代数学特論：数値半群と数値半群環

目次

イントロダクション

代数学とは代数方程式の解法の考察から現れた理論であり，演算を備えた集合である**代数系**を研究する学問である．例えば，以下のような代数系が良く考えられる．

- 半群，モノイド，群 $\cdots$ ある性質を満たす積または和を持つ集合
- 環，体 $\cdots$　ある性質を満たす積と和を持つ集合

これらの代数系は数学の様々な分野において自然に現れ，代数系の研究は数学全般において重要な役割を果たす．この講義では，数値半群と呼ばれる最も初等的な代数系を通して代数的な考え方を学ぶ．

数値半群の概念の元になるのは以下の問題である．

問題 (フロベニウスの硬貨交換問題[*1])**.**
ある国には 3 円と 7 円の硬貨がある．これらの硬貨を用いて過不足なく支払える金額は？

例えば，0 円，3 円，7 円，6 円，10 円などはこれらの硬貨を用いて支払える．

フロベニウスの貨幣交換問題を数学的に表現すれば以下の問題になる．

問題. 方程式 $3x + 7y = k$ が自然数解 (x, y) を持つような自然数 k は？

この講義では，更に一般化された以下の問題を考える．

問題. $a_1, a_2, \ldots, a_n$ を自然数とする．方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k$$

が自然数解 $(x_1, x_2, \ldots, x_n)$ を持つような自然数 k は？

この講義ではより具体的な以下の問題を通して数値半群の基本事項を学ぶ．

- この方程式がいつ解を持つ？
- この方程式が解を持たないような k に上限はあるか？上限があるならそれはいくつか？
- この方程式の解はいくつか？

[*1] Frobenius (1849-1917)

約束事

- 記号 $:=$ で「左辺を右辺で定義する」ことを表す
  （例：$n! := 1 \cdot 2 \cdots (n-1)n$）
- $:\Longleftrightarrow$ と書いたら「左側を右側で定義する」を意味する．
  （例：p が素数 $:\Longleftrightarrow$ p は 2 以上の自然数で 1 と自分自身以外に約数を持たない）
- ギリシャ文字：

α, A：アルファ	η, H：エータ	ν, N：ニュー	τ, T：タウ
β, B：ベータ	θ, Θ：シータ	ξ, Ξ：グザイ，クシー	υ, Υ：ウプシロン
γ, Γ：ガンマ	ι, I：イオタ	o, O：オミクロン	ϕ, φ, Φ：ファイ
δ, Δ：デルタ	κ, K：カッパ	π, Π：パイ	χ, X：カイ
ϵ, E：イプシロン	λ, Λ：ラムダ	ρ, P：ロー	ψ, Ψ：プサイ
ζ, Z：ゼータ	μ, M：ミュー	σ, Σ：シグマ	ω, Ω：オメガ

1　集合と写像の基礎

1.1　集合

集合とは「もの（**要素**または**元**と呼ばれる）の集まり」である．x が集合 A の元であることを $x \in A$ で，x が A の元でないことを $x \notin A$ で表す．

集合の表し方には主に以下の 2 通りがある：

- **外延的記法** $\cdots$ 集合を全ての元を列挙して表す

$$\{1,2,3,4\},\ \{1,3,5,7,\ldots\},\ \{\ldots,-2,-1,0,1,2,\ldots\}$$

- **内包的記法** $\cdots$ 集合を元の満たす条件を用いて表す

$$\{x \mid x \text{ は整数で } 1 \leq x \leq 4\},\ \{x \mid x \text{ は奇数 }\},\ \{x \mid x \text{ は整数 }\}$$

縦線 $|$ の**左側に集合の元**を，**右側に元の満たす条件**を書く

以下の集合を表す記号はよく使われる．

記号.

(1) $\emptyset$：空集合（一つも元を含まない集合）

(2)
- $\mathbb{N} := \{0,1,2,\ldots\}$：自然数全体の集合（この講義では 0 も自然数に含める）
- $\mathbb{Z} := \{\ldots,-2,-1,0,1,2,\ldots\}$：整数全体の集合
- $\mathbb{R}$：実数全体の集合
- $\mathbb{C}$：複素数全体の集合

(3) 1 以上の整数 n に対して，$\mathbb{N}^n, \mathbb{Z}^n, \mathbb{R}^n, \mathbb{C}^n$ でそれぞれ n 個の自然数，整数，実数，複素数を成分に持つベクトル全体の集合を表す：
- $\mathbb{N}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は自然数 }\}$
- $\mathbb{Z}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は整数 }\}$
- $\mathbb{R}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は実数 }\}$
- $\mathbb{C}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は複素数 }\}$

(4) 集合 A の元の個数を $|A|$ を表す．

集合に関する記号を復習する：

定義 1.1.1.

- $A \subseteq B$（A は B の**部分集合**）$:\Longleftrightarrow$ 全ての A の元 a は B の元である
- $A = B$（A と B は**等しい**）$:\Longleftrightarrow A \subseteq B$ かつ $B \subseteq A$

  従って，集合 A と集合 B が等しいことを示したいならば，「全ての A の元が B の元であること」および「全ての B の元が A の元であること」を示せば良い．
- $A \cup B := \{x \mid x \in A \text{ または } x \in B\}$（$A$ と B の**和集合**）
- $A \cap B := \{x \mid x \in A \text{ かつ } x \in B\}$（$A$ と B の**共通集合**）
- $A - B := \{x \mid x \in A \text{ かつ } x \notin B\}$（$A$ と B の**差集合**）

1.2 写像

A, B を集合とする．A の各元 a に対して B の元 b をただ一つ対応させる規則 f を A **から** B **への写像**という．このとき，$a \in A$ に対応する B の元を $f(a)$ と書き，写像 f を

$$f : A \to B,\ a \mapsto f(a) \quad \text{または単に} \quad f : A \to B$$

と表す．

写像 $f : A \to B$ に対して，集合 A を写像 f の**定義域**，集合 B を写像 f の**値域**と呼ぶ．また，B の部分集合

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

を写像 f の**像**と呼ぶ．

二つの写像 $f, g : A \to B$ が**等しい**とは，「全ての $a \in A$ に対して $f(a) = g(a)$」が成り立つときに言い，$f = g$ と表す．

例 1.2.1. (1) 区間 I 上で定義された関数 $f(x)$ は写像 $f : I \to \mathbb{R},\ x \mapsto f(x)$ を定める．従って，写像は関数を一般化した概念である．

f の定義域は I，値域は $\mathbb{R}$，像は $f(\mathbb{R}) = \{f(x) \mid x \in I\}$.

- $f(x) = x^2$ のとき，定義域は $\mathbb{R}$，像は $[0, \infty)$
- $f(x) = e^x$ のとき，定義域は $\mathbb{R}$，像は $(0, \infty)$
- $f(x) = \log(x)$ のとき，定義域は $(0, \infty)$，像は $\mathbb{R}$

(2) 2 次の正方行列 A に対して，写像 $f_A : \mathbb{R}^2 \to \mathbb{R}^2$ が

$$f_A(\boldsymbol{x}) = A\boldsymbol{x} \quad (\boldsymbol{x} \in \mathbb{R}^2)$$

で定まる．従って，線型写像は写像である．

f_A の定義域は $\mathbb{R}^2$，値域は $\mathbb{R}^2$，像は $f_A(\mathbb{R}^2) = \{A\boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{R}^2\}$.

- $A = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ のとき，

$$f_A \begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + y \\ x + 3y \end{pmatrix}$$

であり，像は $\mathbb{R}^2$

- $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ のとき，

$$f_A \begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2y \\ 2x + 4y \end{pmatrix}$$

であり，像は $\{(a, 2a) \mid a \in \mathbb{R}\}$

定義 1.2.2. (1) 集合 A に対して，A の**恒等写像** $\mathsf{id}_A : A \to A$ を

$$\mathsf{id}_A(a) := a \quad (a \in A)$$

で定義する．

(2) 写像 $f : A \to B$, $g : B \to C$ に対して，f と g の**合成写像** $g \circ f : A \to B$ を

$$(g \circ f)(a) := g(f(a)) \quad (a \in A)$$

で定義する．

命題 1.2.3. $f : A \to B, g : B \to C, h : C \to D$ を写像とする．

(1) $(h \circ g) \circ f = h \circ (g \circ f)$ が成り立つ．

(2) $f \circ \mathsf{id}_A = f$ と $\mathsf{id}_B \circ f = f$ が成り立つ．

証明. (1) A の各元 a に対して合成写像の定義から

$$((h\circ g)\circ f)(a)=(h\circ g)(f(a))=h(g(f(a)))$$
$$(h\circ(g\circ f))(a)=h((g\circ f)(a))=h(g(f(a)))$$

となる．従って，全ての $a\in A$ に対して $((h\circ g)\circ f)(a)=(h\circ(g\circ f))(a)$ が示されたので $(h\circ g)\circ f=h\circ(g\circ f)$.

(2) A の全ての元 a に対して

$$(f\circ \mathsf{id}_A)(a)=f(\mathsf{id}_A(f))=f(a)$$

が成り立つので $f\circ \mathsf{id}_A=f$ が成り立つ．同様に $\mathsf{id}_B\circ f=f$. ■

例 1.2.4. (1) $\mathbb{R}$ の恒等写像は関数 $f(x)=x$ で与えられる．

$f(x)$ を区間 I で定義された関数，$g(x)$ が区間 J で定義された関数で，$f(I)\subseteq J$ を満たすとする．このとき，写像 f と g の合成写像は f と g の合成関数 $(g\circ f)(x)=g(f(x))$ で与えられる．

(2) $\mathbb{R}^2$ の恒等写像は f_{E_2} である．

2 次正方行列 A,B に対して，

$$(f_A\circ f_B)(\boldsymbol{x})=f_A(f_B(\boldsymbol{x}))f_A(B\boldsymbol{x})=A(B\boldsymbol{x})=(AB)\boldsymbol{x}=f_{AB}(\boldsymbol{x})$$

となる．従って，$f_A\circ f_B=f_{AB}$.

定義 1.2.5. $f:A\to B$ を写像とする．写像 $g:B\to A$ が f の**逆写像**であるとは，

$$g\circ f=\mathsf{id}_A\quad\text{かつ}\quad f\circ g=\mathsf{id}_B$$

(つまり，「全ての $a\in A$ に対して $g(f(a))=a$ かつ全ての $b\in B$ に対して $f(g(b))=b$」が成り立つ時に言う．この g を f^{-1}（f **インバース**と読む）と書く．

注意. 逆写像の定義より，$a\in A$ と $b\in B$ に対して

$$f(a)=b\Longleftrightarrow f^{-1}(b)=a$$

が成り立つ.

例 1.2.6. (1) $g(x)$ が $f(x)$ の逆関数のとき，g は f の逆写像である．

- $f : \mathbb{R} \to \mathbb{R},\ x \mapsto 2x+1$ は逆写像 $g : \mathbb{R} \to \mathbb{R},\ x \mapsto \dfrac{x-1}{2}$ を持つ．
- $f : \mathbb{R} \to (0,\infty),\ x \mapsto e^x$ は逆写像 $g : (0,\infty) \to \mathbb{R},\ x \mapsto \log(x)$ を持つ．

(2) A が 2 次の正則行列, その逆行列を A^{-1} とする (つまり, $AA^{-1} = A^{-1}A = E_2$)．のとき，例 1.2.4(2) により

$$f_A \circ f_{A^{-1}} = f_{AA^{-1}} = f_{E_2} = \mathrm{id}_{\mathbb{R}^2}$$
$$f_{A^{-1}} \circ f_A = f_{A^{-1}A} = f_{E_2} = \mathrm{id}_{\mathbb{R}^2}$$

従って，f_A は逆写像 $f_{A^{-1}}$ を持つ．

命題 1.2.7. 写像 $f : A \to B$ と $g : B \to C$ を考える．

(1) f と g が逆写像を持つとき $g \circ f$ も逆写像を持ち，$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ が成り立つ．

(2) f が逆写像を持つとき f^{-1} も逆写像を持ち，$(f^{-1})^{-1} = f$ が成り立つ．

証明. (1) f と g が逆写像 f^{-1}, g^{-1} を持つとする．このとき，$f^{-1} \circ g^{-1}$ が $g \circ f$ の逆写像であることを確かめれば良い．これは

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A$$
$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_B \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C$$

となることから従う．

(2) f が逆写像 f^{-1} を持つとする．このとき，f が f^{-1} の逆写像であることを確かめれば良い．f^{-1} が f の逆写像なので

$$f \circ f^{-1} = \mathrm{id}_B, \quad f^{-1} \circ f = \mathrm{id}_A$$

成り立っているが，これは f が f^{-1} の逆写像であることを意味している． ■

定義 1.2.8. $f : A \to B$ を写像とする．

(1) f が**単射**とは，「全ての $a, a' \in A$ に対して，$f(a) = f(a')$ ならば $a = a'$ となる」が成り立つときに言う．

(2) f が**全射**とは,「全ての $b \in B$ に対して, $b = f(a)$ となる $a \in A$ が存在する」が成り立つときに言う.

(3) f が**全単射**とは, f が単射かつ全射（つまり,「全ての $b \in B$ に対して, $b = f(a)$ となる $a \in A$ が**ただ一つ**存在する」）のときに言う.

例 1.2.9. (1) 関数 $f(x) = x^2$ を考える.

- $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ は単射でも全射でもない.
- $f : \mathbb{R} \to [0, \infty),\ x \mapsto x^2$ は全射であるが単射ではない.
- $f : [0, \infty) \to \mathbb{R},\ x \mapsto x^2$ は単射であるが全射ではない.
- $f : [0, \infty) \to [0, \infty),\ x \mapsto x^2$ は全単射である.

(2) 関数 $f(x) = e^x$ を考える.

- $f : \mathbb{R} \to \mathbb{R},\ x \mapsto e^x$ は単射であるが全射ではない.
- $f : \mathbb{R} \to (0, \infty),\ x \mapsto e^x$ は全単射である.

(3) 2 次の正方行列 A を考える.

- A が正則行列のとき, $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \boldsymbol{x} \mapsto A\boldsymbol{x}$ は全単射である.
- A が正則行列でないとき, $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \boldsymbol{x} \mapsto A\boldsymbol{x}$ は全射でも単射でもない.

定理 1.2.10. 写像 $f : A \to B$ に対して,

$$f \text{ が逆写像を持つ} \iff f \text{ が全単射}$$

証明. （$\Longrightarrow$）と（$\Longleftarrow$）をそれぞれ示す.

f が逆写像をもつなら f は全単射：

f が逆写像 $g : B \to A$ を持つとする. まずは f が単射であることを示す. A の元 a, a' が $f(a) = f(a')$ を満たすとする. このとき,

$$a = g(f(a)) = g(f(a')) = a'$$

となるので, f が単射であることが示された（一つ目と三つ目の等号に逆写像の定義 $g \circ f = \mathsf{id}_A$ を用いた）.

