集合・写像・ロジック超入門 2013

関西学院大学　川中　宣明

1　定理とは何か? 数学とは何か?

数学には「定理」というものがある. 定理とは何だろうか? 数学の定理の中でも, 多分, 最も古く（紀元前 500 年か, それ以前), 最も有名な「三平方の定理（＝ピタゴラスの定理)」を例にとって説明しよう. まず, 平面図形について次のことが正しいことは認めよう.

(i)　1 辺の長さが l の正方形の面積は l^2 である.

(ii)　互いに重なり合わない 2 つの平面図形 A, B 全体の面積は

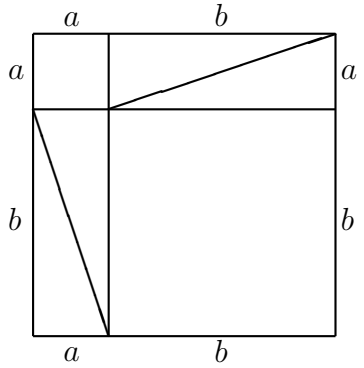
$$(\text{A の面積}) + (\text{B の面積})$$

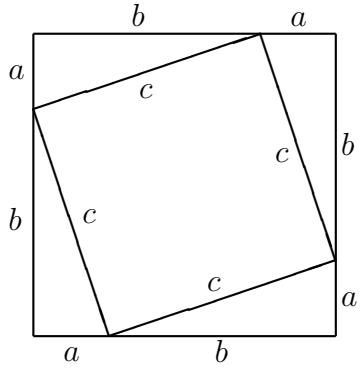
である. 従って, ある平面図形 C から, それに含まれる平面図形 D を除いてできる図形の面積は

$$(\text{C の面積}) - (\text{D の面積})$$

に等しい.

下の 2 つの図を見て欲しい. 左右のどちらの図にも, 1 辺の長さ $a+b$ の正方形の中に直角を挟む 2 辺の長さが a と b であるような直角三角形が 4 つ, 重ならないように配置されている. この直角三角形の斜辺の長さを c としよう.





左右の正方形（1 辺の長さ $a+b$）から, それぞれの内部に図示されている 4 つの直角三角形を取り除こう. 左側の正方形の場合, 残る図形は 1 辺の長さ a の正方形と 1 辺の長さ b の正

方形であり, 右側の正方形の場合は, 残る図形は 1 辺の長さ c の正方形である. よって, 上で「正しい」と認めた (i)(ii) から

$$a^2 + b^2 = c^2$$

という関係式が得られる. これが三平方の定理である.

このように何らかの出発点（この場合は「直角三角形」と (i)(ii)）から, 「全くのあたりまえ」としか言いようのない推論（論理、ロジック）の連鎖により, 驚くような結論（三平方の定理）が導かれる. このように何らかの前提から出発し, ひとつひとつは「全くのあたりまえ」であるようなロジックを積み重ねて, あたりまえでない結論が得られたとき, それを「定理」と呼び, 途中の推論をその定理の「証明」という. 途中の推論は「全くのあたりまえ」だから 100 %正しいと言い切れる. よって得られる結論（定理）も 100 %正しい. だからこそ, 2500 年も前のピタゴラスの定理は今も変わらず正しい. こんなことは数学にしかない. 言い足りない点もあるが, これが数学の仕組みであり, 数学の本質である.

[**無駄話**] 「風が吹けば桶屋（おけや）がもうかる」という古い（江戸時代の？）冗談がある. ほとんどの人は知らないだろうから解説すると

風が吹く⇒ 砂ぼこりが立つ ⇒ 砂が目に入る ⇒ 眼病が増える
⇒ 三味線が売れる（昔は目の不自由な人が音曲で生計を立てることが多かったので）
⇒ 猫が減る（三味線に猫の皮を使うので）⇒ ネズミが増える
⇒ ネズミが桶をかじって穴をあける ⇒ 桶屋がもうかる

というように, 原因と結果の連鎖により, 予想もしないことが起きる, というのである. ひとつひとつは妥当に見える推論を積み重ねると予想外のことが起きる, という点は数学と似ていなくもないが, 数学の場合は途中の推論が疑う余地がないほどの「全くのあたりまえ」で, 特定の時代や場所だけで正しいのでなく, いつでもどこでも正しいのに比べ「風が吹けば」の方は, せいぜい日本のそれもある時代にはそういうことが多かった, という程度の推論の積み重ねであるから, 得られた結論も全く信用できない.

2　なぜ、集合やロジックが重要なのか？

昔の数学の素材は, 数と図形であった. 現代の数学の素材は, 数と集合と写像である.（図形もこれらのもので組み立てるのである.）数と集合と写像は, 建物でいうと木材とか石材とかの建築材料にあたり, 金具とかセメントとかの接着材にあたるのがロジック（論理）である. 文章でいうなら, 単語に相当するのが数と集合と写像で, 文法に相当するのがロジックである. 単語と文法だけ知っていても良い文章は書けないのと同じで, 数学も集合とロジックだけからできているわけではない. しかし, 単語も文法も知らずに外国語の文章を読んだり, 書いたりできないように, これらのことが理解できないと, 今後, 数理科学科で学ぶことは「まったく何も分からなくなる」のは確実である.

高校までに学んだ数学とは全く違う感じがして, 最初はとまどうかもしれない. しかし, 数学を本格的に学ぶことにした以上, ここは避けては通れない. とくに最初が大事だから, 私の話をしっかり聞いてもらいたい. このノートは「板書を筆写する労力を軽減し, その分, 話をしっかり聞いてもらう」というねらいで作成した.

集合にしてもロジックにしても, 一点の間違いもなく厳密に論じようとすると, 結構たいへんであるから, このノートではそういうことはやらない. これから数学を勉強していく人にとって, 最低限必要なことだけに絞って話を進めるつもりである. その結果, 話が「いいかげん」になる箇所も出てくるだろうが, 「いいかげん」でないものを書こうとすると, やたら長くなってしまうので, 多少の妥協はやむを得ないのである.

3　集合, 部分集合, 反例

集合とは何か, というところは本当はかなりたいへん・・・だから, 早速トバシて, 単にモノの集まりということにしておく. 集合 (set) に含まれるモノのことを, その集合の**元** (element) という. （高校教科書では「要素」と呼んでいる. ）集合は A, S などの大文字で, 元は a, x などの小文字で表すことが多い.
「モノ a は A の元である」ということを, 記号で

$$a \in A \quad (\text{ 或いは } \quad A \ni a\ )$$

とかく. 「a は A の元ではない」ということは

$$a \notin A \quad (\text{ 或いは } \quad A \not\ni a\ )$$

とかく. 2つの集合 A, B に対し, B の元がすべて A の元でもあるとする. つまり

$$x \in B \Longrightarrow x \in A \tag{1}$$

上の (1) 式は「x が B の元ならば, x は A の元である」とよむ. より丁寧にいえば

「x が B の**任意の**元ならば, x は**必ず** A の元である.」

「任意の元」は「どんな元かは知らないが, どんな元を選んだとしても」という意味で, 日常生活ではほとんど使わないが大学の数学では多用されるフレーズなので覚えておくこと.

(1) が成り立つとき, B は A の**部分集合**（subset）であるといい, 記号では

$$B \subset A \quad (\text{ 或いは } \quad A \supset B\ ) \tag{2}$$

とかく. つまり (2) の**定義**が (1) である. 「定義」とは, 用語や記号の意味のことだが, 数学の場合はとくに「あいまいさも例外もない, 厳密な意味」のことである.

[**注意**] 記号 $\in$ と記号 $\subset$ を混同してはいけない. 例えば, 集合 B が集合 A の部分集合であるときに, $B \in A$ と書いてはいけない. また, a が A の元であるときに, $a \subset A$ と書いてもいけない.
また,「(1) と (2) が同じ意味」というのを誤解し,「記号 $\subset$ と記号 $\Longrightarrow$ が同じ意味」と思い込む人がいるようだが, これも間違いである. (2) と書く代わりに $B \Longrightarrow A$ と書いてはいけない. また (1) と書く代わりに　$x \in B \subset x \in A$　と書くのもいけない.

あたりまえのことだが「x は A の元 $\Longrightarrow$ x は A の元」である。(2) の定義が (1) なのだから, どんな集合 A についても

$$A \subset A$$

ということになる. つまり, A 自身も A の部分集合である.
「何も元がない」空っぽの集合も考える. これを**空集合**（くうしゅうごう, empty set）と呼び, 記号 $\emptyset$ で表す. どんな集合 A に対しても

$$\emptyset \subset A.$$

すなわち, どんな集合をもってきても, 空集合はその部分集合である. これは必然的なことなのだが, 今は「そういうことになっている」と考えておいて差し支えない.

数学に良く出てくる集合には特別の記号が割り当てられている. 例えば「整数全体の集合」は $\mathbb{Z}$ で,「有理数全体の集合」は $\mathbb{Q}$ で,「実数全体の集合」は $\mathbb{R}$ で表すことになっている. 有理数とは, 整数 m, n を用いて

$$\frac{m}{n}$$

と書けるような数である. （もちろん $n \neq 0$. ）これが「有理数の定義」である. このことから

$$\frac{1}{3} \in \mathbb{Q}, \quad -\frac{2}{5} \in \mathbb{Q}$$

などが分かる. 実数のうちで, 有理数でないもののことを, 無理数という. よって, a が実数のとき $a \notin \mathbb{Q}$ と書けば,「a は無理数である」というのと同じ意味になる. また

$$m \in \mathbb{Z} \implies m = \frac{m}{1} \in \mathbb{Q} \tag{3}$$

が分かる. よって $\mathbb{Z} \subset \mathbb{Q}$ が正しいことが分かった. (3) のように「・・・ $\Longrightarrow$ ＊＊＊ 」（・・・ ならば ＊＊＊ である）という形の数学的な文章のことを**命題**といい, ・・・の部分をこの命題の**条件**（または**仮定**）, ＊＊＊ の部分のことをこの命題の**結論**という. 命題が「・・・ $\Longrightarrow$ ＊＊＊ 」の形をしていないこともあるが, そのときでも殆どの場合にはこの形に書き直せる. 例えば「$\sqrt{2}$ は無理数である. 」という命題は

$$a \in \mathbb{R}, \ \ a^2 = 2 \implies a \notin \mathbb{Q} \tag{4}$$

と書け, こちらの方が意味がはっきりする.

