

尾畑伸明著「情報数理の基礎と応用」

問題略解とヒント (2008.07.27)

1 集合と論理

1.1. A の部分集合は, A の各々の元が含まれるかどうかで特定される. その組み合わせ方は $2^{|A|}$ 通りであるので, 部分集合の個数も $2^{|A|}$ である.

1.2. $\emptyset \in \emptyset$ は偽. $\emptyset \subset \emptyset$ は真.

1.3. $\mathbb{Z} \setminus \mathbb{N} = \{0, -1, -2, -3, \dots\}$.

1.4. まず, $X \cap Y = \emptyset$ ならば $|X \cup Y| = |X| + |Y|$ であることに注意する. そうすれば, $(A \setminus B) \cap (A \cap B) = \emptyset$ から

$$|A| = |(A \setminus B) \cup (A \cap B)| = |A \setminus B| + |A \cap B|.$$

よって,

$$|A \setminus B| = |A| - |A \cap B|. \quad (1.1)$$

次に, $(A \setminus B) \cup B = A$ から

$$|A \cup B| = |(A \setminus B) \cup B| = |A \setminus B| + |B|. \quad (1.2)$$

(1.1) と (1.2) をあわせて,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

が得られる.

3つの集合についても同様の考察によって,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

が得られる.

1.5. ベン図を利用せよ.

1.6. (1) 定義からすぐわかる.

(2) $B = A \ominus X$ の両辺で A との対称差集合をとって, (1) の結果を用いると,

$$A \ominus B = A \ominus (A \ominus X) = (A \ominus A) \ominus X = \emptyset \ominus X = X.$$

1.7. 真理値表を作ると,

P	Q	$P \rightarrow Q$	$(P \rightarrow Q) \wedge P$	$((P \rightarrow Q) \wedge P) \rightarrow Q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

真理値がすべて 1 になっているので, $((P \rightarrow Q) \wedge P) \rightarrow Q$ の恒真命題である.

1.8. 真理値表を作ると,

P	Q	$P \rightarrow Q$	$\neg Q$	$P \wedge \neg Q$	$\neg(P \wedge \neg Q)$
1	1	1	0	0	1
1	0	0	1	0	0
0	1	1	0	1	1
0	0	1	1	0	1

$P \rightarrow Q$ と $\neg(P \wedge \neg Q)$ の真理値が一致しているので, それらは同値である.

1.9. 真理値表を作ると,

P	Q	R	$P \rightarrow Q$	$Q \rightarrow R$	$P \rightarrow R$
1	1	1	1	1	1
1	1	0	1	0	0
1	0	1	0	1	1
1	0	0	0	1	0
0	1	1	1	1	1
0	1	0	1	0	1
0	0	1	1	1	1
0	0	0	1	1	1

$P \rightarrow Q$ と $Q \rightarrow R$ がともに真になる場合, $P \rightarrow R$ も真になっていることから, 推論の有効性がわかる.

1.10. $\sqrt{2}$ が既約分数 q/p で表されると仮定して矛盾を導こう. 実際, 2 乗して分母を払えば,

$$2p^2 = q^2 \quad (1.3)$$

を得る. 左辺が 2 の倍数であることは明らか. q が奇数ならば q^2 も奇数なので, q は偶数でなければならない. そこで $q = 2r$ において, (1.3) に代入すれば,

$$2p^2 = 4r^2 \implies p^2 = 2r^2$$

を得る. 同様の議論で, p が偶数になる. そうすると, p, q ともに偶数となり, 互いに素にとったことに矛盾する. したがって, $\sqrt{2}$ を既約分数であらわすことはできない. すなわち, $\sqrt{2}$ は有理数ではなく, 無理数である.

2 写像

2.1. 単射性に注意せよ. f が単射ならば, $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ が成り立つ.

2.2. (1) まず, $x \in X$ に対して, $x \in f^{-1}(B^c) \Leftrightarrow f(x) \in B^c$ に注意して, これを仮定する. $x \in f^{-1}(B)$ とすると, $f(x) \in B$. これと仮定をあわせて, $f(x) \in B^c \cap B = \emptyset$ となり矛盾である. よって, $x \notin f^{-1}(B)$, すなわち, $x \in (f^{-1}(B))^c$. こうして, $f^{-1}(B^c) \subset (f^{-1}(B))^c$. 逆に, $x \in (f^{-1}(B))^c$ とする. $f(x) \in B$ とすると, $x \in f^{-1}(B)$ であり矛盾. よって, $f(x) \notin B$, すなわち, $f(x) \in B^c$. したがって, $x \in f^{-1}(B^c)$. こうして, $(f^{-1}(B))^c \subset f^{-1}(B^c)$ が示された. 定理 2.3(2) を用いてもよい.

(2) $y \in f(f^{-1}(B)) \Leftrightarrow \exists x \in f^{-1}(B) : y = f(x) \Leftrightarrow \exists x \in X : f(x) \in B, y = f(x) \Leftrightarrow y \in B, y \in f(X) \Leftrightarrow y \in B \cap f(X)$

(3) $y \in f(A)^c$ とする. f は全射なので, $y = f(x)$ となる $x \in X$ をとることができる. $x \in A$ ならば, $y = f(x) \in f(A)$ となり, 初めの仮定に矛盾する. したがって, $x \notin A$, すなわち, $x \in A^c$ である. そうすると, $y = f(x) \in f(A^c)$. これは, $f(A)^c \subset f(A^c)$ を示す.

(4) $y \in f(A^c)$ とすると, $y = f(x)$ をみたす $x \in A^c$ がとれる. f は単射なので, すべての $x' \in A$ に対して $y \neq f(x')$ である. つまり, $y \notin f(A)$, 言い換えれば, $y \in f(A)^c$. こうして, $f(A^c) \subset f(A)^c$.

2.3. $\chi_A = \chi_B \Rightarrow \chi_A^{-1}(1) = \chi_B^{-1}(1) \Rightarrow A = B$ により単射. 任意の $\chi \in \{0, 1\}^X$ に対して, $\chi^{-1}(1) = A$ とおけば, $\chi = \chi_A$. よって全射.

2.4. (1) χ_A の値は 0 と 1 だけであることに注意して, $\chi_{A \cap B}(x) = 1 \Leftrightarrow x \in A \cap B \Leftrightarrow \chi_A(x) = \chi_B(x) = 1 \Leftrightarrow \chi_A(x)\chi_B(x) = 1$

(2), (3) も同様.

2.5. (1), (2) は明らか.

(3) たとえば, $f(1) = 1, f(2) = 2, g(1) = g(2) = g(3) = 1$ で定義される写像 $f : \{1, 2\} \rightarrow \{1, 2, 3\}, g : \{1, 2, 3\} \rightarrow \{1\}$ を考えてみよ.

(4) たとえば, $f(1) = 1, f(2) = 2, g(1) = 1, g(2) = g(3) = 2$ で定義される写像 $f : \{1, 2\} \rightarrow \{1, 2, 3\}, g : \{1, 2, 3\} \rightarrow \{1, 2\}$ を考えてみよ.

2.6. (1)

$$\begin{aligned} y \in f\left(\bigcup_{\lambda} A_{\lambda}\right) &\iff \exists x \in \bigcup_{\lambda} A_{\lambda} : y = f(x) \\ &\iff \exists \lambda, \exists x \in A_{\lambda} : y = f(x) \\ &\iff \exists \lambda : y \in f(A_{\lambda}) \\ &\iff y \in \bigcup_{\lambda} f(A_{\lambda}) \end{aligned}$$

他も同様.

2.7. x が 2 通りの異なる無限小数に表されたとして,

$$\begin{aligned} x &= 0.\alpha_1\alpha_2\cdots\alpha_n\cdots \\ &= 0.\beta_1\beta_2\cdots\beta_n\cdots \end{aligned}$$

とする. 小数点以下を順に見てゆき, 第 n 位で初めて異なったとする. つまり,

$$\alpha_1 = \beta_1, \quad \dots, \quad \alpha_{n-1} = \beta_{n-1}, \quad \alpha_n < \beta_n.$$

そうすると, 差をとって, $0 = \sum_{k=n}^{\infty} (\beta_k - \alpha_k)10^{-k}$ となる. 両辺に 10^n をかけて移項すれば,

$$\beta_n - \alpha_n = - \sum_{k=n+1}^{\infty} (\beta_k - \alpha_k)10^{-(k-n)} = - \sum_{k=0}^{\infty} (\beta_{k+n+1} - \alpha_{k+n+1})10^{-(k+1)}$$

を得る. $|\beta_k - \alpha_k| \leq 9$ であるから, 右辺の和の絶対値は ≤ 1 である. これと $\alpha_n < \beta_n$ をあわせると, $\beta_n - \alpha_n = 1$ である. そうすると, $k \geq n+1$ のすべての k に対して, $\beta_k = 0, \alpha_k = 9$ となり, $0.\beta_1\beta_2\cdots$ が有限小数になって矛盾.

2.8. たとえば,

$$f(x) = \tan \pi \left(\frac{x-a}{b-a} - \frac{1}{2} \right)$$

とおけば, $f: (a, b) \rightarrow \mathbb{R}$ が全単射になる.

2.9. (1) $A_n = \{a_{n1}, a_{n2}, \dots\}$ とする (有限でも無限でもよい). $\bigcup_{n=1}^{\infty} A_n$ の元を

$$\begin{array}{cccc} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \dots & \dots & \dots & \dots \end{array}$$

のように配列して, たとえば, 定理 2.13 の証明にあるような順序で番号付けすればよい. A_n のうちに有限集合があっても, この操作は可能ある.

(2) 与えられた線分の集合を A として, A_n を A に属する線分で長さが $1/n$ 以上のものとする. そのような線分は, 長さ 1 の線分上に高々 k 個しか存在しない. よって, $A = \bigcup_{n=1}^{\infty} A_n$ で $|A_n| \leq n$ が成り立つ. (1) の結果から, A は高々可算集合である.

3 関係

3.1. 反射律, 推移律を満たすが, 対称律は満たさない.

3.2. 反射律と対称律は明らか. 推移律は, 一般に $A \ominus C \subset (A \ominus B) \cup (B \ominus C)$ が成り立つことからわかる.

- 3.3. $xy > 0$ または $x = y = 0$ のときに $x \sim y$ とする.
- 3.4. $\max A$ と $\min A$ は存在しない. $\sup A = 180$, $\inf A = 2$.
- 3.5. $\max A$, $\min A$, $\sup A$ は存在しない. $\inf A = 0$. $\max B$ は存在しない. $\sup B = 1$, $\min B = \inf B = 0$.
- 3.6. 極大元は 8 と 12, 極小元は 2 と 3.
- 3.7. A を無限集合として, A 上の選択関数を f とする. $a_1 = f(A)$, $a_2 = f(A \setminus \{a_1\})$, $a_3 = f(A \setminus \{a_1, a_2\})$, ... とし帰納的に A の元の列 $a_1, a_2, a_3, \dots$ が決まる. 集合 $\{a_1, a_2, a_3, \dots\}$ は A の部分集合で, 可算集合である.