次に f が全射であることを示す．全ての B の元 b に対して，A の元 $a = g(b)$ を考えると，

$$f(a) = f(g(b)) = b$$

となるので f が全射であることも示された（二つ目の等号に逆写像の定義 $f \circ g = \mathsf{id}_B$ を用いた）．

f が全単射なら f は逆写像をもつ：

f が全単射なので，各 $b \in A$ に対して $f(a) = b$ となる $a \in A$ がただ一つ存在する．この a を $g(b)$ と書くことにする．この対応で，写像

$$g : B \to A,\ b \mapsto g(b)$$

を得る．定義より，全ての $b \in B$ に対して $f(g(b)) = b$ が成り立つ．一方で，全ての $a \in A$ に対して $f(g(f(a))) = f(a)$ であるが，f が単射なので $g(f(a)) = a$ が従う．よって，$f \circ g = \mathsf{id}_B$ と $g \circ f = \mathsf{id}_A$ が示されたので g は f の逆写像である． ■

命題 1.2.11. A, B が有限個の元を持つ集合で，$|A| = |B|$ とする．写像 $f : A \to B$ が単射ならば f は全単射となる．

証明. B とその部分集合 $f(A)$ の元の個数が等しいので $B = f(A)$ となる． ■

演習問題

問題 1.1. $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c\}$ とし，写像 $f : A \to B$ を

$$f(1) = a,\ f(2) = b,\ f(3) = b,\ f(4) = a,\ f(5) = b$$

このとき，以下の集合を求めよ：

(1) $f(A)$

(2) $f(\{1, 2\})$

(3) $f(\{1, 4\})$

問題 1.2. 例 1.2.9(3) を確かめよ．

問題 1.3. 次の写像が全射，単射，全単射，どれでもない，のいずれか答えよ．また，全単射の場合はその逆写像も求めよ．

(1) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto e^x$

(2) $f : \mathbb{R} \to \mathbb{R}_{>0},\ x \mapsto e^x$　（ただし，$\mathbb{R}_{>0} := \{x \in \mathbb{R} \mid x > 0\}$）

(3) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^3 - x$

(4) $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 3x+5y \\ 4x+7y \end{smallmatrix}\right)$

(5) $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 4x+2y \\ 2x+y \end{smallmatrix}\right)$

(6) $x \in \{0, 1, 2, 3, 4\}$ に対して x^3 を 5 で割った余り $f(x)$ を対応させる写像

$$f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$$

問題* 1.4. 写像 $f : A \to B$ と $g : B \to C$ に対して以下を示せ.

(1) f と g が単射ならば $g \circ f$ は単射

(2) $g \circ f$ が単射ならば f は単射

(3) f と g が全射ならば $g \circ f$ は全射

(4) $g \circ f$ が全射ならば f は全射

2　整数の剰余と合同式

2.1　整数の剰余

次の命題は a が自然数の場合には中学校か高校で習っている（はず）.

命題 2.1.1 (除法の原理)**.** $a, n \in \mathbb{Z}$（$n \geq 1$）とする．このとき,

$$a = qn + r, \quad 0 \leq r < n$$

を満たすような自然数 q, r がただ一組存在する.

証明. 存在すること：

数直線を区間

$$\ldots,\ [-2n, -n),\ [-n, 0),\ [0, n),\ [n, 2n),\ \ldots$$

に分割する．すると，実数 a はいずれかの区間 $[qn, (q+1)n)$ $(q \in \mathbb{Z})$ に含まれる．このとき，$qn \leq a < (q+1)n$ となるので，$r = a - qn$ と置くと

$$a = qn + r, \quad 0 \leq r < n$$

が成り立つ.

ただ一つであること：

$a = qn + r = q'n + r',\ 0 \leq r, r' < n$ となる整数の組 $(q, r), (q', r')$ を考える．このとき $q = q',\ r = r'$ を示せば良い．等式 $qn + r = q'n + r'$ より $(q - q')n = qn - q'n = r' - r$ となる．今，仮定 $0 \leq r, r' < n$ から $|r' - r| < n$ となることに注意すると，$(q - q')n = qn - q'n = r' - r$ を満たすのは $q - q' = 0,\ r' - r = 0$ となるときのみである．従って $q = q',\ r = r'$. ■

定義 2.1.2. $a = qn + r,\ 0 \leq r < n$ と表されているとき，q を a **を** n **で割った商**，r を a **を** n **で割った余り**という.

定義 2.1.3. (1) a, b を整数とする．$b = qa$ を満たす整数 q が存在するとき，「b **は** a **を割り切る**」，「b **は** a **の倍数**」，「a **は** b **の約数**」などという．このとき,

$a \mid b$ と書く．

(2) 整数 a **と** b **の公約数**とは，$d \mid a$ かつ $d \mid b$ であるような整数 d である．

(3) a, b を 0 でない整数とする．a と b の公約数のうちで最大のものを a **と** b **の最大公約数（greatest common divisor）**といい，これを $\gcd(a, b)$ と書く．
以下，$\gcd(a, 0) = a$, $\gcd(0, b) = b$, $\gcd(0, 0) = 0$ と約束する．

(4) 2 個以上の整数 $a_1, a_2, \ldots, a_n$ に対しても公約数および最大公約数 $\gcd(a_1, a_2, \ldots, a_n)$ を同様に定義する．

注意. 容易に分かるように

$$\gcd(a_1, a_2, \ldots, a_m) = \gcd(\gcd(a_1, a_2, \ldots, a_{m-1}), a_m)$$

が成り立つ．

定理 2.1.4. （ユークリッドの互除法） $a, n \in \mathbb{Z}$（$n \geq 1$）とし，a を n で割った余りを r とする．このとき，

$$\gcd(a, n) = \gcd(n, r)$$

が成り立つ．

証明. a を n で割った余りが r なので，$a = qn + r$ $(q, r \in \mathbb{Z}, 0 \leq r < n)$ と表せる．

$c := \gcd(a, n)$, $d := \gcd(n, r)$ と置いたとき，$c \leq d$ と $d \leq c$ を示せば良い．

$\underline{c \leq d}$：

c は a と n の公約数なので $a = uc$, $n = vc$ $(u, v \in \mathbb{Z})$ と書ける．このとき，

$$r = a - qn = uc - qvc = (u - qv)c$$

となり，c は r の約数である．特に，c が r と n の公約数であることも分かった．d は r と n の最大公約数なので，最大性から $c \leq d$ となる．

$\underline{d \leq c}$：

d は n と r の公約数なので $n = ud$, $r = vd$ $(u, v \in \mathbb{Z})$ と書ける．このとき，

$$a = qn + r = qud + vd = (qu + v)d$$

となり，d は a の約数である．また，d は n の約数でもあるので，結局 d は a と n の公約数である．c は a と n の最大公約数なので，最大性により $d \leq c$ となる．

$c \leq d$ と $d \leq c$ が示されたので，$c = d$ が分かった． ■

例 2.1.5. (1) ユークリッドの互除法（定理 2.1.4）を用いて 39 と 25 の最大公約数を求める．

$39 = 1 \cdot 25 + 14$ なので，$\gcd(39, 25) = \gcd(25, 14)$

$25 = 1 \cdot 14 + 11$ なので，$\gcd(25, 14) = \gcd(14, 11)$

$14 = 1 \cdot 11 + 3$ なので，$\gcd(14, 11) = \gcd(11, 3)$

$11 = 3 \cdot 3 + 2$ なので，$\gcd(11, 3) = \gcd(3, 2)$

$3 = 1 \cdot 2 + 1$ なので，$\gcd(3, 2) = \gcd(2, 1)$

ここで，$\gcd(2, 1) = 1$ より $\gcd(39, 25) = 1$ となる．

(2) ユークリッドの互除法（定理 2.1.4）を用いて 1071 と 1029 の最大公約数を求める．

$1071 = 1 \cdot 1029 + 42$ なので，$\gcd(1071, 1029) = \gcd(1029, 42)$

$1029 = 24 \cdot 42 + 21$ なので，$\gcd(1029, 42) = \gcd(42, 21)$

$42 = 2 \cdot 21 + 0$ なので，$\gcd(42, 21) = \gcd(21, 0)$

ここで，$\gcd(21, 0) = 21$ より $\gcd(1071, 1029) = 21$ となる．

この例では 1 または 0 が現れるまでユークリッドの互除法を繰り返し用いたが，もちろん最大公約数が簡単に求められるようになったらそこで終了しても良い．

命題 2.1.6 (ベズーの補題)**.** a, b を 0 でない整数で $d = \gcd(a, b)$ とする．このとき，

$$ax + by = d$$

を満たす整数 x, y が存在する．

証明. a, b の符号を適当に変えることで，$a \geq b > 0$ としても良い．このとき，b に関する数学的帰納法で証明する．

- $b = 1$ のとき， $d = 1$ なので $x = 0, y = 1$ とすれば

$$0 \cdot a + 1 \cdot 1 = 1$$

となる．

- $b > 1$ とし，$a' \geq b' > 0, b' < b$ なる整数 a', b' に対して主張が正しいと仮定する（$a'x + b'x = \gcd(a', b')$ となる整数 x, y が存在する）．
  命題 2.1.1 より，
  $$a = qb + r, \quad 0 \leq r < b$$
  となる整数 q, r が存在する．従って，ユークリッドの互除法（**??**）により $d = \gcd(a, b) = \gcd(b, r)$ が成立する．ここで，$b \geq r > 0, r < b$ なので数学的帰納法の仮定により
  $$bx + ry = d$$
  となる整数 x, y が存在する．$r = a - qb$ を代入することで
  $$ay + b(x - qy) = d$$
  が従う．

数学的帰納法により，$a \geq b > 0$ なる全ての整数に対して主張が正しいことが示された． ■

コメント. a, b を 0 でない自然数で $d = \gcd(a, b)$ とする．このとき，全ての整数 x, y に対して $d|(ax + by)$ となる．従って，

$$ax + by = k \text{ が整数解 } (x, y) \text{ を持つ} \iff d \mid k$$

例 2.1.7. (1) $a = 39, b = 25$ とする．このとき，例 2.1.5(1) より $\gcd(39, 25) = 1$ となる．
例 2.1.5(1) で計算した割り算の式を繰り返し用いると，

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (11 - 3 \cdot 3) = -11 + 4 \cdot 3 \\ &= -11 + 4 \cdot (14 - 1 \cdot 11) = 4 \cdot 14 - 5 \cdot 11 \\ &= 4 \cdot 14 - 5 \cdot (25 - 1 \cdot 14) = -5 \cdot 25 + 9 \cdot 14 \\ &= -5 \cdot 25 + 9 \cdot (39 - 1 \cdot 25) = 9 \cdot 39 - 14 \cdot 25 \end{aligned}$$

となり，$9 \cdot 39 - 14 \cdot 25 = 1$ と表せる．

(2) $a = 1071, b = 1029$ とする．このとき，例 2.1.5(1) より $\gcd(1071, 1029) = 21$

となる．

例 2.1.5(2) で計算した割り算の式を繰り返し用いると，

$$\begin{aligned} 21 &= 1029 - 24 \cdot 42 \\ &= 1029 - 24 \cdot (1071 - 1 \cdot 1029) = 25 \cdot 1071 - 26 \cdot 1029 \end{aligned}$$

となり，$25 \cdot 1071 - 26 \cdot 1029 = 21$ と表せる．

この命題を用いることで一次不定方程式

$$ax + by = k$$

を解く事ができる．

一次不定方程式 $ax + by = k$ の解き方

(1) $d = \gcd(a, b)$ をユークリッドの互除法で求める．
(2) $d \nmid k$ ならば解なし，$d \mid k$ ならば次に進む．
(3) 例 2.1.7 の方法で $ax_0 + by_0 = d$ を満たす整数解 (x_0, y_0) を一組見つける．
(4) このとき，$ax + by = k$ の一般解は

$$(x, y) = \left(\frac{kx_0 + bu}{d}, \frac{ky_0 - au}{d} \right) \quad (u \in \mathbb{Z})$$

例 2.1.8. (1) $39x + 25y = 3$ の一般解は

$$(x, y) = (27 + 25u, -42 - 39u) \quad (u \in \mathbb{Z})$$

(2) $1071x + 1029y = 42$ の一般解は

$$(x, y) = \left(\frac{42 \cdot 25 + 1029u}{21}, \frac{42 \cdot (-26) - 1071u}{21} \right) = (50+49u, -52-51u) \quad (u \in \mathbb{Z})$$

ベズーの補題を繰り返し用いることで 2 個以上の整数にも拡張できる：

系 2.1.9. $a_1, a_2, \ldots, a_n$ を 0 でない整数で $d = \gcd(a_1, a_2, \ldots, a_n)$ とする．このとき，

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = d$$

を満たす整数 $x_1, x_2, \ldots, x_n$ が存在する.

2.2 合同式

以後，整数 $n > 0$ を一つ固定する.

定義 2.2.1. 整数 a, b が $n|(a-b)$ を満たすとき，$a \equiv b \bmod n$ と表し，a **と** b **は** n **を法として合同である**という.

$$a \equiv b \bmod n \Longleftrightarrow a \text{ と } b \text{ を } n \text{ で割った余りが等しい}$$

以下の事実は容易に分かる.

補題 2.2.2. a, b, c を整数とする.

(1) $a \equiv a \bmod n$
(2) $a \equiv b \bmod n$ ならば $b \equiv a \bmod n$
(3) $a \equiv b \bmod n$ かつ $b \equiv c \bmod n$ ならば $a \equiv c \bmod n$

命題 2.2.3. 整数 a_1, a_2, b_1, b_2 が $a_1 \equiv a_2 \bmod n$, $b_1 \equiv b_2 \bmod n$ を満たすとする. このとき，次が成り立つ：

(1) $a_1 + b_1 \equiv a_2 + b_2 \bmod n$
(2) $a_1 b_1 \equiv a_2 b_2 \bmod n$

証明. $a_1 \equiv a_2 \bmod n$, $b_1 \equiv b_2 \bmod n$ なので，ある整数 k, l を用いて $a_1 - a_2 = kn$, $b_1 - b_2 = ln$ と表せる.

(1) $(a_1+b_1)-(a_2+b_2) = (a_1-a_2)+(b_1-b_2) = (k+l)n$ より, $a_1+b_1 \equiv a_2+b_2 \bmod n$.

(2) $a_1b_1-a_2b_2 = (a_1-a_2)b_1+a_2(b_1-b_2) = (kb_1+la_2)n$ より, $a_1b_1 \equiv a_2b_2 \bmod n$. ■

例 2.2.4. $(m+1)$ 桁の自然数 N は

$$N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$$
$$(0 \leq a_0, a_1, \ldots, a_m \leq 9,\ a_m \neq 0)$$

と表せる（a_i は N の i の位の数字）.
$n = 3$ のとき，$10 \equiv 1 \bmod 3$ なので $10^i \equiv 1^i = 1 \bmod 3$ となる．従って,

$$\begin{aligned} N &= a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_m \cdot 1 + a_{n-1} \cdot 1 + \cdots a_1 \cdot 1 + \overline{a_0} \mod 3 \\ &\equiv a_m + a_{n-1} + \cdots a_1 + \overline{a_0} \mod 3 \end{aligned}$$

となる．このことから，N を 3 で割った余りと N の各桁の和 $a_m + a_{m-1} + \cdots + a_1 + a_0$ を 3 で割った余りは等しい.
$n = 9$ のときも $10 \equiv 1 \bmod 9$ なので上と全く同様にして

$$N \equiv a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0 \bmod 9$$

となる．従って，N を 9 で割った余りと N の各桁の和 $a_m + a_{m-1} + \cdots + a_1 + a_0$ を 9 で割った余りは等しい.
例えば,

$$\begin{aligned} 1859135 &\equiv 1 + 8 + 5 + 9 + 1 + 3 + 5 \\ &= 32 \\ &\equiv 3 + 2 \\ &= 5 \\ &\equiv \begin{cases} 2 \mod 3 \\ 2 \mod 5 \end{cases} \end{aligned}$$

となり，1859135 を 3 で割った余りは 2，9 で割った余りは 5 である.

