2016 年度 前期 代数学演習 1

更新日時 2016-07-19 17:16:54　担当 和地 輝仁

目 次

1　シラバス抜粋

授業の目標　代数学 1 で学んだ複素数や対称群，代数学 2 で学んだ初等整数論や環論，さらに，その基盤にある線型代数学に関する演習を通して，これらに対する理解や習熟を深める．また，代数学 1 や代数学 2 で学んだ内容の発展・応用にあたる内容の演習を通して，より専門的な数学が初歩的な内容に対しても統一的な視点を与えることを実感できるよう習熟を深める．

到達目標

1. 複素数の性質や演算に習熟する．
2. 対称群の性質や演算に習熟する．
3. 行列式・逆行列の計算や性質に習熟する．
4. 線型代数の理論を抽象的なベクトル空間に適用できる．
5. 環とイデアルの性質に習熟する．

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. 複素数の演習
2. 複素数平面の演習
3. ドモアブルの定理の演習
4. 対称群の演習
5. 対称式の演習
6. 行列式の演習
7. 逆行列の演習
8. ベクトル空間の基礎
9. ベクトル空間の演習
10. 線型写像の演習
11. 部分空間の演習
12. 有理整数環の演習
13. 多項式環の演習
14. イデアルの演習
15. 期末試験

成績評価　期末試験 (50%) と，毎回の演習問題の状況 (50%) 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．

2 授業のノート

§1 複素数

(1.1) 基本事項

- (虚数単位 i) $i^2 = -1$ を満たす.
- (複素数の相等) $a + bi = c + di$ ならば $a = c, b = d$
- 実部，虚部，共役な複素数 $\overline{z}$
- 和，差，積，商の計算
- (0 以外に零因子がない) $z, w \neq 0$ ならば $zw \neq 0$.
- (負数の平方根) $a > 0$ のとき，$\sqrt{-a} = \sqrt{a}i$
- (解と係数の関係) $ax^2 + bx + c = 0$ の解を α, β とすると，$\alpha + \beta = -b/a$, $\alpha\beta = c/a$.

(1.2) **問題** 計算して簡単にせよ.
(1) $(2 + 3i) + (4 - 5i)$ (2) $(2 - 3i) - (-4 - 5i)$
(3) $(1 - 2i)(3 + 4i)$ (4) $(2 + 3i)^2$ (5) $(1 + 2i)^3$ (6) i^{10}

(1.3) **問題** 次の等式を満たす実数 x, y の値を求めよ.
(1) $(x + y) + (x - y)i = 5 - i$
(2) $(x + yi)(2x + yi) = 17 - 9i$
(3) $(x + 2i)(x - yi) = 8$

(1.4) **問題** 次の複素数 z に対して，$z + \overline{z}$, $z - \overline{z}$, $z\overline{z}$ を計算せよ.
(1) $z = 1 + i$ (2) $z = 2 - 3i$ (3) $z = a - bi$ (a, b は実数)

(1.5) **問題** 計算して簡単にせよ.
(1) $\dfrac{1}{1+i}$ (2) $\dfrac{1+i}{2+i}$ (3) $\dfrac{1+i}{1-i} - \dfrac{1-i}{1+i}$

(1.6) **問題** 計算して簡単にせよ.
(1) $\sqrt{-3}$ (2) $\sqrt{-4}$ (3) $\sqrt{-2} - \sqrt{-8}$ (4) $\sqrt{-2}\sqrt{-3}$
(5) $\sqrt{-2}\sqrt{-3}\sqrt{-4}$

(1.7) **問題** 次の 2 次方程式を複素数の範囲で解け.
(1) $x^2 = -1$ (2) $x^2 + 2 = 0$ (3) $x^2 + x + 1 = 0$
(4) $x^2 - \sqrt{2}x + 2 = 0$

(1.8) **問題** 次の 2 次式を複素数の範囲で因数分解せよ.
(1) $x^2 + 3$ (2) $x^2 - x + 1$ (3) $x^2 - 2x + 5$

(1.9) **問題** 2 次方程式 $x^2 + x + 1$ の 2 解を α, β とするとき，次の式の値を求めよ.
(1) $\alpha + \beta$ (2) $\alpha\beta$ (3) $\alpha^2 + \beta^2$ (4) $(\alpha - \beta)^2$
(5) $\dfrac{1}{\alpha} + \dfrac{1}{\beta}$ (6) $\dfrac{\beta}{\alpha} + \dfrac{\alpha}{\beta}$

(1.10) **問題** 次の 2 数を解に持つ 2 次方程式を答えよ.
(1) $i, -i$ (2) $1 + i, 1 - i$ (3) $2 - 3i, 2 + 3i$

§2 複素数平面

(2.1) 基本事項

- 平面上の点 (a, b) と複素数 $a + bi$ が対応
- 実軸，虚軸
- 共役複素数は実軸に関して対称な点に相当
- 実数倍，和，差は，ベクトルの同じ操作に相当
- 絶対値 $|z|$, 偏角 $\arg z$, 極形式 $r(\cos\theta + i\sin\theta)$
- 積，商は，原点を中心とする点の回転と拡大に相当．特に，i を掛けると原点中心に 90° 回転する.

- ド・モアブルの定理 $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$
- n 乗根は単位円の n 等分点に相当
- (平行条件) 3 複素数 $0, z, w$ が同一直線上にあることは，z と w の一方が他方の実数倍であることと必要十分.
- (垂直条件) 3 複素数 $0, z, w$ があるとき，$\angle z0w = 90°$ であることは，$0, z, iw$ が同一直線上にあると考えればよい.

(2.2) **問題** 次の複素数 z について，z, $-z$, $2z$, $\overline{z}$ を複素数平面に図示せよ．また，z と虚軸に関して対称な点を求めよ.
(1) $z = 1 + 2i$ (2) $z = -2 + 3i$ (3) $z = 3$ (4) $z = -i$

(2.3) **問題** 次の複素数 z, w について，0, z, w が同一直線上にあるとき，実数 a の値を定めよ.
(1) $z = 2 - i$, $w = a + 2i$ (2) $z = 2 - 3i$, $w = 3 + ai$

(2.4) **問題** 次の複素数 z, w について，z, w, $z + w$, $z - w$ を図示せよ.
(1) $z = 2 - i$, $w = 1 + 2i$ (2) $z = -3 + i$, $w = 2 - 2i$

(2.5) **問題** 次の複素数の絶対値と偏角を求めよ.
(1) $z = 1 + i$ (2) $z = -2 + 2i$ (3) $z = -\sqrt{3} + i$
(4) $z = \sqrt{3} - 3i$ (5) $z = 2$ (6) $z = -i$

(2.6) **問題** 2 つの複素数 z, w に対して，$|z + w| \leq |z| + |w|$ が成り立つことを証明せよ．また，等号成立の条件も言え．[ヒント: $z = a + bi$, $w = c + di$ とおいて，左辺と右辺を a, b, c, d で表して考えるのも 1 つの手段．しかし，3 複素数 $0, z, w$ を複素数平面上に書いて，何か三角形を考えるのがより簡明．]

(2.7) **問題** (1) 実数係数の 2 次方程式が複素数 z を解に持つならば，$\overline{z}$ も解であることを証明せよ.
(2) 実数係数の n 次方程式が複素数 z を解に持つならば，$\overline{z}$ も解であることを証明せよ.
[ヒント: (1) ならば，$ax^2 + bx + c = 0$ が z を解に持つならば，$az^2 + bz + c = 0$ を満たす．これの両辺の複素共役をとり，あとは証明の筋道を組み立てよ．]

(2.8) **問題** 次の複素数を極形式で表せ.
(1) $z = 1 - i$ (2) $z = -2 - 2i$ (3) $z = \sqrt{3} + i$
(4) $z = -\sqrt{3} + 3i$ (5) $z = -2$ (6) $z = 2i$

(2.9) **問題** 複素数 z に対して，次の値を z を用いて表せ.
(1) $|-z|$ (2) $|\overline{z}|$ (3) $\arg(-z)$ (4) $\arg(\overline{z})$ (5) $\arg(-\overline{z})$

(2.10) **問題** $z = \cos\theta + i\sin\theta$ のとき，次の複素数を極形式で表せ.
(1) $-z$ (2) $\overline{z}$ (3) $-\overline{z}$

(2.11) **問題** 積 $r_1(\cos\alpha + i\sin\alpha) \cdot r_2(\cos\beta + i\sin\beta)$ の偏角と絶対値を求めよ．また，極形式で表せ.

(2.12) **問題** 次の問に答えよ.
(1) 複素数 z の逆数 z^{-1} の偏角と絶対値を，z を用いて表せ.
(2) 2 つの複素数 z, w の商 $\dfrac{z}{w}$ の偏角と絶対値を，z, w を用いて表せ.

(2.13) **問題** 次の問に答えよ.
(1) $2 - i$ を原点中心に 30° 回転した点を求めよ.
(2) $-2 + 3i$ を原点中心に 120° 回転した点を求めよ.
(3) 複素数 z を原点中心に 90° 回転した点を z を用いて表せ.
(4) 2 点 z, $-iz$ の位置関係を言え.

(2.14) **問題** 計算し簡単にせよ.
(1) $(\cos 30° + i\sin 30°)^{10}$ (2) $(\cos 120° + i\sin 120°)^{20}$
(3) $(1 + i)^8$ (4) $(\sqrt{3} - i)^{10}$

(2.15) **問題** 次の累乗根を (複素数の範囲で) 求め，複素数平面に図示せよ．
(1) 1 の 3 乗根をすべて求めよ
(2) 2 の 4 乗根をすべて求めよ．
(3) 16 の 8 乗根をすべて求めよ．

(2.16) **問題** 1 の 7 乗根のうち，1 ではないものをひとつとり α とする．1 でも α でもない残り 5 つの 7 乗根を α を用いて表せ．

(2.17) **問題** 次を証明せよ．ただし，α, β, γ, δ は異なる複素数とする．
(1) 3 点 α, β, γ が同一直線上にあるための必要十分条件は，$\dfrac{\gamma-\alpha}{\beta-\alpha}$ が実数であることである．
(2) 2 直線 $\alpha\beta$, $\alpha\gamma$ が垂直に交わるための必要十分条件は，$\dfrac{\gamma-\alpha}{\beta-\alpha}$ が純虚数であることである．
(3) 2 直線 $\alpha\beta$, $\gamma\delta$ が垂直に交わるための必要十分条件は，$\dfrac{\delta-\gamma}{\beta-\alpha}$ が純虚数であることである．

(2.18) **問題** 次の問に答えよ．
(1) 0 ではなく，互いに異なる複素数 α, β が，$\alpha=i\beta$ を満たすとき，0, α, β を頂点とする三角形はどんな形の三角形か．
(2) 互いに異なる複素数 α, β, γ が，$\gamma-i\beta=(1-i)\alpha$ を満たすとき，α, β, γ を頂点とする三角形はどんな形の三角形か．
(3) 異なる複素数 α, β があるとき，α, β, γ を頂点とする三角形が正三角形になるような複素数 γ を求め，α, β を用いて表せ．
(4) 0 ではない複素数 α があるとき，0, α, β を頂点とする三角形が直角二等辺三角形になるような複素数 β を求め，α を用いて表せ．
(5) 四角形 ABCD において，$\mathrm{AB}^2+\mathrm{CD}^2=\mathrm{AD}^2+\mathrm{BC}^2$ が成立するとき，2 つの対角線は直交することを証明せよ．

§3 行列の演算

(3.1) 基本事項

- 行列のサイズ，(i,j) 成分，ベクトル，正方行列
- 1×1 行列は丸括弧なしで表記する．
- 零行列 O, 単位行列 I, 対角行列
- 転置行列 ${}^tA$
- 和，差，スカラー倍，積
- $A\neq0$, $B\neq0$ かつ $AB=0$ となりうる (零因子がある) .
- 積が交換法則を満たさない

(3.2) **問題** 次の行列に対して答えよ．
$A=\begin{pmatrix}0&-4\\5&2\end{pmatrix}$, $B=\begin{pmatrix}3&\sqrt{2}&1\\0&4&5\end{pmatrix}$
(1) A のサイズと A の $(1,2)$ 成分　(2) B のサイズと b_{21}

(3.3) **問題** 次の行列の転置行列を求めよ．
(1) $\begin{pmatrix}0&-4\\5&2\end{pmatrix}$　(2) $\begin{pmatrix}3&\sqrt{2}&1\\0&4&5\end{pmatrix}$　(3) $\begin{pmatrix}1&-2\\4&8\\-5&7\\0&2\end{pmatrix}$

(3.4) **問題** 対角行列は転置しても変わらない．では，転置しても変わらない行列は対角行列であると言えるか．言えるなら証明せよ．言えないなら反例をあげよ．

(3.5) **問題** 次の等式を証明せよ．
(1) A, B が $m\times n$ 行列のとき， $A+B=B+A$.
(2) A, B が $m\times n$ 行列のとき，$k(A+B)=kA+kB$.
(3) A が $m\times n$ 行列，k,l がスカラーのとき， $(k+l)A=kA+lA$.
(4) A が $m\times n$ 行列, B が $n\times p$ 行列, C が $p\times q$ 行列のとき, $(AB)C=A(BC)$.

(5) A, B が $m \times n$ 行列，C が $n \times p$ 行列のとき，$(A+B)C = AC + BC$.
(6) A が $m \times n$ 行列，B, C が $n \times p$ 行列のとき，$A(B+C) = AB + AC$.
(7) A, B が $m \times n$ 行列のとき，${}^t(A+B) = {}^tA + {}^tB$.
(8) A が $m \times n$ 行列，B が $n \times p$ 行列のとき，${}^t(AB) = {}^tB\,{}^tA$.

(3.6) **問題** 次の計算をせよ.
(1) $3\begin{pmatrix}1 & -2 & 8\\ 2 & 5 & -1\end{pmatrix} - 2\begin{pmatrix}1 & 3 & 8\\ 3 & 7 & 0\end{pmatrix}$
(2) $54382\begin{pmatrix}3 & 2\\ 5 & -3\end{pmatrix} + 45618\begin{pmatrix}3 & 2\\ 5 & -3\end{pmatrix}$
(3) $54382\begin{pmatrix}3 & 8\\ -2 & 5\end{pmatrix} + 54382\begin{pmatrix}-2 & 2\\ 2 & 5\end{pmatrix}$

(3.7) **問題** 次の計算をせよ.
(1) $\begin{pmatrix}2 & 3\\ -1 & 2\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ (2) $\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$ (3) $\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$
(4) $\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}2 & 3\\ -1 & 0\\ -2 & 4\end{pmatrix}$ (5) $\begin{pmatrix}2 & 1 & -3\\ 1 & -5 & 2\end{pmatrix}\begin{pmatrix}3 & 1 & 0\\ 2 & 0 & -1\\ -1 & 4 & 1\end{pmatrix}$
(6) $\begin{pmatrix}1\\ -1\\ 2\end{pmatrix}\begin{pmatrix}1 & 3 & 2\end{pmatrix}$ (7) $\begin{pmatrix}1 & 3 & 2\end{pmatrix}\begin{pmatrix}1\\ -1\\ 2\end{pmatrix}$
(8) $\begin{pmatrix}11 & 21\\ 0 & 31\end{pmatrix}\begin{pmatrix}35\\ 53\end{pmatrix} + \begin{pmatrix}11 & 21\\ 0 & 31\end{pmatrix}\begin{pmatrix}-34\\ -54\end{pmatrix}$
(9) $\begin{pmatrix}11 & 21\\ 0 & 31\end{pmatrix}\begin{pmatrix}3\\ 5\end{pmatrix} + \begin{pmatrix}-21 & -11\\ 10 & 69\end{pmatrix}\begin{pmatrix}3\\ 5\end{pmatrix}$

(3.8) **問題** 次の問に答えよ.
(1) n 次正方行列 A, B であって，$AB = BA$ とはならないものを 1 組あげよ.
(2) ともに零行列 O ではない n 次正方行列 A, B であって，$AB \neq O$ だが $BA = O$ であるものを 1 組あげよ.

§4 逆行列

(4.1) **逆行列** n 次正方行列 A, B に対して $AB = BA = I_n$ が成り立つとき，B を A の**逆行列**と呼ぶ．逆行列を持つ行列を**正則行列**と呼ぶ.
2 次正方行列の逆行列は,

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$$

で与えられる.
n 次正方行列の逆行列を求めるには，$n \times 2n$ 行列 $(A|I_n)$ に，次の手順で掃き出し法を実行する．掃き出し法の結果の左半分が単位行列になったならば，右半分に現れた行列が A^{-1} である.

(手順 1) 基本変形を用いて，主成分を作る.
(手順 2) 基本変形を用いて，その主成分の上下を 0 にする.
(手順 3) (1) に戻る．次の主成分が作れなかったら終了.

(4.2) **問題** A, B を n 次正則行列とするとき，次の等式を証明せよ.
(1) $(A^{-1})^{-1} = A$ (2) $(AB)^{-1} = B^{-1}A^{-1}$ (3) $(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$
(4) $({}^tA)^{-1} = {}^t(A^{-1})$ (5) ${}^t(AB)^{-1} = {}^tA^{-1}\,{}^tB^{-1}$
ただし，(5) においては (4) を利用して $({}^tA)^{-1}$ を単に ${}^tA^{-1}$ と書いた.

