2022 年度「数学特論 7 ／組合せ論大意」

講義資料

縫田 光司

（九州大学マス・フォア・インダストリ研究所）

nuida@imi.kyushu-u.ac.jp

最終更新：2022 年 8 月 5 日

目次

1 全単射による証明

唐突ではあるが、以下の命題の証明を考える。

命題 1.1. 整数 $n \geq 1$ について、$n! = 1 + \sum_{k=1}^{n-1} k \cdot k!$ が成り立つ。

証明（その 1）. n についての数学的帰納法を用いる。$n = 1$ のときは両辺とも 1 となり等しいので、以下では $n \geq 2$ として、$n-1$ の場合に主張が成り立つとして n の場合の主張を証明する。$n-1$ の場合の主張により

$$(n-1)! = 1 + \sum_{k=1}^{n-2} k \cdot k!$$

であり、また

$$n! - (n-1)! = n \cdot (n-1)! - (n-1)! = (n-1) \cdot (n-1)!$$

である。これらの式の両辺をそれぞれ加えると、

$$n! = 1 + \sum_{k=1}^{n-2} k \cdot k! + (n-1) \cdot (n-1)! = 1 + \sum_{k=1}^{n-1} k \cdot k!$$

となり、n の場合の主張が導かれる。以上より主張はすべての n について成り立つ。 □

上記の証明は確かに正しいし、数学的帰納法を用いるというある意味での常套手段に則っているので着想しやすいという利点がある。一方で、この命題が「なぜ成り立つのか」という「意味」を実感しづらい点にやや不満が残る（かもしれない。この辺りは個々人の主観による）。次に、以下の別証明を考えてみる。

証明（その 2）. S_n を n 次対称群とする。id を恒等置換（すべての元を固定する置換）とし、$\sigma \in S_n \setminus \{\mathrm{id}\}$ について、$\sigma(a) \neq a$ となる最大の整数 a を $k(\sigma)$ と書く。ここで、$\sigma \neq \mathrm{id}$ のとき、σ は少なくとも二つの元を動かすので、ある $a \geq 2$ について $\sigma(a) \neq a$ である。したがってそのような最大の a が確かに存在し、かつ $k(\sigma) \geq 2$ である。$1 \leq k \leq n-1$ となる整数 k について

$$X_k := \{\sigma \in S_n \setminus \{\mathrm{id}\} \mid k(\sigma) = k+1\}$$

と定めると、上で述べたことから S_n は部分集合 $\{\mathrm{id}\}$ および X_k たちの非交和である。さて、$\sigma \in X_k$ とすると σ は $k+2$ 以上の整数を動かさないので、実質的には S_{k+1} の元と

みなすことができ、一方で $\sigma(k+1) \neq k+1$ であることから S_k の元ではない。この議論より $X_k = S_{k+1} \setminus S_k$ であることがわかり、

$$|X_k| = |S_{k+1}| - |S_k| = (k+1)! - k! = k \cdot k!$$

となる。S_n は $\{\mathsf{id}\}$ および X_k たちの非交和であったから、元の個数を数えると $|S_n| = 1 + \sum_{k=1}^{n-1} k \cdot k!$ が成り立つ。一方で $|S_n| = n!$ であるから、$n! = |S_n| = 1 + \sum_{k=1}^{n-1} k \cdot k!$ となり主張が導かれる。 □

こちらの証明の要点は、主張の両辺の値 $n!$ と $1 + \sum_{k=1}^{n-1} k \cdot k!$ のどちらも、同じ集合の要素の数を別の方法で数えたものである（したがってそれらは互いに等しい）という事実である。等式に現れる値に、ある具体的な集合の要素の数という「意味」が与えられている分だけ、この命題が「なぜ成り立つのか」を実感しやすくなっている（かもしれない）。こうした「同じ集合の要素数を複数の方法で数える」という手法、より一般化すると「等式の一方の値をある集合 X の要素数、他方の値をある集合 Y の要素数として表した上で、X と Y の要素数が互いに等しいことを示す」という手法による証明は、**全単射による証明**（bijective proof）と称される（**組合せ論的証明**（combinatorial proof）や、**数え上げ法**（counting argument）による証明などと称されることもある）。

全単射による証明の別の例を挙げる。

命題 1.2. 整数 $n \geq k \geq 1$ について、$\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}$ である。ここで $\binom{n}{k}$ は二項係数を表す。

二項係数の具体的な表示 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ を既知とすれば証明は明らかであるが、ここでは二項係数の具体的な表示を用いず、「$\binom{n}{k}$ は n 個の元から k 個を選ぶ場合の数である」という定義に立ち返った証明を与える。

証明. 主張の式は $k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$ と等価なのでこちらの等式を示す。$[n] := \{1, 2, \dots, n\}$ とおき、

$$X := \{(I, a) \mid a \in I \subseteq [n], |I| = k\}$$

と定める。この集合 X の要素数を 2 通りの方法で数える。

- X の要素を「先に I を選び、次に I の要素の中から a を選ぶ」という方法で数え上げると、I の選び方が $\binom{n}{k}$ 通り（二項係数の定義）、a の選び方が k 通りあるの

で、$|X| = k \cdot \binom{n}{k}$ である。

- X の要素を「先に a を選び、次に a を含む集合 I を選ぶ」という方法で数え上げると、a の選び方が n 通り、I の選び方が（a は要素に入ることが決まっていて、残り $k-1$ 個の要素を a 以外の $n-1$ 個から選ぶので）$\binom{n-1}{k-1}$ 通りあるので、$|X| = n \cdot \binom{n-1}{k-1}$ である。

これらがそれぞれ示すべき式の左辺と右辺に対応しているため、主張が成り立つ。 □

以降では、Euler の五角数定理（Euler's pentagonal number theorem）と呼ばれる下記の定理について全単射による証明を紹介する。

定理 1.1. $\prod_{n \geq 1}(1-t^n) = \sum_{k=-\infty}^{\infty} (-1)^k t^{k(3k-1)/2}$ が成り立つ。

上の両辺は正式には「（t を変数とする）形式的冪級数」として考えるのであるが、ここでは形式的冪級数の定義は割愛し、上の主張を「両辺を t の冪級数の形に形式的に展開すると、どの N についても t^N の係数が互いに等しい」という意味であると解釈する。例えば左辺における t^6 の係数を考えると、

- 積 $(1-t^6)$ から出てくる項 $-t^6$
- 積 $(1-t^5)(1-t^1)$ から出てくる項 $(-t^5)(-t^1) = t^6$
- 積 $(1-t^4)(1-t^2)$ から出てくる項 $(-t^4)(-t^2) = t^6$
- 積 $(1-t^3)(1-t^2)(1-t^1)$ から出てくる項 $(-t^3)(-t^2)(-t^1) = -t^6$

の和となるので、t^6 の係数は 0 となる。なお、右辺について、k が負の数 $k = -K$ であるときは指数部は $(-K)(-3K-1)/2 = K(3K+1)/2$ となるので、右辺の式を

$$1 + \sum_{k=1}^{\infty}(-1)^k t^{k(3k-1)/2} + \sum_{K=1}^{\infty}(-1)^K t^{K(3K+1)/2}$$

と書いてもよい。また、正整数 k, K について $k(3k-1)/2 \neq K(3K+1)/2$ であることを注意しておく。実際、$k \leq K$ であれば明らかに $k(3k-1)/2 < K(3K+1)/2$ であり、$k > K$ すなわち $k \geq K+1$ のときには

$$\frac{k(3k-1)}{2} \geq \frac{(K+1)(3K+2)}{2} > \frac{K(3K+1)}{2}$$

である。このことから、右辺を展開した際の各項の係数は 0 または ± 1 となる。特に、右辺における定数項すなわち t^0 の項の係数は 1 であり、左辺においても係数は 1 であるから、定理を証明する上では指数部が正の項だけに着目すれば充分である。

主張の左辺の展開式を整理するために、以下の定義を導入する。

定義 1.1. 正の整数を大きい順（等号も含む）に 0 個以上の有限個並べた列

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell) \quad (\lambda_i \text{ たちは整数で } \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0)$$

を**分割**（partition）という。より詳しくは、$|\lambda| := \displaystyle\sum_{i=1}^{\ell} \lambda_i = n$ のとき、λ を整数 n の分割といい、記号 $\lambda \vdash n$ で表す。また、ℓ を分割 λ の**長さ**といい、$\ell(\lambda)$ で表す。（空の列を $\emptyset$ で表すことにすると、$\emptyset$ は 0 個の要素からなる分割と考えられ、このとき $\emptyset \vdash 0$、$\ell(\emptyset) = 0$ である。）

この定義のもとで、左辺の t^N の係数に寄与する項は、成分がすべて異なる N の分割 $\lambda = (\lambda_1, \ldots, \lambda_\ell) \vdash N$ に応じて積 $(1-t^{\lambda_1}) \cdots (1-t^{\lambda_\ell})$ から出てくる項 $(-t^{\lambda_1}) \cdots (-t^{\lambda_\ell}) = (-1)^\ell t^N$ たちである。したがって、成分がすべて異なる N の分割で長さが偶数（、奇数）であるものの個数を $e(N)$（、$o(N)$）で表すと、左辺の t^N の係数は $e(N) - o(N)$ となる。

整数の分割を視覚的に表しやすくする以下の定義を導入する。

定義 1.2. 整数の分割 $\lambda = (\lambda_1, \ldots, \lambda_\ell)$ について、正方形の箱を、上から 1 行目に λ_1 個、上から 2 行目に λ_2 個、…、上から ℓ 行目に λ_ℓ 個並べてできる図形を λ に対応する **Young 図形**（Young diagram）という（図 1 を参照）。

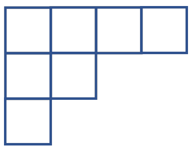


図 1　分割 $\lambda = (4, 2, 1)$ に対応する Young 図形

Young 図形の定義から、各行にある箱の個数は下の行にいくほど広義減少することを注意しておく。以降では、空でない（つまり、箱が 1 個以上ある）Young 図形のうち、各行の長さ（各行にある箱の個数）がすべて互いに異なるもの全体の集合を $\mathcal{Y}$ で表す。また、N 箱からなる Young 図形 $Y \in \mathcal{Y}$ 全体の集合を $\mathcal{Y}_N$ で表し、そのうち偶数行（、奇数行）からなるもの全体の集合を $\mathcal{Y}_{N,e}$（、$\mathcal{Y}_{N,o}$）で表す。先ほどの記号を用いると $e(N) - o(N) = |\mathcal{Y}_{N,e}| - |\mathcal{Y}_{N,o}|$ である。すると直感的には、主張の等式は $\mathcal{Y}_{N,e}$ と $\mathcal{Y}_{N,o}$ の要素数が「少々の誤差を除いて」一致することを意味していると考えられる。より詳しく、この「誤差」を捉えるために以下の Young 図形を定義する。整数 $k \geq 1$ について、k 行からなり、1 行目の箱の数が $2k-1$ 個、以下箱の数が 1 個ずつ減っていき、最後 k 行目の箱の数が k 個である Young 図形を $\widehat{Y}_k$ で表す。同様に、整数 $K \geq 1$ について、K 行

からなり、1 行目の箱の数が $2K$ 個、以下箱の数が 1 個ずつ減っていき、最後 K 行目の箱の数が $K+1$ 個である Young 図形を $\widetilde{Y}_K$ で表す。

$$\mathcal{E} := \{\widehat{Y}_k \mid k \geq 1\} \cup \{\widetilde{Y}_K \mid K \geq 1\}$$

とおく。ここで、$\widehat{Y}_k$ の箱の総数は $((2k-1)+k) \cdot k/2 = k(3k-1)/2$、$\widetilde{Y}_K$ の箱の総数は $(2K+(K+1)) \cdot K/2 = K(3K+1)/2$ であることに注意する。すると、$k \geq 1$ が奇数のとき、$N = k(3k-1)/2$ とすると、主張の右辺における t^N の係数は -1 であるから、$|\mathcal{Y}_{N,e}| - |\mathcal{Y}_{N,o}| = -1$ すなわち $|\mathcal{Y}_{N,e}| = |\mathcal{Y}_{N,o}| - 1$ が示すべき性質となる。これを示すには、$\mathcal{Y}_{N,o}$ から「例外の要素」$\widehat{Y}_k$ を除いた集合と $\mathcal{Y}_{N,e}$ との間に全単射が存在する（したがって要素数が一致する）ことを示せば充分である。また、$k \geq 1$ が偶数のとき、$N = k(3k-1)/2$ とすると、主張の右辺における t^N の係数は 1 であるから、$|\mathcal{Y}_{N,e}| - |\mathcal{Y}_{N,o}| = 1$ すなわち $|\mathcal{Y}_{N,e}| - 1 = |\mathcal{Y}_{N,o}|$ が示すべき性質となる。これを示すには、$\mathcal{Y}_{N,e}$ から「例外の要素」$\widehat{Y}_k$ を除いた集合と $\mathcal{Y}_{N,e}$ との間に全単射が存在することを示せば充分である。$N = K(3K+1)/2$ における t^N の係数の比較についても同様に、$\widetilde{Y}_K$ を「例外の要素」として $\mathcal{Y}_{N,e}$ と $\mathcal{Y}_{N,o}$ とを比較すればよい。それ以外の N については、例外の要素を考える必要はなく、$\mathcal{Y}_{N,e}$ と $\mathcal{Y}_{N,o}$ の間に全単射が存在することを示せばよい。以上をまとめると、示すべきことは「どの $N \geq 1$ についても、$\mathcal{Y}_{N,e} \setminus \mathcal{E}$ と $\mathcal{Y}_{N,o} \setminus \mathcal{E}$ の間に全単射が存在する」ことと端的に表現できる。

$Y \in \mathcal{Y}$ について、Y の一番下の行の長さを $a = a(Y)$ とおき、「Y の 1 行目から k 行目までは長さが 1 ずつ減っていき、$k+1$ 行目では長さが 2 以上減る」を満たす唯一の k を $b = b(Y)$ とおく。ただし $b(Y)$ については、1 行目と 2 行目の長さが 2 以上違う場合は $b(Y) = 1$、またどの行も長さが 1 ずつ減っている場合は $b(Y)$ を Y の行数と定める（図 2)。例えば $\lambda = (7,6,4,3)$ に対応する Young 図形 Y について $a(Y) = 3$、$b(Y) = 2$ である。ここで、以下の操作で得られる $\mathcal{Y}$ の元を $\varphi(Y)$ で表す。

- $a \leq b$ のとき、Y の一番下の行の箱を、上から a 行目までに 1 個ずつ（一番右に）移動させる（図 3 の左側)。
- $a > b$ のとき、Y の上から b 行の一番右の箱たちを、Y の一番下の行の次の行にまとめて移動させる（図 3 の右側)。

ただし、$a \leq b$ の場合、もし Y の行数が b 行でかつ $a = b$ である（つまり $Y = \widehat{Y}_b$ である）とこの操作がうまく定義できない（消去される行と箱が追加される行が重複してしまう）のでその場合は除外する。また $a > b$ の場合、もし Y の行数が b 行でかつ $a = b+1$ である（つまり $Y = \widetilde{Y}_b$ である）とこの操作がうまく定義できない（操作後の b 行目と $b+1$ 行目がともに長さ b となってしまう）のでその場合は除外する。つまり、実際には操作 φ は $\mathcal{Y} \setminus \mathcal{E}$ の元に対して定義されている。この操作について以下の性質が成り立つ。

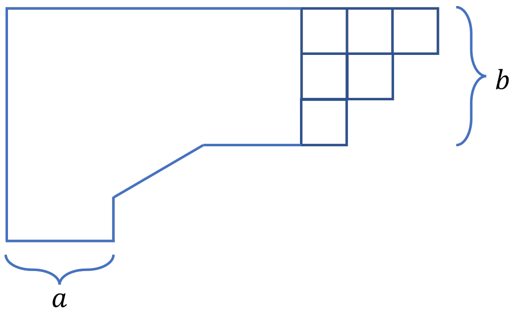


図 2　$a = a(Y)$ と $b = b(Y)$ の定義の模式図

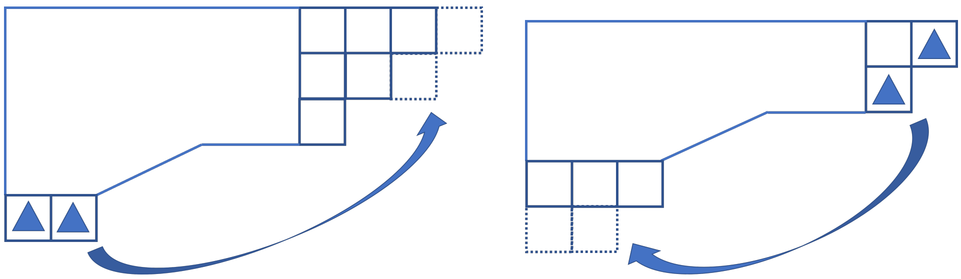


図 3　操作 φ の定義の模式図（左側は $a \leq b$ のとき、右側は $a > b$ のとき）

補題 1.1. $Y \in \mathcal{Y} \setminus \mathcal{E}$ について $\varphi(Y) \in \mathcal{Y} \setminus \mathcal{E}$ である。

証明. $\varphi(Y) \in \mathcal{Y}$ であることについては、$a(Y) \leq b(Y)$ のときは操作 φ で各行の長さの差が減らないことから成り立つ。$a(Y) > b(Y)$ のときは、行の長さの差が変化するのは $b(Y)$ 行目と $b(Y)+1$ 行目の間、および新たに追加される行とその上の行の間だけである。Y の行数が $b(Y)$ 行の場合（このとき、$Y \notin \mathcal{E}$ より $a(Y) \geq b(Y)+2$ である）には、追加される行の長さが $b(Y) < a(Y)-1$ であるため主張が成り立つ。そうでない場合、前者の行間については Y の $b(Y)+1$ 行目と $b(Y)$ 行目の長さが 2 以上違うことから操作後も長さが異なる。後者の行間については、追加される行の長さ $b(Y)$ とその上の行の操作後の長さ $a(Y)$ は上の条件より確かに異なる。以上よりどの場合にも $\varphi(Y) \in \mathcal{Y}$ である。

$\varphi(Y) \notin \mathcal{E}$ を示すために、$\varphi(Y)$ の行の長さがどこも 1 ずつ減っていると仮定する。$a(Y) \leq b(Y)$ のとき、これが起きるには $b(Y) = a(Y)$ である必要があり、$Y \notin \mathcal{E}$ であることから Y の行数は $b(Y)+1$ 行以上である。すると Y の $b(Y)$ 行目の長さは $a(Y)+2 = b(Y)+2$ 以上であり、$\varphi(Y)$ の $b(Y)$ 行目の長さは $b(Y)+3$ 以上となる。このような $\mathcal{E}$ の元は存在しないので、$\varphi(Y) \notin \mathcal{E}$ である。一方 $a(Y) > b(Y)$ のとき、$\varphi(Y)$ は $b(Y)+1$ 行以上からなり最後の行の長さが $b(Y)$ である。このような $\mathcal{E}$ の元は存在しないので、$\varphi(Y) \notin \mathcal{E}$ である。以上よりどの場合にも $\varphi(Y) \notin \mathcal{E}$ であり、主張が成り立つ。 □

補題 1.2. $Y \in \mathcal{Y} \setminus \mathcal{E}$ について $\varphi(\varphi(Y)) = Y$ である。

証明. まず $a(Y) > b(Y)$ のとき、φ の構成より $a(\varphi(Y)) = b(Y)$、$b(\varphi(Y)) \geq b(Y)$ が成り立つので、$a(\varphi(Y)) \leq b(\varphi(Y))$ である。よって $\varphi(Y)$ に操作 φ を行うと、最初の操作 φ で最終行に移動してきた $b(Y)$ 箱が先頭 $b(Y)$ 行に戻されることになり、$\varphi(\varphi(Y))$ が成り立つ。

次に $a(Y) \leq b(Y)$ の場合を考える。Y の行数が $b(Y)+1$ 行以上のとき、Y の下から 2 行目の長さを c とすると、φ の構成より $a(\varphi(Y)) \geq c > a(Y)$、$b(\varphi(Y)) = a(Y)$ が成り立つので、$a(\varphi(Y)) > b(\varphi(Y))$ である。よって $\varphi(Y)$ に操作 φ を行うと、最初の操作 φ で先頭 $a(Y)$ 行に移動してきた箱たちが一番下に戻されることになり、$\varphi(\varphi(Y))$ が成り立つ。

また Y の行数が $b(Y)$ 行のときは、$Y \notin \mathcal{E}$ より $a(Y) < b(Y)$ であり、φ の構成より $a(\varphi(Y)) \geq a(Y)+1$、$b(\varphi(Y)) = a(Y)$ が成り立つので、$a(\varphi(Y)) > b(\varphi(Y))$ である。よって $\varphi(Y)$ に操作 φ を行うと、最初の操作 φ で先頭 $a(Y)$ 行に移動してきた箱たちが一番下に戻されることになり、$\varphi(\varphi(Y))$ が成り立つ。以上より主張が成り立つ。 □

補題 1.2 より φ は自分自身の逆写像であり、したがって $\mathcal{Y} \setminus \mathcal{E}$ からそれ自身への全単射である。また定義より φ は箱の総数を変えず行数を 1 だけ変化させるので、$\varphi(\mathcal{Y}_{N,e} \setminus \mathcal{E}) \subseteq \mathcal{Y}_{N,o} \setminus \mathcal{E}$ および $\varphi(\mathcal{Y}_{N,o} \setminus \mathcal{E}) \subseteq \mathcal{Y}_{N,e} \setminus \mathcal{E}$ が成り立つ。すると φ が全射であることから $\varphi(\mathcal{Y}_{N,e} \setminus \mathcal{E}) = \mathcal{Y}_{N,o} \setminus \mathcal{E}$ および $\varphi(\mathcal{Y}_{N,o} \setminus \mathcal{E}) = \mathcal{Y}_{N,e} \setminus \mathcal{E}$ が成り立つ。こうして各 N について φ は $\mathcal{Y}_{N,e} \setminus \mathcal{E}$ と $\mathcal{Y}_{N,o} \setminus \mathcal{E}$ の間の全単射を与えることが示されたので、定理の主張が成り立つ。

演習問題

■問題 1.　整数 $n \geq k \geq 0$ について、二項係数の表示 $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ を全単射により証明せよ。

（ヒント：分母を払うと $k!(n-k)! \cdot \binom{n}{k} = n!$ が示すべき式となる。右辺は S_n の要素数であるが、S_n の要素数をどのように数えれば左辺の値になるだろうか？）

■問題 2.　整数 $n \geq 1$ について、$\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ を全単射による証明で示せ。

（ヒント：主張を $\displaystyle\sum_{k;\,\text{偶数}} \binom{n}{k} = \sum_{k;\,\text{奇数}} \binom{n}{k}$ という形に書き換える。）

2 母関数

例えば、以下の漸化式で定義される数列 $(b_n)_n$ について考える：

$$b_0 = b_1 = 1 \, , \, b_n = b_{n-1} + b_{n-2} \quad (n \geq 2)$$

よく知られているようにこれは Fibonacci 数であり、初等的な方法によって一般項を決定することができるが、ここでは**母関数**（generating function）という道具を用いて一般項を計算してみる。そのために、数列 $(b_n)_n$ の母関数

$$B(t) := \sum_{n \geq 0} b_n t^n$$

を導入する。正式にはこれは「形式的冪級数」なのであるが詳しくは後述することにして、ひとまず「多項式に似た性質を持つ形式的な和」であると考えておく。この母関数についての「関数等式」を得るべく、多少天下り式ではあるが $\widehat{B}(t) := B(t) - tB(t) - t^2 B(t)$ という式を考える。$n \geq 2$ について $\widehat{B}(t)$ における t^n の係数を計算すると

$$\begin{aligned}
&【B(t) \text{ の } t^n \text{ の係数}】-【tB(t) \text{ の } t^n \text{ の係数}】-【t^2 B(t) \text{ の } t^n \text{ の係数}】\\
&=【B(t) \text{ の } t^n \text{ の係数}】-【B(t) \text{ の } t^{n-1} \text{ の係数}】-【B(t) \text{ の } t^{n-2} \text{ の係数}】\\
&= b_n - b_{n-1} - b_{n-2} = 0
\end{aligned}$$

となる（最後の等号は漸化式から導かれる）。したがって $\widehat{B}(t)$ は t に関する 1 次以下の多項式である。同様に 1 次と 0 次の係数も計算すると、

$$\begin{aligned}
【\widehat{B}(t) \text{ の } t^1 \text{ の係数}】&=【B(t) \text{ の } t^1 \text{ の係数}】-【tB(t) \text{ の } t^1 \text{ の係数}】-【t^2 B(t) \text{ の } t^1 \text{ の係数}】\\
&=【B(t) \text{ の } t^1 \text{ の係数}】-【B(t) \text{ の } t^0 \text{ の係数}】- 0\\
&= b_1 - b_0 = 0 \ ,
\end{aligned}$$

$$\begin{aligned}
【\widehat{B}(t) \text{ の } t^0 \text{ の係数}】&=【B(t) \text{ の } t^0 \text{ の係数}】-【tB(t) \text{ の } t^0 \text{ の係数}】-【t^2 B(t) \text{ の } t^0 \text{ の係数}】\\
&=【B(t) \text{ の } t^0 \text{ の係数}】- 0 - 0\\
&= b_0 = 1
\end{aligned}$$

となる。以上より $\widehat{B}(t) = B(t) - tB(t) - t^2 B(t) = 1$ であり、$B(t)$ をひとまず

$$B(t) = \frac{1}{1 - t - t^2}$$

と決定できる。（「形式的冪級数」としてみたときに右辺の有理式は何を表しているのか、という点が気になるかもしれないがひとまず保留して先に進む。）

上記の式からは $B(t)$ の各項の係数（つまり、$(b_n)_n$ の一般項）が直ちにはわからないので、$1-t-t^2 = \left(1 - \frac{1+\sqrt{5}}{2}t\right)\left(1 - \frac{1-\sqrt{5}}{2}t\right)$ という関係を用いて部分分数分解を行う。

$$B(t) = \frac{1}{1-t-t^2} = \frac{1}{\sqrt{5}t}\left(\frac{1}{1-\frac{1+\sqrt{5}}{2}t} - \frac{1}{1-\frac{1-\sqrt{5}}{2}t}\right) .$$

