代数学 I

@societah

2020 年 1 月

目 次

概 要

Twitter で見たシローの定理を背景とする自作問題をみて群論再考の機運が高まったため代数学 I の復習をする.

1 Groups

定義 1. 群 G の部分群 H が $H = gHg^{-1} = \{ghg^{-1} | h \in H\}$ を満たすとき H を G の正規部分群といい $H \triangleleft G$ とかく. H が G の正規部分群であることを示すには $\forall g \in G\ gHg^{-1} \subset H$ をいえばいい. 群 G の部分集合 H が部分群であるとは $\forall x, y (x, y \in H \Rightarrow xy^{-1} \in H)$ を満たすことである.

定義 2. $H \subset G$ を部分群とする. $a \in H$ に対して $aH = \{ax | x \in H\}, Ha = \{xa | a \in H\}$ とかきそれぞれ左剰余類, 右剰余類という. また部分集合 $X, Y \subset G$ に対して $XY = \{xy | x \in X, y \in Y\}, X^{-1} = \{x^{-1} | x \in X\}$ とかく. H を G の部分群としたとき $H^{-1} = H$ である.
また $a, b \in G$ に対して $a \sim b \Leftrightarrow Ha = Hb$ として G 上に関係 $\sim$ を定めると $\sim$ は同値関係である. $a \sim b \Leftrightarrow aH = bH$ で定まる関係も同値関係. それぞれの関係で G を割ったものを $G/\sim = H\backslash G, G/H$ とかく. $(Prop)$ H を G の部分群とする. $a \sim b \Leftrightarrow aH = bH$ で $\sim$ を定義するとき, $a \nsim b \Leftrightarrow aH \cap bH = \varnothing$ であり $aH \cap bH \neq \varnothing \Rightarrow aH = bH$ である. $(\because)$ $\exists c \in aH \cap bH$ とすると $c = ax = by (\exists x, y \in H)$ 任意に $d \in aH$ をとると $d = az (\exists z \in H)$ で $a = byx^{-1}$ より $d = b(yx^{-1}z) \in bH$ より $aH \subset bH$. 同様にして $aH = bH$.

命題 1. H が G の部分群であるとき $(i)|G/H| = |H\backslash G|$ $(ii)|G| = |H||G/H|$

証明. $(i)\varphi : G \to G; x \mapsto x^{-1}$で定める. $\varphi \circ \varphi = id$ よりφ は全単射である. $\varphi(H) = H^{-1} = H$ で $\varphi(Ha) = a^{-1}H$ であるから $Ha = Hb \Leftrightarrow a^{-1}H = b^{-1}H$. $\overline{\varphi} : H\backslash G \to G/H; Ha \mapsto \varphi(Ha) = a^{-1}H$ で定めることができる. $\overline{\varphi} \circ \overline{\varphi} = id_{H\backslash G}$である. すなわち$\overline{\varphi}$は全単射である. $(ii)\psi_a : H \to aH; x \mapsto ax (x \in H)$ で定まるψ_aは, 逆写像${\psi_a}^{-1}(y) = a^{-1}y$ の存在より全単射であるので $|H| = |aH|$. $G/H = \{a_1H, a_2H, ..., a_rH\}$(ただし $i \neq j$ なら $a_iH \neq a_jH$, $r = |G/H|$) とかける. $|G| = |a_1H| + \cdots + |a_rH| = |H| + \cdots + |H| = |H||G/H|$. 例えば $|\mathbb{Z}| = |n\mathbb{Z}||\mathbb{Z}/n\mathbb{Z}|$ である. □

定義 3. 正規部分群 $H \lhd G$ に対しては集合 $G/H, H\backslash G$ が群となる. 写像 $G/H \times G/H \to G/H; (xH)(yH) \mapsto xyH (x, y \in G)$ と定めるとこれは良定義. つまり写像が剰余集合の代表元の取り方にはよらないという $xH = x'H, yH = y'H \Rightarrow xyH = x'y'H (x', y' \in G)$ を満たす.
$x = x'h, y = y'h' (h, h' \in H)$ であるとする. $xy = x'hy'h'$であるが $H \lhd G :\Leftrightarrow \forall g \in G; gHg^{-1} \subset H$ という定義と $y'^{-1} \in G$ より $y'^{-1}hy' \in H$. よって $xy = x'y'(y'^{-1}hy')h' \in x'y'H \Leftrightarrow xyH = x'y'H$. よって示せた.

定義 4. 群Gと集合Xについて写像$G \times X \to X; (g, x) \mapsto g*x$があって任意の$g, h \in G, x \in X$に対して $(i)(gh)x = g(hx)$ $(ii)1_G x = x$ を満たすとき G は X に (左) 作用するという. G から X への作用が定まっているとき, G から X への全単射全体がなす群 $S(X)$ への準同型φ が $\varphi(g) : X \to X; \varphi(g)(x) := g * x (g \in G, x \in X)$ で定まる. $\varphi(g)$ は全単射であることが分かるので$\varphi(g) \in S(X)$ であり, 逆に準同型$\varphi : G \to S(X)$ が与えられたとき, G から X への作用 $G \times X \to X$ を $(g, x) \mapsto \varphi(g)(x)$ で定めることができる.
$Orb_G(x) = \{gx | g \in G\} = Gx$ を x の G による軌道という. 軌道分解 $X = \coprod_{i \in I} O(x_i)$ が与えれることは次のように $O(x) \cap O(y) \neq \varnothing \Rightarrow O(x) = O(y)$ よりわかる. $z \in O(x) \cap O(y)$ をとると $\exists g, h \in G; z = gx = hy$ である. $y = h^{-1}gx$. $O(y)$ の元は $gy (g \in G)$ で $gy = gh^{-1}gx \in O(x)$ とかけたので $O(y) \subset O(x)$. 同様に逆の包含も成り立つ.