(4.3) **問題** 次を証明せよ.
(1) 正方行列 A が，ある正整数 k に対して $A^k = O$ を満たすならば，A は正則ではない.
(2) A が正則行列ならば A^{-1} も正則行列である.
(3) A が正則行列ならば ${}^tA$ も正則行列である.
(4) A が正則な対称行列ならば，その逆行列も対称である.

(4.4) **問題** 次の行列に逆行列があれば求めよ.

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

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

(8) $\begin{pmatrix}-3&5&-2\\-3&4&-3\\2&-3&2\end{pmatrix}$ (9) $\begin{pmatrix}2&4&-3\\5&5&-2\\-2&-3&2\end{pmatrix}$ (10) $\begin{pmatrix}1&3&2\\3&3&4\\2&4&3\end{pmatrix}$

(11) $\begin{pmatrix}1&1&-1\\2&0&1\\1&-1&3\end{pmatrix}$ (12) $\begin{pmatrix}2&3&2\\3&3&1\\2&1&0\end{pmatrix}$ (13) $\begin{pmatrix}2&1&3\\1&-1&-2\\3&-1&-1\end{pmatrix}$

§5 行列式

(5.1) **基本事項**

- $\begin{vmatrix}a&b\\c&d\end{vmatrix} = ad-bc.$
- 3 次正方行列はサラスの方法が使える (4 次以上は使えない).
- 単位行列の行列式は 1.
- 基本変形でブロック三角行列にすると計算できる: $\begin{vmatrix}A&B\\0&C\end{vmatrix} = |A||C|.$
- 2 つの行 (列) を交換すると行列式は -1 倍になる.
- ある行 (列) を k 倍すると，行列式は k 倍になる.
- 乗法性: $|AB| = |A||B|$.
- 行 (列) に関する展開公式 (余因子展開)
- Cramer の公式 (連立 1 次方程式の解)
- 余因子行列を $\widetilde{A}$ とすると，$A\widetilde{A} = \widetilde{A}A = |A|I$. (幾何学 2 では，余因子行列を転置したものを $\widetilde{A}$ と定めていると思うので注意)

(5.2) **問題** 次の行列式を計算せよ.

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

(5.3) **問題** 次の行列式をサラスの方法で計算せよ.

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

(5.4) **例題** 次の行列式を，基本変形を用いて，および，展開公式を用いて計算せよ．また，余因子を用いて逆行列を求めよ.

$$\begin{vmatrix}2&0&3\\3&-1&3\\4&2&5\end{vmatrix}$$

(解答) まず基本変形を用いて計算する.

$$\begin{vmatrix}2&0&3\\3&-1&3\\4&2&5\end{vmatrix} = -\begin{vmatrix}0&2&3\\-1&3&3\\2&4&5\end{vmatrix} = \begin{vmatrix}-1&3&3\\0&2&3\\2&4&5\end{vmatrix} \quad \begin{pmatrix}1\text{ 列と }2\text{ 列を交換した後，}1\text{ 行と }2\text{ 行を交換した．マイナス注意}\end{pmatrix}$$

$$= \begin{vmatrix}-1&3&3\\0&2&3\\0&10&11\end{vmatrix} \quad (3\text{ 行に }1\text{ 行の }2\text{ 倍を加えた})$$

$$= -1\cdot\begin{vmatrix}2&3\\10&11\end{vmatrix} = 8. \quad \begin{pmatrix}\text{ブロック三角になったので展開して計算した}\end{pmatrix}$$

次に 1 行に関して展開して計算する.

$$\begin{vmatrix}2&0&3\\3&-1&3\\4&2&5\end{vmatrix} = 2\cdot\begin{vmatrix}-1&3\\2&5\end{vmatrix} - 0\cdot\begin{vmatrix}3&3\\4&5\end{vmatrix} + 3\cdot\begin{vmatrix}3&-1\\4&2\end{vmatrix}$$

$$= -22+30 = 8.$$

最後に，余因子を用いて A^{-1} を求める．

$$A_{ij} = (-1)^{i+j}\left|A \text{ の } i \text{ 行と } j \text{ 列を除いた 2 次正方行列}\right|$$

とすると，

$$A_{11} = \begin{vmatrix} -1 & 3 \\ 2 & 5 \end{vmatrix} = -11, \quad A_{12} = -\begin{vmatrix} 3 & 3 \\ 4 & 5 \end{vmatrix} = -3, \quad A_{13} = \begin{vmatrix} 3 & -1 \\ 4 & 2 \end{vmatrix} = 10,$$

$$A_{21} = -\begin{vmatrix} 0 & 3 \\ 2 & 5 \end{vmatrix} = 6, \qquad A_{22} = \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} = -2, \qquad A_{23} = -\begin{vmatrix} 2 & 0 \\ 4 & 2 \end{vmatrix} = -4,$$

$$A_{31} = \begin{vmatrix} 0 & 3 \\ -1 & 3 \end{vmatrix} = 3, \qquad A_{32} = -\begin{vmatrix} 2 & 3 \\ 3 & 3 \end{vmatrix} = 3, \qquad A_{33} = \begin{vmatrix} 2 & 0 \\ 3 & -1 \end{vmatrix} = -2.$$

よって，

$$\widetilde{A} = \begin{pmatrix} -11 & 6 & 3 \\ -3 & -2 & 3 \\ 10 & -4 & -2 \end{pmatrix}, \qquad A^{-1} = \frac{1}{|A|}\widetilde{A} = \frac{1}{8}\begin{pmatrix} -11 & 6 & 3 \\ -3 & -2 & 3 \\ 10 & -4 & -2 \end{pmatrix}.$$

(5.5) **問題** (5.3) の行列式を行列の基本変形を用いて計算せよ．

(5.6) **問題** (5.3) の行列式を行列式の展開公式を用いて計算せよ．

(5.7) **問題** 行列式を計算せよ．

(1) $\begin{vmatrix} 3 & -2 & 3 \\ -3 & 1 & -2 \\ -2 & -5 & 4 \end{vmatrix}$ (2) $\begin{vmatrix} 4 & 1 & -2 \\ -2 & 3 & -2 \\ 2 & -2 & 1 \end{vmatrix}$ (3) $\begin{vmatrix} -2 & 2 & 2 \\ -5 & 2 & 4 \\ -3 & 1 & 4 \end{vmatrix}$

(5.8) **問題** 次の行列式を計算し因数分解せよ．

(1) $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}$ (2) $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^3 & b^3 & c^3 \end{vmatrix}$ (3) $\begin{vmatrix} 1 & 1 & 1 \\ a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \end{vmatrix}$ (4) $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^4 & b^4 & c^4 \end{vmatrix}$

(5) $\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & x & x & x \\ 1 & x & x^2 & x^2 \\ 1 & x & x^2 & x^3 \end{vmatrix}$

(5.9) **問題** 次の行列の逆行列を余因子行列を用いて求めよ．

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

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

(5.10) **問題** 連立方程式

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \qquad\qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

において，$A = (a_{ij})_{1\le i,j\le n}$ とおき，$|A| \neq 0$ とする．この解を求めるクラメール (クラーメル，クラメル，Cramer) の公式

$$x_j = \frac{1}{|A|}\begin{vmatrix} a_{11} & \cdots & b_1 & \cdots & a_{1n} \\ a_{21} & \cdots & b_2 & \cdots & a_{2n} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & b_n & \cdots & a_{nn} \end{vmatrix} \qquad (A \text{ の } j \text{ 列目を } b_1, \ldots, b_n \text{ で上書き})$$

を次の手順で証明せよ.
(1) 証明すべき x_j の式の右辺を，j 列について展開した式を書く.
(2a) $x=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}$, $b=\begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix}$ とおくと，連立方程式は $Ax=b$ と書けるので，この両辺に左から A^{-1} を掛けて，$x=A^{-1}b$ を得る．この等式の A^{-1} を余因子行列を用いて書き直す.
(2b) その式の両辺は n 次の縦ベクトルであるが，その第 j 成分を取り出した等式を書く.
(3) こうして得られた (2b) の等式が，証明すべき (1) の等式に一致することを確かめる.

(5.11) **問題** 次の連立方程式をクラメールの公式を用いて解け．ただし，a,b,c は互いに異なる定数とする.

(1) $\begin{cases}2x+9y &=13,\\ x+5y &=7\end{cases}$ (2) $\begin{cases}x+y &=6,\\ -x+y+4z &=6,\\ x-z &=3\end{cases}$ (3) $\begin{cases}2y-z &=1,\\ x-4y &=-7,\\ 2x+z &=-7\end{cases}$

(4) $\begin{cases}-2x+3y-z &=1,\\ x+5z &=1,\\ 3x-5y+z &=-1\end{cases}$ (5) $\begin{cases}x+y+z &=1,\\ ax+by+cz &=1,\\ a^2x+b^2y+c^2z &=1\end{cases}$

§6 ベクトル空間の基礎

(6.1) ベクトル空間

- 有理数体 $\mathbb{Q}$，実数体 $\mathbb{R}$，複素数体 $\mathbb{C}$ のような四則演算が可能な**体**を考える．数をベクトルと対比して**スカラー**と呼ぶ．以下では断らない限りスカラーとして $\mathbb{R}$ を考える.
- 集合 V が**ベクトル空間**であるとは，ベクトルどうしの和 $(u+v)$ とベクトルのスカラー倍 (kv) が定まっていて，脚注の公理を満足するときを言う[1].
- 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.

(6.2) **例題** 実数成分の n 次の横ベクトル全体の集合はベクトル空間をなすが，(a) 和とスカラー倍は何か答えよ．(b) 和の交換法則を証明せよ．(c) 分配法則を証明せよ.

(解答 (a)) 和とスカラー倍はそれぞれ,

$$(x_1,x_2,\dots,x_n)+(y_1,y_2,\dots,y_n)=(x_1+y_1,x_2+y_2,\dots,x_n+y_n),$$
$$k(x_1,x_2,\dots,x_n)=(kx_1,kx_2,\dots,kx_n)$$

で定める $(x_j,k\in\mathbb{R})$.
(解答 (b)) 次のように，実数の交換法則に帰着して証明される.

$$\begin{aligned}&(x_1,x_2,\dots,x_n)+(y_1,y_2,\dots,y_n)\\ &\quad=(x_1+y_1,x_2+y_2,\dots,x_n+y_n)\\ &\quad=(y_1+x_1,y_2+x_2,\dots,y_n+x_n)\qquad(\because \textbf{実数の}\text{交換法則})\\ &\quad=(y_1,y_2,\dots,y_n)+(x_1,x_2,\dots,x_n)\end{aligned}$$

(解答 (c)) 上と同様に実数の分配法則に帰着して証明されるが，省略する.

(6.3) **問題** 次の集合はベクトル空間をなすが，それぞれについて，(a) 和とスカラー倍は何か答えよ．(b) 和の交換法則を証明せよ．(c) 分配法則を証

[1] ベクトル空間の公理: $u,v,w\in V$ とスカラー a,b に対して,
(1) $u+v=v+u$ (交換法則)
(2) $(u+v)+w=u+(v+w)$ (結合法則)
(3) $u+0=0=0+u$ なるベクトル 0 (零ベクトル) が存在する.
(4) $a(bu)=(ab)u$ (結合法則)
(5) $(a+b)u=au+bu$ (分配法則)
(6) $a(u+v)=au+av$ (分配法則)
(7) $1u=u$
(8) $0u=0$

明せよ．((b) と (c) 両方だと多いので，好きな片方だけでよい)
(1) 実数成分の n 次の縦ベクトル全体の集合 $\mathbb{R}^n$ (数ベクトル空間).
(2) 実数成分の $m \times n$ 行列全体の集合 $\mathrm{Mat}(m,n;\mathbb{R})$.
(3) 実数係数 1 変数多項式全体の集合 $\mathbb{R}[x]$.
(4) 集合 X を定義域とする実数値関数全体の集合 $\mathrm{Map}(X,\mathbb{R})$.

(6.4)　**例題**　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．

(証明) 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
[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．

(6.5)　**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) $A=\begin{pmatrix}1 & 2 & 3\\ -3 & -2 & -1\end{pmatrix}$ のとき，$\mathbb{R}^3$ の部分集合 $\{x\in\mathbb{R}^3 \mid Ax=0\}$.
(3) A を $m\times n$ 行列とするとき，$\mathbb{R}^n$ の部分集合 $\{x\in\mathbb{R}^n \mid Ax=0\}$.
(4)　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).

§7　1 次独立と 1 次従属

(7.1)　**1 次結合，1 次独立，1 次従属**　V をベクトル空間とする．

- 次の形の元を $v_1,v_2,\dots,v_k\in V$ の **1 次結合**と呼ぶ．

$$a_1v_1+a_2v_2+\cdots+a_kv_k\quad (a_1,a_2,\dots,a_k\in K)$$

- $v_1,v_2,\dots,v_k\in V$ が **1 次独立**であるとは，その 1 次結合 $a_1v_1+a_2v_2+\cdots+a_kv_k$ が 0 になるのは，すべての a_j が 0 であるときに限ることを言う．
- $v_1,v_2,\dots,v_k\in V$ が **1 次従属**であるとは，1 次独立ではないことを言う．

※ 1 次独立であるというのは，おおざっぱに言えば，ベクトルがてんでばらばらの方向を向いていると言うことである．もう少し正確に言えば，k 個のベクトルが 1 次独立であるというのは，(位置) ベクトルの表す k 個の点と原点で，k 次元の角錐 ($k=2$ なら三角形，$k=3$ なら三角錐，$k=4$ なら 4 次元の 4 角錐…) をなすことである．

- 行列を簡約化したときの主成分の個数を行列の**階数**と呼ぶ．
- 数ベクトル $v_1,v_2,\dots,v_k\in\mathbb{R}^n$ が 1 次独立であるための必要十分条件は，これらを並べてできる行列 $(v_1,v_2,\dots,v_k)\in\mathrm{Mat}(n,k;\mathbb{R})$ の階数が k に等しいことである．

(7.2)　**例題**　次のベクトル ((3) では複素数) は $\mathbb{R}$ 上 1 次独立かどうか言え．
(1) $\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}2\\4\end{pmatrix}$　(2) $\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}2\\4\end{pmatrix}$　(3) $1,\ 2+3i$

(解答) ここでの解答は，1 次独立性の定義どおりの解答だが，後にあるような，階数を計算する解答の方がずっと効率がよい．
(1) 1 次結合が 0 になったとする．つまり，

$$k\begin{pmatrix}1\\3\end{pmatrix}+l\begin{pmatrix}2\\4\end{pmatrix}=0$$

とする．このとき $k=l=0$ であることを言えば，1 次独立であることが言える．上の式は連立方程式

$$\begin{cases}k+2l=0\\ 3k+4l=0\end{cases}$$

と同値であり，これを解くと $k=0,\ l=0$ となるから，問題のベクトルは 1 次独立である．

(2) (1) と同様に連立方程式を作ると，

$$\begin{cases} k+2l=0 \\ 2k+4l=0 \end{cases}$$

となるが，これは 1 本の方程式 $k+2l=0$ と同値である．これは，$k=t$, $l=-2t$ (t は任意定数) という一意ではない解を持ち，特に，$k=l=0$ ではない解も持つ．したがって問題のベクトルは 1 次従属である．

(7.3) **問題** 次のベクトルは 1 次独立かどうか調べよ．

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

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

(6) $\mathbb{R}[x]$ の元 $1, x, x^2$ (7) $\mathbb{R}[x]$ の元 $1, x+1, x-1$

(7.4) **例題** 次の行列の階数を求めよ．

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

(解答)

(1) 下のように主成分が 2 つあるから，階数は 2 である．

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

(2) 下のように主成分が 1 つあるから，階数は 1 である．

1	2	
2	4	
1	2	
0	0	② + ① × (−2)

(3) 下のように主成分が 3 つあるから，階数は 3 である．

1	3	2	
3	3	4	
2	2	0	
1	3	2	
0	−6	−2	② + ① × (−3)
0	−4	−4	③ + ① × (−2)
1	3	2	
0	−6	−2	
0	1	1	③ × $(-\frac{1}{4})$

1	3	2	
0	0	4	② + ③ × 6
0	1	1	
1	3	2	
0	0	1	② × $\frac{1}{4}$
0	1	1	
1	3	2	
0	1	1	②, ③交換
0	0	1	

(7.5) **問題** (7.3) の (1) から (5) に，行列の簡約化で階数を求めることで答えよ．

(7.6) **問題** 次の問に答えよ．

(1) 3×4 行列の階数は 3 を超えないことを示せ．また，これを用いて $\mathbb{R}^3$ に属する 4 つのベクトル v_1, v_2, v_3, v_4 があったとき，これらは 1 次従属であることを示せ．

(2) $\mathbb{R}^n$ に属するいくつかのベクトルが 1 次独立であるとき，そのベクトルの個数のとりうる範囲を言え．

(7.7) **生成される空間，基底** V をベクトル空間とする．

- ベクトル $v_1, v_2, \dots, v_k \in V$ で**生成される (部分) 空間**とは，$v_1, v_2, \dots, v_k$ の 1 次結合全体のなす集合

$$\{a_1 v_1 + \cdots + a_k v_k \mid a_j \in \mathbb{R}\}$$

  のことを言う．
- ベクトル $v_1, \dots, v_n \in V$ が，V の**基底**であるとは，$v_1, \dots, v_n$ が V を生成し，かつ，1 次独立であるときを言う．
- V には基底が存在し，その濃度は基底の取り方によらず一定であることが知られている．その濃度を V の**次元**と呼ぶ．

