数学の基礎 1 集合論・初級編 4

順序関係

東北大学データ駆動科学・AI 教育研究センター

最終更新: 2025 年 9 月 24 日

この巻で学習することの概要

前巻では関係論の導入から始めて同値関係について学習したが, 本巻では同値関係に並んで重要な順序関係についての基本を学習する. 順序関係はその名の通り大小関係を一般化したものであるが, 最大と最小, 極大と極小などそれにまつわる言葉はたくさんあり, さらにそれらは互いに紛らわしく違いが分かりづらい. 本巻では, 順序関係にまつわるそれらの基本用語たちを, その微妙な違いを意識しながら学習することが目的である. さらに, 整列集合と呼ばれる特別な性質を持つ順序関係と, それに基づく超限帰納法と呼ばれる証明法についても触れる.

Keywords 順序関係, 全順序, 比較可能性, 逆順序と双対, 単調写像, 順序同型, 最大と最小, 上限と下限, 極大と極小, Zorn の補題, 整列集合, 整列可能定理, 超限帰納法

予備知識 第 1 巻『集合と論理』から第 3 巻『同値関係』の内容を理解していること.

Contents

1 順序関係

本巻のメイントピックスは順序関係と呼ばれる関係である．これはその名前の通り, 集合の中で元の間に順序をつける関係である．身近な集合の中でも, 例えば $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 上では数の大小を比較するための順序構造があって, 私たちはそれに基づいて数の大小を判断している．また, 任意の集合 S の冪集合 2^S 上では部分集合どうしの包含関係を考えることができるが, これも $A \subseteq B$ であることを「A は B 以下である」という意味で考えれば, 一種の順序づけであると言える．本巻では, このような順序という構造を一般的な立場から考察していく．

1.1 順序関係の定義

順序関係の定義は, 同値関係の定義も似たようなものだが, 次の通り極めて抽象的である．

順序関係

定義 1.1. 反射的, 反対称的かつ推移的な関係を**順序関係**と言う．

すなわち, 集合 X 上に定義された二項関係 $\leq$ が順序関係であるとは, 次の 3 つの要件が満たされていることを言う:

- **反射性**: $x \leq x$ である．
- **反対称性**: $x \leq y$ かつ $y \leq x$ ならば, $x = y$ である．
- **推移性**: $x \leq y$ かつ $y \leq z$ ならば, $x \leq z$ である．

この定義から分かるように, 同値関係と順序関係の違いは, 対称性の代わりに反対称性が入っていることだけである．たったこれだけの小さな違いだが, 同値関係と順序関係ではその機能がずいぶんと違う．第 3 巻『同値関係』で学んだように, 同値関係の機能は「分類」であるが, 順序関係の機能はその名の通り「順序づけ」である．

集合 X 上に順序関係 $\leq$ が設定されているとき, そのことを明示するために, X と $\leq$ を併記して $(X, \leq)$ と書くことがある．このように, 順序関係が導入された集合のことを**順序集合**と呼ぶ．この定義の下には, ①

土台となる集合 X **と②その上に設定される順序関係** $\leq$ の 2 つが定まって初めて 1 つの順序集合が確定するという考えがある．X が順序集合であるとき，その任意の部分集合も自然に X と同じ順序の下で順序集合をなす．つまり，X **の部分集合も一つの順序集合であると考えることができる**．

♦ **例 1.2** 順序関係の最も簡単な実例は，$\mathbb{R}$ 上での通常の大小関係 $\leq$ である．等号を含まない大小関係 $<$ は反射的ではないし，反対称的でもないので，ここで言う意味では順序関係ではない． □

♦ **例 1.3** (1) $a, b \in \mathbb{N}$ に対して，a が b の約数であることを $a|b$ で表す．この関係 (**整除関係**と言う) は順序関係である．しかし，$\mathbb{Z}$ 上では，整除関係は順序関係ではない．反射性と推移性は問題ないが，反対称性に小さな問題が発生するからである．例えば，$5|-5$ と $-5|5$ は共に成立するが，$5 \neq -5$ である．(一般に，整数 m, n に対して $n|m$ かつ $m|n$ であれば，$m = \pm n$ である．なので，反対称性に問題があるとは言っても，せいぜい符号の違いぐらいである.) この例のように，反射的かつ推移的な関係は，順序関係の一歩手前ということで**前順序関係**と言われることもある．

(2) X を集合，2^X をその冪集合とする．2^X 上で集合の包含関係 $\subseteq$ を二項関係と見なせば，それは順序関係である．$A \subseteq B$ かつ $A \supseteq B$ であれば $A = B$ であるが，これは $\subseteq$ の反対称性そのものである．これを集合の**包含順序**と呼んでおく．

(3) $\mathbb{R}^2$ 上の関係 $\preceq$ を次の式で定める (図 1):

$$(x, y) \preceq (x', y') \overset{\text{def}}{\iff} x \leq x' \text{ かつ } y \leq y'.$$

ここで，$\leq$ は $\mathbb{R}$ 上での通常の大小関係である．$\preceq$ は $\mathbb{R}^2$ 上の順序関係であるが，図 1 の通り，右上にある点ほど大きいと見なす順序である． □

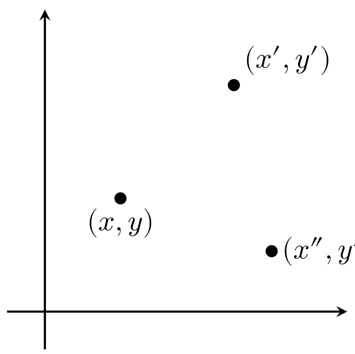

図 1 例 1.3(3) のイメージ．$(x, y) \preceq (x', y')$ であるが，$(x, y) \not\preceq (x'', y'')$ である．

♦ **例 1.4** X, Y をそれぞれ順序関係 $\leq_X$, $\leq_Y$ を持つ集合とするとき，直積集合 $X \times Y$ に導入される順序関係 $\leq$ として代表的なものが 2 つある．

(1) **直積順序**: 任意の $(x, y), (x', y') \in X \times Y$ について，

$$(x, y) \leq (x', y') \overset{\text{def}}{\iff} x \leq_X x' \text{ かつ } y \leq_Y y'.$$

例 1.3(3) の順序関係 $\preceq$ はこの意味での直積順序である．

(2) **辞書式順序**: $(x, y), (x', y') \in X \times Y$ のとき，

$$(x, y) \leq (x', y') \overset{\text{def}}{\iff} x <_X x' \text{ であるか，または } x = x',\ y \leq_Y y' \text{ である．}$$

これらは 3 個以上の順序集合の直積についても同様にして定義される． □

比較可能性と全順序

定義 1.5. $\leq$ を集合 X 上の順序関係とする．

(1) $a, b \in X$ が $\leq$ について**比較可能**であるとは，$a \leq b$ または $b \leq a$ が成立することを言う．$a \leq b$ と $b \leq a$ が両立してもよいが，その場合は反対称性から $a = b$ である．

(2) X の任意の 2 元が $\leq$ について比較可能であるとき，$\leq$ は**全順序**であると言う．

全順序とは限らない順序関係のことを**半順序**と呼ぶこともある．(この用語法では，全順序もまた半順序の特別な場合である．) しかし，この用語は「順序関係に一歩届いていない」という印象を与えるし，全順序ではない順序を指すものと解釈されたりするなど誤解のモトになりかねないので，本巻では使用しない．

$\leq$ が全順序ではないときは，$x \leq y$ **でないからと言って，直ちに** $x > y$ **であるとは言い切れない**．x, y が比較可能でない場合もあり得るからである．

♦ **例 1.6** $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 上での通常の大小関係 $\leq$ は全順序の最も身近な例である． □

♦ **例 1.7** (文字列の辞書式順序) Σ を空でない集合，Σ^* を Σ 上の文字列の全体とする (→第 1 巻『集合と論理』例 4.7)．Σ に順序関係 $\leq$ が設定されていると仮定する．これを Σ^* 上の順序へ次の要領で拡張する．任意の文字列 $w \in \Sigma^*$ について，w の長さを $|w|$ で表し，k 番目の文字を $w_k \in \Sigma$ で表す．相異なる任意の文字列 $u, v \in \Sigma^*$ を考える．それらを比較するにあたって，両者の長さが違う場合には，短い方に仮想的な空白文字 $\square$ をいくつか付け加えて長い方の長さに揃えるものとする．例えば $u = bcb$, $v = bbaac$ の場合には，u に空白文字を 2 つ追加して $u = bcb\square\square$ としてから比較を開始するものとする．ただし，空白文字については全ての文字 $x \in \Sigma$ に対して $\square < x$ であると仮定しておく．この約束の下で，$u < v$ であることを次の条件で定義する: u, v が上記の通り共に長さ n に揃えられているとき，

> ある $1 \leq i \leq n$ が存在して，(i) $u_k = v_k$ $(1 \leq k \leq i-1)$ かつ (ii) $u_k < v_k$ である．(ただし $i = 1$ の場合には最初の条件 (i) は空虚なので無視する．)

これで Σ^* 上に順序関係が定まるが，これを Σ 上の順序から導かれる**辞書式順序**と言う．例えば，アルファベット小文字 26 個が a<b<c··· <y<z と並べられているとき，ball<bat, car<house, white<whitebear, supercalifragilisticexpialidocious<tree などが成り立つ.[*1] Σ 上の順序が全順序であれば，そこから導かれる辞書式順序も全順序である．

上記の辞書式順序とは少し違う辞書式順序が使われることもある．任意の文字列 $u, v \in \Sigma^*$ について，次のように定める．

W1: $|u| < |v|$ であれば，$u < v$ であると定める．

W2: $(|u| = |v| = n$ であるとき$)$ ある $1 \leq i \leq n$ に対して (i) $u_k = v_k$ $(1 \leq k < i)$ かつ (ii) $u_i < v_i$ となるとき，かつその時に限り $u < v$ であると定める．($i = 1$ の場合は (i) は空虚なので無視する．)

この要領で定まる順序のことを**長さに基づく辞書式順序**と呼ぶ．こちらは，先に定義された辞書式順序と

[*1] supercalifragilisticexpialidocious はディズニー映画「メリー・ポピンズ」で使われた楽曲のタイトルであるが，「とても素晴らしい」という意味の形容詞になっているようだ．

☕ Coffee Break ☕

集合と順序集合

集合と順序集合は, どちらも実体としては何らかの元の集まりであるが, 集合は単なる集団とみなされることに対して, 順序集合は単なる集団である以上に, **明確に構造が想定されている**という違いがある. つまり, ある集合を順序集合として考えるという時点で, その集合には順序構造が考慮されているということである.

同じ集合を土台とする順序集合であっても, そこに導入される順序が違えば順序集合としては互いに区別される. 例えば, $\mathbb{N}$ 上で通常の大小順序 $\leq$ と整除順序 $|$ は別物なので, $(\mathbb{N}, \leq)$ と $(\mathbb{N}, |)$ は**順序集合としては**別物である. 両者には, 例えば $(\mathbb{N}, \leq)$ は全順序集合であるが $(\mathbb{N}, |)$ はそうではないという性質の違いがある.

は違って, まず文字列の長さに基づく比較がなされる. したがって, 大小比較にあたってあらかじめ文字列の長さを揃えておく必要はなく, 空白文字を想定する必要もない. 最初の Σ の順序が全順序であれば, 長さに基づく辞書式順序も全順序である. 長さに基づく辞書式順序では, 最初に条件 W1 によって長さの比較が行われるので, 例えば辞書式順序では supercalifragilisticexpialidocious<tree であるが,[*2] 長さに基づく辞書式順序では supercalifragilisticexpialidocious>tree である. □

▶ **演習 1.1**　例 1.3 の 3 つの例はどれも全順序ではないことを示せ. ただし, (2) では $|X| \geq 2$ であるとする.

1.2　Hasse 図

集合上に順序関係が設定されたとき, その構造を視覚的にとらえるために図 (有向グラフ) で表現することがある. 例えば, 図 2 は集合 $X = \{a, b, \dots, h\}$ 上のとある順序関係を図示した一例である.

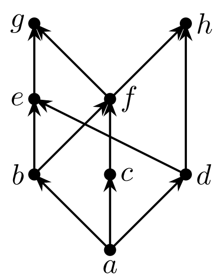

図 2　集合 $X = \{a, b, c, d, e, f, g, h\}$ 上の順序関係を表現した Hasse 図の一例.

辺 $e \to g$ は $e < g$ を意味する. 図には辺 $b \to g$ は描かれていないが, 経路 $b \to e \to g$ に沿って推移的に $b < g$ であると読む. このように, 図をなるべく簡略化するために, 推移性で補完できる辺は省かれている. 順序関係は反射的であることが前提なので, b から b 自身への矢印のようにループする辺も省かれてい

[*2] supercalifragilisticexpialidocious は 1964 年のディズニー映画『メリー・ポピンズ』の劇中歌のタイトルである. この一単語だけで 34 文字もあるもで, もし英和辞典が長さに基づく辞書式順序を採用していれば, かなり後ろの方で登場するだろう.

る．このようにして, 順序集合の構造を図示したものを **Hasse 図**と言う.[*3] 図 2 のように各辺を有向辺として描く代わりに,「上に描かれた元の方が大きい」などのルールを導入して矢印を省略して描くこともある．

e-f 間には互いに他方へ行ける経路が存在しないので,[*4] e と f は互いに比較可能ではない．だから, この順序は全順序ではない．一般に全順序集合を図で描けば, 途中で枝分かれが発生しない一本鎖になる．このことから, 一般に全順序集合を**鎖** (**チェイン**) とも言う．例えば, 図 2 では $a < c < f < g$ や $a < d < h$ などが鎖をなしている．

Hasse 図には矢印に沿って 1 周する閉路は存在しない．例えば, Hasse 図に閉路 $a \to b \to e \to a$ が存在するならば, $a \leq b \leq e \leq a$ であり, 反対称性と推移性から $a = b = e$ となってしまう．

1.3　逆順序と双対原理

集合 X 上に順序関係 $\leq$ が設定されているとする．任意の $x, y \in X$ に対して,

$$x \leq' y \overset{\text{def}}{\iff} y \leq x$$

で定義される関係 $\leq'$ もまた X 上の順序関係となる．このように, $\leq$ の大小関係を逆転させて得られる順序関係を**逆順序**と言う．定義から明らかに, $\leq'$ の逆順序は $\leq$ 自身である．X 上に逆順序 $\leq'$ を導入した順序集合のことを, 元の順序集合 X の**双対**と言う．X とその双対は, 導入されている順序が反転されているが, 集合としての実体としてはどちらも同じである．

x, y が $\leq$ に関して比較可能であるためには, その両者が逆順序 $\leq'$ に関しても比較可能であることが必要十分である．特に, $\leq$ が全順序であるためには, 逆順序 $\leq'$ が全順序であることが必要十分である．

順序集合に関する概念 C に対して, それを逆順序に関して適用して得られる概念は C の**双対**であると言われる．その一例を挙げてみよう．X を任意の順序集合, A をその部分集合として,

- A が**上に閉じている**, あるいは**上に単調**であるとは, 任意の $x, a \in X$ について,

  $$a \leq x,\ a \in A \Rightarrow x \in A$$

  が成り立つことを言う．
- A が**下に閉じている**, あるいは**下に単調**であるとは, 任意の $x, a \in X$ について,

  $$x \leq a,\ a \in A \Rightarrow x \in A$$

  が成り立つことを言う．

明らかに, A が下に閉じていることは, A が逆順序に関して上に閉じていることと全く同じである．同じく, A が上に閉じていることは, A が逆順序に関して下に閉じていることと全く同じである．このように,「上に閉じている」「下に閉じている」という性質は互いに双対な関係になっている．

一般に, **任意の**順序集合について成立する命題 P があるとき, それを双対順序集合について適用すれば, P に現れる全ての概念をその双対概念に置き換えた命題 $\bar{P}$ (P の**双対命題**と言う) もまた任意の順序集合について真であることが分かる．このようにして, 双対順序集合について元命題 P を適用することで P の双対命題を導くことを**双対原理**と言う．双対原理が有効な具体的な事例はこれから先にもたくさん出てくる

[*3] Helmut Hasse に因む.
[*4] 念の為に言っておくと, 辺の向き (矢印) に逆らって進むことは許されない.

が, ここでは上に挙げた「上に閉じている」「下に閉じている」という性質を例にして双対原理が働く事例を見てみよう.

♦ **例 1.8** X を任意の順序集合とし, $\{A_i\}_{i \in I}$ を上に閉じている部分集合 A_i らの族とする. (無限族であってもよい.) このとき, 和集合 $U = \bigcup_{i \in I} A_i$ と共通部分 $M = \bigcap_{i \in I} A_i$ もまた上に閉じていることを示そう. 証明自体は容易である.

- 和集合 U について: $a \in U$, $a \leq x$ ならば $x \in U$ でもあることを示せばよい. $a \in U$ だから, ある $i \in I$ について $a \in A_i$ である. A_i は上に閉じていて, $a \in A_i$, $a \leq x$ だから, $x \in A_i \subseteq U$ である.
- 共通部分 M について: $a \in M$, $a \leq x$ ならば $x \in M$ でもあることを示せばよい. $a \in U$ だから, どの $i \in I$ についても $a \in A_i$ である. A_i は上に閉じていて, $a \in A_i$, $a \leq x$ だから, $x \in A_i$ である. これが全ての $i \in I$ について成り立つから, $x \in M$ である.

この結論は全ての順序集合について有効なので, それを特に逆順序について適用すれば, 直ちに次のことが結論される. これが双対原理の典型的な使用例である.

X を順序集合, $\{A_i\}_{i \in I}$ を下に閉じている部分集合 A_i らの族とするとき, 和集合 $U = \bigcup_{i \in I} A_i$ と共通部分 $M = \bigcap_{i \in I} A_i$ もまた下に閉じている.

もちろん, この結論は双対原理を用いずに次の通り直接証明することもできる.

- 和集合 U について: $a \in U$, $x \leq a$ ならば $x \in U$ でもあることを示せばよい. $a \in U$ だから, ある $i \in I$ について $a \in A_i$ である. A_i は下に閉じていて, $a \in A_i$, $x \leq a$ だから, $x \in A_i \subseteq U$ である.
- 共通部分 M について: $a \in M$, $x \leq a$ ならば $x \in M$ でもあることを示せばよい. $a \in U$ だから, どの $i \in I$ についても $a \in A_i$ である. A_i は下に閉じていて, $a \in A_i$, $x \leq a$ だから, $x \in A_i$ である. これが全ての $i \in I$ について成り立つから, $x \in M$ である.

この証明は「上に閉じている」ケースの焼き直しに過ぎないことが見て取れるだろう. 実際,「上に閉じている」ケースの証明をコピー＆ペーストして「上」を「下」に書き換えて不等号の向きを逆にするだけでこの証明になってしまう. □

▶ **演習 1.2** X を任意の順序集合とする. X 上の**閉包作用素**とは, 写像 $a : 2^X \to 2^X$ で (i) $A \subseteq A^a$; (ii) $A \subseteq B$ ならば $A^a \subseteq B^a$ である; (iii) $(A^a)^a = A^a$ の 3 条件を満たすものを言う.

(1) 任意の部分集合 A に対して

$$A^u \overset{\text{def}}{=} \{x \in X \mid \text{ある } a \in A \text{ に対して } a \leq x \text{ である}\}$$

を対応づける写像 $A \mapsto A^u$ は X 上の閉包作用素であることを示せ. また, A が上に閉じているためには, $A^u = A$ であることが必要十分であることを示せ. さらに, A^u は A を含みかつ上に閉じている部分集合の中で最小であることを示せ.

(2) 任意の部分集合 A に対して

$$A^d \overset{\text{def}}{=} \{x \in X \mid \text{ある } a \in A \text{ に対して } x \leq a \text{ である}\}$$

を対応づける写像 $A \mapsto A^d$ も X 上の閉包作用素であることを示せ. また, A が下に閉じているためには, $A^d = A$ であることが必要十分であることを示せ. さらに, A^d は A を含みかつ下に閉じている部分集合として最小であることを示せ.

1.4 順序同型

X, X' を順序集合とする．あまり行儀は良くないが, X, X' 上の順序を同じ記号 $\leq$ で表す．**文脈をよく見て，その都度 $\leq$ が X, X' のいずれの順序を表しているかを考えながら読むこと**.

単調写像と順序単射

定義 1.9. $f : X \to X'$ を写像とする.

(1) f が**単調**または**単調増加**であるとは, 任意の $x_1, x_2 \in X$ について,

$$x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2) \tag{1}$$

であることを言う．このような写像 f は**順序を保つ**とも言う.

(2) f が**順序単射**であるとは, 任意の $x_1, x_2 \in X$ について次の条件式が成立することを言う:

$$f(x_1) \leq f(x_2) \Rightarrow x_1 \leq x_2. \tag{2}$$

式 (1) と式 (2) は互いに他方の逆条件になっている．順序単射はその名の通り必ず単射であるが (→演習 1.3), 単調写像は必ずしも単射ではない．(例えば, 任意の定数写像 $X \to X'$ は単調であるが, $|X| \geq 2$ のときには単射ではない.) 単調性の定義を少し強めて, 任意の $x_1, x_2 \in X$ について

$$x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$$

であるとき f は**狭義に単調**であると言う.

♦ **例 1.10** X を $\mathbb{Z}$ の有限部分集合の全体とし, 順序は包含順序 $\subseteq$ とする．X' を非負整数の全体とし, 順序は通常の大小順序とする．このとき, $f : X \to X'$, $A \mapsto |A|$ は単調であるが順序単射ではない．例えば, $A = \{2, 3\}$, $B = \{1, 3, 4\}$ とおくと, $f(A) = 2 < 3 = f(B)$ であるが, $A \subseteq B$ ではないので, f は順序単射にはなっていない. □

♦ **例 1.11** $X = X' = \mathbb{N}$ とし, X 上の順序は通常の大小順序, X' 上の順序は整除順序とする．このとき, 恒等写像 $\epsilon : x \mapsto x$ は順序単射である．$x_1 | x_2$ ならば $x_1 \leq x_2$ が成り立つからである．しかし, ϵ は単調写像ではない．例えば, $3 \leq 5$ であるが $3|5$ は成立しない. □

上の 2 つの例から, 単調写像は必ずしも順序単射ではなく, 逆に順序単射は必ずしも単調ではないことがわかる．つまり, 単調写像であることと順序単射であることは論理的には無関係である.

▶ **演習 1.3** (1) $f : X \to X'$ が順序単射ならば, f は単射であることを示せ.
(2) 具体例を挙げよ: $f : X \to X'$ は単射かつ単調であるが, 順序単射ではない.

▶ **演習 1.4** X, X', X'' を順序集合, $f : X \to X'$, $g : X' \to X''$ を写像とする.

(1) f, g が単調写像ならば, 合成 $g \circ f : X \to X''$ も単調写像であることを示せ.
(2) f, g が順序単射ならば, 合成 $g \circ f : X \to X''$ も順序単射であることを示せ.

上の演習 1.4 は写像に関する性質が合成操作で保存されることの一例である．ここでは,「単調である」「順序単射である」という性質がそれぞれ合成で保存されることを見たわけである.

▶ **演習 1.5** X, X', X'' を順序集合, $f: X \to X'$, $g: X' \to X''$ を写像とする.

(1) 合成 $g \circ f$ が単調写像, g が順序単射ならば, f は単調写像であることを示せ.
(2) 合成 $g \circ f$ が順序単射, f が単調かつ全射ならば, g は順序単射であることを示せ.

順序同型

命題 1.12. $f: X \to X'$ を全単射とするとき, 次の 2 条件は同値である:

(1) f は単調であり, かつ逆写像 $f^{-1}: X' \to X$ もまた単調である.
(2) f は単調であり, かつ順序単射でもある.

これらの条件が満たされるとき, f は**順序同型**であると言う.

証明. (1)⇒(2): f が順序単射であることを示せばよい. $x_1, x_2 \in X$, $f(x_1) \leq f(x_2)$ と仮定する. (1) から f^{-1} は単調なので, $f(x_1) \leq f(x_2)$ の両辺を f^{-1} で変換すれば, $x_1 = f^{-1}(f(x_1)) \leq f^{-1}(f(x_2)) = x_2$ が従う. ゆえに, f は順序単射である.