等比級数の和の公式を形式的に適用すると、右辺はさらに

$$\frac{1}{\sqrt{5}t}\left(\sum_{k\geq 0}\left(\frac{1+\sqrt{5}}{2}t\right)^k - \sum_{k\geq 0}\left(\frac{1-\sqrt{5}}{2}t\right)^k\right)$$

と変形できる。この t^n の係数が b_n であったから、括弧内の式における t^{n+1} の係数を $\sqrt{5}$ で割って、

$$b_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$$

を得る。こうして数列 $(b_n)_n$ の一般項が決定できた。

上の例ではそもそも一般項を初等的な方法でも決定できるので母関数の有難みがあまり感じられないかもしれない。次はもう少し複雑な例を考える。整数 $n \geq 0$ について、n 番目の **Catalan 数** C_n を、座標平面の原点 $(0,0)$ から点 $(2n,0)$ まで以下の規則に従って到達する方法の総数と定義する。

- 1 回の移動では「x 軸方向に 1、y 軸方向に 1 進む」または「x 軸方向に 1、y 軸方向に -1 進む」のいずれかを行う。
- 移動中には y 座標が常に非負であるようにする。

なお、このような条件を満たす経路は **Dyck path** と呼ばれる。例えば $n = 3$ のとき、$(1,1)$、$(1,-1)$ の進行をそれぞれ $\nearrow$、$\searrow$ で表すと、$(0,0)$ から $(6,0)$ への Dyck path は

$$\nearrow\nearrow\nearrow\searrow\searrow\searrow\ ,\ \nearrow\nearrow\searrow\nearrow\searrow\searrow\ ,\ \nearrow\nearrow\searrow\searrow\nearrow\searrow\ ,\ \nearrow\searrow\nearrow\nearrow\searrow\searrow\ ,\ \nearrow\searrow\nearrow\searrow\nearrow\searrow$$

の全部で 5 通りあるため、$C_3 = 5$ である。$n = 0$ については空の Dyck path が一つと考えて $C_0 = 1$ とする。この Catalan 数の一般項を、母関数 $C(t) := \sum_{n\geq 0} C_n t^n$ を用いて求めたい。

まず Catalan 数が満たす漸化式を与える。そのために、$n \geq 1$ のとき、Dyck path の各々について、出発後に初めて x 軸に乗る（y 座標が 0 になる）点に着目する。y 座標の増減の仕方に着目すると、このような点は $(2k,0)$（k は整数、$1 \leq k \leq n$）という形をし

ていることがわかる。ここで、点 $(2k,0)$ で初めて x 軸に乗る Dyck path では、1 歩目が $\nearrow$、$2k$ 歩目が $\searrow$ であり、2 歩目から $2k-1$ 歩目までは「点 $(1,1)$ から点 $(2k-1,1)$ までを、y 座標を 1 以上に保ちつつ移動する」ようになっている。この「」部の path は、全体を $(-1,-1)$ だけ平行移動させることで $(0,0)$ から $(2k-2,0)$ までの Dyck path と対応する。一方で、$(2k,0)$ から $(2n,0)$ までの部分については y 座標を非負に保つ以外の制限は特になく、全体を $(-2k,0)$ だけ平行移動させると $(0,0)$ から $(2n-2k,0)$ までの Dyck path と対応する。全体の path はこれら 2 種類の path の組で決定されるので、k が $1 \le k \le n$ の範囲を動くことと合わせて、以下の漸化式を得る。

$$C_0 = 1\,,\, C_n = \sum_{k=1}^{n} C_{k-1}C_{n-k} \quad (n \ge 1)\ .$$

ここで $\widehat{C}(t) := C(t) - tC(t)^2$ という式を考えると、$n \ge 1$ のとき

$$\begin{aligned}
【\widehat{C}(t) \text{ の } t^n \text{ の係数}】 &= 【C(t) \text{ の } t^n \text{ の係数}】 - 【tC(t)^2 \text{ の } t^n \text{ の係数}】\\
&= C_n - 【C(t)^2 \text{ の } t^{n-1} \text{ の係数}】\\
&= C_n - \sum_{k=0}^{n-1} 【C(t) \text{ の } t^k \text{ の係数}】\cdot【C(t) \text{ の } t^{n-1-k} \text{ の係数}】\\
&= C_n - \sum_{k=0}^{n-1} C_k C_{n-1-k}\\
&= C_n - \sum_{k=1}^{n} C_{k-1} C_{n-k} = 0
\end{aligned}$$

となる（最後の等式に上の漸化式を用いた）。よって $\widehat{C}(t)$ は定数であり、t^0 の係数が $C_0 - 0 = 1$ となることから、$\widehat{C}(t) = C(t) - tC(t)^2 = 1$、したがって

$$tC(t)^2 - C(t) + 1 = 0$$

となる。

上記の $C(t)$ に関する 2 次方程式を解きたい。平方完成しやすくするために両辺を $4t$ 倍して、

$$4t^2C(t)^2 - 4tC(t) + 4t = 0$$

としておく。変形すると

$$(2tC(t) - 1)^2 = 1 - 4t$$

となる。右辺の $1 - 4t$ の平方根を求めるために、以下の補題を用意する。

補題 2.1. 実数 λ について

$$F_\lambda(t) := \sum_{n \geq 0} \frac{\lambda(\lambda-1)\cdots(\lambda-n+1)}{n!} t^n$$

と定めると、$F_\lambda(t)F_\mu(t) = F_{\lambda+\mu}(t)$ が成り立つ。

証明. 主張の式の左辺における t^n の係数を $P_n(\lambda,\mu)$、右辺における t^n の係数を $Q_n(\lambda,\mu)$ とおく。これらはどちらも多項式環 $\mathbb{R}[\lambda,\mu]$ の元である。$R_n(\lambda,\mu) := P_n(\lambda,\mu) - Q_n(\lambda,\mu)$ とおく。ここで、整数 $\mu \geq 0$ を任意に固定しておくと、$R_n(\lambda,\mu) \in \mathbb{R}[\lambda]$ とみなせる。またこのとき、$F_\mu(t)$ における $\mu+1$ 次以降の項の係数はすべて 0 となり、

$$F_\mu(t) = \sum_{n=0}^{\mu} \binom{\mu}{n} t^n = (1+t)^\mu$$

が成り立つ。さらに λ も非負整数とすると、同様に $F_\lambda(t) = (1+t)^\lambda$、$F_{\lambda+\mu}(t) = (1+t)^{\lambda+\mu}$ となることから、$F_\lambda(t)F_\mu(t) = F_{\lambda+\mu}(t)$ が成り立ち、したがって $P_n(\lambda,\mu) = Q_n(\lambda,\mu)$ すなわち $R_n(\lambda,\mu) = 0$ である。つまり、整数 $\mu \geq 0$ を任意に固定したとき、λ の多項式 $R_n(\lambda,\mu)$ はすべての非負整数点で 0 となるので、多項式として 0 である。すなわち、どの $\lambda \in \mathbb{R}$ と非負整数 μ についても $R_n(\lambda,\mu) = 0$ が成り立つ。すると今度は実数 λ を任意に固定したとき、μ に関する多項式 $R_n(\lambda,\mu)$ はすべての非負整数点で 0 となるので、多項式として 0 である。すなわち、どの $\lambda,\mu \in \mathbb{R}$ についても $R_n(\lambda,\mu) = 0$ が成り立つ。したがって $P_n(\lambda,\mu)$ と $Q_n(\lambda,\mu)$ は常に一致し、P_n と Q_n の定義より主張の式 $F_\lambda(t)F_\mu(t) = F_{\lambda+\mu}(t)$ が導かれる。 □

補題 2.1 より $F_{1/2}(t)^2 = F_1(t) = 1+t$ が成り立ち、t に $-4t$ を代入することで $F_{1/2}(-4t)^2 = 1-4t$ となる。これを用いると

$$2tC(t) - 1 = \pm F_{1/2}(-4t) \tag{1}$$

となる（後で述べるように形式的冪級数の全体は整域をなすため、ある元の平方根は 2 個以下しか存在しないことを注意しておく）。さらに、

$$\begin{aligned} F_{1/2}(-4t) &= \sum_{n \geq 0} \frac{1/2 \cdot (1/2-1)\cdots(1/2-n+1)}{n!}(-4t)^n \\ &= 1 + \frac{1}{2}\cdot(-4t) + \sum_{n\geq 2} \frac{1\cdot(-1)\cdot(-3)\cdots(-(2n-3))}{2^n \cdot n!}(-4)^n t^n \end{aligned}$$

であり、$n \geq 2$ のとき

$$\begin{aligned}\frac{1\cdot(-1)\cdot(-3)\cdots(-(2n-3))}{2^n\cdot n!}(-4)^n &= \frac{(-1)^{n-1}\cdot 1\cdot 1\cdot 3\cdots(2n-3)}{n!}(-2)^n\\ &= -\frac{(2n-2)!}{2\cdot 4\cdots(2n-2)\cdot n!}2^n\\ &= -\frac{(2n-2)!}{2^{n-1}\cdot 1\cdot 2\cdots(n-1)\cdot n!}2^n\\ &= -\frac{2\cdot(2n-2)!}{(n-1)!n!}\end{aligned}$$

となるので、

$$F_{1/2}(-4t) = 1 - 2t + \sum_{n\geq 2}(-2)\frac{(2n-2)!}{(n-1)!n!}t^n$$

が成り立つ。すると、(1) 式の両辺の定数項を比較することで符号が決定でき、

$$2tC(t) - 1 = -F_{1/2}(-4t)$$

したがって

$$2tC(t) = 1 - F_{1/2}(-4t) = 2t + \sum_{n\geq 2} 2\frac{(2n-2)!}{(n-1)!n!}t^n = \sum_{n\geq 1} 2\frac{(2n-2)!}{(n-1)!n!}t^n$$

となる。両辺を $2t$ で割ると、母関数 $C(t)$ が

$$C(t) = \sum_{n\geq 1}\frac{(2n-2)!}{(n-1)!n!}t^{n-1} = \sum_{n\geq 0}\frac{(2n)!}{n!(n+1)!}t^n$$

と決定できる。以上より、Catalan 数の一般項が

$$C_n = \frac{(2n)!}{n!(n+1)!} = \frac{1}{n+1}\binom{2n}{n}$$

と決定される。なお、Catalan 数については、上記の定義以外にも同値な組合せ論的特徴付けが多数知られている。詳しくは Stanley の著書 [6] の 6 章の Exercise 6.19 を参照されたい（演習問題も参照）。

さて、以下ではこれまで棚上げにしていた「形式的冪級数とは一体何なのか」ということについて考える。素朴に取り扱うならば、多項式環を形式的に定義するときのように、冪指数の集合 $\{0, 1, 2, \ldots\}$ を定義域とする写像の全体にしかるべき方法で和と積を定義して、…という具合に議論することもできるが、ここでは別の方針で議論を進める。大まかにいうと、解析的な意味での収束する冪級数が多項式の列の極限になっているのと同様に、（解析的な意味での冪級数としては必ずしも収束しない、一般の）形式的冪級数を「多項式の極限」として取り扱いたい。そのための定義や性質を準備する。

定義 2.1. K を体とする。写像 $\nu\colon K \to \mathbb{R}_{\geq 0}$ が以下の条件を満たすとき、ν を K 上の**非 Archimedes 的付値**（non-Archimedean valuation）という。

1. $x \in K$ について、$\nu(x) = 0$ と $x = 0$ は同値である。
2. $x, y \in K$ について、$\nu(xy) = \nu(x)\nu(y)$ である。
3. $x, y \in K$ について、$\nu(x+y) \leq \max\{\nu(x), \nu(y)\}$ である。

簡略化のために、以降では非 Archimedes 的付値のことを単に付値と呼ぶ。一般論として以下の性質が知られている（証明は割愛する）。

命題 2.1. $\nu\colon K \to \mathbb{R}_{\geq 0}$ を K 上の付値とする。$d\colon K \times K \to \mathbb{R}$ を $d(x,y) := \nu(x-y)$ で定めると d は K 上の距離関数である。この距離に関する K の完備化を $\widehat{K}$ とすると、$\widehat{K}$ は自然に K の拡大体となり、ν を $\widehat{K}$ 上の付値 $\widehat{\nu}$ に拡張できる。さらに集合 $\{\widehat{x} \in \widehat{K} \mid \widehat{\nu}(\widehat{x}) \leq 1\}$ は $\widehat{K}$ の完備な部分環をなす。

K を体とし、K 上の 1 変数有理式のなす体 $K(t)$ 上の付値 ν を定めたい。まず、$\nu(0) := 0$ とし、多項式 $f(t) = a_d t^d + \cdots + a_{d+\ell} t^{d+\ell}$（$a_d \neq 0$）について $\nu(f) := e^{-d}$ と定める。その上で $h(t) = f(t)/g(t)$（$f(t), g(t) \in K[t]$、$g \neq 0$）について $\nu(h) := \nu(f)/\nu(g)$ と定めると、ν の値は $h(t)$ の表示 $f(t)/g(t)$ の選び方によらず一つにきちんと定まる。

命題 2.2. 上記の ν は $K(t)$ 上の付値である。

証明. ν が $\mathbb{R}_{\geq 0}$ への写像であることおよび定義の条件 1 は、上の議論と $e^{-d} > 0$ から示せる。条件 2 については、$f(t) = a_d t^d + \cdots + a_{d+\ell} t^{d+\ell}$（$a_d \neq 0$）、$g(t) = b_{d'} t^{d'} + \cdots + b_{d'+\ell'} t^{d'+\ell'}$（$b_{d'} \neq 0$）のとき $f(t)g(t) = a_d b_{d'} t^{d+d'} + \cdots$、$a_d b_{d'} \neq 0$、$e^{-(d+d')} = e^{-d} e^{-d'}$ であることを用いて示せる。条件 3 については、まず、$f(t) = a_d t^d + \cdots + a_{d+\ell} t^{d+\ell}$（$a_d \neq 0$）、$g(t) = b_{d'} t^{d'} + \cdots + b_{d'+\ell'} t^{d'+\ell'}$（$b_{d'} \neq 0$）のとき、$f(t) + g(t)$ の $\min\{d, d'\}$ 次未満の係数はすべて 0 であるため、$\nu(f+g) \leq e^{-\min\{d,d'\}} = \max\{e^{-d}, e^{-d'}\} = \max\{\nu(f), \nu(g)\}$ である。このことから

$$\nu\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) = \nu\left(\frac{f_1 g_2 + f_2 g_1}{g_1 g_2}\right) = \frac{\nu(f_1 g_2 + f_2 g_1)}{\nu(g_1)\nu(g_2)}$$

の右辺は

$$\begin{aligned} &\leq \frac{\max\{\nu(f_1 g_2), \nu(f_2 g_1)\}}{\nu(g_1)\nu(g_2)} = \max\left\{\frac{\nu(f_1 g_2)}{\nu(g_1)\nu(g_2)}, \frac{\nu(f_2 g_1)}{\nu(g_1)\nu(g_2)}\right\} \\ &= \max\left\{\frac{\nu(f_1)}{\nu(g_1)}, \frac{\nu(f_2)}{\nu(g_2)}\right\} = \max\{\nu(f_1/g_1), \nu(f_2/g_2)\} \end{aligned}$$

となり、条件 3 が成り立つ。よって主張が成り立つ。 □

この $K(t)$ 上の付値 ν に命題 2.1 を適用して、$\widehat{K(t)}$ 上の付値 $\widehat{\nu}$ を得る。

$$k[[t]] := \{F \in \widehat{K(t)} \mid \widehat{\nu}(F) \leq 1\}$$

は前述のように体 $\widehat{K(t)}$ の完備部分環であり、特に整域である。この $K[[t]]$ を（1 変数）**形式的冪級数環**と呼び、その元を**形式的冪級数**（formal power series）と呼ぶ。

この形式的冪級数が「多項式の極限」であることを示すために、以下の補題を用意する。

補題 2.2. X を距離空間、$(x_n)_n$ をその *Cauchy* 列とし、X の点列 $(y_m^{(n)})_m$（$n \geq 0$）は x_n に一様に収束している（つまり、どの $\varepsilon > 0$ についても、うまく N をとると、すべての n およびすべての $m \geq N$ について $d(y_m^{(n)}, x_n) \leq \varepsilon$ が成り立つ）とする。このとき $(y_n^{(n)})_n$ は $(x_n)_n$ と同値な *Cauchy* 列である。

証明. まず同値性について、$\varepsilon > 0$ とする。$(x_n)_n$ が Cauchy 列であることの定義を $\varepsilon/2 > 0$ について用いると、うまく N_1 をとることで、$m, n \geq N_1$ のとき常に $d(x_m, x_n) \leq \varepsilon/2$ が満たされる。また、$(y_m^{(n)})_m$ が x_n に一様に収束していることの定義を $\varepsilon/2 > 0$ について用いると、うまく N_2 をとることで、すべての n およびすべての $m \geq N_2$ について $d(y_m^{(n)}, x_n) \leq \varepsilon/2$ となり、特に $n = m$ とすることで $d(y_m^{(m)}, x_m) \leq \varepsilon/2$ となる。すると、$m, n \geq \max\{N_1, N_2\}$ のとき常に

$$d(y_m^{(m)}, x_n) \leq d(y_m^{(m)}, x_m) + d(x_m, x_n) \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

（最初の不等号で三角不等式を用いた）が成り立つ。これは $(y_n^{(n)})_n$ が $(x_n)_n$ と同値であることを意味する。$(y_n^{(n)})_n$ が Cauchy 列であることは、Cauchy 列と同値な列が常に Cauchy 列であることから導かれる。よって主張が成り立つ。 □

多項式環 $K[t]$ は $K(t)$ の部分環であり、したがって $\widehat{K(t)}$ の部分環でもあることを注意しておく。

定理 2.1. $K[t]$ は $K[[t]]$ の稠密な部分環である。

証明. $K[t] \subseteq K[[t]]$ であることは、$d \geq 0$ のとき $e^{-d} \leq 1$ であることと $K(t)$ 上の付値 ν の定義より導かれる。

$K[[t]]$ の任意の元をとり、それに対応する $K(t)$ の Cauchy 列 $(h_n)_n$ をとる。$K[[t]]$ の定義より $\lim_{n\to\infty} \nu(h_n) \leq 1$ である。$\nu\colon K(t) \to \mathbb{R}_{\geq 0}$ の像の中で 1 は孤立点であるから、充分大きな n について常に $\nu(h_n) \leq 1$ となる。列 $(h_n)_n$ と同値な列を選び直して、常に $\nu(h_n) \leq 1$ となるようにできる。すると、h_n を既約な有理式で表したとき、分母の定数項は 0 でない。よって特に、$h_n = f_n/(1 + tg_n)$、$f_n, g_n \in K[t]$、の形で表せる。

ここで、$F_{n,m} := f_n \sum_{k=0}^{m} (-tg_n)^k$ とすると、列 $(F_{n,m})_m$ は h_n に一様に収束することを示す。どの n,m についても

$$
\begin{aligned}
F_{n,m} - h_n &= \frac{f_n}{1+tg_n}\left((1+tg_n)\sum_{k=0}^{m}(-tg_n)^k - 1 \right) \\
&= h_n \cdot (1 + (-1)^m (tg_n)^{m+1} - 1) = (-1)^m h_n \cdot (tg_n)^{m+1}
\end{aligned}
$$

であることから

$$
\nu(F_{n,m} - h_n) = \nu(h_n)\nu(t)^{m+1}\nu(g_n)^{m+1} \leq 1 \cdot e^{-m-1} \cdot 1^{m+1} = e^{-m-1}
$$

となる。右辺は n によらない値であり 0 に収束するから、列 $(F_{n,m})_m$ が h_n に一様に収束することがわかる。

すると補題 2.2 より、最初にとった $K[[t]]$ の元は Cauchy 列 $(F_{n,n})_n$ の極限でもある。各 $F_{n,n}$ は $K[t]$ の元であるから、$K[t]$ は $K[[t]]$ の中で稠密である。よって主張が成り立つ。 □

$f_n = a_{n,0} + a_{n,1}t + \cdots + a_{n,d_n}t^{d_n} \in K[t]$ のとき、$(f_n)_n$ が Cauchy 列であることは、どの $k \geq 0$ についても、充分大きな範囲の n について $a_{n,k}$ が定数であることと同値である (ただし、$k > d_n$ のとき $a_{n,k} = 0$ とおいている)。この「定数」を $\widehat{a}_k \in K$ とおき、$(f_n)_n$ の極限として得られる $K[[t]]$ の元を $\sum_{n\geq 0} \widehat{a}_n t^n$ で表すことにすると、これまでに扱ってきたような見た目の「形式的冪級数」が得られる。なお、$(f_n)_n$ と $(g_n)_n$ が同値な Cauchy 列であれば、それらから得られる上記の $\widehat{a}_k$ たちは互いに一致するので、形式的冪級数の表示 $\sum_{n\geq 0} \widehat{a}_n t^n$ は一つに定まることを注意しておく。また、どの数列 $(a_n)_n$ に対しても、$f_n := \sum_{k=0}^{n} a_k t^k$ とおくと $(f_n)_n$ は Cauchy 列であり、その極限として得られる形式的冪級数 $\sum_{n\geq 0} a_n t^n$（つまり、$(a_n)_n$ の母関数）が常に存在することも注意しておく。このように形式的冪級数が多項式の極限として表されることから、多項式の加減乗算が形式的冪級数にも自然に拡張される。

以上のように形式的冪級数を定義すると、これまで形式的冪級数に対して行ってきた色々な形式的操作がきちんと正当化される。例えば、

- Euler の五角数定理の主張に現れた無限積 $\prod_{n\geq 1}(1-t^n)$ について、$f_n := \prod_{k=1}^{n}(1-t^k)$ とおくと $(f_n)_n$ は上記の距離に関して Cauchy 列をなすことがわかり（多項式に

$1-t^n$ を掛けても n 次未満の項の係数は変化しないことに注意せよ)、その極限として $\prod_{n\geq 1}(1-t^n)$ が形式的冪級数の意味できちんと定まる。

- $1-tf$ ($f \in K[t]$) という形の多項式について、$g_n := \sum_{k=0}^{n}(tf)^k$ とおくと、$(g_n)_n$ は Cauchy 列をなす。その極限を $g \in K[[t]]$ とおく。ここで各 n について $(1-tf)g_n = 1-(tf)^{n+1}$ であることから、$(1-tf)g_n$ は $n \geq \infty$ で 1 に収束する。したがって $K[[t]]$ において $(1-tf)\cdot g = 1$ が成り立つ。このことから、$1-tf$ は $K[[t]]$ において可逆であるから、その逆元として有理式 $1/(1-tf)$ が $K[[t]]$ の元としてきちんと定まり、また $1/(1-tf)$ は等比級数の和の公式の形をした元 $\sum_{n\geq 0}(tf)^n \in K[[t]]$ と確かに一致する。

なお、2 変数以上の場合についても、整域 $K[[t_1,\ldots,t_{n-1}]]$ の商体上で変数 t_n に関する有理式の体を考えて上記の構成を適用することで、再帰的に形式的冪級数環 $K[[t_1,\ldots,t_n]]$ を定義することができる。

ここからは、何らかのよい性質を持つ漸化式を満たす数列のクラスや、対応する形式的冪級数のクラスをいくつか考え、それらの相互関係などを調べる。より詳しい内容については [6] の 6 章などを参照されたい。以降では $K=\mathbb{C}$ の場合を考える。

定義 2.2. $\mathbb{C}[[x]]$ の元 $f(x)$ が **algebraic** であるとは、$f(x)$ が体 $\mathbb{C}(x)$ 上代数的な元である、すなわち、ある $d \geq 1$ と $P_0,\ldots,P_d \in \mathbb{C}[x]$ について

$$P_d(x)f(x)^d + \cdots + P_1(x)f(x) + P_0(x) = 0\,,\; P_d \neq 0$$

が成り立つことと定める。

以下の性質は体上代数的な元の一般論から導かれるため証明を割愛する。

命題 2.3. $\mathbb{C}[[x]]$ の *algebraic* な元全体の集合は $\mathbb{C}[[x]]$ の部分環であり $\mathbb{C}(x) \cap \mathbb{C}[[x]]$ を含む。

例えば、Fibonacci 数の母関数 $1/(1-x-x^2)$ や、Catalan 数の母関数 $(1-\sqrt{1-4x})/2x$ は algebraic である（ここで、上の議論で $F_{1/2}(-4x)$ と書いていた、$1-4x$ の平方根の一つを $\sqrt{1-4x}$ で表している）。

$\mathbb{C}[[x]]$ の元に対する形式的微分を $\left(\sum_{n\geq 0} a_n x^n\right)' := \sum_{n\geq 1} n a_n x^{n-1}$ で定める。これは通常の和と積の微分の公式 $(f+g)' = f'+g'$、$(fg)' = f'g+fg'$ を満たす。

定義 2.3. $\mathbb{C}[[x]]$ の元 $f(x)$ が **differentially finite**（または **D-finite**）であるとは、$\mathbb{C}(x)$ 上の線型空間として

$$\dim \mathsf{span}_{\mathbb{C}(x)} \left\{ \left(\frac{d}{dx} \right)^k f \mid k \geq 0 \right\} < \infty$$

であることと定める。

上の条件は、ある $d \geq 0$ と $P_0, \ldots, P_d \in \mathbb{C}[x]$ について

$$P_d(x) f^{(d)}(x) + \cdots + P_1(x) f'(x) + P_0(x) f(x) = 0 \, , \, P_d \neq 0 \tag{2}$$

が成り立つことと同値である。

定理 2.2. $f(x) = \displaystyle\sum_{n \geq 0} a_n x^n \in \mathbb{C}[[x]]$ について以下の条件は同値である。