(7.8) **問題** $\mathbb{R}^n$ のベクトル e_i $(i = 1, 2, \dots, n)$ を

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots, e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

で定める．これらは $\mathbb{R}^n$ の基底をなすことを証明せよ (したがって，$\mathbb{R}^n$ は n 次元のベクトル空間である)．この基底を $\mathbb{R}^n$ の**標準基底**と呼ぶ．[ヒント: $\mathbb{R}^n$ の任意の元が，$e_1, \dots, e_n$ の 1 次結合で書けることと，$e_1, \dots, e_n$ が 1 次独立であることを示せ．]

(7.9) **例題** 次のベクトルは $\mathbb{R}^3$ の基底かどうか答えよ．

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

((1) の解答) (7.8) により，$\mathbb{R}^3$ は 3 次元である．しかし，ベクトルが 2 個しかないので基底ではない．

((2) の解答の準備) 1 次独立，かつ，$\mathbb{R}^3$ を生成することを言えばよいが，1 次独立性を言うには，(7.7) で触れたように，3 つのベクトルを並べてできる行列

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

の階数が 3 であることを言えばよい (この計算は後回しにする)．

他方，$\mathbb{R}^3$ を生成することを言うには，これらのベクトルの 1 次結合で標準基底が書ければよい．なぜなら，それらでさらに 1 次結合を作れば $\mathbb{R}^3$ を生成するからである．つまり，連立方程式

$$\begin{cases} x_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + x_2 \begin{pmatrix} 4 \\ 5 \\ 2 \end{pmatrix} + x_3 \begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \\ y_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + y_2 \begin{pmatrix} 4 \\ 5 \\ 2 \end{pmatrix} + y_3 \begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \\ z_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + z_2 \begin{pmatrix} 4 \\ 5 \\ 2 \end{pmatrix} + z_3 \begin{pmatrix} 2 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \end{cases}$$

が解を持てばよい．ところがこの方程式はまとめて，

$$\begin{pmatrix} 1 & 4 & 2 \\ 2 & 5 & 2 \\ 3 & 2 & -1 \end{pmatrix} \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

と書けるから，$\mathbb{R}^3$ を生成するには行列 A が逆行列を持てばよい．これは，行列 A の階数が 3 であることと同値である．

((2) の解答) 以上を踏まえて，行列 A を簡約化して階数を求めると，

1	4	2	
2	5	2	
3	2	-1	
1	4	2	
0	-3	-2	② + ① × (-2)
0	-10	-7	③ + ① × (-3)
1	4	2	
0	-10	-7	②, ③交換
0	-3	-2	
1	4	2	
0	-1	-1	② + ③ × (-3)
0	-3	-2	

1	4	2	
0	1	1	② × (-1)
0	-3	-2	
1	0	-2	① + ② × (-4)
0	1	1	
0	0	1	③ + ② × 3
1	0	0	① + ③ × 2
0	1	0	② + ③ × (-1)
0	0	1	

となり，階数 3 であるから，与えられたベクトルは 1 次独立である．

(7.10) **基底の条件** (7.9) (2) の解答より，$\mathbb{R}^n$ の n 本のベクトル $v_1, \dots, v_n$ に対して次の 5 つの条件は同値である．

(i) $v_1, \dots, v_n$ は $\mathbb{R}^n$ の基底である
(ii) $v_1, \dots, v_n$ を並べてできる行列の階数は n である
(iii) $v_1, \dots, v_n$ を並べてできる行列は正則である
(iv) $v_1, \dots, v_n$ を並べてできる行列の行列式は 0 ではない
(v) $v_1, \dots, v_n$ で生成される部分空間は n 個の標準基底すべてを含む

(7.11) **問題** (7.10) を利用して次の問に答えよ。(7.3) の結果を用いても用いなくてもよい。
(1) (7.3) の (1) と (2) は，$\mathbb{R}^2$ の基底であるかどうか答えよ．
(2) (7.3) の (4) と (5) は，$\mathbb{R}^3$ の基底であるかどうか答えよ．

(7.12) **問題** $\mathbb{R}^n$ の 2 組の基底 $v_1, \dots, v_n$ と $w_1, \dots, w_n$ があるとき，n 次正則行列 A を用いて $(v_1, \dots, v_n) = (w_1, \dots, w_n)A$ と表せることを証明せよ．この行列 A を**基底の変換行列**と呼ぶ．[ヒント: $X = (v_1, \dots, v_n)$, $Y = (w_1, \dots, w_n)$ とおくと，これらは (7.10) より n 次正則行列である．あとは，$X = YA$ を満たす A を見付ければよい．]

§8 線型写像

(8.1) **線型写像** V, W を $\mathbb{R}$ 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) $f(av) = af(v)$ $\quad (a \in \mathbb{R}, v \in V)$

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．

(8.2) **例題** 次の写像は線型写像かどうか答えよ．
(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = \sin x)$
(2) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = 3x)$
(3) $f : \mathbb{R}^2 \to \mathbb{R}^2$ $\quad \left(f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right)$

((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) 成立．$f(ax) = 3(ax) = a(3x) = af(x)$ だから (L2) 成立．よって線型写像である．
((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) 成立．$f(av) = A(av) = a(Av) = af(v)$ だから (L2) 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にも注意せよ)．

(8.3) **問題** 次の写像は線型写像かどうか答えよ．
(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = x)$
(2) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = -x)$
(3) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = \cos x)$
(4) $f : \mathbb{R}^2 \to \mathbb{R}^2$ $(f(v) = v)$
(5) $f : \mathbb{R}^2 \to \mathbb{R}^2$ $(f(v) = 2v)$
(6) $f : \mathbb{R}^3 \to \mathbb{R}^3$ $\quad \left(f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 5 \\ -1 & \sqrt{2} & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right)$

(8.4) **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．

(8.5) **問題** $f : U \to V$ と $g : V \to W$ がともに線型写像であるとき，合成写像 $g \circ f : U \to W$ も線型写像であることを証明せよ．[ヒント: まず (L1) について，$u, u' \in U$ に対して，$(g \circ f)(u + u') = (g \circ f)(u) + (g \circ f)(u')$ を示せばよい．つまり，$g(f(u + u')) = g(f(u)) + g(f(u'))$ を示せばよい．次に (L2) について，$u \in U$ とスカラー a に対して，$(g \circ f)(au) = a(g \circ f)(u)$ を示せばよい．つまり，$g(f(au)) = ag(f(u))$ を示せばよい．いずれも，f, g の線型性を用いるとよい．]

(8.6) **問題** $f : \mathbb{R}^n \to \mathbb{R}^m$ を線型写像とし，標準基底 $e_1, \ldots, e_n \in \mathbb{R}^n$ の f による像を，それぞれ $a_1, \ldots, a_n \in \mathbb{R}^m$ とする．$a_1, \ldots, a_n$ を並べた行列を $A = (a_1, \ldots, a_n)$ と置くと，$f(v) = Av$ と書けることを示せ．[ヒント: $\mathbb{R}^n$ の元を標準基底の 1 次結合で表しておく．それを f で写し，線型性を用いて式を変形してから行列の表示に直せばよい]

(8.7) **例題** $f : V \to W$ を線型写像とするとき，f の像 $\mathrm{Im}(f)$ は W の部分空間であることを証明せよ．
(証明) [和で閉じていること] $w_1, w_2 \in \mathrm{Im}(f)$ をとったとき，$w_1 + w_2 \in \mathrm{Im}(f)$ であることを示せばよい．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 の線型性より，

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

となり，$w_1 + w_2$ は $v_1 + v_2$ の像だから，$w_1 + w_2 \in \mathrm{Im}(f)$ である．

[スカラー倍で閉じていること] $w \in \mathrm{Im}(f)$ とスカラー k をとったとき，$kw \in \mathrm{Im}(f)$ であることを示せばよい．像の定義より，$w = f(v)$ なる $v \in V$ がある．f の線型性より，

$$kw = kf(v) = f(kv)$$

となり，kw は kv の像だから，$kw \in \mathrm{Im}(f)$ である．

(8.8) **問題** $f : V \to W$ を線型写像とするとき，f の核 $\mathrm{Ker}(f)$ は V の部分空間であることを証明せよ．[ヒント: 和とスカラー倍で閉じていることを示せばよい．まず和について，$v_1, v_2 \in \mathrm{Ker}(f)$ をとったとき，$v_1 + v_2 \in \mathrm{Ker}(f)$ を示せばよい．つまり，$f(v_1) = f(v_2) = 0$ のとき，$f(v_1 + v_2) = 0$ を示せばよい．次にスカラー倍について，$v \in \mathrm{Ker}(f)$ とスカラー a をとったとき，$av \in \mathrm{Ker}(f)$ を示せばよい．つまり，$f(v) = 0$ のとき，$f(av) = 0$ を示せばよい．]

(8.9) **問題** $f : V \to W$ を線型写像とするとき，f が単射であることと，$\mathrm{Ker}(f) = \{0\}$ であることが同値であることを証明せよ．[ヒント: まず f が単射のとき $\mathrm{Ker}(f) = \{0\}$ を示す．つまり，$f(v) = f(v')$ ならば $v = v'$ であることを仮定して，$f(v) = 0$ なる $v \in V$ が $v = 0$ のみであることを示せばよい．これには $f(0) = 0$ を用いればよい．次に，$\mathrm{Ker}(f) = \{0\}$ のとき f が単射であることを示す．$f(v) = 0$ なる $v \in V$ が $v = 0$ のみであることを仮定すれば，f の線型性より，$f(v) = f(v')$ ならば $v = v'$ であることが示せる．]

(8.10) **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．

(8.11) **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 $w_1,\dots,w_m$ の 1 次結合で書けるから，$m\times n$ 行列 A を用いて $(f(v_1),\dots,f(v_n))=(w_1,\dots,w_m)A$ と行列で表示できる．この A を V の基底 $v_1,\dots,v_n$ と W の基底 $w_1,\dots,w_m$ に関する f の**表現行列**と呼ぶ.

(8.12)　**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.

(8.13)　**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.

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

(8.14)　**基底変換**　$f:V\to W$ を線型写像とし，$v_1,\dots,v_n$ と $v'_1,\dots,v'_n$ を V の 2 組の基底，$w_1,\dots,w_m$ と $w'_1,\dots,w'_m$ を W の 2 組の基底とする．このとき，(7.12) より，n 次正則行列 P と m 次正則行列 Q があって,

$$(v'_1,\dots,v'_n)=(v_1,\dots,v_n)P,\qquad (w'_1,\dots,w'_m)=(w_1,\dots,w_m)Q$$

と書けるのだった．f の $v_1,\dots,v_n$ と $w_1,\dots,w_m$ とに関する表現行列を A, $v'_1,\dots,v'_n$ と $w'_1,\dots,w'_m$ に関する表現行列を B とすると，次が成立する:

$$B=Q^{-1}AP.$$

特に，$V=W$ のとき $f:V\to V$ を考え，V の 2 組の基底 $v_1,\dots,v_n$ と $v'_1,\dots,v'_n$ に関する表現行列を，それぞれ A, B とすると,

$$B=P^{-1}AP$$

である.

(8.15)　**例題**　次で定まる線型写像 $f:\mathbb{R}^2\to\mathbb{R}^2$ の，指定された基底に関する表現行列を求めよ.
$f\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}5&-2\\12&-5\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$　　基底: $\begin{pmatrix}1\\3\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix}$
(解答) $A=\begin{pmatrix}5&-2\\12&-5\end{pmatrix}$ は，線型写像 f の，標準基底 $e_1=\begin{pmatrix}1\\0\end{pmatrix}$, $e_2=\begin{pmatrix}0\\1\end{pmatrix}$ に関する表現行列である．$v_1=\begin{pmatrix}1\\3\end{pmatrix}$, $v_2=\begin{pmatrix}1\\2\end{pmatrix}$, $P=\begin{pmatrix}1&1\\3&2\end{pmatrix}$ とおくと，$(v_1,v_2)=(e_1,e_2)P$ だから，P が基底の変換行列である．よって，基底 v_1,v_2 に関する f の表現行列は，$P^{-1}AP=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$ である.

(8.16)　**問題**　次で定まる線型写像 $f:\mathbb{R}^2\to\mathbb{R}^2$ の，指定された基底に関する表現行列を求めよ.

(1) $f\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}19&-6\\22&-4\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$　　基底: $\begin{pmatrix}6\\11\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix}$

(2) $f\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}3&-3\\1&-1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$　　基底: $\begin{pmatrix}3\\1\end{pmatrix},\begin{pmatrix}5\\5\end{pmatrix}$

§9　固有値・固有ベクトル

(9.1)　**固有値・固有ベクトル**　体 K (例えば $K=\mathbb{R}$) 上の線型写像 $f:V\to V$ に対して,

$$f(v)=\lambda v\qquad(\lambda\in K,\ v\in V,\ v\neq 0)$$

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 f の**固有値**，v を f の固有値 λ の**固有ベクトル**と呼ぶ.

線型写像の表現行列を考えると，行列の固有値と固有ベクトルが次のように定められる．n 次正方行列 $A\in\mathrm{Mat}(n,K)$ に対して,

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

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.

(9.2)　**例題**　行列 $\begin{pmatrix}5&-2\\12&-5\end{pmatrix}$ に関して，ベクトル $v_1=\begin{pmatrix}1\\3\end{pmatrix}$ と $v_2=\begin{pmatrix}1\\2\end{pmatrix}$ が固有ベクトルであることを示し，また，その固有値を言え.

(解答) 下の計算により，v_1 は固有値 -1 の固有ベクトル，v_2 は固有値 1 の固有ベクトルである.

$$\begin{pmatrix}5&-2\\12&-5\end{pmatrix}v_1=\begin{pmatrix}-1\\-3\end{pmatrix}=-v_1,\qquad\begin{pmatrix}5&-2\\12&-5\end{pmatrix}v_2=\begin{pmatrix}1\\2\end{pmatrix}=v_2$$

(9.3)　**問題**　次の行列 A に関して，v_1 と v_2 が固有ベクトルであることを示し，また，固有値を言え.

(1) $A=\begin{pmatrix}19&-6\\22&-4\end{pmatrix}$, $v_1=\begin{pmatrix}6\\11\end{pmatrix}$, $v_2=\begin{pmatrix}1\\2\end{pmatrix}$

(2) $A=\begin{pmatrix}3&-3\\1&-1\end{pmatrix}$, $v_1=\begin{pmatrix}3\\1\end{pmatrix}$, $v_2=\begin{pmatrix}5\\5\end{pmatrix}$

(9.4)　**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.

(9.5)　**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).

(9.6)　**問題**　固有多項式を用いて次の行列の固有値を求めよ.

(1) $\begin{pmatrix}5&-2\\12&-5\end{pmatrix}$　(2) $\begin{pmatrix}19&-6\\22&-4\end{pmatrix}$　(3) $\begin{pmatrix}3&-3\\1&-1\end{pmatrix}$

(9.7) **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) (9.5)(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.

(9.8) **問題** (9.6) の行列の固有ベクトルを求めよ ((1) から (3) を個別に 1 問と数える. 3 つとも 1 人が同時にやる必要はない).

(9.9) **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.

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

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 (9.7) 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.

(9.10) **問題** 次の行列の固有値と固有ベクトルを求めよ.

(1) $\begin{pmatrix} 1 & 2 \\ 8 & 1 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$ (3) $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$

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

(7) $\begin{pmatrix} 3 & 2 & -2 \\ -2 & -1 & 2 \\ -1 & -1 & 2 \end{pmatrix}$ (8) $\begin{pmatrix} 3 & 5 & -4 \\ -2 & -2 & 2 \\ -2 & -1 & 1 \end{pmatrix}$ (9) $\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ -1 & 0 & 3 \end{pmatrix}$

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

§10 行列の対角化

(10.1) **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.

線型写像 $f : \mathbb{R}^n \to \mathbb{R}^n$ の, 標準基底に関する表現行列 A が対角化可能であるということは, ある基底に関する f の表現行列が対角行列になることに同値である. これは, A の固有ベクトルで $\mathbb{R}^n$ の基底を構成できることに同値である. したがって, **A が対角化可能であるための必要十分条件は, A が n 個の 1 次独立な固有ベクトルを持つことである.** また, 上で対角化に用いる行列 P は, 固有ベクトルを並べて得られることもわかる.