(2)⇒(1): f^{-1} が単調であることを示せば十分である. $x'_1, x'_2 \in X'$, $x'_1 \leq x'_2$ とする. $x_1 = f^{-1}(x'_1)$, $x_2 = f^{-1}(x'_2)$ とおくと, $x'_1 = f(x_1)$, $x'_2 = f(x_2)$ であるが, $x'_1 \leq x'_2$ であり, (2) から f は順序単射だから, $x_1 \leq x_2$ である. よって, f^{-1} は単調である. □

$f: X \to X'$ が順序同型のとき, $x \in X$ と $f(x) \in X'$ を互いに同一視すれば, X と X' を**順序の構造も含めて完全に同一視できる**. f は全単射なので, x と $f(x)$ の対応は完全に一対一であるし, 命題 1.12 から順序構造も完全にコピーされていると考えられるからである.

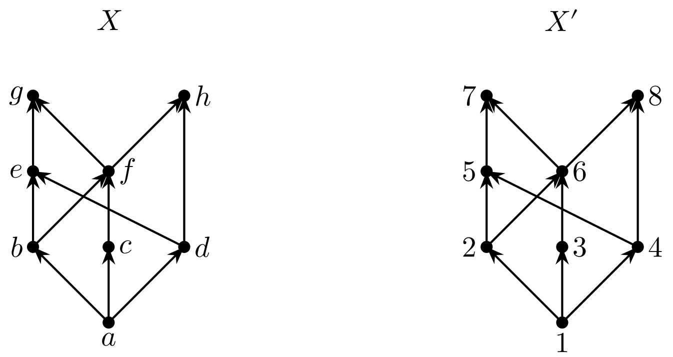

図 3 順序同型 $X \simeq X'$ のイメージ. $1 \mapsto a$, $2 \mapsto b$, ..., $h \mapsto 8$ が同型写像になっている.

順序同型 $f: X \to X'$ が存在するとき, X と X' は順序集合として**同型**であると言う. 互いに同型な順序集合は, 元の表現方法が異なるだけで**順序集合としては全く同じ構造をしている**と考えることができる. 順序集合が互いに同型であるという関係は, 同値の公理 (反射性, 対称性, 推移性) を満たしている:

- 反射性: 恒等写像 $\epsilon: X \to X$ は順序同型である.
- 対称性: $f: X \to X'$ が順序同型ならば, その逆写像 $f^{-1}: X' \to X$ も順序同型である.
- 推移性: $f: X \to X'$, $g: X' \to X''$ が順序同型ならば, 合成 $g \circ f: X \to X''$ も順序同型である.

♦ **例 1.13**　$A = \{a_1, \dots, a_n\}$ を n 個の元から成る有限集合とする．冪集合 2^A 上で集合の包含順序を考えておく．$I = \{0, 1\}$ 上で順序 $0 < 1$ を考え, 直積集合 I^n 上に直積順序を入れておく．つまり, 次のように定義しておく:

$$(x_1, \dots, x_n) \leq (x'_1, \dots, x'_n) \iff x_i \leq x'_i \ (i = 1, 2, \dots, n).$$

$f : 2^A \to I^n$ を次のように定める: 任意の $X \subseteq A$ について,

$$f(X) = (x_1, \dots, x_n), \quad x_i = \begin{cases} 1 & (a_i \in X \text{ のとき}) \\ 0 & (a_i \notin X \text{ のとき}). \end{cases}$$

この写像 f は順序同型であるが, その検証は演習問題とする (→演習 1.6). □

▶ **演習 1.6**　例 1.13 の写像 f が順序同型であることを示せ.

♦ **例 1.14**　(1) $\mathbb{N}$ に通常の大小順序 $\leq$ を入れた順序集合を $(\mathbb{N}, \leq)$ とし, 同じく $\mathbb{N}$ に整除順序 $|$ を入れた順序集合を $(\mathbb{N}, |)$ とする．両者は集合としてはどちらも同じ $\mathbb{N}$ であるが, 順序集合としては互いに同型ではない．$(\mathbb{N}, \leq)$ は全順序集合であるが, $(\mathbb{N}, |)$ は全順序集合ではないからである．(全順序集合に同型な順序集合は必ず全順序集合であることにも注意.)

(2) $\mathbb{N}$ と $\mathbb{Z}$ にそれぞれ通常の大小順序を入れた順序集合を考えると, これらも同型ではない．例えば, $\mathbb{N}$ には最小元 1 が存在するが, $\mathbb{Z}$ には最小元は存在しない．

(3) $\mathbb{Z}$ と $\mathbb{Q}$ にそれぞれ通常の大小順序を入れた順序集合を考える．これらも同型ではない．例えば, $\mathbb{Q}$ では, 任意の $x < y$ に応じて $x < z < y$ を満たす z が必ず存在する．(例えば, $z = (x + y)/2$ など.) しかし, $\mathbb{Z}$ にはそのような性質はない．例えば, $1 < x < 2$ を満たす整数 x は存在しない． □

上で挙げた 3 つの例のように, 一般に 2 つの順序集合が**同型でない**ことを見るためには, 両者が同型であれば共有しているはずの特徴に注目するのが一つのやり方である．例えば, (3) では「任意の $x < y$ に対して $x < z < y$ となる z が存在する」という性質は同型変換で保存されること (つまり, ある順序集合 X がこの性質を持っているならば, X に同型な順序集合も全てその性質を持っているということ) に注意すれば, $\mathbb{Q}$ がこの性質を持っているのに $\mathbb{Z}$ は持っていないということから $\mathbb{Q}$ と $\mathbb{Z}$ は同型ではないと言える．

同型は単調な全単射であるが, 逆に**単調な全単射は必ずしも同型ではない**．例えば, $X = Y = \mathbb{N}$ として, X には整除順序, Y には通常の大小順序を与えるとき, 恒等写像 $f : X \to Y$ は全単射かつ単調であるが順序単射ではないので同型ではない．そもそも X は全順序集合ではないが Y は全順序集合であるという違いがあるので, 両者は同型にはなり得ない．

▶ **演習 1.7**　$f : X \to Y$ を単調な全単射, X は全順序集合とするとき, f は同型であることを示せ.

2 最大元・上限・極大元

本節では, 順序に関する基本的な概念として, 最大元, 上限, および極大元とそれらの双対概念である最小元, 下限, 極小元について解説する．これらの概念は定義が似通っていることもあって互いに紛らわしいが, その微妙な違いをしっかり理解しよう．

2.1 上界と下界

以下, 任意の順序集合 $(X, \leq)$ とその部分集合 A を固定して考える.

上界と下界

定義 2.1. $x \in X$ とする.

(1) x が A の**上界**であるとは, 全ての $a \in A$ について $a \leq x$ であることを言う.
(2) x が A の**下界**であるとは, 全ての $a \in A$ について $x \leq a$ であることを言う.

x が A の上界や下界であるということには, x は A の全ての元と比較可能であるという条件もその前提として入っている. 上界, 下界は双対概念の好例である. x が A の上界であることは, 双対順序について x が A の下界であることと同じであるし, x が A の下界であることは, 双対順序について x が A の上界であることと同じである.

X の中に A の上界が存在するとき, A は**上に有界**であると言う. 同じく, X の中に A の下界があるとき, A は**下に有界**であると言う. A が上にも下にも有界であるとき, 単に A は**有界**であると言う. 形式的には, ($X = \emptyset$ でない限り) $A = \emptyset$ は有界である.*5

♦ **例 2.2** 次の図 4 (図 2 と同じもの) で考える. $A = \{a, b, c, e, f\}$, $B = \{b, e, f, h\}$ とおく.

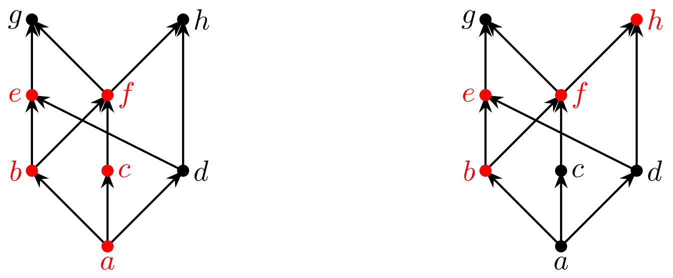

図 4 図 2 の再掲.

(1) g は A の上界である. (どの $x \in A$ についても $x \leq g$ であることを確認せよ.) だから, 特に A は上に有界である. 一方で, $e \in A$ であるが $e \leq h$ は成立しないので, h は A の上界ではない. この図の中で A の上界になっているのは g だけである.
(2) $e \in B$ であるが, $x \in \{a, b, c, d, f, h\}$ のいずれについても $e \leq x$ は成立しないので, a, b, c, d, f, h はどれも B の上界ではない. $h \in B$ であるが $h \leq g$, $h \leq e$ はいずれも成立しないので, e と g も B の上界ではない. よって, この図の中のどの元も B の上界ではない. ゆえに, B は上に有界ではない. □

▶ **演習 2.1** (有向順序) $(X, \leq)$ を順序集合とする. X の全ての有限部分集合が上に有界であるとき, 順序 $\leq$ は**上向き**あると言い, X の全ての有限部分集合が下に有界であるとき, $\leq$ は**下向き**であると言う.

(1) $\leq$ が全順序ならば, $\leq$ は上向きかつ下向きであることを示せ.

*5 $A = \emptyset$ であれば, どの $x \in X$ についても $a \in A \Rightarrow a \leq x$ は真である. 同じく, $a \in A \Rightarrow x \leq a$ も真である.

(2) 図 2 で表される順序 $\le$ は上向き (または下向き) であるか?
(3) 例 1.3(3) の順序 $\preceq$ は上向きかつ下向きであることを示せ.

2.2　最大元と最小元

引き続き, 任意の順序集合 X とその部分集合 A を考える.

最大元と最小元

定義 2.3. $x \in X$ とする.

(1) x が A の**最大元**であるとは, $x \in A$ であり, かつ x が A の上界であることを言う.
(2) x が A の**最小元**であるとは, $x \in A$ であり, かつ x が A の下界であることを言う.

A の最大元は, 文字通り A の中で最も大きな元のことである. それは A の上界だから, A の全ての元と比較可能であることが前提である. 最小元についても同様のことが言えるが, いちいち繰返す必要はないだろう. 定義から明らかに, 最大元と最小元も双対概念の一例である.

下の例 2.5 で見るように, A によってはその最大元が存在しない. A の最大元が存在するならば, 次の命題 2.4 で示す通り, それは A から一意的に決まる. それを $\max A$ と書く. 同じく, A に最小元が存在するならばそれは一意的であり, それを $\min A$ と書く. max と min はそれぞれ maximum, minimum を略した記号である.

命題 2.4. A に最大元が存在するとき, それは一意的である. 最小元についても同様である.

証明. $x, x' \in A$ が共に A の最大元であると仮定すれば, $x = x'$ であることを示せばよい. x は A の最大元でかつ $x' \in A$ だから, $x' \le x$ である. x と x' の立場を入れ替えて同様に考えれば, $x \le x'$ であることもわかる. よって, $\le$ の反対称性から $x = x'$ である. したがって, $\max A$ は一意的である. 双対原理により, $\min A$ も (それが存在する限りは) 一意的であることが言える. □

♦ **例 2.5**　Hasse 図 5 (図 2 と同じもの) で考える. $A = \{a, b, c, e, f\}$, $B = \{b, e, f, h\}$ とおく.

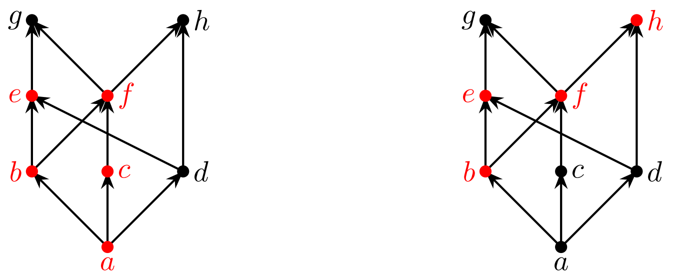

図 5　例 2.5 の Hasse 図.

(1) 例 2.2 で見たように, B には上界が存在しないので, $\max B$ は存在しない.
(2) g は A の上界ではあるが, $g \notin A$ だから, $g = \max A$ ではない. 例 2.2 でも述べたように, X の中で A の上界になれるものは g のみである. その g が $\max A$ でないので, $\max A$ は存在しない. この例は, **A が上に有界であっても, $\max A$ が存在するとは限らない**ことを示している.

(3) a は A の下界である．かつ $a \in A$ だから，$a = \min A$ である． □

▶ 演習 2.2　Hasse 図 6 で，$C = \{b, c, d, f, h\}$ の最大元と最小元はそれぞれ何か？ 存在しない場合は「存在しない」と結論せよ．

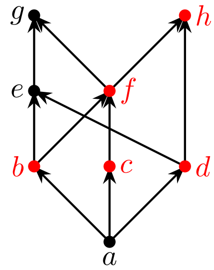

図 6　演習 2.2 の Hasse 図．

♦ 例 2.6　$A = [0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ とおく．任意の $a \in A$ について $0 \leq a$ だから，0 は A の下界である．そして $0 \in A$ だから，$\min A = 0$ である．

1 は A の上界なので，A は上に有界である．しかし，$\max A$ は存在しないことを示す．任意の $x \in A$ について，それが A の上界ではないことを示せば十分である．$x \in A$ だから，$0 \leq x < 1$ である．$c = (1 + x)/2$ とおくと，$0 \leq x < c < 1$ だから，$c \in A$ である．そして $x < c$ だから，x は A の上界ではない．この例では，1 は A の上界ではあるが，$1 \notin A$ だから，$\max A = 1$ ではない． □

♦ 例 2.7　$\mathbb{R}^2$ 上で例 1.3(3) の順序関係 $\preceq$ を考え，

$$A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$$

とおく．全ての $(x, y) \in A$ について $|x|, |y| \leq 1$ なので，特に $(x, y) \preceq (1, 1)$ でもある．したがって，$(1, 1)$ は A の上界であり，A は上に有界である．しかし，$\max A$ は存在しないことを示そう．そのためには，任意の $(x, y) \in A$ について，それが A の上界でないこと，つまり $(x', y') \preceq (x, y)$ とならない $(x', y') \in A$ が存在することを示せばよい．$(x, y) \in A$ とするとき，$x^2 + y^2 \leq 1$ なので，$x \leq 1$, $y \leq 1$ である．$x = 1$ であるときは，$y = 0$ であるが，この場合は $(0, 1) \in A$ に対して $(0, 1) \preceq (x, y)$ が成立しない．$x < 1$ であるときには，$(1, 0) \in A$ に対して $(1, 0) \preceq (x, y)$ が成立しない． □

2.3　上限と下限

引き続き，任意の順序集合 X とその部分集合 A を考える．A の上界の全体を A^+，下界の全体を A^- とおく：

$$A^+ = \{x \in X \mid \text{全ての } a \in A \text{ について } a \leq x \text{ である}\}$$
$$A^- = \{x \in X \mid \text{全ての } a \in A \text{ について } x \leq a \text{ である}\}.$$

上限と下限

定義 2.8. $A \subseteq X$ とする．

(1) $\min A^+$ が存在するとき，それを A の**上限**または**最小上界**と呼んで，$\sup A$ と書く．

(2) $\max A^-$ が存在するとき, それを A の**下限**または**最大下界**と呼んで, $\inf A$ と書く.

sup と inf はそれぞれラテン語由来の supremum, infimum から取られた記号である. 上限と下限も, 最大元と最小元の関係と同じように, 互いに双対な概念である.

定義から $\sup A = \min A^+$ なので, $\sup A \in A^+$ である. つまり, $\sup A$ 自身は A の一つの上界である. よって, A が上に有界でないならば, $\sup A$ は存在しない. ただし, A が上に有界であっても, $\sup A$ が存在するとは限らない. $\inf A$ についても同様のことが言える.

$\sup A$ は, それが存在する限りは唯一つに決まる. (これは $\min A^+$ の一意性による.) ただし, **$\sup A$ が存在しても, $\sup A \in A$ であるとは限らない**. ここは $\max A$ とは違っている. ($\max A$ はその定義上, 必ず A の元であることに注意.) inf についても同様である.

♦ **例 2.9**　Hasse 図 7 (図 2 と同じもの) で考える. $A = \{a, b, c, e, f\}$, $C = \{a, c, d\}$ とする.

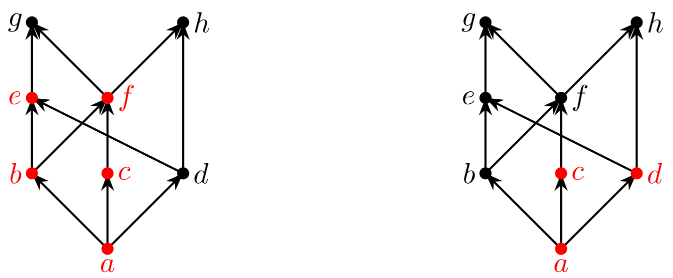

図 7　例 2.9 の Hasse 図.

(1) 例 2.5(2) から, $\max A$ は存在しない. 一方, $A^+ = \{g\}$ なので, $\sup A = \min A^+ = g$ である.

(2) $A^- = \{a\}$ だから, $\inf A = a$ である. そして $a \in A$ でもあるので, $a = \min A$ である.

(3) $C^+ = \{g, h\} \neq \emptyset$ だから, C は上に有界である. しかし, $\min C^+$ は存在しないので, $\sup C$ は存在しない. また, $\max C$ も存在しない. □

♦ **例 2.10**　$A = [0, 1) = \{x \in \mathbb{R} \mid 0 \le x < 1\}$ とおく. 任意の $x \in A$ について $x < 1$ なので, 1 は A の上界である. つまり, $1 \in A^+$ である. しかし $1 \notin A$ なので, $1 = \max A$ であるとは言えない.

1 は A の最大元ではなく, 上限である. つまり, $1 = \sup A$ である. そのことを示すためには $1 = \min A^+$ であることを示せばよいが, $1 \in A^+$ であることは既に分かっているので, 後は 1 が A^+ の下界であること, つまり任意の $c \in A^+$ について $1 \le c$ であることを示せばよい. $c \in A^+$ とする. $0 < \varepsilon \le 1$ を任意に考える. このとき, $0 \le 1 - \varepsilon < 1$ だから $1 - \varepsilon \in A$ である. そして c は A の上界なので, $1 - \varepsilon < c$ である. これがどんな小さな $\varepsilon > 0$ についても常に成立するから, $1 \le c$ である. ($1 > c$ ならば, $\varepsilon = (1 - c)/2 > 0$ に対して $1 - \varepsilon < c$ が成立せず不合理.) よって $1 = \min A^+$, つまり $1 = \sup A$ である. □

♦ **例 2.11**　$\mathbb{N}$ 上で整除順序を考える. 任意の空でない部分集合 $A \subseteq \mathbb{N}$ と $x \in \mathbb{N}$ について, 次の同値が成立する:

$$\begin{aligned} x \text{ が } A \text{ の下界である} &\iff \text{全ての } a \in A \text{ について } x \mid a \text{ である} \\ &\iff x \text{ は } A \text{ の全ての元に渡る\textbf{公約数}である.} \end{aligned}$$

よって, 次の同値が成立する:

$$\begin{aligned} x = \inf A &\iff x \text{ は } A \text{ の下界のうちで (整除関係について) 最大の自然数である} \\ &\iff x \text{ は } A \text{ の全ての元に渡る}\textbf{最大公約数}\text{である.} \end{aligned}$$

同様にして, A の上界とは A の全ての元に渡る公倍数のことであり, $\sup A$ は A の全ての元に渡る**最小公倍数**であることもわかる. □

♦ **例 2.12**　X を集合とし, 冪集合 2^X 上で包含順序を考える. 任意の部分族 $\mathcal{A} \subseteq 2^X$ に対して, $\sup \mathcal{A}$ は全ての $A \in \mathcal{A}$ に渡る和集合

$$\bigcup_{A \in \mathcal{A}} A = \{x \in X \mid x \in A \text{ となる } A \in \mathcal{A} \text{ が存在する}\}$$

であることを示そう. $U = \bigcup_{A \in \mathcal{A}} A$ とおく. U が $\mathcal{A}$ の上界であること, つまり任意の $A \in \mathcal{A}$ について $A \subseteq U$ であることは, U の定義から明らかである. 後は U が $\mathcal{A}$ の上界として最小であることを示せばよい. つまり, U' を $\mathcal{A}$ の任意の上界とするとき, $U \subseteq U'$ であることを示せばよい. $x \in U$ とすると, U の定義から $x \in A$ となる集合 $A \in \mathcal{A}$ が存在する. $A \in \mathcal{A}$ であるが, 一方で U' は $\mathcal{A}$ の上界なので, $A \subseteq U'$ が成り立つ. そして $x \in A$ なので, $x \in U'$ でもある. ゆえに, $U \subseteq U'$ である. 同様にして,

$$\inf \mathcal{A} = \bigcap_{A \in \mathcal{A}} A = \{x \in X \mid \text{全ての } A \in \mathcal{A} \text{ について } x \in A\}$$

であることも分かる. □

▶ **演習 2.3**　$\mathbb{R}^2$ 上で例 1.3(3) の順序関係 $\preceq$ を考える. 集合 $A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ について, $\sup A = (1, 1)$ であることを示せ.

▶ **演習 2.4** (max と sup の関係)　次のことを証明せよ.

(1) $\max A$ が存在するならば, それは $\sup A$ でもある.
(2) $\sup A$ が存在してかつそれが A に属するならば, それは $\max A$ である.
(3) $\sup A$ が存在するがそれが A に属さないとき, $\max A$ は存在しない.

補足: これの双対として, $\min A$ と $\inf A$ についても同様の関係が成立する.

▶ **演習 2.5** (sup の単調性)　X を順序集合, A, B をその部分集合として, $\sup A$, $\sup B$ が共に存在すると仮定する. $A \subseteq B$ ならば, $\sup A \leq \sup B$ であることを示せ. また, この主張の双対命題を考えてみよ.

2.4　極大元と極小元

引き続き, $(X, \leq)$ を順序集合, A をその部分集合とする.

極大元と極小元

定義 2.13. A を X の部分集合, $x \in A$ とする.

(1) x が A で**極大**であるとは, A に x よりも真に大きな元 ($x < a$ を満たす a) が存在しないこと

☕ Coffee Break ☕

実数空間における上限と下限

微分積分学で学習することであるが, 実数の全体 $\mathbb{R}$ 上で通常の大小順序を考えたとき, 上に有界な空でない部分集合 A には必ず上限 $\sup A$ が存在する. (ただし, それが A に属しているという保証はない. 同様に, 下に有界な空でない部分集合 A に下限 $\inf A$ が存在するとも言えるが, それが A に属している保証はない.) これは, 解析学的な観点から見た実数に関して最も基本的な性質の一つであり, 実数の**連続公理**と呼ばれている. 実数の連続公理には他にも複数の別表現がある. 例えば,「上に有界な単調増加数列は収束する」などという比較的イメージしやすい表現もある.

連続公理は数の範囲を実数まで広げることで出てくる性質であり, 有理数までの世界では成立しない. 例えば, $\mathbb{Q}$ の部分集合 $A = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$ は上に有界であるが, $\sup A$ は ($\mathbb{Q}$ の中には) 存在しない.

を言う.

(2) x が A で**極小**であるとは, A に x よりも真に小さな元 ($a < x$ を満たす a) が存在しないことを言う.

注意: 解析学では, 関数の局所的な最大値, 最小値のことをそれぞれ極大値, 極小値と呼ぶことがあるが, ここで言う極大, 極小はその意味とは異なる.

極大元と極小元もまた互いに双対な概念の一例である.

A の中に x より真に大きな元が無いという条件を言い換えれば, $x \leq a$ となる $a \in A$ があれば, それは x 自身に限るということである. すなわち, $x \in A$ のとき:

$$x \text{ が } A \text{ で極大} \iff a \in A,\ x \leq a \text{ ならば } x = a \text{ である.}$$

極小性についても同様の言い換えが可能である. こうなると, 極大と最大, 極小と最小の違いはわかりづらく,「何が違うんだ?」という話になる. 平たく言えば, $x \in A$ のとき,

$$\begin{aligned} x \text{ が } A \text{ で最大} &\iff x \text{ は } A \text{ の中でどの元よりも大きい} \\ x \text{ が } A \text{ で極大} &\iff A \text{ には } x \text{ よりも真に大きな元はない} \end{aligned}$$

である. ますます違いが分かりにくくなった気もするが, この微妙な違いを理解するには**比較可能性**がキーポイントである. いくつかの具体例を見てみよう.