4 素因数分解

- 4.1. $S = \{n \in \mathbb{N} \mid \sigma(n) \neq n\}$ とおく. 公理 (2) によって $1 \in S$. $n \in S$ とすると, S の定義から $\sigma(n) \neq n$. 公理 (1) によって, $\sigma(\sigma(n)) \neq \sigma(n)$. よって, $\sigma(n) \in S$. したがって, $\sigma(S) \subset S$. 公理 (3) によって $S = \mathbb{N}$.
- 4.2. $S = \{2^n \mid n \in \mathbb{N} \cup \{0\}\}$
- 4.3. (1) $n = 1$ のときの証明すべき等式は, $a_0 = a_2 - 1$ であるが, これは成り立つことが簡単にわかる. $n \geq 1$ として, n のときの等式の成立を仮定する. この等式の両辺に a_n を加えて, 右辺にフィボナッチ数列の定義を適用すればよい.
- (2) $n = 0$ のとき等式が成り立つことは簡単にわかる. $n \geq 0$ として, n のときの等式の成立を仮定し, 両辺に a_{n+1}^2 を加える. 右辺にフィボナッチ数列の定義を適用すれば, $n + 1$ の場合の等式が得られる.
- 4.4. 円盤の枚数が 1 枚なら, 確かに移動できる. $n \geq 1$ として, n 枚のときに移動する手順が存在すると仮定する. この手順を P とする. さて, 高さ $n + 1$ 枚の塔に対して, 最下層の円盤を無視して, 上の n 枚を手順 P によって, 第 2 の柱に移動することができる (目標の第 3 の柱を補助として使う). その後, 最下層にあった円盤を第 3 の柱に移動する. 再び, 手順 P によって第 2 の柱にある高さ n の塔を第 3 の柱に移動する (第 1 の柱を補助として使う). こうして, 高さ $n + 1$ 枚の塔を目標の柱に移動できたから, 数学的帰納法によって, 任意の高さの塔を移動する手順が存在する.
- 4.5. n を $n \geq a(a - 1)$ を満たす自然数とする. n を a で割って, $n = qa + r$, $0 \leq r < a$, と表すことができる. $n \geq a(a - 1)$ とあわせると, $0 \leq r \leq a - 1 \leq q$ となる. さて, $n = r(a + 1) + (q - r)a$ であるが, $r \geq 0$, $q - r \geq 0$ である. よって, n は a と $a + 1$ を何個かずつ加えたものとして表された. S の仮定から, そのような n は S に属する.
- 4.6. $x = \lfloor x \rfloor + a$, $y = \lfloor y \rfloor + b$, $0 \leq a < 1$, $0 \leq b < 1$, のように表してみよ.
- 4.7. $b = qa + r$, $0 \leq r < a$, とおいてみよ.

4.8. 45 個

4.9. 1111011, 5EB

4.10. $11 \cdots 1$ (n 桁)

4.11. (1) 110001 (2) 111 (3) 10010110 (4) 10010 余り 100

4.12. (1) n と $n+1$ の公約数を a とすれば, $(n+1) - n$ が a の倍数になる. よって $a = 1$ であり, n と $n+1$ は互いに素である.

(2) $n \geq 2$ から, $n, n+1$ ともに素因数をもつが, (1) よりその素因数は相異なる. よって, $n(n+1)$ は少なくとも 2 個の相異なる素因数をもつ. 後は, 同じ議論の繰り返しで示される.

4.13. m を合成数であると仮定し, $m = ab$ ($a \geq 2, b \geq 2$) とおく. $2^m - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1)$ において, 2つの因数はともに 2 以上である. これは, $2^m - 1$ が素数であることに反する.

4.14. 6 と 28 だけ. 次の完全数は 496 である.

4.15. $a = M(M+1)/2 = (2^m - 1) \cdot 2^{m-1}$. 仮定から $2^m - 1$ は素数ゆえ, a の約数は, $(2^m - 1)^\alpha 2^\beta$, $0 \leq \alpha \leq 1, 0 \leq \beta \leq m-1$ の形をしている. それらの和は,

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

よって, a は完全数である.

4.16. $n, n+1, n+2$ のいずれか 1 つは 2 の倍数であり, それと一致するかどうかは別として, いずれか 1 つは 3 の倍数である.

4.17. $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots, b = p_1^{\beta_1} p_2^{\beta_2} \cdots$ のように表示して, 素因数分解の一意性を用いよ.

4.18. $138600 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11$. したがって, $a = 2 \cdot 3 \cdot 5 = 30, b = 2 \cdot 7 \cdot 11 = 154$.

4.19. $1, 2, \dots, n$ のうちで, p^k で割り切れ, p^{k+1} では割り切れないものの個数を a_k とすると, $n!$ の素因数分解に現れる素数 p の個数 e は, $e = a_1 + 2a_2 + 3a_3 + \cdots$ で与えられる. ここで, $b_k = a_k + a_{k+1} + \cdots$ とおくと, $e = b_1 + b_2 + \cdots$ である. 一方, b_k は p^k の倍数の個数であるから $b_k = \left\lfloor \frac{n}{p^k} \right\rfloor$.

4.20. $ac|ab$ から $ab = ack$ となる $k \in \mathbb{N}$ がとれる. $a \neq 0$ であるから, $b = ck$. したがって $c|b$.

4.21. a, b, m を素因数分解して, その一意性を用いよ.

4.22. 55

- 4.23. $3(4x + z) = -7(y - 5)$ と変形すれば, $y - 5 = 3k$ の形が出る. これを代入して整理すれば, $4x + z = -7k$. こうして, $y = 3k + 5$, $z = -4x - 7k$ (x, k は任意の整数).
- 4.24. $ax_0 + by_0 = k$ と与えられた不定方程式との差をとれば, $a(x - x_0) + b(y - y_0) = 0$ を解くことに帰着する. さらに, $a = ga'$, $b = gb'$ とおけば, $a'(x - x_0) + b'(y - y_0) = 0$ が得られる. a' と b' は互いに素であるから, $x - x_0$ は b' の倍数, $y - y_0$ は a' の倍数である. このことから, $x - x_0 = b'u$, $y - y_0 = -a'u$ ($u \in \mathbb{Z}$) が得られる. このような x, y が与えられた不定方程式の解になっていることは見やすい.
- 4.25. 50, 80, 100, 130, 150, 160, 180, 200, 210, 230, 240, 250, 260, 280, 290, 300, 320, 以降 10 円刻みですべて.

5 合同式

5.1. 展開式

$$(a_1 + \cdots + a_n)^p = \sum \frac{p!}{q_1! \cdots q_n!} a_1^{q_1} \cdots a_n^{q_n}$$

を考えよう. ただし, 和は $q_1, \dots, q_n$ を $q_1 + \cdots + q_n = p$ を満たす非負の整数をすべては走らせてとる. p は素数であるから, $0 \leq q_i < p$ であれば, $q_i!$ は p を素因数に含まない. したがって, $q_1, \dots, q_n$ がすべて $< p$ であれば, 右辺の多項係数は p の倍数であり, $\equiv 0 \pmod{p}$. よって, $(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \pmod{p}$.

5.2. まず,

$$3^6 = 27^2 = (31 - 4)^2 = 31^2 - 8 \cdot 31 + 16 \equiv -8 \cdot 31 + 16$$

これを 2 乗して,

$$\begin{aligned} 3^{12} &\equiv (-8 \cdot 31 + 16)^2 \equiv -16 \cdot 16 \cdot 31 + 16^2 \\ &\equiv -8(31 + 1) \cdot 31 + 8 \cdot 32 \equiv -8 \cdot 31 + 8 \cdot 32 = 8 \end{aligned}$$

よって,

$$3^{15} \equiv 3^3 \cdot 8$$

さらに 2 乗して, 初めの式を利用すれば

$$3^{30} \equiv 3^6 \cdot 8^2 \equiv (-8 \cdot 31 + 16)(2 \cdot 31 + 2) \equiv 16 \cdot 31 + 32 = 17 \cdot 31 + 1$$

- 5.3. 10 進法で $n + 1$ 桁の自然数 x の第 k 位の数を a_{k-1} とする. x が 3 の倍数であるための必要十分条件は, $a_0 + a_1 + \cdots + a_n \equiv 0 \pmod{3}$. x が 11 の倍数であるための必要十分条件は, $a_0 - a_1 + \cdots + (-1)^n a_n \equiv 0 \pmod{11}$.
- 5.4. $ac \equiv bc \pmod{m}$ から $(a - b)c = km$ となる整数 k が存在する. c と m が互いに素であるから, $a - b$ は m の倍数である. よって, $a \equiv b \pmod{m}$ が成り立つ.

5.5.

+	-1	0	1	×	-1	0	1
-1	1	-1	0	-1	1	0	-1
0	-1	0	1	0	0	0	0
1	0	1	-1	1	-1	0	1

5.6. 完全剰余系として $\{0, 1, 2, 3, 4, 5\}$ をとれば, 演算表は次のようになる.

+	0	1	2	3	4	5	×	0	1	2	3	4	5
0	0	1	2	3	4	5	0	0	0	0	0	0	0
1	1	2	3	4	5	0	1	0	1	2	3	4	5
2	2	3	4	5	0	1	2	0	2	4	0	2	4
3	3	4	5	0	1	2	3	0	3	0	3	0	3
4	4	5	0	1	2	3	4	0	4	2	0	4	2
5	5	0	1	2	3	4	5	0	5	4	3	2	1

5.7. $a \equiv b \pmod{m}$ なので, $a = qm + r$, $b = q'm + r$ とおける. 一方で, $\text{GCD}(a, m) = \text{GCD}(a - qm, m) = \text{GCD}(r, m)$ であり, b についても同様であるから, $\text{GCD}(a, m) = \text{GCD}(r, m) = \text{GCD}(b, m)$ である.

5.8. $x \equiv 82 \pmod{105}$

5.9. (1) $1 \leq k \leq p^e$ を満たす整数 k が p と互いに素ということは, p の倍数でないことと同値である. よって, $\varphi(p^e)$ は 1 から p^e にある p の倍数でない整数の個数に一致する.

(2) $n = p_1^{e_1} \cdots p_s^{e_s}$ とおくと, 性質 (2) によって, $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_s^{e_s})$. これに性質 (1) を用いて, 式を少し変形すればよい.

5.10. $N = pq = 221$, $\text{GCD}(e, (p-1)(q-1)) = \text{GCD}(5, 192) = 1$ が確かめられる. $5d \equiv 1 \pmod{192}$ を解いて $d \equiv 77 \pmod{192}$. さて, $M = 9$ を暗号化すると $C \equiv M^e = 9^5 \equiv 42 \pmod{221}$. 復号するには, $42^{77} \pmod{221}$ を計算すればよい. $42^2 \equiv -4$, $42^3 \equiv 53$, $42^5 \equiv 9$ などを準備して, $42^{77} \equiv (42^{15})^5 \cdot 42^2 \equiv 9$ が確認できる.

6 群

6.1. $e \circ x = x$ において $x = f$ とおけば, $e \circ f = f$. また, $x \circ f = x$ において $x = e$ とおけば, $e \circ f = e$. したがって, $e = f$ である. そうすれば, すべての $x \in S$ に対して $e \circ x = x \circ e = x$ が成り立ち, e は半群 S の単位元である.

6.2. (1) 単位元 1 をもつ半群である. 0 に逆元がないので群ではない.

(2) 単位元 1 をもつ群である.

6.3. (1) 与えられた写像を f とする. 任意の $y \in G$ に対して $x = a^{-1}y$ とすれば, $f(x) = a(a^{-1}y) = y$ となるから, f は全射. また, $f(x_1) = f(x_2)$ とすれば, $ax_1 = ax_2$. 両辺の左から a^{-1} をかけて $x_1 = x_2$ を得る. よって, f は単射.

(2) (1) と同様,

(3) 与えられた写像を g とする. 任意の $y \in G$ に対して $x = y^{-1}$ とすれば, $g(x) = x^{-1} = (y^{-1})^{-1} = y$ となる. つまり, g は全射. また, $g(x_1) = g(x_2)$ とすれば, $x_1^{-1} = x_2^{-1}$. 両辺の逆元を考えれば, $x_1 = x_2$ を得る. よって, g は単射.

