代数学序論Ｂ演習

黒木 玄　(東北大学大学院理学研究科数学専攻)

2007年4月10日

目 次

0 この演習のルール

私が渡した文書に誤りを見つけた場合には気軽に指摘して欲しい.

0.1 各演習時間の基本スケジュール

個人学習時間 渡された演習問題を解いて黒板の前で発表する準備をする.
もしくは自主レポートの準備をする.

14 時 40 分〜 黒板の前で発表したい人はこのあいだに解答を黒板に書いておく.
これと平行して自主レポートの提出を受け付ける.
演習の時間に自主レポートを仕上げて演習の終わりに提出してはいけない.

14 時 50 分頃 解答を書き終えた人から黒板の前での発表開始.

演習終了後 個人的に数学の質問に答える. 数学の勉強の仕方に関する相談にものる.

なお, 毎週のように自主レポートを提出する必要はない. 演習の最初の数回では熱心にレポートを提出していたが, 終わりの方では全然レポートを出さなくなってしまうよりも, 数週間に 1 回のペースでの提出を最後まで守る方がずっと優れていることに注意せよ. 数学の勉強は短距離走よりもマラソンに近い.

0.2 数学をマスターするために必要な勉強法

さて, ある程度以上のレベルの数学をマスターするためには**しっかり書かれた数学の本を丸ごと読む**という勉強が必要になる. そのとき必要なことは

- 証明の理解に論理的ギャップがあってはいけない,
- 数学的な具体例にはどのようなものがあるかをよく調べる,
- 本では説明が省略されている部分を完璧に埋める,
- 本よりも詳しい説明が書かれているノートを作る,
- 最終的には自家製の教科書を完成することを目指す,
- 何よりも重要なのは「数学的本質は何か」について考え続けること

などである. 一冊の本を丸ごと読めない場合には少なくとも章単位で丸ごと読むように努力するのが良い. ノートの作成も重要である. 「教科書を読むよりも君のノートを読んだ方がわかりやすい」と他人に言ってもらえるようなノートを書くことを目指して欲しい.

高校までの数学では問題単位で解き方を習得するような勉強の仕方をしていた人が多いと思う. しかし現在勉強しているような数学を習得するためには「数学の世界がどんな様子をしているか, その本質は何か」を理解するように努力しなければいけない.

私がたくさんの演習問題を渡すのはそれらの問題をすべて解いて欲しいからではない. 演習問題を解く過程でまとまった知識の重要性に気付き, 上に書いたような勉強に進むきっかけを作りたいからである. 演習の時間に「余計なこと」を話そうと努力しているのも同様の理由からである.

以上のような考え方に基づき, この演習では自主レポートとして

私が渡した問題を順番に大量に解いて提出することは禁止

する. 私が渡した問題を大量に解き続ける時間があるなら, 上に書いたような勉強の仕方をした方が良い. 逆に, 上で説明した方法で数学を勉強しながら,

疑問を質問にまとめてレポートとして提出することは推奨

される. 場合によっては問題を解いたレポートよりも質問のレポートの方を高く評価することもありえる. 自分が理解できていないことを論理的に説明することは自分が理解していることをまとめるよりも圧倒的に難しい. 個人的に数学科の卒業生には「自分の疑問を論理的にまとめる能力」が要求されると思う.

0.3 論理的に口頭で説明できる能力も身に付けよう

ここの数学科の卒業生が身に付けることができる能力は

- 現代の進んだ数学の知識を身に付けること
- 英語で書かれた数学の文献を読めるようになること

- 単に日本語や英語の数学文献を読めるだけではなく,
  その内容を他人に対して口頭で論理的に説明できること

の 3 つだと思う. 4 年生のときのセミナーで英語の文献を読むことになるので, 卒業までにしっかり勉強すれば英語で書かれた数学の文献も読めるようになる. この演習では「数学の知識」だけではなく,「論理的に説明できること」をも身に付けてもらいたいと考えている.

以上の考え方に基づき, この演習では単位取得の必要条件として一回以上黒板の前で発表することを義務として課すことにする.

単位が欲しければ最低でも一回以上黒板の前で発表すること!

(自主) レポートも成績の参考にするが, 単位を取得するためにはそれだけでは足りない. 最終的に救済措置を設ける可能性もあるが, 最初からそう期待しないこと.

しかし, 残念ながら演習の時間は限られているので話す練習を十分にできないだろう. 一人当たり 1〜3 回程度黒板の前に立つだけで終わってしまうと思う. しかし各自が問題の解答をノートにまとめるときに他人に説明するために使えるような書き方を心がけるようにすれば「話す準備の練習」は十分にできるように思われる. 数学の文章 (問題の解答を含む) を書くときには常に口頭での説明を要求されることを前提に書くべきである. 自分が説明するためにさえ使えないようでは書く意味がない.

問題の解答を書いたレポートや質問を書いたレポートを提出した場合には, レポートを見た後 (提出の次週以降になる) に適当に見繕って

レポートの内容を黒板の前で説明することを要求するかもしれない.

特に黒板に書かれた解答が少ない場合はそうするだろう. 主としてレポートを提出していても黒板の前で発表していない人の中から選ぶ予定である.

黒板の前での発表を強制すると嫌われる場合があるのだが, 数学について口頭での発表ができる能力は数学科の卒業生として当然要求されるべき能力だと思うので以上のような方針を採用することにした.

0.4 成績評価の方針

- 黒板の前での発表と自主レポートの内容で成績を評価する.
- 各問題の基本点は 10 点であるが, 易しい問題にはそれ未満の点数が付けられ, 難しい問題には 20 点〜∞点の点数が付けられる. 黒板の前で発表するとその基本点が 5 倍以上になり, 自主レポートで提出した場合には基本点がそのまま付けられる.
- **単位が欲しければ最低でも一回以上黒板の前で発表すること.**
- 救済措置があるかもしれないが, 最初からそう期待しないこと.
- 黒板の前で一回以上発表して最後まで論理的ギャップを埋めれば C 以上で単位を出す.
- 自力で解いた場合には他の人が黒板ですでに解いてしまったのと同じ問題の解答を黒板で発表してよい.

- 黒板の前での自主的な発表には自主レポート提出の 5 倍以上の点数を付ける.
- **自主レポートの内容を黒板の前で発表することを要求するかもしれない.**
- こちらが指名してレポートの内容を黒板の前で説明してもらった場合には「黒板の前での説明一回分」とはみなさない. しかし説明の内容が特別に良ければ例外的に「黒板の前での説明一回分」とみなされ, 5 倍以上の点数が付けられることになる.
- 内容に論理的にギャップがある場合には減点する.
- **自主レポートで問題を大量に解いて提出することは禁止.**
  1 回のレポート提出あたり 2 問以下にして欲しい.
- 一つのテーマについて同じような問題を複数解いてレポートとして提出するのではなく, 複数のテーマに関して複数のレポートを提出するように努力して欲しい.
- 線形代数学の本を読みながら感じた疑問を質問にまとめてレポートとして提出しても良い. そのようなレポートは高く評価し, 最低でも 30 点以上の点数を付ける. 質問の内容が高度なものであれば 100 点以上の点数を付けてしまうかもしれない. ただし疑問の内容を私が理解できない場合は黒板の前での説明をお願いするかもしれない.
- 現在習っていることよりも進んだ数学について勉強した結果を自主レポートとして提出しても構わない.
- 問題に誤りを見つけた場合には適切に訂正して解こうとすること.

黒板の前で一回以上発表しているという条件を満たしており, 60 点以上なら C, 90 点以上なら B, 120 点以上なら A, 150 点以上なら AA の成績を付ける予定である.

1 群, 環, 体の紹介

問題に誤りがある場合には訂正してから解くこと.

1.1 群の定義

定義 1.1 (群)

1. 集合 G, 2 項演算 $\cdot : G \times G \to G$, 要素 $1 \in G$, 単項演算 $(\ \ )^{-1} : G \to G$ の 4 つ組 $(G, \cdot, 1, (\ \ )^{-1})$ で以下の公理を満たすものを**群 (group)** と呼ぶ:

   (a) $(xy)z = x(yz) \quad (x, y, z \in G)$ **(結合律)**.

   (b) $1x = x1 = x \quad (x \in G)$ **(単位元)**.

   (c) $x^{-1}x = xx^{-1} = 1 \quad (x \in G)$ **(逆元)**.

   1 を G の単位元, x^{-1} を x の逆元と呼ぶ. なお, 4 つ組 $(G, \cdot, 1, (\ \ )^{-1})$ を毎回並べて書くのは面倒なので, 単に G は群であると言うのが普通である.

2. 群 G がさらに次を満たしているとき, G を**可換群 (commutative group)** もしくは **Abel 群 (Abelian group)** と呼ぶ:

   (d) $xy = yx \quad (x, y \in G)$ **(可換性)**.

   Abel 群の $\cdot, 1, (\ )^{-1}$ をそれぞれ $+, 0, -$ と書くことがある. そのとき G は**加法群 (additive group)** であると言う.

3. 群 G が有限集合であるとき, G は**有限群 (finite group)** であると言い, G の要素の個数を G の**位数 (order)** と呼ぶ.

4. 群 G の部分集合 H が演算 $\cdot, (\ )^{-1}$ で閉じているならば, $1 \in H$ も成立し, H は自然に群をなす. このとき H は G の**部分群 (subgroup)** であると言う. □

[1] (群の定義に関する注意, 小問各 3 点) 集合 G に結合律を満たす 2 項演算 $\cdot : G \times G \to G$ が与えられているとき以下が成立する:

1. $1_L, 1_R \in G$ が $1_L x = x 1_R = x$ $(x \in G)$ を満たしていれば $1_L = 1_R$ である. (つまり, 左単位元と右単位元は一致する.)

2. $1_L \in G$ が $1_L x = x$ $(x \in G)$ を満たしていたとしても, $x 1_R = x$ $(x \in G)$ を満たす $1_R \in G$ が存在しない場合がある. (つまり, 左単位元があっても, 右単位元があるとは限らない.)

3. $1 \in G$ が $1x = x1 = x$ $(x \in G)$ を満たしているとき, 任意の $a, l, r \in G$ に対して $la = ar = 1$ ならば $l = r$ である. (つまり, 両側単位元が存在するとき, 左逆元と右逆元は一致する.)

4. $1_L x = x$ $(x \in G)$ を満たす要素 $1_L \in G$ と $x^L x = 1_L$ $(x \in G)$ を満たす写像 $(\ )^L : G \to G$ が存在するならば G は群である. (つまり, 左単位元と左逆元を持つような結合律を満たす 2 項演算が与えられた集合は群である.)

5. $1_L x = x$ $(x \in G)$ を満たす要素 $1_L \in G$ と $x x^R = 1_L$ $(x \in G)$ を満たす写像 $(\ )^R : G \to G$ が存在しても, G が群にならない場合がある. (つまり, 左単位元と右逆元があっても群になるとは限らない.) □

ヒント. 2. 集合 A からそれ自身への写像 $p : A \to A$ が $p \circ p = p$ を満たしていると仮定する. 集合 G を $G := \{\, p \circ f \mid f \text{ は } A \text{ からそれ自身への写像} \,\}$ と定め, G に 2 項演算を写像の合成によって定めておく. このとき, その 2 項演算は結合律を満たし, $p \in G$ は左単位元になる. しかし, $\mathrm{id}_A \notin G$ であることもあり得るので, 右単位元が存在するとは限らない. そのような例を具体的に構成して調べてみよ.

4. $x = 1_L x = x^{LL} x^L x = x^{LL} 1_L$ なので $x x^L = x^{LL} 1_L x^L = x^{LL} x^L = 1_L$. よって, $x 1_L = x x^L x = 1_L x = x$.

5. 集合 A と $a \in A$ に対して, $B := A \setminus \{a\}$ と置き, G を次のように定める:

$$G = \{\, f : A \to A \mid f \text{ の } B \text{ への制限は } B \text{ から } B \text{ への全単射であり, } f(a) \in B \,\}.$$

G は写像の合成に関して閉じているので, 写像の合成によって結合律を満たす 2 項演算を G に定めることができる. そのとき, 任意の $b \in B$ に対して, $1_b \in G$ を $1_b(x) = x$

$(x \in B)$, $1_b(a) = b$ と定めると, 1_b は G の左単位元である. $f \in G$ に対して $f^R \in G$ を $f^R(x) = f^{-1}(x)$ $(x \in B)$, $f^R(a) = f^{-1}(b)$ と定めると $f \circ f^R = 1_b$ が成立する. しかし, $f(a) \neq f(b)$ を満たす $f \in G$ に対して $g \circ f = 1_b$ を満たす $g \in G$ は存在しない. このような f は B が 2 つ以上の元を持てば存在する. 以上の議論の細部を埋めよ. □

[2] (群の直積, 5 点) G, H が群であるとき, 直積集合 $G \times H$ に積を $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ $(g_i \in G, h_i \in H)$ と定義すると $G \times H$ は自然に群をなす. □

定義 1.2 (生成系, 巡回群) 群の部分集合 $A \subset G$ が G を**生成する (generate)** もしくは G の**生成系 (generating system)** であるとは, G の任意の元を A の元およびその逆元の有限個の積で表わすことができることであると定義する. 1 つの元から生成される群を**巡回群 (cyclic group)** と呼ぶ. □

[3] (巡回群) 以下を示せ:

1. $\mathbb{Z}$ は加法に関して巡回群である. (2 点)
2. 任意の巡回群は Abel 群である. (3 点)
3. 位数が素数に等しい有限群は巡回群である. (10 点) □

定義 1.3 (群の準同型 (homomorphism of groups)) 群の間の写像 $f : G \to H$ が (群の) 準同型写像 (homomorophism) であるとは, f が $f(xy) = f(x)f(y)$, $f(1) = 1$, $f(x^{-1}) = f(x)^{-1}$ $(\forall x, y \in G)$ を満たしていることである. □

[4] (群の準同型写像) 以下を示せ:

1. 群の間の写像 $f : G \to H$ が $f(xy) = f(x)f(y)$ $(\forall x, y \in G)$ のみを満たしていることと, f が準同型であることは同値である. (5 点)
2. 群 G の恒等写像 id_G は準同型であり, 準同型写像の合成もまた準同型である. (2 点)
3. 準同型写像が逆写像を持てばその逆写像も準同型である. 逆写像を持つような群の準同型写像を群の**同型写像 (isomorphism of groups)** と呼ぶ. (3 点) □

[5] (像, 核) $f : G \to H$ は群のあいだの準同型写像であるとする. 以下を示せ:

1. f の**像 (image)** $\mathrm{Im}\, f$ を次のように定める:

$$\mathrm{Im}\, f := f(G) = \{\, f(x) \mid x \in G \,\} \subset H.$$

   $\mathrm{Im}\, f$ は群 H の 2 項演算と逆元を取る操作で閉じており, H の単位元を含むので自然に群とみなせる. (つまり $\mathrm{Im}\, f$ は H の**部分群 (subgroup)** である.)

2. f の**核 (kernel)** $\mathrm{Ker}\, f$ を次のように定める:

$$\mathrm{Ker}\, f := f^{-1}(1) = \{\, x \in G \mid f(x) = 1 \,\}.$$

   $\mathrm{Ker}\, f$ は群 G の 2 項演算と逆元を取る操作で閉じており, G の単位元を含むので自然に群とみなせ, さらに任意の $x \in G$, $k \in \mathrm{Ker}\, f$ に対して $xkx^{-1} \in \mathrm{Ker}\, f$ となる. (つまり $\mathrm{Ker}\, f$ は G の**正規部分群 (normal subgroup)**) である.) □

1.2 群の例

1.2.1 置換群, 交代群

定義 1.4 (置換群, 対称群) n 個の元を持つ集合 $\{1,2,\dots,n\}$ からそれ自身への全単射全体の集合を S_n と書き, S_n の元を $1,2,\dots,n$ の**置換 (permutation)** と呼ぶ. 写像の合成に関して S_n は自然に群をなし, **置換群 (permutation group)** もしくは**対称群 (symmetric group)** と呼ばれる. S_n の位数は $n!$ に等しい. 互いに異なる $i,j \in \{1,2,\dots,n\}$ に対して i と j を交換し, 他を動かさない置換を (i,j) と書き, i と j の**互換 (transposition)** と呼ぶ. □

[6] (置換群の生成系, あみだくじの原理, 20 点) $i = 1,\dots,n-1$ に対して隣り合う i と $i+1$ の互換を $s_i = (i, i+1)$ と書くことにする. このとき $\{s_1, s_2, \dots, s_{n-1}\}$ は置換群 S_n の生成系であり, それらは以下の関係式を満たしている:

(a) $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \quad (i = 1,\dots,n-2)$,

(b) $s_i s_j = s_j s_i \quad (|i-j| \geqq 2)$,

(c) $s_i^2 = 1 \quad (i = 1,\dots,n-1)$. □

注意 1.5 上の問題の (a), (b), (c) は実は生成系 $\{s_1, s_2, \dots, s_{n-1}\}$ に関する置換群 S_n の**基本関係式**になっている. □

注意 1.6 $\{s_1, s_2, \dots, s_{n-1}\}$ から生成される群で基本関係式 (a), (b) を持つ群は**組紐群 (くみひも群, braid group)** と呼ばれている. 同様に置換群は**阿弥陀籤群 (あみだくじ群)** と呼ぶべきかもしれない. □

[7] (10 点) 置換群と阿弥陀籤 (あみだくじ) の関係について説明せよ. あみだくじにおける横線は置換群のどの元に対応しているとみなせるか? □

略解. あみだくじにおける i 番目と $i+1$ 番目の縦線のあいだの横線は互換 $s_i = (i, i+1)$ に対応している. 基本関係式にも言及していればさらに 20 点追加する. □

[8] (偶置換, 奇置換, 20 点) 置換群 S_n の元 σ が, 互換の積で表わされているとき, そこに登場する互換が偶数個か奇数個かは表示によらずに決まっている. 偶数のとき σ は**偶置換**であると言い, 奇数のとき**奇置換**であると言う. $\mathrm{sign} : S_n \to \{\pm 1\}$ を σ が偶置換なら $\mathrm{sign}(\sigma) = 1$, 奇置換なら $\mathrm{sign}(\sigma) = -1$ と定めると, sign は群の準同型写像をなす. sign の核を A_n と書き, n 次**交代群 (alternating group)** と呼ぶ. □

ヒント. 互換 $\sigma_1, \dots, \sigma_r$ の積で表示された置換 $\sigma = \sigma_1 \cdots \sigma_r$ の差積 $\prod_{i<j}(x_i - x_j)$ への作用を自力で調べる. もしくは任意の線形代数の教科書の行列式の節を参照せよ. □

[9] (15 点) 縦線が 100 本のあみだくじについて考える. 縦線には左から順番に 1 から 100 までの番号を付けておく. i 番目の縦線の一番上からスタートしてあみだくじの通常のルールにしたがって進むと $\sigma(i)$ 番目の縦線でゴールに達するものとする.

1. i を $\sigma(i)$ に対応させる写像は 100 次の置換を与えることを説明せよ.

2. あみだくじの横線の個数を 1000 本にすると, $i = 1, 2, \ldots, 99$ に対して $\sigma(i) = i+1$ となり $\sigma(100) = 1$ となるようなあみだくじを作ることができないことを証明せよ. □

ヒント. 偶置換と奇置換の概念を自由に用いてよい. □

[10] (20 点) 縦線が n 本のあみだくじについて考える. 縦線には左から順番に 1 から n までの番号を付けておく. i 番目の縦線の一番上からスタートしてあみだくじの通常のルールにしたがって進むと $\sigma(i)$ 番目の縦線でゴールに達するものとする.

1. i を $\sigma(i)$ に対応させる写像は n 次の置換を与えることを説明せよ.

2. 置換 $\sigma \in S_n$ の**長さ (length)** を $\ell(\sigma)$ と書くことにする:

$$\ell(\sigma) = \sharp\{\,(i,j) \mid i,j = 1,2,\ldots,n \text{ かつ } i < j \text{ かつ } \sigma(i) > \sigma(j)\,\}.$$

置換 σ を与える横線の本数が $\ell(\sigma)$ 本のあみだくじを作れることを証明せよ. □

1.2.2 一般線形群, 特殊線形群

[11] (一般線形群) K は任意の体であるとする. K の元を成分に持つ可逆な n 次正方行列全体の集合を $GL_n(K)$ と書くと, $GL_n(K)$ は行列の積に関して自然に群をなすことを示せ. (ただし正方行列が可逆であることとその行列式が 0 にならないことが同値であるという事実を使ってはいけない.) $GL_n(K)$ を K 上の**一般線形群 (general linear group)** と呼ぶ. □

[12] (三角行列のなす群) 体 K に対して, $GL_n(K)$ 内の上三角で対角線上の成分が全て 1 であるような行列全体の集合を $N_n(K)$ と書くと, $N_n(K)$ は $GL_n(K)$ の部分群である. □

[13] (有限体上の一般線形群の位数, 20 点) $\mathbb{F}_q$ は位数 q の (すなわち元の個数が q 個であるような) 有限体であるとする. このとき, $GL_n(\mathbb{F}_q)$ は有限群になり, その位数は

$$(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)(q-1)$$

に等しい. $N_n(\mathbb{F}_q)$ の位数は $q^{n(n-1)/2}$ である. □

ヒント. $GL_n(K)$ と K^n の中の互いに一次独立な n 本のベクトルの組の全体のなす集合は自然に一対一に対応している. まず, 1 本目のベクトルは 0 以外のものを任意に選べる. 2 本目のベクトルは 1 本目のベクトルで張られる直線以外の場所から選ばなければいけない. 3 本目のベクトルは 1 本目と 2 本目のベクトルで張られる平面以外の場所から選ばなければいけない. …… もしも $K = \mathbb{F}_q$ ならば 1 本目のベクトルの選び方は $q^n - 1$ 通りあり, 2 本目のベクトルの選び方は $q^n - q$ 通りあり, 3 本目のベクトルの選び方は $q^n - q^2$ 通りあり, …… □

[14] (特殊線形群) 体 K に対して, 行列式を取る写像 $\det : GL_n(K) \to K^\times$ は群の全射準同型写像である. $\det : GL_n(K) \to K^\times$ の核を $SL_n(K)$ と書き, **特殊線形群 (special linear group)** と呼ぶ. 位数 q 有限体 $\mathbb{F}_q$ に対して, $SL_n(\mathbb{F}_q)$ の位数は次に等しい:

$$q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1). \quad \square$$

注意 1.7 一般に有限群 G の位数 N の素因数分解を $N = p_1^{e_1}\cdots p_r^{e_r}$ (p_i は互いに異なる素数, e_i は正の整数) と書くとき, 素数 $p = p_i$ に対して G の位数 $p_i^{e_i}$ の部分群を G の **Sylow p 部分群 (Sylow p-subgroup)** と呼ぶ. 有限体 $\mathbb{F}_q$ の位数 q はある素数 p のべき p^e に等しい. 以上の問題の結果から $N_n(\mathbb{F}_q)$ は $GL_n(\mathbb{F}_q)$ と $SL_n(\mathbb{F}_q)$ の Sylow p 部分群であることがわかる. □

1.2.3 直交群, 特殊直交群

体 K の元を成分に持つ n 次正方行列全体の集合を $M_n(K)$ と書く.
実縦ベクトルの空間 $\mathbb{R}^n$ に通常の内積とノルムを次のように入れておく:

$$(x,y) := {}^t xy = \sum_{i=1}^{n} x_i y_i \quad (x = {}^t(x_1,\dots,x_n), y = {}^t(y_1,\dots,y_n) \in \mathbb{R}^n),$$
$$|x| := \sqrt{(x,x)} \qquad\qquad (x = {}^t(x_1,\dots,x_n) \in \mathbb{R}^n).$$

このとき次が成立していることに注意せよ:

$$|x+y|^2 - |x-y|^2 = 4(x,y).$$

[15] (直交群, 特殊直交群) 集合 $O(n)$ を次のように定める:

$$O(n) := \{\, A \in M_n(\mathbb{R}) \mid {}^t AA = E \,\}.$$

ここで ${}^t A$ は A の転置であり, E は単位行列である. $O(n)$ の元を**直交行列 (orthogonal matrix)** と呼ぶ. 以下を示せ:

1. $O(n)$ は行列の積に関して自然に群をなす. $O(n)$ を n 次の**直交群 (orthogonal group)** と呼ぶ. (4 点)
2. $O(n) = \{\, A \in M_n(\mathbb{R}) \mid (Ax, Ay) = (x,y)\ (x,y \in \mathbb{R}^n) \,\}$. (2 点)
3. $O(n) = \{\, A \in M_n(\mathbb{R}) \mid |Ax| = |x|\ (x \in \mathbb{R}^n) \,\}$. (2 点)
4. 行列式を取る写像を $\det$ と書くと, $\det : O(n) \to \mathbb{R}^\times$ は群の準同型であり, その像は $\{\det A \mid A \in O(n)\} = \{\pm 1\}$ となる. $\det : O(n) \to \mathbb{R}^\times$ の核を $SO(n)$ と書き, n 次の**特殊直交群 (special orthogonal group)** と呼ぶ. (2 点) □

より具体的には n 次特殊直交群 $SO(n)$ は次のように表わされる:

$$SO(n) = \{\, A \in M_n(\mathbb{R}) \mid \det A = 1,\ {}^t AA = E \,\}.$$

[16] $SO(2) = \left\{ \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix} \,\middle|\, t \in \mathbb{R} \right\}$ が成立することを示せ. □

注意 1.8 特に, $SO(2)$ は円 S^1 に同相であり, コンパクトかつ弧状連結である. このことより, $O(2)$ は 2 つの S^1 の非連結和に同相であることもわかる. □

[17] (Euler 角, 小問各 5 点) $\theta \in \mathbb{R}$ に対して, 行列 $A(\theta)$, $B(\theta)$ を次のように定義する:

$$A(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad B(\theta) = \begin{bmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{bmatrix}.$$

このとき, 以下が成立することを示せ:

1. $A(\theta), B(\theta) \in SO(3)$.

2. 任意の $X \in SO(3)$ に対して, ある $\phi, \theta, \psi \in \mathbb{R}$ が存在して, $0 \leqq \phi < 2\pi$, $0 \leqq \theta \leqq \pi$, $0 \leqq \psi < 2\pi$, および $X = A(\phi)B(\theta)A(\psi)$ が成立する. (このとき, (ϕ, θ, ψ) は X の **Euler 角**であると言う.)

3. (ϕ, θ, ψ), (ϕ', θ', ψ') は X の Euler 角であるとする. $\theta \neq 0, \pi$ ならば, $(\phi, \theta, \psi) = (\phi', \theta', \psi')$ となり, Euler 角の一意性が成立する. しかし, $\theta = 0, \pi$ のとき, Euler 角の一意性は成立しない. □

ヒント. $A(\theta)$, $B(\theta)$ はそれぞれ z 軸および y 軸のまわりの回転を表わす行列である. そのことに注意しながら図を描きながら考えよ. (自力で解けない場合は例えば [山内・杉浦] の p.45 を見よ.) □

注意 1.9 $SO(3)$ は実3次元射影空間 $\mathbb{P}^3(\mathbb{R})$ に同相である. この手のことについては, [横田] p.131 に詳しい解説がある. 特に $SO(3)$ はコンパクトかつ弧状連結である. □

[18] (30 点) $SO(n)$ が弧状連結であることを証明せよ. □

ヒント. [佐武] の p.178 では直交行列の標準形に関する結果を用いて証明している. 他にも Euler 角の考え方を使って n に関する帰納法によって証明することもできる. その方針は以下の通り. $e_n = (0, 0, \ldots, 0, 1)^t$ (第 n 成分のみが 1 で他は 0) と置く. 与えられた $X \in SO(n)$ に対して, 回転行列の合成 A によってベクトル Xe_n を e_n に移すことができる. このとき, $AX \in SO(n)$ かつ行列 AX は $\begin{bmatrix} X' & 0 \\ 0 & 1 \end{bmatrix}$ $(X' \in SO(n-1))$ の形になる. これより $SO(n)$ の弧状連結性は $SO(n-1)$ の弧状連結性に帰着できることがわかる. □

1.2.4 ユニタリ群, 特殊ユニタリ群

複素縦ベクトルの空間 $\mathbb{C}^n$ に通常の内積とノルムを次のように入れておく:

$$(x, y) := x^* y = \sum_{i=1}^{n} \bar{x}_i y_i \quad (x = (x_1, \ldots, x_n)^t, y = (y_1, \ldots, y_n)^t \in \mathbb{C}^n),$$
$$|x| := \sqrt{(x, x)} \qquad (x = (x_1, \ldots, x_n)^t \in \mathbb{C}^n).$$

ノルム $|\cdot|$ は内積 $(\ ,\ )$ を用いて定義された. 次の問題の結果より, 逆にノルムを用いて内積を表示できることがわかる.