通常の整数の等号とは異なり，合同式においては一般に割り算はできない：

$$2 \cdot 6 \equiv 2 \cdot 9 \bmod 6 \text{ だが } 6 \not\equiv 9 \bmod 6$$

合同式の割り算について以下の結果が成り立つ.

命題 2.2.5. a, b, c を整数，$d = \gcd(c, n)$，$m = n/d$ とする．

$$ac \equiv bc \bmod n \Longrightarrow a \equiv b \bmod m$$

特に，c と n が互いに素ならば

$$ac \equiv bc \bmod n \Longrightarrow a \equiv b \bmod n$$

証明. $ac \equiv bc \bmod n$ とすると，$ac - bc = qn$ $(q \in \mathbb{Z})$ と表せる．$c' = c/d$ と書くと $(a-b)c' = ac' - bc' = qm$ となるので c' と m は互いに素なので $a - b$ は m の倍数．従って，$a \equiv b \bmod m$. ■

この命題を用いることで一次合同式

$$ax \equiv b \bmod n$$

を解くことができる．

一次合同方程式 $ax \equiv b \bmod n$ の解き方

(i) $d = \gcd(a, n)$ をユークリッドの互除法で求める．
(ii) $d \nmid b$ ならば解なし，$d \mid b$ ならば次に進む．
(iii) 例 2.1.7 の方法で $ax_0 + ny_0 = d$ を満たす整数解 (x_0, y_0) を一組見つける．
(iv) このとき，$ax \equiv b \bmod n$ の一般解は

$$x = \frac{bx_0 + nu}{d} \quad (u \in \mathbb{Z})$$

例 2.2.6. $18x \equiv 30 \bmod 48$ の解を求める．

(i) ユークリッドの互除法を用いて $\gcd(18, 48)$ を求める：

$$48 = 2 \cdot 18 + 12$$
$$18 = 1 \cdot 12 + 6$$

より，$\gcd(18, 48) = 6$.

(ii) $6 \mid 30$ なのでこの一次合同方程式は解を持つ．

(iii) (1) の計算より

$$6 = 18 - 12 = 18 - (48 - 2 \cdot 18) = 3 \cdot 18 + (-1) \cdot 48$$

(iv) この一次合同方程式の一般解は

$$x = 15 + 8u \quad (u \in \mathbb{Z})$$

演習問題

問題 2.1. 以下の整数 a, b に対して，最大公約数 $\gcd(a, b)$ および $ua + vb = \gcd(a, b)$ を満たすような u, v を一組求めよ.

(1) $(a, b) = (729, 1000)$
(2) $(a, b) = (323, 374)$

問題 2.2. 以下の一次不定方程式の整数解 (x, y) を全て求めよ：

(1) $78x + 163y = 2$
(2) $858x + 1914y = 198$

問題 2.3. 以下の一次合同式の整数解 (x, y) を全て求めよ：

(1) $15x \equiv 6 \mod 33$
(2) $11x \equiv 3 \mod 23$

3　数値半群

この節の内容は主に [1, 3] に基づく．論理的な部分は [3] が，具体的な公式については [1] が詳しい．

3.1　数値半群の定義

定義 3.1.1.　$\mathbb{N}$ の部分集合 S が**部分モノイド**とは，以下の条件を満たすものである：

(i)　$0 \in S$
(ii)　全ての $a, b \in S$ に対して $a + b \in S$

部分モノイド S はさらに条件

(iii)　$\mathbb{N} \setminus S$ が有限集合

を満たすとき，**数値半群**であるという[a]．

[a] 半群というと (i) の条件を課さないことが普通であるが，慣習上数値半群と呼ぶ

命題 3.1.2.　S が $\mathbb{N}$ の部分モノイドとする．

(1)　全ての $a_1, a_2, \ldots, a_n$ に対して $a_1 + a_2 + \cdots a_n \in S$ となる．
(2)　全ての $a \in S$ と $k \in \mathbb{N}$ に対して $ka \in S$ となる．

証明.　(1) 部分モノイドの定義 3.1.1 の (ii) を繰り返し用いて，

$$\begin{aligned} a_1 + a_2 &\in S \\ a_1 + a_2 + a_3 = (a_1 + a_2) + a_3 &\in S \\ a_1 + a_2 + a_3 + a_4 = (a_1 + a_2 + a_3) + a_4 &\in S \\ &\vdots \end{aligned}$$

(2) (1) より

$$kx = \overbrace{a + a + \cdots + a}^{k \text{ 個}} \in S$$

となる．■

定義 3.1.3. S を数値半群とする．

(1) $\mathsf{G}(S) := \mathbb{N} \setminus S$ の元を S の**ギャップ（gap）**という．
(2) $\mathsf{G}(S)$ の元の個数を S の**種数（genus）**といい，$\mathsf{g}(S)$ と書く．
(3) $\mathsf{G}(S)$ の最大の元を S の**フロベニウス数（Frobenius number）**といい，$\mathsf{f}(S)$ と書く．便宜上 $S = \mathbb{N}$ のとき $\mathsf{f}(S) = -1$ と定める．

定義により，S は $\mathsf{f}(S) + 1$ 以上の数を全て含む．これを

$$S = \{0, a_1, a_2, \ldots, a_t, \mathsf{f}(S) + 1, \to\}$$

のように表すことにする．

例 3.1.4. (1) $\{0\}$ は $\mathbb{N}$ の部分モノイド，$\mathbb{N}$ は数値半群である．

(2) $S = \{0, 3, 6, 7, 9, 10, 12, \to\}$ は数値半群で
- $\mathsf{G}(S) = \{1, 2, 4, 5, 8, 11\}$
- $\mathsf{g}(S) = 6$
- $\mathsf{f}(S) = 11$

(3) $S = \{0, 5, 7, 9, 10, 12, 14, \to\}$ は数値半群で
- $\mathsf{G}(S) = \{1, 2, 3, 4, 6, 8, 11, 13\}$
- $\mathsf{g}(S) = 8$
- $\mathsf{f}(S) = 13$

(4) $S = \{0, 6, 7, 9, 12, 13, 14, 15, 16, 18, \to\}$ は数値半群で
- $\mathsf{G}(S) = \{1, 2, 3, 4, 5, 8, 10, 11, 17\}$
- $\mathsf{g}(S) = 9$
- $\mathsf{f}(S) = 17$

命題 3.1.5. $a_1, a_2, \ldots, a_n$ を 0 でない自然数とする．このとき，$\mathbb{N}$ の部分集合

$$\langle a_1, a_2, \ldots, a_n \rangle := \{k_1 a_1 + k_2 a_2 + \cdots + k_n a_n \mid k_1, k_2, \ldots, k_n \in \mathbb{N}\}$$

は $\mathbb{N}$ の部分モノイドである．

証明. 部分モノイドの定義 3.1.1 の条件の (i)(ii) を満たすことを確かめる.

(i) 0 は $0 = 0 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n$ と表せるので $\langle a_1, a_2, \ldots, a_t \rangle$ の元である.

(ii) x, y を $\langle a_1, a_2, \ldots, a_n \rangle$ の元とする. $k_i, l_j \in \mathbb{N}$ を用いて

$$x = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n, \quad y = l_1 a_1 + l_2 a_2 + \cdots + l_n a_n$$

と表すと,

$$\begin{aligned} x + y &= (k_1 a_1 + k_2 a_2 + \cdots + k_n a_n) + (l_1 a_1 + l_2 a_2 + \cdots + l_n a_n) \\ &= (k_1 + l_1) a_1 + (k_2 + l_2) a_2 + \cdots + (k_n + l_n) a_n \end{aligned}$$

は再び $\langle a_1, a_2, \ldots, a_t \rangle$ の元となる.

以上より, $\langle a_1, a_2, \ldots, a_n \rangle$ は $\mathbb{N}$ の部分モノイドとなる. ■

定義 3.1.6. 0 でない自然数 $a_1, a_2, \ldots, a_n$ に対して, $\langle a_1, a_2, \ldots, a_n \rangle$ を $a_1, a_2, \ldots, a_n$ **で生成される** $\mathbb{N}$ **の部分モノイド**, $a_1, a_2, \ldots, a_n$ をその**生成系**と呼ぶ.

$S = \langle a_1, a_2, \ldots, a_n \rangle$ $(a_1 < a_2 < \ldots < a_n)$ の求め方

(i) 自然数を横 a_1 列に並べる

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & a_1 - 1 \\ a_1 & a_1 + 1 & a_1 + 2 & \cdots & 2a_1 - 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

(ii) $0, a_1, a_2, \ldots, a_n$ および同じ列の下にある数に下線を引く

(iii) 下線が引かれていない数を順に見ていき, S に含まれる数が見つかったら, その数および同じ列の数に下線を引く

(iv) この操作を行なっていき, 最終的に下線が引かれている数が S の元となる.

例 3.1.7. (1) $S = \langle 5, 15 \rangle = \{0, 5, 10, 15, \ldots\} = 5\mathbb{N}$

$$\begin{array}{ccccc} \underline{0} & 1 & 2 & 3 & 4 \\ \underline{5} & 6 & 7 & 8 & 9 \\ \underline{15} & 16 & 17 & 18 & 19 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

(2) $S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, \to\}$

$$\begin{array}{ccc} \underline{0} & 1 & 2 \\ \underline{3} & 4 & \underline{5} \\ \underline{6} & 7 & \underline{8} \\ \underline{9} & \underline{10} & \underline{11} \\ \vdots & \vdots & \vdots \end{array}$$

従って，$\mathsf{G}(S) = \{1, 2, 4, 7\}$, $\mathsf{g}(S) = 4$, $\mathsf{f}(S) = 7$.

(3) $\langle 5, 9, 11 \rangle = \{0, 5, 9, 10, 11, 14, 15, 16, 18, \to\}$

$$\begin{array}{ccccc} \underline{0} & 1 & 2 & 3 & 4 \\ \underline{5} & 6 & 7 & 8 & \underline{9} \\ \underline{10} & \underline{11} & 12 & 13 & \underline{14} \\ \underline{15} & \underline{16} & 17 & \underline{18} & \underline{19} \\ \underline{20} & \underline{21} & \underline{22} & \underline{23} & \underline{24} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

従って，$\mathsf{G}(S) = \{1, 2, 3, 4, 6, 7, 8, 12, 17\}$, $\mathsf{g}(S) = 10$, $\mathsf{f}(S) = 17$

$\langle a_1, a_2, \ldots, a_n \rangle$ は以下の意味で $a_1, a_2, \ldots, a_n$ を含む最小の部分モノイドである．

命題 3.1.8. S を $\mathbb{N}$ の部分モノイド，$a_1, a_2, \ldots, a_n$ を S の元とする．このとき，$\langle a_1, a_2, \ldots, a_n \rangle$ は S の部分集合である．

証明. 自然数 $k_1, k_2, \ldots, k_n$ に対して

- 命題 3.1.2(2) より $k_i a_i \in S$
- 命題 3.1.2(1) より $k_1 a_1 + k_2 a_2 + \cdots + k_n a_n \in S$

従って，$\langle a_1, a_2, \ldots, a_t \rangle \subseteq S$ が示された． ■

有限個の自然数で生成される部分モノイドが数値半群になるかどうかは以下の命題を用いて判定できる．

定理 3.1.9. $S = \langle a_1, a_2, \ldots, a_n \rangle$ を $\mathbb{N}$ の部分モノイドとする．このとき，次の条件は同値である：

(1) S は数値半群
(2) $\gcd(a_1, a_2, \ldots, a_n) = 1$

証明. (1) $\Longrightarrow$ (2)：

対偶を示す．$d := \gcd(a_1, a_2, \ldots, a_n)$ が 1 でないとき，$\langle a_1, a_2, \ldots, a_n \rangle$ の元は全て d の倍数なので，$\mathbb{N} \setminus S$ は無限個の元を含む．従って，S は数値半群ではない．

(2) $\Longrightarrow$ (1)：

$\gcd(a_1, a_2, \ldots, a_n) = 1$ なので，系 2.1.9 よりある整数 $k_1, k_2, \ldots, k_n$ が存在して

$$k_1 a_1 + k_2 a_2 + \cdots + k_n a_n = 1$$

が成り立つ．$a_1, a_2, \ldots, a_n$ の順番を適当に入れ替えて $k_1, \ldots, k_m \geq 0$, $k_{m+1}, \ldots, k_n \leq 0$ としても良い．このとき，

$$k_1 a_1 + \cdots + k_m a_m = 1 + (-k_{m+1}) a_{m+1} + \cdots + (-k_n) a_n$$

が成り立つので，$s := (-k_{m+1}) a_{m+1} + \cdots + (-k_n) a_n$ と置けば $s, s+1 \in S$ となる．

このとき，$x \geq s^2 - 1$ ならば $x \in S$ となることを示す．

- $s = 0$ のとき，$1 \in S$ なので $x = x \cdot 1 \in S$.
- $s > 0$ のとき，x を

$$x = qs + r \quad (q, s \in \mathbb{N},\ 0 \leq r < s)$$

と表す．このとき，$x \geq s^2 - 1$ より

$$(q+1)s \geq qs + r + 1 = x + 1 \geq s^2$$

となるので $q \geq s - 1 \geq r$．従って，

$$x = qs + r = (q - r)s + r(s+1) \in S.$$

■

注意. この証明中において $x > s^2 - 2$ ならば $x \in S$ となることが示されているが，一般に $\mathsf{f}(S) = s^2 - 2$ ではない．

コメント. $a_1, a_2, \ldots, a_n$ を 0 でない自然数とし，方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k \qquad (*)$$

を考える．

(1) $\gcd(a_1, a_2, \ldots, a_n) = 1$ のとき，

$$k \notin \mathsf{G}(\langle a_1, a_2, \ldots, a_n \rangle) \Longleftrightarrow \text{方程式 } (*) \text{ が自然数解 } (x_1, x_2, \ldots, x_n) \text{ を持つ}$$

が成り立つ．特に，

$$k > \mathsf{f}(\langle a_1, a_2, \ldots, a_n \rangle) \Longrightarrow \text{方程式 } (*) \text{ が自然数解 } (x_1, x_2, \ldots, x_n) \text{ を持つ}$$

(2) $a_1, a_2, \ldots, a_n$ を 0 でない自然数，$d := \gcd(a_1, a_2, \ldots, a_n)$ とする．このとき，$a'_i := a_i/d$ と置くと $\gcd(a'_1, a'_2, \ldots, a'_n) = 1$ なので，

$$d \mid k \text{ かつ } k/d \notin \mathsf{G}(\langle a'_1, a'_2, \ldots, a'_n \rangle) \Longleftrightarrow \text{方程式 } (*) \text{ が自然数解 } (x_1, x_2, \ldots, x_n) \text{ を持つ}$$

