2020 年度 前期 代数学 2

担当 和地 輝仁

目次

1 **シラバス抜粋** 2

2 **授業のノート** 3
§1 行列の簡約化と連立方程式 3
§2 固有値・固有ベクトル 10
§3 行列の対角化 15
§4 対称行列の対角化 20
§5 合同式 23
§6 オイラーの定理 28
§7 分数と小数 31
§8 循環小数 32
§9 ベクトル空間の基礎 37
§10 線型写像 41

1 シラバス抜粋

授業概要 幾何学で学んだ線型代数学を踏まえ、3 次以上の正方行列の固有値・固有ベクトルや対角化、および、線型写像の基礎について学びます。また、環論の初歩と多項式への応用を学ぶ授業です。

到達目標

1. 行列の固有値・固有ベクトルを計算できる。
2. 行列の対角化ができる。
3. 無限小数の性質を知る。
4. 環とその性質を知る。
5. 多項式の既約性の判定法を理解する。

授業計画 順序を交換する場合もあるので注意すること。

1. 行列の簡約化と連立方程式
2. 固有値・固有ベクトル
3. 行列の対角化
4. 対称行列の対角化
5. 合同式
6. オイラーの定理
7. 有限小数
8. 循環小数
9. 環
10. 有理整数環の剰余環
11. 多項式環
12. 多項式の既約性
13. ベクトル空間の基礎
14. 線型写像
15. 期末試験

成績評価 期末試験 (80%) と、毎回の演習問題の状況 (20%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

備考 2 年生以上を対象にした授業です。受講するためには、代数学 1 の単位を修得している必要があります。

2 授業のノート

§1 行列の簡約化と連立方程式

(1.1) 簡約行列

(M1) 0 だけの行があったとしても、下方に集まっている
(M2) 各行について、左から見ていき初めての 0 でない成分は 1 である (主成分と呼ぶ)
(M3) 主成分のある列では、主成分以外の成分は 0 である
(M4) 主成分は下の行ほど右にある

例えば、次の行列は簡約行列である。

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0&2\\0&1&0\end{pmatrix},\begin{pmatrix}1&2&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&1&1\\0&0&0\end{pmatrix},\begin{pmatrix}0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}0&1&0\\0&0&0\end{pmatrix},$$
$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix},\begin{pmatrix}1&0&2\\0&1&0\\0&0&0\end{pmatrix},\begin{pmatrix}1&2&0\\0&0&1\\0&0&0\end{pmatrix}$$

例えば、次の行列は簡約行列ではない。

$$\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}1&2&0\\0&0&0\\0&0&1\end{pmatrix}\qquad\text{(M1) に違反}$$
$$\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&2&0\\0&0&3\end{pmatrix}\qquad\text{(M2) に違反}$$
$$\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&0&1\\0&0&1\end{pmatrix}\qquad\text{(M3) に違反}$$
$$\begin{pmatrix}0&1&0\\1&0&1\end{pmatrix},\begin{pmatrix}0&1&1\\1&0&0\\0&0&0\end{pmatrix}\qquad\text{(M4) に違反}$$

(1.2) **問題** 次の行列から簡約行列を選べ。

(1) $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$ (3) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$ (4) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$ (5) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$

(6) $\begin{pmatrix} 1 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$ (7) $\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ (8) $\begin{pmatrix} 1 & 3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$ (9) $\begin{pmatrix} 1 & 0 & 3 \\ 1 & 0 & 0 \end{pmatrix}$

(10) $\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}$ (11) $\begin{pmatrix} 1 & 0 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ (12) $\begin{pmatrix} 1 & 3 & 3 \\ 1 & 0 & 0 \end{pmatrix}$ (13) $\begin{pmatrix} 1 & 3 & 3 \\ 0 & 1 & 0 \end{pmatrix}$

(14) $\begin{pmatrix} 1 & 3 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ (15) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ (16) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ (17) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

(18) $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ (19) $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$

(1.3) **行列の簡約化 (掃き出し法)** 行列の行基本変形とは、

(F) 第 i 行を a 倍する。 $(a \neq 0)$
(G) 第 j 行の a 倍を第 i 行に加える。 $(i \neq j)$
(H) 第 i 行と第 j 行を交換する。 $(i \neq j)$

の 3 種類である。

手順 1 行基本変形 (F や G や H) を用いて 1 列目の成分に 1 を作る。なおかつなるべく上に作る (1 列目ならば $(1,1)$ 成分になる)
手順 2 行基本変形 (G) を用いて、1 列目のその他の成分を 0 にする。
手順 3 主成分のできた行は変更しないように、2 列目以降も同様にする。た

だし、主成分が作れない時は、その列に主成分は作らず、それ以降の行を考える。

(1.4) **例** 次の行列を簡約化せよ。

(1) $\begin{pmatrix} 1 & 2 & -1 \\ 3 & 1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 2 & -1 & 1 \\ 3 & 1 & 2 & 2 \\ 2 & 2 & 0 & 3 \end{pmatrix}$

(解答) (1)

$$
\begin{array}{ccc|l}
1 & 2 & -1 & \\
3 & 1 & 2 & \\
2 & 2 & -1 & \\
\hline
1 & 2 & -1 & \\
0 & -5 & 5 & ② + ① \times (-3) \\
0 & -2 & 1 & ③ + ① \times (-2) \\
\hline
1 & 2 & -1 & \\
0 & 1 & 2 & ② + ③ \times (-3) \\
0 & -2 & 1 & \\
\hline
1 & 0 & -5 & ① + ② \times (-2) \\
0 & 1 & 2 & \\
0 & 0 & 5 & ③ + ② \times 2 \\
\hline
1 & 0 & -5 & \\
0 & 1 & 2 & \\
0 & 0 & 1 & ③ \times \frac{1}{5} \\
\hline
1 & 0 & 0 & ① + ③ \times 5 \\
0 & 1 & 0 & ② + ③ \times (-2) \\
0 & 0 & 1 &
\end{array}
$$

よって、$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(2)

1	2	−1	1	
3	1	2	2	
2	2	0	3	
1	2	−1	1	
0	−5	5	−1	② + ① × (−3)
0	−2	2	1	③ + ① × (−2)
1	2	−1	1	
0	1	−1	−4	② + ③ × (−3)
0	−2	2	1	
1	0	1	9	① + ② × (−2)
0	1	−1	−4	
0	0	0	−7	③ + ② × 2
1	0	1	9	
0	1	−1	−4	
0	0	0	1	③ × $(\frac{-1}{7})$
1	0	1	0	① + ③ × (−9)
0	1	−1	0	② + ③ × 4
0	0	0	1	

よって、$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(1.5) **問題** 次の行列を簡約化せよ。

(1) $\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 2 & 1 & 0 & -1 \end{pmatrix}$ (2) $\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 1 & 0 & -1 & -1 \end{pmatrix}$ (3) $\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 1 & 1 & 3 & -1 \end{pmatrix}$

(1.6) **行列の階数** 簡約化は手順が異なっても同じ簡約行列に至る。主成分の個数をその行列の階数と呼ぶ

(1.7) **例** 先の例にあった次の行列の階数はともに 3 である。

(1) $\begin{pmatrix} 1 & 2 & -1 \\ 3 & 1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 2 & -1 & 1 \\ 3 & 1 & 2 & 2 \\ 2 & 2 & 0 & 3 \end{pmatrix}$

(1.8) **問題** 次の行列の階数を求めよ。

(1) $\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 2 & 1 & 0 & -1 \end{pmatrix}$ (2) $\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 1 & 0 & -1 & -1 \end{pmatrix}$ (3) $\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 1 & 1 & 3 & -1 \end{pmatrix}$

(1.9) **連立 1 次方程式の解法と簡約化** 連立 1 次方程式の 1 次の係数を並べた行列を**係数行列**と呼び、定数項も並べた行列を**拡大係数行列**と呼ぶ。例えば、下の (1) の場合、係数行列と拡大係数行列は次のようになる。

$$\begin{pmatrix} 2 & 1 & 2 \\ 3 & 1 & 1 \\ 2 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 2 & 1 & 0 & -1 \end{pmatrix}$$

拡大係数行列の簡約化が方程式を解く手順と対応している。簡約化したときの主成分が、(a) すべて左辺にあれば解あり、(b) 右辺にあれば解なし。さらに、解がある場合、(a1) 主成分の個数が変数の個数と同じなら一意的な解があり、(a2) 変数の個数より少ないなら無数の解がある。

(1) $\begin{cases} 2x+y+2z=3 \\ 3x+y+z=2 \\ 2x+y=-1 \end{cases}$ (2) $\begin{cases} 2x+y+2z=3 \\ 3x+y+z=2 \\ x-z=-1 \end{cases}$ (3) $\begin{cases} 2x+y+2z=3 \\ 3x+y+z=2 \\ x+y+3z=-1 \end{cases}$

(解答) (1) 拡大係数行列は、$\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 2 & 1 & 0 & -1 \end{pmatrix}$ であり、簡約化すると、