6.4. 任意の $x \in H$ の逆元 x^{-1} が H に属することを示せばよい. $x = e$ なら明らかなので, $x \neq e$ とする. このとき, $x, x^2, x^3, \dots$ を考えると, これらは H の元であるが, H は有限集合であるから, $x^p = x^q$ をみたす $1 \leq p < q$ が存在する. $m = q - p$ とおけば, $m \geq 1$ であって, $x^m = e$ となる. $x \neq e$ を仮定しているので, $m \geq 2$ がわかる. そうすれば, $x^{-1} = x^{m-1} \in H$.

6.5. $m > n$ と仮定して矛盾を導こう. 群 G の生成元を a とすれば, $g = a^k$ と表される. $g^m = g^n$ から $a^{k(m-n)} = e$ となり, $|G| \leq k(m-n)$ がわかる. これは G が無限群であることに反する. 同様に, $m < n$ と仮定しても矛盾が出る. したがって, $m = n$ である.

6.6. $g = e$ なら $k = 1$ であるから主張は明らか. $g \neq e$ とする. G は有限群であるから, $g, g^2, g^3, \dots$ はすべて異なるというわけにはゆかず, $g^m = g^n$ となる異なる $m, n \in \mathbb{N}$ が存在する. 両辺を簡約して, $\{k \in \mathbb{N} \mid g^k = e\}$ が空集合ではないことがわかる. その最小元をあらためて k とする. このとき, $H = \{e, g, g^2, \dots, g^{k-1}\}$ は位数 k の G の部分群になる. よって, k は $|G|$ の約数である.

6.7. $\sigma = (12 \cdots m)$ としてよい. $s = qm + r$, $0 \leq r < m$, とおく. $\varepsilon = \sigma^s = \sigma^{qm} \sigma^r = \sigma^r$ から $1 = \sigma^r(1) = 1 + r$. よって, $r = 0$.

6.8. まず,

$$(2\ 3)(1\ 2)(2\ 3) = (1\ 3), \quad (3\ 4)(1\ 3)(3\ 4) = (1\ 4), \quad \dots$$

から $(1\ j)$ が隣同士の互換の積で表される. 同様の操作を $(1\ j)$ に施すことで, 任意の互換 $(i\ j)$ が隣同士の互換の積として表される. 一方, 任意の置換は互換の積 (定理 6.13) である. よって, 任意の置換は隣同士の互換の積で表される.

6.9. 互換 τ について $\tau^{-1} = \tau$. よって, $\sigma^{-1} = (\tau_1 \cdots \tau_m)^{-1} = \tau_m^{-1} \cdots \tau_1^{-1} = \tau_m \cdots \tau_1$. したがって, $\text{sgn}(\sigma^{-1}) = (-1)^m = \text{sgn}(\sigma)$.

6.10. $\text{sgn} : \mathcal{S}(n) \longrightarrow \{\pm 1\}$ は準同型である. その核 N は偶置換の全体と一致し, 互換 $\tau = (12)$ によって τN が奇置換の全体に一致する. $\sigma \mapsto \tau\sigma$ によって N と τN が 1 対 1 対応するから, $|N| = |\tau N| = n!/2$.

6.11. H の含む互換を $(i\ j)$ とする ($i \neq j$). 任意の $a, b \in \{1, 2, \dots, n\}$, $a \neq b$ に対して, $\sigma(a) = i$, $\sigma(b) = j$ を満たす $\sigma \in \mathcal{S}(n)$ を 1 つとる. このとき,

$$(ab) = \sigma^{-1}(i\ j)\sigma$$

が成り立つ. H は正規部分群なので, $\sigma^{-1}H\sigma = H$ である. よって, $(ab) \in H$. こうして, H はすべての互換を含むことになるから, $H = \mathcal{S}(n)$.

- 6.12. 任意の $\sigma \in \mathcal{A}(n)$ と $\tau \in \mathcal{S}(n)$ に対して $\tau^{-1}\sigma\tau$ が偶置換であることを示せばよい. まず, σ は偶数個の互換の積である. τ, τ^{-1} とともに同数の互換の積で表わされるから, $\tau^{-1}\sigma\tau$ も偶数個の互換の積になる.
- 6.13. G を位数 p の群とし, $g \in G$ ($g \neq e$) をとる. $g^k = e$ となる最小の整数 $k \geq 2$ をとる. このとき, k は $|G| = p$ の約数であるが, p は素数なので, $k = p$ である. そうすると, $G = \{e, g, g^2, \dots, g^{p-1}\}$ であり, $\mathbb{Z}_p$ と同型である.
- 6.14. $\text{Ker } f = \{e\}$ と仮定する. $x_1, x_2 \in G$ が $f(x_1) = f(x_2)$ を満たせば, f が準同型であることから $e' = f(x_1)^{-1}f(x_2) = f(x_1^{-1}x_2)$. 仮定によって, $x_1^{-1}x_2 = e$, つまり, $x_1 = x_2$. これは, f が単射であることを意味する. 逆は容易.
- 6.15. G の任意の元 g, h に対して, $\sigma_a(gh) = a(gh)a^{-1} = (aga^{-1})(aha^{-1}) = \sigma_a(g)\sigma_a(h)$. よって, σ_a は準同型である. 次に, $g \in G$ が $\sigma_a(g) = e$ をみたすとき, $aga^{-1} = e$ から $g = e$ がわかる. つまり, $\text{Ker } \sigma_a = \{e\}$ であり, 単射がわかる. 最後に, 任意の $h \in G$ に対して, $\sigma_a(g) = h$ をみたす g を求めよう. 明らかに, $aga^{-1} = h$ より $g = aha^{-1}$. つまり, σ_a は全射. こうして, 準同型 σ_a が全単射であることが示されたので, それは同型である.
- 6.16. $\sigma_{ab}(g) = (ab)g(ab)^{-1} = a(bgb^{-1})a^{-1} = a(\sigma_b(g))a^{-1} = \sigma_a((\sigma_b(g)))$. したがって, $\sigma_{ab} = \sigma_a \circ \sigma_b$ となり, $a \mapsto \sigma_a$ は準同型である. $\text{Ker } \sigma$ を求めるために, $\sigma_a = 1_G$ となる a を考える. 任意の $g \in G$ に対して $\sigma_a(g) = aga^{-1} = g$ が成り立つので, これは $ag = ga$ と同値な条件である.
- 6.17. G の2元 g, h が, ある $a \in G$ によって, $aga^{-1} = h$ という関係にあるとき $g \sim h$ と書く. $\sim$ が反射律と対称律を満たすことは明らか. $g \sim h$ かつ $h \sim k$ とする. 定義から $aga^{-1} = h, bhb^{-1} = k$ となる $a, b \in G$ がとれる. このとき, $k = bhb^{-1} = b(aga^{-1})b^{-1} = (ba)g(ba)^{-1}$ が成り立つ. よって, $g \sim k$. したがって, $\sim$ は推移律も満たすから, G 上の同値関係になる.

7 環と体

7.1. $ab + (-a)b = (a + (-a))b = 0b = 0$ から, $-(ab) = (-a)b$ がわかる. $-(ab) = a(-b)$ も同様である.

7.2. $ab = ac$ から

$$0 = ab + (-ac) = ab + (a(-c)) = a(b + (-c)).$$

R には零因子が存在せず, 仮定から $a \neq 0$ であるから $b + (-c) = 0$. したがって, $b = -(-c) = c$.

7.3. $(a+b)^n$ を分配法則を繰り返し用いて展開すれば,

$$(a+b)^n = \sum_{x_1, \dots, x_n \in \{a, b\}} x_1 x_2 \cdots x_n$$

となる. 一般項 $x_1 x_2 \cdots x_n$ のうち, a を $n-k$ 回, b を k 回含むものは全部で $\binom{n}{k}$ 個ある. R は可換環なので, そのような項はすべて $a^{n-k} b^k$ とまとめられる.

7.4. $x, y \in R$ に対して

$$(x+y)^2 = x+y$$

である. 左辺を展開して, $x^2 = x$ と $y^2 = y$ を代入すれば,

$$x+y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

したがって, $xy = -yx$. ここで, $y = e$ とおけば $x = -x$ がわかり, $xy = -yx = yx$.

7.5. 体 F において $a, b \in F$ が $ab = 0$ を満たしたとする. $a \neq 0$ であれば, a^{-1} をかけて $b = 0$ を得る. したがって, 体 F には零因子が存在しない.

7.6. $J \subset \mathbb{Z}$ をイデアルとする. $J = \{0\}$ ならば $m = 0$ ととればよい. $J \neq \{0\}$ のときは, $m = \min\{a \in J \mid a > 0\}$ とおく. J は $\mathbb{Z}$ の加法部分群であるから m の倍数をすべて含む. つまり, $m\mathbb{Z} \subset J$. 逆に, 任意の $a \in J$ に対して, $q, r \in \mathbb{Z}$ と $0 \leq r < m$ をとって, $a = qm + r$ と表しておく. イデアルの性質から, $r = a - qm \in J$ である. m の選び方から $r = 0$. つまり, J のすべての元は m の倍数であり, $J \subset m\mathbb{Z}$.

7.7. (1) は容易.

(2) $\text{Ker } f$ は $\mathbb{Z}$ のイデアルであるから, 問題 7.6 によって, 整数 $m \geq 0$ によって一意的に $\text{Ker } f = m\mathbb{Z}$ と表される.

(3) 整域 R の標数が 0 でなければ, $m \in \mathbb{N}$ によって, $\text{Ker } f = m\mathbb{Z}$. 準同型定理によって $f(\mathbb{Z})$ は $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ と同型である. $f(\mathbb{Z})$ は, 整域 R の部分環であることから, 整域である. よって, $\mathbb{Z}_m$ も整域である. したがって, m は素数である.

(4) 有限体は整域であり, かつ標数は 0 ではない.

7.8. (1) $\Rightarrow$ (2) を示す. まず,

$$(x+y) \cdot (x+z) = (x+y) \cdot x + (x+y) \cdot z \quad (7.1)$$

が得られる. 交換律と吸収律によって, (7.1) は,

$$= x + z \cdot (x+y)$$

となる. 再び (1) によって,

$$= x + (z \cdot x + z \cdot y).$$

最後に, 結合律と吸収律によって,

$$= (x + z \cdot x) + z \cdot y = x + y \cdot z.$$

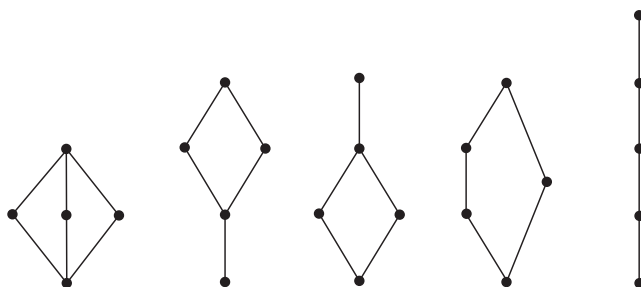
(2) $\Rightarrow$ (1) も同様である.

7.9. (1) $(x + y) + (x^c \cdot y^c) = 1$ と $(x + y) \cdot (x^c \cdot y^c) = 0$ を示せばよい. 初めの等式を示そう. 2 番目も同様である.

