \mod I$ と書くこともある。)

(3) 和と積を次のように定めると，定義 5.6 の 4 条件が満たされ，商集合 $R/I = \{\overline{a} \mid a \in R\}$ は環となる（R/I は零環になることもある)。R が可換なら，環 R/I も可換である。

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

環 R/I を I による R の**剰余類環**という。

(4) 環 R/I が零環であるための必要十分条件は，$1 \in I$，即ち $I = R$ である。

(5) 自然な全射 $f : R \to R/I,\ f(a) = \overline{a}$ は環の準同型写像であって，$I = \mathrm{Ker}\, f$ が成り立つ。

証明. (1) $a - a = 0 \in I$ である。$a - b \in I$ なら $b - a = -(a - b) \in I$ である。 $a - b, b - c \in I$ なら，$a - c = (a - b) + (a - c) \in I$ である。

(2) $x \in \overline{a}$ なら，$x \sim a$ すなわち $x - a \in I$ であるから，$i = x - a$ とおけば，$x = a + i \in a + I$ が得られる。逆に $x \in a + I$ を取り $x = a + i\ (i \in I)$ と表すと，$x - a = i \in I$ であるから，$x \sim a$ が成り立ち，$x \in \overline{a}$ となる。故に，$\overline{a} = a + I$ である。

(3) $\overline{a} = \overline{a_1},\ \overline{b} = \overline{b_1}$ ならば，$a = a_1 + i,\ b = b_1 + j\ (i, j \in I)$ と表されるので，$a + b = (a_1 + b_1) + (i + j),\ ab = a_1 b_1 + (a_1 j + i b_1 + ij)$ である。$i + j,\ a_1 j + i b_1 + ij \in I$ である

から，$a+b \sim a_1+b_1,\ ab \sim a_1b_1$ となり，等式 $\overline{a+b} = \overline{a_1+b_1},\ \overline{ab} = \overline{a_1b_1}$ が成り立つ。即ち，この加法と乗法は，well-defined である。商集合 R/I が環になる（R が可換なら，環 R/I も可換である）ことは，忠実に環の定義を検証することによって確かめることができる。$0 = \overline{0},\ -\overline{a} = \overline{-a},\ 1 = \overline{1}$ である。

(4) $\overline{1} = \overline{0}$ であることと $1 \in I$ は同値である。

(5) $\overline{a} = \overline{0}$ と $a = a - 0 \in I$ とは同値である。故に $\mathrm{Ker}\, f = I$ である。 □

例 5.42.（問題 5.62 参照）$(7) = \{7n \mid n \in \mathbb{Z}\}$ とする。(7) は $\mathbb{Z}$ のイデアルである。$a \in \mathbb{Z}$ を取り

$$a = 7q + r \quad (q, r \in \mathbb{Z},\ 0 \le r \le 6)$$

と表す。即ち r は a を 7 で割った余りである。$a - r = 7q \in (7)$ であるから，$a \sim r$ であり，$\overline{a} = \overline{r}$ となる。故に

$$\mathbb{Z}/(7) = \{\ \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6}\ \}$$

であって，$\mathbb{Z}/(7)$ が**整数を 7 で割った剰余（類）の集合**に他ならないことがわかる。$0 \le i, j \le 6$ の範囲にある整数 i, j については，$i - j$ が 7 の倍数なら $i = j$ であるから，7 つの剰余類 $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ は互いに異なり，$\sharp(\mathbb{Z}/(7)) = 7$ を得る。$\mathbb{Z}/(7)$ は可換環である（定理 5.41）が，積の表

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

より，体をなすことがわかる。（体の定義は，5.58 を見よ。）

定理 5.43. I は環 R のイデアルで $I \neq R$ なるものとし，$f : R \to R/I, a \mapsto \overline{a}$ を自然な環準同型写像とする。このとき次の主張が正しい。

(1) J が環 R のイデアルなら，$f(J) = \{\overline{a} \mid a \in J\}$ は環 R/I のイデアルである。

(2) K が環 R/I のイデアルなら，$f^{-1}(K) = \{a \in R \mid \overline{a} \in K\}$ は環 R のイデアルであって，$I \subseteq f^{-1}(K)$ である。

(3) $\mathcal{S} = \{J \mid J$ は環 R のイデアルで $I \subseteq J\}$，$\mathcal{T} = \{K \mid K$ は環 R/I のイデアル $\}$ とおく。写像 $\varphi : \mathcal{S} \to \mathcal{T}, J \mapsto f(J)$ は全単射である。

(4) $J_1, J_2 \in \mathcal{S}$ のとき，$J_1 \subseteq J_2$ であるための必要十分条件は，$f(J_1) \subseteq f(J_2)$ が成り立つことである。

証明. (1)，(2) は，正直に確認すればよい。(3) を見よう。(2) より，$\forall K \in \mathcal{T}$ について，$f^{-1}(K) \in \mathcal{S}$ であるから，$\psi(K) = f^{-1}(K)$ とおくことにより，写像 $\psi : \mathcal{T} \to \mathcal{S}, K \mapsto f^{-1}(K)$ が得られる。$\varphi{\cdot}\psi = 1_{\mathcal{T}}, \psi{\cdot}\varphi = 1_{\mathcal{S}}$ であることを確かめよう。$J \in \mathcal{S}$ とする。$\psi(\varphi(J)) = f^{-1}(f(J))$ であるから，$J \subseteq \psi(\varphi(J))$ は自明に正しい。$a \in \psi(\varphi(J))$ なら，$f(a) \in f(J)$ であるから，ある $j \in J$ が存在して等式 $f(a) = f(j)$ が成り立つ。$f(a) = \overline{a}, f(j) = \overline{j}$ であるので，$a - j \in I$ となるが，ここで $I \subseteq J$ であるから, $a - j \in J$ が従い，$j \in J$ であるので，$a \in J$ となる。故に $\psi(\varphi(J)) = J$，即ち $\psi{\cdot}\varphi = 1_{\mathcal{S}}$ が得られる。$K \in \mathcal{T}$ とせよ。$\varphi(\psi(K)) = K$ を示す。$\varphi(\psi(K)) = f(f^{-1}(K))$ である。$x \in f(f^{-1}(K))$ なら，$x = f(a)$ $(a \in f^{-1}(K))$ とかくと，$a \in f^{-1}(K) = \{a \in R \mid f(a) \in K\}$ であるから，$x = f(a) \in K$，即ち $f(f^{-1}(K)) \subseteq K$ である。逆に $x \in K$ をとり $x = \overline{a}$ $(a \in R)$ と表すと，$x \in K$ であるので $a \in f^{-1}(K)$ が得られ，$x = f(a) \in f(f^{-1}(K))$ が従う。故に $K \subseteq f(f^{-1}(K))$ であり，等式 $\varphi(\psi(K)) = K$ が得られ，$\varphi{\cdot}\psi = 1_{\mathcal{T}}$ が示される。主張 (4) は明らかである。 □

5.5 環の同型定理

R, S は環とする。

定理 5.44 (環の準同型定理). $f : R \to S$ は環の準同型写像，I は環 R のイデアルとする。$I \subseteq \mathrm{Ker}\, f$ なら，$f = gh$ を満たす環の準同型写像 $g : R/I \to S$ が唯一つ定まる。但し，$h : R \to R/I, a \mapsto \overline{a}$ は自然な環準同型写像とする。

証明. 写像 $g : R/I \to S$ を $g(\overline{a}) = f(a)$ で定める。この写像 g は well-defined である。実際，2 元 $a, b \in R$ が等式 $\overline{a} = \overline{b}$ を満たすなら，$a - b \in I$ である。$I \subseteq \mathrm{Ker}\, f$ であるから，$f(a) - f(b) = f(a - b) = 0$ となり，$f(a) = f(b)$ が得られる。この g が環準同型写像であって，等式 $f = gh$ が成り立つことを確かめるのは，きわめて容易である。写像 g の一意性は，写像 h が全射であることに従う。 □

系 5.45. $f : R \to S$ は環の準同型写像で全射であると仮定し，$I = \mathrm{Ker}\, f$ とおく。$h : R \to R/I, a \mapsto \overline{a}$ は自然な環準同写像とする。このとき，定理 5.44 によって得られた環準同型写像 $g : R/I \to S$ は，全単射（従って $R/I \cong S$）である。

証明. f が全射だから，g も全射である。，$I = \mathrm{Ker}\, f$ であるから，$g(\overline{a}) = f(a) = 0$ なら $a \in I$ となり，$\overline{a} = 0$ が得られる。故に $\mathrm{Ker}\, g = \{0\}$ であって，命題 5.33 より，g は単射であることがわかる。 □

5.6 整域と体

R は環とする。

定義 5.46. 元 $a \in R$ に対し，等式 $ax = xa = 1$ を満たす $x \in R$ が存在するとき，$a \in R$ は R の**単元**であるという。

問題 5.47. 定義 5.46 における $x \in R$ は，元 $a \in R$ に対し，R 内で一意的に定まる。確かめよ。(このxを a の逆元と呼び, $x = a^{-1}$と表す。)

問題 5.48. 次の主張が正しいことを確かめよ。

(1) $1 \in R$ は単元であって，$1^{-1} = 1$ が成り立つ。

(2) $a, b \in R$ が単元なら，ab も単元であって，等式 $(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ。従って $a \in R$ が単元なら，$-a$ も単元である。

(3) $R^\times = \{a \in R \mid a \text{ は } R \text{ の単元である}\}$ とおくと，集合 $R^\times$ は，環 R の積を演算に**群**をなす。

(4) $R^\times \subseteq R \setminus \{0\}$ である。

$R^\times$ を環 R の**単元群**という。（$R^\times$ は，$\mathrm{U}(R)$ とかくこともある。）

問題 5.49. $f : R \to S$ が環の準同型写像なら，$f(R^\times) \subseteq S^\times$ であって，$\forall a \in R^\times$ について等式 $f(a)^{-1} = f(a^{-1})$ が成り立つ。従って，$\varphi : R^\times \to S^\times,\ a \mapsto f(a)$ は，群の準同型写像である。確かめよ。

問題 5.50. I を環 R のイデアルとする。$I = R$ であるための必要十分条件は，$I \cap R^\times \neq \emptyset$ である。確かめよ。

以下 A は可換環とする。

$a, b \in A$ とする。$a \in A^\times$ なら，方程式 $ax = b$ は唯一つの解 $x = a^{-1}{\cdot}b$ を持つ。これを $\dfrac{b}{a}$ と書くことにすれば，$\dfrac{1}{a} = a^{-1}$ であり，次の主張が正しい。

命題 5.51. $a, b, c, d \in A$ で $a, c \in A^\times$ とすると，次の等式が成り立つ。

(1) $\dfrac{b}{a} + \dfrac{d}{c} = \dfrac{bc + ad}{ac},\ \dfrac{b}{a}{\cdot}\dfrac{d}{c} = \dfrac{bd}{ac}$

(2) $\dfrac{cb}{ca} = \dfrac{b}{a}$

(3) $-\dfrac{b}{a} = \dfrac{-b}{a} = \dfrac{b}{-a},\ \dfrac{0}{a} = 0,\ \dfrac{b}{a} - \dfrac{d}{c} = \dfrac{bc - ad}{ac}$

(4) $\dfrac{b}{1} = b$

問題 5.52. 命題 5.51 内の等式が正しいことを確かめよ。

$a \in A$ に対し，写像 $\widehat{a} : A \to A$ を $\widehat{a}(x) = ax, x \in A$ によって定める。

問題 5.53. $a \in A$ について，次の条件は同値である。確かめよ。

(1) $a \in A^{\times}$ である。

(2) 写像 $\widehat{a}$ は全射である。

(3) 写像 $\widehat{a}$ は全単射である。

定義 5.54. $a \in A$ とする。$x \in A$ について，$ax = 0$ ならば必ず $x = 0$ となるとき，元 a は環 A の**非零因子**であるという。

問題 5.55. $a \in A$ とする。次の条件は同値であることを確かめよ。

(1) a は A の非零因子である。

(2) 写像 $\widehat{a}$ は単射である。

従って，$a \in A^{\times}$ なら，元 a は非零因子である。

非零因子は必ずしも単元ではない。例えば，環 $\mathbb{Z}$ 内では，$0 \neq \forall a \in \mathbb{Z}$ は非零因子であるが，$a \neq 1, -1$ なら，単元ではない。

定義 5.56. $0 \neq \forall a \in A$ が非零因子であるとき，即ち，$a, b \in A$ に対し，$a, b \neq 0$ なら必ず $ab \neq 0$ となるとき，環 A は**整域**であるという。

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は整域である。整域の部分環は整域である。$\overline{2} \cdot \overline{3} = \overline{6} = 0$ であるが，$\overline{2}, \overline{3} \neq 0$ であるから，剰余類環 $\mathbb{Z}/(6)$ は整域ではない。

問題 5.57. 問題 5.13 の環 A は整域でないことを確かめよ。

定義 5.58. K は可換環で，環 K の 0 と異なる全ての元が単元であるとき，即ち，等式 $K^{\times} = K \setminus \{0\}$ が成り立つとき，K は**体**であるという。

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である。Galois の理論は体の代数拡大の理論である。その一部は第 10 節で取り扱う。

問題 5.59. $K_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, $K_2 = \{a + bi \mid a, b \in \mathbb{Q}\}$ とおけば，集合 K_1, K_2 は，体 $\mathbb{C}$ の部分環であって，体をなすことを確かめよ。

問題 5.60. A は可換環とする。環 A に関する次の 3 条件は，互いに同値であることを証明せよ。

(1) A は体である。

(2) 環 A のイデアルは，A と $\{0\}$ のみである。

(3) 全ての環準同型写像 $f : A \to B$ は単射である。

問題 5.61. 次の主張が正しい。証明せよ。

(1) 体の部分環は整域である。（逆も正しい。定理 7.10 を見よ。）

(2) A は可換環とする。A が有限集合なら，環 A の非零因子は必ず A の単元である。

(3) 環 A が有限集合で整域なら，A は体である。

問題 5.62. 次の主張 (1), (2), (3) を証明し，問 (4) に答えよ。

(1) $a \geq 2$ は整数とする。環 $\mathbb{Z}/(a)$ は元の個数が a の有限集合である。

(2) $a \geq 2$ は整数とする。$n \in \mathbb{Z}$ について，$\overline{n} \in \mathbb{Z}/(a)$ が環 $\mathbb{Z}/(a)$ の単元であるための必要十分条件は，a, n が互いに素であることである。

(3) 整数 $p \geq 2$ が素数なら，剰余類環 $\mathbb{Z}/(p)$ は体をなす。

(4) 体 $\mathbb{Z}/(11)$ と体 $\mathbb{Z}/(17)$ 内で，次の計算を実行せよ。

$$\overline{3}\,\overline{2} + \overline{7}\,\overline{6}, \quad \overline{5}\,\overline{4} \cdot \overline{10}\,\overline{7}, \quad \overline{6}\,\overline{7} - \overline{4}\,\overline{5}$$

5.7　極大イデアルと素イデアル

A は可換環とする。

定義 5.63. P は環 A のイデアルとする。次の条件を満たすとき，P は環 A の**素イデアル**であるという。

(1) $P \subsetneq A$ である。

(2) $a, b \in A$ のとき，$ab \in P$ ならば，$a \in P$ であるかまたは $b \in P$ が成り立つ。

問題 5.64. P は環 A の素イデアル，$I,\ J$ は A のイデアルとする。このとき，$IJ \subseteq P$ ならば，$I \subseteq P$ であるか $J \subseteq P$ が成り立つ。故に，イデアル $I_1, I_2, \cdots, I_n$ に対し，等式

$$\bigcap_{i=1}^{n} I_i = P$$

が成り立つなら，ある $1 \leq i \leq n$ について $I_i = P$ となる。証明せよ。

定理 5.65. P は環 A のイデアルであって，$P \subsetneq A$ なるものと仮定せよ。このとき，P が環 A の素イデアルであるための必要十分条件は，剰余類環 A/P が整域となることである。

証明. A/P は整域とする。$ab \in P$ ならば，環 A/P 内では $\overline{a}\overline{b} = \overline{ab} = 0$ であるから，$\overline{a} = 0$ か $\overline{b} = 0$ となる。従って $a \in P$ か $b \in P$ が成り立つ。故に P は環 A の素イデアルである。同様に，P が環 A の素イデアルなら A/P が整域となることを確かめることができる。 □

定義 5.66. M は環 A のイデアルとする。次の条件を満たすとき，M は環 A の**極大イデアル**であるという。

(1) $M \subsetneq A$ である。

(2) I を環 A のイデアルで，$M \subseteq I \subseteq A$ なるものとすれば，$M = I$ かまたは $I = A$ が成り立つ。

定理 5.67. M は環 A のイデアルであって，$M \subsetneq A$ なるものと仮定せよ。このとき，M が環 A の極大イデアルであるための必要十分条件は，剰余類環 A/M が体をなすことである。

証明. A/M は体であると仮定し，イデアル I は $M \subsetneq I$ なるものとする。$a \in I$ を $a \notin M$ に取ると，A/M 内では $\overline{a} \neq 0$ であるから，$\overline{a}$ は逆元を持ち，ある $x \in A$ があって等式 $\overline{x}\cdot\overline{a} = \overline{1}$ が成り立つ。$1-ax \in M \subseteq I$ であって $a \in I$ であるから，$1 \in I$ となり，等式 $I = A$ が従う。故に M は環 A の極大イデアルである。逆に，M は環 A の極大イデアルと仮定しよう。$a \in A$ は環 A/M 内で $\overline{a} \neq 0$ なるものとする。故に $a \notin M$ である。従って，$I = (a)+M = \{ax+y \mid x \in A, y \in M\}$ とおくと，I は A のイデアルであって $M \subseteq I$ であるが，$a \in I \setminus M$ であるから，$M \subsetneq I$ となる。M は極大であるから，等式 $I = A$ が成り立ち，$1 = ax + y$ となる $x \in A$ と $y \in M$ が存在することがわかる。故に，A/M 内では，等式 $1 = \overline{a}\cdot\overline{x} + \overline{y} = \overline{a}\cdot\overline{x}$ が成り立ち，元 $\overline{a}$ は A/M の単元であることがわかる。即ち A/M は体である。 □

問題 5.68. 定理 5.67 を，定理 5.43 と問題 5.60 を用いて証明せよ。

系 5.69. M が A の極大イデアルなら，M は素イデアルである。

可換環は，少なくとも一つ極大イデアルを含むことが知られている（定理 6.13）。

5.8 整数環 $\mathbb{Z}$

補題 5.70 (Euclid の補題)**.** n, m は整数で $n > 0$ とする。このとき，等式 $m = nq + r$ $(0 \leq r < n)$ が成り立つような整数の組 (q, r) がただ一つ存在する。

証明. 組 (q, r) としては，$q = \max\{x \in \mathbb{Z} \mid xn \leq m\}$，$r = m - nq$ を取ればよい。整数の組 $(q, r), (q', r')$ がどちらも定理に述べられた条件を満たすなら，$n(q - q') = r' - r$ である。$|r' - r| < n$ であるから，$r' = r$ となり，$q = q'$ が従う。 □

定理 5.71. I が $\mathbb{Z}$ のイデアルなら，整数 $a \geq 0$ によって，$I = (a)$ と表される。（このような整数 $a \geq 0$ は，イデアル I に対し一意的に定まる。）

証明. $I \neq (0)$ としてよい。イデアル I は少なくとも一つ正整数を含む。

$$a = \min\{x \in I \mid x > 0\}$$

とおき，等式 $I = (a)$ が成り立つことを示そう。$a \in I$ であるから，$(a) \subseteq I$ となる。$\forall x \in I$ を取ると，$a > 0$ であるので，補題 5.70 によって，$x = aq + r$，$0 \leq r < a$ と表すことができるが，$r = x - aq \in I$ であるから，正整数 a の最小性より $r = 0$ が従い，$x = aq \in (a)$ が得られる。故に $I = (a)$ である。 □

問題 5.72. 次の等式を満たす整数 $d, \ell > 0$ を求め，それぞれ最大公約数，最小公倍数であることを確かめよ。

(1) $(3) + (7) = (d)$, $(3) \cap (7) = (\ell)$

(2) $(6) + (8) + (12) = (d)$, $(6) \cap (8) \cap (12) = (\ell)$

系 5.73. (1) $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ が $\mathbb{Z}$ のイデアルの昇鎖なら，番号 $k \geq 1$ を選んで，$\forall i \geq k$ について等式 $I_k = I_i$ が成り立つようにすることができる。

(2) $\mathbb{Z}$ のイデアル全体のなす集合を $\mathcal{X}$ とすれば，$\mathcal{X}$ の如何なる空でない部分集合 $\mathcal{S}$ も，少なくとも一つ包含関係に関する極大元 I (即ち，$I \in \mathcal{S}$ であってしかも $I \subsetneq J$ となるような $J \in \mathcal{S}$ が存在しないような元 I) を含む。

証明. (1) $I = \bigcup_{n \geq 1} I_n$ とおけば，I は $\mathbb{Z}$ のイデアルである。等式 $I = (a)$ が成り立つよう $a \in \mathbb{Z}$ をとり，$a \in I_k$ となるよう番号 $k \geq 1$ を選ぶ。このとき，$i \geq k$ なら $a \in I_i$ であるから，$I = (a) \subseteq I_i$ であって，$I_i \subseteq \bigcup_{n \geq 1} I_n = I$ より，$I_i = I$ が従う。

(2) 集合 $\mathcal{S}$ が極大元を含まないならば，如何なる元 $I \in \mathcal{S}$ に対しても，$I \subsetneq J$ となる $J \in \mathcal{S}$ が存在するので，イデアルの昇鎖 $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_i \subsetneq \cdots$ が得られるが，これは (1) により不可能である。 □

問題 5.74. I が $\mathbb{Z}$ のイデアルで $I \neq \mathbb{Z}$ なら，イデアル I を含むような極大イデアル M が少なくとも一つは存在する。確かめよ。

定義 5.75. 整数 p は，イデアル (p) が環 $\mathbb{Z}$ の極大イデアルであるとき，即ち，剰余類環 $\mathbb{Z}/(p)$ が体をなすとき，**素数**であるという。従って，p が素数なら，$p \neq 0, \pm 1$ である。

定理 5.76. p は整数で $p \neq 0, \pm 1$ とする。このとき次の条件は同値である。

(1) p は素数である。

(2) p は**既約である**。即ち，a, b が整数で $p = ab$ なら，$a = \pm 1$ であるか又は $b = \pm 1$ が成り立つ。

証明. (1) $\Rightarrow$ (2) $p = ab$ $(a, b \in \mathbb{Z})$ とする。$ab \in (p)$ である。(p) は素イデアルなので，$a \in (p)$ であるか $b \in (p)$ が成り立つ。$b \in (p)$ とし，$b = pc$ $(c \in \mathbb{Z})$ と表すと，$p = p(ac)$ であるから，$ac = 1$ となり，$a = \pm 1$ が得られる。