定義 5. 群 G が集合 X に作用しているとき $Y \subset X, g \in G$ に対して $gY := \{gy \in X | y \in Y\}$ を Y の g 移動という.(軌道とは違って $g \in G$ は固定されている.) G の部分集合 $Stab_G(Y) = \{g \in G | gY = Y\}$ を Y の固定化部分群という. $Y = \{x\}$ のとき $G_x := \{g \in G | gx = x\}$ とかくことがある. G_xが G の部分群であることは次のようにわかる. $a, b \in G_x$とすると $ax = x, bx = x$ である. $(ab)x = a(bx) = ax = x$ より $ab \in G_x$. $a^{-1}(ax) = a^{-1}x, a^{-1}(ax) = (a^{-1}a)x = x$ より $a^{-1}x = x$ なので $a^{-1} \in G_x$. よって G_xは G の部分群である.
G が X に作用しているとき, X 上の関係 $\sim$ を $x \sim y \Leftrightarrow Gx = Gy$ で定めると $\sim$ は同値関係

である. また $x \in X$ に対して写像$\varphi : G/G_x \ni gG_x \mapsto g * x \in Orb_G(x)$ は全単射であり, ラグランジュの定理より $|Gx| = |G/G_x|$ である. $|G/G_x|$ は $[G : G_x]$ と表記されることもある. 明らかに全射であるが単射性も簡単に次でわかる. $ax = bx$ とすると, $a^{-1}b \in G_x$より $aG_x = bG_x$ であるのでφ は良定義である.

定義 6. G を群とする. G の G への作用 $G \times G \ni (g, x) \mapsto gxg^{-1} \in G$ を内部自己同型作用という. G の内部自己同型作用による軌道 $O_G(x) = \{gxg^{-1} | g \in G\}$ を G の共役類という. 上述より x を含む共役類は $G/C_G(S)$ と集合として同型である.
また $S \subset G$ としたときの $N_G(S) = \{a \in G | aSa^{-1} = S\}$ を正規化部分群といい,
$C_G(S) = \{a \in G | asa^{-1} = s(\forall s \in S)\}$ を中心化群という. $Z(G) = \{a \in G | axa^{-1} = x(\forall x \in G)\}$ を G の中心 (*center*) という. 中心の元 $a \in Z(G)$ の共役類はただ一つの元 $Orb_G(x) = \{x\}$ である.$\cdots(*)$ 特に G が *Abel* 群のときは $Z(G) = G$ より G の全ての共役類は一つの元からなる. この訳によって共役類の大きさは群の可換性を測る目安となる.

命題 2 ($(*)$ を示す)**.** 今後の多くの場面で x の共役類を一時的な表記ではあるが $C_x = \{axa^{-1} | a \in G\}$ とかく. $axa^{-1} = a'ya'^{-1}$を考えて $C_x = C_y \Leftrightarrow \exists a \in G\ x = aya^{-1}$であるがとにかく $y \in C_x (\Leftrightarrow x \in C_y)$ のときに x と y は共役であるといい共役類は同値類をなす.
$(Prop) |C_x| = 1 \Leftrightarrow x \in Z(G)$ を示そう.

証明. $(\Leftarrow) x \in Z(G) \Leftrightarrow ax = xa(\forall a \in G)$. $y, z \in C_x$のとき $y = axa^{-1}, z = bxb^{-1}(\exists a, b \in G)$ である. $ax = xa$ より $y = axa^{-1} = xaa^{-1} = x$ で同様に $z = x$ なので $y = z = x$ より $C_x = \{x\}$ となる. $(\Rightarrow) |C_x| = 1$ なら $C_x = \{x\}$ である. $a \in G$ に対して $axa^{-1} \in C_x = \{x\}$ より $axa^{-1} = x$ で $x \in Z(G)$. □

注 1. G の部分群 H, H'に対して $gHg^{-1} = H'$となる $g \in G$ が存在するとき H と H'は共役な部分群であるという. また, $H \triangleleft N_G(H)$ で $N_G(H)$ は H を含む部分群で H が正規なもののうちで最大のものである.

命題 3. $x, y \in G$ に対して $x \sim_G y \Leftrightarrow x$ と y は共役として $\sim_G$ を定める. 群 G を共役類という同値関係で割ってできる $G/\sim = \{C_x | x \in G\}$ を考える. G を位数 n の有限群とし $G/\sim = \{C_1, C_2, ..., C_r\}$(ただし $\forall i, j (i \neq j \rightarrow C_i \neq C_j)$) とする. $|C_1| \geq |C_2| \geq \cdots \geq |C_k| > |C_{k+1}| = \cdots = |C_r| = 1$ とすると

$$|G| = \sum_{i=1}^{k} |C_i| + |Z(G)|$$

が成り立つ.

