北海道教育大学教育学部札幌分校集中講義

入門代数学

明治大学理工学部　数学教室

教授　後藤 四郎

2002 年 5 月 7,8,9 日

目 次

1　集合と写像 **2**

1.1　集合 2

1.2　集合の表し方 3

1.3　部分集合 4

2　同値関係と類別 **6**

2.1　直積 6

2.2　同値関係 7

2.3　類別と商集合 8

3　写像 **11**

3.1　公式的定義 11

3.2　像と原像 12

3.3　特殊な写像・単射と全射 15

3.4　写像の合成 17

3.5　逆写像 20

4　対称群 S_n **22**

4.1　置換 22

4.2　置換の符号 27

4.3　行列式 28

4.4　偶置換と奇置換 29

5　環 **31**

5.1　演算 31

5.2 環の定義 33
5.3 環の準同型写像 36
5.4 イデアルと剰余類環 37
5.5 整域と体 39
5.6 整数環 $\mathbb{Z}$ の基本的性質 41

読者へ

このノートは北海道教育大学教育学部札幌分校に於ける集中講義のために用意しました。「群と環」概念の「入り口」まで，受講生を導くことが目的であり，第4節と5節が到達目標です。受講生（2・3年生）の皆さんがノートを取り損なった場合に備えて配付します。講義では第5節しかお話しませんが，それ以前の節とは内容的に独立ですから，2年生なら第5節から読むことができます。（3年生には少し易し過ぎて，退屈かも知れません。）「練習問題」には，略解または解答の指針をつけておきました。本文を熟読し，全部解くつもりで，挑戦して下さい。

代数学の優れた教科書は沢山あります。代数学に興味をお持ちの方は，居相真一郎先生と相談の上で，ご自分の力量と能力に見合った教科書を推薦して貰い，読み進まれることを薦めます。

このノートと集中講義が勉学のお役にたつことを願いつつ。

2002年5月

後藤四郎

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？

(0) $100 \in \emptyset$

(1) $100 \notin \mathbb{Z}$

(2) $5 \in \mathbb{Q}$

(3) $-2 \notin \mathbb{Z}$

(4) $1 + \sqrt{2} \in \mathbb{Q}$

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

1.2 集合の表し方

集合を表すには，2 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，集合の形に書きなさい。

(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，$a \in Z$ 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なさい。

(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。次の主張を証明しなさい。

(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. 次の等式を証明しなさい。

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

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なさい。

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なさい。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なさい。商集合 $\mathbb{Z}/R$ は丁度 10 個の要素よりなることを示しなさい。

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なさい。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 に対し拡張しなさい。

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しなさい。

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なさい。

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なさい。また，$f^{-1}(\{0\})=\{-1,1\}$ であることを示しなさい。

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，次の問に答えなさい。

(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なさい。

(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なさい。

(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なさい。

(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なさい。

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。

(1) $a \in f^{-1}(Y_1)$ 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）を述べなさい。

(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 つ作りなさい。

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

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。次の問に答えなさい。

(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なさい。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なさい。

(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なさい。

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なさい。

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なさい。

(2) 写像 g は単射であるが，全射ではないことを確かめなさい。

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，$(g{\cdot}f)(a) = g(f(a))$ がすべての $a \in A$ 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，$1_A(a) = a$ がすべての $a \in A$ 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 $fg, fh, (fg)h, f(gh)$ を求めなさい。

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，それらを合成しなさい。

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なさい。

(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りなさい。

(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りなさい。

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，$g(f(a)) = a$ がすべての $a \in A$ 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なさい。

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 対称群 S_n

4.1 置換

$n \geq 1$ を整数とし，$X = \{1, 2, \cdots, n\}$ とし，$S_n = \{f \mid f : X \to X \text{ は全単射である }\}$ 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。次の主張を証明しなさい。

(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なさい。

(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なさい。

証明. 補題 4.5 の議論を用いよ。 □

命題 4.7. すべ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. すべ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しなさい。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しなさい。