[19] (5 点) $\mathbb{C}^n$ の通常の内積とノルムのあいだには次の関係式が成立している:

$$|x + y|^2 - |x - y|^2 - i|x + iy|^2 + i|x - iy|^2 = 4(x, y).$$

ここで i は虚数単位である. □

ヒント. $c \in \mathbb{C}$, $x, y, z \in \mathbb{C}^n$ に対して $(x, y+z) = (x, y) + (x, z)$, $(x+y, z) = (x, z) + (y, z)$, $(x, cy) = c(x, y)$, $(cx, y) = \bar{c}(x, y)$ が成立することを用いよ. $(y, x) = \overline{(x, y)}$ を使う必要はない. □

[20] (ユニタリ群, 特殊ユニタリ群) 集合 $U(n)$ を次のように定める:

$$U(n) := \{\, A \in M_n(\mathbb{C}) \mid A^*A = E \,\}.$$

ここで A^* は A の随伴行列 (転置の複素共役) であり, E は単位行列である. $U(n)$ の元を**ユニタリ行列 (unitary matrix)** と呼ぶ. 以下を示せ:

1. $U(n)$ は行列の積に関して自然に群をなす. $U(n)$ を n 次の**ユニタリ群 (unitary group)** と呼ぶ. (4 点)
2. $U(n) = \{\, A \in M_n(\mathbb{C}) \mid (Ax, Ay) = (x, y)\ (x, y \in \mathbb{C}^n) \,\}$. (2 点)
3. $U(n) = \{\, A \in M_n(\mathbb{C}) \mid |Ax| = |x|\ (x \in \mathbb{C}^n) \,\}$. (2 点)
4. 行列式を取る写像を $\det$ と書くと, $\det : U(n) \to \mathbb{C}^\times$ は群の準同型であり, 任意の $A \in U(n)$ に対して $|\det A| = 1$ (絶対値が 1) となる. $\det : U(n) \to \mathbb{C}^\times$ の核を $SU(n)$ と書き, n 次の**特殊ユニタリ群 (special unitary group)** と呼ぶ. (2 点) □

より具体的には n 次特殊ユニタリ群 $SU(n)$ は次のように表わされる:

$$SU(n) = \{\, A \in M_n(\mathbb{C}) \mid \det A = 1,\ A^*A = E \,\}.$$

[21] $SU(2) = \left\{ \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \,\middle|\, z, w \in \mathbb{C},\ |z|^2 + |w|^2 = 1 \right\}$ が成立することを示せ. □

注意 1.10 この問題の結果より $SU(2)$ は 3 次元球面 S^3 と同相であることがわかる. (一般に $n-1$ 次元球面は $S^{n-1} = \{x \in \mathbb{R}^n \mid |x| = 1\}$ と定義される. S^2 は 2 点であり, S^1 は円であり, S^2 は (普通の 2 次元) 球面である.) □

[22] (30 点) $U(n)$ と $SU(n)$ は連結かつコンパクトである. □

1.3 環と体の定義

定義 1.11 (環, 可換環) 集合 A とその元 $0, 1 \in A$ と演算 $-: A \to A$, $+, \cdot : A \times A \to A$ の組 $(A, \cdot, 1, +, 0, -)$ が**環 (ring)** であるとは以下が成立していることである:

1. $(A, \cdot, 1)$ はモノイド (単位元付き半群) である. すなわち任意の $a, b, c \in A$ について
   (a) $(ab)c = a(bc)$,
   (b) $1a = a1 = a$.
2. $(A, +, 0, -)$ は可換群である. すなわち任意の $a, b, c \in A$ について
   (a) $(a + b) + c = a + (b + c)$,
   (b) $a + 0 = 0 + a = a$,
   (c) $a + (-a) = (-a) + a = 0$,
   (d) $a + b = b + a$.

3. 加法と乗法のあいだに分配法則が成立している. すなわち $a, b, c \in A$ について

   (a) $a(b+c) = ab + ac$,

   (b) $(a+b)c = ac + bc$.

環 A がさらに次を満たしているとき A は**可換環 (commutative ring)** であるという:

4. 乗法は可換である. すなわち $a, b \in A$ に対して $ab = ba$.

環 A の加法部分群 B が A の積 $\cdot$ について閉じており, A の単位元 1 を含むとき, B は自然に環をなす. このとき B は A の**部分環 (subring)** であると言う. □

例 1.12 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{C}[x]$ は可換環であり, 左の環はそれより右の環の部分環である. (たとえば $\mathbb{Z}$ は $\mathbb{C}[x]$ の部分環である.) □

定義 1.13 (自明な環) 零元 0 だけで構成された集合は $1 = 0$ とみなすことによって自然に環をなす. その環を 0 と書き, **自明な環 (trivial ring)** もしくは**零環 (zero ring)** と呼ぶ. 記号 0 が自明な環と零元の二通りの意味で使われることに注意せよ. □

環 A で $1 = 0$ が成立しているならば任意の $a \in A$ に対して $a = 1a = 0a = 0$ より A は自明な環である. したがって環 A が自明であるための必要十分条件は $1 = 0$ が成立することである. 通常は非自明な環のみを考える.

定義 1.14 (斜体, 体) 可換とは限らない自明でない環 A がさらに次を満たしているとき A は**斜体 (skew field)** であるという:

- 任意の 0 でない A の元 a が A の中に乗法に関する逆元 a^{-1} を持つ.

可換な斜体を単に**体 (field)** と呼んだり, 可換性を強調するために**可換体 (commutative field)** と呼んだりする. □

例 1.15 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は (可換) 体であるが, (有理) 整数環 $\mathbb{Z}$ や (1 変数) 複素多項式環 $\mathbb{C}[x]$ は体ではない. □

定義 1.16 (単数, 単元) 環 A の元 a が A の**単数 (単元, unit)** であるとは A の中に乗法に関する逆元 a^{-1} を持つことである. 環 A の単数全体の集合を $U(A)$ もしくは $A^\times$ と書く. $U(A) = A^\times$ は乗法に関して群をなすので, それを A の**単数群 (単元群, unit group)** と呼ぶ. □

環 A が斜体であるための必要十分条件は $U(A) = A \setminus \{0\}$ が成立することである.

定義 1.17 (零因子, 整域) 環 A の元 a が**左零因子 (left zero-divisor)** であるとはある $b \in A$ で $b \neq 0$ かつ $ab = 0$ を満たすものが存在することである. **右零因子 (right zero-divisor)** も同様に定義される. 可換環では左零因子と右零因子の区別を付ける必要はないので単に零因子と呼ぶ. 0 以外の左右零因子を持たない自明でない環を**整域 (domain, integral domain)** と呼ぶ. すなわち 2 つの 0 でない元の積が決して 0 にならないような自明でない環を整域と呼ぶ. □

可換環だけを主に扱う場合には可換環, 可換整域, 可換体を単に環, 整域, 体と呼ぶことが多い. 可換環の理論は非可換な場合も含む環の一般論とは違う動機 (特に代数幾何 (algebraic geometry) の基礎付け) に基づいて展開されているので, 非可換環の理論は可換環の理論の単純な一般化だとは考えない方が良い.

例 1.18 $\mathbb{Z}$ は整域でかつ $U(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$ である. □

例 1.19 n は 2 以上の自然数であるとする. A は n 次の実対角行列全体集合であるとする. このとき A は可換環であるが整域ではない. □

例 1.20 (行列環) K は任意の (可換) 体であるとし, n は正の整数であるとする. K の元を成分に持つ n 次正方行列全体の集合 $M_n(K)$ は自然に非可換環をなす. $M_n(K)$ の単数群 $U(M_n(K)) = M_n(K)^\times$ は K 上の**一般線形群 (real general linear group)** と呼ばれ, $GL_n(K)$ と書かれる:

$$U(M_n(K)) = M_n(K)^\times = GL_n(K) = \{\, A \in M_n(K) \mid A \text{ は逆行列を持つ} \,\}.$$

n が 2 上ならば $M_n(K)$ は整域ではない. 実際 (i,j) 成分だけが 1 で他の成分が 0 であるような行列を E_{ij} (**行列単位 (matrix unit)** と呼ばれる) と書くと $j \neq k$ のとき $E_{ij}E_{kl} = 0$. □

定義 1.21 (環準同型) A, B は環であるとする. このとき写像 $f : A \to B$ が**環準同型 (ring homomorphism)** であるとは任意の $a, a' \in A$ に対して

$$f(a+a') = f(a) + f(a'), \quad f(aa') = f(a)f(a'), \quad f(1) = 1$$

が成立していることである. 環準同型は

$$f(0) = 0, \quad f(-a) = -f(a).$$

も満たしている. 環準同型は逆写像を持てばその逆写像も環準同型になる. 2 つの環のあいだに全単射環準同型が存在するとき, それら 2 つの環は環として互いに**同型 (isomorphic)** であるという. □

例 1.22 写像 $f : \mathbb{R} \to M_2(\mathbb{R})$ を $f(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ $(a \in \mathbb{R})$ と定める. このとき f は加法群の準同型でかつ $f(ab) = f(a)f(b)$ を満たしているが, $f(1)$ は単位行列に等しくない. 上の環準同型の定義はこのような写像を排除していることに注意せよ. 環準同型は 1 を 1 に移さなければいけない. □

定義 1.23 (代数) K は任意の (可換) 体であるとする. (可換とは限らない) 環 A が K を部分環として含み, 任意の $k \in K$ と任意の $a \in A$ に対して $ka = ak$ が成立するとき, A は K **代数 (K-algebra)** もしくは K **上の代数 (algebra over K)** と呼ばれる. 代数は**多元環**と呼ばれることもある. 乗法が結合律を満たし, 単位元を持つことを強調して, 上の意味での代数を 1 **を持つ結合的代数 (associative algebra with 1)** と呼ぶこともある. (Lie 代数のように結合律を満たさない代数の例もある.) □

例 1.24 多項式環 $\mathbb{C}[x]$ や行列環 $M_n(\mathbb{C})$ は $\mathbb{C}$ 代数である. □

1.4 環と体の例

1.4.1 有理整数環

$\mathbb{Z}$ は可換な整域である.

$\mathbb{Z}$ の最も基本的な性質は商と余りを求める割算を実行できることである. すなわち任意の $f, g \in Z$ に対して, $g \neq 0$ ならばある $q, r \in \mathbb{Z}$ で次の条件を満たすものが一意に存在する:

$$f = gq + r, \quad 0 \leqq r < |f|.$$

このとき q を f **を** g **で割った商 (quotient of** f **divided by** g**)** と呼び, r を f **を** g **で割った余り (remainder of** f **divided by** g**)** と呼ぶのであった.

定義 1.25 (最大公約数) A は可換環であるとする.

1. $g \in A$ が $f \in A$ の**約数 (divisor)** であるとは ある $q \in A$ で $f = gq$ を満たすものが存在することである. このとき f は g で割り切れるもしくは g **は** f **を割る** (g **divides** f) と言い, $g \mid f$ と書く.

2. $g \in A$ が $f_1, \ldots, f_n \in A$ の**公約数 (common divisor)** であるとは, $f_1, \ldots, f_n$ が g で割り切れることである.

3. $g \in A$ が $f_1, \ldots, f_n \in A$ の**最大公約数 (greatest common divisor, g.c.d.)** であるとは, g が $f_1, \ldots, f_n$ の公約数でかつ, g が $f_1, \ldots, f_n$ の任意の公約元で割り切れることである. □

注意 1.26 A は可換環であるとする.

1. 任意の $f \in A$ に対して $1 \mid f$ かつ $f \mid 0$ であることに注意せよ. すなわち 1 はすべての元を割り, 0 はすべての元で割り切れる.

2. A の元を数と呼びたくない場合は公約数を**公約元**と呼ぶことがある. A の元が多項式ならば公約数を**公約多項式**と呼ぶこともある. □

[23] (最大公約数の単数倍を除いた一意性) A は (可換) 整域ならば $f_1, \ldots, f_n \in A$ の最大公約数が存在するならば単数倍を除いて一意的である. □

ヒント. $f_1 = \cdots = f_n = 0$ ならば $f_1, \ldots, f_n$ の最大公約数は 0 しかない. $f_1, \ldots, f_n$ の中に 0 でないものが存在すると仮定する. このとき 0 は $f_1, \ldots, f_n$ の公約数ではない. $g, h \in A$ は $f_1, \ldots, f_n$ の最大公約数であるとする. $g \neq 0$, $h \neq 0$ である. ある $a, b \in A$ が存在して $g = ah$, $h = bg$ となる. よって $g = ah = abg$ であり, A が整域であることから $ab = 1$ となる. ($g = abg$ より $(ab - 1)g = 0$ であるから, $g \neq 0$ と A が整域であることより $ab - 1 = 0$ であることがわかる.) したがって $a, b \in A^\times$ である. これで g, h は互いに相手の単数倍であることがわかった. □

$\mathbb{Z}$ で割算が実行できることを用いて, $f_1, \ldots, f_n \in \mathbb{Z}$ の最大公約数が存在することを示せる. そのためには $f, g \in \mathbb{Z}$ の最大公約数が存在することを示せば十分である. しかも単に存在することを示せるだけではなく, 最大公約数を計算するアルゴリズム (有限で終わる手続き) も得られる. 詳しい説明に関しては以下の問題とそのヒントを見よ.

[24] (Euclid の互除法) $f, g \in \mathbb{Z}$, $g \neq 0$ に対して, f_k $(k = 0, 1, 2, \dots)$ を以下の手続きによって定めることができる:

- $f_0 = f$, $f_1 = g$ と定める.
- もしも $f_k \neq 0$ ならば $q_k, f_{k+1} \in \mathbb{Z}$ を次の条件によって定める:

$$f_{k-1} = q_k f_k + f_{k+1}, \qquad 0 \leqq f_{k+1} < |f_k|.$$

- もしも $f_{k+1} = 0$ すなわち $f_{k-1} = q_k f_k$ ならば手続きを終了する.

$|f_k|$ は単調に減少するのでこの手続きは必ず有限ステップで終了する. $f_{k-1} = q_k f_k$ のとき f_k は f, g の最大公約数になっている. この主張を証明し, 計算の例をひとつ挙げよ. □

ヒント. 上の手続きの結果以下のような計算の列が得られる:

$$\begin{aligned}
&f_0 = f, \\
&f_1 = g \neq 0, \\
&f_0 = q_1 f_1 + f_2, && 0 \leqq f_2 < |f_1|, \\
&f_1 = q_2 f_2 + f_3, && 0 \leqq f_3 < |f_2|, \\
&\quad \cdots\cdots && \quad \cdots\cdots \\
&f_{k-2} = q_{k-1} f_{k-1} + f_k, && 0 \leqq f_k < |f_{k-1}|, \\
&f_{k-1} = q_k f_k.
\end{aligned}$$

これを下から逆順に眺め直すと f_k は $f_{k-1}, f_{k-2}, \dots, f_1, f_0$ の公約数になっていることがわかる. もしも $h \in \mathbb{Z}$ が f_0, f_1 の公約数ならば各ステップの等式を $f_j = f_{j-2} - q_{k-1} f_{k-1}$ と書き直して上から順に見て行けば h は $f_0, f_1, \dots, f_{k-1}, f_k$ すべての約数になっていることもわかる. たとえば 90 と 35 の最大公約数をこの方法で計算してみよ. □

[25] (5 点) 任意の $f, g \in \mathbb{Z}$ に対してある $a, b \in \mathbb{Z}$ で $af + bg$ が f, g の最大公約数になるものが存在する. □

ヒント. $f = g = 0$ ならば 0 が最大公約数であるから自明である. f, g の片方が 0 でない場合について考える. $g \neq 0$ の場合だけを考えれば十分である. Euclid の互除法を使う. Euclid の互除法のステップを上から順番に見て行き, $d = f_k = af_0 + bf_1 = af + bg$ という式が得られることを示す. □

[26] (5 点) 任意の $f_1, \dots, f_n \in \mathbb{Z}$ に対してある $a_1, \dots, a_n \in \mathbb{Z}$ で $a_1 f_1 + \cdots + a_n f_n$ が $f_1, \dots, f_n$ の最大公約数になるものが存在する. □

ヒント. n に関する帰納法. $n = 1$ の場合は明らか. $f_1, \dots, f_{n-1}$ の最大公約数 g と f_n の最大公約数 h は $f_1, \dots, f_{n-1}, f_n$ の最大公約数である. 実際, h は $f_1, \dots, f_{n-1}, f_n$ の公約数であり, $f_1, \dots, f_{n-1}, f_n$ の任意の公約数で h は割り切れる. 帰納法の仮定より g は $g = b_1 f_1 + \cdots + b_{n-1} f_{n-1}$ $(b_i \in \mathbb{Z})$ と表わされる. 上の問題より h は $h = c_1 g + c_2 f_n$ $(c_i \in \mathbb{Z})$ と表わされる. よって, $a_i = c_1 b_i$ $(i = 1, \dots, n-1)$, $a_n = c_2$ と置けば $h = a_1 f_1 + \cdots + a_n f_n$ が成立する. □

以上の２つの問題の結果は非常によく使われる.

最も簡単な応用は以下の通り.

$n \in \mathbb{Z}$, $n \neq 0$ であるとする. $a, b \in \mathbb{Z}$ を n で割った余りが等しいとき $a \equiv b \pmod{n}$ と書き, a **と** b **は** n **を法として合同である** (a **is congruent to** b **modulo** n) と言う. $a \equiv b \pmod{n}$ と $a - b$ が n で割り切れることは同値である.

[27] (5 点) $n \in \mathbb{Z}$, $n \neq 0$ であるとする. $a \in \mathbb{Z}$ と n の最大公約数が 1 ならばある $b \in \mathbb{Z}$ が存在して $ab \equiv 1 \pmod{n}$ となる. すなわち a と n の最大公約数が 1 ならば a は n を法として可逆である. □

ヒント. ある $b, c \in \mathbb{Z}$ が存在して $ba + cn = 1$ となる. このとき $ab = 1 - cn$. □

1.4.2 体上の一変数多項式環

K は任意の体であるとする (たとえば $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$).
K 上の一変数多項式環 $K[x]$ は可換な整域である.

注意 1.27 文字 (不定元) x の多項式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ の中の x は数もしくは K の元ではない. **文字と数を混同しないように注意しなければいけない.** □

多項式 $f \in K[x]$ が $a_0, a_1, \ldots, a_n \in K$ によって

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_n \neq 0$$

と表わされているとき, f の**次数 (degree)** は n であると言い, $\deg f = n$ と置く. $f = 0$ のとき $\deg f = -\infty$ と約束しておく.

[28] (次数の基本性質) $f, g \in K[x]$ に対して

$$\deg(f + g) \leqq \max\{\deg f, \deg g\}, \qquad \deg(fg) = \deg f + \deg g. \quad \square$$

ヒント. f, g の最高次の係数が $f + g$, fg のどこの現われるかを調べよ. □

[29] (多項式環の単元, 5 点) $K[x]$ の単元全体は 0 でない K の元全体に等しい. すなわち $U(K[x]) = K[x]^\times = K^\times$ である. □

ヒント. 上の問題の結果を使う. $f, g \in K[x]$, $1 = fg$ とすると $0 = \deg(fg) = \deg f + \deg g$ である. よって $\deg f = 0$, $degg = 0$ でなければいけない. すなわち $f, g \in K^\times$ である. □

体上の一変数多項式環 $K[x]$ の最も基本的な性質は商と余りを求める割算を実行できることである. すなわち任意の $f, g \in K[x]$ に対して, $g \neq 0$ ならばある $q, r \in K[x]$ で次の条件を満たすものが一意に存在する:

$$f = gq + r, \quad \deg r < \deg g.$$

このとき q を f **を** g **で割った商 (quotient of** f **divided by** g) と呼び, r を f **を** g **で割った余り (remainder of** f **divided by** g) と呼ぶ.

$K[x]$ で割算が実行できることを用いて, $f_1, \ldots, f_n \in K[x]$ の最大公約多項式が存在することを示せる. そのためには $f, g \in K[x]$ の最大公約多項式が存在することを示せば十分である. しかも単に存在することを示せるだけではなく, 最大公約多項式を計算するアルゴリズム (有限で終わる手続き) も得られる. 詳しい説明に関しては以下の問題とそのヒントを見よ.

[30] (Euclid の互除法) $f, g \in K[x]$, $g \neq 0$ に対して, f_k $(k = 0, 1, 2, \dots)$ を以下の手続きによって定めることができる:

- $f_0 = f$, $f_1 = g$ と定める.
- もしも $f_k \neq 0$ ならば $q_k, f_{k+1} \in K[x]$ を次の条件によって定める:

$$f_{k-1} = q_k f_k + f_{k+1}, \qquad \deg f_{k+1} < \deg f_k.$$

- もしも $f_{k+1} = 0$ すなわち $f_{k-1} = q_k f_k$ ならば手続きを終了する.

$\deg f_k$ は単調に減少するのでこの手続きは必ず有限ステップで終了する. $f_{k-1} = q_k f_k$ のとき f_k は f, g の最大公約多項式になっている. この主張を証明せよ. □

ヒント. 上の手続きの結果以下のような計算の列が得られる:

$$\begin{aligned}
&f_0 = f, \\
&f_1 = g \neq 0, \\
&f_0 = q_1 f_1 + f_2, && \deg f_2 < \deg f_1, \\
&f_1 = q_2 f_2 + f_3, && \deg f_3 < \deg f_2, \\
&\quad \cdots\cdots && \quad \cdots\cdots \\
&f_{k-2} = q_{k-1} f_{k-1} + f_k, && \deg f_k < \deg f_{k-1}, \\
&f_{k-1} = q_k f_k.
\end{aligned}$$

これを下から逆順に眺め直すと f_k は $f_{k-1}, f_{k-2}, \dots, f_1, f_0$ の公約多項式になっていることがわかる. もしも $h \in K[x]$ が f_0, f_1 の公約多項式ならば各ステップの等式を $f_j = f_{j-2} - q_{k-1} f_{k-1}$ と書き直して上から順に見て行けば h は $f_0, f_1, \dots, f_{k-1}, f_k$ すべての約多項式になっていることもわかる. □

[31] (5 点) 任意の $f, g \in K[x]$ に対してある $a, b \in K[x]$ で $af + bg$ が f, g の最大公約多項式になるものが存在する. □

ヒント. $f = g = 0$ ならば 0 が最大公約多項式であるから自明である. f, g の片方が 0 でない場合について考える. $g \neq 0$ の場合だけを考えれば十分である. Euclid の互除法を使う. Euclid の互除法のステップを上から順番に見て行き, $d = f_k = af_0 + bf_1 = af + bg$ という式が得られることを示す. □

[32] (5 点) 任意の $f_1, \dots, f_n \in K[x]$ に対してある $a_1, \dots, a_n \in K[x]$ で $a_1 f_1 + \cdots + a_n f_n$ が $f_1, \dots, f_n$ の最大公約多項式になるものが存在する. □

ヒント. n に関する帰納法. $n = 1$ の場合は明らか. $f_1, \dots, f_{n-1}$ の最大公約多項式 g と f_n の最大公約多項式 h は $f_1, \dots, f_{n-1}, f_n$ の最大公約多項式である. 実際, h は $f_1, \dots, f_{n-1}, f_n$ の公約多項式であり, $f_1, \dots, f_{n-1}, f_n$ の任意の公約多項式で h は割り切れる. 帰納法の仮定より g は $g = b_1 f_1 + \cdots + b_{n-1} f_{n-1}$ $(b_i \in K[x])$ と表わされる. 上の問題より h は $h = c_1 g + c_2 f_n$ $(c_i \in K[x])$ と表わされる. よって, $a_i = c_1 b_i$ $(i = 1, \dots, n-1)$, $a_n = c_2$ と置けば $h = a_1 f_1 + \cdots + a_n f_n$ が成立する. □

以上の2つの問題の結果は非常によく使われる.

最も簡単な応用は以下の通り.

$f \in K[x]$, $f \neq 0$ であるとする. $a, b \in K[x]$ を f で割った余りが等しいとき $a \equiv b \pmod{f}$ と書き, a **と** b **は** f **を法として合同である (**a **is congruent to** b **modulo** f**)** と言う. $a \equiv b \pmod{n}$ と $a - b$ が f で割り切れることは同値である.

[33] (5点) $f \in K[x]$, $f \neq 0$ であるとする. $a \in K[x]$ と f の最大公約多項式が 1 ならばある $b \in K[x]$ が存在して $ab \equiv 1 \pmod{f}$ となる. すなわち a と f の最大公約多項式が 1 ならば a は f を法として可逆である. □

ヒント. ある $b, c \in K[x]$ が存在して $ba + cf = 1$ となる. このとき $ab = 1 - cf$. □

以上のように $\mathbb{Z}$ に関する議論と $K[x]$ に関する議論を平行して進めることができる.

参考 1.28 代数の講義の方で「有限生成 Abel 群の基本定理」について習うことになっている. この演習と対応する講義では「行列の Jordan 標準形の理論」について習うことになる. 実は「有限生成 Abel 群の基本定理」は「有限生成 $\mathbb{Z}$ 加群の理論」であり, 「Jordan 標準形の理論」は「有限生成 $K[x]$ 加群の理論」から容易に導くことができる. 以上で説明した Euclid の互除法とその簡単な応用は「有限生成 $\mathbb{Z}$ 加群の理論」や「有限生成 $K[x]$ 加群の理論」を構築するための基本的な道具になる. **このように抽象代数学 (より一般に数学全般) を習うと, 一見して異なる世界を同じアイデアで扱うことが可能になる.** □

多項式に関する Euclid の互助法の計算問題を幾つか出しておく.

[34] (3点) $K = \mathbb{R}$ のとき $f(x) = x^4 + x^3 + 2x^2 + x + 1$, $g(x) = x^3 - 1$ の最大公約元を Euclid の互除法と素因子分解の両方の方法で求めてそれらが定数倍を除いて一致していることを確かめよ. □

略解. 略解: $f(x) = (x^2 + 1)(x^2 + x + 1)$, $g(x) = (x - 1)(x^2 + x + 1)$ であるから, f, g の最大元は $h(x) = x^2 + x + 1$ である. 一方, $f_0 = f$, $f_1 = g$, $f_2(x) = 2x^2 + 2x + 2$ であり, $f_1(x) = (\frac{1}{2}x - \frac{1}{2})f_2(x)$ であるから, f_2 は f_0, f_1 の最大公約元である. $f_2 = 2h$ である. □

[35] (3点) $f, g \in \mathbb{Q}[x]$ を $f(x) = x^4 - 2x^2 + 1$, $g(x) = x^3 - 1$ と定める. 素因子分解と Euclid の互除法の 2 つの方法で f と g の最大公約多項式を求め, 0 でない有理数倍を除いて一致していることを確かめよ. □

略解. $f(x) = (x-1)^2(x+1)^2$, $g(x) = (x-1)(x^2+x+1)$ であるから, f と g の最大公約多項式は $x-1$ である. Euclid の互除法で計算すると $f_2(x) = -2x^2 + x + 1$, $f_3(x) = \frac{3}{4}x - \frac{3}{4}$, $f_4(x) = 0$ となり, 最大公約多項式は $f_3(x) = \frac{3}{4}(x - 1)$ であることがわかる. □

[36] $f, g \in \mathbb{Q}[x]$ を $f(x) = (x + 2)^2(x^2 + x - 1)(x^2 + 1)$, $g(x) = (x - 2)(x^2 - 2)(x^2 + 1)$ と定める. このとき f と g の最大公約多項式が $x^2 + 1$ である. Euclid の互除法で f と g の最大公約多項式を計算すると, 出て来る数字がどんどん大きくなってしまい, 手計算がかなり大変になることを確かめよ. コンピューターを用いて計算しても構わない. その場合はコンピューターをどのように使ったかについても説明すること. □

ヒント. 計算結果は次のようになる. 虫食いを埋めよ:

$$
\begin{aligned}
&f_0(x) = f(x) = x^6 + 5x^5 + \boxed{ア}x^4 + 5x^3 + 3x^2 - 4,\\
&f_1(x) = g(x) = x^5 - \boxed{イ}x^4 - x^3 + 2x^2 - 2x + 4,\\
&f_2(x) = 23x^4 + 10x^3 - \boxed{ウ}x^2 + 10x - 32, \qquad q_1(x) = x + 7,\\
&f_3(x) = \frac{\boxed{オ}}{\boxed{エ}}x^3 + \frac{\boxed{カ}}{\boxed{エ}}x^2 + \frac{\boxed{オ}}{\boxed{エ}}x + \frac{\boxed{カ}}{\boxed{エ}}, \qquad q_2(x) = \frac{1}{23}x - \frac{56}{\boxed{エ}},\\
&f_4(x) = -\frac{42320}{\boxed{キ}}x^2 - \frac{42320}{\boxed{キ}}, \qquad q_3(x) = \frac{12167}{238}x - \frac{670772}{\boxed{キ}},\\
&f_5(x) = 0, \qquad q_4(x) = -\frac{1685159}{11193640}x - \frac{1147041}{\boxed{ク}}. \quad \square
\end{aligned}
$$

略解. $f_0 = f$, $f_1 = g$ と置き, f_{k-1} を f_k で割った余りを f_{k+1} とし, 商を q_k とする計算の結果は次のようになる:

$$
\begin{aligned}
&f_0(x) = f(x) = x^6 + 5x^5 + 8x^4 + 5x^3 + 3x^2 - 4,\\
&f_1(x) = g(x) = x^5 - 2x^4 - x^3 + 2x^2 - 2x + 4,\\
&f_2(x) = 23x^4 + 10x^3 - 9x^2 + 10x - 32, \qquad q_1(x) = x + 7,\\
&f_3(x) = \frac{238}{529}x^3 + \frac{324}{529}x^2 + \frac{238}{529}x + \frac{324}{529}, \qquad q_2(x) = \frac{1}{23}x - \frac{56}{529},\\
&f_4(x) = -\frac{42320}{14161}x^2 - \frac{42320}{14161}, \qquad q_3(x) = \frac{12167}{238}x - \frac{670772}{14161},\\
&f_5(x) = 0, \qquad q_4(x) = -\frac{1685159}{11193640}x - \frac{1147041}{5596820}.
\end{aligned}
$$

f_4 が f, g の最大公約多項式である. $\square$

1.4.3 有限体

[37] (二元体, 5 点) 集合 $\mathbb{F}_2 = \{0, 1\}$ に次のように加法と乗法を定めると $\mathbb{F}_2$ は体になる:

$$
\begin{aligned}
&0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0;\\
&0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1. \quad \square
\end{aligned}
$$

[38] (p 元体, 10 点) p は任意の素数であるとする. 集合 $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ に次のように加法と乗法を定めると $\mathbb{F}_p$ は体になる:

$$
\begin{aligned}
&a + b = (\text{整数としての和 } a + b \text{ を } p \text{ で割った余り}),\\
&a \cdot b = (\text{整数としての積 } ab \text{ を } p \text{ で割った余り}). \quad \square
\end{aligned}
$$

参考 1.29 (有限体) 一般に素数 p が与えられたとき, 集合 $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ に通常の整数の和と積の p で割った余りを考えることによって $\mathbb{F}_p$ の加法と乗法を定めると $\mathbb{F}_p$ は体をなす. 有限個の元しか持たない体を**有限体 (finite field)** と呼ぶ. 有限体の元の個数 (有限体の位数と呼ばれる) は素数の巾 $q = p^e$ (p は素数, e は正の整数) になる. 位数 q の有限体は $\mathcal{F}_q$ と表わされる. $\square$

参考 1.30 (ガロア) なお, 有限体は **Galois 体 (Galois filed)** と呼ばれ $GF(q)$ と表わされることもある. Évariste Galois (エヴァリスト・ガロア, 1811.10.25–1832.5.31) は 19 世紀の初頭に登場した天才数学者の一人である. 決闘で悲劇的な結末をむかえたことで有名である[1]. 群 (group) を導入して対称性 (symmetry) の概念を数学的に明確にし, 方程式をその対称性を調べることに統制するという考え方を導入したのは Galois である. 19 世紀は天才数学者が次々に登場した世紀であり, その歴史は非常に面白い. □

参考 1.31 (有限体上の幾何) 慣れ親しんで来た実数体や複素数体の世界と有限体の世界はまるで違っているように見えるかもしれない. しかし, 実際にはそうではないことが知られている. 実数体をもとにして定義された図形には連続性の直観が適用でき, トポロジーの理論が展開される. 有限体上の代数多様体 (これもある種の図形) に対してもトポロジーの理論を展開することができることがすでに知られている[2]. このような驚くべき数学の発展が 20 世紀のあいだになされた[3]. □

1.4.4 Hamilton の四元数

この節の内容はおまけである.