(2) $\Rightarrow$ (1) $I = (p)$ おく。$I \neq \mathbb{Z}$ である。I が極大イデアルであることを示そう。J を環 $\mathbb{Z}$ のイデアルとし，$I \subseteq J \subsetneq \mathbb{Z}$ と仮定する。$0 \neq p \in J$ である。J は単項であるから，$J = (a)$ となる整数 $a \geq 2$ が得られるが，$a | p$ なので，(2) の仮定より $a = \pm p$ であり，等式 $I = J$ が従う。故に，I は極大イデアルで，p は素数である。 □

定理 5.77. $a \geq 2$ が整数なら，有限個の素数 $p_1, p_2, \cdots, p_n$ $(p_i \geq 2)$ を選んで，等式 $a = p_1 p_2 \cdots p_n$ が成り立つようにできる。素因数分解 $a = p_1 p_2 \cdots p_n$ $(p_i \geq 2)$ は，順序の違いを除いて，整数 $a \geq 2$ に対し一意的に定まる。

証明. 素因数分解を持たない整数 $a \geq 2$ が存在したと仮定する。この時

$$\mathcal{S} = \{(a) \mid 2 \leq a \in \mathbb{Z} \text{ で整数 } a \text{ は素数分解を持たない}\}$$

と定めると，$\mathcal{S} \neq \emptyset$ であるから，集合 $\mathcal{S}$ 内には，包含関係に関する極大元 $I = (a)$ $(a \geq 2)$ が存在する（系 5.73 (2) 参照)。a は素因数分解を持たないので，a は素数ではなく，既約でもない（定理 5.76 参照)。整数 $b, c \geq 2$ を $a = bc$ が成り立つようにとり，$J = (b), K = (c)$ とおけば，$b, c \geq 2$ であるから，$I \subsetneq J, I \subsetneq K$ となる。故に，イデアル I は集合 $\mathcal{S}$ 内で

極大であるので，$J, K \notin \mathcal{S}$ である。故に，整数 b, c はどちらも素因数分解を持ち，従って $a = bc$ も素因数分解を持つことになるが，不可能である。素因数分解の一意性を確認しよう。$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ ($p_i, q_j \geq 2$，素数) とする。$n = 1$ ならば，$p_1 = q_1 q_2 \cdots q_m$ である。p_1 は素数で，従って既約であるから，$m = 1$ が従う。$n > 1$ とし，$n - 1$ 以下では素因数分解の一意性が成り立っていると仮定する。すると，$q_1 q_2 \cdots q_m \in (p_1)$ より，ある素数 q_i について，$q_i \in (p_1)$，即ち $p_1 = q_i$ が成り立つ（定理 5.76)。並べ替えて $p_1 = q_1$ と仮定してよい。すると，$p_2 \cdots p_n = q_2 q_3 \cdots q_m$ であるから，帰納法の仮定より，$n = m$ と $p_i = q_i$ $(2 \leq i \leq n)$ とが従う。 □

整数 a, b について，b が a の倍数であることを，$a|b$ と書く。

系 5.78. 素数の個数は無限である。

証明. 正の素数が有限個 $\{p_1, p_2, \cdots, p_n\}$ しか存在しないと仮定し，$a = p_1 p_2 \cdots p_n + 1$ とおくと，$a \geq 2$ であるから，定理 6.71 によって，$p|a$ となる素数 $p \geq 2$ が存在する。この p は，p_i $(1 \leq i \leq n)$ のどれかであるから，$p = p_1$ とすれば，$p_1|a,\ a = p_1 p_2 \cdots p_n + 1$ より，$p_1|1$ となる。これは不可能である。 □

整数 $a_1, a_2, \cdots, a_n$ を取り，$I = (a_1, a_2, \cdots, a_n)$ とおく。整数 $d \geq 0$ を等式 $I = (d)$ が成り立つように取れば，$a_i \in I = (d)$ であるから，$d|a_i$ が全ての $1 \leq i \leq n$ に対して成り立つ。一方，$d \in I$ であるから，$d = \sum_{i=1}^{n} x_i a_i$ $(x_i \in \mathbb{Z})$ と表すことができる。故に，整数 $e \in \mathbb{Z}$ が全ての $1 \leq i \leq n$ に対し $e|a_i$ なら，$e|d$ が成り立つ。即ち d は $a_1, a_2, \cdots, a_n$ の最大公約数である。即ち，次の定理が得られる。

命題 5.79. $d = \mathrm{GCD}(a_1, a_2, \ldots, a_n)$ とおくと，整数 $\{x_i\}_{1 \leq i \leq n}$ が存在して，等式

$$d = \sum_{i=1}^{n} a_i x_i$$

が成り立つ。

問題 5.80. 整数 $a_1, a_2, \ldots, a_n$ に対し，$0 \leq \ell \in \mathbb{Z}$ を等式

$$\bigcap_{I=1}^{n}(a_i) = (\ell)$$

が成り立つように取ると，ℓ は $a_1, a_2, \ldots, a_n$ の**最小公倍数**である。確かめよ。

系 5.81. a, b を整数とすれば，a, b が互いに素であるための必要十分条件は，等式 $1 = ax + by$ が成り立つような整数 x, y が存在することである。

系 5.82. a, b, c は整数とせよ。a, b が互いに素であって $a|bc$ なら，$a|c$ である。

証明. $bc = ad$ とし，整数 x, y を取り $1 = ax + by$ と表すと，等式 $c = acx + bcy = acx + ady = a(cx + dy)$ が得られ，$a|c$ が従う。 □

6 埋め込みの原理と Zorn の補題

6.1 埋め込みの原理

次の補題が正しい。

補題 6.1. 空でない二つの集合 X，Y を与えれば，$Y \cap Z = \emptyset$ であるような空でない集合 Z と全単射 $\varphi : X \to Z$ の組 (Z, φ) が少なくとも一つ存在する。

補題 6.2. R は環とする。 X は空でない集合で，全単射 $f : R \to X$ が与えられていると仮定せよ。X 上に和と積を

$$a + b = f\left(f^{-1}(a) + f^{-1}(b)\right),\ ab = f(f^{-1}(a)f^{-1}(b))$$

で定めると，集合 X はこの和と積によって環となる。このとき，f は環の同型写像であって，R が可換 (体，あるいは，整域) ならば，環 X も可換 (体，あるいは，整域) となる。

問題 6.3. 補題 6.2 を証明せよ。

定理 6.4 (埋め込みの原理). 写像 $f : A \to B$ は環の準同型写像であって，単射と仮定する。このとき，次の条件を満たすような環 C と環の同型写像の組 (C, g) が少なくとも一つ存在する。

(1) A は環 C の部分環である。

(2) 写像 $i : A \hookrightarrow C$ によって自然な埋め込み $i(a) = a$ を表すと，等式 $i = gf$ が成り立つ。

従って，B が体であれば，C は A を部分環として含む体である。

証明. $B = f(A)$ なら，$C = A$ と取ればよい。$B \neq f(A)$ とせよ。空でない集合 X と全単射 $\varphi : B \setminus f(A) \to X$ の組 (X, φ) を，$X \cap A = \emptyset$ が成り立つように取る。(X, φ) を用いて，集合 C と写像 $g : B \to C$ を下の様に定義しよう。$C = X \cup A$ とおき, 写像 $g : B \to C$ を次のように定める。元 $b \in B$ について，もし $b \in f(A)$ ならば，$b = f(a)$ となる $a \in A$ が唯一つ定まるから，$g(b) = a$ とおく。もし $b \notin f(A)$ なら，$g(b) = \varphi(b)$ とおく。すると，写像 g は全単射であるから，補題 6.2 より，集合 C は環 B の和と積から導かれる和と積によって環となる。$i = gf$ であるから，環 A は環 C の部分環である。 □

6.2 Zorn の補題

X は空ではない集合とする。集合 X 上の関係 $\leq$ が次の 3 条件を満たすとき，関係 $\leq$ を集合 X 上の順序と言い，順序関係が一つ指定されているとき，集合 X は順序集合であるという。

(1) 任意の元 $x \in X$ に対し，$x \leq x$ である。

(2) $x, y \in X$ について，$x \leq y$ であってかつ $y \leq x$ なら，$x = y$ である。

(3) $x, y, z \in X$ について，$x \leq y$ かつ $y \leq z$ ならば，$x \leq z$ である。

例えば, 環 R のイデアル全体からなる集合を $\mathcal{X}$ とすると, 包含関係 $\subseteq$ は，集合 $\mathcal{X}$ 上の順序である。

以下，集合 X は順序集合とする。

定義 6.5. 集合 X の空でない部分集合 $\mathcal{C}$ が**鎖**であるとは，$\mathcal{C}$ の任意の 2 元 a, b に対して $a \leq b$ または $b \leq a$ が成り立つことをいう。

定義 6.6. X の空でない部分集合 $\mathcal{S}$ が X 内で**上に有界**であるとは，ある元 $a \in X$ が存在して，任意の元 $x \in \mathcal{S}$ に対し $x \leq a$ が成り立つことをいう。

定義 6.7. 元 $a \in X$ が X 内で**極大**であるとは，$x \in X$ について，$a \leq x$ ならば $a = x$ が成り立つことをいう。

極大イデアルの定義を言い直すと，下記のようになる。

定義 6.8. A は可換環，M は A のイデアルとする。M が環 A の極大イデアルであるとは，$M \neq A$ であって，M が集合 $X = \{I \mid I \text{ は環 } A \text{ のイデアルで } I \neq A\}$ の中で包含関係に関して極大であることをいう。

補題 6.9 (**Zorn の補題**)**.** 空でない順序集合 X 内で全ての鎖が上に有界であれば，集合 X は少なくとも一つの極大元を含む。

定義 6.10. 順序集合 X は次の条件を満たすとき，**整列集合**であるという。**集合 X の任意の空でない部分集合 S は，最小元 $a \in S$（即ち，任意の $s \in S$ に対して $a \leq s$ であるような元 $a \in S$) を含む。**

定理 6.11 (**整列定理**)**.** 集合 Z が空でないならば，Z 上に順序を定めて，整列集合にすることができる。

補題 6.12 (**選択公理** axiom of choice)**.** 空でない集合 I を添字集合とする，空でない集合のいかなる族 $\{X_i\}_{i \in I}$ に対しても，直積集合

$$\prod_{i \in I} X_i = \{\{x_i\}_{i \in I} \mid \forall i \in I \text{ について } x_i \in X_i\}$$

は空でない。

以上 3 つの主張（Zorn の補題，整列定理，選択公理）は，互いに同値であることが知られている。 折を見て同値性の証明を追体験することを薦める。以下，これらを受け入れて，自由に使う。

6.3 極大イデアルの存在

Zorn の補題の代表的な使用例を 1 つ述べよう。以下，A は可換環とする。

定理 6.13. I を環 A のイデアルで $I \neq A$ なるものとすれば，環 A 内には，$I \subseteq M$ となるような極大イデアル M が，少なくとも一つは含まれている。

証明. $X = \{J \mid J \text{ は } A \text{ のイデアルで } J \neq A\}$ とおく。すると，$I \in X$ であるから，X は空集合ではない。以下，包含関係 $\subseteq$ によって，集合 X を順序集合とみなす。集合 X 内に任意の鎖 $\mathcal{C}$ を取り，$K = \bigcup_{J \in \mathcal{C}} J$ とおくと，部分集合 K は環 A のイデアルで，$K \neq A$ となる。$K \in X$ であって，$J \subseteq K$ が全ての $J \in \mathcal{C}$ に対して成り立つから，Zorn の補題により，極大元 $M \in X$ が存在する。これが求める極大イデアルである。 □

この定理 6.13 は，実は Zorn の補題と同値であることが知られている。

系 6.14. $I \neq A$ を環 A イデアルとすれば, $I \subseteq P$ となる素イデアル P が存在する。

環 A の素イデアル全体のなす集合を $\operatorname{Spec} A$ で表す。$\operatorname{Spec} A \neq \emptyset$ である。

問題 6.15. 環 A のイデアル I に対して，$\mathrm{V}(I) = \{P \in \operatorname{Spec} A \mid I \subseteq P\}$ と定める。集合 $X = \operatorname{Spec} A$ は $\{\mathrm{V}(I) \mid I \text{ は環 } A \text{ のイデアル}\}$ を閉集合族として，位相空間となる。確かめよ。

7 局所化

7.1 積閉集合と局所化

以下 A は可換環とする。A の部分集合 S は，次の条件を満たすとき，A 内の**積閉集合**であるという。

(1) $1 \in S \subseteq A$ である。

(2) $0 \notin S$ である。

(3) $\forall s, t \in S$ に対し，$st \in S$ である。

例 7.1. 次の集合 S は，環 A 内の積閉集合である。

(1) $S = \{a \in A \mid a \text{ は } A \text{ の非零因子である }\}$

(2) べき零でない元 $f \in A$ を取って，$S = \{f^n \mid n \geq 0\}$ とおく。

(3) 素イデアルの族 $\{P_i\}_{i \in I}$ を取って，$S = A \setminus \bigcup_{i \in I} P_i$ とおく。特に，$P \in \operatorname{Spec} A$ を取り，$S = A \setminus P$ とおく。

環 A 内に積閉集合 S が与えられていると仮定し，$X = S \times A$ とおく。2元 $(s, a), (t, b) \in X$ について，ある元 $u \in S$ が存在して等式 $u(sb - ta) = 0$ が成り立つとき，$(s, a) \sim (t, b)$ と書く。

命題 7.2. 関係 $\sim$ は, 集合 $X = S \times A$ 上の同値関係である。

証明. (2) $(s, a) \sim (t, b)$ ならば, ある元 $u \in S$ があって等式 $u(sb - ta) = 0$ が成り立つ。$u(ta - sb) = 0$ であるから，$(t, b) \sim (s, a)$ である。

(3) $(s, a) \sim (t, b)$, $(t, b) \sim (u, c)$ とせよ。元 $v \in S$ を $v(sb - ta) = 0$, $v(tc - ub) = 0$ となるよう共通に取ると，$(vt)(sc - ua) = u[v(sb - ta)] + s[v(tc - ub)] = 0$ であるから，$(s, a) \sim (u, c)$ となる。 □

商集合 $X/\sim$ を $S^{-1}A$ と書き, 元 $(s, a) \in X$ に対し，(s, a) を含む同値類 $\overline{(s, a)}$ を，$\dfrac{a}{s}$ で表す。

補題 7.3. $a, b \in A$ とする。次の主張が正しい。

(1) $s, t \in S$ のとき，$\dfrac{a}{s} = \dfrac{b}{t}$ である必要かつ十分条件は，等式 $u(sb - ta) = 0$ を満たす元 $u \in S$ が存在することである。

(2) $\forall s,t \in S$ に対し，$\dfrac{a}{s} = \dfrac{ta}{ts}$ である。

(3) $\forall s,t \in S$ に対し，$\dfrac{0}{s} = \dfrac{0}{t}$, $\dfrac{s}{s} = \dfrac{t}{t}$ である。

(4) $\forall s,t \in$ に対し，$\dfrac{sa}{s} = \dfrac{ta}{t}$ である。

定理 7.4. 集合 $S^{-1}A$ は，次の和と積

$$\frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}, \quad \frac{a}{s}\cdot\frac{b}{t} = \frac{ab}{st}$$

を演算に可換環となる。$0 \notin S$ であるので $S^{-1}A$ は零環ではない。環 $S^{-1}A$ を環 A の S による**局所化**（11.4 参照）という。

問題 7.5. 定理 7.4 を証明せよ。

写像 $f : A \to S^{-1}A, f(a) = \dfrac{a}{1}$ は，環の準同型写像である。f を**局所化の自然な写像**と呼ぶ。

問題 7.6. 次の主張が正しい。確かめよ。

(1) $\forall s \in S$ について，$f(s) \in (S^{-1}A)^{\times}$ である。

(2) 環 $S^{-1}A$ のいかなる元 x も，$a \in A$ と $s \in S$ を用いて，$x = f(a)f(s)^{-1}$ という形に表すことができる。

(3) $\mathrm{Ker}\, f = \{a \in A \mid \text{ある } s \in S \text{ が存在して } sa = 0\}$ である。

定理 7.7. 環の射 $g : A \to B$ が条件 $g(S) \subseteq B^{\times}$ を満たすなら，等式 $g = h \cdot f$ を満たす環の準同型写像 $h : S^{-1}A \to B$ が唯一つ定まる。

証明. $x \in S^{-1}A$ を取り，$x = \dfrac{a}{s} = \dfrac{a'}{s'}$ と表すと，ある元 $u \in S$ があって等式 $u(sa' - s'a) = 0$ が成り立ち，

$$g(u)[g(s)g(a') - g(s')g(a)] = 0$$

となる。$g(u) \in B^{\times}$ であるから，$g(s)g(a') = g(s')g(a)$ となり, 等式 $g(a)g(s)^{-1} = g(a')g(s')^{-1}$ が得られる。故に，写像 $h : S^{-1}A \to B, h(\frac{a}{s}) = g(a)g(s)^{-1}$ は well-defined であり，$\forall a \in A$ に対し

$$(hf)(a) = h\left(\frac{a}{1}\right) = g(a)g(1)^{-1} = g(a)$$

が成り立つ。写像 h が環の準同型写像であることは，容易に確かめることができる。写像 h の一意性は明らかであるから，証明を省く。

□

問題 7.8. 定理 7.7 の証明を完成せよ。

7.2 全商環と商体

A は可換環とする。環 A の非零因子全体のなす集合を S とすると，自然な写像 $f : A \to S^{-1}A,\ a \mapsto \frac{a}{1}$ は単射である（問題 7.6 (3)）から，埋め込みの原理より，環 Q と環の同型 $g : S^{-1}A \to Q$ の組 (Q, g) で，次の 2 条件を満たすものが存在する。

(1) Q は A を部分環として含む。

(2) $g \cdot f = i$ である。

但し，$i : A \to Q$ は埋め込みの写像である。

定理 7.9. このとき，次の主張が正しい。

(3) 環 A の非零因子は全て環 Q の単元である。

(4) いかなる $x \in Q$ も，元 $a \in A$ と環 A の非零因子 $s \in A$ を選んで

$$x = as^{-1} = \frac{a}{s}$$

と表すことができる。

得られた環 Q を環 A の**全商環**と呼び，$\mathrm{Q}(A)$ と書く。A が整域なら $\mathrm{Q}(A)$ は体をなす。整域 A に対し，体 $\mathrm{Q}(A)$ を A の**商体**という。

次の定理は今や明らかである。

定理 7.10. 整域は体の部分環である。

環 $\mathbb{Z}$ の商体 $\mathrm{Q}(\mathbb{Z})$ を $\mathbb{Q}$ と書き，体 $\mathbb{Q}$ の元を**有理数**と呼ぶ。

8　多項式環

8.1　多項式環と代入原理

以下，単に環といえば，**可換環**を意味する。

定義 8.1. S は環，A は環 S の部分環，$X \in S$ とする。$a_0, a_1, \cdots, a_n \in A$ $(n \geq 0)$ について，S **内で等式** $a_0 + a_1X + \cdots + a_nX^n = 0$ **が成立するなら必ず** $a_i = 0$ $(0 \leq i \leq n)$ **が成り立つ**とき，X は A 上**超越的**であるという。X が A 上超越的でないとき，X は A 上**代数的**であるという。

定理 8.2. 環 A を与えれば，次の 3 条件を満たす組 (S, X) が存在する。

(1) S は環で，A は S の部分環である。

(2) $X \in S$ で A 上超越的である。

(3) $\forall f \in S$ は，元 $a_0, a_1, \cdots, a_n \in A$ $(n \geq 0)$ をうまく選んで，S 内で

$$f = a_0 + a_1X + \cdots + a_nX^n$$

という形に表すことができる。

環 S の元を A 上 X に関する多項式という。S を A 上 X を**不定元**（「変数」ということがないわけではない）に持つ**多項式環**と呼び，$S = A[X]$ と表す。S の元 f に対し，定理 8.2 (3)

の表現は一意的である（一意性の意味は，注意 8.4 を参照せよ)。従って，$f \neq 0$ のとき，定理 8.2 (3) の表現を $a_n \neq 0$ となるよう選べば，整数 $n \geq 0$ が f に対し一意的に定まる。この n を f の次数と呼び，$\deg f$ で表す。

補題 8.3. $A[X]$ は多項式環とする。$0 \neq f, g \in A[X]$ とし，$\deg f = m$, $\deg g = n$ とおき

$$f = a_0 + a_1X + \cdots + a_mX^m, \quad g = b_0 + b_1X + \cdots + b_nX^n$$

$(a_i, b_j \in A,\ a_m, b_n \neq 0)$ と表す。このとき，a_m が環 A の非零因子なら

$$fg \neq 0, \ \deg(fg) = \deg f + \deg g$$

となる。従って，環 A が整域なら多項式環 $A[X]$ も整域である。

証明. 積 fg を展開すると，$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + (a_mb_n)X^{m+n}$ となる。$a_mb_n \neq 0$ であるから，$fg \neq 0$ であり，等式 $\deg(fg) = m + n$ が従う。 □

定理 8.2 の証明は後回しにし, 多項式環 $A[X]$ の性質を述べる。言葉の定義をしよう。加法群 M の元の族 $\{a_i\}_{i\in I}$（但し $I \neq \emptyset$ とする）が与えられたとき

$$\text{殆ど全ての } \mathbf{i} \in \mathbf{I} \text{ に対して } \mathbf{a_i} = \mathbf{0} \text{ である}$$

とは，$\sharp\{i \in I \mid a_i \neq 0\} < \infty$ であるとき，即ち集合 I の次のような空でない有限部分集合 J

$$i \in I \setminus J \text{ なら, } a_i = 0 \text{ である}$$

が存在することをいう。このとき

$$\sum_{i\in I} a_i = \sum_{i\in J} a_i$$

と定め , $\{a_i\}_{i\in I}$ の和と呼ぶ。この定義は集合 J の取り方によらない。$\{b_i\}_{i\in I}$ が M の元の族で，殆ど全ての $i \in I$ に対して $b_i = 0$ なら

$$-\sum_{i\in I} a_i = \sum_{i\in I}(-a_i), \quad \sum_{i\in I} a_i + \sum_{i\in I} b_i = \sum_{i\in I}(a_i + b_i)$$

が成り立つ。

注意 8.4. $I = \{i \in \mathbb{Z} \mid i \geq 0\}$ とおくとき，定理 8.2 (3) は，任意の $f \in S$ に対し，殆ど全ての $i \in I$ に対し $a_i = 0$ となるような A の元の族 $\{a_i\}_{i \in I}$ が存在して等式 $f = \sum_{i \in I} a_i X^i$ が成り立つことを意味し，定理 8.2 (2) は，そのような族 $\{a_i\}_{i \in I}$ が f に対しただ一通りに定まることを示す。

定理 8.5 (代入原理). $A[X]$ は多項式環，$\psi : A \to T$ は環の準同型写像とする。このとき，各 $t \in T$ に対し，環準同型写像 $\varphi : A[X] \to T$ で次の 2 条件を満たすものがただ一つ定まる。

