離散数学

テキスト

成蹊大学 理工学部 理工学科
山本真基

２０２３年４月

はじめに

コンピュータサイエンスで扱われる数学の基礎知識及び基礎概念を学習する．コンピュータがその内部で処理しているのは離散的な値である．そういった離散的な値を対象とした数学，「離散数学」，と呼ばれる数学の基礎を学習する．

まずはじめに，離散数学の基礎事項として，集合，写像，関係，論理を取り上げる．（第１章〜４章.）これらは，コンピュータサイエンスの様々な理論分野[*1]で遭遇する重要な基礎概念である．次に，離散数学で用いられる典型的な証明手法を学習する．（第５章.）離散数学の多くの重要な定理が，これら基本的な証明手法（の組み合わせ）によって導かれているという事実がある．最後に，初等的な整数論，及び，それを応用した暗号を取り上げる．（第６章・７章.）その応用を通じて，離散数学がどのように現実社会に役立っているかを認識してほしい．

離散数学をはじめ，微分積分学，線形代数学などの数学を学ぶとき，学ぶ目的を考えるのは自然なことである．（学んで何の役に立つのか，など.）しかし，分野を概観する前から，初学者が明確な目的を持っていることはかなり稀である．また，目的がないことを続けることも容易でない．離散数学に限って言えば，次のようなことも学ぶ目的の一つとして考えられる[*2]：コンピュータサイエンスの全分野に渡って共通で必須の能力である「プログラミング力」を向上させる．これには二つの意味がある．

一つは，「実装力」の向上という意味である．プログラミングをするとき，単純なことを実装する場合を除いて，たいていは，頭の中や紙の上で対象物を抽象的にとらえる作業が介入する．この作業を通じて，プログラミングをするときの「設計図」ができる．（ソフトウェア開発の言葉では「仕様書」となる.）設計図をつくる際に強力な道具となるのが，離散数学で学ぶ（集合や論理などの）概念，及び，記号や図を用いた数学的表記である．それらを用いて，離散数学で定められた「文法」に則して，離散的な対象物を論理的に正しく記述する．こうした準備のもと，プログラミングでは，言語で定められた文法に則して，設計図で描かれた対象物（及び「機械的手順」）を正確に記述する．このとき，設計図が間違っていれば，プログラムが正しく動作しないことは明らかである．

もう一つは，離散数学の応用という意味である．離散数学とは，コンピュータサイエンス特有の問題を解決するために誕生した数学である．一方で，プログラミングとは，コンピュータサイエンスをコンピュータで具現化するための手段である．離散数学に精通することは，プログラミングをする上での「道具箱」を豊富にすることにつながる．

[*1] 組合せ論，計算理論，情報理論，アルゴリズム論，最適化理論，暗号理論，符号理論，などなど.

[*2] 離散数学の知識や概念を修得して，そこで展開される理論を味わうことが第一の目的ではあるが...

本テキストは，離散数学のごく一部（の初歩的なこと）しか扱っていない．（他にも，「グラフ理論」に代表されるよう，「組合せ論」という重要な分野がある．）離散数学について更に学びたい学生は，参考図書の章であげた教科書や，それらの教科書であげられている参考図書を参照するとよい．

最後に，原稿を丹念に読んで誤りを訂正して下さった，情報科学科教員の姫野哲人氏，脊戸和寿氏，松本直己氏に感謝致します．

２０１８年1月　山本真基

新出用語

本書で学習する新しい用語は，新出時に**太字で**書かれる．更に，それらは，すべて以下のように「定義」として丸枠で囲われる．

定義 1.1

「もの」の集まりのことを**集合**という．集合を成すものを**要素**という．

命題，定理，補題，系

命題とは，真偽を一意に定めることができる言明（statement）のことである．定理とは，命題の中で特に重要な命題のことをいう．補題とは，命題を示すための補助的な命題のことをいう．系とは，命題から（比較的）容易に得られる命題のことをいう[*3]．本書で学習する命題，定理，補題，系は，すべて以下のようにマゼンタ色で塗られる．

命題 1.1. U を全体集合，A, B を U の部分集合とする．このとき，$A \subseteq B$ であるときかつそのときに限り，$\bar{B} \subseteq \bar{A}$ である．

本文中の問

本書にある問は，すべて以下のように灰色で塗られる．

問 1.1. A を 1 から 999 までの自然数の集合とする．このとき，$-1 \in A$, $10 \notin A$, $1000 \in A$ のうち，正しいものはどれか．

[*3] とはいうものの，厳密な区別が（特に命題と定理などに）あるわけではない．

目次

第 1 章

集合

1.1　集合とは

定義 1.1

「もの」の集まりのことを**集合**という．集合を成すものを**要素**という．

定義 1.2

A を集合とする．a が A の要素であるとき，a は A に**属する**といい，$a \in A$ と表す．また，a が A の要素でないとき，a は A に**属さない**といい，$a \notin A$ と表す．

例 1.1 (属する，属さない)**.** A を 5 つの自然数 $1, 2, 3, 4, 5$ からなる集合とする．このとき，$1 \in A$ であり，$0 \notin A$ である．

問 1.1. A を 1 から 999 までの自然数の集合とする．このとき，$-1 \in A$, $10 \notin A$, $1000 \in A$ のうち，正しいものはどれか.

問 1.2. A を首都の集合とする．このとき，ニューヨーク $\in A$, 東京 $\notin A$, ヨーロッパ $\in A$ のうち，正しいものはどれか.

定義 1.3

数の集合の表記としては，以下のものがよく使われる．

$\mathbb{N}$ ： 自然数（natural）の集合
$\mathbb{Z}$ ： 整数（integer）の集合
$\mathbb{Q}$ ： 有理数（rational）の集合
$\mathbb{R}$ ： 実数（real）の集合

また，$\mathbb{N}_0$ を「0 を含めた自然数の集合」とする．

定義 1.4

集合を表すとき，要素すべてを列挙する表し方を**外延的記法**といい，要素のもつ性質を明記する表し方を**内包的記法**という．

例 1.2 (外延的記法，内包的記法)．5 つの自然数 $1, 2, 3, 4, 5$ からなる集合は，以下の二通りに表される．

外延的記法 ： $\{1, 2, 3, 4, 5\}$
内包的記法 ： $\{i \in \mathbb{N} : 1 \leq i \leq 5\}$

問 1.3. 素数の集合，一桁の正の偶数の集合，首都の集合を，外延的記法または内包的記法で表しなさい．

注 1.1. 単に集合といった場合，要素は重複しないものとする．例えば，集合 $\{1, 2, 3, 1, 1, 3\}$ は集合 $\{1, 2, 3\}$ に同じである．また，要素の順序は気にしない．例えば，集合 $\{2, 1, 3\}$ は集合 $\{1, 2, 3\}$ に同じである．

定義 1.5

A を集合とする．A の要素の個数を A の**大きさ**（または**サイズ**）といい，$|A|$ と表す．大きさが 0 の集合，つまり，要素のない集合を**空集合**といい，$\emptyset$ と表す．大きさが有限の集合を**有限集合**，無限の集合を**無限集合**という．

例 1.3 (集合の大きさ)．$A = \{1, 2, 3, 4, 5\}$ とする．このとき，$|A| = 5$ である．よって，A は有限集合である．一方，$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ はすべて無限集合である．

1.2　部分集合

定義 1.6

A, B を集合とする．A のすべての要素が B の要素であるとき，A は B に**含まれる**という．このとき，A は B の**部分集合**であるといい，$A \subset B$ または $A \subseteq B$ と表す．そうでないとき，$A \not\subset B$ または $A \not\subseteq B$ と表す．

A と B が同一の集合であるとき $A = B$ と表す．（厳密には，$A \subseteq B$ かつ $A \supseteq B$ であるとき $A = B$ と表す．）そうでないとき $A \neq B$ と表す．（厳密には，$A \not\subseteq B$ または $A \not\supseteq B$ であるとき $A \neq B$ と表す．）

$A \subseteq B$ かつ $A \neq B$ であるとき，A は B の**真部分集合**であるといい，特に，$A \subsetneq B$ と表す．（このとき，$A \subseteq B$ と表しても間違いではない．）

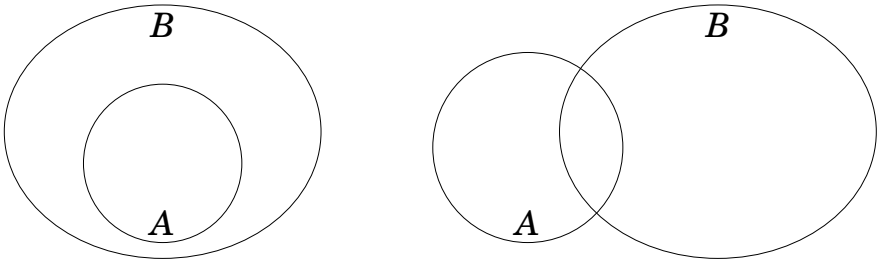

図 1.1　ベン図：$A \subseteq B$（左図）と $A \not\subseteq B$（右図）

例 1.4 (部分集合，真部分集合)**.** $B = \{1, 2, 3, 4, 5\}$ とする．$A = \{1, 2, 5\}$ であるとき，$A \subseteq B$ であり，また $A \subsetneq B$ でもある．（$A \not\subseteq B$ ではない．）

事実 1.1. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$．（同時に，$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$ でもある．）

問 1.4. A を任意の集合とする．以下のうち正しいものはどれか．

(1)　$A \subseteq A$　(2)　$A \not\subseteq A$　(3)　$A \subsetneq A$　(4)　$\emptyset \subseteq \emptyset$　(5)　$\emptyset \subseteq A$

1.3　補集合

定義 1.7

考える対象となる全体の集合を**全体集合**という．U を全体集合，A を U の部分集合とする．このとき，A に属さない U の要素の集合を A の**補集合**といい，$\bar{A}$ と表す．つまり，

$$\bar{A} \stackrel{\text{def}}{=} \{a \in U : a \notin A\}.$$

以降，$X \stackrel{\text{def}}{=} Y$ を「X の定義は Y である」ことを意味するものとする[*1]．

例 1.5 (補集合)**.** $U = \{1, 2, 3, 4, 5\}$ を全体集合とする．$A = \{1, 2, 5\}$ のとき, $\bar{A} = \{3, 4\}$.

問 1.5. 全体集合を $\mathbb{Z}$ とする．$\mathbb{E}$ を偶数の集合とする．このとき，$\overline{\mathbb{E}}$ は何か.

事実 1.2. U を全体集合，A を U の部分集合とする．このとき，

$$\bar{\bar{A}} = A.$$

命題 1.1. U を全体集合，A, B を U の部分集合とする．このとき，$A \subseteq B$ であるときかつそのときに限り，$\bar{B} \subseteq \bar{A}$ である.

証明. この命題を示すためには，以下の二つを示せばよい.

1. $A \subseteq B$ であるとき，$\bar{B} \subseteq \bar{A}$ である
2. $\bar{B} \subseteq \bar{A}$ であるとき，$A \subseteq B$ である

一つ目はベン図を用いて示される．二つ目は一つ目を用いて次のように示される．まず，記号が混同しないように，一つ目を以下のように（A, B でなく）X, Y を用いて表記する.

$$X \subseteq Y \text{ であるとき，} \bar{Y} \subseteq \bar{X} \text{ である} \quad \cdots \quad (*)$$

上の $(*)$ において，$X = \bar{B}, Y = \bar{A}$ と定義する．このとき，（もともとの）仮定 $\bar{B} \subseteq \bar{A}$ より，$X \subseteq Y$ となり，$(*)$ の仮定が成り立つ．よって，その結論である $\bar{Y} \subseteq \bar{X}$ が成り立つ．$X = \bar{B}, Y = \bar{A}$ としたことから，$\bar{X} = B, \bar{Y} = A$ となる．これを $\bar{Y} \subseteq \bar{X}$ に代入すれば $A \subseteq B$ が得られる． ■

[*1] “def” とは definition（定義）の頭文字 3 文字である.

1.4　和集合，積集合

定義 1.8

A, B を集合とする．A と B の少なくとも一方に属する要素の集合を，A と B の**和集合**といい，$A \cup B$ と表す．A と B の両方に属する要素の集合を，A と B の**積集合**といい，$A \cap B$ と表す．つまり，

$$\begin{aligned} A \cup B &\stackrel{\text{def}}{=} \{x : x \in A \text{ または } x \in B\}, \\ A \cap B &\stackrel{\text{def}}{=} \{x : x \in A \text{ かつ } x \in B\}. \end{aligned}$$

例 1.6 (和集合，積集合)**.** $A = \{1, 2, 3, 4, 5\}$，$B = \{1, 5, 10, 11\}$ とする．このとき，

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5, 10, 11\}, \\ A \cap B &= \{1, 5\}. \end{aligned}$$

問 1.6. $A = \{1, 2, 3, 4, 5\}$，$B = \{2, 3, 5, 7, 11\}$ とする．このとき，$A \cup B$, $A \cap B$ を求めなさい．

命題 1.2 (分配則)**.** A, B, C を集合とする．このとき，

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C). \end{aligned}$$

証明. ベン図より明らか. ■

命題 1.3. A, B を集合とする．このとき，

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

証明. ベン図より明らか. ■

定義 1.9

A, B を集合とする．A から B を除いた集合を A と B の**差集合**といい，$A \setminus B$ と表す．A と B のどちらか一方だけに属する要素の集合を A と B の**対称差集合**と

いい，$A \oplus B$ と表す．つまり，

$$\begin{aligned} A \setminus B &\stackrel{\text{def}}{=} \{x : x \in A \text{ かつ } x \notin B\}, \\ A \oplus B &\stackrel{\text{def}}{=} \{x : (x \in A \text{ または } x \in B) \text{ かつ } x \notin A \cap B\}. \end{aligned}$$

例 1.7 (差集合，対称差集合)**.** $A = \{1, 2, 3, 4, 5\}$，$B = \{1, 5, 10, 11\}$ とする．このとき，

$$\begin{aligned} A \setminus B &= \{2, 3, 4\}, \\ A \oplus B &= \{2, 3, 4, 10, 11\}. \end{aligned}$$

問 1.7. $A = \{1, 2, 3, 4, 5\}$，$B = \{2, 3, 5, 7, 11\}$ とする．このとき，$A \setminus B$, $A \oplus B$ を求めなさい．

命題 1.4. A, B を集合とする．このとき，

$$\begin{aligned} A \oplus B &= (A \setminus B) \cup (B \setminus A) \\ &= (A \cup B) \setminus (A \cap B) \end{aligned}$$

証明. ベン図より明らか． ■

1.5　ド・モルガンの法則

定理 1.5 (ド・モルガンの法則)**.** U を全体集合，A, B を U の部分集合とする．このとき，

$$\begin{aligned} \overline{A \cup B} &= \bar{A} \cap \bar{B} \\ \overline{A \cap B} &= \bar{A} \cup \bar{B} \end{aligned}$$

証明. ベン図より明らか． ■

定理 1.6 (ド・モルガンの法則（一般形）)**.** k を任意の自然数とする．U を全体集合，$A_1, \ldots A_k$ を U の部分集合とする．（つまり，$A_1, \ldots, A_k \subseteq U$.）このとき，

$$\begin{aligned} \overline{A_1 \cup \cdots \cup A_k} &= \bar{A}_1 \cap \cdots \cap \bar{A}_k \\ \overline{A_1 \cap \cdots \cap A_k} &= \bar{A}_1 \cup \cdots \cup \bar{A}_k \end{aligned}$$

証明. 一つ目の等式を数学的帰納法により示す.（二つ目の等式も同様にして示される.）$k = 1$ のとき，等式が成り立つのは明らかである．$k-1$（$k \geq 2$）のとき，等式が成り立つとする．つまり，

$$\overline{A_1 \cup \cdots \cup A_{k-1}} \;=\; \bar{A}_1 \cap \cdots \cap \bar{A}_{k-1}. \tag{1.1}$$

また，ド・モルガンの法則より，任意の集合 A, B について，

$$\overline{A \cup B} \;=\; \bar{A} \cap \bar{B} \tag{1.2}$$

この二つの等式より，

$$\begin{aligned}
\overline{A_1 \cup \cdots \cup A_k} &= \overline{(A_1 \cup \cdots \cup A_{k-1}) \cup A_k} \\
&= \overline{(A_1 \cup \cdots \cup A_{k-1})} \cap \bar{A}_k \quad (\because\ (1.2)) \\
&= \left(\bar{A}_1 \cap \cdots \cap \bar{A}_{k-1}\right) \cap \bar{A}_k \quad (\because\ (1.1)) \\
&= \bar{A}_1 \cap \cdots \cap \bar{A}_k.
\end{aligned}$$

■

定義 1.10

任意の自然数 $k \in \mathbb{N}$ に対して，$X = \{1, 2, \ldots, k\}$ とする．任意の $i \in X$ について，A_i を集合とする．このとき，

$$\bigcup_{i \in X} A_i \;\overset{\text{def}}{=}\; A_1 \cup A_2 \cup \cdots \cup A_k$$

$$\bigcap_{i \in X} A_i \;\overset{\text{def}}{=}\; A_1 \cap A_2 \cap \cdots \cap A_k$$

この表記に従えば，ド・モルガンの法則（一般形）は次のように表される．$X = \{1, 2, \ldots, k\}$ として，

$$\overline{\bigcup_{i \in X} A_i} \;=\; \bigcap_{i \in X} \bar{A}_i$$

$$\overline{\bigcap_{i \in X} A_i} \;=\; \bigcup_{i \in X} \bar{A}_i$$

1.6 集合族

定義 1.11

集合の集まり（集合の集合）のことを**集合族**という.

例 1.8 (集合族)**.**

1. $\{\{1\},\{2\},\{3\}\}$,
2. $\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{2,3\},\{1,2,3\}\}$,
3. $\{\{a\},\{e\},\{a,b\},\{b,c\},\{c,d,e\},\{a,b,c,d,e\}\}$.

問 1.8. $\emptyset$ を空集合とする．$\emptyset$ と $\{\emptyset\}$ はどう違うか．（参考までに，$|\emptyset|$, $|\{\emptyset\}|$ を比較しなさい．）

問 1.9. 以下のうち正しいものはどれか．

(1)	$\emptyset \in \emptyset$	(2)	$\emptyset \subseteq \emptyset$	(3)	$\emptyset \in \{\emptyset\}$	(4)	$\emptyset \subseteq \{\emptyset\}$
(5)	$1 \in 1$	(6)	$1 \subseteq 1$	(7)	$1 \in \{1\}$	(8)	$1 \subseteq \{1\}$
(9)	$\{1\} \in \{1\}$	(10)	$\{1\} \subseteq \{1\}$	(11)	$\{1\} \in \{\{1\}\}$		
(12)	$\{1\} \subseteq \{\{1\}\}$	(13)	$1 \in \{1,\{1\}\}$	(14)	$1 \subseteq \{1,\{1\}\}$		
(15)	$\{1\} \in \{1,\{1\}\}$	(16)	$\{1\} \subseteq \{1,\{1\}\}$				

定義 1.12

A を集合とする．A の部分集合のすべてからなる集合を A の**べき集合**といい，2^A と表す．

例 1.9 (べき集合)**.** $A = \{1,2,3\}$ とする．このとき，

$$2^A = \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}.$$

問 1.10. $A = \{0,1\}$ とする．このとき，2^A を求めなさい．

事実 1.3. A を集合とする．$B \in 2^A$ と $B \subseteq A$ は同じことである．

命題 1.7. 任意の有限集合 A について，$|2^A| = 2^{|A|}$.

証明. $S \subseteq A$ を A の任意の部分集合とする．集合 S を，それぞれの $a \in A$ について，a が S に入らないとき 0，a が S に入るとき 1，とした 0/1 の列とみたてる．このとき，集合 2^A を，長さ $|A|$ の 0/1 の列の集合とみなすことができる．長さ $|A|$ の 0/1 の列が $2^{|A|}$ 個あることより，命題が示される． ■

例 1.10. $A = \{1, 2, 3\}$ としたとき，$|2^A| = 2^{|A|} = 2^3 = 8$. 以下の表で示されるように，$0/1$ の列と A の部分集合が対応付けられる.