政治の世界では「正しい」とは「選挙で勝つこと」あるいは「多数決で勝つこと」である. 物理や化学の世界では「正しい」とは「実験でそうなっていることが示されること」である. 数学の世界では, 命題が「正しい」とは「条件から結論を論理的に導くことができる（証明できる）こと」である. 従って, 数学の命題は何千年も前に証明されたもの（例えば, 命題 (4) やピタゴラスの定理）であっても, 現在もこれからも変わらず正しい. また, 数学で「正しい（真である）」とは唯一つの例外もなく完璧に正しいことをいう. もし, たった 1 つでも例外があれば, その命題は「正しくない（偽である）」という. そのような例外のことを, その命題の**反例**という. ある命題が正しいことを示すには, （正しい例を幾つあげてもダメで）証明しなければならない. しかし, ある命題が正しくないことを示すには, 反例を 1 つ示せばそれで十分である.

例題 1 $a, b \in \mathbb{R}$ とする. 次の命題の真偽を確定せよ.
(i) $a, b \in \mathbb{Q} \implies a+b \in \mathbb{Q}$
(ii) $a, b \notin \mathbb{Q} \implies a+b \notin \mathbb{Q}$

(例題 1 の解答例) (i) 真である. 証明は以下の通り. $a, b \in \mathbb{Q}$ であるから $a = \frac{m}{n}$, $b = \frac{m'}{n'}$ となる整数 m, n, m', n' がとれる. （ただし, $n \neq 0$, $n' \neq 0$.）このとき, $a+b = \frac{m}{n} + \frac{m'}{n'} = \frac{mn'+m'n}{nn'}$ であるから $a+b \in \mathbb{Q}$ である.
(ii) 偽である. $a = \sqrt{2}, b = -\sqrt{2}$ とすると, $a, b \notin \mathbb{Q}$ なのに $a+b = 0 \in \mathbb{Q}$ となるから, この場合, 命題が成り立たない. （つまり $a = \sqrt{2}, b = -\sqrt{2}$ は反例である.）

「・・・ $\implies$ ＊＊＊」という命題の証明を書くときは：
上の例題 1(i) の証明のように,「・・・であるから」と書き始め, 次々と論理的に書き進めて, 最後は「よって ＊＊＊である」と締めくくるのが基本型である. この形でない証明として高校でも学んだ「背理法による証明」や「対偶による証明」がある. これらについては, 後で説明する.

また「・・・ $\implies$ ＊＊＊」という命題の反例は：
上の例題 1(ii) のときのように「 ・・・ という条件は成り立っているのに, ＊＊＊ という結論は成り立っていない」ような具体例のことである.

次のことが成り立つ.（ 図を描いてみよう. ）

$$A \subset B,\ B \subset C \implies A \subset C \tag{5}$$

図で納得するだけでは論理的とは言えない. きちんと証明しておこう.

（命題 (5) の証明）条件の $A \subset B$ と $B \subset C$ を用いて, 結論の $A \subset C$ を導けばよい. まず最初の仮定 $A \subset B$ から

$$a \in A \Longrightarrow a \in B. \tag{6}$$

もう一つの仮定 $B \subset C$ から

$$a \in B \Longrightarrow a \in C. \tag{7}$$

(6) と (7) から

$$a \in A \Longrightarrow a \in C$$

が従う. よって $A \subset C$ である. （証明終）

高校の数学は「アマチュアの数学」である. 大学の数理科学科では「プロフェッショナルの数学」を学ぶ. アマとプロの一番の違いは, プロではルールが厳格なことである. 数学のルールは「ロジック（論理）に忠実であること」. 上の証明の場合, (2) 式の定義が (1) であることを使って, きちんとロジックに従って結論を導いている. アマなら「(図を描いて) 図より明らか」としてもよいし「$A \subset B$ より A が B の部分で, $B \subset C$ より B は C の部分. よって, A は C の部分, つまり $A \subset C$」でもよいが, これではプロの証明とは言えないのである.

$A \subset B$ と $A \supset B$ が共に成り立つとき, つまり

$$x \in A \Longleftrightarrow x \in B \tag{8}$$

（「 $x \in A \Longrightarrow x \in B$ 」と「$x \in B \Longrightarrow x \in A$ 」が共に成立）

のとき, 2 つの集合 A と B は**等しい**といい, 記号で

$$A = B \tag{9}$$

とかく. つまり, (9) の定義は (8) である.
既に述べたように $A \subset B$ とかくと $A = B$ の場合も含まれてしまう. そこで $A \subset B$ であるが, $A = B$ ではない と強調したいときには, とくに A は B の**真部分集合**（proper subset）であるといい, 記号で $A \subsetneqq B$ とかく.
集合はその元をリストアップして表すことができる. 例えば

$$A = \{-3, 0, 1, 2\}, \quad B = \{-3\}$$

なら, A は -3,0,1,2 という 4 個の元からなる集合であり, B は -3 というただ 1 個の元からなる集合である. このとき

$$-3 \in B, \quad \{-3\} \subset A, \quad -3 \in A$$

などが成り立つ. $\{-3\}$ はただ 1 個の元をもつ 集合 であるから, $\{-3\} \in A$ ではなく, $\{-3\} \subset A$ と書かなくてはいけない. リストの順序が違ったり, ダブっているときでも (8) が成り立てば同じ集合である. 例えば $\{-3, 0, 1, 2\} = \{1, 2, -3, 0, 1, 2\}$.
リストアップによる表し方は元の個数が有限, それも比較的少数の場合しか使えない. より有効な別の表し方を説明しよう.
開き括弧 { と閉じ括弧 } の間を縦棒 | で区切り, 縦棒 | の左側にはその集合の元を代表的に表す記号をかき, 縦棒 | の右側にはその記号で表される元が今考えている集合に含まれるための必要十分条件をかくのである. 例えば

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

によって, $\mathbb{Z}$ が整数全体の集合であることを表す. 同様に

$$\mathbb{Q} = \{a \mid a \text{ は有理数 }\}, \quad \mathbb{R} = \{r \mid r \text{ は実数 }\}$$

である. また,

$$\mathbb{N} = \{n \mid n \text{ は自然数 }\}, \quad \mathbb{C} = \{a \mid a \text{ は複素数 }\}$$

も意味が固定されている記号である. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ である.

[注意] 「自然数」は日本の高校教科書では正の整数と同じ意味だが, 0 以上の整数と同じ意味で使う数学者も（多数）いる. このノートでは高校の教科書と同じように「自然数＝正の整数」としておく.

上の注意にかいたことを記号では

$$\mathbb{N} = \{n \mid n \in \mathbb{Z},\, n > 0\}$$

と表すことができる. 縦棒の右に 2 つの条件をカンマ , で区切ってかくと, 「それらの条件をすべて満たす」という意味になる. 同じことを

$$\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}$$

とかくこともできる. 一般に, 今, 考えようとしている集合 A が既に定義されている集合 S の部分集合である場合には

$$A = \{s \in S \mid (s \text{ が } A \text{ にふくまれるための必要十分条件 })\}$$

と, 縦棒の右側に S の元 s が A の元であるための必要十分条件をかくことで A を表すことができる. 例えば

$$\{r \in \mathbb{R} \mid r \notin \mathbb{Q}\}$$

は無理数全体の集合を表す. (これを$\{r \notin \mathbb{Q} \mid r \in \mathbb{R}\}$ とかいてはいけない.) 方程式 $x^2+x+1=0$ の実数解の全体の集合は

$$\{x \in \mathbb{R} \mid x^2+x+1=0\},$$

同じ方程式の複素数解全体の集合は

$$\{x \in \mathbb{C} \mid x^2+x+1=0\}$$

で表すことができる. 高校で学んだように

$$\{x \in \mathbb{R} \mid x^2+x+1=0\} = \emptyset, \quad \{x \in \mathbb{C} \mid x^2+x+1=0\} = \{\frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\}$$

である.「方程式を解け」という問題は 正確には「解全体の集合を求めよ」という意味だったのである.
また

$$\{a \in \mathbb{R} \mid 0 \leq a \leq 1\}$$

は閉区間 [0,1] と同じ意味になる. つまり

$$[0,1] = \{a \in \mathbb{R} \mid 0 \leq a \leq 1\}$$

である. ($\leq$ と $\leqq$ は同じ意味の記号である.) 端を入れる区間は閉区間といい, 端を入れない区間は開区間という. 開区間は丸括弧 (,) を用いて表す. 例えば開区間 $(-1,1)$, 半開区間 $(1,5]$ は

$$(-1,1) = \{r \in \mathbb{R} \mid -1 < r < 1\}, \quad (1,5] = \{c \in R \mid 1 < c \leq 5\}$$

で定義される. 上で説明するのをうっかりして忘れていたが, 記号

$$A \not\subset B \quad (\text{ 或いは } \quad B \not\supset A)$$

は「A は B の部分集合ではない」, つまり「$a \in A$ であると同時に $a \notin B$ でもあるような a が存在する」という意味である. 例えば, $-1 \in [-1,1]$ であり $-1 \notin [0,2]$ であるから

$$[-1,1] \not\subset [0,2]$$

である.

4 合併, 交わり, または, かつ

2つの集合 A, B の**合併** (union) $A \cup B$ を

$$A \cup B = \{x \mid x \in A \ \underline{\text{または}} \ x \in B\} \tag{10}$$

で定義する. すなわち, $A \cup B$ は A か B の 少なくとも一方には 含まれるような元の集まりである. これに対し, A と B の**交わり** (intersection) $A \cap B$ は

$$A \cap B = \{x \mid x \in A \ \text{かつ} \ x \in B\} \tag{11}$$

で定義する. すなわち, $A \cap B$ は A と B の 両方に 含まれるような元の集まりである. よって

$$A \cap B = \emptyset$$

とかけば, A と B には共通の元はない, という意味になる. 例えば

$$(-2, 1) \cup (0, 3] = (-2, 3], \quad (-1, 2) \cap [2, 3] = \emptyset$$

である.