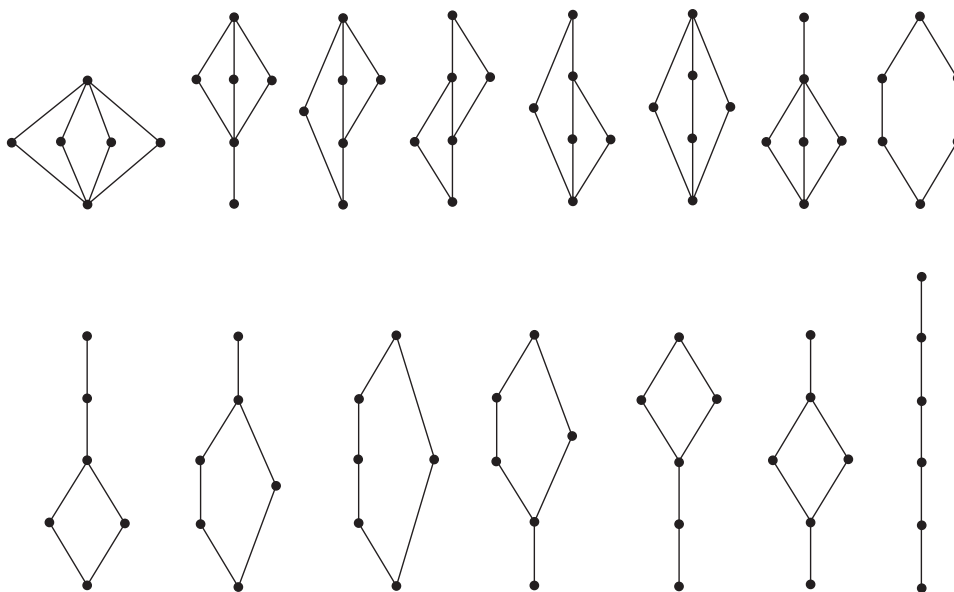
$$\begin{aligned} (x + y) + (x^c \cdot y^c) &= x + (y + x^c \cdot y^c) = x + ((y + x^c) \cdot (y + y^c)) \\ &= x + ((y + x^c) \cdot 1) = x + (y + x^c) = y + 1 = 1. \end{aligned}$$

(2) も同様である.

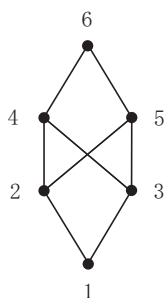
7.10. 5 元束は次の 5 個である.



6 元束は次の 15 個である.



たとえば, 次の半順序集合は束ではない. 実際, $\sup\{2, 3\}$ が存在しない. なぜならば, $U(\{2, 3\}) = \{4, 5, 6\}$ に最小限が存在しないからである.



ちなみに7元束は53個ある.

8 行列

$$8.1. \begin{bmatrix} 2 & -3 & 4 & -5 \\ -3 & 4 & -5 & 6 \\ 4 & -5 & 6 & -7 \end{bmatrix}$$

$$8.2. A^T = A^* = \begin{bmatrix} 1 & 0 \\ 3 & -2 \\ 5 & 1 \end{bmatrix}, \quad B^T = \begin{bmatrix} -1 & 0 & 2i \\ 3+2i & -2 & 3-4i \end{bmatrix}, \quad B^* = \begin{bmatrix} -1 & 0 & -2i \\ 3-2i & -2 & 3+4i \end{bmatrix}$$

$$8.3. 4X + 3A = 2X - 4B \text{ から}$$

$$X = -\frac{3}{2}A - 2B = \begin{bmatrix} -10 & 5 & 2 \\ -2 & -2 & -3 \end{bmatrix}$$

$$8.4. x = 1, y = 2$$

$$8.5. \text{与えられた正方行列 } A \text{ に対して,}$$

$$B = \frac{1}{2}(A + A^T), \quad C = \frac{1}{2}(A - A^T)$$

とおけば, $B^T = B$, $C^T = -C$, $A = B + C$ が確認できる. 一意性のために, 別の対称行列 B' と交代行列 C' で $A = B' + C'$ が成り立ったとする. $A = B + C$ と差をとって, $B - B' = C' - C$. 両辺の転置行列をとれば, $B - B' = -C' + C$. よって, $B - B' = C' - C = O$ が得られ, 一意性が示された.

$$8.6. \text{問題 8.5 と同様.}$$

$$8.7. AB + 2AC = \begin{bmatrix} -12 & -12 & 17 \\ -2 & -2 & 6 \end{bmatrix}, \quad A + BC^T = \begin{bmatrix} 3 & -7 \\ 8 & 1 \end{bmatrix}$$

$$8.8. \text{直接計算すればよい.}$$

$$8.9. X = \pm E, \begin{bmatrix} \pm\sqrt{1-bc} & b \\ c & \mp\sqrt{1-bc} \end{bmatrix} \quad (b, c \text{ は } bc < 1 \text{ を満たす任意の実数})$$

$$8.10. X = 4E, -E, \begin{bmatrix} a & b \\ c & -a+3 \end{bmatrix} \quad (a, b, c \text{ は } bc = -a^2 + 3a + 3 \text{ を満たす任意の複素数})$$

$$8.11. \begin{bmatrix} x & y \\ 0 & x \end{bmatrix} \quad (x, y \text{ は任意})$$

$$8.12. \text{成分で比較せよ.}$$

8.13. 成分で比較せよ.

8.14. $AA^* = A^*A$ から $BC = CB$ がわかる. よって, $A^*A = (B + iC)(B - iC) = B^2 + C^2$.

$$8.15. (1) A^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$(2) B^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -a & 1 & 0 & 0 \\ -b & 0 & 1 & 0 \\ -c & 0 & 0 & 1 \end{bmatrix}$$

8.16. 行列の転置と乗法の関係 (問題 8.12) から, $A^T(A^{-1})^T = (A^{-1}A)^T = E^T = E$. 同様に, $(A^{-1})^T A^T = E$ もわかるから, A^T も正則行列であって, $(A^T)^{-1} = (A^{-1})^T$ が成り立つ. 共役転置行列についても同様である.

8.17. 問題 8.16 に注意すると, A が対称行列のとき, $(A^{-1})^T = (A^T)^{-1} = A^{-1}$. よって, A^{-1} も対称行列である. A が交代行列であれば, $(A^{-1})^T = (A^T)^{-1} = (-A)^{-1} = -A^{-1}$ なので, A^{-1} も交代行列である.

8.18. D が積と逆行列をとる演算で閉じていることから, $GL(n, \mathbb{R})$ の部分群である. また, 対角行列同士の積は可換であるから, D は可換群をなす.

8.19. (1) $[A|E]$ に対して行の基本変形を繰り返す.

$$\begin{aligned} & \begin{bmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{1)} \begin{bmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & -2 & -5 & -2 & 0 & 1 \end{bmatrix} \\ & \xrightarrow{2)} \begin{bmatrix} 1 & 0 & -1 & 1 & -2 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & -1 & -2 & 2 & 1 \end{bmatrix} \xrightarrow{3)} \begin{bmatrix} 1 & 0 & -1 & 1 & -2 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & -2 & -1 \end{bmatrix} \\ & \xrightarrow{4)} \begin{bmatrix} 1 & 0 & 0 & 3 & -4 & -1 \\ 0 & 1 & 0 & -4 & 5 & 2 \\ 0 & 0 & 1 & 2 & -2 & -1 \end{bmatrix} \quad \text{よって} \quad A^{-1} = \begin{bmatrix} 3 & -4 & -1 \\ -4 & 5 & 2 \\ 2 & -2 & -1 \end{bmatrix} \end{aligned}$$

(2) $[B|E]$ に対して行の基本変形を繰り返せば, 途中で行き詰まる. つまり, B は正則ではなく, 逆行列をもたない. あらゆる方法を試すわけにはゆかないが, 途中で行き詰まることを確認して欲しい.

8.20. $S(i, j)^{-1} = S(i, j) = S(j, i)$, $R(i; \alpha)^{-1} = R(i; \alpha^{-1})$, $T(i, j; \alpha) = T(i, j; -\alpha)$.

8.21. 成分で確かめられる. 後半は明らか.

8.22. $(A^T A)_{jj} = \sum_{i=1}^m (A^T)_{ji} (A)_{ij} = \sum_{i=1}^m (A)_{ij} (A)_{ij}$ なので,

$$\mathrm{Tr}(A^T A) = \sum_{j=1}^n (A^T A)_{jj} = \sum_{j=1}^n \sum_{i=1}^m \{(A)_{ij}\}^2$$

$\mathrm{Tr}(A^* A)$ も同様.

8.23. $A = A^T$ に注意して, 問題 8.22 を適用すれば,

$$\mathrm{Tr}(A^2) = \mathrm{Tr}(A^T A) = \sum_{i,j=1}^n \{(A)_{ij}\}^2.$$

$(A)_{ij}$ はすべて実数であるから, $\mathrm{Tr}(A^2) = 0$ から $(A)_{ij} = 0$ がわかる. つまり, $A = O$.

8.24. $AB - BA = E$ の両辺のトレースを考える. 左辺は

$$\mathrm{Tr}(AB - BA) = \mathrm{Tr}(AB) - \mathrm{Tr}(BA) = 0$$

であるが, 右辺は $\mathrm{Tr} E = n$ となり, 矛盾.

8.25. 定理 8.7 によって,

$$\mathrm{Tr}(ABC) = \mathrm{Tr}(A(BC)) = \mathrm{Tr}((BC)A) = \mathrm{Tr}(BCA).$$

残りも同様である. 成分を直接計算してもよい.

9 行列式

9.1. (1) 左辺の行列を $A = [a_{ij}]$ とおく. 行列式の定義

$$|A| = \sum_{\sigma \in \mathcal{S}(n)} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \quad (9.1)$$

を思い出す. A の形から, 右辺の和において, 0 以外の値を与える $\sigma \in \mathcal{S}(n)$ は

$$\sigma(1) = 2, \quad \sigma(2) = 3, \quad \dots, \quad \sigma(n) = 1$$

となるもの唯 1 つである. そのような σ は巡回置換

$$\sigma = (12 \cdots, n)$$

であり, $\mathrm{sgn}(\sigma) = (-1)^{n-1}$. よって, $|A| = (-1)^{n-1}$.

(2) 行列式の定義 (9.1) において, 和に必要な $\sigma \in \mathcal{S}(n)$ は $\sigma(1) = n, \sigma(2) = n-1, \dots, \sigma(n) = 1$ を満たすものだけである. その σ の符号は $(-1)^{n(n-1)/2}$ であることからわかる.

9.2. 一方を示せば他方は転置行列をとればよいので, ここでは2番目の式を示す. B を (m, m) 型, C を (n, n) 型とし,

$$A = \begin{bmatrix} B & O \\ D & C \end{bmatrix}$$

とおく. 行列式の定義に現れる一般項

$$\operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{m+n\sigma(m+n)}$$

を考える. A の形から, $1 \leq i \leq m$ のときは $1 \leq \sigma(i) \leq m$ となっている σ のみに関して和をとることになる. そのような σ は, $m+1 \leq i \leq m+n$ に対しては, $m+1 \leq \sigma(i) \leq m+n$ となっている. したがって, σ は $\{1, 2, \dots, m\}$ と $\{m+1, \dots, m+n\}$ のそれぞれの置換の積になるから, それを $\sigma = \sigma_1 \sigma_2$ と表そう. $\operatorname{sgn}(\sigma_1 \sigma_2) = \operatorname{sgn}(\sigma_1) \operatorname{sgn}(\sigma_2)$ に注意して, 行列式の定義に現れる一般項は,

$$\operatorname{sgn}(\sigma_1) \operatorname{sgn}(\sigma_2) a_{1\sigma_1(1)} \cdots a_{m\sigma_1(m)} a_{m+1\sigma_2(1)} \cdots a_{m+n\sigma_2(n)}$$

の形になる. これに対して $\sigma_1 \in \mathcal{S}(m)$, $\sigma_2 \in \mathcal{S}(n)$ を走らせて和をとればよい.