(1) $\forall a \in A$ に対し $\varphi(a) = \psi(a)$ である。

(2) $\varphi(X) = t$ である。

各元 $f \in S$ に対し，$\varphi(f)$ を $f(t)$ と書き，X に t を代入した f の**値**という。

証明. $I = \{i \in \mathbb{Z} \mid i \geq 0\}$ とおき，$f \in A[X]$ を $f = \sum_{i \in I} a_i X^i$ と表す。但し，$\{a_i\}_{i \in I}$ は A の元の族で，殆ど全ての $i \in I$ に対し $a_i = 0$ であるものとする。このような族 $\{a_i\}_{i \in I}$ は，f に対し唯一通りに定まるので，写像 $\varphi : A[X] \to T$ を $\varphi(f) = \sum_{i \in I} \psi(a_i) t^i$ によって定めることができる。$f, g \in A[X]$ に対し，$f = \sum_{i \in I} a_i X^i$, $g = \sum_{i \in I} b_i X^i$ と表せば，$f + g = \sum_{i \in I} (a_i + b_i) X^i$ であるから，等式 $\varphi(f + g) = \sum_{i \in I} \psi(a_i + b_i) t^i = \sum_{i \in I} \psi(a_i) t^i + \sum_{i \in I} \psi(b_i) t^i = \varphi(f) + \varphi(g)$ が得られる。写像 φ の加法性から，$f = aX^i$, $g = bX^j$ として十分であるので，φ が積を保つことが容易に従う。定義により $\varphi(X) = t$ である。また，$a \in A$ なら $\varphi(a) = \psi(a)$ であるから，$\varphi(1) = 1$ である。写像 φ の一意性は明らかである。 □

系 8.6. $A[X]$ と $A[Y]$ が多項式環なら，環の**同型写像** $\varphi : A[X] \to A[Y]$ で

$$\varphi(X) = Y \text{ であって } \varphi(a) = a, \ \forall a \in A$$

となるものが一意的に定まる。即ち，多項式環 $A[X]$ は A-**代数**として同型の範囲で唯一つ定まる（9.3 参照）。

多項式は**関数ではない**。

例 8.7. k を有限体とし, 多項式

$$f = \prod_{a \in k} (X - a) \in k[X]$$

を考えると，$\forall a \in k$ について $f(a) = 0$ であるが，$k[X]$ は整域であるから，$k[X]$ 内で $f \neq 0$ である。

8.2 多項式環の構成

多項式環を構成しよう。$C = \{(a_0, a_1, a_2, \cdots) \mid a_i \in A\}$ とおく。$f, g \in C$ を取り，$f = (a_0, a_1, a_2, \cdots)$, $g = (b_0, b_1, b_2, \cdots)$ とし，次のように C 内の和と積

$$\begin{aligned} f + g &= (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots), \\ f \cdot g &= (a_0 b_0, a_0 b_1 + a_1 b_0, \cdots, \sum_{i+j=n} a_i b_j, \cdots). \end{aligned}$$

を定めると, C は可換環となる。($0 = (0, 0, \cdots), 1 = (1, 0, 0 \cdots)$, $-f = (-a_0, -a_1, \cdots, -a_n, \cdots)$ である。）そこで

$$T = \{f \in C \mid \text{殆ど全ての } i \in I \text{ に対し } a_i = 0\}$$

とおくと, T は環 C の部分環をなす。但し $I = \{i \in \mathbb{Z} \mid i \geq 0\}$ である。写像 $\phi : A \to T$ を $a \mapsto (a, 0, 0, \cdots)$ によって定め，$t = (0, 1, 0, 0, \cdots)$ とおく。すると，任意の $i \in I$ に対し $t^i = (0, \cdots, 0, 1, 0, \cdots)$（1 は第 i 番目にのみ現れる）であり，任意の $f = (a_0, a_1, a_2, \cdots) \in C$ に対し等式 $f = \sum_{i \in I} \phi(a_i) t^i$ が成り立つ。写像 ϕ は環の準同型写像で単射であるから，埋め込みの原理により，A を部分環として含むような環 S と環の同型 $\xi : C \to S$ を求めて，$\xi\phi = i$ （$i : A \to S$ は埋め込み）が成り立つようにすることができる。$X = \xi(t)$ とおけば, 即ち多項式環 $S = A[X]$ が得られる。

定義 8.8. $n > 0$ は整数とし, $I = \{(\alpha_1, \alpha_2, \cdots, \alpha_n) \mid 0 \leq \alpha_i \in \mathbb{Z}\}$ とおく。与えられた環 A に対し, 次の条件を満たす組 $(S, \{X_i\}_{1 \leq i \leq n})$ が存在する。

(1) S は環で，A は S の部分環である。

(2) 任意の $f \in S$ は，殆ど全ての $\alpha \in I$ に対して $a_\alpha = 0$ であるような，A の元の族 $\{a_\alpha\}_{\alpha \in I}$ を用いて

$$f = \sum_{\alpha \in I} a_\alpha X^\alpha$$

という形に表わすことができる。

(3) 各 $f \in S$ に対し (2) の表現は一意的である。

但し，$\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in I$ に対し，$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n}$ と定める。

環 S を，A 上 $X_1, X_2, \cdots, X_n$ を不定元とする**多項式環**と呼び，$S = A[X_1, X_2, \cdots, X_n]$ で表す。

$A[X_1, X_2, \cdots, X_n]$ の構成法は

$$A[X_1, X_2, \cdots, X_{n-1}, X_n] = (A[X_1, X_2, \cdots, X_{n-1}])[X_n] \quad (n \geq 2)$$

である。このように帰納的に定義された環 $A[X_1, X_2, \cdots, X_n]$ が，定義 8.8 の条件を満たすことは，確かめなければならない。

命題 8.9 (代入原理). $A[X_1, X_2, \cdots, X_n]$ は環 A 上の多項式環とする。$\psi : A \to T$ は環の準同型写像，$t_1, t_2, \cdots, t_n \in T$ とする。このとき，$\varphi(X_i) = t_i$ $(1 \leq i \leq n)$ であって 任意の $a \in A$ について $\varphi(a) = \psi(a)$ が成り立つような環準同型写像 $\varphi : A[X_1, X_2, \cdots, X_n] \to T$ がただ一つ定まる。

証明. 定理 8.5 の証明と同様である。n についての帰納法でも証明することができる　□

例 8.10. 体 k 上の多項式環 $S = k[X_1, X_2, \cdots, X_n]$ $(n \geq 1)$ は整域であるから，その商体 $\mathrm{Q}(S)$ を $k(X_1, X_2, \cdots, X_n)$ と表す。従って，任意の $\xi \in k(X_1, X_2, \cdots, X_n)$ は，$f, g \in k[X_1, X_2, \cdots, X_n]$ $(g \neq 0)$ を用いて，$\xi = \dfrac{f}{g}$ $(= f \cdot g^{-1})$ と表すことができる。$k(X_1, X_2, \cdots, X_n)$ を体 k 上 n 変数の**有理関数体**という。

8.3 代数と部分代数

A は環とする。環 B に対し，環の準同型写像 $\psi : A \to B$ が一つ指定されているとき，B **は** A**-代数である**という。写像 ψ を A-代数 B の**構造射**といい，ψ_B と書くことがある。B が A-代数であって C が B の部分環のとき，$\psi_B(A) \subseteq C$ なら，環準同型写像 $\psi_C : A \to C, a \mapsto \psi_B(a)$ によって，環 C は A-代数となる。このとき，C は B の A-部分代数であるという。

問題 8.11. 環はすべてただ一通りの見方で $\mathbb{Z}$-代数となる。確かめよ。

A は環，B は A-代数とせよ。$x_1, x_2, \cdots, x_n \in B$ $(n \geq 1)$ を与えると，多項式環からの代入射

$$\varphi : A[X_1, X_2, \cdots, X_n] \to B,\ \varphi(X_i) = x_i\ (1 \leq \forall i \leq n)$$

が得られる。写像 φ は環の準同型写像であるから，像 $\operatorname{Im}\varphi$ は B の部分環である。

$$A[x_1, x_2, \cdots, x_n] = \operatorname{Im}\varphi = \{f(x_1, x_2, \cdots, x_n) \mid f \in A[X_1, X_2, \cdots, X_n]\}$$

とおき，環 $A[x_1, x_2, \cdots, x_n]$ を $x_1, x_2, \cdots, x_n$ **で生成された** B **の** A**-部分代数**と呼び，多項式環 $A[X_1, X_2, \cdots, X_n]$ のイデアル

$$\operatorname{Ker}\varphi = \{f \in A[X_1, X_2, \cdots, X_n] \mid f(x_1, x_2, \cdots, x_n) = 0\}$$

を，$x_1, x_2, \cdots, x_n$ **の環** A **上の関係式がなすイデアル**，あるいは，A-代数 $A[x_1, x_2, \cdots, x_n]$ の**定義イデアル**と呼ぶ。

例 8.12. $A = k[X, Y, Z]$ と $B = k[t]$ をそれぞれ体 k 上の多項式環とし，代入射 $\varphi : A \to B$, $\varphi(X) = t^3$,$\varphi(Y) = t^4$,$\varphi(Z) = t^5$ を考え，$\mathfrak{p} = \operatorname{Ker}\varphi$ とする。このとき，$\mathfrak{p}$ は環 A の素イデアルであって，等式

$$\mathfrak{p} = (X^3 - YZ,\ Y^2 - XZ,\ Z^2 - X^2Y)$$

が成り立つ。即ち，k-代数 $k[t^3, t^4, t^5]$ の定義イデアル $\mathfrak{p}$ は 3 元 $X^3 - YZ,\ Y^2 - XZ,\ Z^2 - X^2Y$ で生成される。

証明. $A/\mathfrak{p} \cong \varphi(A)$ であるから $\mathfrak{p}$ は環 A の素イデアルである。$I = (X^3 - YZ,\ Y^2 - XZ,\ Z^2 - X^2Y)$ とおく。$\varphi(X^3 - YZ) = \varphi(Y^2 - XZ) = \varphi(Z^2 - X^2Y) = 0$ であるから，$X^3 - YZ, Y^2 - XZ, Z^2 - X^2Y \in \mathrm{Ker}\,\varphi$ となり，$I \subseteq \mathfrak{p}$ を得る。

$L = \{(\alpha, \beta, \gamma) \in \mathbb{Z}^3 \mid \alpha, \beta, \gamma \geq 0\}$ とおき，整数 $n \in \mathbb{Z}$ に対し

$$\Lambda_n = \{(\alpha, \beta, \gamma) \in L \mid 3\alpha + 4\beta + 5\gamma = n\}$$

と定める。すると $L = \bigcup_{n\in\mathbb{Z}} \Lambda_n$ であり，各 Λ_n は高々有限集合であって，$m \neq n$ なら $\Lambda_m \cap \Lambda_n = \emptyset$ となる。

$n \in \mathbb{Z}$ に対し，$\Lambda_n \neq \emptyset$ のときは

$$A_n = \left\{ \sum_{\lambda=(\alpha,\beta,\gamma)\in\Lambda_n} c_\lambda X^\alpha Y^\beta Z^\gamma \mid c_\lambda \in k \right\}$$

と置き，$\Lambda_n = \emptyset$ のときは $A_n = (0)$ と定める（$A_0 = k, A_n = (0)\ (n < 0)$ である）と，$\{A_n\}_{n\in\mathbb{Z}}$ は A の加法部分群の族であって，各 $f \in A$ は $f = \sum_{n\in\mathbb{Z}} f_n$ (但し，$f_n \in A_n$ で殆ど全ての $n \in \mathbb{Z}$ について $f_n = 0$ とする）という形に一意的に表すことができる。即ち

$$A = \bigoplus_{n\in\mathbb{Z}} A_n (\text{直和})$$

であって，任意の $m, n \in \mathbb{Z}$ と任意の $f \in A_m, g \in A_n$ に対し，$fg \in A_{m+n}$ が成り立つ。（即ち，A は $\{A_n\}_{n\in\mathbb{Z}}$ によって次数付けされた**次数付環**である。）

$\Lambda_n \neq \emptyset$ と仮定し，元 $h \in A_n$ をとり，$h = \sum_{\lambda=(\alpha,\beta,\gamma)\in\Lambda_n} c_\lambda X^\alpha Y^\beta Z^\gamma\ (c_\lambda \in k)$ と表す。すると，$\varphi(h) = \sum_{\lambda=(\alpha,\beta,\gamma)\in\Lambda_n} c_\lambda \cdot (t^3)^\alpha (t^4)^\beta (t^5)^\gamma = (\sum_{\lambda\in\Lambda_n} c_\lambda) t^n$ となり，特に，$\varphi(h) = 0$ であるための必要十分条件は，$\sum_{\lambda\in\Lambda_n} c_\lambda = 0$ であることがわかる。$f \in A$ をとり，$f = \sum_{n\in\mathbb{Z}} f_n$ ($f_n \in A_n$ であって，殆ど全ての $n \in \mathbb{Z}$ について $f_n = 0$）と表すと，$\varphi(f) = \sum_{n\in\mathbb{Z}} \varphi(f_n)$ であって，上に述べたように $\Lambda_n \neq \emptyset$ なら $\varphi(f_n) = ct^n\ (c \in k)$ という形をしていて，$\Lambda_n = \emptyset$ なら $f_n = 0$ であることより

$$\varphi(\mathbf{f}) = \mathbf{0} \text{ なら}, \forall \mathbf{n} \in \mathbb{Z} \text{ に対し} \varphi(\mathbf{f_n}) = \mathbf{0} \text{ である}$$

ことがわかる。即ち，$\mathfrak{p} \subseteq I$ を示すには，任意の $n \in \mathbb{Z}$ に対し $\mathfrak{p} \cap A_n \subseteq I$ が成り立つことを確かめれば十分である。

そこで，ある $n \in \mathbb{Z}$ に対し $\mathfrak{p} \cap A_n \not\subseteq I$ であったと仮定してみよう。すると $A_n \neq (0)$ であるから，$\Lambda_n \neq \emptyset$ であって $n \geq 0$ である。このような整数 $n \in \mathbb{Z}$ を最小に選び，元 $h \in \mathfrak{p} \cap A_n$ を $h \notin I$ となるように取り，$h = \sum_{\lambda=(\alpha,\beta,\gamma)\in\Lambda_n} c_\lambda X^\alpha Y^\beta Z^\gamma$ $(c_\lambda \in k)$ と表すと

$$\varphi(h) = (\sum_{\lambda\in\Lambda_n} c_\lambda)t^n$$

であるから，体 k 内に等式

$$\sum_{\lambda\in\Lambda_n} c_\lambda = 0$$

が得られる。今 $\mu = (\alpha', \beta', \gamma') \in \Lambda_n$ を任意に一つ固定すると

$$h = \sum_{\lambda=(\alpha,\beta,\gamma)\in\Lambda_n} c_\lambda X^\alpha Y^\beta Z^\gamma - \left(\sum_{\lambda\in\Lambda_n} c_\lambda\right) X^{\alpha'} Y^{\beta'} Z^{\gamma'} = \sum_{\lambda\in\Lambda_n} c_\lambda \left(X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'}\right) \notin I$$

であるから，$g = X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'}$ と置くと，$g \notin I$ となる元 $\lambda = (\alpha, \beta, \gamma) \in \Lambda_n$ が存在し，$g \in \mathfrak{p} \cap A_n$ ではあるが $g \notin I$ となっているはずである。従って矛盾を導くには，一般性を失うことなく，$h = X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'} \in A_n$ としてよいことがわかる。

このような元 $h = X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'}$ については，$\alpha = 0$ であるかまたは $\alpha' = 0$ が成り立つ。実際 $\alpha, \alpha' > 0$ ならば，$h = X \cdot (X^{\alpha-1} Y^\beta Z^\gamma - X^{\alpha'-1} Y^{\beta'} Z^{\gamma'}) \in \mathfrak{p}$ であり $\mathfrak{p}$ は素イデアルで $X \notin \mathfrak{p}$ であるから，$h' = X^{\alpha-1} Y^\beta Z^\gamma - X^{\alpha'-1} Y^{\beta'} Z^{\gamma'} \in \mathfrak{p} \cap A_{n-3}$ が従う。$h = Xh' \notin I$ であるから $h' \notin I$ のはずであるが，整数 n の最小性に反する。故に $\alpha = 0$ または $\alpha' = 0$ である。同様に $\beta = 0$ かまたは $\beta' = 0$ であり，$\gamma = 0$ かまたは $\gamma' = 0$ が成り立つ。

さて，もしも $\gamma' \geq 2$ ならば，$Z^2 \equiv X^2 Y \mod I$ より $X^\alpha Y^\beta Z^\gamma \equiv X^{\alpha'} Y^{\beta'} Z^{\gamma'-2} (X^2 Y) \mod \mathfrak{p}$ となる。$X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'-2} (X^2 Y) \notin I$ であるので，上に述べたように $\alpha = \beta = 0$ が従い，$h = Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'}$ となるが，$\gamma' \geq 2$ であるから更に $\gamma = 0$ を得る。ところが，$n = 5\gamma = 3\alpha' + 4\beta' + 5\gamma' = 0$ で $\alpha', \beta', \gamma' \geq 0$ であるから，$h = 0$ が従うが，もちろん不可能である。故に $\gamma' \leq 1$ であって，γ と γ' の対称性より，$\gamma, \gamma' \leq 1$ であることがわかり，一般性を失うことなく，$\gamma = \gamma' = 0$ であるかまたは $\gamma = 1, \gamma' = 0$ であると仮定することができる。

$\gamma = \gamma' = 0$ ならば，$h = X^\alpha - Y^{\beta'}$ $(\alpha, \beta' \geq 1)$ の場合に帰着され，$3\alpha = 4\beta'$ が成り立つ。$\alpha = 4\ell$，$\beta' = 3\ell$ $(1 \leq \ell \in \mathbb{Z})$ と表せば，$h = (X^4)^\ell - (Y^3)^\ell$ で $X^4 \equiv X{\cdot}YZ, Y^3 \equiv Y{\cdot}XZ \mod I$ であるから，直ちに $h \in I$ が得られ，$\gamma = \gamma' = 0$ はあり得ないことがわかる。即ち，$\gamma = 1$，$\gamma' = 0$，$h = X^\alpha Y^\beta Z - X^{\alpha'} Y^{\beta'}$ である。このとき，$\alpha > 0$ ならば $\alpha' = 0, \beta' > 0, \beta = 0$ となり，$h = X^\alpha Z - Y^{\beta'}$ が従う。しかしながら，$XZ \equiv Y^2 \mod I$ であるので $X^{\alpha-1}Y^2 \equiv Y^{\beta'} \mod \mathfrak{p}$ となり，Y で割れば整数 n の最小性が壊れる。故に $\alpha = 0$，$h = Y^\beta Z - X^{\alpha'} Y^{\beta'}$ である。

もし $\beta > 0$ なら $\beta' = 0, \alpha' > 0$ であるが，一方で $X^3 \equiv YZ \mod I$ より $X^{\alpha'} \equiv Y^\beta Z \equiv X^3 Y^{\beta-1} \mod \mathfrak{p}$ となり，X で割ることによって整数 n の最小性が壊れる。故に $\beta = 0$ であり，等式 $5 = 3\alpha' + 4\beta'$ が非負整数 $\alpha', \beta' \geq 0$ について成り立つほかないが，不可能である。故に，すべての $n \in \mathbb{Z}$ について $\mathfrak{p} \cap A_n \subseteq I$ であり，等式 $\mathfrak{p} = I$ が従う。 □

問題 8.13. $A = k[X, Y, Z]$ と $B = k[t]$ をそれぞれ体 k 上の多項式環とし，代入射 $\varphi : A \to B$，$X \mapsto t^4, Y \mapsto t^5, Z \mapsto t^{11}$ を考え，$\mathfrak{p} = \operatorname{Ker} \varphi$ とする。このとき，等式

$$\mathfrak{p} = (X^4 - YZ,\ Y^3 - XZ,\ Z^2 - X^2Y^2)$$

が成り立つ。確かめよ。

問題 8.14. A は環，B は A-代数とする。元 $x_1, x_2, \cdots, x_n \in B$ に対し，環 $A[x_1, x_2, \cdots, x_n]$ は，元 $x_1, x_2, \cdots, x_n$ を含む，B の最小の A-部分代数である。確かめよ。

等式 $B = A[x_1, x_2, \cdots, x_n]$ がなりたつような元 $x_1, x_2, \cdots, x_n \in B$ $(n \geq 1)$ が存在するような A-代数 B は，**A-代数として有限生成である**という。

問題 8.15. 環 A 上の多項式環 $B = A[X_1, X_2, \cdots, X_n]$ $(n \geq 1)$ は，自然に有限生成 A-代数となっている。また，環 B の任意のイデアル I $(I \neq B)$ に対し，環 $C = B/I$ も，自然に有限生成 A-代数となる。確かめよ。

二つの A-代数 B, C に対して，環準同型写像 $\varphi : B \to C$ は，$\varphi \cdot \psi_B = \psi_C$ が成り立つとき，**A-代数の射**であるという。

問題 8.16. A-代数 B に対し，$\mathrm{Aut}_A B = \{\sigma \mid \sigma : B \to B \text{ は } A-\text{代数の射で全単射である}\}$ とおくと，集合 $\mathrm{Aut}_A B$ は群 $\mathrm{Aut}\, B$ の部分群であり，写像の合成を演算に群をなす。確かめよ。

問題 8.17. 問題 5.5 (3) を解け。

問題 8.18. A を環，B を A-代数とする。$S \subseteq B$ に対し

$$A[S] = \bigcup_{x_1, x_2, \cdots, x_n \in S} A[x_1, x_2, \cdots, x_n]$$

とおくと，$A[S]$ は B の A-部分代数であり，S を含む B の A-部分代数の中で最小のものとなる。確かめよ。$A[S]$ を S で生成された部分代数という。

9 体上の一変数の多項式環とその性質

9.1 体上の一変数多項式環

k は体とし，$A = k[X]$ によって k 上の一変数多項式環を表す。A は体ではない整域（補題 8.3 参照）であって，$A^\times = k \setminus \{0\}$ となる。

補題 9.1 (Euclid の互除法)**.** $f \in A$ で $f \neq 0$ なら，任意の $g \in A$ に対し，A の元の組 (q, r) で次の条件を満たすものが，ただ一つ定まる。

(1) $g = fq + r$ である。

(2) $r = 0$ であるか，または $r \neq 0$ であって $\deg r < \deg f$ である。

証明. $\deg f = m$ とおく。条件 (1), (2) を満たす組 (q, r) が存在しないような元 $g \in A$ があったと仮定する。$g \neq 0$ であるから，そのような $g \in A$ で次数 $n = \deg g$ (≥ 0) が最小のものを選ぶことができる。すると $n \geq m$ である。$g = bX^n +$（n より低次の項）$(0 \neq b \in k)$,