斜体の最も有名な例は次の問題の Hamilton の四元数体だと思う. Hamilton の四元数体は複素数体をさらに拡張したものである. Hamilton は最初複素数に虚数単位 i とは別の「数」をひとつだけ付け加えることによって「良い環」を構成しようとしたらしい. しかしある日 Hamilton はひとつだけではなく j と k のふたつを付け加えると「非常に良い環」ができることに気付いた。それが Hamilton の四元数体である.

[39] (Hamilton の四元数体, 小問各 5 点) Hamiton の四元数体 $\mathbb{H}$ を定義しよう. 複素数体 $\mathbb{C}$ を拡張して $\mathbb{H}$ を $\mathbb{R}$ 上のベクトル空間として次のように定める:

$$\mathbb{H} = \{\, a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\}.$$

1, i, j, k は $\mathbb{H}$ の $\mathbb{R}$ 上の基底になっているとする. $a1$ を以下では単に a と書くことにする. さらに複素数体の虚数単位の計算規則を拡張し, 次のように i, j, k のあいだの積を定める:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

以下を示せ:

1. $\mathbb{H}$ には自然に環構造が入る.
2. 任意の 0 でない $\mathbb{H}$ の元は乗法に関する逆元を持つ.

よって $\mathbb{H}$ は斜体をなす. $\mathbb{H}$ を **Hamilton の四元数体 (Hamiltonian quaternion field)** と呼び, $\mathbb{H}$ の元を**四元数 (quaternion)** と呼ぶ. さらに次を示せ:

3. $p, q, r \in \mathbb{R}$, $p^2 + q^2 + r^2 = 1$ に対して $I = pi + qj + rk$ と置く. このとき $I^2 = -1$ である. よって $\mathbb{C}_I = \{\, a + bI \mid a, b \in \mathbb{R} \,\} \subset \mathbb{H}$ は複素数体と同型な体をなす.

[1] おすすめの伝記はインフェルト [Infeld] である.

[2] Grothendieck の etale topology の理論.

[3] 有限体上の幾何は純粋数学的に重要なだけではなく, 我々の実生活に関わる応用面でも重要である. 有限体はコンピューターと相性が良い.

このように Hamilton の四元数体の中には連続的に無限個の複素数体 $\mathbb{C}_I$ が含まれているとみなせる. □

ヒント. 1. 問題は結合律の証明. 直接証明することは少し面倒だが易しい. このヒントでは四元数を行列で表現することによる証明法を紹介しよう. $\mathbb{R}$ 上の線形写像 $A : \mathbb{H} \to M_4(\mathbb{R})$ を $\alpha = a + bi + cj + dk \in \mathbb{H}$ に対して

$$A(\alpha) = \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}.$$

と定める. たとえば $A(1)$ は単位行列になり,

$$A(i) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad A(j) = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad A(k) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

このとき $\alpha, \beta \in \mathbb{H}$ に対して $A(\alpha\beta) = A(\alpha)A(\beta)$ が成立する. ($\alpha, \beta = i, j, k$ のすべての組み合わせについて確認せよ.) このことと行列の積が結合律を満たすことと $A : \mathbb{H} \to M_4(\mathbb{R})$ が単射であることより, $\mathbb{H}$ の乗法も結合律を満たしていることがわかる.

2 と 3 は次の公式を使えば簡単である. $\alpha = a + bi + cj + dk \in \mathbb{H}$ に対して

$$\overline{\alpha} = a - bi - cj - dk, \quad |\alpha| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

と置くと $\alpha\overline{\alpha} = \overline{\alpha}\alpha = |\alpha|^2$. □

例 1.32 $R = \{\, a + bi + cj + dk \in \mathbb{H} \mid a, b, c, d \in \mathbb{Z} \,\}$ は自然に $\mathbb{H}$ の部分環をなす. R は非可換な整域である. □

2 体上のベクトル空間の理論

2.1 環上の加群と体上のベクトル空間の定義

定義 2.1 (環上の加群と体上のベクトル空間) R は環であるとする. 集合 M が R **上の加群 (module over** R**)** もしくは R **加群 (**R**-module)** であるとは加法 $+ : M \times M \to M$, 零元 $0 \in M$ と加法に関する逆元を取る操作 $- : M \to M$ と R の元の M の元への作用 $\cdot : R \times M \to M$ が定義されていて, 以下の R 加群の公理が成立していることである:

1. M は加法に関して可換群をなす. すなわち任意の $u, v, w \in M$ に対して,
   (a) $(u + v) + w = u + (v + w)$;
   (b) $0 + u = u + 0 = u$;
   (c) $(-u) + u = u + (-u) = 0$;
   (d) $u + v = v + u$.

2. スカラー倍 $\cdot : R \times M \to M$ は結合的かつ**双加法的 (bi-additive)** であり, $1 \in R$ の作用は恒等写像になる. すなわち任意の $a, b \in R$, $u, v \in M$ に対して,

   (a) $(ab)u = a(bu)$;

   (b) $a(u + v) = au + av$;

   (c) $(a + b)u = au + bu$;

   (d) $1u = u$.

特に R が体 K に等しいならば R 加群を K **上のベクトル空間 (vector space over K)** もしくは K **上の線形空間 (linear space over K)** もしくは K **ベクトル空間 (K-vector space)** もしくは K **線形空間 (K-linear space)** と呼ぶ. □

[40] (5 点) K は体であるとし, 可換環 R は体 K 上の一変数多項式環 $K[\lambda]$ であるとし, $M = K^n$ (縦ベクトルの空間) と置き, 正方行列 $A \in M_n(K)$ を任意に固定する. $f(\lambda) \in K[\lambda]$ の λ に A を代入することによって行列 $f(A) \in M_n(K)$ が自然に定義される. そのことを利用して写像 $\cdot : R \times M \to M$ を

$$f(\lambda) \cdot v := f(A)v \qquad (f(\lambda) \in R = K[\lambda],\ v \in M = K^n)$$

と定める. このとき M は自然に $R = K[\lambda]$ 上の加群をなす. □

ヒント. $M = K^n$ は K 上のベクトル空間なので始めから, $+$, 0, $-$ が定められている. スカラー倍 $R \times M \to M$ は問題のように定められている. よってそれらが R 加群の公理を満たしているかどうかを確かめればよい. ($M = K^n$ はベクトル空間なので加法に関して可換群をなすことは改めてチェックしなくてよいだろう.) □

参考 2.2 上の問題で定義した $K[\lambda]$ 上の加群 M は正方行列 $A \in M_n(K)$ の Jordan 標準形の理論を扱うときに重要になる. 正方行列 A の標準形の理論と A に対応する $K[\lambda]$ 加群 M の構造に関する理論は本質的に等しくなる. 代数学の基本は環と加群の理論である. □

[41] (連続函数全体のなすベクトル空間, 5 点) 閉区間 $[a, b]$ 上の実数値連続函数全体のなす集合を $C([a, b], \mathbb{R})$ と書くことにする. $C([a, b], \mathbb{R})$ は自然に $\mathbb{R}$ 上のベクトル空間をなす. □

ヒント. まず, $C([a, b], \mathbb{R})$ に $+$, 0, $-$ とスカラー倍 $\cdot : \mathbb{R} \times C([a, b], \mathbb{R}) \to C([a, b], \mathbb{R})$ を定義せよ. それらが well-defined であることを証明し, さらにそれらがベクトル空間の公理を満たしていることを示せ. たとえば $[a, b]$ 上の実数値連続函数 f と g の和もまた連続函数になることなどを証明しなければいけない. □

参考 2.3 K^n のようなベクトル空間を扱うのではなく, より抽象的に体上のベクトル空間を扱う利点の一つは, 上の問題のようにある種の函数全体の空間 (函数空間) をもベクトル空間として扱えるようになることである. すでに十分習熟しつつあると思われる K^n およびその部分空間でやしなった直観を函数空間にも拡大するように努力せよ. □

[42] (連続函数全体のなす可換環, 5 点) 閉区間 $[a, b]$ 上の実数値連続函数全体のなす集合を $C([a, b], \mathbb{R})$ と書くことにする. $C([a, b], \mathbb{R})$ は自然に可換環をなす. □

ヒント. $f, g \in C([a,b],\mathbb{R})$ に対して $[a,b]$ 上の函数 fg を $(fg)(x) = f(x)g(x)$ $(x \in [a,b])$ と定めると, fg が $[a,b]$ 上の連続函数になること (すなわち $fg \in C([a,b],\mathbb{R})$ となること) などを証明する必要がある. □

n 回微分可能でかつ n 階の導函数が連続になる函数を C^n **級函数 (class-C^∞ function)** もしくは C^n **函数 (C^∞-function)** と呼ぶ. 任意有限回微分可能な函数を C^∞ **級函数 (class-C^∞ function)** もしくは C^∞ **函数 (C^∞-function)** と呼ぶ.

[43] (Leibnitz rule, 5 点) f, g が開区間 (a,b) 上の実数値 C^∞ 函数であるとき, $h(x) = f(x)g(x)$ $(x \in (a,b))$ と置くと, h も開区間 (a,b) 上の実数値 C^∞ 函数であり, その n 階の導函数 $h^{(n)}$ に関して次の公式が成立している:

$$h^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x) \qquad (x \in (a,b)).$$

この公式を積の微分に関する **Leibnitz rule (ライプニッツ則)** と呼ぶ. □

ヒント. n に関する帰納法. n から $n+1$ に進むときに $(fg)' = f'g + fg'$ および二項係数 $\binom{n}{k}$ が Pascal の三角形と呼ばれる漸化式を満たしていることを使え. □

[44] (C^∞ 函数全体のなす可換環, 5 点) 開区間 (a,b) 上の実数値 C^∞ 函数全体のなす集合を $C^\infty((a,b),\mathbb{R})$ と書くと以下が成立している:

1. $C^\infty((a,b),\mathbb{R})$ は自然に $\mathbb{R}$ 上のベクトル空間をなす.
2. $C^\infty((a,b),\mathbb{R})$ は自然に可換環をなす. □

ヒント. 記号の簡単のため $A = C^\infty((a,b),\mathbb{R})$ と置く.

1. $+ : A \times A \to A$, $0_A \in A$, $- : A \to A$, $\cdot : \mathbb{R} \times A \to A$ を次のように定める: $f, g \in A$, $\alpha \in \mathbb{R}$, $x \in (a,b)$ に対して,

$$(f+g)(x) = f(x) + g(x), \quad 0_A(x) = 0, \quad (-f)(x) = -f(x), \quad (\alpha \cdot f)(x) = \alpha f(x).$$

この定義のもとで A が $\mathbb{R}$ 上のベクトル空間の公理を満たしていることを示せ.

2. さらに, $\cdot : A \times A \to A$, $1_A \in A$ を次のように定める: $f, g \in A$, $a \in (a,b)$ に対して,

$$(f \cdot g)(x) = f(x)g(x), \quad 1_A(x) = 1.$$

問題 **[43]** より, $f \cdot g$ もまた C^∞ 函数なので, 写像 $\cdot : A \times A \to A$ は well-defined である (うまく定義されている). よって以上の定義のもとで A が可換環をなすことを示せばよい. □

2.2 加群の準同型とベクトル空間の線形写像の定義

定義 2.4 (加群の準同型とベクトル空間の線形写像) R は可換環であり, M, N は R 上の加群であるとし, $f : M \to N$ は任意の写像であるとする. このとき f が R **加群の準同型**もしくは**準同型写像 (homomorphism of R-modules)** であるとは以下の条件が成立していることである:

1. $f(u+v) = f(u) + f(v) \quad (u, v \in M)$;
2. $f(\alpha u) = \alpha f(u) \quad (\alpha \in R,\, u \in M)$.

R 加群の準同型写像は R **準同型 (R-homomorphism)** と呼ばれることも多い.

環 R が体 K に等しいとき, R 加群 ($= K$ 加群) は K 上のベクトル空間と呼ばれるのであった. そのとき R 加群の準同型は K 上の**線形写像 (linear mapping)** と呼ばれる. □

[45] (準同型の合成, 5 点) L, M, N は可換環 R 上の加群であり, $f : L \to M$, $g : M \to N$ は R 準同型であるとする. そのとき合成 $g \circ f : L \to N$ も R 準同型である. □

[46] (Hom_R, 5 点) R は可換環であるとし, M, N は R 加群であるとし,

$$\mathrm{Hom}_R(M, N) = \{\, f : M \to N \mid f \text{ は } R \text{ 準同型} \,\}$$

とおく. $\mathrm{Hom}_R(M, N)$ に加法とスカラー倍の演算を次のように定めることができることを示せ: $f, g \in \mathrm{Hom}_R(M, N)$, $u \in M$, $\alpha \in R$ に対して,

$$(f+g)(u) := f(u) + g(u), \qquad (\alpha \cdot f)(u) := \alpha f(u).$$

これによって $\mathrm{Hom}_R(M, N)$ は自然に R 加群とみなせる. □

注意 2.5 上の問題で特に R が体 K に等しいとき, M, N は K 上のベクトル空間であり,

$$\mathrm{Hom}_R(M, N) = \mathrm{Hom}_K(M, N) = \{\, f : M \to N \mid f \text{ は } K \text{ 上の線形写像} \,\}$$

である. $\mathrm{Hom}_K(M, N)$ は自然に K 上のベクトル空間をなす. □

[47] (行列の定める線形写像, 5 点) K は任意の体であるとし, K の元を成分に持つ n 次元縦ベクトル全体の空間を K^n と表わし, $m \times n$ 行列全体の空間を $M_{m,n}(K)$ と書くことにする. このとき, 任意の $m \times n$ 行列 $A \in M_{m,n}(K)$ に対して, 写像 $f_A : K^n \to K^m$ を

$$f_A(u) := Au \in K^m \qquad (u \in K^n)$$

と定めると, f_A は K 上の線形写像である. □

ヒント. この問題の結果はほとんど自明 (trivial) である. 我々は f_A のことを単に A と書いてきたのであった. □

[48] (積分作用素, 15 点) 問題 [41] の結果より, 閉区間 $[a, b]$ 上の実数値連続函数全体の集合 $C([a, b], \mathbb{R})$ は自然に $\mathbb{R}$ 上のベクトル空間とみなされる[4]. $K(x, y)$ は $[a, b] \times [a, b]$ 上の任意の実数値連続函数であるとする. このとき, $\mathbb{R}$ 上の線形写像 $T : C([a, b], \mathbb{R}) \to C([a, b], \mathbb{R})$ を

$$(Tf)(x) := \int_a^b K(x, y) f(y)\, dy \qquad (f \in C([a, b], \mathbb{R}),\ x \in [a, b])$$

と定めることができることを示せ (Tf もまた $[a, b]$ 上の連続函数になることも示せ). この T は**積分作用素 (integral operator)** と呼ばれ, $K(x, y)$ はその**核函数 (kernel function)** と呼ばれる[5]. □

[4]「連続な」という形容詞は英語では "continuous" である. 記号 $C([a, b], \mathbb{R})$ の C は「連続」という意味である.

[5]線形写像 $f : U \to V$ の核 $\mathrm{Ker}\, f = \{\, x \in U \mid f(x) = 0 \,\}$ とは無関係であることに注意せよ.

ヒント. 閉区間 $[a,b]$ 上の積分について以下が成立することを自由に用いてよい[6]:

1. (連続函数の積分可能性)　任意の $f \in C([a,b],\mathbb{R})$ は $[a,b]$ 上で積分可能である.
2. (積分の線形性)　任意の $f,g \in C([a,b],\mathbb{R})$ と $\alpha \in \mathbb{R}$ に対して,
$$\int_a^b (f(x)+g(x))\,dx = \int_a^b f(x)\,dx + \int_a^b g(x)\,dx, \qquad \int_a^b \alpha f(x)\,dx = \alpha \int_a^b f(x)\,dx.$$
3. (積分の単調性)　任意の $f,g \in C([a,b],\mathbb{R})$ に対して,
$$f(x) \leqq g(x)\ (x \in [a,b]) \implies \int_a^b f(x)\,dx \leqq \int_a^b g(x)\,dx.$$
4. (積分の絶対値の評価)　$f \in C([a,b],\mathbb{R})$ に対して, その絶対値 $|f|$ の $[a,b]$ での最大値を M と書くと[7],
$$\left|\int_a^b f(x)\,dx\right| \leqq \int_a^b |f(x)|\,dx \leqq \int_a^b M\,dx = M(b-a).$$

さらに, $K(x,y)$ の $[a,b]\times[a,b]$ 上での一様連続性を用いてよい[8].

$f \in C([a,b],\mathbb{R})$ を任意に取り, $|f|$ の $[a,b]$ での最大値を M と書くと, 任意の $x_0, x \in [a,b]$ に対して,

$$\begin{aligned}|(Tf)(x)-(Tf)(x_0)| &= \left|\int_a^b (K(x,y)-K(x_0,y))f(y)\,dy\right| \\ &\leqq \int_a^b |K(x,y)-K(x_0,y)||f(y)|\,dy \\ &\leqq M\int_a^b |K(x,y)-K(x_0,y)|\,dy.\end{aligned}$$

連続函数 $K(x,y)$ の $[a,b]\times[a,b]$ 上での一様連続性より, 任意の $\varepsilon > 0$ に対して, ある $\delta > 0$ が存在して, $|x-x_0| \leqq \delta$ ならば $|K(x,y)-K(x_0,y)| \leqq \varepsilon/(M(b-a))$ ($y \in [a,b]$ は任意でよい) となる. よって $|x-x_0| \leqq \delta$ ならば

$$|(Tf)(x)-(Tf)(x_0)| \leqq M\int_a^b \frac{\varepsilon}{M(b-a)}\,dy = \varepsilon.$$

これで Tf が $[a,b]$ 上の連続函数であることが示された. □

注意 2.6 (積分作用素と行列の定める線形写像の類似) 積分作用素 T の定義は行列の定める線形写像の定義と似ている. 実際, $A = [a_{ij}] \in M_{m,n}(\mathbb{R})$, $v = [v_i] \in \mathbb{R}^n$ に対して, $Av \in \mathbb{R}^m$ の第 i 成分を $(Av)_i$ と書くと,

$$(Av)_i = \sum_{j=1}^n a_{ij}v_j.$$

[6]以下の条件は積分の定義の仕方 (Riemann, Lebesgue) によらずに成立している. 以下の条件は積分が x 軸と函数のグラフで囲まれた部分の面積 (x 軸より下の部分の面積は -1 倍する) であるという直観より, 当然成立すべき事柄ばかりである.

[7]一般に $\mathbb{R}^n$ の有界閉集合上の実数値連続函数は最大値と最小値を持つ.

[8]一般に $\mathbb{R}^n$ の有界閉集合上の実数値連続函数は一様連続である.

一方, 積分作用素 T は次のように定義されたのであった:

$$(Tf)(x) = \int_a^b K(x,y)f(y)\,dy.$$

以上の 2 つの式を比べれば, 以下のような類似関係があることがわかる:

$$\text{積分作用素 } T \leftrightarrow \text{行列 } A, \qquad \text{函数 } f \leftrightarrow \text{縦ベクトル } v,$$
$$\text{核函数 } K(x,y) \leftrightarrow \text{行列の成分 } a_{ij}, \qquad \text{積分 } \int_a^b dy \leftrightarrow \text{有限和 } \sum_{j=1}^{n}. \quad \square$$

[49] (微分作用素, 10 点) 問題 **[44]** の結果より, 開区間 (a,b) 上の実数値 C^∞ 函数全体のなす集合 $C^\infty((a,b),\mathbb{R})$ は自然に $\mathbb{R}$ 上のベクトル空間でかつ可換環とみなされる. 記号の簡単のため $A = C^\infty((a,b),\mathbb{R})$ と置く. 以下が成立することを示せ:

1. $f \in A$ に対して, 写像 $\hat{f} : A \to A$ を
$$\hat{f}(g) := f \cdot g \qquad (g \in A)$$
と定めると, $\hat{f}$ は $\mathbb{R}$ 上の線形写像である.

2. 写像 $\partial : A \to A$ を
$$\partial(f) := f' \qquad (f \in A,\ f' \text{ は } f \text{ の導函数})$$
と定めると, ∂ は $\mathbb{R}$ 上の線形写像である.

3. $a_0, a_1, \ldots, a_n \in A$ に対して写像 $P : A \to A$ を
$$P(f) := a_n f^{(n)} + a_{n-1} f^{(n-1)} + \cdots + a_1 f' + a_0 f \quad (f \in A)$$
と定める. ここで $f^{(k)}$ は f の k 階の導函数である. このとき P は $\mathbb{R}$ 上の線形写像である.

4. 任意の $f \in A$ に対して $[\partial, \hat{f}] = \widehat{f'}$. ($[A,B] = AB - BA$ である.)

P は**線形常微分作用素 (linear ordinary differential operator)** と呼ばれ,

$$P = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_1\partial + a_0$$

と書かれる. $\square$

ヒント. 4 は次のようにして証明される. 任意の $g \in A$ を取ると,

$$\partial(\hat{f}(g)) = \partial(fg) = (fg)' = f'g + fg' = \widehat{f'}(g) + \hat{f}(\partial(g))$$

なので $\partial(\hat{f}(g)) - \hat{f}(\partial(g)) = \widehat{f'}(g)$. これで $[\partial, \hat{f}] = \partial\widehat{f} - \widehat{f}\partial = \widehat{f'}$ が証明された. $\square$

参考 2.7 積分作用素と微分作用素は線形写像を作るための材料として行列と同じくらい基本的である. 数ベクトルと行列の理論をベクトル空間と線形写像の理論に一般化しておくことのメリットの一つはある種の函数全体のなす空間のあいだの微分作用素や積分作用素も扱えるようになることである. $\square$

[50] (多項式係数の微分作用素, 10 点) 複素係数の一変数多項式環 $\mathbb{C}[x]$ は自然に $\mathbb{C}$ 上のベクトル空間をなす. 以下が成立することを示せ:

1. $f \in \mathbb{C}[x]$ に対して, 写像 $\hat{f} : \mathbb{C}[x] \to \mathbb{C}[x]$ を
$$\hat{f}(g) := f \cdot g \qquad (g \in \mathbb{C}[x])$$
と定めると, $\hat{f}$ は $\mathbb{C}$ 上の線形写像である.
2. 写像 $\partial : \mathbb{C}[x] \to \mathbb{C}[x]$ を
$$\partial(f) := f' \qquad (f \in \mathbb{C}[x],\ f' \text{ は } f \text{ の導函数})$$
と定めると, ∂ は $\mathbb{C}$ 上の線形写像である.
3. $a_0, a_1, \ldots, a_n \in \mathbb{C}[x]$ に対して写像 $P : \mathbb{C}[x] \to \mathbb{C}[x]$ を
$$P(f) := a_n f^{(n)} + a_{n-1} f^{(n-1)} + \cdots + a_1 f' + a_0 f \quad (f \in A)$$
と定める. ここで $f^{(k)}$ は f の k 階の導函数である. このとき P は $\mathbb{C}$ 上の線形写像である.
4. $[\partial, \widehat{x^i}] = i\widehat{x^{i-1}}$. 特に $[\partial, \hat{x}] = 1$. ($[A, B] = AB - BA$ である.)

P は**多項式係数の線形常微分作用素 (linear ordinary differential operator with polynomial coefficients)** と呼ばれ,

$$P = a_n \partial^n + a_{n-1} \partial^{n-1} + \cdots + a_1 \partial + a_0$$

と書かれる. □

2.3 一般のベクトル空間における部分空間, 一次独立性, 基底

体 K 上の変数 x に関する 1 変数多項式環を $K[x]$ と書くことにする. $K[x]$ は自然に K 上の線形空間とみなされる.

[51] (5 点) $V := \{ f \in \mathbb{C}[x] \mid f(-a) = \overline{f(a)}\ (a \in \mathbb{R}) \}$ ($\overline{\ }$ は複素共役) と置く. $\mathbb{C}[x]$ は自然に $\mathbb{C}$ 上および $\mathbb{R}$ 上のベクトル空間とみなされる. V は $\mathbb{C}[x]$ の $\mathbb{C}$ 上の部分空間ではないが, $\mathbb{R}$ 上の部分空間になることを示せ. □

[52] (5 点) $\mathbb{F}_2 = \{0, 1\}$ は二元体であるとし, $V := \{ f \in \mathbb{F}_2[x] \mid f(-x)^2 = f(x)^2 \}$ と置く. このとき $V = \mathbb{F}_2[x]$ であることを示せ. □

[53] (5 点) $\mathbb{R}$ 上の複素数値 C^∞ 函数全体の集合 $C^\infty(\mathbb{R})$ は自然に $\mathbb{C}$ 上のベクトル空間とみなされる. 任意に $a, b \in C^\infty(\mathbb{R})$ を取り, $C^\infty(\mathbb{R})$ の部分集合 V を

$$V := \{ v \in C^\infty(\mathbb{R}) \mid v'' + av' + bv = 0 \}$$

と定める. ここで $v'' + av' + bv = 0$ は $v''(x) + a(x)v'(x) + b(x)v(x) = 0\ (x \in \mathbb{R})$ が成立するという意味である. このとき V は $C^\infty(\mathbb{R})$ の $\mathbb{C}$ 上の部分空間である. □

[54] (二階の線形常微分方程式の解空間, 5 点) $\mathbb{R}$ 上の複素数値 C^∞ 函数全体の集合 $C^\infty(\mathbb{R})$ は自然に $\mathbb{C}$ 上のベクトル空間とみなされる. 任意に $a, b \in C^\infty(\mathbb{R})$ を取り, $V \subset C^\infty(\mathbb{R})$ を

$$V := \{\, v \in C^\infty(\mathbb{R}) \mid v'' + av' + bv = 0 \,\}$$

と定める. ここで「$v'' + av' + bv = 0$」は 「任意の $x \in \mathbb{R}$ に対して $v''(x) + a(x)v'(x) + b(x)v(x) = 0$ が成立する」という意味である. このとき V は $C^\infty(\mathbb{R})$ の部分空間である. □

[55] (10 点) K は任意の体であるとし, $a_{ij} \in K$ $(i > j \geq 0)$ を任意に取る. $f_i \in K[x]$ $(i = 0, 1, 2, \ldots)$ を次のように定義する:

$$f_i(x) = a_{i0} + a_{i1}x + \cdots + a_{i,i-1}x^{i-1} + x^i,$$

($f_0(x) = 1$ であることに注意.) このとき $f_0, f_1, f_2, \ldots$ が $K[x]$ の基底になることを示せ. □

ヒント. $f_0, f_1, f_2, \ldots$ の一次独立性および任意の $f \in K[x]$ が $f_0, f_1, f_2, \ldots$ の K 係数有限一次結合で表わされることを示せばよい. (もしくは任意の $f \in K[x]$ が $f_0, f_1, f_2, \ldots$ の K 係数有限一次結合で一意に表わされることを示せばよい.) □

[56] (10 点) A は $\mathbb{R}$ の任意の無限部分集合であるとする. A 上の実数値函数全体の集合は自然に実ベクトル空間をなす (このことは認めて使ってよい). 0 以上の整数 i に対して A 上の実数値函数 f_i を

$$f_i(x) = x^i \qquad (x \in A)$$

と定める. このとき $f_0, f_1, f_2, \ldots$ が一次独立であることを示せ. □

ヒント. A は無限集合なので任意の $n = 1, 2, 3, \ldots$ に対して互いに異なる元 $a_1, \ldots, a_n \in A$ を取れる. このとき Vandermonde 行列式の公式より, $n \times n$ 行列

$$A_n = \begin{bmatrix} a_1^0 & a_2^0 & \cdots & a_n^0 \\ a_1^1 & a_2^1 & \cdots & a_n^0 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix}$$

は可逆になる. このことを使って $f_0, f_1, \ldots, f_{n-1}$ が一次独立であることを示せ. □

[57] (15 点) p は素数であるとし, $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ は p 元体であるとする. $\mathbb{F}_p$ 上の $\mathbb{F}_p$ 値函数全体の集合は $\mathbb{F}_p$ 上のベクトル空間をなす. $\mathbb{F}_p$ 上の $\mathbb{F}_p$ 値函数 $f_0, f_1, f_2, \ldots$ を次のように定める:

$$f_i(x) = x^i \qquad (x \in \mathbb{F}_p).$$

このとき $f_0, f_1, \ldots, f_{p-1}$ は一次独立であるが, $f_1, f_2, \ldots, f_p$ は一次従属であることを示せ. □

ヒント. $f_0, f_1, \ldots, f_{p-1}$ の一次独立性の証明は問題 **[56]** と同じ. 実は任意の $a \in \mathbb{F}_p$ に対して $a^p = a$ となる (この結果の証明は代数学の教科書を参照せよ). 感じがつかめなければ $p = 2, 3, 5$ の場合にどうなっているかをチェックしてみよ. □

注意 2.8 上の問題の結果を見て変数 x に関する $\mathbb{F}_p$ 上の多項式環 $\mathbb{F}_p[x]$ においても $x^p = x$ であると誤解してはいけない. $\mathbb{F}_p$ 係数の多項式とそれを $\mathbb{F}_p$ 上の函数とみなしたものは厳密に区別されなければいけない. K が無限体であれば $K[x]$ の元と K 上の多項式函数を同一視できるのでそのような区別は必要ない. □

2.4 Zorn の補題と基底の存在

「任意のベクトル空間に基底が存在する」もしくはより強い「任意のベクトル空間の一次独立な部分集合を基底に拡張できる」という定理は **Zorn の補題 (ツォルンの補題)** を用いて証明される.

しかし, Zorn の補題についてまだ十分に習っていないようなので, この節では選択公理から Zorn の補題を導く方法について詳しく説明する.

2.4.1 選択公理

選択公理 (axiom of choice) とは次の命題のことである:

(AC) 任意の $x \in X$ に対してある $y \in Y$ で条件 $P(x,y)$ を満たすものが存在するならば, ある写像 $f : X \to Y$ が存在して任意の $x \in X$ に対して条件 $P(x, f(x))$ が成立する.

このような写像 f は**選択函数 (choice function)** と呼ばれる. 選択公理を論理式で書くと次のようになる:

$$\forall x \in X\, \exists y \in Y\, P(x,y) \implies \exists f : X \to Y\, \forall x \in X\, P(x, f(x)).$$

形式的に選択公理は $\forall$ と $\exists$ の順序を引っくり返す形をしている.