が成り立つ．特に，

$$d \mid k \text{ かつ } k/d > \mathsf{f}(\langle a'_1, a'_2, \ldots, a'_n \rangle) \Longrightarrow \text{方程式 } (*) \text{ が自然数解 } (x_1, x_2, \ldots, x_n) \text{ を持つ}$$

注意. 方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k$$

の自然数解は整数解（節 2.1 参照）と比べて非常に複雑である．例えば，n が 3 以上の場合は解が存在するような k，および解の個数を与えるような公式は存在しない．この講義では $n = 2$ の場合に公式を与え，一般の n の場合にはこれらの計算方法を解説していく．

実は全ての数値半群は有限個の自然数で生成されることが分かる．

命題 3.1.10. S を数値半群とする．このとき，$S = \langle a_1, a_2, \ldots, a_n \rangle$ となる 0 でない自然数 $a_1, a_2, \ldots, a_n$ が存在する．

証明. S の 0 でない元の中で最小のものを m とする．このとき，各 $i = 1, \ldots, m-1$ に対して，$s \equiv i \bmod m$ となる S の元 s の中で最小なものを a_i と表す（$\mathbb{N} \setminus S$ は有限集合なので必ずこのような s が存在する）．このとき，$S = \langle m, a_1, \ldots, a_{m-1} \rangle$ が成り立つ．実際，定義から $m, a_1, a_2, \ldots, a_{m-1} \in S$ なので命題 3.1.8 より $\langle m, a_1, \ldots, a_{m-1} \rangle \subseteq S$ となる．

一方で，S の 0 でない元 s を

$$s = km + r \quad (k, r \in \mathbb{N},\ 0 \leq r < m)$$

と表す．また，$a_r \equiv r \bmod m$ なので，

$$a_r = lm + r \quad (l \in \mathbb{N})$$

と表せる．a_r の最小性から $s \geq a_r$ なので $k \geq l$ となり，

$$s = km + r = (k-l)m + (lm + r) = (k-l)m + a_r \in \langle m, a_1, \ldots, a_{m-1} \rangle$$

従って，逆の包含 $\langle m, a_1, \ldots, a_{m-1} \rangle \subseteq S$ も示された． ■

生成系から余分なものを取り除いていくことで以下の概念に到達する．

定義 3.1.11. S を $\mathbb{N}$ の部分モノイドとする．S の生成系 $a_1, a_2, \ldots, a_n$ が**極小生成系**であるとは，「各 $i = 1, 2, \ldots, n$ に対して $\langle a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \rangle \subsetneq S$」が成り立つときに言う．

命題 3.1.12. S を数値半群とする．このとき，

(1) S は極小生成系を持つ．
(2) S の極小生成系は一通りに決まる．

証明. (1) 命題 3.1.10 より S は有限個の自然数 $a_1, a_2, \ldots, a_n \geq 1$ で生成される．

$S \setminus \{0\}$ の部分集合 X を

$$X := \{ s \in S \setminus \{0\} \mid s \text{ は 2 個の } S \setminus \{0\} \text{ の元の和で書けない } \}$$

と定義する．このとき，$s \in T$ は $\langle a_1, a_2, \ldots, a_n \rangle$ の元なので，$a_1, a_2, \ldots, a_n$ 達のいくつかの和で表せる．s は 2 つ以上の $S \setminus \{0\}$ の元の和で書けないので，$s = a_i$ となる i が存在する．従って，$X \subseteq \{a_1, a_2, \ldots, a_t\}$ となる．特に，X は有限集合．また，定義から X は S の極小生成系となる．

(2) $a_1, a_2, \ldots, a_n$ を S の極小生成系とする．このとき，(1) の証明により $X \subseteq \{a_1, a_2, \ldots, a_n\}$ となる．$a_1, a_2, \ldots, a_n$ が S の極小生成系であることから $X = \{a_1, a_2, \ldots, a_n\}$ となり，極小生成系は一通りに決まる． ■

S の極小生成系の求め方

(i) S の 0 でない元の中で最小のもの m を見つける．

(ii) 各 $i = 1, \ldots, m-1$ に対して $s \equiv i \bmod m$ となる S の元 s の中で最小のもの a_i を見つける．

(iii) $a_0 := m, a_1, \ldots, a_{m-1}$ の中で他の元の和で表せるものを取り除く．このとき，残った元達が極小生成系となる．

例 3.1.13. (1) 数値半群 $S = \{0, 3, 6, 7, 9, 10, 12, \to\}$ を考える．

(i) $S \setminus \{0\}$ の中で最小の元は 3 である．

(ii)
- $s \equiv 1 \bmod 3$ となる $s \in S$ の中で最小のものは 7
- $s \equiv 2 \bmod 3$ となる $s \in S$ の中で最小のものは 14

従って，$S = \langle 3, 7, 14 \rangle$

(iii) $14 = 7 + 7$ と表せるので 14 を取り除いて，3, 7 が S の極小生成系．

(2) 数値半群 $S = \{0, 5, 7, 9, 10, 12, 14, \to\}$ を考える．

(i) $S \setminus \{0\}$ の中で最小の元は 5 である．

(ii)
- $s \equiv 1 \bmod 5$ となる $s \in S$ の中で最小のものは 16
- $s \equiv 2 \bmod 5$ となる $s \in S$ の中で最小のものは 7
- $s \equiv 3 \bmod 5$ となる $s \in S$ の中で最小のものは 18
- $s \equiv 4 \bmod 5$ となる $s \in S$ の中で最小のものは 9

従って，$S = \langle 5, 7, 9, 16, 18 \rangle$．

(iii) $16 = 7 + 9$, $18 = 9 + 9$ なのでこれらを取り除いて，5, 7, 9 が S の極小生成系．

(3) 数値半群 $S = \{0, 6, 7, 9, 12, 13, 14, 15, 16, 18, \to\}$ を考える．

(i) $S \setminus \{0\}$ の中で最小の元は 6 である．

(ii)
- $s \equiv 1 \bmod 6$ となる $s \in S$ の中で最小のものは 7
- $s \equiv 2 \bmod 6$ となる $s \in S$ の中で最小のものは 14
- $s \equiv 3 \bmod 6$ となる $s \in S$ の中で最小のものは 9
- $s \equiv 4 \bmod 6$ となる $s \in S$ の中で最小のものは 16
- $s \equiv 5 \bmod 6$ となる $s \in S$ の中で最小のものは 23

従って，$S = \langle 6, 7, 9, 14, 16, 23 \rangle$．

(iii) $4 = 7 + 7$, $16 = 7 + 9$, $23 = 2 \cdot 7 + 9$ なのでこれらを取り除いて，$6, 7, 9$ が S の極小生成系．

以後，特に断らない限り $S = \langle a_1, a_2, \ldots, a_n \rangle$ と書いたら $a_1, a_2, \ldots, a_n$ は S の極小生成系で $a_1 < a_2 < \cdots < a_n$ となるものとする．

定義 3.1.14. S を数値半群とする．命題 3.1.12 より，S の極小生成系 $a_1, a_2, \ldots, a_n$ は一意に決まる．

(1) a_1 を S の**重複度（multiplicity）**といい，$\mathsf{m}(S)$ と表す．
(2) n を S の**埋め込み次元（embedding dimension）**といい，$\mathsf{e}(S)$ と表す．

例 3.1.15. (1) $S = \{0, 3, 6, 7, 9, 10, 12, \to\} = \langle 3, 7 \rangle$ に対して，
- $\mathsf{m}(S) = 3$
- $\mathsf{e}(S) = 2$

(2) $S = \{0, 5, 7, 9, 10, 12, 14, \to\} = \langle 5, 7, 9 \rangle$ に対して，
- $\mathsf{m}(S) = 5$
- $\mathsf{e}(S) = 3$

(3) $S = \{0, 6, 7, 9, 12, 13, 14, 15, 16, 18, \to\} = \langle 6, 7, 9 \rangle$ に対して，
- $\mathsf{m}(S) = 6$
- $\mathsf{e}(S) = 3$

命題 3.1.10 の証明により，$m = \mathsf{m}(S)$ を S の重複度とすると，S は m 個の元からなる生成系を持つ．命題 3.1.12(2) の証明により，これは S の極小生成系を含む．従って，以

下のことが分かる.

系 3.1.16. S を数値半群とする．このとき，$\mathsf{e}(S) \leq \mathsf{m}(S)$ が成り立つ.

演習問題

問題 3.1. 以下の数値半群 S の $\mathsf{G}(S)$, $\mathsf{g}(S)$, $\mathsf{f}(S)$ を求めよ.

(1) $S = \langle 4, 7 \rangle$
(2) $S = \langle 3, 4, 7 \rangle$
(3) $S = \langle 3, 5, 11 \rangle$
(4) $S = \langle 4, 5, 6 \rangle$
(5) $S = \langle 5, 6, 7, 10 \rangle$
(6) $S = \langle 5, 7, 9, 11 \rangle$

問題 3.2. S を数値半群とする．このとき，以下の問に答えよ.

(1) $T := S \cup \{\mathsf{f}(S)\}$ も数値半群であることを示せ.
(2) $\mathsf{e}(T) = \mathsf{e}(S)$，$\mathsf{e}(T) = \mathsf{e}(S) + 1$ となる例をそれぞれ一つ見つけよ.

問題 3.3. S, T を数値半群とする.

(1) $S \cap T$ が数値半群であることを示せ.
(2) $S + T := \{s + t \mid s \in S, t \in T\}$ が数値半群であることを示せ.

問題 3.4. S を数値半群，$x \in S$ とする．このとき,

$$S \setminus \{x\} \text{ が数値半群} \Leftrightarrow x \text{ が } S \text{ の極小生成系に含まれる}$$

を示せ.

3.2 アペリー集合

前節で与えた極小生成系を用いる方法が最も簡単に数値半群を表現する方法である．しかしながら，これまでの具体例の計算からわかるように極小生成系が分かったとしてもそ

の数値半群にどのような元が含まれるかはすぐには分からない．この節では，数値半群に含まれる元を明確に表す方法の一つであるアペリー集合を導入する．

定義 3.2.1. S を数値半群とする．このとき，

$$\mathsf{Ap}(S) := \{s \in S \mid s - \mathsf{m}(S) \notin S\}$$

を S の**アペリー集合（Apéry set）**と呼ぶ．

例 3.2.2. (1) $S = \langle 3, 7\rangle = \{0, 3, 6, 7, 9, 10, 12, \to\}$ のとき，
$S - 3 = \{-3, 0, 3, 4, 6, 7, 9, \to\}$.
この中で S に含まれない数は $-3, 4, 11$ なので，

$$\mathsf{Ap}(S) = \{0, 7, 14\}$$

(2) $S = \langle 5, 7, 9\rangle = \{0, 5, 7, 9, 10, 12, 14, \to\}$ のとき，
$S - 5 = \{-5, 0, 2, 4, 5, 7, 9, \to\}$.
この中で S に含まれない数は $-5, 2, 4, 11, 13$ なので，

$$\mathsf{Ap}(S) = \{0, 7, 9, 16, 18\}$$

(3) $S = \langle 6, 7, 9\rangle = \{0, 6, 7, 9, 12, 13, 14, 15, 16, 18, \to\}$ のとき，
$S - 6 = \{-6, 0, 1, 3, 6, 7, 8, 9, 10, 12, \to\}$.
この中で S に含まれない数は $-6, 1, 3, 8, 10, 17$ なので，

$$\mathsf{Ap}(S) = \{0, 7, 9, 14, 16, 23\}$$

実はアペリー集合は命題 3.1.10 の証明においてすでに現れている．

命題 3.2.3. S を数値半群，$m = \mathsf{m}(S)$ を S の重複度とする．各 $i = 0, 1, \ldots, m-1$ に対して，w_i を $s \equiv i \bmod m$ となるような S の元 s で最小のものとする．このとき，

$$\mathsf{Ap}(S) = \{w_0 = 0, w_1, \ldots, w_{m-1}\}$$

証明. $\bullet \{w_0, w_1, \ldots, w_{m-1}\} \subseteq \mathsf{Ap}(S)$：
各 $i = 0, 1, \ldots, m-1$ に対して $w_i \equiv i \bmod m$ なので，ある $k \in \mathbb{N}$ を用いて $w_i = km + i$

と表せる．w_i はこのような S の元のうち最小なものなので，$w_i - m = (k-1)m + i \notin S$ となる．よって，$w_i \in \mathsf{Ap}(S)$ が分かる．従って，$\{w_0, w_1, \ldots, w_{m-1}\} \subseteq \mathsf{Ap}(S)$ が示された．

• $\mathsf{Ap}(S) \subseteq \{w_0 = 0, w_1, \ldots, w_{m-1}\}$：

$w \in \mathsf{Ap}(S)$ とする．w を m で割った余りを i とすると，$w \equiv i \bmod m$ である．アペリー集合の定義から $w - m \notin S$ が成り立つので，w は $w \equiv i \bmod m$ を満たす最小の S の元である．このことから $w = w_i$ が分かる．従って，$\mathsf{Ap}(S) \subseteq \{w_0 = 0, w_1, \ldots, w_{m-1}\}$. ■

コメント. 自然数を以下のように $m = \mathsf{m}(S)$ 列で書いたとき，第 i 列目において S に入る最も上の行の元が w_i である $(i = 0, 1, \ldots, m-1)$.

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & m-1 \\ m & m+1 & m+2 & \cdots & 2m-1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

数値半群の全ての元は以下のようにアペリー集合の元を用いることで表現することができる．

命題 3.2.4. S を数値半群，$m = \mathsf{m}(S)$ を S の重複度とする．全ての $s \in S$ に対して，

$$s = km + w$$

となるような $k \in \mathbb{N}$ と $w \in \mathsf{Ap}(S)$ がただ一通り存在する．

証明. s を m で割った余りを i とする．w_i は $w_i \equiv i \bmod n$ となる最小の S の元なので，

$$s = km + w_i$$

と表せる． ■

アペリー集合は数値半群 S を完全に決定するので，原理的には数値半群の不変量をアペリー集合の元を用いて表すことができるはずである．実際，フロベニウス数と種数を表す以下の公式が知られている．

命題 3.2.5 (セルマーの公式)**.** S を数値半群, $m = \mathsf{m}(S)$ を S の重複度とする．このとき，次が成り立つ：

(1) $\mathsf{f}(S) = \max(\mathsf{Ap}(S)) - m$
(2) $\mathsf{g}(S) = \dfrac{1}{m} \displaystyle\sum_{w \in \mathsf{Ap}(S)} w - \frac{m-1}{2}$

証明. (1) $w = \max(\mathsf{Ap}(S))$ と置く．このとき次の 2 つを示せば良い：

(i) $w - m \notin S$
(ii) $n > w - m$ ならば $n \in S$

(i) はアペリー集合の定義から分かる.

(ii) $n+m > w$ なので w の最大性により $n+m \notin \mathsf{Ap}(S)$ である．$n+m$ を m で割った余りを i とすると，$n+m = km+w_i$ $(k>0)$ と表せる．従って，$n = (k-1)m+w_i \in S$.

(2) 各 $i = 0, 1, \ldots, m-1$ に対して $w_i = k_i m + i$ $(k_i \in \mathbb{N})$ と表す.