1	2	3	2^A
0	0	0	$\emptyset$
1	0	0	$\{1\}$
0	1	0	$\{2\}$
0	0	1	$\{3\}$
1	1	0	$\{1, 2\}$
1	0	1	$\{1, 3\}$
0	1	1	$\{2, 3\}$
1	1	1	$\{1, 2, 3\}$

問 1.11. $2^\emptyset$ を求めなさい.（上の命題より，$|2^\emptyset| = 2^0 = 1$.）

1.7 集合の分割

定義 1.13

A を集合とする. $A_1, A_2, \ldots, A_k \subseteq A$ が以下を満たすとき，$A_1, A_2, \ldots, A_k$ を A の**分割**という.

1. $A = A_1 \cup A_2 \cup \cdots \cup A_k$,
2. すべての $i, j : i \neq j$ について $A_i \cap A_j = \emptyset$.

例 1.11 (分割)**.** $\mathbb{E}$ を偶数の集合，$\mathbb{O}$ を奇数の集合とすれば，$\mathbb{E}, \mathbb{O}$ は $\mathbb{Z}$ の分割である.

問 1.12. $\mathbb{Z}$ の分割となる例をあげなさい.

章末問題

以下の問いに答えなさい.

1. 以下の集合を内包的記法で表記しなさい.
   (a) -5 から 10 までの整数の集合
   (b) 無理数の集合
   (c) 都道府県庁所在地の集合
   (d) 3 で割ったら 2 余る自然数の集合
   (e) 60 の約数のうち，12 以下の自然数の集合
2. 上の問題の集合のうち有限集合はどれか．また，有限集合であればその大きさを求めなさい.
3. 以下のうち正しいものはどれか.

   1. $\{5\} \in \{2,3,5,\{7\}\}$
   2. $\{5\} \subseteq \{2,3,5,\{7\}\}$
   3. $\{7\} \in \{2,3,5,\{7\}\}$
   4. $\{7\} \subseteq \{2,3,5,\{7\}\}$
   5. $\{\{5\}\} \subseteq \{2,3,5,\{7\}\}$
   6. $\{\{7\}\} \subseteq \{2,3,5,\{7\}\}$
   7. $\{a,d\} \in \{a,b,c,\{a,d\}\}$
   8. $\{a,d\} \subseteq \{a,b,c,\{a,d\}\}$
   9. $\{a,\{a,d\}\} \in \{a,b,c,\{a,d\}\}$
   10. $\{a,\{a,d\}\} \subseteq \{a,b,c,\{a,d\}\}$
   11. $\emptyset \subseteq \emptyset$
   12. $\emptyset \in \{\emptyset\}$

4. $U = \{i \in \mathbb{Z} : 1 \leq i \leq 10\}$ を全体集合とする．また，$A = \{2,3,5,7\}$, $B = \{1,2,3,4,5\}$, $C = \{1,3,5,7,9\}$ とする．このとき，以下を求めなさい.
   (a) $\bar{A}$, $\bar{B}$, $\bar{C}$
   (b) $\overline{A \cup B \cup C}$
   (c) $\overline{A \cap B \cap C}$

   このとき，(b), (c) について，ド・モルガンの法則が成り立つことを確認しなさい.
5. 2 で割り切れる整数の集合を A，3 で割り切れる整数の集合を B とする．このとき，以下の集合を内包的記法で表記しなさい.
   (a) $A \cup B$
   (b) $A \cap B$
   (c) $A \setminus B$
   (d) $A \oplus B$
6. $A = \{a,b,c\}$ とする．このとき，A のべき集合を求めなさい.
7. $|A| = n$ とする．このとき，A のべき集合の大きさはいくらか.

第 2 章

写像

2.1 写像とは

定義 2.1

A, B を集合とする．A の任意の要素が B のある一つの要素に対応しているとき，その「対応」f を A から B への**写像**または**関数**といい，$f : A \to B$ と表す．このとき，A を f の**定義域**，B を f の**値域**という．

例 2.1 (写像，関数)**.** 以下のような $f : \mathbb{R} \to \mathbb{R}$ はすべて写像である．

1. $f(x) = 10$
2. $f(x) = x^2 + x - \sqrt{2}$
3. $f(x) = \sin x + \cos x$

また，以下のように表で示された $f : \{0, 1, \ldots, 5\} \to 2^{\{a,b,c\}}$ も写像である[*1]．

x	0	1	2	3	4	5
$f(x)$	$\{a\}$	$\{a\}$	$\{a, b, c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$

問 2.1. 写像でない例を挙げなさい．

定義 2.2

A, B を集合，f を A から B への写像とする．$A' \subseteq A$ とする．このとき，以

[*1] あくまで（表で示される）写像の「具体例」である．（この表と異なる例はいくらでもある．）

下で定義される $f(A')$ を，f による A' の**像**という．

$$f(A') \stackrel{\text{def}}{=} \{f(a) \in B : a \in A'\}.$$

例 2.2 (像)**.** $f(x) = \sin x$ とする．このとき，$f(\mathbb{R}) = [-1, 1]$．また，例 2.1 の関数 $f : \{0, 1, \ldots, 5\} \to 2^{\{a,b,c\}}$ では,

$$f(\{0, 1, \ldots, 5\}) \;=\; \{\{a\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

問 2.2. $f(x) = \sin x$ とする．このとき，$f([0, \pi/2])$ を求めなさい．

問 2.3. f を例 2.1 の関数 $f : \{0, 1, \ldots, 5\} \to 2^{\{a,b,c\}}$ とする．このとき，$f(\{0, 1, 3, 4, 5\})$ を求めなさい．

事実 2.1. $f : A \to B$ を写像とする．このとき，任意の $A' \subseteq A$ について $f(A') \subseteq B$.

2.2　全射，単射，全単射

定義 2.3

A, B を集合，f を A から B への写像とする．$f(A) = B$ であるとき，f を**全射**という．（つまり，任意の $b \in B$ についてある $a \in A$ が存在して $f(a) = b$.）任意の $a, a' \in A$ について，$a \neq a'$ ならば $f(a) \neq f(a')$ が満たされるとき，f を**単射**という．f が全射であり単射であるとき，f を**全単射**という．

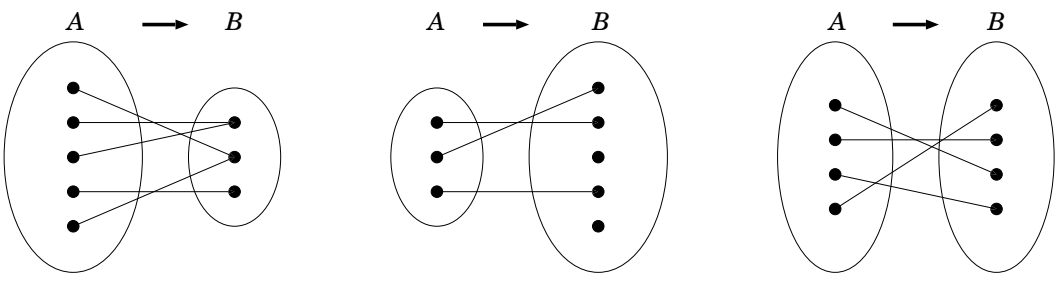

図 2.1　全射（左図），単射（中図），全単射（右図）

問 2.4. $f : \mathbb{R} \to \mathbb{R}$ を $f(x) = x^2$ とする．このとき，関数 f は，全射であるか．また，関数 f は，単射であるか．

問 2.5. $A, B \subseteq \mathbb{R}$ を実数の部分集合とする．$f : A \to B$ を $f(x) = x^2$ とする．A, B が以下であるとき，関数 f は，全射，単射，全単射，のいずれになるか．

1. $A = \{a \in \mathbb{R} : a \geq 0\}$, $B = \mathbb{R}$
2. $A = \mathbb{R}$, $B = \{b \in \mathbb{R} : b \geq 0\}$
3. $A = \{a \in \mathbb{R} : a \geq 0\}$, $B = \{b \in \mathbb{R} : b \geq 0\}$

命題 2.1. A, B を有限集合とする．A から B への全単射が存在するときかつそのときに限り，$|A| = |B|$ である．

証明. この命題を示すためには，以下の二つを示せばよい．

1. A から B への全単射が存在するとき，$|A| = |B|$ である
2. $|A| = |B|$ であるとき，A から B への全単射が存在する

一つ目を示す．A から B への全単射 f が存在するとする．f が全射であることから，$|B| \leq |A|$．また，f が単射であることから，$|A| \leq |B|$．よって，$|B| \leq |A|$ かつ $|A| \leq |B|$ より $|A| = |B|$ が導かれる．

二つ目を示す．$|A| = |B| = s$ であるとする．このとき，一般性を失うことなく，$A = \{a_1, \ldots, a_s\}$，$B = \{b_1, \ldots, b_s\}$ と表せる．写像 $f : A \to B$ を次のように定義する．任意の $i : 1 \leq i \leq s$ について $f(a_i) = b_i$．この写像が全単射であることは明らかである． ■

注 2.1. この命題の A, B を無限集合にしたものがベルンシュタインの定理である．（その証明は有限の場合ほど単純でない．）

2.3 恒等写像，逆写像

定義 2.4

A を集合，f を A から A への写像とする．このとき，任意の $a \in A$ について $f(a) = a$ であるとき，f を**恒等写像**（または**恒等関数**）という．

問 2.6. $f : \mathbb{R} \to \mathbb{R}$ を $f(x) = 1$ とする．このとき，関数 f は恒等写像か．

命題 2.2. A, B を集合，$f : A \to B$ を全単射とする．このとき，次のように定義された対応 g は B から A への写像である．$f(a) = b$ を満たす任意の $a \in A, b \in B$ に対して $g(b) = a$.

証明. 上のように定義された g が B から A への写像であることを示す．f が全単射であることから，任意の[*2] $b \in B$ に対して，$f(a) = b$ を満たす唯一の[*3] $a \in A$ が存在する．このことから，B の任意の要素が A のある一つの要素に対応していることが示される．これは g が B から A への写像であることを意味する． ■

定義 2.5

A, B を集合, $f : A \to B$ を全単射とする．このとき, 上の命題の写像 $g : B \to A$ を，f の**逆写像**（または**逆関数**）といい，f^{-1} と表す．

注 2.2. 全単射でない写像には逆写像は定義されない．

問 2.7. $f : \mathbb{R} \to \mathbb{R}$ を $f(x) = 2x - 1$ とする．このとき，$f^{-1}(x)$ を求めなさい．

事実 2.2. A, B を集合，$f : A \to B$ を全単射とする．このとき，$f^{-1} : B \to A$ は全単射である．

2.4　合成写像

定義 2.6

A, B, C を集合，f を A から B への写像，g を B から C への写像とする．このとき，$g \circ f$ を f と g の**合成写像**（または**合成関数**）といい，次のように定義す

[*2] f が全射であることから．
[*3] f が単射であることから．

る．任意の $a \in A$ について，

$$(g \circ f)(a) \stackrel{\text{def}}{=} g(f(a)).$$

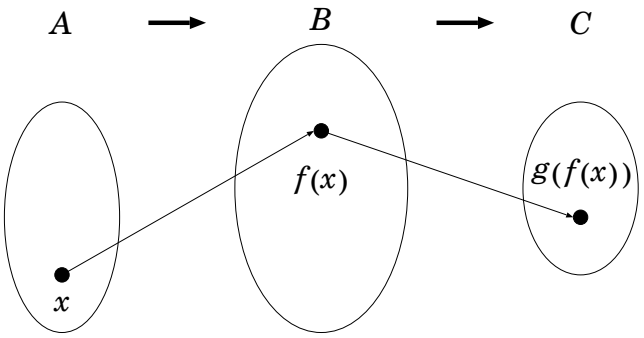

図 2.2　合成写像：$h = g \circ f$

問 2.8. $f(x) = x + 1$, $g(x) = x^2 + 2x - 3$ とする．このとき，合成写像 $g \circ f$ を求めなさい．

命題 2.3. A, B を集合，$f : A \to B$ を全単射とする．このとき，$f^{-1} \circ f$ 及び $f \circ f^{-1}$ は恒等写像である．

証明. $f^{-1} \circ f$ が恒等写像となることを示す．（$f \circ f^{-1}$ についても同様にして示される．）$a \in A$ を任意とする．$b = f(a)$ とすれば，逆写像の定義より $a = f^{-1}(b)$ となる．よって，

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

任意の $a \in A$ について $(f^{-1} \circ f)(a) = a$ であることから，$(f^{-1} \circ f)$ が恒等写像であることが示される． ■

命題 2.4. $f : X \to Y$, $g : Y \to Z$ を全単射とする．このとき，合成写像 $g \circ f : X \to Z$ は全単射である．

証明. $g \circ f : X \to Z$ が全射であり単射であることを示す．$z \in Z$ を任意とする．$g : Y \to Z$ が全射であることから，ある $y \in Y$ が存在して $g(y) = z$．同様にして，ある

$x \in X$ が存在して $f(x) = y$. よって，任意の $z \in Z$ について，ある $x \in X$ が存在して，

$$(g \circ f)(x) \;=\; g(f(x)) \;=\; g(y) \;=\; z.$$

これは，$g \circ f$ が全射であることを意味する．次に，$x, x' \in X$ を任意とする．（ただし，$x \neq x'$.）$f : X \to Y$ が単射であることから，ある $y, y' \in Y$ が存在して，$y \neq y'$ かつ $y = f(x)$, $y' = f(x')$. 同様にして，ある $z, z' \in Z$ が存在して，$z \neq z'$ かつ $z = g(y)$, $z' = g(y')$. よって，任意の x, x' について，（$x \neq x'$ なら）$(g \circ f)(x) \neq (g \circ f)(x')$. これは，$g \circ f$ が単射であることを意味する． ■

定理 2.5. $f : X \to Y$, $g : Y \to Z$ を全単射とする．（上の命題より合成写像 $g \circ f : X \to Z$ は全単射であり，それゆえ $g \circ f$ に逆写像が定義できる.）このとき，$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ である.

証明. 任意の $z \in Z$ について，$(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z)$ であることを示す．$z \in Z$ を任意とする．$g : Y \to Z$ が全単射であることから $y = g^{-1}(z)$ とする．（$z = g(y)$.）更に，$f : X \to Y$ が全単射であることから $x = f^{-1}(y)$ とする．（$y = f(x)$.）このとき，

$$(g \circ f)(x) \;=\; g(f(x)) \;=\; g(y) \;=\; z,$$

より $(g \circ f)^{-1}(z) = x$ となる．また，

$$(f^{-1} \circ g^{-1})(z) \;=\; f^{-1}(g^{-1}(z)) \;=\; f^{-1}(y) \;=\; x.$$

よって，任意の $z \in Z$ について，$(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z) = x$. ■

2.5　無限集合 *

定義 2.7

A, B を集合とする．（有限でも無限でもよい.）A から B への全単射が存在するとき，A と B の**濃度**は等しいという.

注 2.3. 実際，有限集合であれば，これは（集合の大きさに関しての）命題となる．（命題 2.1 参照.）

「濃度」とは，二つの無限集合の大きさを比較するために，有限集合の要素の個数という概念を拡張させたものである．以下では，集合 A から集合 B への全単射が存在することを $A \sim B$，存在しないことを $A \not\sim B$ と表す.

定義 2.8

A を集合とする．ある自然数 n が存在して，$A \sim \{1, \ldots, n\}$ であるとき，A を**有限集合**という．このとき，$|A| = n$ である．任意の自然数 n について，$A \not\sim \{1, \ldots, n\}$ であるとき，A を**無限集合**という．

命題 2.6. 自然数の集合を $\mathbb{N}$，正の偶数の集合を $\mathbb{E}^+$ とする．このとき，$\mathbb{E}^+ \sim \mathbb{N}$.

証明. 任意の $n \in \mathbb{N}$ について，$2n \in \mathbb{E}^+$ を割り当てる写像を考える． ■

命題 2.7. 自然数の集合を $\mathbb{N}$，正の有理数の集合を $\mathbb{Q}^+$ とする．このとき，$\mathbb{N} \sim \mathbb{Q}^+$.

証明. 二次元平面上の格子点（(x, y), $x, y \in \mathbb{N}$）を考える． ■

命題 2.8. 自然数の集合を $\mathbb{N}$，正の実数の集合を $\mathbb{R}^+$ とする．このとき，$\mathbb{N} \not\sim \mathbb{R}^+$.

証明. $\mathbb{N} \not\sim (0,1) \subseteq \mathbb{R}^+$ を示せば十分である．背理法により示す．$\mathbb{N} \sim (0,1)$ であるとする．つまり，全単射 $f : \mathbb{N} \to (0,1)$ が存在したとする．任意の $i \in \mathbb{N}$ について，$y_i = f(i)$ $(y_i \in (0,1))$ とする．更に，y_i の 10^{-i} の位の数字を $b_i \in \{0, 1, \ldots, 9\}$ とする．ここで，次のような実数 $r \in (0,1)$ を考える．任意の $i \in \mathbb{N}$ について，r の 10^{-i} の位 r_i を以下のように定義する．

$$r_i \overset{\text{def}}{=} \begin{cases} 6 & b_i \in \{0, 1, \ldots, 4\} \\ 1 & b_i \in \{5, 6, \ldots, 9\} \end{cases}$$

このとき，任意の $i \in \mathbb{N}$ について $r \neq f(i)$．これは，f が $\mathbb{N}$ から $(0,1)$ への全単射であることに反する．よって，矛盾が導かれ，$\mathbb{N} \not\sim (0,1)$ が示される． ■

この命題を示すのに使われた証明手法を**対角線論法**という．上の命題の証明を図示すると以下のようになる．

	0.	10^{-1}	10^{-2}	10^{-3}	$\cdots$	$\cdots$	10^{-i}	$\cdots$
1	0.	b_1	?	?	$\cdots$	$\cdots$	$\cdots$	?
2	0.	?	b_2	?	$\cdots$	$\cdots$	$\cdots$	?
3	0.	?	?	b_3	$\cdots$	$\cdots$	$\cdots$	?
$\vdots$	$\vdots$				$\ddots$		$\vdots$	
$\vdots$	$\vdots$					$\ddots$	$\vdots$	
i	0.	?	?	?	$\cdots$	$\cdots$	b_i	$\cdots$
$\vdots$	$\vdots$						$\vdots$	$\ddots$

章末問題

以下の問いに答えなさい.

1. 以下の表で定義された $f : \{0,1,2,3,4,5\} \to 2^{\{a,b,c\}}$ は，写像であるか．そうでない場合はその理由を述べなさい.