♦ **例 2.14** Hasse 図 8 (図 2 と同じもの) で考える. $A = \{a, b, c, e, f\}$ とおく. 例 2.2 で見た通り, $\max A$ は存在しない. それでは, A に極大元は存在するだろうか. まず, $a < b < e$, $c < f$ だから, a, b, c は極大ではない. A には $e < x$ となる x が存在しないので, e は極大である. しかし, $e = \max A$ ではない. $f \in A$ に対して $f \not\leq e$ だからである. 同じ理由で, f も A で極大だが最大ではないことがわかる. □

♦ **例 2.15** X を 2 以上の自然数の全体とし, その上で整除順序を考える. ($x \leq y$ であることを, x は y

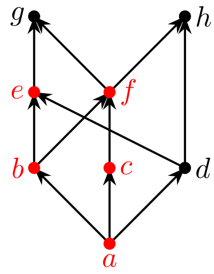

図 8　例 2.14 の Hasse 図.

の約数であることと考える.) 任意の $x \in X$ について,

$$
\begin{aligned}
x \text{ が } X \text{ で極小である} &\iff y|x \text{ ならば } x = y \text{ である} \\
&\iff y \text{ が } x \text{ の約数ならば } x = y \text{ である} \\
&\iff x \text{ の } (1 \text{ でない}) \text{ 約数は } x \text{ のみである} \\
&\iff x \text{ は素数である.}
\end{aligned}
$$

一方で, $\min X$ は存在しない. $\min X$ が存在するならば, それは 2 以上の全ての自然数に渡る公約数であるが, そんな自然数は X の中には無いからである. □

♦ 例 2.16　$A = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ とおき, $\mathbb{R}^2$ 上で例 1.3(3) の順序 $\preceq$ を考える. A の極大元を全て特定してみよう. (x,y) が A で極大であるとする. $(x,y) \in A$ だから, $(-x)^2 + y^2 = x^2 + y^2 \leq 1$ であり, $(-x,y) \in A$ でもある. $x < 0$ ならば, $(-x,y)$ は (x,y) よりも真に大きな元であるが, これは (x,y) の極大性からあり得ない. よって $x \geq 0$ である. 同様に, $y \geq 0$ でもある. $(0,0)$ は $(1/2,1/2) \in A$ よりも真に小さいので極大ではありえない. ゆえに, $(x,y) \neq (0,0)$ である.

$r = x^2 + y^2$ とおく. $(x,y) \in A$, $(x,y) \neq (0,0)$ だから, $0 < r \leq 1$ であるが, ここで $r < 1$ と仮定すると, $c = (1+r)/2 > 0$, $(x',y') = (cx/r, cy/r)$ とおけば, $(x',y') \in A$ であり, かつ (x,y) よりも真に大きいので, (x,y) の極大性に反する. したがって, $r = 1$ である. 以上から, (x,y) が A の極大元ならば, $x, y \geq 0$, $x^2 + y^2 = 1$ であることが分かる.

逆に, $x, y \geq 0$, $x^2 + y^2 = 1$ ならば, (x,y) は A の極大元であることを示す. $(x',y') \in A$, $(x,y) \preceq (x',y')$ とする. $(x,y) \preceq (x',y')$ だから, $0 \leq x \leq x'$, $0 \leq y \leq y'$ である. $(x',y') \in A$ だから, ${x'}^2 + {y'}^2 \leq 1$ である. よって, $1 = x^2 + y^2 \leq {x'}^2 + {y'}^2 \leq 1$ である. ゆえに, $x^2 + y^2 = 1 = {x'}^2 + {y'}^2$ であり, 整理すると $x^2 - {x'}^2 = {y'}^2 - y^2$ となる. この左辺は ≤ 0, 右辺は ≥ 0 だから, この両辺は 0 である. よって, $x = x'$, $y = y'$ であり, $(x',y') = (x,y)$ を得る. ゆえに, (x,y) は A で極大である.

以上から, A の極大元は $x^2 + y^2 = 1$, $x, y \geq 0$ を満たす点 (x,y) であり, かつそのような点に限る (図 9). 例えば, $(1,0)$, $(0,1)$, $(1/\sqrt{2}, 1/\sqrt{2})$ は A の極大元の一例である. これらは A の極大元ではあるが, 最大元ではない. □

これらの例のように, 全順序集合ではない順序集合では「最大ではないが極大ではある」「最小ではないが極小ではある」という元が存在し得る. また, 一般に A の極大元や極小元は複数個, 場合によっては無限個存在することもある.

▶ 演習 2.6 (最大元と極大元の関係)　$(X, \leq)$ を順序集合, A をその部分集合とする. $x \in A$ とするとき, 次のことを証明せよ.

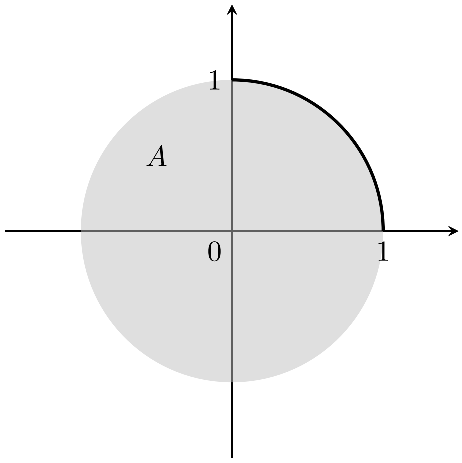

図 9 例 2.16: A の極大元 (太線の部分).

(1) $x = \max A$ ならば, x は A の唯一つの極大元である.

(2) $\leq$ が全順序ならば: $x = \max A \iff x$ は A の極大元.

補足: 双対的に, $\min A$ と極小元についても同様のことが言える.

▶ 演習 2.7 X が有限個の元から成る順序集合ならば, 任意の $x \in X$ に応じて, $x \leq w$ となる極大元 w が存在することを示せ. (双対的に, $v \leq x$ となる極小元 v の存在も言える.)

2.5 極大性・極小性の利用例

最大性や最小性, および極大性や極小性は,「もうこれ以上何らかの条件を保ったまま大きく (または小さく) できない」という**ギリギリのところを攻める**概念である. 上限と下限もそれぞれ,「**最小**の上界」「**最大**の下界」ということで, やはりギリギリのところを攻める概念である. こういった「ギリギリさ」を利用した事例をいくつか紹介しておこう. いずれの例でも, どのように「ギリギリさ」が使われているかに注目してほしい.

♦ 例 2.17 **初等整数論の基本定理**は「任意の自然数は有限個の素数の積である」ことを主張する. (ただし, 同じ素数を複数回利用してもよい. また, 形式的に 1 は 0 個の素数の積であると見なしておき, 任意の素数は 1 個の素数の積と見なす.) これは要するにどの自然数も**素因数分解**を持っていることを主張していて, この事実自体はよく知られている. 実際には, 初等整数論の基本定理は全ての自然数がそれぞれ**一意的な**素因数分解を持つことまで主張するが, 一意性はともかくとして, 素因数分解の存在だけならごく簡単な背理法で次のようにして証明できる.

素因数分解を持たない自然数の全体を F で表す. これが空集合ではないと仮定しよう. 任意の $k \in F$ を選び, F の中で k 以下である数の全体を F_k とする. これはせいぜい $\{1, 2, \dots, k\}$ の部分集合なので有限集合であり, したがってその最小値 n が存在する. n は F 全体に渡る最小値でもある. 1 は「0 個の素数の積」と見なされているから, $n \geq 2$ である. n 自身は合成数だから, $n = ab$, $1 < a, b < n$ と分解できる. $n = \min F$ であり, $a, b < n$ なので, $a, b \notin F$ である. よって, a, b はそれぞれ有限個の素数の積に分解できる. すると, $n = ab$ もまた有限個の素数の積であることになり, $n \in F$ であること (n が素因数分解を持たないこと) に反する. よって, $F = \emptyset$ でなければならない. □

♦ **例 2.18** 7 以上の全ての自然数は, $2a+3b$ $(a,b\in\mathbb{N})$ という形式の和で書けることを示そう. 背理法を用いる. この主張が正しくないと仮定して, 反例となる最小の自然数 k を考える. $k\geq 7$ であり, かつ 7, 8 は反例ではない $((a,b)=(2,1)$ に対して $7=2a+3b$ であり, $(a,b)=(1,2)$ に対して $8=2a+3b$ である) ので, $k\geq 9$ である. $k-2\geq 7$ だから, k の反例としての最小性から $k-2=2a'+3b$ $(a',b\in\mathbb{N})$ と書ける. すると, $k=2(a'+1)+3b$ であり, k が反例であることに反する. □

♦ **例 2.19** A を 2 次正則行列から成る集合とする. 2 次正方行列 x が A で**生成**されるとは, x が A に属する行列あるいはそれらの逆行列を有限個用いた積で記述できること, すなわち

$$x=x_1x_2\cdots x_n,\quad (x_i\in A \text{ または } x_i^{-1}\in A)$$

という形式で書けることを言う. ここで, $x_1,\dots,x_n$ の中には 2 回以上現れる行列があってもよい. また, $n=0$ のときには, この「空っぽの積」は単位行列 e を表しているものとする. (だから, 単位行列 e は A で生成されると考える.) 各々の x_i は正則行列だから, x も正則行列である.

ここで, A が次の 2 つの行列から成る集合 $A=\{s,t\}$ であるとする:

$$s=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad t=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

どちらも整数成分の正則行列であり, $\det s=\det t=1$ である. よって, 逆行列 s^{-1}, t^{-1} も整数成分の行列であり, $\det s^{-1}=\det t^{-1}=1$ である. 行列 x が $A=\{s,t\}$ で生成されるならば,

$$x=x_1x_2\cdots x_n,\quad (\text{各 } x_i \text{ は } s,\ t,\ s^{-1},\ t^{-1} \text{ のどれか})$$

と書けるが, x もまた整数成分行列であり, $\det x=1$ である.

ここからが話のメインである. 逆に, 整数成分の 2 次正方行列で行列式が 1 であるものは $A=\{s,t\}$ で生成できることを示そう. これが正しくないとすると, その反例が存在するはずである. すなわち, 行列式 1 を持つ 2 次整数成分行列 x で, A で生成できないものが存在する. そのような反例 x のうちで, $(2,1)$-成分 x_{21} の絶対値 $|x_{21}|$ が最小であるものを考える. ここで, s, t に関して

$$s^2=-e=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad t^k=\begin{pmatrix}1&k\\0&1\end{pmatrix}\quad (k \text{ は任意の整数})$$

であることに注意しておく. $s^2=-e$ は直接計算ですぐにわかるし, t^k についても k に関する数学的帰納法を使えば確かめられる.

(I) $x_{21}\neq 0$ であることを示す. $x_{21}=0$ と仮定する. $1=\det x=x_{11}x_{22}-x_{21}x_{22}=x_{11}x_{22}$ であり, x_{11}, x_{22} は整数なので, (i) $x_{11}=x_{22}=1$ または (ii) $x_{11}=x_{22}=-1$ である. (i) の場合には, $x=t^{x_{12}}$ であり, x は A で生成できる. (ii) の場合は, $s^2x=-x=t^{-x_{12}}$ だから $x=s^{-2}t^{-x_{12}}$ であり, やはり x は A で生成できる. よって, いずれにせよ x は A で生成できて, x の選び方に反する. ゆえに, $x_{21}\neq 0$ である.

(II) x_{11} を x_{21} で割って商が q, 余りが r であるとすると, $x_{11}=qx_{21}+r$, $0\leq r<|x_{21}|$ である. すると,

$$t^{-q}x=\begin{pmatrix}1&-q\\0&1\end{pmatrix}\begin{pmatrix}x_{11}&x_{12}\\x_{21}&x_{22}\end{pmatrix}=\begin{pmatrix}x_{11}-qx_{21}&x_{12}-qx_{22}\\x_{21}&x_{22}\end{pmatrix}=\begin{pmatrix}r&x_{12}-qx_{22}\\x_{21}&x_{22}\end{pmatrix}$$

であり, したがって

$$st^{-q}x=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}r&x_{12}-qx_{22}\\x_{21}&x_{22}\end{pmatrix}=\begin{pmatrix}-x_{21}&-x_{22}\\r&x_{12}-qx_{22}\end{pmatrix}\tag{3}$$

である．これは整数成分行列であり，行列式 1 を持つが，$0 \leq r < |x_{21}|$ だから，x の選び方 ($|x_{21}|$ の最小性) から，$st^{-q}x$ は A で生成できる．つまり，$st^{-q}x = x_3x_4 \cdots x_n$ ($x_i \in \{s, t, s^{-1}, t^{-1}\}$) と書ける．よって，$x_1 = s^{-1}$, $x_2 = t^q$ に対して

$$x = s^{-1}t^q(st^{-q}x) = x_1x_2x_3 \cdots x_n \tag{4}$$

となり，x は A で生成できる．しかし，これは x が反例であることに矛盾する． □

これら 3 つの例では，主張が正しくないと仮定して，何らかの意味で最小である反例を考えることで矛盾を導いている．このような論法は**最小反例法**などと呼ばれる.[*6] 次の例は，やや手がこんでいるものの，基本的な発想は似たようなものである．

♦ **例 2.20**　$x^2 + y^2 = 3z^2$ を満たす自然数組 (x, y, z) が存在しないことを証明する．背理法を用いる．次の集合

$$D = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + y^2 = 3z^2\}$$

が空ではないと仮定して矛盾を導けばよい．まず準備として，次の 2 つの主張を用意しておこう．

(I) まず，任意の整数 x について，$x^2 \bmod 3$ (x^2 を 3 で割った余り) は 0 または 1 であることを示す．x を 3 で割って商が q, 余りが r であるとすると，$x = 3q + r$, $r \in \{0, 1, 2\}$ であり，

$$x^2 = (3q + r)^2 = 3(3q^2 + 2qr) + r^2$$

である．よって，$x^2 \bmod 3$ は $r^2 \bmod 3$ と同じである．r は 0, 1, 2 のうちのどれかであるが，その各々に応じて $r^2 \bmod 3$ は 0, 1, 1 となる．したがって，$x^2 \bmod 3$ は 0, 1 のどちらかである．

(II) 次に，任意の $(x, y, z) \in D$ について，x, y, z は全て 3 の倍数であることを示す．x^2, y^2 をそれぞれ 3 で割った時の商を u, v, 余りを r, s とすると，$x^2 = 3u+r$, $y^2 = 3v+s$ であり，$x^2+y^2 = 3(u+v)+r+s$ である．$x^2 + y^2 = 3z^2$ なので，$x^2 + y^2$ は 3 の倍数である．したがって，$r + s$ も 3 の倍数である．ここで，(I) から $r, s \in \{0, 1\}$ であるから，$r + s$ が 3 の倍数となるのは $r = s = 0$ の時だけである．ゆえに，x^2, y^2 はどちらも 3 の倍数である．そして 3 は素数なので，x, y 自身も 3 の倍数でなければならない．

そこで，改めて $x = 3u$, $y = 3v$ と書いておくと，$3z^2 = x^2 + y^2 = 9(u^2 + v^2)$ となるので，両辺を 3 で割ると $z^2 = 3(u^2 + v^2)$ となって，z^2 が 3 の倍数であることがわかる．ゆえに，z も 3 の倍数である．

(III) ここからが本番である．背理法の仮定から，D は空集合でないので，D に属する (x, y, z) のうちで x の値が最小であるものが少なくとも 1 つは存在する．そのような (x, y, z) を任意に一つ選ぶ．(II) から，x, y, z はそれぞれ 3 の倍数である．よって，$x = 3x'$, $y = 3y'$, $z = 3z'$ ($x', y', z' \in \mathbb{N}$) と分解できる．これらを $x^2 + y^2 = 3z^2$ に代入すると，$9x'^2 + 9y'^2 = 27z'^2$ となるが，この両辺を 9 で割れば，$x'^2 + y'^2 = 3z'^2$ となる．つまり，$(x', y', z') \in D$ である．ところが，$x' < x$ なので，これは (x, y, z) の選び方 (x の最小性) に矛盾する．以上から，$x^2 + y^2 = 3z^2$ を満たす自然数の組 (x, y, z) は存在しない． □

この証明では，x が最小であるというギリギリいっぱいのところを攻めていて，その最小性を用いてうまく矛盾を導いている．このように，最小 (あるいは極小) であるところを突いて，実はそれよりも小さいものが存在することを示すことで最小性 (あるいは極小性) に反するという矛盾を導く証明法は**無限降下法**と呼

[*6] 最小反例法で書かれた証明は，後で述べる帰納法を用いて (背理法を用いずに) 書き直すことができるものも多い．

ばれている.[*7] これも最小反例法の一種と見ることができる.[*8]

♦ 例 2.21 (この例では線型代数学の基本的な知識を仮定する.) V を実ベクトル空間とする. V がその部分集合 E で**生成**されるとは, どのベクトル $x \in V$ も有限個の元 $v_1, \dots, v_m \in E$ と係数 $r_1, \dots, r_m \in \mathbb{R}$ らを用いて

$$x = \sum_{i=1}^{m} r_i v_i$$

という形式の和——$v_1, \dots, v_m$ らの**線型結合**——で記述できることを言う. V が**有限生成**であるとは, V が有限な部分集合 E で生成できることを言う. また, V の部分集合 E が**線型独立**であるとは, 有限個の任意の元 $v_1, \dots, v_m \in E$ および任意の係数 $r_1, \dots, r_m \in \mathbb{R}$ らについて

$$\sum_{i=1}^{m} r_i v_i = 0 \implies r_1 = r_2 = \cdots = r_m = 0$$

が成り立つことを言う. 空集合 $\emptyset$ は空虚な意味で線型独立である. V の**基底**とは, V の線型独立な部分集合でなおかつ V 全体を生成するものを言う.

さて, V が有限生成であるとき, V は必ず基底を持っていることを示そう. 仮定から, V は有限な部分集合 E で生成される. $\mathcal{P}$ を E の部分集合で線型独立であるものの全体とする. これは冪集合 2^E の部分集合であるが, E は有限集合だから 2^E も有限集合であり, したがって $\mathcal{P}$ も有限集合である. そして, $\emptyset \in \mathcal{P}$ だから, $\mathcal{P}$ 自身は空集合ではない. よって, 演習 2.7 から, $\mathcal{P}$ には集合の包含順序について極大な元 P が存在する. $P \in \mathcal{P}$ なので, P は E に含まれる線型独立な部分集合である.

P に属さない任意の元 $x \in E$ を考えて, $Q = P \cup \{x\}$ とおく. これは E の部分集合である. $x \notin P$ だから, Q は P よりも真に大きい. もし Q が線型独立ならば, $Q \in \mathcal{P}$ であるが, Q は P よりも真に大きいから, これは P が $\mathcal{P}$ の極大元であることに矛盾してしまう. よって, Q は線型独立ではない. したがって, ある $v_1, \dots, v_m \in P$ および実数 $r, r_1, r_2, \dots, r_m \in \mathbb{R}$ に対して

$$rx + \sum_{i=1}^{m} r_i v_i = 0$$

であり, なおかつ $r, r_1, \dots, r_m$ のうち少なくとも一つは 0 ではない. $r = 0$ とすると, $\sum_{i=1}^{m} r_i v_i = 0$ であるが, P は線型独立なので $r_1 = \cdots = r_m = 0$ であり, したがって $r, r_1, \dots, r_m$ は全て 0 になってしまう. したがって, $r \neq 0$ であり,

$$x = \sum_{i=1}^{m} \left(-\frac{r_i}{r}\right) v_i$$

となって x は P で生成できることになる. ゆえに, P は E に属する全ての元を生成できる.

任意の $x \in V$ を考える. E は V 全体を生成するので, ある $v_1, \dots, v_m \in E$ および実数 $r_1, r_2, \dots, r_m \in \mathbb{R}$ に対して

$$x = \sum_{i=1}^{m} r_i v_i$$

*7 反例 x_0 が存在するならば, それよりも真に小さい x_1 が存在し, 同様にしてそれよりも真に小さい反例が存在し…というように, 反例の無限降下を引き起こす論法であることから「無限降下法」と呼ばれている.

*8 細かく見れば, 例 2.17, 例 2.18, 2.19 では, 最小の反例が実は反例ではなかったというオチであったが, 例 2.20 では最小の反例が実は「最小」ではなかったというオチであるという違いがある.

と書ける．ここで，各々の v_i は P で生成できるので，

$$v_i = \sum_{j=1}^{m_i} r_{i,j} w_{i,j}, \quad (r_{i,j} \in \mathbb{R},\ w_{i,j} \in P)$$

という形式で書ける．よって，

$$x = \sum_{i=1}^{m} r_i v_i = \sum_{i=1}^{m} r_i \left(\sum_{j=1}^{m_i} r_{i,j} w_{i,j} \right) = \sum_{i=1}^{m} \sum_{j=1}^{m_i} r_i r_{i,j} w_{i,j}$$

であるが，これは x が P に属するベクトル $w_{i,j}$ らの線型結合であることを示している．ゆえに，P は V 全体を生成する．以上から，P は V の基底である．

この議論は V が複素ベクトル空間であっても同様に通用する．そして実は，V が「有限生成である」という仮定は不要であり，任意のベクトル空間に基底が存在することも，ほぼ同様の議論で言える．上の議論で V が有限生成でない場合に問題になるのは，$\mathcal{P}$ が有限であるとは限らなくなるせいで，その極大元 P が存在することが自明ではなくなることである．この問題点については，次の項で説明する「Zorn の補題」と呼ばれるものを用いれば解決できる． □

2.6 Zorn の補題

極大性・極小性は便利な概念であり，これまでいくつかの例を見てきたように，うまく利用すれば様々な定理を効果的に証明することができる．実際，数学における重要な定理の中でも，極大性や極小性を巧みに利用して証明されるものは多い．例 2.21 で述べた「有限生成なベクトル空間は基底を持つ」という定理はそのいい一例である．

有限な空でない順序集合であれば，演習 2.7 で見た通り必ず極大元および極小元が存在するので，安心して極大元や極小元を利用できる．一方で，無限順序集合は極大元や極小元を持たないことがあり得る．例えば，$\mathbb{Z}$ は通常の大小順序の下で全順序集合であるが，どの $x \in \mathbb{Z}$ に対しても，$x+1$ は x よりも大きいので，x は $\mathbb{Z}$ の極大元ではない．すなわち，$\mathbb{Z}$ にはそもそも極大元が全く存在しない．

順序集合における極大元の存在については，下の定理 3.8 が応用上とくに重要であり，広く用いられている．順序集合 X が**帰納的**であるとは，X 上の鎖が全て上に有界であることを言う．[*9] ここで，X 上の**鎖**とは全順序部分集合のこと，つまり X の部分集合でその中のどの 2 つの元も互いに比較可能であるものを言う．論理的には，空部分集合や単元部分集合も鎖であり，これらは上に有界である．

Zorn の補題

定理 2.22. 空でない帰納的順序集合は極大元を持つ．

♦ **例 2.23**　X を $\mathbb{N}$ の有限部分集合の全体とする．X は集合の包含順序について順序集合である．X は帰納的ではない．実際，

$$\{1\} \subseteq \{1,2\} \subseteq \{1,2,3\} \subseteq \cdots$$

[*9] 空集合も空虚な意味で鎖であるが，それは空虚な意味で上に有界なので，X 上の空でない鎖が全て上に有界であれば，X が帰納的であるには十分である．

は X 上の鎖であるが, これは上に有界ではない. 空でない任意の $A \in X$ に対して, A に属する最大の自然数 n に対して $A \subsetneq \{1, 2, \dots, n+1\}$ であり, A がこの鎖の上界になることはあり得ないからである. また, これと同様の議論から, X は極大元を持たないことも言える.

注意! Zorn の補題は, 帰納的順序集合には極大元が存在することを主張するが, 逆に**帰納的でない順序集合には極大元が存在しないとは言っていない**. (この例の X が極大元を持たないのは, Zorn の補題による帰結ではない.) 例えば, $\mathbb{N}$ に整除順序を導入した順序集合を考えて, その部分集合

$$X = \{2^1, 2^2, 2^3, \dots\} \cup \{3\}$$

を考えれば, X は上に有界でない鎖 $2^1 < 2^2 < 2^3 < \cdots$ を持つから帰納的ではないが, 3 は X の極大元である. このように, Zorn の補題は順序集合が極大元を持つための一つの十分条件を与えているが, それは必要条件ではない. □

詳細は付録 B で述べるが, Zorn の補題は選択公理と同値であることが知られている. つまり, **Zorn の補題は順序関係の言葉を用いた選択公理の別表現**である. ここでは, Zorn の補題の応用事例をいくつか見ておくことにしよう. いずれの例も, ある帰納的順序集合を作ってその極大元を Zorn の補題を利用して得たのち, 極大性をうまく利用して何らかの結果を証明しようというものである.