[**重要な注意**] 「または」と「かつ」の使い方は重要である. 数学で 2 つの命題（あるいは条件）$\mathcal{P}, \mathcal{Q}$ を並べて「$\mathcal{P}$ または $\mathcal{Q}$ （$\mathcal{P}$ or $\mathcal{Q}$)」といえば「$\mathcal{P}$ と $\mathcal{Q}$ の 少なくとも一方（が成り立つ)」という意味であり, 「$\mathcal{P}$ かつ $\mathcal{Q}$（$\mathcal{P}$ and $\mathcal{Q}$)」といえば「$\mathcal{P}$ と $\mathcal{Q}$ の 両方（が成り立つ)」という意味である.

[**半ば無駄, 半ば本気の話**] 日常生活で使われる「または」と数学で使われる「または」は意味が違うことがある. 例えば, レストランで「食後に, コーヒーまたは紅茶がつきますが, どうなさいますか？」とお店の人に尋ねられたとき「両方とも!」とは普通は言わない. しかし, 数学で「$\mathcal{P}$ または $\mathcal{Q}$」というときには, 「$\mathcal{P}$ と $\mathcal{Q}$ の 少なくとも一方（が成り立つ)」という意味だから, 両方とも成り立つ場合も含まれている のである.

合併の定義 (10) は次のように言い換えられる.

$$x \in A \cup B \iff x \in A \text{ または } x \in B \tag{12}$$

同様に共通部分の定義 (11) は次のように言い換えられる.

$$x \in A \cap B \iff x \in A \text{ かつ } x \in B \tag{13}$$

集合 A, B, C と $\cup$ や $\cap$ を含む簡単な関係式を幾つか挙げておこう.

$$A \cup A = A, \quad A \cap A = A \tag{14}$$

$$A \subset A \cup B, \quad A \cap B \subset A \tag{15}$$

$$A \cup B = B \cup A, \quad A \cap B = B \cap A \quad \text{(可換法則)} \tag{16}$$

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C \quad \text{(結合法則)} \tag{17}$$

すべて「自明」に近いものばかりであるが, 幾つか選んで証明しておこう. ほかのものは自分で証明しておくこと.

[(15) の第二式　$A \cap B \subset A$ **の証明**]

$x \in A \cap B$ とする. (11) により, このことは $x \in A$ かつ $x \in B$ と言い換えられる. よって, $x \in A$ である. 従って

$$x \in A \cap B \Longrightarrow x \in A$$

となる. つまり $A \cap B \subset A$ である. （証明終）

[(17) の第一式　$A \cup (B \cup C) = (A \cup B) \cup C$ **の証明**]

(10) により, 左辺は

$$\{x \mid x \in A \text{ または } x \in B \cup C\} = \{x \mid x \in A \text{ または } x \in B \text{ または } x \in C\}$$

に等しい. 同様に, 右辺は

$$\{x \mid x \in A \cup B \text{ または } x \in C\} = \{x \mid x \in A \text{ または } x \in B \text{ または } x \in C\}$$

に等しい. よって, 左辺＝右辺である.　（証明終）

次のことも成り立つ.

$$A \subset B \cap C \iff A \subset B \quad \text{かつ} \quad A \subset C \tag{18}$$

[(18) の**証明**] まず、最初に $A \subset B \cap C$ と仮定する. (15) により, $B \cap C \subset B$ であるから, $A \subset B \cap C \subset B$ となる. よって, (5) により $A \subset B$ が得られる. 同様にして $A \subset C$ も得られる. よって

$$A \subset B \cap C \implies A \subset B \quad \text{かつ} \quad A \subset C$$

が証明された. 次に「$A \subset B$ かつ $A \subset C$」と仮定しよう. $a \in A$ とすると, $A \subset B$ により $a \in B$ が成り立ち, $A \subset C$ により $a \in C$ も成り立つ. よって, $a \in A$ のとき $a \in B \cap C$ である. つまり, $A \subset B \cap C$ となる. これで

$$A \subset B \quad \text{かつ} \quad A \subset C \implies A \subset B \cap C$$

が証明され (18) の証明が完成した.　（証明終）

[**注意**] 上の証明からも分かるように, 一般に 2 つの命題（あるいは条件）$\mathcal{A}$, $\mathcal{B}$ に対して

$$\mathcal{A} \Longleftrightarrow \mathcal{B}$$

のタイプのことを証明するには, まずどちらか一方の向きの矢印（$\mathcal{A} \Longrightarrow \mathcal{B}$（$\mathcal{A}$ を仮定して $\mathcal{B}$ を示す）または $\mathcal{A} \Longleftarrow \mathcal{B}$（$\mathcal{B}$ を仮定して $\mathcal{A}$ を示す））を証明し, 続いて残っている方を証明する, という手順を踏むことが多い.

上で証明した (18) は前に出てきた (13)（$=$ $\cap$ の定義）と見かけが似ている. さて, それでは一見 (12)（$=$ $\cup$ の定義）と似た感じの

$$A \subset B \cup C \iff A \subset B \quad \text{または} \quad A \subset C \tag{19}$$

は正しいだろうか？

例題 2 次の命題の真偽を確定せよ.
(i) $A \subset B \cup C \impliedby A \subset B$ または $A \subset C$
(ii) $A \subset B \cup C \implies A \subset B$ または $A \subset C$
(iii) $A \subset B \cup C \iff A \subset B$ または $A \subset C$

（解答例）(i) 真である. 「$A \subset B$ または $A \subset C$」とする. つまり $A \subset B$ か $A \subset C$ のうち, 少なくとも一方は成り立つ. $a \in A$ とする. $A \subset B$ が成り立つなら $a \in B$ であるし $A \subset C$ が成り立つなら $a \in C$ である. 従って $a \in B$ か $a \in C$ の少なくとも一方は成り立つ. よって $a \in B \cup C$ である. よって $A \subset B \cup C$ である.
(ii) 偽である. $A = [-1, 1]$, $B = [-2, 0]$, $C = [0, 2]$ とすると $B \cup C = [-2, 2]$ であるから, 確かに $A \subset B \cup C$ であるが, $A \not\subset B$ であり $A \not\subset C$ であるから「$A \subset B$」と「$A \subset C$」のどちらも成り立たない. つまり「$A \subset B$ または $A \subset C$」は成り立たない.
(iii) 偽である. 既に (ii) が偽であることを示したから.

例題 3 次の範囲を数直線上に図示せよ.
(i) $(x-1)(x-3) < 0$ であるような実数 x の範囲.
(ii) $(x-2)(x-4) > 0$ であるような実数 x の範囲.

(解答例) (i) 一般に 2 つの実数の積が負になるのは, 2 数のどちらか一方が正, 他方が負になるときだから

$$(x-1)(x-3) < 0 \Leftrightarrow (x-1 > 0 \text{ かつ } x-3 < 0) \text{ または } (x-1 < 0 \text{ かつ } x-3 > 0)$$

である. ところが $(x-1 < 0$ かつ $x-3 > 0)$ となる実数 x はない. よって

$$(x-1)(x-3) < 0 \Leftrightarrow x-1 > 0 \text{ かつ } x-3 < 0$$

となる. よって $x > 1$ と $x < 3$ の 共通部分, つまり $1 < x < 3$ の範囲を図示すればよい. (図は省略する.)
(ii) 一般に 2 つの実数の積が正になるのは, 2 数がともに正か, ともに負の場合であるから

$$(x-2)(x-4) > 0 \Leftrightarrow (x-2 > 0 \text{ かつ } x-4 > 0) \text{ または } (x-2 < 0 \text{ かつ } x-4 < 0)$$

である. ところが $(x-2 > 0$ かつ $x-4 > 0)$ という条件は $x > 4$ と同じことであり, また

$(x-2<0$ かつ $x-4<0)$ は $x<2$ と同じことである. よって

$$(x-2)(x-4)>0 \Leftrightarrow x>4 \text{ または } x<2$$

となる. よって $x>4$ の範囲と $x<2$ の範囲の 合併 を図示すればよい. (図は省略する.)

[**注意**] 1. 例題 3 の解答例では高校の「数学 I」にある「2 次不等式の解法」を敢えて論理的に扱ってみた. 高校教科書で習ったのはグラフを使った直観的な解法であった. 上の方法は論理的であるために, 多少, メンドクサイと感じるかもしれないが, ずっと広い範囲の問題に適用できる優れた方法なのである.
2. 高校の教科書では例題 3 の 2 次不等式の解を「$x<2, x>4$」(あるいは「$x<2, 4<x$」) のように書いているが, これは本来は「$x<2$ または $x>4$」と書くべきである. 高校では論理をあまり厳格には教えないという方針なので, 高校教科書ではここのところを (教育的配慮により)「ごまかす」ことにしているのである.

演習問題 次の範囲を数直線上に図示せよ.
(i) $(x-1)(x-3)>0$ かつ $(x-2)(x-4)\leq 0$ であるような実数 x の範囲.
(ii) $(x-1)(x-3)>0$ または $(x-2)(x-4)\leq 0$ であるような実数 x の範囲.

5 否定と補集合

数学には「・・・でない」という否定文 (あるいはそれを表す式) が良く出てくる. 例えば, このノートの中にも

「a, b が有理数で ない なら $a+b$ も有理数で ない, という命題は偽である」
(5 ページ例題 1(ii)),

「方程式 $x^2+x+1=0$ は実数解を持た ない」 (8 ページ, 7 行目の左側の式)

などが既に現れている. 数学を学んだり使ったりする上では「否定」をよく理解しておく必要がある. 別に難しいことではない. 「否定」の基本法則は次の 2 つである.