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。$\varepsilon(\sigma)^2 = \prod_{i<j} \dfrac{\sigma(j) - \sigma(i)}{j - i} \cdot \displaystyle\prod_{j<i} \frac{\sigma(j) - \sigma(i)}{j - i}$ であるから

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

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。$\sigma=(a,b)$ $(1\le a<b\le n)$ 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

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

の符号を求めなさい。

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しなさい。

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なさい。

5 環

5.1 演算

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 の元の組 (a, b) から得られる 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，

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

$(a_i, b_i \in \mathbb{R})$ 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 $\mu : A \times A \to A$,

$$\left(\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \right) \mapsto \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}$$

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 $\mathbb{R}^3$ 上の演算の一つであることがわかる。

例 5.2. $A = S_n$ とすれば，$\sigma, \tau \in S_n$ 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 上に演算を定める。

例 5.3. $A = \{1, 2, 3\}$ とすれば，集合 A 上には全部で 3^9 個の演算が定義できるが，これらの演算のうち，数学的に価値のあるものはさほど多くない。

問題 5.4. 上に定めた $\mathbb{R}^3$ 内の和 $+$ について，次の主張が正しいことを確かめなさい。

(1) 任意の元 $a, b, c \in \mathbb{R}^3$ に対し，等式 $(a+b)+c = a+(b+c)$ が成り立つ。

(2) 任意の元 $a, b \in \mathbb{R}^3$ に対し，等式 $a+b = b+a$ が成り立つ。

(3) 等式 $a+0 = 0+a = a$ を任意の $a \in \mathbb{R}^3$ 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) 条件 (3) を満たす元 $0 \in \mathbb{R}^3$ は，$\mathbb{R}^3$ 内で一意的に定まる。

(5) $a \in \mathbb{R}^3$ 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。

(5) 条件 (4) を満たす $x \in R$ は，R 内で元 $a \in \mathbb{R}^3$ に対し一意的に定まる。

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) 次の主張が正しいことを確かめなさい。

(1.1) 任意の $\alpha, \beta, \gamma \in G$ 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，任意の $\alpha \in G$ 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) 次の主張が正しいかどうか調べなさい。「任意の $\alpha, \beta \in G$ に対して等式 $\alpha\beta = \beta\alpha$ が成り立つ。」

問題 5.6. $a * b = a + b + ab$ と定めれば，$*$ は集合 $\mathbb{Z}$ 上の演算である。

(1) 任意の $a, b, c \in \mathbb{Z}$ について次の等式が成り立つことを確かめなさい。

(1.1) $(a * b) * c = a * (b * c)$

(1.2) $a * b = b * a$

(1.3) $a * 0 = 0 * a = a$

(2) 次の主張が正しいかどうか調べなさい。「任意の $a \in \mathbb{Z}$ に対し，等式 $a * x = x * a = 0$ を成り立たせるような元 $x \in \mathbb{Z}$ が存在する。」

5.2 環の定義

定義 5.7. 空でない集合 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，R が環であるとは，次の 4 条件が満たされることをいう。

(1) $+$ については，次の主張が正しい。

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

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

(1.3) 等式 $a + 0 = 0 + a = a$ が任意の元 $a \in R$ 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) 任意の元 $a, b, c \in R$ に対し，等式 $(ab)c = a(bc)$ が成り立つ。

(3) 任意の元 $a, b, c \in R$ に対し，等式 $a(b + c) = ab + ac$，$(a + b)c = ac + bc$ が成り立つ。

(4) 等式 $a1 = 1a = a$ が任意の元 $a \in R$ 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 5.8. 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，R 内で一意的に定まる。

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

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

証明. (1) $0' \in R$ であって，等式 $a + 0' = 0' + a = a$ が任意の $a \in R$ について成り立つとする。$a = o$ と取れば $0' + 0 = 0$ である。一方で等式 $a + 0 = 0 + a = a$ が任意の $a \in R$ について成り立つはずであるから，$a = 0'$ と取ることによって，$0' + 0 = 0'$ が得られる。故に $0 = 0'$ である。