表

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & m-1 \\ m & m+1 & m+2 & \cdots & 2m-1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

において，$\mathsf{G}(S)$ の元は w_i よりも上に現れる自然数である．i 列目において，w_i よりも上にあるのは $i, n+i, \ldots, (k_i-1)n+i$ の k_i 個である．従って，

$$\begin{aligned} \mathsf{G}(S) &= k_1 + k_2 + \cdots + k_{m-1} \\ &= \frac{1}{m}\{(k_1 m + 1) + (k_2 m + 2) + \cdots (k_{m-1} n + (m-1))\} - \frac{n-1}{2} \\ &= \frac{1}{m} \sum_{w \in \mathsf{Ap}(S)} w - \frac{m-1}{2} \end{aligned}$$

■

S の埋め込み次元が 2 の場合，アペリー集合を具体的に与えることができる.

命題 3.2.6. $S = \langle a, b \rangle$ を数値半群とする．このとき,

$$\mathsf{Ap}(S) = \{0, b, 2b, \ldots, (a-1)b\}$$

証明. a と b は互いに素なので，$0, b, \ldots, (a-1)b$ を a で割った余りは全て異なる．実際，ある kb, lb $(0 \leq k < l \leq a-1)$ を a で割った余りが等しいと仮定すると，$(l-k)b = lb - kb$ は a で割り切れることになり，a と b が互いに素であることに矛盾する．このことから $\mathsf{Ap}(S) = \{0, b, 2b, \ldots, (a-1)b\}$ が分かる． ■

以上の二つの命題を合わせることで，シルヴェスターによる以下の公式を得る．

命題 3.2.7 (シルヴェスターの公式)**.** 数値半群 $S = \langle a, b \rangle$ に対して，

(1) $\mathsf{f}(S) = ab - a - b$
(2) $\mathsf{g}(S) = \dfrac{ab - a - b + 1}{2}$

証明. (1) $\mathsf{f}(S) = \max(\mathsf{Ap}(S)) - a = (a-1)b - a = ab - a - b$

(2) $\mathsf{g}(S) = \dfrac{1}{a}\displaystyle\sum_{i=0}^{a-1}(ib) - \frac{a-1}{2} = \frac{1}{a} \cdot \frac{1}{2}a(a-1)b - \frac{a-1}{2} = \frac{ab - a - b - 1}{2}$ ■

コメント. 埋め込み次元が 3 以上の数値半群の場合，そのフロベニウス数を与える公式は存在しない！！（Curtis）

演習問題

問題 3.5. 以下の数値半群 S の $\mathsf{Ap}(S)$, $\mathsf{t}(S)$ を求めよ．

(1) $S = \langle 4, 7 \rangle$
(2) $S = \langle 3, 4, 7 \rangle$
(3) $S = \langle 3, 5, 11 \rangle$
(4) $S = \langle 4, 5, 6 \rangle$
(5) $S = \langle 5, 6, 7, 10 \rangle$
(6) $S = \langle 5, 7, 9, 11 \rangle$

問題 3.6. S を重複度 3, 埋め込み次元 3 を持つ数値半群とする．つまり，極小生成系 $3, a, b$ を用いて $S = \langle 3, a, b \rangle$ と書けるとする．このとき，以下の問に答えよ：

(1) 命題 3.2.3 の記号で $\mathsf{Ap}(S) = \{w_0, w_1, w_2\}$ と表したとき，w_1, w_2 を a, b を用いて

表せ.

ヒント：$w_1 < w_2$ と $w_1 > w_2$ で場合分けをして a, b を 3 で割った余りに着目.

(2) $a = 3\mathsf{g}(S) - \mathsf{f}(S)$, $b = \mathsf{f}(S) + 3$ を示せ.

問題 3.7. a, b を 0 以上の整数で $2b \geq a - 1$ を満たすとする．$S = \langle a, a+1, \ldots, a+b \rangle$ と置いたとき，以下の問に答えよ.

(1) $\mathsf{Ap}(S)$ を a, b を用いて表せ.
(2) $\mathsf{f}(S)$ と $\mathsf{g}(S)$ を a, b を用いて表せ.

難しければ具体的な a, b（例えば $(a, b) = (5, 8)$）の場合に答えよ.

3.3 擬フロベニウス数

以下の概念は比較的最近 Rosales-Branco (2002) により導入されたものであり，フロベニウス数よりも精密に数値半群の構造を調べるための道具である.

定義 3.3.1. S を数値半群とする.

(1) $x \in \mathbb{Z} \setminus S$ が「全ての $s \in S \setminus \{0\}$ に対して $x + s \in S$」を満たすとき，x を**擬フロベニウス数（pseudo-Frobenius number）**と呼ぶ．$\mathsf{PF}(S)$ で S の擬フロベニウス数の集合を表す.
(2) $\mathsf{PF}(S)$ の元の個数を S の**型（type）**と呼び，$\mathsf{t}(S)$ と表す.

コメント. 定義より $\mathsf{f}(S)$ は $\mathsf{PF}(S)$ の最大の元である.

S を数値半群とする．$a, b \in \mathbb{Z}$ に対して,

$$a <_S b :\Longleftrightarrow b - a \in S \setminus \{0\}$$

と定める．このとき，$A \subseteq \mathbb{Z}$ に対して

$$\mathsf{M}_S(A) := \{a \in A \mid a <_S b \text{ となる } b \in A \setminus \{a\} \text{ が存在しない } \}$$

と置く．このとき，$a, b \in S \setminus \{0\}$ に対して

$$a <_S b \Longleftrightarrow b - a \in S \setminus \{0\} \Longleftrightarrow b = a + c \text{ となる } c \in S \setminus \{0\} \text{ が存在する}$$

が成り立ち，従って

$$a \in \mathsf{M}_S(S \setminus \{0\}) \Longleftrightarrow a = b + c \text{ となる } b, c \in S \setminus \{0\} \text{ が存在しない.}$$

このことから $\mathsf{M}_S(S \setminus \{0\})$ は S の極小生成系となることが分かる（命題 3.1.12 の証明中の記号で $\mathsf{M}_S(S \setminus \{0\}) = X$）.

以下の定理は擬フロベニウス数が極小生成系の双対概念であることを示す.

命題 3.3.2. $\mathsf{PF}(S) = \mathsf{M}_S(\mathbb{Z} \setminus S)$

証明. $x \in \mathbb{Z} \setminus S$ に対して

$$\begin{aligned} x \notin \mathsf{PF}(S) &\Longleftrightarrow x + s \in \mathbb{Z} \setminus S \text{ となる } s \in S \setminus \{0\} \text{ が存在する} \\ &\Longleftrightarrow x <_S y \text{ となる } y \in \mathbb{Z} \setminus S \text{ が存在する} \\ &\Longleftrightarrow x \notin \mathsf{M}_S(\mathbb{Z} \setminus S) \end{aligned}$$

となるので $\mathsf{PF}(S) = \mathsf{M}_S(\mathbb{Z} \setminus S)$. ■

命題 3.3.3. S を数値半群とする．このとき，$x \in \mathbb{Z}$ に対して

$$x \in \mathbb{Z} \setminus S \Longleftrightarrow x + y \in \mathsf{PF}(S) \text{ となる } y \in S \text{ が存在する}$$

証明. まず，命題 3.3.2 より $\mathsf{M}_S(\mathbb{Z} \setminus S) = \mathsf{PF}(S)$ となることに注意しておく.

$(\Longrightarrow)$：$x <_S n$ となる $n \in \mathbb{Z} \setminus S$ が存在しなければ $x \in \mathsf{M}_S(\mathbb{Z} \setminus S) = \mathsf{PF}(S)$ となるので，$y = 0$ とすれば良い.

$x <_S n$ となる $n \in \mathbb{Z} \setminus S$ が存在するとする．そのような n の中で最も大きいものを取ると，$n <_S k$ となる $k \in \mathbb{Z} \setminus S$ が存在しないので，$n \in \mathsf{M}_S(\mathbb{Z} \setminus S) = \mathsf{PF}(S)$ となる．よって，$y = n - x \in S$ とすれば $x + y = n \in \mathsf{PF}(S)$.

$(\Longleftarrow)$：背理法で示す．$x \in S$ と仮定すると $x + y \in S$ となるので，擬フロベニウス数の定義より $x + y \notin \mathsf{PF}(S)$ となり，矛盾．よって，$x \notin S$ である． ■

他の不変量と同様に擬フロベニウス数もアペリー集合を用いて与えられる.

命題 3.3.4. S を数値半群，$m = \mathsf{m}(S)$ を S の重複度とする．このとき，

$$\mathsf{PF}(S) = \{w - m \mid w \in \mathsf{M}_S(\mathsf{Ap}(S))\}$$

証明. $x \in \mathsf{PF}(S)$ とする．このとき，$x \notin S$ かつ全ての $s \in S \setminus \{0\}$ に対して $x+s \in S$. 特に $x+m \in S$ かつ $(x+m)-m \notin S$ となるので $w := x+m \in \mathsf{Ap}(S)$. $w <_S w'$ となる $w' \in AP(S)$ が存在するとすると，$w'-w \in S \setminus \{0\}$. 従って，$s = w'-w \in S \setminus \{0\}$ と置くと $x+s = w'-m \notin S$. これは x が擬フロベニウス数であることに矛盾する．以上より，$\mathsf{PF}(S) \subseteq \{w-m \mid w \in \mathsf{M}_S(\mathsf{Ap}(S))\}$ が示された.

次に逆の包含を示す．$w \in \mathsf{M}_S(\mathsf{Ap}(S))$ とする．このとき，$w \in \mathsf{Ap}(S)$ なので $w-m \notin S$. $w-m \notin \mathsf{PF}(S)$ と仮定すると，$(w-m)+s \notin S$ となる $s \in S \setminus \{0\}$ が存在する．つまり，$w+s \in \mathsf{Ap}(S)$ かつ $w \leq_S (w+s)$ となるので $w \in \mathsf{M}_S(\mathsf{Ap}(S))$ であることに矛盾する．よって $w-m \in \mathsf{PF}(S)$ となる．以上より，逆の包含 $\{w-m \mid w \in \mathsf{M}_S(\mathsf{Ap}(S))\} \subseteq \mathsf{PF}(S)$ も示された. ■

この擬フロベニウス数の特徴付けの良いところは，有限集合 $\mathsf{Ap}(S)$ の元の引き算という有限回の計算で判定できるところにある.

例 3.3.5. (1) $S = \langle 3, 7 \rangle$ のとき，例 3.2.2(1) より $\mathsf{Ap}(S) = \{0, 7, 14\}$ であった.

- $7-0 = 7 \in S \setminus \{0\}$ より $0 <_S 7$
- $14-7 = 7 \in S \setminus \{0\}$ より $7 <_S 14$
- $14-0 = 14 \in S \setminus \{0\}$ より $0 <_S 14$

より，$\mathsf{M}_S(\mathsf{Ap}(S)) = \{14\}$. 従って，$\mathsf{PF}(S) = \{11\}$.

(2) $S = \langle 5, 7, 9 \rangle$ のとき，例 3.2.2(2) より $\mathsf{Ap}(S) = \{0, 7, 9, 16, 18\}$ であった.

- $7-0 = 7 \in S \setminus \{0\}$ より $0 <_S 7$
- $9-7 = 7 \in S \setminus \{0\}$ より $7 <_S 9$
- $16-9 = 7 \in S \setminus \{0\}$ より $9 <_S 16$
- $18-16 = 2 \notin S \setminus \{0\}$ より $16 \not<_S 18$

より，$\mathsf{M}_S(\mathsf{Ap}(S)) = \{16, 18\}$. 従って，$\mathsf{PF}(S) = \{11, 13\}$.

(3) $S = \langle 6, 7, 9 \rangle$ のとき，例 3.2.2(3) より $\mathsf{Ap}(S) = \{0, 7, 9, 14, 16, 23\}$ であった.

- $7-0 = 7 \in S \setminus \{0\}$ より $0 <_S 7$
- $9-7 = 7 \in S \setminus \{0\}$ より $7 <_S 9$
- $16-9 = 7 \in S \setminus \{0\}$ より $9 <_S 16$
- $23-14 = 9 \in S \setminus \{0\}$ より $14 <_S 23$
- $23-16 = 7 \in S \setminus \{0\}$ より $16 <_S 23$

より，$\mathsf{M}_S(\mathsf{Ap}(S)) = \{23\}$. 従って，$\mathsf{PF}(S) = \{17\}$.

0 は $\mathsf{Ap}(S)$ の中で $\mathsf{M}_S(\mathsf{Ap}(S))$ の元になり得ないので，$\mathsf{M}_S(\mathsf{Ap}(S)) \subseteq \mathsf{Ap}(S) \setminus \{0\}$ となる．$\mathsf{M}_S(\mathsf{Ap}(S))$ と $\mathsf{PF}(S)$ の元の個数は等しいので次の不等式が従う．

系 3.3.6. S を数値半群とすると，

$$\mathsf{t}(S) \leq \mathsf{m}(S) - 1$$

演習問題

問題 3.8. 以下の数値半群 S の対して $\mathsf{PF}(S)$ を求めよ．

(1) $S = \langle 4, 7 \rangle$
(2) $S = \langle 3, 4, 7 \rangle$
(3) $S = \langle 3, 5, 11 \rangle$
(4) $S = \langle 4, 5, 6 \rangle$
(5) $S = \langle 5, 6, 7, 10 \rangle$
(6) $S = \langle 5, 7, 9, 11 \rangle$

問題 3.9. S を数値半群，$\mathsf{PF}(S) = \{f_1, f_2, \ldots, f_t\}$ $(f_1 > f_2 > \cdots > f_t)$ とする．

(1) $k \in \{1, 2, \ldots, t\}$ に対して，$S \cup \{f_1, f_2, \ldots, f_k\}$ が数値半群となることを示せ．
(2) 数値半群 S と $k \in \{2, \ldots, t\}$ で $S \cup \{f_k\}$ が数値半群とならないような例を一つ見つけよ．

3.4 対称的数値半群

この節では数値半群の性質の中で最も重要な物である対称的という性質について解説する．

補題 3.4.1. (1) $2\mathsf{g}(S) \geq \mathsf{f}(S) + 1$ が成り立つ．
(2) $2\mathsf{g}(S) = \mathsf{f}(S) + 1 \iff$ 全ての $n \in \mathbb{Z} \setminus S$ に対して $\mathsf{f}(S) - n \in S$ が成り立つ

証明. (1) $\mathsf{f}(S) \notin S$ なので，任意の $s \in S$ に対して $\mathsf{f}(S) - s \notin S$ が成り立つ．従って，写像

$$f : \{s \in S \mid s < \mathsf{f}(S)\} \to \mathsf{G}(S),\ s \mapsto \mathsf{f}(S) - s$$

が定まる．これは単射なので，

$$|\{s \in S \mid s < \mathsf{f}(S)\}| \leq |\mathsf{G}(S)|$$

が成り立つ．ここで，$\{s \in S \mid s < \mathsf{f}(S)\}$ は $0, 1, \ldots, \mathsf{f}(S) - 1$ の中で $\mathsf{G}(S)$ に含まれないものの集合なので，$\mathsf{f}(S) - \mathsf{g}(S) + 1$ 個の元からなる．従って，$2\mathsf{g}(S) \geq \mathsf{f}(S) + 1$ が示された．