選択公理の直観的な説明. もしも任意の $x \in X$ に対して条件 $P(x,y)$ を満たす $y \in Y$ が存在するならば各 $x \in X$ ごとにそのような $y \in Y$ を一つずつ選んで $f(x) = y$ と定めることによって選択函数 $f : X \to Y$ を作ることができる. そのとき f の作り方より任意の $x \in X$ に対して条件 $P(x, f(x))$ が成立している.

非常に疑い深い人の考え方. もしも X が無限集合ならば全ての $x \in X$ に対して条件 $P(x,y)$ を満たす $y \in Y$ を一つずつ選び出すことができないかもしれない.

このように疑う自由はあるが, 選択公理は自然であり (実際選択公理を意識せずに使ってしまう人が大部分だろう), 非常に便利なので数学の公理として仮定されることになる.

選択公理は上に述べた形とは異なる形で述べられることも多い. たとえば

(AC') $\{Y_x\}_{x \in X}$ が空でない集合の集合族ならばある写像 $f : X \to \bigcup_{x \in X} Y_x$ が存在して任意の $x \in X$ に対して $f(x) \in Y_x$ が成立する.

直観的な説明. 各 $x \in X$ ごとに空でない集合 Y_x から一つずつ元を選び, その元を $f(x)$ と定めることによって写像 $f : X \to \bigcup_{x \in X} Y_x$ を作ることができる. このとき f の作り方より任意の $x \in X$ に対して $f(x) \in Y_x$ が成立している.

[58] (5 点) (AC) と (AC') が同値であることを証明せよ. □

ヒント. (AC) $\implies$ (AC'). (AC) を仮定し, $\{Y_x\}_{x \in X}$ は空でない集合で構成された集合族であると仮定する. $Y = \bigcup_{x \in X} Y_x$ と置き, $x \in X$, $y \in Y$ に対して条件 $P(x,y)$ が成立するとは $y \in Y_x$ が成立することであると定める.

(AC') $\implies$ (AC). (AC') を仮定し, 任意の $x \in X$ に対してある $y \in Y$ で条件 $P(x,y)$ を満たすものが存在すると仮定する. $x \in X$ に対して $Y_x = \{\, y \in Y \mid P(x,y) \,\}$ と置く. □

2.4.2 順序集合に関する言葉の準備

定義 2.9 (順序集合) 集合と二項関係の組 $(X, \leqq)$ が**順序集合 (ordered set)** であるとは以下の条件が成立していることである:

- 任意の $x \in X$ に対して $x \leqq x$.
- 任意の $x, y, z \in X$ に対して $x \leqq y$ かつ $y \leqq z$ ならば $x \leqq z$.
- 任意の $x, y \in X$ に対して $x \leqq y$ かつ $y \leqq x$ ならば $x = y$.

このとき $\leqq$ は**順序 (order)** と呼ばれる. さらに

- 任意の $x, y \in X$ に対して $x \leqq y$ または $y \leqq x$ (x と y は比較可能)

が成立しているとき $(X, \leqq)$ は**全順序集合 (totally ordered set)** と呼ばれ, $\leqq$ は**全順序 (total order)** であると言う. $x \leqq y$ を $y \geqq x$ と書くこともある. また $x \leqq y$ かつ $x \neq y$ のとき $x < y$ と書くことにする. □

例 2.10 (順序集合の例) 順序集合には以下のような例がある:

1. 実数全体の集合 $\mathbb{R}$ は通常の大小関係に関する全順序集合である.
2. 正の整数全体の集合を $\mathbb{Z}_{>0} = \{\, n \in \mathbb{Z} \mid n > 0 \,\}$ と書く. 整数 a が整数 b の約数であるとき $a \mid b$ と書く. このとき $(\mathbb{Z}_{>0}, \mid)$ は順序集合であるが, 全順序集合ではない.
3. 集合の集合は包含関係に関する順序集合とみなされる.
4. 任意の順序集合の部分集合は自然に順序集合とみなされる. □

定義 2.11 (上界, 最小元, 上限, 極大元) $(X, \leqq)$ は順序集合であるとし, $A \subset X$ であるとする.

- $x \in X$ が A の**上界 (upper bound)** であるとは, 任意の $a \in A$ に対して $a \leqq x$ が成立することである. A の上界は存在するとは限らないし, 存在しても唯一とは限らない.
- $a_0 \in A$ が A の**最小元 (minimum)** であるとは, 任意の $a \in A$ に対して $a_0 \leqq a$ が成立することである. A の最小元は存在すれば唯一であり, そのとき $\min A$ と表わされる.
- $s \in X$ が A の**上限 (supremum)** であるとは s が A の**最小上界 (minimum upper bound)** すなわち A の上界全体の集合の最小元であることである. A の上限は存在すれば唯一であり, そのとき $\sup A$ と表わされる.
- $m \in A$ が X の**極大元 (maximal element)** であるとは任意の $x \in A$ に対して $x \geqq m$ ならば $x = m$ となることである. (すなわち $x \in A$ で $x > m$ を満たすものが存在しないことである.) A の極大元は存在するとは限らないし, 存在しても唯一とは限らない.

順序関係を逆転させることによって, **下界 (lower bound)**, **最大元 (maximum)**, $\max A$, **下限 (infimum)**, $\inf A$, **極小元 (mimimal element)** が同様に定義される. □

定義 2.12 (帰納的順序集合) 順序集合 $(X, \leqq)$ が**帰納的 (inductive)** であるとは X の任意の全順序部分集合が上界を持つことである. □

例 2.13 (帰納的順序集合およびそうでない順序集合の例)

- 最大元を持つ順序集合は帰納的順序集合である.
- 有限順序集合は帰納的順序集合である.
- 帰納的順序集合 $(X, \leqq)$ と $x_0 \in X$ に対して, $X_{\geqq x_0} = \{\, x \in X \mid x \geqq x_0 \,\}$ も帰納的順序集合になる.
- $(\mathbb{Z}_{>0}, |\,)$ は順序集合だが, 帰納的ではない.
- $(\mathbb{R}, \leqq)$ は全順序集合だが, 帰納的ではない.
- K は任意の体であるとし, V は K 上の任意のベクトル空間であるとする. V の一次独立な部分集合全体の集合 $\mathcal{L}$ は包含関係に関して帰納的順序集合である. □

[59] (5 点) 順序集合 $(\mathbb{Z}_{>0}, |\,)$, $(\mathbb{R}, \leqq)$ が帰納的でないことを示せ. □

[60] (5 点) 帰納的順序集合 $(X, \leqq)$ と $x_0 \in X$ に対して, $X_{\geqq x_0} = \{\, x \in X \mid x \geqq x_0 \,\}$ も帰納的順序集合になることを示せ. □

2.4.3 Zorn の補題

Zorn の補題 (Zorn's lemma) とは次の命題のことである:

(ZL) 空でない任意の帰納的順序集合 $(X, \leqq)$ とその任意の元 $x_0 \in X$ に対して X の極大元 m で $m \geqq x_0$ を満たすもの (x_0 以上の極大元 m) が存在する.

次のように見かけ上弱い形で Zorn の補題が述べられることもある:

(ZL') 空でない任意の帰納的順序集合 $(X, \leqq)$ は極大元を持つ.

これらは同値である.

[61] (5 点) (ZL) と (ZL') の同値性を証明せよ. □

ヒント. 問題 [60] の結果を使えば簡単である. □

さて目標は選択公理 (AC) から Zorn の補題 (ZL) を導くことである.
まず証明の概略を説明しよう.

証明の概略. 選択公理を仮定する. $(X, \leqq)$ は帰納的順序集合であり, $x_0 \in X$ であると仮定する. X には x_0 以上の極大元が存在しないと仮定して矛盾を導けばよい.

x_0 を含む X の全順序部分集合全体の集合を $\mathcal{C}$ と書くことにする. (全順序部分集合は chain と呼ばれることがあるのでその頭文字を取って $\mathcal{C}$ と書くことにした.)

X が帰納的であるという仮定より, 任意の $C \in \mathcal{C}$ に対して C の上界 $y \in X$ が存在する. このとき特に $y \geqq x_0$ である.

X には x_0 以上の極大元が存在しないという仮定より, y は X の極大元ではない. よってある $z \in X$ で $z > y$ を満たすものが存在する.

選択公理を仮定したので, 各 $C \in \mathcal{C}$ に対して上のような $z \in X$ を対応させる選択函数 $f : \mathcal{C} \to X$ が存在して, 任意の $C \in \mathcal{C}$, $x \in C$ に対して $f(C) > x$ が成立する (特に $f(C) \notin C$ である).

$C_0 = \{x_0\} \in \mathcal{C}$, $C_1 = C_0 \cup \{f(C_0)\} \in \mathcal{C}$, $C_2 = C_1 \cup \{f(C_1)\} \in \mathcal{C}$, ... が成立する. この構成を **"限りなく最大限続けることによって"** $C_{\max} \in \mathcal{C}$ を構成する. もしも $f(C_{\max}) \notin C_{\max}$ ならばさらに $C_{\max+1} = C_{\max} \cup \{f(C_{\max})\}$ によって次のステップに進むことができるので, **"限りなく最大限続けることによって"** の「最大限」という言葉に矛盾してしまう. よって $f(C_{\max}) \in C_{\max}$ でなければいけない. **(この段落だけは曖昧過ぎるので数学的に不完全である.)**

しかし $C_{\max} \in \mathcal{C}$ より $f(C_{\max}) \notin C_{\max}$ でなければいけない.

これで矛盾が導かれた. □

以上の証明の概略は一つの段落を除けば完全である. 残された問題は「$C_0, C_1, C_2, \ldots$ の構成を **"限りなく最大限続けることによって"** $C_{\max}$ を構成する」の部分をどのように数学的に正当化するかである.

注意 2.14 目標である $C_{\max}$ の構成のためには, 自然数 n に対する C_n を構成するだけでは不十分である. なぜならば自然数 n に対して $f(C_n) \notin C_n$ だからである. よってこの証明を完結させるためには数学的帰納法だけでは不十分である. すべての自然数 n に対して C_n が構成された後は $C_\omega = \bigcup_{n=0}^{\infty} C_n$ によって次のステップに進むことになる. しかし, 以下ではこういう方針を取らずに集合の演算を巧妙に使って $C_{\max}$ を構成することにする. □

上の証明の概略の曖昧な部分の数学的正当化.

Step 1. $\mathcal{T}_{\min} \subset \mathcal{C}$ の構成

$\mathcal{T} \subset \mathcal{C}$ が塔 (tower) であるとは次の 3 つの条件を満たすことであると定める:

(a) $\{x_0\} \in \mathcal{T}$.

(b) $T \in \mathcal{T}$ ならば $T \cup \{f(T)\} \in \mathcal{T}$.

(c) $\mathcal{S}$ が $\mathcal{T}$ の包含関係に関する全順序部分集合になっているならば $\bigcup_{S \in \mathcal{S}} S \in \mathcal{T}$.

たとえば $\mathcal{C}$ 自身は塔である (容易なので自分で証明してみよ).

塔全体の共通部分を $\mathcal{T}_{\min} = \bigcap_{\mathcal{T} \text{ は塔}} \mathcal{T}$ と書くことにする. (少なくとも一つ塔が存在するので $\mathcal{T}_{\min}$ は well-defined である.)

(解説: この $\mathcal{T}_{\min}$ は上の証明の概略中で **"限りなく最大限続けることによって"** 構成された $C_0, C_1, C_2, \ldots$ 全体の集合である. 証明の概略中では構成の仕方は非常に曖昧だったが上の構成法は論理的に明確である. $C_{\max}$ は $\mathcal{T}_{\min}$ の包含関係に関する最大元として構成される. アイデアが必要な本質的なステップはこの Step 1 だけであり, $\mathcal{T}_{\min}$ の明確な構成の仕方さえわかっていれば残りの部分は機械的な作業 (routine) に過ぎない. 機械的に論理的な作業をこなす能力が身に付けば直観的で曖昧な議論をどのように論理的に明確にするかに意識を集中できるようになる. 直観的な議論を自由に進めながら, 曖昧な細部を徐々に論理的に明確にして行くのは非常に楽しい.)

Step 2. $\mathcal{T}_{\min}$ が最小の塔になることの証明 (容易)

(a) すべての塔は $\{x_0\}$ を含むので $\{x_0\} \in \mathcal{T}_{\min}$ である.

(b) $T \in \mathcal{T}_{\min}$ ならば任意の塔 $\mathcal{T}$ に対して $T \in \mathcal{T}$ であるから $T \cup \{f(T)\} \in \mathcal{T}$ である. よって $T \in \mathcal{T}_{\min}$ である.

(c) $\mathcal{S}$ が $\mathcal{T}_{\min}$ の全順序部分集合ならば $\mathcal{S}$ は任意の塔 $\mathcal{T}$ の全順序部分集合でもあるので $\bigcup_{S\in\mathcal{S}} S \in \mathcal{T}$ である. よって $\bigcup_{S\in\mathcal{S}} S \in \mathcal{T}_{\min}$ である.

これで $\mathcal{T}_{\min}$ が塔であることがわかった. $\mathcal{T}_{\min}$ は任意の塔に含まれるので最小の塔である.

Step 3. $\mathcal{T}_{\min}$ が包含関係に関する全順序集合であることの証明 (少し面倒)

$\mathcal{T}_{\min}$ の部分集合 $\mathcal{T}_0$ を次のように定める:

$$\mathcal{T}_0 = \{\, S \in \mathcal{T}_{\min} \mid \text{任意の } T \in \mathcal{T}_{\min} \text{ に対して } S \subset T \text{ または } T \subset S \,\}.$$

($\mathcal{T}_0$ は $\mathcal{T}_{\min}$ の任意の元と比較可能な $\mathcal{T}_{\min}$ の元全体のなす集合である.)

$\mathcal{T}_0$ は包含関係に関して全順序集合になる. 実際任意に $S, T \in \mathcal{T}_0$ 取ると $T \in \mathcal{T}_{\min}$ なので $S \subset T$ または $T \subset S$ が成立する.

よって $\mathcal{T}_0 = \mathcal{T}_{\min}$ を証明すればよい. $\mathcal{T}_{\min}$ が最小の塔であることより, そのためには $\mathcal{T}_0$ も塔であることを示せば十分である.

(a) 任意の $T \in \mathcal{T}_{\min} \subset \mathcal{C}$ に対して $\{x_0\} \subset T$ であるから $\{x_0\} \in \mathcal{T}_0$ である.

(b) $\mathcal{T}_0$ が (b) を満たすことの証明は長くなるので次のステップで証明する.

(c) $\mathcal{S}$ は $\mathcal{T}_0$ の包含関係に関する全順序部分集合であると仮定する. $\mathcal{S}$ は $\mathcal{T}_{\min}$ の包含関係に関する全順序部分集合でもあるので $\bigcup_{S\in\mathcal{S}} S \in \mathcal{T}_{\min}$ である. 任意に $T \in \mathcal{T}_{\min}$ を取る. 任意の $S \in \mathcal{S}$ に対して $S \subset T$ または $T \subset S$ である. もしも $T \subset S$ を満たす $S \in \mathcal{S}$ が存在するならば $T \subset \bigcup_{S\in\mathcal{S}} S$ となる. もしもそのような S が存在しなければ任意の $S \in \mathcal{S}$ に対して $S \subset T$ となるので $\bigcup_{S\in\mathcal{S}} S \subset T$ となる. したがって $\bigcup_{S\in\mathcal{S}} S \subset T$ または $T \subset \bigcup_{S\in\mathcal{S}} S$ が成立する. よって $\bigcup_{S\in\mathcal{S}} S \in \mathcal{T}_0$ である.

Step 4. $\mathcal{T}_0$ が (b) を満たすことの証明 (再度同じ方法を使う)

$C \in \mathcal{T}_0$ を任意に取る. $C \in \mathcal{T}_{\min}$ でもあるので $C \cup \{f(C)\} \in \mathcal{T}_{\min}$ である. $\mathcal{T}_{\min}$ の部分集合 $\mathcal{T}_C$ を次のように定める:

$$\mathcal{T}_C = \{\, T \in \mathcal{T}_{\min} \mid T \subset C \text{ または } C \cup \{f(C)\} \subset T \,\}.$$

$\mathcal{T}_0$ が (b) を満たすことを示すためには $\mathcal{T}_C = \mathcal{T}_{\min}$ であることを示せば十分である. $\mathcal{T}_{\min}$ が最小の塔であることから, そのためには $\mathcal{T}_C$ が塔であることを示せば十分である.

(a) $\{x_0\} \subset C$ なので $\{x_0\} \in \mathcal{T}_C$ である.

(b) $T \in \mathcal{T}_C$ を任意に取る. このとき $T \subset C$ または $C \cup \{f(C)\} \subset T$ である. $C \cup \{f(C)\} \subset T$ のとき $C \cup \{f(C)\} \subset T \cup \{f(T)\}$ であるから $T \cup \{f(T)\} \in \mathcal{T}_C$ である. そこで $T \subset C$ と仮定する. $C \in \mathcal{T}_0$ より $T \cup \{f(T)\} \subset C$ または $C \subset T \cup \{f(T)\}$ である. $T \cup \{f(T)\} \subset C$ のとき $T \in \mathcal{T}_C$ である. そこで $C \subset T \cup \{f(T)\}$ と仮定する. $T \subset C$ より $C = T$ または $C = T \cup \{f(T)\}$ である. $C = T$ のとき $C \cup \{f(C)\} = T \cup \{f(T)\}$ (特に $C \cup \{f(C)\} \subset T \cup \{f(T)\}$) なので $T \cup \{f(T)\} \in \mathcal{T}_C$ である. $C = T \cup \{f(T)\}$ のとき特に $T \cup \{f(T)\} \subset C$ なので $T \cup \{f(T)\} \in \mathcal{T}_C$ である. これで $T \in \mathcal{T}_C$ ならば常に $T \cup \{f(T)\} \in \mathcal{T}_C$ となることがわかった.

(c) $\mathcal{S}$ は $\mathcal{T}_C$ の包含関係に関する全順序部分集合であるとする. $\mathcal{S}$ は $\mathcal{T}_{\min}$ の包含関係に関する全部分集合でもあるので $\bigcup_{S\in\mathcal{S}} S \in \mathcal{T}_{\min}$ である. 任意に $S \in \mathcal{S}$ を取る. $S \subset C$ または $C \cup \{f(C)\} \subset S$ である. もしもある $S \in \mathcal{S}$ で $C \cup \{f(C)\} \subset S$ を満たすものが存在するならば $C \cup \{f(C)\} \subset \bigcup_{S\in\mathcal{S}} S$ である. もしもそのような S が存在しなければ任意の $S \in \mathcal{S}$ に対して $S \subset C$ となるので $\bigcup_{S\in\mathcal{S}} S \subset C$ となる. したがって $\bigcup_{S\in\mathcal{S}} S \in \mathcal{T}_C$ である.

Step 5. $\mathcal{T}_{\min}$ の包含関係に関する最大元 $C_{\max}$ の構成 (容易)

$C_{\max} = \bigcup_{C\in\mathcal{T}_{\min}} C$ と置く. 任意の $C \in \mathcal{T}_{\min}$ に対して $C \subset C_{\max}$ である. $\mathcal{T}_{\min}$ は塔でかつ包含関係に関する全順序集合なので $\mathcal{T}_{\min}$ に関する条件 (c) より $C_{\max} \in \mathcal{T}_{\min}$ である. これで $C_{\max}$ は $\mathcal{T}_{\min}$ の包含関係に関する最大元であることが示された.

Step 6. $f(C_{\max}) \in C_{\max}$ の証明 (容易)

$C_{\max}$ に関する条件 (b) より $C_{\max} \cup \{f(C_{\max})\} \in \mathcal{T}_{\min}$ である. しかし $C_{\max}$ は包含関係に関する $\mathcal{T}_{\min}$ の最大元なので $C_{\max} \cup \{f(C_{\max})\} = C_{\max}$ でなければいけない. よって $f(C_{\max}) \in C_{\max}$ である.

Step 7. Zorn の補題の証明の完了 (容易)

$f(C_{\max}) \in C_{\max}$ であることが証明されてしまったが, $C_{\max} \in \mathcal{C}$ なので f の定義より $f(C_{\max}) \notin C_{\max}$ である. これは矛盾である. したがって帰納的順序集合 X とその元 x_0 に対して x_0 以上の X の極大元が存在しなければいけない. □

[62] (10 点) Zorn の補題から選択公理を導け. □

ヒント. $\mathcal{F} = \{\, (A, f) \mid A \subset X,\ f : A \to Y,\ \text{任意の } x \in A \text{ に対して } P(x, f(x)) \text{ が成立する} \,\}$ と置く. $(A, f), (B, g) \in \mathcal{F}$ に対して $(A, f) \leqq (B, g)$ であるとは $A \subset B$ かつ g が f の拡張になっていることであると定める. このとき $\mathcal{F}$ は帰納的順序集合である. □

2.4.4 任意のベクトル空間の基底の存在

[63] (10 点, 任意のベクトル空間の基底の存在定理) K は任意の体であるとし, V は K 上の任意のベクトル空間であるとする. V の一次独立な部分集合全体の集合 $\mathcal{L}$ は包含関係に関する帰納的順序集合であることを示せ. 次節で解説する Zorn の補題を用いて, V の一次独立な任意の部分集合を基底に拡張できることを証明せよ. □

ヒント. $\mathcal{A} \subset \mathcal{L}$ は包含関係に関して $\mathcal{L}$ の全順序部分集合であるとする. $B = \bigcup_{A\in\mathcal{A}} A$ と置く. そのとき任意の $A \in \mathcal{A}$ に対して $A \subset B$ である. B も一次独立な V の部分集合になること (すなわち $B \in \mathcal{L}$) を示せ. □

2.4.5 Zorn の補題の他の応用

[64] (10 点) Zorn の補題を用いて次を示せ. K は任意の体であり, U, V は K 上の任意のベクトル空間であるとし, W は V の任意の部分空間であるとする. このとき任意の線形写像 $f : W \to U$ に対してある線形写像 $g : V \to U$ で g の W 上への制限が f に等しいものが存在する. □

ヒント. V の部分空間 A と線形写像 $g : A \to U$ の組 (A, g) 全体の集合に「写像の拡張になっているか否か」で順序関係を入れて Zorn の補題を適用せよ. □

[**65**] **(10 点)** Zorn の補題を用いて次を示せ. K は任意の体であり, V は K 上の任意のベクトル空間であるとし, W は V の任意の部分空間であるとする. このとき V のある部分空間 W' で $V = W \oplus W'$ (すなわち $V = W + W'$ かつ $W \cap W' = \{0\}$) を満たすものが存在する. □

ヒント. V の部分空間 W' で $W \cap W' = \{0\}$ を満たすもの全体の集合に包含関係で順序を入れ, Zorn の補題を適用せよ. □

注意 2.15 以上の結果は「ベクトル空間 V の任意の一次独立な部分集合を V の基底に拡張できる」という Zorn の補題を使って証明できる結果を使えば容易に証明できる. □

2.5 直和と補空間

有限次元とは限らないベクトル空間の基底の存在を用いて補空間の存在を証明しよう.

[**66**] **(直和, 5 点)** K 上のベクトル空間 V とその部分空間 $V_1, \ldots, V_N$ に関して以下の 2 条件は互いに同値である:

(a) 任意の $v \in V$ は $v = v_1 + \cdots + v_N$, $v_i \in V_i$ と一意に表わされる.

(b) 任意の $v \in V$ は $v = v_1 + \cdots + v_N$, $v_i \in V_i$ と表わされ, 任意の $v_i \in V_i$ $(i = 1, \ldots, N)$ に対して $v_1 + \cdots + v_N = 0$ ならば $v_i = 0$ $(i = 1, \ldots, N)$ である.

この同値な条件のどちらかが成立するとき, $V = V_1 \oplus \cdots \oplus V_N$ と書き, V は $V_1, \ldots, V_N$ の**直和 (direct sum)** であると言う. さらに各 V_i が有限次元でかつ $V = V_1 \oplus \cdots \oplus V_N$ ならば

$$\dim V = \dim V_1 + \cdots + \dim V_N$$

が成立する. □

[**67**] **(補空間の存在, 10 点)** 体 K 上のベクトル空間 U とその部分空間 V に対して, V の基底を U の基底に拡張できることを用いて, U の部分空間 W で $U = V \oplus W$ を満たすものが存在することを示せ. そのような W を U における V の **(線形) 補空間 (linear complement)** と呼ぶ. □

ヒント. V の基底 $\{v_i\}_{i \in I}$ を U の基底 $\{v_i\}_{i \in I} \cup \{w_j\}_{j \in J}$ に拡張して, W を $\{w_j\}_{j \in J}$ で張られる U の部分空間とすると $U = V \oplus W$ である. □

2.6 線形写像の行列表示

K は体であるとし, U, V は K 上の有限次元ベクトル空間であるとし, $f : U \to V$ は K 上の任意の線形写像であるとする. 線形写像 f 自身は極めて抽象的な数学的対象であるが, U と V に基底を定めることによって, f を具体的に行列で表現することができる.

$u_1, \ldots, u_n$ は U の基底であり, $v_1, \ldots, v_m$ は V の基底であるとする. このとき, 任意の $u \in U$, $v \in V$ は次のように一意に表わされる:

$$u = \sum_{j=1}^{n} \alpha_j u_j = \sum_{j=1}^{n} u_j \alpha_j = [u_1, \ldots, u_n] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \qquad (\alpha_j \in K),$$

$$v = \sum_{i=1}^{m} \beta_i v_i = \sum_{i=1}^{m} v_i \beta_i = [v_1, \ldots, v_m] \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix} \qquad (\beta_i \in K).$$

これによって $u \in U$ と $\alpha = {}^t[\alpha_1, \ldots, \alpha_n] \in K^n$ が一対一に対応し, $v \in V$ と $\beta = {}^t[\beta_1, \ldots, \beta_m] \in K^m$ が一対一に対応する. この対応を用いて, 線形写像 $f : U \to V$ と行列 $A = [a_{ij}] \in M_{m,n}(K)$ の一対一対応を構成可能であることを説明しよう.

まず, 各 $f(u_j) \in V$ は

$$f(u_j) = \sum_{i=1}^{m} a_{ij} v_i = \sum_{i=1}^{m} v_i a_{ij} = [v_1, \ldots, v_m] \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix} \qquad (a_{ij} \in K)$$

と一意に表わされるので,

$$[f(u_1), \ldots, f(u_n)] = [v_1, \ldots, v_m] \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

よって

$$\begin{aligned} f(u) &= \sum_{j=1}^{n} \alpha_j f(u_j) = \sum_{j=1}^{n} f(u_j) \alpha_j \\ &= [f(u_1), \ldots, f(u_n)] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = [v_1, \ldots, v_m] \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}. \end{aligned}$$

以上の記号のもとで線形写像 f は

$$[u_1, \ldots, u_n] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \in U \text{ を } [v_1, \ldots, v_m] \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \in V \text{ に}$$

対応させる写像に等しい. 以上のようにして線形写像 f に対応する行列 $A = [a_{ij}]$ が得られる. 逆に行列 $A = [a_{ij}]$ が与えられれば上の対応によって線形写像 $f : U \to V$ が得られることもわかる. 行列 $A = [a_{ij}]$ を線形写像 f の基底 u_j, v_i に関する**行列表示**と呼ぶことにする.

要約 2.16 (線形写像の行列表示) U の基底 $u_1, \dots, u_n$ と V の基底 $v_1, \dots, v_m$ に関する線形写像 $f : U \to V$ の行列表示 $A = [a_{ij}] \in M_{m,n}(K)$ は次の条件によって一意に決定される[9]:

$$[f(u_1), \dots, f(u_n)] = [v_1, \dots, v_m] \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

この条件は次と同値である:

$$f(u_j) = \sum_{i=1}^{m} a_{ij} v_i = \sum_{i=1}^{m} v_i a_{ij} \qquad (j = 1, \dots, n). \quad \square$$

[68] (5 点) $U = \mathbb{R}^3$, $V = \mathbb{R}^2$ とし, 行列

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix}$$

の積の定める U から V への線形写像を f と書くことにする (すなわち $f(u) = Au$ $(u \in U = \mathbb{R}^3)$). $u_1, u_2, u_3 \in U$ と $v_1, v_2 \in V$ を次のように定める:

$$u_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad u_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad u_3 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}, \qquad v_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}.$$

このとき, u_1, u_2, u_3 は U の基底であり, v_1, v_2 は V の基底であり, それらに関する f の行列表示を B とすると, B は

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

と簡単な形になることを示せ. $\square$

ヒント. $[f(u_1), f(u_2), f(u_3)] = [v_1, v_2]B$ を示せ. $[f(u_1), f(u_2), f(u_3)] = [Au_1, Au_2, Au_3] = A[u_1, u_2, u_3]$ なので $A[u_1, u_2, u_3] = [v_1, v_2]B$ が成立することを直接的な計算で示せばよい. というわけでこの問題は非常に簡単な問題である. $\square$

注意 2.17 (標準的な基底以外のより適切な基底を見付けることの重要性) 上の問題のように行列 A 自身は複雑な形をしていても, 標準的な基底とは別の基底に関して行列表示し直すと簡単な形になることがよくある. 与えられた線形写像の本質を見極めるためには適切な基底を見付けて行列表示してみることが役に立つ.

実は行列の基本変形や (後で習うことになっている) 行列の対角化や Jordan 標準形の理論はどれも「行列もしくは線形写像の本質を見極めるために役に立つ基底の見付け方に関する理論」とみなせる. $\square$

[69] (5 点) K は体であるとし, $m \times n$ 行列 $A \in M_{m,n}(K)$ を任意に取る. K^l の標準的基底を $e_1^{(l)}, \dots, e_l^{(l)}$ と書くことにする. すなわち $e_i^{(l)} \in K^l$ は第 i 成分のみが 1 で他の成分は 0 であるとする. 基底 $e_j^{(n)}$, $e_i^{(m)}$ に関する A の定める線形写像 $A : K^n \to K^m$ の行列表示は A 自身に等しい. $\square$

[9] 定義域の基底を横に並べたものに f を左から作用させて, 右側にポコッと出て来る行列 $A = [a_{ij}]$ を計算すれば線形写像 f の行列表示が得られる.