1. f は *D-finite* である。
2. ある $d \geq 0$ と $P_0, \ldots, P_d, Q \in \mathbb{C}[x]$ について
$$P_d(x) f^{(d)}(x) + \cdots + P_1(x) f'(x) + P_0(x) f(x) = Q(x) \, , \, P_d \neq 0$$
が成り立つ。
3. ある $d \geq 0$ と $P_0, \ldots, P_d \in \mathbb{C}[x]$（$P_d \neq 0$）をとると、
$$P_0(n) a_n + P_1(n) a_{n+1} + \cdots + P_d(n) a_{n+d} = 0$$
がすべての $n \geq 0$ について成り立つ。

証明.【$1 \Rightarrow 3$】関係式 (2) から出発する。P_i たちの次数の最大値を D で表し、$0 \leq k \leq D$ について P_i における x^k の係数を $p_{i,k}$ で表す。すると、(2) 式の左辺における x^n の係数は

$$\begin{aligned} &\sum_{i=0}^{d} \sum_{j=0}^{D} p_{i,j} \cdot \text{【} f^{(i)} \text{ での } x^{n-j} \text{ の係数】} \\ &= \sum_{i=0}^{d} \sum_{j=0}^{D} p_{i,j} \cdot (n-j+i)(n-j+i-1) \cdots (n-j+1) a_{n-j+i} \end{aligned}$$

であり、これが常に 0 に等しい。ただし $k < 0$ のとき $a_k := 0$ とおいている。よって、$-D \leq k \leq d$ について

$$R_k(n) := \sum_{\substack{0 \leq i \leq d \, , \, 0 \leq j \leq D \\ i-j=k}} p_{i,j} \cdot (n-j+i)(n-j+i-1) \cdots (n-j+1)$$

とおくとこれは n についての多項式であり、すべての $n \geq 0$ について

$$\sum_{k=-D}^{d} R_k(n) a_{n+k} = 0$$

が成り立つ。ここで、$P_d \neq 0$ であるから、少なくとも一つの j_0 について $p_{d,j_0} \neq 0$ である。この j_0 について、$R_{d-j_0}(n)$ は

$$p_{d,j_0} \cdot (n - j_0 + d) \cdots (n - j_0 + 1) + \text{【} n \text{ の } d-1 \text{ 次以下の多項式】}$$

という形であるから、$R_{d-j_0} \neq 0$ である。したがって R_k たちのどれかは 0 でないので、ある $-D \leq d' \leq d$ をとると、すべての $n \geq 0$ について

$$\sum_{k=-D}^{d'} R_k(n) a_{n+k} = 0 \, , \; R_{d'} \neq 0$$

が成り立つ。$0 \leq k \leq d' + D$ について $\widehat{R}_k(n) := R_{k-D}(n)$ とおき、$m \geq 0$ について $n := m + D$ とおくことで、上の関係式は

$$\sum_{k=-D}^{d'} \widehat{R}_{k+D}(m+D) a_{m+k+D} = \sum_{k'=0}^{d'+D} \widehat{R}_{k'}(m+D) a_{m+k'} = 0$$

となる。$\widehat{R}_{k'}(m+D)$ たちは m の多項式であり $\widehat{R}_{d'+D}(m+D)$ は零多項式ではないので、これが条件 3 の関係式を与えている。

【$3 \Rightarrow 2$】$0 \leq \ell \leq d$ について、$(x+\ell)(x+\ell-1)\cdots(x+\ell-j+1)$（$j \geq 0$）が j 次多項式でありその最高次係数が 1 であることから、D 次以下のどの多項式も $j = 0, \ldots, D$ に関する上記の多項式たちの一次結合で表せる。これを踏まえて、条件 3 の関係式について、P_i たちの次数の最大値を D で表し、

$$P_\ell(x) = \sum_{j=0}^{D} b_{\ell,j} (x+\ell)(x+\ell-1)\cdots(x+\ell-j+1) \, , \; b_{\ell,j} \in \mathbb{C}$$

と表しておく。また、

$$Q(x) := \sum_{\ell=0}^{d} \sum_{j=0}^{D} b_{\ell,j} x^{j+d-\ell} f^{(j)}(x)$$

とする。ここで、$m \geq d+D$ のとき、$Q(x)$ における x^m の係数は

$$\begin{aligned}
&\sum_{\ell=0}^{d}\sum_{j=0}^{D} b_{\ell,j}\cdot【f^{(j)} \text{ における } x^{m-j-d+\ell} \text{ の係数}】\\
&=\sum_{\ell=0}^{d}\sum_{j=0}^{D} b_{\ell,j}\cdot(m-d+\ell)(m-d+\ell-1)\cdots(m-d+\ell-j+1)a_{m-d+\ell}\\
&=\sum_{\ell=0}^{d} P_\ell(m-d)a_{m-d+\ell}
\end{aligned}$$

となる。この右辺は条件 3 の関係式の左辺で $n=m-d$ としたものに等しいので、その値は 0 である。よって $Q(x)$ は $d+D-1$ 次以下の多項式である。さらに、$P_d \neq 0$ であることから、ある j_0 について $b_{d,j_0} \neq 0$ である。すると、$Q(x)$ の定義式の右辺における $f^{(j_0)}(x)$ の係数は

$$b_{d,j_0}x^{j_0} + 【x \text{ の } j_0+1 \text{ 次以上の項たち}】$$

という形であることから零多項式ではない。よって、$Q(x) \in \mathbb{C}[x]$ の定義式を整理することで、条件 2 の形の関係式が得られる。

【$2 \Rightarrow 1$】条件 2 の関係式の両辺を $\deg Q+1$ 回微分すると、右辺は 0 となり、左辺はある多項式 $R_0,\dots,R_{d+\deg Q}$ について $R_{d+\deg Q}(x)f^{(d+\deg Q)}(x)+\cdots+R_1(x)f'(x)+R_0(x)f(x)$ という形になる。さらに $R_{d+\deg Q}(x)=P_d(x)\neq 0$ であることから、(2) 式の形の関係式が得られる。以上で主張が示された。 □

この定理により、D-finite というクラスは、係数が n の多項式である一次結合の形の漸化式をもつ数列の母関数のクラスであると捉えることができる。

algebraic な形式的冪級数の場合と同様に、以下の性質が成り立つ。

命題 2.4. $\mathbb{C}[[x]]$ の *D-finite* な元全体の集合は $\mathbb{C}[[x]]$ の部分環であり $\mathbb{C}(x)\cap\mathbb{C}[[x]]$ を含む。

証明. $\mathbb{C}(x)$ を含む、という主張については、定理 2.2 の条件 2 で $d=0$ としたものを考えればよい。残りの主張について、$f,g\in\mathbb{C}[[x]]$ が D-finite であるとする。定義より、有限次元 $\mathbb{C}(x)$-線型空間 V_f,V_g で、$f^{(n)}$ たちはすべて V_f に属し、$g^{(n)}$ たちはすべて V_g に属し、かつ V_f と V_g が $\mathbb{C}[[x]]$ の有限部分集合で生成されるものが存在する。すると、$n\geq 0$ のとき $(f\pm g)^{(n)}\in V_f+V_g$ となり、V_f+V_g も有限次元であるから、定義より $f\pm g$ も D-finite である。また、$\{\alpha_1,\dots,\alpha_{d_f}\}\subseteq\mathbb{C}[[x]]$ を V_f の有限な生成系、$\{\beta_1,\dots,\beta_{d_g}\}\subseteq\mathbb{C}[[x]]$ を V_g の有限な生成系とすると、元 $\alpha_i\beta_j$（$1\leq i\leq d_f$、$1\leq j\leq d_g$）たちで生成される $\mathbb{C}(x)$-線型空間 W も有限次元であり、$n,m\geq 0$ のとき常に $f^{(n)}g^{(m)}\in W$ が成り立つ。すると

$n \geq 0$ について

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)} \in W$$

となるので、定義より fg も D-finite である。以上より主張が成り立つ。 □

上記二つのクラス（algebraic と D-finite）について、以下の関係が成り立つ。

定理 2.3. $f \in \mathbb{C}[[x]]$ が *algebraic* ならば *D-finite* である。

証明. f が algebraic であることから、$\mathbb{C}(x)$ に f を添加した体 $\mathbb{C}(x, f)$ は $\mathbb{C}(x)$ 上有限次元であることを注意しておく。f が algebraic であることから導かれる関係式

$$P_d f^d + \cdots + P_1 f + P_0 = 0\,,\ P_i \in \mathbb{C}[x]\,,\ P_d \neq 0$$

のうち、d が最小のものをとる。両辺を微分すると

$$\sum_{i=0}^{d} P_i' f^i + \left(\sum_{i=1}^{d} P_i \cdot i f^{i-1} \right) \cdot f' = 0$$

となる。ここで d の最小性より、f' の係数部分は 0 でないので、f' について整理した式より $f' \in \mathbb{C}(x, f)$ が成り立つ。すると、もし $f^{(n)} \in \mathbb{C}(x, f)$ であれば、商の微分の公式により $f^{(n+1)}$ は x と f と f' に関する有理式となり、$f' \in \mathbb{C}(x, f)$ であることからこれは $\mathbb{C}(x, f)$ の元となる。これを再帰的に用いると、すべての $n \geq 0$ について $f^{(n)}$ は有限次元 $\mathbb{C}(x)$-線型空間 $\mathbb{C}(x, f)$ の元となる。よって定義より f は D-finite であり、主張が成り立つ。 □

定理 2.3 より、例えば Catalan 数の母関数は D-finite であることがわかる（が、これは Catalan 数の元々の定義からは明らかなことではないであろう）。なお、定理 2.3 の逆は成立しないことが知られている（[6] の 6 章の Exercise 6.1 を参照）。

次に、二つの数列の母関数がともに D-finite であれば、それらの数列を項ごとに掛け算してできる数列の母関数もまた D-finite である、ということを示す。そのために準備を行う。

定義 2.4. $\mathbb{C}$-値の数列の集合上の同値関係 $\sim$ を、

$$(a_n)_n \sim (b_n)_n \overset{\text{def}}{\Leftrightarrow} \text{ある } N \text{ をうまくとると、すべての } m \geq N \text{ について } a_m = b_m$$

で定める。その同値類 $[a_n]_n$ を、$(a_n)_n$ を含む**芽**（germ）と呼ぶ。

数列の項ごとの和や積は、芽に対する和や積の演算を自然に導くことを注意しておく。なお、「母関数が D-finite である」という性質は上記の同値関係によって保たれる。すなわち以下が成り立つ。

命題 2.5. 数列 $(a_n)_n$ と $(b_n)_n$ が上の意味で同値であるとし、$f(x)$ と $g(x)$ をそれぞれ $(a_n)_n$ と $(b_n)_n$ の母関数とする。このとき、f が *D-finite* であれば g も *D-finite* である。

証明. 前提より、すべての $f^{(n)}$ たちはある有限次元 $\mathbb{C}(x)$-線型空間 V に属する。また $(a_n)_n \sim (b_n)_n$ より、ある多項式 $P(x)$ について $g = f + P$ となる。するとどの $n \geq 0$ についても $g^{(n)} = f^{(n)} + P^{(n)} \in V + \mathbb{C}(x)$ が成り立ち、$V + \mathbb{C}(x)$ も $\mathbb{C}(x)$ 上有限次元であるから、g は D-finite である。よって主張が成り立つ。 □

補題 2.3. $f(x)$ を数列 $(a_n)_n$ の母関数とすると、以下は同値である。

1. f は *D-finite* である。
2. $\{[a_{n+i}]_n \mid i \geq 0\}$ が生成する $\mathbb{C}(n)$ 上の線型空間は有限次元である。

証明.【$1 \Rightarrow 2$】定理 2.2 の条件 3 における関係式を P_d で割って整理すると、

$$a_{n+d} = Q_0(n)a_n + Q_1(n)a_{n+1} + \cdots + Q_{d-1}(n)a_{n+d-1}\,,\, Q_i \in \mathbb{C}(x)$$

という形の関係式が得られる。$k \geq 0$ について、上記の n に $n + k$ を代入することで、どの $n \geq 0$ についても

$$a_{n+d+k} = Q_0(n+k)a_{n+k} + Q_1(n+k)a_{n+k+1} + \cdots + Q_{d-1}(n+k)a_{n+k+d-1}$$

が成り立つ。したがって、芽についての関係として、$m \geq d$ のとき常に $[a_{n+m}]_n$ は $[a_n]_n, [a_{n+1}]_n, \ldots, [a_{n+m-1}]_n$ たちの $\mathbb{C}(n)$ 上の一次結合で表せる。これを再帰的に用いると、どの $[a_{n+m}]_n$ も $[a_n]_n, [a_{n+1}]_n, \ldots, [a_{n+d-1}]_n$ が生成する $\mathbb{C}(x)$ 上の有限次元線型空間に属することがわかる。よって条件 2 が成り立つ。

【$2 \Rightarrow 1$】前提より、ある $d \geq 0$ と $P_0, \ldots, P_d \in \mathbb{C}[x]$（$P_d \neq 0$）について、芽の関係式として

$$P_0(n)[a_n]_n + \cdots + P_d(n)[a_{n+d}]_n = [0]$$

が成り立つ。したがって、ある N をうまくとると、$n \geq N$ のとき常に

$$P_0(n)a_n + \cdots + P_d(n)a_{n+d} = 0$$

が成り立つ。すると、$R(x) := x(x-1)\cdots(x-N+1)$ について、$n \geq N$ のとき

$$P_0(n)R(n)a_n + \cdots + P_d(n)R(n)a_{n+d} = 0$$

が成り立つ。また、$0 \leq n \leq N-1$ のときも、$R(n) = 0$ であることからやはり上の関係式が成り立つ。$P_dR \neq 0$ であるから、$(a_n)_n$ について定理 2.2 の条件 3 が成り立っている。よって f は D-finite であり、主張が成り立つ。 □

定理 2.4. $f(x)$ と $g(x)$ をそれぞれ数列 $(a_n)_n$ と $(b_n)_n$ の母関数とし、数列 $(a_n b_n)_n$ の母関数を $f * g$ で表す。このとき、f と g がともに *D-finite* であれば、$f * g$ も *D-finite* である。

証明. 芽 $[a_{n+i}]_n$（$i \geq 0$）たちが生成する $\mathbb{C}(x)$-線型空間を V_a、芽 $[b_{n+i}]_n$（$i \geq 0$）たちが生成する $\mathbb{C}(x)$-線型空間を V_b で表す。補題 2.3 よりこれらはともに有限次元である。$(\alpha_1, \ldots, \alpha_{d_a})$ を V_a の基底、$(\beta_1, \ldots, \beta_{d_b})$ を V_b の基底とすると、元 $\alpha_i \beta_j$（$1 \leq i \leq d_a$、$1 \leq j \leq d_b$）たちで生成される $\mathbb{C}(x)$-線型空間 W も有限次元であり、$i \geq 0$ のとき常に $[a_{n+i} b_{n+i}]_n = [a_{n+i}]_n \cdot [b_{n+i}]_n \in W$ が成り立つ。よって補題 2.3 より $f * g$ も D-finite である。 □

この節の最後に、多次元数列の「対角部分」として得られる数列の母関数に関する下記の事実を紹介する。証明はここでは割愛する。主張の前半部については [6] の 6 章の Exercise 6.61 を、後半部については [6] の 6 章の Theorem 6.3.3 を参照されたい。

定理 2.5. n 変数の形式的冪級数

$$f(x_1, \ldots, x_n) = \sum_{k_1, \ldots, k_n \geq 0} a_{k_1, \ldots, k_n} x_1^{k_1} \cdots x_n^{k_n} \in \mathbb{C}[[x_1, \ldots, x_n]]$$

について、$\mathrm{diag}(f)(x) := \sum_{k \geq 0} a_{k, \ldots, k} x^k$ と定める。この f が $\mathbb{C}(x_1, \ldots, x_n)$ の元でもあるとき、$\mathrm{diag}(f)(x)$ は *D-finite* である。さらに、上の状況で $n = 2$ の場合には、$\mathrm{diag}(f)(x)$ は *algebraic* である。

演習問題

■問題 1.　前述した Fibonacci 数をここでは $(F_n)_n$ で表し、また、Lucas 数 $(L_n)_n$ を $L_0 = 2$、$L_1 = 1$、および漸化式 $L_{n+2} = L_n + L_{n+1}$ で定める。このとき、関係式 $L_n = 2F_n - F_{n-1}$（$n \geq 1$）が成り立つことを母関数を用いて証明せよ。

（ヒント：Fibonacci 数と Lucas 数の母関数について、各項の係数を決定する必要はなく、有理式としての表示が得られれば本問には充分である。）

■問題 2.　整数 $n \geq 1$ について、分割 (n, n) に対応する Young 図形を Y とする。Y の箱の各々に 1 から $2n$ までの数字を一つずつ、異なる箱の中身が互いに異なるように入れることを考える。このような配置のうち、以下の条件を満たすものを形が Y の**標準 Young 盤**（standard Young tableau）と呼ぶ。

- 同じ行に入っている数字は、右にいくほど大きくなる。

- 同じ列に入っている数字は、下にいくほど大きくなる。

このとき、形が Y の標準 Young 盤の総数が C_n に等しいことを、$(0,0)$ から $(2n,0)$ までの Dyck path 全体の集合と形が Y の標準 Young 盤全体の集合の間に全単射を構成することで証明せよ。

■問題 3.　整数 $n \geq 0$ について、$(1,0)$、$(0,1)$、$(1,1)$ という 3 種類のベクトルたちの和で (n,n) を作る方法の総数（和の順序も込みで考える）を a_n とするとき、その母関数 $\sum_{n \geq 0} a_n x^n$ が algebraic であることを示せ。

（ヒント：定理 2.5 の後半部分を用いる。母関数が有理式となる 2 次元数列 $(b_{n,m})_{n,m}$ で $a_n = b_{n,n}$ を満たすものを適切に構成せよ。）

■問題 4.　Catalan 数 C_n について $D_n := C_n^2$ とするとき、数列 $(D_n)_n$ について定理 2.2 の条件 3 のような関係式を構成せよ。

（コメント：前述のように Catalan 数の母関数は D-finite であるから、定理 2.4 により $(D_n)_n$ の母関数も D-finite であり、したがって上記のような関係式が存在することは保証されている。）

3 包除原理と Möbius 反転公式

本節の内容は Stanley の著書 [5] の 3 章を参考にしている。

n 次対称群の元 $\sigma \in S_n$ が**攪乱順列**（derangement）であるとは、固定点をもたない、つまりどの $a \in \{1, \ldots, n\}$ についても $\sigma(a) \neq a$ であることと定める。n 文字の攪乱順列の集合をここでは D_n と書くことにする。例えば、$n = 3$ として、D_3 の要素数を調べてみる。S_3 の要素数は全部で

$$3!$$

であるが、この中には 1 を固定する元、2 を固定する元、3 を固定する元が余分に含まれている。これらはそれぞれ（2 個の元に対する置換の総数なので）2! 個ずつあるので、調整のためにそれらを引き算すると

$$3! - 3 \cdot 2!$$

となる。しかし、今度は 1 と 2 をともに固定する元を考えたとき、上の式ではそれらが $1 - 2 = -1$ 回数えられてしまっている。これを打ち消すために、そうした元（1 個の元に対する置換となる）の個数 1! を加える。1 と 3 をともに固定する元、2 と 3 をともに固定する元についても同様にすると、

$$3! - 3 \cdot 2! + 3 \cdot 1!$$

となる。しかしそうすると、1 と 2 と 3 をすべて固定する元（0 個の元に対する置換）は $1 - 3 + 3 = 1$ 回数えられてしまっているので、それを打ち消すためにその個数 0! を引く必要がある。結果として、

$$|D_3| = 3! - 3 \cdot 2! + 3 \cdot 1! - 0! = 6 - 3 \cdot 2 + 3 \cdot 1 - 1 = 2$$

が得られる（実際、$D_3 = \{(123), (132)\}$ である）。

上の議論を一般化すると、同様に足し引きの調整をうまく行うことで

$$\begin{aligned} |D_n| &= n! - \binom{n}{1} \cdot (n-1)! + \binom{n}{2} \cdot (n-2)! - \cdots + (-1)^n \cdot 0! \\ &= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx \frac{n!}{e} \end{aligned}$$

が得られる。以降では、この「足し引きの調整をうまく行うことで」の部分をきちんと定式化して取り扱うことができる**包除原理**（Principle of Inclusion-Exclusion）という理論（「包含と排除の原理」とも呼ばれる）について説明する。

包除原理は、一般には半順序集合における Möbius 関数という対象を用いて記述される。

定義 3.1. P を集合、$\preceq$ を P 上の二項関係とする。以下の条件が成り立つとき、$(P, \preceq)$ は（あるいは単に、P は）**半順序集合**（partially ordered set, poset）であるという。また、このような $\preceq$ を**半順序**（partial order）という。

1. $x \in P$ について、$x \preceq x$（反射律、reflexivity）
2. $x, y \in P$ について、$x \preceq y$ かつ $y \preceq x$ であれば $x = y$（反対称律、antisymmetry）
3. $x, y, z \in P$ について、$x \preceq y$ かつ $y \preceq z$ であれば $x \preceq z$（推移律、transitivity）

また、さらに

- どの $x, y \in P$ についても、$x \preceq y$ または $y \preceq x$

が成り立つとき、P は**全順序集合**（totally ordered set）であるといい、また $\preceq$ を**全順序**（total order）という。

以下では、順序を表すのに $\preceq$ という記号を用いているときは、「$x \preceq y$ かつ $x \neq y$」という関係を $x \prec y$ で表すこととする。

例 3.1. 半順序集合 P の元 x, y について、$x \prec y$ でありかつ、$x \prec z \prec y$ を満たす z が存在しないとき、y は x を**カバーする**、x は y に**カバーされる**という。P の元を点として、y が x をカバーしているとき x と y を線で結び、y が x より上側にくるように配置してできる図のことを P の **Hasse 図**（Hasse diagram）という。例えば、非負整数の集合 $\mathbb{Z}_{\geq 0}$ 上で通常の大小関係を考えると全順序集合となり、その Hasse 図（の一部）は図 4 の左側のようになる。（推移律より、1 本の線で直接結ばれていない場合にも、ある元から上向きにいくつかの線を辿った先の元との間には順序関係が存在することを注意しておく。）また、集合 $\{1, 2, 3\}$ の部分集合の全体に包含関係 $\subseteq$ で順序を定めてできる半順序集合の Hasse 図は図 4 の中央のようになり、すべての Young 図形の集合に（図形を左上に揃えて置いた際の）包含関係で順序を定めてできる半順序集合の Hasse 図（の一部）は図 4 の右側のようになる。

定義 3.2. $(P, \preceq_P)$ と $(Q, \preceq_Q)$ を半順序集合とし、$f \colon P \to Q$ とする。$x, y \in P$、$x \preceq_P y$ のとき常に $f(x) \preceq_Q f(y)$ であるならば、f は**順序保存**（order-preserving）であるという。また、f が全単射であり f と f^{-1} がともに順序保存であるとき、f を**同型写像**（isomorphism）という。このような同型写像が存在するとき P と Q は**同型**（isomorphic）であるといい、$P \simeq Q$ で表す。

定義 3.3. P を半順序集合とする。$x, y \in P$、$x \preceq y$ のとき、

$$[x, y]_P := \{z \in P \mid x \preceq z \preceq y\}$$

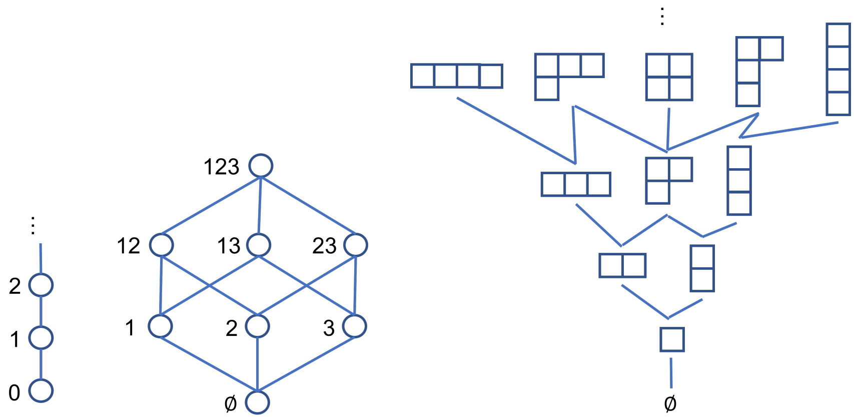


図 4　半順序集合の Hasse 図の例

と定める。この記号のもと、$x, y \in P$ が $x \preceq y$ であれば常に $[x, y]_P$ が有限集合であるとき、P は**局所有限**（locally finite）であるという。

局所有限な半順序集合 P について、

$$I(P) := \{(x, y) \in P^2 \mid x \preceq y\}$$

と定めて、集合 $\mathbb{C}^{I(P)} := \{f\colon I(P) \to \mathbb{C}\}$ 上の和と積を以下のように定める：$f, g \in \mathbb{C}^{I(P)}$ と $(x, y) \in I(P)$ について、

$$(f + g)(x, y) := f(x, y) + g(x, y)\,,\ (fg)(x, y) := \sum_{\substack{z\,;\\ x \preceq z \preceq y}} f(x, z)g(z, y)\ .$$

また、$\mathbb{C}^{I(P)}$ 上のスカラー倍を、$f \in \mathbb{C}^{I(P)}$、$\alpha \in \mathbb{C}$ と $(x, y) \in I(P)$ について

$$(\alpha \cdot f)(x, y) := \alpha f(x, y)$$

で定める。一方、集合 $\mathbb{C}^P := \{f\colon P \to \mathbb{C}\}$ について和と積とスカラー倍を $(f + g)(x) := f(x) + g(x)$、$(fg)(x) := f(x)g(x)$ および $(\alpha \cdot f)(x) := \alpha f(x)$ で定めると、$\mathbb{C}^P$ が $\mathbb{C}$-代数となることが直ちに確かめられる。

命題 3.1. 上の定義のもと、$\mathbb{C}^{I(P)}$ は $\mathbb{C}$-代数となり、$\delta\colon I(P) \to \mathbb{C}$ を

$$\delta(x, y) = \begin{cases} 1 & (x = y\text{ のとき}) \\ 0 & (\text{それ以外}) \end{cases}$$