$f = aX^m +$(m より低次の項$)$ $(0 \neq b \in k)$ と表し，$h = g - \dfrac{b}{a}X^{n-m} \cdot f$ とおくと，$h \neq 0$ であって $\deg h < n$ であるから，次数 $n = \deg g$ の最小性より，元 h に対し条件 (1)，(2) を満たす組 (q', r) が存在して，$h = fq' + r$ が成り立つはずである。このとき，$g = f(q' + \dfrac{b}{a}X^{n-m}) + r$ となり，g に対しても条件 (1), (2) を満たす元の組 $(q = q' + \frac{b}{a}X^{n-m}, r)$ が存在するが，不可能である。

一意性を確かめよう。$g = fq + r = fq' + r'$ と二通りに書けたとする。等式 $f(q - q') = r' - r$ 内で，もし $r' - r \neq 0$ なら，$q - q' \neq 0$ であって

$$\deg f + \deg(q - q') = \deg(r' - r)$$

が成り立つはずである（補題 8.3 参照）が，$\deg(r' - r) < \deg f$ であるから，不可能である。故に $r = r'$ で，$f(q - q') = 0$ となる。A は整域で $f \neq 0$ であるから，$q = q'$ が得られる。 □

$f, g \in A$ について，$f \in (g)$ であること，即ち A 内で g が f を割り切ることを，$g|f$ と書く。

定理 9.2. 次の主張が正しい。

(1) $f \in A$，$a \in k$ とする。$f(a) = 0$ であるための必要十分条件は，$(X - a)|f$ である。

(2) $0 \neq \forall f \in A$ について，$\sharp\{a \in k \mid f(a) = 0\} \leq \deg f$ である。

証明. (1) $f = (X - a)q + r$ $(r \in k)$（補題 9.1 参照）と表せば，$f(a) = r$ が得られる。故に，$f(a) = 0$ と $X - a \mid f$ は同値である。

(2) $a \in k$ が f の根ならば，$f = (X - a)q$ $(q \in A)$ と表すことが出来る。$b \in k$ が a とは異なる根であれば，$f(a) = (a - b)q(b) = 0$ より，$q(b) = 0$ である。故に，$q = (X - b)q_1$ $(q_1 \in A)$ と表すことが出来る。この議論は高々 $\deg f$ 回しか行うことが出来ない。故に，f はたかだか $\deg f$ 個しか k 内に根を持たない。 □

系 9.3. k が有限体ではないなら，k の元をすべて根に持つ $f \in A$ は，$f = 0$ に限る。

系 9.4. 環 $A = k[X]$ のイデアルはすべて単項である。

証明. 環 A のイデアル $I \neq (0)$ を取る。 $I = (f)$ $(f \in A)$ を示したい。$I \neq (0)$ としてよい。I の元 $f \neq 0$ を $\deg f$ が最小になるように取る。このとき，任意の $g \in I$ に対し，補題 9.1 より，等式 $g = fq + r$ が成り立つような元 $q, r \in A$ を，$r \neq 0$ なら $\deg r < \deg f$ を満たすように選ぶことができる。もし $r \neq 0$ なら，$r = g - fq \in I$ であって $\deg r < \deg f$ であるから，$\deg f$ の最小性が壊れる。故に $r = 0$ で，$g = fq \in (f)$ である。 □

定義 9.5. $f \in A$ とせよ。次の 2 条件を満たすとき，多項式 f は k 内で**既約**であるという。

(1) $f \notin k$ である。

(2) $g, h \in A$ について，等式 $f = gh$ が成り立つなら，$g \in k$ であるか $h \in k$ である。

定理 9.6. 次の主張が正しい。

(1) $f \in A$ が k 内で既約なら，(f) は A の極大イデアルで，環 $A/(f)$ は体をなす。

(2) M が A の極大イデアルなら，$M = (f)$ となる多項式 $f \in A$ をとると，f は必ず k 内で既約である。

証明. (1) $I = (f)$ とおく。$f \notin k$ であるから，$I \neq A$ である。J は A のイデアルで $I \subseteq J \subsetneq A$ なるものとする。$J = (g)$ と表す。$g \notin k$ で $f \in (g)$ であるから $f = gh$ $(h \in k[X])$ と表すと，f は既約なので，$0 \neq h \in k$ となる。故に，$g = fh^{-1} \in I$ となり，$J \subseteq I$ が得られ，等式 $I = J$ が従う。故に I は極大イデアルである。

(2) $f \notin k$ である。$f = gh$ $(g, h \in A, g \notin k)$ と仮定せよ。このとき，$M = (f) \subseteq (g) \subsetneq A$ であるから，イデアル M の極大性より $(f) = (g)$ が従う。$g = f\ell$ $(\ell \in A)$ とすると，$f = gh = f(\ell h)$ より，$\ell h = 1$ となる。故に $h \in k$ であり，多項式 f は k 内で既約である。 □

極大イデアルは素イデアルであるから，次が正しい。

系 9.7. $f \in A$ は k 内で既約とする。このとき，$g, h \in A$ について $f|gh$ なら，$f|g$ または $f|h$ が成り立つ。

$k = \mathbb{R}$ のとき $f = X^2 + 1 \in \mathbb{R}[X]$ は $\mathbb{R}$ 内で既約である。実際，$g, h \in \mathbb{R}[X]$ をとり，$X^2 + 1 = gh$，$g, h \notin \mathbb{R}$ とする。すると

$$\deg(X^2 + 1) = \deg g + \deg h = 2$$

であるから，$\deg g = \deg h = 1$ である。$a, b, c, d \in \mathbb{R}$ $(a, c \neq 0)$ をとり $g = aX + b$, $h = cX + d$ とかくと，$X^2 + 1 = (ac)X^2 + (ad + bc)X + bd$ であるから

$$ac = 1, \quad ad + bc = 0, \quad bd = 1$$

となる。よって，$\frac{a}{b} + \frac{b}{a} = 0$ が従い，$a^2 + b^2 = 0, a \neq 0, b \neq 0$ が得られるが，これは $\mathbb{R}$ 内では不可能である。故に $f = X^2 + 1$ は $\mathbb{R}$ 内で既約であり，$\mathbb{R}[X]/(X^2 + 1)$ は体をなす。

問題 9.8 (複素数体 $\mathbb{C}$)**.** 体 $\mathbb{R}[X]/(X^2 + 1)$ と体 $\mathbb{C}$ とは，$\mathbb{R}$-代数として同型である。確かめよ（定理 10.3 参照）。

複素数体 $\mathbb{C}$ の構成の仕方には，もう一つ，行列環 $\mathrm{M}_2(\mathbb{R})$ の部分環

$$\mathbb{C} \cong \left\{ \left(\begin{array}{cc} x & y \\ -y & x \end{array} \right) \middle| x, y \in \mathbb{R} \right\} \subseteq \mathrm{M}_2(\mathbb{R})$$

を用いる方法がある。対応は $a + bi \mapsto \left(\begin{array}{cc} a & b \\ -b & a \end{array} \right)$ $(a, b \in \mathbb{R})$ である。

定理 9.9. $f \in A$ が定数でないならば，k 内で既約な多項式 $p_1, p_2, \cdots, p_n \in A$ $(n \geq 1)$ を選んで $f = p_1 p_2 \cdots p_n$ と表すことができる。この表現は, 定数と順序の違いを除いて，f に対し一意的に定まる。

証明. 定理のようには表すことが出来ない $f \in A$ が存在したと仮定し，$\deg f$ を最小にとる。すると f は既約ではないので，定数ではない $g, h \in A$ を選んで，$f = gh$ と表すことが出来

る。$\deg g < \deg f, \deg h < \deg f$ であるから，$\deg f$ の最小性より，g, h はそれぞれ有限個の既約多項式の積として表すことができ，多項式 f も有限個の既約多項式の積となるが，不可能である。

次に，$f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ (p_i, q_j は既約多項式) とせよ。$n = 1$ ならば，$p_1 = q_1 q_2 \cdots q_m$ であって，p_1 は既約であるから，$m = 1$ が従う。$n > 1$ とし，$n-1$ 以下では一意性が正しいと仮定する。すると，$q_1 q_2 \cdots q_m \in (p_1)$ であるから，系 9.7 より，ある既約多項式 q_i について，$q_i \in (p_1)$，即ち $q_i = c_1 p_1 \ \ (0 \neq c_1 \in k)$ が成り立つ。並べ替えて $q_1 = c_1 p_1$ と仮定してよい。すると，$(c_1 p_2) \cdot p_2 \cdots p_n = q_2 q_3 \cdots q_m$ であるが，$c_1 p_2$ は既約多項式であるから，帰納法の仮定より，$n = m$ と $q_i = c_i q_i \ \ (2 \leq i \leq n)$ とが従う。 □

系 9.10. $\mathrm{Max}\, A = \{M \mid M \text{ は } A \text{ の極大イデアル}\}$ は，有限集合でない。

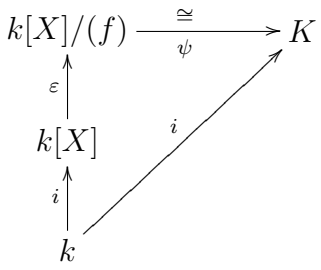
証明. $n = \sharp \mathrm{Max}\, A < \infty$ と仮定し，$\mathrm{Max}\, A = \{M_1, M_2, \cdots, M_n\}$ とする。各 $1 \leq j \leq n$ に対し，$M_j = (f_j)$ となる既約多項式 $f_j \in A$ をとり，$f = 1 + \prod_{j=1}^{n} f_j$ とおくと，多項式 $f \in A$ は定数ではないので，定理 9.9 により，$f = p_1 p_2 \cdots p_m \ \ (m \geq 1$，各 p_iは既約多項式) の形に因数分解される。$M = (p_1)$ とせよ。故に $f \in M$ である。一方で，M は A の極大イデアルであるから，ある $1 \leq i \leq n$ があって，$M = M_i$ となる。このとき，$f_i \in M$ であるから，$f, f_i \in M$ が成り立ち，従って $1 = f - \prod_{j=1}^{n} f_j \in M$ となるが，不可能である。 □

体 K が体 k を部分環として含むとき，K は k の**拡大体**である，または K/k は**体の拡大**であるという。

定理 9.11 (Kronecker の分解定理)**.** 定数でない $f \in A$ を与えれば，k の拡大体 K をうまく選んで，f は K 内に少なくとも一つの根を持つようにすることが出来る。

証明. 定理 9.9 より，f は k 内で既約として十分である。定理 9.6 より $k[X]/(f)$ は体をなす。合成射 $k \xrightarrow{i} k[X] \xrightarrow{\varepsilon} k[X]/(f)$ を通し，体 $k[X]/(f)$ を k-代数とみなす。但し i は埋め込みの

写像である。下の図



内で，射 $k \xrightarrow{i} k[X] \xrightarrow{\varepsilon} k[X]/(f)$ は単射であるから，埋め込みの原理（定理 6.4）より，k の拡大体 K とこの図を可換にするような環の同型写像 ψ の組 (K, ψ) が得られる。$\alpha = \psi(\overline{X})$ とおくと，$\alpha \in K$ であって，$f(\alpha) = \psi(\overline{f}) = 0$ が成り立つ。 □

系 9.12. 定数ではないいかなる $f \in k[X]$ に対しても，k の拡体体 K を選んで，f が K 内で一次式の積に分解するようにできる。

既約性の判定は必ずしも容易ではない。

問題 9.13. $k = \mathbb{Z}/(2)$ とするとき $X^2 + X + 1$ は k 内で既約である。任意の $n \geq 1$ に対し，n 次の 既約多項式が環 $k[X]$ 内に少なくとも一つは存在することを証明せよ。

9.2 Eisenstein の既約判定法

目標は次の定理である。

定理 9.14 (Eisenstein の既約判定法)**.** $a_0, a_1, \cdots, a_n \ \ (n \geq 1)$ と p は整数で，p は素数とし，$\mathbb{Z}$ 内で次の 3 条件 $\quad p|a_i, \ \ 0 \leq \forall i \leq n-1 \quad p \not| a_n \quad p^2 \not| a_0$ が満たされていると仮定する。このとき，多項式 $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Q}[X]$ は，$\mathbb{Q}$ 内で既約である。

証明には次の二つの補題を必要とする。

補題 9.15. pが素数なら，pが多項式環 $\mathbb{Z}[X]$ 内で生成する単項イデアル $P = \{pf \mid f \in \mathbb{Z}[X]\}$ は，$\mathbb{Z}[X]$ の素イデアルである。

証明. $k=\mathbb{Z}/(p)$ とし $k[Y]$ は体 k 上の多項式環とする。射 $\mathbb{Z}\xrightarrow{\varepsilon}k\xrightarrow{i}k[Y]$ によって $k[Y]$ を $\mathbb{Z}$-代数とみなす。(但し ε は自然な環準同型写像, i は埋め込み写像を表す。) 代入射 $\varphi:\mathbb{Z}[X]\to k[Y], X\mapsto Y$ を見るに, $f=a_0+a_1X+\cdots+a_nX^n$ $(a_i\in\mathbb{Z})$ なら

$$\varphi(f)=\overline{a_0}+\overline{a_1}Y+\cdots+\overline{a_n}Y^n$$

$(\overline{a_i}=\varepsilon(a_i))$ であるから, φ が全射で $\operatorname{Ker}\varphi=P$ となることが容易に従う。故に P は素イデアルである。 □

補題 9.16. $f\in\mathbb{Z}[X]$, $\varphi,\psi\in\mathbb{Q}[X]$ とし, φ,ψ は定数ではないと仮定する。$f=\varphi\psi$ なら, 多項式 $g,h\in\mathbb{Z}[X]$ を選んで, $f=gh$ かつ $\deg g=\deg\varphi$, $\deg h=\deg\psi$ が成り立つようにすることができる。

証明. 自然数 a,b を $a\varphi,b\psi\in\mathbb{Z}[X]$ にとり, $c=ab$ とおく。$cf=(a\varphi)(b\psi)$ であり, 等式 $\deg\varphi=\deg a\varphi$, $\deg\psi=\deg b\psi$ が成り立つ。故に, 自然数 c と多項式 $g,h\in\mathbb{Z}[X]$ が存在して,

$$cf=gh,\quad \deg g=\deg\varphi,\quad \deg h=\deg\psi$$

が成り立つことがわかる。このような $g,h\in\mathbb{Z}[X]$ を選ぶことが出来る自然数 c を最小に選ぶ。このとき, $c\neq1$ なら $p|c$ となる素数 $p\geq2$ をとり $P=\{pf\mid f\in\mathbb{Z}[X]\}$ とおくと, 補題 9.15 より P は $\mathbb{Z}[X]$ の素イデアルであって $gh=cf\in P$ であるから, $g\in P$ かまたは $g\in P$ が成り立つ。もし $g\in P$ ならば, $g=pg_1$ $(g_1\in\mathbb{Z}[X])$ と表すと, $\dfrac{c}{p}\cdot f=g_1h$ となって, 自然数 c の最小性が壊れる。故に $c=1$ である。 □

Eisenstein の定理の証明をしよう。

証明. 条件　,　,　が満たされるが, 多項式 f が $\mathbb{Q}$ 内で既約でないならば, 補題 9.16 によって, 定数ではない二つの多項式 $g,h\in\mathbb{Z}[X]$ を選んで, $f=gh$ と表すことができる。$\ell=\deg g, m=\deg h$ とおく。補題 9.15 の証明内の代入射 $\varphi:\mathbb{Z}[X]\to k[Y], X\mapsto Y$ を考え,

$\overline{f} = \varphi(f), \overline{g} = \varphi(g), \overline{h} = \varphi(h)$ とおく。g の ℓ 次の項の係数を b_ℓ とし h の m 次の項の係数を c_m とすると，$a_n = b_\ell c_m$ であるから，条件　より $p \not| b_\ell, p \not| c_m$ となり，等式

$$\deg \overline{g} = \ell > 0, \quad \deg \overline{h} = m > 0$$

が従う。一方で，$\overline{f} = \overline{g}\overline{h}$ であるから，条件　より $\overline{g}\overline{h} = \overline{a_n} Y^n$ が得られる。$Y \in k[Y]$ は既約であるから，素因数分解の一意性（定理 9.9）より $\overline{g} = \overline{b_\ell} Y^\ell, \overline{h} = \overline{c_m} Y^m$ と表すことを得るが，このことは同時に，g, h の定数項がどちらも p の倍数であることを導く。g の定数項と h の定数項の積は f の定数項 a_0 に等しいので，$p^2 | a_0$ が従うが，条件　に反する。故に f は $\mathbb{Q}$ 内で既約である。 □

系 9.17. $a, p \in \mathbb{Z}$ とし，p は素数，$\mathbb{Z}$ 内で $p|a$ であるがしかし $p^2 \not| a$ と仮定せよ。このとき，任意の自然数 $n > 0$ に対し，多項式 $X^n - a \in \mathbb{Z}[X]$ は $\mathbb{Q}$ 内で既約である。

問題 9.18. 任意の素数 $p \geq 2$ に対し，多項式 $f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ は，$\mathbb{Q}$ 内で既約であることを証明せよ。

10　体の代数拡大

k は体とし $A = k[X]$ は多項式環とする。K/k は体の拡大とする。

K 内の積を用いて，K を k 上のベクトル空間と見ることが出来る。このとき k 上のベクトル空間としての K の次元を $[K : k]$ で表し，K/k の拡大次数という。$L/K, K/k$ を体の拡大とすると

$$[L : k] = [L : K][K : k]$$

が成り立つ。

$\alpha \in K$ とせよ。埋め込み写像 $i : k \to K$ によって体 K を k-代数とみなし，代入射 $\varphi : A = k[X] \to K, \varphi(X) = \alpha$ を考え，$P = \mathrm{Ker}\, \varphi$ とおく。$\varphi(A)$ は K の部分環で $A/P \cong \varphi(A)$ であるから，A/P は整域であり，故に P は環 A の素イデアルである。元 $\alpha \in K$ が k 上で代数的

であることと $P \neq (0)$ であることは同値である。α は k 上代数的であると仮定しよう。すると，$0 \neq f \in P$ を次数 $n = \deg f$ が最小になるよう取り，n 次の項 X^n の係数が 1 であるようにすることが出来る。このとき次が正しい。

補題 10.1. $P = (f)$ であって，f は k 内で既約である。

証明. $g \in P$ を取り，$g = fq + r$ $(q, r \in A$ であって, $r \neq 0$ なら $\deg r < n)$ と表すと，$g(\alpha) = f(\alpha)q(\alpha) + r(\alpha)$ より，$r(\alpha) = 0$ となり，$r \in P$ が得られる。次数 $n = \deg f$ の最小性より $r = 0$ が従い，$g \in (f)$，故に $P = (f)$ である。$f = gh$ $(bg, h \in A)$ で g, h が定数でないなら，$\deg g < \deg f, \deg h < \deg f$ であるが，$f(\alpha) = g(\alpha)h(\alpha) = 0$ であるから，$g(\alpha) = 0$ または $h(\alpha) = 0$ が従い，$\deg f$ の最小性が壊れる。故に f は k 内で既約である。, □

このような $f \in P$ は，$\alpha \in K$ に対し，ただ一通りに定まる。実際 $0 \neq g \in P$ が f と同じく，その次数 $n = \deg g$ が最小であって n 次の項 X^n の係数が 1 ならば，系 10.1 より，$P = (f) = (g)$ が得られる。故に $g = fh$ $(h \in A)$ と表すことが出来るが，$\deg f = \deg g$ であって，どちらもその n 次の項 X^n の係数が 1 であるから，$h = 1$，即ち $f = g$ が従う。

定義 10.2. $f \in k[X]$ を元 $\alpha \in K$ の k 上の**最小多項式**という。

定理 10.3. K/k は体の拡大とし，$\alpha \in K$ とせよ。α は k 上代数的であると仮定し，α の k 上の最小多項式を f とする。このとき次の主張が正しい。

(1) f は k 内で既約である。

(2) $k[\alpha]$ は K の部分体であって，k-代数として $k[X]/(f) \cong k[\alpha]$ である。

(3) $[k[\alpha] : k] = \deg f < \infty$ である。

(4) $\beta \in K$ は k 上代数的とし，$g \in k[X]$ を β の k 上の最小多項式とする。このとき，k-代数の同型 $\varphi : k[\alpha] \to k[\beta]$ で $\varphi(\alpha) = \beta$ を満たすものが存在するための必要十分条件は，$f = g$ が成り立つことである。

証明. (3) $n = \deg f$ とおく。$n > 0$ である。$g \in A$ をとり，$g = fq + r$ $(q, r \in A, r \neq 0$ なら $\deg r < n)$ と表すと，$g(\alpha) = r(\alpha)$ である。故に

$$k[\alpha] = \{r(\alpha) \mid r \in A, r \neq 0 \text{ なら } \deg r < n\}$$

が得られ，$1, \alpha, \cdots, \alpha^{n-1}$ が，k-ベクトル空間 $k[\alpha]$ を張ることが分かる。$n = \deg f$ の最小性から直ちに，元 $1, \alpha, \cdots, \alpha^{n-1}$ が k 上で一次独立であることが従う。故に，$1, \alpha, \cdots, \alpha^{n-1}$ は，k 上のベクトル空間 $k[\alpha]$ の基底をなす。従って $[k[\alpha] : k] = n$ である。 □

$\alpha_1, \alpha_2, \cdots, \alpha_n \in K$ $(n \geq 1)$ に対し，部分環 $k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ の商体を K 内で考え，これを $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ で表す。$k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ は体 K の部分体である。$n \geq 2$ なら

$$k[\alpha_1, \alpha_2, \cdots, \alpha_n] = [k[\alpha_1, \alpha_2, \cdots, \alpha_{n-1}]][\alpha_n],\ k(\alpha_1, \alpha_2, \cdots, \alpha_n) = [k(\alpha_1, \alpha_2, \cdots, \alpha_{n-1})](\alpha_n)$$

が成り立つ。

系 10.4. $\alpha \in K$ とする。$k[\alpha]$ が体をなすための必要十分条件は，α が k 上で代数的であることである。

定義 10.5. K/k は体拡大とする。 $\forall \alpha \in K$ が k 上 代数的であるとき，**体拡大 K/k は代数的である**という。

補題 10.6. K/k は体拡大とする。$[K : k] < \infty$ なら，K/k は代数的である。

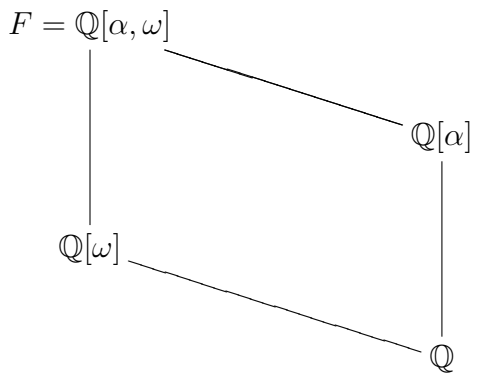
証明. $n = [K : k]$ とおくと，いかなる元 $\alpha \in K$ についても $n + 1$ 個の元 $\{\alpha^i\}_{0 \leq i \leq n}$ は k 上で一次独立になることはない。従って α は k 上で代数的である。 □