ヒント. $[Ae_1^{(n)}, \dots, Ae_n^{(n)}] = [e_1^{(m)}, \dots, e_m^{(m)}]A$ を示せばよいがほとんど自明である. □

[70] (10 点) 変数 x に関する複素係数 1 変数多項式環 $\mathbb{C}[x]$ の部分空間 V

$$V = \{\, f \in \mathbb{C}[x] \mid f \text{ の次数は } 3 \text{ 以下} \,\}$$

と定め, 線形写像 $T : V \to V$ を

$$Tf(x) = f(x+1) \qquad (f \in V)$$

と定める. このとき以下を計算せよ:

1. V の基底 $(v_0, v_1, v_2, v_3) = (1, x, x^2, x^3)$ に関する T の行列表現.
2. V の別の基底

$$(u_0, u_1, u_2, u_3) = \left(1, x, \frac{x(x-1)}{2}, \frac{x(x-1)(x-2)}{6}\right)$$

に関する T の行列表現. □

ヒント. 1. 基底 (v_0, v_1, v_2, v_3) に関する T の行列表現とは

$$[Tv_0, Tv_1, Tv_2, Tv_3] = [v_0, v_1, v_2, v_3]A$$

を満たす行列 A のことである. 2 についても同様であるが, 二項係数に関する Pascal の三角形 (の一般化) との関係に気付けば簡単に計算できる. □

略解. 小問 1, 2 の解答はそれぞれ次の行列になる:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$k = 0, 1, 2, \dots$ に対して x の多項式 $\binom{x}{k} \in \mathbb{Q}[x]$ を

$$\binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$$

と定めると

$$\binom{x}{0} = 1, \quad \binom{x}{1} = x, \quad \binom{x}{2} = \frac{x(x-1)}{2}, \quad \binom{x}{3} = \frac{x(x-1)(x-2)}{6}$$

であり, 次の Pascal の三角形の公式が成立している:

$$\binom{x+1}{k} = \binom{x}{k-1} + \binom{x}{k}. \quad \square$$

[71] (基底の変換, 5 点) K は体であるとし, U, V は K 上の有限次元ベクトル空間であり, $u_1, \dots, u_n$ は U の基底であり, $v_1, \dots, v_m$ は V の基底であるとする. $f : U \to V$ は線形写像であり, $A \in M_{m,n}(K)$ は基底 u_j, v_i に関する f の行列表示であるとする. $u'_1, \dots, u'_n$ と $v'_1, \dots, v'_m$ はそれぞれ U, V の別の基底であるとする. 以下を示せ.

1. ある可逆な行列 $Q \in GL_n(K)$, $P \in GL_m(K)$ で[10]

$$[u'_1, \dots, u'_n] = [u_1, \dots, u_n]Q, \qquad [v'_1, \dots, v'_m] = [v_1, \dots, v_m]P$$

をみたすものが一意に存在する.

2. 基底 u'_j, v'_i に関する f の行列表示は $P^{-1}AQ$ になる. □

ヒント. 2. $[f(u'_1), \dots, f(u'_n)] = [v'_1, \dots, v'_m]P^{-1}AQ$ を 1 を用いて示せばよい. □

[72] (5 点) K は体であるとし, $u_1, \dots, u_n \in K^n$ は K^n の基底であり, $v_1, \dots, v_m \in K^m$ は K^m の基底であるとし, $Q = [u_1, \dots, u_n] \in M_n(K)$, $P = [v_1, \dots, v_m] \in M_m(K)$ とおく. このとき, $m \times n$ 行列 $A \in M_{m,n}(K)$ の定める線形写像 $A : K^n \to K^m$ の基底 u_j, v_i に関する行列表示は $P^{-1}AQ$ になる. □

ヒント. 問題 **[69]**, **[71]** からただちに得られる. もしくは $[Au_1, \dots, Au_n] = AQ = PP^{-1}AQ = [v_1, \dots, v_m]P^{-1}AQ$. □

[73] (5 点) $V = \mathbb{R}^2$ とし, 行列

$$A = \frac{1}{5}\begin{bmatrix} 9 & -2 \\ -2 & 6 \end{bmatrix}$$

が定める V からそれ自身への線形写像を f と書くことにする. $v_1, v_2 \in V$ を

$$v_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} -2 \\ 1 \end{bmatrix}$$

と定めると, v_1, v_2 は V の基底である (v_1, v_2 を平面上の図示せよ). 基底 v_i に関する f の行列表示を求めよ. □

ヒント. $[f(v_1), f(v_2)] = [v_1, v_2]B$ を満たす行列 $B \in M_2(\mathbb{R})$ が答である. □

略解. $Av_1 = v_1$, $Av_2 = 2v_2$ なので $B = \mathrm{diag}(1, 2)$. □

[74] (10 点) 問題 **[73]** の結果を用いて, 次の常微分方程式の初期値問題を解け:

$$\frac{d}{dt}u = Au, \qquad u(0) = u_0.$$

ここで u は $t \in \mathbb{R}$ の $V = \mathbb{R}^2$ に値を持つ函数であり, $u_0 = e_2 = {}^t[0, 1]$. □

ヒント. まず今まで渡したプリントの「行列の指数函数」に関する説明を読め. $P = [v_1, v_2]$ と置くと $A = PBP^{-1}$ であるから,

$$e^{tA} = Pe^{tB}P^{-1}.$$

実は B は対角行列になるので e^{tB} は容易に計算される. その結果を用いて $u(t) = e^{tA}u_0$ を整理したものが答になる. □

[10] $GL_n(K)$ は K の元を成分に持つ可逆な $n \times n$ 行列全体の集合である. $GL_n(K)$ は群をなし, 一般線形群と呼ばれる.

略解. $e^{tB} = \mathrm{diag}(e^t, e^{2t})$ であり, $P = \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$, $P^{-1} = \frac{1}{5}\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} = \frac{1}{5}\,{}^tP$ なので

$$e^{tA} = Pe^{tA}P^{-1} = \frac{1}{5}\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} e^t & 0 \\ 0 & e^{2t} \end{bmatrix}\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} e^t + 4e^{2t} & 2e^t - 2e^{2t} \\ 2e^t - 2e^{2t} & 4e^t + e^{2t} \end{bmatrix}.$$

よって $u(t) = e^{tA}u_0 = e^{tA}e_2 = \frac{1}{5}\begin{bmatrix} 2e^t - 2e^{2t} \\ 4e^t + e^{2t} \end{bmatrix}$. □

[75] (一次変換の対角化, 10 点) V は体 K 上のベクトル空間であり, f は V の一次変換 (すなわち V からそれ自身への線形写像) であるとする. もしも V の基底 $v_1, \ldots, v_n$ が $f(v_i) = \alpha_i v_i$ $(\alpha_i \in K)$ を満たしているならば, 基底 v_i に関する f の行列表示は対角行列 $D = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ になる. □

ヒント. $[f(v_1), \ldots, f(v_n)] = [v_1, \ldots, v_n]D$ を示せばよいので簡単である. □

[76] (巡回行列とその行列式, 20 点) $n \times n$ 行列 Λ を次のように定める:

$$\Lambda = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ 1 & & & & 0 \end{bmatrix} = E_{12} + E_{23} + \cdots + E_{n-1,n} + E_{n,1} \in M_n(\mathbb{C}).$$

ここで E_{ij} は行列単位 (第 (i,j) 成分だけが 1 で他の成分がすべて 0 であるような行列) である. $\zeta = e^{2\pi i/n}$ (1 の原始 n 乗根) とおき,

$$v_k = \begin{bmatrix} 1 \\ \zeta^k \\ \zeta^{2k} \\ \vdots \\ \zeta^{(n-1)k} \end{bmatrix} \in \mathbb{C}^n \qquad (k \in \mathbb{Z})$$

とおく. このとき以下が成立する:

1. $\Lambda^k \neq E$ $(k = 1, \ldots, n-1)$, $\Lambda^n = E$.
2. $\Lambda v_k = \zeta^k v_k$ $(k \in \mathbb{Z})$.
3. $v_0, v_1, \ldots, v_{n-1}$ は $\mathbb{C}^n$ の基底である.
4. 基底 $v_0, v_1, \ldots, v_{n-1}$ に関する Λ の定める $\mathbb{C}^n$ の一次変換の行列表示は対角行列 $D = \mathrm{diag}(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$ になる.
5. $P = [v_0, v_1, \ldots, v_{n-1}] \in M_n(\mathbb{C})$ とおくと, P は可逆であり, $\Lambda = PDP^{-1}$.
6. $X = x_0E + x_1\Lambda + x_2\Lambda^2 + \cdots + x_{n-1}\Lambda^{n-1}$ とおくと,

$$\det X = \prod_{k=0}^{n-1}(x_0 + x_1\zeta^k + x_2\zeta^{2k} + \cdots + x_{n-1}\zeta^{(n-1)k}).$$ □

ヒント. 3. $|P| \neq 0$ を Vandermonde の行列式の公式を用いて示せばよい.
4. $[\Lambda v_0, \Lambda v_1, \ldots, \Lambda v_{n-1}] = [v_0, v_1, \ldots, v_{n-1}]D$ を示せばよい.
6. $X = P(x_0E + x_1D + x_2D^2 + \cdots + x_{n-1}D^{n-1})P^{-1} = P\,\mathrm{diag}(x_0 + x_1\zeta^k + x_2\zeta^{2k} + \cdots + x_{n-1}\zeta^{(n-1)k})_{k=0}^{n-1}P^{-1}$. □

[77] (複素数の実行列表示, 5 点) 複素数体 $\mathbb{C}$ は自然に実数体 $\mathbb{R}$ 上の 2 次元のベクトル空間とみなせ[11], $1, i$ は $\mathbb{C}$ の $\mathbb{R}$ 上の基底である. $z = x + iy \in \mathbb{C}$ $(x, y \in \mathbb{R})$ に対して, 写像 $\hat{z} : \mathbb{C} \to \mathbb{C}$ を

$$\hat{z}(w) := zw \qquad (w \in \mathbb{C})$$

と定めると, $\hat{z}$ は $\mathbb{R}$ 上の線形写像である. 基底 $1, i$ に関する $\hat{z}$ の行列表示を $A(z) \in M_2(\mathbb{R})$ と書くと,

$$A(z) = A(x + iy) = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}. \quad \square$$

ヒント. $[z1, zi] = [1, i]A(z)$ を示せばよいだけなので非常に簡単である. □

[78] (5 点) 複素数 $z = x + iy \in \mathbb{C}$ $(x, y \in \mathbb{R})$ に対して実 2 次正方行列 $A(z) = A(x + iy)$ を次のように定める:

$$A(z) = A(x + iy) := \begin{bmatrix} x & -y \\ y & x \end{bmatrix}.$$

このとき $z, w \in \mathbb{C}$ に対して次が成立する:

$$A(z + w) = A(z) + A(w), \qquad A(zw) = A(z)A(w), \qquad A(1) = E;$$
$$\det A(z) = |z|^2, \qquad \mathrm{tr}\, A(z) = 2\,\mathrm{Re}\, z, \qquad e^{A(z)} = A(e^z). \quad \square$$

[79] (ベクトル積の定義, 15 点) $\mathbb{R}^3$ の 2 つのベクトル $u = {}^t[u_1, u_2, u_3]$, $v = {}^t[v_1, v_2, v_3]$ の**ベクトル積 (vector product)** $u \times v$ を次のように定義する:

$$u \times v := \begin{bmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{bmatrix}.$$

このとき以下が成立する:

1. 第 i 成分だけが 1 で他の成分が 0 であるような 3 次元縦ベクトルを e_i と書くと,

$$e_i \times e_j = e_k, \quad e_j \times e_i = -e_k \qquad \big((i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)\big),$$
$$e_i \times e_i = 0 \qquad (i = 1, 2, 3).$$

2. ベクトル $u = {}^t[u_1, u_2, u_3]$ に対して行列 $X(u)$ を次のように定める:

$$X(u) = \begin{bmatrix} 0 & u_1 & u_3 \\ -u_1 & 0 & u_2 \\ -u_3 & -u_2 & 0 \end{bmatrix}.$$

[11]「複素平面」という言葉は複素数全体の集合が実数体上 2 次元のベクトル空間をなすことを含意している.

さらに行列 A, B の**交換子 (commutator)** $[A,B]$ を次のように定義する:

$$[A,B] = AB - BA.$$

このとき $u, v \in \mathbb{R}^3$ に対して

$$[X(u), X(v)] = X(u \times v).$$

3. ベクトル $u = {}^t[u_1, u_2, u_3]$ に対して行列 $Y(u)$ を次のように定める:

$$Y(u) = -\frac{i}{2}(u_1\sigma_1 + u_2\sigma_2 + u_3\sigma_3).$$

ここで σ_1, σ_2, σ_3 は次のように定義される **Pauli 行列**と呼ばれる行列である:

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

このとき $u, v \in \mathbb{R}^3$ に対して

$$[Y(u), Y(v)] = Y(u \times v).$$

4. $u, v, w \in \mathbb{R}^3$ に対して以下が成立している[12]:

$$v \times u = -u \times v, \qquad (u \times v) \times w = u \times (v \times w) - v \times (u \times w).$$

5. ベクトル積は行列式を用いて形式的に次のように表わされる:

$$u \times v = \begin{vmatrix} u_1 & v_1 & e_1 \\ u_2 & v_2 & e_2 \\ u_3 & v_3 & e_3 \end{vmatrix}.$$

この等式は「右辺の形式的な行列式の第 3 列に関する形式的な余因子展開が左辺に等しい」と読む. □

参考 2.18 上の問題の 2 と 3 はもちろん偶然ではない. 実はベクトル積は 3 次元 Euclid 空間の (無限小) 回転を表現しているのである. 実は上の問題は 3 次元 Euclid 空間の回転の表現の仕方には様々な方法があることを示していることになっている.

力学の教科書で回転運動の章を見るとベクトル積が登場する. それは回転運動を数学的に表現するためである. また量子物理の教科書を読むと Pauli 行列がよく登場する. それは我々が住んでいる物理的な 3 次元空間の回転対称性を表現するためである.

実は上の問題の 3 は **Hamilton の四元数体 (quaternion)** と関係している. 四元数体とは複素数をさらに拡張した非可換体であり, 実数体に i, j, k で

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

を満たすものを付け加えることによって構成される. $I = -i\sigma_1, J = -i\sigma, K = -i\sigma_3$ は i, j, k の満たすべき公式と同じ公式を満たしている. したがって, 複素数が実 2 次正方行列で表現できたように (問題 [**78**] を見よ), 四元数は複素 2 次正方行列で表現できる. □

[12] ヒント: n 次正方行列 A, B, C に対して $[[A,B],C] = [A,[B,C]] - [B,[A,C]]$ が成立している. これを交換子の **Jacobi 律**と呼ぶ.

[80] (ベクトル積と平行四辺形の面積, 15 点) 上の問題の続き. $\mathbb{R}^3$ 内で原点 0 と u を結ぶ線分, u と $u+v$ を結ぶ線分, $u+v$ と v を結ぶ線分 v と 0 を結ぶ線分で囲まれた平行四辺形を考える. このとき $u \times v$ はその平行四辺形に垂直になり, $u \times v$ の長さはその平行四辺形の面積に等しくなる. □

ヒント. $u \times v$ と u, v の内積が 0 になることが問題 **[79]** におけるベクトル積の定義もしくは 5 の表示から導かれる. 平行四辺形の面積との関係については平行四辺形の面積が $||u||\ ||v|| \sin\theta$ であることを使え. ここで θ は u と v のあいだの角度である. □

[81] (Hamilton の四元数の行列表示, 10 点) $1, i, j, k$ を基底に持つ $\mathbb{R}$ 上のベクトル空間

$$\mathbb{H} = \{\, a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\}$$

に積を次の規則で定める:

$$1^2 = 1, \quad 1i = i1 = i, \quad 1j = j1 = j, \quad 1k = k1 = k,$$
$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

このとき $\mathbb{H}$ の元を **Hamilton の四元数 (quaternion)** と呼ぶ. $a, b \in \mathbb{R}$ のとき四元数 $a1 + bi \in \mathbb{H}$ と複素数 $a + bi \in \mathbb{C}$ を同一視することにする. $q = a1 + bi + cj + dk \in \mathbb{H}$ $(a, b, c, d \in \mathbb{R})$ と置く. 写像 $\hat{q} : \mathbb{H} \to \mathbb{H}$ を

$$\hat{q}(r) = qr \qquad (r \in \mathbb{H})$$

と定めると, $\hat{q}$ は $\mathbb{R}$ 上の一次変換である. このとき以下が成立する.

1. $\mathbb{R}$ 上の基底 $1, i, j, k$ に関する $\hat{q}$ の行列表示を $A(q)$ と書くと,

$$A(q) = \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}.$$

2. $z = a + bi$, $w = c + di$, $a, b, c, d \in \mathbb{R}$ とすると, $q = z1 + wj = 1z + j\overline{w}$ であるから, $\mathbb{H}$ は $1, j$ を基底に持つ $\mathbb{C}$ 上の 2 次元のベクトル空間とみなされる. ただし $\mathbb{C}$ の元による右からの掛け算によって $\mathbb{H}$ に $\mathbb{C}$ 上のベクトル空間の構造を入れておくものとする. このとき $\hat{q}$ は $\mathbb{C}$ 上の一次変換になる (この事実も証明せよ). $\mathbb{C}$ 上の基底 $1, j$ に関する $\hat{q}$ の行列表示を $B(q)$ と書くと,

$$B(q) = \begin{bmatrix} z & -w \\ \bar{w} & \bar{z} \end{bmatrix}.$$

ここで $\bar{z}, \bar{w}$ はそれぞれ z, w の複素共役である. □

ヒント. 1. $[q1, qi, qj, qk] = [1, i, j, k]A(q)$ を示せばよい. 2. $[q1, qj] = [1, j]B(q)$ を示せばよい. $zj = j\bar{z}$ を用いよ. □

参考 2.19 問題 [**79**] で定義された Pauli 行列 $\sigma_1, \sigma_2, \sigma_3$ と四元数の複素 2×2 行列表現 $B(q)$ のあいだには $B(i) = i\sigma_3$, $B(j) = -i\sigma_2$, $B(k) = -i\sigma_1$ という関係がある. したがって, $\pm i$ 倍と順序の違いを除けば Pauli 行列と四元数 i, j, k の複素 2×2 行列表示は本質的に一致する. □

[**82**] **(15 点)** 問題 [**50**] の記号をそのまま用いる. $v_i = x^i$ と置く. 任意に $\lambda \in \mathbb{C}$ を取り, $\mathbb{C}[x]$ の一次変換 e, f, h を

$$e = \partial, \quad h = -2x\partial + \lambda, \quad f = -x^2\partial + \lambda x$$

と定める. このとき以下が成立している:

1. $hv_i = (\lambda - 2i)v_i, \quad ev_i = iv_{i-1}, \quad fv_i = (\lambda - i)v_{i+1}$.
2. 特に $\quad hv_0 = \lambda v_0, \quad ev_0 = 0$.
3. $[h, e] = 2e, \quad [h, f] = -2f, \quad [e, f] = h$.

ここで $[A, B] = AB - BA$ (交換子) である. □

ヒント. たとえば

$$fv_4 = (-x^2\partial + \lambda x)(x^4) = -x^2(x^4)' + \lambda x \cdot x^4 = -4x^5 + \lambda x^5 = (\lambda - 4)x^5 = (\lambda - 4)v_5.$$

3 の計算は交換子に関する一般的な公式

$$[A, A] = 0, \quad [B, A] = -[A, B],$$
$$[AB, C] = [A, C]B + A[B, C], \quad [A, BC] = [A, B]C + B[A, C]$$

と $[\partial, x^i] = ix^{i-1}$ を用いて実行せよ. たとえば

$$[\partial, -x^2\partial] = -[\partial, x^2]\partial - x^2[\partial, \partial] = -2x\partial - x^2 0 = -2x\partial. \quad \square$$

参考 2.20 (sl_2-triplet) 2×2 行列 E, F, H を

$$E = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad F = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad H = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

と定めると

$$[H, E] = 2e, \quad [H, F] = -2F, \quad [E, F] = H$$

が成立している. E, F, H を sl_2-triplet (sl_2 の三つ組) と呼ぶ. 上の問題 [**82**] の e, f, h は多項式係数の微分作用素による sl_2-triplet の表現になっている.

Lie 代数 $\mathrm{sl}_2(\mathbb{C})$ の有限次元表現論は 3 次元空間の回転を司る Lie 群 $SU(2)$ の表現論と同値である. Lie 群および Lie 代数の表現論に関する入門的な解説は山内・杉浦 [山内・杉浦] にある. □

[**83**] **(15 点)** 問題 [**82**] の続き. $\lambda = \ell \in \mathbb{Z}_{\geq 0}$ と仮定する. 以下を示せ:

1. ℓ 次以下の一変数多項式全体のなす $\mathbb{C}[x]$ の部分集合を V_ℓ と書くことにする:

$$V_\ell = \{\, a_0 + a_1 x + x_2 x^2 + \cdots + a_\ell x^\ell \mid a_0, a_1, \ldots, a_\ell \in \mathbb{C} \,\}.$$

このとき V_ℓ は $\mathbb{C}[x]$ の部分空間であり,

$$v_0 = 1, \quad v_1 = x, \quad v_2 = x^2, \quad \ldots, \quad v_\ell = x^\ell$$

は V_ℓ の基底をなす.

2. e, f, h の $\mathbb{C}[x]$ への作用は V_ℓ を保つ. すなわち, 任意の $v \in V_\ell$ に対して $ev, fv, hv \in V_\ell$.

3. e, f, h の定める V_ℓ の一次変換の基底 v_i に関する行列表示をそれぞれ E_ℓ, F_ℓ, H_ℓ と書くと,

$$E_\ell = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & 2 & & \\ & & 0 & \ddots & \\ & & & \ddots & \ell \\ 0 & & & & 0 \end{bmatrix}, \qquad F_\ell = \begin{bmatrix} 0 & & & & 0 \\ \ell & & 0 & & \\ & \ell-1 & & 0 & \\ & & & \ddots & \ddots \\ 0 & & & & 1 \quad 0 \end{bmatrix},$$

$$H_\ell = \begin{bmatrix} \ell & & & & 0 \\ & \ell-2 & & & \\ & & \ddots & & \\ & & & -\ell+2 & \\ 0 & & & & -\ell \end{bmatrix} = \operatorname{diag}(\ell, \ell-2, \ell-4, \ldots, -\ell+4, -\ell+2, -\ell).$$

たとえば $\ell = 3$ のとき

$$E_3 = \begin{bmatrix} 0 & 1 & & \\ & 0 & 2 & \\ & & 0 & 3 \\ & & & 0 \end{bmatrix}, \quad F_\ell = \begin{bmatrix} 0 & & & \\ 3 & 0 & & \\ & 2 & 0 & \\ & & 1 & 0 \end{bmatrix}, \quad H_3 = \begin{bmatrix} 3 & & & \\ & 1 & & \\ & & -1 & \\ & & & -3 \end{bmatrix}. \quad \square$$

注意 2.21 特に $\ell = 1$ のとき $E_1 = E$, $F_1 = F$, $H_1 = H$ である. $\square$

参考 2.22 実は Lie 代数 $\mathrm{sl}_2(\mathbb{C})$ の (したがってコンパクト Lie 群 $SU(2)$ の) 有限次元既約表現の同型類の全体は表現 V_ℓ ($\ell = 0, 1, 2, \ldots$) で代表される[13]. この事実は 3 次元空間の回転を量子論的に実現する方法が非負の整数 ℓ で分類されることを意味している.

H_ℓ の固有値 $\ell, \ell-2, \ldots, -\ell+2, -\ell$ は表現 V_ℓ のウェイト (weight) と呼ばれており, その最高値の ℓ は表現 V_ℓ の最高ウェイト (highest weight) と呼ばれている.

物理学では sl_2 の三つ組 E, F, H の代わりに $\sigma_z = \frac{1}{2}H$, $\sigma_+ = \frac{1}{\sqrt{2}}E$, $\sigma_- = \frac{1}{\sqrt{2}}F$ の三つ組を用いることが多い. それらは次の交換関係を満たしている:

$$[\sigma_z, \sigma_\pm] = \pm\sigma_\pm, \qquad [\sigma_+, \sigma_-] = \sigma_z.$$

[13] しかも e, f, h が微分作用素で表わされたのも偶然ではない. 半単純 Lie 代数 (もしくは半単純 Lie 群) の表現に関する幾何学的な理論 (Borel-Weil-Bott 理論) が存在し, それを用いれば半単純 Lie 代数の有限次元表現の微分作用素による表示が自然に得られる. この辺の問題は Lie 代数および Lie 群の表現論 (representation theory) という大きな理論の一部分を切り取ることによって作成された.

だから, H の作用 H_ℓ の固有値のウェイトではなく, σ_z の作用 $\frac{1}{2}H_\ell$ の固有値を用いることが多い. $j=\ell/2$ の方を用を表現 V_ℓ のスピンと呼ぶ[14].

以上のコメントに関する詳しい解説については山内・杉浦 [山内・杉浦] を参照せよ. □

[84] (15 点) 正の整数 $n\in\mathbb{Z}>0$ と複素数 $\alpha\in\mathbb{C}$ に対して, $(t-\alpha)^k\neq 0$ $(k=1,\dots,n-1)$, $(t-\alpha)^n=0$ を満たす文字 t を用意し[15], $1,t,t^2,\dots,t^{n-1}$ を基底に持つ $\mathbb{C}$ 上のベクトル空間 V を次のように定める:

$$V:=\{\,\beta_0+\beta_1 t+\beta_2 t^2+\cdots+\beta_{n-1}t^{n-1}\mid \beta_0,\beta_1,\beta_2,\dots,\beta_{n-1}\in\mathbb{C}\,\}.$$

写像 $f:V\to V$ を $f(v)=tv$ $(v\in V)$ と定めると, f は V の $\mathbb{C}$ 上の一次変換 (V からそれ自身への線形写像) である. 以下が成立することを示せ:

1. 基底 $1,t,t^2,\dots,t^{n-1}$ に関する f の行列表示を A と書くと,

$$A=\begin{bmatrix} 0 & & & 0 & -a_{n-1}\\ 1 & 0 & & & -a_{n-2}\\ & 1 & \ddots & & \vdots\\ & & \ddots & 0 & -a_1\\ 0 & & & 1 & -a_0 \end{bmatrix}.$$

ここで $a_0,a_1,\dots,a_{n-2},a_{n-1}\in\mathbb{C}$ は $(\lambda-\alpha)^n$ の展開

$$(\lambda-\alpha)^n=\lambda^n+a_0\lambda^{n-1}+a_1\lambda^{n-2}+\cdots+a_{n-2}\lambda+a_{n-2}$$

によって定められたものである. 二項定理より,

$$a_{i-1}=\binom{n}{i}(-\alpha)^i\qquad(i=1,\dots,n).$$

よって $a_0=-n\alpha$, $a_1=\frac{n(n-1)}{2}\alpha^2$, …, $a_{n-2}=n(-\alpha)^{n-1}$, $a_{n-1}=(-\alpha)^n$.

2. V の $\mathbb{C}$ 上の基底として $1,t-\alpha,(t-\alpha)^2,\dots,(t-\alpha)^{n-1}$ も取れる.

3. 基底 $1,t-\alpha,(t-\alpha)^2,\dots,(t-\alpha)^{n-1}$ に関する f の行列表示を B と書くと,

$$B=\begin{bmatrix} \alpha & & & & 0\\ 1 & \alpha & & & \\ & 1 & \alpha & & \\ & & \ddots & \ddots & \\ 0 & & & 1 & \alpha \end{bmatrix}\qquad(n\times n\text{ 行列}).\quad\square$$

ヒントと. 1. $(t-\alpha)^n=0$ を用いて, $[t1,tt,tt^2,\dots,tt^{n-1}]=[1,t,t^2,\dots,t^{n-1}]A$ を示せばよい.

2. $k=0,1,\dots,n-1$ とする. $(t-\alpha)^k$ を展開することによって, $(t-\alpha)^k$ は $1,t,\dots,t^k$ の一次結合で書けることがわかる. 逆に $t^k=((t-\alpha)+\alpha)^k$ を展開することによって, t^k は

[14]電子や陽子のスピンは $1/2$ である.

[15]厳密にはそのような文字 t は多項式環 $\mathbb{C}[\lambda]$ の剰余環 $\mathbb{C}[\lambda]/((\lambda-\alpha)^n)$ の λ で代表される元として構成される ($t=\lambda \bmod (\lambda-\alpha)^n$). 剰余環 $\mathbb{C}[\lambda]/((\lambda-\alpha)^n)$ の構成に関しては問題 **[95]**, **[96]** を参照せよ.

$1, t-\alpha, \ldots, (t-\alpha)^k$ の一次結合で書けることがわかる. このことより, $1, t-\alpha, \ldots, (t-\alpha)^{n-1}$ も V の基底であることがわかる.

3. $[t1, t(t-\alpha), t(t-\alpha)^2, \ldots, t(t-\alpha)^{n-1}] = [1, t-\alpha, (t-\alpha)^2, \ldots, (t-\alpha)^{n-1}]B$ を示せばよい. そのとき $t(t-\alpha)^k = (\alpha + (t-\alpha))(t-\alpha)^k = \alpha(t-\alpha)^k + (t-\alpha)^{k+1}$ と $(t-\alpha)^n = 0$ を用いよ. □

注意 2.23 (Jordan 標準形の理論との関係) ${}^tA$ は参考 2.24 のコンパニオン行列の形をしている. ${}^tB$ は問題 [**132**] の Jordan ブロックの形をしている. 実は上の問題 [**84**] は単因子論を経由する Jordan 標準形の存在証明の一部分になっている.

その方針での Jordan 標準形の理論の解説に関しては堀田 [堀田] がおすすめである. □

参考 2.24 (コンパニオン行列) 次の形の n 次正方行列のを **コンパニオン行列 (同伴行列, companion matrix)** と呼ぶ:

$$C(a_0, \ldots, a_{n-1}) = \begin{bmatrix} 0 & 1 & & & 0 \\ & 0 & \ddots & & \\ & & \ddots & 1 & \\ 0 & & & 0 & 1 \\ -a_{n-1} & -a_{n-2} & \cdots & -a_1 & -a_0 \end{bmatrix}.$$

コンパニオン行列 $C = C(a_0, \ldots, a_{n-1})$ の特性多項式[16]は

$$p_C(\lambda) = \det(\lambda E - C(a_0, \ldots, a_{n-1})) = \lambda^n + a_0\lambda^{n-1} + a_1\lambda^{n-2} + \cdots + a_{n-2}\lambda + a_{n-1}$$

となる.