$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & 2 \end{pmatrix}$ である (上の問題参照)。これは、「(a) すべて左辺にあれば解あり」の「(a1) 主成分の個数が変数の個数と同じなら一意的な解があり」のタイプであり、連立方程式に戻すと、

$$\begin{cases} x = 1 \\ y = -3 \\ z = 2 \end{cases}$$

となる。これは連立方程式の解そのものである。

(2) 拡大係数行列は、$\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 1 & 0 & -1 & -1 \end{pmatrix}$ であり、簡約化すると、$\begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & 4 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ である (上の問題参照)。これは、「(a) すべて左辺にあれば解あり」の「(a2) 変数の個数より少ないなら無数の解がある」のタイプであり、連立方程式に戻すと、

$$\begin{cases} x - z = -1 \\ y + 4z = 5 \\ 0 = 0 \end{cases}$$

となる。3 式目は常に成立するから、

$$\begin{cases} x - z = -1 \\ y + 4z = 5 \end{cases}$$

としてよい。未知数が x, y, z の 3 つだが式が 2 本で不足しているため、解が一意に決まらず無数にあるという理屈である。この場合、式が 1 本不足しているので、未知数 1 つを任意定数とする。簡約化を用いて式を整理した場

合は、後ろの変数から任意定数にすると計算が楽な場合が多い。$z = k$ (定数) とおくと、

$$\begin{cases} x = -1 + k \\ y = 5 - 4k \qquad (k \text{ は定数}) \\ z = k \end{cases}$$

が解である。

(3) 拡大係数行列は、$\begin{pmatrix} 2 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \\ 1 & 1 & 3 & -1 \end{pmatrix}$ であり、簡約化すると、$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ である (上の問題参照)。これは、「(b) 右辺にあれば解なし」のタイプであり、連立方程式に戻すと、

$$\begin{cases} x - z = 0 \\ y + 4z = 0 \\ 0 = 1 \end{cases}$$

となる。このように、主成分が右辺にあると、第 3 式の $1 = 0$ のように、常に不成立の式が現れる。つまり、解なしである。

(1.10) **問題** 次の連立方程式を解け。

(1) $\begin{cases} 2x + 3y + 2z = 2 \\ 3x + 4y + 2z = 1 \\ 4x + 2y + 3z = 9 \end{cases}$ (2) $\begin{cases} 2x + 3y + 2z = 2 \\ 3x + 4y + 2z = 1 \\ x + 2y + 2z = 3 \end{cases}$

$$(3)\ \begin{cases} 2x+3y+2z=2 \\ 3x+4y+2z=1 \\ 3x+5y+4z=3 \end{cases}$$

(1.11) **注意** 3 変数で式が 3 本である連立 1 次方程式の場合、一意的な解を持つことと係数行列が正則であることは同値である。なぜなら、一意的な解を持つということは係数行列の簡約化が単位行列になるということであり、係数行列の簡約化が単位行列になるということは、掃き出し法で逆行列が求められるということである。

§2 固有値・固有ベクトル

このテキストでは、ベクトルを太字にしたり、矢印をつけたりせずに、単に v のように記すことが多い。

(2.1) **固有値・固有ベクトル** K は複素数全体の集合 $\mathbb{C}$, 実数全体の集合 $\mathbb{R}$, 有理数全体の集合 $\mathbb{Q}$ のいずれかとする。K 成分の n 次正方行列 A に対して、

$$Av = \lambda v \qquad (\lambda \in K,\ v \in K^n,\ v \neq 0)$$

となるようなスカラー λ と 0 ではないベクトル v があったとき、λ を A の**固有値**、v を A の固有値 λ の**固有ベクトル**と呼ぶ。

(2.2) **例** 行列 $A = \begin{pmatrix} 5 & -2 \\ 12 & -5 \end{pmatrix}$ に関して、ベクトル $v_1 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ と $v_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ は、それぞれ、固有値 -1 の固有ベクトル、固有値 1 の固有ベクトルである。

なぜなら、

$$Av_1 = \begin{pmatrix} 5 & -2 \\ 12 & -5 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} -1 \\ -3 \end{pmatrix} = (-1) \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = (-1) \cdot v_1,$$
$$Av_2 = \begin{pmatrix} 5 & -2 \\ 12 & -5 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} = v_2 = 1 \cdot v_2$$

だからである。

(2.3) **定理** n 次正方行列 A に対して、A の**固有多項式** $g_A(t)$ を、

$$g_A(t) = |tI - A| \qquad (I \text{ は } n \text{ 次単位行列})$$

で定める[*1]と、A の固有値は $g_A(t) = 0$ の解である。

(証明) λ が固有値であるとは、n 次のベクトル $v \neq 0$ が存在して、$Av = \lambda v$ となることであった。変形すると、$(\lambda I - A)v = 0$ となるが、これを満たす $v \neq 0$ が存在するための必要十分条件は、$\lambda I - A$ が正則ではないことである (なぜか)。よって、λ が固有値であるための必要十分条件は、この行列の行列式が 0 となることである。

[*1] 幾何学で学んだ固有多項式・固有方程式とは行列の符号が逆なので注意。

(2.4) **例** $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の固有多項式を求める。

$$g_A(t) = |tI - A| = \left| \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right| = \begin{vmatrix} t-a & -b \\ -c & t-d \end{vmatrix}$$
$$= t^2 - (a+d)t + (ad - bc)$$

(2.5) **例題** 固有多項式を用いて次の行列の固有値を求めよ。

(1) $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (2) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

(解答) (1) $g_A(t) = \begin{vmatrix} t-1 & -1 \\ 0 & t-1 \end{vmatrix} = (t-1)^2$ より、固有値は 1.

(2) $g_A(t) = \begin{vmatrix} t & -1 \\ 1 & t \end{vmatrix} = t^2 + 1$ より固有値は、なし (スカラーが実数，有理数の場合)、あるいは、$\pm\sqrt{-1}$ (スカラーが複素数の場合)。

(2.6) **例題** $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ の固有値と固有ベクトルを求めよ。

(解答) (2.5)(1) より固有値は 1 であった。$v = \begin{pmatrix} x \\ y \end{pmatrix}$ を固有値 1 の固有ベクトルとすると、

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 1 \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

である。右辺は、$1\cdot\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$ にできるから、左辺に移項すると、

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}-\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=0,$$
$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=0.$$

これを連立方程式と見ると (2 本目は $0=0$ となり不要なので) $y=0$ のみ残る。x の条件がなく任意の定数と置けるから、固有ベクトルは、

$$v=\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}k\\0\end{pmatrix}\quad (k \text{ は任意定数})$$

である。また、例えば $k=1$ と置いて、固有ベクトルとして

$$v=\begin{pmatrix}1\\0\end{pmatrix}$$

を答えてもよい。

(2.7) **例題** 行列 $\begin{pmatrix}1&1&1\\3&1&1\\1&-1&1\end{pmatrix}$ の固有値と固有ベクトルを求めよ。

(解答) 行列のサイズが大きい場合, 固有多項式をサラスの方法などで単に展開すると, 次数の高い式の因数分解が困難になり固有値が求めづらい. そこ

で以下のように基本変形を用いて固有多項式を計算する.

$$\begin{aligned} g_A(t) &= \begin{vmatrix} t-1 & -1 & -1 \\ -3 & t-1 & -1 \\ -1 & 1 & t-1 \end{vmatrix} = \begin{vmatrix} t-2 & 0 & t-2 \\ -3 & t-1 & -1 \\ -1 & 1 & t-1 \end{vmatrix} \quad (①+③した) \\ &= (t-2)\begin{vmatrix} 1 & 0 & 1 \\ -3 & t-1 & -1 \\ -1 & 1 & t-1 \end{vmatrix} \quad (次数が下がればサラスも可) \\ &= (t-2)\begin{vmatrix} 1 & 0 & 0 \\ -3 & t-1 & 2 \\ -1 & 1 & t \end{vmatrix} \quad (③列 -①列した) \\ &= (t+1)(t-2)^2. \end{aligned}$$

よって固有値は $-1, 2$ である.

次に固有ベクトルを、固有値ごとに別々に求める。まず、固有値 -1 のとき (2.6) と同様にして、

$$\begin{pmatrix} 1 & 1 & 1 \\ 3 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -1 \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$
$$\begin{pmatrix} 2 & 1 & 1 \\ 3 & 2 & 1 \\ 1 & -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

この連立方程式を簡約化を用いて解くと (どうやるのだったろう)、

$$\begin{cases} x + z = 0 \\ y - z = 0 \end{cases}$$

となる (1 本は無意味になり結果として 2 本だけ残る)。$z = k$ を任意定数とすると、

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -z \\ z \\ z \end{pmatrix} = \begin{pmatrix} -k \\ k \\ k \end{pmatrix} = k \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$$

となる。よって固有ベクトルは、$\begin{pmatrix} -k \\ k \\ k \end{pmatrix}$ (k は任意定数)、あるいは、$\begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$ と答えればよい。

次に、固有値 2 のときも同様に連立方程式を解くと、

$$\begin{cases} x + z = 0 \\ y + 2z = 0 \end{cases}$$

となる。再び $z = k$ (任意定数) と置けば、固有ベクトルは

$$\begin{pmatrix} -k \\ -2k \\ k \end{pmatrix}, \quad \text{あるいは} \quad \begin{pmatrix} -1 \\ -2 \\ 1 \end{pmatrix}$$