(10.2) **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) (9.2) 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) (9.5) 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 (9.9) 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，

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

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

$$= (t+1)(t^2-t-2) = (t+1)^2(t-2)$$

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 (9.9) 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．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．

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**)．

(10.3) **問題** 次の行列が対角化可能ならば対角化せよ．以前の問題の結果が利用できる場合はその問題番号を記すので，その問題で得られている固有値や固有ベクトルは利用して解答してよい: (1) と (2) は (9.3)，(3) から (7) は (9.10)，(8) から (10) はヒントなし．

(1) $\begin{pmatrix} 19 & -6 \\ 22 & -4 \end{pmatrix}$ (2) $\begin{pmatrix} 3 & -3 \\ 1 & -1 \end{pmatrix}$ (3) $\begin{pmatrix} 1 & 2 \\ 8 & 1 \end{pmatrix}$ (4) $\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$ (5) $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$

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

(8) $\begin{pmatrix} 7 & 3 & -3 \\ -7 & -3 & 3 \\ 5 & 3 & -1 \end{pmatrix}$ (9) $\begin{pmatrix} -1 & 3 & -2 \\ 1 & 1 & -2 \\ -1 & -3 & 0 \end{pmatrix}$ (10) $\begin{pmatrix} -1 & 4 & -5 \\ 2 & -3 & 5 \\ 2 & -4 & 6 \end{pmatrix}$

(10.4) **例題** $A = \begin{pmatrix} 5 & -2 \\ 12 & -5 \end{pmatrix}$ とおくとき，非負整数 n に対して A^n を求めよ．

(解答) まず，対角行列の n 乗は，

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$$

と容易に計算できることに注意しておく．

(10.2) により，$P = \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$ とおくと，$P^{-1}AP = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ であった．

したがって，

$$\begin{aligned} A^n &= \left(P \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} P^{-1} \right)^n \\ &= \left(P \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} P^{-1} \right) \left(P \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} P^{-1} \right) \cdots \left(P \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} P^{-1} \right) \\ &= P \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^n P^{-1} = \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} (-1)^n & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix} \\ &= \begin{pmatrix} -2(-1)^n + 3 & (-1)^n - 1 \\ -6(-1)^n + 6 & 3(-1)^n - 2 \end{pmatrix} \end{aligned}$$

(10.5) **問題** 非負整数 n に対して，次の行列の n 乗を計算せよ．

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

§11 有理整数環

(11.1) **基本事項** 整数全体の集合を $\mathbb{Z}$ と書く．整数 a, b, n があるとき，a と b が n を法として**合同**であるとは，

$$a - b \in n\mathbb{Z}$$

を満たすときを言い，

$$a \equiv b \pmod{n}$$

と書く．ただし，$n\mathbb{Z}$ は n の倍数全体の集合である．

(a, b が負でないならば) $a \equiv b \pmod{n}$ とは，n で割った余りが等しいことを表すとも言える．

(11.2) **問題** $x \equiv a \pmod{n}$ かつ $y \equiv b \pmod{n}$ のとき，次を証明せよ．

(1) $x + y \equiv a + b \pmod{n}$ (2) $xy \equiv ab \pmod{n}$

(11.3) **問題** 次の等式を満たす x を答えよ．ただし，無数にある x のうち，最小の非負整数で答えよ．
(1) $x \equiv 22 + 33 \pmod 4$
(2) $x \equiv 22 \cdot 33 \pmod 4$
(3) $x \equiv 221 \cdot 331 \pmod{23}$
(4) $x \equiv 22^{33} \pmod 5$

(11.4) **問題** 正整数 a, b に対し、次の問に答えよ。
(a) a と b の最小公倍数と，最大公約数の定義を言え[2]．
(b) a と b の最小公倍数を m，最大公約数を d とする．(a) の定義に基づいて，$ab = md$ を証明せよ．

(11.5) **問題** a, b を整数とし，a と b の最大公約数を (a, b) と書く．
(1) $(a, b) = (a, b - a)$ を証明せよ．
(2) 整数 k に対して，$(a, b) = (a, b - ka)$ を，(1) の主張を利用して証明せよ．
(3) 整数 n が，$n \equiv b \pmod a$ を満たすとき，$(a, b) = (a, n)$ を，(2) の主張を利用して証明せよ．

(11.6) **問題** 環において，積に関する逆元が存在する元を**単元**と呼ぶ．整数全体のなす環 $\mathbb{Z}$ の元のうち，単元をすべて言え．

(11.7) **問題 (ベズーの等式)** 次の問に答えよ．
(1) a, b を互いに素な 0 ではない整数とするとき，$ax + by = 1$ を満たす整数 x, y が存在することを証明せよ．
(2) a, b を互いに素な 0 ではない整数とし，k を整数とするとき，$ax + by = k$ を満たす整数 x, y が存在することを，(1) の主張を利用して証明せよ．
(3) 0 ではない整数 a, b の最大公約数を d とし，k を d の倍数とするとき，$ax + by = k$ を満たす整数 x, y が存在することを，(2) の主張を利用して証明せよ．

[2] a と 0 の最大公約数は a と定め，負かも知れない整数 a, b の最大公約数は，$|a|$ と $|b|$ の最大公約数で定めることにする．

(11.8) **例題** $29x + 96y = 1$ の整数解を 1 組求めよ。また、すべての整数解を求めよ。
(解答)

$$96 \div 29 = 3 \text{ あまり } 9 \qquad \text{より } 9 = 96 - 29 \cdot 3, \tag{a}$$
$$29 \div 9 = 3 \text{ あまり } 2 \qquad \text{より } 2 = 29 - 9 \cdot 3, \tag{b}$$
$$9 \div 2 = 4 \text{ あまり } 1 \qquad \text{より } 1 = 9 - 2 \cdot 4, \tag{c}$$

したがって，

$$\begin{aligned} 1 &\overset{\text{c}}{=} 9 - 2 \cdot 4 \\ &\overset{\text{b}}{=} 9 - (29 - 9 \cdot 3) \cdot 4 = 9 \cdot 13 - 29 \cdot 4 \\ &\overset{\text{a}}{=} (96 - 29 \cdot 3) \cdot 13 - 29 \cdot 4 = 96 \cdot 13 - 29 \cdot 43. \end{aligned}$$

よって，$x = -43, y = 13$ は 1 組の整数解である。
次に、$29x+96y = 1$ と $29\cdot(-43)+96\cdot(13) = 1$ の辺々を引いて $29(x+43)+96(y-13) = 0$ となるが、29 と 96 が互いに素だから、$x+43$ は 96 の倍数であり、$x+43 = 96k$ (k は整数) と書ける。よって $29\cdot 96k+96(y-13) = 0$ より、$y-13 = -29k$ である。以上より、すべての整数解は、$(x, y) = (-43 + 96k, 13 - 29k)$ (k は整数) である。

(11.9) **問題** 次の方程式を満たす整数解を 1 組答えよ。
(1) $8x - 13y = 1$ (2) $100x + 37y = 2$ (3) $118x + 22y = 4$

(11.10) **問題** (11.9) の各方程式に対し、整数解をすべて答えよ．

(11.11) **問題** 次の合同式を満たす整数 x を 1 つ答えよ．
(1) $8x \equiv 1 \pmod{13}$
(2) $100x \equiv 2 \pmod{37}$
(3) $118x \equiv 4 \pmod{22}$

(11.12) **問題** a, b を 0 でない互いに素な整数とする．$ax \equiv 1 \pmod{b}$ を満たす整数 x が存在することを，ベズーの等式を利用して証明せよ．

(11.13) **素因数分解の一意性** 正整数 n は，素数のベキの積に，

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

と，素数の順番を除いて一意的に分解する．

n がある素数 p で割り切れるということは，n の素因数分解に p が現れることに他ならない．また，正整数 a と b が互いに素ということは，a, b それぞれの素因数分解に共通な素数が現れないことに他ならない．

(11.14) **問題** 正整数 $a_1, a_2, \ldots, a_m$ と $b_1, b_2, \ldots, b_n$ があり，任意の $i = 1, \ldots, m$ と $j = 1, \ldots, n$ に対して，a_i と b_j は互いに素であるとき，$a_1 a_2 \cdots a_m$ と $b_1 b_2 \cdots b_n$ は互いに素であることを示せ．

(11.15) **問題** p が素数のとき，$k = 1, 2, \ldots, p-1$ に対して，二項係数 $\binom{p}{k} = {}_p\mathrm{C}_k$ は p の倍数であることを示せ．

(11.16) **問題** $\sqrt{2}$ が無理数であることを以下の方針で証明せよ．
(方針) 背理法で証明する．正整数 m, n を用いて $\sqrt{2} = \dfrac{m}{n}$ と書けたとすると，$2n^2 = m^2$ である[3]．ここで，両辺の素因数分解を考えて素数の個数を比較し，矛盾を導け．

(11.17) **問題** 次の数が無理数であることを証明せよ。
(1) $\sqrt{6}$ (2) $\sqrt{60}$

(11.18) **オイラーの関数** 正整数 n に対して，n 以下の正整数であって n と互いに素なものの個数を $\varphi(n)$ と書き，**オイラーの関数**と呼ぶ．

[3] よく見る証明では，ここで，m が偶数であることを導き，それから n も偶数であることを導く．そして，あらかじめ m, n を互いに素にとっておき矛盾していると結論するが，今の方針はこれとは異なる．

(11.19) **問題** 次の問に答えよ．
(1) 正整数 n とその (正の) 約数 e がある．n 以下の正整数であって，n との最大公約数が e であるようなものの個数は，n/e と互いに素な n/e 以下の正整数の個数に等しいことを証明せよ．
(2) n を正整数とするとき，(1) を利用して次の等式を証明せよ．

$$\varphi(n) = \sum_{d \text{ は } n \text{ の正の約数}} \varphi(d)$$

(11.20) **問題** $\varphi(27)$ と $\varphi(1024)$ を (次の問題の主張は使わずに) 答えよ．

(11.21) **問題** 次の問に答えよ．
(1) 素数 p に対して，$\varphi(p) = p - 1$ を証明せよ．
(2) 素数 p と正整数 n に対して，$\varphi(p^n) = p^{n-1}(p-1)$ を証明せよ．
(3) 相異なる素数 p, q に対して，$\varphi(pq) = (p-1)(q-1)$ を証明せよ．
(4) m, n が互いに素な正整数のとき、(11.19) を利用して次を証明せよ。

$$\varphi(mn) = \varphi(m)\varphi(n)$$

[(4) のヒント: mn の約数は、m の約数と n の約数の積になるが、m, n が互いに素だから、m の約数と n の約数の積たちに重複はなく、d が mn の約数を動くような和は、d_1 が m の約数、d_2 が n の約数を動くような二重の和で $d = d_1 d_2$ とするのと同じである。]

(11.22) **問題** 上の問題を利用して次を求めよ．
(1) $\varphi(27)$ (2) $\varphi(1024)$ (3) $\varphi(100)$ (4) $\varphi(900)$

(11.23) **問題** 次の問に答えよ．
(1) a, m を互いに素な正整数とするとき，$a^{\varphi(m)} \equiv 1 \pmod{m}$ であることを証明せよ (少し難しい)．
(2) **(フェルマーの小定理)** p を素数とし，a が p の倍数ではない正整数であるとき，$a^{p-1} \equiv 1 \pmod{p}$ であることを，(1) を利用して証明せよ．

(3) (**フェルマーの小定理**) p を素数とするとき、$a^p \equiv a \pmod{p}$ であることを，(2) を利用して証明せよ.

§12 イデアル

(12.1) **イデアル** R を可換環とする．$I \subset R$ が R の**イデアル**であるとは，次の条件を満たすことを言う.

(I1) $0 \in I$
(I2) $x, y \in I$ ならば $x + y \in I$
(I3) $x \in I$, $a \in R$ ならば $ax \in I$

(12.2) **例題** $m \in \mathbb{Z}$ に対し，$\mathbb{Z}$ の部分集合 (m) を

$$(m) = \{x \mid x \text{ は } m \text{ の倍数 }\}$$

と定めると，(m) は $\mathbb{Z}$ のイデアルである．(m) を m **で生成される (単項) イデアル**と呼ぶ.

(証明) まず (I1) について，$x, y \in (m)$ とすると，ともに m の倍数だから，$x = mx'$, $y = my'$ と書ける．すると，$x + y = m(x' + y')$ は m の倍数だから，$x + y \in (m)$ である.

次に (I1) について，$x \in (m)$, $a \in \mathbb{Z}$ とすると，$x = mx'$ と書ける．すると，$ax = amx'$ は m の倍数だから，$ax \in (m)$ である.

(12.3) **問題** 次の集合は $\mathbb{Z}$ のイデアルであることを証明せよ.
(1) $\{0\}$ (2) $\mathbb{Z}$

(12.4) **問題** $m, n \in \mathbb{Z}$ と、イデアル (m), (n) に対して、次の条件を考える。
(a) m は n の約数である。 (b) $n \in (m)$. (c) $(n) \subset (m)$.
このとき次を示せ。
(1) (a) ならば (b)
(2) (b) ならば (a)
(3) (b) ならば (c)
(4) (c) ならば (b)

(12.5) **問題** 可換環 R の元 a に対して,

$$(a) = \{ax \mid x \in R\}$$

と定めると，R のイデアルになることを証明せよ．(a) を a **で生成される単項イデアル**と呼ぶ.

(12.6) **問題** 可換環 R の元 $a, b \in R$ と、これらで生成される単項イデアル (a), (b) に対して、次の条件を考える。
(a) $a \in (b)$. (b) $(a) \subset (b)$.
このとき次を示せ。
(1) (a) ならば (b)
(2) (b) ならば (a)

(12.7) **例題** I と J を，可換環 R のイデアルとするとき,

$$IJ = \left\{ \sum_{\text{有限和}} x_i y_i \mid x_i \in I,\ y_i \in J \right\}$$

は R のイデアルであることを証明せよ.

(12.8) **問題** I と J を，可換環 R のイデアルとするとき，次の集合は R のイデアルであることを証明せよ.

(1) $I \cap J$
(2) $I + J = \{x + y \mid x \in I,\ y \in J\}$

(12.9) **例題** $\mathbb{Z}$ のイデアルは，$m \in \mathbb{Z}$ を用いて (m) の形に書ける．つまり，$\mathbb{Z}$ のイデアルはすべて単項イデアルである．このような環を**単項イデアル環**と呼ぶ．

(証明) $I \subset \mathbb{Z}$ をイデアルとする．$I = \{0\}$ ならば，$I = (0)$ と，(m) の形に書けるから，$I \neq \{0\}$ のときを考える．

$x \in I$ ならば $-x \in I$ であることに注意しておく．すると，I には正整数が少なくとも 1 つ属するので，それを m とおく．明らかに $I \supset (m)$ である．反対に，$I \subset (m)$ であることを以下で示す．$x \in I$ を任意にとる．x を m で割り，

$$x = mp + q \quad (p, q \in \mathbb{Z},\ 0 \leq q < m)$$

と書くと，$q = x - mp$ は，$m \in I$ より $mp \in I$ であり，$x \in I$ でもあるから，$q \in I$ である．ところが，$0 \leq q < m$ だから，m の最小性より $q = 0$ である．つまり，$x = mp \in (m)$ だから，$I \subset (m)$ が示せた．

以上より，$I = (m)$ である．

(12.10) **問題** $I = (4)$, $J = (6)$ とするとき，次の $\mathbb{Z}$ のイデアルを，(m) の形に書け．
(1) $I + J$　(2) $I \cap J$　(3) IJ

§13　多項式環

(13.1) **問題** $\mathbb{R}$ 係数の 1 変数多項式環 $\mathbb{R}[x]$ には，0 以外に零因子のないことを証明せよ．

(13.2) **問題** 次の集合は $\mathbb{R}[x]$ のイデアルであることを証明せよ．
(1) $\{0\}$
(2) 定数項が 0 である多項式全体のなす集合

(13.3) **既約性の判定その 1** $\mathbb{Z}[x]$ を $\mathbb{Z}$ 係数の 1 変数多項式全体のなす環とする．素数 p を固定する．$f \in \mathbb{Z}[x]$ とし，f の係数を $\bmod p$ で考えたものを $\overline{f}$ と書く．このとき，f の最高次係数が p の倍数ではなく，$\overline{f} = \overline{g}\overline{h}$ と $\overline{f}$ より低次の多項式の積に分解しないならば，f は $\mathbb{Z}$ 係数の多項式としても，低次の多項式の積に分解しない．

(13.4) **既約性の判定その 2 (アイゼンシュタインの既約性判定法)** 最高次係数が 1 である多項式

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

が，次の 2 条件を満たすならば，f は既約である．
(i) $a_{n-1}, \ldots, a_0$ は p の倍数．　(ii) a_0 は p^2 の倍数ではない．

(13.5) **既約性の判定その 3** 整数係数の多項式が，整数係数の範囲で因数分解できないならば，有理数係数の範囲でも因数分解できない．

(13.6) **問題** 次の多項式が，有理数係数の範囲で既約かどうか判定せよ．既約でないならば因数分解せよ．
(1) $x^2 + x + 1$　(2) $3x^3 + 3x + 1$　(3) $x^3 + 4x^2 - 2$
(4) $x^2 + 2x + 2$　(5) $x^3 + 3x + 3$　(6) $2x^3 + 4x^2 - 4$

(13.7) **例題** $\mathbb{R}[x]$ のイデアルは，$f(x) \in \mathbb{R}[x]$ を用いて，

$$(f(x)) = \{f(x)p(x) \mid p(x) \in \mathbb{R}[x]\}$$

の形に書けることを証明せよ．つまり，$\mathbb{R}[x]$ は単項イデアル環である．

(証明) $I \subset \mathbb{R}[x]$ をイデアルとする．$I = \{0\}$ ならば，$I = (0)$ と，$(f(x))$ の形に書けるから，$I \neq \{0\}$ のときを考える．

I に属する 0 でない多項式のうち，次数最小のものを $f(x)$ とおく．明らかに $I \supset (f(x))$ である．反対に，$I \subset (f(x))$ であることを以下で示す．$g(x) \in I$

を任意にとる．g を f で割り，

$$g(x) = f(x)p(x) + q(x) \quad (p, q \in \mathbb{R}[x],\ \deg(q) < \deg(f))$$

と書くと，$q = g - fp$ は，$f \in I$ より $fp \in I$ であり，$g \in I$ でもあるから，$q \in I$ である．ところが，$\deg(q) < \deg(f)$ だから，f の次数の最小性より $q = 0$ である．つまり，$g = fp \in (f(x))$ だから，$I \subset (f(x))$ が示せた．