1. (・・・ または ＊＊＊) の否定 ＝ (・・・ でない, かつ ＊＊＊ でない)
2. (・・・ かつ ＊＊＊) の否定 ＝ (・・・ でない, または ＊＊＊ でない)

要するに, 否定をとるとき「かつ」と「または」が入れ替わるという法則である. これを**ド・モルガン** (de Morgan) **の法則**という.

[**非数学的な例**] ある人が (「甘いものが好き」かつ「辛いものが好き」) とは「甘いものも, 辛いものもどちらも好き」という意味であるから, これの否定は (「甘いものが好きでない」または「辛いものが好きでない」), つまり「甘いものか, 辛いもののうち, 少なくとも一方は好きでない」ということになる. また, ある人が (「サッカーの選手である」または「水泳の選手である」) とは「サッカーか, 水泳の少なくとも一方の選手」ということだから, これの否定は (「サッカーの選手でない」かつ「水泳の選手でない」), つまり「サッカーの選

手でもなく, 水泳の選手でもない」ということになる.

ある集合 U を一つ決めておいて, その元や部分集合だけを考えることがよくある（というか, ほとんどがそうである）. そのとき最初にとった集合 U のことを**全体集合** (universal set) という. 例えば, 実数について考えているときは $U = \mathbb{R}$ とし, 整数の話をしているときは $U = \mathbb{Z}$ とする, といった具合である.
全体集合が定められているとき, 集合 $A\,(\subset U)$ に対して, その**補集合**（complement）A^c を

$$A^c = \{u \in U \mid u \notin A\} = (A \text{ の元でないような } U \text{ の元}) \text{ の全体}$$

で定義する. よって, 補集合の意味は全体集合 U のとり方によって変わる. 次の 2 式は前ページに出てきたド・モルガンの法則を集合のことばで言いなおしたものである. （こちらも**ド・モルガンの法則**という. 区別したければ, 前ページのは「論理のド・モルガン法則」, 下のは「集合のド・モルガン法則」と言えばよい. ）

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c \tag{20}$$

(20) の第 1 式の左辺は

$$\{x \in U \mid (x \in A \text{ または } x \in B) \text{ でない } \}$$

という意味である. これは論理のド・モルガン法則によって

$$\{x \in U \mid x \notin A \ \text{ かつ } \ x \notin B\}$$

に等しいが, (11) により上式は $A^c \cap B^c$ と同じものである. よって (20) の第 1 式が証明された.

演習問題 (20) の第 2 式を証明せよ.

数学においては
1. ある命題とその否定がともに成り立つことはない. (「・・・であり, しかも・・・でない」ということは決してない.)
2. ある命題が成り立つか, またはその否定が成り立つかのどちらかである. (しかし, 成り立つのがどちらなのか, は分からないかもしれない.)
3. ある命題の否定の否定は元の命題である. ((・・・ でない）でない ＝ ・・・ である.)

これらのことに対応して, 集合 A ($\subset U$) に対して, 次の式が成り立つ.

$$A \cap A^c = \emptyset, \qquad A \cup A^c = U, \qquad (A^c)^c = A \tag{21}$$

例えば, (21) の最初の式は上の 1 に対応し「A の元であり, かつ A 元でない（U の）元はない」という意味である. その次の式は 2 に対応し「(U の）任意の元は A の元か, そうでな

いかのどちらかである」という意味である. 生物の世界には, ある観点からは動物だが, 別の観点からはそうでないものもいるらしいが, 数学ではそういうものがいないような世界を扱うのである. (21) の最後の式は, もちろん 3 に対応する.

さて, 次に, 「否定」と「または」を使えば「・・・ であるならば ＊＊＊ である」の「ならば」という言葉や「・・・ （である）$\Longrightarrow$ ＊＊＊ （である）」の $\Longrightarrow$ という記号が 消去できる（不必要になる）, という話をしよう. 「**そんなバカな！**」と思わず, まあ聞いて欲しい. 命題

$$\text{・・・ （である）} \Longrightarrow \text{ ＊＊＊ （である）} \tag{22}$$

は言うまでもなく, 「・・・ であるならば ＊＊＊ である」という意味だが, そもそも

(a) ・・・ でない,

(b) ・・・ である,

のどちらかが成り立つ. （このことは前ページの 2 で述べた. 繰り返すが, 数学はそういう世界なのである. ）そして, 元の命題 (22) は, (b) のとき ＊＊＊ である, と主張している. よって, 命題 (22) は

$$\text{((a) のとき)・・・ でない, または （((b) のとき）＊＊＊ である}$$

と同じことを言っているのである. これで (22) は

$$\text{・・・ でない, または ＊＊＊ である} \tag{23}$$

と同じであることが分かり, $\Longrightarrow$ が消去できたことになる.
さて, (23) は（前後を入れ替えて）次のように書き換えることができる.

$$\text{＊＊＊ である, または ・・・でない} \tag{24}$$

これは, 前ページの 3 を使えば, 次のように書き換えられる.

$$\text{（＊＊＊ でない）でない, または ・・・でない} \tag{25}$$

そして, (22) $\Leftrightarrow$ (23) を（逆の向きに）使って (25) を書き直すと

$$\text{＊＊＊ でない} \Longrightarrow \text{ ・・・でない} \tag{26}$$

となる. (22) $\Leftrightarrow$ (23) $\Leftrightarrow$ (24) $\Leftrightarrow$ (25) $\Leftrightarrow$ (26) だから, 元の命題 (22) と最後に得られた命題 (26) は論理的には全く同じ内容である. (26) のことを (22) の**対偶**という. （逆に, (26) の対偶は (22) である. ）命題 (22) が成り立てば, その対偶 (26) も成り立ち, 逆に (26) が成り立てば元の命題 (22) も成り立つ.

例題 4 集合 $A, B \subset U$ に対し

$$A \subset B \Longleftrightarrow B^c \subset A^c \tag{27}$$

であることを証明せよ.

（解答例）「$A \subset B$」は 「$x \in A \Longrightarrow x \in B$」という意味である. この対偶は「$(x \in B)$ でない $\Longrightarrow (x \in A)$ でない 」, つまり「$x \notin B \Longrightarrow x \notin A$」, つまり「$x \in B^c \Longrightarrow x \in A^c$」, つまり「$B^c \subset A^c$」である. すなわち,「$A \subset B$」の対偶が「$B^c \subset A^c$」である. よって, (27) が成り立つ. （証明終）

演習問題 $s \in \mathbb{R}$ とし, $t \in \mathbb{Q}$ とする. 次のことを証明せよ.

$$s \text{ は無理数} \implies s+t \text{ は無理数} \tag{28}$$

(ヒント：対偶を証明すればよい.)

6 分配法則

「・・・ または ＊＊＊ または ＃＃＃ 」などと幾つも「または」を続けると 「・・・と ＊＊＊と ＃＃＃ のうちの最低 1 つは成り立つ」という意味になる. 同様に「・・・ かつ ＊＊＊ かつ ＃＃＃」は「 ・・・と ＊＊＊と ＃＃＃ のどれもが成り立つ」 という意味である. このように「または」だけ, あるいは「かつ」だけを, たくさん並べたときの意味ははっきりしていて混乱が起きる心配はない. しかし, 11 ページの例題 3 の解答のように「または」と「かつ」が混合すると, 括弧をつけないと意味がはっきりしなくなる. これは $a+b+c+\cdots$ や $a \times b \times c \times \cdots$ のように, 1 種類だけの演算が繰り返される場合には括弧はなくても混乱は起きないが, 2 種類の演算が混じっているとき（例えば $(a+b) \times c$ や $a+b \times c$ など）においては ($+$ と $\times$ の優先順位を決めるための）括弧または規則が必要になるのと同じである. 基本となるのは次の 2 つの法則である. これらを（論理の）**分配法則**という. 数の分配法則 $a \times (b+c) = a \times b + a \times c$ と良く似た形をしている.

1. ・・・ かつ (＊＊＊ または ＃＃＃)
   = (・・・ かつ ＊＊＊) または (・・・ かつ ＃＃＃)
2. ・・・ または (＊＊＊ かつ ＃＃＃)
   = (・・・ または ＊＊＊) かつ (・・・ または ＃＃＃)

[**非数学的な例**] ある会社では

1. 「コンピュータに精通している」かつ (「英語が話せる」 または 「中国語が話せる」)

という人材を募集しているとする. これは

(「コンピュータに精通している」かつ「英語が話せる」)

または

(「コンピュータに精通している」かつ「中国語が話せる」)

という人材を募集しているというのと同じである. また

2. 「コンピュータに精通している」または (「英語が話せる」 かつ 「中国語が話せる」)

という人材を募集しているとするなら, それは
(「コンピュータに精通している」または「英語が話せる」)
かつ
(「コンピュータに精通している」または「中国語が話せる」)
という人材を募集しているというのと論理的には全く同じことである.

論理の分配法則に対応して, 集合 A, B, C については, 次の 2 つの等式が成り立つ. これらも（集合の）**分配法則**という.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{29}$$

例題 5 (29) の第 1 式を論理の分配法則から導け.

（解答例）$A \cap (B \cup C)$
$= \{x \mid x \in A \quad \text{かつ} \quad x \in B \cup C\}$ ($\cap$ の定義)
$= \{x \mid x \in A \quad \text{かつ} \quad (x \in B \quad \text{または} \quad x \in C)\}$ ($\cup$ の定義)
$= \{x \mid (x \in A \quad \text{かつ} \quad x \in B) \quad \text{または} \quad (x \in A \quad \text{かつ} \quad x \in C)\}$ (分配法則)
$= \{x \mid x \in A \cap B \quad \text{または} \quad x \in A \cap C\}$ ($\cap$ の定義)
$= (A \cap B) \cup (A \cap C)$ ($\cup$ の定義) (証明終)

演習問題 (29) の第 2 式を論理の分配法則から導け.