(a)

x	0	1	2	3	4	5
$f(x)$	$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$

(b)

x	0	1	2	3	4	5
$f(x)$	$\{a\}$	$\{a\}$		$\{a,b\}$	$\{a,c\}$	$\{b,c\}$

(c)

x	0	1	2	3	4	5
$f(x)$	$\{a\}$	$\{a\}$	$\{a\},\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$

2. $f_1, f_2 : \mathbb{R} \to \mathbb{R}$ を，それぞれ $f_1(x) = \sin x, f_2(x) = \cos x$，$f_3 : \mathbb{R} \setminus \{\pi/2 \pm k\pi : k \in \mathbb{N}_0\} \to \mathbb{R}$ を，$f_3(x) = \tan x$ とする．このとき，$f_1([0,\pi/2])$, $f_2([0,\pi/2])$, $f_3([0,\pi/2))$ をそれぞれ求めなさい.
3. 以下の写像 $f : \mathbb{R} \to \mathbb{R}$ は，全射，単射，全単射，またはそのいずれでもないかのどれか．また，全単射であるならば，その逆写像を求めなさい.
   (a) $f(x) = x + 1$
   (b) $f(x) = x^2 - x - 1$
   (c) $f(x) = x^3$
   (d) $f(x) = x^3 + 2x^2 + x + 1$
   (e) $f(x) = 2^x$
4. $f : \{0,1,...,5\} \to \{0,1,...,5\}$ を以下のような写像とする.

x	0	1	2	3	4	5
$f(x)$	0	0	1	2	3	4

   このとき，合成写像 $f \circ f$ を求めなさい.
5. $A = \{1,2,3\}$, $X = \{a,b,c\}$ とする．$f : A \to X$, $g : X \to A$ を以下のような写像とする.

x	1	2	3
$f(x)$	c	a	b

x	a	b	c
$g(x)$	3	1	2

このとき，(1) $g \circ f$ を求めその逆写像 $(g \circ f)^{-1} : A \to A$ を求めなさい．更に，(2) f^{-1} 及び g^{-1} を求め $f^{-1} \circ g^{-1} : A \to A$ を求めなさい．これを通じて，定理 2.5 を確認しなさい．

第 3 章

関係

3.1 関係とは

定義 3.1

A, B を集合とする．A と B の要素の（順序を考慮した）「対」の集合 $\{(a,b) : a \in A, b \in B\}$ を，A と B の**直積**といい，$A \times B$ と表す．一般に，$A_1, \ldots, A_n$ を集合として，$\{(a_1, \ldots, a_n) : a_1 \in A_1, \ldots, a_n \in A_n\}$ を $A_1, \ldots, A_n$ の直積といい，$A_1 \times \cdots \times A_n$ と表す．$A_1 = \cdots = A_n = A$ のとき，$A_1 \times \cdots \times A_n$ を A^n と表す．

例 3.1 (直積)**.** $A = \{0, 1\}$ とする．このとき，

$$\begin{aligned} A^2 &= \{(0,0), (0,1), (1,0), (1,1)\}, \\ A^3 &= \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}. \end{aligned}$$

問 3.1. $A = \{1, \ldots, 6\}$ をサイコロの出る目の集合としたとき，A^2 にはどのような解釈ができるか.

問 3.2. $\mathbb{R}^2$，$\mathbb{R}^3$ にはどのような解釈ができるか.

定義 3.2

A, B を集合とする．A と B の直積 $A \times B$ の部分集合 $R \subseteq A \times B$ を A と B の**二項関係**, または単に**関係**という．一般に, 集合 $A_1, \ldots, A_n$ の直積 $A_1 \times \cdots \times A_n$ の部分集合 $R \subseteq A_1 \times \cdots \times A_n$ を $A_1, \ldots, A_n$ の n **項関係**という．特に, $A_1 = \cdots = A_n = A$ であるとき，$R \subseteq A^n$ を A 上の n 項関係という．

例 3.2 (二項関係)**.** $R = \{(1,2)\} \subseteq \mathbb{N}^2$, $R = \{(1,2),(2,3),(3,1)\} \subseteq \mathbb{N}^2$ は $\mathbb{N}$ 上の，$R = \{(0,0),(-1,789),(123,10),(2,3),(5,7)\} \subseteq \mathbb{Z}^2$ は $\mathbb{Z}$ 上の，二項関係である[*1].

例 3.3 (二項関係)**.** $R_{=} = \{(a,b) : a = b\} \subseteq \mathbb{N}^2$，$R_{\leq} = \{(a,b) : a \leq b\} \subseteq \mathbb{N}^2$，は $\mathbb{N}$ 上の二項関係である[*2]．また，$R_{=} = \{(a,b) : a = b\} \subseteq \mathbb{R}^2$，$R_{\leq} = \{(a,b) : a \leq b\} \subseteq \mathbb{R}^2$，は $\mathbb{R}$ 上の二項関係である．

例 3.4 (二項関係)**.** k を任意の自然数とする．$R_k = \{(a,b) : k$ は $a - b$ を割り切る $\} \subseteq \mathbb{N}_0^2$ は $\mathbb{N}_0$ 上の二項関係である．

例 3.5 (二項関係)**.** A を集合とする．$R_A = A \times A$ は A 上の二項関係である．また，$R_{\text{size}} = \{(B,C) : |B| = |C|\} \subseteq (2^A)^2$ は 2^A 上の二項関係である．

問 3.3. $A = \{0,1\}$ とする．2^A 上の二項関係 $R_{\text{size}} = \{(B,C) : |B| = |C|\} \subseteq (2^A)^2$ を，外延的記法で示しなさい．

例 3.6 (二項関係)**.** $f : \mathbb{R} \to \mathbb{R}$ を関数とする．$R_f = \{(x,y) : y = f(x)\} \subseteq \mathbb{R}^2$，及び，$R_{f\_eq} = \{(x,x') : f(x) = f(x')\} \subseteq \mathbb{R}^2$ は，ともに $\mathbb{R}$ 上の二項関係である．

問 3.4. $A = \{a,b,c\}$ として，$f : A \to \{0,1\}$ を以下の表で定義される関数とする．

x	a	b	c
$f(x)$	0	1	0

A 上の二項関係 $R_{f\_eq} = \{(x,x') : f(x) = f(x')\} \subseteq A^2$ を，外延的記法で示しなさい．

3.2　同値関係

定義 3.3

A を集合，$R \subseteq A^2$ を関係とする．R が以下の 3 つを満たしているとき，R を A 上の**同値関係**という．

1. 反射律：任意の $a \in A$ について $(a,a) \in R$.
2. 対称律：任意の $(a,a') \in A^2$ について，$(a,a') \in R$ なら $(a',a) \in R$.

[*1] 部分集合であれば関係である！（それが意味のある関係であるかは別として.）

[*2] $R_{=} = \{(a,b) \in \mathbb{N}^2 : a = b\}$，$R_{\leq} = \{(a,b) \in \mathbb{N}^2 : a \leq b\}$ と表記しても同じことである．

3. 推移律：任意の $(a, a'), (a', a'') \in A^2$ について，$(a, a') \in R$ かつ $(a', a'') \in R$ なら $(a, a'') \in R$.

同値関係とは，二つの対象が「ある意味で」同じである（同一視できる）という関係を一般化した概念である．

例 3.7 (同値関係)**.** 関係 $R_= = \{(a, b) : a = b\} \subseteq \mathbb{N}^2$ は，$\mathbb{N}$ 上の同値関係である．また，関係 $R_= = \{(a, b) : a = b\} \subseteq \mathbb{R}^2$ は，$\mathbb{R}$ 上の同値関係である．

問 3.5. 関係 $R_\leq = \{(a, b) : a \leq b\} \subseteq \mathbb{R}^2$ は，$\mathbb{R}$ 上の同値関係か．

例 3.8 (同値関係)**.** k を任意の自然数とする．関係 $R_k = \{(a, b) : k$ は $a - b$ を割り切る $\} \subseteq \mathbb{N}_0^2$ は $\mathbb{N}_0$ 上の同値関係である．

問 3.6. 関係 $R_3 = \{(a, b) : 3$ は $a - b$ を割り切る $\} \subseteq \mathbb{N}_0^2$ が $\mathbb{N}_0$ 上の同値関係であることを示しなさい．

例 3.9 (同値関係)**.** A を集合とする．関係 $R_{\text{size}} = \{(B, C) : |B| = |C|\} \subseteq (2^A)^2$ は 2^A 上の同値関係である．

問 3.7. 関係 $R_{\text{size}} = \{(B, C) : |B| = |C|\} \subseteq (2^A)^2$ が 2^A 上の同値関係であることを示しなさい．

問 3.8. 関係 $R_A = A \times A$ は，A 上の同値関係か．

例 3.10 (同値関係)**.** $f : \mathbb{R} \to \mathbb{R}$ を関数とする．関係 $R_{f\_eq} = \{(x, x') : f(x) = f(x')\} \subseteq \mathbb{R}^2$ は $\mathbb{R}$ 上の同値関係である．

問 3.9. 関係 $R_{f\_eq} = \{(x, x') : f(x) = f(x')\} \subseteq \mathbb{R}^2$ が $\mathbb{R}$ 上の同値関係であることを示しなさい．

問 3.10. 関係 $R_f = \{(x, y) : y = f(x)\} \subseteq \mathbb{R}^2$ は，$\mathbb{R}$ 上の同値関係か.

3.3　同値類

定義 3.4

A を集合，$R \subseteq A^2$ を同値関係とする．このとき，任意の $a \in A$ について，$\{a' \in A : (a, a') \in R\}$ を a の**同値類**といい，$R[a]$ と表す.

a の同値類 $R[a]$ とは，a と「同値関係 R の意味で」同じものの集合のことである.

例 3.11 (同値類)**.** $R_= = \{(a, b) : a = b\}$ を $\mathbb{R}$ 上の同値関係とする．このとき，任意の $a \in \mathbb{R}$ について $R_=[a] = \{a\}$.

例 3.12 (同値類)**.** k を任意の自然数として，関係 $R_k = \{(a, b) : k$ は $a - b$ を割り切る $\}$ を $\mathbb{N}_0$ 上の同値関係とする．このとき，任意の $a \in \mathbb{N}_0$ について，

$$R_k[a] \;=\; \{b \in \mathbb{N}_0 : (a, b) \in R_k\} \;=\; \{b \in \mathbb{N}_0 : k \text{ は } a - b \text{ を割り切る }\}.$$

つまり，$R_k[a] = \{b \in \mathbb{N}_0 :$ $a \div k$ 及び $b \div k$ の余りが等しい $\}$.

問 3.11. 関係 $R_3 = \{(a, b) : 3$ は $a - b$ を割り切る $\}$ を $\mathbb{N}_0$ 上の同値関係とする．このとき，$R_3[0], R_3[1], R_3[2]$ を求めなさい．更に，$R_3[3], R_3[4], R_3[5], \ldots$ がどのような値になるかを確かめなさい.

例 3.13 (同値類)**.** A を集合とする．関係 $R_{\text{size}} = \{(B, C) : |B| = |C|\} \subseteq (2^A)^2$ を 2^A 上の同値関係とする．このとき，任意の $B \subseteq A$ について，

$$R_{\text{size}}[B] \;=\; \{C \in 2^A : (B, C) \in R_{\text{size}}\} \;=\; \{C \subseteq A : |C| = |B|\}.$$

例 3.14 (同値類)**.** $f : \mathbb{R} \to \mathbb{R}$ を関数とする．関係 $R_{f\_eq} = \{(x, x') : f(x) = f(x')\} \subseteq \mathbb{R}^2$ を $\mathbb{R}$ 上の同値関係とする．このとき，任意の $x \in \mathbb{R}$ について，

$$R_{f\_eq}[x] \;=\; \{x' \in \mathbb{R} : (x, x') \in R_{f\_eq}\} \;=\; \{x' \in \mathbb{R} : f(x') = f(x)\}.$$

事実 3.1. A を集合，$R \subseteq A^2$ を同値関係とする．このとき，任意の $a \in A$ について $a \in R[a]$.

定理 3.1. A を集合，$R \subseteq A^2$ を同値関係とする．任意の a, b について，$R[a] \cap R[b] \neq \emptyset$ ならば $R[a] = R[b]$.

証明. $R[a] = R[b]$ を示すためには，$R[a] \subseteq R[b]$ かつ $R[b] \subseteq R[a]$ を示せばよい．まず，$R[a] \subseteq R[b]$ を示す．（$R[b] \subseteq R[a]$ についても同様にして示される．）このためには，任意の $x \in R[a]$ について $x \in R[b]$ を示せばよい.

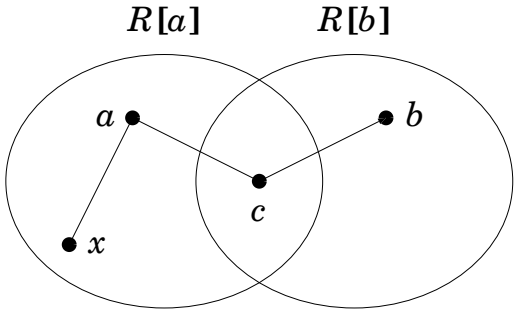

図 3.1　証明の概略図：要素 u, v が辺（線分）で結ばれているなら $(u, v) \in R$.

任意に $x \in R[a]$ をとる．（図 3.1 を参照.）$R[a]$ の定義より，$(a, x) \in R$ である．一方，定理の仮定より，$R[a] \cap R[b] \neq \emptyset$ であるから，ある $c \in A$ が存在して，$c \in R[a]$ かつ $c \in R[b]$ である．（図 3.1 を参照.）定義より，$(a, c), (b, c) \in R$ である．これより，$(b, a) \in R$.（反射律より $(c, a) \in R$，更に，$(b, c), (c, a) \in R$ に推移律を適用することから.）よって，$(b, a), (a, x) \in R$ より，$(b, x) \in R$.（推移律より.）これは，$x \in R[b]$ を意味する．よって，$R[a] \subseteq R[b]$ が示される．同様にして，$R[b] \subseteq R[a]$ も示される．よって，$R[a] = R[b]$. ■

系 3.2. A を集合，$R \subseteq A^2$ を同値関係とする．このとき，任意の $a \in A$ について，$b \in R[a]$ ならば $R[b] = R[a]$.

証明. 定理 3.1 を用いて，次のようにして示される．$b \in R[a]$ かつ $b \in R[b]$（事実 3.1）より，$R[a] \cap R[b] \neq \emptyset$. よって，定理 3.1 より $R[a] = R[b]$ が示される． ■

3.4　商集合 *

定義 3.5

A を集合，$R \subseteq A^2$ を同値関係とする．同値類の集合，つまり，$\{R[a] : a \in A\}$ を，R による A の**商集合**といい，A/R と表す．

例 3.15 (商集合)．$R_= = \{(a,b) : a = b\} \subseteq \mathbb{R}^2$ とする．このとき，$\mathbb{R}/R_= = \{\{a\} : a \in \mathbb{R}\}$.

例 3.16 (商集合)．k を任意の自然数として，$R_k = \{(a,b) : k$ は $a-b$ を割り切る $\}$ を $\mathbb{N}_0$ 上の同値関係とする．このとき，任意の $i \in \{0,1,\ldots,k-1\}$ について $R_k[i] = \{a \in \mathbb{N}_0 : a$ を k で割った余りが $i\}$ であり，

$$\mathbb{N}_0/R_k \;=\; \{R_k[i] : i \in \{0,1,\ldots,k-1\}\}.$$

問 3.12. 関係 $R_3 = \{(a,b) :$ 3 は $a-b$ を割り切る $\}$ を $\mathbb{N}_0$ 上の同値関係とする．$\mathbb{N}_0/R_3$ を求めなさい．

例 3.17 (商集合)．A を集合とする．関係 $R_{\text{size}} = \{(B,C) : |B| = |C|\} \subseteq (2^A)^2$ を 2^A 上の同値関係とする．このとき，$R_{\text{size}}(i) = \{B \subseteq A : |B| = i\}$ とすれば，

$$2^A/R_{\text{size}} \;=\; \{R_{\text{size}}[B] : B \subseteq A\} \;=\; \{R_{\text{size}}(i) : 0 \le i \le |A|\}.$$

例 3.18 (商集合)．$f : \mathbb{R} \to \mathbb{R}$ を関数とする．関係 $R_{f\_eq} = \{(x,x') : f(x) = f(x')\} \subseteq \mathbb{R}^2$ を $\mathbb{R}$ 上の同値関係とする．このとき，$R_{f\_eq}(y) = \{x \in \mathbb{R} : y = f(x)\}$ とすれば，

$$\mathbb{R}/R_{f\_eq} \;=\; \{R_{f\_eq}[x] : x \in \mathbb{R}\} \;=\; \{R_{f\_eq}(y) : y \in \mathbb{R}\}.$$

定理 3.3 (商集合による分割)．A を集合，$R \subseteq A^2$ を同値関係とする．このとき，A/R は A の分割である．

証明. 商集合の定義（$A/R = \{R[a] : a \in A\}$）と，分割の定義（定義 1.13）より，以下の二つを示せばよい．（以下の二つ目については集合の要素は重複しないことから．）

1. $A = \bigcup_{a \in A} R[a]$
2. すべての $a, a' \in A$ について $R[a] \neq R[a']$ ならば $R[a] \cap R[a'] = \emptyset$

まず，一つ目について，$A \subseteq \bigcup_{a\in A} R[a]$ かつ $A \supseteq \bigcup_{a\in A} R[a]$ を示せばよい．前者は，任意の $a \in A$ について $a \in R[a]$ であることから明らか．後者は，任意の $a \in A$ について $R[a] \subseteq A$ であることから明らか．

次に，二つ目について，定理 3.1 より[*3]，$R[a] \neq R[a']$ ならば $R[a] \cap R[a'] = \emptyset$．以上より，$A/R$ は A の分割であることが示される． ■

例 3.19 (商集合による分割)．$R_= = \{(a, b) : a = b\} \subseteq \mathbb{R}^2$ とする．このとき，$\mathbb{R}/R_=$ は $\mathbb{R}$ の分割である．

例 3.20 (商集合による分割)．k を任意の自然数として，関係 $R_k = \{(a, b) : k \text{ は } a - b \text{ を割り切る }\}$ を $\mathbb{N}_0$ 上の同値関係とする．このとき，任意の $i \in \{0, 1, \ldots, k-1\}$ について $R_k[i] = \{a \in \mathbb{N}_0 : a \text{ を } k \text{ で割った余りが } i\}$ であり，

$$\mathbb{N}_0/R_k \;=\; \{R_k[i] : i \in \{0, 1, \ldots, k-1\}\}$$

は $\mathbb{N}_0$ の分割である．

問 3.13. 関係 $R_3 = \{(a, b) : 3 \text{ は } a - b \text{ を割り切る }\}$ を $\mathbb{N}_0$ 上の同値関係とする．このとき，$\mathbb{N}_0/R_3$ が $\mathbb{N}_0$ の分割であることを確かめなさい．

3.5 順序関係 *

定義 3.6

A を集合，$R \subseteq A^2$ を関係とする．R が以下の 3 つを満たしているとき，R を A 上の**半順序関係**といい，A を R における**半順序集合**という．

1. 反射律：任意の $a \in A$ について $(a, a) \in R$.
2. 反対称律：任意の $(a, a') \in A^2$ について，$(a, a') \in R$ かつ $(a', a) \in R$ なら $a = a'$.
3. 推移律：任意の $(a, a'), (a', a'') \in A^2$ について，$(a, a') \in R$ かつ $(a', a'') \in R$ なら $(a, a'') \in R$.