系 10.7. $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$ とせよ。元 α_i がすべて k 上で代数的なら，環 $k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ は体をなし，$\big[k[\alpha_1, \alpha_2, \cdots, \alpha_n] : k\big] < \infty$ である。従って，$k(\alpha_1, \alpha_2, \cdots, \alpha_n) = k[\alpha_1, \alpha_2, \cdots, \alpha_n]$ であり，体拡大 $k(\alpha_1, \alpha_2, \cdots, \alpha_n)/k$ は代数的となる。

証明. n についての帰納法で，定理 10.3 と補題 10.6 から，容易に従う。 □

問題 10.8. $f = X^3 - 2 \in \mathbb{Q}[X]$ は $\mathbb{Q}$ で既約である（系 9.17）。f は $\mathbb{C}$ 内で一次式の積 $f = (X-\alpha)(X-\beta)(X-\gamma)$ に分解する。実際, $\alpha = \sqrt[3]{2}$, $\omega = \dfrac{-1 \pm i\sqrt{3}}{2}$ とおき，$\beta = \alpha\omega$, $\gamma = \alpha\omega^2$ とすればよい。このとき $F = \mathbb{Q}[\alpha, \beta, \gamma]$ は $\mathbb{C}$ の部分体をなし，$F = \mathbb{Q}[\alpha, \omega]$, $[F : \mathbb{Q}] = 6$ が成り立つ。

証明. $\alpha, \beta = \alpha\omega, \gamma = \alpha\omega^2 \in F$ より $\alpha, \omega \in F$ である。故に $F = \mathbb{Q}[\alpha, \omega]$ となる。α, ω は $\mathbb{Q}$ 上で代数的で，$F = \mathbb{Q}[\alpha, \omega]$ は $\mathbb{C}$ の部分体をなす。$\omega^2 + \omega + 1 = 0$ であるから，ω は $\mathbb{Q}[\alpha]$ 上でも代数的である。$\mathbb{Q}[\alpha] \subseteq \mathbb{R}$ であるから，$\omega \notin \mathbb{Q}[\alpha]$ となり，故に $\big[F : \mathbb{Q}[\alpha]\big] = 2$ を得る。$\big[\mathbb{Q}[\alpha] : \mathbb{Q}\big] = 3$ であることが上と同様にして示され，$[F : \mathbb{Q}] = [F : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$ が従う。すべての $\theta \in F$ は $\mathbb{Q}$ 上代数的で，その最小多項式を f とし $\deg f = n$ とおくと, $n = [\mathbb{Q}[\theta] : \mathbb{Q}]$ であって $[F : \mathbb{Q}[\theta]] \cdot [\mathbb{Q}[\theta] : \mathbb{Q}] = [F : \mathbb{Q}] = 6$ であるから，$n|6$ となり，$n = 1, 2, 3, 6$ であることが分かる。



□

定理 10.9. $L/K, K/k$ を体の拡大とする。L/k が代数的ための必要十分条件は，L/K, K/k が代数的であることである。

証明. L/K, K/k は代数的と仮定し，$\alpha \in L$ とし $f = c_0 + c_1 X + \cdots + c_n X^n$ を α の K 上の最小多項式とすると，体拡大 K/k は代数的であるから，$E = k[c_0, c_1, \cdots, c_n]$ は体をなし, α は E 上でも代数的である。故に $E[\alpha]$ は体をなし, $\big[E[\alpha] : E\big] < \infty$ が従う。一方で, $[E : k] < \infty$

であるから $\big[E[\alpha]:k\big] = [E[\alpha]:E][E:k] < \infty$ となり，α は 体 k 上で代数的であることが従う。 □

定義 10.10. k を体とする。k が代数閉体であるとは，K/k が体の代数拡大なら $K = k$ が成り立つことをいう。

例 10.11. $\mathbb{C}$ は代数閉体である（代数学の基本定理）。

補題 10.12. 体 k について，次の 3 条件は同値である。

(1) k は代数閉体である。

(2) $f \in k[X]$ が定数でないならば，f は k 内で一次式の積に分解する。

(3) $f \in k[X]$ が定数でないならば，f は k 内に少なくとも一つの根をもつ。

証明. (1)⇒(3) 定数ではない $f \in k[X]$ を取ると，定理 9.11 より，体拡大 K/k と $\alpha \in K$ を見つけて，$f(\alpha) = 0$ が成り立つようにすることができる。このとき，体拡大 $k[\alpha]/k$ は代数的であるので，等式 $k[\alpha] = k$ が成り立ち，$\alpha \in k$ が得られる。

(3)⇒(2) 明らかである。

(2)⇒(1) K/k を体の代数拡大とし $\alpha \in K$ とすると，α の k 上の最小多項式は既約であるから，仮定 (2) より $\deg f = 1$ が従い，$\alpha \in k$ が得られる。 □

系 10.13. 代数閉体は有限体でない。

証明. k を有限体とし，定数でない多項式 $f = 1 + \prod_{a \in k}(X - a) \in k[X]$ を取ると，いかなる $a \in k$ も f の根にはなり得ない。 □

問題 10.14. 次が知られている。証明せよ。「k を体とすると，体の代数拡大 K/k で，K が代数閉体であるものが存在する。」（例えば，S. Lang 著：「Algebra」を参照せよ。）

11　一意分解整域

11.1　素元と既約元

A は整域とする。$a, b \in A$ のとき，$a|b$ によって，$b \in (a)$，即ち, ある $x \in A$ に対し等式 $b = ax$ が成り立つことを表す。

定義 11.1. $a \in A$ は，$a \neq 0$ であってかつ $(a) \in \operatorname{Spec} A$ であるとき, A の**素元**であるという。

定義 11.2. $a \in A$ とする。次の 2 条件を満たすとき，a は A 内で**既約**であるという。

(1) a は零でも単元でもない。

(2) $b, c \in A$ で $a = bc$ なら，b が A の単元であるかまたは c が A の単元であるか，どちらかが成り立つ。

補題 11.3. 素元は既約である。

証明. $a \in A$ を素元とする。$a = bc$ とすると，$bc \in (a)$ であるから $b \in (a)$ であるか又は $c \in (a)$ が成り立つ。$b \in (a)$ とし，$b = da$ $(d \in A)$ と表す。$a = bc$ に代入すれば，$a = (dc)a$ となる。A は整域であるから，$dc = 1$ となり，c が A の単元であることが従う。　□

命題 11.4. $p_1, p_2, \cdots, p_n$ と $q_1, q_2, \cdots, q_m$ は A の素元とする。等式 $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ が成り立つなら，$n = m$ であって，適当な並び替えの後に，全ての $1 \leq i \leq n$ についてイデアルの等式 $(p_i) = (q_i)$ が成り立つ。

証明. $n = 1$ のときは，$p_1 = q_1 q_2 \cdots q_m$ となるが，p_1 は既約であるから，$m = 1$，$p_1 = q_1$ である。$n > 1$ で $n - 1$ まで正しいとする。$m > 1$ である。$q_1 \cdots q_m \in (p_1)$ より $q_1 \in (p_1)$ としてよい。q_1 は既約であるから，適当な単元 $\varepsilon \in$A を求めて $q_1 = \varepsilon_1 p_1$ と表すことができる。故に，$(p_1) = (q_1)$ であって，$p_2 \cdots p_n = \varepsilon_1 q_2 \cdots q_m$ となるので，n に関する帰納法より定理が従う。　□

11.2 Euclid 整域・単項イデアル整域と一意分解整域

定義 11.5. $a \in A$ が零でも単元でもないなら，必ず素元分解を持つとき，即ち，A の素元 $p_1, p_2, \cdots, p_n$ $(n \geq 1)$ を用いて，$a = p_1 p_2 \cdots p_n$ と表すことができるとき, 環 A は**一意分解整域** (UFD, Unique Factorization Domain) であるという。

補題 11.6. A は一意分解整域とする。$a \in A$ が既約なら，a は素元である。

全てのイデアルが単項のとき，A は**単項イデアル整域** (PID, Principal Ideal Domain) であるという。$\mathbb{Z}$ と体上の多項式環 $k[X]$ は単項イデアル整域で，典型的な一意分解整域である。$\mathbb{Z}$ が一意分解整域であることの証明 (6.8 参照) をそっくり用いて，下記の定理が証明される。

定理 11.7. 単項イデアル整域は一意分解整域である。

定義 11.8. $A^* = A \setminus \{0\}$ とする。次の 2 条件を満たす写像 $\varphi : A^* \to \mathbb{Z}$ が存在するとき，A は Euclid 整域であるという。

(1) $\forall a \in A^*$ に対し $\varphi(a) \geq 0$ である。

(2) 任意の $a, b \in A$ $(a \neq 0)$ に対し，等式 $b = aq + r$ を満たす $q, r \in A$ が存在し，$r \neq 0$ ならば $\varphi(r) < \varphi(a)$ が成り立つ。

例 11.9. (1) 整数環 $\mathbb{Z}$ は写像 $\varphi : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$, $\varphi(a) = |a|$ によって Euclid 整域となる（補題 5.70 参照)。

(2) 体 k 上の多項式環 $A = k[X]$ は写像 $\varphi : A \setminus \{0\} \to \mathbb{Z}$, $\varphi(f) = \deg f$ によって Euclid 整域となる（補題 9.1 参照)。

(3) $\mathbb{C}$ の部分環 $\mathbb{Z}[i] = \{a + b\,i \mid a, b \in \mathbb{Z}\}$ は Euclid 整域である。

証明. (3) $A = \mathbb{Z}[i]$ とおく。$\alpha = a + bi \in A$ $(a, b \in \mathbb{Z})$ に対し

$$\varphi(\alpha) = |\alpha|^2 = |\sqrt{a^2 + b^2}|^2 = a^2 + b^2$$

と定める。 この $\varphi : A \setminus \{0\} \to \mathbb{Z}$ が求める写像である。$\alpha, \beta \in A\ (\alpha \neq 0)$ とせよ。$\mathbb{Z}[i]$ を複素平面上の格子点（座標が整数であるような点）と同一視すれば，点 $\dfrac{\beta}{\alpha}$ に対し，$|\dfrac{\beta}{\alpha} - \gamma| < 1$ となるような $\gamma \in \mathbb{Z}[i]$ を選ぶことができる。 $\lambda = \dfrac{\beta}{\alpha} - \gamma$ とおけば，$\beta = \gamma\alpha + \lambda\alpha$ であって $\varphi(\alpha\lambda) < \varphi(\alpha)$ となるからである。 □

定理 11.10. Euclid 整域は単項イデアル整域で，一意分解整域である。

証明. 環 A のイデアル $I \neq (0)$ を取る。 $I = (a)\ (a \in A)$ を示したい。$I \neq (0)$ としてよい。I の元 $a \neq 0$ を $\varphi(a)$ が最小になるように取る。$b \in I$ とせよ。A は Euclid 整域であるから, 等式 $b = aq + r$ が成り立つような元 $q, r \in A$ を，$r \neq 0$ ならば $\varphi(r) < \varphi(a)$ となるように取ることができる。このとき，実際に $r \neq 0$ なら，$r = b - aq \in I$ であって $\varphi(r) < \varphi(a)$ であるから，$\varphi(a)$ の最小性が壊れる。故に，$r = 0$ で，$b = aq \in (a)$ である。即ち $I = (a)$ となる。 □

11.3 一意分解整域上の多項式環

A は一意分解整域とする。$K = \mathrm{Q}(A)$ を A の商体，$A[X] \subseteq K[X]$ は多項式環とする。

補題 9.15 と全く同様にして，次が得られる。

補題 11.11. $p \in A$ が A の素元なら，p は多項式環 $A[X]$ 内でも素元である。

補題 11.12. $a_1, a_2, \cdots, a_n \in A\ (n \geq 1)$ を与えれば，次の 2 条件を満たす $d \in A$ が存在する。

(1) $1 \leq \forall i \leq n$ に対し $d | a_i$ である。

(2) $d' \in A$ が $1 \leq \forall i \leq n$ に対し $d' | a_i$ なら，$d' | d$ である。

このような元 d は，単元の違いを除いて，$a_1, a_2, \cdots, a_n$ に対し一意的に定まる。d を $a_1, a_2, \cdots, a_n$ の**最大公約元**と言い，$d = \mathrm{GCD}(a_1, a_2, \cdots, a_n)$ と書く。

定義 11.13. 多項式 $0 \neq f \in A[X]$ が**原始的**であるとは, $f = a_0 + a_1 X + \cdots + a_n X^n$ と表したときに，$\mathrm{GCD}(a_0, a_1, \cdots, a_n) = 1$ が成り立つことをいう。

$0 \neq g \in A[X]$ なら，多項式 g の係数の最大公約元を c とすると，$h = \dfrac{g}{c} \in A[X]$ は原始的である。

命題 11.14 (Gauss の補題)**.** $f, g \in A[X]$ とする。 次の主張が正しい。

(1) f と g が原始的なら，積 fg も原始的である。

(2) f は原始的と仮定する。$K[X]$ 内で $f|g$ なら, $A[X]$ 内でも $f|g$ である。故に，原始多項式 $f \in A[X]$ が K 内で既約なら，f は $A[X]$ の素元である。

証明. (1) fg が原始的でないなら, 環 A の素元 p を取って，fg の全ての係数を A 内で割るようできる。故に $fg \in pA[X]$ であるが，$pA[X]$ は素イデアルであるから，$f \in pA[X]$ であるかまたは $g \in pA[X]$ が成り立つ。 これは f と g が原始的であることに反する。

(2) $g \neq 0$ として十分である。 多項式環 $K[X]$ 内で等式 $g = \varphi f$ を満たす元 $\varphi \in K[X]$ を取る。多項式 φ の係数の共通分母 $0 \neq d \in A$ を取り, $d\varphi = ch$ ($0 \neq c \in A$, $h \in A[X]$ で原始的) と表すと, $dg = d(\varphi f) = c(fh)$ となる。一方で，$g = e\ell$ ($0 \neq e \in A$, $\ell \in A[X]$ は原始的) と表すと，(1) に示したように積 fh は原始的であるから，等式 $c(fh) = dg = (de)\ell$ より，$c = de\varepsilon$ を満たす環 A の単元 ε が存在することがわかる。故に，$dg = de\varepsilon(fh)$ が成り立ち，$g = e\varepsilon(fh)$, 即ち $f|g$ が $A[X]$ 内で成り立つ。 □

定理 11.15. A が一意分解整域なら多項式環 $A[X]$ も一意分解整域である。

証明. 原始多項式が素元分解されることを示せば十分である。定数でない原始多項式 $f \in A[X]$ を取り，$f = \varphi_1\varphi_2\cdots\varphi_\ell$ を多項式環 $K[X]$ 内での素元分解とする。各 φ_i に対し，$0 \neq d_i \in A$ を φ_i の係数の共通分母に取り, $d_i\varphi_i = c_i g_i$ ($c_i \in A$, $g_i \in A[X]$ で原始的) と表す。$g_i K[X] = \varphi_i K[X]$ であるから命題 11.14 により，g_i は環 $A[X]$ の素元である。$d = \prod_{i=1}^{\ell} d_i$，$c = \prod_{i=1}^{\ell} c_i$，$g = \prod_{i=1}^{\ell} g_i$ とおく。すると，$df = cg$ であって，g は原始的なので，環 A の単元 ε を取り $c = \varepsilon d$ と表すことができる。$f = \varepsilon g$ であって，各 g_i は環 $A[X]$ の素元であるから，f は環 $A[X]$ 内でも素元分解を持つ。故に，多項式環 $A[X]$ は一意分解整域である。 □

系 11.16. 多項式環$\mathbb{Z}[X_1, X_2, \cdots, X_n]$ $(n \geq 1)$と体k上の多項式環$k[X_1, X_2, \cdots, X_n]$ $(n \geq 1)$は，一意分解整域である。

問題 11.17 (Eisenstein の既約判定法). Aを一意分解整域としKをその商体とする。Aに係数を持つ多項式

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad (n > 0)$$

に対し，素元$p \in A$が次の条件を満たすように取れるなら，多項式fはK内で既約であることを証明せよ。

$$\mathbf{1 \leq \forall i \leq n-1}\text{について}\ \mathbf{p | a_i}\text{であるが,}\ \mathbf{p^2} \not| \mathbf{a_0}\text{である。}$$

12 Noether環

Aは可換環とする。

12.1 イデアルの演算と生成系

$\mathcal{F}$によってAのイデアル全体のなす集合を表す。$I, J \in \mathcal{F}$に対し

$I + J = \{a + b \mid a \in I, b \in J\}$,
$IJ = \{\sum_{i=1}^{n} a_i b_i \mid n > 0$で，各$1 \leq i \leq n$について$a_i \in I, b_i \in J$である$\}$,
$I \cap J = \{a \in A \mid a \in I$かつ$a \in J\}$,
$I : J = \{a \in A |$ 全ての$x \in J$に対して$ax \in I$である$\}$

と定め，それぞれIとJの和，積，共通部分，商という。イデアルの和，積，共通部分，商は，イデアルである。

問題 12.1. $I, J, K \in \mathcal{F}$とするとき，次の主張が正しい。確かめよ。

(1) $I \cup J \subseteq I + J$，$IJ \subseteq I \cap J$，$I \subseteq I : J$である。

(2) $J \subseteq I$なら$I + J = I$である。

(3) $I + J = J + I$, $IJ = JI$である。

(4) $I+(J+K)=(I+J)+K$, $I(JK)=(IJ)K$ である。

(5) $(0)+I=I+(0)=I$，$AI=IA=I$ である。

(6) $I(J+K)=IJ+IK$，$(I+J)K=IK+JK$ である。

$(\mathcal{F},+)$ と $(\mathcal{F},\cdot)$ は，それぞれ (0), A を単位元に持つ可換半群で，$\mathcal{F}$ 内では有限和 $\sum_{i=1}^{n} I_i$ と有限積 $\prod_{i=1}^{n} I_i$ が定義される。従って，冪

$$I^0=A,\ I^n=I^{n-1}I\ \ (n\geq 1)$$

が定義され，指数法則

$$I^mI^n=I^{m+n},\ (I^m)^n=I^{mn},\ (IJ)^n=I^nJ^n\ \ (m,n\geq 0)$$

と等式

$$(I+J)^n=\sum_{i+j=n} I^iJ^j\ \ (n\geq 0)$$

が成り立つ。ここで $I,J\in\mathcal{F}$ とする。

問題 12.2. 次の主張が正しいことを確かめよ。

(1) $a\in A$，J は A のイデアルとし，$aJ=\{aj\mid j\in J\}$ とおくと，$(a)J=aJ$ である。

(2) $a_1,a_2,\cdots,a_n\in A$ をとり，$I=(a_1,a_2,\cdots,a_n)$ とすると，$IJ=\sum_{i=1}^{n} a_iJ$ である。

命題 12.3 (modular law)**.** I,J,K は A のイデアルとする。このとき，$J\subseteq I$ なら，等式

$$I\cap(J+K)=J+(I\cap K)$$

が成り立つ。

証明. $i\in I\cap(J+K)$ をとって $i=j+k$ $(j\in J,k\in K)$ と表せば，$J\subseteq I$ であるから，$k=i-j\in I\cap K$ となり，$i=j+k\in J+(I\cap K)$ が成り立ち，$I\cap(J+K)\subseteq J+(I\cap K)$ であることが従う。 □

A の部分集合 S に対し，$S \neq \emptyset$ なら

$$(S) = \{\sum_{i=1}^{n} a_i s_i \mid n > 0,\ \text{各}\, 1 \leq i \leq n \,\text{に対し}\, a_i \in A, s_i \in S\}$$

とし，$(\emptyset) = \{0\}$ と定め，これを集合 S で生成された A のイデアルという。(S) は S を含む最小のイデアルであるから，この表記法によれば，$I, J \in \mathcal{F}$ のとき，等式

$$IJ = (ab \mid a \in I,\ b \in J),\ \ I^n = (\prod_{i=1}^{n} a_i \mid \text{各}\, 1 \leq i \leq n \,\text{について}\, a_i \in I)\ (n \geq 1)$$

が成り立つ。

$S \subseteq A$ なら，$I : (S) = \{a \in A \mid as \in I, \forall s \in S\}$ である。$I : (S)$ は $I : S$ と表すことが多い。特に $I : (x)$ は単に $I : x$ と書くのが普通である。

与えられたイデアル I に対し，等式 $I = (S)$ が成り立つような集合 $S \subseteq I$ を，I の生成系という。I が有限集合 S を生成系として含むとき，I は有限生成であると言い，一元で生成されたイデアルを，単項イデアルと呼ぶ。

空ではない集合 Λ を添字に持つ A のイデアルの族 $\{I_\lambda\}_{\lambda\in\Lambda}$ に対し

$$\sum_{\lambda\in\Lambda} I_\lambda = \{\sum_{\lambda\in\Lambda} a_\lambda \mid \forall\lambda \in \Lambda\text{に対し}\, a_\lambda \in I_\lambda\text{で，殆ど全ての}\lambda \in \Lambda\text{に対し}\, a_\lambda = 0\}$$

と定め，$\{I_\lambda\}_{\lambda\in\Lambda}$ の和という。和 $\sum\limits_{\lambda\in\Lambda} I_\lambda$ は $\bigcup\limits_{\lambda\in\Lambda} I_\lambda$ で生成されたイデアルに等しい。共通部分 $\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ もイデアルである。

12.2 イデアルの根基

I は A のイデアルとする。

$$\sqrt{I} = \{a \in A |\ \text{ある整数}\, n > 0\, \text{に対し}\, a^n \in I\, \text{が成り立つ}\,\}$$

と定め，これを I の根基（radical）という。$I \subseteq \sqrt{I}$ である。$I \in \operatorname{Spec} A$ なら，等式 $\sqrt{I} = I$ が成り立つ。

定理 12.4. I が A のイデアルなら，$\sqrt{I}$ も A のイデアルで，$I \neq A$ なら等式

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{V}(I)} \mathfrak{p}$$

が成り立つ。

証明. $I \neq A$ として十分である。$a, b \in \sqrt{I}$ とせよ。整数 $n \gg 0$ を $a^n, b^n \in I$ が成り立つようにとる。すると，$(ca)^n = c^n a^n \in I$ であるから，任意の $c \in A$ について $ca \in \sqrt{I}$ である。$(a+b)^{2n} = \sum_{i+j=2n} \binom{2n}{i} a^i b^j$ であるが，$i \geq n$ なら $a^i \in I$ で，$i < n$ なら $j > n$ であるから $b^j \in I$ となり，どちらの場合も $a^i b^j \in I$ であるので，$(a+b)^{2n} \in I$ となり，$a+b \in \sqrt{I}$ であることが分かる。故に $\sqrt{I}$ は A のイデアルである。