(2) ($\Longrightarrow$)：$2\mathsf{g}(S) = \mathsf{f}(S) + 1$ が成り立つとき，$|\{s \in S \mid s < \mathsf{f}(S)\}| = |\mathsf{G}(S)|$ となるので，命題 1.2.11 より f は全単射．従って，

$$n \in \mathsf{G}(S) = \mathbb{N} \setminus S \Longleftrightarrow n = f(s), s < \mathsf{f}(S) \text{ となる } s \in S \text{ が存在する} \Longleftrightarrow \mathsf{f}(S) - n \in S$$

が分かる．

($\Longleftarrow$)：$n \in G(S)$ を考えると $n \in \mathbb{Z} \setminus S$ なので，仮定より $\mathsf{f}(S) - n \in S$．$s := \mathsf{f}(S) - n \in S$ と置くと，$s < \mathsf{f}(S)$ かつ $f(s) = \mathsf{f}(S) - s = n$ となるので，f は全射になる．従って，f は全単射なので $\mathsf{f}(S) - \mathsf{g}(S) + 1 = |\{s \in S \mid s < \mathsf{f}(S)\}| \leq |\mathsf{G}(S)| = \mathsf{g}(S)$ となり，$2\mathsf{g}(S) = \mathsf{f}(S) + 1$ が従う． ■

定義 3.4.2. 「全ての $n \in \mathbb{Z} \setminus S$ に対して $\mathsf{f}(S) - n \in S$」が成り立つとき，S を**対称的数値半群**と呼ぶ．

コメント. 数直線上において S の元を黒丸で，$\mathbb{Z} \setminus S$ の元を白丸で印をつけた時，

$$S \text{ が対称的} \Longleftrightarrow \text{白丸と黒丸が対称になっている}$$

例 3.4.3. (1) $S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, \to\}$ とする．$\mathsf{g}(S) = 4$, $\mathsf{f}(S) = 7$ であり，$2\mathsf{g}(S) = 8 = \mathsf{f}(S) + 1$ が成り立つので S は対称的．

$$\cdots \quad \overset{-2}{\circ} \quad \overset{-1}{\circ} \quad \overset{0}{\bullet} \quad \overset{1}{\circ} \quad \overset{2}{\circ} \quad \overset{3}{\bullet} \quad \overset{4}{\circ} \quad \overset{5}{\bullet} \quad \overset{6}{\bullet} \quad \overset{7}{\circ} \quad \overset{8}{\bullet} \quad \overset{9}{\bullet} \quad \cdots$$

(2) $S = \langle 4, 6, 7 \rangle = \{0, 4, 6, 7, 8, 10, \to\}$ とする．$\mathsf{g}(S) = 5$, $\mathsf{f}(S) = 9$ であり，$2\mathsf{g}(S) = 10 = \mathsf{f}(S) + 1$ が成り立つので S は対称的．

$$\cdots \quad \overset{-2}{\circ} \quad \overset{-1}{\circ} \quad \overset{0}{\bullet} \quad \overset{1}{\circ} \quad \overset{2}{\circ} \quad \overset{3}{\circ} \quad \overset{4}{\bullet} \quad \overset{5}{\circ} \quad \overset{6}{\bullet} \quad \overset{7}{\bullet} \quad \overset{8}{\bullet} \quad \overset{9}{\circ} \quad \overset{10}{\bullet} \quad \overset{11}{\bullet} \quad \cdots$$

(3) $S = \langle 5, 6, 7\rangle = \{0, 5, 6, 7, 10, \to\}$ とする．$\mathsf{g}(S) = 6$, $\mathsf{f}(S) = 9$ であり，$2\mathsf{g}(S) = 12 \neq 10 = \mathsf{f}(S) + 1$ となるので S は対称的ではない．

$$\cdots \quad \overset{-2}{\circ} \quad \overset{-1}{\circ} \quad \overset{0}{\bullet} \quad \overset{1}{\circ} \quad \overset{2}{\circ} \quad \overset{3}{\circ} \quad \overset{4}{\circ} \quad \overset{5}{\bullet} \quad \overset{6}{\bullet} \quad \overset{7}{\bullet} \quad \overset{8}{\circ} \quad \overset{9}{\circ} \quad \overset{10}{\bullet} \quad \overset{11}{\bullet} \quad \cdots$$

命題 3.4.4. $S = \langle a, b\rangle$ を埋め込み次元が 2 の数値半群とする．このとき，S は対称的．

証明. シルヴェスターの公式（命題 3.2.7）より，$2\mathsf{g}(S) = ab - a - b + 1 = \mathsf{f}(S)$ が成り立つ． ■

やはり対称性もアペリー集合を用いて特徴付けられる．

命題 3.4.5. S を数値半群，$m = \mathsf{m}(S)$ を S の重複度とする．$\mathsf{Ap}(S) = \{a_1, a_2, \ldots, a_m\}$ $(a_1 < a_2 < \cdots < a_m)$ とする．このとき，

$$S \text{ が対称的} \iff \text{全ての } i = 1, 2, \ldots, m \text{ に対して } a_i + a_{m-i+1} = a_m$$

証明. セルマーの公式（命題 3.2.5）より $\mathsf{f}(S) = a_m - m$ となることに注意しておく．

まずは以下の主張を示す：

主張. $a_j - a_i \in S$ ならばある k が存在して $a_j - a_i = a_k$ となる．

主張の証明. $\{(a_j - a_i) - m\} + a_i = a_j - m \notin S$ なので $(a_j - a_i) - m \notin S$．よって $a_j - a_i \in \mathsf{Ap}(S)$ が分かる． □

$(\Longrightarrow)$：$a_i - m \notin S$ であることと S が対称的であることから，$a_m - a_i = \mathsf{f}(S) - (a_i - m) \in S$． 主張より $a_m - a_i = a_j$ と表せるが，$a_1 < a_2 < \cdots < a_m$ なので $j = m - i + 1$ となることが分かる．

$(\Longleftarrow)$：$i = 1, 2, \ldots, m-1$ のとき $a_m = a_i + a_{m-i+1} \in S \setminus \{0\}$ なので $a_i <_S a_m$．従って，$a_i \notin \mathsf{M}_S(\mathsf{Ap}(S))$ また，a_m は $\mathsf{Ap}(S)$ の最大の元なので $a_m \in \mathsf{M}_S(\mathsf{Ap}(S))$．以上より，$\mathsf{M}_S(\mathsf{Ap}(S)) = \{a_m\}$ が従う．

命題 3.3.2 と命題 3.3.3 より

$$\begin{aligned} x \in \mathbb{Z} \setminus S &\iff x + y = a_m - m = \mathsf{f}(S) \text{ となる } y \in S \text{ が存在する.} \\ &\iff \mathsf{f}(S) - x \in S \end{aligned}$$

となり，S は対称的. ■

系 3.4.6. 数値半群 S に対して次の条件は同値：

(1) S は対称的
(2) $\mathsf{PF}(S) = \{\mathsf{f}(S)\}$
(3) $\mathsf{t}(S) = 1$

系 3.4.7. S を対称的数値半群で $\mathsf{m}(S) \geq 3$ とする．このとき，

$$2 \leq \mathsf{e}(S) \leq \mathsf{m}(S) - 1$$

証明. $\mathsf{e}(S) = 1$ は $\mathbb{N}$ を意味するので，$\mathsf{m}(S) = 3$ より $\mathsf{e}(S) \geq 2$ が分かる.

$\mathsf{Ap}(S) = \{a_1, a_2, \ldots, a_m\}$ $(a_1 < a_2 < \cdots < a_m)$ と表すと，命題 3.4.5 より $a_i + a_{m-i+1} = a_m$ $(i = 1, 2, \ldots, m)$．特に，$a_2 + a_{m-1} = a_m$ となるので a_m は S の極小生成系には含まれない．一方，命題 3.1.10 の証明より $\{m, a_2, \ldots, a_m\}$ は S を生成する．これらのことから S の極小生成系は $m, a_2, \ldots, a_{m-1}$ に含まれることが分かる．従って，$\mathsf{e}(S) \leq m - 1$. ■

この系により，対称的数値半群 S において重複度 $\mathsf{m}(S)$ と埋め込み次元 $\mathsf{e}(S)$ には $2 \leq \mathsf{e}(S) \leq \mathsf{m}(S) - 1$ という関係がある．逆に，この不等式を満たす整数を重複度，埋め込み次元に持つような対称的数値半群が存在することが知られている．

定理 3.4.8. e, m を $2 \leq e \leq m - 1$ を満たす整数とする．このとき，$\mathsf{e}(S) = e$, $\mathsf{m}(S) = m$ を満たす対称的数値半群 S が存在する.

証明. 詳細は省略するが以下のように具体的に構成できる：

- $e = 2$ のとき，$S = \langle m, m + 1 \rangle$ とすれば良い.
- $e \geq 3$ かつ $e - m = 2q$ が偶数のとき，

$$S = \langle m, m + 1, qm + 2q + 2, qm + 2q + 3, \ldots, qm + m - 1 \rangle$$

とすれば良い.

- $e \geq 3$ かつ $e - m = 2q + 1$ が奇数のとき,

  $S = \langle m, m+1, (q+1)m + q + 2, (q+1)m + q + 3, \ldots, (q+1)m + m - q - 2 \rangle$

  とすれば良い.

■

演習問題

問題 3.10. 以下の数値半群 S が対称的かどうか判定せよ.

(1) $S = \langle 4, 7 \rangle$
(2) $S = \langle 3, 4, 7 \rangle$
(3) $S = \langle 3, 5, 11 \rangle$
(4) $S = \langle 4, 5, 6 \rangle$
(5) $S = \langle 5, 6, 7, 10 \rangle$
(6) $S = \langle 5, 7, 9, 11 \rangle$

問題 3.11. $S = \langle a, a+1, a+2, \ldots, a+b \rangle$ $(0 < a < b)$ とする．このとき，以下のことが成り立つ

$$S \text{ が対称的} \iff a \equiv 2 \bmod b \qquad (*)$$

(1) $b = 3$ のときに $(*)$ を示せ.
(2) $b = 5$ のときに $(*)$ を示せ.
(3) $b = 7$ のときに $(*)$ を示せ.
(4) $(*)$ を示せ.

3.5 一般化フロベニウス数

自然数 $a_1, a_2, \ldots, a_n$ が $\gcd(a_1, a_2, \ldots, a_n) = 1$ を満たすとし，方程式

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = k$$

を考える．前節までは集合 $\langle a_1, a_2, \ldots, a_n \rangle$，つまり，上の方程式が自然数解を持つような k の集合について考えた．この節ではこの方程式の自然数解の個数について考察する.

定義 3.5.1. 数値半群 $S = \langle a_1, a_2, \ldots, a_n \rangle$ を考える．自然数 k に対して方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k$$

の自然数解 $(x_1, x_2, \ldots, x_n)$ の個数を $\mathsf{d}_k(S)$ と表す．このとき，自然数 s に対して，

$$\mathsf{f}_s(S) = \max\{k \in \mathbb{N} \mid \mathsf{d}_k(S) \leq s\}$$

と定め，S の **s-フロベニウス数**という．

注意. 自然数 k に対して

$$\mathsf{d}_k(S) > 0 \Longleftrightarrow a_1x_1 + a_2x_2 + \cdots + a_nx_n = k \text{ が自然数解を持つ} \Longleftrightarrow k \in S$$

であることに注意すると，

$$\mathsf{f}_0(S) = \max(\mathbb{N} \setminus S) = \mathsf{f}(S)$$

が成り立つ.

この節では互いに素な自然数 a, b に対して $d_k(\langle a, b \rangle)$, $f_k(\langle a, b \rangle)$ を計算していく.

補題 3.5.2. 全ての $k \in \mathbb{Z}$ は

$$am + bn = k \quad (m, n \in \mathbb{Z}, 0 \leq m < b)$$

とただ一通りに表せる.

証明. 命題 2.1.6 より，ある整数 m, n を用いて $am+bn = k$ と表せる．$m = qb+r$ $(q, r \in \mathbb{Z}, 0 \leq r < b)$ と表すと $k = am + bn = ar + b(n + qa)$ と書ける.

$am + bn = am' + bn' = k$ $(m, m', n, n' \in \mathbb{Z}, 0 \leq m, m' < b)$ と表せたとする．このとき，$a(m - m') = b(n' - n)$ となるので，a と b が互いに素であることから $m - m'$ は b の約数となる．$0 \leq m, m' < b$ なので，$m = m'$ でなければならない．また，$b(n' - n) = a(m - m') = 0$ となり，$n = n'$. ■

補題 3.5.3. 全ての $k \in \langle a, b \rangle$ は

$$am + bn = k \quad (m, n \in \mathbb{N}, 0 \leq m < b)$$

とただ一通りに表せる.

証明. $k \in \langle a, b \rangle$ なので $am + bn = k$ となる $m, n \in \mathbb{N}$ が存在する. $m = qb + r$ $(q, r \in \mathbb{N}, 0 \leq r < b)$ と表すと $k = am + by = ar + b(n + qa)$ と書ける. 補題 3.5.2 よりこの表示は一通り. ■

補題 3.5.4. $k \in \langle a, b \rangle$ を

$$am + bn = k \quad (m, n \in \mathbb{N}, 0 \leq m < b)$$

と表す. このとき, $d_k(\langle a, b \rangle) = \left\lfloor \frac{n}{a} \right\rfloor + 1$ となる. ここで, $\lfloor r \rfloor$ は実数 r の整数部分を表す.

証明. $d := \left\lfloor \frac{n}{a} \right\rfloor$ と置くと $da < n$ である. 従って, k は

$$a(m + ib) + b(n - ia) = k \quad (i = 0, 1, \ldots, d)$$

と少なくとも $d + 1$ 通りに表せる.

一方で, $au + bv = k$ $(u, v \in \mathbb{N})$, $u = qb + r$ $(q, r \in \mathbb{N}, 0 \leq r < b)$ と表したとき $ar + b(v + aq) = k$ と書けるが, 補題 3.5.3 の表示の一意性から $r = m, v + qa = n$ となる. 従って,

$$(u, v) = (m + qb, n - qa)$$

となる.

従って, 方程式 $ax + by = k$ は $d + 1$ 個の自然数解 $(m + ib, n - ia)$ $(i = 0, 1, \ldots, d)$ を持ち, $\mathsf{d}_k(\langle a, b \rangle) = d + 1$. ■

補題 3.5.5. 全ての $k \in \mathbb{N}$ に対して

$$\mathsf{d}_{k+ab}(\langle a, b \rangle) = \mathsf{d}_k(\langle a, b \rangle) + 1$$

が成り立つ.

証明. $k \notin \langle a,b\rangle$ のとき，$\mathsf{d}_{k+ab}(\langle a,b\rangle) = 1$ を示せば良い．$k+ab \geq ab-a-b = \mathsf{f}(\langle a,b\rangle)$ なので，$am+bn = k+ab$ $(m,n \in \mathbb{N}, 0 \leq m < b)$ と表せる．このとき，$\mathsf{d}_{k+ab}(\langle a,b\rangle) = \left\lfloor \frac{n}{a} \right\rfloor + 1$．$\mathsf{d}_{k+ab}(\langle a,b\rangle) > 1$ とすると，$n \geq a$ となり $k = am + b(n-a) \in \langle a,b\rangle$ となり矛盾．従って，$\mathsf{d}_{k+ab}(\langle a,b\rangle) = 1$.