である。

(2.8) **問題** 次の行列の固有値・固有ベクトルを求めよ。

(1) $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & -1 \\ 3 & 2 & 1 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & -2 & 3 \\ -3 & 4 & -7 \\ 1 & 2 & -1 \end{pmatrix}$ (3) $\begin{pmatrix} 3 & 3 & -1 \\ -2 & -2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

(4) $\begin{pmatrix} 3 & 2 & -2 \\ -2 & -1 & 2 \\ -1 & -1 & 2 \end{pmatrix}$ (5) $\begin{pmatrix} 3 & 5 & -4 \\ -2 & -2 & 2 \\ -2 & -1 & 1 \end{pmatrix}$ (6) $\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ -1 & 0 & 3 \end{pmatrix}$

(7) $\begin{pmatrix} 6 & -3 & -2 \\ 7 & 0 & -6 \\ -2 & -2 & 5 \end{pmatrix}$

§3 行列の対角化

(3.1) **行列の対角化** n 次正方行列 A の**対角化**とは、n 次正則行列 P を用いて、

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

と表すことを言う。行列 A が対角化できるとき、A は**対角化可能**であるという。

(3.2) **対角化の方法** v が固有値 λ の固有ベクトルであれば、$Av = \lambda v$ である。$v_1, v_2, \ldots, v_n$ を、それぞれ、固有値 $\lambda_1, \lambda_2, \ldots, \lambda_n$ の固有ベクトルとし、行列 P をこれら n 個の固有ベクトル (縦ベクトル) を並べてできる行列とすると、

$$AP = P \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

となる。P が逆行列を持てば、両辺に左から P^{-1} を掛けると、A が対角化できる。

以上をまとめると、対角化の手順は次のようになる。

(1) n 次正方行列 A の固有値 $\lambda_1, \ldots, \lambda_n$ と、その固有ベクトル $v_1, \ldots, v_n$ を求める。

ここで、n 個の 1 次独立な固有ベクトルが求まらなければ、対角化可能ではない。**また、この先の手順で、一切の計算は不要であることに注意。P の逆行列を求めたり、3 つの行列の積 $P^{-1}AP$ を計算したりは、決してしないこと。**

(2) 縦ベクトル $v_1, \ldots, v_n$ を並べてできる n 次正則行列を P とおく。

(3) $P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$ と対角化できる。

(3.3) **例題** 次の行列が対角化可能ならば対角化せよ。

(1) $\begin{pmatrix} 5 & -2 \\ 12 & -5 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (3) $\begin{pmatrix} 1 & 1 & 1 \\ 3 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}$ (4) $\begin{pmatrix} 1 & 1 & -1 \\ -2 & -2 & 1 \\ -4 & -2 & 1 \end{pmatrix}$

(解答) (1) (2.2) により、固有値は $\lambda = -1, 1$ であり、それぞれの固有ベクトルは、$\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ と $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ であった。したがって、与えられた行列を A とし、$P = \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$ とおくと、$P^{-1}AP = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ と対角化できる。

(2) (2.5) により、固有値は $\lambda = 1$ であり、固有ベクトルは $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ である。ところが、2 次正方行列が対角化できるためには、1 次独立な固有ベクトルは 2 個必要だから、A は対角化可能ではない。

(3) 同様に (2.7) によれば、1 次独立な固有ベクトルが 2 個しかないため対角化可能ではない。

(4) これは再利用できる以前の問題がないので真面目に計算する。まず固有値を求め、次に固有ベクトルを求め、最後に対角化する。

与えられた行列を A とすると、固有多項式は、

$$\begin{aligned} g_A(t) &= \begin{vmatrix} t-1 & -1 & 1 \\ 2 & t+2 & -1 \\ 4 & 2 & t-1 \end{vmatrix} = \begin{vmatrix} t+1 & t+1 & 0 \\ 2 & t+2 & -1 \\ 4 & 2 & t-1 \end{vmatrix} \\ &= (t+1)\begin{vmatrix} 1 & 1 & 0 \\ 2 & t+2 & -1 \\ 4 & 2 & t-1 \end{vmatrix} = (t+1)\begin{vmatrix} 1 & 0 & 0 \\ 2 & t & -1 \\ 4 & -2 & t-1 \end{vmatrix} \\ &= (t+1)(t^2-t-2) = (t+1)^2(t-2) \end{aligned}$$

だから、固有値は $\lambda = -1, 2$ である。

固有値 $\lambda = 2$ の固有ベクトルを求める。

$$\begin{pmatrix} 1 & 1 & -1 \\ -2 & -2 & 1 \\ -4 & -2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 2 \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

より、連立方程式を作り解くと (行列の簡約化を用いる方法がよいが、詳細は (2.7) を参照)、固有ベクトルは

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$$

である。

固有値 $\lambda = -1$ のときの固有ベクトルを求める。

$$\begin{pmatrix} 1 & 1 & -1 \\ -2 & -2 & 1 \\ -4 & -2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = - \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

より、連立方程式を作り解いていくと、

$$2x + y - z = 0$$

の 1 本しか残らない。3 個の未知数に対して式が 1 本で、**2 本不足しているので任意定数を 2 個導入して** $y = k$, $z = l$ とおくと，$x = \frac{1}{2}(-k + l)$ であ

る。したがって、固有ベクトルは、

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(-k+l) \\ k \\ l \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}k \\ k \\ 0 \end{pmatrix} + \begin{pmatrix} \frac{1}{2}l \\ 0 \\ l \end{pmatrix} = k \begin{pmatrix} -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix} + l \begin{pmatrix} \frac{1}{2} \\ 0 \\ 1 \end{pmatrix}$$

により、例えば $(k,l) = (2,0), (0,2)$ の 2 通りにすると 1 次独立な 2 つのベクトルが得られる[*2]。

よって、固有ベクトルは、

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$$

である。(**この先一切の新たな計算は必要としない**)。

1 次独立な固有ベクトルが 3 つ得られたので、対角化可能である。最後に対角化をする。このステップでは逆行列 P^{-1} を求めたり、行列の積 $P^{-1}AP$ を求めたりといった**計算は一切必要とせず対角化できる**ことに注意すること。得られた 3 つの固有ベクトルを並べて、

$P = \begin{pmatrix} -1 & -1 & 1 \\ 1 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$ とおくと、$P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ と対角化できる (**新たな計算は必要としない**)。最後の対角行列の対角成分は、固有ベクトルの並び順と対応する固有値である (**新たな計算は必要としない**)。

(3.4) **問題** 対角化可能ならば対角化せよ。

(1) $\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$ (3) $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & -1 \\ 3 & 2 & 1 \end{pmatrix}$ (4) $\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ -1 & 0 & 3 \end{pmatrix}$

[*2] もちろん $(k,l) = (1,0), (0,1)$ でも良いが、分数を避けて $(k,l) = (2,0), (0,2)$ を採用した。

(5) $\begin{pmatrix} 7 & 3 & -3 \\ -7 & -3 & 3 \\ 5 & 3 & -1 \end{pmatrix}$ (6) $\begin{pmatrix} -1 & 3 & -2 \\ 1 & 1 & -2 \\ -1 & -3 & 0 \end{pmatrix}$ (7) $\begin{pmatrix} -1 & 4 & -5 \\ 2 & -3 & 5 \\ 2 & -4 & 6 \end{pmatrix}$

§4 対称行列の対角化

(4.1) **内積と対称行列** $v, w \in \mathbb{R}^n$ を 2 つの縦ベクトルとし、$v \cdot w$ で内積を表すと、v と w をともに $n \times 1$ 行列と見たときの行列の積 ${}^t vw$ が内積 $v \cdot w$ に一致する。なぜなら、内積は、

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = v_1 w_1 + \cdots + v_n w_n$$

であり、行列の積は、

$${}^t \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1 v_2 \cdots v_n \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = v_1 w_1 + \cdots + v_n w_n$$

だからである。

また、A を n 次対称行列とすると、2 つの内積 $Av \cdot w$ と $v \cdot Aw$ は一致する。なぜなら

$$Av \cdot w = {}^t(Av)w = {}^t v\, {}^t A w = {}^t v({}^t A w) = v \cdot ({}^t A w)$$

であるが、A が対称行列なので最後の式は $v \cdot Aw$ に等しい。

(4.2) **命題** A を n 次の対称行列とし、v を固有値 λ の固有ベクトル、w を固有値 μ の固有ベクトルとする。$\lambda \neq \mu$ ならば、v と w は直交する。

Proof. v と w の内積が 0 であることを示せばよい。

$$(\lambda v)\cdot w = Av\cdot w = v\cdot Aw = v\cdot(\mu w)$$

となるので、$\lambda(v\cdot w)=\mu(v\cdot w)$ である。ここで、$\lambda\neq\mu$ なので、$v\cdot w=0$ である。 □

(4.3) **グラム・シュミットの直交化の簡単な場合** $v,w\in\mathbb{R}^n$ を 1 次独立なベクトルとする。一般には v と w は直交していないが、

$$w' = w - \frac{v\cdot w}{v\cdot v}v$$

と定めると、v と w' は直交する。

Proof. 内積の分配法則などを用いて実際に内積を計算すると、

$$v\cdot w' = v\cdot\left(w-\frac{v\cdot w}{v\cdot v}v\right) = v\cdot w - \frac{v\cdot w}{v\cdot v}v\cdot v = 0$$