以上より，$I = (f(x))$ である．

(13.8) **問題** $I_1 = (x^2 - 1)$, $I_2 = (x^3 - 1)$, $I_3 = (x^3 + 1)$, $I_4 = (x^4 - 1)$ のとき，次の $\mathbb{R}[x]$ のイデアルを単項イデアルの形で書け．

(1) $I_1 + I_2$ (2) $I_1 I_2$ (3) $I_1 \cap I_2$
(4) $I_1 + I_3$ (5) $I_1 I_3$ (6) $I_1 \cap I_3$
(7) $I_1 + I_4$ (8) $I_1 I_4$ (9) $I_1 \cap I_4$
(10) $I_2 + I_3$ (11) $I_2 I_3$ (12) $I_2 \cap I_3$
(13) $I_2 + I_4$ (14) $I_2 I_4$ (15) $I_2 \cap I_4$
(16) $I_3 + I_4$ (17) $I_3 I_4$ (18) $I_3 \cap I_4$

§14 剰余環

(14.1) $\mathbb{Z}$ **の剰余環** $m \in \mathbb{Z}$ を固定する．$a \in \mathbb{Z}$ に対して，

$$\begin{aligned}\overline{a} &= \{x \in \mathbb{Z} \mid x - a \in (m)\} \\ &= \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}\end{aligned}$$

と定め，

$$\begin{aligned}\mathbb{Z}/(m) &= \{\overline{a} \mid a \in \mathbb{Z}\} \\ &= \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}\end{aligned}$$

とおく．$\mathbb{Z}/(m)$ には自然に積や和が定義され，環構造が入る．$\mathbb{Z}/(m)$ を (m) による $\mathbb{Z}$ の**剰余環**と呼ぶ．

(14.2) **問題** $\mathbb{Z}/(6)$ の元のうち，単元，零因子をすべて言え．

(14.3) **問題** $\mathbb{Z}/(m)$ において，$\overline{0}$ 以外のすべての元が逆元を持つための条件を言え．

(14.4) **問題** $\mathbb{Z}/(15)$ において，次の元に逆元がある否か答えよ．あれば逆元も答えよ．

(1) $\overline{11}$ (2) $\overline{12}$ (3) $\overline{13}$ (4) $\overline{14}$

(14.5) $\mathbb{R}[x]$ **の剰余環** I を $\mathbb{R}[x]$ のイデアルとする．$g(x) \in \mathbb{R}[x]$ に対して，

$$\overline{g(x)} = \{h(x) \in \mathbb{R}[x] \mid h(x) - g(x) \in I\}$$

と定め，

$$\mathbb{R}[x]/I = \{\overline{g(x)} \mid g(x) \in \mathbb{R}[x]\}$$

とおく．$\mathbb{R}[x]/I$ には，$\mathbb{Z}/(m)$ と同様に，自然に積や和が定義され，環構造が入る．$\mathbb{R}[x]/I$ を I による $\mathbb{R}[x]$ の**剰余環**と呼ぶ．

$\mathbb{R}[x]$ のイデアルはすべて単項イデアルだから，$\mathbb{R}[x]$ の剰余環はすべて，$\mathbb{R}[x]/(f(x))$ の形をしている．

(14.6) **例題** $\mathbb{R}[x]$ の剰余環 $A = \mathbb{R}[x]/(x^3 + 1)$ について答えよ。

(1) $f(x) \in \mathbb{R}[x]$ に対して、$\overline{f(x)} \in A$ を考える。このとき、高々2 次の $g(x) \in \mathbb{R}[x]$ であって、$\overline{f(x)} = \overline{g(x)}$ となるものが存在することを示せ。
(2) A は $\mathbb{R}$ 上 3 次元ベクトル空間であることを示せ。
(3) A において、$\overline{x^4} = \overline{g(x)}$ となる高々2 次の g を求めよ。

(証明) (1) f を x^3+1 で割り、$f(x) = (x^3+1)p(x)+g(x)$ と書く $(\deg g < 3)$。$f - g \in (x^3 + 1)$ だから、$\overline{f} = \overline{g}$ である。

(2) どんな $\overline{f}$ も高々2 次式で表せるので、$1, \overline{x}, \overline{x^2}$ の $\mathbb{R}$ 上 1 次結合で書けるから、3 次元である。

(3) x^4 を $x^3 + 1$ で割った余りは、$-x$ だから、$g(x) = -x$ である。

(14.7) **問題** $\mathbb{R}[x]/(x^2+1)$ において，次の等式を証明せよ．ただし，$a, b \in \mathbb{R}$ とする．

(1) $\overline{x^2} = \overline{-1}$
(2) $\overline{x+1} \cdot \overline{x-1} = \overline{-2}$
(3) $(\overline{a+bx})^2 = \overline{a^2 - b^2 + 2abx}$
(4) $\overline{a+bx} \cdot \overline{a-bx} = \overline{a^2+b^2}$

(14.8) **問題** $\mathbb{R}[x]/(x^2+1)$ において，次の元たちが $\mathbb{R}$ 上 1 次独立か 1 次従属か答えよ．

(1) $\overline{1}, \overline{x}$
(2) $\overline{1}, \overline{x^2}$
(3) $\overline{x}, \overline{x^2}$

(14.9) **問題** 次の問に答えよ．

(1) $\mathbb{R}[x]/(x^2+1) = \{\overline{g(x)} \mid g(x) \in \mathbb{R}[x], \deg(g) < 2\}$ を示せ．
(2) $\mathbb{R}[x]/(x^2+1)$ が $\mathbb{R}$ 上 2 次元ベクトル空間であることを示せ．

(14.10) **例題** 写像 $f : \mathbb{Z}/(9) \to \mathbb{Z}/(3)$ を

$$\begin{array}{rccc} f: & \mathbb{Z}/(9) & \to & \mathbb{Z}/(3) \\ & \overline{a} & \mapsto & \overline{a} \end{array}$$

で定めるとき，次の問に答えよ．ただし，上の定義において，定義域の $\overline{a}$ は $\mathbb{Z}/(9)$ の元であり，像の $\overline{a}$ は $\mathbb{Z}/(3)$ の元である．このように，どの剰余環の元か紛らわしい場合もあるので，$\overline{a}$ を $a+(9)$ や $a+(3)$ のようにも表す．一般には，可換環 R のイデアル I があるとき，剰余環 R/I の元を，$a+I$ と表す．この a を $a+I$ の**代表元**と呼ぶ．

(1) 写像 f が矛盾なく定義されていることを証明せよ．
(2) 任意の $a, b \in \mathbb{Z}$ に対して，$f(\overline{a}+\overline{b}) = f(\overline{a}) + f(\overline{b})$ を示せ．
(3) 写像 g を $g : \mathbb{Z}/(3) \to \mathbb{Z}/(9)$ $(a+(3) \mapsto a+(9))$ と定めようとしても，矛盾なく定めることはできないことを示せ．

(14.11) **問題** 上の例題と同じく $f : \mathbb{Z}/(9) \to \mathbb{Z}/(3)$ $(a+(9) \mapsto a+(3))$ と定めるとき，次の問に答えよ．

(1) 写像 f が全射であることを証明せよ．
(2) 写像 f が単射ではないことを証明せよ．
(3) 任意の $a, b \in \mathbb{Z}$ に対して，$f(\overline{a} \cdot \overline{b}) = f(\overline{a}) \cdot f(\overline{b})$ を示せ．

(14.12) **問題** m, n を正整数とし，写像 f を

$$\begin{array}{rccc} f: & \mathbb{Z}/(m) & \to & \mathbb{Z}/(n) \\ & a+(m) & \mapsto & a+(n) \end{array}$$

で定める．このとき，次の問に答えよ．

(1) m が n の倍数のとき，f は矛盾なく定義されることを示せ．
(2) m が n の倍数ではないとき，f は矛盾なく定義できないが，矛盾の生じる具体例をあげよ．(m, n は倍数の関係にない一般の正整数であるが，具体例をあげるにあたっては，m, n を自分で適当に決めてもよいことにする．)

(14.13) **問題** 写像 $f : \mathbb{R}[x]/(x^4-1) \to \mathbb{R}[x]/(x^2-1)$ を

$$\begin{array}{rccc} f: & \mathbb{R}[x]/(x^4-1) & \to & \mathbb{R}[x]/(x^2-1) \\ & p(x)+(x^4-1) & \mapsto & p(x)+(x^2-1) \end{array}$$

で定める．このとき，次の問に答えよ．

(1) 写像 f が矛盾なく定義されていることを証明せよ．
(2) 任意の $p(x), q(x) \in \mathbb{R}[x]$ に対して，

$$f\left(\overline{p(x)} + \overline{q(x)}\right) = f\left(\overline{p(x)}\right) + f\left(\overline{q(x)}\right)$$

を示せ．
(3) 写像 g を $g : \mathbb{R}[x]/(x^2-1) \to \mathbb{R}[x]/(x^4-1)$

$$\begin{array}{rccc} g: & \mathbb{R}[x]/(x^2-1) & \to & \mathbb{R}[x]/(x^4-1) \\ & p(x)+(x^2-1) & \mapsto & p(x)+(x^4-1) \end{array}$$

と定めようとしても，矛盾なく定めることはできないことを示せ．

(14.14) **問題** 上の例題と同じく $f : \mathbb{R}/(x^4-1) \to \mathbb{R}/(x^2-1)$ をと定めるとき，次の問に答えよ．

(1) 写像 f が全射であることを証明せよ．
(2) 写像 f が単射ではないことを証明せよ．
(3) 任意の $p(x), q(x) \in \mathbb{R}[x]$ に対して，

$$f\left(\overline{p(x)} \cdot \overline{q(x)}\right) = f\left(\overline{p(x)}\right) \cdot f\left(\overline{q(x)}\right)$$

を示せ．

(14.15) **問題** $\alpha(x), \beta(x) \in \mathbb{R}[x]$ とし，$\alpha(x)$ は $\beta(x)$ の倍元であるとするとき，写像

$$\begin{array}{rccc} f: & \mathbb{R}/(\alpha(x)) & \to & \mathbb{R}[x]/(\beta(x)) \\ & a+(\alpha(x)) & \mapsto & a+(\beta(x)) \end{array}$$

は，矛盾なく定義されることを示せ．

(14.16) **問題** 可換環 R の 2 つのイデアル I, J があり，$I \subset J$ を満たしているとき，写像 f を

$$\begin{array}{rccc} f: & R/I & \to & R/J \\ & a+I & \mapsto & a+J \end{array}$$

で定める．

(1) f は矛盾なく定義されることを示せ．
(2) 任意の $a, b \in R$ に対して，$f(\overline{a}+\overline{b}) = f(\overline{a}) + f(\overline{b})$ を示せ．
(3) 任意の $a, b \in R$ に対して，$f(\overline{a}\cdot\overline{b}) = f(\overline{a}) \cdot f(\overline{b})$ を示せ．

§15 素イデアル・極大イデアル

(15.1) **素イデアル・極大イデアル** R を可換環、I をその真のイデアル (つまり、$I \neq R$) とする。

(1) $ab \in I$ $(a, b \in R)$ ならば、$a \in I$ または $b \in I$ となるような I を**素イデアル**と呼ぶ。

例えば、$\mathbb{Z}$ のイデアル (6) は、$2 \cdot 3 \in (6)$ であるが、2 も 3 も (6) に属さないから、素イデアルではない。他方、(5) は素イデアルである。

(2) I より真に大きい R のイデアルが R 自身に限るとき、I を**極大イデアル**と呼ぶ。

例えば、$\mathbb{Z}$ のイデアル (6) は、それより真に大きいイデアル (2) があるから、極大イデアルではない。他方、(5) は極大イデアルである。

(15.2) **問題** 次の $\mathbb{Z}$ のイデアルが、素イデアルかどうか、極大イデアルかどうかを答えよ。ただし、(15.5) は用いないこと。
(1) (1)　(2) (2)　(3) (3)　(4) (4)　(5) (7)

(15.3) **問題** 次の $\mathbb{R}[x]$ のイデアルが、素イデアルかどうか、極大イデアルかどうかを答えよ。ただし、(15.6) は用いないこと。
(1) $(x-1)$　(2) (x^2)　(3) (x^2-1)　(4) (x^2+1)

(15.4) **問題** 次の $\mathbb{C}[x]$ のイデアルが、素イデアルかどうか、極大イデアルかどうかを答えよ。ただし、(15.6) は用いないこと。
(1) $(x-1)$　(2) (x^2)　(3) (x^2+1)

(15.5) **問題** $m \in \mathbb{Z}$ が素数ならば、イデアル (m) は素イデアル、かつ、極大イデアルであることを示せ。

(15.6) **問題** K を体とする。$f \in K[x]$ が、定数ではない既約多項式ならば、イデアル (f) は素イデアル、かつ、極大イデアルであることを示せ。

(15.7) **整域・体** 可換環 R が**整域**であるとは、0 以外の零因子がないことを言う。可換環 R が**体**であるとは、0 以外の元に逆元が存在することを言う。

例えば、$\mathbb{Z}$ は整域であるが体ではない。$\mathbb{Q}$ は体である。

(15.8) **問題** 体は整域であることを示せ。

(15.9) **問題** R を整域とする。$a,b,c \in R$ に対して、$ab = ac$ かつ $a \neq 0$ ならば、$b = c$ であることを示せ。

(15.10) **問題** R を可換環、I をそのイデアルとする。
(1) I が素イデアルであることと、剰余環 R/I が整域であることは同値であることを示せ。
(2) I が極大イデアルであることと、剰余環 R/I が体であることは同値であることを示せ。
(3) 極大イデアルは素イデアルであることを示せ。

§16 準同型

(16.1) **準同型写像** 可換環 R から S への写像 $f : R \to S$ が**準同型写像**であるとは、次を満たすことを言う。

(H1) $f(a+b) = f(a) + f(b) \quad (a,b \in R)$
(H2) $f(ab) = f(a)f(b) \quad (a,b \in R)$
(H3) $f(1) = 1$

(16.2) **例題** 次の写像が準同型であることを証明せよ。

(1) $f : \mathbb{Z} \to \mathbb{Q} \quad (f(x) = x)$
(2) $f : \mathbb{Q}[x] \to \mathbb{Q} \quad (p(x) \mapsto p(1))$ (1 を代入)

(証明) (1) $f(x+y) = x+y = f(x)+f(y)$ より (H1) が成り立つ。$f(xy) = xy = f(x)f(y)$ より (H2) が成り立つ。$f(1) = 1$ より (H3) が成り立つ。
(2) $f(p+q) = (p+q)(1) = p(1)+q(1) = f(p)+f(q)$ より (H1) が成り立つ。$f(pq) = (pq)(1) = p(1)q(1) = f(p)f(q)$ より (H2) が成り立つ。
また、$\mathbb{Q}[x]$ における乗法単位元は、定数多項式 $I(x) = 1$ であるから、$f(I) = I(1) = 1$ より (H3) が成り立つ。

(16.3) **問題** 次の写像が準同型であることを証明せよ。

(1) $f : \mathbb{Z} \to \mathbb{Z}/(m) \quad (f(x) = \overline{x})$
(2) $f : \mathbb{Q}[x] \to \mathbb{Q}[x]/(x^2+1) \quad (f(p) = \overline{p})$
(3) 可換環 R のイデアル I があるとき、$f : R \to R/I \quad (f(a) = \overline{a})$
(4) 可換環 R のイデアル I と J が、$I \subset J$ のとき、$f : R/I \to R/J \quad (f(a+I) = a+J)$

(16.4) **核** 可換環 R から S への準同型写像 $f : R \to S$ があるとき、f の**核** (**カーネル**) $\mathrm{Ker}(f)$ を

$$\mathrm{Ker}(f) = \{a \in R \mid f(a) = 0\}$$

で定める。

(16.5) **例題** (1) 可換環 R から S への準同型写像 $f : R \to S$ があるとき、$\mathrm{Ker}(f)$ は R のイデアルであることを証明せよ。
(2) $f : \mathbb{Z} \to \mathbb{Z}/(m) \quad (a \mapsto \overline{a})$ の核を求めよ。
(証明) [(I1)] $x,y \in \mathrm{Ker}(f)$ とする。$f(x+y) = f(x)+f(y) = 0+0 = 0$ だから、$x+y \in \mathrm{Ker}(f)$ である。
[(I2)] $x \in \mathrm{Ker}(f)$, $a \in R$ とする。$f(ax) = f(a)f(x) = f(a)0 = 0$ だから、$ax \in \mathrm{Ker}(f)$ である。
(2) $a \in \mathbb{Z}$ が $\mathrm{Ker}(f)$ に属するのは、$\overline{a} = 0$ のとき、つまり、$a \in (m)$ のときだから、$\mathrm{Ker}(f) = (m)$ である。

(16.6) **問題** 次の準同型写像の核を求めよ。
(1) $f : \mathbb{Z} \to \mathbb{Z}/(2) \quad (a \mapsto \overline{a})$
(2) 可換環 R のイデアル I があるとき、$f : R \to R/I \quad (f(a) = \overline{a})$

(16.7) **問題** $\phi : R \to S$ を可換環の準同型写像とする。写像 $\widetilde{\phi} : R[x] \to S[x]$ を、$\widetilde{\phi}(a_0 + a_1x + \cdots + a_nx^n) = \widetilde{\phi}(a_0) + \widetilde{\phi}(a_1)x + \cdots + \widetilde{\phi}(a_n)x^n$ で定めると、環の準同型写像になることを示せ。