で定めると、δ は $\mathbb{C}^{I(P)}$ の乗法単位元となる。さらに、$f \in \mathbb{C}^P$ に対して $\widehat{f} \in \mathbb{C}^{I(P)}$ を $\widehat{f}(x, y) := f(x)\delta(x, y)$ で定めると、対応 $f \mapsto \widehat{f}$ は $\mathbb{C}^P$ から $\mathbb{C}^{I(P)}$ への $\mathbb{C}$-代数の準同型である。

証明. $\mathbb{C}^{I(P)}$ が $\mathbb{C}$-線型空間であることは定義から明らかである。

積の結合法則は、

$$\begin{aligned}((fg)h)(x,y) &= \sum_{x\preceq z\preceq y}(fg)(x,z)\cdot h(z,y)\\ &= \sum_{x\preceq w\preceq z\preceq y}f(x,w)g(w,z)\cdot h(z,y)\\ &= \sum_{x\preceq w\preceq y}f(x,w)\cdot(gh)(w,y)=(f(gh))(x,y)\end{aligned}$$

より成り立つ。

分配法則の片側は、

$$\begin{aligned}((f+g)h)(x,y) &= \sum_{x\preceq z\preceq y}(f+g)(x,z)\cdot h(z,y)\\ &= \sum_{x\preceq z\preceq y}(f(x,z)+g(x,z))\cdot h(z,y)\\ &= \sum_{x\preceq z\preceq y}(f(x,z)h(z,y)+g(x,z)h(z,y))\\ &= (fh)(x,y)+(gh)(x,y)=(fh+gh)(x,y)\end{aligned}$$

より成り立つ。逆側についても同様である。

$f,g\in\mathbb{C}^{I(P)}$、$\alpha\in\mathbb{C}$、$(x,y)\in I(P)$ について

$$\begin{aligned}(\alpha\cdot(fg))(x,y) &= \alpha(fg)(x,y)\\ &= \alpha\sum_{x\preceq z\preceq y}f(x,z)g(x,y)\\ &= \sum_{x\preceq z\preceq y}(\alpha f(x,z))g(x,y)\\ &= \sum_{x\preceq z\preceq y}(\alpha\cdot f)(x,z)g(x,y)=((\alpha\cdot f)g)(x,y)\end{aligned}$$

より $\alpha\cdot(fg)=(\alpha\cdot f)g$ であり、同様に $\alpha\cdot(fg)=f(\alpha\cdot g)$ である。以上より $\mathbb{C}^{I(P)}$ は $\mathbb{C}$-代数である。

$$(\delta f)(x,y)=\sum_{x\preceq z\preceq y}\delta(x,z)f(z,y)=1\cdot f(x,y)=f(x,y)$$

より $\delta f=f$ であり、同様に $f\delta=f$ となるので、δ は $\mathbb{C}^{I(P)}$ の乗法単位元である。

$f, g \in \mathbb{C}^P$、$\alpha \in \mathbb{C}$、$(x, y) \in I(P)$ について、

$$\begin{aligned}(\widehat{f} + \widehat{g})(x, y) &= \widehat{f}(x, y) + \widehat{g}(x, y) \\ &= f(x)\delta(x, y) + g(x)\delta(x, y) \\ &= (f(x) + g(x))\delta(x, y) \\ &= (f + g)(x)\delta(x, y) = \widehat{f + g}(x, y) \ ,\end{aligned}$$

$$\begin{aligned}(\widehat{f}\widehat{g})(x, y) &= \sum_{x \preceq z \preceq y} \widehat{f}(x, z)\widehat{g}(z, y) \\ &= \sum_{x \preceq z \preceq y} f(x)\delta(x, z)g(z)\delta(z, y) \\ &= f(x)g(x)\delta(x, y) \\ &= (fg)(x)\delta(x, y) = \widehat{fg}(x, y) \ ,\end{aligned}$$

$$\begin{aligned}(\alpha \cdot \widehat{f})(x, y) &= \alpha\widehat{f}(x, y) \\ &= \alpha f(x)\delta(x, y) \\ &= (\alpha \cdot f)(x)\delta(x, y) = \widehat{\alpha \cdot f}(x, y)\end{aligned}$$

となる。よって対応 $f \mapsto \widehat{f}$ は $\mathbb{C}$-代数の準同型である。以上より主張が成り立つ。 □

以降では、$x \in P$ について $\wedge^x := \{w \in P \mid w \preceq x\}$ が常に有限集合であると仮定する。$f \in \mathbb{C}^{I(P)}$ と $\varphi \in \mathbb{C}^P$ について、$\varphi * f \in \mathbb{C}^P$ を

$$(\varphi * f)(x) := \sum_{w \preceq x} \varphi(w) f(w, x)$$

で定める。

補題 3.1. $f, g \in \mathbb{C}^{I(P)}$ と $\varphi \in \mathbb{C}^P$ について、$\varphi * (fg) = (\varphi * f) * g$ および $\varphi * \delta = \varphi$ が成り立つ。

証明. $x \in P$ について、

$$\begin{aligned}(\varphi * (fg))(x) &= \sum_{w \preceq x} \varphi(w)(fg)(w, x) \\ &= \sum_{w \preceq z \preceq x} \varphi(w) f(w, z) g(z, x) \\ &= \sum_{z \preceq x} (\varphi * f)(z) g(z, x) = ((\varphi * f) * g)(x) \ ,\end{aligned}$$

$$(\varphi * \delta)(x) = \sum_{w \preceq x} \varphi(w)\delta(w, x) = \varphi(x)\delta(x, x) = \varphi(x)$$

が成り立つ。よって主張が成り立つ。 □

定義 3.4. P を局所有限な半順序集合とする。P 上の **Möbius 関数** $\mu = \mu_P \in \mathbb{C}^{I(P)}$ を、$x \in P$ のとき $\mu(x,x) := 1$、$x \prec y$ のとき $\mu(x,y) := -\sum_{\substack{z\,;\\ x \prec z \preceq y}} \mu(z,y)$ で再帰的に定義する。

以降では P を局所有限な半順序集合とする。

補題 3.2. すべての $(x,y) \in I(P)$ について $\mathbb{1}(x,y) = 1$ となる $\mathbb{1} \in \mathbb{C}^{I(P)}$ について、$\mathbb{1}\mu = \delta$ が成り立つ。

証明. $x \in P$ について

$$(\mathbb{1}\mu)(x,x) = \mathbb{1}(x,x)\mu(x,x) = 1 = \delta(x,x)$$

が成り立ち、また $x \prec y$ のとき

$$\begin{aligned}(\mathbb{1}\mu)(x,y) &= \sum_{x \preceq z \preceq y} \mathbb{1}(x,z)\mu(z,y)\\ &= \sum_{x \preceq z \preceq y} \mu(z,y)\\ &= \mu(x,y) + \sum_{x \prec z \preceq y} \mu(z,y) = 0 = \delta(x,y)\end{aligned}$$

が成り立つ。以上より主張が成り立つ。 □

補題 3.3. $\mu\mathbb{1} = \delta$ が成り立つ。

証明. 主張の等式は、各 $(x,y) \in I(P)$ について $\sum_{x \preceq z \preceq y} \mu(x,z) = \delta(x,y)$ であることと等価である。後者の性質を、P の Hasse 図で x から y まで上向きに辿る最長経路が含む辺の数についての数学的帰納法で示す。$x = y$ のときは $\mu(x,x) = 1 = \delta(x,x)$ より主張が成り立つ。以降では $x \prec y$ とする。μ の再帰的な定義より

$$\sum_{x \preceq z \preceq y} \mu(x,z) = 1 + \sum_{x \prec z \preceq y} \mu(x,z) = 1 - \sum_{x \prec z \preceq y} \sum_{x \prec w \preceq z} \mu(w,z) = 1 - \sum_{x \prec w \preceq y} \sum_{w \preceq z \preceq y} \mu(w,z)$$

である。帰納法の仮定より、各 $w \in [x,y]_P \setminus \{x\}$ について $\sum_{w \preceq z \preceq y} \mu(w,z) = \delta(w,y)$ であるから、

$$\sum_{x \preceq z \preceq y} \mu(x,z) = 1 - \sum_{x \prec w \preceq y} \delta(w,y) = 1 - \delta(y,y) = 1 - 1 = 0 = \delta(x,y)$$

となる。以上より主張が成り立つ。 □

定理 3.1. $f, g \in \mathbb{C}^P$ について、$g = f * \mathbb{1}$ と $f = g * \mu$ は互いに同値である。この性質を ***Möbius* の反転公式**（*Möbius inversion formula*）と呼ぶ。

証明. 補題 3.2 と補題 3.3 より μ は $\mathbb{1}$ の（両側）逆元であるから、$g = f * \mathbb{1}$ のとき

$$g * \mu = (f * \mathbb{1}) * \mu = f * (\mathbb{1}\mu) = f * \delta = f$$

であり、また $f = g * \mu$ のとき

$$f * \mathbb{1} = (g * \mu) * \mathbb{1} = g * (\mu\mathbb{1}) = g * \delta = g$$

である。よって主張が成り立つ。 □

Möbius の反転公式の適用例として、冒頭の撹乱順列の例を再考する。$T \subseteq \{1, \dots, n\}$ について

$$\mathcal{F}(T) := \{\sigma \in S_n \mid \sigma(a) \neq a \Leftrightarrow a \in T\}, \, f(T) := |\mathcal{F}(T)| \ ,$$

$$\mathcal{G}(T) := \{\sigma \in S_n \mid \sigma(a) \neq a \Rightarrow a \in T\}, \, g(T) := |\mathcal{G}(T)|$$

と定める。定義より $D_n = \mathcal{F}(\{1, \dots, n\})$ である。ここで $\mathcal{G}(T)$ は $U \subseteq T$ に対する $\mathcal{F}(U)$ たちの非交和であるので、$g(T) = \sum_{U \subseteq T} f(U)$ である。半順序集合 P として $\{1, \dots, n\}$ の部分集合全体に包含関係で順序を定めたものを考えると、上の関係式は

$$g(T) = \sum_{U \subseteq T} f(U) = \sum_{U \subseteq T} f(U)\mathbb{1}(U, T) = (f * \mathbb{1})(T)$$

したがって $g = f * \mathbb{1}$ を意味する。すると Möbius の反転公式より $f = g * \mu_P$ となり、特に

$$|D_n| = f(\{1, \dots, n\}) = \sum_{U \subseteq \{1, \dots, n\}} g(U)\mu_P(U, \{1, \dots, n\})$$

が成り立つ。さらにこの場合の Möbius 関数は以下のように決定できる。

命題 3.2. 上の P について、$\mu_P(I, J) = (-1)^{|J|-|I|}$ が成り立つ。

証明. $|J| - |I|$ についての数学的帰納法を用いる。$I = J$ のときは定義より明らかである。$I \subsetneq J$ のとき、

$$\mu_P(I, J) = -\sum_{I \subsetneq K \subseteq J} \mu_P(K, J) = -\sum_{I \subsetneq K \subseteq J} (-1)^{|J|-|K|}$$

（ここで帰納法の仮定を用いた）

$$
\begin{aligned}
&= -\sum_{k=1}^{|J|-|I|} \binom{|J|-|I|}{k} (-1)^{|J|-(|I|+k)} \\
&= (-1)^{|J|-|I|} - \sum_{k=0}^{|J|-|I|} \binom{|J|-|I|}{k} (-1)^{|J|-|I|-k} \\
&= (-1)^{|J|-|I|} - (1-1)^{|J|-|I|} = (-1)^{|J|-|I|}
\end{aligned}
$$

となりやはり主張が成り立つ。以上より主張が成り立つ。 □

この結果を上の関係式に代入することで、

$$
|D_n| = \sum_{U \subseteq \{1,\dots,n\}} (-1)^{n-|U|} g(U)
$$

となる。さらに、$\mathcal{G}(U)$ は U に属さない点をすべて固定する元の集合であるから、$g(U) = |U|!$ が成り立つ。以上より

$$
\begin{aligned}
|D_n| = \sum_{U \subseteq \{1,\dots,n\}} (-1)^{n-|U|} |U|! &= \sum_{k \geq 0} (-1)^{n-k} \binom{n}{k} k! \\
&= \sum_{k \geq 0} (-1)^{n-k} \frac{n!}{(n-k)!} = \sum_{k \geq 0} (-1)^k \frac{n!}{k!}
\end{aligned}
$$

となり、この節の冒頭に述べた事実が導かれる。

別の例として、P を正整数全体の集合とし、$a, b \in P$ について $a \mid b$（つまり a が b の約数）であるとき $a \preceq b$ として順序関係を定めると、これは半順序集合となる。この場合の Möbius 関数は以下のように決定できる。

命題 3.3. 上の P について、$b/a = p_1^{e_1} \cdots p_\ell^{e_\ell}$（$p_i$ たちは異なる素数、$e_i > 0$）と素因数分解する。このとき、e_i たちがすべて 1 であれば $\mu_P(a,b) = (-1)^\ell$ であり、それ以外のとき $\mu_P(a,b) = 0$ である。

証明. $e_1 + \cdots + e_\ell$ についての数学的帰納法を用いる。e_i たちがすべて 1 であるとき、集合 $\{1, \dots, \ell\}$ の部分集合全体 $\mathcal{P}(\{1, \dots, \ell\})$ から $[a,b]_P$ への写像 f を $f(\{i_1, \dots, i_k\}) := a p_{i_1} \cdots p_{i_k}$ で定めると f は同型写像である。定義より $\mu_P(a,b)$ の値は $[a,b]_P$ の順序構造のみから定まるため、上で決定した $\mathcal{P}(\{1, \dots, \ell\})$ の Möbius 関数の形より $\mu_P(a,b) = (-1)^\ell$ が成り立つ。

一方、e_i たちの少なくとも一つが 2 以上であるとき、定義より

$$
\mu_P(a,b) = -\sum_{\substack{c \neq a\,; \\ a|c\,,\, c|b}} \mu_P(c,b)
$$

である。ここで b/c が平方因子をもつときは帰納法の仮定より $\mu_P(c,a)=0$ であるため、上記の和における c は実質的に、b/c が平方因子をもたないような c 全体を動く（現在の仮定より b/a は平方因子をもつことを注意しておく）。すると

$$\mu_P(a,b)=-\sum_{\substack{c\,;\\ bp_1^{-1}\cdots p_\ell^{-1}\mid c\,,\,c\mid b}}\mu_P(c,b)=-\sum_{c\in[bp_1^{-1}\cdots p_\ell^{-1},b]_P}\mu_P(c,b)=0$$

となる。以上より主張が成り立つ。 □

正整数 n の関数 f と g について、$g(n)=\sum_{d\mid n}f(d)$ が常に成り立つことは $g=f*\mathbb{1}$ と等価である。このとき、Möbius の反転公式より $f=g*\mu_P$ となるので、$f(n)=\sum_{d\mid n}g(d)\mu_P(d,n)$ が導かれる。これは初等整数論における Möbius の反転公式である。

演習問題

■問題 1. $P=\{1,2,\ldots,10\}$ とし、a が b の約数であるとき $a\preceq b$ として P 上の半順序を定める。この P の Hasse 図を描画せよ。

■問題 2. 半順序集合 P,Q と写像 $f\colon P\to Q$ で、f が全単射かつ順序保存であるが同型写像ではないような例を構成せよ。

（コメント：例えば群については、$f\colon G\to H$ が全単射かつ準同型であれば常に同型写像となる。同様の性質が半順序集合の場合には成り立たない、ということである。）

■問題 3. P,Q を半順序集合、$f\colon P\to Q$ を全単射な順序保存写像とする。さらに P 上の順序が全順序であれば、f は同型写像であることを証明せよ。

■問題 4. P を箱が 3 個以下の Young 図形全体の集合とし、包含関係で順序を定める。このとき、すべての $Y\in P$ について $\mu_P(\emptyset,Y)$ の値を決定せよ。

4 順序集合と束

本節の内容は [5] の 3 章を参考にしている。

組合せ論（あるいは離散数学）の分野では半順序集合自体も研究対象になっており、さまざまな概念や、特殊な半順序集合のなす部分クラスなどが考えられている。

定義 4.1. P を半順序集合、S をその部分集合とする。P における順序関係を S に制限することで S も半順序集合となる。このような半順序集合を P の**部分半順序集合**と呼ぶ。また、

- $x \in P$ が S の**上界**（upper bound）であるとは、どの $y \in S$ についても $x \succeq y$ が成り立つことと定める。同様に、$x \in P$ が S の**下界**（lower bound）であるとは、どの $y \in S$ についても $x \preceq y$ が成り立つことと定める。
- $x \in S$ が S において**極大**（maximal）であるとは、$y \in S$ が $y \succeq x$ を満たせば常に $y = x$ であることと定める。同様に、$x \in S$ が S において**極小**（minimal）であるとは、$y \in S$ が $y \preceq x$ を満たせば常に $y = x$ であることと定める。
- $x \in S$ が S において**最大**（maximum）であるとは、x 自身が S の上界であることと定める。同様に、$x \in S$ が S において**最小**（minimum）であるとは、x 自身が S の下界であることと定める。

P が最大元（、最小元）をもつとき、その元を $\max P$ や 1 や 1_P（、$\min P$ や 0 や 0_P）で表すことがある。

例 4.1. $P = \{1, 2, \dots, 10\}$ に整除関係、つまり $a \preceq b \Leftrightarrow a \mid b$ で順序を定めたものを考える。$S_1 = \{2, 3\}$ の上界となるのは 6 だけであり、S_1 の下界となるのは 1 だけである。$S_2 = \{4, 6\}$ の上界は存在せず、S_2 の下界となるのは 1 と 2 である。P の極大元は $6, 7, 8, 9, 10$ であり、P には最大元は存在しない。P の最小元は 1 であり、P の極小元も 1 のみである（演習問題を参照）。

定義 4.2. P を半順序集合、$S \subseteq P$ とする。P における S の上界全体の集合が最小元をもつとき、その元を S の**結び**（join）といい、$\bigvee S$ や $\bigvee_{x \in S} x$ などの記号で表す。S が有限集合 $\{x_1, \dots, x_n\}$ である場合にはその結びを $x_1 \vee \cdots \vee x_n$ とも書く。また、P における S の下界全体の集合が最大元をもつとき、その元を S の**交わり**（meet）といい、$\bigwedge S$ や $\bigwedge_{x \in S} x$ などの記号で表す。S が有限集合 $\{x_1, \dots, x_n\}$ である場合にはその交わりを $x_1 \wedge \cdots \wedge x_n$ とも書く。

例 4.2. 文字 a, b, c を有限個（0 個も含む）並べてできる文字列全体の集合を P とし、$w, v \in P$ について w が v の中に連続する部分列として現れるとき $w \preceq v$ として順序関係を定める。例えば $aba \preceq cabab$ であるが $abb \not\preceq acbb$、といった具合である。このとき、$w = ab$、$v = bc$ とすると、w と v の共通の下界は $\emptyset$（空の文字列）および b であり、$\emptyset \preceq b$ であるから、その交わりは $w \wedge v = b$ である。一方、w と v の共通の上界全体の集合に最小元は存在せず、したがって w と v の結び $w \vee v$ は存在しない。

定義 4.3. P を半順序集合とする。P の空でない有限部分集合が常に結びと交わりをもつとき、P は**束**（そく）(lattice）であるという。また、P の空でない部分集合が常に結びと交わりをもつとき、P は**完備束**（complete lattice）であるという。

定義より、有限な束は完備束であることを注意しておく。

例 4.3.
- あらゆる全順序集合は束である。
- ある群 G の部分群全体の集合 P に包含関係で順序を入れたもの（つまり、$H_1 \preceq H_2 \Leftrightarrow H_1 \subseteq H_2$）は完備束である。この場合、$H_\lambda \in P$（$\lambda \in \Lambda$）たちの交わりは $\bigcap_{\lambda \in \Lambda} H_\lambda$、結びは $\bigcup_{\lambda \in \Lambda} H_\lambda$ が生成する G の部分群である。
- 正整数全体の集合 $\mathbb{Z}_{>0}$ に整除関係で順序を入れたものは束である。この場合、$a_1, \ldots, a_n \in \mathbb{Z}_{>0}$ の結びはそれらの最小公倍数、交わりはそれらの最大公約数である。一方、$\mathbb{Z}_{>0}$ の空でない部分集合は常に交わりをもつ（演習問題を参照）が、$\mathbb{Z}_{>0}$ は完備束ではない。実際、$S = \{p \in \mathbb{Z}_{>0} \mid p \text{ は素数}\}$ とすると S は結びをもたない。

命題 4.1. L を空でない完備束とする。このとき L には最大元と最小元が存在する。

証明. L は完備束であり $L \neq \emptyset$ であるから、特に L 自身の結びと交わりがともに存在する。前者が L の最大元、後者が L の最小元である。 □

命題 4.2. P を半順序集合とし、条件「$x, y \in P$ のとき常に結び $x \vee y$ が存在する」を満たすとする。このとき、P の空でない有限部分集合は常に結びをもつ。上記の大小関係を入れ換えた主張（結びの代わりに交わりを考える）も成り立つ。特に、P の 2 元が常に結びと交わりをもてば P は束である。

証明. 結びについての主張を示せば残りの主張も導かれる。1 元集合については明らかに $\bigvee\{x\} = x$ である。以降では、$x \in P$ および空でない有限部分集合 $S \subseteq P$ について $\bigvee(S \cup \{x\})$ が存在して $(\bigvee S) \vee x$ に等しいことを $|S|$ についての数学的帰納法で示す。S が 1 元集合 $\{y\}$ である場合には主張は前提より明らかである。以降では $|S| \geq 2$ とする。帰納法の仮定により $\bigvee S$ は存在する。このとき $a := (\bigvee S) \vee x$ は x の上界であり、また

S の上界 $\bigvee S$ の上界であるから S の上界でもある。よって a は $S \cup \{x\}$ の上界である。また、b を $S \cup \{x\}$ の上界とすると、$b \succeq x$ であり、また b は S の上界であるから、$\bigvee S$ の定義より $b \succeq \bigvee S$ である。これらより $b \succeq (\bigvee S) \vee x = a$ である。よって a は $S \cup \{x\}$ の最小の上界であり、a が $S \cup \{x\}$ の結びとなる。以上よりすべての S について上記の主張が成り立つ。このことから元々の主張が導かれる。 □

半順序集合 P の Möbius 関数 μ_P について、P が束であれば μ_P の値が比較的計算しやすいことを述べる。有限束 L について、L を基底とする $\mathbb{C}$-線型空間を $A(L)$ で表し、$A(L)$ の $\mathbb{C}$-代数としての積を $xy := x \wedge y$（$x, y \in L$）で定義する。$A(L)$ の乗法単位元は L の最大元 1_L である。各 $x \in L$ について

$$\zeta_x := \sum_{y \preceq x} \mu_L(y, x) y \in A(L)$$

と定める。

補題 4.1. 上の状況で、$x \in L$ のとき $x = \sum_{y \preceq x} \zeta_y$ である。

証明. $z \in L$ について、$A(L)$ の元にその z の係数を対応させる射影を π_z と書くと、$\pi_z(\zeta_x) = \sum_{y \preceq x} \mu_L(y, x) \pi_z(y)$ である。$f_z, g_z \colon L \to \mathbb{C}$ を $f_z(x) := \pi_z(\zeta_x)$、$g_z(x) := \pi_z(x)$ と定めると、上の式は $\mathbb{C}^L$ における関係式 $f_z = g_z * \mu_L$ を意味する。すると Möbius の反転公式より $g_z = f_z * \mathbb{1}$、したがって

$$\pi_z(x) = g_z(x) = \sum_{y \preceq x} \mathbb{1}(y, x) f_z(y) = \sum_{y \preceq x} \pi_z(\zeta_y)$$

となる。よって $x = \sum_{y \preceq x} \zeta_y$ であり、主張が成り立つ。 □

補題 4.1 により、ζ_x たちは $A(L)$ の $\mathbb{C}$-線型空間としての生成系である。さらに個数を比較することで、ζ_x たちは $A(L)$ の $\mathbb{C}$-線型空間としての基底でもある。

補題 4.2. $A(L)$ から $\mathbb{C}$ の $|L|$ 個の直和（後者の基底を $\widehat{x}$（$x \in L$）で表す）への $\mathbb{C}$-線型写像 θ を $\theta(\zeta_x) := \widehat{x}$（$x \in L$）で定めると、$\theta$ は $\mathbb{C}$-代数の同型写像である。特に $x, y \in L$ のとき

$$\zeta_x \zeta_y = \begin{cases} \zeta_x & (x = y \text{ のとき}) \\ 0 & (x \neq y \text{ のとき}) \end{cases}$$

が成り立つ。

証明. 主張の前半が成り立てば後半は θ の定義から直ちに導かれる。θ が $\mathbb{C}$-線型空間の同型写像であることは定義から明らかであるので、あとは θ が積を保つことを示せばよく、

そのためには $x, y \in L$ について $\theta(x)\theta(y) = \theta(x \wedge y)$ であることを示せばよい。

$$\begin{aligned}
\theta(x)\theta(y) &= \theta\left(\sum_{z \preceq x} \zeta_z\right)\theta\left(\sum_{w \preceq y} \zeta_w\right)\\
&= \left(\sum_{z \preceq x} \widehat{z}\right)\left(\sum_{w \preceq y} \widehat{w}\right)\\
&= \sum_{z \preceq x\,,\, w \preceq y} \widehat{z}\widehat{w}\\
&= \sum_{z\,;\, z \preceq x\,,\, z \preceq y} \widehat{z}\\
&= \sum_{z \preceq x \wedge y} \widehat{z} = \theta\left(\sum_{z \preceq x \wedge y} \zeta_z\right) = \theta(x \wedge y)
\end{aligned}$$

であるので、主張が成り立つ。 □

最大元 1_P をもつ半順序集合 P について、1_P にカバーされる P の元を P の **coatom** という。同様に、最小元 0_P をもつ半順序集合 P について、0_P をカバーする P の元を P の **atom** という。

定理 4.1. *L を有限束とし、L の coatom 全体の集合を A^* で表す。非負整数 k について*

$$N_k := \left|\left\{S \subseteq A^* \colon |S| = k\,,\, \bigwedge S = 0_L\right\}\right|$$

とすると、$\mu_L(0_L, 1_L) = \sum_{k \geq 0} (-1)^k N_k$ である。

証明. $x \in A^*$ について、$A(L)$ において

$$1_L - x = \sum_{y \preceq 1_L} \zeta_y - \sum_{y \preceq x} \zeta_y = \sum_{y\,,\, y \not\preceq x} \zeta_y$$