証明. $G = C_1 \sqcup \cdots \sqcup C_r$である. よって $|G| = \sum_{i=1}^{r} |C_i| = \sum_{i=1}^{k} |C_i| + r - k$. $C_j = C_{x_j} (\exists x_j \in G)$ に対して $|C_j| = 1 \Leftrightarrow x_j \in Z(G)$(ただし $k + 1 \leq j \leq r$) より $r - k = |Z(G)|$ □

補題 1. $H, N \subset G$ は部分群で $HN = NH$ を満たすとする. このとき HN も G の部分群.

証明. 勝手な $x, y \in HN$ をとると, $x = h_1n_1, y = n_2h_2$とおける. $xy = h_1(n_1n_2)h_2$. $h_1(n_1n_2) \in HN = NH$ より $h_1(n_1n_2) = n_3h_3$とおけ $xy = n_3h_3h_2 \in NH = HN$. また $x^{-1} = {n_1}^{-1}{h_1}^{-1} \in NH = HN$. よって HN は部分群である. □

定義 7. p を素数, G を群とする. $H \subset G$ は有限部分群とする. $|H| = p^r (r \geq 1)$ のとき H は p 群という. G は有限群で $|G| = p^n m$(ただし $gcd(p, m) = 1$) としこのとき部分群 $H \subset G$ が $|H| = p^n$ を満たすとき H は　G の $pSylow$ 群という. 部分群の位数は $|G|$ の約数だから $sylow\ p$ 群は G の極大 p 群である.

命題 4. $|G| = p^n m$ のとき G の $pSylow$ 群が少なくとも一つ存在する.

証明. $X = \{A \subset G | A$ は G の部分群で $|A| = p^n\}$ とおく. $g \in G$ の $A \in X$ への作用を $gA = \{ga | a \in A\} \in X$ とおく. X の定義より $|X| = {}_{p^n m}C_{p^n} \equiv \frac{\prod_{i=0}^{p^n m-1}(p^n m-i)}{\prod_{i=0}^{p^n-1}(p^n-i)}$. ところで一般に $k \in \mathbb{Z}$ に対し k が p^rの倍数で p^{r+1}の倍数でないとき $ord_p k = r$ とかく.($ord_p 0 = \infty$ と約束する)
${}_{p^n m}C_{p^n} \equiv m (\mathrm{mod} p)$ である.

(∵) 体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 上の二項展開で示す. ${}_pC_i = \frac{p!}{(p-i)!i!} = \begin{cases} 0 & \mathrm{mod} p (0 < i < p) \\ 1 & \mathrm{mod} p (i = 0, p) \end{cases}$ なので, 体 $\mathbb{F}_p$ 上の多項式整域 $\mathbb{F}_p[X]$ において $(1+X)^p = 1 + X^p$であるから $(1+X)^{p^n} = 1 + X^{p^n}$. m 冪すると $(1+X)^{p^n m} = 1 + mX^{p^n} + \cdots + {}_mC_i X^{p^n i} + \cdots$. よって