♦ **例 2.24**　例 2.21 で, V が有限生成であるという前提を外してみよう. V を (有限生成とは限らない) 実ベクトル空間として, V が基底を持つことを証明する. 基本的なアイデアは例 2.21 と変わらない.

E を V の部分集合で V 全体を生成するものとする. (例えば, $E = V$ でもよい. V が有限生成であれば E として有限な部分集合を選べたが, 今はその保証はない.) $\mathcal{P}$ を E の部分集合で線型独立であるものの全体とする. これは空集合を含んでいるから, $\mathcal{P}$ 自身は空集合ではない. $\mathcal{P}$ は集合の包含順序について順序集合になっていて, これの極大元を利用したい. しかし, 今は E が有限集合とは限らず, したがって $\mathcal{P}$ も有限集合である保証はないので, 例 2.21 と違って気軽に $\mathcal{P}$ の極大元を取るというわけにはいかない.

そこで, Zorn の補題の出番である. まず, $\mathcal{P}$ が帰納的であることを示す. $\{P_i\}_{i \in I}$ を $\mathcal{P}$ 上の空でない鎖として, これが $\mathcal{P}$ において上に有界であることを示せばよい. $P = \bigcup_{i \in I} P_i$ とおく. どの P_i も E の部分集合なので, $P \subseteq E$ である. P が線型独立であることを示す. $v_1, \dots, v_m \in P$, $r_1, \dots, r_m \in \mathbb{R}$ かつ $\sum_{k=1}^{m} r_k v_k = 0$ であると仮定する. どの v_k もある P_{i_k} に属しているが, $\{P_i\}_{i \in I}$ は鎖だから, 一般性を失わず $P_{i_1} \subseteq P_{i_2} \subseteq \cdots \subseteq P_{i_m}$ であると仮定してもよい. すると, 全ての $v_1, \dots, v_m$ は P_{i_m} に属するが, P_{i_m} は線型独立なので, $r_1 = \cdots = r_m = 0$ である. よって, P は線型独立であり, したがって $P \in \mathcal{P}$ である. そして, どの $i \in I$ についても $P_i \subseteq P$ だから, P は $\mathcal{P}$ における $\{P_i\}_{i \in I}$ の上界である. 以上から, $\mathcal{P}$ は帰納的であることが言えた.

ここで, Zorn の補題を使えば, $\mathcal{P}$ に極大元 P が存在することが分かる. この後は, 例 2.21 と同じ要領で P が V の基底であることが言える. □

♦ **例 2.25**　X, Y を空でない集合, $f : X \to Y$ を任意の写像とする. f が X の部分集合 E 上で単射であるとは, 始域を E に制限した写像 $f|_E : E \to Y$ が単射であること, すなわち $x, x' \in E$, $f(x) = f(x')$ ならば $x = x'$ が成り立つことを言うものとする. X の部分集合 E で, 次の 2 条件を満たすものが存在することを示す:

E1: f は E 上で単射である.

E2: 任意の $x \in X$ に応じて, $f(x) = f(e)$ を満たす $e \in E$ が存在する.

X の部分集合 E で条件 E1 を満たすものの全体を $\mathcal{E}$ で表す．これは $\emptyset$ および全ての単元部分集合 $\{x\}$ $(x \in X)$ を含んでおり，空ではない．$\mathcal{E}$ は集合の包含順序の下で順序集合になっている．

これの極大元 E は条件 E1, E2 を満たしていることを先に確認しておく．まず，$E \in \mathcal{E}$ なので条件 E1 は成り立つ．条件 E2 を考える．$x \in X$ とするとき，$x \in E$ であれば，$e = x$ に対して $e \in E$ かつ $f(x) = f(e)$ となる．$x \notin E$ のとき，$E' = E \cup \{x\}$ は E よりも真に大きいから，E の $\mathcal{E}$ における極大性から $E' \notin \mathcal{E}$ である．よって，f は E' 上では単射ではない．したがって，相異なる 2 つの元 $a, b \in E'$ で $f(a) = f(b)$ を満たすものが存在する．f は E 上では単射なので，$a, b \in E$ ではあり得ず，a または b のうち一方は x である．一般性を失わず $a = x$ とするとき，$e = b$ に対して $e \in E$, $f(x) = f(e)$ が成り立つ．よって，条件 E2 も満たされる．

これで，後は $\mathcal{E}$ の極大元を取るだけでよくなった．X が有限集合であれば，$\mathcal{E}$ も有限集合だから，$\mathcal{E}$ が極大限を持つことは演習 2.7 から明らかである．問題なのは X が無限集合の場合であるが，その場合には次のようにして Zorn の補題を利用して $\mathcal{E}$ が極大元を持つことを保証する．$\mathcal{E}$ が帰納的であることを示そう．$\{E_i\}_{i \in I}$ を $\mathcal{E}$ 上の空でない鎖として，これが $\mathcal{E}$ において上に有界であることを示せばよい．$E = \bigcup_{i \in I} E_i$ とおく．$x, x' \in E$, $f(x) = f(x')$ と仮定する．それぞれ，$x \in E_{i_1}$, $x' \in E_{i_2}$ となる $i_1, i_2 \in I$ が存在するが，$\{E_i\}_{i \in I}$ は鎖だから，一般性を失わず $E_{i_1} \subseteq E_{i_2}$ と仮定できる．すると，$x, y \in E_{i_2}$ であるが，E_{i_2} は条件 E1 を満たしているので，$x = x'$ が従う．よって，E は条件 E1 を満たしており，$E \in \mathcal{E}$ が成り立つ．そして，全ての $i \in I$ について $E_i \subseteq E$ であり，E は $\mathcal{E}$ における $\{E_i\}_{i \in I}$ の上界である．以上から，$\mathcal{E}$ は帰納的であり，したがって Zorn の補題からそれは極大元を持つことが保証される． □

♦ **例 2.26**　X を集合，R をその上の順序関係とするとき，X 上には R を含む全順序関係が存在することを示そう．つまり，X 上の順序関係は全て，何らかの全順序関係の一部になっているということである．

X 上の順序関係で R を含むものの全体集合を $\mathcal{X}$ で表す．$R \in \mathcal{X}$ なので，$\mathcal{X} \neq \emptyset$ である．$\mathcal{X}$ は集合の包含順序の下で順序集合であるが，それが帰納的であることを示そう．$\{R_i\}_{i \in I}$ を $\mathcal{X}$ 上の空でない鎖として，$R_* = \bigcup_{i \in I} R_i$ とおく．全ての $i \in I$ について，$R \subseteq R_i \subseteq R_*$ である．R_* が順序関係であることも次のようにして分かる．

- 任意の $x \in X$ について，R の反射性から $(x, x) \in R \subseteq R_*$ である．よって，R_* は反射的である．
- $(x, y) \in R_*$ かつ $(y, z) \in R_*$ と仮定する．それぞれ，$(x, y) \in R_i$, $(y, z) \in R_j$ となる $i, j \in I$ が存在するが，$\{R_i\}_{i \in I}$ は鎖なので，$R_i \subseteq R_j$ または $R_i \supseteq R_j$ である．前者の場合には，$(x, y) \in R_i \subseteq R_j$, $(y, z) \in R_j$ なので，R_j の推移性から $(x, z) \in R_j \subseteq R_*$ である．後者の場合にも同様にして，R_i の推移性から $(x, z) \in R_i \subseteq R_*$ が言える．よって，R_* は推移的である．
- $(x, y) \in R_*$ かつ $(y, x) \in R_*$ と仮定する．それぞれ，$(x, y) \in R_i$, $(y, x) \in R_j$ となる $i, j \in I$ が存在するが，$\{R_i\}_{i \in I}$ は鎖なので，$R_i \subseteq R_j$ または $R_i \supseteq R_j$ である．前者の場合には，$(x, y) \in R_i \subseteq R_j$, $(y, x) \in R_j$ なので，R_j の反対称性から $x = y$ である．後者の場合にも同様にして，R_i の反対称性から $x = y$ が言える．よって，R_* は反対称的である．

ゆえに，$R_* \in \mathcal{X}$ であり，これは $\mathcal{X}$ における鎖 $\{R_i\}_{i \in I}$ の上界である．したがって，$\mathcal{X}$ は帰納的である．

ここで，Zorn の補題から $\mathcal{X}$ が極大元を持つことが言える．[*10] S を $\mathcal{X}$ の任意の極大元とする．S は R を含む順序関係であるが，これが全順序であることを示せばよい．S が全順序ではないとすると，S

[*10] X が有限集合であれば，$\mathcal{X}$ も有限集合であり，その極大元を得るために Zorn の補題は不要である．

に関して比較不可能な 2 つの元 $x, y \in X$ が存在する．ここで，$K = \{(a,b) \in X^2 \mid (a,x), (y,b) \in S\}$，$S' = S \cup K$ とおく．$R \subseteq S \subseteq S'$ であり，さらに S' は順序関係である (→演習 2.8)．よって，$S' \in \mathcal{X}$ であるが，一方で $(x,y) \notin S$ かつ $(x,y) \in K \subseteq S'$ なので $S \subsetneq S'$ である．これは S が $\mathcal{X}$ の極大元であることに反する．以上から，S は R を含む全順序である．□

▶ **演習 2.8**　例 2.26 で，S' が X 上の順序関係であることを示せ．

X を順序集合とする．X 上の鎖 (全順序部分集合) C が**極大鎖**であるとは，X が C を真に含む鎖を持たないことを言うものとする．

命題 2.27. X を空でない順序集合とし，上に有界な極大鎖を持っていると仮定する．このとき，X は極大元を持つ．

証明. X が上に有界な極大鎖 C を持っていると仮定する．$x \in X$ を C の上界とする．$a \in X$, $x < a$ とすると，a もまた C の上界であり，なおかつ $a \notin C$ である．(x は C の上界なので，もし $a \in C$ であれば $x \leq a$ であるはず.) よって，$\bar{C} = C \cup \{a\}$ は C よりも真に大きな鎖であるが，C が極大鎖なのでこれはあり得ない．ゆえに，X には x より真に大きな元は存在せず，x は X の極大元である．□

この命題も，順序集合が極大元を持つための十分条件を鎖を用いて記述しているところは Zorn の補題と共通している．こちらでは，X の全ての鎖が上に有界であることは要求されていないが，そのかわり上に有界な ‘極大’ な鎖が存在するというところで鎖の極大性が要求されている．この命題を利用すると，Zorn の補題を直接的に言い換えた別の有用な表現を得ることができる．それを次の 2 つの演習問題にしておこう．

▶ **演習 2.9** (Hausdorff の極大性原理)　Zorn の補題は次の主張と同値であることを証明せよ．

任意の順序集合において，全ての鎖は極大鎖に含まれている．

集合族 $\mathcal{F}$ が**有限的**であるとは，それが任意の集合 X について次の条件を満たすことを言うものとする:

$X \in \mathcal{F}$ であるためには，X の全ての有限部分集合が $\mathcal{F}$ に属することが必要十分である．

▶ **演習 2.10** (Teichmüller-Tukey の補題)　Zorn の補題は次の主張と同値であることを証明せよ．

空でない有限的な集合族は集合の包含関係に関する極大元を持つ．

3 整列順序と帰納法

この節では，整列順序と呼ばれる特別な種類の順序関係を取り扱う．整列順序は数学的帰納法に代表される帰納法と呼ばれる証明手法と深い関係にある他，自然数の「ものの順序を数える」という機能を一般化した概念である「順序数」と呼ばれる数概念を構成する際に用いられる重要な順序構造である (→第 5 巻『集合の濃度と順序数』)．

3.1 整列順序とは

$(X, \leq)$ を順序集合とする．

整列順序と整列集合

定義 3.1. $\leq$ が X 上の**整列順序**であるとは, X の空でない全ての部分集合 A について最小元 $\min A$ が存在することを言う. 整列順序が設定された順序集合を**整列集合**と呼ぶ.

定義から, X が整列集合ならば, その部分集合も (X と同じ順序の下で) 整列集合である.

命題 3.2. 整列順序は全順序である.

証明. $x, y \in X$ とする. $\leq$ は整列順序だから, $z = \min\{x, y\}$ が存在する. z は x, y のうちどちらかであるが, $x = z$ ならば $x \leq y$ であるし, $y = z$ ならば $y \leq x$ である. □

♦ **例 3.3**　整列順序の代表例は, $\mathbb{N}$ 上での通常の大小順序である. しかし, $\mathbb{Z}$ 上では通常の大小順序は全順序ではあるが整列順序ではない. 例えば, $\min \mathbb{Z}$ は存在しない. □

♦ **例 3.4**　X, Y を整列集合とする. $X \times Y$ では, 直積順序 (→例 1.4(1)) は一般に全順序ですらない. 実際, X, Y が共に 2 個以上の元を持っているとき, $x_1 < x_2$, $y_1 < y_2$ を満たす元 $x_1, x_2 \in X$, $y_1, y_2 \in Y$ を取れば, (x_1, y_2) と (x_2, y_1) は直積順序について比較可能ではない.

一方, $X \times Y$ 上で辞書式順序 (→例 1.4(2)) は整列順序である. 実際, A を $X \times Y$ の空でない部分集合とするとき, 次の手順で辞書式順序に関する最小元 $\min A$ を見つけることができる.

S1: $A \neq \emptyset$ だから, $A_X = \{x \in X \mid$ ある $y \in Y$ について $(x, y) \in A$ である$\}$ は X の空でない部分集合である. よって, $x_0 = \min A_X$ が存在する.

S2: $x_0 \in A_X$ だから, $A_Y = \{y \in Y \mid (x_0, y) \in A\}$ は Y の空でない部分集合であり, $y_0 = \min A_Y$ が存在する.

このとき, $(x_0, y_0) = \min A$ であることが, 次のようにして分かる. まず, x_0, y_0 の選び方から $(x_0, y_0) \in A$ であることは明らかである. 任意の $(x, y) \in A$ を取る. A_X の定義から $x \in A_X$ だから, $x_0 \leq x$ である. $x_0 < x$ ならば, $(x_0, y_0) < (x, y)$ である. $x_0 = x$ のときは, $y \in A_Y$ であり, $y_0 \leq y$ および $(x_0, y_0) \leq (x, y)$ が成り立つ. ゆえに, いずれにせよ $(x_0, y_0) \leq (x, y)$ である. 以上から, $(x_0, y_0) = \min A$ である. □

♦ **例 3.5**　Σ を空でない整列集合, Σ^* を Σ 上の文字列の全体とする. 例 1.4 で見たように, Σ の整列順序は Σ^* 上の辞書式順序を導く. $|\Sigma| \geq 2$ であるとき, この辞書式順序は全順序ではあるが整列順序ではない. 実際, Σ が相異なる 2 つの元 0, 1 $(0 < 1)$ を含んでいるとき,

$$1 > 01 > 001 > 0001 > \cdots$$

であり, この降鎖に現れる文字列の全体 $A = \{1, 01, 001, 0001, \dots\}$ について最小元 $\min A$ が存在しない.

一方で, 長さに基づく辞書式順序は整列順序である. A を Σ^* の空でない任意の部分集合として, 長さに基づく辞書式順序について $\min A$ が存在することを示す. A に属する文字列の長さの最小値を n とする. $n = 0$ のときは $\min A = \lambda$ (空文字列) なので, $\lambda \notin A$, $n \geq 1$ と仮定してよい. A に属する文字列のうちで長さが n であるものの全体を $A_n = \{w \in A \mid |w| = n\}$ とする. (絶対値記号 $|w|$ は文字列 w の長さを表す.) 長さに基づく辞書式順序では, 文字列の大小比較の際にまず長さの比較が行われるので, $\min A$ は A_n の中にある. そこで, $\min A_n$ が求められれば, それが $\min A$ である. $\min A_n$ を求めるための次の手続きを考える. ここで, 文字列 w に対して w_k は w の k 番目の文字を表す.

S1: (初期設定) $L = A_n$ とおく.

S2: $k = 1, 2, \ldots, n$ の順番で次の S2a と S2b を繰り返す.

S2a: $u_k = \min\{w_k \mid w \in L\}$ とおく. (この min は Σ における最小元を表す.)

S2b: L から $w_k = u_k$ ではない文字列 w を全て削除する.

S3: $u = u_1 u_2 \cdots u_n$ を出力して停止する.

この手続きで得られる文字列 u が $\min A_n$ であり, したがってそれが $\min A$ である. □

3.2　整列可能定理

集合 X 上に何らかの整列順序を設定することを X を**整列する**と言う. 整列と言うと, 図 10 のようなイメージが思い浮かぶかも知れないが, このイメージはあながち間違っていない. 最小元 $x_0 = \min X$ が先頭で, それを除く中で最小の元 x_1 がその次で, x_0 と x_1 を除く中で最小の元 x_2 がその次で…という具合にして, X の元が $x_0 < x_1 < x_2 < \cdots$ というように整列されていくからである. このイメージがそぐわないところもないわけではない. 例えば, 図 10 では先頭を除くどの人にもその「直前」の人がいるが, これは一般の整列集合では必ずしも言えない. (直前の元については, 後の 3.3 項で述べる.)

図 10　整列のイメージ. (『いらすとや』から引用)

X が有限集合ならば, X の元を任意の順番で一列に列挙して, その順番で $x_1 < x_2 < \cdots < x_n$ であると定義すれば, X を整列できる. X が無限集合であっても, 全単射 $f : X \to \mathbb{N}$ が存在ならば, これを利用して任意の $x, y \in X$ に対して

$$x \leq y \overset{\text{def}}{\iff} f(x) \leq f(y)$$

と定義すれば X を整列できるが, これは要するに f が順序同型となるように X を整列しようということである. X が $\mathbb{N}$ との間に全単射を持たないぐらいに '大きな' 無限集合であるときには, このような手軽な整列手法を提示するのは簡単ではない. しかし, 実は X が非可算集合であったとしても, 選択公理を認めておけば, X を整列すること自体は原理的には可能である.

整列可能定理

定理 3.6. 任意の集合は整列順序を持つ.

この定理によれば, 例えば $\mathbb{R}$ も整列できる. もちろん, その整列順序は通常の大小順序とは違う順序である. さらに言えば, 例えば $2^{2^{\mathbb{R}}}$ (冪集合 $2^{\mathbb{R}}$ の冪集合) のようなもっとややこしい集合であっても, 原理的には必ず整列できると主張しているのが整列可能定理である. ただし, 整列可能定理は整列順序の**存在**を主張

するのみである. 例えば, 具体的に $2^{2^{\mathbb{R}}}$ を整列したいと言っても, 具体的にどうしたらいいのかということはまた別問題である.

詳しいことは付録 B で説明するが, Zorn の補題と同じように, 整列可能定理は選択公理と論理的には全く同値であり, **整列可能定理もまた順序集合の言葉を借りた選択公理の別表現である**ことが知られている. 歴史的には, Ernst Zermelo が整列可能定理を証明しようとして, 現在では選択公理として認識されていることを一つの原理として利用したことが一大論争を巻き起こし, 選択公理にスポットライトが当たるきっかけを作った. ちなみに, この Zermelo が ZF 公理系の 'Z' である.

☕ Coffee Break ☕

選択公理は自明だが整列可能定理は偽?

第 2 巻『写像』第 6 節で述べたように, 選択公理は「空でない集合らに渡る直積集合は空ではない」「空でない集合らに対しては選択関数 (あるいは選択集合) が存在する」という主張である. これは直観的には自明だと思う人の方が多いだろう. 一方で, それと論理的に同値であるはずの整列可能定理になると, 一気に雲行きが怪しくなる. 例えば, $2^{2^{\mathbb{R}}}$ のようなややこしい集合であっても必ず整列できると言われても, にわかには信じ難い.

The Axiom of Choice is obviously true,
the well-ordering principle obviously false,
and who can tell about Zorn's lemma?
— Jerry Bonna

これはもちろん, 選択公理, 整列可能定理, Zorn の補題が全て論理的には同値であることを踏まえてのジョークである. 確かに, Zorn の補題は自明だともウソだともよくわからない, 絶妙な塩梅の主張である.

3.3 極限元と後続元

$(X, \leq)$ を整列集合とする. 任意の $x \in X$ について, x よりも真に大きな元の全体を

$$X^{\uparrow}(x) \overset{\text{def}}{=} \{a \in X \mid x < a\}$$

で表す. $x = \max X$ であれば $X^{\uparrow}(x) = \emptyset$ であるが, そうでなければ $X^{\uparrow}(x) \neq \emptyset$ である.[*11] $\leq$ は整列順序なので, もし $x \neq \max X$ であれば $X^{\uparrow}(x)$ に最小元が存在する. それは x より真に大きな元のうちで最も小さい元なので, それを x の**直後**と呼び, 記号で

$$x + 1 \overset{\text{def}}{=} \min X^{\uparrow}(x)$$

と表すことにする. この記法は「x の直後である」ことを印象的に表すシンボルに過ぎず,「x に 1 を加える」という意味ではない. とは言うものの, もし $x + 1 \neq \max X$ であれば $x + 1$ の直後 $(x + 1) + 1$ が存在するが, それを $x + 2$ で表すなどということは自然な成り行きである. この調子で一般に, $x + n$ の直後

*11 $\leq$ は全順序なので, 演習 2.6(2) から, $x \neq \max X$ であれば x は極大元ではなく, したがって $x < y$ となる元 $y \in X$ が存在する. その y は $X^{\uparrow}(x)$ に属するから, $X^{\uparrow}(x) \neq \emptyset$ である.