A と B の**差集合** (difference set) $A \setminus B$ は

$$A \setminus B = \{a \in A \mid a \notin B\} \tag{30}$$

で定義する. すなわち, $A \setminus B$ は A の元のうち B に含まれないようなもの全体からなる集合である. （$A - B$ とかく人もいる. ）例えば

$$(-2, 3) \setminus [-1, 1] = (-2, -1) \cup (1, 3)$$

である. 全体集合 U を考えれば

$$A \setminus B = A \cap B^c \tag{31}$$

と定義することもできる. こちらの定義の方が便利なことも多い.

例題 6 3 つの集合 A, B, C についての次の等式を証明せよ.

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

（解答例）$A \setminus (B \cap C) = A \cap (B \cap C)^c$ (差集合の定義)
$= A \cap (B^c \cup C^c)$ (ド・モルガンの法則)

$$= (A \cap B^c) \cup (A \cap C^c) \quad (\text{ 分配法則 })$$
$$= (A \setminus B) \cup (A \setminus C) \quad (\text{ 差集合の定義 }) \qquad (\text{証明終})$$

演習問題 2 つの集合 A, B についての次の等式を証明せよ.

$$(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

7 「任意の (for any)」と「存在する (there exists)」

2 つの集合の合併や交わりについては, 7 ページで述べた. 3 個の集合 A_1, A_2, A_3 について, (17) 式で述べたように

$$(A_1 \cup A_2) \cup A_3 = A_1 \cup (A_2 \cup A_3), \quad (A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3)$$

が成り立つ. これらの式は 3 個の集合の**合併**

$$\bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3 \tag{32}$$

や 3 個の集合のの**交わり**

$$\bigcap_{i=1}^{3} A_i = A_1 \cap A_2 \cap A_3 \tag{33}$$

を考えるとき, 括弧をどこにつけても意味が変わらないということ, つまりこれらの式には括弧をつける必要がないことを言っている. 集合 (32) は, A_1, A_2, A_3 のうち少なくともひとつには含まれる ような元全体の集合のことである. また, 集合 (33) は, A_1, A_2, A_3 の どれにも共通に含まれる ような元全体の集合のことである. これらの集合はまた

$$\bigcup_{i=1}^{3} A_i = \{a \mid a \in A_i \text{となる } (1 \text{ 以上 } 3 \text{ 以下の }) \ i \text{ が 存在する }\},$$

$$\bigcap_{i=1}^{3} A_i = \{a \mid (1 \text{ 以上 } 3 \text{ 以下の }) \text{ 任意の } i \text{ に対して } a \in A_i\}$$

と「**存在する** (there exists)」や「**任意の** (for any)」という「数学語」を使って言い表すことができる. 一般に n を自然数とし, n 個の集合 $A_1, A_2, \ldots A_n$ を考えたときでも $A_1 \cup A_2 \cup \cdots \cup A_n$ や $A_1 \cap A_2 \cap \cdots \cap A_n$ にどのように括弧をつけても全て同じ意味で

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$
$$= \{a \mid a \in A_i \text{となる } (1 \text{ 以上 } n \text{ 以下の }) \ i \text{ が 存在する }\},$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$
$$= \{a \mid (1 \text{ 以上 } n \text{ 以下の}) \underline{\text{任意の}}\ i \text{ に対して } a \in A_i\}$$

となる. 上の $\bigcup_{i=1}^{n} A_i$ や $\bigcap_{i=1}^{n} A_i$ は $I = \{1, 2, \ldots, n\}$ とおいて

$$\bigcup_{i \in I} A_i, \qquad \bigcap_{i \in I} A_i$$

とかくこともできる. さらに $I = \mathbb{N}$ あるいは $I = \mathbb{R}$ など, I が無限集合のときでも, おのおのの $i \in I$ に対して集合 A_i が決まってさえいれば, 集合の集まり A_i $(i \in I)$ に対して, それらの合併 $\bigcup_{i \in I} A_i$ や共通部分 $\bigcap_{i \in I} A_i$ を考えることができて

$$\bigcup_{i \in I} A_i = \{a \mid a \in A_i \text{ となる } i \in I \text{ が } \underline{\text{存在する}}\}, \tag{34}$$

$$\bigcap_{i \in I} A_i = \{a \mid \underline{\text{任意の}}\ i \in I \text{ に対して } a \in A_i\} \tag{35}$$

となる. このような使い方をする集合 I のことを「添字（そえじ）集合（index set)」という. 添字集合はあくまで添えもの、脇役であって, 主役は A_i のほうである.

[**半ば無駄, 半ば本気の話**]「任意の $i \in I$ に対して・・・となる」ということと「すべての $i \in I$ に対して・・・となる」ということは内容的には同じ意味である. 任意の, つまり勝手に選んだひとつひとつの i に対し・・・が成り立てば, それはすべての i について・・・が成り立つのと同じことだからである。数学の本には「任意の」の方が「すべての」より多く出てくる. その理由は「すべての」が多数のモノを同時に相手にしているのに比べ, 「任意の」には眼の前のたったひとつのモノだけに集中するという「気持ち」が込められているからである. 一歩ずつ着実に論理を進めていく数学には「任意の」という表現の方が合っているのである.

例題 7 次の等式を証明せよ.

$$\bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 1\right] = (0, 1]$$

（解答例）任意の $n \in \mathbb{N}$ に対して $\left[\frac{1}{n}, 1\right] \subset (0, 1]$ なので $\bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 1\right] \subset (0, 1]$ は明らかである. a を $(0, 1]$ の任意の元とする. $\lim_{n \to \infty} \frac{1}{n} = 0$ であるから $\frac{1}{n} < a$ となる $n \in \mathbb{N}$ が存在する. そのような n に対しては $a \in \left[\frac{1}{n}, 1\right]$ であるから, $a \in \left[\frac{1}{n}, 1\right]$ となる $n \in \mathbb{N}$ が存在することが分かった. よって $(0, 1] \subset \bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 1\right]$ である. $\bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 1\right] \subset (0, 1]$ と $(0, 1] \subset \bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 1\right]$ がともに示されたので $\bigcup_{n=1}^{\infty} \left[\frac{1}{n}, 1\right] = (0, 1]$ が証明された. （証明終）

演習問題 $\bigcap_{n=1}^{\infty}\left(0,\,\frac{1}{n}\right)=\emptyset$ を証明せよ. (背理法 (8 節) を用いる.)

集合の集まりに対しても, ド・モルガンの法則は成り立つ. すなわち添字集合 I のひとつひとつの元 i に対して集合 A_i が決まっているなら

$$(\bigcup_{i\in I}A_i)^c=\bigcap_{i\in I}A_i^c,\qquad (\bigcap_{i\in I}A_i)^c=\bigcup_{i\in I}A_i^c \tag{36}$$

が成り立つ.

$\forall$ は 「任意の (for any)」を意味する論理記号, $\exists$ は「・・・が存在する (there exists)」を意味する論理記号である. (下線を引いた文字の大文字をひっくり返して作られた記号らしい.) ヘンな記号だが, それなりに便利なこともあるので, 一応, 覚えておいてもらいたい. 例えば (34) (35) 式はそれぞれ次のようにかくことができる.

$$\bigcup_{i\in I}A_i=\{a\mid \exists i\in I,\ a\in A_i\},$$

$$\bigcap_{i\in I}A_i=\{a\mid \forall i\in I,\ a\in A_i\}$$

上の行の右辺の $\{\quad\}$ 内の

$$\exists i\in I,\ a\in A_i \tag{37}$$

は「$a\in A_i$ となるような $i\in I$ が存在する」(There exists an element i of I such that a is an element of A_i.) と読む. また下の行の $\{\quad\}$ 内の

$$\forall i\in I,\ a\in A_i \tag{38}$$

は「I の任意の元 i に対して $a\in A_i$ である」(For any element i of I, a is an element of A_i.) と読む.

[**無駄話**] (37), (38) とも英語の語順にあわせて記号が並んでいて, 日本語の語順からみると分かりにくい. 実は, これは数学のほとんどの記号について言えることである.

例 $\frac{a}{b}$ ($\leftarrow a$ over b), $f(x)$ ($\leftarrow$ function f of x), $a=b$ ($\leftarrow a$ is equal to b) 他.

「私たちのご先祖様が数学で世界を制覇しておいてくれたら, こんな苦労はなかったのに」なんて言うのはやめよう. 今さら文句を言ってみても始まらないのだから.

不特定の $i\in I$ を含む式

$$a\in A_i$$

はそれ単独では意味がはっきりしない. (37) と (38) は, その式が「成り立つような i が存在する」という意味なのか, それとも「任意の i について成り立つ」という意味なのかとい

うことを, 区別して明確に表現しているのである.

一般化されたド・モルガンの法則 (36) より

$$(\exists i \in I,\ a \in A_i \text{ である }) \text{ でない } = \forall i \in I,\ (a \in A_i \text{ でない }) = \forall i \in I,\ a \notin A_i$$

および

$$(\forall i \in I,\ a \in A_i \text{ である }) \text{ でない } = \exists i \in I,\ (a \in A_i \text{ でない }) = \exists i \in I,\ a \notin A_i$$

が成り立つ. 否定をとると, ∃(「存在する」) と ∀(「任意の」) が入れ替わる ことに注意して欲しい.

一般に, $\mathcal{A}(i)$ を集合 I の不特定な元 i を含む命題「$i \in I$ について・・(i を含む式)・・が成り立つ」とすると

$$(\exists i \in I,\ \mathcal{A}(i) \text{ である }) \text{ でない } = \forall i \in I,\ (\mathcal{A}(i) \text{ でない }) \tag{39}$$

および

$$(\forall i \in I,\ \mathcal{A}(i) \text{ である }) \text{ でない } = \exists i \in I,\ (\mathcal{A}(i) \text{ でない }) \tag{40}$$

が成り立つ. (これらの式が成り立つように, 「任意の (∀)」や「存在する (∃)」という用語や記号の意味を定めたと言ったほうが, より正確だろう.) 具体的な例については, 次の節にかく.