コンパニオン行列の最小多項式は特性多項式に等しく, しかもその固有値 α に属する Jordan 細胞は唯一になることが知られている[17]. □

2.7 商ベクトル空間

K は体であるとし, V は K 上の任意のベクトル空間であるとし, W は V の部分空間であるとする. 任意の $v \in V$ に対して

$$v + W = \{\, v + w \mid w \in W \,\}$$

とおき, 集合の集合 V/W を次のように定める:

$$V/W = \{\, v + W \mid v \in V \,\}.$$

[85] (5 点) $v, v' \in V$ に対して, $v + W = v' + W$ と $v' - v \in W$ は同値である. □

[16]一般に n 次正方行列 A の**特性多項式 (characteristic polynomial)** $p_A(\lambda)$ は $p_A(\lambda) = \det(\lambda E - A)$ と定義される. ここで E は n 次の単位行列である.

[17]「最小多項式」や「Jordan 細胞」などの用語の意味は後で **Jordan 標準形 (Jordan normal form, Jordan canonical form)** の理論を習うときに教わることになるだろう. もちろん各自が自由に自習して構わない. 数学の得意な人の特徴は学校の授業の先の勉強を勝手にやってしまうことである.

ヒント. $v+W=v'+W$ ならば $v'\in v'+W$ に対してある $w\in W$ で $v'=v+w$ をみたすものが存在する. そのとき $v'-v=w\in W$ である. 逆に $v'-v\in W$ ならば任意の $w\in W$ に対して $v'+w=v+(v'-v)+w\in v+W$ である. よって $v'+W\subset v+W$ である. 逆向きの包含関係も同様にして示されるので $v+W=v'+W$ である. □

[86] **(5 点)** 写像 $+:(V/W)\times(V/W)\to(V/W)$ と $\cdot:K\times(V/W)\to(V/W)$ を

$$(u+W)+(v+W)=(u+v)+W,\quad \alpha(u+W)=(\alpha u)+W\qquad (u,v\in V,\ \alpha\in K)$$

と定義することができることを示せ. □

ヒント. これは well-definedness (うまく定義されること) を示す問題である. 写像がうまく定義されることを示すためには同じものが同じものに移ることを示さなければいけない. そのためには $u+W=u'+W$, $v+W=v'+W$, $u,u',v,v'\in V$, $\alpha\in K$ のとき,

$$(u+v)+W=(u'+v')+W,\qquad (\alpha u)+W=(\alpha u')+W$$

となることを示せばよい. □

[87] **(5 点)** 上の問題で定義された演算 $+,\cdot$ に関して V/W は K 上のベクトル空間をなすことを示せ. □

ヒント. 写像 $-:V/W\to V/W$ を $-(u+W)=(-u)+W$ $(u\in V)$ と定義することができる. さらに, $0_{V/W}=0+W=W$ とおき, ベクトル空間の公理を機械的にチェックすればよい. □

定義 2.25 (商ベクトル空間) 以上のようにして構成された V/W を V を W で割ってできる V の**商ベクトル空間 (quotient vector space)** もしくは**商空間 (quotient space)** と呼ぶ. □

参考 2.26 (商ベクトル空間の元の記号について) V/W の元 $v+W$ は

$$v+W=v\bmod W=[v]=\bar{v}$$

のように書かれることも多い. $v\bmod W$ は「ベクトル v の W の元による平行移動方向の成分を無視したもの」という意味を持ち, $[v]$ や $\bar{v}$ は v で代表される**同値類 (equivalence class)** によく使われる記号である. □

参考 2.27 以上の商ベクトル空間の構成はそのまま一般の環 R 上の加群の商加群の構成に一般化される. □

参考 2.28 (M/N という記号法について) 代数学において加群 (ベクトル空間も加群の一種であることに注意) M とその部分加群 N に対して, M/N は分子の加群 M の中で分母の部分加群 N をゼロにつぶしてできる商加群を意味している. □

注意 2.29 商ベクトル空間は集合の集合として定義されたが, V/W **が集合の集合であることにこだわりすぎると商ベクトル空間の正しい理解に失敗する**. 商ベクトル空間 V/W の元は通常のベクトルだと考えた方がよい.

それでは V/W の元はどのようなベクトルだと考えればよいのだろうか. 問題 [**85**] によれば, $v, v' \in V$ に対応する商ベクトル空間 V/W の元 $v+W$, $v'+W$ が互いに等しくなるための必要十分条件は $v'-v \in W$ すなわち $v' \in v+W$ である. よって V の中の v を通り W に平行な部分集合 $v+W$ 上のすべてのベクトルが商ベクトル空間 V/W の一点に対応している. つまり, 直観的に V/W は V を W 方向につぶして[18]できるベクトル空間とみなせる. この点に関しては問題 [**88**], [**89**] を参考にせよ. □

[**88**] **(10 点)** $\mathbb{R}^3$ の部分空間 Z を $Z = \{\, (0,0,z) \mid z \in \mathbb{R} \,\}$ と定める. このとき, $\mathbb{R}^3/Z$ は $\mathbb{R}$ 上の 2 次元のベクトル空間になる. □

ヒント. e_1+Z, e_2+Z が $\mathbb{R}^3/Z$ の基底をなすことを示せ. □

注意 2.30 $\mathbb{R}^3/Z$ は直観的に 3 次元空間 $\mathbb{R}^3$ を z 軸方向に潰してできる 2 次元空間だとみなせる. すなわち $\mathbb{R}^3$ の中の z 軸 Z に平行な直線を一点に潰してできる 2 次元空間が $\mathbb{R}^3/Z$ である. □

[**89**] **(10 点)** $\mathbb{R}^3$ の部分空間 W を $W = \{\, (x,y,0) \mid x, y \in \mathbb{R} \,\}$ と定める. このとき, $\mathbb{R}^3/W$ は $\mathbb{R}$ 上の 1 次元のベクトル空間になる. □

ヒント. e_3+W が $\mathbb{R}^3/W$ の基底をなすことを示せ. □

注意 2.31 $\mathbb{R}^3/W$ は直観的に 3 次元空間 $\mathbb{R}^3$ を xy 平面方向に潰してできる 1 次元空間だとみなせる. すなわち $\mathbb{R}^3$ の中の xy 平面 W に平行な平面を一点に潰してできる 1 次元空間が $\mathbb{R}^3/W$ である. □

[**90**] **(自然な射影, 5 点)** 写像 $p : V \to V/W$ を

$$p(v) = v + W \qquad (v \in V)$$

と定めると, p は K 上の線形写像でかつ全射である. p は V から商空間 V/W への**自然な射影 (canonical projection)** もしくは**自然な写像 (canonical mapping)** と呼ばれる. □

[**91**] **(準同型定理, 20 点)** U, V は体 K 上のベクトル空間であり, $f : U \to V$ は線形写像であるとする. f の**核 (kernel)** $\operatorname{Ker} f$ と**像 (image)** $\operatorname{Im} f$ を

$$\operatorname{Ker} f = \{\, u \in U \mid f(u) = 0 \,\}, \qquad \operatorname{Im} f = \{\, f(u) \mid u \in U \,\}$$

と定めると, $\operatorname{Ker} f$ は U の部分空間であり, $\operatorname{Im} f$ は V の部分空間である. 写像 $\phi : U/\operatorname{Ker} f \to \operatorname{Im} f$ を

$$\phi(u + \operatorname{Ker} f) = f(u) \qquad (u \in U)$$

と定義することができ (すなわち $u, u' \in U$ に対して $u + \operatorname{Ker} f = u' + \operatorname{Ker} f$ ならば $f(u) = f(u')$), ϕ は K 上のベクトル空間の同型写像になる. □

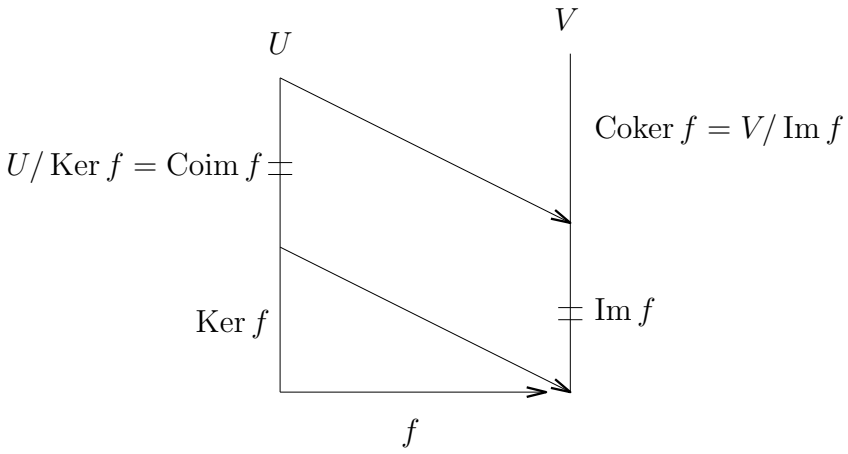

図 2.1: 準同型定理

ヒント. 記号の簡単のため $\overline{u} = u + \operatorname{Ker} f$ $(u \in U)$ とおく.

ϕ の well-definedness: $u, u' \in U$, $\overline{u} = \overline{u'}$ と仮定する. そのとき $u - u' \in \operatorname{Ker} f$ である. よって $f(u) - f(u') = f(u - u') = 0$ すなわち $f(u) = f(u')$ である.

ϕ の線形性: $u, u' \in U$, $\alpha \in K$ に対して, $\phi(\overline{u} + \overline{u'}) = \phi(\overline{u + u'}) = f(u + u') = f(u) + f(u') = \phi(\overline{u}) + \phi(\overline{u'})$, $\phi(\alpha\overline{u}) = \phi(\overline{\alpha u}) = f(\alpha u) = \alpha f(u) = \alpha\phi(\overline{u})$.

ϕ の単射性: $u \in U$, $\phi(\overline{u}) = 0$ と仮定する. $0 = \phi(\overline{u}) = f(u)$ より $u \in \operatorname{Ker} f$ である. よって $\overline{u} = 0$.

ϕ の全射性: $\operatorname{Im}\phi = \{\, \phi(\overline{u}) \mid u \in U \,\} = \operatorname{Im} f$. □

参考 2.32 $f : U \to V$ の**余核 (cokernel)** $\operatorname{Coker} f$ と**余像 (coimage)** $\operatorname{Coim} f$ が

$$\operatorname{Coker} f = V/\operatorname{Im} f, \qquad \operatorname{Coim} = U/\operatorname{Ker} f$$

と定義される. 準同型定理は余像と像が自然に同型になることを意味している. このことをよく図 2.1 のように描く. □

参考 2.33 準同型定理は一般の環 R 上の加群にそのまま一般化される. 証明の仕方はベクトル空間の場合とまったく同じである. □

[92] (10 点) U は体 K 上のベクトル空間であり, V はその部分空間であるとし, W は U における V の補空間であるとする. このとき自然な射影 $p : U \twoheadrightarrow U/V$ の W への制限 $p|_W : W \to U/V$ は同型写像になる. よって $(W \oplus V)/V \cong W$ という自然な同型を得る. □

ヒント. $p|_W$ が単射であることと全射であることを補空間の定義に戻って地道に証明せよ. もしくは写像 $q : U/V \to W$ を $q((w + v) \bmod V) = w$ $(w \in W, v \in V)$ と定めることができ (well-definedness のチェックが必要), q が $p|_W$ の逆写像になることを示せ. □

[93] (次元公式, image と kernel の次元の関係, 10 点) U, V は体 K 上のベクトル空間であり, U は有限次元であると仮定する. このとき任意の線形写像 $f : U \to V$ に対して

$$\dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim U. \quad \square$$

[18] 「つぶす」という言葉を用いると, 紙屑などを「グシャッ」と潰す様子を想像する人が結構いるようである. しかし, 商ベクトル空間 V/W を作るために V を W 方向につぶす場合には「グシャッ」ではなく「スーッ」と滑らかに潰れる様子を想像しなければいけない.

[94] (5 点) K は任意の体であるとし, U, V, W は K 上の有限次元ベクトル空間であり, $\dim V = \dim U + 4$ であると仮定する. $f : U \to V$, $g : V \to W$ は線形写像であり, $\dim \mathrm{Ker}\, f = 1$, $\dim \mathrm{Im}\, g = 3$ を満たしていると仮定する. $\dim \mathrm{Ker}\, g - \dim \mathrm{Im}\, f$ を求めよ. (ヒント: 次元公式を使え.) □

[95] (15 点) 体 K 上の一変数多項式環 $K[\lambda]$ を考え, 任意にゼロでない多項式 $f \in K[\lambda]$ を取る. このとき, $K[\lambda]$ の部分集合 (f) を

$$(f) = K[\lambda]f = \{\, af \mid a \in K[\lambda] \,\}$$

と定める[19]. 以下を示せ.

1. (f) は $K[\lambda]$ の $K[\lambda]$ 部分加群である. すなわち任意の $g, h \in (f)$ と $a \in K[\lambda]$ に対して $g + h \in (f)$ かつ $af \in (f)$ である. 特に (f) は $K[\lambda]$ の K 上のベクトル部分空間である.

2. $R = K[\lambda]/(f)$ (商ベクトル空間) とおき, $a \in K[\lambda]$ に対する $a + (f) \in R$ を $a \bmod f$ と書くことにする. このとき, 積 $\cdot : R \times R \to R$ を

$$(a \bmod f) \cdot (b \bmod f) = ab \bmod f \qquad (a, b \in K[\lambda])$$

と定めることができる (すなわち $a, b, c, d \in K[\lambda]$ に対して $a \bmod f = c \bmod f$, $b \bmod f = d \bmod f$ ならば $ab \bmod f = cd \bmod f$ が成立する).

3. これによって R は可換環をなす[20]. □

ヒント. 1. $a, b, c \in K[\lambda]$ に対して $af + bf = (a + b)f \in (f)$ であり, $a(bf) = (ab)f \in (f)$. 2. $a \bmod f = c \bmod f$ と $a - c \in (f)$ は同値であり, $b \bmod f = d \bmod f$ と $b - d \in (f)$ は同値であるから, $ab - cd = ab - ad + ad - cd = a(b - d) + d(a - c) \in (f)$. 3. $1_R = 1 \bmod f$ と置き, 可換環の公理を機械的にチェックすればよい. □

参考 2.34 $R = K[\lambda]/(f)$ は $K[\lambda]$ の中で f をゼロとみなすことによって得られる可換環である. f がゼロとみなされるならば任意の $a \in K[\lambda]$ に対する af もゼロとみなされなければいけない. (f) はそのような af 全体のなす集合である.

本当は上の問題は可換環とイデアルと剰余環の理論としてより一般的にやるべき事柄である. □

[96] (10 点) 上の問題 **[95]** のつづき. f の次数が n ならば $\dim_K R = \dim_K(K[\lambda]/(f)) = n$ であることを証明せよ. □

ヒント 1. $t = \lambda \bmod f$ と置くと, $t^i = \lambda^i \bmod f$ である. $1, t, t^2, \ldots, t^{n-1}$ が R の K 上の基底になることを示せばよい.

任意の $g \in K[\lambda]$ は g を f で割ることによって $g = qf + r$, $q, r \in K[\lambda]$, $\deg r < n$ と一意に表わされる[21] (商が q で余りが r). そのとき $g \bmod f = r \bmod f$ であり, r は次数

[19] (f) は f から生成される $K[\lambda]$ の**単項イデアル (principal ideal)** と呼ばれる.

[20] $R = K[\lambda]/(f)$ は $K[\lambda]$ をイデアル (f) で割ってできる**剰余環 (residue ring, residue-class ring)** と呼ばれる.

[21] $\deg r$ は r の次数である. $r = 0$ のとき $\deg r = -\infty$ と考える.

が n 未満なので $1, \lambda, \ldots, \lambda^{n-1}$ の一次結合で表わされるので, $g \bmod f$ は $1, t, \ldots, t^{n-1}$ の一次結合で表わされる.

もしも $g \in K[\lambda]$, $\deg g < n$ かつ $g \bmod f = 0_R = (f)$ ならば $g = af$, $a \in K[\lambda]$ と表わされる. $\deg g < n$ より $a = 0$ でなければいけないので $g = 0$ となる. これより $1, t, \ldots, t^{n-1}$ の一次独立性が出る. □

ヒント 2. 次数が n 未満の λ の多項式全体のなす n 次元のベクトル空間を V と書き, 線形写像 $\phi : V \to R$ を $\phi(v) = v \bmod f$ $(v \in V)$ と定義する. ϕ が同型写像であることを示せば R の次元も n であることがわかる.

任意の $g \in K[\lambda]$ は g を f で割ることによって $g = qf + r$, $q, r \in K[\lambda]$, $\deg r < n$ と一意に表わされるので, $g \bmod f = r \bmod f = \phi(r)$ である. よって ϕ は全射である.

もしも $g \in V$ かつ $\phi(g) = g \bmod f = 0_R = (f)$ ならば $g = af$, $a \in K[\lambda]$ と表わされる. $\deg g < n$ より $a = 0$ でなければいけないので $g = 0$ となる. よって ϕ は単射である. □

2.8 双対空間

[97] (双対空間の定義, 5 点) 体 K 上のベクトル空間 V に対して V から K への線形写像全体のなす集合 V^* は自然に体 K 上のベクトル空間をなすことを示せ. V^* は V の **双対ベクトル空間 (dual vector space)** もしくは **双対空間 (dual space)** と呼ばれる. $f \in V^*$ と $v \in V$ に対して $f(v)$ を $\langle f, v \rangle$ と表わすことがある. □

ヒント. 問題 **[46]** の特別な場合. $V^* = \mathrm{Hom}_K(V, K)$. □

[98] (横ベクトルの空間と縦ベクトルの空間の双対性, 5 点) K は体であるとする. K の元を成分に持つ n 次元縦ベクトル全体のなすベクトル空間を K^n と書き, n 次元横ベクトル全体のなすベクトル空間を仮に ${}^t(K^n)$ と書くことにする. 写像 $\iota : {}^t(K^n) \to (K^n)^*$ を横ベクトルと縦ベクトルの積によって

$$\left\langle \iota([x_1, \ldots, x_n]), \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \right\rangle := [x_1, \ldots, x_n] \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \sum_{i=1}^{n} x_i y_i \qquad (x_i, y_i \in K)$$

と定義する. このとき ι は同型写像になることを示せ. ι を通して横ベクトルの空間 ${}^t(K^n)$ と縦ベクトルの空間 K^n の双対空間 $(K^n)^*$ は自然に同一視される. □

参考 2.35 (ブラとケット) 量子力学には, ブラベクトル (bra vector) $\langle v^* |$ やケットベクトル (ket vector) $|v\rangle$ のような記号が登場し[22], ブラ $\langle v^* |$ とケット $|v\rangle$ のあいだには $\langle v^* | v \rangle \in \mathbb{C}$ と書かれる内積が定義されている.

実はブラベクトル全体のなすベクトル空間はケットベクトル全体のなすベクトル空間の双対空間と同一視できる. 直観的にブラベクトルは横ベクトルのようなものであり, ケットベクトルは縦ベクトルのようなものだと考えればよい. 横ベクトルと縦ベクトルのあいだには上の問題のように自然に内積が定義される. □

[22] Dirac [Dirac] などの量子力学の教科書を参照せよ.

[99] (基底の定める座標, 5 点) V は体 K 上の有限次元ベクトル空間であり, $v_1, \dots, v_n$ は V の基底であるとする. 任意の $v \in V$ は $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ $(\alpha_i \in K)$ と一意に表わされる. よって v に対して α_i を対応させる写像 x_i が定まる. $x_i \in V^*$ であることを示せ. (x_i を基底 v_i の定める V 上の座標と呼ぶことにする.) □

[100] (双対基底, 10 点) V は体 K 上の有限次元ベクトル空間であるとする. V の基底 $v_1, \dots, v_n$ に対して, $v_1^*, \dots, v_n^* \in V^*$ を

$$\langle v_i^*, v_j \rangle = \delta_{ij} \qquad (i, j = 1, \dots, n)$$

という条件によって一意に定めることができる. このとき $v_1^*, \dots, v_n^*$ は双対空間 V^* の基底になる. 特に $\dim V^* = \dim V$ である. $v_1^*, \dots, v_n^*$ を $v_1, \dots, v_n$ の**双対基底 (dual basis)** と呼ぶ. □

ヒント. 任意の $f \in V^*$ に対して, $g = \sum_{j=i}^n \langle f, v_i \rangle v_i^* \in V^*$ と置くと, $\langle g, v_j \rangle = \langle f, v_j \rangle$ $(j = 1, \dots, n)$ であるから, $f = g$ であることがわかる. よって V^* は $v_1^*, \dots, v_n^*$ で張られる. $v^* := \sum_{i=1}^n \alpha_i v_i^* = 0$, $\alpha_i \in K$ と仮定する. このとき $0 = \langle v^*, v_j \rangle = \alpha_j$ $(j = 1, \dots, n)$ である. よって $v_1^*, \dots, v_n^*$ は一次独立である. □

注意 2.36 問題 [99] の x_i と問題 [100] の v_i^* は等しい. □

[101] (1 の分解, 10 点) V は体 K 上の有限次元ベクトル空間であるとする. V の基底 $v_1, \dots, v_n$ とその双対基底 $v_1^*, \dots, v_n^* \in V^*$ を任意に取る. V の一次変換 $\sum_{i=1}^n v_i v_i^*$ を次のように定める:

$$\left(\sum_{i=1}^n v_i v_i^* \right) (v) = \sum_{i=1}^n v_i \langle v_i^*, v \rangle \qquad (v \in V).$$

この $\sum_{i=1}^n v_i v_i^*$ は V の恒等写像 id_V に等しい. $\mathrm{id}_V = \sum_{i=1}^n v_i v_i^*$ を 1 **の分割**と呼ぶ. □

ヒント. $v \in V$ を $v = \sum_{j=1}^n \alpha_j v_j$, $\alpha_j \in K$ と表わし, $\sum_{i=1}^n v_i \langle v_i^*, v \rangle$ を計算してみよ. □

注意 2.37 $V = K^n$, $v_i = e_i$ ならば $v_i^* = {}^t e_i$ である. $\sum_{i=1}^n e_i \, {}^t e_i$ が単位行列になることは容易に示される. 上の問題の結果はこれの一般化である. □

参考 2.38 量子力学では[23], 1 の分割をブラとケットの記号を用いて $1 = \sum_i |i\rangle\langle i|$ のように書くことが多い. $|i\rangle$ はケットベクトル全体の空間の基底であり, $\langle i|$ はその双対基底である. □

[102] (双対の双対, 10 点) V は体 K 上の有限次元ベクトル空間であるとする. このとき, 写像 $\iota : V \to (V^*)^*$ を

$$\langle \iota(v), f \rangle = \iota(v)(f) := \langle f, v \rangle = f(v) \qquad (v \in V, \ f \in V^*)$$

と定めると, ι は同型写像である. $\iota : V \xrightarrow{\sim} (V^*)^*$ を通して, $(V^*)^*$ は V と自然に同一視される. □

[23] Dirac [Dirac] などを見よ.

[103] (転置写像, 10 点) $f : U \to V$ は体 K 上のベクトル空間のあいだの線形写像であるとする. このとき線形写像 ${}^t f : V^* \to U^*$ を

$$\langle {}^t f(v^*), u\rangle = \langle v^*, f(u)\rangle \qquad (v^* \in V^*,\ u \in U)$$

と定義できることを示せ. ${}^t f$ を f の**転置写像**と呼ぶことにする. □

[104] (行列の転置との関係, 10 点) K は体であるとし, K の元を成分に持つ n 次元縦ベクトル全体の空間を K^n と表わし, 写像 $\iota : K^n \to (K^n)^*$ を

$$\langle \iota(x), y\rangle = \iota(x)(y) := {}^t xy = \sum_{i=1}^{n} x_i y_i \qquad (x = [x_i], y = [y_i] \in K^n)$$

と定めると, ι は同型写像である. ι を用いて $(K^n)^*$ と K^n 自身を同一視することにする. そのとき, 任意に $A \in M_{m,n}(K)$ を取ると, A の定める K^n から K^m への線形写像の転置写像が ${}^t A$ の定める K^m から K^n への線形写像になることを示せ. □

ヒント. $x, y \in K^n$ を任意に取る. $\langle \iota({}^t Ax), y\rangle = \langle \iota(x), Ay\rangle$ を示せばよい. □

[105] (商空間と部分空間の双対, 20 点) U は体 K 上のベクトル空間であり, V はその部分空間であるとし,

$$V^\perp = \{\, u^* \in U^* \mid \langle u^*, v\rangle = 0 \ (v \in V)\,\}$$

とおく[24]. V から U への包含写像を i と書き[25], U から U/V への自然な射影を p と書くことにする:

$$V \xrightarrow{\ i\ } U \xrightarrow{\ p\ } U/V.$$

双対空間の移ると次のような転置写像の列ができる:

$$V^* \xleftarrow{\ {}^t i\ } U^* \xleftarrow{\ {}^t p\ } (U/V)^*.$$

以下を示せ:

1. ${}^t p : (U/V)^* \to U^*$ は単射である.
2. $\mathrm{Ker}\ {}^t i = V^\perp$.
3. $\mathrm{Ker}\ {}^t i = \mathrm{Im}\ {}^t p$ である.
4. ${}^t p$ は自然な同型 $(U/V)^* \xrightarrow{\sim} V^\perp$, $x^* \mapsto {}^t p(x^*)$ を誘導する.
5. ${}^t i : U^* \to V^*$ は全射である.
6. ${}^t i$ は自然な同型 $U^*/V^\perp \xrightarrow{\sim} V^*$, $u^* \bmod V^\perp \mapsto {}^t i(u^*)$ を誘導する. □

[24] $V^\perp$ は V の U^* における**直交補空間 (orthogonal complement)** と呼ばれる. この用語法は計量ベクトル空間における直交補空間の概念を双対空間の場合に一般化したものである.

[25] i は $v \in V$ を $v \in U$ に対応させる写像である.

ヒント. 1. 任意の $u \in U$, $x^* \in (U/V)^*$ に対して, $\langle {}^tp(x^*), u\rangle = \langle x^*, u \bmod V\rangle$ であるから, ${}^tp(x^*) = 0$ ならば $x^* = 0$ である. よって $\mathrm{Ker}\ {}^tp = 0$ である. これで ${}^tp$ は単射であることが示された.

2. 任意の $u^* \in U$, $v \in V$ に対して, $\langle {}^ti(u^*), v\rangle = \langle u^*, v\rangle$ であるから, ${}^ti(u^*) = 0$ と $\langle u^*, v\rangle = 0$ $(v \in V)$ は同値である. これで $\mathrm{Ker}\ {}^ti = V^\perp$ が示された.

3. 任意の $x^* \in (U/V)^*$, $v \in V$ に対して, $\langle {}^ti({}^tp(x^*)), v\rangle = \langle {}^tp(x^*), i(v)\rangle = \langle {}^tp(x^*), v\rangle = \langle x^*, p(v)\rangle = \langle x^*, 0\rangle = 0$ であるから, $\mathrm{Im}\ {}^tp \subset \mathrm{Ker}\ {}^ti$ である. 任意の $u^* \in \mathrm{Ker}\ {}^ti$, $v \in V$ に対して, $0 = \langle {}^ti(u^*), v\rangle = \langle u^*, v\rangle$ であるから, $x^* \in (U/V)^*$ を $\langle x^*, u \bmod V\rangle = \langle u^*, u\rangle$ $(u \in U)$ と定めることができる. そのとき ${}^tp(x^*) = u^*$ であるから, $\mathrm{Ker}\ {}^ti \subset \mathrm{Im}\ {}^tp$ である.

4. ${}^tp : (U/V)^* \to U^*$ は単射であるから, 同型 $(U/V)^* \xrightarrow{\sim} \mathrm{Im}\ {}^tp = \mathrm{Ker}\ {}^ti = V^\perp$ を誘導する.

5. V の U における補空間 W が存在する (問題 **[67]** の結果). $v^* \in V^*$ に対して $u^* \in U^*$ を $\langle u^*, v + w\rangle = \langle v^*, v\rangle$ $(v \in V,\ w \in W)$ と定めると, ${}^ti(u^*) = v^*$ である. よって ${}^ti$ は全射である.

6. 準同型定理を ${}^ti$ に適用すると, 2, 5 より同型 $U^*/V^\perp \xrightarrow{\sim} V^*$, $u^* \bmod V^\perp \mapsto {}^ti(u^*)$ が得られる. □

3 2 次および 3 次正方行列の Jordan 標準形

この節では, 固有値と固有ベクトルについて簡単に説明し, 2 次および 3 次正方行列のジョルダン標準形 (Jordan normal form) の計算の仕方を扱う.

3.1 固有値と固有ベクトル

複素 n 次正方行列 A と複素数 α に対して, 0 でない縦ベクトル u で

$$Au = \alpha u$$

を満たすものが存在するとき, α を A の**固有値 (eigen value)** と呼び, u を A の**固有ベクトル (eigen vector)** と呼ぶ. 行列 A を与えてその固有値と固有ベクトルをすべて求める問題を固有値問題と呼ぶ. 固有値 α に対して,

$$\{\, u \in \mathbb{C}^n \mid Au = \alpha u \,\} = \{\, u \in \mathbb{C}^n \mid (A - \alpha E)u = 0 \,\} = \mathrm{Ker}(A - \alpha E)$$

を α に対応する**固有空間 (eigen space)** と呼ぶ.

複素 n 次正方行列 A と複素数 α に 0 でない縦ベクトル u がある $k = 1, 2, 3, \ldots$ に関して

$$(A - \alpha E)^k u = 0$$

を満たしているとき, u を A の**一般固有ベクトル**と呼ぶ. $(A - \alpha E)^k u = 0$ となる最小の k を取るとき, $k = 1$ ならば u は固有ベクトルになり, $k > 1$ の場合には $v = (A - \alpha E)^{k-1}u$ と置けば v は固有値 α に対する固有ベクトルになる. よって α は A の固有値になる. 行列 A を与えてその固有値と一般固有ベクトルをすべて求める問題を一般固有値問題と呼ぶ. 固有値 α に対して,

$$W(A, \alpha) = \{\, u \in \mathbb{C}^n \mid (A - \alpha E)^k u = 0\ (\exists k = 1, 2, 3, \ldots) \,\}$$

を α に対応する**一般固有空間 (generalized eigen space)** と呼ぶ.

複素 n 次正方行列 A に対して, その**トレース (trace)**, **行列式 (determinant)** をそれぞれ $\operatorname{tr} A$, $\det A = |A|$ と書くことにし, A の**特性多項式 (characteristic polynomial)** $p_A(\lambda)$ を次のように定める:

$$p_A(\lambda) = \det(\lambda E - A).$$

ここで, E は n 次単位行列である. このとき λ に関する n 次方程式 $p_A(\lambda) = 0$ を A の**特性方程式 (characteristic equation)** と呼ぶ.