(2) $y \in R$ が等式 $a + y = y + a = 0$ を満たすなら，$y = y + 0 = y + (a + x) = (y + a) + x = 0 + x = x$ である。故に $y = x$ が成り立つ。

(3) $1' \in R$ であって，等式 $a1' = 1'a = a$ が任意の $a \in R$ について成り立つとする。$a = 1$ と取れば $1'1 = 1$ である。一方で等式 $a1 = 1a = a$ が任意の $a \in R$ について成り立つはずであるから，$a = 1'$ と取ることによって，$1'1 = 1'$ が得られる。故に $1 = 1'$ である。 □

乗法について交換法則が成り立つような環 (即ち，任意の 2 元 $a, b \in R$ に対し，等式 $ab = ba$ が成り立つような環) を可換環という。

例 5.9. (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 次の実正方行列全体のなす集合を $\mathrm{M}_n(\mathbb{R})$ によって表すと，集合 $\mathrm{M}_n(\mathbb{R})$ 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ないので，$\mathrm{M}_n(\mathbb{R})$ 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 $ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $ba = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = a$ 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。従って $a - a = 0$, $0 - a = -a$ である。

補題 5.10. R は環とし，$a, b \in R$ とすれば，等式

$$(a + b) - b = a, \ (a - b) + b = a$$

が成り立つ。

証明. $(a+b)-b=(a+b)+(-b)=a+[b+(-b)]=a+0=a$，$(a-b)+b=[a+(-b)]+b=a+[(-b)+b]=a+0=a$ である。 □

系 5.11 (移項の原理). R は環とし，$a,b,c\in R$ とする。次の条件は同値である。

(1) $a=b+c$

(2) $a-c=b$

特に，$a=b$ であることと，$a-b=0$ とは同値である。

証明. 補題 5.10 による。 □

命題 5.12 (環演算の基本). R は環とする。

(1) $-0=0$ である。

(2) $a\in R$ とせよ。$a+a=a$ なら $a=0$ である。

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

(4) 任意の $a,b,c\in R$ に対し次の等式が成り立つ。

(4.1) $a0=0a=0$

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

(4.3) $-a=(-1)a$，$(-a)(-b)=ab$

(4.4) $a(b-c)=ab-ac$，$(a-b)c=ac-bc$

証明. (1) $0+0=0$ による。

(2) $a+a=a$ なら，$a=(a+a)-a=a-a=0$ である。

(3) $a+b=0$ なら，$a=(a+b)-b=0-b=-b$ である。$b+a=0$ でもあるから $b=-a$ が成り立つ。$(-a)+a=0$ であるから，$-(-a)=a$ である。

(4.1) $0+0=0$ であるから $a(0+0)=a0$ である。故に $a0+a0=a0$ であるから，$a0=0$ が得られる。同様に，$(0+0)a=0a$ であるので，$0a=0$ が得られる。

(4.2) $b+(-b)=0$ であるから，両辺に a を掛ければ，左辺は $a[b+(-b)]=ab+a(-b)$，右辺は $a0=0$ となる。故に，$a(-b)+ab=0$ であるから，$a(-b)=-ab$ である。$0b=0$ であるので，$[a+(-a)]b=ab+(-a)b$ を使えば，$(-a)b=-ab$ が得られる。

(4.4) $a(b-c)=a[b+(-c)]=ab+a(-c)=ab+(-ac)=ab-ac$ である。同様に，$(a-b)c=[a+(-b)]c=ac+(-b)c=ac+(-bc)=ac-bc$ となる。 □

従って，環 R 内で等式 $1=0$ が成り立てば，如何なる元 $a\in R$ 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。

問題 5.13. $R=\mathbb{Z}\times\mathbb{Q}$ とする。集合 R は，次の加法と乗法を演算に,「可換環」をなすことを確かめなさい。

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

この環 R の中では，任意の $x,y\in\mathbb{Q}$ について等式 $(0,x)(0,y)=0$ が成り立つ。

証明. 定義を満たすことをしっかり確かめる。この環の中では，$1=(1,0)$，$0=(0,0)$ である。 □

5.3 環の準同型写像

R,S は環とする。

定義 5.14. 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) 環 R の任意の 2 元 a,b に対し，等式 $f(a+b)=f(a)+f(b)$，$f(ab)=f(a)f(b)$ が成り立つ。

(2) $f(1)=1$.