となるから直交している。 □

(4.4) **対称行列の直交行列による対角化** A を n 次対称行列とする。対称行列は必ず対角化できることが知られている。従って、特に、1 次独立な n 個の固有ベクトル $v_1,v_2,\dots,v_n$ が存在することが保証されている。

その固有ベクトルのうち v_i と v_j の固有値が異なるならば、(4.2) より直交している。また、同じ固有値の固有ベクトルが複数あるときは、それらに対してグラム・シュミットの直交化を行い、互いに直交するベクトルにすることができる (3 個以上のベクトルに対する直交化も可能であるが、この授業では扱わない)。従って、$v_1,v_2,\dots,v_n$ はどの 2 つも直交しているベクトルでとることができる。

最後に、固有ベクトルの長さを 1 に縮める (場合によっては伸ばす) ことで、

$$v_i \cdot v_j = \begin{cases} 1 & (i = j) \\ 0 & (i \neq j) \end{cases}$$

を満たすような固有ベクトルがとれる。

この固有ベクトルを用いて、$P = (v_1\ v_2\ \cdots\ v_n)$ と定めると、

$$P\,{}^tP = I$$

を満たす。この条件を満たす行列を**直交行列**と呼ぶ。

以上をまとめると、対称行列 A は直交行列 P を用いて、

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

と対角化できる。

(4.5) **例題** $\begin{pmatrix} 5 & 1 & 1 \\ 1 & 5 & -1 \\ 1 & -1 & 5 \end{pmatrix}$ を直交行列で対角化せよ。

(解答) 固有値を求めると $\lambda = 3, 6$ である (6 が重解)。計算過程は省略する。

固有ベクトルは (これも求める過程は省略)、

$$\lambda = 3 : v_1 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}, \qquad \lambda = 6 : v_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

である。

同じ固有値の固有ベクトル同士は直交しているとは限らないので、v_2 と v_3 を直交化すると、

$$v_3' = v_3 - \frac{v_2 \cdot v_3}{v_2 \cdot v_2} v_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}$$

となり、これにより、v_1, v_2, v_3' は互いに直交する固有ベクトルである。分数の計算を避けるため、v_3' の代わりに $2v_3'$ を考えると、それぞれの大きさが、$\sqrt{3}, \sqrt{2}, \sqrt{6}$ なので、$v_1/\sqrt{3}, v_2/\sqrt{2}, 2v_3'/\sqrt{6}$ を並べて直交行列 P を作ると、

$$P = \begin{pmatrix} -1/\sqrt{3} & 1/\sqrt{2} & 1/\sqrt{6} \\ 1/\sqrt{3} & 1/\sqrt{2} & -1/\sqrt{6} \\ 1/\sqrt{3} & 0 & 2/\sqrt{6} \end{pmatrix} \text{ とおくと、} P^{-1}AP = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

と対角化できる。

(4.6) **問題** $\begin{pmatrix} 7 & 1 & -1 \\ 1 & 7 & -1 \\ -1 & -1 & 7 \end{pmatrix}$ を直交行列で対角化せよ。

§5 合同式

(5.1) **合同** 整数 a, b と整数 m に対し、$a - b$ が m の倍数であるとき、a と b は m を法として**合同**であると言い、$\boldsymbol{a \equiv b \pmod{m}}$ と書く。

例えば、

$$7 \equiv 13 \pmod{3},$$
$$7 \not\equiv 13 \pmod{4}$$

である。

m が正ならば、「m で割った余りが等しい」という関係と思ってよい。ただし、a や b が負の場合の割り算の余りには注意が必要である。

(5.2) **同値関係** 合同の関係は、次を満たす。

(E1) $a \equiv a \pmod{m}$ (反射律)
(E2) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$ (対称律)
(E3) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$ (推移律)

Proof. (1) $a - a = 0$ は、m の倍数だからである。
(2) $a - b$ が m の倍数ならば、$b - a$ も m の倍数だからである。
(3) 略 □

(5.3) **補題** 整数 a, b, c, d と整数 m に対して、$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ とするとき次が成り立つ。

(1) $a + c \equiv b + d \pmod{m}$
(2) $a - c \equiv b - d \pmod{m}$
(3) $ac \equiv bd \pmod{m}$

Proof. $a \equiv b \pmod{m}$ より、$a - b = km$ (k は整数)、$c \equiv d \pmod{m}$ より、$c - d = lm$ (l は整数) と書けることに注意しておく。
(1) $(a+c)-(b+d) = km-lm$ は m の倍数だから、$a+c \equiv b+d \pmod{m}$ である。
(2) 略
(3) $ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d) = kmb + blm$ は m の倍数だから、$ac \equiv bd \pmod{m}$ である。 □

(5.4) **例** $9+12 \equiv 4+2 \equiv 6 \equiv 1 \pmod 5$.

(5.5) **問題** 次の問に答えよ。

(1) $221 \times 329 \pmod{11}$ を簡単にせよ。
(2) $22^{22} \pmod 5$ を簡単にせよ。
(3) 23^{23} を 7 で割った余りを求めよ。

【ヒント】(2) では、

$$22^{22} \equiv 2^{22} \equiv (2^2)^{11} \equiv 4^{11} \pmod 5$$

のように、徐々に指数を減らすのが安直な方法である。

(5.6) **例 (n の倍数であることの判定法)**

(1) 正の整数の各位の数を加えて 3 の倍数になれば、元の整数も 3 の倍数である。
(2) 正の整数の各位の数を加えて 9 の倍数になれば、元の整数も 9 の倍数である。
(3) 正の整数の各位の数の交代和 (符号を交互に変えた和) が 11 の倍数になれば、元の整数も 11 の倍数である。
(4)「下 2 桁 + 残りの 2 倍」が 7 の倍数ならば、元の整数も 7 の倍数である (余りも保存)。例えば、12345 は、$123 \times 2 + 45 = 291$ であり、まだ 7 の倍数かどうか暗算でわからないので、$2 \times 2 + 91 = 95$ として、これは 7 で割ると 4 余るので、12345 も 7 で割ると 4 余るとわかる。

Proof. 正の整数 x を、0 から 9 までの整数 $a_0, \ldots, a_n$ を用いて、

$$x = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0$$

と表す。

(1) 3 を法として計算すると

$$\begin{aligned} x &\equiv 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 \\ &\equiv 1^n a_n + 1^{n-1} a_{n-1} + \cdots + 1a_1 + a_0 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3 \end{aligned}$$

となる。

最後の式は x の整数の各位の数を加えたものだから、x の整数の各位の数を加えて 3 の倍数になることと、x は 3 の倍数であることは同値である。

(2) 3 の倍数の場合と同様である。

(3) 11 を法として計算すると

$$\begin{aligned} x &\equiv 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 \\ &\equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \cdots + (-1)a_1 + a_0 \pmod{11} \end{aligned}$$

となる。

最後の式は x の整数の各位の数の交代和 (あるいはその -1 倍) だから、x の整数の各位の交代和が 11 の倍数になることと、x は 11 の倍数であることは同値である。

(4) 正の整数 x の下 2 桁を z $(0 \leq z \leq 99)$ とし、それより上の位を y とおく。つまり、$x = 100y + z$ である。「下 2 桁 + 残りの 2 倍」は $z + 2y$ と表せる。

$$100y + z \equiv 2y + z \pmod 7$$

なので、x を 7 で割った余りと「下 2 桁 + 残りの 2 倍」を 7 で割った余りは等しいから、x が 7 の倍数であることと、「下 2 桁 + 残りの 2 倍」が 7 の倍数であることは同値である □

(5.7) **問題** 次の問に答えよ。

(1) n を非負整数とするとき、$3^{n+2}+4^{2n+1}$ が 13 の倍数であることを示せ。
(2) n を非負整数とするとき、$3^{4n+1}+4^{n+1}$ が 7 の倍数であることを示せ。

【ヒント】普通、例えば高校の教科書でも、数学的帰納法で証明することが多い。ここでは、合同式を用いるのが速い。(1) であれば、13 を法として、$3^{n+2}+4^{2n+1} \equiv 3^n \times 3^2 + 4^{2n} \times 4^1 \equiv 3^n \times 9 + 16^n \times 4 \equiv 3^n \times 9 + 3^n \times 4 \pmod{13}$ と変形するとよい。

(5.8) **例題** 方程式 $96x \equiv 1 \pmod{29}$ の整数解を求めよ。
(解) まず、$96x + 29y = 1$ の整数解を求める (互除法を用いて解く方法があった)。経過は省略するが、$(x, y) = (13, -43)$ がひとつの解である。従って、$96 \cdot 13 - 29 \cdot 43 = 1$ である。これを法 29 で考えると、$96 \cdot 13 \equiv 1 \pmod{29}$ となるから、$x = 13$ が問題の方程式の 1 つの整数解である。

$96x \equiv 1 \pmod{29}$ と $96 \cdot 13 \equiv 1 \pmod{29}$ の辺々を引くと、$96(x-13) \equiv 0 \pmod{29}$ なので、96 と 29 が互いに素であることから、$x - 13$ は 29 の倍数であり、$x - 13 = 29k$ (k は整数) と書ける。よって、すべての解は、$x = 13 + 29k$ (k は整数) である。 □

(5.9) **問題** 次の方程式の整数解を求めよ。
(1) $13x \equiv 1 \pmod{35}$
(2) $35x \equiv 2 \pmod{13}$

§6 オイラーの定理

(6.1) 定義 (オイラーの関数) 正の整数 n に対して、1 から n までの整数のうち n と互いに素なものの個数を、$\boldsymbol{\phi(n)}$ で書く。この ϕ を**オイラーの関数**と呼ぶ。

例えば、$\phi(2)=1$, $\phi(3)=2$, $\phi(4)=2$, $\phi(5)=4$, $\phi(6)=2$ などである。

(6.2) 命題 (オイラーの関数の性質)

(1) 素数 p に対して、$\phi(p)=p-1$.
(2) 素数 p と正整数 n に対して、$\phi(p^n)=p^n-p^{n-1}$.
(3) 互いに素な正整数 m,n に対して、$\phi(mn)=\phi(m)\phi(n)$.