[106] (簡単過ぎるので 3 点) 複素 2 次正方行列 A の特性多項式 $p_A(\lambda)$ について以下が成立することを直接的な計算によって証明せよ:

(1) $p_A(\lambda) = \lambda^2 - \operatorname{tr}(A)\lambda + \det(A)$.

(2) $p_A(A) = 0$ (2 次正方行列の Cayley-Hamilton の定理). □

参考: この結果は受験数学の勉強でおなじみであろう. 忘れた人は復習して欲しい. 以下の問題の結論のほとんどが一般の n 次正方行列に対して適切に一般化される. Cayley-Hamilton の定理の証明として,

$$p_A(A) = \det(AE - A) = \det(A - A) = \det 0 = 0$$

は**誤り**である.

どこがまずいかを理解するためには記号に騙されないようにしなければいけない. $p_A(A)$ は行列である. $AE - A$ も行列である. しかし $\det(AE - A)$ は数である. $p_A(A) = \det(AE - A)$ という計算は左辺が行列で右辺が数なのでナンセンスである.

しかし, 実は上のナンセンスな計算にかなり近い考え方で Cayley-Hamilton の定理を証明することができる (佐武 [佐武] 137 頁, 杉浦 [杉浦] 65–66 頁). 第 5 節 の前半でその方法を紹介する.

ついでに述べておけば, 「$\det 0$」の 0 は行列のゼロであるが, その次の「$= 0$」の 0 は数のゼロである. この 2 つの「0」は同じ記号で書かれているが意味が違うことに注意しなければいけない. この演習ではベクトルのゼロも単に「0」と書く.

[107] (5 点) 2 つの縦ベクトル $u = {}^t[a, c]$, $v = {}^t[b, d]$ に対して[26], 2 次正方行列 A を

$$A := [u, v] = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

と定める. このとき, 以下の条件は互いに同値であることを直接証明せよ:

(a) A の逆行列が存在する.

(b) $\det(A) \neq 0$.

(c) 任意の $\xi, \eta \in \mathbb{C}$ に対して, $\xi u + \eta v = 0$ ならば $\xi = \eta = 0$. □

[26] ${}^t[\ ]$ は転置を意味している.

解説: このように u と v が一次独立であるという条件 (c) と条件 (a), (b) は同値なのである. もちろん, 同様の結果が n 次正方行列に対しても成立する. 一般の場合を証明するには線形代数の一般論を展開することが自然であるが, $n = 2$ の特殊な場合は直接計算のみで証明することも易しいので, 一度は経験しておくべきである.

[108] (15 点) A は n 次正方行列であるとする. このとき以下の条件は互いに同値である:

(a) A の逆行列が存在する.

(b) $\det A \neq 0$.

(c) A の n 本の列ベクトルは一次独立である.

(d) A の n 本の行ベクトルは一次独立である.

(e) 任意のゼロでない縦ベクトル u に対して $Au \neq 0$. □

ヒント: 線形代数の任意の教科書を参照せよ. なお, この問題の結論はその証明を復習した後では証明抜きで自由に用いて良い. □

[109] (5 点) A は複素 n 次正方行列であり, $p_A(\lambda)$ はその特性多項式であるとする. このとき, 複素数 α が A の固有値であるための必要十分条件は $p_A(\alpha) = 0$ が成立することである. □

ヒント: 問題 **[108]** を $A - \alpha E$ に適用せよ. □

[110] (5 点) 任意の $a, b, c \in \mathbb{C}$ に対して, $a \neq 0$ ならば, ある $\alpha, \beta \in \mathbb{C}$ で次を満たすものが存在することを厳密に証明せよ:

$$a\lambda^2 + b\lambda + c = a(\lambda - \alpha)(\lambda - \beta). \quad \square$$

参考: これは 2 方程式に関する結果だが, 同様のことが任意の複素係数 n 次代数方程式に対して成立する (代数学の基本定理). これ以後この演習では代数学の基本定理を証明抜きで自由に用いて良いことにする. (代数学の基本定理には様々な証明の仕方がある. おそらく複素函数論の授業で証明の仕方の一つを習うことになるだろう.) □

3.2 2 次正方行列の Jordan 標準形と指数函数の計算の仕方

[111] (簡単だが一度はやるべき問題なので 10 点) 行列 B を次のように定める:

$$B = \begin{bmatrix} 7 & 2 \\ -8 & -1 \end{bmatrix}.$$

可逆な行列 P と数 α で $P^{-1}BP = \begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}$ をみたすものを求めよ. □

略解とコメント. B の固有多項式は $(\lambda-3)^2$ なので Cayley-Hamilton の定理より $(B-3E)^2=0$. よって $v=\begin{bmatrix}0\\1\end{bmatrix}$ と置き, $u=(B-3E)v=(B-3E$ の第 2 列$)=\begin{bmatrix}2\\-4\end{bmatrix}$ と置くと, $(B-3E)u=(B-3E)^2v=0$. そのとき

$$Bu=3u, \qquad Bv=u+3v.$$

すなわち $P=[u,v]=\begin{bmatrix}2&0\\-4&1\end{bmatrix}$ と置くと $P^{-1}BP=\begin{bmatrix}3&1\\0&3\end{bmatrix}$.

コメント. 2 次や 3 次の正方行列の Jordan 標準形への相似変換の計算は Cayley-Hamilton の定理を使うと楽にできる. □

[112] (10 点) 複素 2 次正方行列 A の特性方程式 $p_A(\lambda)=0$ の解を α, β と書くことにする. $\alpha\neq\beta$ であるとき, 以下が成立する:

(1) $A\neq\alpha E$ かつ $A\neq\beta E$.

(2) 行列 $A-\beta E$ の 0 でない列ベクトルの 1 つを u と書き[27], 行列 $A-\alpha E$ の 0 でない列ベクトルの 1 つを v と書くことにする. このとき次が成立する:

$$Au=\alpha u, \qquad Av=\beta v.$$

(ヒント: $Au=\alpha u$ と $(A-\alpha E)u=$ は同値である. この考え方は今後自由に使われる. Cayley-Hamilton の定理より $(A-\alpha E)(A-\beta E)=0$ であるが, その等式を $A-\alpha E$ が $A-\beta E$ の 2 本の列ベクトルに作用する式とみなしてみよ. この考え方も今後頻繁に用いられる.)

(3) 2 次正方行列 P を $P:=[u,v]$ と定めると[28], P は逆行列を持つ.

(4) 次が成立する:

$$P^{-1}AP=\begin{bmatrix}\alpha&0\\0&\beta\end{bmatrix}.$$

(5) 任意の $k=1,2,3,\ldots$ に対して,

$$A^k=P\begin{bmatrix}\alpha^k&0\\0&\beta^k\end{bmatrix}P^{-1}.$$

(6) 任意の $t\in\mathbb{C}$ に対して,

$$e^{At}=P\begin{bmatrix}e^{\alpha t}&0\\0&e^{\alpha t}\end{bmatrix}P^{-1}. \quad \square$$

---

[27]行列 $X=\begin{bmatrix}a&b\\c&d\end{bmatrix}$ に対して, ベクトル $\begin{bmatrix}a\\c\end{bmatrix}$, $\begin{bmatrix}b\\d\end{bmatrix}$ を X の列ベクトルと呼ぶ. $X\neq0$ ならば列ベクトルの少なくともいずれか片方は 0 ではない.

[28]縦ベクトル $u=\begin{bmatrix}a\\c\end{bmatrix}$, $v=\begin{bmatrix}b\\d\end{bmatrix}$ に対して, $[u,v]=\begin{bmatrix}a&b\\c&d\end{bmatrix}$ であると考えよ.

[113] (15 点) 2 次正方行列 A の特性方程式 $p_A(\lambda)=0$ が重解 α を持ち, $A\neq\alpha E$ であると仮定する. このとき, 以下が成立する:

(1) 行列 $A-\alpha E$ の 0 でない列ベクトルの 1 つを u と書くことにする. このとき, $Au=\alpha u$ が成立する. (ヒント: $(A-\alpha E)(A-\alpha E)=0$.)

(2) ある縦ベクトル v で $(A-\alpha E)v=u$ を満たすものが存在する. (ヒント: u が $A-\alpha E$ の左側の列ベクトルならば $v={}^t[1,0]$ とし, 右側の列ベクトルならば $v={}^t[0,1]$ とすれば良い.)

(3) $P:=[u,v]$ と置くと P は逆行列を持つ. (ヒント: u と v の一次結合に $A-\alpha E$ を作用させてみよ.)

(4) 次が成立する:

$$P^{-1}AP=\begin{bmatrix}\alpha & 1\\ 0 & \alpha\end{bmatrix}.$$

(5) 任意の $k=1,2,3,\ldots$ に対して,

$$A^k=P\begin{bmatrix}\alpha^k & k\alpha^{k-1}\\ 0 & \alpha^k\end{bmatrix}P^{-1}.$$

(6) 任意の $t\in\mathbb{C}$ に対して,

$$e^{At}=P\begin{bmatrix}e^{\alpha t} & te^{\alpha t}\\ 0 & e^{\alpha t}\end{bmatrix}P^{-1}.\quad\square$$

以上によって, 複素 2 次正方行列 A に対して, 正則行列 P をうまくとって, $P^{-1}AP$ を次のどちらかの形にできることがわかった:

$$\begin{bmatrix}\alpha & 0\\ 0 & \beta\end{bmatrix},\qquad\begin{bmatrix}\alpha & 1\\ 0 & \alpha\end{bmatrix}.$$

この結果は任意の複素 n 次正方行列 (より一般には代数閉体上の n 次正方行列) に拡張される (Jordan 標準型の理論).

3.3 2 次正方行列の Jordan 標準形の計算と応用

[114] (5 点) 行列 $A=\begin{bmatrix}0 & 4\\ -1 & 4\end{bmatrix}$ の固有値と固有ベクトルをすべて求めよ. $\square$

略解: $p_A(\lambda)=(\lambda-2)^2$ かつ $A\neq 2E$. よって固有値は 2 だけ. 固有ベクトルとして $A-2E$ の列ベクトルが取れる. $\square$

[115] (小問各 5 点) 以下の行列の k 乗を求めよ $(k=1,2,3,\ldots)$:

$$(1)\quad\begin{bmatrix}1 & 2\\ 2 & 4\end{bmatrix},\qquad(2)\quad\begin{bmatrix}1 & 3\\ 1 & -1\end{bmatrix},\qquad(3)\quad\begin{bmatrix}1 & -1\\ 1 & 3\end{bmatrix},\qquad(4)\quad\begin{bmatrix}5 & 1\\ -1 & 3\end{bmatrix}.\quad\square$$

ヒント: 問題 [**106**], [**112**], [**113**] の結果を使うことを考えよ. □

略解:

(1) $\begin{bmatrix}1&2\\2&4\end{bmatrix}^2 = 5\begin{bmatrix}1&2\\2&4\end{bmatrix}$ より, $\begin{bmatrix}1&2\\2&4\end{bmatrix}^k = 5^{k-1}\begin{bmatrix}1&2\\2&4\end{bmatrix}$.

(2) $\begin{bmatrix}1&3\\1&-1\end{bmatrix}^2 = 4E$ を用いて k の偶奇で場合分けするか, 問題 [**112**] の結果を用いて,

$$\begin{bmatrix}1&3\\1&-1\end{bmatrix}^k = \begin{bmatrix}3&-1\\1&1\end{bmatrix}\begin{bmatrix}2^k&0\\0&(-2)^k\end{bmatrix}\frac{1}{4}\begin{bmatrix}1&1\\-1&3\end{bmatrix} = \frac{1}{4}\begin{bmatrix}3\cdot 2^k+(-2)^k & 3\cdot 2^k-3\cdot(-2)^k\\ 2^k-(-2)^k & 2^k+3\cdot(-2)^k\end{bmatrix}.$$

(3) 問題 [**113**] の結果を用いて,

$$\begin{bmatrix}1&-1\\1&3\end{bmatrix}^k = \begin{bmatrix}-1&1\\1&0\end{bmatrix}\begin{bmatrix}2^k&k\cdot 2^{k-1}\\0&2^k\end{bmatrix}\begin{bmatrix}0&1\\1&1\end{bmatrix} = \begin{bmatrix}2^k-k\cdot 2^{k-1} & -k\cdot 2^{k-1}\\ k\cdot 2^{k-1} & 2^k+k\cdot 2^{k-1}\end{bmatrix}.$$

(4) 問題 [**113**] の結果を用いて,

$$\begin{bmatrix}5&1\\-1&3\end{bmatrix}^k = \begin{bmatrix}1&0\\-1&1\end{bmatrix}\begin{bmatrix}4^k&k\cdot 4^{k-1}\\0&4^k\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix} = \begin{bmatrix}4^k+k\cdot 4^{k-1} & k\cdot 4^{k-1}\\ -k\cdot 4^{k-1} & 4^k-k\cdot 4^{k-1}\end{bmatrix}.$$

以上の式が実際に正しいことを $k=1,2,3$ の場合に確かめてみよ. □

[**116**] **(20 点)** 次の微分方程式の初期値問題を解け:

$$\begin{aligned}&\ddot{x} = -2x+y, && x(0)=-1, && \dot{x}(0)=1,\\ &\ddot{y} = x-2y, && y(0)=1, && \dot{y}(0)=1.\end{aligned}$$

ここで, $\dot{x}$, $\ddot{x}$, etc は t による導函数 dx/dt, d^2x/dt^2, etc を表わしているものとする. □

ヒント: 縦ベクトル値函数 u を $u = {}^t[x,y]$ と定め, 行列 A を $A = \begin{bmatrix}-2&1\\1&-2\end{bmatrix}$ と定め, 縦ベクトル u_0, u_1 を $u_0 = {}^t[-1,1]$, $u_1 = {}^t[1,1]$ と定めると, 問題の方程式は次のように書き直される:

$$\ddot{u} = Au, \qquad u(0)=u_0, \qquad \dot{u}(0)=u_1.$$

このとき, 可逆行列 P を用いて, $u=Pv$ と置くと, この方程式は次のように変形される:

$$\ddot{v} = P^{-1}APv, \qquad v(0)=P^{-1}u_0, \qquad \dot{v}(0)=P^{-1}u_1.$$

問題 [**112**] の方法を使うと, 適当な P を見付けて $P^{-1}AP$ を実対角行列にできることがわかる. (実は, P として直交行列がとれることもわかる.) その対角成分は負であるので, 問題は次の形の微分方程式を解くことに帰着されることがわかる:

$$\ddot{z} = -\alpha^2 z, \qquad z(0)=a, \qquad \dot{z}(0)=\alpha b \qquad (\alpha>0).$$

この方程式の解は $z = a\cos\alpha t + b\sin\alpha t$ である. □

略解: $P = \dfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ と置くと, P は直交行列 (すなわち $P^{-1} = {}^tP$) でかつ, $P^{-1}AP = \begin{bmatrix} -1 & 0 \\ 0 & -3 \end{bmatrix}$. よって, $\begin{bmatrix} x \\ y \end{bmatrix} = P\begin{bmatrix} X \\ Y \end{bmatrix}$ と置くと, 問題の方程式は次の方程式に変換される:

$$\ddot{X} = -X, \qquad X(0) = 0, \qquad \dot{X}(0) = \sqrt{2},$$
$$\ddot{Y} = -Y, \qquad Y(0) = \sqrt{2}, \qquad \dot{Y}(0) = 0.$$

これを解くと,

$$X = \sqrt{2}\sin t, \qquad Y = \sqrt{2}\cos\sqrt{3}t.$$

よって, x, y は

$$x = \sin t - \cos\sqrt{3}t, \qquad y = \sin t + \cos\sqrt{3}t.$$

となる. □

3.4 3 次以上の正方行列の特性多項式

[117] (5 点) A は n 次正方行列であり, α はその固有値であり, u は対応する固有ベクトルであるとする. このとき, 文字 λ の任意の多項式 $f(\lambda)$ に対して $f(A)u = f(\alpha)u$ が成立する. □

ヒント: たとえば $f(\lambda) = \lambda^k$ のとき $f(A)u = A^k u = \alpha^k u$. □

[118] (8 点) 複素 3 次正方行列 $A = [a_{ij}]$ の特性多項式 $p_A(\lambda)$ に対して以下が成立することを直接的な計算によって証明せよ:

(1) $p_A(\lambda) = \lambda^3 - \mathrm{tr}(A)\lambda^2 + b\lambda - \det(A)$. ここで,

$$\mathrm{tr}(A) = a_{11} + a_{22} + a_{33},$$
$$b = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix},$$
$$\det(A) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}.$$

(2) $p_A(A) = 0$ (3 次正方行列の Cayley-Hamilton の定理). □

[119] (20 点) 複素 n 次正方行列 $A = [a_{ij}]$ の特性多項式を

$$p_A(\lambda) = \lambda^n - s_1\lambda^{n-1} + s_2\lambda^{t-2} + \cdots + (-1)^n s_n$$

と書くとき,

$$s_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \begin{vmatrix} a_{i_1 i_1} & \cdots & a_{i_1 i_k} \\ \vdots & & \vdots \\ a_{i_k i_1} & \cdots & a_{i_k i_k} \end{vmatrix}. \quad \square$$

解説: この問題の結論は上の問題 [118] (1) の一般化になっている. □

3.5 3 次正方行列の Jordan 標準形の求め方

以下の問題 [**120**], . . . , [**124**] を解く前に [**125**] を先に解いて感じをつかんでおいた方が良いかもしれない.

[**120**] **(10 点)** 複素 3 次正方行列 A が互いに異なる 3 つの固有値 α, β, γ を持つとき, 以下が成立する:

(1) $(A-\alpha E)(A-\beta E)\neq 0$ かつ $(A-\alpha E)(A-\gamma E)\neq 0$ かつ $(A-\beta E)(A-\gamma E)\neq 0$. (ヒント: γ に対応する固有ベクトルに $(A-\alpha E)(A-\beta E)$ を作用させると 0 にならないことがわかる.)

(2) $(A-\beta E)(A-\gamma E)$ の 0 でない列ベクトルの 1 つを u と書き, $(A-\alpha E)(A-\gamma E)$ の 0 でない列ベクトルの 1 つを v と書き, $(A-\alpha E)(A-\beta E)$ の 0 でない列ベクトルの 1 つを w と書くことにする. このとき次が成立する:

$$Au=\alpha u,\quad Av=\beta v,\quad Aw=\gamma w.$$

(ヒント: $(A-\alpha E)(A-\beta E)(A-\gamma E)=0$)

(3) 3 次正方行列 P を $P:=[u,v,w]$ と定めると P は逆行列を持つ.

(4) 次が成立する:

$$P^{-1}AP=\begin{bmatrix}\alpha & 0 & 0\\ 0 & \beta & 0\\ 0 & 0 & \gamma\end{bmatrix}.\quad \square$$

[**121**] **(15 点)** 複素 3 次正方行列 A の特性多項式 $p_A(\lambda)$ は

$$p_A(\lambda)=(\lambda-\alpha)^2(\lambda-\gamma),\qquad \alpha\neq\gamma$$

という形をしており,

$$(A-\alpha E)(A-\gamma E)\neq 0$$

が成立していると仮定する. このとき, 以下が成立する:

(1) $(A-\alpha E)^2\neq 0$. (ヒント: γ に対応する固有ベクトルに $(A-\alpha E)^2$ を作用させると 0 にならないことがわかる.)

(2) $(A-\alpha E)(A-\gamma E)$ の 0 でない列ベクトルの 1 つを u と書き, $(A-\alpha E)^2$ の 0 でない列ベクトルの 1 つを w と書くことにする. このとき次が成立する:

$$Au=\alpha u,\qquad Aw=\gamma w.$$

(3) $A-\gamma E$ の 0 でない列ベクトル v で $u=(A-\alpha E)v$ を満たすものが存在する.

(4) 3 次正方行列 P を $P:=[u,v,w]$ と定めると P は逆行列を持つ.

(5) 次が成立する:

$$P^{-1}AP=\begin{bmatrix}\alpha & 1 & 0\\ 0 & \alpha & 0\\ 0 & 0 & \gamma\end{bmatrix}.\quad \square$$

[122] (15 点) 複素 3 次正方行列 A の特性多項式 $p_A(\lambda)$ は

$$p_A(\lambda) = (\lambda - \alpha)^2(\lambda - \gamma), \qquad \alpha \neq \gamma$$

という形をしており,

$$(A - \alpha E)(A - \gamma E) = 0$$

が成立していると仮定する. このとき, 以下が成立する:

(1) $A - \alpha E$ の 0 でない列ベクトル w を取れる.

(2) $A - \gamma E$ の 2 つの列ベクトル u, v で一次独立なものを取れる. (ヒント: もしもそうでないならば $\mathrm{rank}(A - \gamma E) = 1$ となる. したがって γ に対応する固有空間の次元は $3 - \mathrm{rank}(A - \gamma E) = 2$ になる. そのとき, 特性多項式 $p_A(\lambda)$ は $(\lambda - \gamma)^2$ で割り切れるので最初の仮定に反する.)

(3) 3 次正方行列 P を $P := [u, v, w]$ と定めると P は逆行列を持つ.

(4) 次が成立する:

$$P^{-1}AP = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \gamma \end{bmatrix}. \quad \square$$

[123] (15 点) 複素 3 次正方行列 A の特性多項式 $p_A(\lambda)$ は

$$p_A(\lambda) = (\lambda - \alpha)^3$$

という形をしており,

$$(A - \alpha E)^2 \neq 0$$

が成立していると仮定する. このとき, 以下が成立する:

(1) $(A - \alpha E)^2$ の 0 でない列ベクトルの 1 つを u とすると, ある縦ベクトル w で $u = (A - \alpha E)^2 w$ を満たすものが存在する. $v = (A - \alpha E)w$ と置く.

(2) 3 次正方行列 P を $P := [u, v, w]$ と定めると P は逆行列を持つ.

(3) 次が成立する:

$$P^{-1}AP = \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{bmatrix}. \quad \square$$

[124] (15 点) 複素 3 次正方行列 A の特性多項式 $p_A(\lambda)$ は

$$p_A(\lambda) = (\lambda - \alpha)^3$$

という形をしており,

$$A \neq \alpha E, \qquad (A - \alpha E)^2 = 0$$

が成立していると仮定する. このとき, 以下が成立する:

(1) $A-\alpha E$ の 0 でない列ベクトルの1つを u とする. ある縦ベクトル v で $(A-\alpha E)v = u$ を満たすものが存在する.

(2) u と一次独立な縦ベクトル w で $Aw = \alpha w$ を満たすものが存在する. (ヒント: もしもそうでなければ $3 - \mathrm{rank}(A-\alpha) = 1$ である. しかし, $(A-\alpha E)^2 = 0$ より $2(3 - \mathrm{rank}(A-\alpha E)) \geq 3$ であるから, 矛盾する.)

(3) 3 次正方行列 P を $P := [u, v, w]$ と定めると P は逆行列を持つ.

(4) 次が成立する:

$$P^{-1}AP = \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{bmatrix}. \quad \square$$

以上によって, 複素 3 次正方行列 A に対して, 正則行列 P をうまくとって, $P^{-1}AP$ を次のどれかの形にできることがわかった:

$$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix}, \qquad \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \gamma \end{bmatrix}, \qquad \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{bmatrix}.$$

すなわち, 複素 3 次正方行列は上の形の行列のどれかに相似である. この形の行列を **Jordan 標準形**と呼ぶ.

この結果は任意の複素 n 次正方行列 (より一般には代数閉体上の n 次正方行列) に対して拡張される (Jordan 標準型の理論). 以上の $n = 3$ の場合でもまだわかり難いかもしれないが, 任意の複素 n 次正方行列 A は問題 [**132**] の $J = J(k, \alpha)$ の形の行列を対角線に並べた行列と相似になることを証明できる. A と相似な J の形の行列を対角線に並べた行列を A の **Jordan 標準形** と呼ぶ. J の形の行列を並べる順序だけが違う Jordan 標準形は同じものだとみなす. 二つの複素 n 次正方行列 (より一般には代数閉体上の二つの n 次正方行列) が互いに相似であるための必要十分条件は同じ Jordan 標準形を持つことであることが講義の方で証明されることになる.

[**125**] **(小問各 8 点)** 以下の行列の Jordan 標準形と標準形に相似変換する行列を求めよ:

$$(1) \quad A = \begin{bmatrix} -1 & 0 & 0 \\ -5 & 2 & 3 \\ -1 & 0 & -1 \end{bmatrix}, \qquad (2) \quad B = \begin{bmatrix} 3 & 0 & -1 \\ 1 & 4 & -7 \\ 0 & 1 & -1 \end{bmatrix}. \quad \square$$

ヒント: (1) $p_A(\lambda) = (\lambda+1)^2(\lambda-2)$ でかつ $(A+E)(A-2E) \neq 0$ なので問題 [**121**] を使えば良い. (2) $p_B(\lambda) = (\lambda-2)^3$ でかつ $(A-2E)^2 \neq 0$ なので問題 [**123**] を使えば良い.

略解: 計算結果は次のようになる:

$$(1) \quad A = PJP^{-1}, \quad P = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & -1 \\ -1 & 1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

$$(2) \quad B = QKQ^{-1}, \quad Q = \begin{bmatrix} 1 & 1 & 1 \\ 3 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}. \quad \square$$

4 行列の指数函数

複素 n 次正方行列 A の指数函数 $\exp A = e^A$ を次のように定める:

$$\exp A = e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k = E + A + \frac{1}{2}A^2 + \frac{1}{3!}A^3 + \frac{1}{4!}A^4 + \cdots .$$

ここで E は単位行列である. この演習では, この定義の無限級数が複素正方行列 A に関して広義一様絶対収束するという事実や A の成分に関する偏微分を項別微分によって計算できるという事実などを証明抜きで自由に用いて良い. 無限級数の収束性などについては気にせずに形式的な計算を自由に行なって良い.

この演習の主要な目標の一つは具体的に与えられた正方行列 A に対して e^{At} を計算できるようになることである.

他にも様々な目標があるが, この演習を受講する人はこの目標を常に頭の片隅に置いておくことが望ましい.

4.1 行列の指数函数の基本性質

[126] (8 点) A は複素正方行列であるとする. このとき, 複素数 t の行列値函数 e^{At} は次を満たしている:

$$\frac{d}{dt}e^{At} = Ae^{At} = e^{At}A, \qquad e^{A0} = E. \quad \square$$

[127] (8 点) A, P は複素 n 次正方行列であり, P は逆行列を持つと仮定する. このとき,

$$e^{PAP^{-1}} = Pe^AP^{-1}. \quad \square$$

[128] (15 点) 2 つの複素 n 次正方行列 A, B が互いに可換[29]ならば,

$$e^{A+B} = e^Ae^B = e^Be^A. \quad \square$$

ヒント: $AB = BA$ であれば次の二項定理を利用できる:

$$(A+B)^k = \sum_{i=0}^{k} \binom{k}{i} A^iB^{k-i}.$$

ここで,

$$\binom{k}{i} = \frac{k!}{i!(k-i)!}. \quad \square$$

注意: 可換性の仮定は本質的である. その条件を外すとこの問題の結論は一般に成立しなくなる. $\square$

[129] (15 点) $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ と $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ に対して e^{At+Bs}, $e^{At}e^{Bs}$, $e^{Bs}e^{At}$ は互いに異なる. $\square$

ヒント: $e^{At} = \begin{bmatrix} e^t & 0 \\ 0 & e^{-t} \end{bmatrix}$, $e^{Bs} = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}$, $e^{At+Bs} = \begin{bmatrix} e^t & st^{-1}\sinh t \\ 0 & e^{-t} \end{bmatrix}$. $\square$

[29] A と B が**可換 (commutative)** であるとは $AB = BA$ が成立することである.