9.3. $A = [a_{ij}]$ とすると, $\alpha A = [\alpha a_{ij}]$. よって,

$$\begin{aligned} |\alpha A| &= \sum_{\sigma \in \mathcal{S}(n)} \operatorname{sgn}(\sigma) (\alpha a_{1\sigma(1)}) (\alpha a_{2\sigma(2)}) \cdots (\alpha a_{n\sigma(n)}) \\ &= \alpha^n \sum_{\sigma \in \mathcal{S}(n)} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \\ &= \alpha^n |A|. \end{aligned}$$

9.4. (1) $m > n$ に注意して, 0 ばかりからなる列または行を追加して (m, m) 型行列

$$\tilde{A} = [A \ O], \quad \tilde{B} = \begin{bmatrix} B \\ O \end{bmatrix}$$

を定義する. これらは正方行列であるから, 行列式の積公式で $|\tilde{A}\tilde{B}| = |\tilde{B}\tilde{A}|$ が成り立つ. 一方, $\tilde{A}\tilde{B} = AB$,

$$\tilde{B}\tilde{A} = \begin{bmatrix} BA & O \\ O & O \end{bmatrix}$$

が成り立つ. よって, $|AB| = |\tilde{A}\tilde{B}| = |\tilde{B}\tilde{A}| = 0$.

(2) 略.

9.5. $(a+b+c)(a^2+b^2+c^2-bc-ca-ab) = (a+b+c)(a+b\omega+c\omega^2)(a+b\omega^2+c\omega)$ ただし, ω は 1 の虚立方根の 1 つ.

9.6. たとえば, 次のように変形する.

$$\begin{aligned}
 & \begin{vmatrix} 1+a & 1 & 1 & 1 \\ 1 & 1+b & 1 & 1 \\ 1 & 1 & 1+c & 1 \\ 1 & 1 & 1 & 1+d \end{vmatrix} = abcd \begin{vmatrix} 1/a+1 & 1/a & 1/a & 1/a \\ 1/b & 1/b+1 & 1/b & 1/b \\ 1/c & 1/c & 1/c+1 & 1/c \\ 1/d & 1/d & 1/d & 1/d+1 \end{vmatrix} \\
 & = abcd \left(1 + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d}\right) \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1/b & 1/b+1 & 1/b & 1/b \\ 1/c & 1/c & 1/c+1 & 1/c \\ 1/d & 1/d & 1/d & 1/d+1 \end{vmatrix} \\
 & = abcd \left(1 + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d}\right) \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1/b & 1 & 0 & 0 \\ 1/c & 0 & 1 & 0 \\ 1/d & 0 & 0 & 1 \end{vmatrix}
 \end{aligned}$$

$$9.7. \begin{vmatrix} A & B \\ B & A \end{vmatrix} = \begin{vmatrix} A-B & B \\ B-A & A \end{vmatrix} = \begin{vmatrix} A-B & B \\ O & A+B \end{vmatrix} = |A+B||A-B|$$

9.8. A, B の成分の多項式として等式を示せばよい. $AB \operatorname{adj}(AB) = |AB|E$ の左から $\operatorname{adj} A$ をかけて, $|A|B \operatorname{adj}(AB) = |AB| \operatorname{adj} A$. よって, $B \operatorname{adj}(AB) = |B| \operatorname{adj} A$. さらに, 左から $\operatorname{adj} B$ をかけて, $\operatorname{adj}(AB) = (\operatorname{adj} B)(\operatorname{adj} A)$.

9.9. 問題 9.7 と同様.

9.10. 略.

10 線形空間と線形写像

10.1. $M(n, \mathbb{R})$ は実線形空間である. つまりスカラー体は $\mathbb{R}$ である. A, B が対称行列であれば $A+B$ も対称行列, A が対称行列で α がスカラーなら αA も対称行列である. よって, V は $M(n, \mathbb{R})$ の部分空間である.

10.2. (1) V が和で閉じていることはよいが, $M(n, \mathbb{C})$ を複素線形空間とみなすとき, スカラー体は $\mathbb{C}$ である. A がエルミート行列であっても, $\alpha \in \mathbb{C}$ に対して αA はエルミート行列であるとは限らない. $(\alpha A)^* = \bar{\alpha} A^*$ に注意しよう.

(2) スカラー体を実数に限れば, V はスカラー倍でも閉じている.

10.3. $\operatorname{Im} f = \{\varphi \in \mathbb{K}[x] \mid \deg \varphi \leq n-1\}$. $\operatorname{Ker} f = \{\varphi \in \mathbb{K}[x] \mid \deg \varphi = 0\}$ (0 次多項式とは定数のことである).

10.4. $\operatorname{Ker} f = \{0\}$ を仮定する. $f(\mathbf{x}) = f(\mathbf{y})$ ならば, $f(\mathbf{x}) - f(\mathbf{y}) = f(\mathbf{x} - \mathbf{y}) = 0$. よって, $\mathbf{x} - \mathbf{y} \in \operatorname{Ker} f = \{0\}$ となり, $\mathbf{x} = \mathbf{y}$ がわかる. つまり, f は単射である. 逆も同様である.

10.5. 置換行列 $S(\sigma)$ について $(S(\sigma))_{ij} = \delta_{i\sigma(j)}$ であることを用いて, 定義に基づいて計算で示すことができる. $S(\varepsilon) = E$ は明らか. $\sigma \mapsto S(\sigma)$ の単射性は, 準同型であることから, $S(\sigma) = E \implies \sigma = \varepsilon$ を示せば十分である. これは容易.

10.6. 行列式の定義から,

$$\begin{aligned} |S(\sigma)| &= \sum_{\tau \in S(n)} \text{sgn}(\tau) S(\sigma)_{1\tau(1)} S(\sigma)_{2\tau(2)} \cdots S(\sigma)_{n\tau(n)} \\ &= \sum_{\tau \in S(n)} \text{sgn}(\tau) \delta_{1\sigma(\tau(1))} \delta_{2\sigma(\tau(2))} \cdots \delta_{n\sigma(\tau(n))} \end{aligned}$$

である. 和に現れる各項は, $\tau \neq \sigma^{-1}$ のとき 0, $\tau = \sigma^{-1}$ のとき, $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$ である.

10.7. f_A が同型であれば, ある線形変換 g があって $f_A \circ g = g \circ f_A = 1$ となる. 一方で, g はある行列 B によって $g = f_B$ と表される. よって, $1 = f_A \circ f_B = f_{AB}$. したがって, $AB = E$. 同様に, $BA = E$. よって, A は正則であって, $A^{-1} = B$. したがって, $(f_A)^{-1} = g = f_B = f_{A^{-1}}$. 逆も同様に示される.

10.8. 背理法で示す. m 個のベクトル $\mathbf{a}_1, \dots, \mathbf{a}_m$ が一次独立になったとする. $\mathbb{K}^n$ の標準基底 $\mathbf{e}_1, \dots, \mathbf{e}_n$ を考えれば, 線形空間 $\mathbb{K}^n$ が有限次元であることが定義からわかる. したがって, 定理 10.11 によって, $\mathbf{a}_1, \dots, \mathbf{a}_m$ に有限個のベクトルを付け加えて $\mathbb{K}^n$ の基底が得られる. それを $\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{a}_{m+1}, \dots, \mathbf{a}_l$ としよう. ここで, 補題 10.13 によれば, $n = l$ である. したがって, $m \leq n$ を得る. これは, $m > n$ に反するので, m 個のベクトル $\mathbf{a}_1, \dots, \mathbf{a}_m$ が一次独立になりえない.

定理 10.11 の証明を省略したので, ここに概略を示しておこう. 有限次元ベクトル空間の定義から, 有限個のベクトル $\mathbf{w}_1, \dots, \mathbf{w}_n \in V$ で V のすべての元がその線形結合で表示できる. $V \neq \{\mathbf{0}\}$ であるから, $n \geq 1$ である. また, $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n$ を順に見て, 前の番号のベクトルの線形結合で表わされるものを除くことで, はじめから $\mathbf{w}_1, \dots, \mathbf{w}_n \in V$ は一次独立になっているとしてよい.

さて, $\mathcal{V} = \{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ が一次独立とする. これに, $\mathbf{w}_1, \dots, \mathbf{w}_n \in V$ を順に付け加えることを考える. まず, $\mathbf{w}_1$ が $\mathcal{V}$ の一次結合で表わされるかどうかによって,

$$\mathcal{V}_1 = \begin{cases} \mathcal{V}, & \mathbf{w}_1 \text{ が } \mathcal{V} \text{ の一次結合で表わされる,} \\ \mathcal{V} \cup \{\mathbf{w}_1\}, & \mathbf{w}_1 \text{ が } \mathcal{V} \text{ の一次結合で表わされない,} \end{cases}$$

とする. 次に, $\mathbf{w}_2$ が $\mathcal{V}_1$ の一次結合で表わされるかどうかによって,

$$\mathcal{V}_2 = \begin{cases} \mathcal{V}_1, & \mathbf{w}_2 \text{ が } \mathcal{V}_1 \text{ の一次結合で表わされる,} \\ \mathcal{V}_1 \cup \{\mathbf{w}_2\}, & \mathbf{w}_2 \text{ が } \mathcal{V}_1 \text{ の一次結合で表わされない.} \end{cases}$$

これを繰り返して得られる $\mathcal{V}_n$ が V の基底になる. 実際, 作り方から, $\mathcal{V}_n$ は一次独立である. さらに, すべての $\mathbf{w}_i$ は $\mathcal{V}_n$ の一次結合になるから, すべての V のベクトルは $\mathcal{V}_n$ の一次結合になる.

10.9. W は $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_n)\}$ で張られるが, 各 $f(\mathbf{v}_i) \in \text{Im } f$ は明らかなので, $\text{Im } f = W$ となる. つまり, f は全射. 単射のためには, $f(\mathbf{u}) = \mathbf{0} \implies \mathbf{u} = \mathbf{0}$ を示せばよい. $\mathbf{u} = \sum_{k=1}^n \alpha_k \mathbf{v}_k$ と書いて, f で写し, $\{f(\mathbf{v}_1), \dots, f(\mathbf{v}_n)\}$ が 1 次独立であることを用いればよい.

10.10. V が有限次元であれば, 定義によって W 自身も有限次元線形空間である. W の基底を $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ ($r = \dim W$) とする. それらは, W のベクトルとしても 1 次独立であるから, それを拡張して V の基底が得られる. よって, $\dim W = r \leq \dim V$. ここで等号が成り立てば, $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ が V の基底になり, $W = V$ が成り立つ. 逆に, $W = V \implies \dim W = \dim V$ は明らか.

10.11. $A = \begin{bmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ -1 & 1 & 0 \end{bmatrix}$

10.12. (1) 2

(2) 行の基本変形によって,

$$\begin{bmatrix} a & 1 & 1 & 1 \\ 1 & a & 1 & 1 \\ 1 & 1 & a^2 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & a & 1 & 1 \\ 0 & 1-a & a-1 & 0 \\ 0 & 0 & 1-a & a^2-1 \end{bmatrix}$$

したがって, $a = 1$ なら 階数 1, $a \neq 1$ なら 階数 3.

(3) 行の基本変形によって,

$$\begin{bmatrix} a & b & b \\ b & a & b \\ b & b & a \end{bmatrix} \longrightarrow \begin{bmatrix} a+2b & a+2b & a+2b \\ b & a & b \\ b & b & a \end{bmatrix}$$

(i) $a+2b \neq 0$, $a \neq b$ のとき, 階数 3. (ii) $a+2b \neq 0$, $a = b$ のとき, 階数 1. (iii) $a+2b = 0$, $b \neq 0$ のとき, 階数 2. (iv) $a = b = 0$ のとき, 階数 0.