半順序関係とは，二つの対象が「ある意味で」順序付けられる，という関係を一般化した概念である．

例 3.21 (半順序関係)．関係 $R_\leq = \{(a, b) : a \leq b\} \subseteq \mathbb{R}^2$ は，$\mathbb{R}$ 上の半順序関係である．

[*3] 実際には，その定理の対偶（第 5.3 節を参照）をとることにより．

問 3.14. 関係 $R_{=} = \{(a, b) : a = b\} \subseteq \mathbb{R}^2$ は，$\mathbb{R}$ 上の半順序関係か．

問 3.15. 関係 $R_{<} = \{(a, b) : a < b\} \subseteq \mathbb{R}^2$ は，$\mathbb{R}$ 上の半順序関係か．

例 3.22 (半順序関係)**.** S を集合とする．関係 $R = \{(A, B) : A \subseteq B\} \subseteq (2^S)^2$ は，2^S 上の半順序関係である．

例 3.23 (半順序関係)**.** 関係 $R = \{(a, b) : a$ は b を割り切る $\} \subseteq \mathbb{N}^2$ は，$\mathbb{N}$ 上の半順序関係である．

問 3.16. 同値関係であれば半順序関係となるか．そうでなければ反例をあげなさい．また，半順序関係であれば同値関係となるか．そうでなければ反例をあげなさい．

以降では，半順序関係を $\leq_*$ で表し，$(a, a') \in \leq_*$ であるとき，$a \leq_* a'$ と表す．

定義 3.7

A を集合，$\leq_*$ を A 上の半順序関係とする．$a, a' \in A$ について，$a \leq_* a'$ または $a' \leq_* a$ が成り立つとき，a と a' は**比較可能**であるという．任意の $a, a' \in A$ について a と a' が比較可能であるとき，$\leq_*$ を A 上の**全順序関係**といい，A を $\leq_*$ における**全順序集合**という．

例 3.24 (全順序関係)**.** $\leq_* = \{(a, b) : a \leq b\} \subseteq \mathbb{R}^2$ とする．このとき，$\mathbb{R}$ は $\leq_*$ における全順序集合である．

問 3.17. S を集合として，$\leq_* = \{(A, B) : A \subseteq B\} \subseteq (2^S)^2$ とする．このとき，2^S は $\leq_*$ における全順序集合か．

問 3.18. $\leq_* = \{(a, b) : a$ は b を割り切る $\} \subseteq \mathbb{N}^2$ とする．このとき，$\mathbb{N}$ は $\leq_*$ における全順序集合か．

定義 3.8

A を集合，$\leq_*$ を A 上の半順序関係とする．このとき，

- $a \in A$ が**最大**であるとは，任意の $a' \in A$ について $a' \leq_* a$ を満たすことである．
- $a \in A$ が**最小**であるとは，任意の $a' \in A$ について $a \leq_* a'$ を満たすことである．
- $a \in A$ が**極大**であるとは，任意の $a' \in A$ について，a と a' が比較可能であるなら $a' \leq_* a$ を満たすことである．
- $a \in A$ が**極小**であるとは，任意の $a' \in A$ について，a と a' が比較可能であるなら $a \leq_* a'$ を満たすことである．

定義より，最大・最小は，存在するならばそれぞれ唯一である．一方，極大・極小は，複数存在することもある．

例 3.25 (最大最小・極大極小)**.** $S = \{a, b, c\}$ とする．$\leq_* = \{(A, B) : A \subseteq B\} \subseteq (2^S)^2$ とする．このとき，最大：$\{a, b, c\}$，最小：$\emptyset$，極大：$\{a, b, c\}$，極小：$\emptyset$ である．（極大・極小はそれぞれの最大・最小に等しい．図 3.2 を参照.）

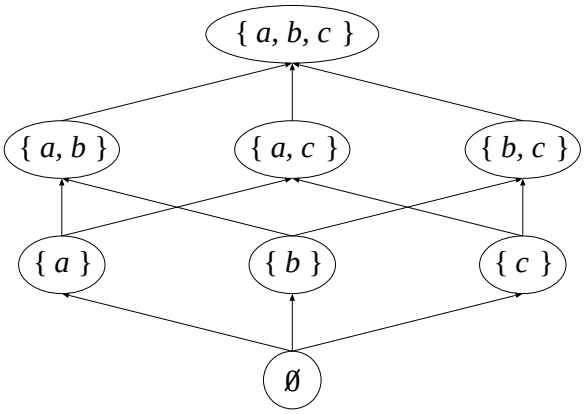

図 3.2 $\{a, b, c\}$ のべき集合上の半順序関係（包含関係）を示したハッセ図

問 3.19. $A = \{i \in \mathbb{N} : 1 \leq i \leq 10\}$ とする．$\leq_* = \{(a, b) : a \leq b\} \subseteq A^2$ とする．このとき，最大，最小，極大，極小の要素を求めなさい．

問 3.20. $A = \{i \in \mathbb{N} : 1 \leq i \leq 12\}$ とする．$\leq_* = \{(a, b) : a$ は b を割り切る $\} \subseteq A^2$ とする．このとき，最大，最小，極大，極小の要素を求めなさい．

章末問題

以下の問いに答えなさい.

1. A, B, C を集合とする．$A \times B \times C$ を内包的記法で表しなさい.
2. $A = \{0, 1\}$, $B = \{a, b, c\}$ とする．$A \times B$ を外延的記法で表しなさい.
3. $A = \{1, 2, \ldots, k\}$ とする．このとき，$|A^n|$ を k, n で表しなさい.
4. $A = \{a, b, c\}$ とする．A 上の二項関係 $R_1, R_2, R_3 \subseteq A^2$ を以下のように定義する.

$$\begin{aligned} R_1 &= \{(a,a),(a,b),(b,a),(b,b)\}, \\ R_2 &= \{(a,a),(a,b),(b,b),(c,c)\}, \\ R_3 &= \{(a,a),(a,b),(b,a),(b,b),(b,c),(c,b),(c,c)\}. \end{aligned}$$

   R_1, R_2, R_3 はそれぞれ同値関係であるか．もしそうでないなら理由を述べなさい.
5. $A = \mathbb{N}^2$ とする．A 上の二項関係 $R \subseteq A^2$ を以下のように定義する.

$$R = \{((a,b),(x,y)) : ay = bx\}.$$

   (a) R が同値関係であることを示しなさい[*4].
   (b) 同値類 $R[(1,1)]$ を求めなさい.
   (c) 商集合 A/R を求めなさい.
6. Ω を英単語すべての集合とする．(アルファベット一文字も一つの英単語とする.)
   Ω 上の二項関係 $R \subseteq \Omega^2$ を以下のように定義する.

$$R = \{(\alpha, \beta) : \alpha \text{ と } \beta \text{ は頭文字が同じ }\}.$$

   (a) R が同値関係であることを示しなさい.
   (b) 同値類 $R[\mathrm{apple}]$ を求めなさい.
   (c) $\Sigma = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \ldots, \mathrm{x}, \mathrm{y}, \mathrm{z}\}$ をアルファベットの集合として，商集合 Ω/R を求めなさい.
7. A を集合，$R \subseteq A^2$ を同値関係とする．このとき，以下を証明しなさい.
   (a) 任意の $a \in A$ について $b \in R[a]$ ならば $a \in R[b]$.
   (b) 任意の $a \in A$ について $b, c \in R[a]$ ならば $(b, c) \in R$.

[*4] $A = \mathbb{N}_0^2$（0 を入れる）とすれば，R は同値関係でなくなる.（なぜ？）

第 4 章

論理

4.1　命題とは

（おおざっぱに言って,）ある事柄を述べたものを**言明**といい，それが（万人にとって）正しければ**真**（**true**）であるといい，そうでなければ**偽**（**false**）であるという．

定義 4.1

「真」か「偽」のどちらか一方に一意に定められる言明を**命題**という．

例 4.1 (命題)**.** 以下はすべて命題である．

1. 1 たす 1 は 2 である．（真である．）
2. 1 たす 1 は 3 である．（偽である．）
3. A を集合，$R \subseteq A^2$ を同値関係とした場合，A/R は A の分割である．（真である．）

一方，次のようなものは命題で**ない**．

1. 離散数学は難しい．
2. $x + y = 1$ は成り立つ．

問 4.1. 以下のうち命題であるものどれか．（ただし，いずれも $a, b \in \mathbb{R}$.）

1. 一次関数 $y = x + b$ の（x-y 座標における）直線は，点 $(x, y) = (1, b-1)$ を通る．
2. 関数 x^a を x について微分した式は ax^{a-1} である．
3. x についての二次方程式 $x^2 + ax + b = 0$ は実数解をもつ．

4.2　命題論理

真を **1**，偽を **0** と表す．0 または 1 を値にとる変数を**論理変数**という[*1]．論理変数の演算には次のようなものがある．

定義 4.2

x, y を論理変数とする．$x \vee y$ を x と y の**論理和**といい，「x または y」を意味する．$x \wedge y$ を x と y の**論理積**といい，「x かつ y」を意味する．$\bar{x}$ を x の**否定**といい，「x でない」を意味する．これらを**真理値表**で表すと以下のようになる．

x	y	$x \vee y$	$x \wedge y$	$\bar{x}$	$\bar{y}$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	1
1	1	1	1	0	0

注 4.1. 論理和について，x が 1 であれば y の値によらず $x \vee y$ は真となる．論理積について，x が 0 であれば y の値によらず $x \wedge y$ は偽となる．

問 4.2. x, y, z を論理変数とする．論理和 $x \vee y \vee z$，論理積 $x \wedge y \wedge z$ の真理値表をそれぞれ示しなさい．

事実 4.1. 一般に，k 変数 $x_1, x_2, \ldots, x_k$ 上の論理和・論理積について，

- $x_1 \vee x_2 \vee \cdots \vee x_k$：$x_1 = x_2 = \cdots = x_k = 0$ のときかつそのときに限り偽．逆に，一つでも 1 の変数があれば（他の変数の 0/1 にかかわらず）真．
- $x_1 \wedge x_2 \wedge \cdots \wedge x_k$：$x_1 = x_2 = \cdots = x_k = 1$ のときかつそのときに限り真．逆に，一つでも 0 の変数があれば（他の変数の 0/1 にかかわらず）偽．

定義 4.3

論理変数，$\vee$, $\wedge$, 及び否定で表される式を，**命題論理による論理式**または単に**論理式**という．厳密には，以下のように帰納的に定義される．

[*1] ここでは，次のようにして，論理変数は命題を表す変数とみなす：x を論理変数とする．$x = 1$ は「命題 x が真である」ことを，$x = 0$ は「命題 x が偽である」ことを意味する．

1. 論理変数自体は論理式である．
2. x, y が論理式である場合，$x \vee y$, $x \wedge y$, $\bar{x}$, $\bar{y}$ は論理式である．

論理式 φ が論理変数 $x_1, \ldots, x_n$ からなるとき，φ を $x_1, \ldots, x_n$ **上の論理式**という．

例 4.2 (論理式)**.** 以下のものはすべて論理式である．

1. x.
2. $x \vee \bar{y}$.
3. $((x_1 \vee x_2) \wedge (\overline{x_1 \vee \bar{x}_3})) \vee (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3)$.

問 4.3. 以下の論理式の真理値表をそれぞれ示しなさい．

- $x \vee \bar{y}$
- $x \vee (y \wedge z)$

注 4.2. 論理積の記号 $\wedge$ は省略されることがある．例えば，$x \vee (y \wedge z)$ は $x \vee (yz)$ と表記される．また，演算記号の結合の強さによってカッコは省略されることがある．例えば，結合は $\vee$ より $\wedge$ の方が強いことから，$x \vee (yz)$ は $x \vee yz$ と表記される．

定理 4.1 (分配則)**.** x, y, z を論理変数とする．このとき，

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \end{aligned}$$

証明. 真理値表より明らか． ■

4.3　ド・モルガンの法則（命題論理）

定理 4.2 (ド・モルガンの法則)**.** x, y を論理変数とする．このとき，

$$\begin{aligned} \overline{x \vee y} &= \bar{x} \wedge \bar{y} \\ \overline{x \wedge y} &= \bar{x} \vee \bar{y} \end{aligned}$$

証明. 真理値表より明らか. ■

定理 4.3 (ド・モルガンの法則（一般形）). $x_1, \ldots, x_k$ を論理変数とする．このとき,

$$\begin{aligned} \overline{x_1 \vee \cdots \vee x_k} &= \bar{x}_1 \wedge \cdots \wedge \bar{x}_k \\ \overline{x_1 \wedge \cdots \wedge x_k} &= \bar{x}_1 \vee \cdots \vee \bar{x}_k \end{aligned}$$

証明. 数学的帰納法より示す.（定理 1.6 の証明を参照.） ■

定義 4.4

任意の自然数 $k \in \mathbb{N}$ に対して，$A = \{1, 2, \ldots, k\}$ とする．任意の $i \in A$ について，x_i を論理変数とする．このとき,

$$\bigvee_{i \in A} x_i \stackrel{\text{def}}{=} x_1 \vee x_2 \vee \cdots \vee x_k$$

$$\bigwedge_{i \in A} x_i \stackrel{\text{def}}{=} x_1 \wedge x_2 \wedge \cdots \wedge x_k$$

この表記に従えば，ド・モルガンの法則（一般形）は次のように表される．$A = \{1, 2, \ldots, k\}$ として,

$$\begin{aligned} \overline{\bigvee_{i \in A} x_i} &= \bigwedge_{i \in A} \bar{x}_i \\ \overline{\bigwedge_{i \in A} x_i} &= \bigvee_{i \in A} \bar{x}_i \end{aligned}$$

問 4.4. ド・モルガンの法則を用いて，以下の論理式を否定記号が複数の変数にまたがらない形にしなさい.

- $\overline{x \vee yz}$
- $\overline{(x \vee y)(x \vee z)}$

4.4　論理関数

定義 4.5

φ を論理変数 $x_1, \ldots, x_n$ 上の論理式とする．任意の $(a_1, \ldots, a_n) \in \{0,1\}^n$ について，$(x_1, \ldots, x_n) = (a_1, \ldots, a_n)$ と代入することを（$x_1, \ldots, x_n$ への）**真理値割り当て**または単に**割り当て**という．このとき，φ の真理値を $\varphi(a_1, \ldots, a_n)$ と表記する．

例 4.3 (割り当て)**.** $\varphi = x \vee yz$ とする．このとき，

1. $(x, y, z) = (0, 1, 0)$ の割り当てに対して $\varphi(0, 1, 0) = 0$.
2. $(x, y, z) = (1, 0, 0)$ の割り当てに対して $\varphi(1, 0, 0) = 1$.

事実 4.2. 真理値表は，真理値割り当てを表にしたものである．

命題 4.4. φ を論理変数 $x_1, \ldots, x_n$ 上の論理式とする．このとき，φ は $\{0,1\}^n$ から $\{0,1\}$ への（$x_1, \ldots, x_n$ 上の）関数となる．

証明. 命題論理による論理式の定義より，変数 $x_1, \ldots, x_n$ への任意の割り当てについて，論理式 φ の値（0 または 1 の）が一意に定められることから示される．（関数の定義を参照.）　■

定義 4.6

$\{0,1\}^n$ から $\{0,1\}$ への関数を**論理関数**という．

以降では，論理変数 $x_1, \ldots, x_n$ 上の論理式 φ は，$x_1, \ldots, x_n$ 上の論理関数として扱い，$\varphi(x_1, \ldots, x_n)$ と表記する．

定義 4.7

φ, φ' を論理変数 $x_1, \ldots, x_n$ 上の論理関数とする．任意の $a \in \{0,1\}^n$ について $\varphi(a) = \varphi'(a)$ であるとき，φ と φ' は**同値**であるといい，$\varphi \equiv \varphi'$ と表す．（単に，$\varphi = \varphi'$ と表すこともある.）

定義 4.8

φ を論理変数 $x_1, \ldots, x_n$ 上の論理関数とする．任意の $a \in \{0,1\}^n$ について $\varphi(a) = 1$ であるとき，φ は**恒真**であるといい，$\varphi \equiv 1$ と表す．（単に，$\varphi = 1$ と表すこともある．）

また，任意の $a \in \{0,1\}^n$ について $\varphi(a) = 0$ であるとき，φ は**矛盾**であるといい，$\varphi \equiv 0$ と表す．（単に，$\varphi = 0$ と表すこともある．）

例 4.4 (恒真，矛盾)**.** $x \vee \bar{x}$ は恒真であり，$x \wedge \bar{x}$ は矛盾である．（$\overline{x \vee \bar{x}} \equiv x \wedge \bar{x}$.）また，$\bar{y} \vee \bar{z} \vee yz$ は恒真であり，$yz(\bar{y} \vee \bar{z})$ は矛盾である．（$\overline{\bar{y} \vee \bar{z} \vee yz} \equiv yz(\bar{y} \vee \bar{z})$.）

問 4.5. 以下の論理式が恒真であることを示しなさい．

- $\bar{y} \vee \bar{z} \vee yz$
- $\overline{x \vee yz} \vee (x \vee y)(x \vee z)$

4.5　標準形論理式

定義 4.9

ℓ_i^j を論理変数またはその否定とする．以下のような形式の論理式を**和積標準形**（CNF）という．

$$(\ell_1^1 \vee \ell_2^1 \vee \ell_3^1 \vee \cdots) \wedge (\ell_1^2 \vee \ell_2^2 \vee \ell_3^2 \vee \cdots) \wedge (\ell_1^3 \vee \ell_2^3 \vee \ell_3^3 \vee \cdots) \wedge \cdots .$$

また，以下のような形式の論理式を**積和標準形**（DNF）という．

$$(\ell_1^1 \wedge \ell_2^1 \wedge \ell_3^1 \wedge \cdots) \vee (\ell_1^2 \wedge \ell_2^2 \wedge \ell_3^2 \wedge \cdots) \vee (\ell_1^3 \wedge \ell_2^3 \wedge \ell_3^3 \wedge \cdots) \vee \cdots .$$

例 4.5 (CNF, DNF)**.** 以下は，論理変数 x, y, z 上の CNF, DNF 論理式である．

$$\begin{array}{ll} \text{CNF} & : \quad x(\bar{x} \vee y)(\bar{x} \vee z)(x \vee \bar{y} \vee z)(x \vee y \vee \bar{z})(\bar{x} \vee \bar{y} \vee \bar{z}). \\ \text{DNF} & : \quad xy \vee xz \vee \bar{x}yz \vee x\bar{y}\bar{z} \vee \bar{x}\bar{y}\bar{z}. \end{array}$$

命題 4.5. 任意の論理式は，和積標準形（ＣＮＦ）及び積和標準形（ＤＮＦ）論理式で表される．

証明. 命題 4.4 より，任意の論理式はある論理関数である．任意の論理関数は和積標準形

及び積和標準形で表される．（詳細は略．問 4.6 を参照.）　■

問 4.6. 以下の表で表された論理関数 $f : \{0,1\}^3 \to \{0,1\}$ を，和積標準形（ＣＮＦ）及び積和標準形（ＤＮＦ）で表しなさい.

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

4.6　含意，同値

定義 4.10

x, y を論理変数（論理関数）とする．$x \oplus y$ を x と y の**排他的論理和**といい，「x または y のどちらか一方（のみ）」を意味する．$x \Rightarrow y$ を**含意**といい，「x ならば y」を意味する．$x \Leftrightarrow y$ を**同値**といい，「$x \Rightarrow y$ かつ $y \Rightarrow x$」を意味する．これらを真理値表で表すと以下のようになる.

x	y	$x \oplus y$	$x \Rightarrow y$	$x \Leftrightarrow y$
0	0	0	1	1
0	1	1	1	0
1	0	1	0	0
1	1	0	1	1

命題 4.6. x, y を論理変数（論理関数）とする．このとき，

$$x \oplus y \ \equiv \ (x \vee y) \wedge (\bar{x} \vee \bar{y}).$$

証明. 真理値表より明らか. ■

問 4.7. $x \oplus y \oplus z$ の真理値表を示しなさい.

事実 4.3. $x_1, x_2 \ldots, x_n$ を論理変数とする．このとき，$x_1 \oplus x_2 \oplus \cdots \oplus x_n$ は，値が 1 である x_i の個数の偶奇を示している．（偶数であれば 0，奇数であれば 1.）

命題 4.7. x, y を論理変数（論理関数）とする．このとき，

$$x \Rightarrow y \ \equiv \ \bar{x} \vee y.$$

証明. 真理値表より明らか. ■

4.7　述語論理

定義 4.11

A を集合とする．A から $\{0,1\}$ への関数を**述語**という.

例 4.6 (述語)**.** 以下のような関数 φ はすべて述語である.

1. 任意の論理関数 $\varphi : \{0,1\}^n \to \{0,1\}$.
2. 以下のような関数 $\varphi : \mathbb{N} \to \{0,1\}$

$$\varphi(x) \ = \ \begin{cases} 1 & : \ x \text{ が素数} \\ 0 & : \ \text{それ以外} \end{cases}$$

3. A を世界の都市の集合として，以下のような関数 $\varphi : A \to \{0,1\}$

$$\varphi(a) \ = \ \begin{cases} 1 & : \ a \text{ が首都} \\ 0 & : \ \text{それ以外} \end{cases}$$

定義 4.12

A を集合，$\varphi : A \to \{0,1\}$ を述語とする．$A' \subseteq A$ とする．すべての $x \in A'$ について $\varphi(x) = 1$ であることを，$\forall x \in A'[\varphi(x) = 1]$ （または，単に $\forall x \in A'[\varphi(x)]$）と表す．このような命題を**全称命題**といい，$\forall$ を**全称記号**という.