$$ {}_{p^n m}C_{p^n} \equiv m \ (\mathrm{mod} p) \tag{1.1} $$

(つまり $pa = 0 (a \in \mathbb{Z}/p\mathbb{Z})$ となるから $\mathbb{F}_p$上の多項式環 $\mathbb{F}_p[X, Y]$ の元として $(X+Y)^{p^n} = X^{p^n} + Y^{p^n}$が成立し $(X+Y)^{p^n m} = (X^{p^n} + Y^{p^n})^m = X^{p^n m} + mX^{(m-1)p^n} Y^{p^n} + \cdots$における係数と と $(X+Y)^{p^n m} = X^{p^n m} + \cdots + {}_{p^n m}C_i X^{(p^n m-i)} Y^i + \cdots$における $i = p^n$の場合の $X^{p^n(m-1)} Y^{p^n}$の係数${}_{p^n m}C_{p^n}$を比べているというだけなのが (1.1) である.)
すなわち $|X|$ と p は互いに素である. あるいは $ord_p : \mathbb{Q}^\times \to \mathbb{Z}; \frac{n_1}{n_2} \mapsto ord_p(n_1) - ord_p(n_2)$ で定義すると $\forall r, r' \in \mathbb{Q}^\times\ ord_a(rr') = ord_a(r) + ord_a(r')$ が成り立つ. このような関数値 $ord_p(r)$ は r の p 進付置 ($p - adic\ valuation$) と呼ばれている. 挙げた性質を示すには素因数分解の一意性を用いる. では初等整数論の基礎の基礎を手記風にまとめる. $(Prop) 1 < \forall a \in \mathbb{Z}$ は素因数をもつ. これは次による. $S := \{\ell \in \mathbb{Z} | \ell > 1, \ell | a\}$ とおく. $a \in S$ より $\varnothing \neq S \subset \mathbb{N}$ より最小元 $p \in S$ が存在する. $x|p$ かつ $x > 1$ ならば $x \in S$ であるが p の S における最小性から $x = p$. $\forall x (x|p$ ならば $x = p)$ ということは p は素数であるということである. $(Prop) a \in \mathbb{Z}, p$ を素数とすると $p|a$ または $d = gcd(a, p) = 1$ である. これは次による. $p \nmid a$ とすると $d|a$ より $d \neq p$ より $d = 1$. $(Prop) a_1, ..., a_n \in \mathbb{Z}$ で p を素数とするとき $p|a_1 \cdots a_n \Rightarrow \exists i; p|a_i$が成り立つ. 特に $q_1, ..., q_n$が素数のとき $p|q_1 \cdots q_n \Rightarrow \exists i; p = q_i$である. これは次による. 背理法で任意の $i \in \{1, ..., n\}$ に対して $p \nmid a_i$とする. $\forall i$ について $gcd(p, a_i) = 1$ より $gcd(p, a_1, ..., a_n) = 1$ となり矛盾. (Def) ただ単に $ord_p(a)$ は $v_p(a)$ とかくことにする. すなわち $a \in \mathbb{Z}$ に対して $p^i | a$ なる $0 \leq i \in \mathbb{Z}$ で最大のものを $v_p(a)$ とかく. $(Thm) \forall a (1 < a \in \mathbb{Z} \Rightarrow a = {p_1}^{n_1} \cdots {p_r}^{n_r})$ と表せる. ただし $p_1, ..., p_r$は相異なる素数であり, $\{p_1, ..., p_r\}$ は a の素因数全体の集合であって任意の $i \in \{1, ..., r\}$ に対して $v_p(a) = n_i$ が成り立つ. すなわち素因数分解は一意である.
これは一つには次の a についての帰納法によって示す. $a = 2$ のときは $r = 1, p_1 = 2, n_1 = 1$ とすればよい. $a \geq 3$ として $2 \leq b < a$ なる $b \in \mathbb{Z}$ に対しては素因数分解表示が可能であるとする. さて a の素因数のうち最小のものを p_1とする. $n_1 := v_{p_1}(a)$ とおくと $a = {p_1}^{n_1} b (1 \leq \exists b < a \in \mathbb{Z}, gcd(b, p) = 1)$. $b < a$ より帰納法の仮定から $b = {p_2}^{n_2} \cdots {p_r}^{n_r} (p_2, ..., p_r$は相異なる素数) とかけ $p_1 \nmid b$ なので $a = {p_1}^{n_1} \cdots {p_r}^{n_r}$である. $p_1, ..., p_r$が a の素因数であるのは自明であるけども逆に p が a の素因数であるとすると, $p|{p_1}^{n_1} \cdots {p_r}^{n_r}$なので補題

より $\exists i; p = p_i$である. これは $\{p_1, ..., p_r\}$ は a の素因数全体であってそれに限られることを意味する. 最後に任意の $i = 1, ..., r$ に対して $n_{p_i}(a) = n_i$を示す. ${p_i}^{n_i}|a$ なので少なくとも $n_i \leq v_{p_i}(a)$. そこで $n_i < v_{p_i}(a)$ と仮定すると, ${p_i}^{n_i+1}|a$ であるので $\exists b \in \mathbb{Z}; {p_i}^{n_i+1}b = {p_1}^{n_1} \cdots {p_i}^{n_i} \cdots {p_r}^{n_r}$. よって $p_i b = {p_1}^{n_1} \cdots {p_{i-1}}^{n_i-1} {p_{i+1}}^{n_{i+1}} \cdots {p_r}^{n_r}$. p_iは $p_1, ..., p_{i-1}, p_{i+1}, ..., p_r$のどれかに一致するがこれは矛盾である. □

補題 2. p 進付置の加法についての性質を示すために, まず「$a \in \mathbb{Z}, p$ を素数としたときに $v_p(a) = n \Leftrightarrow \exists a' \in \mathbb{Z} s.t. a = p^n a'$かつ $gcd(p, a') = 1$」をいう. これは次による. $(\Rightarrow) p^n|a$ より $\exists a' \in \mathbb{Z}; a = p^n a'$と表す. もし $p|a'$ならば $p^{n+1}|a$ となって $v_p(a) = n$ に反するから $p \nmid a'$ となって $gcd(p, a') = 1$ である. $(\Leftarrow) p^{n+1} \nmid a$ を言いたい. もし $p^{n+1}a$ ならば $\exists a'' \in \mathbb{Z}; a = p^{n+1}a''$. $p^{n+1}a'' = p^n a'$より $pa'' = a' \Leftrightarrow p|a'$.($p$ と a'は互いに素であるのに反した)
$(Thm) a_1, ..., a_r \in \mathbb{Z}, p$ を素数とする.

$$v_p(a_1 \cdots a_r) = v_p(a_1) + \cdots + v_p(a_r)$$

が成り立つ. $(\because) n_i = v_p(a_i)$ とおくと

$$\exists {a_i}' \in \mathbb{Z}; a_i = p^{n_i} {a_i}' \text{かつ } gcd(p, {a_i}') = 1$$

このとき $a_1 \cdots a_r = p^{n_1+\cdots+n_r}({a_1}' \cdots {a_r}')$(ただし $gcd(p, {a_1}', ..., {a_r}') = 1$ である) すなわち $v_p(a_1 \cdots a_r) = n_1 + \cdots + n_r$が成り立つ.