例 5.15. 例 5.13 で，$f:R\to\mathbb{Z}$ を $f(a,x)=a$ と定めれば，f は環の準同型写像である。

命題 5.16. $f:R\to S$ が環の準同型写像なら，任意の 2 元 $a,b\in R$ 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。

証明. $0+0=0$ であるから，$f(0+0)=f(0)$ が成り立ち，故に $f(0)+f(0)=f(0)$ である。従って $f(0)=0$ である。$f(a)+f(-a)=f(a+(-a))=f(a+(-a))=f(0)=0$ であるから，$f(-a)=-f(a)$ である。故に $f(a-b)=f(a+(-b))=f(a)+f(-b)=f(a)+[-f(b)]=f(a)-f(b)$ が得られる。 □

問題 5.17. 次の主張が正しいことを確かめなさい。

(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 5.18. 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ことを確かめなさい。

証明. $x, y \in S$ を取り，$x = f(a),\ y = f(b)\ (a, b \in R)$ と表せば，$x + y = f(a) + f(b) = f(a + b),\ xy = f(a)f(b) = f(ab)$ が成り立つ。故に，$f^{-1}(x + y) = a + b = f^{-1}(x) + f^{-1}(y),\ f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$ である。$f(1) = 1$ であるから，$f^{-1}(1) = 1$ が成り立つ。 □

定義 5.19. 環の準同型写像 $f : R \to S$ に対し，$\mathrm{Ker}\, f = f^{-1}(\{0\})\ (= \{a \in R \mid f(a) = 0\})$ と定め，これを f の核と呼ぶ。集合 $\mathrm{Ker}\, f$ 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 $x + y,\ ax,\ xa \in \mathrm{Ker}\, f$ となる。 □

命題 5.20. 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，等式 $\mathrm{Ker}\, f = \{0\}$ 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 $a - b = 0$ であるので，等式 $a = b$ が従う。即ち写像 f は単射である。 □

5.4 イデアルと剰余類環

定義 5.21. 集合 $\mathbb{Z}$ の空でない部分集合 I は，次の条件

$$a \in \mathbb{Z},\ x, y \in I \text{ なら}, x + y,\ ax \in I$$

を満たすとき，イデアルであるという。

例えば，集合 $\{0\}$ と $\mathbb{Z}$ 自身は，イデアルである。

補題 5.22. I がイデアルであれば，必ず $0 \in I$ であって，任意の $x, y \in I$ に対し $-y,\ x-y \in I$ となる。

証明. $z \in I$ を取れば，必ず $0 = 0z \in I$ である。$x, y \in I$ なら，$-y = (-1)y \in I$ であるから，$x - y = x + (-y) \in I$ となる。 □

命題 5.23. 整数 a に対し $I = \{na | n \in \mathbb{Z}\}$ とおけば，I はイデアルである。(これを (a) と書く。)

証明. $a = 1a \in I$ であるから，$I \neq \emptyset$ である。$\ell \in \mathbb{Z}$ とし $x, y \in I$ とせよ。$x = ma,\ y = na\ (m, n \in \mathbb{Z})$ と表せば，$x + y = (m + n)a,\ \ell x = (\ell m)a$ であるから，$x + y,\ \ell x \in I$ となり，集合 I がイデアルであることがわかる。 □

補題 5.24. イデアルについては，$I = \mathbb{Z}$ であることと $1 \in I$ とは同値である。

証明. $1 \in I$ なら，任意の $x \in \mathbb{Z}$ について $x = x1 \in I$ であるから，等式 $I = \mathbb{Z}$ が得られる。 □