である。よって

$$\prod_{x \in A^*} (1_L - x) = \prod_{x \in A^*} \sum_{y \not\preceq x} \zeta_y$$

となる。補題 4.2 を用いて右辺を ζ_y たちの一次結合に展開したとき、消えずに残る項はどの $x \in A^*$ についても $y \not\preceq x$ となる y についての ζ_y の項だけである。A^* の定義より、このような y は $y = 1_L$ のみであるので、

$$\prod_{x \in A^*} (1_L - x) = \zeta_{1_L} = \sum_{z \in L} \mu_L(z, 1_L) z$$

となる。両辺における 0_L の係数を比較すると、

$$\sum_{k\geq 0}(-1)^k N_k = \mu_L(0_L, 1_L)$$

となる。よって主張が成り立つ。 □

束の中でさらに何らかの条件を満たすもののなす部分クラスが色々と考えられている。ここではその一つを紹介する。

定義 4.4. 束 L が**分配束**（distributive lattice）であるとは、$x, y, z \in L$ について常に分配法則 $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ および $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ が成り立つことと定める。

注意 4.1. 束 L の元 x, y, z について常に $x \vee (y \wedge z) \preceq (x \vee y) \wedge (x \vee z)$ かつ $x \wedge (y \vee z) \succeq (x \wedge y) \vee (x \wedge z)$ であるから、分配束の条件については $x \vee (y \wedge z) \succeq (x \vee y) \wedge (x \vee z)$ および $x \wedge (y \vee z) \preceq (x \wedge y) \vee (x \wedge z)$ という向きだけを確かめれば充分である。

例 4.4.
- 集合 S の冪集合 $\mathcal{P}(S)$ に包含関係で順序を入れたものを考えると $\mathcal{P}(S)$ は分配束である。実際、$\mathcal{P}(S)$ における結びと交わりはそれぞれ和集合をとる操作、共通部分集合をとる操作に対応しており、分配束の定義の条件は和集合と共通部分集合の分配法則にほかならない。
- P を半順序集合とする。部分集合 $I \subseteq P$ について、$x, y \in P$ が $x \in I$ と $y \preceq x$ を満たすとき常に $y \in I$ であれば、I を P の **order ideal** という。

  $$J(P) := \{I \subseteq P \mid \ I \text{ は } P \text{ の order ideal }\}$$

  と定めると、$(J(P), \subseteq)$ は分配束である。実際、$I_1, I_2 \in J(P)$ のとき $I_1 \cap I_2 \in J(P)$ かつ $I_1 \cup I_2 \in J(P)$ であることから、$I_1 \wedge I_2 = I_1 \cap I_2$、$I_1 \vee I_2 = I_1 \cup I_2$ であり、特に $J(P)$ は束である。すると分配束の条件は集合の包含関係の性質より導かれる。
- 群 G の部分群の全体がなす束 L は一般に分配束とは限らない。実際、$G = S_3$ として、部分群 $H_1 = \langle (12) \rangle$, $H_2 = \langle (13) \rangle$, $H_3 = \langle (23) \rangle$ を考えると、$H_2 \wedge H_3 = \{\mathsf{id}\}$ より $H_1 \vee (H_2 \wedge H_3) = H_1 \vee \{\mathsf{id}\} = H_1$ である。一方、$H_1 \vee H_2 = H_1 \vee H_3 = S_3$ より $(H_1 \vee H_2) \wedge (H_1 \vee H_3) = S_3 \wedge S_3 = S_3$ である。よって $H_1 \vee (H_2 \wedge H_3) \neq (H_1 \vee H_2) \wedge (H_1 \vee H_3)$ であるから L は分配束ではない。

分配束については以下の特徴付けが知られている。

定理 4.2. L を有限分配束とする。このとき、$L \simeq J(P)$ を満たす半順序集合 P が同型を除いてただ一つ存在する。

証明. まず、主張のような P が存在することを示す。L の元 x が **join-irreducible** であるということを、$y, z \prec x$ かつ $y \vee z = x$ となる $y, z \in L$ が存在しないことと定める。

$$P := \{x \in L \mid \ x \text{ は join-irreducible } \}$$

と定めて、写像 $f \colon L \to J(P)$ と $g \colon J(P) \to L$ を

$$f(x) := P \cap \wedge^x \, , \, g(I) := \bigvee I$$

で定める。ここで $\wedge^x := \{y \in L \mid y \preceq x\}$ としている。$x, y \in L$、$x \preceq y$ のとき $\wedge^x \subseteq \wedge^y$ であることから $f(x) \subseteq f(y)$ であり、f は順序保存である。また、$I_1, I_2 \in J(P)$、$I_1 \subseteq I_2$ のとき $\bigvee I_1 \preceq \bigvee I_2$ であることから $g(I_1) \preceq g(I_2)$ であり、g も順序保存である。

$x \in L$ のとき $g(f(x)) = x$ であることを、Hasse 図上で 0_L から x まで上向きに辿る経路が含む辺数の最大値（これをここでは $\rho(x)$ で表す）に関する数学的帰納法で示す。$x \in P$ のとき（これは $\rho(x) = 0$ すなわち $x = 0_L$ のときを含む）は、f の定義より x が $f(x)$ の最大元であることから $g(f(x)) = x$ となる。一方 $x \not\in P$ のときは、P の定義より $y, z \prec x$ かつ $y \vee z = x$ となる $y, z \in L$ がとれる。$\rho(x) > \rho(y)$ かつ $\rho(x) > \rho(z)$ であるから、帰納法の仮定により $g(f(y)) = y$ すなわち $y = \bigvee(P \cap \wedge^y)$、かつ $g(f(z)) = z$ すなわち $z = \bigvee(P \cap \wedge^z)$ である。ここで $y \prec x$ より $P \cap \wedge^y \subseteq P \cap \wedge^x$ であるから、$\bigvee(P \cap \wedge^y) \preceq \bigvee(P \cap \wedge^x)$ であり、同様に $\bigvee(P \cap \wedge^z) \preceq \bigvee(P \cap \wedge^x)$ である。また、x が $P \cap \wedge^x$ の上界であることから $\bigvee(P \cap \wedge^x) \preceq x$ である。以上より

$$x = y \vee z = \left(\bigvee(P \cap \wedge^y)\right) \vee \left(\bigvee(P \cap \wedge^z)\right) \preceq \bigvee(P \cap \wedge^x) \preceq x$$

となるので、$x = \bigvee(P \cap \wedge^x) = g(f(x))$ となる。よって $x \in L$ のとき $g(f(x)) = x$ が成り立つ。

逆に、$I \in J(P)$ のとき $f(g(I)) = I$ であることを示す。$x \in I$ $(\subseteq P)$ のとき、$x \preceq g(I)$ であることから $x \in \wedge^{g(I)}$、したがって $x \in f(g(I))$ である。よって $I \subseteq f(g(I))$ となる。一方、$x \in f(g(I))$ のとき、f と g の定義より $x \preceq \bigvee I$ である。L は分配束であるから、$x = x \wedge (\bigvee I) = \bigvee_{y \in I}(x \wedge y)$ となる。$x \in P$ より x は join-irreducible であるから、ある $y \in I$ について $x \wedge y = x$、したがって $x \preceq y$ となる。I は order ideal であるから $x \in I$ となる。よって $f(g(I)) \subseteq I$ となる。以上より $f(g(I)) = I$ が成り立つ。このことから f と g は互いの逆写像であり、したがって f は L から $J(P)$ への同型写像となる。こうして主張のような P が存在することが示された。

次に主張のような P の一意性を示すために、Q が有限半順序集合であるとき、$I \in J(Q)$ が $J(Q)$ において join-irreducible であることと、$I = \wedge^x$ を満たす $x \in Q$ がただ一つ存在することが同値であることを示す。後者の条件が成り立っているとき、$K_1, K_2 \in J(Q)$、

$K_1 \cup K_2 = I$ であるとすると、$x \in I$ であることからどちらかの i について $x \in K_i$ である。すると K_i が order ideal であることから $I = \wedge^x \subseteq K_i$ であり、一方で $K_1 \cup K_2 = I$ より $I \supseteq K_i$ である。よって $K_i = I$ となる。これは I が join-irreducible であることを意味する。

逆に前者の条件が成り立っているとする。I が有限な order ideal であることから、$I = \bigcup_{y \in I\,;\,\text{極大}} \wedge^y$ が成り立つ。各 y について $\wedge^y \in J(Q)$ であり、また I は join-irreducible であるから、I のある極大元 y について $I = \wedge^y$ となる。一方、$z \in Q$ について $I = \wedge^z$ でもあるとすると、$y \in I = \wedge^z$ より $y \preceq z$ であり、同様に $z \preceq y$ であるから、$z = y$ である。よって後者の条件が成り立つ。以上より上記の同値性が示された。このことから、$J(Q)$ の join-irreducible な元全体の集合 $L(J(Q))$ から Q への写像を、$I = \wedge^x$ に $x \in Q$ を対応させることで定めることができ、これは $L(J(Q))$ から Q への同型写像である。

さて、半順序集合 P_1 と P_2 について $L \simeq J(P_1) \simeq J(P_2)$ であるとすると、$J(P_i)$ はともに有限集合であり、また $x \in P_i$ について $\wedge^x$ たちは $J(P_i)$ の異なる元である。このことから $|P_i| < \infty$ である。ここで、join-irreducible という性質は同型写像で保たれるので、上で示した同型 $L(J(P_i)) \simeq P_i$ とあわせて、$P_1 \simeq L(J(P_1)) \simeq L(J(P_2)) \simeq P_2$ となる。よって主張のような P は同型を除いてただ一つに定まる。以上より主張がすべて成り立つ。 $\square$

演習問題

■問題 1.　P を半順序集合とする。

1. $x \in P$ が P の最大元であれば、x は P の唯一の極大元であることを証明せよ。
2. P が有限集合であるとする。このとき、$x \in P$ が P の唯一の極大元であれば、x は P の最大元であることを証明せよ。
3. P が無限集合である場合には、上記「$x \in P$ が P の唯一の極大元であれば、x は P の最大元である」は必ずしも成り立たない。このことを示す具体例を挙げよ。

（コメント：順序関係の大小を入れ換えても同様の性質が成り立つ。）

■問題 2.　例 4.2 の状況で、P の元 $w = ab$ と $v = bc$ の結び $w \vee v$ が存在しないことを証明せよ。

■問題 3.　半順序集合 P が局所有限かつ最小元 0_P をもち、さらに P の空でない有限部分集合が常に結びをもつとする。このとき P の空でない部分集合は常に交わりをもつことを証明せよ。

■問題 4. 束 L の元 x, y, z について常に $x \vee (y \wedge z) \preceq (x \vee y) \wedge (x \vee z)$ であることを証明せよ。

（コメント：同様に $x \wedge (y \vee z) \succeq (x \wedge y) \vee (x \wedge z)$ であることも示せる。）

5　整列順序と数学的帰納法

本節の内容は書籍 [4] の 1 章を参考にしている。

数学的帰納法の原理においては、非負整数全体の集合における大小関係の性質が大きく寄与している。その性質を抽象化したものが以下の定義である。

定義 5.1. 半順序集合 $(P, \preceq)$ について、P の空でない部分集合が常に最小元をもつとき、P を**整列順序集合**（well-ordered set）あるいは整列集合といい、また $\preceq$ を**整列順序**（well-order）という。P が整列順序集合のとき、$x \in P$ について $\mathrm{prec}_P(x) := \{y \in P \mid y \prec x\}$ と定め、P の x による**切片**という。

補題 5.1. 整列順序は全順序である。

証明. P を整列順序集合とし、$x, y \in P$ とすると、定義より $\{x, y\}$ は最小元 z をもつ。$z = x$ のときは、z の定義より $x \preceq y$ が成り立つ。同様に、$z = y$ のときは $y \preceq x$ が成り立つ。よって $x \preceq y$ または $y \preceq x$ が成り立つので、P は全順序集合である。 □

整列順序集合上の数学的帰納法、とでも呼ぶべき以下の性質が成り立つ。

定理 5.1. P を空でない整列順序集合とし、φ を P の元についての何らかの命題とする。「$\min P$ について φ が真である」および「$x \in P \setminus \{\min P\}$ のとき、もし $\mathrm{prec}_P(x)$ 上で常に φ が真であるならば φ は x でも真である」が成り立つとき、P 上で φ は常に真である。

証明. P のある元について φ が偽になると仮定して矛盾を導けばよい。この仮定より $\{x \in P \mid \varphi(x)$ が偽$\}$ は P の空でない部分集合であるので、その最小元 a が存在する。前提の前者の条件より $a \neq \min P$ であり、また a の定義より $\mathrm{prec}_P(a)$ 上では φ は常に真である。すると前提の後者の条件より φ は a でも真であるが、これは矛盾である。以上より主張が成り立つ。 □

非負整数全体の集合 $\mathbb{Z}_{\geq 0}$ は整列順序集合である。この $\mathbb{Z}_{\geq 0}$ に定理 5.1 を適用することで、通常の数学的帰納法（の一形態、いわゆる累積帰納法）が導かれる。また、$\mathbb{Z}_{\geq 0}$ が整列順序集合であることから以下の事実も導かれる。

定理 5.2 (鳩の巣原理（pigeonhole principle）)**.** 整数 $n > m \geq 1$ と写像 $f\colon \{1, \dots, n\} \to \{1, \dots, m\}$ について、f は単射でない。

証明. 主張が成り立たない m があると仮定し、そのような最小の m をとり、単射な f をとる。明らかに $m > 1$ である。f は単射であるから、$|f^{-1}[m]|$ は 0 または 1 で

ある。$|f^{-1}[m]| = 0$ であるとすると $f\colon \{1,\dots,n\} \to \{1,\dots,m-1\}$ も単射となるが、これは m の最小性に矛盾する。よって $|f^{-1}[m]| = 1$ である。$f^{-1}[m]$ の唯一の元を a とすると、全単射 $g\colon \{1,\dots,n-1\} \to \{1,\dots,n\} \setminus \{a\}$ が存在する。このとき $f \circ g\colon \{1,\dots,n-1\} \to \{1,\dots,m-1\}$ も単射となるが、これは m の最小性に矛盾する。以上より主張が成り立つ。 □

整列順序の重要な性質を示す準備としていくつかの性質を示す。

補題 5.2. 整列順序集合 $(P, \preceq_P)$ と $(Q, \preceq_Q)$ について、$f\colon P \to Q$ を同型写像、$x \in P$ とすると、$f(\mathrm{prec}_P(x)) = \mathrm{prec}_Q(f(x))$ である。

証明. f が順序保存であることから $f(\mathrm{prec}_P(x)) \subseteq \mathrm{prec}_Q(f(x))$ である。また、f^{-1} が順序保存であることから $f^{-1}(\mathrm{prec}_Q(f(x))) \subseteq \mathrm{prec}_P(x)$ であり、したがって $\mathrm{prec}_Q(f(x)) \subseteq f(\mathrm{prec}_P(x))$ である。よって $f(\mathrm{prec}_P(x)) = \mathrm{prec}_Q(f(x))$ となり主張が成り立つ。 □

補題 5.3. 整列順序集合 $(P, \preceq)$ と $x \in P$ について $P \not\simeq \mathrm{prec}_P(x)$ である。

証明. 同型写像 $f\colon \mathrm{prec}_P(x) \to P$ が存在すると仮定して矛盾を導く。$S := \{y \in \mathrm{prec}_P(x) \mid f(y) \neq y\}$ が空でないと仮定して、その最小元 y をとる。すると $f|_{\mathrm{prec}_P(y)}$ は恒等写像となり、f を $\mathrm{prec}_P(x) \setminus \mathrm{prec}_P(y)$ へ制限したものは $P \setminus \mathrm{prec}_P(y)$ への同型写像となる。この同型写像は $\mathrm{prec}_P(x) \setminus \mathrm{prec}_P(y)$ の最小元 y を $P \setminus \mathrm{prec}_P(y)$ の最小元 y へと写すので、$f(y) = y$ となる。これは $y \in S$ と矛盾するので、$S = \emptyset$ となる。するとすべての $y \in \mathrm{prec}_P(x)$ について $f(y) = y$ となるので、$f(y) = x \in P$ となる $y \in \mathrm{prec}_P(x)$ が存在せず、f が全射であることと矛盾する。以上より主張が成り立つ。 □

補題 5.4. $(P, \preceq_P)$ と $(Q, \preceq_Q)$ を整列順序集合とすると、P から Q への同型写像は存在すればただ一つに定まる。

証明. $f, g\colon P \to Q$ を同型写像として、$f(x) \neq g(x)$ となる $x \in P$ が存在すると仮定して矛盾を導く。そのような最小の x をとると、$f|_{\mathrm{prec}_P(x)} = g|_{\mathrm{prec}_P(x)}$ となる。その像を X とすると、f も g も $P \setminus \mathrm{prec}_P(x)$ から $Q \setminus X$ への同型写像である。x は $P \setminus \mathrm{prec}_P(x)$ の最小元であるから、$f(x)$ も $g(x)$ も $Q \setminus X$ の最小元となり、x の定義と矛盾する。よって $f = g$ となり、主張が成り立つ。 □

整列順序については以下の性質が特徴的である。

定理 5.3. $(P, \preceq_P)$ と $(Q, \preceq_Q)$ を整列順序集合とすると、以下のちょうど一つが成り立つ：

1. $P \simeq Q$
2. ある $x \in P$ について $\mathrm{prec}_P(x) \simeq Q$

3. ある $y \in Q$ について $P \simeq \mathrm{prec}_Q(y)$

証明. まず、主張の条件が二つ同時には成り立たないことを示す。条件 1 が成り立つとする。もし条件 2 も成り立つとすると、$P \simeq \mathrm{prec}_P(x)$ となるが、これは補題 5.3 と矛盾する。条件 3 が成り立った場合も同様に矛盾する。よって条件 1 は他の条件と同時には成り立たない。次に、条件 2 と条件 3 が同時に成り立つと仮定して矛盾を導く。$f\colon P \to \mathrm{prec}_Q(y)$ を同型写像とすると、補題 5.2 より $f(\mathrm{prec}_P(x)) = \mathrm{prec}_{\mathrm{prec}_Q(y)}(f(x)) = \mathrm{prec}_Q(f(x))$ となる。よって、条件 2 の同型写像と合成することで同型写像 $Q \to \mathrm{prec}_Q(f(x))$ が得られるが、これは補題 5.3 と矛盾する。以上より、主張の条件は二つ同時には成り立たない。

あとは、主張の条件の少なくとも一つが成り立つことを示せばよい。何らかの $a \in P$ についての部分集合 $\mathrm{prec}_P(a) \cup \{a\} \subseteq P$ から、何らかの $b \in Q$ についての部分集合 $\mathrm{prec}_Q(b) \cup \{b\} \subseteq Q$ への同型写像の全体を $\mathcal{F}$ で表す。$\mathcal{F}$ に属する写像の定義域たちすべての和集合を $X \subseteq P$ とする。写像 $F\colon X \to Q$ を、$a \in X$ が $f \in \mathcal{F}$ の定義域に属するとき $F(a) := f(a)$ として定めたい。$a \in X$ が $f, g \in \mathcal{F}$ の定義域の両方に属し、かつ $f(a) \neq g(a)$ となることがあると仮定して矛盾を導く。このような最小の a と、対応する f, g をとる。$\mathcal{F}$ の定義より、f も g もその定義域は $\mathrm{prec}_P(a) \cup \{a\}$ を含む。補題 5.2 より $f(\mathrm{prec}_P(a)) = \mathrm{prec}_Q(f(a))$ かつ $g(\mathrm{prec}_P(a)) = \mathrm{prec}_Q(g(a))$ であり、また a の定義より $\mathrm{prec}_P(a)$ 上では f と g は一致するので、$\mathrm{prec}_Q(f(a)) = \mathrm{prec}_Q(g(a))$ したがって $f(a) = g(a)$ となる。これは a の定義と矛盾する。よって $a \in X$ が $f, g \in \mathcal{F}$ の定義域の両方に属すれば $f(a) = g(a)$ である。このことから写像 F はきちんと定義できている。

$x, y \in X$ のとき、$\mathcal{F}$ の定義より、x, y をともに定義域に含む $f \in \mathcal{F}$ が存在することを注意しておく（x と y の大きい方を定義域に含む $f \in \mathcal{F}$ をとればよい）。$x, y \in X$、$x \prec_P y$ のとき、x, y を定義域に含む $f \in \mathcal{F}$ をとると、f は同型写像であるから $F(x) = f(x) \prec_Q f(y) = F(y)$ となる。よって F は順序保存かつ単射である。$Y := F(X)$ とする。$x, y \in X$、$F(x) \prec_Q F(y)$ のとき、x, y を定義域に含む $f \in \mathcal{F}$ をとると、$f(x) = F(x) \prec_Q F(y) = f(y)$ であり、f は同型写像であるから $x \prec_P y$ となる。よって F は X から Y への同型写像である。

$\mathcal{F}$ の元の定義域と像はどちらも order ideal であるから、その和集合で表される X および Y もまた order ideal である。よって、$X \neq P$ であれば $x := \min(P \setminus X)$ について $X = \mathrm{prec}_P(x)$ であり、同様に、$Y \neq Q$ であれば $y := \min(Q \setminus Y)$ について $Y = \mathrm{prec}_Q(y)$ である。よって、$X = P$ または $Y = Q$ であれば主張の条件の少なくとも一つが成り立つ。あとは、$X \neq P$ かつ $Y \neq Q$ であると仮定して矛盾を導けばよい。上記のように $X = \mathrm{prec}_P(x)$、$Y = \mathrm{prec}_Q(y)$ と表すと、$\overline{F}(x) := y$ および X 上で $\overline{F} = F$ と定めることで同型写像 $\overline{F}\colon X \cup \{x\} \to Y \cup \{y\}$ が得られる。すると定義より $\overline{F} \in \mathcal{F}$ となるが、これは $x \notin X$ と矛盾する。以上より主張が成り立つ。 □

数学的帰納法に現れる各ステップは「有限番目」のステップであったが、これを「無限番目」のステップを含む議論に拡張したい。そのために順序数という概念を導入する。以下しばらく、順序数について論じている際には、どの集合のどの要素もまた集合であると仮定する。これはつまり、ある集合の二つの要素 x, y について、「$a \in x$ と $a \in y$ が等価」という性質を示すことで $x = y$ と結論付けることができる、ということである。

定義 5.2. 集合 x が**推移的**（transitive）であるとは、$y \in x$ かつ $z \in y$ のとき $z \in x$ が成り立つことと定める（この条件は、$y \in x$ のとき $y \subseteq x$ となることと等価である）。また、集合 α が以下の条件を満たすとき、α を**順序数**（ordinal number）という：

1. α は推移的である。
2. $\beta \in \alpha$ のとき $\beta \notin \beta$ である。
3. $\beta \preceq_\alpha \gamma$ となるのは $\beta = \gamma$ または $\beta \in \gamma$ のとき、として定まる α 上の関係 $\preceq_\alpha$ は整列順序である。

すべての順序数からなる集まり（クラス）を ON で表す。

なお、ON 自体は集合ではない（集合として取り扱うと矛盾が生じる）ことが知られている。この事実は **Burali-Forti の逆理**（Burali-Forti paradox）と呼ばれている。また、上の条件 2 より、α が順序数のとき $\alpha \notin \alpha$ であることを注意しておく。

例 5.1. $\ulcorner 0 \urcorner := \emptyset$、$\ulcorner 1 \urcorner := \{\ulcorner 0 \urcorner\}$、$\ulcorner 2 \urcorner := \{\ulcorner 0 \urcorner, \ulcorner 1 \urcorner\}$、$\ulcorner 3 \urcorner := \{\ulcorner 0 \urcorner, \ulcorner 1 \urcorner, \ulcorner 2 \urcorner\}$、$\cdots$という具合に非負整数 n に対して $\ulcorner n \urcorner$ を定義していくとこれらは順序数となる。これらを**有限順序数**と呼ぶ。（以降では非負整数 n と $\ulcorner n \urcorner$ とを同一視する。）また、$\omega := \{\ulcorner n \urcorner \mid n \in \mathbb{Z}_{\geq 0}\}$ や $\omega \cup \{\omega\}$ も順序数となる。これらは無限順序数の例である。

以降では順序数のいろいろな性質を紹介していく。

命題 5.1. α を順序数、$\beta \in \alpha$ とすると、β も順序数であり $\mathrm{prec}_\alpha(\beta) = \beta$ が成り立つ。

証明. 主張の後半について、$\gamma \in \mathrm{prec}_\alpha(\beta)$ とすると $\gamma \prec_\alpha \beta$、したがって $\gamma \in \beta$ となる。よって $\mathrm{prec}_\alpha(\beta) \subseteq \beta$ である。逆に、$\gamma \in \beta$ とすると、前提 $\beta \in \alpha$ および α が推移的であることから $\gamma \in \alpha$ となり、$\gamma \in \beta$ より $\gamma \prec_\alpha \beta$、したがって $\gamma \in \mathrm{prec}_\alpha(\beta)$ となる。よって $\beta \subseteq \mathrm{prec}_\alpha(\beta)$ となり、$\mathrm{prec}_\alpha(\beta) = \beta$ が成り立つ。

主張の前半については、主張の後半より β が α の部分集合であることから β も整列順序集合であり、また条件「$\gamma \in \beta$ のとき $\gamma \notin \gamma$」も α と同様に成り立つ。また、$\delta \in \gamma \in \beta$ とすると、前提 $\beta \in \alpha$ および α が推移的であることから $\gamma \in \alpha$ および $\delta \in \alpha$ が成り立つ。すると $\delta \prec_\alpha \gamma \prec_\alpha \beta$ となるので $\delta \prec_\alpha \beta$、したがって $\delta \in \beta$ となる。よって β も推移的で

あり、したがって β も順序数である。以上より主張が成り立つ。 $\square$

命題 5.2. 順序数 α, β について、α と β が整列順序集合として同型であれば $\alpha = \beta$ である。

証明. $f \colon \alpha \to \beta$ を同型写像とする。$S := \{\gamma \in \alpha \mid f(\gamma) \neq \gamma\}$ が空でないと仮定して矛盾を導く。S の最小元を γ とする。