Proof. (1) 明らか。

(2) p^n と互いに素ということは p と互いに素ということだから、1 から p^n のうち、p の倍数が p^n/p 個あることよりわかる。

(3) $A=\{1,2,\dots,mn\}$, $M=\{0,1,\dots,m-1\}$, $N=\{0,1,\dots,n-1\}$ とおく。

まず、$a\in A$ に対して、$(a,mn)=1$ であることは、$(a,m)=1$ かつ $(a,n)=1$ であることと同値である $(*)$。

また、

$$\begin{array}{rccc} f: & A & \to & M\times N \\ & a & \mapsto & (a_1,a_2) \end{array}$$
$$a_1=(a\text{ を }m\text{ で割った余り}),\ a_2=(a\text{ を }n\text{ で割った余り})$$

と定めると、全単射である。実際、$a\equiv b \pmod m$ かつ $a\equiv b \pmod n$ とすると、m, n は互いに素だから $a-b$ は mn の倍数になるが、$-mn<$

$a-b<mn$ なので $a=b$ である。つまり、f は単射である。$|A|=|M\times N|$ なので全射である。

$(a_1,a_2)\in M\times N$ であって、$(a_1,m)=1$ であるものは $\phi(m)$ 個、$(a_2,n)=1$ であるものは $\phi(n)$ 個なので、f の全単射性と $(*)$ より、$(a,mn)=1$ となる $a\in A$ は $\phi(m)\phi(n)$ 個である。

□

(6.3) **オイラーの定理** 互いに素な正の整数 a,n に対して次の合同式が成立する。

$$a^{\phi(n)}\equiv 1 \pmod{n}.$$

Proof. $X=\{x_1,\dots,x_k\}$ を、1 から n までの整数のうち n と互いに素なもの全体とする $(k=\phi(n))$。また、n と互いに素な整数 a をとり、$Y=\{ax_1,\dots,ax_k\}$ とおくと、ax_j たちは mod n で重複はない。実際 $ax_i\equiv ax_j \pmod{n}$ ならば、$(a,n)=1$ より $x_i\equiv x_j \pmod{n}$ である。

mod n で X と Y は一致しているので、積をとっても一致しており、$ax_1\cdots ax_k\equiv x_1\cdots x_k \pmod{n}$ である。$x_1\cdots x_k$ は n と互いに素だから、$a^k\equiv 1 \pmod{n}$ を得る。 □

(6.4) **フェルマーの小定理** 素数 p と整数 a に対して、$a^p\equiv a \pmod{p}$.

Proof. オイラーの定理において、n を素数 p にすると、「a と p が互いに素のとき、$a^{\phi(p)}\equiv 1 \pmod{p}$」が得られる。$p$ が素数だから $\phi(p)=p-1$ なので、この両辺に a を掛けると、「a と p が互いに素のとき、$a^p\equiv a \pmod{p}$」が得られる。以上で a が p の倍数ではないときの証明が完了した。

a が p の倍数のときは、証明すべき式の両辺とも p の倍数であるから、$0 \equiv 0 \pmod{p}$ の形で合同式は成立しており、a が p の倍数のときも証明が完了した。 □

(6.5) **問題** 次の整数を、指定された法に関して合同な、最小の正整数にせよ。

(1) $5^{22} \pmod{19}$
(2) $19^{17} \pmod{17}$
(3) $22^{23} \pmod{17}$
(4) $5^{16} \pmod{48}$
(5) $7^{18} \pmod{60}$

【ヒント】例えば (1) では、安直な方法としては、

$$5^{22} \equiv (5^2)^{11} \equiv 25^{11} \equiv 6^{11} \pmod{19}$$

のように、徐々に指数を減らす方法もある。

あるいは、オイラーの定理を用いて $5^{18} \equiv 1 \pmod{19}$ がわかるので、これを利用すると少し楽になる。

(6.6) **ウィルソンの定理** 素数 p に対して、$(p-1)! \equiv -1 \pmod{p}$.

Proof. 1 から $p-1$ のうち、$x^2 \equiv 1$ を満たすのが、$x \equiv \pm 1$ だから、単元全体の積は -1. □

(6.7) **ウィルソンの定理の逆** 1 より大きい整数 m に対して、$(m-1)! \equiv -1 \pmod{m}$ ならば、m は素数である。

Proof. m が合成数ならば階乗の中に約数があるが、それは可逆ではないので階乗が単元にはならない。 □

§7 分数と小数

(7.1) **定義 (10 進表記)** 0 から 9 までの数字たち $a_n, a_{n-1}, \ldots, a_1, a_0$ と $b_1, b_2, b_3, \ldots$ が与えられたとする。a_n は 0 と異なるとする。このとき、**10 進表記**

$$a_n a_{n-1} \cdots a_1 a_0 \,.\, b_1 b_2 b_3 \cdots$$

の値を、

$$\begin{aligned} &10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 + \frac{b_1}{10^1} + \frac{b_2}{10^2} + \cdots \\ &\quad = \lim_{m\to\infty} (10^n a_n + \cdots + 10^1 a_1 + 10^0 a_0 + \frac{b_1}{10^1} + \frac{b_2}{10^2} + \cdots + \frac{b_m}{10^m}) \end{aligned}$$

で定める。

＊ これは絶対収束する (連続の公理と、小数部分が m によらず 1 を超えないので上界が存在することによる)。

＊ 1 つの表記に対して 1 つの実数が定まるのであり、1 つの実数に対して 1 つの表記が定まるというわけではない。つまり、1 という実数に対して「1」と「$0.999\cdots$」という 2 つの表記があることは、何の矛盾も引き起こさない。

(7.2) **問題** 有理数は有限小数または循環小数で表されることを示せ。

(7.3) **問題** 次の循環小数を既約分数に直せ。

(1) $0.1\dot{2}\dot{3} = 0.1232323\cdots$
(2) $1.2\dot{3}4\dot{5} = 1.2345345\cdots$

§8 循環小数

(8.1) **定義 (循環節)** 循環小数の、循環する部分のことを**循環節**と呼ぶ。また、循環小数が**純循環小数**であるとは、例えば $0.123123\cdots$ のように、循環節が小数第 1 位から始まることを言う。逆に、例えば $0.99123123\cdots$ のように、循環節が小数第 1 位よりも後ろから始まる循環小数を**混循環小数**と言う。

(8.2) **定理** 互いに素な正の整数 m, n に対して、既約分数 m/n を考える。a, b, c, n' を

$$n = 2^a 5^b n' \quad (n' \text{ は } 2 \text{ も } 5 \text{ も約数に持たない}),$$
$$c = \max\{a, b\}$$

で定める。

(1) m/n が有限小数であることと、$n' = 1$ であることは必要十分である。
(2) m/n が純循環小数であることと、$a = b = 0$ かつ $n' > 1$ であることは必要十分である。
(3) m/n が混循環小数であることと、$c > 0$ かつ $n' > 1$ であることは必要十分である。

また、これらの場合次が成り立つ。

(4) 有限小数の場合、小数第 c 位まである。

(5) 純循環小数の場合、循環節の長さは e である。
(6) 混循環小数の場合、循環節の長さは e であり、小数第 $c+1$ 位から循環が始まる。

ただし、e は、$10^e \equiv 1 \pmod{n'}$ を満たす最小の自然数である (存在は (6.3))。

Proof. (1) $n' = 1$ ならば、$m/n = m/(2^a 5^b)$ は分母を 10^c にできるから有限小数である。

反対に、有限小数は、分母が 10^e の形の分数で書け、これを既約分数に約分すれば、分母は $2^a 5^b$ の形になる。

(2) $n = n'$ だから、$10^e \equiv 1 \pmod{n}$ より $10^e = nk + 1$ と書ける (k は整数)。すると、

$$\begin{aligned} \frac{m}{n} = \frac{mk}{nk} &= \frac{mk}{10^e - 1} \\ &= \frac{mk \cdot 10^{-e}}{1 - 10^{-e}} \qquad \leftarrow (\text{等比級数の和の形をしている}) \\ &= \frac{mk}{10^e} + \frac{mk}{10^{2e}} + \frac{mk}{10^{3e}} + \cdots . \end{aligned}$$

ここで、$m < n$ より、$mk < nk = 10^e - 1$ だから mk は高々 e 桁の整数である。よって、m/n は e 桁ごとに同じ数字の来る小数に展開される。また、循環が小数第 1 位から始まることもわかる。