定理 5.25. I はイデアルとする。

(1) $\sim = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \in I\}$ とおけば，$\sim$ は $\mathbb{Z}$ 上の同値関係である。

(2) 元 $a \in \mathbb{Z}$ に対し，$\overline{a}$ によって，a の同値類 $C(a) = \{x \in \mathbb{Z} \mid x \sim a\}$ を表すと，等式

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

が成り立つ。

(3) 加法と乗法を次のように定めることによって，商集合 $\mathbb{Z}/I = \{\overline{a} \mid a \in \mathbb{Z}\}$ は，可換環となる。

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

環 $\mathbb{Z}/I$ を I による $\mathbb{Z}$ の剰余類環という。

(4) 自然な全射 $f : \mathbb{Z} \to \mathbb{Z}/I,\ f(a) = \overline{a}$ は環の準同型写像であって，等式 $I = \mathrm{Ker}\, f$ 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) $x\sim a$ なら，$x-a\in I$ であるから，$n=x-a$ とおけば，$n\in I$ であって等式 $x=a+n$ が得られる。逆に $n\in I$ を取り $x=a+n$ とおけば，$x-a=n\in I$ より，$x\sim a$ が成り立つ。故に $\overline{a}=\{a+n\mid n\in I\}$ である。

(3) $\overline{a}=\overline{a_1},\ \overline{b}=\overline{b_1}$ ならば，$a=a_1+x,\ b=b_1+y\ (x,y\in I)$ と表されるので，$a+b=(a_1+b_1)+(x+y),\ ab=a_1b_1+(a_1y+xb_1+xy)$ である。$x+y,\ a_1y+xb_1+xy\in I$ 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 であることが確かめられる。商集合 $\mathbb{Z}/I$ が可換環になることは，忠実に定義を検証することによる。$0=\overline{0},\ -\overline{a}=\overline{-a},\ 1=\overline{1}$ である。

(4) $\overline{a}=0$ であることは，$\overline{a}=\overline{0}$ と同値であって，後者は $a=a-0\in I$ であることにほかならない。故に $\mathrm{Ker}\, f=I$ である。 □

問題 5.26. 定理 5.24 のようにして，集合 $\mathbb{Z}/(7)$ が可換環をなすことを，もう一度確かめなさい。

5.5 整域と体

以下 R は可換環とする。

定義 5.27. 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，$a\in R$ は環 R の単元であるという。

問題 5.28. 定義 (5.20) における $x\in R$ は，元 $a\in R$ に対し，環 R 内で一意的に定まることを確かめなさい。(これを a の逆元と呼び, $x=a^{-1}$ と表す。)

問題 5.29. 次の主張が正しいことを確かめなさい。

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

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

(3) a が単元であって $ax=ay$ なら，$x=y$ である。

定義 5.30. $a\in R$ に対し，写像 $\widehat{a}: R\to R$ を $\widehat{a}(x)=ax$ によって定める。

問題 5.31. $a\in R$ について次の条件は同値であることを確かめなさい。

(1) a は環 R の単元である。

(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 5.32. $x \in R$ について，$ax = 0$ ならば必ず $x = 0$ となるとき，元 a は環 R の非零因子であるという。

単元は必ず非零因子である。

問題 5.33. $a \in R$ とする。次の条件は同値であることを確かめなさい。

(1) a は R の非零因子である。

(2) 写像 $\widehat{a}$ は単射である。

定義 5.34. R が零環でなくかつ任意の元 $0 \neq a \in R$ が非零因子であるとき，環 R を整域という。

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 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，剰余環 $\mathbb{Z}/(6)$ は整域ではない。

問題 5.35. 例 5.13 の環 R は整域でないことを確かめなさい。

定義 5.36. 零環でない環 K であって，0 でない全ての元が単元であるとき，K を体という。

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である。

問題 5.37. $K_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, $K_2 = \{a + bi \mid a, b \in \mathbb{Q}\}$ とおけば，集合 K_1, K_2 は，数の和と積を演算に，体をなすことを確かめなさい。