8 背理法は否定から始まる

例題 8 $a \in \mathbb{R}$ とする. 次の命題 (p. 4 の命題 (4)) を証明せよ.

$$a^2 = 2 \implies a \notin \mathbb{Q}$$

(解答例) 背理法で証明する. 結論 $a \notin \mathbb{Q}$ を否定すると $a \in \mathbb{Q}$ となる. これは

$$a = \frac{m}{n} \tag{41}$$

となる $m, n \in \mathbb{Z}$ $(n \neq 0)$ が存在することと同じである. (41) と条件 $a^2 = 2$ より

$$\frac{m^2}{n^2} = 2 \tag{42}$$

である. (42) より

$$m^2 = 2n^2 \tag{43}$$

が得られる. (43) より m^2 は偶数である. このことから m も偶数である. (もし m が奇数なら, $m = 2k + 1$ となるような整数 k が存在する. しかし, このとき $m^2 = (2k + 1)^2 =$

$4k^2+4k+1=2(2k^2+2k)+1$ は奇数である．よって「m は奇数 $\Longrightarrow m^2$ は奇数 」が証明された．従って, この対偶「m^2 は隅数 $\Longrightarrow m$ は隅数 」も正しい．） m は偶数だから $m=2r$ となる整数 r が存在する．よって, (43) から $4r^2=2n^2$, つまり

$$2r^2=n^2$$

である．よって n^2 は偶数である．従って, 前と同様にして, n も偶数である．以上から (41) の右辺の分子 m と分母 n はともに偶数である．ところで, (41) の右辺は, 前もって約分することにより m か n の少なくともどちらかは奇数であるようにしておくことができる．その場合, m と n がともに偶数であるのは矛盾である．この矛盾は $a\in\mathbb{Q}$ としたことから生じた．よって, $a\in\mathbb{Q}$ は誤りで $a\notin\mathbb{Q}$ でなければならない．（証明終）

ある命題を証明したいとき,「その命題を否定すると矛盾が導かれる」ということを示せば, そうなった原因は命題を否定したことにあるのだから, 命題の否定が誤りである．つまり, 元の命題は正しいと結論できる．これが背理法である．数学における非常に多くの定理の証明が背理法によってなされる．実際, 難しい定理の証明には背理法を使うことが多いのである．ただし, 背理法を使わずに証明できることまで背理法を使おうとすると, かえってうまくいかない．念のため！

多くの命題は $\mathcal{A}\Longrightarrow\mathcal{B}$ の形をしている．(p. 4 の末尾を見よ．）これを背理法で証明しようとするときには「条件 $\mathcal{A}$ は成り立っているのに, 結論 $\mathcal{B}$ は成り立たない」あるいは「条件 $\mathcal{A}$ は成り立っているのに, 結論 $\mathcal{B}$ は成り立たいないことがある」と仮定して矛盾を導けばよい．（3 ページでも述べたように, 数学では「成り立たないことがある」ときは「成り立たない」と判断する．）

[**無駄話**] 矛盾というコトバは中国の「韓非子」という昔の本に出ている次の故事が元になっている．「楚の国の商人で矛（ほこ、中国の刀のこと）と盾を売るものがいた．『この盾はどんなものでも防ぐ』と言って盾を売り, 『この矛はどんなものでも貫く』と言って矛を売っていた．ある人が『あなたの矛であなたの盾を突いたらどうなるのか』と尋ねた．商人は答えられなかった．」こんな単純な矛盾なら, すぐに見破れる．数学の背理法の場合, 矛盾が思わぬところに潜んでいることがある（例題 8 の解答例を見よ）ので, しっかり見張っていないといけない．

演習問題 $\log_2 3$ は無理数であることを証明せよ．

例題 9 「$n\in\mathbb{N}\Longrightarrow 2^n$ は 3 では割り切れない」を証明せよ．

（解答例）この命題は「任意の $n\in\mathbb{N}$ に対し, 2^n は 3 で割り切れない」という意味である．背理法を使うために, この命題を否定すると「2^n が 3 で割り切れような $n\in\mathbb{N}$ が 存在する」

となる. さて, そのような n が存在すると仮定して, そのうち最小のものを n_0 とする. (つまり, 2^{n_0} は 3 で割り切れるが, $n < n_0$ である自然数 n については 2^n は 3 で割り切れないとする.) 2^1=2 は 3 では割り切れないから, $n_0 \geq 2$ である. さて, 2^{n_0} が 3 で割り切れることから, $2^{n_0} = 3a$ となる自然数 a がある. もし, a が奇数なら $3a$ は奇数, 2^{n_0} は偶数であるから矛盾する. よって a は偶数であるから, $a = 2b$ (b は自然数) とおける. よって $2^{n_0} = 2 \cdot 3b$. よって $2^{n_0-1} = 3b$. しかし, これは $n < n_0$ では 2^n は 3 で割り切れないとしたことに矛盾する. よって, 元の命題は正しい.

背理法による命題 $\mathcal{A}$ の証明は, それの否定「$\mathcal{A}$ でない」が成り立つと仮定することからスタートする. 従って, ある命題が与えられたとき, その否定を正確にかく (考える) 技術を身につけることは, 数学を学ぶ上での最重要課題である.

[**半ば無駄話**] 命題 $\mathcal{A} \Longrightarrow \mathcal{B}$ を証明するとき, 使ってよい条件は $\mathcal{A}$ である. $\mathcal{B}$ はこれから証明しようとしていることだから, 当然, 使えない. $\mathcal{A}$ だけから証明できればいいのだが, どうやってもうまくいかないときがある. これは買いたいもの (証明したいこと) があるのに, 今, 持っているお金 (使ってよい条件) ではどうしても足りない, という状況と似ている. 買い物の場合はあきらめるか, 所持金が増えるまで待つのが正解だろうが, 数学の証明の場合, 所持金 (使ってよい条件) が増えることは有り得ないように見える. しかし, その有り得ないことを現実のものにする魔法のような手段が「背理法」である. 背理法では $\mathcal{A}$ のほかに「$\mathcal{B}$ でない」も条件として使ってよい! これは夢のような, まるでタダでお金がもらえるようなウマ過ぎるハナシである. ただし, 借金は借金であって最後にはキチンと返済して (矛盾を導いて) おかないといけないのだが, ともかくも足りないと思っていたお金 (条件) が急に増えるおかげで高価な品物 (難しい定理) が買いやすく (証明しやすく) なるのは事実である.

9 集合の直積

A, B を集合とする. $a \in A$ と $b \in B$ を並べたもの (a, b) を A と B の元の対 (つい, pair) という. $a \neq b$ のとき, 対 (a, b) と対 (b, a) は異なると考える. (これに対し, 集合 $\{a, b\}$ と集合 $\{b, a\}$ は常に等しい. ← 「等しい」の意味は 2 ページで述べた.) A と B の元の対の全体からなる集合を A と B の**直積** (direct product) または単に 積 (product) といい, 記号 $A \times B$ で表す. つまり

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

である. また, 3 つの集合 A, B, C の直積 $A \times B \times C$ は

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

で定義する. 4 個以上の集合の直積も同様である. とくに自然数 n に対し $A\times A\times\cdots\times A=\{(a_1,a_2,\ldots,a_n)\mid a_i\in A\,(1\leq i\leq n)\}$ を n 個の A の直積といい, A^n で表す.
集合 A の元の個数が有限のとき, A は**有限集合**であるといい, その個数を $|A|$ で表す. A,B が有限集合のとき, $A\times B, A^n$ も有限集合で $|A\times B|=|A||B|$, $|A^n|=|A|^n$ が成り立つ.

集合の直積で, 一番よく目にするのは平面

$$\mathbb{R}^2=\{(a,b)\mid a,b\in\mathbb{R}\}$$

や 3 次元空間

$$\mathbb{R}^3=\{(a,b,c)\mid a,b,c\in\mathbb{R}\}$$

であろう. 実数の対 (a,b) を (「点の座標」というより)「平面上の点」そのものと考え, そのような点全体の集合を「平面」と定義することによって, 点や平面をどう定義するか, というやっかいな問題をうまく回避しているのである. p,q,r を実数とし, $(p,q)\neq(0,0)$ とするとき, 平面 $\mathbb{R}^2$ の部分集合

$$\{(x,y)\in\mathbb{R}^2\mid px+qy+r=0\,\}$$

を $\mathbb{R}^2$ における**直線**といい, 同様に p,q,r,s を実数とし, $(p,q,r)\neq(0,0,0)$ とするとき, 3 次元空間 $\mathbb{R}^3$ の部分集合

$$\{(x,y,z)\in\mathbb{R}^3\mid px+qy+rz+s=0\,\}$$

を空間 $\mathbb{R}^3$ における**平面**という. さらに, $\mathbb{R}^3$ における相異なる 2 平面 H_1, H_2 の交わり $H_1\cap H_2$ は, もしそれが $\emptyset$ でなければ, $\mathbb{R}^3$ における**直線**という. このように, 平面や空間における点や図形 (直線, 平面, 円など) を集合 $\mathbb{R}^2$ や $\mathbb{R}^3$ の部分集合として考えることを受け入れるならば, n 次元空間 $\mathbb{R}^n$ の部分集合も高次元の図形として考える道が開けてくる. 例えば, 最近, ペレルマンによって解決されたポアンカレ予想は「3 次元」球面

$$\{(w,x,y,z)\in\mathbb{R}^4\mid w^2+x^2+y^2+z^2=1\}\ (\leftarrow 4\text{ 次元空間内の }3\text{ 次元図形})$$

に関する予想であった. (関学図書館に NHK 制作の DVD :「ポアンカレ予想 100 年の格闘 : 数学者はキノコ狩りの夢を見る」がある.)

演習問題 A,B,C,D を集合とする.

$$A\times(B\cup C)=(A\times B)\cup(A\times C),\ A\times(B\cap C)=(A\times B)\cap(A\times C)$$

を証明せよ. $(A\cup C)\times(B\cup D)=(A\times B)\cup(C\times D)$ や $(A\cap C)\times(B\cap D)=(A\times B)\cap(C\times D)$ は正しいか? 正しいなら証明し, 正しくないなら反例を示せ.