さて, 話を $|X|$ と p が互いに素であることをいうための証明はこの p 進付置の性質を使うこともできるということに戻そう. ところで p 進付置は彌永昌吉『集合と位相Ⅱ』を参考とした.

$$ord_p|X| = \sum_{i=0}^{p^m-1} \Big(ord_p(p^n m - i) - ord_p(p^n - i) \Big) = 0$$

よって, $|X|$ と p は互いに素である.
$A \in X$ をとり群による軌道と固定部分群 $GA = \{gA \in X | g \in G\}, G_A = \{g \in G | gA = A\}$ を考える. $|GA| = |G/G_A| = |G_A \backslash G|$(特に G が有限群のときは $|GA|$ は $|G| = p^n m$ の約数) であり X は群 G によって $A_1, ..., A_r \in X$ として次のように軌道分解される. $X = GA_1 \sqcup \cdots \sqcup GA_r$. $gcd(|X|, p) = 1$ よりもし任意の i について $gcd(|GA_i|, p) \neq 1$ とすると $|X| \perp p$ に反するので $gcd(|GA_i|, p) = 1$ となる $i \in \{1, ..., r\}$ が存在する. この i に注目する. そのような i が存在し $|G_{A_i}||GA_i| = |G| = p^n m$ ゆえに $|G_{A_i}|$ は p^nの倍数であり $|GA_i|$ は m の約数である. 次に $a_0 \in A_i$ を固定する. $g \in G_{A_i}$に対して $ga_0 \in A_i$を対応させる写像 $f : G_{A_i} \ni g \mapsto ga_0 \in A_i$は単射であるから $|G_{A_i}| \leq |A_i| = p^n$. $|G_{A_i}|$ は p^nの倍数でもあったから $|G_{A_i}| = p^n$となり $pSylow$ 群 G_{A_i}の存在がいえた.

補題 3. 群の同型定理とはすべていわゆる準同型 $f : G \to f(G)$ に対する $f(G) \cong G/ker(f)$ から同等に導かれる次のものたちをさす.
(i) $f : G \to G'$を全射準同型, $H' \triangleleft G'$とするとき, $f^{-1}(H') \triangleleft G$が成り立ち同型写像$G/f^{-1}(H') \cong G'/H'; xf^{-1}(H') \mapsto f(x)H'$が存在する.
(ii) H, N を G の部分群とし $N \triangleleft G$ とするとき, HN は G の部分群であり (すでに示した.) $N \triangleleft HN, H \cap N \triangleleft H$ が成り立つ. 同型写像 $H/(H \cap N) \cong HN/N; h(H \cap N) \mapsto hN$ が存在する.
$(iii) H, N \triangleleft G$ で $N \subset H$ とするとき, $G/H \cong (G/N)/(H/N)$.

定理 1. $|G| = p^n m$(ただし $gcd(p,m) = 1$) とする. また H は G の p 群 (すなわち $|H| = p^r$ とかける) とする. このとき
(*i*)H を含む G の *pSylow* 部分群が存在する.
(*ii*)G のすべての *pSylow* 群は互いに共役である. つまり *pSylow* 群 P_1, P_2に対して $\exists g \in G; gP_1g^{-1} = P_2$である.
(*iii*)G の *pSylow* 群の個数を s とすると s は $|G|$ の約数で $s \equiv 1 (\mathrm{mod}\ p)$

証明. $P_0 \subset G$ を一つの *pSylow* 群とし $Y = \{P \subset G | \exists g \in G\ P = gP_0g^{-1}\}$ とおく. N を G の部分群とし軌道と固定群をそれぞれ前と別の記号で一般に $O_N(P) = \{gPg^{-1} | g \in N\}$, $Stab_N(P) = \{g \in N | gPg^{-1} = P\}$ とかく. これは [4] では「G の内部自己同型作用による G 軌道」と呼ばれている. 一般に $|O_N(P)||Stab_N(P)| = |N|$. いま $N = G$ の場合を考えると $|O_G(P_0)||Stab_G(P_0)| = |G| = p^n m$. $x \in P_0$なら $xP_0x^{-1} = P_0$より $P_0 \subset Stab_G(P_0)$(部分群) で $|P_0| = p^n$より $|Stab_G(P_0)|$ は p^n の倍数である. 定義より $O_G(P_0) = Y$ だから $|O_G(P_0)| = |Y|$ は m の約数で p と互いに素である.
次は $N = H$ の場合を考える. $|H| = p^r$ より $|O_H(P_0)| = p^k (\exists k \leq r)$ である. $P_1, P_2 \in Y$ に対して $O_H(P_1) \cap O_H(P_2) \neq \varnothing \Rightarrow O_H(P_1) = O_H(P_2)$ よりある $P_1, ..., P_t \subset Y$ が存在して Y の軌道分解 $Y = O_H(P_1) \sqcup \cdots \sqcup O_H(P_t)$ を得る.(ただし $|O_H(P_i)| = p^{k_i}$) $gcd(|Y|, p) = 1$(いや, Y はある *pSylow* 群と共役な群全体という定義であり (2) が正しいなら上述の X と Y は一致するからそれは $gcd(|Y|, p) = 1$ であるが.) より $k_i = 0$ となる i が存在する. つまりある i に対して $O_H(P_i) = \{P_i\}$ である. この P_iを改めて以下では P とかこう. すると $O_N(P)$ の定義より $\forall g(g \in H \Rightarrow gPg^{-1} = P)$ である. $gP = Pg$ で $HP = PH$ が成り立つ. 補題より HP は G の部分群である. また任意の $g \in HP$ に対して $gPg^{-1} \subset P$. よって $P \lhd HP$ で同型定理 (*ii*) より