$\delta \in \gamma$ とすると、$\gamma \in \alpha$ および α が推移的であることから $\delta \in \alpha$ となる。すると $\delta \prec_\alpha \gamma$ となり、γ の定義より $f(\delta) = \delta$ である。f は順序保存であるから、$\delta \in \gamma$ より $\delta = f(\delta) \in f(\gamma)$ となる。よって $\gamma \subseteq f(\gamma)$ が成り立つ。

$\delta \in f(\gamma)$ とすると、$f(\gamma) \in \beta$ および β が推移的であることから $\delta \in \beta$ となる。$\eta := f^{-1}(\delta) \in \alpha$ とすると、$f(\eta) = \delta \in f(\gamma)$ となり、f が同型写像であることから $\eta \in \gamma$、したがって $\eta \in \mathrm{prec}_\alpha(\gamma)$ となる。γ の定義より $f(\eta) = \eta$ である。すると $\delta = f(\eta) = \eta \in \gamma$ となる。よって $f(\gamma) \subseteq \gamma$ も成り立ち、$f(\gamma) = \gamma$ となる。これは $\gamma \in S$ と矛盾する。

よって $S = \emptyset$ であり、$\gamma \in \alpha$ のとき常に $f(\gamma) = \gamma$ である。すると、$\gamma \in \alpha$ について $\gamma = f(\gamma) \in \beta$ となるので $\alpha \subseteq \beta$ である。また、$\gamma \in \beta$ について $\gamma = f(f^{-1}(\gamma)) = f^{-1}(\gamma) \in \alpha$ となるので $\beta \subseteq \alpha$ である。よって $\alpha = \beta$ となり主張が成り立つ。 $\square$

定理 5.4. 順序数 α, β について、$\alpha = \beta$、$\alpha \in \beta$、$\beta \in \alpha$ のうちちょうど一つが成り立つ。

証明. まず、$\alpha \notin \alpha$ であることから、$\alpha = \beta$ であれば $\alpha \notin \beta$ かつ $\beta \notin \alpha$ である。また、$\alpha \in \beta$ かつ $\beta \in \alpha$ であるとすると、α が推移的であることから $\alpha \in \alpha$ となり、これは上記の事実と矛盾する。よって主張の条件は二つ以上同時には成り立たない。

定理 5.3 より、$\alpha \simeq \beta$ であるか、ある $\gamma \in \alpha$ について $\mathrm{prec}_\alpha(\gamma) \simeq \beta$ であるか、ある $\gamma \in \beta$ について $\alpha \simeq \mathrm{prec}_\beta(\gamma)$ であるかのいずれかである。一つ目の場合には命題 5.2 より $\alpha = \beta$ となる。二つ目の場合には、命題 5.1 より γ は順序数で $\mathrm{prec}_\alpha(\gamma) = \gamma$ となるので、命題 5.2 より $\gamma = \beta$ となり、したがって $\beta \in \alpha$ である。三つ目の場合にも同様に $\alpha \in \beta$ である。以上より主張が成り立つ。 $\square$

定理 5.5. S を順序数からなる集合とし、$\alpha, \beta \in S$ について $\alpha = \beta$ または $\alpha \in \beta$ のときに $\alpha \leq \beta$ と定めると、$(S, \leq)$ は整列順序集合である。

証明. まず、$(S, \leq)$ が半順序集合であることを示す。反射律は定義より直ちに成り立つ。反対称律については、$\alpha \leq \beta$、$\beta \leq \alpha$ とし、$\alpha \neq \beta$ と仮定して矛盾を導けばよい。このとき $\leq$ の定義より $\alpha \in \beta$ かつ $\beta \in \alpha$ であるが、これは定理 5.4 と矛盾する。推移律について、$\alpha \leq \beta$、$\beta \leq \gamma$ として $\alpha \leq \gamma$ を示せばよい。$\alpha = \beta$ または $\beta = \gamma$ のときは明らかであ

るから $\alpha \neq \beta$、$\beta \neq \gamma$ とする。このとき $\leq$ の定義より $\alpha \in \beta$ かつ $\beta \in \gamma$ であり、γ が推移的であることから $\alpha \in \gamma$、したがって $\alpha \leq \gamma$ となる。よって $(S, \leq)$ は半順序集合である。

あとは $\emptyset \neq T \subseteq S$ としたときに T が $\leq$ に関する最小元をもつことを示せばよい。$\alpha \in T$ をとる。この α が T の最小元であれば主張が成り立つので、以降ではそうでないとする。このとき $X := \{\beta \in T \mid \alpha \not\leq \beta\}$ は空でない。また、$\beta \in X$ とすると、$\alpha \neq \beta$ かつ $\alpha \notin \beta$ であるから、定理 5.4 より $\beta \in \alpha$ である。よって $X \subseteq \alpha$ となり、α は整列順序集合であるから、X の最小元 γ が存在する。もし $\delta \in T$ かつ $\gamma \not\leq \delta$ であるとすると、γ が X の最小元であることから $\delta \notin X$ である。すると $\alpha \leq \delta$ となり、一方で $\gamma \in X \subseteq \alpha$ より $\gamma \leq \alpha$ となるので、$\leq$ の推移性より $\gamma \leq \delta$ となる。これは矛盾であるから、$\delta \in T$ であれば $\gamma \leq \delta$ となり、したがって γ は T の最小元である。以上より主張が成り立つ。 □

注意 5.1. 定理 5.5 と同様の論法により、順序数からなる空でない集まりには最小の要素が存在することがわかる。

以降では、順序数の間に定理 5.5 のような整列順序関係 $\leq$ が定まっているものとする。

順序数を用いると、「無限の長さの数学的帰納法」、正式には**超限帰納法**（transfinite induction）あるいは**超限再帰**（transfinite recursion）と呼ばれる論法を導入できる。超限帰納法の正確な定式化はやや煩雑なのでここでは割愛するが、超限帰納法の具体例として、選択公理から Zorn の補題を導く証明を紹介する。その準備として以下の定義を導入する。

定義 5.3. α を順序数とする。α が順序集合として最大元をもつとき、α を**後続型順序数**（successor ordinal）という。$\alpha \neq 0$ かつ α が後続型でない場合、α を**極限順序数**（limit ordinal）という。

α が後続型順序数のとき、$\beta = \max \alpha$ とすると β は α 未満の最大の順序数であることを注意しておく。

定理 5.6 (Zorn の補題)**.** P を空でない半順序集合とする。P の全順序部分集合が常に P 内に上界をもつならば、P は極大元をもつ。

証明. まず、P の空でない部分集合全体の族に選択公理を適用することで、P の空でない部分集合全体を定義域とする写像 ι で $\iota(S) \in S$ を常に満たすものがとれる。

P が極大元をもたないと仮定して矛盾を導く。順序数 α ごとに P の元 x_α を、条件「$\beta < \alpha$ のとき $x_\beta \prec x_\alpha$」を満たすよう、以下の要領で再帰的に定める。$\alpha = 0$ については $x_0 := \iota(P)$ とする。以下では $\alpha \neq 0$ として、α 未満の順序数 β については x_β が既に定まっているとする。

- α が後続型順序数のとき、α の最大元を β とする。P についての仮定より $x_\beta \in P$ は極大元でないので、$S := \{y \in P \mid x_\beta \prec y\}$ は空でない。$x_\alpha := \iota(S)$ とする。このとき定義より $x_\beta \prec x_\alpha$ であり、また β 未満の順序数 γ については、$x_\gamma \prec x_\beta$ という条件より $x_\gamma \prec x_\alpha$ となる。よって上記の条件が満たされている。
- α が極限順序数のとき、$C := \{x_\beta \mid \beta < \alpha\}$ とすると、上記の条件より C は P の全順序部分集合である。前提より $S := \{y \in P \mid y$ は C の上界$\}$ は空でない。$x_\alpha := \iota(S)$ とする。このとき、$\beta < \alpha$ について $x_\beta \preceq x_\alpha$ である。また、α は極限順序数であるから β は α 未満の最大の順序数ではなく、$\beta < \gamma < \alpha$ を満たす順序数 γ が存在する。すると $x_\beta \prec x_\gamma \preceq x_\alpha$ となり、$x_\beta \prec x_\alpha$ となる。よって上記の条件が満たされている。

こうしてすべての順序数 α に応じて上記の条件を満たす元 x_α が定まる（やや直感的な議論であるが、もし x_α が定まらないような α が存在するとすると、そのような最小の α をとることができるが、その α については上記の規則で x_α が定まるはずであるから矛盾である)。上記の条件によりこの x_α たちはすべて異なる元である。すると（ここもやや直感的な議論であるが)「上記の規則で集合 P のある元に対応する順序数全体の集合」として ON 自体が集合をなすことになるが、これは Burali-Forti の逆理と矛盾する。以上より主張が成り立つ。 □

Zorn の補題を用いた標準的な議論によって以下の性質が導かれる。

定理 5.7 (整列可能定理（Well-Ordering Theorem）). どの集合も、何らかの順序関係について整列順序集合となる。

整列可能定理と順序数の概念に基づいて、集合の濃度の（集合論的な）定義を与えることができる。

定理 5.8. X を集合とすると、ある順序数 α と全単射 $X \to \alpha$ が存在する。そのような最小の順序数 α を X の**濃度**（*cardinality*）といい、$|X|$ で表す。

証明. 整列可能定理より、X は整列順序集合であるとしてよい。定理 5.3 より、どの順序数 α についても X との間に定理 5.3 の条件のどれか一つが成り立つ。ここで、$x \in X$ の各々について、命題 5.2 より、$\mathrm{prec}_X(x) \simeq \alpha$ を満たす順序数 α は一つ以下しか存在しない。このことを踏まえて、（ここもやや直感的であるが)「上記の要領で X の元と対応する順序数の集合」を S とすると、Burali-Forti の逆理より ON 自体は集合ではないので、S は ON とは一致せず、S に属さない順序数 α が存在する。この α については定理 5.3 の条件のうち、「$X \simeq \alpha$」もしくは「ある $\beta \in \alpha$ について $X \simeq \mathrm{prec}_\alpha(\beta) = \beta$」（最後の等号は命題 5.1 に基づく）のいずれかが成り立つ。どちらの場合にも、X から順序数 α また

は β への全単射が存在する。以上より主張が成り立つ。 $\square$

演習問題

■問題 1. $(P, \preceq_P)$ と $(Q, \preceq_Q)$ を整列順序集合とする。P と Q の非交和 $P \sqcup Q$ 上の関係 $\preceq$ を、P 上では $\preceq_P$ に一致し、Q 上では $\preceq_Q$ に一致し、かつ $x \in P$ と $y \in Q$ について常に $x \preceq y$ となるよう定める。このとき $\preceq$ は整列順序であることを証明せよ。

■問題 2. $(P, \preceq_P)$ と $(Q, \preceq_Q)$ を整列順序集合とする。P と Q の直積集合 $P \times Q$ 上の関係 $\preceq$ を、$(x_1, x_2) \preceq (y_1, y_2)$ となるのは $x_2 \prec y_2$ もしくは「$x_2 = y_2$ かつ $x_1 \preceq y_1$」のとき、として定める。このとき $\preceq$ は整列順序であることを証明せよ。
（コメント：このような順序を辞書式順序という。）

■問題 3. α, β を順序数とするとき、$\alpha \in \beta$ と $\alpha \subsetneq \beta$ が同値であることを証明せよ。

■問題 4. Burali-Forti の逆理を証明せよ。
（ヒント：ON が集合であるとすると ON 自体が順序数となることを示す。）

■問題 5. （Zorn の補題を用いて）整列可能定理を証明せよ。

6　グラフ理論

この節以降のグラフ理論に関する内容は書籍 [2] および [3] を参考にしている。

何らかの対象たちが互いに「繋がっている／いない」という状況を表す道具の一つであるグラフについて述べる。

定義 6.1. **無向**(むこう)**グラフ**（undirected graph）とは、集合 V と E、および写像 $\iota\colon E \to \{\{x,y\} \mid x,y \in V\}$ の三つ組 (V,E,ι) として定義される。

無向グラフを表す際に、ι を省略して (V,E) と表される場合も多々ある。また、無向グラフのことを単にグラフ（graph）と呼ぶことも多い。V と E がともに有限集合であるとき、無向グラフ (V,E,ι) は有限であるという。

無向グラフ $G=(V,E,\iota)$ について、V を G の**頂点集合**（vertex set）、E を G の**辺集合**（edge set）と呼ぶ。V と E の要素をそれぞれ G の**頂点**（vertex）、**辺**（edge）と呼ぶ。G の辺が無向グラフの辺であることを強調する際には、無向辺（undirected edge）と呼ばれることもある。直感的には、G の頂点 x,y と辺 e が $\iota(e)=\{x,y\}$ を満たすとき、e は点 x,y を結ぶ向きの無い線であると考えることができる。この x と y を e の**端点**（endpoint）と呼ぶ。またこのとき、x と y は辺 e に**接続している**という。G の頂点 x と接続している辺の本数を x の**次数**（degree）といい、$\deg(x)$ などと表す。$|\iota(e)|=1$ を満たす辺 e、つまり両端点が一致する辺 e のことを **loop** と呼ぶ。また、辺 e_1,e_2 について $\iota(e_1)=\iota(e_2)$ が成り立つとき、e_1 と e_2 は**平行**（parallel）である、あるいは**多重辺**（multiple edge）である、などといわれる。図 5 の左側は 5 個の頂点と 9 本の辺をもつ無向グラフの例であり、e_1 は loop（$\iota(e_1)=\{x,x\}=\{x\}$）、e_2 と e_3 は平行な辺（$\iota(e_2)=\iota(e_3)=\{y,z\}$）である。なお、loop も多重辺ももたないグラフは**単純**（simple）であるという。単純な無向グラフについては、ι が単射であるから、辺 e を V の部分集合 $\iota(e)$ と同一視することもできる。以降ではしばしばそのような同一視を断りなしに行う。

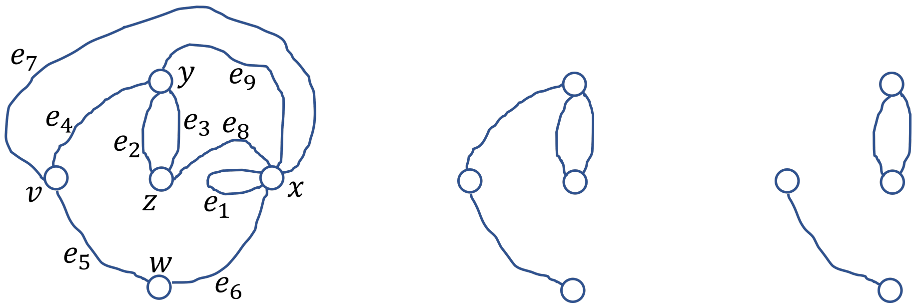


図 5　無向グラフとその部分グラフの例

$G = (V, E, \iota)$ を無向グラフとする。V のある部分集合 V' と E のある部分集合 E' について $(V', E', \iota|_{E'})$ という形に表されるグラフを G の**部分グラフ**（subgraph）という。また、この部分グラフについて $E' = \{e \in E \mid \iota(e) \subseteq V'\}$ が成り立っているとき、この部分グラフを**誘導部分グラフ**（induced subgraph）という。誘導部分グラフは **full subgraph** と呼ばれることもある。例えば、図 5 の中央のグラフは図 5 の左側のグラフの誘導部分グラフである。一方、図 5 の右側のグラフは図 5 の左側のグラフの部分グラフであるが誘導部分グラフではない。

$G = (V, E, \iota)$ を無向グラフとする。G における**道**（path）とは、列 $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$（$n \geq 0$）で、各 i について $v_i \in V$、$e_i \in E$、$\iota(e_i) = \{v_{i-1}, v_i\}$ を満たすもののことと定める。この道を $e_1 e_2 \cdots e_n$ で表すこともある。直感的には、これは頂点 $v_0, v_1, \ldots, v_n$ をこの順番に、辺 $e_1, e_2, \ldots, e_n$ を通って辿る経路を意味している。上記のような道が $v_n = v_0$ を満たすとき、**閉路**（closed path、circuit）と呼ばれる。例えば、図 5 の左側のグラフにおいて、$P_1 := y e_4 v e_5 w$ や $P_2 := y e_2 z e_3 y e_4 v e_4 y$ は道であり、$P_3 := v e_5 w e_6 x e_7 v$ や $P_4 := v e_7 x e_8 z e_3 y e_9 x e_6 w e_5 v$ は閉路である。道 $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$ に含まれる頂点 v_i たちがすべて異なるとき、この道は**単純**であるという。また、閉路 $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$ に含まれる頂点 v_i たちが、組 $v_n = v_0$ を除いてすべて異なるとき、この閉路は**単純**であるという。上の例では、道 P_1 と閉路 P_3 は単純であり、道 P_2 と閉路 P_4 は単純ではない。なお、単純グラフにおいては端点を指定することで辺が（存在すれば）一つに定まるため、道 $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$ をより簡潔に $v_0 v_1 \cdots v_{n-1} v_n$ と表すことが多い。

無向グラフ G について、その頂点 x, y に対する関係 $x \sim y$ を、x から y への道が存在することとして定める。このとき $\sim$ は G の頂点集合上の同値関係である。その同値類 V' の各々について、頂点集合 V' をもつ G の誘導部分グラフのことを G の**連結成分**（connected component）という。G の連結成分が 1 個以下しか存在しないとき、G は**連結**（connected）であるという。

無向グラフ G について、G が長さ（辺数）正の単純閉路をもたないとき、G を**林**（forest）という。連結な林のことを**木**（tree）という。図 6 の左側のグラフは連結であるが林ではない。図 6 の中央のグラフは林であるが連結ではない（2 個の連結成分をもつ）。図 6 の右側のグラフは連結な林、すなわち木である。なお、林は単純グラフであることを注意しておく。また、G の部分グラフ G' の頂点集合が G の頂点集合と同一であり、かつ G' が木であるとき、G' を G における**全域木**（spanning tree）という。例えば、図 6 の右側のグラフは図 6 の左側のグラフの全域木である。

無向グラフとは異なり、グラフの辺に「向き」が定まっている状況も考えられる。

定義 6.2. **有向**（ゆうこう）**グラフ**（directed graph）とは、集合 V と E、および写像 $\iota \colon E \to V \times V$ の三つ組 (V, E, ι) として定義される。

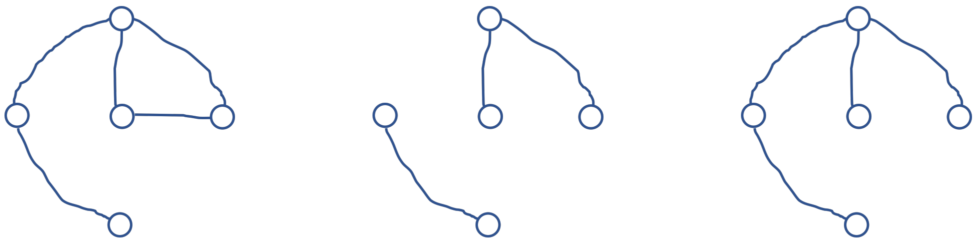


図 6　連結なグラフや林の例

無向グラフと同様に有向グラフについても、ι を省略して (V, E) と表される場合も多々ある。また、頂点集合 V と辺集合 E がともに有限集合であるときに、その有向グラフは有限であるという。

直感的には、G の頂点 $x, y \in V$ と**有向辺**（directed edge）$e \in E$（単に辺とも呼ばれる）が $\iota(e) = (x, y)$ を満たすとき、e は点 x と点 y を結ぶ線であり x から y への向きが付いていると考えることができる。$\iota(e) = (x, y)$ のとき、x を辺 e の**始点**（source）、y を辺 e の**終点**（terminal）といい、それぞれ記号 $s(e)$、$t(e)$ などで表される場合もある。G の頂点 x について、$s(e) = x$ を満たす辺 e の本数を x の**出(で)次数**といい、$t(e) = x$ を満たす辺 e の本数を x の**入(いり)次数**という。$s(e) = t(e)$ を満たす辺 e のことを **loop** と呼ぶ。辺 e_1, e_2 について $\iota(e_1) = \iota(e_2)$ が成り立つとき、e_1 と e_2 は**平行**である、あるいは**多重辺**である、などといわれる。loop も多重辺ももたない有向グラフは**単純**であるという。単純な有向グラフについては、ι が単射であるから、辺 e を頂点の組 $\iota(e)$ と同一視することもできる。以降ではしばしばそのような同一視を断りなしに行う。例えば、半順序集合の Hasse 図において各辺に下から上への向きを付けたものは単純な有向グラフである。また、無向グラフの場合と同様に有向グラフの部分グラフも定義される。

$G = (V, E, \iota)$ を有向グラフとする。G における**有向道**（あるいは単に道）とは、列 $v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$（$n \geq 0$）で、各 i について $v_i \in V$、$e_i \in E$、$\iota(e_i) = (v_{i-1}, v_i)$ を満たすもののことと定める。この道を $e_1 e_2 \cdots e_n$ で表すこともある。上記のような道が $v_n = v_0$ を満たすとき、（有向）**閉路**と呼ばれる。無向グラフの場合と同様に単純な道や単純な閉路が定義される。また、やはり無向グラフの場合と同様に、単純有向グラフにおいては上記の道をより簡潔に $v_0 v_1 \cdots v_{n-1} v_n$ と表すことが多い。G のどの頂点 $x, y \in V$ についても x から y への有向道が存在するとき、G は**強連結**（strongly connected）であるという。

定義 6.3. $G = (V, E, \iota)$ を有限単純無向グラフとする。

- G が**二部グラフ**（bipartite graph）であるとは、V の分割 $V = A \sqcup B$ をうまく選ぶと、G のどの辺も A に属する頂点と B に属する頂点を結んでいるようにできる

ことと定める。

- $U \subseteq V$ が G の**頂点被覆**（vertex cover）であるとは、G のどの辺 e についても $\iota(e) \cap U \neq \emptyset$ が成り立つことと定める。
- $M \subseteq E$ が G の**マッチング**（matching）であるとは、M の異なる 2 元 e_1, e_2 について常に $\iota(e_1) \cap \iota(e_2) = \emptyset$ が成り立つことと定める。さらに $\bigcup_{e \in M} \iota(e) = V$ が成り立つとき、マッチング M は**完全**（perfect）であるという。

二部グラフにおける頂点被覆とマッチングの大きさについては以下の性質が成り立つ。このような形の定理は「ミニマックス型」の定理と称されることがある。

定理 6.1. 有限な二部グラフ $G = (V, E)$ について、

$$\min\{|U| \colon U \text{ は } G \text{ の頂点被覆}\} = \max\{|M| \colon M \text{ は } G \text{ のマッチング}\}$$

が成り立つ。

証明. まず、U を頂点被覆、M をマッチングとすると、頂点被覆の定義よりどの $e \in M$ についても $\iota(e) \cap U \neq \emptyset$ である。その共通部分から要素を選ぶことで写像 $f \colon M \to U$ を作れる。さらにマッチングの定義と f の定義より f は単射である。よって $|M| \leq |U|$ が成り立つ。これはどの U と M についても成り立つことから、主張の右辺の値は左辺の値以下となる。あとは、主張の左辺の値が右辺の値以下であることを示せばよい。

M を G の要素数最大のマッチングとする。$V = A \sqcup B$ を二部グラフの定義における分割とする。ここで、

（∗）$v_0 e_1 v_1 \cdots e_{2k+1} v_{2k+1}$、ただし $v_0 \in A$ は M のどの辺にも接続せず、またどの整数 i についても $e_{2i} \in M$

という形の、途中で後戻りしない（つまり、$e_i \neq e_{i-1}$ である）道が存在するような頂点 $v_{2k+1} \in B$ の全体を B' で表す。また、M の辺で B' 内の頂点を通らないものたちについて、その端点で A に属するものをすべて集めた集合を A' で表す。以降では $A' \cup B'$ が G の頂点被覆であり $|A' \cup B'| = |M|$ であることを示す。これが示されれば、主張の左辺の値は $|A' \cup B'| = |M|$ 以下となり、主張が導かれる。

そのために以下の主張を示す。

主張. B' のどの点も、M に属する辺のどれかに接続している。

主張の証明. $x \in B'$ が M のどの辺にも接続していないと仮定して矛盾を導く。B' の定義より、条件（∗）を満たす道 $v_0 e_1 v_1 \cdots e_{2k+1} v_{2k+1}$ で $v_{2k+1} = x$ を満たすものが存在する。このとき、上の仮定と条件（∗）より v_0 と v_{2k+1} は M の

どの辺にも接続していない。また、マッチングの定義より、各 i について v_{2i-1} と v_{2i} は e_{2i} 以外の M の辺には接続していない。特に $e_1, e_3, \dots, e_{2k+1} \notin M$ であり、$v_0, \dots, v_{2k+1}$ たちはすべて異なる頂点である。これらの条件より、M から $e_2, e_4, \dots, e_{2k}$ を除いて $e_1, e_3, \dots, e_{2k+1}$ を追加した集合 M' も G のマッチングとなる。$|M'| = |M| + 1$ であるから、これは M が最大であることと矛盾する。よってこの主張が成り立つ。 □

M の辺 e について、$\iota(e) \cap B' \neq \emptyset$ であるときにはその唯一の要素（G が二部グラフであることと $B' \subseteq B$ より、e は B' の 2 点を結ばないことに注意）を $g(e)$ とする。また $\iota(e) \cap B' = \emptyset$ であるときには、e の端点で A に属するもの（G が二部グラフであることからただ一つに定まる）は A' の定義より A' に属する。それを $g(e)$ とする。この写像 $g\colon M \to A' \cup B'$ について、M がマッチングであることから g は単射であり、また A' の定義および上の主張より g は全射である。よって g は全単射であり、$|A' \cup B'| = |M|$ が成り立つ。あとは $A' \cup B'$ が G の頂点被覆であることを示せばよい。