$k \in \langle a,b\rangle$ のとき，k を $am+by = k$ $(m,n \in \mathbb{N}, 0 \leq m < b)$ と表すと，$k+ab$ は $am+b(n+a) = k+ab$ と表せる．従って，補題 3.5.4 より

$$\mathsf{d}_{k+ab}(\langle a,b\rangle) = \left\lfloor \frac{n+a}{a} \right\rfloor + 1 = \left\lfloor \frac{n}{a} \right\rfloor + 2 = \mathsf{d}_k(\langle a,b\rangle) + 1$$

が成り立つ． ■

以上の準備の下でシルヴェスターの公式（命題 3.2.7）の拡張を示すことができる．

定理 3.5.6. a,b を互いに素な 0 でない整数とする．このとき，全ての自然数 s に対して

$$\mathsf{f}_s(\langle a,b\rangle) = (s+1)ab - a - b$$

証明. $k > (s+1)ab-a-b$ のとき，補題 3.5.5 より

$$\mathsf{d}_k(\langle a,b\rangle) = \mathsf{d}_{k-ab}(\langle a,b\rangle) + 1 = \mathsf{d}_{k-2ab}(\langle a,b\rangle) + 2 = \cdots = \mathsf{d}_{k-sab}(\langle a,b\rangle) + s$$

となる．また，$k - sab > ab-a-b = \mathsf{f}(\langle a,b\rangle)$ より $\mathsf{d}_{k-sab}(\langle a,b\rangle) \geq 1$ となるので，$\mathsf{d}_k(\langle a,b\rangle) \geq s+1$．従って，$\mathsf{d}_k(\langle a,b\rangle) \leq s$ ならば $k \leq (s+1)ab-a-b$ となる．このことから，

$$\mathsf{f}_s(\langle a,b\rangle) = \max\{k \in \mathbb{N} \mid \mathsf{d}_k(\langle a,b\rangle) \leq s\} \leq (s+1)ab-a-b$$

が分かる．一方で，$ab-a-b = \mathsf{f}(\langle a,b\rangle) \notin \langle a,b\rangle$ より

$$\mathsf{d}_{(s+1)ab-a-b}(\langle a,b\rangle) = \mathsf{d}_{ab-a-b}(\langle a,b\rangle) + s = s.$$

以上より，$\mathsf{f}_s(\langle a,b\rangle) = (a+1)ab-a-b$ が示された． ■

演習問題

問題 3.12. 以下の a,b,k に対して

$$ax + by = k$$

の自然数解を全て求めよ．

(1) $(a, b, k) = (3, 5, 11)$

(2) $(a, b, k) = (4, 7, 39)$

(3) $(a, b, k) = (5, 6, 60)$

4　数値半群環

この節では環についての基本的な言葉遣いを解説し，環と数値半群の繋がりについて説明する．この節の内容は主に [4] に基づく．

4.1　環の基礎

定義 4.1.1. 集合 A の 2 元 a, b に対して和と積

$$a+b, \quad ab \quad (a, b \in A)$$

定まっているとする．これらが以下の性質を満たすとき，A を**（可換）環**という：

(i) A の全ての元 a, b, c に対して $(a+b)+c = a+(b+c)$
(ii) **零元**と呼ばれる A の元 0 が存在して，全ての A の元 a に対して $a+0 = 0+a = 0$ を満たす
(iii) A の各元 a に対して**逆元**と呼ばれる A の元 $-a$ が存在して，$a+(-a) = (-a)+a = 0$ を満たす
(iv) A の全ての元 a, b に対して $a+b = b+a$
(v) A の全ての元 a, b, c に対して $(ab)c = a(bc)$
(vi) **単位元**と呼ばれる A の元 1 が存在して, 全ての A の元 a に対して $a1 = 1a = a$ を満たす
(vii) A の全ての元 a, b, c に対して $(a+b)c = ac+bc$, $a(b+c) = ab+ac$
(viii) A の全ての元 a, b に対して $ab = ba$

定義 4.1.2. A を環とする．

(1) A の元 a, b が $ab = 1$ を満たすとき，b を a の**逆元**と呼び，a^{-1} または $\dfrac{1}{a}$ と表す．
(2) A の全ての 0 でない元が逆元を持つとき，A を**体**と呼ぶ．

これらの定義は非常に抽象的に見えるが，通常の数の和と積と同じような計算ができるものと思えば良い．この講義では以下の例を理解していれば十分である．

例 4.1.3. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は通常の和と積で環となる．また，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である．

(2) $x_1, x_2, \ldots, x_n$ を変数とする実数係数の多項式とは，

$$\sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$$

の形の有限個の単項式 $a_\alpha x^\alpha$ の和のことであった．ここで，$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$ に対して $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ と定義している．
$x_1, x_2, \ldots, x_n$ を変数とする実数係数の多項式の集合を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ と書く．

多項式

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha, \quad g = \sum_{\alpha \in \mathbb{N}^n} b_\alpha x^\alpha$$

の和と積を

- $f + g = \displaystyle\sum_{\alpha \in \mathbb{N}^n} (a_\alpha + b_\alpha) x^\alpha$
- $fg = \displaystyle\sum_{\gamma \in \mathbb{N}^n} \left(\sum_{\alpha + \beta = \gamma} a_\alpha b_\beta \right) x^\gamma$

で定義すると $\mathbb{R}[x_1, x_2, \ldots, x_n]$ は可換環となる．これを n **変数多項式環**と呼ぶ．

定義 4.1.4. A を環とする．A の部分集合 B が

(i) 全ての $a, b \in B$ に対して $a - b,\ ab \in B$
(ii) $1 \in B$

を満たすとき，B を A の**部分環**と呼ぶ．このとき，B は A と同じ和と積で環となる．

例 4.1.5. $\mathbb{R}[x]$ を 1 変数多項式環，S を数値半群とする．このとき，$\mathbb{R}[x]$ の部分集合

$$\mathbb{R}[S] := \left\{ \sum_{s \in S} a_s x^s \;\middle|\; a_s \in \mathbb{R} \right\}$$

は $\mathbb{R}[x]$ の部分環となる．これを S の**数値半群環**と呼ぶ．

$S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, \to\}$ のとき，$\mathbb{R}[S]$ の元は

$$a_0 + a_3x^3 + a_5x^5 + a_6x^6 + a_8x^8 + \cdots$$

の形をしている．

$S = \langle 5, 7, 9 \rangle = \{0, 5, 7, 9, 10, 12, 14, \to\}$ のとき，$\mathbb{R}[S]$ の元は

$$a_0 + a_5x^5 + a_7x^7 + a_9x^9 + a_{10}x^{10} + a_{12}x^{12} + a_{14}x^{14} + \cdots$$

の形をしている．

定義 4.1.6. A を環とする．A の部分集合 I が

(i) $0 \in I$
(ii) 全ての $a, b \in I$ に対して $a + b \in I$
(iii) 全ての $a \in A$ と $b \in I$ に対して $ab \in I$

を満たすとき，I を A の**イデアル**とは呼ぶ．

例 4.1.7. (1) A を環とする．$\{0\}$ と A は A のイデアルである．

(2) A を環とする．$a_1, a_2, \ldots, a_t \in A$ に対して

$$\langle a_1, a_2, \ldots, a_t \rangle := \{b_1a_1 + b_2a_2 + \cdots + b_ta_t \mid b_1, b_2, \ldots, b_t \in A\}$$

は A のイデアルとなる（代数学 III の命題 2.8 を見よ）．これを $a_1, a_2, \ldots, a_t$ で**生成されるイデアル**と呼ぶ．

(3) 自然数 n に対して，(1) より

$$\langle n \rangle = n\mathbb{Z} := \{nm \mid m \in \mathbb{Z}\}$$

は $\mathbb{Z}$ のイデアルとなる．次の命題により $\mathbb{Z}$ のイデアルは全てこの形をしていることが分かる．

(4) 1 変数多項式環 $\mathbb{R}[x]$ の元 f に対して，(1) より

$$\langle f \rangle = f\mathbb{R}[x] := \{fg \mid g \in \mathbb{R}[x]\}$$

は $\mathbb{R}[x]$ のイデアルとなる．次の命題により $\mathbb{R}[x]$ のイデアルは全てこの形をしていることが分かる．

一般の多項式環 $\mathbb{R}[x_1, x_2, \ldots, x_n]$ においても全てのイデアルは有限個の多項式で生成されることが知られている（ヒルベルトの基底定理）が，必ずしも n 個の元で生成されているとは限らない．

命題 4.1.8. $\mathbb{Z}$, $\mathbb{R}[x]$ のイデアルは全て一つの元で生成される．

証明. $\mathbb{R}[x]$ の場合のみ示す．$\mathbb{Z}$ については演習問題．

I を $\mathbb{R}[x]$ のイデアルとする．$I = \{0\}$ のとき $I = \langle 0 \rangle$ となるので，I は一つの元 0 で生成される．従って，$I \neq \{0\}$ として示す．

I には 0 でない元が含まれるので，I に含まれる 0 でない元の次数の最小値を n とする．また，$0 \neq f \in I$ を $\deg(f) = n$ となる元とする．このとき，$I = \langle f \rangle$ を示す．$f \in I$ なので $\langle f \rangle \subseteq I$ はイデアルの定義からすぐに分かる．そこで，逆の包含 $I \subseteq \langle f \rangle$ を示す．任意の元 $0 \neq g \in I$ が $\langle f \rangle$ の元，つまり f の倍多項式になることを示す．g を f で割り算し，

$$g = qf + r \quad (q, r \in \mathbb{R}[x],\ r = 0 \text{ または } \deg(r) < \deg(f) = n)$$

と表す．このとき，イデアルの定義から $r = g - qf \in I$ となる．$r \neq 0$ とすると $\deg(r) < n$ となるので n の最小性に矛盾する．従って，$r = 0$ となり，$g = qf \in \langle f \rangle$．逆の包含 $I \subseteq \langle f \rangle$ も示されたので，$I = \langle f \rangle$ となる． ■

$\mathbb{Z}$ や $\mathbb{R}[x]$ のように全てのイデアルが一つの元で生成されるような環のことを**単項イデアル整域（PID）**と呼び，環論や整数論における重要な研究対象である．PID の素朴な一般化として，全てのイデアルが n 個の元で生成されている環のことを n **項イデアル整域**と呼ぶことにする[*2]．$\mathbb{R}[x]$ が PID であることの素朴な一般化として，以下の事実を証明することができる．

定理 4.1.9. S を重複度 m を持つ数値半群とする．このとき，$\mathbb{R}[S]$ のイデアルは全て高々 m 個の元で生成される．

[*2] この用語はこの講義だけの非公式なもの

証明. I を $\mathbb{R}[S]$ のイデアルとし，I が高々 m 個の元で生成されることを示す．$I=\{0\}$, $I=\mathbb{R}[x]$ のとき，それぞれ $I=\langle 0\rangle$, $I=\langle 1\rangle$ なので一つの元で生成される．そこで，$I\neq\{0\},\mathbb{R}[x]$ として示す．このとき，I には 0 次の多項式は含まれないことに注意しておく．

各 $i=0,1,\ldots,m-1$ に対して，$\deg(f)\equiv i \bmod m$ となる $f\in I$ が存在するとき，このような f で次数が最小なものを f_i と表す．$\deg(f)\equiv i \bmod m$ となる $f\in I$ が存在しないとき，$f_i=0$ と定める．このとき，$I=\langle f_0,f_1,\ldots,f_{m-1}\rangle$ を示す．$\langle f_0,f_1,\ldots,f_{m-1}\rangle\subseteq I$ は $f_0,f_1,\ldots,f_{m-1}\in I$ であることとイデアルの定義からすぐに分かるので，逆の包含 $I\subseteq\langle f_0,f_1,\ldots,f_{m-1}\rangle$ を示す．

g を 0 でない I の元とし，$\deg(g)\equiv i \bmod m$ とする．このとき，$\deg(g)$ と $\deg(f_i)$ を m で割った余りはどちらも i なので，f_i の次数の最小性より

$$\deg(g)=ka+\deg(f_i)\quad(k\in\mathbb{N})$$

と表せる．このとき，$g-x^{ka}f_i\in I$ の最高次の項が打ち消し合うので，$g-x^{ka}f_i=0$ または $\deg(g-x^{ka}f_i)<\deg(g)$ となる．$g-x^{ka}f_i=0$ ならば $g-x^{ka}f_i\in\langle f_0,f_1,\ldots,f_{m-1}\rangle$ である．$\deg(g-x^{ka}f_i)<\deg(g)$ のとき，$g-x^{ka}f_i$ に対して同じ操作を行う．これを 0 になるまで繰り返していくことで，$g\in\langle f_0,f_1,\ldots,f_{m-1}\rangle$ が分かる．逆の包含 $I\subseteq\langle f_0,f_1,\ldots,f_{m-1}\rangle$ も示されたので，$I=\langle f_0,f_1,\ldots,f_{m-1}\rangle$ が成り立つ． ■

4.2 ヒルベルト級数

この節では環論における重要な道具であるヒルベルト級数を数値半群環に限って導入する．まずは形式的べき級数の基本事項を紹介する．

定義 4.2.1. t を変数とする実数係数の単項式の（有限とは限らない）和

$$\sum_{n=0}^{\infty}a_nt^n$$

を**形式的べき級数**と呼ぶ[a]．形式的べき級数の集合を $\mathbb{R}[\![t]\!]$ と表す．
多項式と同様に形式的べき級数

$$f=\sum_{n=0}^{\infty}a_nt^n,\quad g=\sum_{n=0}^{\infty}b_nt^n$$

の和と積を

- $f+g=\displaystyle\sum_{n=0}^{\infty}(a_n+b_n)t^n$
- $fg=\displaystyle\sum_{n=0}^{\infty}\left(\sum_{k+l=n}a_kb_l\right)t^n$

で定義すると $\mathbb{R}[\![t]\!]$ は環となる．これを**形式的べき級数環**と呼ぶ．

[a] 無限個の項の足し算だが収束性などは気にしない

形式的べき級数に対しても高校で学んだ等比級数の公式と同様のことが成り立つ．

補題 4.2.2. m を自然数とする．このとき，形式的べき級数の等式

$$(1-t^m)(1+t^m+t^{2m}+\cdots)=1$$

が成り立つ．特に，

$$1+t^m+t^{2m}+\cdots=\frac{1}{1-t^m}$$

と表す．

証明. 左辺を展開して計算すると，

$$\begin{aligned}(1-t^m)(1+t^m+t^{2m}+\cdots) &:= (1+t^m+t^{2m}+\cdots)-t^m(1+t^m+t^{2m}+\cdots)\\ &=(1+t^m+t^{2m}+\cdots)-(t^m+t^{2m}+t^{3m}+\cdots)\\ &=1\end{aligned}$$

となる． ■

注意. この補題より，自然数 m に対して等比数列の和の公式と同様の式

$$\sum_{i=0}^{n}t^{mi}=\frac{1-t^{m(n+1)}}{1-t^m}$$

も成り立つことが分かる．実際，$(1-t^m)\displaystyle\sum_{i=0}^{n}t^{mi}=1-t^{m(n+1)}$ が成り立つので両辺に $\dfrac{1}{1-t^m}$ を掛ければ良い．

定義 4.2.3. S を数値半群とする．このとき，形式的べき級数

$$\mathsf{H}(S,t) := \sum_{s\in S} t^s$$

を S の**ヒルベルト級数**と呼ぶ.