§17　追加の問題

(17.1)　例題

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

を満たす整数 x を 1 つ求めよ。

(解) ベズーの方程式を解くと、$5\cdot(-4)+7\cdot 3 = 1$ がわかる。特に、$5\cdot(-4) \equiv 1 \pmod 7$, $7\cdot 3 \equiv 1 \pmod 5$ である。

さて、$x = 5\cdot(-4)\times 4 + 7\cdot 3 \times 3$ とおくと、$x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$ となるから、$x = -17$ が 1 つの解である。

このようにして、一般に、m, n が互いに素であるとき、連立合同式 $x \equiv a \pmod m$, $x \equiv b \pmod n$ の解を求めることができる。

(17.2)　問題　次の連立合同式を満たす整数 x を 1 つ求めよ。

(1) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 8 \end{cases}$　(2) $\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod{19} \end{cases}$　(3) $\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 10 \pmod{13} \end{cases}$

(17.3)　問題　m, n が互いに素であるとき、連立合同式 $x \equiv a \pmod m$, $x \equiv b \pmod n$ を考える。

(1) この連立合同式の 1 つの解 $x = t$ があるとき、$x = t + mnk$ $(k \in \mathbb{Z})$ は、すべて、この連立合同式の解であることを示せ。

(2) $0 \le a < m$, $0 \le b < n$ に対して、この連立合同式の解が $1 \le x \le mn$ にただ 1 つ存在することを示せ。

(3) ϕ をオイラーの関数とするとき、$\phi(mn) = \phi(m)\phi(n)$ であることを示せ。

(17.4)　問題　I と J を可換環 R のイデアルとするとき、次を示せ。

(1) $I \cap J \subset I + J$

(2) $IJ \subset I \cap J$

(3) $I + J = R$ ならば $1 \in I + J$

(4) $1 \in I + J$ ならば $I + J = R$

(5) $I + J = R$ ならば $IJ = I \cap J$

(6) $I \cup J$ が R のイデアルならば、$I \subset J$ または $J \subset I$ であることを示せ。

[(4) のヒント: 1 がイデアルに属するならば、そのどんな倍元もそのイデアルに属することを用いる]

[(5) のヒント: $IJ \supset I \cap J$ を示せばよい、つまり、$x \in I \cap J$ をとり $x \in IJ$ を示せばよい。$1 = a + b$ $(a \in I$, $b \in J)$ と表せるから、$x = 1x = (a + b)x$ という表示を用いる。]

[(6) のヒント: $I \not\subset J$ と仮定して、$J \subset I$ を導く。$I \not\subset J$ ならば $a \in I - J$ がとれる。任意の $b \in J$ に対し、$a + b \in I \cup J$ であり (なぜ?)、$a + b \notin J$ である (なぜ?) から、$a + b \in I$ である (なぜ?)。$a \in I$ だから、$b \in I$ がわかり (なぜ?)、$J \subset I$ となる (なぜ?)。]

(17.5)　問題　R を可換環とし、$a \in R$ を単元とする。このとき、写像 $f : R \to R$ $(f(x) = ax)$ と定める。

(1) f が単射であることを示せ。

(2) f が全射であることを示せ。

(17.6)　問題　可換環 R において、0 以外のすべての元が単元であるとき、R を体と呼ぶ。体 R には、R 自身と $\{0\}$ 以外にイデアルがないことを示せ。

(17.7)　問題　R を可換環とする。$a \in R$ が**冪零元**であるとは、ある正整数 n が存在して、$a^n = 0$ となることを言う。

(1) R の冪零元全体の集合を I と置くと、I はイデアルであることを示せ。

(2) $a \in R$ を冪零元とするとき、$1 - a$ は単元であることを示せ。

[(1) のヒント: 和と、R の元による積で閉じていることを言えばよい。まず和について。$a, b \in I$ をとり、$a^m = b^n = 0$ を満たすとする。$a + b$ を何乗かすれば 0 になることを示せばよい。次に積について。$a \in I$ をとり $a^m = 0$ を満たすとし、$x \in R$ もとる。xa を何乗かすれば 0 になることを示せばよい。]

[(2) のヒント: $1 - a^m$ の因数分解公式を用いる。]

(17.8) **問題** p を素数とする。有理数の集合 R と I を

$$R = \left\{ \frac{a}{b} \;\middle|\; b \text{ は } p \text{ の倍数ではない} \right\}$$
$$I = \left\{ \frac{a}{b} \;\middle|\; b \text{ は } p \text{ の倍数ではなく、} a \text{ は } p \text{ の倍数である} \right\}$$

で定める。
(1) R は環であることを示せ。
(2) R の部分集合 I は R のイデアルであることを示せ。

(17.9) **問題** i を虚数単位とする。複素数の集合 $\mathbb{Z}[i]$ を

$$\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$$

で定める。
(1) $\mathbb{Z}[i]$ は環であることを示せ。
(2) $\mathbb{Z}[i]$ の単元をすべて求めよ。

(17.10) **問題** 実数の集合 $\mathbb{Q}(\sqrt{2})$ を

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$$

で定める。
(1) $\mathbb{Q}(\sqrt{2})$ は環であることを示せ。
(2) $\mathbb{Q}(\sqrt{2})$ は体であることを示せ。

(17.11) **問題** $f(x) \in \mathbb{R}[x]$ が (実数の) 重根を持つとは、ある $a \in \mathbb{R}$ に対して、$(x-a)^2$ が $f(x)$ を割り切ることとする。次の 2 条件は同値であることを示せ。
(a) $f(x)$ は重根を持つ。
(b) $f(a) = 0$ かつ $f'(a) = 0$

(17.12) **問題** 次の問に答えよ。
(1) $\mathbb{Z}/(6)$ のすべてのイデアルを求めよ。
(2) p を素数とするとき、$\mathbb{Z}/(p)$ のすべてのイデアルを求めよ。

(17.13) **問題** $a \in \mathbb{R}$ に対して、写像 $p : \mathbb{R}[x] \to \mathbb{R}$ を $p(f) = f(a)$ で定める (a を代入する写像)。これは環の準同型写像であるが、この写像の核 $\mathrm{Ker}(p)$ を求めよ。

§18 群

(18.1) **群の定義** 集合 G が**群**であるとは、G に演算 $a \cdot b$ $(a, b \in G)$ が定義されており、次の条件を満たすことをいう。

(G1) $(ab)c = a(bc)$ $(a, b, c \in G)$ (結合法則)
(G2) ある元 $e \in G$ が存在して、任意の $a \in G$ に対して $ea = ae = a$ を満たす。このような元 e を **単位元**という。
(G3) 任意の $a \in G$ に対して、$b \in G$ が存在して $ab = ba = e$ を満たす。このような b を a の**逆元**といい、$\boldsymbol{a^{-1}}$ と書く。

群 G が、さらに、

(G4) $ab = ba$ $(a, b \in G)$ (交換法則)

を満たすとき、 G を**アーベル群** (**可換群**) と呼ぶ。
演算が交換法則を満たす和である群を**加法群**と呼ぶことがある。
また、群 G の元の個数を**位数**とよぶ。位数が有限の群を**有限群**、無限の群を**無限群**とよぶ。

(18.2) **問題** 次の集合が指定された演算で群になることを示せ[4]。
(1) $\mathbb{Z}$ (演算は和)
(2) $\mathbb{Q}_+ = \{a \in \mathbb{Q} \mid a > 0\}$ (演算は積)
(3) $A = \{1, -1\}$ (演算は積)
(4) $GL_n(\mathbb{R}) = \{\mathbb{R}$ 成分の n 次正則行列全体 $\}$ (演算は行列の積)
(5) $B = \{\mathbb{R}$ 成分の n 次正則対角行列全体 $\}$ (演算は行列の積)
(6) $C = \{\mathbb{R}$ 成分の n 次正則上三角行列全体 $\}$ (演算は行列の積)

[4] 上三角行列とは、対角成分よりも下側の成分は 0 である行列。

(7) X を集合とするときの、$\mathrm{Aut}(X) = \{f : X \to X \mid f$ は全単射 $\}$ (演算は写像の合成)
(8) $D = \{z \in \mathbb{C} \mid z^5 = 1\}$ (演算は積)

(18.3) **単元群** R を環とするとき、R の**単元群**を、

$$R^\times = \{a \in R \mid a \text{ は単元 }\}$$

で定める[5]。

(18.4) **例題** 次の環の単元群を求めよ。
(1) $\mathbb{Z}$ (2) $\mathbb{Z}/(6)$
(解答)
(1) 整数であって、その逆元が再び整数であるのは 1 と -1 だから、$\mathbb{Z}^\times = \{1, -1\}$ である。
(2) $\mathbb{Z}/(6) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ のうち、逆元を持つものは $\overline{1}$ と $\overline{5}$ なので、$(\mathbb{Z}/(6))^\times = \{\overline{1}, \overline{5}\}$ である。

(18.5) **問題** 次の環の単元群を求めよ。
(1) $\mathbb{Q}$
(2) $\mathbb{Z}/(8)$
(3) $\mathbb{Z}[x]$
(4) $\mathbb{Q}[x]$
(5) $\mathrm{Mat}_n(\mathbb{R}) = \{\mathbb{R}$ 成分の n 次正方行列 $\}$
(6) $A = \{\mathbb{R}$ 成分の n 次対角行列全体 $\}$
(7) $B = \{\mathbb{R}$ 成分の n 次上三角行列全体 $\}$

(18.6) **元の位数** 単位元 e を持つ群 G の元 g の**位数**が n であるとは、$g^n = e$, かつ、$1 \leq k < n$ に対しては $g^k \neq e$ であることを言う。単位元の位数は 1 とする。また、そのような n がない場合は g の位数は ∞ であると定める。

例えば、加法群 $\mathbb{Z}/(4)$ において、$\overline{3}$ は 4 回加えると、初めて単位元 $\overline{0}$ になるので、位数は 4 である。他方、$\overline{2}$ の位数は 2 である。

(18.7) **問題** 次の群の元の位数を求めよ。
(1) 加法群 $\mathbb{Z}/(6)$ の元 $\overline{2}$.
(2) 加法群 $\mathbb{Z}$ の元 2.
(3) $GL_2(\mathbb{R})$ の元 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
(4) $GL_3(\mathbb{R})$ の元 $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.
(5) 対称群 S_3 の元 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
(6) 対称群 S_4 の元である巡回置換 $(1\,2\,3\,4)$.
(7) 対称群 S_5 の元 $(1\,3)(2\,5\,4)$.

(18.8) **問題** 次の問に答えよ。
(1) 群 G の元 g の位数が n であるならば、g^{-1} の位数も n であることを示せ。
(2) 群 G の位数を n とすると、G の元の位数は n 以下であることを示せ[6]。

(18.9) **問題** 次の S_6 の元を、まず、数字に共通部分のない巡回置換の積に分解せよ。次に隣接互換の積で表せ。
(1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$ (2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ (3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ (4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$

(18.10) **問題** 次の問に答えよ。
(1) S_n の元 σ を、数字に共通部分のない巡回置換の積に分解したとき、$\sigma = (a_1\, a_2 \cdots a_k)(b_1\, b_2 \cdots b_l)$ となったとすると、σ の位数は k と l の最小公倍数であることを示せ。
(2) S_3 の元で位数が 2 であるものをすべて答えよ。

[5] 単元とは逆元を持つ元のこと

[6] さらに強く、n の約数になることも証明できる。

(3) S_4 の元で位数が 3 であるものをすべて答えよ。
(4) S_4 の元で位数が 2 であるものをすべて答えよ。
(5) S_5 の元で位数が 3 であるものはいくつあるか。
(6) S_5 の元で位数が 2 であるものはいくつあるか。
(7) S_n の元は $n!$ 乗すると単位元になることを示せ。

(18.11) **部分群** 群 G の空ではない部分集合 H が G の**部分群**であるとは、次の 2 条件を満たすことを言う。

(S1) $x, y \in H$ ならば $xy \in H$
(S2) $x \in H$ ならば $x^{-1} \in H$

(18.12) **問題** H を群 G の部分群であるとし、e を G の単位元であるとする。
(1) $e \in H$ を示せ。
(2) H は群であることを示せ。

(18.13) **問題** G を群とし、単位元を e とする。
(1) G は G の部分群であることを示せ。
(2) $\{e\}$ は G の部分群であることを示せ。

(18.14) **問題** G をアーベル群とする。$H = \{g^2 \mid g \in G\}$ と定めると、H は G の部分群であることを示せ。

(18.15) **例題** 次の群の部分群をすべて答えよ。
(1) 加法群 $\mathbb{Z}/(3)$
(2) 対称群 S_3
(解答)
(1) 部分群を H とすると、H は $\overline{0}$ を必ず含む。これしか含まない場合 $H = \{\overline{0}\}$ は部分群である。

H が $\overline{1}$ も含むならば、和で閉じていることから $\overline{1} + \overline{1} = \overline{2}$ も含む。つまり、$H = G$ となり、これは部分群である。また、H が $\overline{2}$ を含むとしても、$H = G$ となる。

以上より、すべての部分群は、$\{\overline{0}\}$ と G である。
(2) 部分群を H とすると、H は恒等置換 e を必ず含む。これしか含まない場合 $H = \{e\}$ は部分群である。

[$\{e, (1\,2)\} \subset H$ の場合] $H = \{e, (1\,2)\}$ は明らかに積と逆元で閉じているので部分群になっている。

[$\{e, (1\,2), (2\,3)\} \subset H$ の場合] すべての置換は隣接互換の積で表せることから、$H = S_3$ となりこれは部分群である。

[$\{e, (1\,2), (1\,2\,3)\} \subset H$ の場合] H は $(1\,2\,3)(1\,2)(1\,2\,3)(1\,2\,3) = (2\,3)$ も含むので、$H = S_3$ となる。

[$\{e, (1\,2), (1\,3\,2)\} \subset H$ の場合] 同様に $H = S_3$ となる。以上で H が $(1\,2)$ を含む場合は終了である。

[$\{e, (2\,3)\} \subset H$ の場合] 同様に、$H = \{e, (2\,3)\}$ と $H = S_3$ が部分群として得られる。

[$\{e, (1\,3)\} \subset H$ の場合] 同様に、$H = \{e, (1\,3)\}$ と $H = S_3$ が部分群として得られる。

[$\{e, (1\,2\,3)\} \subset H$ の場合] H は $(1\,2\,3)^2 = (1\,3\,2)$ も含み、$H = \{e, (1\,2\,3), (1\,3\,2)\}$ は明らかに積と逆元で閉じているから部分群である。さらに、これに加えて $(1\,2)$, $(2\,3)$ あるいは $(1\,3)$ も含む場合は、上と同様にして $H = S_3$ となる。

[$\{e, (1\,3\,2)\} \subset H$ の場合] 同様に、$H = \{e, (1\,2\,3), (1\,3\,2)\}$ と $H = S_3$ が得られる。

以上をまとめると、すべての部分群は、$\{e\}$, $\{e, (1\,2)\}$, $\{e, (2\,3)\}$, $\{e, (1\,3)\}$, $\{e, (1\,2\,3), (1\,3\,2)\}$, S_3 である。

(18.16) **問題** 次の問に答えよ。
(1) 加法群 $\mathbb{Z}/(4)$ の部分群をすべて答えよ。
(2) 加法群 $\mathbb{Z}/(6)$ の部分群をすべて答えよ。

(3) 対称群 S_4 の部分群で位数が 2 のものをすべて答えよ。
(4) 対称群 S_4 の部分群で位数が 3 のものをすべて答えよ。
(5) 加法群 $\mathbb{Z}$ の部分群をすべて答えよ。

(18.17) **巡回群** 群 G が**巡回群**であるとは、ある $g \in G$ があって、G のすべての元が g^n $(n \in \mathbb{Z})$ の形に表せることを言う。このとき g を**生成元**と呼ぶ。

G が位数 n の有限群ならば、$g^n = e$ となり、$G = \{e = g^0, g, g^2, \ldots, g^{n-1}\}$ となる。G が無限群ならば、$G = \{g^n \mid n \in \mathbb{Z}\}$ となり、$m \neq n$ ならば $g^m \neq g^n$ となる。

(18.18) **例** (1) 加法群 $\mathbb{Z}/(5)$ は、$\overline{1}$ を生成元とする位数 5 の巡回群である。また、$\overline{2}, \overline{3}, \overline{4}$ も生成元である。

(2) 加法群 $\mathbb{Z}$ は 1 を生成元とする無限巡回群である。他に、-1 も生成元である。

(3) $G = \{z \in \mathbb{C} \mid z^4 = 1\}$ は、虚数単位 i を生成元とする巡回群である。

(18.19) **問題** 位数 n の巡回群 G があるとする。k を n の約数とすると、G は、位数 k であり、かつ、巡回群であるような部分群を持つことを証明せよ。

(18.20) **問題** 次の問に答えよ。
(1) 巡回群はアーベル群であることを示せ。
(2) 位数 n の有限巡回群の生成元の個数を求めよ。

(18.21) **問題** 群 G とその元 g があるとき、写像 $f : G \to G$ を $f(x) = gx$ で定める。
(1) f は単射であることを示せ。
(2) f は全射であることを示せ。

(18.22) **問題** 群 G とその元 g があるとき、写像 $f : G \to G$ を $f(x) = gxg^{-1}$ で定める。
(1) $x, y \in G$ のとき、$f(xy) = f(x)f(y)$ を示せ。
(2) $x \in G$ のとき、$f(x)^{-1} = f(x^{-1})$ を示せ。

3 演習問題

(50.1) **問題** 計算して簡単にせよ．ただし，$i = \sqrt{-1}$ とする．
(1) $(4+3i) - (2-3i)$ (2) $(3-4i)^3$ (3) $\dfrac{4+3i}{2-3i}$ (4) $\sqrt{-1}\sqrt{-3}\sqrt{-6}$

(50.2) **問題** 次の問に答えよ．ただし，$i = \sqrt{-1}$ とする．

(1) $(3i-y)(ix+y) = 2+4i$ を満たす満たす実数 x, y の値を求めよ．
(2) x, y を実数とし，次で A, B を定める．$A = B$ のとき，A の値を求めよ．

$$A = \frac{y+i}{x+i}, \quad B = \frac{1+yi}{1+xi}$$

(50.3) **問題** 次の問に答えよ．
(1) 2 次方程式 $x^2 - 2x + 3 = 0$ の 2 解を α, β とするとき，$\dfrac{\alpha^2+\beta^2}{(\alpha-\beta)^2}$ を計算せよ．
(2) 2 数 $1+2i$, $1-2i$ を解に持つような 2 次方程式を言え．

(50.4) **問題** 偏角 $-315°$, 絶対値 4 である複素数を z とするとき，次の問に答えよ．

(1) z を $a+bi$ の形で答えよ．
(2) z^2 の偏角と絶対値を答えよ．
(3) z^{-1} の偏角と絶対値を答えよ．

(50.5) **問題** 次の問に答えよ.
(1) $\sqrt{3}-3i$ を極形式で表せ.
(2) 複素数 $3+i$ を原点中心に 120° 回転した点を複素数で答えよ.
(3) $(1+\sqrt{3}i)^9$ を計算し簡単にせよ.
(4) 1 の 5 乗根をすべて求め，極形式で答えよ.