ある $x \in A'$ が存在して $\varphi(x) = 1$ であることを，$\exists x \in A'[\varphi(x) = 1]$ （または，単に $\exists x \in A'[\varphi(x)]$）と表す．このような命題を**存在命題**といい，$\exists$ を**存在記号**と

いう．

$\forall, \exists$ を**量化子**または**限定子**という．

注 4.3. 全称命題，存在命題において，（文脈から）A' が明らかなとき（例えば，$\{0,1\}$ や $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ など）は省略される．

定義 4.13

論理変数，述語，$\wedge$, $\vee$, 否定，及び $\forall, \exists$ で表される式を，**述語論理による論理式**または単に**論理式**という．（厳密には帰納的な形式で定義される．）

例 4.7 (述語論理による論理式)**.** A を集合とする．以下のものはすべて述語論理による論理式である．

1. 命題論理による論理式．
2. $(\forall x \in A[\varphi(x) = 1]) \vee (y \wedge z)$．（$\varphi : A \to \{0,1\}$．）
3. $\forall x_1 \in A, \exists x_2 \in A, \forall x_3 \in A[\varphi(x_1, x_2, x_3, y) = 1]$．（$\varphi : A^4 \to \{0,1\}$．）

注 4.4. 述語論理による論理式では，$\forall, \exists$ の量化子（限定子）が使われる．（命題論理による論理式には量化子が出現しない．）

例 4.8 (論理式)**.** 以下のそれぞれの命題を論理式で記述すると，次のようになる．

1. すべての自然数は整数である．
   $\forall x \in \mathbb{N}[x \in \mathbb{Z}]$.
2. すべての実数 x に対して，$x \geq 0$ ならば $x^2 \leq x^3$ である．
   $\forall x \in \mathbb{R}[x \geq 0 \Rightarrow x^2 \leq x^3]$.
3. ある実数 c が存在して，すべての実数 x に対して，$x \geq c$ ならば $x^2 \leq x^3$ である．
   $\exists c \in \mathbb{R}, \forall x \in \mathbb{R}[x \geq c \Rightarrow x^2 \leq x^3]$.

問 4.8. 以下の命題を論理式で表しなさい．また，その真偽，更に真偽の理由を述べなさい．

1. すべての実数 x に対して，ある実数 y が存在して，$x \geq 0$ ならば $y^2 < x$ を満たす．
2. ある実数 a が存在して，すべての実数 b に対して，2次方程式 $x^2 + ax + b = 0$ が実数解をもつ．

3. ある実数 b が存在して，すべての実数 a に対して，2 次方程式 $x^2+ax+b=0$ が実数解をもつ．
4. すべての実数 x に対して，ある実数 a が存在して，$x \in \{y \in \mathbb{R} : |y| < a\}$ を満たす．
5. すべての実数 a に対して，ある実数 x が存在して，$x \in \{y \in \mathbb{R} : |y| < a\}$ を満たす．

問 4.9. 以下の式は（一般的に）成り立つか．つまり，任意の述語 φ について以下が成り立つか．

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}[\varphi(x,y)=1] \ \equiv \ \forall y \in \mathbb{R}, \exists x \in \mathbb{R}[\varphi(x,y)=1].$$

そうでなければ，成り立つ例と成り立たない例をあげなさい．

注 4.5. 上の問が示すように，一般には，量化子を記述する順序を変えると異なった論理式になる．

4.8　ド・モルガンの法則（述語論理）

定理 4.8 (ド・モルガンの法則)**.** φ を任意の述語とする．このとき，

$$\begin{aligned} \overline{\forall x[\varphi(x)]} &\equiv \exists x[\overline{\varphi(x)}], \\ \overline{\exists x[\varphi(x)]} &\equiv \forall x[\overline{\varphi(x)}]. \end{aligned}$$

証明. 定義より明らか． ■

定理 4.9 (ド・モルガンの法則（一般形）)**.** φ を任意の述語とする．このとき，

$$\begin{aligned} & \overline{\forall x_1, \exists x_2, \forall x_3, \ldots, Q x_k[\varphi(x_1, x_2, x_3 \ldots, x_k)]} \\ \equiv \ & \exists x_1, \forall x_2, \exists x_3, \ldots, Q' x_k[\overline{\varphi(x_1, x_2, x_3 \ldots, x_k)}], \end{aligned}$$

ただし，$Q = \forall$ のとき $Q' = \exists$，$Q = \exists$ のとき $Q' = \forall$ である．また，

$$\begin{aligned} & \overline{\exists x_1, \forall x_2, \exists x_3, \ldots, Q x_k[\varphi(x_1, x_2, x_3 \ldots, x_k)]} \\ \equiv \ & \forall x_1, \exists x_2, \forall x_3, \ldots, Q' x_k[\overline{\varphi(x_1, x_2, x_3 \ldots, x_k)}], \end{aligned}$$

ただし，$Q = \forall$ のとき $Q' = \exists$，$Q = \exists$ のとき $Q' = \forall$ である．

証明. 数学的帰納法により示す．（定理 1.6 の証明を参照．） ■

4.9　論理と集合

命題 4.10 (論理と集合)**.** A を集合とする．φ, φ' を A 上の述語とする．このとき，以下の二つが成り立つ．

1.（論理和）：
$$\begin{aligned} & \{a \in A : (\varphi \vee \varphi')(a) = 1\} \\ = \ & \{a \in A : \varphi(a) = 1\} \cup \{a \in A : \varphi'(a) = 1\} \end{aligned}$$

2.（論理積）：
$$\begin{aligned} & \{a \in A : (\varphi \wedge \varphi')(a) = 1\} \\ = \ & \{a \in A : \varphi(a) = 1\} \cap \{a \in A : \varphi'(a) = 1\} \end{aligned}$$

証明. ベン図より明らか. ■

例 4.9. φ, φ' を $\mathbb{N}_0$ 上の以下の述語とする．

$$\begin{aligned} \varphi(x) &= \begin{cases} 1 & : \ x \text{ が } 2 \text{ の倍数} \\ 0 & : \ \text{それ以外} \end{cases} \\ \varphi'(x) &= \begin{cases} 1 & : \ x \text{ が } 3 \text{ の倍数} \\ 0 & : \ \text{それ以外} \end{cases} \end{aligned}$$

このとき，$\varphi \vee \varphi', \varphi \wedge \varphi'$ は以下の述語となる．

$$\begin{aligned} (\varphi \vee \varphi')(x) &= \begin{cases} 1 & : \ x \text{ が } 2 \text{ の倍数または } 3 \text{ の倍数} \\ 0 & : \ \text{それ以外} \end{cases} \\ (\varphi \wedge \varphi')(x) &= \begin{cases} 1 & : \ x \text{ が } 2 \text{ の倍数かつ } 3 \text{ の倍数} \\ 0 & : \ \text{それ以外} \end{cases} \end{aligned}$$

これより，上の命題の等式が成り立つことが分かる．

命題 4.11 (論理と集合)**.** A を集合とする．φ, φ' を A 上の述語とする．集合 $A_\varphi, A_{\varphi'}$ を以下のように定義する．

$$\begin{aligned} A_\varphi &\overset{\text{def}}{=} \{a \in A : \varphi(a) = 1\}, \\ A_{\varphi'} &\overset{\text{def}}{=} \{a \in A : \varphi'(a) = 1\}. \end{aligned}$$

このとき，以下が成り立つ．

$$\varphi \Rightarrow \varphi' \ \Leftrightarrow \ A_\varphi \subseteq A_{\varphi'}.$$

証明. ベン図より明らか． ■

例 4.10. φ, φ' を $\mathbb{N}_0$ 上の以下の述語とする．

$$\begin{aligned} \varphi(x) &= \begin{cases} 1 & : \ x \text{ が } 4 \text{ の倍数} \\ 0 & : \ \text{それ以外} \end{cases} \\ \varphi'(x) &= \begin{cases} 1 & : \ x \text{ が } 2 \text{ の倍数} \\ 0 & : \ \text{それ以外} \end{cases} \end{aligned}$$

集合 $A_\varphi, A_{\varphi'}$ を上の命題で定義されたものとする．このとき，

$$\varphi \Rightarrow \varphi' \ \Leftrightarrow \ A_\varphi \subseteq A_{\varphi'}.$$

問 4.10. φ, φ' を $\mathbb{Z} \times \mathbb{Z}$ 上の以下の述語とする．

$$\begin{aligned} \varphi(x,y) &= \begin{cases} 1 & : \ x+y \text{ が奇数} \\ 0 & : \ \text{それ以外} \end{cases} \\ \varphi'(x,y) &= \begin{cases} 1 & : \ x, y \text{ のうち少なくとも一つは奇数} \\ 0 & : \ \text{それ以外} \end{cases} \end{aligned}$$

集合 $A_\varphi, A_{\varphi'}$ を以下のように定義する．

$$\begin{aligned} A_\varphi &\stackrel{\text{def}}{=} \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : \varphi(a,b) = 1\}, \\ A_{\varphi'} &\stackrel{\text{def}}{=} \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : \varphi'(a,b) = 1\}. \end{aligned}$$

φ, φ' の含意，及び，$A_\varphi, A_{\varphi'}$ の包含関係を示しなさい．

章末問題

以下の問いに答えなさい.

1. 以下の言明のうち，命題であるのはどれか．また，命題であれば，真偽を求めなさい.
   (a) 一郎と二郎が同じチームで，かつ，二郎と三郎が同じチームであれば，一郎と三郎は同じチームである.
   (b) 四朗と五郎は異なるチームである.
   (c) $n+1$ は自然数である.
   (d) 33 は素数である.
   (e) 101 までの自然数のうち，偶数と奇数の個数は同じである.
2. 論理式 $(x \oplus y) \Rightarrow z$ の真理値表を作成しなさい.
3. 以下の論理式を簡単に（更に短い式に）しなさい.
   (a) $x \vee \overline{(x \vee \bar{y})}$　　(b) $x \wedge \overline{(x \wedge \bar{y})}$
   (c) $x \vee (x \wedge y)$　　(d) $x \wedge (x \vee y)$
   (e) $(x \vee \bar{y}) \wedge (\bar{x} \vee y) \wedge (\bar{x} \vee \bar{y})$　　(f) $(x \wedge \bar{y}) \vee (\bar{x} \wedge y) \vee (\bar{x} \wedge \bar{y})$
   (g) $x \Rightarrow x$　　(h) $x \Rightarrow (y \Rightarrow x)$
4. x, y, z を論理変数とする．このとき，$x \oplus y \oplus z$ を，$\vee$, $\wedge$，及び否定を用いて示しなさい.（ヒント：事実 4.3 を参考に論理式を構成する.）
5. 以下の論理関数を，ＣＮＦ論理式，ＤＮＦ論理式でそれぞれ表しなさい.

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

6. 関係 $\equiv$（定義 4.7）は同値関係であることを示しなさい.
7. $A = \{a_1, a_2, \ldots, a_n\} \subseteq \mathbb{N}$ を自然数の集合，$x \in \mathbb{N}$ を自然数とする．このとき，$x \in A$, $x \notin A$ それぞれを，限定子 $\forall, \exists$ を用いて表しなさい.

8. 以下の定義を，$\forall, \exists, \wedge, \vee$，否定，及び数学記号を使って表しなさい．
   (a) $A \subseteq B$
   (b) $A \cup B$
   (c) $A \cap B$
   (d) 写像 $f : A \to B$ が全射である
   (e) 写像 $f : A \to B$ が単射である
   (f) 写像 $f : A \to A$ が恒等写像である
   (g) 同値関係における 3 つの条件（反射律，対称律，推移律）
9. φ, φ' を $\mathbb{R}^3$ 上の以下の述語とする．

$$\begin{aligned} \varphi(x,y,z) &= \begin{cases} 1 & : \quad x+y+z>0 \\ 0 & : \quad \text{それ以外} \end{cases} \\ \varphi'(x,y,z) &= \begin{cases} 1 & : \quad x,y,z \text{ のうち少なくとも一つは正} \\ 0 & : \quad \text{それ以外} \end{cases} \end{aligned}$$

   集合 $A_\varphi, A_{\varphi'}$ を以下のように定義する．

$$\begin{aligned} A_\varphi &\stackrel{\text{def}}{=} \{(a,b,c) \in \mathbb{R}^3 : \varphi(a,b,c) = 1\} \\ A_{\varphi'} &\stackrel{\text{def}}{=} \{(a,b,c) \in \mathbb{R}^3 : \varphi'(a,b,c) = 1\}. \end{aligned}$$

   φ, φ' の含意，及び，$A_\varphi, A_{\varphi'}$ の包含関係を示しなさい．

第 5 章

離散数学における証明，再帰

5.1　等号の証明

事実 5.1. x, y を値とする．(x, y の値が「明示」されていない場合) $x = y$ の証明は，$x \leq y$ かつ $x \geq y$ を示すことでなされる．(命題 2.1 の証明の前半部分を参照.)

事実 5.2 (定義 1.6)**.** A, B を集合とする．(A, B が「明示」されていない場合) $A = B$ の証明は，$A \subseteq B$ かつ $A \supseteq B$ を示すことで証明される．(定理 3.1 の証明を参照.)

5.2　必要十分条件の証明

定義 5.1

P, Q を命題とする．$P \Rightarrow Q$ であるとき，P であるための**必要条件**は Q であるといい，Q であるための**十分条件**は P であるという．$P \Leftrightarrow Q$ であるとき，P であるための**必要十分条件**は Q であるという．(これを，P であるときかつそのときに限り Q である，ともいう.) このとき，P と Q は**同値**であるという．

事実 5.3. $P \Leftrightarrow Q$ を示すためには，$P \Rightarrow Q$ かつ $P \Leftarrow Q$ を示せばよい.

例 5.1 (必要十分条件)**.** x を実数とする．このとき，$x^2 - x - 2 = 0$ であるための必要十分条件は，$x = 2$ または $x = -1$ である.

例 5.2 (必要十分条件：命題 2.1)**.** A, B を有限集合とする．$|A| = |B|$ であるための必要十分条件は，A から B への全単射が存在することである.

5.3　対偶による証明

定義 5.2

P, Q を命題とする．論理式 $\bar{Q} \Rightarrow \bar{P}$ を論理式 $P \Rightarrow Q$ の**対偶**という．

事実 5.4. P, Q を命題とする．このとき，

$$P \Rightarrow Q \ \equiv \ \bar{Q} \Rightarrow \bar{P}.$$

命題 5.1. x, y を整数とする．このとき，$x + y$ が奇数であれば，x, y のうち少なくとも一つは奇数である．

証明. 対偶をとって示す．つまり，x, y が共に偶数であるなら $x + y$ が偶数であることを示す．この事実は明らか． ■

命題 5.2. x, y, z を実数とする．このとき，$x + y + z > 0$ であれば，x, y, z のうち少なくとも一つは正の実数である．

証明. 対偶をとって示す．つまり，x, y, z がいずれも 0 以下の実数であるなら $x+y+z \leq 0$ である．この事実は明らか． ■

5.4　背理法

命題 5.3. 素数は無限個存在する．

証明. そうでないとして矛盾を導く．つまり，素数が有限個しかなかったとする．それら素数の集合を $P = \{p_1, p_2, \ldots, p_t\}$ とする．このとき，

$$N \stackrel{\text{def}}{=} (p_1 \cdot p_2 \cdot \cdots \cdot p_t) + 1,$$

は素数となる．（P のいずれでも割り切れないので．系 6.3 を参照.）明らかに $N \notin P$ である．よって，素数全体の集合が P であることに矛盾する． ■

命題 5.4. $\sqrt{2}$ は無理数である．

証明. そうでないとして矛盾を導く．つまり，$\sqrt{2}$ が有理数であるとする．よって，ある互いに素な自然数 a, b が存在して $\sqrt{2} = a/b$．これより，

$$a^2 = 2b^2. \tag{5.1}$$

これは，a^2 が偶数であることを意味する．

主張 5.1. a^2 が偶数であれば，a は（正の）偶数である．

証明. 対偶をとれば明らか． ■

よって，ある自然数 c が存在して $a = 2c$．これを等式 (5.1) に代入すると，$b^2 = 2c^2$．同様の理由から，b が（正の）偶数であることがいえる．これは，a, b が互いに素であることに矛盾する． ■

5.5　数学的帰納法

事実 5.5. 任意の整数 $n \geq 0$ について，A_n を命題とする．以下の二つの論理式が成り立つとする．

1. A_0
2. $\forall k \in \mathbb{N}\ [A_{k-1} \Rightarrow A_k]$

このとき，任意の整数 $n \geq 0$ について，A_n が成り立つ．

命題 5.5. 任意の自然数 n について，

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

証明. $n = 1$ のとき，等式は明らかに成り立つ．$n = k - 1$（$k \geq 2$）のとき，等式が成り立つと仮定する．このとき，

$$\begin{aligned} 1 + 2 + \cdots + k &= (1 + 2 + \cdots + (k-1)) + k \\ &= \frac{(k-1)k}{2} + k \quad (\because \text{帰納仮定}) \\ &= \frac{k(k+1)}{2}. \end{aligned}$$

これより，任意の $n \geq 1$ について等式が成り立つ． ■

命題 5.6. 2 以上の任意の自然数は，素数の積として表される．ただし，素数そのものは，素数の積として表されているものとみなす．

証明. $n = 2$ のとき，n は素数であるので，2 は素数の積となっている．n（$n \geq 3$）未満のすべての自然数は素数の積として表せられると仮定する．（このもとで，n が素数の積として表されることを示す．）n が素数であれば，明らかに命題は成り立つ．n が素数でないとき，素数の定義より（定義 6.3 参照），n は 1, n 以外の約数 a をもつ．つまり，n 未満（2 以上）のある自然数 b が存在して，

$$n \ = \ ab. \quad (2 \leq a, b \leq n-1)$$

ここで，（$a, b \leq n-1$ だから）帰納仮定より，ある素数 $a_1, a_2, \ldots, a_s$, $b_1, b_2, \ldots, b_t$ に対して，a, b が以下のように表される．

$$a \ = \ a_1 \cdot a_2 \cdot \cdots \cdot a_s, \quad b \ = \ b_1 \cdot b_2 \cdot \cdots \cdot b_t.$$

よって，

$$n \ = \ ab \ = \ a_1 \cdots a_s \cdot b_1 \cdots b_t.$$

これより，任意の自然数 $n \geq 2$ は素数の積として表される． ■

問 5.1. 以下が成り立つことを数学的帰納法より示しなさい．（n_0 の値はいくらにすればよいか．）

$$\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N} \ [n \geq n_0 \Rightarrow n^2 + 2n + 3 \leq 2^n].$$

5.6 再帰的定義

例 5.3 (再帰的定義)**.** 関数 $f(n) = n!$（$n \geq 0$）は次のように定義される．

$$\begin{array}{lll} n = 0 & : & f(0) = 1 \\ n \geq 1 & : & f(n) = n \cdot f(n-1) \end{array}$$

例 5.4 (再帰的定義)**.** フィボナッチ数列 $F(n)$ は次のように定義される．

$$\begin{array}{l} F(1) = F(2) = 1 \\ F(n) = F(n-1) + F(n-2) \end{array}$$

問 5.2. 関数 $f(n) = \sum_{i=0}^{n} i$（$n \geq 0$）を再帰的に定義しなさい.

問 5.3. 関数 $f(n) = 2^n$（$n \geq 0$）を再帰的に定義しなさい.

例 5.5 (再帰的定義)**.** 自然数の集合 $\mathbb{N}$ は次のように定義される.

$$1 \in \mathbb{N}$$
$$n \in \mathbb{N} \Rightarrow n + 1 \in \mathbb{N}$$

問 5.4. 非負の偶数，及び非負の奇数を再帰的に定義しなさい.