問題 5.38. 次の主張が正しいことを証明しなさい。

(1) 体は整域である。

(2) 有限環の非零因子は単元に限る。

(3) 有限整域は体をなす。

K は体とする。2 元 $a, b \in K$ $(a \neq 0)$ に対し，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 5.39. K は体であって，$a,b,c,d \in K$ ($a,c \neq 0$) 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) $\dfrac{b}{1}=b$

証明. $(ac)\left(\dfrac{b}{a}+\dfrac{d}{c}\right)=(ac)\dfrac{b}{a}+(ac)\dfrac{d}{c}=bc+ad$ より，等式 (1) が従う。残りも同様である。 □

問題 5.40. (1) $a \geq 2$ は整数とする。$n \in \mathbb{Z}$ について，$\overline{n} \in \mathbb{Z}/(a)$ が環 $\mathbb{Z}/(a)$ の単元なら，$(a,n)=1$ であることを証明しなさい。但し (a,n) は a,n の最大公約数を表す。

(2) 整数 $p \geq 2$ が素数なら，剰余環 $\mathbb{Z}/(p)$ は体をなすことを確かめなさい。

(3) 体 $\mathbb{Z}/(2)$ と体 $\mathbb{Z}/(11)$ 内で，次の計算を実行しなさい。

$$\frac{\overline{3}}{\overline{2}}+\frac{\overline{7}}{\overline{6}},\ \frac{\overline{5}}{\overline{4}}\cdot\frac{\overline{10}}{\overline{7}},\ \frac{\overline{6}}{\overline{7}}-\frac{\overline{4}}{\overline{5}},\ -\frac{\overline{10}}{\overline{9}}$$

5.6 整数環 $\mathbb{Z}$ の基本的性質

補題 5.41 (Euclid). $n>0, m$ を整数とすれば，等式 $m=nq+r$ $(0 \leq r < n)$ が成り立つような整数の組 (q,r) が唯一つ存在する。

証明. 組 (q,r)としては, $q=\max\{x \in \mathbb{Z} | xn \leq m\}$，$r=m-nq$ を取ればよい。一意性を確かめよう。2 つの組 $(q,r),(q',r')$ がどちらも整数 $n>0,m$ に対し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 5.42. イデアル I は，必ずある整数 $a \geq 0$ 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. $I \neq (0)$ としてよいであろう。イデアル I は少なくとも一つ正整数 c を含むので，$a=\min\{c \in I | c>0\}$ とおき，等式 $I=(a)$ が成立することを示そう。$a \in I$ より，$(a) \subseteq I$ を得る。元 $x \in I$ をとり，$x=aq+c$，$0 \leq c < a$ と表すと，$c=x-aq \in I$ となる。正整数 a の最小性から $c=0$ が従い，$x=aq \in (a)$ が得られる。故に $I=(a)$ である。 □

系 5.43. (1) $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ をイデアルの昇鎖とすれば，整数 $k \geq 1$ を選び，全ての整数 $i \geq k$ について等式 $I_k = I_i$ が成り立つようにできる。

(2) イデアル全体のなす集合を $\mathfrak{S}$ とすれば，$\mathfrak{S}$ 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，(即ち，$M \in \mathcal{S}$ であってしかも $M \subsetneq I$ となるような $I \in \mathcal{S}$ は存在しないような M) を含む。

証明. (1) $I = \bigcup_{i \geq 1} I_i$ とおけば，I はイデアルである。等式 $I = (a)$ が成り立つよう $0 \leq a \in I$ をとり，$a \in I_k$ となるよう整数 $k \geq 1$ を選ぶ。$i \geq k$ とすれば，$I = (a) \subseteq I_i$ であって $I_i \subseteq \bigcup_{i \geq 1} I_i = I$ あるので，等式 $I_i = I$ 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 $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_i \subsetneq \cdots$ を作ることができるが，これは系 5.43 により不可能である。 □