$$HP/P \cong H/(H \cap P)$$

よって $|H||P| = |HP||H \cap P|$ であり特に $|HP| = p^\ell$とかける. 自明に $P \subset HP$ より $n \leq \ell$が成り立つ. 他方で HP は G の部分群より p^ℓは $|G| = p^n m (p, m$ は互いに素) の約数であることから $\ell \leq n$. よって $\ell = n$ である. $|HP| = p^n$, $H \subset HP = P$. 従って P は H を含む *pSylow* 群である.
(*i*) はこれで終わった. (*ii*) は次で終わる. P_0と P_1を任意の *pSylow* 群とする. H は (*i*) では p 群ではあるがここで適当に $H = P_1$として (*i*) の証明を見ると, H を含む *pSylow* 群 $P \in Y$ となるものがあるということなので, Y の定義より P_0と P_1は共役である.
(*iii*) を示す. (*ii*) より Y は G の *pSylow* 群全体の集合であるから $s = |Y|$. $Y = O_N(P_1) \sqcup \cdots \sqcup O_N(P_t), |O_N(P_i)| = p^{k_i}$であった. $k_1 = \cdots = k_n = 0 < k_{n+1} \leq \cdots \leq k_t$と仮定してよく, $n \geq 2$ として矛盾を導く.
すべての *pSylow* 群は共役であることから $\forall i = 1, ..., t$ に対して $P_0 \in O_N(P_i)$ である. $i \leq n$ のとき $P_0 \in O_N(P_i) = \{P_i\}$ より $P_0 = P_i$. $n \geq 2$ ならば $P_0 = P_1 = P_2$で $O_N(P_1) \cap O_N(P_2) = \varnothing$と矛盾. よって $s = 1 + p^{k_2} + \cdots + p^{k_t} \equiv 1$. □

定義 8. G と H が群のとき集合 $G \times H$ には $1_{G\times H} = (1_G, 1_H)$ や逆元があり自然に群となる. $f : G \to G \times H; x \mapsto (x, 1_H)$, $g : G \times H \to H; (x, y) \mapsto y$ で定めると

$$1 \to G \xrightarrow{f} G \times H \xrightarrow{g} H \to 1$$

は明らかに完全系列 (*exact*) である.
$h = (h, 1), n = (1, n) \in H \times N$ とみなすとき $hn = (h, n)$ であるのに注意.

補題 4. H, N を G の部分群とする. $G = H \times N \Leftrightarrow$ (1) 任意の $h \in H, n \in N$ に対して $hn = nh$ (2)$\forall g \in G \exists h \in H \exists n \in N; g = hn$ (3)$h_1 n_1 = h_2 n_2 \Rightarrow h_1 = h_2, n_1 = n_2$.

証明. ($\Rightarrow$) 上の注意事項より (1)$hn = (h, 1)(1, n) = (1h, n1) = (1, n)(h, 1) = nh$. (3)$(h_1, n_1) = h_1 n_1 = h_2 n_2 = (h2, n_2)$ ならば $h_1 = h_2, n_1 = n_2$である. ($\Leftarrow$)$\varphi : H \times N \to G; (h, n) \mapsto hn$ と定めるとφ は$\varphi(h_1 h_2, n_1 n_2) = h_1 h_2 n_1 n_2 = \varphi(h_1, n_1)\varphi(h_2, n_2)$ と準同型である. (2) はφ が全射なのをいい (3) は単射であるのをいう. □

命題 5. $H_1, ..., H_n \subset G$ を部分群とするとき $G = H_1 \times \cdots \times H_n \Leftrightarrow$ (1)$H_i \triangleleft G (\forall i)$ かつ (2)$G = H_1 \cdots H_n$かつ (3)$(H_1 H_2 \cdots H_{i-1}) \cap H_i = \{1\} (\forall i = 1, ..., n)$ である.