$\sqrt{I} \subseteq \bigcap_{P \in \mathrm{V}(I)} \mathfrak{p}$ である。元 $f \in \bigcap_{\mathfrak{p} \in \mathrm{V}(I)} \mathfrak{p}$ があって，$f \notin \sqrt{I}$ であると仮定すると，f のいかなる冪 f^n $(n \geq 0)$ もイデアル I には含まれない。積閉集合 $S = \{f^n | n \geq 0\}$ を考え，$B = S^{-1}A$ とおき，$\varphi : A \to B$ を局所化の自然な写像とする。$I \cap S = \emptyset$ であるので，B のイデアル $J = \{\frac{a}{s} \mid a \in I, s \in S\}$ は，B とは異なる。もし $J = B$ なら，$1 \in J$ であるから $\frac{1}{1} = \frac{a}{s}$ $(a \in I, s \in S)$ と表され，ある $t \in S$ に対して $t(1 \cdot a - s \cdot 1) = 0$ が成り立ち，$ts = ta \in I \cap S$ となるからである。故に，B 内にはイデアル J を含む極大イデアル M が存在し，$\mathfrak{p} = \varphi^{-1}(M)$ とおけば，$\mathfrak{p} \in \operatorname{Spec} A$ で，$\varphi(I) \subseteq J$ より $I \subseteq \mathfrak{p}$ が成り立つ。故に $f \in \mathfrak{p}$ で，$\varphi(f) = \frac{f}{1} \in M$ となるが，$\frac{f}{1}$ は B の単元であるから，不可能である。 □

問題 12.5. 次の主張を証明せよ。

(1) 任意のイデアル I に対し，$\sqrt{\sqrt{I}} = \sqrt{I}$ が成り立つ。

(2) I_1, I_2 を A のイデアルとすれば，$\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$ である。

定義 12.6. (1) イデアル $\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$ を A の冪零根基と呼び，$\sqrt{(0)} = (0)$ が成り立つとき A は reduced であるという。

(2) イデアル $\bigcap_{\mathfrak{m} \in \operatorname{Max} A} \mathfrak{m}$ を A の Jacobson 根基と呼び，$\mathrm{J}(A)$ と表す。

(3) A 内に極大イデアルがただ一つしか含まれていないとき，A は局所環 (local ring) であるという。

問題 12.7. 次の主張を証明せよ。

(1) $\mathrm{J}(A) = \{a \in A \mid \forall x \in \text{に対し } 1 - ax \in A^\times\}$ である。

(1) A は局所環で $a \in A$ とする。$a = a^2$ なら，$a = 0$ であるかまたは $a = 1$ である。

命題 12.8 (Krull-東屋の補題)**.** $J = \mathrm{J}(A)$ とおき，I を環 A の有限生成イデアルとする。このとき，$I = JI$ なら，$I = (0)$ である。

証明. I は有限生成であるから，$I = (x_1, x_2, \cdots, x_n)$ となる A の元 $\{x_i\}_{1 \le i \le n}$ が存在するような整数 $n \ge 0$ を最小に取る。$I \neq (0)$ なら $n \ge 1$ である。すると，$x_n \in JI$ であるから $x_n = \sum_{i=1}^{n} a_i x_i$ $(a_i \in J)$ と表すと，$(1 - a_n)x_n = \sum_{i=1}^{n-1} a_i x_i$ で $1 - a_n \in A^\times$ であるから，$x_n \in (x_1, x_2, \cdots, x_{n-1})$ となって，$I = (x_1, x_2, \cdots, x_{n-1})$ が従い，整数 n の最小性が壊れる。故に $I = (0)$ である。 □

命題 12.9. I を A のイデアルとせよ。$\sqrt{I}$ が有限生成なら，十分大きな任意の整数 $m \gg 0$ に対し，$(\sqrt{I})^m \subseteq I$ が成り立つ。

証明. $\sqrt{I} = (a_1, a_2, \ldots, a_n)$ $(n \ge 1)$ と表し，$a_i^q \in I$ が $1 \le \forall i \le n$ に対し成り立つよう整数 $q > 0$ をとる。すると，$\forall m \ge 1$ に対し

$$(\sqrt{I})^m = (\prod_{i=1}^{n} a_i^{\alpha_i} \mid 1 \le \forall i \le n \text{ について } 0 \le \alpha_i \in \mathbb{Z} \text{ であって } \sum_{i=1}^{n} \alpha_i = m)$$

であるから，整数 m を $m \ge n(q-1) + 1$ が成り立つようにとれば，$\sum_{i=1}^{n} \alpha_i = m$ となる非負整数 $\alpha_1, \alpha_2, \cdots, \alpha_n$ の中に，少なくとも一つは $\alpha_i \ge q$ を満たすものが現れ，$\prod_{i=1}^{n} a_i^{\alpha_i} \in I$ が得られる。故に $(\sqrt{I})^m \subseteq I$ である。 □

12.3 Prime avoidance theorem と Davis の補題

定理 12.10 (Prime avoidance theorem)**.** $I, P_1, P_2, \cdots, P_n$ $(n \geq 1)$ は A のイデアルで，イデアル $P_1, P_2, \cdots, P_n$ の中で素イデアルでないものは，たかだか 2 個しかないと仮定する。このとき $I \subseteq \bigcup_{i=1}^{n} P_i$ なら，ある $1 \leq i \leq n$ に対し $I \subseteq P_i$ が成り立つ。

証明. $n \geq 2$ としてよい。如何なる $1 \leq i \leq n$ に対しても $I \not\subseteq P_i$ であると仮定し，そのような $n \geq 2$ を最小にとる。$n = 2$ なら，$a_1 \in I$ と $a_2 \in I$ を，それぞれ $a_1 \notin P_2$，$a_2 \notin P_1$ ととり，$a = a_1 + a_2$ とおく。すると，$a_i \in I \subseteq P_1 \cup P_2$ であるので，$a_i \in P_i$ $(i = 1, 2)$ である。一方で，$a \in I$ であるから，$a \in P_1$ であるか又は $a \in P_2$ が成り立つはずであるが，$a = a_1 + a_2 \in P_1$ なら，$a_1 \in P_1$ であるから $a_2 \in P_1$ が従い，$a = a_1 + a_2 \in P_1$ なら，$a_2 \in P_2$ であるから $a_1 \in P_2$ が従う。どちらも不可能である。

故に $n \geq 3$ である。さて，必要なら並べ替えて，P_1 は A の素イデアルであるとしてよい。n の最小性より，如何なる $1 \leq i \leq n$ に対しても $I \not\subseteq \cup_{j \neq i} P_j$ となる。元 $a_i \in I$ を $a_i \notin \cup_{j \neq i} P_j$ が成り立つように取る。$a_i \in P_i$，$a_i \notin P_j$ $(j \neq i)$ である。$a = a_1 + \prod_{i=2}^{n} a_i$ とおく。すると，$a \in I$ であるが，$a \notin \cup_{i=1}^{n} P_i$ である。実際，$a = a_1 + \prod_{i=2}^{n} a_i \in P_1$ なら，$a_1 \in P_1$ より $\prod_{i=2}^{n} a_i \in P_1$ であるが，P_1 は素イデアルであって $a_i \notin P_1$ $(i \geq 2)$ であるから，不可能である。従って，$a = a_1 + \prod_{i=2}^{n} a_i \in P_j$ が成り立つような j は 2 以上であるが，$\prod_{i=2}^{n} a_i \in P_j$ であるから，$a_1 \in P_j$ が従い，やはり不可能である。 □

定理 12.11 (Davis)**.** $a \in A$，I は A のイデアル，$P_1, P_2, \cdots, P_n$ $(n \geq 1)$ は A の素イデアルとせよ。このとき，$(a) + I \not\subseteq \bigcup_{i=1}^{n} P_i$ なら，ある $x \in I$ を選び，$a + x \notin \bigcup_{i=1}^{n} P_i$ が成り立つようにすることができる。

証明. $n = 1$ とせよ。$\forall x \in I$ について $a + x \in P_1$ であるなら，$a = a + 0 \in P_1$ であってかつ $I \subseteq P_1$ が成り立ち，$(a) + I \subseteq P_1$ となる。$n \geq 2$ であって我々の主張は $n - 1$ までは正しいと仮定する。$\bigcup_{i=1}^{n-1} P_i \not\subseteq P_n$ であるとしてよい。すると，$(a) + I \not\subseteq \bigcup_{i=1}^{n-1} P_i$ であるから，元

$y \in I$ を $a+y \notin \bigcup_{i=1}^{n-1} P_i$ と選ぶことができる。もし $a+y \notin P_n$ なら，この $y \in I$ が求める元である。$a+y \in P_n$ とせよ。すると $I \not\subseteq P_n$ である。実際, もし $I \subseteq P_n$ なら，$a+y \in P_n$ であるから，$a \in P_n$ となって，$(a)+I \subseteq P_n$ が従うからである。 イデアル P_n は素であるから，$I \cdot \prod_{i=1}^{n-1} P_i \not\subseteq P_n$ である（問題 5.64 参照)。元 $z \in I \cdot \prod_{i=1}^{n-1} P_i$ を $z \notin P_n$ が成り立つように選び，$x = y+z$ とおけば，この $x \in I$ が求める元である。実際，$a+x \in P_i$ とすると，$i = n$ なら，$a+y \in P_n$ であるから $z \in P_n$ が従い，$i < n$ なら，$z \in P_i$ であるから $a+y \in P_i$ が従うが，どちらも不可能だからである。 □

12.4 イデアルの拡大と制限

$\varphi : A \to B$ は環の準同型写像とする。

A のイデアル I に対し $\varphi(I)$ で生成された B のイデアルを，IB あるいは I^e と表す。即ち，

$$I^e = \left\{ \sum_{i=1}^{n} \varphi(a_i) b_i \;\middle|\; n > 0 \text{ であって，各 } 1 \leq i \leq n \text{ について } a_i \in I,\ b_i \in B \right\}$$

である。$I \subseteq J$ なら $I^e \subseteq J^e$ である。また，等式 $(I+J)^e = I^e + J^e$，$(IJ)^e = I^e J^e$ が，A の任意のイデアル I, J に対し成り立つ。$I = (a_1, a_2, \ldots, a_n)A$ なら，$I^e = (\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n))B$ となり，I^e も有限生成である。

逆に，B のイデアル J に対し，$\varphi^{-1}(J)$ を $J \cap A$ または J^c と表し，イデアル J の A への制限，あるいは引き戻しという。J^c は A のイデアルであって，$J^{ce} \subseteq J$ が成り立ち，A のイデアル I については，$I \subseteq I^{ec}$ が成り立つ。故に A の任意のイデアル I に対し，$I^{ece} = I^e$ となる。Q を B の素イデアルとすれば，Q の制限 Q^c は A の素イデアルである。

S を A 内の積閉集合とし，自然な写像 $f : A \to S^{-1}A$, $f(a) = \dfrac{a}{1}$ を考える。

定理 12.12. 次の主張が正しい。

(1) J を $S^{-1}A$ のイデアルとすれば，$J = J^{ce}$ である。

(2) I を A のイデアルとすれば，$I^e = \{\dfrac{a}{s} \mid a \in I, s \in S\}$，$I^{ec} = \{a \in A \mid \text{ある } s \in S \text{ が存在して } sa \in I\}$ となる。

証明. (1) $\frac{a}{s} \in J$ とすれば，$\frac{a}{1} = \frac{s}{1}\cdot\frac{a}{s} \in J$ であるから $\frac{a}{1} \in J$ となり，$a \in J^c$ が得られて，$J \subseteq J^{ce}$ を得る。

(2) $a \in I$，$s \in S$ ならば，$\frac{a}{s} = \frac{a}{1}\cdot\frac{1}{s} \in I^e$ である。逆に，$x \in I^e$ とすれば，$a_i \in I$，$\frac{b_i}{s} \in S^{-1}A$ を取って $x = \sum_{i=1}^{n} \frac{a_i}{1}\cdot\frac{b_i}{s} = \sum_{i=1}^{n} \frac{a_i b_i}{s} = \frac{a}{s}$ $(a = \sum_{i=1}^{n} a_i b_i \in I)$ と表すことができ，$I^e = \left\{\frac{a}{s} \mid a \in I, s \in S\right\}$ が従う。

次に，等式 $I^{ec} = \{a \in A \mid \text{ある } s \in S \text{ に対し } sa \in I\}$ が成り立つことを示そう。$a \in I^{ec}$ ならば，ある $b \in I$ と $s \in S$ によって $\frac{a}{1} = \frac{b}{s}$ と表すことができるから，$t \in S$ を等式 $t(1\cdot b - a\cdot s) = 0$ が成り立つように取ることができ，$(ts)a = tb \in I$ が従う。$a \in A$，$s \in S$ で $sa \in I$ なら，$\frac{a}{1} = \frac{sa}{s} \in I^e$ より，$a \in I^{ec}$ が得られる。 □

系 12.13. I を A のイデアルとする。$I^e = S^{-1}A$ であるための必要十分条件は，$I \cap S \neq \emptyset$ である。

系 12.14. P は A の素イデアルであって，$P \cap S = \emptyset$ とすると，拡大イデアル P^e は $S^{-1}A$ の素イデアルである。また，写像

$$\Phi : \{P \in \operatorname{Spec} A \mid P \cap S = \emptyset\} \to \operatorname{Spec} S^{-1}A,\ \Phi(P) = P^e$$

は，包含関係を保つような全単射である。

証明. P は A の素イデアルであって $P \cap S = \emptyset$ であるから，$P^{ec} = P$，$P^e \neq S^{-1}A$ である。$\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ が $\frac{a}{s}\cdot\frac{b}{t} = \frac{ab}{st} \in P^e$ を満たすなら，$ab \in P^{ec} = P$ となり，$a \in P$ か又は $b \in P$ が従う。即ち，$\frac{a}{s} \in P^e$ か又は $\frac{b}{t} \in P^e$ となって，P^e が $S^{-1}A$ の素イデアルであることを得る。$P^{ec} = P$ であるから，写像 Φ は単射である。Q を $S^{-1}A$ の素イデアルとし $P = Q^c$ とおけば，$P \in \operatorname{Spec} A$ であって $P^e = Q \neq S^{-1}A$ が成り立つ。故に，$P \cap S = \emptyset$ であって，写像 Φ は全射でもある。 □

$P \in \operatorname{Spec} A$ に対し，$S = A \setminus P$ と定めて局所化 $S^{-1}A$ を考えると，$S^{-1}A$ は $P^e = \{\frac{a}{s} \mid a \in P, s \in A \setminus P\}$ を唯一つの極大イデアルとするような局所環である（命題 12.14 参照）。

定義 12.15. $S^{-1}A$ を A_P と表し，点 P における A の**局所環**という。

問題 12.16. I, J を A のイデアルとすれば，等式 $(I \cap J)^e = I^e \cap J^e$ が成り立つ。確かめよ。

12.5 Noether 環

A は環とする。

定義 12.17. A 内のいかなるイデアルも有限生成であるとき，A は Noether 環であるという。

命題 12.18. A に関する次の 3 条件は，互いに同値である。

(1) A は Noether 環である。

(2) $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ を A のイデアルの昇鎖とすれば，十分大きな番号 $k \geq 1$ があって $I_k = I_i$ が $\forall i \geq k$ に対し成り立つ。

(3) 集合 $\mathcal{F}$ の空でないいかなる部分集合 $\mathcal{S}$ も，包含関係に関する極大元を含む。但し，$\mathcal{F}$ は A のイデアル全体よりなる集合を表す。

証明. (1)⇒(2) $I = \bigcup_{i \geq 1} I_i$ と置くと，I は環 A のイデアルである。I は有限生成であるから，$I = (a_1, a_2, \cdots, a_n)$ $(n \geq 1)$ と表し，番号 $N \geq 1$ を $1 \leq \forall i \leq n$ について $a_i \in I_N$ となるよう取れば，$i \geq N$ である限り等式 $I = I_N = I_i$ が成り立つ。

(2)⇒(3) 集合 $\mathcal{S}$ 内に極大元が一つも含まれていないならば，如何なる $I \in \mathcal{S}$ に対しても，$I \subsetneq J$ となるような $J \in \mathcal{S}$ が I に対して少なくとも一つは存在し，従って集合 $\mathcal{S}$ の元の昇鎖 $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_i \subsetneq \cdots$ が得られる。これは仮定 (2) に反する。

(3)⇒(1) A 内に有限生成でないイデアル I が存在したと仮定し，$\mathcal{S} = \{J \mid J$ は A の有限生成イデアルで $J \subseteq I\}$ とおけば，$(0) \in \mathcal{S}$ より $\mathcal{S} \neq \emptyset$ であるから，極大元 $J \in \mathcal{S}$ を含む。$J \neq I$ であるので，$a \in I$ を $a \notin J$ を満たすように取って，$K = J + (a)$ とおくと，イデアル K は有限生成であってかつ $K \subseteq I$ であるから，$K \in \mathcal{S}$ となるが，$J \subsetneq K$ であるのでイデアル J の極大性が壊れる。故に，A のイデアルはすべて有限生成である。 □

定理 12.19. A は Noether 環とする。

(1) I $(\neq A)$ を A のイデアルとすれば，A/I も Noether 環である.

(2) A 内のいかなる積閉集合についても，局所化 $S^{-1}A$ は Noether 環である。

(3) 多項式環 $A[X_1, X_2, \cdots, X_n]$ $(n \geq 1)$ は Noether 環である。

従って，Noether 環 A から出発して，(1), (2), (3) の操作を繰り返して得られる環 B は，すべて Noether 環である。

証明. (1)，(2) $B = A/I$ または $B = S^{-1}A$ とおき，自然な写像 $\varphi : A \to B$ を考えると，B の如何なるイデアル J に対しても等式 $J^{ce} = J$ が成り立つ。故に B も Noether 環である。

(3) (E. Artin) n に関する帰納法により，$n = 1$ として十分である。$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ を多項式環 $B = A[X]$ のイデアルの昇鎖とせよ。各 $j \geq 0$ に対し

$$\mathfrak{a}_{i,j} = \{a \in A \mid f = aX^j + (j \text{ より低次の項}) \text{となるような } f \in I_i \text{が存在する}\}$$

とおく。$\mathfrak{a}_{i,j}$ は環 A のイデアルで，任意の整数 $i, j \geq 0$ に対し $\mathfrak{a}_{i,j} \subseteq \mathfrak{a}_{i+1,j}$，$\mathfrak{a}_{i,j} \subseteq \mathfrak{a}_{i,j+1}$ が成り立ち，下の図が得られる。

$$\begin{array}{ccccccccc}
\vdots & & \vdots & & \vdots & & & & \vdots \\
\cup| & & \cup| & & \cup| & & & & \cup| \\
\mathfrak{a}_{0,j} & \subseteq & \mathfrak{a}_{1,j} & \subseteq & \mathfrak{a}_{2,j} & \subseteq \cdots \subseteq & & & \mathfrak{a}_{i,j} \subseteq \cdots \\
\cup| & & \cup| & & \cup| & & & & \cup| \\
\vdots & & \vdots & & \vdots & & & & \vdots \\
\cup| & & \cup| & & \cup| & & & & \cup| \\
\mathfrak{a}_{0,1} & \subseteq & \mathfrak{a}_{1,1} & \subseteq & \mathfrak{a}_{2,1} & \subseteq \cdots \subseteq & & & \mathfrak{a}_{i,1} \subseteq \cdots \\
\cup| & & \cup| & & \cup| & & & & \cup| \\
\mathfrak{a}_{0,0} & \subseteq & \mathfrak{a}_{1,0} & \subseteq & \mathfrak{a}_{2,0} & \subseteq \cdots \subseteq & & & \mathfrak{a}_{i,0} \subseteq \cdots
\end{array}$$

この図の対角線上を見ると，$\mathfrak{a}_{0,0} \subseteq \mathfrak{a}_{1,1} \subseteq \mathfrak{a}_{ii} \subseteq \cdots$ であるから，$\mathfrak{a}_{n,n} = \mathfrak{a}_{n+1,n+1} = \mathfrak{a}_{n+2,n+2} = \cdots$ となるような番号 $n \geq 0$ が得られ，任意の $i, j \geq n$ について等式 $\mathfrak{a}_{n,n} = \mathfrak{a}_{i,j}$ が従う。

さて，$0 \leq j \leq n$ とする。このとき，$\mathfrak{a}_{0,j} \subseteq \mathfrak{a}_{1,j} \subseteq \mathfrak{a}_{2,j} \subseteq \cdots \subseteq \mathfrak{a}_{i,j} \subseteq \cdots$ という A のイデアルの昇鎖から，$\mathfrak{a}_{\alpha_j,j} = \mathfrak{a}_{\alpha_j+1,j} = \mathfrak{a}_{\alpha_j+2,j} = \cdots$ となる番号 $\alpha_j \geq 0$ が存在することがわ

かるので，$N = \max[\{\alpha_j \mid 0 \leq j \leq n\} \bigcup \{n\}]$ とおくと，$\forall j \geq 0$ と $\forall i \geq N$ について等式 $\mathfrak{a}_{i,j} = \mathfrak{a}_{i+1,j}$ が成り立つ。$i \geq N$ なら $I_i = I_{i+1}$ が成り立つことを確かめよう。$f \in I_{i+1}$ を取り $f \notin I_i$ であると仮定する。このような f を特に $j = \deg f$ が最小となるよう選ぶ。このとき，$f = aX^j + (j$ より低次の項$)$ $(a \in A)$ とおけば，$a \in \mathfrak{a}_{i+1,j} = \mathfrak{a}_{i,j}$ であるから，$g \in I_i$ を $g = aX^j + (j$ より低次の項$)$ が成り立つように選ぶことができる。しかし，$h = f - g$ とおくと，$h \in I_{i+1}$，$h \notin I_i$ で $\deg h < j$ であるから，$j = \deg f$ の最小性が壊れる。故に $\forall i \geq N$ について等式 $I_i = I_{i+1}$ が成り立ち，多項式環 $B = A[X]$ も Noether 環であることが分かる。 □

定理 12.20 (I. S. Cohen)**.** 環 A に対し次の条件は同値である。

(1) A は Noether 環である。

(2) 全ての $P \in \operatorname{Spec} A$ は有限生成である。

証明. (2)⇒(1) A は Noether 環でないと仮定し，有限生成でないイデアル全体のなす集合を $\mathcal{S}$ とおく。集合 $\mathcal{S}$ 内の空でない鎖 $\mathcal{C}$ をとって $I = \bigcup_{J \in \mathcal{C}} J$ とおくと，イデアル I は有限生成でない。故に，Zorn の補題により，集合 $\mathcal{S}$ 内に極大元 I を得る。$I \neq A$ であってかつ $I \notin \operatorname{Spec} A$ でもあるので，元 $x, y \in A$ を $xy \in I$，$x, y \notin I$ を満たすよう選ぶことができる。$I \subsetneq I + x$ であるから，イデアル $I + x$ は有限生成である。$J = I : x$ とおけば，$I \subsetneq I + (y) \subseteq J$ であるから，イデアル J も有限生成となる。$I + (x) = (a_1 + r_1 x, a_2 + r_2 x, \cdots, a_m s + r_m x)$ $(a_i \in I, r_i \in A)$ $(m \geq 1)$ とし，$J = (z_1, z_2, \cdots, z_n)$ $(n \geq 1)$ とする。このとき，$\forall a \in I$ をとり $a = \sum_{i=1}^{m} s_i(a_i + r_i x)$ $(s_i \in A)$ と表すと，$a - \sum_{i=1}^{m} s_i a_i = \left(\sum_{i=1}^{m} s_i r_i\right) x \in I$ であるから，$\sum_{i=1}^{m} s_i r_i \in I : x = J$ となり，$\left(\sum_{i=1}^{m} s_i r_i\right) x \in xJ = (xz_1, xz_2, \cdots, xz_n)$ を得る。故に，$a \in (a_1, a_2, \cdots, a_m) + (xz_1, xz_2, \cdots, xz_n)$ となって，$I = (a_1, a_2, \cdots, a_m) + (xz_1, xz_2, \cdots, xz_n)$ が得られるが，勿論不可能である。 □