10.13. 部分空間に関して $\text{Im } AB \subset \text{Im } A$ は明らかである. したがって, 定理 10.20 によって, $\text{rank } AB = \dim \text{Im } AB \leq \dim \text{Im } A = \text{rank } A$. この結果を転置行列に適用しよう. 定理 10.18 も考慮して, $\text{rank } AB = \text{rank}(AB)^T = \text{rank } B^T A^T \leq \text{rank } B^T = \text{rank } B$.

10.14. まず,

$$A = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

とにおいて, 連立方程式 $A\mathbf{x} = \mathbf{0}$ を考えよう. 題意の共有点を (x_0, y_0) とすれば, $(x_0, y_0, 1)$ は上の連立方程式の非自明解である. 同次方程式 $A\mathbf{x} = \mathbf{0}$ が非自明解をもつための必要十分条件は $|A| = 0$ である.

10.15. (1) $x = 2, y = 3$

(2) $x_1 = k + 1, x_2 = 2k - 1, x_3 = -k + 2, x_4 = k$ (k は任意定数)

10.16. 階段行列を目指して、拡大係数行列に行の変形を施す.

$$[A|\mathbf{b}] = \begin{bmatrix} 1 & 1 & 1 & a \\ 2 & -1 & 1 & 5 \\ 1 & 3 & -b & -8 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & -b-1 & -2a-3 \\ 0 & 1 & b+2 & 3a+3 \\ 0 & 0 & 3b+5 & 7a+14 \end{bmatrix}$$

簡約階段行列の一手前であるが、解の存在に関する考察にはこれで十分である. (i) $3b+5 \neq 0$ のときは、 $\text{rank } A = 3$ となるから A は正則行列になる. よって、一意的な解が存在する. (ii) $3b+5 = 0$ のときは、 $\text{rank } A = 2$ となる. 解が存在するための必要十分条件は $\text{rank } A = \text{rank}[A|\mathbf{b}]$ であるが、それは $7a+14 = 0$ と同値である. このとき、解の自由度は $3 - 2 = 1$ である.

11 固有値と行列の標準化

11.1. (1) 固有値は 1, 2. 固有空間は

$$W(1) = \left\{ c \begin{bmatrix} 1 \\ 1 \end{bmatrix} \mid c \in \mathbb{C} \right\}, \quad W(2) = \left\{ c \begin{bmatrix} 2 \\ 3 \end{bmatrix} \mid c \in \mathbb{C} \right\}$$

(2) 固有値は $\pm i$. 固有空間は

$$W(i) = \left\{ c \begin{bmatrix} 1 \\ i \end{bmatrix} \mid c \in \mathbb{C} \right\}, \quad W(-i) = \left\{ c \begin{bmatrix} 1 \\ -i \end{bmatrix} \mid c \in \mathbb{C} \right\}$$

(3) 固有値は 2 と -1 (重複度 2). 固有空間は

$$W(2) = \left\{ c \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \mid c \in \mathbb{C} \right\}, \quad W(-1) = \left\{ c_1 \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} \mid c_1, c_2 \in \mathbb{C} \right\}$$

11.2. $\mathbf{u} \neq \mathbf{0}$ を AB の $\lambda (\neq 0)$ に関する固有ベクトルとすると、 $AB\mathbf{u} = \lambda\mathbf{u}$. 左から B をかけると、 $BAB\mathbf{u} = \lambda B\mathbf{u}$. もし、 $B\mathbf{u} = \mathbf{0}$ ならば、 $\mathbf{0} = AB\mathbf{u} = \lambda\mathbf{u}$. $\lambda \neq 0$ とあわせて、 $\mathbf{u} = \mathbf{0}$ を得て矛盾である. よって、 $B\mathbf{u} \neq \mathbf{0}$ であり、 $B\mathbf{u}$ は BA の固有値 λ に関する固有ベクトルになっている.

11.3. $A^m = O$ とする. $A\mathbf{u} = \lambda\mathbf{u}$, $\mathbf{u} \neq \mathbf{0}$, とおき、両辺に A を $m-1$ 回かければ、 $\mathbf{0} = A^m\mathbf{u} = \lambda^m\mathbf{u}$ を得る. よって、 $\lambda^m = 0$, すなわち、 $\lambda = 0$.

11.4. 問題 11.3 と同様に考えると、 $A\mathbf{u} = \lambda\mathbf{u}$ から $\lambda\mathbf{u} = A\mathbf{u} = A^{m+1}\mathbf{u} = \lambda^{m+1}\mathbf{u}$ が得られる. よって、 $\lambda^{m+1} = \lambda$.

11.5. 右辺のノルムを内積で表して展開すればよい.

11.6. 左辺を内積で計算する. まず,

$$\begin{aligned}\|\mathbf{a} + \mathbf{b}\|^2 &= \langle \mathbf{a} + \mathbf{b}, \mathbf{a} + \mathbf{b} \rangle \\ &= \langle \mathbf{a}, \mathbf{a} \rangle + \langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{b}, \mathbf{a} \rangle + \langle \mathbf{b}, \mathbf{b} \rangle \\ &= \|\mathbf{a}\|^2 + \langle \mathbf{a}, \mathbf{b} \rangle + \langle \mathbf{b}, \mathbf{a} \rangle + \|\mathbf{b}\|^2.\end{aligned}$$

同様に,

$$\|\mathbf{a} - \mathbf{b}\|^2 = \|\mathbf{a}\|^2 - \langle \mathbf{a}, \mathbf{b} \rangle - \langle \mathbf{b}, \mathbf{a} \rangle + \|\mathbf{b}\|^2.$$

上の2式を加えて,

$$\|\mathbf{a} + \mathbf{b}\|^2 + \|\mathbf{a} - \mathbf{b}\|^2 = 2\|\mathbf{a}\|^2 + 2\|\mathbf{b}\|^2.$$

11.7. f の定義に基づいた計算で確かめられる.

11.8. $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ として,

$$\sum_{i=1}^n \alpha_i \mathbf{e}_i = \mathbf{0}$$

を仮定する. 両辺において, $\mathbf{e}_j$ と内積をとれば,

$$0 = \sum_{i=1}^n \langle \mathbf{e}_j, \alpha_i \mathbf{e}_i \rangle = \sum_{i=1}^n \alpha_i \delta_{ji} = \alpha_j$$

が得られる.

11.9. $\text{rank } A = r$ とおく. $\dim \text{Im } A = r$ なので, $A\mathbf{v}_1, \dots, A\mathbf{v}_r$ が $\text{Im } A$ の基底になるように, $\mathbf{v}_1, \dots, \mathbf{v}_r \in \mathbb{K}^n$ を選ぶ. このとき, $A^T A\mathbf{v}_1, \dots, A^T A\mathbf{v}_r \in \mathbb{K}^n$ が1次独立になることを示そう. 実際,

$$\sum_{i=1}^r \alpha_i A^T A\mathbf{v}_i = \mathbf{0}$$

と仮定すると,

$$0 = \left\langle \sum_{j=1}^r \alpha_j \mathbf{v}_j, \sum_{i=1}^r \alpha_i A^T A\mathbf{v}_i \right\rangle = \left\langle \sum_{j=1}^r \alpha_j A\mathbf{v}_j, \sum_{i=1}^r \alpha_i A\mathbf{v}_i \right\rangle = \left\| \sum_{j=1}^r \alpha_j A\mathbf{v}_j \right\|^2$$

が成り立つ. これより, $\sum_{i=1}^r \alpha_i A\mathbf{v}_i = \mathbf{0}$ が出る. $A\mathbf{v}_1, \dots, A\mathbf{v}_r$ は $\text{Im } A$ の基底であるから, $\alpha_1 = \dots = \alpha_r = 0$ が導かれる. こうして, $A^T A\mathbf{v}_1, \dots, A^T A\mathbf{v}_r \in \mathbb{R}^n$ が1次独立であるから,

$$\text{rank } A^T A = \dim \text{Im } A^T A \geq r$$

がわかる. 一方, 問題 10.13 から $\text{rank } A^T A \leq \text{rank } A = r$ がわかるので,

$$\text{rank } A^T A = \text{rank } A.$$

この等式で A を A^T に置き換えれば,

$$\text{rank } AA^T = \text{rank } A^T = \text{rank } A$$

もわかる.

11.10. (1) 右辺を展開すればわかる.

(2) 仮定と (1) から $\langle \mathbf{y}, A\mathbf{x} \rangle = 0$ がすべての $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ に対して成り立つ. したがって, すべての $\mathbf{x} \in \mathbb{R}^n$ に対して, $A\mathbf{x} = \mathbf{0}$ が成り立ち, $A = O$ がわかる.

11.11. 問題 11.10 と同様に, $\text{Re } \langle \mathbf{y}, A\mathbf{x} \rangle = 0$ と $\text{Im } \langle \mathbf{y}, A\mathbf{x} \rangle = \text{Re } \langle i\mathbf{y}, A\mathbf{x} \rangle = 0$ を導け. あるいは, 極化公式 (問題 11.5) に類似の公式を導いて利用せよ.

11.12. (1) $E = A^T A$ の両辺の行列式をとって, $1 = |A^T A| = |A^T| \cdot |A| = |A|^2$.

(2) $E = U^* U$ の両辺の行列式をとって, $1 = |U^* U| = |U^*| \cdot |U| = \overline{|U|} \cdot |U|$.

11.13. (1) $\Rightarrow$ (2) はノルムの定義から明らか.

(2) $\Rightarrow$ (1) は極化公式を用いよ.

11.14. (1) $(A^* A)^* = A^* (A^*)^* = A^* A$ からわかる.

(2) $A^* A$ はエルミート行列なので, その固有値はすべて実数. 固有値を λ , それに対応する固有ベクトルを $\mathbf{v}$ とすれば, $\lambda \langle \mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{v}, A^* A \mathbf{v} \rangle = \langle A \mathbf{v}, A \mathbf{v} \rangle \geq 0$. したがって, $\lambda \geq 0$.

(3) $\text{Tr}(A^* A) = \sum_{i=1}^n \lambda_i^2$ である. あとは $\text{Tr}(A^* A)$ を成分で表せばよい.

11.15. (1) A は実対称行列なので直交行列で対角化される. A の固有値は $-2, 4$ である. それぞれの固有ベクトルでノルムが 1 となるものを求めて $\mathbf{u}_1, \mathbf{u}_2$ とする. $S = [\mathbf{u}_1 \ \mathbf{u}_2]$ が求める直交行列になる.

$$S^T A S = \begin{bmatrix} -2 & 0 \\ 0 & 4 \end{bmatrix}, \quad S = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$$

(2) B はエルミート行列なのでユニタリ行列で対角化される. B の固有値は 1 と 4 (重複度 2) の 2 個である. 固有空間 $W(1)$ から単位ベクトル $\mathbf{u}_1$ を, $W(4)$ から直交する単位ベクトル $\mathbf{u}_2, \mathbf{u}_3$ を選び, $U = [\mathbf{u}_1 \ \mathbf{u}_2 \ \mathbf{u}_3]$ とおく.

$$U^* B U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \quad U = \begin{bmatrix} i/\sqrt{3} & -i/\sqrt{6} & 1/\sqrt{2} \\ 1/\sqrt{3} & 2/\sqrt{6} & 0 \\ -i/\sqrt{3} & i/\sqrt{6} & 1/\sqrt{2} \end{bmatrix}$$

11.16. (1) A の固有値は $1, 3, -2$ でいずれも重複度は 1 である. したがって対角化可能.

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -2 \end{bmatrix}, \quad T = \begin{bmatrix} -1 & 2 & 0 \\ -2 & 1 & 1 \\ 3 & -2 & -1 \end{bmatrix}$$

として, $T^{-1}AT = D$ がわかる.