証明. 前補題より n に関する帰納法で従う. $n = 2$ の場合について $H = H_1, N = H_2$とかく. $H \triangleleft G, H \subset N$ より $H \triangleleft N \Leftrightarrow \forall n \in N; nH = Hn$ より $HN = NH$. $G = HN = NH$, (3) より $H \cap N = \{1\}$. 補題の (1) の $nh = hn (h \in H, n \in N)$ を示す. $hnh^{-1}n^{-1} = h(nh^{-1}n^{-1}) = (hnh^{-1})n^{-1} \in H \cap N = \{1\}$. よって $hn = nh$ である. 補題の (3) を示す. $h_1, h_2 \in H, n_1, n_2 \in N$ とし $h_1 n_1 = h_2 n_2$とする. $1 = h_1 n_1 {n_2}^{-1} {h_2}^{-1} = (h_1 {h_2}^{-1})(n_1 {n_2}^{-1})$ より $h_2 {h_1}^{-1} = n_1 {n_2}^{-1} \in H \cap N$ より, $h_1 = h_2, n_1 = n_2$である. 補題の仮定がすべて満たされて $G = H \times N$. 次に $n \geq 3$ として $n - 1$ まで正しいと仮定する.
正規部分群の性質のいくつかのまとめ $\to$ (*i*)$K \triangleleft G, K \subset H$ ならば $K \triangleleft H$ (*ii*) $H, K \triangleleft G$ ならば $H \cap K \triangleleft G$ (*iii*) すでに示したが, 群 G の部分群 H と G の正規部分群 N に対して HN は G の部分群. (*iv*) 正規性は群の直積をとっても保存される.
この (*iv*) より, $N = H_1 H_2 \cdots H_{n-1} \subset G$ とおいたとき $H_i \triangleleft G$ より $N \triangleleft G$ である. また (*i*) ゆえに $i \neq n$ の i に対して $H_i \triangleleft N$. 帰納法の仮定から $N = H_1 \times \cdots \times H_{n-1}$である. (3) でいう $N \cap H_n = \{1\}$ が成り立つ. $n = 2$ の場合より $G = N \times H_n = (H_1 \times \cdots \times H_{n-1}) \times H_n$. □

命題 6.

$$1 \to H \xrightarrow{f} G \xrightarrow{g} N \to 1 \ (exact)$$

において次の (1) から (3) は同値.
(1) ある準同型 $h : G \to H$ が存在して $h \circ f = id_H : H \to H$ を満たす.
(2) ある準同型 $n : N \to G$ が存在して $N' = \mathrm{Im}\, n \triangleleft G$ であり $g \circ n = id_N$.
(3) N と同型な G の部分群 N'が存在して, $G = f(H) \times N'$.

注 2 (R 加群の split)**.** R を可換環とし

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

を R 加群の短完全列とする. (*i*) から (*iii*) はすべて同値でありいずれか一つ (よって全て) が成り立つときに完全列は分裂するという.
(*i*) $B \cong A \oplus C$ である.
(*ii*) ある R 準同型 $i' : C \to B$ で $p \circ i' = id_C$となるものがある.
(*iii*) ある R 準同型 $p' : B \to A$ で $p' \circ i = id_A$となるものがある.
また, C が自由加群のときは完全列は分裂することが示される. これの解答に相当するものは Google ドライブに保存した.

証明. 命題 6 について. 完全系列は群とその間の準同型がかかれていることに注意. (1) ⇒ (3) については $N' = \mathrm{Ker}\, h, H' = \mathrm{Im}\, f = \mathrm{Ker}\, g$ とおく. f は単射なので $f : H \xrightarrow{\simeq} H'$ と群同型写像である. $g' := g|_{N'} : N' \ni x \mapsto g(x) \in N$ とおく.

$$\begin{array}{ccc} H & \xrightarrow{\quad f \quad} & H' \\ & {\scriptstyle id_H} \searrow \quad \cup \quad \swarrow {\scriptstyle h} & \\ & H & \end{array} \tag{1.2}$$

$\forall z \in H' \cap N'$をとる. $z \in N' = \mathrm{Ker}\, h$ より $h(z) = 1$. $z \in H'$であるので $z = f(h(z)) = f(1) = 1$ (ただし準同型は単位元を単位元に写すことに注意.) よって $H' \cap N' = \{1\}$. 次に $G = H'N'$を示す. 任意に $z \in G$ をとる. $x := f(h(z)) \in H'$. $y := x^{-1}z \in G$ とおくと $x \in H'$より $x^{-1} \in \mathrm{Ker}\, g$ なので $g(y) = g(x^{-1})g(z) = g(z)$. また $f(h(y)) = f(h(x^{-1}))f(h(z)) = x^{-1}x = 1$ なので $y \in N'$である. よって $z = xy \in H'N'$で $G = H'N'$. 明らかに $N' = \mathrm{Ker}\, h \lhd G, H' = \mathrm{Ker}\, g \lhd G$ であり前命題より $G = H' \times N'$が成り立つ.
(3) ⇒ (1) まず群の直積について約束事をかく. H_iを群として $G = H_1 \times \cdots \times H_n$に対して $l_k : H_k \ni h_k \mapsto (1, ..., 1, h_k, 1, ..., 1) \in G$ で単射 l_kを定めると l_kを包含写像とみなして $H_k \subset G$ とみなす. つまりは $h_k \in H_k$と $(1, ..., 1, h_k, 1, ..., 1) \in G$ を同一視する. (3) の仮定から $G = f(H) \times N' \ni (x, y)$(ただし $\exists x' \in H$ があって $x = f(x')$ とかいた). $h : G \to H$ を $h(x, y) = x'$で定義すると $h \circ f(x') = h(x, 1) = x'$. つまり $h \circ f = id_H$である.
(2) ⇒ (3) を示す. $g \circ n = id_N$より n は単射である. (これは簡単に $g \circ n$ が単射なら言える) $N' = \mathrm{Im}\, n \subset G$ とおく. $H' = \mathrm{Im}\, f = \mathrm{Ker}\, g \lhd G$ とかく.