$(x+n)+1$ が存在する限りそれを $x+(n+1)$ で表す．もちろん, $x+0=x$ であると考えるのも自然なことである．

一方, x の「直前」についてはどうだろうか．それは

$$X^{\downarrow}(x) \overset{\text{def}}{=} \{a \in X \mid a < x\} \tag{5}$$

の最大元であると考えるのが相応しいだろう．一般的には $X^{\downarrow}(x)$ に最大元が存在するとは限らないが, もしそれが存在するならば, それを

$$x-1 \overset{\text{def}}{=} \max X^{\downarrow}(x)$$

で表し, x の**直前**と呼ぶ．もちろん, この記法も「x の直前である」ことを印象的に表すに過ぎず,「x から 1 を引く」という意味ではない．直後の元の場合と同様に, $x-n$ の直前がある限りそれを $(x-n)-1=x-(n+1)$ で表す．また, $x-0=x$ であると考えるのも自然である．

▶ **演習 3.1** 整列集合 X において, $x=y+1$ ならば $y=x-1$ であることを示せ.[*12]

$x=\min X$ であれば $X^{\downarrow}(x)=\emptyset$ だから, $x-1$ が存在しないのは当たり前である．一方で, $x>\min X$ であるときには, 確かに $X^{\downarrow}(x)$ は空集合ではないが, それに最大元が存在するかどうかはまた別問題である．実際, $x>\min X$ であってもその直前 $x-1$ が存在しないこともあり得る．

♦ **例 3.7** 例 3.4 から, 辞書式順序が導入された $\mathbb{N}\times\mathbb{N}$ は整列集合である．$(2,1)$ はその最小元ではないが, 直前の元を持たない．$(x,y)<(2,1)$ であれば, $x=1$ であり, したがって $(x,y)<(x,y+1)<(2,1)$ となるから, (x,y) は $(2,1)$ の直前ではあり得ない． □

$x\in X$ が**後続元**であるとは, x がある別の元 y の直後であることを言う．演習 3.1 から, これは x の直前が存在することと同じである．x が $\min X$ でも後続元でもないとき, x は**極限元**であると言う.[*13]

▶ **演習 3.2** X を空でない整列集合とする．$\min X$ および極限元をまとめて**非後続元**と呼ぶことにする．このとき, 任意の元 $x\in X$ は

$$x=a+n \quad (a \text{ は非後続元}, n\in\mathbb{N}_0)$$

の形式で一意的に表されることを証明せよ．

3.4 整列性と超限帰納法

整列順序は**数学的帰納法**と関係が深い概念である．ここでは, 整列集合上で展開される一般的な帰納法を説明する．

まず, 最も基本的な $\mathbb{N}$ 上での数学的帰納法を復習しておく．自然数 n に関する命題関数 $P(n)$ があるとき, これが全ての $n\in\mathbb{N}$ について真であることを証明するために, 次の 2 つのステップを踏む．

(1) **基本ステップ**: $P(1)$ を証明する．
(2) **帰納ステップ**: ($n\geq 2$ のとき) $P(n-1)$ を仮定して, $P(n)$ を証明する．

[*12] くどいけど, 見た目だけで「こんなの当たり前だ」とは思わないこと．これは直後・直前の定義に従って証明する練習である．
[*13] この定義では, $\min X$ は後続元でも極限元でもない．$\min X$ を極限元に含める文献もあるので, 他書を見る際には要注意．

これで $P(n)$ が全ての n について真であることが証明される．その理屈は第 1 巻『集合と論理』例 3.11 で紹介したが, もう一度その議論を振り返っておこう．

> $P(n)$ が偽となる $n \in \mathbb{N}$ の全体を F とする．$F \neq \emptyset$ と仮定する．$\mathbb{N}$ は整列集合なので, F の最小値 $n = \min F$ が存在する．基本ステップから, $P(1)$ は正しいので, $1 \notin F$ である．よって, $n \geq 2$ である．n の最小性から $n-1 \notin F$ なので, $P(n-1)$ は真である．したがって, 帰納ステップから $P(n)$ も真である．ゆえに $n \notin F$ であるが, 一方で $n = \min F$ だから $n \in F$ でもあり, 不合理である．よって, $F = \emptyset$ である．したがって, $P(n)$ は全ての $n \in \mathbb{N}$ について真である．

この議論のキーポイントは, $F \neq \emptyset$ ならば最小元 $\min F$ が存在するはずだという部分である．これはまさに整列順序の定義条件と同じ構造である．

これと同じようなことを一般の整列集合 $(X, \leq)$ 上で考えよう．ただし, 一般の整列集合上では, 上記の議論で言う n に対する $n-1$ に相当するものをどうするかが問題になる．$n-1$ は n の直前の元であるが, 例 3.7 で見た通り, 一般の整列集合ではたとえ $x > \min X$ であっても直前の元 $x-1$ が存在しない場合があり得る．このような場合に対応するにはどうすればよいだろうか．$x-1$ は次の集合

$$X^{\downarrow}(x) = \{w \in X \mid w < x\}$$

の最大元であるが, ここでは $x-1$ にこだわるのではなく, $X^{\downarrow}(x)$ そのものを利用することが有効である．

超限帰納法の原理

定理 3.8. 整列集合 X の部分集合 P が次の条件式を満たすならば, $P = X$ である:

$$\text{全ての } x \in X \text{ について:} \quad X^{\downarrow}(x) \subseteq P \Rightarrow x \in P. \tag{6}$$

証明. 対偶を証明する．$P \subsetneq X$ ならば, $P^{\mathrm{c}} = X \setminus P$ は X の空でない部分集合である．$\leq$ は整列順序だから, 最小元 $x = \min P^{\mathrm{c}}$ が存在する．$w \in X^{\downarrow}(x)$ とすると, $w < x = \min P^{\mathrm{c}}$ だから $w \notin P^{\mathrm{c}}$, つまり $w \in P$ である．ゆえに, $X^{\downarrow}(x) \subseteq P$ である．しかし $x \notin P$ なので, x は条件式 (6) を破っている． □

整列集合 X 上の元 x に関する命題関数 $P(x)$ があって, これが全ての $x \in X$ について真であることを証明したいとする．そのために, 次のことを証明する:

T1: $x = \min X$ に対して $P(x)$ は真である．
T2: ($x > \min X$ のとき) $w < x$ である全ての $w \in X$ について $P(w)$ が真ならば, $P(x)$ も真である．

これで, 全ての $x \in X$ について $P(x)$ が真であることを証明できる．この論法が**超限帰納法**である．その理屈は次の通りである．集合 P を次の式で定める:

$$P = \{x \in X \mid P(x) \text{ が真である}\}.$$

T2 によれば, $X^{\downarrow}(x) \subseteq P$ であれば $x \in P$ でもあるから, 定理 3.8 から $P = X$ が成立する．したがって, $P(x)$ は全ての $x \in X$ について真である．

$x = \min X$ の場合には, T2 でやるべきことは

$$[w \in X^{\downarrow}(x) \Rightarrow P(w)] \Rightarrow P(x)$$

という論理式を証明することであるが, $X^{\downarrow}(x) = \emptyset$ だから $w \in X^{\downarrow}(x) \Rightarrow P(w)$ は必ず真 (True) であり*14, したがって T2 で示すべきことは True $\Rightarrow P(x)$ であること, つまり $P(x)$ が真であること, ということになる. これが T1 である.

例えば, $\mathbb{N}$ 上では次のような帰納法が通用する:

- **基本ステップ**: $P(1)$ が真であることを示す.
- **帰納ステップ** ($n \geq 2$ のとき): $P(1), P(2), \dots, P(n-1)$ が全て真ならば, $P(n)$ も真であることを示す.

普通の数学的帰納法と比べて, 帰納ステップがやや違っている. つまり, 普通の数学的帰納法では $P(n-1)$ のみを仮定するが, ここでは $P(n-1)$ だけではなく, $P(1)$ から $P(n-1)$ までを全て仮定として用いてよいことになっている点が違っていて, 使用できる仮定が増えている. もっとも, この程度のことなら, $Q(n) = P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ に対する通常の数学的帰納法だと考えることもできる. ただ, **「$n-1$ の場合を仮定して n の場合を示す」ことだけが帰納法ではない**ということは知っておいて損はない.

♦ **例 3.9** (Euclid の互除法と拡張互除法)　超限帰納法を利用して, 任意の整数 a, b に対して

$$ax + by = \gcd(a, b) \tag{7}$$

を満たす整数 x, y が存在することを示そう. ここで, gcd は最大公約数を表している.

(I) $b \neq 0$ とし, a を b で割った時の商を q, 余りを r とするとき, $\gcd(a, b) = \gcd(b, r)$ であることを示そう. a を b で割ったときの商を q, 余りを r とするとき, $0 \leq r < |b|$, $a = bq + r$ である. $\alpha = \gcd(a, b)$, $\beta = \gcd(b, r)$ とおく. $a = bq + r$ であり, かつ b と r は共に β の倍数だから, a も β の倍数である. ゆえに, β は a と b の公約数である. したがって, $\beta | \alpha$ である. 一方, $r = a - bq$ であり, かつ a と b は共に α の倍数だから, r も α の倍数である. ゆえに, α は b と r の公約数であり, したがって $\alpha | \beta$ である. 以上から, $\gcd(a, b) = \alpha = \beta = \gcd(b, r)$ である.

(II) 0 以上の整数を動く変数 k について, 次の命題関数 $P(k)$ を考える:

> $P(k)$: 任意の整数 a, b (ただし $|b| \leq k$) について, $ax + by = \gcd(a, b)$ を満たす整数の組 (x, y) が存在する.

これが全ての $k \geq 0$ について成り立つことを証明すればよいが, ここに超限帰納法を用いる. (0 以上の整数の全体 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ が整列集合であることを用いる.) 任意の $k > 0$ について次のことを証明すればよい:

> 任意の $0 \leq k' < k$ について $P(k')$ が成り立つならば, $P(k)$ も成り立つ.

a, b を整数, $|b| \leq k$ とする. $b = 0$ ならば $\gcd(a, b) = a$ なので, $(x, y) = (1, 0)$ とおくと, $ax + by = \gcd(a, b)$ となる. ($x = 1$ でさえあれば, y の値はどうでもよい.)

$|b| > 0$ とする. a を b で割った商を q, 余りを r とすると, $a = bq + r$, $0 \leq r < |b|$ である. $|r| < |b| \leq k$ なので, 超限帰納法の仮定から $P(|r|)$ は真である. よって, 整数 x', y' で $bx' + ry' = \gcd(b, r) = \gcd(a, b)$ となるものが存在する. (最後の等号は (I) から従う.) これに $r = a - bq$ を代入すると, $bx' + (a - bq)y' = \gcd(a, b)$ となる. よって, $(x, y) = (y', x' - qy')$ に対して $ax + by = \gcd(a, b)$

*14 仮定部の $w \in X^{\downarrow}(x)$ が必ず False だからである.

Algorithm Euclid

input: 整数 a, b (ただし $(a,b) \neq (0,0)$).

output: 最大公約数 $\gcd(a,b)$.

begin algorithm

$b=0$ ならば, a を出力して終わる.

($b \neq 0$ のとき): $a = bq + r$ $(0 \leq r < |b|)$ と分解する.

再帰的に $\gcd(b,r)$ を求めて, それを出力して終わる.

end of the algorithm.

図 11　Euclid の互除法.

である．これが $|b| \leq k$ である任意の a, b について成り立つので, $P(k)$ も真である．これで式 (7) の証明は完了した.

(I) で示されたことを利用すると, 任意の整数組 $(a,b) \neq (0,0)$ に対して最大公約数 $\gcd(a,b)$ を「余りのある除法」だけを用いて求めることができる簡単な再帰的アルゴリズムが得られる (図 11)．このアルゴリズムは **Euclid の互除法**と呼ばれていて, 計算量が比較的少なくて済み, コンピュータ上でも簡単に実装できて便利なので, 実際に広く使われている．例として $a=108$, $b=45$ の最大公約数を互除法を用いて手計算で求めてみよう:

$$\begin{aligned} 108 &= 2 \times 45 + 18, &\qquad \gcd(108,45) &= \gcd(45,18) \\ 45 &= 2 \times 18 + 9, & \gcd(45,18) &= \gcd(18,9) \\ 18 &= 2 \times 9 + 0 & \gcd(18,9) &= \gcd(9,0) \end{aligned}$$

なので,

$$\gcd(108,45) = \gcd(45,18) = \gcd(18,9) = \gcd(9,0) = 9$$

である．互除法の計算過程では, $\gcd(\bullet,\bullet)$ の第 2 項目の値が $45 \to 18 \to 9 \to 0$ というように着実に減少して最後は 0 に辿り着くことに注目しておこう．したがって, 余りのある除法を際限無く繰り返すという必要はなく, 必ずいつかは計算が終わる.

さらに進んで, 超限帰納法の部分の議論から, $ax + by = \gcd(a,b)$ となる整数組 (x,y) を求める再帰的アルゴリズムを構成することもできる (**拡張互除法**, 図 12)．例として, 先ほどと同じ $a=108$, $b=45$ の場合について, 拡張互除法を手計算で実行してみよう.

(1-1) $108 = 2 \times 45 + 18$ $(q=2,\ r=18)$ と分解する.

(1-2) $45x_0 + 18y_0 = \gcd(45,18)$ となる整数 x_0, y_0 が求まれば, $(x,y) = (y_0, x_0 - 2y_0)$ を出力して終わればよい.

(2-1) そこで x_0, y_0 を求めよう．まず $45 = 2 \times 18 + 9$ $(q=2,\ r=9)$ と分解する.

(2-2) $18x_1 + 9y_1 = \gcd(18,9)$ となる整数 x_1, y_1 が求まれば, $(x_0,y_0) = (y_1, x_1 - 2y_1)$ と置けばよい.

(3-1) そこで, x_1, y_1 を求めよう．$18 = 2 \times 9 + 0$ $(q=2,\ r=0)$ と分解する.

(3-2) $9x_2 + 0y_2 = \gcd(9,0) = 9$ となる整数 x_2, y_2 が求まれば, $(x_1,y_1) = (y_2, x_2 - 2y_2)$ と置けばよい．ここでは $(x_2,y_2) = (1,0)$ としておけば十分なので, $(x_1,y_1) = (y_2, x_2 - 2y_2) = (0,1)$ である.

Algorithm GeneralizedEuclid

input: 整数 a, b (ただし $(a,b) \neq (0,0)$).

output: $ax + by = \gcd(a,b)$ となる整数 x, y.

begin algorithm

$b = 0$ ならば, $(x,y) = (1,0)$ を出力して終わる.

($b \neq 0$ のとき): $a = bq + r$ $(0 \leq r < |b|)$ と分解する.

$bx' + ry' = \gcd(b,r)$ となる整数 x', y' を再帰的に求める.

$(x,y) = (y', x' - qy')$ を出力して終わる.

end of the algorithm.

図 12 Euclid の拡張互除法.

(4) ここで (2-2) に戻ると, $(x_0, y_0) = (y_1, x_1 - 2y_1) = (1, -2)$ となる.

(5) さらに (1-2) に戻ると, $(x,y) = (y_0, x_0 - 2y_0) = (-2, 5)$ となる. これを出力して停止する.

以上から,

$$-2 \times 108 + 5 \times 45 = 9$$

となるが, 先に見た通り $\gcd(108,45) = \gcd(45,18) = \gcd(18,9) = \gcd(9,0) = 9$ だから, $(-2) \times 108 + 5 \times 45 = \gcd(108,45)$ であることがわかる. □

♦ **例 3.10** 例 2.19 では, 整数成分の 2 次正則行列 x で行列式 $\det x = 1$ を持つものは次の 2 つの行列 s, t で生成できることを, 最小反例法によって証明した:

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

その証明は, ほとんどそのままの形で, x の $(2,1)$-成分 x_{21} の絶対値 $|x_{21}|$ に関する超限帰納法を用いて書き換えることができる. まず, 基本ステップは $|x_{21}| = 0$ (つまり $x_{21} = 0$) の場合であるが, この場合に主張が正しいことは例 2.19 の (I) の議論から明らかである.[*15] $|x_{21}| > 0$ の場合は, 例 2.19 の (II) での議論と同じように, x_{11} を x_{21} で割って商を q, 余りを r $(0 \leq r < |x_{21}|)$ とすれば, $st^{-q}x$ の $(2,1)$-成分が r になることから (→式 (3)), それに対して帰納法の仮定を使えば $st^{-q}x = x_3 x_4 \cdots x_n$ $(x_i \in \{s, t, s^{-1}, t^{-1}\})$ と書けて, したがって x は式 (4) のようにして s, t で生成できることが言える. □

3.5 整礎順序と整礎帰納法

整列順序とは, 任意の空でない部分集合に最小元が存在するという順序であるが, この定義条件を少し緩めて, 最小元の代わりに極小元の存在を要求したものを整礎順序と言う. すなわち, 集合 X 上の順序関係が**整礎順序**であるとは, X の空でない全ての部分集合に対して極小元が存在することを言う. 整列順序が設定された順序集合を「整列集合」と言うように, 整礎順序が設定された順序集合を**整礎集合**と言う.

[*15] 例 2.19 の (I) では背理法が使われているが, その議論はそのまま基本ステップ $x_{21} = 0$ の証明に使える.

命題 3.11. X を集合, $\leq$ を X 上の順序関係とする. $\leq$ が整礎順序であるためには, X の元から成る任意の無限降鎖

$$x_1 \geq x_2 \geq \cdots \geq x_n \geq \cdots$$

が有限であることが必要十分である. ただし, この降鎖が「有限」であるとは, ある番号 n が存在して,

$$x_n = x_{n+1} = x_{n+2} = \cdots$$

が成立することを言う.

証明. (I) $\leq$ が整礎順序であると仮定して, X 上の無限降鎖は全て有限であることを示す. X 上で任意の無限降鎖 $x_1 \geq x_2 \geq \cdots \geq x_n \geq \cdots$ を考えて, ここに現れる元 x_i らの全体を A とする. A は X の空でない部分集合であるが, $\leq$ は整礎順序だから, A は極小元を持つ. それは A の元のいずれかであるから, 仮に x_n が A の極小元であるとしておこう. $m \geq n$ であるとき, $x_n \geq x_m$ であるが, $x_m \in A$ であり, x_n は A の極小元であるから, $x_m = x_n$ である. ゆえに, $x_n = x_{n+1} = x_{n+2} = \cdots$ となる.

(II) $\leq$ が整礎的ではないと仮定して, X 上に有限ではない無限降鎖が存在することを示す. $\leq$ は整礎的でないから, X の空でない部分集合 A で極小元を持たないものが存在する. $A \neq \emptyset$ なので, A から任意に一つの元 x_1 を選ぶことができる. これは A の極小元ではないので, $x_1 > x_2$ となる $x_2 \in A$ が存在する. x_2 も A の極小元ではないので, $x_2 > x_3$ となる $x_3 \in A$ が存在する. これを繰り返せば, A 上で有限ではない無限降鎖 $x_1 > x_2 > \cdots > x_n > \cdots$ が生じる. □

補足 3.12 上記の (II) の議論は一見素直ではあるが, 実はちょっとゴマカシがある. 上の議論で示していることは, 任意の自然数 n について長さが n の有限降鎖があること, そして $n+1$ 個目の元をその最後に付け加えることができるということだけであり, このことと「無限降鎖が存在する」ことの間には, 厳密に言えばギャップがある.

このギャップは選択公理を用いて回避できる. 任意の $x \in A$ に対して, $A_x = \{a \in A \mid a < x\}$ とおく. 仮定から x は A の極小元ではないので, $A_x \neq \emptyset$ である. よって, 選択公理から, 関数 $f : A \to X$ で全ての $x \in A$ について $f(x) \in A_x$, つまり $f(x) \in A$ かつ $f(x) < x$ となるものが存在する. 任意の $x_1 \in A$ から開始して, 以下再帰的に $x_n = f(x_{n-1})$ $(n \geq 2)$ と定義すれば, 望み通りの無限降鎖 $x_1 > x_2 > \cdots$ が得られる. □

定義から, 整列順序は全て整礎順序でもある. この逆は一般に成立せず, 整礎順序は必ずしも整列順序ではなく, それどころか全順序であるとも限らない. 例えば, 有限集合上で定義される順序関係は, それが全順序であってもなくても全て整礎順序である. 全順序集合上では極小元は全て最小元でもあるので (→演習 2.6(2)), 全順序な整礎集合は全て整列集合である. つまり, **整列集合とは「全順序な整礎集合」に他ならない**.

♦ **例 3.13** X を $\mathbb{Z}$ の有限部分集合の全体として, その上で包含順序を考える. A を X の空でない部分集合とする. A のそれぞれの要素 a は $\mathbb{Z}$ の有限部分集合であるから,

$$I = \{|a| \mid a \in A\}$$

は $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ の空でない部分集合である. $\mathbb{N}_0$ は通常の大小順序の下で整列集合だから, $n = \min I$ が存在する. A の中から $|a| = n$ となる任意の集合 a を選べばそれは A の極小元である. ゆえに, X は整礎集合である. この X は全順序集合ではないので, 整列集合ではない.

一方で, $\mathbb{Z}$ の冪集合 $2^{\mathbb{Z}}$ を考えると, $\mathbb{Z}$ の無限部分集合も話の中に入ってくるので, 上記の議論は通用しない. 実際, 冪集合 $2^{\mathbb{Z}}$ 上では集合の包含順序は整礎順序ではなく, 例えば

$$\mathbb{Z} \supsetneq \{0\}^{\mathrm{c}} \supsetneq \{0,1\}^{\mathrm{c}} \supsetneq \{0,1,2\}^{\mathrm{c}} \supsetneq \cdots$$

のように有限ではない降鎖が存在する. ここで, c は $\mathbb{Z}$ における補集合を表している. □

♦ **例 3.14** X, Y を順序集合とし, 直積集合 $X \times Y$ 上に直積順序 $\preceq$ (→例 1.4(1)) を考える. X, Y がそれぞれが整列集合であっても $\preceq$ は必ずしも整列順序ではなく, それどころか全順序であるとすら限らない. 一方で, X, Y が整礎集合であれば, $\preceq$ も整礎順序であることは次のようにして確かめられる.

A を $X \times Y$ の空でない部分集合として, これが $\preceq$ に関して極小元を持つことを示せばよい.

$$A_1 = \{x \in X \mid \text{ある } y \in Y \text{ に対して } (x,y) \in A \text{ である}\},$$
$$A_2 = \{y \in Y \mid \text{ある } x \in X \text{ に対して } (x,y) \in A \text{ である}\}$$

とおく. $A \neq \emptyset$ なので, $A_1, A_2 \neq \emptyset$ である. X, Y は整礎集合だから, A_1 の極小元 a と A_2 の極小元 b がそれぞれ存在する. $a \in A_1$ だから, $(a,d) \in A$ となる $d \in Y$ が存在するが, Y は整礎集合だから, そのような d のうちで極小であるものが存在する. (a,d) は A の極小元であることを示す. $(x,y) \in A$, $(x,y) \preceq (a,d)$ とする. $(x,y) \in A$ だから $x \in A_1$ であり, $(x,y) \preceq (a,d)$ なので $x \leq a$ である. したがって, A_1 における a の極小性から $x = a$ である. $(a,y) = (x,y) \preceq (a,d)$ なので $y \leq d$ であり, したがって d の極小性から $y = d$ である. よって, $(x,y) = (a,d)$ である. ゆえに, (a,d) は A の極小元である. なお, この主張は命題 3.11 を用いて証明することもできる (→演習 3.3). □

▶ **演習 3.3** 例 3.14 の主張を, 命題 3.11 を用いて証明せよ.

X 上に整礎順序 $\leq$ が設定されているとき, これを用いて整列集合における超限帰納法と同様のことができる.

整礎帰納法の原理 (cf. 定理 3.8)

定理 3.15. 整礎集合 X の部分集合 P が全ての $x \in X$ について次の条件式を満たすならば, $P = X$ である:

$$X^{\downarrow}(x) \subseteq P \Rightarrow x \in P. \tag{8}$$

証明. 定理 3.8 の証明とほとんど同じである. 対偶を証明する. $P \subsetneq X$ ならば, $P^{\mathrm{c}} = X \setminus P$ は X の空でない部分集合である. $\leq$ は整礎順序だから, P^{c} の極小元 x が存在する. (ここでは, x は P^{c} の最小元であるとは限らない.) $w \in X^{\downarrow}(x)$ とすると, $w < x$ であるが, x は P^{c} の極小元であるから, $w \in P^{\mathrm{c}}$ ではない. つまり, $w \in P$ である. ゆえに, $X^{\downarrow}(x) \subseteq P$ である. しかし $x \notin P$ なので, x は条件式 (8) を破っている. □

♦ **例 3.16** $\mathbb{N}$ 上の通常の大小順序は整列順序だから, それはもちろん整礎順序でもある. 一方で, 整除順序 (約数・倍数の関係) は全順序ではないので整列順序ではないが, 整礎順序にはなっている.

例 2.17 では, 全ての自然数が素因数分解を持つことを, 最小の反例を利用した背理法によって証明したが, その議論は $\mathbb{N}$ 上の整除順序に基づく整礎帰納法の例とも見ることができる. 実際, その議論は「整除

順序に関して n 未満の自然数は有限個の素数の積である」という帰納法の仮定から n が有限個の素数の積であることを導く議論になっているとも読める. □

次の演習は, 同義反復的な物言いだが, 整礎帰納法が通用する順序集合は必ず整礎集合であることを示している.

▶ **演習 3.4** $(X, \leq)$ を任意の順序集合とする. X の部分集合 P が全ての $x \in X$ について式 (8) を満たすときには, 必ず $P = X$ であると仮定する. このとき, $\leq$ は整礎順序であることを証明せよ.

3.6 再帰的定義と構成的定義

帰納法はもちろん証明手法としても有効であるが, 定理の証明だけではなく, 集合, 写像, 数列など様々な数学的対象を定義する際にも利用できる考え方である. 本シリーズの中でも, 既にそのような考え方を何度か用いている.

♦ **例 3.17** 自然数 n に対して, 1 から n までの自然数の積 $n(n-1)(n-2)\cdots 1$ を n の**階乗**と言い, $n!$ と表す. $n = 0$ に対しては特別に $0! = 1$ と約束しておく. この階乗関数を

$$f(n) = \begin{cases} 1 & (n = 0 \text{ のとき}) \\ nf(n-1) & (n \geq 1 \text{ のとき}) \end{cases} \tag{9}$$

と定義することもできる. ここでは, f の定義に f 自身を利用しているが, このような**循環的定義**は「発電機を発明するために発電機が必要」という訳の分からない話になるので, 本来ならば禁忌である. 式 (9) の定義も一見すると循環的だが, 実際は関数 f の定義として正当な意味を持つ. $f(n)$ を定めるためには, n 未満の m に対する $f(m)$ が定まっていればよいという**帰納法的な構造**であることがポイントである. この定義に従えば, 例えば $n = 4$ のときは

$$\begin{aligned} f(4) &= 4 \times f(3) \\ &= 4 \times 3 \times f(2) \\ &= 4 \times 3 \times 2 \times f(1) \\ &= 4 \times 3 \times 2 \times 1 \times f(0) \\ &= 4 \times 3 \times 2 \times 1 \end{aligned}$$

となる. 最後の等号は基本ステップ $f(0) = 1$ から従うもので, ここで式変形が停止する. このように, 帰納法的な考え方を使った定義を**再帰的定義**と言う. $f(n)$ を計算するために $f(n-1)$ らを利用することを, f を**再帰的に利用する**と言う. 基本ステップは再帰の連鎖を止める役割を果たすが, 再帰的定義ではこのように**再帰連鎖の回数が必ず有限である**ことを保証しておく必要がある. □

♦ **例 3.18** 数列の**漸化式**は数列を再帰的に定義する方法の一例である. 例えば,

$$a_n = \begin{cases} 1 & (n \in \{1, 2\} \text{ のとき}) \\ a_{n-1} + a_{n-2} & (n \geq 3 \text{ のとき}) \end{cases} \tag{10}$$

は数列 $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$ を定めている. $n = 1, 2$ の場合が基本ステップに当たり, $n \geq 3$ のときの定めが再帰ステップに当たる. ここでは, 基本ステップが $n = 1$ と $n = 2$ の 2 通り必要であることにも注意しよう. 式 (10) で定まる数列は **Fibonacci 数列**という有名な数列である. □

♦ **例 3.19** (素数の再帰的定義)　$\mathbb{N}$ の部分集合 P を次のように定義する:

(1) $2 \in P$ である.
(2) 任意の $x \in \mathbb{N}$ $(x \geq 3)$ について: $x \in P$ となるのは, x 未満の全ての $a \in P$ について a が x の約数ではないときであり, かつそのときに限る.