そのためには、$a \in A \setminus A'$ と $b \in B \setminus B'$ を結ぶ辺 e が存在すると仮定して矛盾を導けばよい。$b \notin B'$ より道 aeb は条件（∗）を満たさず、したがって a は M のある辺 e' に接続している。$\iota(e') = \{a, b'\}$（$b' \in B$）とすると、$a \notin A'$ より $b' \in B'$ である。すると条件（∗）を満たす道 $v_0 e_1 \cdots e_{2k+1} v_{2k+1}$ で $v_{2k+1} = b'$ となるものが存在する。このとき、この道の後ろに $e'aeb$ をつなげた道も条件（∗）を満たすが、これは $b \notin B'$ であることと矛盾する。以上より定理の主張が成り立つ。 □

有限二部グラフにおける完全マッチングの存在条件に関する定理を紹介する（下記の定理を $|A| = |B|$ の場合に適用すると完全マッチングの存在条件が得られる）。

定理 6.2 (Hall's Marriage Theorem)**.** G を有限二部グラフとし、$V = A \sqcup B$ を対応する分割とする。このとき以下は互いに同値である。

1. G のマッチング M で、A のどの頂点も M のある辺に接続しているものが存在する。
2. A の部分集合 S について、S の頂点と辺で結ばれている頂点全体の集合を $N(S)$ で表すとき、常に $|N(S)| \geq |S|$ が成り立つ。

証明.【1 ⇒ 2】$v \in S$ について、条件 1 より v を端点にもつ M の辺 e が存在し、またマッチングの定義よりそのような e はただ一つに定まる。この e の v ではない方の端点を $f(v)$ で表すと、f は S から $N(S)$ への写像であり、またマッチングの定義より f は単射である。よって確かに $|S| \leq |N(S)|$ が成り立つ。

【2 ⇒ 1】二部グラフの定義より、G における最大のマッチング M の要素数は $|A|$ 以下

である。ここで $|M| = |A|$ が成り立てばよいので、$|M| < |A|$ であると仮定して矛盾を導く。定理 6.1 より、G の頂点被覆 U で $|U| < |A|$ となるものが存在する。$A' := U \cap A$、$B' := U \cap B$ とすると、$|U| = |A'| + |B'| < |A|$ であるから $|B'| < |A \setminus A'|$ である。一方で U は頂点被覆であるから $N(A \setminus A') \subseteq B'$ となり、したがって $|N(A \setminus A')| \leq |B'|$ である。よって $|N(A \setminus A')| < |A \setminus A'|$ となるが、これは条件 2 と矛盾する。以上より主張が成り立つ。 □

定義 6.4. 木 T とその頂点 r の組 (T, r) を**根付き木**（rooted tree）といい、r をその**根**（root）という。

根付き木が与えられると、その頂点集合に自然な半順序構造が定まる。以降ではそのことを説明する。

補題 6.1. 木 T の 2 頂点 x, y について、x と y を結ぶ単純な道がただ一つ存在する。

証明. まず、木の定義より T は連結であるから、x と y を結ぶ道が存在し、そのような長さ最短の道は単純である。あとは、x と y を結ぶ単純な道 $P_1 := z_0 z_1 \cdots z_n$、$P_2 := w_0 w_1 \cdots w_m$（$z_0 = w_0 = x$、$z_n = w_m = y$）について、それらが異なると仮定して矛盾を導けばよい。対称性より $n \leq m$ として差し支えない。

$z_0 = w_0$ より、$z_k = w_k$ を満たす最大の添字 k が存在する。ここで $P_1 \neq P_2$ であり、また P_2 は単純であるから $i < m$ のとき $w_i \neq y$ である。このことから $k < n \leq m$ であり、k の定義より $z_{k+1} \neq w_{k+1}$ である。$v := z_k = w_k$ とおき、非負整数の組 $(\ell_1, \ell_2) \neq (0, 0)$ で $z_{k+\ell_1} = w_{k+\ell_2}$ を満たすもののうち $\ell_1 + \ell_2$ が最小のものをとる（$z_n = w_m$ よりそのような組は確かに存在する）。$u := z_{k+\ell_1} = w_{k+\ell_2}$ とおくと、$z_k z_{k+1} \cdots z_{k+\ell_1}$ と $w_k w_{k+1} \cdots w_{k+\ell_2}$ はともに v から u への単純な道であり、$\ell_1 + \ell_2$ の最小性より、両者には始点 v と終点 u 以外に共通の頂点が存在しない。すると $v z_{k+1} \cdots z_{k+\ell_1 - 1} u w_{k+\ell_2 - 1} \cdots w_{k+1} v$ は T の単純閉路となるが、これは T が木であることと矛盾する。以上より主張が成り立つ。 □

命題 6.1. (T, r) を根付き木とする。T の 2 頂点 x, y について、T における x から y への単純な道を $P_{x,y}$ で表す。このとき、頂点 x, y についての関係 $x \preceq y$ を「$P_{r,y}$ が x を含む」ことと定めると、$\preceq$ は T の頂点集合 $V(T)$ 上の半順序である。

証明. 反射律について：$P_{r,x}$ は定義から x を含むので $x \preceq x$ である。

反対称律について：$x \preceq y$ かつ $y \preceq x$ とする。$x \preceq y$ より $P_{r,y}$ は x を含み、$P_{r,y}$ の r から x までの部分 P' が $P_{r,x}$ となる。$y \preceq x$ よりこの $P_{r,x} = P'$ は y を含むが、そうなるのは $x = y$ の場合に限られる。よって $x = y$ である。

推移律について：$x \preceq y$、$y \preceq z$ とする。$y \preceq z$ より $P_{r,z}$ は y を含み、$P_{r,z}$ の r から y までの部分が $P_{r,y}$ となる。$x \preceq y$ よりこの $P_{r,y}$ が x を含むので、元々の $P_{r,z}$ も x を含む。よって $x \preceq z$ である。以上より主張が成り立つ。 □

定義 6.5. 単純無向グラフ G において、G のどの 2 頂点についてもそれらを結ぶ辺が存在するとき、G を**完全グラフ**（complete graph）という。n 頂点からなる完全グラフを K_n で表す。

完全グラフにおける全域木の個数は以下のように決定される。

定理 6.3. $n \geq 2$ のとき、K_n の全域木の個数は n^{n-2} である。

以降では定理 6.3 について全単射による証明を与える。頂点集合 $V = \{a_1, \dots, a_n\} \subseteq \mathbb{Z}$ ($n \geq 2$) 上の完全グラフの全域木全体の集合を $\mathcal{T}[V]$ とおき、$T \in \mathcal{T}[V]$ について、T の端点（次数 1 の頂点）で $\mathbb{Z}$ の元として最小のものを $v(T)$ とおく。また、$s = (s_1, \dots, s_{n-2}) \in V^{n-2}$ について、$V \setminus \{s_1, \dots, s_{n-2}\}$ の最小元を $w_V(s)$ とおく。写像 $f_V \colon \mathcal{T}[V] \to V^{n-2}$ と $g_V \colon V^{n-2} \to \mathcal{T}[V]$ を以下のように $n \geq 2$ について再帰的に定める（$n = 2$ の場合には、$\mathcal{T}[V]$ の要素は V 上の完全グラフ自体のみ、V^{n-2} の要素は空文字列のみであるため、対応関係は自明に定まる）：

- $T \in \mathcal{T}[V]$ のとき、T で $v(T)$ に隣接する唯一の頂点を $s_1(T)$ として、$s_1(T)$ の後ろに列 $f_{V \setminus \{v(T)\}}(T \setminus \{v(T)\})$ をつなげてできる列を $f_V(T)$ とする。ここでグラフ G とその頂点集合 $V(G)$ の部分集合 S について、G から S を取り除いてできるグラフ、より正確には頂点集合 $V(G) \setminus S$ をもつ誘導部分グラフを $G \setminus S$ で表している。
- $s = (s_1, \dots, s_{n-2}) \in V^{n-2}$ のとき、木 $g_{V \setminus \{w_V(s)\}}(s_2, \dots, s_{n-2})$ の頂点 s_1 に新しい頂点 $w_V(s)$ をつなげてできる木を $g_V(s)$ とする。（定義より $w_V(s) \notin \{s_1, \dots, s_{n-2}\}$ であるから $s_1 \in V \setminus \{w_V(s)\}$ が成り立つことを注意しておく。）

このとき $f_V \circ g_V$ と $g_V \circ f_V$ がともに恒等写像であることを示せば、f_V が全単射でありしたがって $|\mathcal{T}[V]| = |V^{n-2}| = n^{n-2}$ が成り立つことが示され、定理 6.3 の主張が導かれる。$n = 2$ の場合にはこの主張は明らかであるため、以降では n がより小さい場合にこの主張が成り立っていると仮定して現在の $n \geq 3$ における主張を示す。

補題 6.2. 上の状況において、$T \in \mathcal{T}[V]$、$f_V(T) = (s_1, \dots, s_{n-2})$ とすると、$\{s_1, \dots, s_{n-2}\}$ は T の次数 2 以上の頂点の集合と一致し、$v(T) = w_V(f_V(T))$ が成り立つ。

証明. もしある s_i が T における端点であるとすると、f_V の定義より、s_i が $f_V(T)$ に追加される段階での木 T' における端点 $v(T')$ が s_i と隣接していたことになる。すると、s_i

は T' において次数 1 以下の点であるため、木の連結性より T' は s_i と $v(T')$ およびそれらを結ぶ辺だけからなるグラフとなる。一方で f_V の定義より T' の頂点数は 3 以上であるから、これは矛盾である。よって s_i たちはどれも次数 2 以上をもつ。

逆に、v を T の次数 2 以上の点とし、u_1, u_2 を v と隣接する相異なる点とする。このとき、f_V の再帰的な構成において木の端点が順に消去されていく過程で、最終的に木の頂点が 2 個になるまでの間に u_1 または u_2 のいずれかが必ず消去される（u_1 と u_2 がともに残っている間は v は端点にならないので、v が先に消去されることはない）。そして u_i ($i \in \{1,2\}$) が消去される段階の木 T' について $v(T') = u_i$ であり、したがって u_i と隣接している v がその時点で列 $f_V(T)$ に追加される。よって v は列 $f_V(T)$ に現れる。以上より主張の前半が成り立つ。主張の後半は、主張の前半および $v(T)$ と $w_V(s)$ の定義より導かれる。 □

補題 6.3. 上の状況において、$s = (s_1, \ldots, s_{n-2}) \in V^{n-2}$ のとき $v(g_V(s)) = w_V(s)$ が成り立つ。

証明. $g_V(s)$ の端点全体の集合を X、$g_{V \setminus \{w_V(s)\}}(s_2, \ldots, s_{n-2})$ の端点全体の集合を Y で表す。g_V の再帰的構成より

$$X = \{w_V(s)\} \sqcup (Y \setminus \{s_1\})$$

が成り立つ。ここで前述の仮定より

$$f_{V \setminus \{w_V(s)\}}(g_{V \setminus \{w_V(s)\}}(s_2, \ldots, s_{n-2})) = \{s_2, \ldots, s_{n-2}\}$$

であるため、補題 6.2 より

$$Y = (V \setminus \{w_V(s)\}) \setminus \{s_2, \ldots, s_{n-2}\}$$

である。このことから、$u \in Y \setminus \{s_1\}$ とすると u は $V \setminus \{s_1, \ldots, s_{n-2}\}$ の元で $w_V(s)$ と異なるものであり、$w_V(s)$ の定義より $w_V(s) < u$ となる。よって $v(g_V(s)) = w_V(s)$ となり主張が成り立つ。 □

$T \in \mathcal{T}[V]$、$f_V(T) = (s_1, \ldots, s_{n-2})$ とする。定義より $g_V(f_V(T))$ は、$V \setminus \{s_1, \ldots, s_{n-2}\}$ の最小の元 $w = w_V(f_V(T))$ を $g_{V \setminus \{w\}}(s_2, \ldots, s_{n-2})$ の点 s_1 につなげたグラフである。補題 6.2 より $w = v(T)$ であり、f_V の再帰的構成と前述の仮定より

$$g_{V \setminus \{w\}}(s_2, \ldots, s_{n-2}) = g_{V \setminus \{w\}}(f_{V \setminus \{w\}}(T \setminus \{w\})) = T \setminus \{w\} = T \setminus \{v(T)\}$$

となる。このことから $g_V(f_V(T))$ は $T \setminus \{v(T)\}$ の点 s_1 に $v(T)$ をつなげたグラフであり、f_V の構成よりこれは T 自体に等しい。よって $g_V(f_V(T)) = T$ となる。以上より $g_V \circ f_V = \mathrm{id}$ が成り立つ。

逆に、$s = (s_1, \dots, s_{n-2}) \in V^{n-2}$、$T := g_V(s)$ とする。T で点 $v(T)$ に隣接する唯一の点を s'_1 とすると、定義より $f_V(T)$ は s'_1 の後ろに $f_{V \setminus \{v(T)\}}(T \setminus \{v(T)\})$ をつなげた列である。補題 6.3 より $v(T) = w_V(s)$ であり、g_V の構成より $s'_1 = s_1$、$g_V(s) \setminus \{w_V(s)\} = g_{V \setminus \{w_V(s)\}}(s_2, \dots, s_{n-2})$ となる。これと前述の仮定より

$$f_{V \setminus \{v(T)\}}(g_V(s) \setminus \{v(T)\}) = f_{V \setminus \{w_V(s)\}}(g_{V \setminus \{w_V(s)\}}(s_2, \dots, s_{n-2})) = (s_2, \dots, s_{n-2})$$

となり、

$$f_V(g_V(s)) = f_V(T) = (s'_1, s_2, \dots, s_{n-2}) = (s_1, s_2, \dots, s_{n-2}) = s$$

となる。以上より $f_V \circ g_V = \mathrm{id}$ が成り立つ。こうして定理 6.3 が証明された。

演習問題

■問題 1.　有限無向グラフ $G = (V, E)$ が loop をもたないとき、$\sum_{v \in V} \deg(v) = 2|E|$ が成り立つことを証明せよ。
（ヒント：数え上げの手法を用いて証明できる。）

■問題 2.　2 頂点以上をもつ有限な木には次数 1 の頂点が常に存在することを証明せよ。
（コメント：無限な木においては反例が存在する。例えば、整数全体を頂点集合とし、隣り合う整数を辺で結んだグラフを考えればよい。）

■問題 3.　頂点集合が空でない有限な木 $G = (V, E)$ において、$|E| = |V| - 1$ が成り立つことを証明せよ。
（ヒント：一つ前の演習問題と数学的帰納法を用いる。）

■問題 4.　頂点集合が空でない連結な無向グラフには常に全域木が存在することを証明せよ。
（ヒント：頂点集合が無限集合である場合には Zorn の補題を用いる。）

7 Ramsey 理論

定義 7.1. 単純無向グラフ $G = (V, E)$ の**補グラフ**（complement graph）$\overline{G} = (V', E')$ を、$V' := V$ および

$$E' := \{\{x, y\} \mid x, y \in V, x \neq y, \{x, y\} \notin E\}$$

によって定める。

例えば、r 頂点の完全グラフ K_r の補グラフ $\overline{K_r}$ は、r 頂点からなる辺を一つももたないグラフである。

定義 7.2. 有限無向グラフの誘導部分グラフで、ある r について K_r の形であるものをそのグラフの**クリーク**（clique）といい、ある r について $\overline{K_r}$ の形であるものをそのグラフの**独立集合**（independent set）という。

グラフ理論において、「充分に大きなグラフはある種の特殊な構造を含む」という形の定理が多く研究されている。以降で紹介する性質はその一例である。

定理 7.1. $r \geq 2$ を整数とすると、頂点数が 2^{2r-3} 以上のどの単純無向グラフ $G = (V, E)$ も、r 頂点のクリークまたは r 頂点の独立集合を含む。

証明. $|V| = 2^{2r-3}$ の場合に証明すれば充分である。$V_1 := V$、$I, J := \emptyset$ とおき、$v_1 \in V_1$ をとる。集合 I と J を更新しつつ、$i = 2, \dots, 2r-2$ について $|V_i| = 2^{2r-2-i}$ を満たす $V_i \subseteq V_{i-1}$ と $v_i \in V_i$ を以下のように再帰的に選ぶ（$i = 1$ の場合にも $|V_1| = 2^{2r-2-1}$ および $v_1 \in V_1$ が成り立つことを注意しておく）：

- V_{i-1} には v_{i-1} 以外に $2^{2r-2-(i-1)} - 1$ 個の点が属しているので、以下のいずれかが成り立つ。
  - V_{i-1} の点のうち $2^{2r-3-(i-1)} = 2^{2r-2-i}$ 点以上が v_{i-1} と隣接している。
  - V_{i-1} の点のうち $2^{2r-3-(i-1)} = 2^{2r-2-i}$ 点以上が v_{i-1} と隣接していない。

  前者のときは v_{i-1} と隣接している V_{i-1} の点を 2^{2r-2-i} 個とって V_i として、I に $i-1$ を追加して、$v_i \in V_i$ をとる。後者のときは v_{i-1} と隣接していない V_{i-1} の点を 2^{2r-2-i} 個とって V_i として、J に $i-1$ を追加して、$v_i \in V_i$ をとる。

上記の構成より、$I \cup J = \{1, \dots, 2r-3\}$、$I \cap J = \emptyset$ となるので、$|I| \geq r-1$ または $|J| \geq r-1$ が成り立つ。$|I| \geq r-1$ のときには、$\{v_i \mid i \in I\} \cup \{v_{2r-2}\}$ から r 点を選び出すとそれらがサイズ r のクリークをなす。一方、$|J| \geq r-1$ のときには、

$\{v_i \mid i \in J\} \cup \{v_{2r-2}\}$ から r 点を選び出すとそれらがサイズ r の独立集合をなす。以上より主張が成り立つ。 □

定義 7.3. $r \geq 2$ を整数とする。「頂点数が n のどの単純無向グラフもサイズ r のクリークまたはサイズ r の独立集合を含む」という性質をもつ n の最小値を $R(r)$ で表し、**Ramsey 数**と呼ぶ。

定理 7.1 より Ramsey 数 $R(r)$ は有限の値として確定し、$R(r) \leq 2^{2r-3}$ が成り立つ。例えば $r = 3$ について $R(3) \leq 2^3 = 8$ である（演習問題を参照)。

Ramsey 数の下界の一つを与えるために、以下のような確率論的手法を用いる。n 頂点の集合上の異なる 2 点 x, y について、x と y が独立に確率 p で辺で結ばれる、として定まる単純無向グラフの確率変数を $\mathcal{G}(n,p)$ で表す。

補題 7.1. $n \geq k \geq 2$ のとき、上の $\mathcal{G}(n,p)$ について

$$p_1 := \Pr[\mathcal{G}(n,p) \text{ がサイズ } k \text{ の独立集合をもつ}] \leq \binom{n}{k}(1-p)^{\binom{k}{2}} \ ,$$

$$p_2 := \Pr[\mathcal{G}(n,p) \text{ がサイズ } k \text{ のクリークをもつ}] \leq \binom{n}{k}p^{\binom{k}{2}}$$

が成り立つ。

証明. V を $\mathcal{G}(n,p)$ の頂点集合とする。$S \subseteq V$ について、S のどの 2 点間にも辺が結ばれない確率は $(1-p)^{\binom{|S|}{2}}$ であり、S のすべての 2 点間に辺が結ばれる確率は $p^{\binom{|S|}{2}}$ である。このことから

$$p_1 \leq \sum_{S \subseteq V\,;\,|S|=k} \Pr[S \text{ が独立集合となる}] = \sum_{S \subseteq V\,;\,|S|=k} (1-p)^{\binom{k}{2}} = \binom{n}{k}(1-p)^{\binom{k}{2}} \ ,$$

$$p_2 \leq \sum_{S \subseteq V\,;\,|S|=k} \Pr[S \text{ がクリークとなる}] = \sum_{S \subseteq V\,;\,|S|=k} p^{\binom{k}{2}} = \binom{n}{k}p^{\binom{k}{2}}$$

となり、主張が成り立つ。 □

定理 7.2. $r \geq 3$ のとき $R(r) > 2^{r/2}$ が成り立つ。

証明. $r = 3$ については、$R(3) = 6$ である（演習問題を参照）から $R(3) > 2^{3/2}$ が成り立

つ。以降では $r \geq 4$ とする。$n \leq 2^{r/2}$ のとき、補題 7.1 より

$$\begin{aligned}
&\Pr[\mathcal{G}(n,1/2) \text{ がサイズ } r \text{ のクリークをもつ}] \\
&\leq \binom{n}{r}\left(\frac{1}{2}\right)^{\binom{r}{2}} \\
&= \frac{n(n-1)\cdots(n-r+1)}{r!}2^{-r(r-1)/2} \\
&< \frac{n^r}{2^r}2^{-r(r-1)/2}
\end{aligned}$$

（$r \geq 4$ より $r! > 2^r$ であることを用いた）

$$\leq \frac{(2^{r/2})^r}{2^{r(r-1)/2+r}} = \frac{2^{r^2/2}}{2^{r^2/2+r/2}} = \frac{1}{2^{r/2}} < \frac{1}{2}$$

となり、同様に $\Pr[\mathcal{G}(n,1/2)$ がサイズ r の独立集合をもつ$] < 1/2$ である。このことから、$\mathcal{G}(n,1/2)$ がサイズ r のクリークまたはサイズ r の独立集合をもつ確率は $1/2+1/2=1$ 未満であり、$\mathcal{G}(n,1/2)$ がサイズ r のクリークもサイズ r の独立集合ももたない確率は正の値である。したがって、$n \leq 2^{r/2}$ のときには、n 頂点からなる単純無向グラフでサイズ r のクリークもサイズ r の独立集合ももたないものが存在する。よって $R(r) > 2^{r/2}$ となり主張が成り立つ。 □

「充分に大きなグラフはある種の特殊な構造を含む」という形の命題をもう一つ紹介する。頂点集合の分割 $V = A \sqcup B$ をもつ二部グラフで、$|A| = n$、$|B| = m$、かつ A の頂点と B の頂点が常に辺で結ばれているものを $K_{n,m}$ で表し、**完全二部グラフ**と呼ぶ。

命題 7.1. $r \geq 2$ を整数とすると、以下を満たす整数 N が存在する：頂点数が N 以上のどの連結な単純無向グラフ $G = (V,E)$ も、K_r、$K_{1,r}$、または長さ（辺の数）r の単純道 P_r を誘導部分グラフにもつ。

証明. まず、G のある頂点 v が次数 $R(r)$ 以上をもつ場合を考える。v と隣接する頂点たちのなす G の誘導部分グラフ G' は $R(r)$ 個以上の頂点をもつので、$R(r)$ の定義より G' は K_r または $\overline{K_r}$ を誘導部分グラフにもつ。前者の場合にはその K_r が主張の条件を満たし、後者の場合にはその $\overline{K_r}$ と v をあわせた誘導部分グラフが $K_{1,r}$ となる。よってこの場合には主張が成り立つ。

以降では残る可能性として、G のどの頂点も次数が $R(r)-1$ 以下である場合を考える。ある頂点 v と集合 $V_0 := \{v\}$ から出発して、集合 V_i（$1 \leq i \leq r-1$）を

$$V_i := \left\{ u \in V \setminus \bigcup_{j<i} V_j \mid u \text{ は } V_{i-1} \text{ のある頂点と隣接する} \right\}$$

で再帰的に定める。このとき、上記の次数の条件により $|V_i| \leq (R(r)-1)|V_{i-1}|$ が成り立つので、$|V_i| \leq (R(r)-1)^i$ となる。よって

$$\left|\bigcup_{i=0}^{r-1} V_i\right| \leq \sum_{i=0}^{r-1} (R(r)-1)^i$$

となる。この右辺（これは G によらず定まる）を M とおくと、$|V| \geq M+1$ のときには、どの V_i にも属さない $u \in V$ がとれる。G は連結であるから、u と v を結ぶ単純道 P が存在し、u の選び方から P の長さは r 以上である。すると、P の先頭 $r+1$ 頂点のなす誘導部分グラフが P_r となり、主張の条件が成り立つ。以上より主張が成り立つ。 □

演習問題

■問題 1. Ramsey 数について $R(3) = 6$ であることを証明せよ。

8　グラフの隣接行列

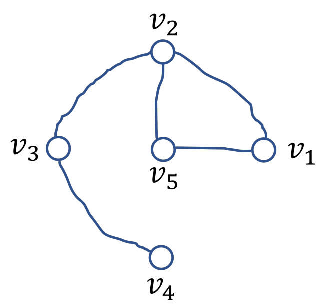
この節では $G=(V,E)$ を有限単純無向グラフとする。

定義 8.1. V の元を $\{v_1,\dots,v_n\}$ と並べるとき、グラフ G の**隣接行列**（adjacency matrix）$A=A(G)=(a_{ij})_{i,j=1}^n$ を

$$a_{ij} := \begin{cases} 1 & (\{v_i,v_j\}\in E \text{ のとき}) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

で定める。

グラフの隣接行列の例を図 7 に挙げる。なお、定義より隣接行列 A は対称行列であり、A の i 行目の成分の総和は v_i の次数 $\deg(v_i)$ に等しいことを注意しておく。



$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

図 7　グラフの隣接行列の例

グラフの隣接行列が与えられると元々のグラフの形を復元できるので、原理的にはグラフに関する情報はすべて隣接行列から導き出せるはずである（もちろん、その情報を簡単に導き出せるとは限らない）。例えば以下の性質が成り立つ。

命題 8.1. A を G の隣接行列とすると、A^k の (i,j)-成分は、G における v_i から v_j への長さ k の道の本数に等しい。

証明. 行列の積の定義より、A^k の (i,j)-成分は

$$\sum_{\substack{\ell_0,\ell_1,\dots,\ell_k \\ \ell_0=i,\,\ell_k=j}} a_{\ell_0,\ell_1}a_{\ell_1,\ell_2}\cdots a_{\ell_{k-1},\ell_k}$$

と表せる。この和に現れる $a_{\ell_0,\ell_1}a_{\ell_1,\ell_2}\cdots a_{\ell_{k-1},\ell_k}$ は、$\{v_{\ell_0},v_{\ell_1}\},\{v_{\ell_1},v_{\ell_2}\},\dots,\{v_{\ell_{k-1}},v_{\ell_k}\}$ がすべて辺であるとき、すなわち $v_{\ell_0}v_{\ell_1}\cdots v_{\ell_{k-1}}v_{\ell_k}$ が道であるときに 1 となり、それ以