反対に、m/n が純循環小数だとし、循環節の長さが e' とすると、$m/n = m' \cdot 10^{-e'} + m' \cdot 10^{-2e'} + m' \cdot 10^{-3e'} + \cdots$ と書けるから、$m/n = m'/(1 - 10^{e'})$ となる。この分母は約分されたとしても 2 とも 5 とも互いに素であるから、$a = b = 0$ である。

(3) 転換法を用いると (1) と (2) より従う。

(4) 分母を 10^c にしたとき、分子が 10 の倍数ではないことと、小数点の移動量を考えると、ちょうど小数第 c 位まであることがわかる。

(5) (2) の証明の最後から続けると、m と n は互いに素だから、整数 k を用いて、$mk = m'$、$nk = 1 - 10^{e'}$ と書けるので、$10^{e'} \equiv 1 \pmod{n}$ となる。つまり、$10^e \equiv 1 \pmod{n}$ であることと、小数表示で e 桁ごとに同じ数字が来ることは同値である。従って、$10^e \equiv 1 \pmod{n}$ を満たす e の最小性と、循環節が反復する部分列のうち最小の長さのものと定義されていることから、循環節の長さは e である。

(6) $m/n = 10^{-c}(10^c m/n)$ と書くと、$c = \max\{a, b\}$ であることから、$10^c m/n$ は整数と純循環小数の和で表せる。従って循環節の長さが e であることはよい (分母にしかよらないので)。またこの変形から、m/n は遅くとも小数第 $c+1$ 位以降は循環することがわかる。

仮に、m/n が小数第 $c+1$ 位よりも早く、小数 $c'+1$ 位 ($c' < c$) から循環が始まるとすると、m/n に、ある $10^{c'}$ を掛けたときの小数部分が純循環小数になる。よって、$10^{c'} m/n$ を約分した後の分母は、素因数に 2 も 5 も含まない。これは c のとり方に反するので、m/n が小数第 $c+1$ 位よりも早く、循環を開始することはない。 □

(8.3) **注意** (1) 有限小数になるかどうかは、上で見たように進法に関係している。例えば、有限 2 進小数になる既約分数は、分母が 2^e の形の場合に限る。

(2) 循環小数の循環節の長さは分母のみで決まるが、既約でなければ、$1/21 = 0.\dot{0}47619\dot{}$ と $7/21 = 0.\dot{3}$ のように循環節の長さは異なるかも知れない。

(8.4) **例題** 次の分数が、有限小数、純循環小数、混循環小数のどれか。有限小数のとき小数第何位まであるか、純または混循環小数のとき循環節の長

さ、混循環小数のとき小数第何位から循環が始まるかも答えよ。ただし、実際に分子割る分母を計算することなく答えよ。
(1) $\frac{1}{40}$ (2) $\frac{3}{11}$ (3) $\frac{5}{12}$ (4) $\frac{1}{41}$

(解答) (1) 分母は $40 = 2^3 \cdot 5$ と、素因数が 2 と 5 しかないので有限小数である。ベキは 3 と 1 なので、大きい方をとって $c = 3$ だから、小数第 3 位までである。
(2) 分母の素因数に 2 も 5 もないので、純循環小数である。$10^e \equiv 1 \pmod{11}$ を満たす最小の正整数 e を探すと、

$$10^1 \equiv 10 \pmod{11}$$
$$10^2 \equiv 100 \equiv 1 \pmod{11}$$

だから $e = 2$. よって循環節の長さは 2 である。
(3) 分母は $12 = 2^2 \cdot 3$ であり、素因数に 2 (あるいは 5) も、2 や 5 以外も含むから混循環小数である。2 と 5 のベキはそれぞれ 2 と 0 なので、$c = 2$ であり、小数第 3 位から循環が始まる。また、循環節の長さは 1/3 と同じなので、1 である。
(4) 分母の素因数に 2 も 5 もないので、純循環小数である。$10^e \equiv 1 \pmod{41}$ を満たす最小の正整数 e を探すと、

$$10^1 \equiv 10 \pmod{41}$$
$$10^2 \equiv 100 \equiv 18 \pmod{41}$$
$$10^3 \equiv 1000 \equiv 16 \pmod{41}$$
$$10^4 \equiv 10000 \equiv 37 \pmod{41}$$
$$10^5 \equiv 100000 \equiv 1 \pmod{41}$$

だから $e = 5$. よって循環節の長さは 5 である。

ところが、10^5 を 41 で割った余りを安直に計算すると、分数 1/41 を単に割り算で小数にする計算と同じであり、効率はかえって悪くなっている。そ

こで、少し工夫すると、

$$\begin{aligned}
10^1 &\equiv 10 \pmod{41}\\
10^2 &\equiv 100 \equiv 18 \pmod{41}\\
10^3 &\equiv 180 \equiv 16 \pmod{41}\\
10^4 &\equiv 160 \equiv 37 \pmod{41}\\
10^5 &\equiv 370 \equiv 1 \pmod{41}
\end{aligned}$$

などとも計算できる。

(8.5) **問題** 次の分数が、有限小数、純循環小数、混循環小数のどれか。有限小数のとき小数第何位まであるか、純または混循環小数のとき循環節の長さ、混循環小数のとき小数第何位から循環が始まるかも答えよ。ただし、実際に分子割る分母を計算することなく答えよ。
(1) $\dfrac{1}{13}$ (2) $\dfrac{3}{220}$ (3) $\dfrac{7}{1280}$

(8.6) **例 (循環節の長さ)** 次の例では、循環節の長さがオイラーの関数の約数になっていることが確認できる。

(1) 分数 $1/7$ を考える。$1/7 = 0.\dot{1}42857\dot{}$ であり、循環節の長さは 6 である。オイラーの関数は $\phi(7) = 6$ である。
(2) 分数 $11/21$ を考える。$11/21 = 0.\dot{5}23809\dot{}$ であり、循環節の長さは 6 である。また、オイラーの関数は $\phi(21) = 12$ である。
(3) 分数 $10/13$ を考える。$10/13 = 0.\dot{7}69230\dot{}$ であり、循環節の長さは 6 である。また、オイラーの関数は $\phi(13) = 12$ である。

(8.7) 命題 (指数) 互いに素な正の整数 a, n に対して合同式

$$a^e \equiv 1 \pmod{n}.$$

が成立するような最小の正整数 e は、オイラーの関数 $\phi(n)$ の約数である。

従って、m を正整数、n を 10 と互いに素な正整数とするとき、既約真分数 m/n を循環小数にしたときの循環節の長さは、$\phi(n)$ の約数である。

＊このことから、($a = 10$ とすると) 上の例で見た事実が、常に成り立つことがわかる。

Proof. $\phi(n)$ を e で割り、

$$\phi(n) = e \cdot p + r \quad (p, r \in \mathbb{Z},\ 0 \leq r < e)$$

と表す。オイラーの定理より、$a^{\phi(n)} \equiv 1 \pmod{n}$ が成り立つから、

$$1 \equiv a^{\phi(n)} \equiv a^{ep+r} \equiv (a^e)^p \cdot a^r \equiv a^r \pmod{n}$$

となり、r も $a^r \equiv 1 \pmod{n}$ を満たすが、r は e より小さいので、e の最小性より $r = 0$ でなくてはならない。つまり、$\phi(n) = e \cdot p$ となり、e は $\phi(n)$ の約数である。 □

(8.8) 問題 (有限、純循環、混循環小数になる分数を求める)

(1) 小数第 5 位まである有限小数になるような分数を 1 つ答えよ。
(2) 純循環小数になるような分数を 1 つ答えよ。
(3) 小数第 4 位から循環節が始まるような混循環小数になるような分数を 1 つ答えよ。

§9 ベクトル空間の基礎

(9.1) **ベクトル空間** 集合 V が体 K 上の**ベクトル空間**であるとは、V に和 $(v+w)$ と、K の元によるスカラー倍 (kv) が定義されており、$u,v,w \in V$ と $a,b \in K$ に対して、(V1)–(V8) を満たすことを言う。

(V1) $u+v=v+u$ (和の交換法則)
(V2) $(u+v)+w=u+(v+w)$ (和の結合法則)
(V3) $u+0=u=0+u$ なるベクトル 0 (零ベクトル) が存在する
(V4) $a(bu)=(ab)u$ (スカラー倍の結合法則)
(V5) $(a+b)u=au+bu$ (分配法則)
(V6) $a(u+v)=au+av$ (分配法則)
(V7) $1u=u$
(V8) $0u=0$

ベクトル空間 V の部分集合 W が, V の**部分空間**であるとは, W が零ベクトルを含み, V と同じ和とスカラー倍で閉じているときを言う. つまり, 任意の $w_1,w_2,w \in W$ と スカラー k に対して, $w_1+w_2 \in W$ かつ $kw \in W$ なるときを言う.