$x = 2, 3, 4, 5, 6, \cdots$ に対して, $x \in P$ であるかどうかを考えてみよう.

- (1) から, $2 \in P$ である.
- $x = 3$ のとき: 3 未満の P の元は $a = 2$ だけであり, そして $2 \nmid 3$ なので, (2) から $3 \in P$ である.
- $x = 4$ のとき: 4 未満の P の元は $a = 2, 3$ であるが, $2|4$ なので, (2) から $4 \notin P$ である.
- $x = 5$ のとき: 5 未満の P の元は $a = 2, 3$ であるが, そのいずれについても $a \nmid 5$ なので, (2) から $5 \in P$ である.
- $x = 6$ のとき: 6 未満の P の元は $a = 2, 3, 5$ であるが, $3|6$ なので, (2) から $6 \notin P$ である.

この調子で考えていくと, P は素数の全体であることがわかるだろう. (1) は基本ステップであり, (2) は帰納ステップに当たる. (2) では, $x \in P$ であるか否かを決定するために, x 未満の a に対する条件しか使っていないところがポイントである. □

♦ **例 3.20**　$\{A_i\}_{i \in I}$ を集合族とするとき, これに対して次の 3 条件を満たす集合族 $\{B_i\}_{i \in I}$ が存在することを示そう. ただし, 添字集合 I は有限であるとは限らない.

U1: 全ての $i \in I$ について $B_i \subseteq A_i$ である.
U2: $\bigcup_{i \in I} A_i = \bigcup_{i \in I} B_i$ である.
U3: $i, j \in I$, $i \neq j$ ならば $B_i \cap B_j = \emptyset$ である.

まず, I に任意の整列順序を導入しておく. $0 = \min I$ に対して $B_0 = A_0$ とおき, $i > \min I$ のときには超限再帰を用いて

$$B_i = A_i \setminus \bigcup_{j \in I[j<i]} B_j$$

とおく. ここで, $\bigcup_{j \in I[j<i]} B_j$ は $j < i$ を満たす全ての $j \in I$ に渡る B_j らの和集合であり, B_i を定義する際には $j < i$ なる全ての j に対して B_j が既に決まっていることを超限再帰的に仮定しているという構造である. この定義から, 条件 U1 は明らかに成立する. U1 から $\bigcup_{i \in I} A_i \supseteq \bigcup_{i \in I} B_i$ であることは明らかである. これの逆向きの包含を示そう. $x \in \bigcup_{i \in I} A_i$ として, $x \in A_i$ となる最小の $i \in I$ を考える. $i = 0$ ならば $x \in A_0 = B_0$ である. $i > 0$ とする. i の最小性から, $j < i$ ならば $x \notin A_j$ であり, したがって U1 から $x \notin B_j$ でもある. よって, $x \in A_i$, $x \notin \bigcup_{j<i} B_j$ であり, B_i の定義から $x \in B_i$ である. ゆえに, $\bigcup_{i \in I} A_i \subseteq \bigcup_{i \in I} B_i$ でもある. これで U2 が示された. $i \neq j$ のとき, 一般性を失わず $i > j$ と仮定すると, B_i の定義から $B_i \cap B_j = \emptyset$ である. よって, U3 も成立する. □

▶ **演習 3.5**　例 3.19 に倣って, 正の奇数の全体を再帰的に定義せよ.

▶ **演習 3.6**　自然数 n に対して, その約数の個数を対応させる関数 $\sigma : \mathbb{N} \to \mathbb{N}$ の再帰的定義を与えよ.

▶ **演習 3.7**　A から Z までのアルファベットの大文字 26 文字から成る文字列が入力として与えられたとき, それが回文になっているか否かを判定するための (なるべく簡単な) 再帰的アルゴリズムを与

えよ．ここで，回文とは，例えば “ROTOR” や “ABBA” のように左から読んでも右から読んでも同じ文字列を言う．

再帰的定義とは趣が異なるが，**構成的定義**も様々な概念の定義によく利用される．これは，ある概念を定義する際に，それを作り上げる基本材料と構成法を明示するという方法である．

♦ **例 3.21**　「偶集合」という概念の構成的定義として次の定義を考えてみよう．

P1: 空集合 $\emptyset$ は偶集合である．
P2: 相異なる任意の整数 x, y について，$\{x, y\}$ は偶集合である．
P3: A, B を互いに交わらない偶集合とすると，$A \cup B$ は偶集合である．
P4: A が偶集合であるとは，A が上記の P1–P3 を有限回用いて得られることを言う．(それ以外の場合は A は偶集合ではないという意味も込められている.)

構成的定義では，この最後の条件 P4 のような締めくくりの条件が付けられるのが一般的であり，**P4 が省略されている場合でも実際には P4 に相当する条件が仮定されていると考える**のが普通である．

この定義に従って，例えば $A = \{2, 3, 5, 6\}$ が偶集合であることは次のようにして具体的に A を構成することで確かめられる:

- P2 から，$\{2, 3\}$ は偶集合である．同様に，$\{5, 6\}$ は偶集合である．
- $\{2, 3\}$, $\{5, 6\}$ は互いに交わらない偶集合なので，P3 から $A = \{2, 3\} \cup \{5, 6\}$ は偶集合である．

これで，P1–P3 を有限回用いて (実際には，P2 と P3 のみを用いて) A が得られている．この例では，「偶集合」とはまさに $\mathbb{Z}$ の有限部分集合で偶数個の元から成るもののことである．なお，P2–P4 だけでは空集合が偶集合であることは出てこないので，空集合については個別に P1 にて偶集合であると定めている．　□

♦ **例 3.22**　多項式を構成的に定義すると，次のような感じになる．ただし，係数は実数であるものとして，変数は n 個あるものとしておく．

P1: 任意の実数および各々の変数 $x_1, x_2, \ldots, x_n$ は多項式である．
P2: f, g が多項式ならば，$f + g$ および fg も多項式である．
P3: P1 と P2 を有限回適用して得られる式，かつそのような式だけが，n 変数多項式である．

要するに，係数と変数を基本材料として，和と積を取る操作を有限回繰り返して作られる式が多項式だというわけである．　□

♦ **例 3.23**　V を実ベクトル空間，S をその部分集合とするとき，「S で生成される元」を次のように構成的に定義する．

P1: ゼロベクトル 0 および S に属する元は全て S で生成される．
P2: x, y が S で生成されるならば，$x + y$ も S で生成される．
P3: x が S で生成されるならば，全ての実数 c について cx も S で生成される．
P4: P1–P3 を有限回適用して S で生成される元のみを「S で生成される元」と認める．

この意味で S で生成される元の全体 $\langle S \rangle$ は,

$$x = \sum_{i=1}^{n} r_i v_i, \qquad (r_1, \dots, r_n \in \mathbb{R},\ v_1, \dots, v_n \in S)$$

という形式の有限和で記述できる元 x の全体に一致する. (ただし $n = 0$ のときは, この和はゼロベクトルを表していると考える.) これは S が生成する部分空間であり, それはすなわち V の中で S を部分空間で最小のものである. □

一般に, ある概念 P の構成的定義が与えられたとき, x が P に該当することは, 少なくとも原理的には実際にその構成的定義に従って x を構成できることを具体的な手順と共に示せば確かめることができる. しかし, x が P に**該当しない**ことの証明は必ずしも簡単ではない. 例えば, 次のような方法が考えられる:

- どのような構成手順に従っても, 有限回のステップでは x が構成できないことを示す. これには, 背理法を用いて x を構成する手順が存在すれば何らかの矛盾が導かれることを示すという方法があり得る. 例えば, x を構成するための最短の手順を仮定すれば, それをうまく変形すればさらに短い手順が構成できて最短性に反することを示せばいいのかもしれない. あるいは, x が構成可能であれば, その手順をうまく変形すれば, 既に構成不可能であることが分かっている別の x' が構成できてしまうことを示すというやり方もあり得る.
- x が構成可能であれば満たしているはずの何らかの条件に注目して, x がそれを満たしていないことを示す. 例えば, 上記の例 3.21 の場合, 偶集合は必ず偶数個の元から成っているので, 奇数個の元から成る集合は偶集合ではないと結論できる.

一般的に言って,「不可能である」ことを示すことは「可能である」ことを示すよりも難しいことが多い.

3.7 整列集合の比較定理

X を整列集合とする. 任意の元 $x \in X$ について, X の x における**切片**を

$$X(x) = \{a \in X \mid a < x\}$$

と書く. 式 (5) ではこれを $X^{\downarrow}(x)$ と書いていたが, ここでは $\downarrow$ を省略して記号を簡略化する. 本項では, 任意の整列集合 X, Y が与えられたとき, 両者が同型である場合は別として, そうでない場合はどちらかがどちらかの切片として埋め込まれることを示す. 目標は次の定理を確立することである.

整列集合の比較定理

定理 3.24. X, Y を整列集合とするとき, 次の 3 つのうちちょうどどれか一つだけが成立する (図 13).

S1: X と Y は同型である.
S2: X は Y のある切片に同型である.
S3: Y は X のある切片に同型である.

X, Y を任意の整列集合とする. まず最初に, $x_1 = \min X$ と $y_1 = \min Y$ を取り出す. 次は, x_1 の後続元 $x_2 \in X$ と y_1 の後続元 $y_2 \in Y$ をそれぞれ取り出す. 続けて, x_2, y_2 の後続元 $x_3 \in X$, $y_3 \in Y$ をそれぞれ

図 13 定理 3.24 のイメージ．2 つの整列集合が同型である様子 (左) と, 一方がもう一方の切片になっている様子 (右).

取り出す．この操作を繰り返していき, もし先に X の方が空っぽになったら S2 が成立して, Y が先に空っぽになったら S3 が成立する．そして, X と Y が同時に空っぽになった時には S1 が成立する．これが定理 3.24 の簡単なイメージである．

これは運動会の玉入れ競争の結果判定と同じような簡単な理屈ではあるが, もちろん X, Y は有限集合とは限らないので, この議論だけでは数学的な証明としては不十分である．正確な証明にはもっと精密な議論が必要である．

まずは準備として, 整列集合における切片集合の基本的な性質を調べておこう．一般に任意の順序集合 X において, 部分集合 A が**下に単調**であるとは, どの $x \in X$ についても

$$x \leq a,\ a \in A \Rightarrow x \in A$$

が成り立つことを言う．(論理的には, $A = \emptyset$ も空虚な意味で下に単調である.) 任意の切片集合 $X(x)$ が下に単調であることは順序の推移性から明らかである．$X(x)$ は x を含まないので, 必ず X の真部分集合である．

補題 3.25. X を整列集合, A をその真部分集合で下に単調であるものとする．このとき, $A = X(x)$ となる $x \in X$ が唯一つ存在する．

証明. A は真部分集合なので, 補集合 $A^c = X \setminus A$ は空ではない．そして X は整列集合だから, 最小元 $x = \min A^c$ が存在する．A は下に単調であり, かつ $x \notin A$ なので, $x \leq y$ であれば $y \notin A$ でもある．これの対偶から, $y \in A$ ならば $x > y$, つまり $y \in X(x)$ となる.[*16] よって, $A \subseteq X(x)$ である．これの逆向きの包含を示そう．$z \in X(x)$, つまり $z < x$ とするとき, x は A^c で最小なので $z \notin A^c$, つまり $z \in A$ である．よって, $A \supseteq X(x)$ でもあり, $A = X(x)$ が成り立つ．

x の一意性を示す．ある $y \in X$ に対して $A = X(y)$ でもあると仮定する．$y \notin A$, つまり $y \in A^c$ だから, x の選び方から $x \leq y$ である．ここで $x < y$ であれば, $x \in X(y) = A = X(x)$ となり, $x < x$ が出て矛盾する．よって, $x = y$ である．これで x の一意性も言えた． □

この補題から, 整列集合 X では下に単調な真部分集合はまさに切片のことであり, なおかつ x によって $X(x)$ は全て異なることがわかった．

さて, いくつかの自然数を小さい順に $x_1 < x_2 < x_3 < \cdots$ と並べていくと, k 番目の数 x_k は必ず k 以上である．次の補題は, この簡単な事実の一般化である．

補題 3.26. X を整列集合, $f : X \to X$ を単調な単射とするとき, 全ての $x \in X$ について $x \leq f(x)$ である．

証明. $E = \{x \in X \mid x > f(x)\}$ とおく．$E \neq \emptyset$ と仮定すると, X の整列性から $x = \min E$ が存在する．$x \in E$ なので, $f(x) < x$ である．x は E で最小なので $f(x) \notin E$ であり, したがって $f(x) \leq f(f(x))$ である．一方で, f は単射かつ単調なので, $f(x) < x$ から $f(f(x)) < f(x)$ であり, $f(x) \leq f(f(x))$ に矛盾する．よって, $E = \emptyset$ である．つまり, 全ての $x \in X$ について $x \leq f(x)$ である． □

[*16] 整列順序は全順序なので, $x \leq y$ でなければ $x > y$ であることにも注意.

この補題を利用して, 整列集合はその切片部分集合とは決して同型にならないことを示す.

補題 3.27. X を整列集合とするとき, X からその切片の中への単調な単射は存在しない. 特に, X はその切片とは同型にならない.

証明. $f: X \to X(x)$ がある切片 $X(x)$ の中への単調な単射であるとする. f は $X(x)$ の中への写像なので $f(x) \in X(x)$, したがって $f(x) < x$ であるが, これは補題 3.26 に反する. よって, X からその切片への単調な単射は存在しない. 同型写像は単調な単射なので, X からその切片への同型写像も存在しない. □

さて, $x < x'$ ならば, 切片 $X(x')$ は x を含むが, $X(x')$ の x における切片 $X(x')(x)$ は切片 $X(x)$ と同じである. よって, 補題 3.27 から次の補題も直ちに得られる. つまり, 相異なる点における切片どうしは決して同型にはならない.

補題 3.28. X を整列集合, $x, x' \in X$ とするとき, $X(x)$ と $X(x')$ が同型であるのは $x = x'$ であるときに限る.

X が有限であれば, この補題は理解しやすい. そもそも $x \neq x'$ のときには, $X(x)$ と $X(x')$ では元の個数が違うから同型にはなり得ない. X が無限であるときには, $x \neq x'$ であっても $X(x)$ と $X(x')$ は全単射で結ばれる可能性はある. しかし, その全単射は順序集合の同型写像ではあり得ない.

さて, 以上の準備をもとに, 定理 3.24 の証明を始めよう. まず, S1, S2, S3 は互いに排反な条件であることを確認しておく. S1 と S2 が両立するならば, S2 からある $y \in Y$ に対して同型 $f: X \to Y(y)$ が存在して, S1 から同型 $g: Y \to X$ が存在するが, このとき合成 $f \circ g: Y \to Y(y)$ も同型となって, Y はその切片 $Y(y)$ と同型であることになり, 補題 3.27 に矛盾する. だから, S1 と S2 は排反である. 同様の理由で, S1 と S3 も排反であることが分かる. S2 と S3 が両立するならば, ある $x \in X$, $y \in Y$ に対して同型 $f: X \to Y(y)$ と $g: Y \to X(x)$ がそれぞれ存在する. $e: Y(y) \to Y$ を包含写像とすると, 合成 $g \circ e \circ f$ は X から $X(x)$ への単調な単射となるが, これは補題 3.27 に矛盾する. ゆえに, S2 と S3 も排反である. 以上から, S1, S2, S3 は全て排反である.

これで, 後は S1, S2, S3 のうちのどれかが成立することを示せば, 定理 3.24 の証明が完了する. $X = \emptyset$ のときには, X は Y の最小値 $y = \min Y$ における切片 $Y(y)$ と同型である. $Y = \emptyset$ のときも対称的に同様のことが言える. 以下, $X, Y \neq \emptyset$ の場合のみを考える. X にも Y にも属さない特別な元 $\perp$ を用意する. 超限再帰を用いて, 各々の $x \in X$ に対して $f(x) \in Y \cup \{\perp\}$ を次のように定める:

X1: $f(\min X) = \min Y$ とおく.

X2: $x > \min X$ として, 超限再帰的に, 全ての $x' \in X(x)$ について $f(x')$ が既に決まっていることを仮定する. $Y_x = \{f(x') \mid x' \in X(x)\}$ とおく. $Y_x \subsetneq Y$ ならば, $f(x) = \min(Y \setminus Y_x)$ とおく. それ以外の場合, つまり $Y_x = Y$ または $\perp \in Y_x$ の場合は, $f(x) = \perp$ とおく.

$x = \min X$ に対しては特別に $Y_x = \emptyset$ と定めることにすれば, どの $x \in X$ についても

$$Y_x \subsetneq Y \Rightarrow f(x) = \min(Y \setminus Y_x)$$

が成り立つことに注意しておく.

補題 3.29. $x \in X$, $Y_x \subseteq Y$ とする.

(1) $Y_x \subsetneq Y$ ならば, 全ての $x' \in X(x)$ について $f(x') = \min(Y \setminus Y_{x'})$ である.

(2) $f(x) = \perp \iff Y_x = Y$.

(3) Y_x は下に単調である.

(4) $f(x) \in Y$ であれば, $f(x)$ は $Y_x = Y(y)$ を満たす唯一つの元 $y \in Y$ である.

(5) $x_1, x_2 \in X(x)$, $x_1 < x_2$ ならば, $f(x_1) < f(x_2)$ である.

証明. (1) $x' \in X(x)$ ならば, $x' < x$ なので, $Y_{x'} \subseteq Y_x \subsetneq Y$ である. よって, $f(x') = \min(Y \setminus Y_{x'})$ である.

(2) $f(x) = \perp$ と仮定する. $x = \min X$ ならば, X1 から $f(x) = \min Y \neq \perp$ のはずだから, $x > \min X$ である. よって, $f(x)$ は X2 に従って決まる. 仮定から $Y_x \subseteq Y$ なので, $\perp \in Y_x$ ではない. よって, もし $Y_x \subsetneq Y$ ならば, $f(x) = \min(Y \setminus Y_x) \neq \perp$ であるはずだから, $Y_x = Y$ である.

逆に, $Y_x = Y$ と仮定すると, $x > \min X$ であり, X2 から $f(x) = \perp$ である.

(3) $Y_x = Y$ であれば, Y_x は下に単調だから, $Y_x \subsetneq Y$ と仮定しておいてよい. $y < y'$, $y' \in Y_x$ ならば, $y \in Y_x$ であることを示せばよい. $y' \in Y_x$ なので, ある $x' \in X(x)$ を用いて $y' = f(x')$ と書ける. (1) から $y' = f(x') = \min(Y \setminus Y_{x'})$ であるが, 一方で $y < y'$ だから, $y \notin Y \setminus Y_{x'}$, すなわち $y \in Y_{x'}$ である. $x' < x$ なので, $X(x') \subseteq X(x)$, したがって $Y_{x'} \subseteq Y_x$ であり, ゆえに $y \in Y_x$ でもある.

(4) $f(x) \in Y$ とする. $f(x) \neq \perp$ だから, (2) から $Y_x \subsetneq Y$ であり, かつ (3) から Y_x は下に単調である. よって, 補題 3.25 から $Y_x = Y(y)$ となる $y \in Y$ が唯一つ存在する. そして, $f(x) = \min(Y \setminus Y_x) = \min(Y \setminus Y(y)) = y$ である.

(5) $x_1, x_2 \in X(x)$, $x_1 < x_2$ とする. $f(x_1), f(x_2) \in Y_x \subseteq Y$ であり, したがって (4) から $Y(f(x_1)) = Y_{x_1} \subseteq Y_{x_2} = Y(f(x_2))$ である. よって, $f(x_1) \leq f(x_2)$ である.[*17] $x_1 < x_2$ だから, $f(x_1) \in Y_{x_2}$ である. 一方で, (1) から $f(x_2) = \min(Y \setminus Y_{x_2})$ だから $f(x_2) \notin Y_{x_2}$ である. ゆえに, $f(x_1) \neq f(x_2)$ である. 以上から, $f(x_1) < f(x_2)$ である. □

ある $x \in X$ に対して $f(x) = \perp$ であると仮定する. X は整列集合なので, そのような最小の x が存在する. X1 から $f(\min X) \neq \perp$ だから $x > \min X$ である. $\perp \in Y_x$ であれば, ある $x' \in X(x)$ に対して $f(x') = \perp$ となっているはずで, x の最小性に反する. よって, $Y_x \subseteq Y$ である. したがって, 補題 3.29(2) から $Y_x = Y$, つまり $f(X(x)) = Y$ である. 補題 3.29(5) から f は $X(x)$ 上で単調かつ単射なので, f の制限 $f|_{X(x)} : X(x) \to Y$ は単調な全単射である. ここで $X(x)$ は全順序集合だから, 演習 1.7 から f は同型であり, S3 が成立する.

次に, $f(X) \subseteq Y$ であると仮定する. この場合は, どの $x \in X$ についても $f(x) = \min(Y \setminus Y_x)$ であり, 補題 3.29(4) から $f(x)$ は $Y_x = Y(y)$ を満たす唯一つの $y \in Y$ である. f は X から Y の中への単調な単射であることを示す. 議論は補題 3.29(5) の証明とほぼ同じである. $x_1, x_2 \in X$, $x_1 < x_2$ とする. $x_1 < x_2$ なので, $Y(f(x_1)) = Y_{x_1} \subseteq Y_{x_2} = Y(f(x_2))$ であり, したがって $f(x_1) \leq f(x_2)$ である. $x_1 < x_2$ だから, $f(x_1) \in Y_{x_2}$ であるが, 一方で $f(x_2) = \min(Y \setminus Y_{x_2})$ だから $f(x_2) \notin Y_{x_2}$ である. よって, $f(x_1) \neq f(x_2)$ である. 以上から, $f(x_1) < f(x_2)$ である. これで, f は X から Y の中への単調な単射であることが分かった. よって, $f(X) = Y$ であれば, 演習 1.7 から f は X から Y への同型であり, S1 が成立する. $f(X) \subsetneq Y$ であるときを考える. 補題 3.29(3) の証明と同様にして $f(X)$ は Y の部分集合として下に単調であることがわかるので, 補題 3.25 から $f(X) = Y(y)$ となる $y \in Y$ が唯一つ存在する. f の終集合を $Y(y)$ に制限した写像は X から $Y(y)$ への全単射な単調写像であり, 演習 1.7 からそれは X と $Y(y)$ の同型を与える. ゆ

[*17] $f(x_1) > f(x_2)$ であれば, $f(x_2) \in Y(f(x_1)) \subseteq Y(f(x_2))$, つまり $f(x_2) < f(x_2)$ となって矛盾する.

えに, S2 が成立する. これで定理 3.24 の証明が完成した. □

♦ **例 3.30**　$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ 上に次の 2 つの順序 $\leq_1$, $\leq_2$ を考える. $\leq_1$ は通常の大小順序とする. $\leq_2$ は次の通り, 0 を特別扱いして定義される:

- 0 以外の全ての $x \in \mathbb{N}_0$ について, $x <_2 0$ である.
- 0 以外の $x, y \in \mathbb{N}_0$ に対しては, $x \leq_2 y$ は $x \leq_1 y$ (通常の意味で $x \leq y$) であることと同じである.