第 6 章

整数

6.1 素数，合成数

定義 6.1

数の集合の表記としては，以下のものがよく使われる．

$$\begin{array}{lcl} \mathbb{N} & : & \text{自然数の集合} \\ \mathbb{Z} & : & \text{整数の集合} \\ \mathbb{Q} & : & \text{有理数の集合} \\ \mathbb{R} & : & \text{実数の集合} \\ \mathbb{Z}_n & : & \{0, 1, 2, \ldots, n-1\} \\ [n] & : & \{1, 2, \ldots, n\} \end{array}$$

定義 6.2

整数 $a, b \in \mathbb{Z}$ に対して，$a = bc$ を満たす整数 $c \in \mathbb{Z}$ が存在するとき，b は a を**割り切る**（a は b で**割り切れる**）といい，$b \mid a$ と表す．このとき，b は a の**約数**，a は b の**倍数**という．b が a を割り切らない（a が b で割り切れない）とき，$b \nmid a$ と表す．

定義 6.3

自然数 $p \geq 2$ が，± 1, $\pm p$ 以外の約数を持たないとき，p を**素数**という．素数でない（2 以上の）自然数を**合成数**という．

定理 6.1 (命題 5.3)**.** 素数は無限個存在する．

定理 6.2 (算術の基本定理)**.** 任意の自然数 $n \geq 2$ は，（n 以下の）ある素数 $p_1, \ldots, p_t$ と，ある自然数 $a_1, \ldots, a_t$ が存在して，

$$n \ = \ p_1^{a_1} \cdots p_t^{a_t},$$

のように一意に素因数分解できる．

問 6.1. $n = 2310$ を素因数分解しなさい．

系 6.3. p が素数であることと，p が $p-1$ 以下の（任意の）素数で割り切れないことは同値である．

証明. ($\Rightarrow$) 素数の定義より明らか．（p が素数であれば，p は $p-1$ 以下（2 以上）の任意の自然数で割り切れない．）

($\Leftarrow$) 上の定理より，p の素因数分解を $p = p_1^{a_1} \cdots p_t^{a_t}$ とする．このとき，$p_1, \ldots, p_t$ は素数である．（$t \geq 1$.）p が $p-1$ 以下の素数で割り切れないことから $t = 1$（更に，$a_1 = 1$）となることが必要である．（そうでなければ，p が $p-1$ 以下のある素数で割り切れるので．）よって，$p = p_1$，つまり，p は素数である． ■

6.2　商，余り

定理 6.4 (除法の原理)**.** 任意の整数 a，任意の自然数 n に対して，

$$a \ = \ qn + r,$$

となる整数 q 及び $r : 0 \leq r < n$ が一意に存在する．

定義 6.4

a を整数，n を自然数として，$a = qn + r$ とする．（ただし，$0 \leq r < n$.）このとき，q を**商**，r を**余り**といい，それぞれ $a \operatorname{div} n$，$a \bmod n$ と表す．

問 6.2. $(a,n)=(17,3)$ のとき，商と余りを求めなさい．また，$(a,n)=(-17,3)$ のときの商と余りを求めなさい．

6.3　合同式

定義 6.5

a,b を整数，n を自然数とする．$a \bmod n = b \bmod n$ であるとき，a と b は**法** n のもとで**合同**であるといい，$a \equiv_n b$（または $a \equiv b \pmod{n}$）と表す．$a \equiv_n b$ を**合同式**という．また，$a \equiv_n b$ でないとき，$a \not\equiv_n b$ と表す．

例 6.1 (合同式)**.** 以下の合同式が成り立つ．

$$2 \equiv_2 32, \qquad -2 \equiv_2 1024, \qquad 3 \equiv_2 101, \qquad 12 \equiv_3 123, \qquad 15 \equiv_4 103.$$

問 6.3. 以下は成り立つか．

$$1 \not\equiv_2 32, \qquad -3 \not\equiv_2 1024, \qquad 3 \not\equiv_2 100, \qquad 12 \not\equiv_5 123, \qquad 55 \not\equiv_7 125.$$

事実 6.1. a を整数，n を自然数として，$b = a \bmod n$ とする．このとき，$a \equiv_n b$ である．

問 6.4. 上の事実を示しなさい．

命題 6.5 (例 3.8)**.** 任意の自然数 n について，関係 $\equiv_n$ は $\mathbb{Z}$ 上の同値関係である．つまり，$\equiv_n$ は，反射律，対称律，推移律を満たす．特に，推移律より，$a \equiv_n b$ かつ $b \equiv_n c$ なら $a \equiv_n c$.

命題 6.6. a,b を整数，n を自然数とする．このとき，

$$a \equiv_n b \iff n \mid (a-b).$$

証明. ($\Rightarrow$) $a \equiv_n b$ より，（定義より $a \bmod n = b \bmod n$ であるから）ある整数 q_1, q_2, r

が存在して $a = q_1 n + r$, $b = q_2 n + r$. これより，$a - b = (q_1 - q_2)n$. $q_1 - q_2$ は整数であることから，$n \mid (a - b)$.

($\Leftarrow$) $n \mid (a - b)$ より，ある整数 q_1 が存在して $a - b = q_1 n$. つまり，$a = q_1 n + b$ である．ここで，$b = q_2 n + r$ とする．（ただし，$r < n$.）つまり，$q_2 = b \operatorname{div} n$, $r = b \bmod n$ とする．これより，

$$a = q_1 n + b = q_1 n + q_2 n + r = (q_1 + q_2)n + r.$$

よって，$a \bmod n = r$.（$r < n$ より.）また，$b \bmod n = r$ であることから，$a \bmod n = b \bmod n$，つまり，$a \equiv_n b$. ■

系 6.7. a を整数，n を自然数とする．このとき，$a \equiv_n 0$ と $n \mid a$ は同値である．

命題 6.8. a, a', b, b' を整数，n を自然数とする．$a \equiv_n a'$, $b \equiv_n b'$ のとき，

$$\begin{aligned} a + b &\equiv_n a' + b' \\ a - b &\equiv_n a' - b' \\ ab &\equiv_n a'b' \end{aligned}$$

証明. $a + b \equiv_n a' + b'$ を証明する．（$a - b \equiv_n a' - b'$ も同様にして示される.）$a \equiv_n a'$, $b \equiv_n b'$ より，（命題 6.6 より）$n \mid (a - a')$, $n \mid (b - b')$ が成り立つ．つまり，ある整数 A, B が存在して，$a - a' = An$, $b - b' = Bn$. これらより，

$$\begin{aligned} a + b - (a' + b') &= (a - a') + (b - b') \\ &= An + Bn \\ &= (A + B)n \end{aligned}$$

これより，

$$n \mid ((a + b) - (a' + b')).$$

よって，命題 6.6 より，$a + b \equiv_n a' + b'$.

次に，$ab \equiv_n a'b'$ を証明する．$a \equiv_n a'$, $b \equiv_n b'$ より，（ある整数 $q_1, q_1', q_2, q_2', r_1, r_2$ が存在して）

$$\begin{aligned} a &= q_1 n + r_1, \quad a' = q_1' n + r_1 \\ b &= q_2 n + r_2, \quad b' = q_2' n + r_2 \end{aligned}$$

これより，

$$\begin{array}{rcccl} ab & = & (q_1 n + r_1)(q_2 n + r_2) & = & q_1 q_2 n^2 + (q_1 r_2 + q_2 r_1)n + r_1 r_2 \\ a'b' & = & (q_1' n + r_1)(q_2' n + r_2) & = & q_1' q_2' n^2 + (q_1' r_2 + q_2' r_1)n + r_1 r_2 \end{array}$$

よって, $n \mid (ab - r_1 r_2)$, $n \mid (a'b' - r_1 r_2)$, つまり, (命題 6.6 より) $ab \equiv_n r_1 r_2$, $a'b' \equiv_n r_1 r_2$. よって, (命題 6.5 より) $\equiv_n$ は推移律を満たすから, $ab \equiv_n a'b'$. ■

注 6.1. この命題は, 合同式 $a \equiv_n b$ は, 整数の和・差・積については, 通常の等式 $a = b$ と同じように扱えることを意味している. (両辺に「同じ」整数を足したり・引いたり・掛けたりできる.) 一方, 商については成り立たない. ($a \div b$ が必ずしも整数にはならないので.)

注 6.2. それぞれについて逆は成り立たない. 例えば, $a + b \equiv_n a' + b'$ ならば $a \equiv_n a'$ かつ $b \equiv_n b'$ は成り立たない. ($n = 2$ のとき, $1 + 1 \equiv_n 0 + 2$ であるが, $1 \not\equiv_n 0$ かつ $1 \not\equiv_n 2$ である.)

系 6.9 (合同式における移項)**.** 任意の $a, b, c, d \in \mathbb{Z}$, 任意の $n \in \mathbb{N}$ について,

$$a + b \equiv_n c + d \iff a + b - c \equiv_n d.$$

問 6.5. 上の系を証明しなさい.

系 6.10. 任意の $a, b, c \in \mathbb{Z}$ 任意の $n \in \mathbb{N}$ に対して, 以下の二つが成り立つ.

1. $b \equiv_n 0 \quad \Rightarrow \quad a + b \equiv_n a$,
2. $c \equiv_n 1 \quad \Rightarrow \quad ca \equiv_n a$.

問 6.6. 上の系を証明しなさい.

問 6.7. $ma + nb \equiv_n 1$ であるための必要十分条件が $ma \equiv_n 1$ であることを示しなさい.

6.4　フェルマーの小定理

定義 6.6

整数 a, b が（1 以外に）共通の約数をもたないとき，a, b は**互いに素**であるという．自然数 n について，

$$\mathbb{Z}_n^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n \setminus \{0\} : a, n \text{ は互いに素 }\}.$$

例 6.2 $(\mathbb{Z}_n^*)$**.**

$$\begin{aligned} \mathbb{Z}_{10}^* &= \{1, 3, 7, 9\} \\ \mathbb{Z}_7^* &= \{1, 2, 3, 4, 5, 6\} \end{aligned}$$

事実 6.2. n が素数であれば，

$$\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}.$$

補題 6.11. p を素数とする．任意の整数 a, b に対して，$ab \equiv_p 0$ ならば $a \equiv_p 0$ または $b \equiv_p 0$ である．

証明. $a, b \geq 0$ とする．（そうでないときも同様にして示される．）$a = p_1^{a_1} \cdots p_t^{a_t}$, $b = q_1^{b_1} \cdots q_s^{b_s}$ とする．（p_i, q_j は素数，a_i, b_j は自然数．）このとき，$ab = (p_1^{a_1} \cdots p_t^{a_t}) \cdot (q_1^{b_1} \cdots q_s^{b_s})$．仮定 $ab \equiv_p 0$ より $p \mid ab$．（系 6.7 より．）よって，ある $i : 1 \leq i \leq t$ が存在して $p = p_i$，または，ある $j : 1 \leq j \leq s$ が存在して $p = q_j$．ゆえに，$p \mid a$ または $p \mid b$，つまり，$a \equiv_p 0$ または $b \equiv_p 0$ である． ■

注 6.3. p が素数でないなら，この補題は成り立たない．（$p = 4$, $a = b = 2 \cdot 3 = 6$ のとき，$ab \equiv_p 0$ であるが，$a \not\equiv_p 0$ かつ $b \not\equiv_p 0$ である．）

系 6.12. p を素数，x を $x \not\equiv_p 0$ を満たす任意の整数とする．このとき，任意の整数 a, b に対して，

$$ax \equiv_p bx \iff a \equiv_p b$$

証明. 命題 6.8 より，$\Leftarrow$ は明らか．以降，$\Rightarrow$ を示す．任意の整数 a, b, x について，

$$ax \equiv_p bx \iff ax - bx \equiv_p 0 \iff (a-b)x \equiv_p 0.$$

$x \not\equiv_p 0$ であることから，補題より，$a - b \equiv_p 0$，つまり，$a \equiv_p b$. ■

注 6.4. この系の $\Rightarrow$ の命題は次のことを意味する．両辺に共通因数 x があった場合，$x \not\equiv_p 0$ であれば（つまり，$p \nmid x$ であれば），両辺をその共通因数で「割る」ことができる．更に一般的に，p と x が互いに素であれば（p が素数でなくても），両辺を共通因数 x で割ることができる．

定理 6.13 (フェルマーの小定理)**.** p を素数，x を $x \not\equiv_p 0$ を満たす任意の自然数とする．このとき，

$$x^{p-1} \equiv_p 1.$$

証明. 任意の $i \in \mathbb{Z}_p^*$ について，$r_i = (ix) \bmod p$ とする．このとき，定義より，$r_i \in \mathbb{Z}_p$.

主張 6.1. $r_i \in \mathbb{Z}_p^*$.

問 6.8. この主張を証明しなさい.

主張 6.2. 任意の $i, j \in \mathbb{Z}_p^*$ に対して，$i \neq j$ であれば $r_i \neq r_j$.

問 6.9. この主張を証明しなさい.

上の二つの主張より，

$$\{r_1, r_2, \ldots, r_{p-1}\} = \{1, 2, \ldots, p-1\}.$$

ここで，

$$r_1 \cdot r_2 \cdots r_{p-1} = 1 \cdot 2 \cdots (p-1) \not\equiv_p 0. \tag{6.1}$$

また，r_i の定義より，$r_i \equiv_p ix$. つまり，

$$r_1 \equiv_p 1x, \quad r_2 \equiv_p 2x, \quad \ldots, \quad r_{p-1} \equiv_p (p-1)x. \tag{6.2}$$

以上より，(6.2) の辺々をかけて，

$$\begin{aligned} & r_1 \cdot r_2 \cdots r_{p-1} \equiv_p 1x \cdot 2x \cdot \cdots \cdot (p-1)x \\ \iff & r_1 \cdot r_2 \cdots r_{p-1} \equiv_p 1 \cdot 2 \cdots (p-1) \cdot x^{p-1} \\ \iff & x^{p-1} \equiv_p 1. \quad (\because \text{系 6.12 と (6.1).}) \end{aligned}$$

■

6.5　ユークリッドの互除法

定義 6.7

a, b を整数とする．$c \mid a$ かつ $c \mid b$ のとき，c を a, b の**公約数**といい，正の公約数の最大を**最大公約数**という．整数 a, b の最大公約数を $\gcd(a, b)$ と表す．整数 a, b が $\gcd(a, b) = 1$ を満たすとき，a, b は**互いに素**であるという．

$a \mid c$ かつ $b \mid c$ のとき，c を a, b の**公倍数**といい，正の公倍数の最小を**最小公倍数**という．整数 a, b の最小公倍数を $\mathrm{lcm}(a, b)$ と表す．

以降では，議論を簡略化させるため，自然数 a, b の公約数・公倍数を考える．（a, b が負の数であっても同様にして考えられる．）

問 6.10. $a = 90, b = 42$ とする．（$a = 2^1 \cdot 3^2 \cdot 5^1 = 90$, $b = 2^1 \cdot 3^1 \cdot 7^1 = 42$.）$\gcd(a, b)$ 及び $\mathrm{lcm}(a, b)$ を求めなさい．（gcd, lcm の値は素因数分解された形でよい．）

命題 6.14. 任意の自然数 a, b について，

$$\gcd(a, b) \cdot \mathrm{lcm}(a, b) \;=\; a \cdot b.$$

証明. 一般性を失うことなく $a \leq b$ とする．b 以下の素数を $p_1 = 2 < p_2 < \cdots < p_t \leq b$ とする．このとき，ある整数 $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_t \geq 0$ に対して，

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}, \\ b &= p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t}, \end{aligned}$$

と，a, b が素因数分解されたとする．また，任意の $i : 1 \leq i \leq t$ について，

$$\begin{aligned} x_i &= \min\{\alpha_i, \beta_i\} \\ y_i &= \max\{\alpha_i, \beta_i\} \end{aligned}$$

としたとき，

$$\begin{aligned} \gcd(a, b) &= p_1^{x_1} \ldots p_t^{x_t}, \\ \mathrm{lcm}(a, b) &= p_1^{y_1} \ldots p_t^{y_t}. \end{aligned}$$

よって，

$$\begin{aligned} \gcd(a, b) \cdot \mathrm{lcm}(a, b) &= (p_1^{x_1} \ldots p_t^{x_t}) \cdot (p_1^{y_1} \ldots p_t^{y_t}) \\ &= p_1^{x_1 + y_1} \ldots p_t^{x_t + y_t} \end{aligned}$$

$$
\begin{aligned}
&= p_1^{\alpha_1+\beta_1} \dots p_t^{\alpha_t+\beta_t} \\
&= (p_1^{\alpha_1} \dots p_t^{\alpha_t}) \cdot (p_1^{\beta_1} \dots p_t^{\beta_t}) \\
&= a \cdot b.
\end{aligned}
$$

■

この命題より，gcd か lcm かのどちらかが計算できれば，もう一方も計算できることになる．以下，（素因数分解することなく[*1]）gcd を求める方法（アルゴリズム）を示す．

補題 6.15. a, b を自然数とする．$r = a \bmod b$ とする．（$0 \leq r < b.$）a, b の公約数の集合を $\mathrm{CD}(a, b)$，b, r の公約数の集合を $\mathrm{CD}(b, r)$ とする．このとき，

$$\mathrm{CD}(a, b) \;=\; \mathrm{CD}(b, r).$$

証明. $r = a \bmod b$ より，ある整数 q に対して $a = qb + r$ とする．以下，$\mathrm{CD}(a, b) \subseteq \mathrm{CD}(b, r)$ かつ $\mathrm{CD}(a, b) \supseteq \mathrm{CD}(b, r)$ を示す．

($\subseteq$)　これは次の事実から示される．a, b の公約数は b, r の公約数である．つまり，任意の自然数 x について，

$$x \mid a \text{ かつ } x \mid b \implies x \mid b \text{ かつ } x \mid r$$

これは，$r = a - qb$ より示される．

($\supseteq$)　これは次の事実から示される．b, r の公約数は a, b の公約数である．つまり，任意の自然数 x について，

$$x \mid b \text{ かつ } x \mid r \implies x \mid a \text{ かつ } x \mid b$$

これは，$a = qb + r$ より示される． ■

定理 6.16 (ユークリッドの補題)**.** a, b を自然数とする．$r = a \bmod b$ とする．（$0 \leq r < b.$）このとき，

$$\gcd(a, b) \;=\; \gcd(b, r).$$

証明. 上の補題より明らか． ■

[*1] 素因数を効率よく求めることはできないと思われている．（そのようなアルゴリズムは発見されていない．）

系 6.17 (ユークリッドの互除法)**.** 任意の自然数 a, b について,

$$\begin{array}{lcllll} a & = & q_1 \cdot b & + & r_1 & (0 < r_1 < b) \\ b & = & q_2 \cdot r_1 & + & r_2 & (0 < r_2 < r_1) \\ r_1 & = & q_3 \cdot r_2 & + & r_3 & (0 < r_3 < r_2) \\ \vdots & \vdots & & \vdots & & \\ r_{k-1} & = & q_{k+1} \cdot r_k & + & r_{k+1} & (0 < r_{k+1} < r_k) \\ r_k & = & q_{k+2} \cdot r_{k+1} & & & (r_{k+2} = 0) \end{array}$$

とする．このとき,

$$\gcd(a, b) = r_{k+1}.$$

証明. 上の定理より,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k, r_{k+1}) = r_{k+1}.$$

■

問 6.11. ユークリッドの互除法を用いて，$\gcd(450, 195)$ を求めなさい.

問 6.12. ユークリッドの互除法を用いて，$\gcd(314, 136)$ を求めなさい.