外のときは 0 となる。したがって、和の条件 $v_{\ell_0} = v_i$ と $v_{\ell_k} = v_j$ に注意すると、上の和は v_i から v_j への長さ k の道の本数に等しい。よって主張が成り立つ。 □

系 8.1. A を G の隣接行列とすると、A^2 の (i,i)-成分は $\deg(v_i)$ に等しい。

証明. G は単純グラフであるから、v_i から v_i への長さ 2 の道は、v_i と隣接する頂点 u について $v_i u v_i$ という形のものに限られる。このことと命題 8.1 より主張が成り立つ。 □

定義 8.2. 定義 8.1 の状況で、対角成分に $\deg(v_1), \dots, \deg(v_n)$ を並べてそれ以外の成分をすべて 0 にした $n \times n$ 行列を D としたとき、$D - A$ を G の **Laplacian 行列**という。

命題 8.2. G の辺を $E = \{e_1, \dots, e_m\}$ と番号付けした上で、各辺に何らかの向きを定める。すなわち各辺の端点のどちらかを「始点」、もう一方を「終点」と定める。そして、$n \times m$ 行列 $B = (B_{ij})_{i,j}$ を

$$b_{ij} = \begin{cases} 1 & (v_i \text{ が } e_j \text{ の始点のとき}) \\ -1 & (v_i \text{ が } e_j \text{ の終点のとき}) \\ 0 & (\text{それ以外のとき}) \end{cases}$$

で定める。このとき $BB^{\mathrm{T}} = D - A$ が成り立つ。特に $D - A$ は半正定値対称行列である。

証明. まず、BB^{T} の (i,i)-成分は

$$\sum_j b_{ij} b_{ij} = \sum_j {b_{ij}}^2$$

と表せる。この和に現れる項について、v_i が e_j の端点であれば（辺の向きにかかわらず）${b_{ij}}^2 = 1$ であり、そうでないとき ${b_{ij}}^2 = 0$ である。よってこの項は v_i と接続する辺の本数の分だけ 1 となるので、上の和は $\deg(v_i)$ に等しい。G が単純グラフであることから A の対角成分は 0 であり、したがって上の和は $D - A$ の (i,i)-成分に等しい。

次に $i \neq j$ のとき、BB^{T} の (i,j)-成分は

$$\sum_k b_{ik} b_{jk}$$

と表せる。この和に現れる項について、e_k が v_i から v_j への辺であれば $b_{ik} b_{jk} = 1 \cdot (-1) = -1$、$e_k$ が v_j から v_i への辺であれば $b_{ik} b_{jk} = (-1) \cdot 1 = -1$、それ以外のとき $b_{ik} b_{jk} = 0$ である。すると、G は単純グラフであるから、上の和は v_i と v_j が隣接するとき -1 であり、それ以外のとき 0 である。この値は $D - A$ の (i,j)-成分に等しい。以上より主張が成り立つ。 □

グラフの全域木の個数について以下が成り立つ。

定理 8.1 (Kirchhoff の行列木定理（matrix-tree theorem）)**.** G の *Laplacian* 行列 $D-A$ の (i,i)-余因子は G の全域木の総数に等しい。

証明. まず、頂点の並べ方について、v_i を一番後ろに移動させる並べ替えを行った後の Laplacian 行列の (n,n)-余因子はもとの Laplacian 行列の (i,i)-余因子と一致する。したがって、はじめから $i=n$ であるとして差し支えない。

命題 8.2 のように $D-A=BB^{\mathrm{T}}$ と表しておく。B の最後の行を削除した行列を $B'=(b_{ij})_{1\le i\le n-1\,,\,1\le j\le m}$ とすると、$D-A$ の (n,n)-余因子は $\det(B'B'^{\mathrm{T}})$ と表せる。$B'B'^{\mathrm{T}}$ の (i,j)-成分が $\sum_{k=1}^{m} b_{ik}b_{jk}$ であることを踏まえると、$D-A$ の (n,n)-余因子は

$$\begin{aligned}&\sum_{\sigma\in S_{n-1}}\mathrm{sgn}(\sigma)\sum_{k_1,\dots,k_{n-1}\in\{1,\dots,m\}} b_{1,k_1}b_{\sigma(1),k_1}b_{2,k_2}b_{\sigma(2),k_2}\cdots b_{n-1,k_{n-1}}b_{\sigma(n-1),k_{n-1}}\\ &=\sum_{k_1,\dots,k_{n-1}\in\{1,\dots,m\}}\sum_{\sigma\in S_{n-1}}\mathrm{sgn}(\sigma)b_{1,k_1}b_{\sigma(1),k_1}b_{2,k_2}b_{\sigma(2),k_2}\cdots b_{n-1,k_{n-1}}b_{\sigma(n-1),k_{n-1}}\end{aligned} \tag{3}$$

となる。項 $b_{1,k_1}b_{\sigma(1),k_1}b_{2,k_2}b_{\sigma(2),k_2}\cdots b_{n-1,k_{n-1}}b_{\sigma(n-1),k_{n-1}}$ を P_σ で表す。P_σ は、$i\in\{1,\dots,n-1\}$ の各々について v_i と $v_{\sigma(i)}$ が e_{k_i} の端点であるときに ±1 となり、そうでないとき 0 となることを注意しておく。以降では $P_\sigma\ne0$ となる場合に着目する。

ある $i\ne j$ について $k_i=k_j$ であるとする。このとき、e_{k_i} が v_i と v_j を結ぶ辺でなければ $P_\sigma=0$ となるので、以降では e_{k_i} が v_i と v_j を結ぶ辺である場合を考える。このとき、$P_\sigma\ne0$ となるためには $\sigma(i)\in\{i,j\}$ および $\sigma(j)\in\{i,j\}$ である必要があり、したがって $(\sigma(i),\sigma(j))=(i,j)$ または $(\sigma(i),\sigma(j))=(j,i)$ である必要がある。前者の条件を満たす σ と後者の条件を満たす σ は対応 $\sigma\mapsto(i,j)\sigma$ によって一対一に対応し、このとき $b_{i,k_i}b_{i,k_i}b_{j,k_i}b_{j,k_i}=b_{i,k_i}b_{j,k_i}b_{j,k_i}b_{i,k_i}$ であることから $P_{(i,j)\sigma}=P_\sigma$ である。これと $\mathrm{sgn}((i,j)\sigma)=-\mathrm{sgn}(\sigma)$ より、和 $\sum_{\sigma\in S_{n-1}}\mathrm{sgn}(\sigma)P_\sigma$ において σ に対応する項と $(i,j)\sigma$ に対応する項がちょうど打ち消し合い、上記の和は 0 となる。以上より、(3) 式の右辺において、k_i たちがすべて異なる場合を除き和の項が常に 0 となる。そこで以降では k_i たちがすべて異なる場合のみを考える。

$i_1,i_2,\dots,i_\ell$ がすべて異なるとして、辺 $e_{k_{i_1}},e_{k_{i_2}},\dots,e_{k_{i_\ell}}$ がこの順番に単純閉路をなすとする（特に $\ell\ge3$ である)。ここでこの単純閉路の辺は、$e_{k_{i_1}}$ の端点 v_{i_1} が（$e_{k_{i_2}}$ ではなく）$e_{k_{i_\ell}}$ の端点でもあるように並べているものとする。このとき、$j=\ell-1,\dots,2,1$ について、v_{i_j} が $e_{k_{i_j}}$ と $e_{k_{i_{j+1}}}$ の共通の端点であることが再帰的に示される。したがって上記の単純閉路は $v_{i_1}e_{k_{i_1}}v_{i_2}e_{k_{i_2}}\cdots v_{i_\ell}e_{k_{i_\ell}}v_{i_1}$ という形である。

$$P'_\sigma:=b_{i_1,k_{i_1}}b_{\sigma(i_1),k_{i_1}}b_{i_2,k_{i_2}}b_{\sigma(i_2),k_{i_2}}\cdots b_{i_\ell,k_{i_\ell}}b_{\sigma(i_\ell),k_{i_\ell}}\,,\ P''_\sigma:=P_\sigma/P'_\sigma$$

とする。また、各 j について $v_{\sigma(i_j)}$ も $e_{k_{i_j}}$ の端点であることを注意しておく。特に $\sigma(i_1) \in \{i_1, i_2\}$ である。ここで、

- $\sigma(i_1) = i_1$ のとき、$j = \ell, \ell-1, \dots, 2$ について $\sigma(i_j) = i_j$ であることを再帰的に示す。$j = \ell$ については、$v_{\sigma(i_\ell)}$ が $e_{k_{i_\ell}}$ の端点であることから $\sigma(i_\ell) \in \{i_\ell, i_1\}$ であり、$\sigma(i_\ell) \neq \sigma(i_1) = i_1$ より確かに $\sigma(i_\ell) = i_\ell$ である。また $j+1$ までで主張が成り立つとき、$v_{\sigma(i_j)}$ が $e_{k_{i_j}}$ の端点であることから $\sigma(i_j) \in \{i_j, i_{j+1}\}$ であり、$\sigma(i_j) \neq \sigma(i_{j+1}) = i_{j+1}$ より確かに $\sigma(i_j) = i_j$ である。
- $\sigma(i_1) = i_2$ のとき、$j = 1, 2, \dots, \ell$ について $\sigma(i_j) = i_{j+1}$（ただし $i_{\ell+1} := i_1$）であることを再帰的に示す。$j = 1$ については既に成り立っている。また $j-1$ までで主張が成り立つとき、$v_{\sigma(i_j)}$ が $e_{k_{i_j}}$ の端点であることから $\sigma(i_j) \in \{i_j, i_{j+1}\}$ であり、$\sigma(i_j) \neq \sigma(i_{j-1}) = i_j$ より確かに $\sigma(i_j) = i_{j+1}$ である。

$\tau := (i_1, i_2, \dots, i_\ell) \in S_n$ とおくと、前者の σ と後者の σ は対応 $\sigma \mapsto \tau\sigma$ によって一対一に対応し、$P''_\sigma = P''_{\tau\sigma}$ である。前者の σ については $P'_\sigma = {b_{i_1,k_{i_1}}}^2 \cdot {b_{i_2,k_{i_2}}}^2 \cdots {b_{i_\ell,k_{i_\ell}}}^2 = 1$、後者の $\tau\sigma$ については

$$
\begin{aligned}
P'_{\tau\sigma} &= (b_{i_1,k_{i_1}} b_{i_2,k_{i_1}}) \cdot (b_{i_2,k_{i_2}} b_{i_3,k_{i_2}}) \cdots (b_{i_\ell,k_{i_\ell}} b_{i_1,k_{i_\ell}}) \\
&= (-1) \cdot (-1) \cdots (-1) = (-1)^\ell
\end{aligned}
$$

および $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma) = (-1)^{\ell-1}\mathrm{sgn}(\sigma)$ が成り立つ。このことから、和 $\displaystyle\sum_{\sigma \in S_{n-1}} \mathrm{sgn}(\sigma) P_\sigma$ において σ に対応する項と $\tau\sigma$ に対応する項がちょうど打ち消し合い、上記の和は 0 となる。

以上より、部分グラフ $G' := (V, \{e_{k_1}, \dots, e_{k_{n-1}}\})$ が単純閉路をもたず、かつ、成分がすべて異なる列 $(k_1, \dots, k_{n-1})$ 全体の集合を $\mathcal{G}$ とすると、(3) 式の右辺は

$$
\sum_{(k_1,\dots,k_{n-1}) \in \mathcal{G}} \sum_{\sigma \in S_{n-1}} \mathrm{sgn}(\sigma) P_\sigma \tag{4}
$$

となる。$|V| = n$ より、G' が単純閉路をもたないという条件は G' が G の全域木であることと等価である。ここで、G' を G の全域木としたとき、$v \in V \setminus \{v_n\}$ について、G' における v_n から v への唯一の単純道が最後に通る辺を $\varphi(v)$ で表す。すると、$(k_1, \dots, k_{n-1}) \in \mathcal{G}$ かつ $P_\sigma \neq 0$ であるとき、$1 \leq i \leq n-1$ について $e_{k_i} = \varphi(v_i)$ かつ $\sigma(i) = i$ が成り立つことを、v_n から v_i への G' における単純道の長さに関する数学的帰納法で示す。

- G' において v_i が v_n と隣接しているとき、v_i と v_n を結ぶ辺を $e_{k_j} = \varphi(v_i)$ とすると、$P_\sigma \neq 0$ より v_j は e_{k_j} の端点である必要があり、$v_j \neq v_n$ より $v_j = v_i$ したがって $j = i$、$e_{k_i} = \varphi(v_i)$ となる。また、$P_\sigma \neq 0$ より $v_{\sigma(i)}$ も e_{k_i} の端点でなければならず、$v_{\sigma(i)} \neq v_n$ より $v_{\sigma(i)} = v_i$、$\sigma(i) = i$ である。

- それ以外のとき、G' における v_n から v_i への単純道が v_i の一つ前に通る頂点を v_j とすると、帰納法の仮定より $e_{k_j} = \varphi(v_j)$ かつ $\sigma(j) = j$ である。$\varphi(v_i) = e_{k_\ell}$ とすると e_{k_ℓ} は v_i と v_j を結ぶ辺である。$P_\sigma \neq 0$ より v_ℓ は e_{k_ℓ} の端点、すなわち v_i または v_j であるが、$v_i \neq v_j$ より $e_{k_\ell} = \varphi(v_i) \neq \varphi(v_j) = e_{k_j}$、したがって $\ell \neq j$ である。よって $v_\ell = v_i$、$\ell = i$、したがって $\varphi(v_i) = e_{k_i}$ が成り立つ。また、$P_\sigma \neq 0$ より $v_{\sigma(i)}$ も e_{k_i} の端点、すなわち v_i または v_j であるが、$i \neq j$ より $\sigma(i) \neq \sigma(j) = j$ であるため、$v_{\sigma(i)} = v_i$、$\sigma(i) = i$ である。

このことから、全域木 G' を固定したとき、$P_\sigma \neq 0$ を満たす $(k_1, \dots, k_{n-1})$ と σ の組は、各 i について $\varphi(v_i) = e_{k_i}$ かつ $\sigma(i) = i$ という条件によってただ一つに定まる。さらにこのとき、$\sigma = \mathsf{id}$ であるため、$\mathrm{sgn}(\sigma)P_\sigma = {b_{1,k_1}}^2 \cdots {b_{n-1,k_{n-1}}}^2 = 1$ となる。よって、(4) 式の値は、G の全域木 G' の個数分だけ 1 を足し合わせたもの、すなわち G の全域木の総数と一致する。以上より主張が成り立つ。 □

例 8.1. $n \geq 2$ のとき、$G = K_n$ の全域木の総数が n^{n-2} 個であることは定理 6.3 で既に述べたが、ここでは定理 8.1 を用いてこの事実を再確認する。K_n の Laplacian 行列は

$$\begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix} \qquad (n \text{ 次正方行列})$$

であり、その $(1,1)$-余因子は

$$\det \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix} \qquad (n-1 \text{ 次正方行列の行列式})$$

である。上記の行列に対して、「2 行目を 3 行目〜$n-1$ 行目から引く」および「2 行目の $n-1$ 倍を 1 行目に足す」行基本変形を行うことで、その行列式は

$$\det \begin{pmatrix} 0 & n^2-2n & -n & -n & \cdots & -n \\ -1 & n-1 & -1 & -1 & \cdots & -1 \\ 0 & -n & n & 0 & \cdots & 0 \\ 0 & -n & 0 & n & \cdots & 0 \\ \vdots & \vdots & & & \ddots & \vdots \\ 0 & -n & 0 & 0 & \cdots & n \end{pmatrix} = \det \begin{pmatrix} n^2-2n & -n & -n & \cdots & -n \\ -n & n & 0 & \cdots & 0 \\ -n & 0 & n & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ -n & 0 & 0 & \cdots & n \end{pmatrix}$$

（$n-2$ 次正方行列の行列式）となる。さらに 2 行目〜$n-2$ 行目を 1 行目に足すことで、

上記の行列式は（$n^2 - 2n - (n-3)n = n$ より）

$$\det\begin{pmatrix} n & 0 & 0 & \cdots & 0 \\ -n & n & 0 & \cdots & 0 \\ -n & 0 & n & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ -n & 0 & 0 & \cdots & n \end{pmatrix} = n^{n-2}$$

（最後の行列が下三角行列であることを用いた）となる。以上より主張が成り立つ。

どの頂点も次数が一定の値 d であるグラフを **d-正則グラフ**（d-regular graph）という。

定義 8.3. 部分集合 $S \subseteq V$ について、S の頂点と $V \setminus S$ の頂点とを結ぶ辺全体の集合を ∂S で表す。このとき

$$h(G) := \min\left\{\frac{|\partial S|}{|S|} : S \subseteq V\,,\, 0 < |S| \leq \frac{1}{2}|V|\right\}$$

を G の**拡大係数**（expansion constant）と呼ぶ。同一の d に対する d-正則グラフの族 $(G_i = (V_i, E_i))_{i \geq 1}$ が**エクスパンダー族**（expander family）であるとは、$\lim_{n\to\infty} |V_n| = \infty$ であり、かつ、ある正の実数が $\{h(G_n) \mid n = 1, 2, \dots\}$ の下界となることと定める。

グラフの拡大係数と隣接行列の関係をいくつか紹介する。

定義 8.4. G の隣接行列 A の固有値のうち（重複を込めて）k 番目に大きなものを $\lambda_k = \lambda_k(G)$ と書き、G の**第 k 固有値**と呼ぶ。また、$\lambda_1(G) - \lambda_2(G)$ を G の**スペクトルギャップ**（spectral gap）と呼ぶ。

グラフ G の第 k 固有値 λ_k は G の頂点の並べ方によらず定まることを注意しておく。なぜなら、頂点の並べ替えは隣接行列 A を $P^{-1}AP$（P はある置換行列）に変化させるが、この操作で固有値は変わらないからである。

補題 8.1. G が d-正則グラフであるとき、$\lambda_1(G) = d$ である。

証明. まず、G が d-正則であることから、すべての成分が 1 であるベクトル $\vec{1}$ について $A\vec{1} = d\vec{1}$ が成り立ち、したがって d は G の固有値である。一方、G が d-正則であることから $D = dI$（I は単位行列）であり、また命題 8.2 より $D - A$ は半正定値対称行列である。よって $dI - A$ の固有値はすべて非負実数であり、一方で $d - \lambda_1(G)$ は $dI - A$ の固有値であるから、$d - \lambda_1(G) \geq 0$ したがって $d \leq \lambda_1(G) \leq d$ が成り立つ。以上より主張が成り立つ。 □

証明は割愛するが、グラフの拡大係数とスペクトルギャップの関係について以下の事実が知られている。

定理 8.2 (Allon–Milman)**.** G が d-正則グラフである（したがって $\lambda_1(G) = d$ である）とき、

$$\frac{d - \lambda_2(G)}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2(G))}$$

が成り立つ。

連結グラフ G について、G の 2 頂点間を結ぶ最短道の長さの最大値 $\mathrm{diam}(G)$ を G の**直径**（diameter）と呼ぶ。証明は割愛するが、以下の事実が知られている。

定理 8.3 (Nilli)**.** G を連結な d-正則グラフとし、$\mathrm{diam}(G) \geq 2m + 2 \geq 4$ が成り立つとすると、

$$\lambda_2(G) > 2\sqrt{d-1} - \frac{2\sqrt{d-1} - 1}{m}$$

が成り立つ。

G が d-正則グラフであるとき、

$$\lambda(G) := \max\{|\lambda_j(G)| \colon \lambda_j(G) \neq \pm d\}$$

と定める。証明は割愛するが、連結な d-正則グラフ G について、G が 3 頂点以上をもつ二部グラフである場合には $\lambda(G) = \lambda_2(G)$ が成り立ち、また G が二部グラフでない場合には $2 \leq i \leq n$（n は G の頂点数）について $|\lambda_i(G)| < d$ であり、したがって $\lambda(G) = \max\{|\lambda_2(G)|, |\lambda_n(G)|\}$ が成り立つことが知られている。特に、いずれの場合にも $\lambda(G) \geq \lambda_2(G)$ である。さて、定理 8.3 を踏まえて、$\lambda(G)$ が「理論上ほぼ最小」の値をとる場合に G は Ramanujan グラフと呼ばれている。より正確には以下のように定義される。

定義 8.5. 連結な d-正則グラフ G について、$\lambda(G) \leq 2\sqrt{d-1}$ が成り立つとき、G を **Ramanujan グラフ**という。

本節の最後に、グラフ上のランダムウォークとグラフのスペクトルギャップの関係について述べる。G を n 頂点からなる、二部グラフではない連結な d-正則グラフとするとき、G 上のランダムウォークでは、G のある頂点から出発し、各ステップにおいて現在の頂点と隣接する G の頂点の一つに等確率（確率 $1/d$）で進む、という操作を繰り返す。このランダムウォークの極限分布および収束の速さについて考察する。G の頂点を $v_1, \ldots, v_n$ と番号付けて、出発点を頂点 v_1 とする。まず、k ステップ目までの手順では、v_1 を始点

とする長さ k の道がどれも等確率で現れることを注意しておく。ここで命題 8.1 より、v_1 から v_j までの長さ k の道の総数は A^k の $(1,j)$-成分と等しく、その値は ${e_1}^{\mathrm{T}}A^k e_j$ と表せる。ここで e_i は第 i 単位ベクトルを表す。このことから、すべての成分が 1 である n 次元ベクトルを $\vec{1}$ で表すとき、v_1 を始点とする長さ k の道の総数は ${e_1}^{\mathrm{T}}A^k\vec{1}$ となる。G は d-正則であるから、この値は ${e_1}^{\mathrm{T}}\cdot d^k\vec{1}=d^k$ に等しい。よって、k ステップ目に v_j へ辿り着く確率 $p_j=p_j^{\langle k\rangle}$ は

$$p_j=\frac{{e_1}^{\mathrm{T}}A^k e_j}{d^k}$$

となる。

ここで A は実対称行列であるから、直交行列によって対角化できる。すなわち、$\mathbb{R}^n$ の正規直交基底 $(u_1,\dots,u_n)$ で、各 i について $Au_i=\lambda_i(G)u_i$ を満たすものが存在する。このとき $A=\sum_{i=1}^{n}\lambda_i(G)u_i\cdot{u_i}^{\mathrm{T}}$ と表せて、$A^k=\sum_{i=1}^{n}\lambda_i(G)^k u_i\cdot{u_i}^{\mathrm{T}}$、したがって

$${e_1}^{\mathrm{T}}A^k e_j=\sum_{i=1}^{n}\lambda_i(G)^k\cdot{e_1}^{\mathrm{T}}u_i\cdot{u_i}^{\mathrm{T}}e_j$$

となる。G は d-正則であるから $\lambda_1(G)=d$ であり、$u_1=n^{-1/2}\vec{1}$ ととれる。よって

$${e_1}^{\mathrm{T}}A^k e_j=\frac{d^k}{n}+\sum_{i=2}^{n}\lambda_i(G)^k\cdot{e_1}^{\mathrm{T}}u_i\cdot{u_i}^{\mathrm{T}}e_j$$

となる。したがって

$$\left|p_j-\frac{1}{n}\right|\le\sum_{i=2}^{n}\frac{|\lambda_i(G)^k|}{d^k}\cdot|{e_1}^{\mathrm{T}}u_i|\cdot|{u_i}^{\mathrm{T}}e_j|$$

である。Cauchy–Schwarz の不等式より、上記の右辺は

$$\le\sum_{i=2}^{n}\frac{|\lambda_i(G)|^k}{d^k}\cdot||e_1||\cdot||u_i||\cdot||u_i||\cdot||e_j||=\sum_{i=2}^{n}\frac{|\lambda_i(G)|^k}{d^k}$$

となる。さらに G が二部グラフでないことから、前述の性質により $2\le i\le n$ について $|\lambda_i(G)|\le\max\{|\lambda_2(G)|,|\lambda_n(G)|\}=\lambda(G)$ が成り立つ。よって

$$\left|p_j-\frac{1}{n}\right|\le(n-1)\cdot\left(\frac{\lambda(G)}{d}\right)^k$$

となり、$0\le\lambda(G)<d$ であるから、$\lim_{k\to\infty}p_j=\dfrac{1}{n}$ が成り立つ。以上より、このランダムウォークの極限分布は G の頂点集合上の一様分布であり、また上記の評価式より、$\lambda(G)$

が小さい（すなわち、スペクトルギャップが大きい）ほど一様分布への収束が速くなることがわかる。

このように、$\lambda(G)$ が小さいグラフを用いると極限分布への収束の速いランダムウォークを実現することができる。こうした理由から、Ramanujan グラフは純粋なグラフ理論的な興味に留まらず応用上も重要な研究対象となっている。例えば、特殊な楕円曲線（超特異楕円曲線）とその間の同種写像と呼ばれる写像を用いて Ramanujan グラフを構成できることが知られており、その Ramanujan グラフ上のランダムウォークを応用した暗号学的ハッシュ関数の構成が提案されている。詳しくは [1] を参照されたい。

演習問題

■問題 1.　図 7 のグラフの Laplacian 行列を記し、このグラフが全域木を 3 個もつことを定理 8.1 を用いて確かめよ。また、このグラフの全域木をすべて挙げよ。

■問題 2.　完全二部グラフ $K_{n,m}$ の全域木の総数を計算せよ。

参考文献

[1] D. X. Charles, K. E. Lauter, E. Z. Goren, “Cryptographic Hash Functions from Expander Graphs”, Journal of Cryptology, vol.22, pp.93–113, 2009

[2] R. Diestel（著）、根上 生也、太田 克弘（訳）、『グラフ理論』、シュプリンガー・フェアラーク東京、2000 年

[3] 木本 一史、『レクチャー離散数学』、サイエンス社、2019 年

[4] K. Kunen (著)、藤田 博司 (訳)、『集合論　独立性証明への案内』、日本評論社、2008 年

[5] R. P. Stanley, “Enumerative Combinatorics”, Volume 1, Cambridge University Press, 1997

[6] R. P. Stanley, “Enumerative Combinatorics”, Volume 2, Cambridge University Press, 1999