(2) B の固有値は 3 (重複度 4). 固有空間 $W(3)$ は 2 次元. よって対角化不可能. この場合, 可能なジョルダン標準形は 2 通りあるが, 計算によってどちらになるかがわかる.

$$J = \begin{bmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

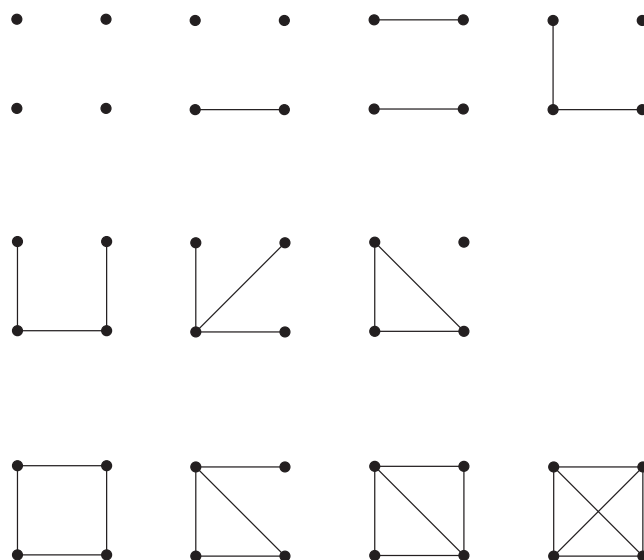
として, $T^{-1}AT = J$ がわかる.

12 グラフ

12.1. 握手の補題を用いる.

12.2. $\sum_{y \in V} (A)_{yx} = \sum_{y \sim x} (A)_{yx} = |\{y \in V \mid y \sim x\}| = d(x)$.

12.3. 辺の個数 e で分類するのが便利であろう. $e = 0$ のとき 1 個. $e = 1$ のとき 1 個. $e = 2$ のとき 2 個. $e = 3$ のとき 3 個. $e = 4$ のとき 2 個. $e = 5$ のとき 1 個. $e = 6$ のとき 1 個.



12.4. $V_1 = \{1, 2, \dots, p\}$, $V_2 = \{p+1, \dots, n\}$ のように番号付けをすれば, $i \in V_1$, $j \in V_2$ のとき, 仮定から $(A)_{ij} = (A)_{ji} = 0$ である. このことは, A がブロック対角行列になっていることを示す.

12.5. $n(n-1)/2$

12.6. n が偶数のとき $\text{diam } C_n = n/2$. n が奇数のとき $\text{diam } C_n = (n-1)/2$.

12.7. 問題 12.3 から連結グラフを選ばばよい. グラフの個数のみ示す. $e = 3$ のとき 2 個. $e = 4$ のとき 2 個. $e = 5$ のとき 1 個. $e = 6$ のとき 1 個.

12.8. 頂点数 n に関する数学的帰納法で証明する. $n = 1$ のとき明らか. $n \geq 1$ として頂点数 n のアサイクリックなグラフについて主張が正しいとする. 頂点数 $n + 1$ のアサイクリックなグラフ G を考える. 最長の有向路 L を考えれば, 有向閉路がないという仮定から, L の終点から出てゆく有向辺はない. この終点の番号を $n + 1$ として, この終点とこの終点につながっている辺をすべて取り除いたグラフを G' とする. G' は頂点数 n のアサイクリックなグラフであるから, 帰納法の仮定から, その隣接行列が下三角になるような頂点の番号付けが可能である. こうして, G の頂点すべてに番号がついた. G の隣接行列 A について, $i, j \in \{1, 2, \dots, n\}$ で $i < j$ なら $(A)_{ij} = 0$ である. さらに, $n + 1$ から出て行く有向辺がないので, すべての i に対して $(A)_{i, n+1} = 0$ である. よって, A は下三角行列である.

12.9. $\text{Tr}(A^m) = \sum_{x \in V} (A^m)_{xx}$ に注意すればよい. x からそれ自身への長さ 1 の歩道は存在しないから $\text{Tr}(A) = 0$. x からそれ自身への長さ 2 の歩道の個数は, x から出ている辺の個数に一致する. よって, $\text{Tr}(A^2) = 2|E|$. x からそれ自身への長さ 3 の歩道の個数は, x を含む三角形の個数の 2 倍 (回り方が 2 通りある). したがって, $\text{Tr}(A^3)$ はすべての頂点について, そのような歩道の和であるが, 1 つの三角形は 6 回数えられることになる.

12.10. 次の簡単な事実を確認しておこう.

(i) 連結な有限グラフ $G = (V, E)$ において, 連結性をたもったまま 1 頂点を削除できる. つまり, 頂点 $a \in V$ で $G' = G[V \setminus \{a\}]$ が連結グラフになるものが存在する. 実際, V から任意の 1 頂点を選んで x_1 とし, x_1 と辺で結ばれている頂点を $x_2, \dots, x_k$, それらと辺で結ばれている頂点を $x_{k+1}, \dots, x_l$ というように, V の頂点に番号付けをする. このとき, G の誘導部分グラフ $G_m = G[\{x_1, x_2, \dots, x_m\}]$ はすべて連結である. V の頂点で最後の番号をもつものを a とすればよい.

(ii) 連結な有限グラフ $G = (V, E)$ において, $|E| \geq |V| - 1$ が成り立つ. $|V|$ に関する帰納法で示す. まず, $|V| = 1$ のときは, 1 頂点のみからなるグラフであるから $|E| = 0$ は明らか. この場合は, $0 = 0$ として $|E| \geq |V| - 1$ が成り立っている. $|V| = n$ のとき, 主張が正しいとして, $|V| = n + 1$ の場合も正しいことを示す. さて, $G = (V, E)$ を連結な有限グラフで $|V| = n + 1$ とする. (i) で述べたように, $G' = (V', E') = G[V \setminus \{a\}]$ が連結グラフになるような $a \in V$ をとる. 帰納法の仮定により,

$$|E'| \geq |V'| - 1$$

である. また, G' の作り方から

$$|V'| = |V| - 1, \quad |E'| \leq |E| - 1.$$

したがって,

$$|E| - 1 \geq |E'| \geq |V'| - 1 = |V| - 2.$$

よって, $|E| \geq |V| - 1$.

以上の2つの事実から, 定理 12.10 (2) $\implies$ (1) を示すのは易しい. $|V|$ に関する帰納法で示そう. $|V| = 1$ のときは明らか. $|V| = n$ のとき, 主張が正しいとして, $|V| = n + 1$ のときも正しいことを示す. さて, $G = (V, E)$ を連結な有限グラフで $|V| = n + 1$, $|E| = n$ とする. (i) で述べたように, $G' = (V', E') = G[V \setminus \{a\}]$ が連結グラフになるような $a \in V$ をとる. このとき, $|V'| = n$, $|E'| \leq n - 1$ となる. (ii) の不等式を G' に適用して,

$$n - 1 \geq |E'| \geq |V'| - 1 = n - 1.$$

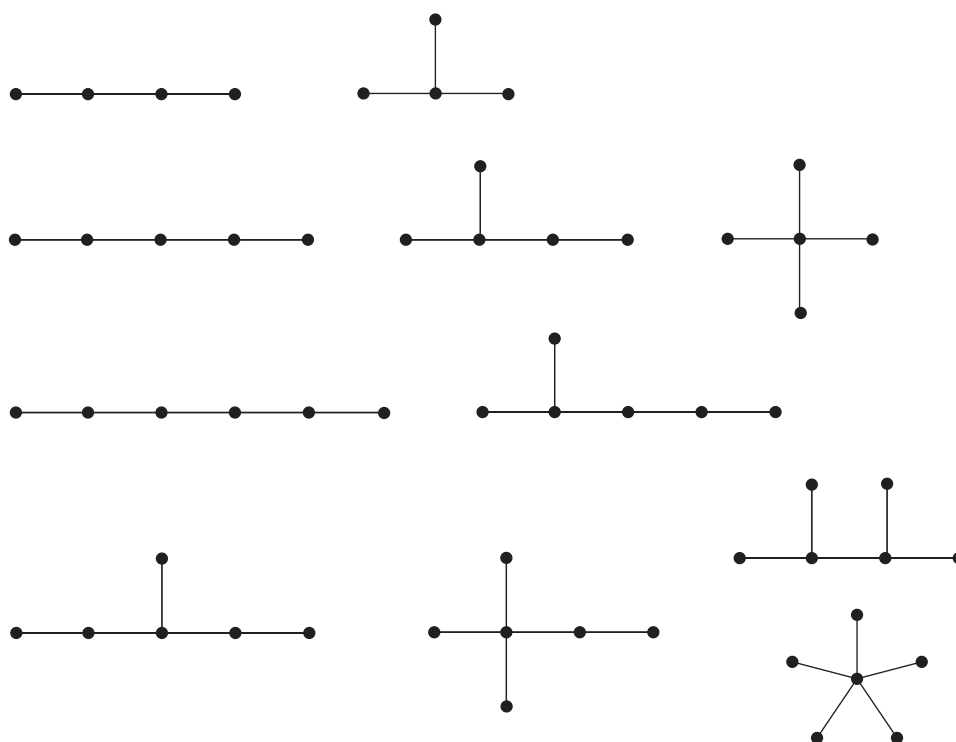
したがって, 上の不等式はすべて等式となり, $|E'| = |V'| - 1 (= n - 1)$. さらに, 帰納法の仮定によって, G' は木である. さて, G と G' の差異をみると,

$$|V| = |V'| + 1, \quad |E| = |E'| + 1$$

となっている. これは $\deg(a) = 1$ を示す. つまり, G は G' に頂点 a を加えて, a と G' の1頂点を辺1本で結んでできたグラフである. よって, G も木である.

12.11. 木の定義に基づいて考えよ.

12.12. 頂点数 4 の木は 2 個. 頂点数 5 の木は 3 個. ちなみに, 頂点数 6 の木は 6 個.



12.13. 定理 12.11 の証明と定理 12.12 の前半の証明を見直せ.

12.14. 可能.

12.15. 行列に関する等式 $P^{n-m} = P^{l-m}P^{n-l}$ を成分で書けば,

$$(P^{n-m})_{ij} = \sum_{k \in S} (P^{l-m})_{ik} (P^{n-l})_{kj}$$

を得る.

12.16. $P(T_0 = 1|X_0 = 1) = 1 - p$, $P(T_0 = n|X_0 = 1) = p(1 - q)^{n-2}q$ ($n \geq 2$). したがって, $P(T_0 < \infty|X_0 = 1) = 1$ となり, 状態 0 は再帰的である. 状態 1 についても同様.

12.17. $\pi = [\alpha \ 0 \ 0 \ 1 - \alpha]$ ($0 \leq \alpha \leq 1$)

13 グラフのスペクトル

13.1. V の頂点を $a, b, \dots$ の順序に番号付けをして, 隣接行列を書き下せば,

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & * & \cdots & * \\ 0 & * & & & \\ \vdots & \vdots & & A'' & \\ 0 & * & & & \end{bmatrix}, \quad A' = \begin{bmatrix} 0 & * & \cdots & * \\ * & & & \\ \vdots & & A'' & \\ * & & & \end{bmatrix}$$

ここで, A'' は G'' の隣接行列, A から第 1 行と第 1 列を削除した A' は G' の隣接行列である. $|\lambda E - A|$ を第 1 行で余因子展開することで,

$$\varphi_G(\lambda) = |\lambda E - A| = \lambda \varphi_{A'}(\lambda) + \begin{vmatrix} -1 & * & \cdots & * \\ 0 & & & \\ \vdots & & \lambda E - A'' & \\ 0 & & & \end{vmatrix}$$

したがって, $\varphi_G(\lambda) = \lambda \varphi_{G'}(\lambda) - \varphi_{G''}(\lambda)$.