(9.2) **例** 以下はすべて $\mathbb{R}$ 上のベクトル空間の例である。
(1) 実数成分の n 次の縦ベクトル全体の集合 $\mathbb{R}^n$
ベクトルの通常の和と実数倍によりベクトル空間になる。以下の例も含め、たいていの場合、一番重要なのは和、とスカラー倍で閉じていることであり、(V1)–(V8) は明らかに成立していることが多い。
(2) 実数成分の $m \times n$ 行列全体の集合 $\mathrm{Mat}(m,n;\mathbb{R})$
これも同様に、行列どうしの和と、行列の実数倍で閉じていることをチェックすれば良い。行列には積があるが、ベクトル空間として見る場合は、行列どうしの積は無関係である (そもそも正方行列の集合でなければ積が定義されない)。
また、この例では、「縦ベクトル」のような、高校までの数ベクトルは無関

係であることにも注意する。ベクトル空間とは数ベクトルの集合のことではなく、和とスカラー倍で閉じている集合のことである。

(3) 実数係数 1 変数多項式全体の集合 $\mathbb{R}[x]$

この例も数ベクトルは無関係である。多項式どうしの和と、多項式の実数倍によりベクトル空間になる。また、先の例と同じく、$\mathbb{R}[x]$ をベクトル空間と見る場合は、多項式どうしの積や商は無関係である。

(4) 正の実数全体の集合 $\mathbb{R}_+$ から $\mathbb{R}$ への写像全体の集合 $\mathrm{Map}(\mathbb{R}_+, \mathbb{R})$

和は、$f, g \in \mathrm{Map}(\mathbb{R}_+, \mathbb{R})$ に対して、写像 $f+g$ を

$$\begin{aligned}(f+g) :&\mathbb{R}_+ \to \mathbb{R}\\ &x \mapsto f(x)+g(x)\end{aligned}$$

で定める。つまり、$(f+g)(x) = f(x)+g(x)$ である。

$f+g$ の定義域が $\mathbb{R}_+$ であることは明らかで、$f(x), g(x) \in \mathbb{R}$ より $f(x)+g(x) \in \mathbb{R}$ だから、$f+g$ の像が $\mathbb{R}$ に属することもわかる。よって、$f+g \in \mathrm{Map}(\mathbb{R}_+, \mathbb{R})$ であり、和で閉じている。

実数倍は、$k \in \mathbb{R}$ と $f \in \mathrm{Map}(\mathbb{R}_+, \mathbb{R})$ に対して、

$$\begin{aligned}(kf) :&\mathbb{R}_+ \to \mathbb{R}\\ &x \mapsto k(f(x))\end{aligned}$$

で定める。つまり、$(kf)(x) = k(f(x))$ である。

kf の定義域が $\mathbb{R}_+$ であることは明らかで、$k, f(x) \in \mathbb{R}$ より、$k(f(x)) \in \mathbb{R}$ だから、kf の像が $\mathbb{R}$ に属することもわかる。よって、$kf \in \mathrm{Map}(\mathbb{R}_+, \mathbb{R})$ であり、実数倍で閉じている。

他方、以下はベクトル空間ではない。

(5) 整数成分の n 次の縦ベクトル全体の集合 $\mathbb{Z}^n$

$\mathbb{R}$ などの体には $1/2$ が属するので、スカラー倍で閉じていないからである。

(6) 0 以上の実数を成分とする n 次の縦ベクトル全体の集合

$\mathbb{R}$ などの体には -1 が属するので、スカラー倍で閉じていないからである。

(7) $\mathbb{R}$ から正の実数全体の集合 $\mathbb{R}_+$ への写像全体の集合 $\mathrm{Map}(\mathbb{R}, \mathbb{R}_+)$

先の (4) と同様にスカラー倍で閉じているかを考えたとき、$k \in \mathbb{R}$ と $f \in \mathrm{Map}(\mathbb{R}, \mathbb{R}_+)$ に対して、$k \in \mathbb{R}$ だが、$f(x) \in \mathbb{R}_+$ なので、$k(f(x)) \in \mathbb{R}_+$ とは限らない。よって、$kf \notin \mathrm{Map}(\mathbb{R}, \mathbb{R}_+)$ であり、スカラー倍では閉じていない。

(9.3) **例題** 次の部分集合が部分ベクトル空間 (部分空間) であることを証明せよ。

(1) 平面上の x 軸をベクトル空間 $\mathbb{R}^2$ の部分集合とみたとき、部分空間であることを証明せよ。

(2) $A = \begin{pmatrix} 1 & 2 & 3 \\ -3 & -2 & -1 \end{pmatrix}$ のとき, $\mathbb{R}^3$ の部分集合 $V = \left\{ x \in \mathbb{R}^3 \mid Ax = 0 \right\}$ が部分空間であることを証明せよ。

Proof. (1) 和とスカラー倍で閉じていることを言えばよい。

[和で閉じていること] x 軸上の 2 点 $(a, 0), (b, 0)$ に対して、その和 $(a, 0) + (b, 0) = (a + b, 0)$ も x 軸上にあるから、和で閉じている。

[スカラー倍で閉じていること] 実数 k と x 軸上の点 $(a, 0)$ に対して、$k(a, 0) = (ka, 0)$ も x 軸に属するから、スカラー倍で閉じている。

(2) 行列 A の成分が具体的に書かれているが、実は必要ない。

ベクトル x が集合 V に属する条件は、$Ax = 0$ である。従って、(a) あるベクトル x が集合 V に属していれば、$Ax = 0$ を満たす。そして、この逆を活用できない人も多いが、(b) あるベクトル x が集合 V に属することを示したいならば、$Ax = 0$ を示せばよいことに注意する。

[和で閉じていること] $x, y \in V$ を取る。(a) により $Ax = 0$ と $Ay = 0$ が成立する。$A(x + y) = Ax + Ay = 0 + 0 = 0$ だから、(b) により $x + y \in V$

である。よって、V は和で閉じている。

[スカラー倍で閉じていること] $k \in \mathbb{R}$ と $x \in V$ を取る。(a) により、$Ax = 0$ である。$A(kx) = k(Ax) = k0 = 0$ だから、(b) により $kx \in V$ である。よって、V はスカラー倍で閉じている。 □

(9.4) **問題** 次の部分集合がベクトル空間 (部分空間) であることを証明せよ。

(1) xy-平面 $\mathbb{R}^2$ の部分集合，直線 $y = x$.

(2) A を $m \times n$ 行列とするとき，$\mathbb{R}^n$ の部分集合 $\{x \in \mathbb{R}^n \mid Ax = 0\}$.

(3) n 次正方行列全体のなすベクトル空間 $\mathrm{Mat}(n;\mathbb{R})$ の部分集合 $\{B \in \mathrm{Mat}(n;\mathbb{R}) \mid b_{ij} = 0\ (i > j)\}$ (**上三角行列**全体の集合).

§10 線型写像

(10.1) **線型写像** V, W を体 K 上のベクトル空間とするとき、写像 $f : V \to W$ が**線型写像**であるとは、次の条件を満たすことを言う。

(L1) $f(v_1 + v_2) = f(v_1) + f(v_2) \quad (v_1, v_2 \in V)$
(L2) $f(av) = af(v) \quad (a \in K, v \in V)$

このとき、

$$\mathrm{Ker}(f) = \{v \in V \mid f(v) = 0\}, \qquad \mathrm{Im}(f) = \{f(v) \in W \mid v \in V\},$$

と定め、それぞれ f の**核** (**カーネル**)、**像** (**イメージ**) と呼ぶ。

少しややこしいが、$v \in V$ のとき $f(v)$ のことも v の f による**像**と呼ぶ。

(10.2) **問題** $f : V \to W$ を線型写像とするとき、次を証明せよ。
(1) $f(0) = 0$
(2) $v, v' \in V$ に対して、(L1′) $f(v - v') = f(v) - f(v')$

【ヒント】(1) $0 \cdot 0 = 0$ (左辺の左の 0 はスカラー、左辺の右の 0 と右辺の 0 は零ベクトル) を f で写して、(L2) を用いよ。

(2) $v - v' = v + (-1)v'$ という変形をした後、(L1) と (L2) を用いよ。

(10.3) **命題** 線型写像 $f : V \to W$ の線型写像の核は V の、像は W の、それぞれ部分空間である。

Proof. まず、核について、和とスカラー倍で閉じていることを示す。$v \in V$ が、$\mathrm{Ker}(f)$ に属するための条件は、$f(v) = 0$ である。従って、(a) $v \in \mathrm{Ker}(f)$ ならば、$f(v) = 0$ であり、反対に、(b) $v \in V$ が $v \in \mathrm{Ker}(f)$ であることを示したいならば、$f(v) = 0$ であることを示せばよいことに注意する。

[核が和で閉じていること] $v_1, v_2 \in \mathrm{Ker}(f)$ を取ると、(a) より、$f(v_1) = f(v_2) = 0$ である。このとき、f は線型写像だから (L1) を用いると、$f(v_1 + v_2) = f(v_1) + f(v_2) = 0 + 0 = 0$ である。よって、(b) より、$v_1 + v_2 \in \mathrm{Ker}(f)$ である。

[核がスカラー倍で閉じていること] $v \in \mathrm{Ker}(f)$ とスカラー a をとったとき、(a) より、$f(v) = 0$ である。このとき、f は線型写像だから (L2) を用いると、$f(av) = af(v) = a0 = 0$ である。よって、(b) より、$av \in \mathrm{Ker}(f)$ である。