(50.6) **問題** 次の問に答えよ.

(1) a を実数とする．複素数平面上の異なる 3 点，原点 O, $a+2i$, $2+ai$ が同一直線上にあるとき，a の値を求めよ.
(2) 原点 O, $1+i$, α が正三角形をなすとき，複素数 α を求めよ.

(50.7) **問題** 計算して簡単にせよ.
$$\begin{pmatrix}2&-3\\0&4\end{pmatrix}\begin{pmatrix}662&584&-391\\816&-767&5\end{pmatrix}-\begin{pmatrix}2&-3\\0&4\end{pmatrix}\begin{pmatrix}362&-16&-191\\-184&-167&4\end{pmatrix}$$

(50.8) **問題** $A=\begin{pmatrix}1&-2\\2&-4\end{pmatrix}$ とおくとき，次の問に答えよ．ただし，O は 2 次の零行列とする.
(1) $AB\neq BA$ となるような 2 次正方行列 B を 1 つ求めよ.
(2) $AC\neq O$ だが，$CA=O$ となるような 2 次正方行列 C を 1 つ求めよ.

(50.9) **問題** A, B, C を n 次正方行列とするとき、次を示せ。
(1) ${}^t(ABC)={}^tC\,{}^tB\,{}^tA$
(2) ${}^t(A^3)=({}^tA)^3$
(3) ${}^t(A^m)=({}^tA)^m$ (m は正整数)

(50.10) **問題** 次の行列の逆行列を求めよ.
(1) $\begin{pmatrix}2&-3\\1&4\end{pmatrix}$ (2) $\begin{pmatrix}2&-3&1\\3&4&5\\1&2&2\end{pmatrix}$

(50.11) **問題** 次の行列 A に対して，その逆行列を B とし，B の転置行列を C とし，C の逆行列を D とする．D を答えよ.
$$A=\begin{pmatrix}2&-3&1\\3&4&5\\1&2&2\end{pmatrix}$$

(50.12) **問題** 次の行列式を計算せよ．ただし，(3) と (4) は因数分解した形で答えよ.
(1) $\begin{vmatrix}2&-3\\1&4\end{vmatrix}$ (2) $\begin{vmatrix}2&-3&1\\3&4&5\\1&2&2\end{vmatrix}$ (3) $\begin{vmatrix}a&a&b\\a&b&a\\b&a&a\end{vmatrix}$ (4) $\begin{vmatrix}1&1&1\\a^2&b^2&c^2\\a^4&b^4&c^4\end{vmatrix}$

(50.13) **問題** 次の連立方程式を Cramer の公式を用いて解け．ただし，a,b は 0 でも 1 でもない実数で，$a\neq b$ であるとする.
$$\begin{cases}x+y+z=1\\ax+by+cz=2\\a^2x+b^2y+c^2z=4\end{cases}$$

(50.14) **問題** $\mathbb{R}^n$ 以外のベクトル空間の例を 3 つあげよ.

(50.15) **問題** $\mathbb{R}^n$ のベクトル $v_1,\dots,v_k$ が 1 次独立であることの定義を述べよ.

(50.16) **問題** 次のベクトルが 1 次独立かどうか答えよ.
(1) $\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}3\\4\end{pmatrix}$ (2) $\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}2\\3\end{pmatrix},\begin{pmatrix}3\\4\end{pmatrix}$
(3) $\begin{pmatrix}1\\2\\3\end{pmatrix},\begin{pmatrix}4\\5\\6\end{pmatrix}$ (4) $\begin{pmatrix}1\\1\\0\end{pmatrix},\begin{pmatrix}-1\\0\\1\end{pmatrix},\begin{pmatrix}1\\2\\3\end{pmatrix}$

(50.17) **問題** 前の問題のベクトルは $\mathbb{R}^2$ または $\mathbb{R}^3$ の基底になっているか，それぞれ答えよ．

(50.18) **問題** ベクトル空間 V, W の間の写像 $f : V \to W$ について，f が線型写像であることの定義を述べよ．

(50.19) **問題** 次の写像が線型写像か否か理由とともに答えよ．
(1) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = -x)$
(2) $f : \mathbb{R} \to \mathbb{R}$ $(f(x) = x + 1)$
(3) $f : \mathbb{R}^2 \to \mathbb{R}^3$ $\left(f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x+y \\ y \end{pmatrix} \right)$

(50.20) **問題** $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ とする．$f\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix}$ で定まる写像 $f : \mathbb{R}^2 \to \mathbb{R}^2$ が線型写像であることを証明せよ．

(50.21) **問題** 次の写像 f が線型写像であることを示し、f の核を求めよ。

$$f : \mathbb{R}^3 \to \mathbb{R}^3, \quad f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x-y \\ y-z \\ z-x \end{pmatrix}$$

(50.22) **問題** 次の行列の固有値と固有ベクトルを求めよ．
(1) $\begin{pmatrix} 3 & 8 \\ 7 & 2 \end{pmatrix}$ (2) $\begin{pmatrix} -20 & 25 \\ -16 & 20 \end{pmatrix}$
(3) $\begin{pmatrix} -9 & -6 & -7 \\ 6 & 3 & 7 \\ -1 & -1 & 1 \end{pmatrix}$ (4) $\begin{pmatrix} 6 & 4 & 4 \\ -8 & -6 & -4 \\ 7 & 6 & -1 \end{pmatrix}$

(50.23) **問題** 次の行列が対角化可能ならば対角化せよ．
(1) $\begin{pmatrix} 3 & 8 \\ 7 & 2 \end{pmatrix}$ (2) $\begin{pmatrix} -20 & 25 \\ -16 & 20 \end{pmatrix}$ (3) $\begin{pmatrix} -9 & -6 & -7 \\ 6 & 3 & 7 \\ -1 & -1 & 1 \end{pmatrix}$
(4) $\begin{pmatrix} 6 & 4 & 4 \\ -8 & -6 & -4 \\ 7 & 6 & -1 \end{pmatrix}$ (5) $\begin{pmatrix} 5 & 4 & 4 \\ -4 & -3 & -4 \\ 1 & 1 & 2 \end{pmatrix}$ (6) $\begin{pmatrix} 2 & 6 & 4 \\ -3 & -7 & -4 \\ 3 & 6 & 3 \end{pmatrix}$

(50.24) **問題** 次の等式を満たす x を答えよ．ただし，無数にある x のうち，最小の非負整数で答えよ．
(1) $x \equiv 26 + 77 \pmod 5$ (2) $x \equiv 26 + 77 \pmod{23}$
(3) $x \equiv 26 \cdot 77 \pmod 5$ (4) $x \equiv 26 \cdot 77 \pmod{23}$
(5) $x \equiv 77^{26} \pmod 5$ (6) $x \equiv 77^{26} \pmod{23}$

(50.25) **問題** 次の方程式を満たす整数解を 1 組答えよ．
(1) $96x + 29y = 1$ (2) $35x + 13y = 2$ (3) $34x - 24y = 4$

(50.26) **問題** 次の合同式を満たす整数 x を 1 つ答えよ．
(1) $96x \equiv 1 \pmod{29}$ (2) $35x \equiv 2 \pmod{13}$ (3) $34x \equiv 4 \pmod{24}$
(4) $29x \equiv 1 \pmod{96}$ (5) $13x \equiv 2 \pmod{35}$ (6) $24x \equiv 30 \pmod{34}$

(50.27) **問題** $\sqrt{8}$ が無理数であることを証明せよ。

(50.28) **問題** 次の問に答えよ．
(1) オイラーの関数 $\varphi(n)$ の定義を述べよ．
(2) $\varphi(30)$, $\varphi(40)$, $\varphi(999)$, $\varphi(1000)$ を求めよ．

(50.29) **問題** $\mathbb{Z}$ のイデアル $I = (6)$ を考える。
(1) I を部分集合として含むような $\mathbb{Z}$ のイデアルをすべて言え。
(2) I の部分集合になっているような $\mathbb{Z}$ のイデアルはどのようなイデアルか答えよ。

(50.30) **問題** $\mathbb{Z}$ のイデアルについて、次のイデアルを単項イデアルで答えよ。
(1) $(6)+(8)$ (2) $(6)\cap(8)$ (3) $(6)(8)$

(50.31) **問題** 次の多項式が，有理数係数の範囲で因数分解できるなら因数分解せよ．
(1) x^3+x+1 (2) x^3-2x+6 (3) $x^4+x^3+x^2+2$

(50.32) **問題** $\mathbb{R}[x]$ のイデアル $I=(x^2-1)$ と $J=(x^3+1)$ を考える。次のイデアルを単項イデアルで答えよ。
(1) $I+J$ (2) $I\cap J$ (3) IJ

(50.33) **問題** $\mathbb{Q}[x]$ のイデアル I が、x^2-x と x^2+2 を含むとする。このとき $I=\mathbb{Q}[x]$ であることを示せ。

(50.34) **問題** $\mathbb{Z}/(100)$ の単元をすべて言え。また $\overline{3}$ の逆元を答えよ。

(50.35) **問題** $\mathbb{R}[x]/(x^3+1)$ において、$\overline{x^2-x+1}$ の逆元がないことを示せ。

(50.36) **問題** 次の写像 f は環の準同型写像であることを示せ。また f の核を求めよ。

$$f:\mathbb{R}[x]\to\mathbb{R},\qquad \sum_{k=0}^{n}a_kx^k\mapsto a_0$$

4 演習問題の解答

(50.1) **の解答** (1) $2+6i$ (2) $-117-44i$ (3) $\frac{-1+18i}{13}$ (4) $-3\sqrt{2}i$

(50.2) **の解答** $x=-1,\ y=1$

(50.3) **の解答** (1) $\dfrac{1}{4}$
(2) $\alpha=1+2i,\ \beta=1-2i$ とおけば，$\alpha+\beta=2,\ \alpha\beta=5$ より，$x^2-2x+5=0$

(50.4) **の解答** (1) $2\sqrt{2}+2\sqrt{2}i$
(2) $\arg z=45^\circ$ なので，$\arg z^2=2\arg z=90^\circ$ (これは，-630° でもよいけれど)．$|z^2|=|z|^2=16$.
(3) $\arg z^2=2\arg z=450^\circ$ (これは，315° でもよいけれど)．$|z^{-1}|=|z|^{-1}=\frac{1}{4}$.

(50.5) **の解答** (1) $2\sqrt{3}(\cos 60^\circ+i\sin 60^\circ)$
(2) $(3+i)(\cos 120^\circ+i\sin 120^\circ)=\frac{-3-\sqrt{3}}{2}+\frac{-1+3\sqrt{3}}{2}i$
(3) $(1+\sqrt{3})^9=(2(\cos 60^\circ+i\sin 60^\circ))^9=2^9(\cos 540^\circ+i\sin 540^\circ)=-512$
(4) $\cos(k\cdot 72^\circ)+i\sin(k\cdot 72^\circ)\quad(k=0,1,2,3,4)$

(50.6) **の解答** (1) $a:2=2:a$ より，$a^2=4$ なので，$a=\pm 2$．ところが，$a=2$ だと 2 点が一致して「異なる 3 点」に反するので，$a=-2$.
(2) α は $1+i$ を原点中心に $\pm 60^\circ$ 回転した点である．

$$\begin{aligned}\alpha&=(1+i)(\cos(\pm 60^\circ)+i\sin(\pm 60^\circ))\\&=(1+i)\left(\frac{1}{2}\pm\frac{\sqrt{3}}{2}i\right)=\left(\frac{1}{2}\mp\frac{\sqrt{3}}{2}\right)+\left(\frac{1}{2}\pm\frac{\sqrt{3}}{2}\right)i\end{aligned}$$

(50.7) **の解答** $\begin{pmatrix}-2400 & 3000 & -403\\ 4000 & -2400 & 4\end{pmatrix}$

(50.8) **の解答** (1) $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ (2) $\begin{pmatrix}2 & 2\\ 1 & 1\end{pmatrix}$

(50.9) の解答　(1) まず ${}^t(AB) = {}^tB\,{}^tA$ を証明する (成分表示を使う。省略)。
${}^t(ABC) = {}^t(A(BC)) = {}^t(BC)\,{}^tA = ({}^tC\,{}^tB)\,{}^tA = {}^tC\,{}^tB\,{}^tA$.
(2) (1) において B と C をともに A とすればよい。
(3) m に関する帰納法を用いる。$m = 1$ のときは明らか。m まで成立しているとすると、$m+1$ のとき、${}^t(A^{m+1}) = {}^t(AA^m) = {}^t(A^m)\,{}^tA$ ここで帰納法の仮定を用いると、次に等しい: $({}^tA)^m\,{}^tA = ({}^tA)^{m+1}$. よって $m+1$ のときも成立している。

(50.10) の解答　(1) $\begin{pmatrix} \frac{4}{11} & \frac{3}{11} \\ -\frac{1}{11} & \frac{2}{11} \end{pmatrix}$　(2) $\begin{pmatrix} -2 & 8 & -19 \\ -1 & 3 & -7 \\ 2 & -7 & 17 \end{pmatrix}$

(50.11) の解答　$|A| = 1$ なので逆行列が存在することは，一応注意しておく (だが実際には求めない). $B = A^{-1}$, $C = {}^tB$, $D = C^{-1}$ より，

$$D = C^{-1} = ({}^tB)^{-1} = ({}^t(A^{-1}))^{-1} = {}^t((A^{-1})^{-1}) = {}^tA = \begin{pmatrix} 2 & 3 & 1 \\ -3 & 4 & 2 \\ 1 & 5 & 2 \end{pmatrix}.$$

(50.12) の解答　(1) 11　(2) 1　(3) $-(a-b)^2(2a+b)$ (4) $(a-b)(a+b)(b-c)(b+c)(c-a)(c+a)$

(50.13) の解答　ファンデルモンドの行列式を知っていれば楽だし，そうでなくても，係数行列の行列式さえ求めれば，a や b や c をそれぞれ 2 にすると，Cramer の公式の分子になっていることに気付けば楽.

$A = \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}$ とおくと，$|A| = (a-b)(b-c)(c-a)$ であるから，

$$x = \frac{(2-b)(b-c)(c-2)}{(a-b)(b-c)(c-a)} = \frac{(2-b)(c-2)}{(a-b)(c-a)},$$
$$y = \frac{(a-2)(2-c)(c-a)}{(a-b)(b-c)(c-a)} = \frac{(a-2)(2-c)}{(a-b)(b-c)},$$
$$z = \frac{(a-b)(b-2)(2-a)}{(a-b)(b-c)(c-a)} = \frac{(b-2)(2-a)}{(b-c)(c-a)}.$$

(50.14) の解答　$\mathbb{Q}^n$, $\mathbb{C}^n$, $\mathrm{Mat}(n, \mathbb{R})$ (実数成分 n 次正方行列全体の空間), $\mathbb{Q}(x)$ (x の分数式全体の空間) など.

(50.15) の解答　$v_1, v_2, \ldots, v_k \in V$ が **1 次独立**であるとは，その 1 次結合 $a_1v_1 + a_2v_2 + \cdots + a_kv_k$ が 0 になるのは，すべての $a_j \in \mathbb{R}$ が 0 であるときに限ることを言う.

(50.16) の解答　ベクトルを並べてできる行列の階数を計算する方法 (階数がベクトルの本数に一致することが 1 次独立であるための必要十分条件) が，比較的楽である.
並べてできる行列が正方行列ならば，もう少し簡単な方法がある．その正方行列が正則であることが，1 次独立であるための必要十分条件だから，正方行列の行列式が 0 でないならば 1 次独立である.
(1) 1 次独立である．(2) 1 次独立ではない.
(3) 1 次独立である．(4) 1 次独立である.