10 写像

A, B を集合とする. (この節では集合 $A, B, ...$ はすべて空でないとしておく.) A の任意の元 a に対し, B の元をただひとつ対応させる規則 f のことを A から B への**写像** (map, mapping) といい, a に対応する B の元を $f(a)$ で表す. また, f が A から B への写像であることを

$$f\colon A \longrightarrow B$$

で表す. $a, b, c \in \mathbb{R}$ とするとき, 1 次関数 $g(x) = ax + b$ や 2 次関数 $h(x) = ax^2 + bx + c$ は $\mathbb{R}$ から $\mathbb{R}$ への写像である. 一般に, $f\colon A \longrightarrow \mathbb{R}$ または $f\colon A \longrightarrow \mathbb{C}$ の形の（つまり, →の先が「数」の集合であるような）写像 f のことを, 集合 A 上の **関数** (function) という. P を $m \times n$ 実行列とすると

$$F(\mathbf{x}) = P\mathbf{x}, \quad \mathbf{x} \in \mathbb{R}^n$$

によって写像

$$F\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m$$

が定義される. このような F を $\mathbb{R}^n$ から $\mathbb{R}^m$ への線形写像といい, とくに $m = n$ のとき, $\mathbb{R}^n$ の線形変換という. 一般に, $f\colon A \longrightarrow A$ の形の（つまり, → の根元と先が同一の集合であるような）写像 f のことを集合 A の**変換** (transformation) ということがある.

$$f\colon A \longrightarrow B$$

とする. $A' \subset A$ に対し

$$f(A') = \{\, f(a') \mid a' \in A' \,\}$$

とおき, A' の f による**像** (image) という. とくに, $f(A)$ のことを単に f の像という. また, $B' \subset B$ に対し

$$f^{-1}(B') = \{\, a \in A \mid f(a) \in B' \,\} \tag{44}$$

とおき, B' の f による**逆像** (inverse image) という. (45) を言い換えれば

$$a \in f^{-1}(B') \Longleftrightarrow f(a) \in B'$$

である. $B' = \{b\}$ のとき, つまり部分集合 B' がただひとつの元しかもたないとき, 集合 (44) のことを $f^{-1}(\{b\})$ とかくとわずらわしいので, 単に $f^{-1}(b)$ とかく. つまり $b \in B$ に対して

$$f^{-1}(b) = \{\, a \in A \mid f(a) = b \,\} \tag{45}$$

とする. 集合 (45) は空集合 $\emptyset$ となることもある.

例題 10 $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $f(x) = x^2 + x$ で定義する. $f([-1,1])$ と $f^{-1}([0,1])$ を求めよ.

(解答例) $f([-1,1]) = \{f(x) \mid -1 \leqq x \leqq 1\}$ であるから, 高校教科書で関数

$$y = x^2 + x \qquad (-1 \leqq x \leqq 1) \tag{46}$$

の値域と呼んでいるものが, $f([-1,1])$ である. よって, 関数 (46) のグラフから $f([-1,1]) = [-\frac{1}{4}, 2]$ となる. また

$$f^{-1}([0,1]) = \{x \in \mathbb{R} \mid 0 \leqq x^2 + x \leqq 1\}$$

であるから, $f^{-1}([0,1])$ は「$0 \leqq x^2 + x$ かつ $x^2 + x \leqq 1$」であるような実数 x 全体の集合である. よって

$$\begin{aligned} f^{-1}([0,1]) &= \{x \in \mathbb{R} \mid 0 \leqq x^2 + x\} \cap \{x \in \mathbb{R} \mid x^2 + x \leqq 1\} \\ &= \{(-\infty, -1] \cup [0, \infty)\} \cap [\frac{-1-\sqrt{5}}{2}, \frac{-1+\sqrt{5}}{2}] \\ &= \{(-\infty, -1] \cap [\frac{-1-\sqrt{5}}{2}, \frac{-1+\sqrt{5}}{2}]\} \\ &\quad \cup \{([0, \infty) \cap [\frac{-1-\sqrt{5}}{2}, \frac{-1+\sqrt{5}}{2}])\} \quad \text{(分配法則)} \\ &= [\frac{-1-\sqrt{5}}{2}, -1] \cup [0, \frac{-1+\sqrt{5}}{2}] \end{aligned}$$

である. もちろん, $y = x^2 + x$ のグラフを使っても解けるが, あえて集合を用いて解いてみた.

例題 11 A, B を集合とし, S_1, $S_2 \subset A$, T_1, $T_2 \subset B$ とする. 次の命題の真偽を確定せよ.
(a) 写像 $f\colon A \longrightarrow B$ に対し $f(S_1) \cap f(S_2) = f(S_1 \cap S_2)$
(b) 写像 $f\colon A \longrightarrow B$ に対し $f^{-1}(T_1) \cap f^{-1}(T_2) = f^{-1}(T_1 \cap T_2)$

(解答例) (a) 偽である. $A = B = \mathbb{R}$, $S_1 = \{x \in \mathbb{R} \mid x > 0\}$, $S_2 = \{x \in \mathbb{R} \mid x < 0\}$ とし $f(x) = x^2$ とすると $f(S_1) = f(S_2) = (0, \infty)$ だから $f(S_1) \cap f(S_2) = (0, \infty)$. しかし $S_1 \cap S_2 = \emptyset$ だから $f(S_1 \cap S_2) = f(\emptyset) = \emptyset$. よって, このとき (a) は成り立たない.
(b) 真である. 証明は以下の通り.
$f^{-1}(T_1) \cap f^{-1}(T_2) = \{a \in A \mid a \in f^{-1}(T_1),\, a \in f^{-1}(T_2)\}$
$= \{a \in A \mid f(a) \in T_1,\, f(a) \in T_2\} = \{a \in A \mid f(a) \in T_1 \cap T_2\} = f^{-1}(T_1 \cap T_2)$

演習問題 (例題 10 の続き) 次は正しいか？
(c) $f(S_1) \cup f(S_2) = f(S_1 \cup S_2)$
(d) $f^{-1}(T_1) \cup f^{-1}(T_2) = f^{-1}(T_1 \cup T_2)$

写像 $f\colon A \longrightarrow B$ において

$$f(A) = B \tag{47}$$

が成り立っているとき, f は A から B への **全射写像** (surjective map), あるいは A **から** B **の上への写像** (map from A onto B) である, という. つまり, (47) は

$$\text{任意の } b \in B \text{ に対し } f(a) = b \text{ となる } a \in A \text{ が存在する} \tag{48}$$

と言い換えることができる. (「任意の」と「存在する」をうまく使っている.) 全射写像の定義としては (47) でも (48) でも良いわけだが, 実際には (48) の方が使いやすいことが多い.

例 1 写像 $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $f(x) = x^2$ で定義する. この f は全射ではない. $b \in \mathbb{R}$ を負とすると, $f(x) = b$ となる $x \in \mathbb{R}$ が存在しないからである.

写像 $f\colon A \longrightarrow B$ において

$$f(a) = f(a') \text{ となる } a, a' \in A \text{ がある} \quad \Longrightarrow \quad a = a' \tag{49}$$

が成り立つとき, f は A から B への **単射写像** (injective map), あるいは A **から** B **への１対１写像** であるという.

例 2 例 1 と同様に, 写像 $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $f(x) = x^2$ で定義する. この f は単射ではない. $a \in \mathbb{R}$ を 0 でないとすると, $f(a) = f(-a)$ かつ $a \neq -a$ となるからである.

写像 $f\colon A \longrightarrow B$ が全射かつ単射の写像であるとき, **全単射写像** (bijective map) であるという.

例 3 $s, t \in \mathbb{R}$ を定数とし, 写像 $g\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $g(x) = sx + t$ で定義する. $s \neq 0$ のとき g は全単射写像である.

写像 $f\colon A \longrightarrow B$ が与えられたとき, 任意の空でない $A' \subset A$ に対して, A' への **制限写像** (restriction map) $f|A'\colon A' \longrightarrow B$ を

$$(f|A')(a') = f(a'), \qquad a' \in A'$$

で定義することができる. つまり, $f|A'$ は f とほとんど同じで, 考える範囲だけを小さく制限してできる写像である.

例 4 例 1 と同様に, 写像 $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $f(x) = x^2$ で定義する. $\mathbb{R}_{\geqq 0} = \{\, r \in \mathbb{R} \mid r \geqq 0 \,\}$ とおく. このとき, 制限写像 $f|\mathbb{R}_{\geqq 0}\colon \mathbb{R}_{\geqq 0} \longrightarrow \mathbb{R}$ は単射になる.

集合 A から A 自身への写像 $i_A\colon A \longrightarrow A$ を

$$i_A(a) = a, \qquad a \in A$$

で定義する. すなわち, i_A は A の任意の元 a を「動かさない」写像である. この i_A を集合 A の**恒等写像** (identity map) という. 恒等写像は全単射写像である.

A, B, C を集合とし, $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$ とする. このとき, f と g の **合成写像** (composition map) $g \circ f\colon A \longrightarrow C$ を

$$g \circ f(a) = g(f(a)), \qquad a \in A$$

によって定義する.

例 5 例 1, 例 3 と同様に, 写像 $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $f(x) = x^2$ で定義し, 写像 $g\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $g(x) = sx + t$ で定義する. このとき

$$g \circ f(x) = sx^2 + t, \qquad x \in \mathbb{R},$$

$$f \circ g(x) = (sx + t)^2, \qquad x \in \mathbb{R}$$

である. このように合成する写像がどちらも関数であるとき, 合成 写像 という代わりに合成 関数 というのが普通である.

写像 $f_1\colon A \longrightarrow B$ と写像 $f_2\colon A \longrightarrow B$（どちらも A から B への写像）が与えられているとき

$$f_1 = f_2$$

であるとは, 任意の $a \in A$ に対し

$$f_1(a) = f_2(a)$$

が成り立っていることである, と定義する.

例 5 任意の写像 $f\colon A \longrightarrow B$ に対し

$$f \circ i_A = f, \quad i_B \circ f = f$$

が成り立つ.