次に像について証明する。

[像が和で閉じていること] $w_1, w_2 \in \mathrm{Im}(f)$ をとったとき、像の定義より、$w_1 = f(v_1)$, $w_2 = f(v_2)$ なる $v_1, v_2 \in V$ がある。f は線型写像だから (L1) を用いると、

$$w_1 + w_2 = f(v_1) + f(v_2) = f(v_1 + v_2)$$

であり、w_1+w_2 は v_1+v_2 の f による像であるから、$w_1+w_2 \in \mathrm{Im}(f)$ である。

[像がスカラー倍で閉じていること] $w \in \mathrm{Im}(f)$ とスカラー a をとったとき、像の定義より、$w=f(v)$ なる $v \in V$ がある。このとき、f は線型写像だから (L2) を用いると、

$$aw = af(v) = f(av)$$

となり、aw は av の f による像だから、$aw \in \mathrm{Im}(f)$ である。 □

(10.4) **例題** 次の写像は線型写像かどうか答えよ。また、線型写像であるものは、その核と像を求めよ。

(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = \sin x)$

(2) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = 3x)$

(3) $f : \mathbb{R}^2 \to \mathbb{R}^2$ $\left(f\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}1&2\\3&6\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}\right)$

((1) の解答) $\sin(x+y) = \sin x + \sin y$ は成り立たないし、$\sin ax = a\sin x$ も成り立たないから線型写像ではない。

((2) の解答) $f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$ だから (L1) は成立。$f(ax) = 3(ax) = a(3x) = af(x)$ だから (L2) も成立。よって線型写像である。

核は、

$$\mathrm{Ker}(f) = \{x \in \mathbb{R} \mid f(x) = 0\} = \{x \in \mathbb{R} \mid 3x = 0\} = \{0\}$$

である。

像について、x が $\mathbb{R}$ 全体を動くとき、$f(x) = 3x$ も $\mathbb{R}$ 全体を動くから、$\mathrm{Im}(f) = \mathbb{R}$ である。

((3) の解答) $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$, $v = \begin{pmatrix} x \\ y \end{pmatrix}$, $v' = \begin{pmatrix} x' \\ y' \end{pmatrix}$ とおくと、$f(v+v') = A(v+v') = Av + Av' = f(v) + f(v')$ だから (L1) は成立。$f(av) = A(av) = a(Av) = af(v)$ だから (L2) も成立。よって線型写像である ((2) の証明とほぼ同様だったことと、A の成分は必要ではなかったことにも注意せよ)。

核は、

$$\begin{aligned} \mathrm{Ker}(f) &= \{v \in \mathbb{R}^2 \mid Av = 0\} \\ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; \begin{array}{l} x + 2y = 0, \\ 3x + 5y = 0 \end{array} \right\} \end{aligned}$$

となるが、最後の条件の連立方程式は、一意的な解 $x = y = 0$ を持つ (行列 A が正則だからという理由でも良い)。従って、$\mathrm{Ker}(f) = \{0\}$ である (零ベクトルを単に 0 と書いている)。

像を求める。行列 A が正則だから、任意の $w \in \mathbb{R}^2$ (ここの $\mathbb{R}^2$ は定義域の $\mathbb{R}^2$ ではなく、写像の行き先の $\mathbb{R}^2$ である) を取ったとき、$v = A^{-1}w$ と置くと、$f(v) = Av = AA^{-1}w = w$ である。つまり、任意の $w \in \mathbb{R}^2$ は f の像になっているから、$\mathrm{Im}(f) = \mathbb{R}^2$ (これも写像の行き先の $\mathbb{R}^2$) である。

(10.5) **問題** 次の写像は線型写像かどうか答えよ。また、線型写像であるものは、その核と像を求めよ。

(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = -x)$

(2) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = \cos x)$

(3) $f : \mathbb{R}^2 \to \mathbb{R}^2$ $(f(v) = 2v)$

(4) $f : \mathbb{R}^3 \to \mathbb{R}^3$ $\left(f \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 5 \\ -1 & \sqrt{2} & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right)$

(10.6) **問題** $\mathbb{R}[x]$ を実数係数の 1 変数多項式全体のなすベクトル空間とする。

(1) 写像 $D : \mathbb{R}[x] \to \mathbb{R}[x]$ を、微分 $D(f) = f'$ で定めたとき、D は線型写像であることを証明せよ。
(2) 写像 $I : \mathbb{R}[x] \to \mathbb{R}[x]$ を、定積分

$$I(f) = \int_0^x f(t)\,dt$$

で定めたとき、I は線型写像であることを証明せよ。

(10.7) **命題** $f : U \to V$ と $g : V \to W$ がともに線型写像であるとき、合成写像 $g \circ f : U \to W$ も線型写像である。

Proof. まず (L1) について。$u, u' \in U$ に対して、

$$\begin{aligned}
(g \circ f)(u + u') &= g(f(u + u')) \\
&= g(f(u) + f(u')) && (f \text{ の (L1) を用いた}) \\
&= g(f(u)) + g(f(u')) && (g \text{ の (L1) を用いた}) \\
&= (g \circ f)(u) + (g \circ f)(u')
\end{aligned}$$

だから、$g \circ f$ は (L1) を満たす。

次に (L2) について。$u \in U$ とスカラー a に対して、

$$\begin{aligned}
(g \circ f)(au) &= g(f(au)) \\
&= g(af(u)) && (f \text{ の (L2) を用いた}) \\
&= ag(f(u)) && (g \text{ の (L2) を用いた}) \\
&= a(g \circ f)(u)
\end{aligned}$$

だから、$g \circ f$ は (L2) を満たす。 □

(10.8) **命題** $f : V \to W$ を線型写像とするとき、f が単射であることと、$\mathrm{Ker}(f) = \{0\}$ であることは同値である。

Proof. f が単射であることの定義は、$v, v' \in V$ に対して、$f(v) = f(v')$ ならば、$v = v'$ となることであった (単射を形式的に言えば、「f を外せる」ことである)。

[f が単射ならば $\mathrm{Ker}(f) = \{0\}$] f が単射であるとする。$v \in \mathrm{Ker}(f)$ に対して、$f(v) = 0$ であるが、$f(0) = 0$ でもあるから、f の単射性により、$v = 0$ である。よって $\mathrm{Ker}(f) = \{0\}$ である。

[$\mathrm{Ker}(f) = \{0\}$ ならば f が単射] $v, v' \in V$ に対して、$f(v) = f(v')$ とする。(L1′) を用いると、$0 = f(v) - f(v') = f(v - v')$ となり、$v - v' \in \mathrm{Ker}(f)$ である。しかし、核が $\{0\}$ なので、$v - v' = 0$、つまり、$v = v'$ となる。よって、f は単射である。 □

(10.9) **問題** 線型写像 $f : \mathbb{R}^n \to \mathbb{R}^m$ の像 $\mathrm{Im}(f)$ について答えよ。
(1) $v_1, \ldots, v_n$ を $\mathbb{R}^n$ の基底とするとき、$\mathrm{Im}(f)$ は $f(v_1), \ldots, f(v_n)$ で生成されることを証明せよ。[ヒント: 任意の $\mathbb{R}^n$ の元は，$v_1, \ldots, v_n$ の 1 次結合で表せることを用いて、任意の $\mathrm{Im}(f)$ の元が，$f(v_1), \ldots, f(v_n)$ の 1 次結合で表せることを示す]
(2) $v_1, \ldots, v_n$ を並べてできる行列の階数を k とすると、$\mathrm{Im}(f)$ の次元は k であることを証明せよ。

(10.10) **表現行列** $v_1, \ldots, v_n$ をベクトル空間 V の基底とし、$w_1, \ldots, w_m$ をベクトル空間 W の基底とする。線型写像 $f : V \to W$ があるとき、その

像に属するベクトルは $w_1, \ldots, w_m$ の 1 次結合で書けるから、$m \times n$ 行列 A を用いて $(f(v_1), \ldots, f(v_n)) = (w_1, \ldots, w_m)A$ と行列で表示できる。この A を V の基底 $v_1, \ldots, v_n$ と W の基底 $w_1, \ldots, w_m$ に関する f の**表現行列**と呼ぶ。

(10.11) **例題** 線型写像 $f : \mathbb{R}^2 \to \mathbb{R}^3$ は

$$f\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\2\\3\end{pmatrix}, \qquad f\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}4\\5\\6\end{pmatrix}$$

で定められている。このとき、$\mathbb{R}^2$ と $\mathbb{R}^3$ の標準基底に関する f の表現行列は、

$$A = \begin{pmatrix}1 & 4\\2 & 5\\3 & 6\end{pmatrix}$$

であることを示せ。

(解答) 与えられた式を $\mathbb{R}^2$ と $\mathbb{R}^3$ の標準基底を用いて書き直すと、$f(e_1) = 1e_1 + 2e_2 + 3e_3$, $f(e_2) = 4e_1 + 5e_2 + 6e_3$ である。これを行列で表示すれば、

$$(f(e_1), f(e_2)) = (e_1, e_2, e_3)\begin{pmatrix}1 & 4\\2 & 5\\3 & 6\end{pmatrix}$$

だから、表現行列が A であることが示された。

(10.12) **問題** 次で定まる線型写像 $f : \mathbb{R}^3 \to \mathbb{R}^2$ の、$\mathbb{R}^3$ と $\mathbb{R}^2$ の標準基底に関する f の表現行列を求めよ。

$$f\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\3\end{pmatrix}, \qquad f\begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}4\\5\end{pmatrix}, \qquad f\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}7\\2\end{pmatrix}.$$