(50.17) の解答　$\mathbb{R}^n$ は n 次元だから，$\mathbb{R}^n$ の基底とは，n 本の 1 次独立なベクトルのことである.
(1) 基底である．(2) 基底ではない．(3) 基底ではない．(4) 基底である.

(50.21) **の解答**　線型性の証明は省略。$\mathrm{Ker}(f) = \left\{ \begin{pmatrix} x \\ x \\ x \end{pmatrix} \mid x \in \mathbb{R} \right\}$.

(50.22) **の解答**　(1) 固有値を求めると，$\lambda = -5, 10$ である (計算過程は省略)．$\lambda = -5$ のとき，$\begin{pmatrix} 3 & 8 \\ 7 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -5 \begin{pmatrix} x \\ y \end{pmatrix}$ より，$\begin{pmatrix} 8 & 8 \\ 7 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ を解くと，1 つの固有ベクトルは，$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ である．

同様に，$\lambda = 10$ のときは，$\begin{pmatrix} -7 & 8 \\ 7 & -8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ を解くことになり，1 つの固有ベクトルは，$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 8 \\ 7 \end{pmatrix}$ である．

(2) 固有値を求めると，$\lambda = 0$ である (計算過程は省略)．$\lambda = 0$ のとき，$\begin{pmatrix} -20 & 25 \\ -16 & 20 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ を解くと，固有ベクトルは，$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$ である．

(3) 固有値を求めると，$\lambda = 1, -3$ である (計算過程は省略)．$\lambda = 1$ のとき，連立方程式を簡約化を用いて解くと，

-10	-6	-7	
6	2	7	
-1	-1	0	
-1	-1	0	①③交換
6	2	7	
-10	-6	-7	
1	1	0	① $\times (-1)$
6	2	7	
-10	-6	-7	
1	1	0	
0	-4	7	② + ① $\times (-6)$
0	4	-7	③ + ① $\times 10$
1	1	0	
0	1	$\frac{-7}{4}$	② $\times (\frac{-1}{4})$
0	4	-7	
1	0	$\frac{7}{4}$	① + ② $\times (-1)$
0	1	$\frac{-7}{4}$	
0	0	0	③ + ② $\times (-4)$

よって，固有ベクトルは，$z = k$ (任意定数) と置くと，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -\frac{7}{4}k \\ \frac{7}{4}k \\ k \end{pmatrix}$．あるいは，$k = 4$ と置いて，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -7 \\ 7 \\ 4 \end{pmatrix}$.

$\lambda = -3$ のとき，連立方程式を簡約化を用いて解くと，

-6	-6	-7	
6	6	7	
-1	-1	4	
-1	-1	4	①③交換
6	6	7	
-6	-6	-7	
1	1	-4	① $\times (-1)$
6	6	7	
-6	-6	-7	
1	1	-4	
0	0	31	② $+$ ① $\times (-6)$
0	0	-31	③ $+$ ① $\times 6$
1	1	-4	
0	0	1	② $\times \frac{1}{31}$
0	0	-31	
1	1	0	① $+$ ② $\times 4$
0	0	1	
0	0	0	③ $+$ ② $\times 31$

よって，固有ベクトルは，$y = k$ (任意定数) と置くと，
$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -k \\ k \\ 0 \end{pmatrix}$. あるいは，$k = 1$ と置いて，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$.

(4) 固有値を求めると，$\lambda = 3, -2$ である (計算過程は省略)．$\lambda = 3$ のとき，

連立方程式を簡約化を用いて解くと，

3	4	4	
-8	-9	-4	
7	6	-4	
3	4	4	
1	3	8	② $+$ ① $\times 3$
7	6	-4	
1	3	8	①②交換
3	4	4	
7	6	-4	
1	3	8	
0	-5	-20	② $+$ ① $\times (-3)$
0	-15	-60	③ $+$ ① $\times (-7)$
1	3	8	
0	1	4	② $\times (\frac{-1}{5})$
0	-15	-60	
1	0	-4	① $+$ ② $\times (-3)$
0	1	4	
0	0	0	③ $+$ ② $\times 15$

よって，固有ベクトルは，$z = k$ (任意定数) と置くと，
$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4k \\ -4k \\ k \end{pmatrix}$. あるいは，$k = 1$ と置いて，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \\ 1 \end{pmatrix}$.

$\lambda = -2$ のとき，連立方程式を簡約化を用いて解くと，

8	4	4	
-8	-4	-4	
7	6	1	
1	-2	3	① + ③ × (-1)
-8	-4	-4	
7	6	1	
1	-2	3	
0	-20	20	② + ① × 8
0	20	-20	③ + ① × (-7)
1	-2	3	
0	1	-1	② × $(\frac{-1}{20})$
0	20	-20	
1	0	1	① + ② × 2
0	1	-1	
0	0	0	③ + ② × (-20)

よって，固有ベクトルは，$z = k$ (任意定数) と置くと，
$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -k \\ k \\ k \end{pmatrix}$. あるいは，$k = 1$ と置いて，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$.

(50.23) の解答　(1) (50.22) (1) により，固有値は $\lambda = -5, 10$ であり，対応する固有ベクトルは，$\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 8 \\ 7 \end{pmatrix}$ である．よって，$P = \begin{pmatrix} 1 & 8 \\ -1 & 7 \end{pmatrix}$ とおくと，$P^{-1}AP = \begin{pmatrix} -5 & 0 \\ 0 & 10 \end{pmatrix}$ と対角化できる．

(2) (50.22) (2) によれば，1 次独立な固有ベクトルが 1 つしかないので，対角化可能ではない．

(3) (50.22) (3) によれば，1 次独立な固有ベクトルが 2 つしかないので，対角化可能ではない．

(4) (50.22) (4) によれば，1 次独立な固有ベクトルが 2 つしかないので，対角化可能ではない．

(5) 固有値を計算すると，$\lambda = 2, 1$ である (過程は省略).
$\lambda = 2$ のとき，連立方程式を簡約化を用いて解くと，

3	4	4	
-4	-5	-4	
1	1	0	
1	1	0	①③交換
-4	-5	-4	
3	4	4	
1	1	0	
0	-1	-4	② + ① × 4
0	1	4	③ + ① × (-3)
1	1	0	
0	1	4	②③交換
0	-1	-4	
1	0	-4	① + ② × (-1)
0	1	4	
0	0	0	③ + ②

よって，固有ベクトルは，$\begin{pmatrix} 4 \\ -4 \\ 1 \end{pmatrix}$.

$\lambda = 1$ のとき，連立方程式を簡約化を用いて解くと，

4	4	4	
-4	-4	-4	
1	1	1	
1	1	1	①③交換
-4	-4	-4	
4	4	4	
1	1	1	
0	0	0	② + ① × 4
0	0	0	③ + ① × (-4)

となり，$y = k, z = l$ (任意定数) とおくと，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -k-l \\ k \\ l \end{pmatrix} = k \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + l \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ である．特に，1 次独立な固有ベクトルとして，$\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ と $\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ がとれる．

よって，$P = \begin{pmatrix} 4 & -1 & -1 \\ -4 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ 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．

(6) 固有値を計算すると，$\lambda = 0, -1$ である (過程は省略).

$\lambda = 2$ のとき，連立方程式を簡約化を用いて解くと，

2	6	4	
-3	-7	-4	
3	6	3	
2	6	4	
1	5	4	② + ① × 2
3	6	3	
1	5	4	①②交換
2	6	4	
3	6	3	
1	5	4	
0	-4	-4	② + ① × (-2)
0	-9	-9	③ + ① × (-3)
1	5	4	
0	-4	-4	
0	-1	-1	③ + ② × (-2)
1	5	4	
0	-1	-1	②③交換
0	-4	-4	
1	5	4	
0	1	1	② × (-1)
0	-4	-4	
1	0	-1	① + ② × (-5)
0	1	1	
0	0	0	③ + ② × 4

よって，固有ベクトルは，$\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$.

$\lambda = -1$ のとき，連立方程式を簡約化を用いて解くと，

3	6	4	
-3	-6	-4	
3	6	4	
1	2	$\frac{4}{3}$	① $\times \frac{1}{3}$
-3	-6	-4	
3	6	4	
1	2	$\frac{4}{3}$	
0	0	0	② $+$ ① $\times 3$
0	0	0	③ $+$ ① $\times (-3)$

となり，$y = k$, $z = l$ (任意定数) とおくと，$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -2k - \frac{4}{3}l \\ k \\ l \end{pmatrix} = k\begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} + l\begin{pmatrix} -\frac{4}{3} \\ 0 \\ 1 \end{pmatrix}$ である．特に，1 次独立な固有ベクトルとして，$\begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}$ と $\begin{pmatrix} -\frac{4}{3} \\ 0 \\ 1 \end{pmatrix}$ がとれる．

よって，$P = \begin{pmatrix} 1 & -2 & -4 \\ -1 & 1 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ とおくと，$P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ と対角化できる．

(50.24) の解答 (1) $x = 3$ (2) $x = 11$ (3) $x = 2$ (4) $x = 1$ (5) $x = 4$ (6) $x = 2$

(50.25) の解答 (1)

$$\begin{aligned} 96 \div 29 = 3 \text{ あまり } 9 &\qquad \text{より } 9 = 96 - 29 \cdot 3, &\text{(a)}\\ 29 \div 9 = 3 \text{ あまり } 2 &\qquad \text{より } 2 = 29 - 9 \cdot 3, &\text{(b)}\\ 9 \div 2 = 4 \text{ あまり } 1 &\qquad \text{より } 1 = 9 - 2 \cdot 4, &\text{(c)} \end{aligned}$$

したがって，

$$\begin{aligned} 1 &\overset{\text{c}}{=} 9 - 2 \cdot 4 \\ &\overset{\text{b}}{=} 9 - (29 - 9 \cdot 3) \cdot 4 = 9 \cdot 13 - 29 \cdot 4 \\ &\overset{\text{a}}{=} (96 - 29 \cdot 3) \cdot 13 - 29 \cdot 4 = 96 \cdot 13 - 29 \cdot 43. \end{aligned}$$

よって，$(x, y) = (13, -43)$.

(2)

$$\begin{aligned} 35 \div 13 = 2 \text{ あまり } 9 &\qquad \text{より } 9 = 35 - 13 \cdot 2, &\text{(a)}\\ 13 \div 9 = 1 \text{ あまり } 4 &\qquad \text{より } 4 = 13 - 9, &\text{(b)}\\ 9 \div 4 = 2 \text{ あまり } 1 &\qquad \text{より } 1 = 9 - 4 \cdot 2, &\text{(c)} \end{aligned}$$

したがって，

$$\begin{aligned} 1 &\overset{\text{c}}{=} 9 - 4 \cdot 2 \\ &\overset{\text{b}}{=} 9 - (13 - 9) \cdot 2 = 9 \cdot 3 - 13 \cdot 2 \\ &\overset{\text{a}}{=} (35 - 13 \cdot 2) \cdot 3 - 13 \cdot 2 = 35 \cdot 3 - 13 \cdot 8. \end{aligned}$$

この両辺を 2 倍すると，$2 = 35 \cdot 6 - 13 \cdot 16$ となるので，$(x, y) = (6, -16)$.

(3) $17x - 12y = 2$ を解く．

$$\begin{aligned} 17 \div 12 = 1 \text{ あまり } 5 &\qquad \text{より } 5 = 17 - 12, &\text{(a)}\\ 12 \div 5 = 2 \text{ あまり } 2 &\qquad \text{より } 2 = 12 - 5 \cdot 2, &\text{(b)}\\ 5 \div 2 = 2 \text{ あまり } 1 &\qquad \text{より } 1 = 5 - 2 \cdot 2, &\text{(c)} \end{aligned}$$

したがって,

$$\begin{aligned} 1 &\overset{\text{c}}{=} 5 - 2 \cdot 2 \\ &\overset{\text{b}}{=} 5 - (12 - 5 \cdot 2) \cdot 2 = 5 \cdot 5 - 12 \cdot 2 \\ &\overset{\text{a}}{=} (17 - 12) \cdot 5 - 12 \cdot 2 = 17 \cdot 5 - 12 \cdot 7. \end{aligned}$$

となり, 両辺を 2 倍すると, $2 = 17{\cdot}10 - 12{\cdot}14$ である. よって, $(x, y) = (10, 14)$.

(50.26) **の解答**　(50.26) の結果を使うとよい. 例えば, (1) ならば, $96x + 29y = 1$ において, $(x, y) = (13, -43)$ として, mod 29 すればよい.
(1) $x = 13$　(2) $x = 6$　(3) $x = 10$　(4) $x = -43$ $(x = 53)$　(5) $x = -16$ $(x = 19)$　(6) $x = 14$

(50.27) **の解答**　背理法で証明する。$\sqrt{8} = a/b$ $(a, b$ は正整数$)$ と仮定すると、$8b^2 = a^2$ となる。a, b を素因数分解して、$a = p_1 p_2 \cdots p_s$, $b = q_1 q_2 \cdots q_t$ となったとすると、$2^3 q_1^2 \cdots q_t^2 = p_1^2 \cdots p_s^2$ である。左辺は素数が奇数個の積で、右辺が素数が偶数個の積であるから、素因数分解の一意性に矛盾する。よって仮定が誤りで、$\sqrt{8}$ は無理数である。
(別証明) まず $\sqrt{2}$ が無理数であることを示し (省略)、$\sqrt{8} = 2\sqrt{2}$ なので $\sqrt{8}$ が有理数ならば $\sqrt{2}$ も有理数になってしまい矛盾、という証明方法もある。

(50.28) **の解答**　(1) 1 以上 n 以下の整数のうち，n と互いに素なものの個数.
(2) $\varphi(30) = 8$,　$\varphi(40) = 16$,　$\varphi(999) = 648$,　$\varphi(1000) = 400$.

(50.30) **の解答**　(1) $(1), (2), (3), (6)$ の 4 つ。　(2) 6 の倍数が生成する単項イデアル。つまり、整数 k に対して $(6k)$.

(50.30) **の解答**　(1) (2)　(2) (24)　(3) (48)

(50.31) **の解答**　(1) 係数を mod 2 で考えると，$x^3 + x + \overline{1}$ は，$x = \overline{0}$ を代入しても，$x = \overline{1}$ を代入しても $\overline{0}$ にならないから，どんな 1 次式でも割り切れない．3 次式なので既約であり，因数分解できない．従って，元の $x^3 + x + 1$ も因数分解できない.
(2) アイゼンシュタインの既約性判定法で $p = 2$ とすると，既約であるとわかる．従って因数分解できない.
(3) $(x^2 - x + 1)(x^2 + 2x + 2)$ と因数分解できる.
以下は，この因数分解をどうやるのかわからない人への説明．まず，アイゼンシュタインなどで既約性がなかなか言えず，因数分解できるのではと思い始める．整数係数の範囲で因数分解できるとすると，もし 1 次式で割り切れるなら，定数項を見ると $x \pm 1$ と $x \pm 2$ しか可能性はない．4 通り試してみてどれでも割り切れないことがわかる．残る可能性は 2 次式 2 つの積に因数分解されることだけである．それも，$(x^2 + ax + 1)(x^2 + bx + 2)$ と，$(x^2 + ax - 1)(x^2 + bx - 2)$ しか可能性はないから，順に展開して，係数比較して a, b を決定すればよい.

(50.32) **の解答**　(1) $(x + 1)$　(2) $(x^4 - x^3 + x - 1)$　(3) $(x^5 - x^3 + x^2 - 1)$

(50.33) **の解答**　$x^2 - x$ と $x^2 + 2$ は互いに素だから、$I \supset (x^2 - x, x^2 + 2) = (1) = \mathbb{Q}[x]$. よって、$I = \mathbb{Q}[x]$.

(50.34) **の解答**　単元は、$\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$, $\overline{11}$, $\overline{13}$, $\overline{17}$, $\overline{19}$, $\overline{21}$, $\overline{23}$, $\overline{27}$, $\overline{29}$, $\overline{31}$, $\overline{33}$, $\overline{37}$, $\overline{39}$, $\overline{41}$, $\overline{43}$, $\overline{47}$, $\overline{49}$, $\overline{51}$, $\overline{53}$, $\overline{57}$, $\overline{59}$, $\overline{61}$, $\overline{63}$, $\overline{67}$, $\overline{69}$, $\overline{71}$, $\overline{73}$, $\overline{77}$, $\overline{79}$, $\overline{81}$, $\overline{83}$, $\overline{87}$, $\overline{89}$, $\overline{91}$, $\overline{93}$, $\overline{97}$, $\overline{99}$.
$\overline{3}$ の逆元は、$3x + 100y = 1$ を解けば $(x, y) = (-33, 1)$ が 1 つの解なので、$\overline{-33} = \overline{67}$.

(50.35) **の解答**　$x^3 + 1$ と $x^2 - x + 1$ は互いに素ではないから、$\overline{x^2 - x + 1}$ は逆元を持たない。

(50.36) **の解答**　$p(x) \in \mathbb{R}[x]$ の定数項は $p(0)$ だから、$f(p) = p(0)$ である。
和について、$f(p + q) = (p + q)(0) = p(0) + q(0) = f(p) + f(q)$ である。積について、$f(pq) = (pq)(0) = p(0)q(0) = f(p)f(q)$ である。単位元について、

$f(I) = I(0) = 1$ である。ただし $I(x) = 1 \in \mathbb{R}[x]$ である。以上より f は準同型である。

また、

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

だから、$\mathrm{Ker}(f) =$ { 定数項が 0 である実数係数多項式 } である。