定理 6.18 (ベズーの等式)**.** a, b を自然数とする．このとき，ある整数 m, n が存在して,

$$\gcd(a, b) \ = \ ma + nb.$$

証明. ユークリッドの互除法より,

$$\begin{array}{lcllll} r_{k+1} & = & r_{k-1} & - & q_{k+1} & \cdot \ r_k \\ r_k & = & r_{k-2} & - & q_k & \cdot \ r_{k-1} \\ r_{k-1} & = & r_{k-3} & - & q_{k-1} & \cdot \ r_{k-2} \\ \vdots & \vdots & & \vdots & & \\ r_3 & = & r_1 & - & q_3 & \cdot \ r_2 \\ r_2 & = & b & - & q_2 & \cdot \ r_1 \\ r_1 & = & a & - & q_1 & \cdot \ b \end{array}$$

ただし，$r_{k+1} = \gcd(a, b)$．まず，上の式の「$r_{k+1} = \cdots$」に「$r_k = \cdots$」を代入する．このとき，

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1}) \\ &= r_{k-1} - q_{k+1} r_{k-2} + q_{k+1} q_k r_{k-1} \\ &= -q_{k+1} r_{k-2} + (q_{k+1} q_k + 1) r_{k-1}. \end{aligned}$$

これより，ある整数 m_k, n_k が存在して（つまり，$m_k = -q_{k+1}, n_k = q_{k+1}q_k + 1$），

$$r_{k+1} = m_k r_{k-2} + n_k r_{k-1}.$$

次に，この式に上の式の「$r_{k-1} = \cdots$」を代入する．このとき，

$$\begin{aligned} r_{k+1} &= m_k r_{k-2} + n_k(r_{k-3} - q_{k-1} r_{k-2}) \\ &= m_k r_{k-2} + n_k r_{k-3} - n_k q_{k-1} r_{k-2} \\ &= n_k r_{k-3} + (m_k - n_k q_{k-1}) r_{k-2}. \end{aligned}$$

これより，ある整数 m_{k-1}, n_{k-1} が存在して，

$$r_{k+1} = m_{k-1} r_{k-3} + n_{k-1} r_{k-2}.$$

同様にして，$r_{k-2}, \ldots, r_1$ を代入していくと，ある整数 m_1, n_1 が存在して，

$$r_{k+1} = m_1 a + n_1 b.$$

$r_{k+1} = \gcd(a, b)$ より定理が示される． ■

注 6.5. 上の定理の証明に沿えば，m, n の値を（具体的に）求めることができることが分かる．「拡張ユークリッドの互除法」と呼ばれる，これと本質的には同じ（見た目は異なる）求め方のアルゴリズムがある．

問 6.13. 上の定理の証明を用いて，$\gcd(450, 195) = 450m + 195n$ を満たす整数 m, n を求めなさい．

問 6.14. 上の定理の証明を用いて，$\gcd(314, 136) = 314m + 136n$ を満たす整数 m, n を求めなさい．

第 7 章

暗号への応用

メッセージを送信する者を**送信者**といい，メッセージを受信する者を**受信者**という．公共の通信網を使って送信者が受信者にメッセージを送信する場合，送信されたメッセージが第三者に洩れるのが通常である．それを防ぐために，送信者はメッセージの暗号文を受信者に送信する．ここで，暗号文のもとのメッセージを**平文**という．平文を暗号文にすることを**暗号化**といい，暗号文をもとの平文にすることを**復号化**という．暗号化・復号化に使われる「鍵」を，それぞれ**暗号鍵・復号鍵**という．暗号化・復号化で鍵が同じであるものを**共通鍵暗号**，鍵が異なるものを**公開鍵暗号**という．

7.1 シーザー暗号

共通鍵暗号の古典的なものとして，換字式暗号の一つであるシーザー暗号を取り上げる．２６個の（大文字の）アルファベット $\Sigma = \{A, B, C, \ldots, Z\}$ からなる平文を考える．シーザー暗号の暗号化は，平文の各文字を辞書式順で k シフトさせたものである[*1]．（例えば，$k = 3$ のとき，文字 A は D となる．）復号化は，暗号文の各文字を $-k$ シフトさせたものである．（例えば，$k = 3$ のとき，文字 Z は W となる．）以下は，$k = 1$ のときのシーザー暗号の例である．

暗号化　：　TO BE, OR NOT TO BE: THAT IS THE QUESTION.
$\xrightarrow{+1}$　UP CF, PS OPU UP CF: UIBU JT UIF RVFTUJPO.

復号化　：　UP CF, PS OPU UP CF: UIBU JT UIF RVFTUJPO.
$\xrightarrow{-1}$　TO BE, OR NOT TO BE: THAT IS THE QUESTION.

[*1] 実際，$k = 3$ のものがシーザー暗号と呼ばれる．

7.2　アフィン暗号

共通鍵暗号のもう一つの例として，換字式暗号の一つであるアフィン暗号を取り上げる．２６個のアルファベット $\Sigma = \{A, B, C, \ldots, Z\}$ からなる平文を考える．ここでは，以下のように，各文字が数字 $\{0, 1, \ldots, 25\}$（つまり，$\mathbb{Z}_{26}$）に対応付けられているものとする．

A	B	C	⋯ ⋯	Y	Z
0	1	2	⋯ ⋯	24	25

問 7.1. 上のように文字コードを決めた場合，SEIKEI はどのような数字列になるか．

命題 7.1. m を任意の自然数，a を $\gcd(m, a) = 1$ である任意の自然数とする．このとき，$a'a \equiv_m 1$ となる $a' \in \mathbb{Z}_m$ が（一意に）存在する．

証明. 定理 6.18 より，ある整数 s, t が存在して，

$$\gcd(m, a) = sm + ta.$$

$\gcd(m, a) = 1$ より，$sm + ta = 1$.（つまり，$ta = 1 - sm$.）よって，

$$ta \equiv_m 1 - sm \equiv_m 1. \quad (\because\ sm \equiv_m 0).$$

$t \in \mathbb{Z}$ が $t \in \mathbb{Z}_m$ である場合，$a' = t$ とすれば命題が示される．そうでない場合，任意の $k \in \mathbb{Z}$ について，

$$ta + kma \equiv_m 1. \quad (\because\ kma \equiv_m 0)$$

よって，$(t + km)a \equiv_m 1$．これより，$t + km \in \mathbb{Z}_m$ となる k を用いて $a' = t + km$ とすれば命題が示される．（そのような k は一意に存在する．） ■

定義 7.1

m を任意の自然数，a を $\gcd(m, a) = 1$ である任意の自然数とする．$a'a \equiv_m 1$ を満たす $a' \in \mathbb{Z}_m$ を，（m を法とした）a の**逆元**といい，a^{-1} と表記する．

問 7.2. $m = 30$ を法とした $a = 13$ の逆元を求めなさい．また，$m = 13$ を法とした $a = 30$ の逆元を求めなさい．

以降，$m = 26$ とする．$a \in \mathbb{N}$ を $\gcd(m, a) = 1$ である任意の自然数として，a^{-1} を a の逆元とする．また，$b \in \mathbb{N}$ を任意とする．アフィン暗号の暗号化関数 $E : \mathbb{Z}_m \to \mathbb{Z}_m$ は，任意の $x \in \mathbb{Z}_m$ に対して，

$$E(x) \stackrel{\text{def}}{=} ax + b \pmod{m}.$$

また，復号化関数 $D : \mathbb{Z}_m \to \mathbb{Z}_m$ は，任意の $y \in \mathbb{Z}_m$ に対して，

$$D(y) \stackrel{\text{def}}{=} a^{-1}(y - b) \pmod{m}.$$

このとき，(a, b) が暗号鍵，$(a^{-1}, -b)$ が復号鍵となる．

例 7.1. $(a, b) = (25, 1)$ としてアフィン暗号を用いた場合（$m = 26$），ABC のアフィン暗号文は，

$$\begin{array}{lllll} \mathrm{A} & : & E(0) = 1 & \equiv_m & 25 \cdot 0 + 1 \\ \mathrm{B} & : & E(1) = 0 & \equiv_m & 25 \cdot 1 + 1 \\ \mathrm{C} & : & E(2) = 25 & \equiv_m & 25 \cdot 2 + 1 \end{array}$$

より，（アルファベット表記で）BAZ となる．このとき，復号化関数は（$a^{-1} = 25$ より）$D(y) = 25(y - 1) \pmod{m}$ となる．

問 7.3. 自然数 $(a, b) = (25, 1)$ としてアフィン暗号を用いた場合（$m = 26$），SEIKEI の暗号文は（アルファベット表記で）何か．

命題 7.2. 任意の $x \in \mathbb{Z}_m$ について，

$$D(E(x)) \equiv_m x.$$

証明. 関数 E, D を合成すると，

$$D(E(x)) = a^{-1}(((ax + b) \bmod m) - b) \pmod{m}.$$

よって，ある整数 q が存在して，

$$D(E(x)) \equiv_m a^{-1}(((ax + b) \bmod m) - b)$$

$$
\begin{aligned}
&\equiv_m a^{-1}(((ax+b)-mq)-b)\\
&\equiv_m a^{-1}(ax-mq)\\
&\equiv_m a^{-1}ax - a^{-1}mq\\
&\equiv_m a^{-1}ax \quad (\because\ a^{-1}mq \equiv_m 0)\\
&\equiv_m x. \quad (\because\ a^{-1}a \equiv_m 1)
\end{aligned}
$$

■

この命題は，任意のアルファベット $x \in \mathbb{Z}_m$ について，x を暗号化 $E(x)$ して復号化 $D(y)$ すれば，もとのアルファベット x に戻ることを意味する．

7.3　RSA 暗号

公開鍵暗号として，RSA 暗号を取り上げる．２６個の（大文字の）アルファベット $\Sigma = \{A, B, C, \ldots, Z\}$ からなる平文を考える．さきほどと同じように，以下のように，各文字が数字 $\{0, 1, \ldots, 25\}$ （つまり，$\mathbb{Z}_{26}$）に対応付けられているものとする．

A	B	C	⋯	⋯	Y	Z
0	1	2	⋯	⋯	24	25

RSA 暗号の暗号化・復号化を示す前に，まず，暗号鍵・復号鍵の生成法を以下に示す．（以下は，受信者側でなされる．）

1. 大きな二つの素数 p, q を（ランダムに）生成して $N = pq$ とする．
2. $\gcd(e, (p-1)(q-1)) = 1$ となる e を（ランダムに）生成する[*2]．
3. $ed \equiv 1 \pmod{(p-1)(q-1)}$ となる自然数 d を求める[*3]．
4. (N, e) を暗号鍵（公開鍵），d を復号鍵（秘密鍵）とする．

図 7.1　RSA 暗号．(N, e) が公開鍵，d が秘密鍵

[*2] ただし，$e \neq 1$ とする．（そうでなければ，e の逆元が簡単に求まってしまうので．）
[*3] d は（$(p-1)(q-1)$ を法とした）e の逆元である．（よって，$e = 1$ なら $d = 1$ となる！）

ここでは，話を簡単にするため，一文字ずつ暗号化することを考える[*4]．つまり，送信されるメッセージ M は $\{0,1,2,\ldots,25\}$ の要素である．RSA 暗号の暗号化関数 $E:\mathbb{Z}_N \to \mathbb{Z}_N$ は，任意の $M \in \mathbb{Z}_N$ に対して，

$$E(M) \stackrel{\text{def}}{=} M^e \pmod N.$$

RSA 暗号の復号化関数 $D:\mathbb{Z}_N \to \mathbb{Z}_N$ は，任意の $C \in \mathbb{Z}_N$ に対して，

$$D(C) \stackrel{\text{def}}{=} C^d \pmod N.$$

このとき，(N,e) が暗号鍵（公開），d が復号鍵（秘密）となる．

注 7.1. $M \in \mathbb{Z}_N$ であるため，$N \geq 26$ となるように素数 p,q を定める必要がある．

例 7.2. $(p,q)=(5,7)$, $e=5$ として RSA 暗号を用いた場合（$N=35$, $\gcd(5,24)=1$），ABC の RSA 暗号文は，

$$\begin{array}{lllll} \text{A} & : & E(0) & = & 0 \equiv_N 0^5 \\ \text{B} & : & E(1) & = & 1 \equiv_N 1^5 \\ \text{C} & : & E(2) & = & 32 \equiv_N 2^5 \end{array}$$

より，（数字の列で）$(0,1,32)$ となる．このとき，復号化関数は（$d = e^{-1} = 5$ より）$D(C) = C^5 \pmod N$ となる．

問 7.4. $d = e^{-1} = 5$ となることを確認しなさい．

命題 7.3. a,b を整数，n を自然数とする．このとき，

$$ab \equiv_n (a \bmod n)\cdot b.$$

証明. $a = qn + r$（$0 \leq r < n$）とする．これより，

$$\begin{array}{ll} \text{左辺} : & ab = (qn+r)\cdot b = qnb + rb \equiv_n rb. \\ \text{右辺} : & (a \bmod n)\cdot b = rb. \end{array}$$

■

[*4] 実際には，何文字かまとめて暗号化される．

系 7.4. a, b を整数，n を自然数とする．このとき，

$$ab \equiv_n (a \bmod n) \cdot (b \bmod n).$$

問 7.5. この系を証明しなさい．

例 7.3. $(p, q) = (5, 7)$, $e = 5$ として RSA 暗号を用いた場合（$N = 35$），EFG の暗号文は，

$$\begin{array}{lllll} \mathrm{E} & : & E(4) & = & 9 \quad \equiv_N \ 4^5 \equiv_N 4^3 \cdot 4^2 \equiv_N (4^3 \bmod N) \cdot 4^2 \equiv_N 29 \cdot 4^2 \\ & & & & \quad \equiv_N \ (29 \cdot 4) \cdot 4 \equiv_N 116 \cdot 4 \equiv_N (116 \bmod N) \cdot 4 \equiv_N 11 \cdot 4 \\ & & & & \quad \equiv_N \ 44 \equiv_N 9 \\ \mathrm{F} & : & E(5) & = & 10 \\ \mathrm{G} & : & E(6) & = & 6 \end{array}$$

より，$(9, 10, 6)$ となる．

問 7.6. 上の例において，$E(5)$, $E(6)$ の途中計算式を示しなさい．

補題 7.5. a, b を任意の整数とする．n_1, n_2 を互いに素な自然数とする．このとき，$a \equiv_{n_1} b$ かつ $a \equiv_{n_2} b$ であるならば，$a \equiv_{n_1 n_2} b$.

証明. $a \equiv_{n_1} b$, $a \equiv_{n_2} b$ より，

$$n_1 \mid (a - b), \quad n_2 \mid (a - b).$$

n_1, n_2 は互いに素であることから，

$$n_1 n_2 \mid (a - b).$$

よって，$a \equiv_{n_1 n_2} b$. ■

命題 7.6. 任意の $M \in \mathbb{Z}_N$ について，

$$D(E(M)) \equiv M \pmod{N}.$$

証明. [*5] 関数 E, D を合成すると,

$$D(E(M)) \;=\; (M^e \bmod N)^d \pmod N.$$

よって，ある整数 $q \geq 0$ が存在して,

$$\begin{aligned} D(E(M)) &\equiv_N (M^e \bmod N)^d \\ &\equiv_N (M^e - qN)^d \\ &\equiv_N M^{ed}. \quad (\because \text{二項定理：定理 7.7}) \end{aligned}$$

主張 7.1.

$$M^{ed} \;\equiv_p\; M.$$

証明. $M \equiv_p 0$ のときは明らか．以下，$M \not\equiv_p 0$ とする．e, d の定義より，ある整数 $r \geq 0$ が存在して $ed = r(p-1)(q-1)+1$ である．$M \not\equiv_p 0$ より，$M^{r(q-1)} \not\equiv_p 0$ である．よって，フェルマーの小定理より $(M^{r(q-1)})^{p-1} \equiv_p 1$ が成り立つ．これより,

$$\begin{aligned} M^{ed} &\equiv_p M^{1+r(p-1)(q-1)} \\ &\equiv_p M \cdot (M^{r(q-1)})^{p-1} \\ &\equiv_p M. \quad (\because (M^{r(q-1)})^{p-1} \equiv_p 1) \end{aligned}$$

■

主張 7.2.

$$M^{ed} \;\equiv_q\; M.$$

証明. 上と同様. ■

これら二つの主張より，p, q は互いに素であるから，上の補題より,

$$D(E(M)) \;\equiv_N\; M^{ed} \;\equiv_{pq}\; M.$$

よって，$D(E(M)) \equiv_N M$. ■

この命題は，任意の $M \in \mathbb{Z}_N$ について，M を暗号化 $E(M)$ して復号化 $D(C)$ すれば，もとの M に戻ることを意味する.

定理 7.7 (二項定理)**.** 任意の実数 a, b，任意の整数 $n \geq 0$ について,

$$(a+b)^n \;=\; \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

[*5] オイラーの定理を用いずに示す.（フェルマーの小定理は用いる.）

章末問題

以下の問いに答えなさい.

1. $m = 29$ として $a = 12$ の逆元を求めなさい.
2. $m = 26$ として，アフィン暗号について以下の設問に答えなさい.
   (a) $(a, b) = (23, 1)$ とする．暗号化関数 $E : \mathbb{Z}_m \to \mathbb{Z}_m$，及び，復号化関数 $D : \mathbb{Z}_m \to \mathbb{Z}_m$ を求めなさい．また，SEIKEI の暗号文が（アルファベット表記で）何になり，それを復号化したら元に戻ることを確認しなさい.
   (b) $(a, b) = (27, 1)$ とする．暗号化関数 $E : \mathbb{Z}_m \to \mathbb{Z}_m$，及び，復号化関数 $D : \mathbb{Z}_m \to \mathbb{Z}_m$ を求めなさい．また，SEIKEI の暗号文が（アルファベット表記で）何になり，それを復号化したら元に戻ることを確認しなさい.
   (c) (a, b) の値を適当に決めて，暗号化関数 $E : \mathbb{Z}_m \to \mathbb{Z}_m$，及び，復号化関数 $D : \mathbb{Z}_m \to \mathbb{Z}_m$ を求めなさい.
3. $(p, q) = (3, 11)$, $N = pq$ として，RSA 暗号について以下の設問に答えなさい.
   (a) $e = 3$（$\gcd(e, (3-1)(11-1)) = 1$）として，暗号化関数 $E : \mathbb{Z}_N \to \mathbb{Z}_N$，及び，復号化関数 $D : \mathbb{Z}_N \to \mathbb{Z}_N$ を求めなさい．また，ABE の暗号文が（数字の列で）何になり，それを復号化したら元に戻ることを確認しなさい.
   (b) $e = 7$（$\gcd(e, (3-1)(11-1)) = 1$）として，暗号化関数 $E : \mathbb{Z}_N \to \mathbb{Z}_N$，及び，復号化関数 $D : \mathbb{Z}_N \to \mathbb{Z}_N$ を求めなさい．また，ABE の暗号文が（数字の列で）何になり，それを復号化したら元に戻ることを確認しなさい.
   (c) 自然数 3, 7 の他に，e の値としてなりえる一桁の自然数を求めなさい．更に，この値を e として用いた場合の，暗号化関数 $E : \mathbb{Z}_N \to \mathbb{Z}_N$，及び，復号化関数 $D : \mathbb{Z}_N \to \mathbb{Z}_N$ を求めなさい.

各章の問，及び章末問題の略解

集合

1. なし.
2. なし.
3. - $\{i : i$ は素数 $\}$.
   - $\{2, 4, 6, 8\}$.
   - $\{a : a$ は首都 $\}$.
4. (1), (4), (5).
5. 奇数の集合.
6. - $A \cap B = \{2, 3, 5\}$.
   - $A \cup B = \{1, 2, 3, 4, 5, 7, 11\}$.
7. - $A \setminus B = \{1, 4\}$.
   - $A \oplus B = \{1, 4, 7, 11\}$.
8. $\emptyset$ は空集合.（$|\emptyset| = 0.$）$\{\emptyset\}$ は空集合（だけ）を要素とした集合.（$|\{\emptyset\}| = 1.$）
9. (2), (3), (4), (7), (10), (11), (13), (15), (16).
10. $2^A = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.
11. $2^\emptyset = \{\emptyset\}$.
12. - A を正の整数，B を負の整数，$C = \{0\}$ とした場合の A, B, C.
    - A_i を 5 で割ったら i 余る整数の集合とした場合の A_0, A_1, A_2, A_3, A_4.