命題 4.2.4. S を重複度 m を持つ数値半群とする．このとき，

$$\mathsf{H}(S,t) = \frac{1}{1-t^m} \sum_{w\in \mathsf{Ap}(S)} t^w$$

証明. $S = \mathsf{Ap}(S) + m\mathbb{N}$ なので，

$$\mathsf{H}(S;t) = \sum_{s\in S} t^s = \sum_{w\in \mathsf{Ap}(S)} \sum_{n=0}^{\infty} t^{nm+w} = \sum_{n=0}^{\infty} t^{nm} \cdot \sum_{w\in \mathsf{Ap}(S)} t^w = \sum_{w\in \mathsf{Ap}(S)} t^w \cdot \frac{1}{1-t^m}$$

■

コメント. $S = \langle a_1, a_2, \ldots, a_n\rangle$ のとき，この命題により多項式

$$\mathsf{Q}(S,t) := (1-t^{a_2})\cdots(1-t^{a_n}) \sum_{w\in \mathsf{Ap}(S)} t^w$$

を用いて

$$\mathsf{H}(S,t) = \frac{\mathsf{Q}(S,t)}{(1-t^{a_1})(1-t^{a_2})\cdots(1-t^{a_n})}$$

と表せることが分かる.

例 4.2.5. (1) $S = \langle 3,5\rangle$ のとき，$\mathsf{Ap}(S) = \{0,5,10\}$

$$\mathsf{H}(S,t) = \frac{1}{1-t^3}\cdot(1+t^5+t^{10}) = \frac{(1+t^5+t^{10})(1-t^5)}{(1-t^3)(1-t^5)} = \frac{1-t^{15}}{(1-t^3)(1-t^5)}$$

(2) $S = \langle 3, 4, 5 \rangle$ のとき，$\mathsf{Ap}(S) = \{0, 4, 5\}$ なので，

$$\begin{aligned}\mathsf{H}(S,t) = \frac{1}{1-t^3} \cdot (1 + t^4 + t^5) &= \frac{(1+t^4+t^5)(1-t^4)(1-t^5)}{(1-t^3)(1-t^4)(1-t^5)} \\ &= \frac{1 - t^8 - t^9 - t^{10} + t^{13} + t^{14}}{(1-t^3)(1-t^4)(1-t^5)}\end{aligned}$$

(3) $S = \langle 4, 5, 6 \rangle$ のとき，$\mathsf{Ap}(S) = \{0, 5, 6, 11\}$ なので，

$$\begin{aligned}\mathsf{H}(S,t) = \frac{1}{1-t^4} \cdot (1 + t^5 + t^6 + t^{11}) &= \frac{(1+t^5+t^6+t^{11})(1-t^5)(1-t^6)}{(1-t^4)(1-t^5)(1-t^6)} \\ &= \frac{1 - t^{10} - t^{12} + t^{22}}{(1-t^4)(1-t^5)(1-t^6)}\end{aligned}$$

(4) $S = \langle 5, 7, 9 \rangle$ のとき，$\mathsf{Ap}(S) = \{0, 7, 9, 16, 18\}$ なので，

$$\begin{aligned}\mathsf{H}(S,t) = \frac{1}{1-t^5} \cdot (1 + t^7 + t^9 + t^{16} + t^{18}) &= \frac{(1+t^7+t^9+t^{16}+t^{18})(1-t^7)(1-t^9)}{(1-t^5)(1-t^7)(1-t^9)} \\ &= \frac{1 - t^{14} - t^{25} - t^{27} + t^{32} + t^{34}}{(1-t^5)(1-t^7)(1-t^9)}\end{aligned}$$

埋め込み次数が小さい数値半群のヒルベルト級数の公式はよく知られている．

命題 4.2.6. $S = \langle a, b \rangle$ $(a < b)$ とする．このとき，

$$\mathsf{H}(S,t) = \frac{1 - t^{ab}}{(1-t^a)(1-t^b)}$$

証明. 命題 3.2.7 より $\mathsf{Ap}(S) = \{0, b, 2b, \cdots, (a-1)b\}$ となるので，

$$\sum_{w \in \mathsf{Ap}(S)} t^w = \sum_{i=0}^{a-1} (t^b)^i = \frac{1 - (t^b)^a}{1 - t^b} = \frac{1 - t^{ab}}{1 - t^b}$$

が分かる．従って，

$$\mathsf{H}(S,t) = \frac{1}{1-t^a} \cdot \frac{1 - t^{ab}}{1 - t^b} = \frac{1 - t^{ab}}{(1-t^a)(1-t^b)}$$

■

埋め込み次元が 3 の場合のヒルベルト級数の公式は Herzog [2] により与えられている．証明はかなり込み入っているので結果だけ紹介する．

定理 4.2.7 (Herzog (1970))**.** $S = \langle a_1, a_2, a_3 \rangle$ が対称的でないとする．r_1, r_2, r_3 をそれぞれ $r_1 a_1 \in \langle a_2, a_3 \rangle$, $r_2 a_2 \in \langle a_1, a_3 \rangle$, $r_3 a_3 \in \langle a_1, a_2 \rangle$ となる最小の 0 でない自然数とする．また, $r_1 a_1 = s_{12} a_2 + s_{13} a_3$, $r_2 a_2 = s_{21} a_1 + s_{23} a_3$, $r_3 a_3 = s_{31} a_1 + s_{32} a_2$ と表し,

$$
\begin{aligned}
m &:= s_{23} a_3 + r_1 a_1 = s_{31} a_1 + r_2 a_2 = s_{12} a_2 + r_3 a_3 \\
n &:= s_{32} a_2 + r_1 a_1 = s_{13} a_3 + r_2 a_2 = s_{21} a_1 + r_3 a_3
\end{aligned}
$$

と置く．このとき,

$$
\mathsf{H}(S,t) = \frac{1 - t^{r_1 a_1} - t^{r_2 a_2} - t^{r_3 a_r} + t^m + t^n}{(1-t^{a_1})(1-t^{a_2})(1-t^{a_3})}
$$

が成り立つ.

S のヒルベルト級数を用いることで $\mathsf{d}_k(S)$ を以下のように帰納的に求めることができる．

$S = \langle a_1, a_2, \ldots, a_n \rangle$ とする．このとき,

$$
\frac{1}{(1-t^{a_i})} = \sum_{x=0}^{\infty} t^{a_i x}
$$

より，等式

$$
\begin{aligned}
\frac{1}{(1-t^{a_1})(1-t^{a_2})\cdots(1-t^{a_n})} &= \left(\sum_{x_1=0}^{\infty} t^{a_1 x_1}\right)\left(\sum_{x_2=0}^{\infty} t^{a_2 x_2}\right)\cdots\left(\sum_{x_n=0}^{\infty} t^{a_n x_n}\right) \\
&= \sum_{k=0}^{\infty}\left(\sum_{a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = k} 1\right) t^k \\
&= \sum_{k=0}^{\infty} \mathsf{d}_k(S) t^k
\end{aligned}
$$

が成り立つ．従って，多項式 $\mathsf{Q}(S,t)$ を

$$
\mathsf{Q}(S,t) := \sum_{k=0}^{\infty} q_k t^k
$$

と表したとき，等式

$$\mathsf{H}(S,t)=\frac{\mathsf{Q}(S,t)}{(1-t^{a_1})(1-t^{a_2})\cdots(1-t^{a_n})}=\left(\sum_{k=0}^{\infty}\mathsf{d}_k(S)t^k\right)\left(\sum_{k=0}^{\infty}q_kt^k\right)=\sum_{k=0}^{\infty}\left(\sum_{i+j=k}q_i\mathsf{d}_j(S)\right)t^k$$

の両辺を比較することで各 $k\in\mathbb{N}$ に対して等式

$$\sum_{i+j=k}q_i\mathsf{d}_j(S)=\begin{cases}1 & (k\in S\text{ のとき})\\ 0 & (k\notin S\text{ のとき})\end{cases}$$

が成り立つ．従って，

$$\begin{aligned}q_0\mathsf{d}_0(S)&=1\\ q_1\mathsf{d}_0(S)+q_0\mathsf{d}_1(S)&=0\text{ or }1\\ q_2\mathsf{d}_0(S)+q_1\mathsf{d}_1(S)+q_0\mathsf{d}_2(S)&=0\text{ or }1\\ q_3\mathsf{d}_0(S)+q_2\mathsf{d}_1(S)+q_1\mathsf{d}_2(S)+q_0\mathsf{d}_3(S)&=0\text{ or }1\\ &\vdots\end{aligned}$$

を用いて順番に $\mathsf{d}_1(S)$, $\mathsf{d}_2(S)$, $\mathsf{d}_3(S),\cdots$ を計算していくことができる．ここで，いつでも $q_0=\mathsf{d}_0(S)=1$ であることに注意しておく．

例 4.2.8. $S=\langle 3,4,5\rangle$ のとき，$\mathsf{Ap}(S)=\{0,4,5\}$ なので

$$\mathsf{Q}(S,t):=(1+t^4+t^5)(1-t^4)(1-t^5)=1-t^8-t^9-t^{10}+t^{13}+t^{14}.$$

これを用いると

$$\begin{aligned}\mathsf{d}_1=\mathsf{d}_2&=0\\ \mathsf{d}_3=\cdots=\mathsf{d}_7&=1\\ \mathsf{d}_8-1&=1\\ \mathsf{d}_9-\mathsf{d}_1-1&=1\\ \mathsf{d}_{10}-\mathsf{d}_2-\mathsf{d}_1-1&=1\\ \mathsf{d}_{11}-\mathsf{d}_3-\mathsf{d}_2-\mathsf{d}_1&=1\\ \mathsf{d}_{12}-\mathsf{d}_4-\mathsf{d}_3-\mathsf{d}_2&=1\\ \mathsf{d}_{13}-\mathsf{d}_5-\mathsf{d}_4-\mathsf{d}_3+1&=1\\ \mathsf{d}_{14}-\mathsf{d}_6-\mathsf{d}_5-\mathsf{d}_4+\mathsf{d}_1+1&=1\\ \mathsf{d}_{15}-\mathsf{d}_7-\mathsf{d}_6-\mathsf{d}_5+\mathsf{d}_2+\mathsf{d}_1&=1\\ &\vdots\end{aligned}$$

という方程式が得られるので，これを用いて順に計算していくと

$\mathsf{d}_1 = \mathsf{d}_2 = 0,\ \mathsf{d}_3 = \cdots = \mathsf{d}_7 = 1,\ \mathsf{d}_8 = \mathsf{d}_9 = \mathsf{d}_{10} = \mathsf{d}_{11} = 2,\ \mathsf{d}_{12} = \mathsf{d}_{13} = \mathsf{d}_{14} = 3,\ \mathsf{d}_{15} = 4, \ldots$

を得る．

4.3 対称的数値半群とゴレンシュタイン環

最後に，数値半群の対称性と環論や整数論における重要な環のクラスであるゴレンシュタイン環の関係について簡単に述べる．

定義 4.3.1. $S = \langle a_1, a_2, \ldots, a_n \rangle$ を数値半群とする．数値半群環 $\mathbb{R}[S]$ の部分集合

$$\omega_{\mathbb{R}[S]} := \left\{ \sum_{n \in \mathbb{Z} \setminus S} a_n t^{\mathsf{f}(S)-n} \;\middle|\; a_n \in \mathbb{R} \right\}$$

は $\mathbb{R}[S]$ のイデアルとなる．これを $\mathbb{R}[S]$ の**正準イデアル**と呼ぶ．
$\omega_{\mathbb{R}[S]} = \mathbb{R}[S]$ が成り立つとき，$\mathbb{R}[S]$ は**ゴレンシュタイン環**であるという．

コメント．正準イデアル（一般にはイデアルにはならないので正準加群と呼ばれる）とゴレンシュタイン環の概念は数値半群環だけでなくもっと一般の環に対して定義されるもので，これらの概念は環論において中心的な役割を果たす．それだけでなく，ワイルズによるフェルマーの最終定理の証明において，ある環がゴレンシュタインであることを示すことが一つの重要なステップであるなど，環論以外でも重要な意味を持つことが多い．

一般の環のゴレンシュタイン性判定は簡単ではないが，数値半群環の場合には以下の特徴付けを用いることで簡単に判定することができる．

定理 4.3.2 (Kunz (1970))**.** S を数値半群とする．このとき，次は同値：

(1) $\mathbb{R}[S]$ がゴレンシュタイン
(2) $\mathsf{H}(S,t) = -t^{\mathsf{f}(S)}\mathsf{H}(S,t^{-1})$

(3) S が対称的

証明. (1) と (2) の同値性は以下のように分かる：

$$\omega_{\mathbb{R}[S]} = \mathbb{R}[S] \iff \{\mathsf{f}(S) - n \mid n \in \mathbb{Z} \setminus S\} = S \iff S \text{ は対称的.}$$

また,

$$\begin{aligned} -t^{\mathsf{f}(S)}\mathsf{H}(S, t^{-1}) &= t^{\mathsf{f}(S)} \cdot \frac{1}{1 - t^{-m}} \cdot \sum_{w \in \mathsf{Ap}(S)} t^{-w} \\ &= \frac{1}{1 - t^{m}} \cdot \sum_{w \in \mathsf{Ap}(S)} t^{\mathsf{f}(S)+m-w} \end{aligned}$$

より

$$\mathsf{H}(S, t) = -t^{\mathsf{f}(S)}\mathsf{H}(S, t^{-1}) \iff \mathsf{Ap}(S) = \{\mathsf{f}(S) + m - w \mid w \in \mathsf{Ap}(S)\}$$

が分かる．ここで，$\mathsf{Ap}(S) = \{a_1, a_2, \ldots, a_m\}$ $(a_1 < a_2 < \cdots < a_m)$ と表すと，$a_m = \mathsf{f}(S) + m$ となる．従って，命題 3.4.5 を用いることで (2) と (3) の同値性が以下のように示される：

$$\begin{aligned} \mathsf{Ap}(S) = \{\mathsf{f}(S) + m - w \mid w \in \mathsf{Ap}(S)\} &\iff a_i = \mathsf{f}(S) + m - a_{m+1-i} \ (i = 1, 2, \ldots, m) \\ &\iff a_i = a_m - a_{m+1-i} \ (i = 1, 2, \ldots, m) \\ &\overset{\text{命題 3.4.5}}{\iff} S \text{ が対称的} \end{aligned}$$

■

演習問題

問題 4.1. $\mathbb{Z}$ のイデアルが全て一つの元で生成されることを示せ.

問題 4.2. 以下の数値半群 S に対して $\mathsf{Q}(S, t)$ を求め，それを用いて $\mathsf{d}_k(S)$ を好きなだけ計算せよ：

(1) $S = \langle 4, 6, 7 \rangle$
(2) $S = \langle 5, 6, 9 \rangle$

参考文献

[1] J. R. Alfonsín; The Diophantine Frobenius problem, *Oxford University Press*, 2005.

[2] J. Herzog; Generators and relations of abelian semigroup rings, *Manuscripta Math.* **3** (1970), 175–193.

[3] J. C. Rosales and P. A. García-Sánchez; Numerical semigroups, *Springer*, 2009.

[4] 後藤四郎，渡辺敬一著; 可換環論, 日本評論社 (2011).