$\leq_1$, $\leq_2$ は共に整列順序である. $(\mathbb{N}_0, \leq_1)$ と $(\mathbb{N}_0, \leq_2)$ はどちらも同じ集合 $\mathbb{N}_0$ を土台とする整列集合であるが, 両者は同型ではない. $\leq_1$ に関する最大元は存在しないが, $\leq_2$ については $0 = \min \mathbb{N}_0$ だからである. このように, 同一の集合を土台とする整列集合どうしであっても同型でないことが起こり得る. この例では, $(\mathbb{N}_0, \leq_1)$ が $(\mathbb{N}_0, \leq_2)$ の 0 における切片になっている. □

X, Y を任意の整列集合とする. X と Y が同型であることを $X \simeq Y$ で表し, X が Y の切片に同型であるときには $X < Y$ で表す. この両方を合わせて $X \leq Y$ と書く.[*18] 定理 3.24 は, どの 2 つの整列集合 X, Y に対しても, $X \simeq Y$, $X < Y$, $X > Y$ のうちどれか一つだけが成り立つことを主張している.

命題 3.31 (埋め込み)**.** X, Y を任意の整列集合とする. $X \leq Y$ であるためには, 写像 $f : X \to Y$ で次の 2 条件を満たすものが存在することが必要十分である.

E1: f は単射かつ単調増加である.
E2: 像 $f(X)$ は Y の部分集合として下に単調である.

この 2 条件を満たす写像 f は**埋め込み**であると言う. 特に, $X < Y$ であるためには, X から Y への**真の埋め込み** (全射ではない埋め込み) が存在することが必要十分である.

証明. $X \leq Y$ と仮定する. $X \simeq Y$ であれば, 同型 $f : X \to Y$ が存在するが, この f について条件 E1, E2 がどちらも成り立つ. $X < Y$ の場合を考える. X から Y のある切片 $Y(y)$ への同型 $g : X \to Y(y)$ が存在するが, これに包含写像 $e : Y(y) \to Y$ を合成した写像を $f = e \circ g$ とおく. g と e は共に単射かつ単調増加なので, f もそうである. $f(X) = e(g(X)) = g(X) = Y(y)$ であるが, これは下に単調である. よって, f に対して条件 E1, E2 がどちらも成り立ち, なおかつ f は全射ではないので真の埋め込みである.

次は逆に, 条件 E1, E2 を満たす写像 $f : X \to Y$ が存在すると仮定する. $f(X) = Y$ とすると, 条件 E1 から f は全単射かつ単調増加であるが, Y は整列集合, したがって全順序集合なので, 演習 1.7 から f は同型であり, $X \simeq Y$ が成り立つ. $f(X) \neq Y$ とする. 条件 E2 から $f(X)$ は下に単調なので, 補題 3.25 から $f(X)$ はある点 $y \in Y$ における切片 $Y(y)$ である. 条件 E1 から, f の終域を $f(X) = Y(y)$ に制限した写像 $\hat{f} : X \to Y(y)$ は全単射かつ単調増加であるが, $Y(y)$ は整列集合, したがって全順序集合なので, 演習 1.7 から $\hat{f}$ は同型であり, $X \simeq Y(y)$ が成り立つ. よって, $X < Y$ である. □

次の命題の主張は全て命題 3.31 の証明の中で既に示されている.

命題 3.32. X, Y を整列集合, $f : X \to Y$ を埋め込みとする.

(1) f が同型であるためには, f が全射であることが必要十分である.
(2) f が真の埋め込みであるとき, 像 $f(X)$ は Y の切片である.

[*18] ここの $\leq$ の下棒線は等号ではなく同型 $\simeq$ である.

(3) f は X と像 $f(X)$ との間の同型である.

$\leq$ は順序の公理 (反射性, 推移性, 反対称性) のうち, 反射性と推移性を満たす. 特に, 推移性は次の命題 3.33 から直ちに従う.

命題 3.33. $f : X \to Y$ と $g : Y \to Z$ を整列集合の埋め込みとすると, 合成 $g \circ f : X \to Z$ も埋め込みである.

証明. E1 から f, g は共に単射かつ単調なので, $g \circ f$ も単射かつ単調である. 像 $g(f(X))$ が下に単調であることを示す. $z, z' \in Z$, $z \leq z'$, $z' \in g(f(X))$ と仮定する. $z' \in g(f(X))$ だから, ある $x' \in X$ を用いて $z' = g(f(x'))$ と書ける. $z' \in g(f(X)) \subseteq g(Y)$ であるが, $z < z'$ であり, E2 から $g(Y)$ は下に単調なので, $z \in g(Y)$ でもある. よって, ある $y \in Y$ を用いて $z = g(y)$ と書ける. $g(y) = z \leq z' = g(f(x'))$ であるが, 命題 3.32(3) から g は Y と像 $g(Y)$ との同型だから, $y \leq f(x')$ である. ここで E1 から $f(X)$ は下に単調なので, $y \in f(X)$ である. よって, $z = g(y) \in g(f(X))$ である. これで $g \circ f$ も E2 を満たすことが言えた. □

$\leq$ は厳密な意味では反対称的ではないが, $X \leq Y$ かつ $X \geq Y$ であれば $X \simeq Y$ なので (→演習 3.8), $\leq$ はやや緩い意味で反対称的になっている. このように, **同型な整列集合どうしは同じものと見なせば**, $\leq$ は整列集合の間の順序であると考えることができる.

▶ **演習 3.8**　整列集合 X, Y に対して, $X \leq Y$ かつ $X \geq Y$ ならば, $X \simeq Y$ であることを示せ.

▶ **演習 3.9**　Y を整列集合, X をその部分集合とするとき, $X \leq Y$ であることを示せ.

付録 A　演習問題解答例

ここに示されているのはあくまで解答の一例であり，これだけが唯一絶対の正しい解答というわけではない．参考程度の略解という位置付けである．

演習 1.1.　(1) 3 と 5 は比較可能ではない．

(2) $x, y \in X$, $x \neq y$ ならば, $\{x\}$, $\{y\}$ は比較可能ではない．

(3) $(1, 2)$ と $(2, 1)$ は比較可能ではない．　□

演習 1.2.　(1) $\leq$ の反射性から, 任意の $x \in A$ について, $a = x$ に対して $a \in A$, $a \leq x$ が成り立つから $x \in A^u$ である．よって, $A \subseteq A^u$ である．$A \subseteq B$, $x \in A^u$ のとき, ある $a \in A$ が存在して $a \leq x$ であるが, $a \in A \subseteq B$ なので $x \in B^u$ でもある．よって, $A \subseteq B \Rightarrow A^u \subseteq B^u$ である．$x \in (A^u)^u$ のとき, ある $y \in A^u$ に対して $y \leq x$ であるが, さらにある $a \in A$ に対して $a \leq y$ なので, 推移性から $a \leq x$ である．よって, $x \in A^u$ である．したがって, $(A^u)^u \subseteq A^u$ である．以上から, u は X 上の閉包作用素である．

$x \leq y$, $x \in A^u$ であるとき, ある $a \in A$ について $a \leq x$ であるから, 推移性から $a \leq y$ でもあり, したがって $y \in A^u$ である．よって, A^u は上に閉じている．ゆえに, $A = A^u$ であれば A は上に閉じている．逆に, A が上に閉じているとすると, 任意の $x \in A^u$ に対して, $a \leq x$ となる $a \in A$ を取れば, (A が上に閉じていることから) $x \in A$ であることが従うから, $A^u \subseteq A$ である．

B を X の部分集合で A を含みなおかつ上に閉じているものとする．$A \subseteq B$ だから, $A^u \subseteq B^u$ でもあるが, B は上に閉じているから $B^u = B$ であり, したがって $A^u \subseteq B$ である．よって, A^u は A を含みかつ上に閉じている部分集合のうちで最小のものである．

(2) これは (1) の双対命題なので, (1) に双対原理を適用すれば直ちに得られる．　□

演習 1.3.　(1) $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ と仮定する．f は順序単射, $f(x_1) \leq f(x_2)$ なので, $x_1 \leq x_2$ である．対称的な議論で $x_1 \geq x_2$ も言えるので, 反対称性から $x_1 = x_2$ である．ゆえに, f は単射である．

(2) $X = X' = \mathbb{N}$ とし, X 上の順序は整除順序, X' 上の順序は通常の大小順序とすると, 恒等写像 $X \to X'$ は単射かつ単調であるが, 順序単射ではない．　□

演習 1.4.　$x_1, x_2 \in X$, $x_1 \leq x_2$ とする．f は単調だから, $f(x_1) \leq f(x_2)$ である．そして g も単調なので, $g(f(x_1)) \leq g(f(x_2))$ である．ゆえに, $g \circ f$ は単調である．

(2) $x_1, x_2 \in X$, $g(f(x_1)) \leq g(f(x_2))$ であるとする．g は順序単射なので, $f(x_1) \leq f(x_2)$ である．f も順序単射なので, $x_1 \leq x_2$ である．よって, $g \circ f$ は順序単射である．　□

演習 1.5.　(1) $x_1, x_2 \in X$, $x_1 \leq x_2$ とする．$g \circ f$ は単調だから, $g(f(x_1)) \leq g(f(x_2))$ である．そして g は順序単射なので, $f(x_1) \leq f(x_2)$ である．ゆえに, f は単調である．

(2) $x'_1, x'_2 \in X'$, $g(x'_1) \leq g(x'_2)$ とする．f は全射なので, $x'_1 = f(x_1)$, $x'_2 = f(x_2)$ となる $x_1, x_2 \in X$ が存在する．$g(f(x_1)) = g(x'_1) \leq g(x'_2) = g(f(x_2))$ であるが, $g \circ f$ は順序単射なので, $x_1 \leq x_2$ である．そして f は単調なので, $x'_1 = f(x_1) \leq f(x_2) = x'_2$ である．したがって, g は順序単射である．

演習 1.6.　f が単調であることを示す．$X, X' \in 2^A$, $X \subseteq X'$ とする．$f(X) = (x_1, \dots, x_n)$, $f(X') = (x'_1, \dots, x'_n)$ とするとき, $x_i = 1$ であれば $a_i \in X$, したがって $a_i \in X'$ でもあるので, $x'_i = 1$ である．ゆえに, $f(X) \leq f(X')$ である．これで f が単調であることが言えた．

任意の $y=(y_1,\dots,y_n)\in I^n$ について, $g(y)$ は $a_i=1$ となる全ての $i=1,2,\dots,n$ に渡る a_i らの全体とする．これで写像 $g:I^n\to 2^A$ が定義されるが, これが f の逆写像であることを示す．$X\in 2^A$, $f(X)=(x_1,\dots,x_n)$ とすると, $x_i=1 \iff a_i\in X$ だから, $g(f(X))=X$ である．よって, $gf=\epsilon_{2^A}$ である．$y=(y_1,\dots,y_n)\in I^n$, $X=g(y)$ とおくと, $a_i\in X \iff y_i=1$ なので $f(X)=y$ である．これは $fg=\epsilon_{I^n}$ であることを示している．ゆえに, g は f の逆写像である．

g が単調であることを示す．$y=(y_1,\dots,y_n), y'=(y'_1,\dots,y'_n)\in I^n$, $y\le y'$ とする．$a_i\in g(y)$ ならば $y_i=1$ であるが, $y\le y'$ だからこのとき必ず $y'_i=1$ でもあり, したがって $a_i\in g(y')$ でもある．よって, $g(y)\subseteq g(y')$ であり, g は単調である． □

演習 1.7. f が順序単射であることを示せば十分である．すなわち, $x,x'\in X$, $f(x)\le f(x')$ ならば $x\le x'$ であることを示せばよい．X は全順序集合なので, $x\le x'$ でないとすれば $x>x'$ である．f は単調なので $f(x)\ge f(x')$ であるが, ここで f は単射, $x\ne x'$ なので, $f(x)\ne f(x')$ であり, したがって $f(x)>f(x')$ である．この対偶から, $f(x)\le f(x')$ ならば $x\le x'$ である． □

演習 2.1. (1) $\le$ は全順序であると仮定する．$A=\{a_1,\dots,a_n\}$ を任意の有限部分集合とする．$\le$ は全順序なので, 適当な並び替えによって $a_1\le\dots\le a_n$ となるが, このとき a_1 は A の下界, a_n は A の上界となるので, A は上にも下にも有界である．よって, $\le$ は上向きかつ下向きである．

(2) $\{g,h\}$ は上に有界でないので $\le$ は上向きではない．どの有限部分集合についても a はその下界であるから, $\le$ は下向きである．

(3) $A=\{(x_1,y_1),\dots,(x_n,y_n)\}$ を $\mathbb{R}^2$ の有限部分集合とし, $x=-\sum_{i=1}^n|x_i|$, $y=-\sum_{i=1}^n|y_i|$ とおく．どの $1\le i\le n$ についても, $x\le-|x_i|\le x_i$ かつ $y\le-|y_i|\le y_i$ だから $(x,y)\preceq(x_i,y_i)$ であり, (x,y) は A の下界である．よって, $\preceq$ は下向きである．同様に, $x=\sum_{i=1}^n|x_i|$, $y=\sum_{i=1}^n|y_i|$ を考えれば, $\preceq$ が上向きであることもわかる． □

演習 2.2. h は C の上界であり, かつ $h\in C$ なので, $h=\max C$ である．a は C の唯一つの下界であるが, $a\notin C$ なので, $\min C$ は存在しない． □

演習 2.3. $(1,1)$ が A の上界であることはすぐ分かる．$(1,1)$ が A の最小の上界であることを示す．(x,y) を A の任意の上界とする．任意の $r\in(0,1)$ を考える．$(1-r,0)\in A$ なので, $(1-r,0)\preceq(x,y)$ つまり $1-r\le x$ である．同様に $(0,1-r)\in A$ なので, $(0,1-r)\preceq(x,y)$, つまり $1-r\le y$ である．これが全ての $r\in(0,1)$ について言えるので, $x,y\ge1$ である．よって, $(1,1)\preceq(x,y)$ である．これで $(1,1)$ が A の上界として最小であることが言えた． □

演習 2.4. (1) $x=\max A$ が存在すると仮定する．$\max A$ の定義から, x は A の上界であり, かつ $x\in A$ である．よって, y を A の上界とすると $x\le y$ である．ゆえに, x は A の上界として最小であり, $x=\sup A$ である．

(2) $x=\sup A$ が存在して, かつ $x\in A$ であるとする．$\sup A$ の定義から x は A の上界である．そして $x\in A$ なので, $x=\max A$ である．

(3) $x=\sup A$ が存在して, $x\notin A$ であるとする．$\max A$ が存在するならば, (1) から $x=\sup A=\max A$, したがって $x\in A$ であるが, これは $x\notin A$ に反する．ゆえに, $\max A$ は存在しない． □

演習 2.5. $x=\sup A$, $y=\sup B$ とする．任意の $a\in A$ について, ($A\subseteq B$ から) $a\in B$ でもあるが, $y=\sup B$ は B の上界なので, $a\le y$ である．ゆえに, y は A の上界である．一方で $x=\sup A$ は A の最

小の上界だから, $x \leq y$ である.

これの双対命題は,「$A \subseteq B \Rightarrow \inf A \geq \inf B$」である. (不等号の向きに注意.) □

演習 2.6. (1) $a \in A$, $x \leq a$ とする. $x = \max A$, $a \in A$ だから $a \leq x$ でもあり, したがって反対称性から $a = x$ である. ゆえに, x は A の極大元である. y を A の任意の極大元とする. $y \in A$, $x = \max A$ なので $y \leq x$ であるが, y は A で極大, $x \in A$ なので, $y = x$ である. ゆえに, x は A の唯一の極大元である.

(2) $x = \max A$ ならば x は A の極大元であることは (1) で示した. x が A で極大であるとする. 任意の $a \in A$ を考える. $\leq$ は全順序なので, $a \leq x$ または $x \leq a$ であるが, 後者の場合であっても x の極大性から $a = x$ となるので, いずれにせよ $a \leq x$ である. ゆえに, x は A の上界である. そして $x \in A$ なので, $x = \max A$ である. □

演習 2.7. x 自身が極大元であれば $w = x$ とすればよい. そうでなければ, $x < x_1$ となる $x_1 \in X$ が存在するが, この x_1 が極大元であれば, $w = x_1$ とすればよい. そうでなければ, $x < x_1 < x_2$ となる $x_2 \in X$ が存在する. この議論を繰り返していけば, X 上で昇鎖

$$x < x_1 < x_2 < x_3 < \cdots$$

が生じるが, そもそも X 上には有限個の元しかないので, この議論が無限に続いていくことはない. つまり, 必ずある時点での x_n が極大元となり, その x_n のことを w とすればよい. □

演習 2.8. S が反射的なので, S' も反射的である.

S' が推移的であることを示す. $(a, b) \in S'$ かつ $(b, c) \in S'$ とする. $(a, b), (b, c) \in S$ であれば, S の推移性から $(a, c) \in S \subseteq S'$ でもある. $(a, b) \in K$, $(b, c) \in S$ のとき, $(a, y) \in S$, $(y, b) \in S$, $(b, c) \in S$ なので, S の推移性から $(a, c) \in S \subseteq S'$ である. $(a, b) \in S$, $(b, c) \in K$ のとき, $(a, b) \in S$, $(b, x) \in S$ なので S の推移性から $(a, x) \in S$ であり, そして $(y, c) \in S$ でもあるから, $(a, c) \in K \subseteq S'$ である. $(a, b) \in K$, $(b, c) \in K$ のとき, $(a, x) \in S$ かつ $(y, c) \in S$ だから, $(a, c) \in K \subseteq S'$ である. 以上から, S' は推移的である.

S' が反対称的であることを示す. $(a, b) \in S'$ かつ $(b, a) \in S'$ とする. $(a, b) \in K$, $(b, a) \in S$ のとき, $(a, x) \in S$ かつ $(b, a) \in S$ なので S の推移性から $(b, x) \in S$ であり, さらに $(y, b) \in S$ なので, S の推移性から $(y, x) \in S$ となるが, これは x, y の取り方からあり得ない. 同様にして, $(a, b) \in S$, $(b, a) \in S$ の場合もあり得ないことが分かる. $(a, b) \in K$, $(b, a) \in K$ とすると, $(a, x) \in S$ かつ $(y, a) \in S$ だから, S の推移性から $(y, x) \in S$ となるが, これは x, y の取り方からあり得ない. よって, $(a, b), (b, a) \in S$ の場合しかあり得ないが, そうすると S の反対象性から $a = b$ である. □

演習 2.9. (I) Zorn の補題から Hausdorff の極大性原理を導く. X を順序集合, C を X 上の鎖とする. X 上で C を含む鎖の全体集合を $\mathcal{C}$ で表す. $C \in \mathcal{C}$ だから, $\mathcal{C} \neq \emptyset$ である. $\mathcal{C}$ は集合の包含順序の下で順序集合になっているが, それが帰納的であることを示す. $\{C_i\}_{i \in I}$ を $\mathcal{C}$ 上の任意の鎖とする. $C_* = \bigcup_{i \in I} C_i$ とおく. C_* が鎖であることを示す. 任意の $x, y \in C_*$ について, それぞれ $x \in C_i$, $y \in C_j$ となる $i, j \in I$ が存在する. $\{C_i\}_{i \in I}$ は鎖だから, 一般性を失わず $C_i \subseteq C_j$ であると仮定してよい. すると, $x, y \in C_j$ であるが, C_j は鎖なので, x と y は比較可能である. したがって, C_* は鎖である. そして, 全ての $i \in I$ について $C \subseteq C_i \subseteq C_*$ である. よって, $C_* \in \mathcal{C}$ であり, これが $\mathcal{C}$ における $\{C_i\}_{i \in I}$ の上界になっていることがわかる. ゆえに, $\mathcal{C}$ は帰納的である. したがって, Zorn の補題から $\mathcal{C}$ は極大元 $\hat{C}$ を持っている. $\hat{C} \in \mathcal{C}$ なので,

$\hat{C}$ は X 上で C を含む鎖である．X 上で $\hat{C}$ を含む鎖 $\tilde{C}$ があれば, $C \subseteq \hat{C} \subseteq \tilde{C}$ だから $\tilde{C} \in \mathcal{C}$ であり, したがって $\hat{C}$ の極大性から $\hat{C} = \tilde{C}$ となる．ゆえに, $\hat{C}$ は X 上の鎖として極大である．

(II) Hausdorff の極大性原理から Zorn の補題を導く．X を空でない帰納的順序集合として, X に極大元が存在することを示せばよい．任意の点 $x \in X$ について, $\{x\}$ は鎖であるが, Hausdorff の極大性原理から $\{x\}$ を含む極大鎖 C が存在する．X は帰納的なので, C は上に有界である．よって, 命題 2.27 から X は極大元を持つ． □

演習 2.10.　(I) Zorn の補題から Teichmüller-Tukey の補題を導く．$\mathcal{F}$ を空でない集合族で有限的であるものとする．これは集合の包含順序について順序集合になっているが, それが帰納的であることを示す．$\{F_i\}_{i\in I}$ を $\mathcal{F}$ 上の空でない鎖として, $F = \bigcup_{i\in I} F_i$ とおく．全ての $i \in I$ について $F_i \subseteq F$ であることは明白なので, $F \in \mathcal{F}$ であることを示せば, これが $\mathcal{F}$ における鎖 $\{F_i\}_{i\in I}$ の上界であることが分かる．X を F の有限部分集合とする．各々の元 $x \in X$ はそれぞれ何らかの F_i に含まれているが, $\{F_i\}_{i\in I}$ は鎖だから, X の全ての元を含む F_i が存在する．ここで $F_i \in \mathcal{F}$ であり, かつ $\mathcal{F}$ は有限的なので, F_i の有限部分集合である X もまた $\mathcal{F}$ に属している．これが F の任意の有限部分集合 X について成り立つが, $\mathcal{F}$ は有限的なので, $F \in \mathcal{F}$ である．

以上から, $\mathcal{F}$ は帰納的である．よって, Zorn の補題から $\mathcal{F}$ の極大元が存在する．

(II) Teichmüller-Tukey の補題から Zorn の補題を導く．X を空でない帰納的順序集合として, X 上の鎖の全体を $\mathcal{C}$ とする．これは全ての単元部分集合を含んでいるので空集合ではない．X の部分集合 C が鎖であるためには, その全ての有限部分集合が鎖であることが必要十分なので, $\mathcal{C}$ は有限的である．よって, Teichmüller-Tukey の補題から $\mathcal{C}$ は集合の包含順序に関する極大元 C を持っている．C は X における極大鎖であり, なおかつ X は帰納的だからそれは上に有界である．ゆえに, 命題 2.27 から X は極大元を持つ． □

演習 3.1.　$x = y + 1$ だから, $y < x$, つまり $y \in X^{\downarrow}(x)$ である．$y < z < x$ となる z が存在すれば, x が $X^{\uparrow}(y)$ の最小元であることに反するので, $z < x$ であれば必ず $z \leq y$ でなければならない, すなわち任意の $z \in X^{\downarrow}(x)$ について $z \leq y$ である．よって, $y = \max X^{\downarrow}(x) = x - 1$ である． □

演習 3.2.　(I) x に関する超限帰納法で分解 $x = a + n$ の存在を示そう．x が非後続元ならば, $a = x$, $n = 0$ とすればよい．x が後続元の場合を考える．y を x の直前とする．$y < x$ なので, 帰納法の仮定から, $y = a+m$ (a は非後続元, $m \in \mathbb{N}_0$) と書ける．演習 3.1 から $x = y+1$ なので, $x = y+1 = (a+m)+1 = a+n$ (ただし, $n = m + 1$ と置いた) である．これでまず分解 $x = a + n$ の存在は示された．

(II) 分解の一意性を示す．$a + n = b + m$ (a, b は非後続元, $m, n \in \mathbb{N}_0$) と仮定して, $a = b$, $m = n$ を示せばよい．n に関する数学的帰納法を利用する．$n = 0$ のときは, $b + m = a + 0 = a$ なので, $b + m$ も非後続元であり, したがって $m = 0$ である．[*19] よって, $a = b$ も従う．$n \geq 1$ とする．このとき, $m \geq 1$ でもある．$a + n = b + m$ は後続元であり, 両辺で直前を見れば $a + (n - 1) = b + (m - 1)$ となるので, 帰納法の仮定から $a = b$, $n - 1 = m - 1$ (つまり $n = m$) が従う．これで分解の一意性も示された． □

演習 3.3.　$(x_1, y_1) \succeq (x_2, y_2) \succeq \cdots$ を $X \times Y$ 上の任意の無限降鎖として, これが有限であることを示せばよい．第 1 成分から X 上の無限降鎖 $x_1 \geq x_2 \geq \cdots$ が生じるが, X は整礎集合だから, ある番号 m が存在して $x_m = x_{m+1} = \cdots$ となる．同じく第 2 成分から, Y 上の無限降鎖 $y_1 \geq y_2 \geq \cdots$ が生じるが,

[*19] $m \geq 1$ ならば, $b + (m - 1)$ が b の直前であり, b は後続元であるはず.