13.2. $V_1 = \{1, 2, \dots, p\}$, $V_2 = \{p+1, \dots, n\}$ のように番号付けをする. V_1 に属する頂点間には辺がないので, すべての $i, j \in V_1$ に対して, $(A)_{ij} = 0$ である. 同様に, すべての $i, j \in V_2$ に対しても $(A)_{ij} = 0$ である. したがって, A は主対角ブロックが零行列 O であるようなブロック対角行列になる.

13.3. 二部グラフ G の隣接行列は

$$A = \begin{bmatrix} O & B \\ B^T & O \end{bmatrix}$$

の形にかける. A の 0 でない固有値の 1 つを $\lambda \neq 0$, それに対応する固有ベクトルを $\mathbf{v}$ とする. A のブロック分けに整合するように $\mathbf{v} = \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix}$ とすれば, $A\mathbf{v} = \lambda\mathbf{v}$ は,

$B\mathbf{y} = \lambda\mathbf{x}$, $B^T\mathbf{x} = \lambda\mathbf{y}$ と同値である. ここで, $\tilde{\mathbf{v}} = \begin{bmatrix} \mathbf{x} \\ -\mathbf{y} \end{bmatrix}$ を考えれば,

$$A\tilde{\mathbf{v}} = \begin{bmatrix} O & B \\ B^T & O \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ -\mathbf{y} \end{bmatrix} = \begin{bmatrix} -B\mathbf{y} \\ B^T\mathbf{x} \end{bmatrix} = \begin{bmatrix} -\lambda\mathbf{x} \\ \lambda\mathbf{y} \end{bmatrix} = -\lambda\tilde{\mathbf{v}}$$

がわかる.

次に, λ の重複度を m として, 1 次独立な固有ベクトルを $\mathbf{v}_1, \dots, \mathbf{v}_m$ とする. $\tilde{\mathbf{v}}_1, \dots, \tilde{\mathbf{v}}_m$ が 1 次独立であることを示そう.

$$\alpha_1\tilde{\mathbf{v}}_1 + \dots + \alpha_m\tilde{\mathbf{v}}_m = \mathbf{0}$$

を仮定する. $\mathbf{x}$ 成分と $\mathbf{y}$ 成分に分ければ,

$$\begin{aligned} \alpha_1\mathbf{x}_1 + \dots + \alpha_m\mathbf{x}_m &= \mathbf{0}, \\ \alpha_1(-\mathbf{y})_1 + \dots + \alpha_m(-\mathbf{y})_m &= \mathbf{0}. \end{aligned}$$

したがって,

$$\alpha_1\mathbf{v}_1 + \dots + \alpha_m\mathbf{v}_m = \mathbf{0}$$

が得られ, $\alpha_1 = \dots = \alpha_m = 0$ が従う.

- 13.4.** $K_{1,n}$ の特性多項式を $\varphi_n(\lambda)$ とする. 行列式 $|\lambda E - A|$ を余因子展開して, $\varphi_n(\lambda) = \lambda\varphi_n(\lambda) - \lambda^{n-1}$ がわかる. これから帰納的に, $\varphi_n(\lambda) = \lambda^{n-1}(\lambda^2 - n)$ が出る. したがって,

$$\text{Spec}(K_{1,n}) = \begin{pmatrix} -\sqrt{n} & 0 & \sqrt{n} \\ 1 & n-1 & 1 \end{pmatrix}$$

- 13.5.** P_3 の相異なる固有値は $\pm\sqrt{2}, 0$ であるから, 求める歩道の個数 $N_m = N_m(a, c)$ は, 適当な定数 c_1, c_2, c_3 によって $N_m = c_1(\sqrt{2})^m + c_2(-\sqrt{2})^m + c_30^m$ と表される. $N_0 = N_1 = 0$, $N_2 = 1$ を代入して定数を決めれば,

$$N_0 = 0, \quad N_m = \frac{1}{4} \{(\sqrt{2})^m + (-\sqrt{2})^m\}, \quad m = 1, 2, \dots$$

- 13.6.** 3 角形の相異なる固有値は, $-1, 2$ の 2 個である. したがって, 適当な定数 c_1, c_2 によって $N_m(a, b) = c_1(-1)^m + c_22^m$ のように表される. $N_0(a, b) = 0$, $N_1(a, b) = 1$ から定数を決めて,

$$N_m(a, b) = \frac{1}{3} \{2^m - (-1)^m\}, \quad m = 0, 1, 2, \dots$$

同様にして,

$$N_m(a) = \frac{1}{3} \{2(-1)^m + 2^m\}, \quad m = 0, 1, 2, \dots$$

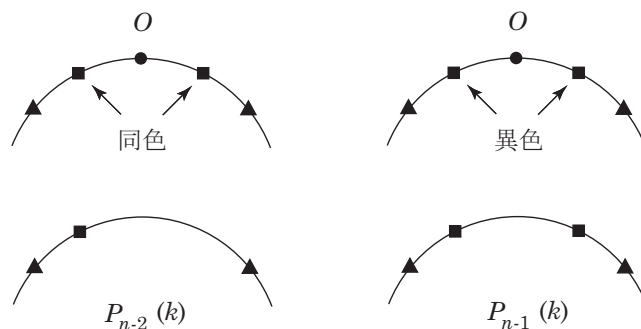
- 13.7.** 補題 13.14 から $\bar{d}(G) \leq \lambda_{\max}(G) \leq d_{\max}(G)$ であるが, G は κ -正則グラフであるから, $\bar{d}(G) = d_{\max}(G) = \kappa$. したがって, $\lambda_{\max}(G) = \kappa$ が成り立つ.

- 13.8. (1) 完全グラフ K_n を彩色するためには, 各頂点ごとに異なる色を配するほかない. したがって, $1 \leq k \leq n-1$ のときは, $P(K_n, k) = 0$. $k \geq n$ のときは,

$$P(K_n, k) = k(k-1)(k-2) \cdots (k-n+1).$$

(この式は, $1 \leq k \leq n-1$ でも通用する.)

- (2) $P_n(k) = P(C_n, k)$ とおく. C_n の 1 つの頂点 O に注目する. C_n の彩色は, 頂点 O の両側が同色であるか, 異色であるかで場合分けができる.



- (i) 頂点 O の両側が同色であるとき. O とその隣の頂点のうち 1 つを削除して C_{n-2} をつくと, 与えられた C_n の彩色は C_{n-2} の彩色を与える. 逆に, C_{n-2} の 1 つの彩色から, C_n の彩色で, 頂点 O の両側が同色であるものが $k-1$ 通り得られる. したがって, 頂点 O の両側が同色であるような C_n の彩色は

$$(k-1)P_{n-2}(k)$$

通りある.

- (ii) 頂点 O の両側が異色であるとき. O を削除して C_{n-1} をつくと, 与えられた C_n の彩色は C_{n-1} の彩色を与える. 逆に, C_{n-1} の 1 つの彩色から, C_n の彩色で, 頂点 O の両側が異色であるものが $k-2$ 通り得られる. したがって, 頂点 O の両側が異色であるような C_n の彩色は

$$(k-2)P_{n-1}(k)$$

通りある.

以上から,

$$P_n(k) = (k-2)P_{n-1}(k) + (k-1)P_{n-2}(k), \quad n \geq 3 \quad (13.1)$$

がわかる. 初期条件として

$$P_1(k) = 0, \quad P_2(k) = k(k-1) \quad (13.2)$$

がとれる. あとは, (13.1) を解けばよい. 移項して,

$$\begin{aligned} P_n(k) + P_{n-1}(k) &= (k-1)P_{n-1}(k) + (k-1)P_{n-2}(k) \\ &= (k-1)(P_{n-1}(k) + P_{n-2}(k)) \end{aligned}$$

となる. これを繰り返し用いて, 初期条件 (13.2) を考慮すれば,

$$\begin{aligned} P_n(k) + P_{n-1}(k) &= (k-1)^{n-2}(P_2(k) + P_1(k)) \\ &= (k-1)^{n-2}k(k-1) \\ &= k(k-1)^{n-1} \end{aligned} \quad (13.3)$$

がわかる. また, (13.1) から

$$\begin{aligned} P_n(k) - (k-1)P_{n-1}(k) &= -P_{n-1}(k) + (k-1)P_{n-2}(k) \\ &= -(P_{n-1}(k) - (k-1)P_{n-2}(k)) \end{aligned}$$

もわかる. これを繰り返し用いて, 初期条件 (13.2) を考慮すれば,

$$\begin{aligned} P_n(k) - (k-1)P_{n-1}(k) &= (-1)^{n-2}(P_2(k) + (k-1)P_1(k)) \\ &= (-1)^{n-2}k(k-1) \end{aligned} \quad (13.4)$$

がわかる. (13.3), (13.4) を連立させて解けば,

$$P_n(k) = (k-1)^n + (-1)^n(k-1)$$

が得られる. [注意: (13.1) は定係数の 3 項間漸化式であるから定石どおりに解くことができる.]

13.9. (1) φ_n と U_n の満たす漸化式を比較すればよい.

(2) $\varphi_n(\lambda) = 0 \Leftrightarrow U_n(\lambda/2) = 0$ に注意する. 第 2 種チェビシェフ多項式の定義によって,

$$U_n(\cos \theta) = \frac{\sin(n+1)\theta}{\sin \theta}$$

である. これは,

$$\theta = \frac{k\pi}{n+1}, \quad k = 1, 2, \dots, n$$

のとき 0 になる. しかも,

$$\cos \frac{k\pi}{n+1}, \quad k = 1, 2, \dots, n$$

は互いに異なる. $U_n(x)$ は n 次多項式であるから, $U_n(x) = 0$ の根は, 重複度をこめて丁度 n 個ある. よって,

$$x = \cos \frac{k\pi}{n+1}, \quad k = 1, 2, \dots, n$$

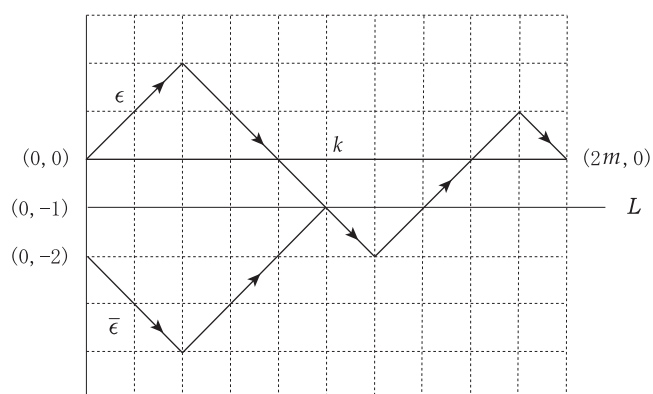
が $U_n(x) = 0$ の根を尽くす. したがって, $\text{Spec}(P_n)$ は $\lambda = 2 \cos k\pi/(n+1)$ ($k = 1, 2, \dots, n$) で, いずれも重複度 1 となる.

(3)

$$\begin{aligned}\lim_{n \rightarrow \infty} \int_{-\infty}^{+\infty} f(x) \mu_n(dx) &= \lim_{n \rightarrow \infty} \sum_{k=1}^n f\left(2 \cos \frac{k\pi}{n+1}\right) \frac{1}{n} \\ &= \int_0^1 f(2 \cos t\pi) dt = \frac{1}{\pi} \int_{-2}^2 f(x) \frac{dx}{\sqrt{4-x^2}}\end{aligned}$$

したがって, $\rho(x)dx$ は分散 2 の逆正弦則である.

- 13.10. (1) $(0,0)$ から $(2m,0)$ に至るすべての折れ線から, $y < 0$ を通過するものを引けばよい. 補助線 $y = -1$ を引いてみよ.



- (2) $(0,0)$ から始まって, 初めて x 軸に触れるときの x 座標で折れ線を分類すればよい.