写像 $f\colon A \longrightarrow B$ が 全単射 であるとする. f が全射であるから, 任意の $b \in B$ に対し $f(a) = b$ となる $a \in A$ が存在する. ((48) を見よ.) また, f が単射であるから, 上のような a はただひとつである. ((49) を見よ.) よって, 任意の b に対し $f(a) = b$ となる $a \in A$ がただひとつ決まるから, ひとつひとつの $b \in B$ に $f(a) = b$ となる $a \in A$ を対応させることによって, B から A への写像をつくることができる. これを f の **逆写像** (inverse map) といい, 記号 f^{-1} で表す. つまり, 全単射写像 $f\colon A \longrightarrow B$ にはその逆写像

$$f^{-1}\colon B \longrightarrow A \tag{50}$$

を考えることができるのである. (f が全単射でなくても定義できる逆像 (45) との違いに注意せよ. (45) で定義される逆像 $f^{-1}(b)$ は A の部分集合であって, 空であることもあり, 多数の元を含むこともある. これに対し, (50) における逆写像 f^{-1} では $f^{-1}(b)$ は A の (1 個の) 元である.)

例 6 写像 $g\colon \mathbb{R} \longrightarrow \mathbb{R}$ を $g(x) = sx + t$ で定義する. $s \neq 0$ とする. 例 3 で述べたようにこのとき g は $\mathbb{R}$ から $\mathbb{R}$ への全単射写像である. $b \in \mathbb{R}$ を任意にとると $g(a) = b$, つまり $sa + t = b$ となる a が, ただひとつ決まり, それは $a = \frac{b-t}{s}$ である. よって, $\mathbb{R}$ のひとつひとつの元 b に対し $a = \frac{b-t}{s}$ を対応させる写像が g の逆写像である. つまり

$$g^{-1}(x) = \frac{x-t}{s}, \qquad x \in \mathbb{R}$$

である. このように元の写像も, その逆写像も関数であるとき, 逆写像という代わりに逆関数というのが普通である.

写像 $f\colon A \longrightarrow B$ が 全単射 であるとき, その逆写像 $f^{-1}\colon B \longrightarrow A$ も全単射で

$$(f^{-1})^{-1} = f, \quad f^{-1} \circ f = i_A, \quad f \circ f^{-1} = i_B$$

が成り立つ. (例 6 の場合にチェックせよ. 一般の場合を証明せよ.)

一般に (全単射とは限らない) 写像 $f\colon A \longrightarrow B$ と写像 $g\colon B \longrightarrow A$ について

$$g \circ f = i_A$$

が成り立つとすると, f は単射, g は全射である. (証明せよ.) 従って, 写像 $f\colon A \longrightarrow B$ に対し, 写像 $g\colon B \longrightarrow A$ があって

$$g \circ f = i_A, \quad f \circ g = i_B$$

の両方が成り立っているとすると f も g も全単射となる. このとき $g = f^{-1}$ となる. (証明せよ.)

11　数学的帰納法の根拠

自然数のもつ次の性質は, 通常は意識されることなく, 正しいと認められている.

($\mathcal{N}$) **自然数全体の集合 $\mathbb{N}$ の空でない部分集合 S は最小元をもつ.**
(注意) これは $\mathbb{N}$ の性質である. $\mathbb{Z}$ や $\mathbb{R}$ などは この性質をもたない！

例 まず, 次の定義をしておく. $n \in \mathbb{N}$, $n \neq 1$ とする. n が**素数**であるとは

$$n = n_1 n_2 \quad (n_1 \neq 1,\, n_2 \neq 1)$$

となる $n_1, n_2 \in \mathbb{N}$ が存在しないことである. このとき, 次のこと（素因数分解の存在）が成り立つ.
「任意の $n \in \mathbb{N}$（ただし $n \neq 1$）に対し

$$n = p_1 p_2 \cdots p_k \quad (k \text{ はある自然数 }) \tag{51}$$

となる素数 $p_1, p_2, \ldots, p_k$ が存在する.」

(証明 1) n が素数のとき $k = 1$, $p_1 = n$ とすれば (52) は成り立つ. n が素数でないとき, $n = n_1 n_2$ $(n_1, n_2 \in \mathbb{N},\ n_1 \neq 1, n_2 \neq 1)$ と分解できる. n_1, n_2 がともに素数なら $k = 2$, $p_1 = n_1$, $p_2 = n_2$ とすれば (51) が成り立つ. n_1, n_2 の少なくともどちらかが素数でないなら, それをさらに分解して同様のことを繰り返していくと, 最終的に (51) の形の分解が得られる.

この証明で普通は十分であるとされている。気になるところがあるとすれば「同様のことを繰り返していくと, 最終的に」目的が達成されるとしているところであろう. そこが気になる (少数の) 人のために, 次の証明がある.

(証明 2)「任意の $n \in \mathbb{N}$ ($n \neq 1$) は (51) の形にかける」を背理法で示すために「(51) のようにはかけない $n \in \mathbb{N}$ ($n \neq 1$) が存在する」と仮定する. そのような n 全体の集合を S とすると, 今, 仮定したことにより $S \neq \emptyset$ である. S に ($\mathcal{N}$) を適用すると, S は最小元をもつことになる. その最小元を m とする. m が素数なら (51) の形にかけることは既に示したから $m \in S$ に矛盾する. よって m は素数でない. よって $m = m_1 m_2$ $(m_1, m_2 \in \mathbb{N},\ m_1 \neq 1, m_2 \neq 1)$ とかける. このとき $m_1 < m$, $m_2 < m$ であることと m が S の最小元であることから $m_1 \notin S$, $m_2 \notin S$ である. これは $m_1 = q_1 q_2 \cdots q_s$, $m_2 = r_1 r_2 \cdots r_t$ $(q_1, q_2, \ldots q_s, r_1, r_2, \ldots r_t$ は素数) とかけることを意味する. よって $m = m_1 m_2 = q_1 q_2 \cdots q_s r_1 r_2 \cdots r_t$ となるが, これは $m \in S$ であることに矛盾する.

よって「任意の $n \in \mathbb{N}$ ($n \neq 1$) が (51) の形にかける」ことが証明された.

繰り返しになるが, 通常は (証明 1) で十分であって (証明 2) のような詳しい証明をかく必要はない. ただ, (証明 2) は「同様にして」といった言い方はしていないことに注意してほしい.

注意 上で証明したことは (51) のような分解の「存在」だけである. 自然数 n が与えられたとき (51) のような分解がただ一通りであること（ 素因数分解の一意性 ）の証明はこれより, ずっと微妙である. そのことは代数関係の授業で学ぶであろう.

さて, 数学的帰納法は高校教科書には次のように書かれている.

「自然数 n を含む命題 $\mathrm{P}(n)$ がすべての自然数 n について成り立つことを示すには, 次の 2 つのことを確かめればよい.

［1］命題 $\mathrm{P}(1)$ は成り立つ.

［2］2 以上の任意の自然数 k について,

　　命題 $\mathrm{P}(k-1)$ が成り立つなら命題 $\mathrm{P}(k)$ も成り立つ. 」

(数学的帰納法の「証明」) 命題 $\mathrm{P}(n)$ に対して［1］［2］が証明されているとする. このとき「任意の自然数 n に対して $\mathrm{P}(n)$ が成り立つ」ことを背理法で証明するために「$\mathrm{P}(n)$ が成立しないような自然数 n が存在する」と仮定する. そのような自然数の全体を S とすると, 上の仮定から $S \neq \emptyset$ である. よって $(\mathcal{N})$ により S には最小元が存在する. その最小元を m とする. ［1］より $1 \notin S$ であるから $m \neq 1$ である. よって $m-1 \in \mathbb{N}$ である. また m が S の最小元だから $m-1 \notin S$ である. これは $\mathrm{P}(m-1)$ が成り立つことを意味する. ところが［2］が既に示されているから $\mathrm{P}(m)$ も成り立つことがわかる. これは $m \in S$ であることに矛盾する. よって「任意の自然数 n に対して $\mathrm{P}(n)$ が成り立つ」ことが証明された.

以上により, 数学的帰納法の根拠は $(\mathcal{N})$ にあることがわかった. （ 実は, $(\mathcal{N})$ と数学的帰納法とは同値であるが, そのことにこれ以上は立ち入らない. ）それでは $(\mathcal{N})$ が正しい根拠は何であろうか？実際に $(\mathcal{N})$ を証明しようとすると, 結局 $(\mathcal{N})$ と同値な命題を使うことになってしまう. つまり, 我々は「終点」（あるいは「始点」というべきか？）に到達し, これより基礎的な命題にはさかのぼれないのである.（$(\mathcal{N})$ は自然数の定義の一部と考えられている. ）数学的帰納法より $(\mathcal{N})$ の方が使いやすい場合がある. たとえば, 上の例の (証明 2) は普通の数学的帰納法ではかきにくい. この (証明 2) の論法も数学的帰納法と呼ばれることがある.

[**半ば無駄話**] 高校の数学の段階では, 数学的帰納法は「特殊な方法」といった感じがするかもしれないが, 上で述べたこと（自然数の定義の一部であること）からも分かるように極めて普遍的な方法であって, 至る所で（知らぬうちに）用いられている. 例えば, 小学校で「分数を既約分数にする」ことを習うが, どんな分数も既約にできることを証明するには（数学

的帰納法と同値な）($\mathcal{N}$) が必要になる．一般に, 数学の定理・定義・証明などは「有限個のことば・記号」で記述できないといけない（さもないと最後まで読めない）という強い制約がある．しかし, 一方では数学では無限集合・無限大・無限遠点など, 無限にかかわるものを扱いたいという強い欲求がある（さもないと退屈である)．この相矛盾するかに見える「制約」と「欲求」をうまく調整する装置（のひとつ）が数学的帰納法である．数学的帰納法（または ($\mathcal{N}$)）は有限個のことば・記号で無限個のものをうまく処理していることに注目してもらいたい．

あと幾らでもつけ加えたいことがあるが, 学期末が来てしまったので, これで一応, おしまいということにする．ここで学んだことは, 今後, さらに深い数学を学んでいく上で, きっと役に立つであろう．そうなることを願っている．