Y は整礎集合だから, ある番号 n が存在して $y_n = y_{n+1} = \cdots$ となる．ここで $l = \max\{m, n\}$ とおけば, $(x_l, y_l) = (x_{l+1}, y_{l+1}) = \cdots$ が成り立つ． □

演習 3.4.　X の部分集合 A で極小元を持たないものは $A = \emptyset$ しかないことを示せばよい．$P = A^c$ とおく．$x \in A$, $X^{\downarrow}(x) \subseteq P$ と仮定する．x は A の極小元ではないので, $a < x$ となる $a \in A$ が存在するが, すると $a \in X^{\downarrow}(x) \subseteq P$ となって, 矛盾 $a \in P \cap A = \emptyset$ が生じる．ゆえに, $X^{\downarrow}(x) \subseteq P$ であれば必ず $x \notin A$, すなわち $x \in P$ である．よって, 全ての $x \in X$ について式 (8) が成り立つので, 仮定から $P = X$, つまり $A = \emptyset$ である． □

演習 3.5.　(i) $1 \in E$ である．(ii) ($n \geq 2$ のときは) $n - 1 \notin E$ であるとき, かつそのときに限り $n \in E$ である． □

演習 3.6.　(i) $\sigma(1) = 1$ である．(ii) n が素数であれば $\sigma(n) = 2$ である．(iii) n が 2 以上の合成数であるとき, p を n の最小の素因数, $n = p^k m$ ($\gcd(m, p) = 1$) と分解すれば, $\sigma(n) = \sigma(n/p) + \sigma(m)$. □

演習 3.7.　入力された文字列を w とし, その長さを $|w|$ で表す．

- S1: $|w| \leq 1$ ならば, w を回文と判定して停止する．
- S2: ($|w| \geq 2$ のとき) w の最初の文字を a, 最後の文字を b として, $w = aw'b$ と分解する．ここで $a \neq b$ であれば w は回文ではないと判定して停止する．$a = b$ であるときには, w' が回文であるとき, かつそのときに限り w は回文であると判定して停止する． □

演習 3.8.　$X \leq Y$ かつ $X \geq Y$ と仮定すると, 命題 3.31 からそれぞれ埋め込み $f : X \to Y$, $g : Y \to X$ が存在する．$X = \emptyset$ であれば, 埋め込み g の存在から $Y = \emptyset$ でもある．(空でない集合から空集合への写像は存在しないので.) $X \neq \emptyset$ の場合を考える．命題 3.33 から, 合成 $h = g \circ f$ は X から X への埋め込みである．命題 3.32 から, $h(X) \neq X$ であれば, h は X とそのある切片との同型を与えることになるが, これは補題 3.27 からあり得ない．よって, $h(X) = X$ である．ここで, $X = h(X) = g(f(X)) \subseteq g(Y) \subseteq X$ なので, $g(Y) = X$ であり, したがって g は同型である．ゆえに, $X \simeq Y$ である． □

演習 3.9.　定理 3.24 から, $X < Y$, $X = Y$, $X > Y$ のうちいずれか一つだけが成り立つ．$X > Y$ とすると, ある点 $x \in X$ に対して同型 $f : Y \to X(x)$ が存在する．$X(x) \subseteq X \subseteq Y$ なので, 包含写像 $e : X(x) \to Y$ を合成すれば単調な単射 $g = e \circ f : Y \to Y$ が得られる．$g(x) = e(f(x)) = f(x) \in X(x)$ だから $g(x) < x$ であるが, 補題 3.26 からこれはあり得ない．よって, $X < Y$ または $X = Y$ であり, すなわち $X \leq Y$ である． □

付録 B　選択公理・Zorn の補題・整列可能定理

選択公理には, 順序関係の言葉を借りた同値表現がいくつか知られている．この付録では, それらのうちの代表的なものとして, 本文中でも紹介した Zorn の補題と整列可能定理について, 選択公理との同値性を示しておくことにする．ここで述べる証明を知らなくても, 選択公理・Zorn の補題・整列可能定理が全て同値であることを知っているだけでも困ることはないだろうが, もし証明に少しでも興味があれば, **数学的な証明を読み解く練習題材として**読んでみるといいと思う．

B.1　選択公理から Zorn の補題へ

選択公理は, 空でない集合から成る集合族については常に選択関数 (あるいは選択集合) が存在するという主張であるが, まずはそこから Zorn の補題を導こう．この議論には複数の方法が知られているが, ここでは整列順序を利用した比較的簡潔な証明を紹介しておく.[20] 整列順序に関しては, 本文中で解説した知識があればこの証明を理解するには十分である.

Zorn の補題が成立しないと仮定して矛盾を導く背理法を用いる．X が空でない帰納的順序集合で極大元を全く持たないものとする．X は極大元を持たないので, 特に X は無限集合である．X の部分集合 C について, C の上界で C 自身に属さないものを**真の上界**と呼ぶ.

C を X の部分集合で上に有界であるものとすると, C の上界 $x \in X$ が存在する．$x \notin C$ であれば, x は C の真の上界である．$x \in C$ であれば, $x = \max C$ であるが, これは X の極大元ではない．(そもそも X は極大元を持たないから.) よって, x より真に大きな元 $x' \in X$ が存在するが, これは C の真の上界である．したがって, X の上に有界な部分集合は全て真の上界を持つ.

X の鎖 (全順序な部分集合) の全体を $\mathcal{C}$ とする．これは全ての単元部分集合 $\{x\}$ を含んでいるので空集合ではない．X は帰納的なので, 任意の $C \in \mathcal{C}$ は上に有界である．よって, C は必ず真の上界を持つ．ここで選択公理を仮定すれば, 任意の $C \in \mathcal{C}$ についてその真の上界 $g(C)$ を与える選択関数 g が存在する．(選択公理のパワーを借りるのはこの箇所だけである.)

X の部分集合 A が **g-集合**であるとは, 次の条件 G1, G2 が満たされることを言うものとする:

- G1: A は X の順序の下で整列されている．(特に, $A \in \mathcal{C}$ である.)
- G2: 全ての $x \in A$ について, $g(A(x)) = x$ である．ここで, $A(x)$ は x における A の切片である．(G1 から, 切片 $A(x)$ は鎖であり, したがって $A(x) \in \mathcal{C}$ であることに注意しておく.)

$A = \emptyset$ は空虚な意味で g-集合である.

補題 B.1. A, B を X の相異なる g-部分集合とするとき, 一方がもう一方の切片である.

証明. $C = \{x \in A \cap B \mid A(x) = B(x)\}$ とおく．C は A の部分集合であるが, ここで $C \neq A$ である場合を考える．C は下に単調であることを示す．$x, y \in A$, $x \leq y$ かつ $y \in C$ と仮定する．任意の $w \in A(x)$ を取る．$w \in A$ かつ $w < x \leq y$ なので $w \in A(y)$ であるが, 一方で $y \in C$ なので $A(y) = B(y)$ であり, したがって $w \in B(y)$ でもある．よって, 特に $w \in B$ である．そして $w < x$ なので, $w \in B(x)$ である．ゆえに, $A(x) \subseteq B(x)$ である．A と B の立場を入れ替えて同様にすれば $A(x) \supseteq B(x)$ も得られるので, $A(x) = B(x)$, すなわち $x \in C$ である．したがって, C は下に単調である．ゆえに, 補題 3.25 から C は A の切片である．よって, $C = A$ であるか, C は A の切片であるかのいずれかである．B についても同様の議論ができるので, $C = B$ であるか, C は B の切片であるかのいずれかである．仮定から $A \neq B$ なので, $C = A$ と $C = B$ は両立し得ない．したがって, もし $C = A$ であれば, C は B の切片であるが, この場合は A が B の切片である．対称的に, $C = B$ でれば, C は A の切片である.

残る可能性は, C が A と B の両方の切片になっている場合であるが, この場合はあり得ないことを示そう．$C = A(a)$, $C = B(b)$ となる $a \in A$, $b \in B$ を取る．A と B は g-集合なので, 条件 G2 から $a = g(A(a)) = g(C) = g(B(b)) = b$ であり, さらに $A(a) = C = B(b)$ だから $a = b \in C$ となる．する

[20] ここで紹介する証明は, Jonathan W. Levin, “A simple proof of zorn’s lemma”, The American Mathematical Monthly, 98(4), pp. 353–354 に基づいている.

と, $a \in C = A(a)$ となるので矛盾である. □

X の全ての g-部分集合に渡る和集合を E とする. この E 自身が g-部分集合であり, したがって E は X の最大の g-部分集合であることを示す. まず, E が整列集合であることを示すが, その前段として, E が全順序集合であることを示そう. 任意の $x, y \in E$ を取ると, それぞれ x を含む g-部分集合 A と y を含む g-部分集合 B が存在する. 補題 B.1 から, $A \subseteq B$ または $A \supseteq B$ であるが, そのそれぞれの場合について $x, y \in A$ または $x, y \in B$ であり, そして A, B はどちらも整列集合, 特に全順序集合なので, $x \leq y$ または $x \geq y$ が成り立つ. よって, まず E が全順序集合であることは言えた.

次に, E が整列集合であることを示すが, そのためには E が**整礎集合**であることを示せば十分である. 先に示した通り E は全順序集合なので, それが整礎集合であれば自ずと整列集合になるからである. 次の補題を利用する.

補題 B.2. $x \in E$ とし, A を X の g-部分集合で x を含むものとする. このとき, $E(x) = A(x)$ である.

証明. $A \subseteq E$ なので, $A(x) \subseteq E(x)$ である. この逆向きの包含を示せばよい. $y \in E(x)$ とする. $y \in E$ なので, y を含む g-部分集合 B が存在する. $y \in E(x)$ だから $y < x$ であり, そして $y \in B$ なので, $y \in B(x)$ である. $A = B$ であれば, $y \in A$ でもあり, そして $y < x$ なので, $y \in A(x)$ でもある. $A \neq B$ のときは, 補題 B.1 から A が B の切片であるか, B が A の切片であるかのいずれかである. B が A の切片であれば, 特に $B \subseteq A$ なので, $y \in B(x) \subseteq A(x)$ である. A が B の切片である場合を考える. $A = B(b)$ となる $b \in B$ を取る. $x \in A = B(b)$ だから, $x \in B$ かつ $x < b$ である. そして $y < x$ なので, 推移性から $y < b$ でもあり, したがって $y \in B(b) = A$ であり, これと $y < x$ から $y \in A(x)$ が従う. よって, いずれにせよ $y \in A(x)$ であり, $A(x) \supseteq E(x)$ が成り立つ. □

E が整礎集合ではないと仮定すると, 命題 3.11 から E 上に無限降鎖 $x_1 > x_2 > x_3 > \cdots$ が存在する. $x_1 \in E$ なので, x_1 を含む g-部分集合 A が存在する. 補題 B.2 から $E(x_1) = A(x_1)$ であるが, x_2 以降の項は全て $E(x_1) = A(x_1)$ に属するので, $x_2 > x_3 > x_4 > \cdots$ は $A(x_1)$ 上の無限降鎖であるが, A は整列集合, したがって整礎集合でもあるので, これはあり得ない. ゆえに, E は整礎集合であり, したがって整列集合である.

次に, E が条件 G2 を満たすことを示そう. 任意の $x \in E$ を考える. x はある g-部分集合 A に含まれている. 補題 B.2 から $E(x) = A(x)$ であるが, A は g-集合なので, $g(E(x)) = g(A(x)) = x$ である. よって, E は条件 G2 も満たし, したがって g-集合であることが分かる. 以上から, E は X の最大の g-集合である.

補題 B.3. A が X の g-部分集合ならば, $A \cup \{g(A)\}$ も g-集合である.

証明. $\bar{A} = A \cup \{g(A)\}$ とする. A は整列集合であり, $g(A)$ は A の真の上界なので, $\bar{A}$ は $g(A)$ を最大元に持つ整列集合である. A は g-集合なので, 任意の $x \in A$ に対して $g(\bar{A}(x)) = g(A(x)) = x$ である. $x = g(A)$ に対しては, $\bar{A}(x) = A$ なので, $g(\bar{A}(x)) = g(A) = x$ である. よって, $\bar{A}$ も g-集合である. □

この補題から, $\bar{E} = E \cup \{g(E)\}$ も g-集合であるが, $g(E)$ は E の真の上界であって, E に属さないので, $E \subsetneq \bar{E}$ である. しかし, これは E が最大の g-集合であることに反する. 以上から, 背理法により Zorn の補題が示された.

B.2 Zorn の補題から整列可能定理へ

整列可能定理 (→定理 3.6) はどんな集合でも必ず整列できることを主張する．ここでは, Zorn の補題 (→定理 2.22) を利用して整列可能定理を導く議論を概観しておこう．(これは Zermelo が最初に与えた証明とは異なる道筋の議論である.)

X を任意の集合として, この上の整列順序が存在することを示せばよい．$X = \emptyset$ のときには, $\emptyset$ が X 上で唯一の二項関係であるが, これは空虚な意味で整列順序である．

以下, $X \neq \emptyset$ の場合のみを考える．A が X の部分集合であり, その上に整列順序 α があるとき, もし $A \neq X$ であれば, A に属さない任意の $x \in X$ を取って, $\bar{A} = A \cup \{x\}$ とおき, さらに

$$\bar{\alpha} = \alpha \cup \{(a, x) \mid a \in A\} \cup \{(x, x)\}$$

とおけば, (A, α) を切片に持つさらに大きな整列集合 $(\bar{A}, \bar{\alpha})$ を構成できる．つまり, A が整列可能であれば, その範囲を少しだけ広げた $\bar{A}$ も整列できるというわけである．この調子で, X の中で整列可能な範囲をどんどん広げていきたい, というのが基本的な発想である．ただし, X が無限集合である場合には, この操作を無限回やっても X 全体を整列するには至らないかも知れない．ここのところを, Zorn の補題を利用した議論でうまく回避するわけである．

X の空でない部分集合 A とその上の整列順序 $\alpha \subseteq A \times A$ との組 (A, α) の全体集合を $\mathcal{R}$ とする．任意の $x \in X$ について, $A = \{x\}$ 上で $\alpha = \{(x, x)\}$ は整列順序になっていて, $(A, \alpha) \in \mathcal{R}$ である．よって, $\mathcal{R} \neq \emptyset$ である．任意の $(A, \alpha), (B, \beta) \in \mathcal{R}$ に対して,

$$(A, \alpha) \preceq (B, \beta) \overset{\text{def}}{\iff} (A, \alpha) = (B, \beta) \text{ であるか, または } (A, \alpha) \text{ が } (B, \beta) \text{ の切片である} \tag{11}$$

と定義する．$\preceq$ は $\mathcal{R}$ 上の順序関係である．この定義から, $(A, \alpha) \preceq (B, \beta)$ であるとき, $A \subseteq B$ であり, かつ任意の $x, y \in A$ について $(x, y) \in \alpha \iff (x, y) \in \beta$ が成り立つ．次の補題は, この順序 $\preceq$ が帰納的であることを示している．これはもちろん, 後でこの順序に対して Zorn の補題を使うための準備であるが, この補題の証明が一番重たいところである．

補題 B.4. 式 (11) の順序関係 $\preceq$ は帰納的である．

証明. (I) $\{(A_i, \alpha_i)\}_{i \in I}$ を $\mathcal{R}$ における空でない鎖 (全順序な部分集合) として, これが上に有界であることを示せばよい．$A = \bigcup_{i \in I} A_i$ とおき, この上の二項関係 α を次の要領で定める．任意の $x, y \in A$ を取る．$\{(A_i, \alpha_i)\}_{i \in I}$ は鎖なので, $x, y \in A_i$ を満たす $i \in I$ が存在するが, $(x, y) \in \alpha_i$ であるとき, かつその時に限り $(x, y) \in \alpha$ であると定義する．

(II) $x, y \in A_i$ となる $i \in I$ の選び方によらず, $(x, y) \in \alpha$ であるか否かは (x, y) によって一通りに決まることを確かめておく．$x, y \in A_i$, $x, y \in A_j$ $(i, j \in I)$ とする．$\{(A_i, \alpha_i)\}_{i \in I}$ は鎖だから, 一般性を失わず $(A_i, \alpha_i) \preceq (A_j, \alpha_j)$ と仮定しておいてよい．すると, $(x, y) \in \alpha_i \iff (x, y) \in \alpha_j$ であるが, これは $(x, y) \in \alpha$ であるかどうかは $(x, y) \in \alpha_i$ か否かで判断しても $(x, y) \in \alpha_j$ か否かで判断しても同じ結論になることを示している．よって, α の定義はうまくいっている．

(III) α は A 上の順序関係であることを示す．任意の $x \in A$ について, $x \in A_i$ となる任意の $i \in I$ を選んでおけば, α_i の反射性から $(x, x) \in \alpha_i$ なので, $(x, x) \in \alpha$ である．よって, α は反射的である．$x, y, z \in A$, $(x, y) \in \alpha$, $(y, z) \in \alpha$ と仮定する．$\{(A_i, \alpha_i)\}_{i \in I}$ は鎖だから, $x, y, z \in A_i$ を満たす $i \in I$ が存在する．$(x, y) \in \alpha$ かつ $(y, z) \in \alpha$ だから, $(x, y), (y, z) \in \alpha_i$ であり, α_i の推移性から $(x, z) \in \alpha_i$ で

あり, したがって $(x,z)\in\alpha$ であることが従う. よって, α は推移的である. $x,y\in A$, $(x,y),(y,x)\in\alpha$ とすると, $x,y\in A_i$ を満たす添字 $i\in I$ が存在するが, $(x,y),(y,x)\in\alpha$ なので $(x,y),(y,x)\in\alpha_i$ であり, α_i の反対称性から $x=y$ が得られる. ゆえに, α は反対称的でもある. 以上から, α は A 上の順序関係である.

(IV) α は整列順序であることを示そう. S を A の空でない部分集合として, α に関して S の最小元が存在することを示せばよい. $S\neq\emptyset$ なので, 少なくとも一つの添字 $i\in I$ に対して $S\cap A_i\neq\emptyset$ である. $S\cap A_i$ は A_i の空でない部分集合であるが, α_i は A_i 上の整列順序なので, α_i に関する最小元 $x=\min(S\cap A_i)$ が存在する. これが α に関する S の最小元であることを示せばよい. それには, 任意の $a\in S$ を取り, $(x,a)\in\alpha$ であることを示せばいい. $a\in A_i$ ならば, $a\in S\cap A_i$ なので, x の選び方から $(x,a)\in\alpha_i$ であり, したがって $(x,a)\in\alpha$ でもある.

$a\in S\subseteq A$ なので, $a\in A_j$ を満たす添字 $j\in I$ が存在する. $\{(A_i,\alpha_i)\}_{i\in I}$ は鎖だから, $(A_i,\alpha_i)\preceq(A_j,\alpha_j)$ または $(A_i,\alpha_i)\succeq(A_j,\alpha_j)$ が成り立つ. $(A_i,\alpha_i)\succeq(A_j,\alpha_j)$ のときは, $a\in A_j\subseteq A_i$ なので, $(x,a)\in\alpha$ が成り立つ. $(A_i,\alpha_i)\preceq(A_j,\alpha_j)$ のときを考える. $(A_i,\alpha_i)=(A_j,\alpha_j)$ ならば, $a\in A_j=A_i$ なので, $(x,a)\in\alpha$ が成り立つ. (A_i,α_i) が (A_j,α_j) のある点 $y\in A_j$ における切片であるときを考える. $x\in A_i$ だから, $x\in A_j$ であり, かつ順序 α_j について $x<y$, すなわち $(x,y)\in\alpha_j$ である. よって, $(y,a)\in\alpha_j$ ならば, α_j の推移性から $(x,a)\in\alpha_j$ であり, したがって $(x,a)\in\alpha$ でもある. $(y,a)\notin\alpha_j$ のときには, A_j 上で順序 α_j に関して $a<y$ なので, $a\in A_i$ であり, したがって $(x,a)\in\alpha$ が成り立つ. 以上から, α に関して $x=\min S$ であることが分かった.

(V) (IV) から, $(A,\alpha)\in\mathcal{R}$ である. これが $\mathcal{R}$ における鎖 $\{(A_i,\alpha_i)\}_{i\in I}$ の上界であることを示す. 任意の $i\in I$ について, $(A_i,\alpha_i)\preceq(A,\alpha)$ であることを示せばよい. $A_i=A$ であれば, $\alpha_i=\alpha$ でもあって, $(A_i,\alpha_i)=(A,\alpha)$ であり, したがって $(A_i,\alpha_i)\preceq(A,\alpha)$ である.

$A_i\subsetneq A$ の場合を考えて, α に関する $A\setminus A_i$ の最小元を x とする. (A_i,α_i) がこの点 x における (A,α) の切片 $A(x)$ であることを示す. x の $A\setminus A_i$ における最小性から, $A(x)\subseteq A_i$ である. この逆の包含を示すために, 任意の $z\in A_i$ を考える. $z\in A_i$ かつ $x\notin A_i$ なので, $z\neq x$ である. α は全順序なので, それに関して $z<x$ または $z>x$ が成り立つ.

$z>x$ の場合を考える. $x\in A$ だから, $x\in A_j$ となる $j\in I$ が存在する. $\{(A_i,\alpha_i)\}_{i\in I}$ は鎖だから, $(A_i,\alpha_i)\preceq(A_j,\alpha_j)$ または $(A_i,\alpha_i)\succeq(A_j,\alpha_j)$ である. $(A_i,\alpha_i)\succeq(A_j,\alpha_j)$ ならば, $x\in A_j\subseteq A_i$ であり, $x\notin A_i$ に反する. よって, $(A_i,\alpha_i)\preceq(A_j,\alpha_j)$ である. $(A_i,\alpha_i)=(A_j,\alpha_j)$ ならば, $x\in A_j=A_i$ となるが, これは $x\notin A_i$ に反する. ゆえに, (A_i,α_i) は (A_j,α_j) のある点 w における切片 $A_j(w)$ である. α_j の下で $x<w$ であれば, $x\in A_j(w)=A_i$ なって, $x\notin A_i$ に反する. よって, α_j の下で $w\leq x$ であり, したがって α の下でも $w\leq x$ である. 一方, $z\in A_i=A_j(w)$ なので, α_j の下で $z<w$ であり, したがって α の下でも $z<w$ である. ゆえに, α の下で $z<w\leq x$ であるが, これは $z>x$ に反するのであり得ない. したがって, $z>x$ ではあり得ず, $z<x$, すなわち $z\in A(x)$ が成り立つ.

以上から, $A_i=A(w)$ であり, (A_i,α_i) は x における (A,α) の切片である. よって, $(A_i,\alpha_i)\preceq(A,\alpha)$ である. □

よって, Zorn の補題を用いて順序 $\preceq$ に関する $\mathcal{R}$ の極大元 (A,α) が存在することが分かる. 後は $A=X$ であることを示せば, α は X 上の整列順序であることになり, 整列可能定理が証明されることになるが, その議論は本項の冒頭で述べたアイデアの通りである.

$A \subsetneq X$ であると仮定して, A に属さない任意の $x \in X$ を選ぶ. $\bar{A} = A \cup \{x\}$ とおき, さらに

$$\bar{\alpha} = \alpha \cup \{(a, x) \mid a \in A\} \cup \{(x, x)\}$$

と定義することで, $\bar{\alpha}$ は $\bar{A}$ 上の整列順序であり, $(\bar{A}, \bar{\alpha}) \in \mathcal{R}$ であることが分かる. なおかつ, (A, α) は x における $(\bar{A}, \bar{\alpha})$ の切片なので, 順序 $\preceq$ に関して $(\bar{A}, \bar{\alpha})$ は (A, α) よりも真に大きい. しかし, これは (A, α) の $\mathcal{R}$ における極大性に反する. 以上から, $A = X$ でなければならない. これで, Zorn の補題から整列可能定理が導かれた.

B.3　整列可能定理から選択公理へ

最後に, 整列可能定理を仮定してそこから選択公理へ里帰りする. これは易しい. $\{A_i\}_{i \in I}$ を空でない集合 A_i らの族とするとき, 整列可能定理から各々の集合 A_i は空でない整列集合であると仮定してよく, したがって選択関数 $f : I \to U$ ($U = \bigcup_{i \in I} A_i$) を $f(i) = \min A_i$ によって具体的に構成できる.