定義 5.44. イデアル I が次の 2 条件

(1) $I \neq \mathbb{Z}$

(2) イデアル J が包含関係 $I \subseteq J$ 満たすならば，$I = J$ であるか又は $J = \mathbb{Z}$ が成り立つ

を満たすとき，I は極大イデアルであるという。極大イデアル全体から成る集合を $\mathcal{M}$ で表す。

系 5.43(2) より，I がイデアルで $I \neq \mathbb{Z}$ ならば，I を含むような極大イデアルが少なくとも一つは存在する。故に $\mathcal{M} \neq \emptyset$ である

定義 5.45. 整数 p に対し，イデアル (p) が極大イデアルであるとき，p は素数であるという。

極大イデアル M に対し，等式 $M = (p)$ が成り立つ整数 p を取れば，定義により p は素数であって，必ず $p \neq 0, \pm 1$ が成り立つ。

補題 5.46. I をイデアルとしたとき，剰余環 $\mathbb{Z}/I$ が体であるための必要十分条件は，$I \in \mathcal{M}$ である。

証明. $M \in \mathcal{M}$ とせよ。剰余環 $\mathbb{Z}/M$ の元 $\alpha \neq 0$ を取り，$\alpha = \overline{a}$ $(a \in \mathbb{Z})$ と表すと，$a \notin M$ であって，イデアル $J = \{ax + y | x \in \mathbb{Z},\ y \in M\}$ は，$a \in J$ であるから，包含関係 $M \subsetneq J$ を満たす。M は極大イデアルであるので，等式 $J = \mathbb{Z}$ が従う。$1 = ax + y$ が成立するよう $x \in \mathbb{Z}$ と $y \in M$ を選べば，$\mathbb{Z}/M$ 内では $\overline{1} = \overline{ax} + \overline{y} = \overline{a} \cdot \overline{x}$ が成り立ち，$\alpha = \overline{a}$ は $\mathbb{Z}/M$ の単元であ

ることがわかる。逆に，I をイデアルとし，剰余環 $\mathbb{Z}/I$ が体であると仮定すると，$I \neq \mathbb{Z}$ であるから，$I \subseteq M$ となる $M \in \mathcal{M}$ が存在する。$I = M$ であることを確かめよう。$I \subsetneq M$ と仮定し，I に含まれないような M の元 a を取り，$\alpha = \overline{a}$ とおくと，α は体 $\mathbb{Z}/I$ の単元であるから，$1 - ax \in I$ となるような $x \in \mathbb{Z}$ が存在する。即ち，等式 $1 = ax + i$ を成り立たせるような $i \in I$ が存在するが，$a \in M$ であって $I \subseteq M$ であるから，$1 = ax + i \in M$ となり，不可能な等式 $M = \mathbb{Z}$ が得られる。故に $I = M$ であり，$I \in \mathcal{M}$ である。 □

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

系 5.47. p を素数とし a, b を整数とすれば，次の主張が正しい。

(1) $p|ab$ ならば，$p|a$ であるか又は $p|b$ が成り立つ。
(2) $a|p$ ならば，$a = \pm 1$ であるか又は $a = \pm p$ が成り立つ。

証明. $ab \in (p)$ であると仮定せよ。体 $\mathbb{Z}/(p)$ 内では $\overline{a}\overline{b} = 0$ であって，体は整域であるから，$\overline{a} = 0$ であるか又は $\overline{b} = 0$ が成り立つ。即ち，$a \in (p)$ であるか又は $b \in (p)$ である。$p \in (a)$ ならば，(p) は $\mathbb{Z}$ の極大イデアルであるから，等式 $(a) = (p)$ が成り立つか，又は $(a) = \mathbb{Z}$ が成り立つ。即ち $a = \pm p$ であるかまたは $a = \pm 1$ である。 □

系 5.48. $a \geq 1$ は整数とする。次の条件は同値である。

(1) a は素数である。
(2) $a \geq 2$ であって，a は既約である（即ち，整数 $d \geq 1$ が $d|a$ を満たすなら必ず $d = 1$ であるか又は $d = a$ が成り立つ）。