4.2 簡単に計算できる行列の指数函数の例

[130] (15 点) 複素正方行列 A, B, C を次のように定義する:

$$A = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}, \quad B = \begin{bmatrix} \alpha & 1 \\ 0 & \alpha \end{bmatrix}, \quad C = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

ここで $\alpha, \beta \in \mathbb{C}$ である. e^{At}, e^{Bt}, e^{Ct} を計算せよ. $e^{C(t+s)} = e^{Ct}e^{Cs}$ から三角函数の加法公式を導け. □

[131] (簡単なので 5 点) A は複素 m 次正方行列であり, B は複素 n 次正方行列であるとし, $m+n$ 次正方行列 X を $X = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ と定める. このとき, $e^X = \begin{bmatrix} e^A & 0 \\ 0 & e^B \end{bmatrix}$. □

[132] (15 点) 複素数 α に対して k 次正方行列 $J = J(k, \alpha)$ を次のように定める:

$$J = J(k,\alpha) = \begin{bmatrix} \alpha & 1 & & 0 \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{bmatrix} \quad (k \text{ 次正方行列}).$$

この形の行列を **Jordan ブロック**と呼ぶ. e^{Jt} を計算せよ. □

ヒント: 対角成分の一つ右上に 1 が並び他の成分が 0 の n 次正方行列を N と書くと, $J = \alpha E + N$ である. αE と N は互いに可換なので, **[128]** より,

$$e^{Jt} = e^{\alpha t E}e^{tN} = e^{\alpha t}e^{tN}.$$

よって, e^{tN} を計算すれば良い. □

4.3 定数係数線形常微分方程式と定数係数線形差分方程式への応用

函数 f に対して,

$$a_n(x)f^{(n)} + a_{n-1}(x)f^{(n-1)} + \cdots + a_2(x)f'' + a_1(x)f' + a_0(x)f$$

を対応させる微分作用素を

$$a_n(x)\partial^n + \cdots + a_2(x)\partial^2 + a_1(x)\partial + a_0(x)$$

と書くことにする. 例えば,

$$\begin{aligned}
&\partial f = df/dx = f', \\
&(\partial^2 + a(x))f = f'' + a(x)f, \\
&(\partial + a(x))(\partial + b(x))f = (\partial + a(x))(f' + b(x)f) \\
&\quad = f'' + (b(x)f)' + a(x)(f' + b(x)f) = f'' + (a(x) + b(x))f' + (b'(x) + a(x)b(x))f.
\end{aligned}$$

[133] (25 点) 次の線形常微分方程式の解空間を求めよ:

$$(\partial - \alpha_1)^{k_1} \cdots (\partial - \alpha_m)^{k_m} u = 0.$$

ここで, $\alpha_1, \ldots, \alpha_m$ は互いに異なる複素数であり, $k_1, \ldots, k_m$ は正の整数であるとする. □

ヒント: 公式 $\partial(e^{\alpha x} f) = e^{\alpha x}(\partial + \alpha) f$ より, $(\partial - \alpha)^k (e^{\alpha x} f) = e^{\alpha x} \partial^k f$ が成立することがわかる. これより, 線形常微分方程式

$$(\partial - \alpha)^k u = 0 \qquad (*)$$

の任意の解は

$$u = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) e^{\alpha x}, \qquad a_i \text{ は定数}$$

と表わされることがわかる. なお, 上の問題を解くために, 問題の方程式の解の全体が自然に $(k_1 + \cdots + k_m)$ 次元のベクトル空間をなすという結果を用いて良い. □

参考: $v_0, v_1, \ldots, v_{k-1}$ を $v_j = (\partial - \alpha)^j u \quad (j = 0, 1, \ldots, k-1)$ と定め,

$$v = \begin{bmatrix} v_0 \\ \vdots \\ v_{k-1} \end{bmatrix}, \quad J = \begin{bmatrix} \alpha & 1 & & 0 \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{bmatrix} \quad (k \text{ 次正方行列})$$

と置くと, 方程式 $(*)$ は方程式 $\partial v = Jv$ に変換される. J が Jordan ブロックの形になっていることに注意せよ. 線形常微分方程式 $\partial v = Jv$ の一般解は

$$v = e^{Jx} v_0, \qquad v_0 \text{ は定数ベクトル}$$

と書ける. この結果に問題 **[132]** を適用しても上のヒントの結論が得られる. □

整数 $x \in \mathbb{Z}$ の函数 $f(x)$ に対して, 整数 x の函数

$$x \mapsto a_n(x) f(x+n) + a_{n-1}(x) f(x+n-1) + \cdots + a_1(x) f(x+1) + a_0(x) f(x)$$

を対応させる差分作用素を

$$a_n(x)\sigma^n + a_{n-1}(x)\sigma^{n-1} + \cdots + a_2(x)\sigma^2 + a_1(x)\sigma + a_0(x)$$

と書くことにする. 例えば,

$$\begin{aligned}
&\sigma f(x) = f(x+1), \\
&(\sigma^2 + a(x)) f(x) = f(x+1) + a(x) f(x), \\
&(\sigma + a(x))(\sigma + b(x)) f(x) = (\sigma + a(x))(f(x+1) + b(x) f(x)) \\
&\quad = f(x+2) + b(x+1) f(x+1) + a(x)(f(x+1) + b(x) f(x)) \\
&\quad = f(x+2) + (a(x) + b(x+1)) f(x+1) + (b(x+1) + a(x) b(x)) f(x).
\end{aligned}$$

[134] (25 点) 次の線形差分方程式の解空間を求めよ:

$$(\sigma - \alpha_1)^{k_1} \cdots (\sigma - \alpha_m)^{k_m} u = 0.$$

ここで, $\alpha_1, \ldots, \alpha_m$ は 0 でない互いに異なる複素数であり, $k_1, \ldots, k_m$ は正の整数であるとする. □

ヒント: 公式 $(\sigma-\alpha)(\alpha^x f(x)) = \alpha^{x+1}(\sigma-1)f(x)$ より, $(\sigma-\alpha)^k(\alpha^x f(x)) = \alpha^{x+k}(\sigma-1)^k f(x)$ が成立することがわかる. これより, $\alpha \neq 0$ のとき線形差分方程式

$$(\sigma - \alpha)^k u = 0 \qquad (*)$$

の任意の解は

$$u(x) = (a_0 + a_1 x + a_2 x^{[2]} + \cdots + a_{k-1}x^{[k-1]})\alpha^x, \qquad a_i \text{ は定数}$$

と表わされることがわかる. ここで,

$$x^{[i]} = x(x-1)\cdots(x-i+1)$$

である. $x^{[i]}$ は $(\sigma-1)x^{[i]} = ix^{[i-1]}$ を満たしている. □

参考: $v_0, v_1, \ldots, v_{k-1}$ を $v_j = (\sigma-\alpha)^j u \quad (j = 0, 1, \ldots, k-1)$ と定め,

$$v = \begin{bmatrix} v_0 \\ \vdots \\ v_{k-1} \end{bmatrix}, \quad J = \begin{bmatrix} \alpha & 1 & & 0 \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{bmatrix} \quad (k \text{ 次正方行列})$$

と置くと, 方程式 $(*)$ は方程式 $\sigma v = Jv$ に変換される. J が Jordan ブロックの形になっていることに注意せよ. 線形差分方程式 $\sigma v = Jv$ の一般解は次のようになる:

$$v = J^x v_0, \qquad v_0 \text{ は定数ベクトル}$$

と書ける. この結果を用いて上のヒントの結論を導くこともできる.

対角成分の一つ右上に 1 が並び他の成分が 0 の n 次正方行列を N と書くと, $J = \alpha E + N$ である. αE と N は互いに可換なので, x が 0 以上の整数のとき二項定理が適用できる. $N^k = 0$ であるから,

$$J^x = (\alpha E + N)^x = \sum_{i=0}^{k-1} \binom{x}{i} \alpha^{x-i} N^i.$$

ここで,

$$\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!} = \frac{x^{[i]}}{i!}.$$

これは x が負の整数であっても定義されていることに注意せよ. □

[135] (10 点) 整数 x の函数 u に関する次の線形差分方程式の解空間を求めよ:

$$u(x+2) - 5u(x+1) + 6u(x) = 0. \quad \square$$

ヒント: この問題の方程式は $(\sigma-2)(\sigma-3)u = 0$ と書き直せる. よって, 解は $u(x) = a2^x + b3^x$ の形をしている. □

[136] (10 点) 整数 x の函数 u に関する次の線形差分方程式の解空間を求めよ:

$$u(x+2) - 4u(x+1) + 4u(x) = 0. \quad \square$$

ヒント: この問題の方程式は $(\sigma-2)^2 u = 0$ と書き直せる. よって, 解は $u(x) = 2^x(a+bx)$ の形をしている. □

5 Cayley-Hamilton の定理

以下, 単に「数」「n 次正方行列」を言えば「複素数」「複素 n 次正方行列」であることにする. 体について知っている人は「体 K の元」「K の元を成分に持つ n 次正方行列」であると考えても良い. E は n 次単位行列であるとする.

数を係数とする多項式 $f(\lambda) = \sum_{i=1}^{N} a_i \lambda^i$ と n 次正方行列 A に対して, n 次正方行列 $f(A)$ を次のように定義する:

$$f(A) = \sum_{i=0}^{N} a_i A^i = a_N A^N + a_{N-1} A^{N-1} + \cdots + a_1 A + a_0 E$$

$f(\lambda)$ の定数項 a_0 が $f(A)$ では $a_0 E$ となっていることに注意せよ.

定理 5.1 (Cayley-Hamilton の定理) 任意の n 次正方行列 A とその特性多項式 $p_A(\lambda) = \det(\lambda E - A)$ について $p_A(A) = 0$. □

5.1 Cayley-Hamilton の定理の直接的証明

Cayley-Hamilton の定理の直接的証明: $A = [a_{ij}]$ は n 次正方行列であるとし, その特性多項式を $p_A(\lambda) = \det(\lambda E - A)$ と表わす. $\lambda E - A$ の (i, j) 余因子を $f_{ij}(\lambda)$ と書くと,

$$p_A(\lambda)\delta_{ik} = \sum_{j=1}^{n} f_{ij}(\lambda)(\delta_{kj}\lambda - a_{kj}).$$

この等式の両辺は λ の多項式なので λ に A を代入できる:

$$p_A(A)\delta_{ik} = \sum_{j=1}^{n} f_{ij}(A)(\delta_{kj}A - a_{kj}E).$$

さらにこの等式の両辺を e_k に[30]左から作用させて $k = 1, \ldots, n$ について和を取ると,

$$p_A(A)e_i = \sum_{j=1}^{n} f_{ij}(A)\Big(Ae_j - \sum_{k=1}^{n} a_{kj}e_k\Big) = 0.$$

最後の等号は $Ae_j = \sum_{k=1}^{n} e_k a_{kj}$ から出る. よって $p_A(A) = 0$ である. □

[137] (15 点) 上の証明の細部を埋め, 黒板を用いて詳しく説明せよ. □

Cayley-Hamilton の定理の上のような証明の背後には行列係数の多項式の剰余定理が隠れている. 直接的に行列版の剰余定理を用いることを避けている分だけ証明が簡単になっている.

[30] $e_1, \ldots, e_n$ は K^n の標準的な基底.

5.2 行列係数多項式の剰余定理を用いた証明

以下の証明の方針は杉浦 [杉浦] の 65–66 頁にある.

[138] (行列係数多項式の剰余定理, 20 点) A は n 次正方行列であり, $F(\lambda)$ は n 次正方行列を係数とする λ の多項式であるとする:

$$F(\lambda) = \sum_{i=0}^{N} F_i \lambda^i = \sum_{i=0}^{N} \lambda^i F_i, \qquad F_i \text{ は } n \text{ 次正方行列.}$$

このとき, 以下が成立する:

(1) n 次正方行列 R と n 次正方行列を係数とする λ の多項式 $Q(\lambda)$ で

$$F(\lambda) = Q(\lambda)(\lambda E - A) + R$$

を満たすものが一意に存在し, 次が成立する:

$$R = \sum_{i=0}^{N} F_i A^i.$$

(2) n 次正方行列 R と n 次正方行列を係数とする λ の多項式 $Q(\lambda)$ で

$$F(\lambda) = (\lambda E - A)Q(\lambda) + R$$

を満たすものが一意に存在し, 次が成立する:

$$R = \sum_{i=0}^{N} A^i F_i.$$

(3) 数が係数の任意の多項式 $f(\lambda)$ に対して, $f(A) = 0$ (行列としてゼロ) が成立するための必要十分条件はある n 次正方行列係数の多項式 $G(\lambda)$ で $f(\lambda)E = G(\lambda)(\lambda E - A)$ を満たすものが存在することである.

(4) 数が係数の任意の多項式 $f(\lambda)$ に対して, $f(A) = 0$ (行列としてゼロ) が成立するための必要十分条件はある n 次正方行列係数の多項式 $G(\lambda)$ で $f(\lambda)E = (\lambda E - A)G(\lambda)$ を満たすものが存在することである. □

ヒント: $\lambda E - A$ に関して割り算の筆算の仕方がそのまま成立していることがすぐにわかる. ただし, 行列の積の順序は一般に交換不可能なので右割り算と左割り算の区別をしなければいけないことに注意しなければいけない. たとえば $N = 3$ の場合にその筆算を実行してみよ. 一般の N でも場合も同様であることがすぐに納得できるだろう.

証明の方針は以下の通り. (2), (4) は (1), (3) と同様に証明できるので, (1), (3) のみについて証明の方針を説明する.

(1) の証明の方針: N に関する数学的帰納法によって R, $Q(\lambda)$ の存在を証明する. (帰納法の仮定に R の形に関する仮定も入れておく.) R, $Q(\lambda)$ の一意性を示すために, R_1, $Q_1(\lambda)$ も $F(\lambda) = Q_1(\lambda)(\lambda E - A) + R_1$ を満たしていると仮定する. そのとき, $(Q(\lambda) - Q_1(\lambda))(\lambda E - A) = R_1 - R$ であるから, もしも $Q(\lambda) \neq Q_1(\lambda)$ ならば左辺には λ を含む項が残るが, 右辺は定数行列なので矛盾する. よって, $Q(\lambda) = Q_1(\lambda)$ かつ $R_1 = R$ である.

(3) の証明の方針: $F(\lambda) = f(\lambda)E$ に (1) を適用すれば, ある行列係数の多項式 $Q(\lambda)$ が存在して

$$f(\lambda)E = Q(\lambda)(\lambda E - A) + f(A)$$

が成立する. よって, $f(A) = 0$ ならば $G(\lambda) = Q(\lambda)$ と置けば $f(\lambda)E = G(\lambda)(\lambda E - A)$ を満たす $G(\lambda)$ の存在が示される. 逆に, そのような $G(\lambda)$ が存在するならば, (1) の一意性の主張より $G(\lambda) = Q(\lambda)$ かつ $0 = f(A)$ である. □

参考: 一般に行列係数のモニックな多項式による割り算も同様に可能である. ここで, 行列係数の多項式が**モニック (monic)** であるとは最高次の係数が単位行列であることである.

[139] (15 点) $F(\lambda)$, $A(\lambda)$ は n 次正方行列係数の多項式であり, $A(\lambda)$ はモニックでかつ d 次であるとする (すなわち $A(\lambda)$ の最高次の項は $E\lambda^d$). このとき, n 次正方行列係数の多項式 $Q(\lambda)$ と次数が $d-1$ 以下の n 次正方行列係数の多項式 $R(\lambda)$ で

$$F(\lambda) = Q(\lambda)A(\lambda) + R(\lambda)$$

を満たすものが一意的に存在する. □

[140] (15 点) 問題 **[138]** の (3) または (4) を用いて, Cayley-Hamilton の定理を証明せよ. □

ヒント: 一般に n 次正方行列 X に対して, その (j,i) 余因子を (i,j) 成分に持つ n 次正方行列を Δ と書くと, $\Delta X = X\Delta = \det(X)E$ が成立する. この結果を $X = \lambda E - A$ に適用する. $\lambda E - A$ の (j,i) 余因子を (i,j) 成分に持つ行列を $G(\lambda)$ と書くと, $G(\lambda)(\lambda E - A) = (\lambda E - A)G(\lambda) = p_A(\lambda)E$. □

まとめ: 数を係数とする多項式に関する剰余定理は行列を係数とする多項式に拡張される. 行列版の剰余定理を前提にすれば行列式に関する基本的な結果から Cayley-Hamilton の定理がただちに導かれる.

5.3 正方行列の三角化可能性を用いた証明

Cayley-Hamilton の定理は別のやり方でも証明できる. 以下では最も素朴な方法だと考えられる行列の三角化可能性を用いた証明を紹介しよう.

[141] (10 点) A は対角成分がすべて 0 であるような上三角 n 次正方行列であるとする. このとき $A^n = 0$. □

ヒント: A の (i,j) 成分を a_{ij} と書くと, A に関する仮定は $a_{ij} = 0$ $(j < i+1)$ と同値になる. A^p の (i,j) 成分が $j < i+p$ のとき 0 になることを示せ. $p = 1, 2, 3, \ldots$ に対して A^p を計算するとその 0 でない成分のありかがだんだん右上に移動して行く. □

[142] (複素正方行列の三角化可能性, 20 点) A は複素 n 次正方行列であるとする[31]. A の特性多項式 $p_A(\lambda) = \det(\lambda E - A)$ の互いに異なる根の全体は $\alpha_1, \ldots, \alpha_r$ であり, $p_A(\lambda)$ は次のように表わされているとする:

$$p_A(\lambda) = \det(\lambda E - A) = (\lambda - \alpha_1)^{n_1} \cdots (\lambda - \alpha_r)^{n_r}.$$

[31] 代数閉体の元を成分に持つ行列を考えても良い.

このとき, 正則な複素 n 次正方行列 P で $P^{-1}AP$ が上三角行列になり, しかも $P^{-1}AP$ の対角部分が特性多項式の根を重複を含めて全部並べた $\mathrm{diag}(\alpha_1,\dots,\alpha_1,\dots,\alpha_r,\dots,\alpha_r)$ (各 α_i が n_i 個ずつ順番に並ぶ) に等しくなるものが存在する. □

ヒント. n に関する数学的帰納法. A の固有値 α とそれに付随する固有ベクトル v が存在する. v は単位ベクトルに取れ, v を含む正規直交基底 $p_1 = v, p_2, \dots, p_n$ が取れる. このとき, $P = [p_1 \ \cdots \ p_n]$ と置くと, $P^{-1}AP$ は次の形になる:

$$P^{-1}AP = \begin{bmatrix} \alpha & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{bmatrix}.$$

行列 $B = [b_{ij}]_{2\le i,j\le n}$ に帰納法の仮定を用いよ. □

[143] (15 点) 問題 **[141]**, **[142]** の結果を用いて Cayley-Hamilton の定理を証明せよ. □

ヒント: $p_A(P^{-1}AP) = P^{-1}p_A(A)P$ より, A は問題 **[142]** における $P^{-1}AP$ の形をしていると仮定して良い. A の対角線部分には対角成分がすべて α_i であるような n_i 次の上三角行列が並んでいるとみなせる. よって, $(A-\alpha_j E)^{n_j}$ の対角線部分には対角成分がすべて $(\alpha_i-\alpha_j)^{n_i}$ であるような n_i 次上三角行列が並ぶ. ただし, $i=j$ 番目のブロックは問題 **[141]** の結果より n_j 次の巾零行列になる. 実はこのことだけから $(A-\alpha_j)^{n_j}$ を $j=1,\dots,r$ について掛け合わせると零行列になることを示せる. たとえば $r=4$ の場合は

$$\begin{aligned}
&\begin{bmatrix} 0 & * & * & * \\ & * & * & * \\ & & * & * \\ & & & * \end{bmatrix}\begin{bmatrix} * & * & * & * \\ & 0 & * & * \\ & & * & * \\ & & & * \end{bmatrix}\begin{bmatrix} * & * & * & * \\ & * & * & * \\ & & 0 & * \\ & & & * \end{bmatrix}\begin{bmatrix} * & * & * & * \\ & * & * & * \\ & & * & * \\ & & & 0 \end{bmatrix} \\
=&\begin{bmatrix} 0 & 0 & * & * \\ & 0 & * & * \\ & & * & * \\ & & & * \end{bmatrix}\begin{bmatrix} * & * & * & * \\ & * & * & * \\ & & 0 & * \\ & & & * \end{bmatrix}\begin{bmatrix} * & * & * & * \\ & * & * & * \\ & & * & * \\ & & & 0 \end{bmatrix} \\
=&\begin{bmatrix} 0 & 0 & 0 & * \\ & 0 & 0 & * \\ & & 0 & * \\ & & & * \end{bmatrix}\begin{bmatrix} * & * & * & * \\ & * & * & * \\ & & * & * \\ & & & 0 \end{bmatrix} \\
=&\begin{bmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 0 & 0 \\ & & & 0 \end{bmatrix}. \quad \square
\end{aligned}$$

まとめ: 複素 n 次正方行列[32]の三角化可能性を n に関する帰納法で証明できる. その結果から Cayley-Hamilton の定理がただちに導かれる.

[32] もしくは代数閉体の元を成分に持つ n 次正方行列

比較: 第 5.1 節と第 5.2 節の方法の特徴は特性多項式の根 (固有値) を一切使わずに Cayley-Hamilton の定理を証明できたことである. そのために行列式に関する基本的な結果と (本質的に) 行列係数多項式の剰余定理を用いた. それに対して第 5.3 節では行列係数多項式の剰余定理を用いていないが, 特性多項式の根を本質的に用いている. 特性多項式の根を自由に利用するためには代数学の基本定理[33] が必要になる[34]. どちらの方法も一長一短なので両方覚えておくと良いだろう.

6 最小二乗法

何らかの理由で観測できる量 $x_1, \dots, x_n, y \in \mathbb{R}$ が近似的に

$$y = a_1 x_1 + \cdots + a_n x_n \qquad (a_i \in \mathbb{R} \text{ は定数}) \tag{$*$}$$

の関係で結ばれていることがわかっていると仮定する. そのとき, 実際に観測された量 $x_{i1}, \dots, x_{in}, y_i \in \mathbb{R}$ $(i = 1, \dots, N)$ から係数 $a_1, \dots, a_n \in \mathbb{R}$ を推定するために最小二乗法がよく使われる.

最小二乗法では, 誤差 $a_1 x_{i1} + \cdots + a_n x_{in} - y_i$ $(i = 1, \dots, N)$ の二乗和が最小になるような $a_1, \dots, a_n \in \mathbb{R}$ を求める.

次の節では行列 $X = [x_{ij}] \in M_{N,n}(\mathbb{R})$ の rank が n であるとき, 実際にそのような $a_1, \dots, a_n \in \mathbb{R}$ が一意的に存在することを証明する. ただし証明の細部は演習問題とする. 実際に証明をフォローしてみれば数学科の授業で普通に習っている線形代数学が役に立つことが納得できるだろう.

さらにその次の節では経済学における **Okun の法則 (Okun's law)** を題材に取り, 最小二乗法によって日本経済の Okun 係数を求める. ただし例によって詳しい計算は演習問題とする.

注意 6.1 y と x_i たちの関係式に定数項がある場合

$$y = a_1 x_1 + \cdots + a_n x_n + b \qquad (a_i, b \in \mathbb{R} \text{ は定数})$$

は $a_{n+1} = b$ でかつ x_{n+1} が常に 1 であると仮定すれば $(*)$ の特殊な場合とみなせる. □

6.1 基礎: 最小値の存在と一意性

[144] (実対称行列の対角化, 10 点) P が n 次の実対称行列であるならば, ある n 次直交行列 U で $U^{-1}PU = D$ が実対角行列になるものが存在する. そのとき D の対角成分には P の全ての固有値が重複を込めて並ぶ. 特に実対称行列の固有値はすべて実数であり, $\det P$ は P の固有値全体の積に等しい. □

ヒント. n に関する帰納法で P を直交行列で三角化する. P が対称行列であることより ${}^tPP = P^2 = P\,{}^tP$ が成立するので, その三角化は実は対角化であることがわかる. 別のより洗錬された証明も存在するので, 複数の教科書を見た方が良いだろう. □

[33] 代数学の基本定理とは「1 次以上の複素係数 1 変数多項式は複素数の中に必ず根を持つ」という定理である.

[34] 複素数体の部分体 (例えば実数体や有理数体) の元を成分に持つ行列ではなく, 一般の体 K の元を成分に持つ行列を扱う場合には K 係数多項式の分解体の存在定理が必要になる.

[145] (5 点) P が n 次の実対称行列ならば次の二つの条件は互いに同値である:

(a) P の固有値はすべて正である.

(b) 任意の 0 でないベクトル $v \in \mathbb{R}^n = M_{n,1}(\mathbb{R})$ に対して ${}^t vPv > 0$ となる. □

[146] (5 点) P は n 次の実対称行列であるとし, $q \in \mathbb{R}^n = M_{n,1}(\mathbb{R})$, $r \in \mathbb{R}$ を任意に取り, $a \in \mathbb{R}^n$ の函数 $S(a)$ を次のように定める:

$$S(a) := {}^t aPa + 2\,{}^t qa + r.$$

P の固有値がすべて正ならば $S(a)$ を最小にする $a \in \mathbb{R}^n$ が唯一存在し, 次のように表わされる:

$$a = -P^{-1}q. \quad \square$$

ヒント. $pa^2 - 2qa = p(x - q/p)^2 - q^2/p$ の行列版を考える. ${}^t(a - P^{-1}q)P(a - P^{-1}q)$ を計算してみよ. □

[147] (5 点) 実 $N \times n$ 行列 $X \in M_{N,n}(\mathbb{R})$ を任意に取り, $P = {}^t XX$ と置く. このとき P は n 次の実対称行列であり, P の全ての固有値は 0 以上である. 特に P の全ての固有値が正であるための必要十分条件は $\det P \neq 0$ が成立することである. □

ヒント. P が実対称行列であることはすぐにわかる. 問題 **[144]** の結果より, P は対角化可能であり, その固有値はすべて実数である. $v \in \mathbb{R}^n = M_{n,1}(\mathbb{R})$ に対して ${}^t vPv = {}^t(Xv)Xv \geq 0$. □

[148] (Laplace 展開, 10 点) K は任意の体であるとし, $N > n$ であるとする. 縦長の行列 $X = [x_{ij}] \in M_{N,n}(K)$ と横長の行列 $Y = [y_{ij}] \in M_{n,N}(K)$ について以下が成立する:

$$|YX| = \sum_{1 \leq i_1 < \cdots < i_n \leq N} \begin{vmatrix} y_{1i_1} & \cdots & y_{1i_n} \\ \vdots & & \vdots \\ y_{ni_1} & \cdots & y_{ni_n} \end{vmatrix} \begin{vmatrix} x_{i_1 1} & \cdots & x_{i_1 n} \\ \vdots & & \vdots \\ x_{i_n 1} & \cdots & x_{i_n n} \end{vmatrix}. \quad \square$$

ヒント. $N = n$ の場合の公式 $|YX| = |Y||X|$ の証明の一般化. □

[149] (5 点) K は任意の体であり, $N > n$ であるとし, 縦長の行列 $X = [x_{ij}] \in M_{N,n}(K)$ を任意に取る. このとき X の rank が n であるための必要十分条件はある $i_1, \ldots, i_n$ で $1 \leq i_1 < \cdots < i_n \leq N$ かつ

$$\begin{vmatrix} x_{i_1 1} & \cdots & x_{i_1 n} \\ \vdots & & \vdots \\ x_{i_n 1} & \cdots & x_{i_n n} \end{vmatrix} \neq 0$$

を満たすものが存在することである. □

[150] (最小二乗法, 5 点) $N > n$ であるとし, $X = [x_{ij}] \in M_{N,n}(\mathbb{R})$, $y = [y_i] \in \mathbb{R}^N = M_{N,1}(\mathbb{R})$ を任意に取り, $a = [a_j] \in \mathbb{R}^n = M_{n,1}(\mathbb{R})$ の函数 $S(a)$ を次のように定める:

$$S(a) = {}^t(Xa - y)(Xa - y) = \sum_{i=1}^{N} \left(\sum_{j=1}^{n} a_j x_{ij} - b_i \right)^2.$$

もしも A の rank が n ならば $S(a)$ を最小にする $a \in \mathbb{R}^n$ が唯一存在し, 次のように表わされる:

$$a = \left({}^t XX\right)^{-1} {}^t Xy. \quad \square$$

ヒント. 以上の問題を総合すれば簡単に証明できる. □

6.2 応用: Okun の法則

ほとんどの国では経済成長率と失業率の変化の間に次の形のかなり安定した関係が成立している:

$$(\text{経済成長率}) = -\alpha(\text{失業率の変化}) + \beta \qquad (\alpha, \beta \text{ は正の定数})$$

この結果は経済学者の Arthur Okun によって 1960 年代に発見されたので, **Okun の法則 (Okun's law)** と呼ばれている. α は **Okun 係数**と呼ばれており, たとえば $\alpha = 3$ ならば失業率が 1% 増えると経済成長率はその 3 倍の 3% 減少することになる.

Okun の法則は**潜在成長率** (持続可能な自然な経済成長率) を求めるためによく使われる. 失業率はマイナスにはなれないので, 失業率を減らしながらの経済成長はいつかは不可能になってしまう. 逆に失業率を毎年増やしながらの経済成長も持続不可能だろう. したがって持続可能な経済成長率は失業率の変化をゼロにするような成長率であると考えられる. すなわち

$$(\text{Okun の法則から推定した潜在成長率}) = \beta.$$

これはかなり大雑把な推定であるが, Okun の法則は複雑な経済の世界で珍しいことにかなり安定しているので現実の政策を考えるときには非常に役に立つ. 潜在成長率を達成できなかった中央政府と中央銀行は経済政策に失敗した可能性が相当に高い. (Okun の法則によって潜在成長率の達成に失敗すると失業率が上昇してしまうことに注意せよ.)

歴年	失業率 (%)	失業率の変化 (%)	経済成長率 (%)
1988	2.5		
1989	2.3	−0.2	5.3
1990	2.1	−0.2	5.2
1991	2.1	0.0	3.4
1992	2.2	0.1	1.0
1993	2.5	0.3	0.2
1994	2.9	0.4	1.1
1995	3.2	0.3	1.9
1996	3.4	0.2	3.4
1997	3.4	0.0	1.9
1998	4.1	0.7	−1.1
1999	4.7	0.6	0.1
2000	4.7	0.0	2.9
2001	5.0	0.3	0.4
2002	5.4	0.4	−0.5
2003	5.3	−0.1	2.5

表 6.1: 日本の失業率と経済成長率

[151] (日本経済の Okun 係数と潜在成長率の推定, 15 点) 表 6.1 はインターネットからダウンロードした統計データ [失業率], [GDP] から数字をコピーして作成した. 表 6.1 に最小二乗法を適用して日本経済の Okun 係数 α と潜在成長率 β を推定せよ. □

ヒント. $y = $(経済成長率), $n = 2$, $x_1 = $(失業率の変化), $x_2 = 1$, $a_1 = -\alpha$, $a_2 = \beta$, $N = 15$ とみなし, 前節までの結果を用いよ. まず 15×2 行列 X の第 1 列に表 6.1 の失業率の変化を代入し, 第 2 列の成分はすべて 1 であるとする. 次に $y \in \mathbb{R}^{15}$ には表 6.1 の経済成長率を代入する. そして $a = {}^t[-\alpha, \beta]$ を $a = ({}^tXX)^{-1}\,{}^tXy$ によって計算する. 電卓やコンピューターを用いて α, β の近似値を求めよ. □

略解. $\alpha = 6.11034 = $(Okun 係数の推定値), $\beta = 2.98726\% = $(潜在成長率の推定値). 日本経済の潜在成長率は 3% 程度である可能性が高く, 日本政府と日本銀行は経済政策に 10 年以上に渡って失敗し続け, 失業率を 2% 台から 5% に上昇させてしまった. 失業率を 1% 下げるためには潜在成長率よりも 6% も高い経済成長率を必要とする. □

参考文献

[Dirac] ディラック, P. A. M.: 量子力学, 原書第 4 版, 朝永振一郎他共訳, 岩波書店, 1968

[Infeld] インフェルト, L.: ガロアの生涯—神々の愛でし人市井三郎訳, 日本評論社, 新版第 3 版, 1996

[佐武] 佐武一郎: 線型代数学, 裳華房数学選書 1, 324 頁.

[杉浦] 杉浦光夫, Jordan 標準形と単因子論 I, II, 岩波講座基礎数学, 線型代数 iii, 1976

[堀田] 堀田良之: 加群十話 — 代数学入門, 朝倉書店, すうがくぶっくす 3, 186 頁.

[横田] 横田一郎: 群と位相, 裳華房, 基礎数学選書 5

[山内・杉浦] 山内恭彦, 杉浦光雄: 連続群論入門, 培風館, 新数学シリーズ 18

[失業率] 労働力調査　長期時系列データ
`http://www.stat.go.jp/howto/case1/01.htm`
から「第 3 表 (3) 年齢階級 (5 歳階級), 男女別完全失業者数及び完全失業率」
`http://www.stat.go.jp/data/roudou/longtime/zuhyou/lt03-03.xls`
をダウンロード

[GDP] 平成 15 年度国民経済計算
`http://www.esri.cao.go.jp/jp/sna/h17-nenpou/17annual-report-j.html`
から「4. 主要系列表（3）経済活動別国内総生産　実質暦年」
`http://www.esri.cao.go.jp/jp/sna/h17-nenpou/80fcm3r_jp.xls`
をダウンロード