章末問題

1. (a) $\{i \in \mathbb{Z} : -5 \leq i \leq 10\}$.
   (b) $\{a \in \mathbb{R} : a$ は無理数 $\}$.
   (c) $\{a : a$ は都道府県庁所在地 $\}$.
   (d) $\{i \in \mathbb{N} : i$ は 3 で割ったら 2 余る $\}$.
   (e) $\{i \in \mathbb{N} : i$ は 60 の約数かつ $i \leq 12\}$.

2. (a), (c), (e). 大きさは，それぞれ 16, 47, 8.
3. 2, 3, 6, 7, 10, 11, 12
4. (a) $\bar{A} = \{1, 4, 6, 8, 9, 10\}$, $\bar{B} = \{6, 7, 8, 9, 10\}$, $\bar{C} = \{2, 4, 6, 8, 10\}$
   (b) $\overline{A \cup B \cup C} = \{6, 8, 10\}$
   (c) $\overline{A \cap B \cap C} = \{1, 2, 4, 6, 7, 8, 9, 10\}$
5. (a) $A \cup B = \{i \in \mathbb{Z} : i$ は 2 または 3 で割り切れる $\}$
   (b) $A \cap B = \{i \in \mathbb{Z} : i$ は 2 と 3 の両方で割り切れる $\}$
   (c) $A \setminus B = \{i \in \mathbb{Z} : i$ は 2 で割り切れるが 3 では割り切れない $\}$
   (d) $A \oplus B = \{i \in \mathbb{Z} : i$ は 2 または 3 のどちらか一方だけで割り切れる $\}$
6. $2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
7. $|2^A| = 2^n$

写像

1. $f(x) \in \{y \in \mathbb{R} : y^2 = x\}$ で定義される $f : \mathbb{R} \to \mathbb{R}$ など.
2. $f([0, \pi/2]) = [0, 1]$.
3. $f(\{0, 1, 3, 4, 5\}) = \{\{a\}, \{a, b\}, \{a, c\}, \{b, c\}\}$.
4. 全射でも単射でもない.
5. 順に，単射，全射，全単射.
6. 恒等写像でない.
7. $f^{-1}(x) = (x + 1)/2$.
8. $(g \circ f)(x) = x^2 + 4x$.

章末問題

1. (a) 写像である.
   (b) 写像でない.（$\because f(2)$ が未定義である）
   (c) 写像でない.（$\because f(2)$ が一意でない）
2. $f_1([0, \pi/2]) = [0, 1]$, $f_2([0, \pi/2]) = [0, 1]$, $f_3([0, \pi/2)) = \{i \in \mathbb{R} : i \geq 0\}$
3. (a) 全単射. $f^{-1}(x) = x - 1$
   (b) いずれでもない.
   (c) 全単射. $f^{-1}(x) = \sqrt[3]{x}$
   (d) 全射.
   (e) 単射.

4. $(f \circ f)$ は以下.

x	0	1	2	3	4	5
$(f \circ f)(x)$	0	0	0	1	2	3

5. 合成写像 $g \circ f$ は以下.（逆写像はその逆.）

x	1	2	3
$(g \circ f)(x)$	2	3	1

関係

1. 区別のつくサイコロを 2 個ふったときの出る目の組みの集合.
2. $\mathbb{R}^2$：2 次元平面. $\mathbb{R}^3$：3 次元空間.
3. $\{(\phi,\phi),(\{0\},\{0\}),(\{0\},\{1\}),(\{1\},\{0\}),(\{1\},\{1\}),(\{0,1\},\{0,1\})\}$.
4. $\{(a,a),(b,b),(c,c),(a,c),(c,a)\}$.
5. 同値関係でない.（なぜ？）
6. 同値関係の定義に従い，反射律，対称律，推移律が成り立つことをそれぞれ示す.
   - 反射律：すべての $a \in \mathbb{N}_0$ について，$a-a=0$ より $a-a$ は 3 で割り切れる. よって，$(a,a) \in R_3$.
   - 対称律：すべての $a, a' \in \mathbb{N}_0$ について，$a-a'$ が 3 で割り切れれば $a'-a = -(a-a')$ は 3 で割り切れる. よって，$(a,a') \in R_3$ なら $(a',a) \in R_3$.
   - 推移律：すべての $a, a', a'' \in \mathbb{N}_0$ について，$a-a'$, $a'-a''$ が 3 で割り切れれば $a-a'' = (a-a')+(a'-a'')$ は 3 で割り切れる. よって，$(a,a'),(a',a'') \in R_3$ なら $(a,a'') \in R_3$.
7. 同値関係の定義に従い，反射律，対称律，推移律が成り立つことをそれぞれ示す.
8. 同値関係である.
9. 同値関係の定義に従い，反射律，対称律，推移律が成り立つことをそれぞれ示す.
10. 関数 f が $f(x)=x$ のときかつそのときに限り同値関係となる.
11. $R_3[0] = \{0,3,6,\dots\}$, $R_3[1] = \{1,4,7,\dots\}$, $R_3[2] = \{2,5,8,\dots\}$. $R_3[3] = R_3[0]$, $R_3[4] = R_3[1]$, $R_3[5] = R_3[2]$, $R_3[6] = R_3[0]$, ...
12. $\mathbb{N}_0/R_3 = \{R_3[0], R_3[1], R_3[2]\}$.
13. 以下であることから確かめられる.

$$\begin{aligned} R_3[0] &= \{a \in \mathbb{N}_0 : a \text{ を } 3 \text{ で割った余りが } 0\} \\ R_3[1] &= \{a \in \mathbb{N}_0 : a \text{ を } 3 \text{ で割った余りが } 1\} \\ R_3[2] &= \{a \in \mathbb{N}_0 : a \text{ を } 3 \text{ で割った余りが } 2\} \end{aligned}$$

14. 半順序関係.

15. 半順序関係でない.
16. そうでない.（反例：$R_k = \{(a,b) : k \text{ は } a-b \text{ を割り切る }\} \subseteq \mathbb{N}_0^2$.）そうでない.（反例：$R_{\leq} = \{(a,b) : a \leq b\} \subseteq \mathbb{R}^2$.）
17. 全順序集合でない.
18. 全順序集合でない.
19. 最大：10，最小：1，極大：10，極小：1.
20. 最大：なし，最小：1，極大：7, 8, 9, 10, 11, 12，極小：1.

章末問題

1. $A \times B \times C = \{(a,b,c) : a \in A, b \in B, c \in C\}$
2. $A \times B = \{(0,a),(0,b),(0,c),(1,a),(1,b),(1,c)\}$
3. $|A^n| = k^n$.
4. いずれも同値関係ではない.（R_1 は反射律が，R_2 は対称律が，R_3 は推移律が成り立たない.）
5. (a) 同値関係の三つの条件が成り立つことを示す.
   (b) $R[(1,1)] = \{(x,y) \in A : x = y\}$
   (c) $A/R = \{R[(x,y)] : x, y \in \mathbb{N}\}$
6. (a) 同値関係の三つの条件が成り立つことを示す.
   (b) $R[\text{apple}] = \{\alpha \in \Omega : \alpha \text{ の頭文字は a}\}$
   (c) $\Omega/R = \{R[\gamma] : \gamma \in \Sigma\}$
7. (a) 同値類の定義, 対称律の定義を用いて示される.（同値類の定義より $(a,b) \in R$. 対称律より $(b,a) \in R$. よって，同値類の定義より $a \in R[b]$.）
   (b) 同値類の定義，対称律・推移律の定義を用いて示される.（同値類の定義より $(a,b),(a,c) \in R$. 対称律より $(b,a) \in R$. このこのから，$(b,a),(a,c) \in R$. よって，推移律より $(b,c) \in R$.）

論理

1. 1, 2.
2.

x	y	z	$x \vee y \vee z$	$x \wedge y \wedge z$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

3.

x	y	$x \vee \bar{y}$
0	0	1
0	1	0
1	0	1
1	1	1

x	y	z	$x \vee (y \wedge z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

4.
- $\overline{x \vee yz} = \bar{x} \wedge (\bar{y} \vee \bar{z})$
- $\overline{(x \vee y)(x \vee z)} = \bar{x}\bar{y} \vee \bar{x}\bar{z}$

5.
- $\bar{y} \vee \bar{z}$ にド・モルガンの法則を用いて，$\bar{y} \vee \bar{z} \vee yz \equiv \overline{yz} \vee yz$ より明らか．（次のように示すのでもよい．$\bar{y} \vee \bar{z}$ が 0 になるのは，$y = z = 1$ のときかつそのときに限る．一方，そのときは $yz = 1$ になる．）
- $(x \vee y)(x \vee z)$ に分配則を用いて，$\overline{x \vee yz} \vee (x \vee y)(x \vee z) \equiv \overline{x \vee yz} \vee (x \vee yz)$ より明らか．（次のように示すのでもよい．$\overline{x \vee yz} = \bar{x} \wedge (\bar{y} \vee \bar{z})$ より，$x = 0$ のときは $(\bar{y} \vee \bar{z}) \vee yz$ となり（一つ目より）恒真，$x = 1$ のときは $(1 \vee y)(1 \vee z)$ となり恒真となる．いずれも恒真なので．）

6. • CNF：$(x \vee y \vee z)(x \vee y \vee \bar{z})(x \vee \bar{y} \vee \bar{z})(\bar{x} \vee \bar{y} \vee z)$.
   • DNF：$\bar{x}y\bar{z} \vee x\bar{y}\bar{z} \vee x\bar{y}z \vee xyz$.

7.

x	y	z	$x \oplus y \oplus z$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

8. • $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}[x \geq 0 \Rightarrow y^2 < x]$．偽（$x = 0$ のとき，$y^2 < x$ を満たす $y \in \mathbb{R}$ は存在しない．）
   • $\exists a \in \mathbb{R}, \forall b \in \mathbb{R}[x^2 + ax + b = 0$ が実数解をもつ$]$．偽（任意の $a \in \mathbb{R}$ に対して，b を十分大きくすれば条件は成り立たない．）
   • $\exists b \in \mathbb{R}, \forall a \in \mathbb{R}[x^2 + ax + b = 0$ が実数解をもつ$]$．真（$b = 0$ とすればよい．）
   • $\forall x \in \mathbb{R}, \exists a \in \mathbb{R}[x \in \{y \in \mathbb{R} : |y| < a\}]$．真（$a = |x| + 1$ とすればよい．）
   • $\forall a \in \mathbb{R}, \exists x \in \mathbb{R}[x \in \{y \in \mathbb{R} : |y| < a\}]$．偽（$a = 0$ のとき，任意の $x \in \mathbb{R}$ に対して条件は成り立たない．）

9. 成り立たない．
   • 成り立つ例：$\varphi(x, y) \equiv x \leq y^2$.
   • 成り立たない例：$\varphi(x, y) \equiv x \leq y$.

10. $\varphi \Rightarrow \varphi'$, $A_\varphi \subseteq A_{\varphi'}$.

章末問題

1. (a)：真, (d)：偽, (e)：偽
2.

x	y	z	$(x \oplus y) \Rightarrow z$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

3. (a) $x \vee y$（ド・モルガンの法則＋分配法則）
   (b) $x \wedge y$（ド・モルガンの法則＋分配法則）
   (c) x（ベン図で考える）
   (d) x（ベン図で考える）
   (e) $\overline{x \vee y}$（$\bar{x} \wedge \bar{y}$ でもよい）
   (f) $\overline{x \wedge y}$（$\bar{x} \vee \bar{y}$ でもよい）
   (g) 1
   (h) 1
4. $x\bar{y}\bar{z} \vee \bar{x}y\bar{z} \vee \bar{x}\bar{y}z \vee xyz$.
5. - DNF論理式：$\bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}yz \vee xy\bar{z}$
   - CNF論理式：$(x \vee \bar{y} \vee z)(\bar{x} \vee y \vee z)(\bar{x} \vee y \vee \bar{z})(\bar{x} \vee \bar{y} \vee \bar{z})$
6. 論理式上の二項関係 $R_{\equiv}$ を，$R_{\equiv} = \{(\varphi, \varphi) : \varphi \equiv \varphi'\}$ と定義する．同値関係の定義に従い，$R_{\equiv}$ に対して，反射律，対称律，推移律が成り立つことをそれぞれ示す．
7. $[n] = \{1, 2, \ldots, n\}$（定義 6.1 参照）とすれば，

$$\begin{array}{rcl} x \in A & : & \exists i \in [n][a_i = x] \\ x \notin A & : & \forall i \in [n][a_i \neq x] \end{array}$$

8. (a) $A \subseteq B \stackrel{\text{def}}{=} \forall x \in A\ [x \in B]$
   (b) $A \cup B \stackrel{\text{def}}{=} \{x : (x \in A) \vee (x \in B)\}$
   (c) $A \cap B \stackrel{\text{def}}{=} \{x : (x \in A) \wedge (x \in B)\}$
   (d) 関数 $f : A \to B$ が全射である $\stackrel{\text{def}}{=} \forall b \in B, \exists a \in A\ [f(a) = b]$
   (e) 関数 $f : A \to B$ が単射である $\stackrel{\text{def}}{=} \forall a, a' \in A\ [a \neq a' \Rightarrow f(a) \neq f(a')]$
   (f) 写像 $f : A \to A$ が恒等写像である $\stackrel{\text{def}}{=} \forall a \in A\ [f(a) = a]$
   (g) $R \subseteq A^2$ が同値関係であるとは以下の 3 つの条件を満たすことである．
   - 反射律 $\stackrel{\text{def}}{=} \forall a \in A\ [(a, a) \in R]$
   - 対称律 $\stackrel{\text{def}}{=} \forall a, a' \in A\ [(a, a') \in R \Rightarrow (a', a) \in R]$

- 推移律 $\stackrel{\text{def}}{=} \forall a, b, c \in A\ [(((a, b) \in R) \wedge ((b, c) \in R)) \Rightarrow (a, c) \in R]$

9. $\varphi \Rightarrow \varphi'$, $A_\varphi \subseteq A_{\varphi'}$.

離散数学における証明，再帰

1. $n_0 = 6$ として帰納法により示す.
2. $f(0) = 0$, $f(n) = n + f(n-1)$.
3. $f(0) = 1$, $f(n) = 2f(n-1)$.
4. $\mathbb{E}, \mathbb{O}$ をそれぞれ非負の偶数・奇数の集合としたとき,
   - $0 \in \mathbb{E}$, $n \in \mathbb{E} \Rightarrow n + 2 \in \mathbb{E}$.
   - $1 \in \mathbb{O}$, $n \in \mathbb{O} \Rightarrow n + 2 \in \mathbb{O}$.

整数

1. $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.
2. - $17 = 5 \cdot 3 + 2$.
   - $-17 = (-6) \cdot 3 + 1$.
3. 最後を除いてすべて成り立つ.
4. $b \mod n = b$ であることより示される.
5. ($\Rightarrow$) 与式と $c \equiv_n c$ の辺々を引く．($\Leftarrow$) 与式と $c \equiv_n c$ の辺々を足す.
6. (a) 与式 $b \equiv_n 0$ と $a \equiv_n a$ の辺々を足す.
   (b) 与式 $c \equiv_n 1$ と $a \equiv_n a$ の辺々を掛ける.
7. $nb \equiv_n 0$ であることから，必要性は $ma + nb \equiv_n 1$ との辺々を引くことにより，十分性は $ma \equiv_n 1$ との辺々を足すことにより示される.
8. $i \not\equiv_p 0$ かつ $x \not\equiv_p 0$ より，補題 6.11 の対偶を用いると，$ix \not\equiv_p 0$ となる．よって，$r_i \neq 0$ となり，$r_i \in \mathbb{Z}_p^*$ である．($\equiv_p$ は推移律を満たすから，$r_i \equiv_p 0$ なら ($r_i \equiv_p ix$ より) $ix \equiv_p 0$ なので，その対偶より.)
9. 系 6.12 より，$ix \equiv_p jx$ なら $i \equiv_p j$．よって，$i \neq j$ なら ($i \not\equiv_p j$ より) $ix \not\equiv_p jx$. よって，$r_i \neq r_j$ である．($\equiv_p$ は推移律を満たすから，$r_i \equiv_p r_j$ なら ($r_i \equiv_p ix$, $r_j \equiv_p jx$ より) $ix \equiv_p jx$ なので，その対偶より.)
10. $\gcd(a, b) = 2 \cdot 3$, $\operatorname{lcm}(a, b) = 2 \cdot 3^2 \cdot 5 \cdot 7$.
11. $\gcd(450, 195) = 15$.
12. $\gcd(314, 136) = 2$.
13. $(m, n) = (-3, 7)$.

14. $(m, n) = (13, -30)$.

暗号

1. $(18, 4, 8, 10, 4, 8)$.
2. - $7 \cdot 13 \equiv_{30} 1$ より，$a^{-1} = 7$.
   - $-3 \cdot 30 \equiv_{13} 1$ より $10 \cdot 30 \equiv_{13} 1$．よって，$a^{-1} = 10$.
3. JXTRXT（数字の列では $(9, 23, 19, 17, 23, 19)$.）
4. $(p-1)(q-1) = 24$ を法としたときの $e = 5$ の逆元が $d = 5$ であることを示す．$(e, (p-1)(q-1)) = (5, 24)$ に対してユーグリッドの互除法を適用することにより，$(-1) \cdot 24 + 5 \cdot 5 = 1$．よって，

$$1 \equiv_{24} (-1) \cdot 24 + 5 \cdot 5 \equiv_{24} 5 \cdot 5.$$

5. 命題において，$a = b$, $b = a \bmod n$ とすればよい．つまり，

$$ab \ \equiv_n \ (a \bmod n)b \ = \ b(a \bmod n) \ \equiv_n \ (b \bmod n)(a \bmod n).$$

6. 以下のよう：

$$\begin{aligned} E(5) \ &\equiv_N \ 5^5 \equiv_N 5^3 \cdot 5^2 \equiv_N (5^3 \bmod N) \cdot 5^2 \equiv_N 20 \cdot 5^2 \equiv_N (20 \cdot 5) \cdot 5 \\ &\equiv_N \ 100 \cdot 5 \equiv_N (100 \bmod N) \cdot 5 \equiv_N 30 \cdot 5 \equiv_N 150 \equiv_N 10 \\ E(6) \ &\equiv_N \ 6^5 \equiv_N (6^2 \bmod N) \cdot (6^2 \bmod N) \cdot 6 \equiv_N 1 \cdot 1 \cdot 6 \equiv_N 6. \end{aligned}$$

   更に，$E(5)$ の計算は，以下のようにすることも可能：

$$\begin{aligned} E(5) \ &\equiv_N \ 5^5 \equiv_N 5^2 \cdot 5^2 \cdot 5 \equiv_N 25 \cdot 25 \cdot 5 \equiv_N (-25) \cdot (-25) \cdot 5 \\ &\equiv_N \ 10 \cdot 10 \cdot 5 \equiv_N 500 \equiv_N 10 \end{aligned}$$

章末問題

1. $a^{-1} = 17$.
2. （a）ZPDXPD, $E(x) = 23x + 1 \pmod m$. $D(y) = 17(y-1) \pmod m$.
   （b）TFJLFJ, $E(x) = 27x + 1 \pmod m$. $D(y) = y - 1 \pmod m$.
   （c）略.
3. （a）(0,1,31), $E(M) = M^3 \pmod N$, $D(C) = C^7 \pmod N$.
   （b）(0,1,16), $E(M) = M^7 \pmod N$, $D(C) = C^3 \pmod N$.
   （c）$e = 9$. $E(M) = M^9 \pmod N$, $D(C) = C^9 \pmod N$.

参考図書

本テキストは，離散数学のごく一部（の初歩的なこと）しか扱っていない．（他にも，「グラフ理論」に代表されるよう，「組合せ論」という重要な分野がある．）離散数学について更に学びたい学生は，以下の教科書や，そこであげられている参考図書を参照するとよい．

1. 黒澤 馨，工学のための離散数学，数理工学社，２００８．
2. 守屋 悦朗，離散数学入門，サイエンス社，２００６．

索引