12.6 イデアルの準素分解

A は環とする。

定義 12.21. I は A のイデアルとする。次の 2 条件を満たすとき，I は A の準素イデアルであるという。

(1) $I \neq A$ である。

(2) $a, b \in A$ のとき, $ab \in I$ なら，$a \in I$ であるか又は $b \in \sqrt{I}$ が成り立つ。

素イデアルは準素イデアルである。$\mathfrak{m}$ が A の極大イデアルなら， 任意の整数 $n > 0$ に対し $A/\mathfrak{m}^n$ は局所環であるから，冪 $\mathfrak{m}^n$ は A の準素イデアルとなる。

補題 12.22. I が準素イデアルなら，$\sqrt{I} \in \operatorname{Spec} A$ である。

証明. $I \neq A$ であるから $\sqrt{I} \neq A$ である。$a, b \in A$ とせよ。$ab \in \sqrt{I}$, $a \notin \sqrt{I}$ ならば，ある整数 $n > 0$ に対して $(ab)^n = a^n b^n \in I$ となる。I は A の準素イデアルであって $a^n \notin I$ であるから，$b^n \in \sqrt{I}$ となり，$b \in \sqrt{I}$ が得られる。故に $\sqrt{I}$ は素イデアルである。 □

A の準素イデアル I に対して，$\sqrt{I} = P$ が成り立つとき，I は P-準素イデアルであるという。I_1, I_2 が P-準素イデアルならば，$I_1 \cap I_2$ も P-準素イデアルである (問題 12.5)。

イデアル I $(\neq A)$ は，有限個の準素イデアルの共通部分 $I = \bigcap_{i=1}^{n} Q_i$ $(n \geq 1)$ として表されるとき，A 内で準素分解を持つという。イデアル I の準素分解 $I = \bigcap_{i=1}^{n} Q_i$ が無駄のない分解であるとは，$\{P_i = \sqrt{Q_i}\}_{1 \leq i \leq n}$ が互いに異なっていて，$1 \leq \forall i \leq n$ について $\bigcap_{j \neq i} Q_j \not\subseteq Q_i$ が成り立つことをいう。イデアルは準素分解を持てば必ず無駄のない分解を持つ。

定義 12.23. A のイデアル I は，$I \neq A$ であって，$I = J \cap K$ であるようなイデアル J, K が $J = I$ 又は $K = I$ に限るとき，**既約**であるという。

補題 12.24. I を Noether 環 A のイデアル $(I \neq A)$ とすると，イデアル I は有限個の既約イデアルの共通部分である。

証明. 有限個の既約イデアルの共通部分ではないイデアル I $(\neq A)$ が Noether 環 A 内に存在したと仮定し，このような I を極大にとれば，イデアル I は既約ではないので，環 A のイデ

アル $J, K \supsetneq I$ を等式 $I = J \cap K$ が成り立つよう取ることができる。すると，$J, K \neq A$ であるので，イデアル I の極大性から，J, K は有限個の既約イデアルの共通部分として表され，従って必ず I も有限個の既約イデアルの共通部分として表されるが，不可能である。 □

補題 12.25. Noether 環内では既約イデアルは準素イデアルである.

証明. I を既約イデアルとし，$ab \in I$，$b \notin \sqrt{I}$ であるとせよ。このとき，イデアルの昇鎖 $I : b \subseteq I : b^2 \subseteq \cdots \subseteq I : b^n \subseteq \cdots$ を考え，整数 $n > 0$ を $k \geq n$ なら等式 $I : b^n = I : b^k$ が成り立つように取ると，$(I : b) \cap [I + (b^n)] = I$ である。実際，$x \in (I : b) \cap [I + (b^n)]$ なら $x = i + b^n y$ $(i \in I, y \in A)$ と表すと，$b^{n+1} y = bx - bi \in I$ であるから $y \in I : b^{n+1} = I : b^n$ となり，$x = i + b^n y \in I$ が従う。故に，$(I : b) \cap [I + (b^n)] = I$ であって $b \notin \sqrt{I}$ であるので，イデアル I の既約性から，$a \in I : b = I$ が得られる。 □

よって次の定理が得られた。

定理 12.26 (Laker-Noether の分解定理)**.** Noether 環 A のイデアル I $(\neq A)$ は準素分解を持つ。

A は Noether 環，I $(\neq A)$ はイデアルとせよ。$I = \bigcap_{i=1}^{n} Q_i$ はイデアル I の無駄のない準素分解とし，$P_i = \sqrt{Q_i}$ とおく。このとき次の等式が成り立つ。

定理 12.27. $\{P_1, P_2, \cdots, P_n\} = \{P \in \operatorname{Spec} A \mid \text{ある } x \in A \text{ に対し } P = I : x \text{ となる }\}$。

この定理の証明には，少し準備が必要である。S を環 A 内の積閉集合で $I \cap S = \emptyset$ なるものとし，局所化 $S^{-1}A$ を考える。$\Lambda = \{i \mid 1 \leq i \leq n, P_i \cap S = \emptyset\}$ とおく。すると，$I \cap S = \emptyset$ であるから $\Lambda \neq \emptyset$ であって，分解 $I^e = \bigcap_{i \in \Lambda} Q_i^e$ は，環 $S^{-1}A$ 内での拡大イデアル I^e の無駄のない準素分解となっている。実際，$i \in \Lambda$ とすると，Q_i は P_i-準素イデアルで $P_i \cap S = \emptyset$ であるから，$Q_i^{ec} = Q_i$ であって，$\sqrt{Q_i^e} = P_i^e \in \operatorname{Spec} S^{-1}A$ であることを得る。次に，環 $S^{-1}A$ の 2 元 x, y について，$xy \in Q_i^e$ ならば，$x = \dfrac{a}{s}$，$y = \dfrac{b}{t}$ と表した後に，$xy = \dfrac{ab}{st} \in Q_i^e$ を見ると，

ある $u \in S$ に対し $u(ab) \in Q_i$ となることがわかる。故に，$ua \in Q_i$ であるか又は $b \in P_i$ が成り立ち，これより $x \in Q_i^e$ または $y \in P_i^e$ であることが従う。即ち Q_i^e は P_i^e-準素イデアルである。$P_i^{ec} = P_i$ であるから，$\{P_i^e\}_{i\in\Lambda}$ は相異なる。また，$i \in \Lambda$ について，もし $Q_i^e \supseteq \bigcap_{j\in\Lambda\setminus\{i\}} Q_j^e$ なら $Q_i = Q_i^{ec} \supseteq \bigcap_{j\in\Lambda\setminus\{i\}} Q_j^{ec} = \bigcap_{j\in\Lambda\setminus\{i\}} Q_j$ となるので，$\forall i \in \Lambda$ について $Q_i^e \not\supseteq \bigcap_{j\in\Lambda\setminus\{i\}} Q_j^e$ であることが従う。

以上により，下記の結果が得られる。

補題 12.28. 分解 $I^e = \bigcap_{j\in\Lambda} Q_i^e$ は，I の拡大イデアル I^e の $S^{-1}A$ 内での無駄のない準素分解である。

定理 12.27 の証明を述べよう。

証明. $1 \leq i \leq n$ をとって $S = A \setminus P_i$ とおき，上の議論を適用しよう。$I^e = \bigcap_{P_j\subseteq P_i} Q_j^e$ は無駄のない準素分解であった。等式 $I^e : y = P_i^e$ が成り立つような元 $y = \dfrac{x}{s} \in A_{P_i}$ が存在すると仮定せよ。すると，$I^e : \dfrac{x}{1} = P_i^e$ であるから，$xP_i \subseteq I^{ec}$ であってかつイデアル P_i が有限生成であることより，$t \in A \setminus P_i$ を $txP_i \subseteq I$ が成り立つよう取ることができる。即ち $P_i \subseteq I : tx$ が成り立つ。このとき，元 $a \in A$ について，もし $a(tx) \in I$ なら，$\dfrac{a}{1}\cdot\dfrac{x}{1} \in I^e$ となるので，$\dfrac{a}{1} \in P_i^e$ が得られる。$a \in P_i^{ec} = P_i$ であるから，等式 $I : tx = P_i$ が従う。逆に，$P \in \operatorname{Spec} A$ のとき，$x \in A$ に対して等式 $P = I : x$ が成り立つなら，A_P 内の等式 $I^e : \dfrac{x}{1} = P^e$ と拡大イデアル I^e の $I^e = \bigcap_{P_i\subseteq P} Q_i^e$ という無駄のない準素分解が得られる。即ち，定理 12.27 内の等式は，局所化 A_{P_i} と A_P を通し，A が極大イデアル $\mathfrak{m}$ を持つ局所環であって，$P_i = \mathfrak{m}$ あるいは $P = \mathfrak{m}$ の場合に帰着されることがわかる。

$P_i = \mathfrak{m}$ とせよ。このとき，A の元 $x \notin Q_i$ を，$\forall j \neq i$ について $x \in Q_j$ と取れば，$x \notin I$ であり，$xQ_i \subseteq \bigcap_{j=1}^n Q_j = I$ であるから，$Q_i \subseteq I : x$ となる。故に，$\mathfrak{m}^\ell \subseteq Q_i$ となる整数 $\ell > 0$ を取れば，必ず $x\mathfrak{m}^\ell \subseteq I$ となる。ここで，$x\mathfrak{m}^\ell \subseteq I$ を満たす整数 $\ell \geq 1$ を最小に取れば，$x\mathfrak{m}^{\ell-1} \not\subseteq I$ であるから，元 $y \in x\mathfrak{m}^{\ell-1}$ を $y \notin I$ が成り立つように取ることができ，この

y については $y\mathfrak{m} \subseteq I$ であるので，$\mathfrak{m} \subseteq I : (y) \subsetneq A$ が成り立ち，$\mathfrak{m}$ が A の極大イデアルであることから，$\mathfrak{m} = I : (y)$ が得られる。

逆に，ある $x \in A$ に対して $\mathfrak{m} = I : (x)$ が成り立つなら，$x\mathfrak{m} \subseteq I$ であって $x \notin I$ である。故に，$x \notin Q_i$ となる $1 \leq i \leq n$ を取れば，$x\mathfrak{m} \subseteq Q_i$ で Q_i が準素イデアルであることより，$\mathfrak{m} \subseteq P_i$ となって，$\mathfrak{m} = P_i$ が従う。即ち，$\{P_1, P_2, \cdots, P_n\} = \{P \in \operatorname{Spec} A |$ ある $x \in A$ に対し $P = I : x\}$ が成り立つ。 □

環 A のイデアル I に対し

$$\operatorname{Ass}_A A/I = \{P \in \operatorname{Spec} A \mid \text{ある } x \in A \text{があって } P = I : x \text{が成り立つ }\}$$

とおき，$\operatorname{Ass}_A A/I$ の元を，I に随伴する素イデアル，あるいは，I の素因子という。

以上の議論を纏めておくと，下記のようになる。

定理 12.29. I を Noether 環 A のイデアルとすれば，次の主張が正しい。

(1) $\operatorname{Ass}_A A/I$ は有限集合である。

(2) $\operatorname{Ass}_A A/I \neq \emptyset$ であるための必要十分条件は $I \neq A$ である。

(3) $I \neq A$ とする。このとき，等式

$$I = \bigcap_{P \in \operatorname{Ass}_A A/I} I(P)$$

を満たすようなイデアルの族 $\{I(P)\}_{P \in \operatorname{Ass}_A A/I}$ が存在する。ここで，各 P に対し，$I(P)$ は P-準素イデアルである。この準素分解には無駄がない。また，$P \in \operatorname{Ass}_A A/I$ が $\operatorname{Ass}_A A/I$ 内で包含関係について極小なら，$I(P) = I^{ec}$ が成り立つので，イデアル $I(P)$ は準素分解 $I = \bigcap_{P \in \operatorname{Ass}_A A/I} I(P)$ の取り方にはよらず，I に対し一意的に定まる。

命題 12.30. I は Noether 環 A のイデアル $(I \neq A)$ とせよ。$a \in A$ の像が A/I 内で零因子であるための必要十分条件は，$a \in P$ となるような $P \in \operatorname{Ass}_A A/I$ が少なくとも一つ存在する

ことである。故に，等式

$$\bigcup_{P\in \mathrm{Ass}_A\, A/I} P = \{a \in A \mid a \text{の像は } A/I \text{ 内で零因子である}\}$$

が成り立つ。

証明. $I = \bigcap_{i=1}^{n} Q_i$ は無駄のない準素分解とする。$y \notin I$ が $ay \in I$ を満たすなら，全ての i について $ay \in Q_i$ であるが，特に $y \notin Q_i$ となる i に対しては，$a \in P_i$ が成り立つ。逆に，$P \in \mathrm{Ass}_A\, A/I$ とし，元 $a \in P$ を取れば，$P = I : x$ となる $x \in A$ に対し必ず $ax \in I$ が成り立つ。$x \notin I$ であるので，元 a の像は A/I 内で零因子である。 □

$\mathrm{Ass}\, A = \mathrm{Ass}_A\, A/(0)$ とおく。

系 12.31. Noether 環 A 内では等式

$$\bigcup_{P\in \mathrm{Ass}\, A} P = \{a \in A \mid a \text{は } A \text{ の零因子である}\}$$

が成り立つ。

問題 12.32. I は Noether 環 A のイデアルとする。I が少なくとも一つ A の非零因子を含むなら，イデアル I は非零因子で生成される，即ち，等式 $I = (a_1, a_2, \cdots, a_n)$ $(n \geq 1)$ を満たすような，A の非零因子 $\{a_i\}_{1\leq i\leq n}$ $(n \geq 1)$ が存在することを証明せよ。

系 12.33. $\mathfrak{m}$ が Noether 環 A の極大イデアルなら，次の条件は同値である。

(1) $\mathfrak{m} \in \mathrm{Ass}\, A$ である。

(2) $\mathfrak{m}$ の元は全て A の零因子である。

証明. (2)⇒(1) $\mathrm{Ass}\, A$ は有限集合である（系 12.31）。$\mathfrak{m} \subseteq \bigcup_{P\in \mathrm{Ass}\, A} P$ であるから，定理 12.10 より $\mathfrak{m} \subseteq P$ がある $P \in \mathrm{Ass}\, A$ に対し成り立つ。イデアル $\mathfrak{m}$ は極大であるから，$\mathfrak{m} = P \in \mathrm{Ass}\, A$ となる。 □

13　次元論

13.1　Artin 環

A は環とする。

定義 13.1. 環 A がイデアルに関する降鎖律を満たすとき，A は Artin 環であるという。即ち，$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_i \supseteq \cdots$ が A のイデアルの降鎖なら，番号 $k \geq 1$ をとって，$\forall i \geq k$ について $I_k = I_i$ が成り立つようにできることをいう。

この条件は，A のイデアルよりなる空でないいかなる集合も，包含関係に関する極小元を含むことと同値である。

補題 13.2. A は極大イデアル $\mathfrak{m}$ を持つ局所環であって，$\mathfrak{m}$ は冪零，即ち，$\mathfrak{m}^n = (0)$ がある整数 $n \geq 1$ に対し成り立つと仮定せよ。このとき，$\mathfrak{m}$ が有限生成なら，A は Artin 環である。

証明. $n = 1$ なら，A は体であって，自明なイデアルしか含まず，Artin 環である。$n > 1$ とし，$n-1$ まで主張は正しいと仮定し

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_i \supseteq \cdots$$

を A 内のイデアルの降鎖とする。$\mathfrak{m} \cdot \mathfrak{m}^{n-1} = (0)$ であるから，$\mathfrak{m}^{n-1}$ は体 $A/\mathfrak{m}$ 上の有限次元ベクトル空間である。（体 $A/\mathfrak{m}$ の加法群 $\mathfrak{m}^{n-1}$ への作用は，$a \in A$ と $x \in \mathfrak{m}^{n-1}$ に対し，$\overline{a}x = ax$ と定める。ここで $\overline{a}$ は，a の $A/\mathfrak{m}$ 内での像を表す。）$\{I_i \cap \mathfrak{m}^{n-1}\}_{i \geq 1}$ はベクトル空間 $\mathfrak{m}^{n-1}$ の部分空間の降鎖であるから，部分空間の次元を考察することにより，十分大なる番号 $k \geq 1$ では，$\forall i \geq k$ に対し $I_k \cap \mathfrak{m}^{n-1} = I_i \cap \mathfrak{m}^{n-1}$ が成り立つことがわかる。一方で，$(\mathfrak{m}/\mathfrak{m}^{n-1})^{n-1} = (0)$ であるから，n についての仮定により，局所環 $A/\mathfrak{m}^{n-1}$ は，Artin 環である。$\{(I_i + \mathfrak{m}^{n-1})/\mathfrak{m}^{n-1}\}_{i \geq k}$ は $A/\mathfrak{m}^{n-1}$ 内のイデアルの降鎖であるから，十分大なる番号 $\ell \geq k$ を見つけて，$i \geq \ell$ である限り必ず等式 $(I_\ell + \mathfrak{m}^{n-1})/\mathfrak{m}^{n-1} = (I_i + \mathfrak{m}^{n-1})/\mathfrak{m}^{n-1}$ が成り立つようにすることができる。故に $i \geq \ell$ ならば，$I_\ell + \mathfrak{m}^{n-1} = I_i + \mathfrak{m}^{n-1}$ であるので，補題

12.3 より，$I_i = I_i \cap (I_\ell + \mathfrak{m}^{n-1}) = I_\ell + (I_i \cap \mathfrak{m}^{n-1})$ が成り立つ。$I_i \cap \mathfrak{m}^{n-1} = I_\ell \cap \mathfrak{m}^{n-1}$ であるので，等式 $I_i = I_\ell + (I_\ell \cap \mathfrak{m}^{n-1}) = I_\ell$ が従い，A は Artin であることを得る。 □

補題 13.3. A は Artin 環とする。次の主張が正しい。

(1) A が整域なら A は体である.

(2) A の素イデアルは極大イデアルであって，Spec A は有限集合である。

証明. A が Artin 整域で $0 \neq a \in A$ なら，$(a^n) = (a^{n+1})$ となる整数 $n > 0$ が存在し，ある $(x \in A)$ に対し $a^n = xa^{n+1}$ となり，$a^n(1 - ax) = 0$，即ち $1 = ax$ が得られ，A は体であることが従う。$P \in \mathrm{Spec}\, A$ なら，A/P は Artin であるから A/P は体をなし，P が極大イデアルであることが従う。Spec A が無限集合なら，相異なる極大イデアルの族 $\{\mathfrak{m}_i\}_{i\geq 1}$ をとって，A のイデアルの真の降鎖 $\mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supsetneq \cdots \supsetneq \bigcap_{i=1}^{n} \mathfrak{m}_i \supsetneq \cdots$ を得る（問題 5.64 参照)。故に A が Artin 環なら Spec A は有限集合である。 □

A の極大イデアルの集合を Max A で表す。

定理 13.4. 次の条件は同値である。

(1) A は Artin 環である.