証明. (2)⇒(1) のみで十分であろう。$I = (a)$ とすれば，$I \neq \mathbb{Z}$ であるので，$I \subseteq M$ となる $M \in \mathcal{M}$ を取ることができ，等式 $M = (p)$ をみたす整数 $p \geq 2$ が得られる。$p|a$ であるので，仮定 (2) より $a = p$ が従い，a は素数であることがわかる。 □

定理 5.49. $a \geq 2$ が整数なら，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 $a = p_1 p_2 \cdots p_n$ は，順序の違いを除いて，整数 a に対し一意的に定まる。

証明. 定理のようには表せない整数 $a \geq 2$ が存在したと仮定する。この時，$\mathcal{S} = \{(x) | 2 \leq x \in \mathbb{Z}$ であって x 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 $\mathcal{S}$ には包含関係に関する極大元 $I = (b)$ $(b \geq 2)$ が存在する。$I \neq \mathbb{Z}$ であるから，I はある極大イデアル

$M = (p)$ $(p \geq 2)$ に含まれる。$b \in (p)$ であるから，整数 $c \geq 2$ を $b = pc$ が成り立つようとり，$J = (c)$ とおけば，$I \subsetneq J$ となる。イデアル I は集合 $\mathcal{S}$ 内で極大であるので，$J \notin \mathcal{S}$ であり，故に，整数 c は素因数分解を持ち，$b = pc$ も素因数分解を持つことが従うが，これは不可能である。次に，$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ $(p_i, q_j \geq 2$，素数$)$ とせよ。$n = 1$ ならば，$p_1 = q_1 q_2 \cdots q_m$ であって，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，$q_1 q_2 \cdots q_m \in (p_1)$ 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。並べ替えて $p_1 = q_1$ と仮定してよい。すると，$p_2 \cdots p_n = q_2 q_3 \cdots q_m$ であるので，帰納法の仮定より，$n = m$ と $p_i = q_i$ $(2 \leq i \leq n)$ とが従う。 □

系 5.50. 素数の個数は無限である。

証明. 素数が有限個 $\{\pm p_1, \pm p_2, \cdots, \pm p_n\}$ $(p_i \geq 2)$ 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 1.15 によって，$p|a$ となる素数 $p \geq 2$ が存在する。勿論この 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，$p_1|a = p_1 p_2 \cdots p_n + 1$ より，$p_1|1$ となる。これは不可能である。 □

さて，整数 $a_1, a_2, \cdots, a_n$ を取り，$I = \{\sum_{i=1}^{n} r_i a_i | r_i \in \mathbb{Z}\}$ とおく。集合 I はイデアルである。整数 a を等式 $I = (a)$ が成り立つよう取れば，$a_i \in I = (a)$ であるから，$a|a_i$ が全ての $1 \leq i \leq n$ に対して成り立つ。一方，$a \in I$ であるから，$a = \sum_{i=1}^{n} r_i a_i$ $(r_i \in \mathbb{Z})$ と表すことができる。故に，整数 $d \in \mathbb{Z}$ が全ての $1 \leq i \leq n$ に対し $d|a_i$ ならば，$d|a$ が成り立つことがわかる。即ち a は $a_1, a_2, \cdots, a_n$ の最大公約数である。故に，$a_1, a_2, \ldots, a_n$ の最大公約数を a とすれば，等式 $(a) = \{\sum_{i=1}^{n} r_i a_i | r_i \in \mathbb{Z}\}$ が成り立つことがわかる。

系 5.51. a, b を整数とすれば，a, b の最大公約数が 1 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 $x, y \in \mathbb{Z}$ が存在することである。

系 5.52. a, b, c は整数とせよ。a, b の最大公約数が 1 であってかつ $a|bc$ ならば，$a|c$ である。

証明. $bc = ad$ とし，$x, y \in \mathbb{Z}$ をとって $1 = ax + by$ と表すと，等式 $c = acx + bcy = acx + ady = a(cx + dy)$ が得られ，$a|c$ が従う。 □