(2) A は Noether 環で Spec A = Max A である。

証明. (1)⇒(2) まず，Artin 局所環は Noether 環であることを示そう。A を Artin 局所環，$\mathfrak{m}$ をその極大イデアルとする。

補題 13.5. $\mathfrak{m}$ は冪零である。

証明. （M. F. Atitah – I. G. MacDonald : Introduction to Commutative Algebra からの引用）降鎖 $\{\mathfrak{m}^i\}_{i\geq 0}$ を考えることによって，整数 $k \geq 1$ を選んで，$\forall i \geq k$ に対し等式 $\mathfrak{m}^k = \mathfrak{m}^i$ が成り立つようにすることができる。$I = \mathfrak{m}^k$ とおき，$I \neq (0)$ と仮定する。

$$\mathcal{S} = \{J \mid J \text{ は } A \text{ のイデアルで, } JI \neq (0) \text{ を満たす }\}$$

とおくと，整数 k の選び方により $I = I^2 \neq (0)$ となるので，$I \in \mathcal{S}$ である。A は Artin であるから，集合 $\mathcal{S}$ は包含関係について極小な元 J を含む。$JI \neq (0)$ であるので，元 $x \in J$ をとって，$xI \neq (0)$ とすることができるが，$(x) \subseteq J$ であるから，イデアル J の極小性より，$J = (x)$ が従う。一方で，$I = I^2$ より，$(0) \neq xI = xI^2$ であるから，$xI \in \mathcal{S}$ であって $xI \subseteq J = (x)$ より，$xI = (x)$ が従う。$x = xi$ $(i \in I)$) と表せば，$(1-i)x = 0$ であるが，$i \in I \subseteq \mathfrak{m}$ であるから，$1 - i \in A^\times$ であって，$x = 0$ となる。$JI \neq (0)$ であるから，不可能である。 □

命題13.4の証明を続けよう。$\mathfrak{m}$ は冪零であるから，補題13.2より，A が Noether であることを示すには，イデアル $\mathfrak{m}$ が有限生成であることを示せば十分である。整数 $n \geq 1$ を $\mathfrak{m}^n = (0)$ にとる。$n = 1$ なら，A は体であって，確かに Noether である。$n > 1$ とし，$n-1$ までは我々の主張は正しいと仮定しよう。$A/\mathfrak{m}^{n-1}$ は Artin 局所環で，$(\mathfrak{m}/\mathfrak{m}^{n-1})^{n-1} = (0)$ であるから，$n-1$ についての仮定より，その極大イデアル $\mathfrak{m}/\mathfrak{m}^{n-1}$ は有限生成である。一方で，$\mathfrak{m}\cdot\mathfrak{m}^{n-1} = (0)$ であって A は Artin であるから，体 $A/\mathfrak{m}$ 上のベクトル空間 $\mathfrak{m}^{n-1}$ は部分空間の真の減少列を含まない。即ち $\mathfrak{m}^{n-1}$ は $A/\mathfrak{m}$ 上有限次元のベクトル空間であって，A のイデアルとしても有限生成である。$\mathfrak{m}^{n-1}$ と $\mathfrak{m}/\mathfrak{m}^{n-1}$ がともに有限生成であるので，$\mathfrak{m}$ も有限生成であることが従う。故に A は Noether 環である。

次に，$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ は，必ずしも局所環ではない Artin 環 A 内のイデアルの昇鎖とする。$\mathfrak{m} \in \operatorname{Max} A$ とする。局所環 $A_\mathfrak{m}$ は Artin であって，従って Noether である。$\operatorname{Max} A$ は有限であるので，$A_\mathfrak{m}$ 内の拡大イデアルの昇鎖 $\{{I_i}^e = I_i A_\mathfrak{m}\}_{i\geq 1}$ を考察すれば，整数 $k \geq 1$ を選んで，$i \geq k$ である限り全ての $\mathfrak{m} \in \operatorname{Max} A$ に対し等式 $I_k A_\mathfrak{m} = I_i A_\mathfrak{m}$ が成り立つようにすることができる。このとき，$i \geq k$ なら等式 $I_k = I_i$ が成り立つ。実際，$I_k \subsetneq I_i$ なら，$x \in I_i$ を $x \notin I_k$ であるように取って $\mathfrak{a} = I_k : x$ とおけば，$\mathfrak{a} \neq A$ であるから，$\mathfrak{a} \subseteq \mathfrak{m}$ を満たす $\mathfrak{m} \in \operatorname{Max} A$ が存在する。一方で，$\dfrac{x}{1} \in I_i A_\mathfrak{m} = I_k A_\mathfrak{m}$ であるから，元 $s \in A \setminus \mathfrak{m}$ を見つけて $sx \in I_k$ が成り立つようにできる筈である。このとき，$s \in I_k : x = \mathfrak{a}$ であるから，

$s \in \mathfrak{m}$ が従うが，不可能である。故に，如何なる昇鎖 $\{I_i\}_{i\geq 1}$ も，十分大なる $k \geq 1$ に対し $I_k = I_{k+1} = \cdots$ が成り立ち，A は Noether 環であることを得る。

(2)⇒(1) 集合 $\operatorname{Max} A$ は有限であるので，(2)⇒(1) の証明に於けると同様の理由により，A は局所環としてよいことがわかる。$\mathfrak{m}$ を A の極大イデアルとすれば，$\mathfrak{m}$ は有限生成であって $\operatorname{Spec} A = \{\mathfrak{m}\}$ であるから，十分大きな整数 $n \geq 1$ に対し $\mathfrak{m}^n = (0)$ となる。故に補題 13.2 より A は Artin 環である。 □

系 13.6. Artin 環 A 内では $\mathrm{J}(A) = \sqrt{(0)}$ である。故に $\mathrm{J}(A)$ は冪零である。

問題 13.7. 整数 $n \geq 1$ に対し $A_n = \mathbb{Z}/2\mathbb{Z}$ とおき，$A = \prod_{n\geq 1} A_n$ （直積）とする。次の主張が正しいことを証明せよ。

(1) $\forall f \in A$ に対し $f^2 = f$ である。

(2) $\forall P \in \operatorname{Spec} A$ について $A_P \cong \mathbb{Z}/2\mathbb{Z}$ である。従って局所環 A_P は体である。

(3) $\operatorname{Spec} A = \operatorname{Max} A$ が成り立つが，A は Artin 環ではない。

補題 13.8 (CRT, Chinese Remainder Theorem)**.** (1) I, J は A のイデアルとする。このとき，$I + J = A$ なら $IJ = I \cap J$ である。

(2) $\{I_i\}_{1\leq i\leq n}$ は A のイデアルで，$i \neq j$ なら $I_i + I_j = A$ が成り立つと仮定せよ。このとき，環準同型写像 $\varphi : A \to \prod_{i=1}^n A/I_i$，$\varphi(a) = \{a \mod I_i\}_{1\leq i\leq n}$ は全射で $\operatorname{Ker}\varphi = \bigcap_{i=1}^n I_i$ である。

証明. (1) $a \in I$ と $b \in J$ を取り $1 = a + b$ と表せば，$\forall x \in I \cap J$ に対し $x = ax + bx \in IJ$ となり，$I \cap J = IJ$ が従う。

(2) 写像 φ が全射であることを示せば十分である。$n = 2$ とし $1 = a_1 + a_2$ $(a_i \in I_i)$ と書くと，$x_1, x_2 \in A$ に対し $\varphi((x_1 - x_1a_1) + (x_2 - x_2a_2)) = (x_1 \mod I_1, x_2 \mod I_2)$ であるので，φ は全射である。$n \geq 3$ であって $n - 1$ まで我々の主張が正しいと仮定し $J = \bigcap_{i=2}^n I_i$ と

おくと，$I_1 + J = A$ である。実際，$I_1 + J \neq A$ なら，A の極大イデアル $\mathfrak{m}$ を $I_1 + J \subseteq \mathfrak{m}$ と取ると，$\mathfrak{m}$ は素イデアルで $\prod_{i=2}^{n} I_i \subseteq J \subseteq \mathfrak{m}$ であるから，$I_i \subseteq \mathfrak{m}$ がある $2 \leq i \leq n$ に対して成り立ち（問題 5.64 参照），$I_1 + I_i \subseteq \mathfrak{m}$ となるが，不可能である。故に，写像 $\varphi_1 : A \to A/I_1 \times A/J,\ \varphi_1(a) = (a \mod I_1,\ a \mod J)$ は全射である。一方で，写像 $\varphi_2 : A \to \prod_{i=2}^{n} A/I_i,\ \varphi_2(a) = \{a \mod I_i\}_{2 \leq i \leq n}$ は，n についての仮定により全射であるので，写像 $\varphi_3 = id_{A/I_1} \times \varphi_2 : A/I_1 \times A/J \to A/I_1 \times \prod_{i=2}^{n} A/I_i = \prod_{i=1}^{n} A/I_i$ は全射となる。故に，合成 $\varphi = \varphi_3 \cdot \varphi_1$ も全射である。 □

定理 13.9 (Artin 環の構造定理)**.** A が Artin 環ならば，環準同型写像

$$\varphi : A \to \prod_{\mathfrak{m} \in \operatorname{Max} A} A_{\mathfrak{m}},\ a \mapsto \{\frac{a}{1} \in A_{\mathfrak{m}}\}_{\mathfrak{m} \in \operatorname{Max} A}$$

は同型である。従って，Artin 環は有限個の Artin 局所環の直積と同型である。

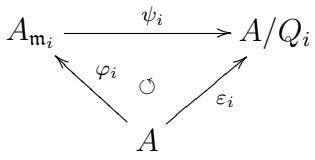
証明. A は Artin 環であるから，$\operatorname{Ass} A = \operatorname{Max} A$ となる。$\operatorname{Max} A = \{\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_n\}$ $(n = \sharp \operatorname{Max} A)$ とし，A 内でイデアル (0) の無駄のない準素分解

$$(0) = \bigcap_{i=1}^{n} Q_i$$

を，各 $1 \leq i \leq n$ について $\mathfrak{m}_i = \sqrt{Q_i}$ が成り立つようにとる。すると $i \neq j$ なら，$\mathfrak{m}_i + \mathfrak{m}_j = A$ であるので $Q_i + Q_j = A$ が従い，補題 [CRT] によって環準同型写像

$$\Phi : A \to \prod_{i=1}^{n} A/Q_i,\ a \mapsto (a \mod Q_i)_{1 \leq i \leq n}$$

は同型である。$\varphi_i : A \to A_{\mathfrak{m}_i}$,$\varepsilon_i : A \to A/Q_i$ を自然な写像とし，$s \in A \setminus \mathfrak{m}_i$ とすれば，A/Q_i は極大イデアルが $\mathfrak{m}_i/Q_i$ であるような局所環であるから，元 $\varepsilon_i(a) = a \mod Q_i$ は A/Q_i 内で単元となり，環準同型写像 $\psi_i : A_{\mathfrak{m}_i} \to A/Q_i$ が等式 $\varepsilon_i = \psi_i \cdot \varphi_i$ を満たすように定まって，次の可換図形が得られる（定理 7.7 参照）：



ε_i が全射であるから，ψ_i も全射である。写像 $\psi_i : A_{\mathfrak{m}_i} \to A/Q_i$ が単射であることを示そう。$y \in \operatorname{Ker}\psi_i$ なら，y は $a \in A$ と $s \in A \setminus \mathfrak{m}_i$ を取って $y = \dfrac{a}{s}$ と表わせるから，$\psi_i(y) = \overline{a}\cdot\overline{s}^{-1} = 0$ より，$a \in Q_i$ となる。（但し，$\overline{a} = a \mod Q_i, \overline{s} = s \mod Q_i$ である。）故に，$\frac{a}{1} \in Q_i A_{\mathfrak{m}_i} = (0)$ であるから，$y = \frac{a}{s} = 0$ が得られ，写像 ψ_i が単射であることが従う。 □

13.2 Noether 環の次元

A は Noether 環とする。

$I = \bigcap_{i=1}^{n} Q_i$ を A のイデアル I の無駄のない準素分解とする。$P \in \operatorname{Spec} A$ が $P \supseteq I$ を満たすための必要十分条件は，ある $1 \leq i \leq n$ に対し $P \supseteq Q_i$，即ち $P \supseteq P_i = \sqrt{Q_i}$ が成り立つことである。故に集合 $\mathrm{V}(I)$ の包含関係に関する極小元は I の極小素因子である。I の極小素因子全体のなす集合を $\operatorname{Min}_A A/I$ で表す。即ち

$$\operatorname{Min}_A A/I = \{P \in \mathrm{V}(I) \mid P \text{ は } \mathrm{V}(I) \text{ 内で包含関係について極小である }\}$$

とおく。$\operatorname{Min}_A A/I \subseteq \operatorname{Ass}_A A/I$ であるから $\operatorname{Min}_A A/I$ は有限集合となる。特に

$$\operatorname{Min} A = \{P \in \operatorname{Spec} A \mid P \text{ は } \operatorname{Spec} A \text{ 内で包含関係について極小である }\}$$

と定める。$\operatorname{Min} A \subseteq \operatorname{Ass} A$ である。

補題 13.10. *A は極大イデアルが $\mathfrak{m}$ であるような局所環とし，$f \in \mathfrak{m}$，$\mathfrak{p} \in \operatorname{Spec} A$ とする。このとき，$\mathfrak{m} = \sqrt{(f)}$ であってかつ $\mathfrak{p} \subsetneq \mathfrak{m}$ ならば，$\mathfrak{p} \in \operatorname{Min} A$ である.*

証明. 整数 $\ell \geq 1$ に対し $\mathfrak{p}^{(\ell)} = \mathfrak{p}^{\ell}A_{\mathfrak{p}} \cap A$ とおく。即ち

$$\mathfrak{p}^{(\ell)} = \{a \in A \mid \text{ある } s \in A \setminus \mathfrak{p} \text{ があって } sa \in \mathfrak{p}^{\ell}\}$$

である。$\mathfrak{p}^{(\ell)}$ は $\mathfrak{p}$-準素イデアルで $\mathfrak{p}^{\ell} \subseteq \mathfrak{p}^{(\ell)}$ が成り立つ。$\mathfrak{p}^{(\ell+1)} \subseteq \mathfrak{p}^{(\ell)}$ であるから，$\{[\mathfrak{p}^{(\ell)} + (f)]/(f)\}_{\ell \geq 1}$ は Artin 局所環 $A/(f)$ 内で降鎖をなし，等式 $\mathfrak{p}^{(\ell)} + (f) = \mathfrak{p}^{(\ell+1)} + (f)$ を満たす整数 $\ell \geq 1$ を得る。$f \notin \mathfrak{p}$ であって $\mathfrak{p}^{(\ell)}$ は $\mathfrak{p}$-準素であるから，$\mathfrak{p}^{(\ell)} \cap (f) = f\mathfrak{p}^{(\ell)}$ である。故に

$$\mathfrak{p}^{(\ell)} = \mathfrak{p}^{(\ell)} \cap [\mathfrak{p}^{(\ell+1)} + (f)] = \mathfrak{p}^{(\ell+1)} + [\mathfrak{p}^{(\ell)} \cap (f)] = \mathfrak{p}^{(\ell+1)} + f\mathfrak{p}^{(\ell)}$$

となり，Krull-東屋の補題より $\mathfrak{p}^{(\ell)} = \mathfrak{p}^{(\ell+1)}$ が従う。よって，$\mathfrak{p}^\ell A_\mathfrak{p} = \mathfrak{p}^{\ell+1} A_\mathfrak{p}$ であるから $(\mathfrak{p}A_\mathfrak{p})^\ell = (0)$ となり，$A_\mathfrak{p}$ は Artin 環，即ち $\mathfrak{p} \in \operatorname{Min} A$ であることを得る。 □

定義 13.11. A の素イデアル $\mathfrak{p}$ に対し

$$\operatorname{ht}_A \mathfrak{p} = \sup\{0 \leq n \in \mathbb{Z} \mid A \text{ 内の素イデアルの列 } \mathfrak{p} = \mathfrak{p}_n \supsetneq \mathfrak{p}_{n-1} \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0 \text{が存在する } \}$$

と定め，$\mathfrak{p}$ の高さと呼ぶ。

$(A, \mathfrak{m})$ が局所環で $\mathfrak{m} = \sqrt{(f)}$ を満たす $f \in \mathfrak{m}$ が存在するなら，$\operatorname{ht}_A \mathfrak{m} \leq 1$ である（補題 13.10）。

定理 13.12 (W. Krull)**.** A のイデアル I が n 個の元 $f_1, f_2, \cdots, f_n$ $(n \geq 0)$ で生成されるなら，任意の $\mathfrak{p} \in \operatorname{Min}_A A/I$ に対し $\operatorname{ht}_A \mathfrak{p} \leq n$ が成り立つ。

証明. 局所化 $A_\mathfrak{p}$ を通し，A は極大イデアル $\mathfrak{m}$ を持つ局所環で，$\mathfrak{m} \in \operatorname{Min}_A A/I$ が成り立つと仮定してよい。$\operatorname{ht}_A \mathfrak{m} \leq n$ であることを示す。$n \geq 2$ であって $n-1$ 以下まで正しいと仮定せよ。$\operatorname{ht}_A \mathfrak{m} \geq n+1$ なら，素イデアルの列 $\mathfrak{m} = \mathfrak{p}_{n+1} \supsetneq \mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_0$ が存在する。$I_i = (f_1, f_2, \ldots, f_i)$ $(0 \leq i \leq n)$，$\mathfrak{q} = \mathfrak{p}_n$ とし，イデアルの列

$$\mathfrak{q} + I = \mathfrak{q} + I_n \supseteq \mathfrak{q} + I_{n-1} \supseteq \cdots \supseteq \mathfrak{q} = \mathfrak{q} + I_0$$

を考える。$\mathfrak{m}$ はイデアル $\mathfrak{q} + I_n$ の極小素因子であるので，$\mathfrak{m} = \sqrt{\mathfrak{q} + I_n}$ が成り立つ。そこで $\mathfrak{m} = \sqrt{\mathfrak{q} + I_i}$ となる整数 $0 \leq i \leq n$ を最小に取る。すると，$\mathfrak{m} \supsetneq \mathfrak{q}$ であるから $1 \leq i$ であり，$\mathfrak{m}$ はイデアル $\mathfrak{q} + I_{i-1}$ の極小素因子ではない。$\mathfrak{q} + I_{i-1}$ の極小素因子 $\mathfrak{p}$ を $\mathfrak{m}$ とは異なるよう取れば，$\mathfrak{m} = \sqrt{\mathfrak{q} + I_i}$ であって $\mathfrak{q} + I_i \subseteq \mathfrak{p} + (f_i) \subseteq \mathfrak{m}$ であるから，整数 $\ell \geq 1$ を $\mathfrak{m}^\ell \subseteq \mathfrak{p} + (f_i)$ となるように選ぶことができる。

$$f_j^\ell = p_j + a_j f_i$$

$(p_j \in \mathfrak{p}, a_j \in A, i < j \leq n)$ とし，$J = I_{i-1} + (p_j \mid i < j \leq n)$ とおくと，$f_j^\ell \in J + (f_i) \subseteq \mathfrak{p}$ が成り立ち，$I \subseteq \sqrt{J + (f_i)}$ となる。即ち，剰余類環 A/J 内で $\mathfrak{m}/J = \sqrt{(\overline{f_i})}$ が得られ，$J \subseteq \mathfrak{p} \subsetneq \mathfrak{m}$

であるから $\mathfrak{m}/J \supsetneq \mathfrak{p}/J$ であって，補題 13.10 より，素イデアル $\mathfrak{p}/J$ は A/J 内で極小であることが従う。故に，$\mathfrak{p}$ は J の極小素因子となり，帰納法の仮定から

$$\mathrm{ht}_A \mathfrak{p} \leq (i-1) + (n-i) = n-1$$

が従うが，$\mathfrak{p} \supseteq \mathfrak{q}$ であって $\mathrm{ht}_A \mathfrak{q} \geq n$ であるので，これは不可能である。 □

この定理から Noether 環内の素イデアルの高さは有限であることが従う。

定義 13.13.

$$\dim A = \sup_{\mathfrak{p} \in \mathrm{Spec}\, A} \mathrm{ht}_A \mathfrak{p}$$

とおき，これを A の次元と呼ぶ。

環 B が A の準同型像であれば，$\dim A \geq \dim B$ が成り立つ。環の次元は有限とは限らない。A が極大デアルが $\mathfrak{m}$ を持つ局所環であれば，$\dim A = \mathrm{ht}_A \mathfrak{m}$ であって，$d = \dim A$ は非負整数となる。$\mathfrak{p} \in \mathrm{Spec}\, A$ なら，等式

$$\mathrm{ht}_A \mathfrak{p} = \mathrm{ht}_{A_\mathfrak{p}} \mathfrak{p}A_\mathfrak{p} = \dim A_\mathfrak{p}$$

が成り立つ。

定義 13.14. A のイデアル I $(\neq A)$ に対し $\mathrm{ht}_A I = \min_{\mathfrak{p} \in \mathrm{V}(I)} \mathrm{ht}_A \mathfrak{p}$ と定め，イデアル I の高さと呼ぶ。

命題 13.15. I が高さ n のイデアルなら，I 内には n 個の元 $f_1, f_2, \cdots, f_n$ が存在し，全ての整数 $0 \leq i \leq n$ に対して等式 $\mathrm{ht}_A(f_1, f_2, \cdots, f_i) = i$ が成り立つ。

証明. イデアル I 内に i $(< n)$ 個の元 $f_1, f_2, \cdots, f_i$ が既に選ばれていて，等式 $\mathrm{ht}_A(f_1, f_2, \cdots, f_j) = j$ が $1 \leq \forall j \leq i$ に対し成り立っていると仮定せよ。$J = (f_1, f_2, \cdots, f_i)$ を含み $\mathrm{ht}_A \mathfrak{p} = i$ を持つ素イデアル $\mathfrak{p}$ は，J の極小素因子であるから有限個しか存在せず，I を含むことがない。故に，元 $f_{i+1} \in I$ を $f_{i+1} \notin \bigcup_{\mathfrak{p} \in \mathrm{V}(J), \mathrm{ht}_A \mathfrak{p} = i} \mathfrak{p}$ となるよう選べば，定理 13.12 より等式 $\mathrm{ht}_A(f_1, f_2, \cdots, f_{i+1}) = i+1$ が従う。 □

系 13.16. A が極大デアル $\mathfrak{m}$ を持つ次元 d の局所環なら，等式 $\mathfrak{m} = \sqrt{(f_1, f_2, \cdots, f_d)}$ が成り立つような d 個の元 $f_1, f_2, \cdots, f_d \in \mathfrak{m}$ が存在する。

定義 13.17. A は極大イデアル $\mathfrak{m}$ を持つ局所環とし $d = \dim A$ とおく。元 $f_1, f_2, \cdots, f_d \in \mathfrak{m}$ に対し等式

$$\mathfrak{m} = \sqrt{(f_1, f_2, \ldots, f_d)}$$

が成り立つ，即ち，等式 $\dim A/(f_1, f_2, \ldots, f_d) = 0$ が成り立つとき，$f_1, f_2, \ldots, f_d$ は A の巴系であるという。

A は局所環とし $d = \dim A$ とせよ。

$$\operatorname{Assh} A = \{\mathfrak{p} \in \operatorname{Spec} A \mid \dim A = \dim A/\mathfrak{p}\}$$

とおく。$\operatorname{Assh} A \subseteq \operatorname{Min} A \subseteq \operatorname{Ass} A$ である。A 内には長さ d の素イデアルの列

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{m}$$

が含まれていて，必ず $\mathfrak{p}_0 \in \operatorname{Assh} A$ であるから，$\operatorname{Assh} A$ は空でない。

定理 13.18. $f \in \mathfrak{m}$ とせよ。次の主張が正しい。

(1) $d - 1 \leq \dim A/(f) \leq d$.

(2) $\dim A/(f) = d - 1$ であるための必要十分条件は，元 f がいかなる $\mathfrak{p} \in \operatorname{Assh} A$ にも含まれないことである。このとき f は A の巴系に拡大される。

証明. $\overline{A} = A/(f)$ とおく。$\dim \overline{A} \leq d$ である。$\dim \overline{A} \leq d - 2$ なら，$\mathfrak{m}$ 内に $d - 2$ 個の元 $g_1, g_2, \cdots, g_{d-2}$ を取って $\dim A/[(f) + (g_1, g_2, \ldots, g_{d-2})] = 0$ が成り立つようにできる。即ち

$$\mathfrak{m} = \sqrt{(f) + (g_1, g_2, \ldots, g_{d-2})}$$

であるから，定理 13.12 より，不可能な評価 $d = \dim A = \operatorname{ht}_A \mathfrak{m} \leq d-1$ が得られる。$f \in \mathfrak{p}$ がある $\mathfrak{p} \in \operatorname{Assh} A$ に対して成り立つなら，$A/\mathfrak{p}$ は $\overline{A}$ の準同型像であって $d = \dim A/\mathfrak{p} \leq \dim \overline{A}$

となり，等式 $\dim \overline{A} = d$ が得られる。$\dim \overline{A} = d$ なら，$\overline{\mathfrak{p}} \in \operatorname{Assh} \overline{A}$ を取って $\overline{\mathfrak{p}} = \mathfrak{p}/(f)$ $(\mathfrak{p} \in \operatorname{Spec} A, f \in \mathfrak{p})$ と表すと，$A/\mathfrak{p} \cong \overline{A}/\overline{\mathfrak{p}}$ であるので，等式 $\dim A/\mathfrak{p} = \dim \overline{A}/\overline{\mathfrak{p}} = d$ が従い，$\mathfrak{p} \in \operatorname{Assh} A$ を得る。$\dim \overline{A} = d - 1$ なら，$\overline{A}$ 内で巴系をなすような $f_2, f_3, \ldots, f_d \in \mathfrak{m}$ と併せれば元 $f = f_1, f_2, \ldots, f_d$ は A 内で巴系をなす。 □

系 13.19. A は極大イデアル $\mathfrak{m}$ を持つ局所環とする。$f \in \mathfrak{m}$ が非零因子なら，等式

$$\dim A/(f) = \dim A - 1$$

が成り立つ。

証明. $\operatorname{Assh} A \subseteq \operatorname{Ass} A$ だからである。 □