$$\begin{array}{ccc} N & \xrightarrow{\quad n \quad} & N' \\ & {\scriptstyle id_N} \searrow \quad \cup \quad \swarrow {\scriptstyle g|_{N'}} & \\ & N & \end{array} \tag{1.3}$$

$G = H'N'$と $H' \cap N' = \{1\}$ であることを順にいう. 任意に $z \in G$ をとる. $y := n(g(z)) \in N' \subset G$ とおき $x = y^{-1}z \in G$ とおく. $n(g(x)) = n(g(y^{-1}))n(g(z)) = y^{-1}y = 1$ より $g(x) = 1$ で $x \in \mathrm{Ker}\, g = \mathrm{Im}\, f = H'$. よって $z = y^{-1}x \in N'H'$である. さて $H' \lhd G$ より $N'H' = H'N'$なので $G = H'N'$である.
次に任意に $z \in H' \cap N'$をとると $z \in H'$より $\exists x \in H; z = f(x)$. $g(z) = g(f(x)) \overset{f(x) \in H' = \mathrm{Ker}\, g}{=} 1$. $z = 1$ より $H' \cap N' = \{1\}$.
同値性はこれですべていえたことであるが (3) ⇒ (2) は, $G = H' \times N'$で $g|_{N'} : N' \xrightarrow{\cong} N$ であり次のように $n : N \to G$ を定めればいい.

$$y \in N \text{ として } n(y) = (g|_{N'})^{-1}(y) \in N' \subset G$$

□

定義 9. 高校生にとっても常識的であるが, $x, y \in \mathbb{Z}$ に対して $ax + by = d$ であって $gcd(a, b) = d$ を満たす $a, b \in \mathbb{Z}$ が存在する. 有限アーベル群に対しては演算を $+$ でかくことにし, 単位元は 0 で $x \in G$ に対する逆元は $-x$ でかくことにする. また $x \in G$ に対し $nx = 0$ を満たす最小の自然数 n を x の位数といい $n = ord(x)$ とかく. 群の元 a の位数とは $a^m = 1$(アーベル群の場合は 0 と表記) であるような m で最小の正の整数であり, そのような m が存在しなければ a の位数は ∞ であるという. 元 a の位数は $|a|$ とかくこともある.

命題 7 (中国剰余定理)**.** $l, n \in \mathbb{N},\ gcd(l,n) = 1$ ならば $\mathbb{Z}/ln\mathbb{Z} \cong \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ である.

証明. $x \in \mathbb{Z}$ とする. まずは写像φ を$\varphi : \mathbb{Z}/ln\mathbb{Z} \ni x + ln\mathbb{Z} \mapsto (x + l\mathbb{Z}, x + n\mathbb{Z}) \in \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ で定義するとφ は準同型. $gcd(l,n) = 1$ より $la + nb = 1$ を満たす $a, b \in \mathbb{Z}$ がある. $(y + l\mathbb{Z}, z + n\mathbb{Z}) \in \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} (y, z \in \mathbb{Z})$ に対し $x := nby + laz$ とおくと $1 = la + nb \equiv nb (\mathrm{mod}\ l)$ より $x \equiv 1y = y (\mathrm{mod}\ l)$. 同様に $x \equiv z (\mathrm{mod}\ n)$ でありよって$\varphi(x + ln\mathbb{Z}) = (y + l\mathbb{Z}, z + n\mathbb{Z})$ となり φ は全射. 全射かつ $|\mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}| = ln = |\mathbb{Z}/ln\mathbb{Z}|$ なのでφ は同型. □

定義 10. R を可換環とする. I, J を R のイデアルとする. $I + J := \{x + y | x \in I, y \in J\},\ IJ := \{\sum_i^r x_i y_i | x_i \in I, y_i \in J\}$ でイデアル同士の演算を定める. すると

(1) $I \cap J$ は R のイデアル (2) $I + J$ は $I \cup J$ を含む最小のイデアル (3) IJ はイデアルで $IJ \subset I \cap J$

であることがすぐに従う. たとえば (3) は次のように終わる.
$\sum_i^r x_i y_i + \sum_j^s x_j' y_j' = \sum_i^{r+s} x_i y_i \in IJ$(ただし $j = 1, ..., s$ に対し $x_{r+j} = x_j', y_{i+j} = y_j'$) より IJ は部分加群. $z \in R$ に対して, $z(\sum_i^r x_i y_i) = \sum_i^r (z x_i) y_i \in IJ$ より IJ はイデアル.

注 3. R の I, J が互いに素とは $I + J = R$ となることである. $I + J$ が互いに素なとき

(1) $IJ = I \cap J$ (2) 自然な環準同形 $R/I \cap J \to R/I \times R/J$ は同形である.

なぜなら, $IJ \subset IR \subset I, IJ \subset J$ より $IJ \subset I \cap J$ は常に成り立つ. 逆は $x \in I, y \in J, x + y = 1$ を満たすものをとる. 任意の $z \in I \cap J$ に対して $z = 1z = (x+y)z = xz + yz \in IJ$ より $I \cap J \subset IJ$ である. (2) 単射なのは明らかなので全射であることをいう. $x \in I, y \in J, x + y = 1$ とする.
任意の $a, b \in R$ に対し $z = ay + bx$ とおくと $z \equiv ay (\mathrm{mod}\ I) = a(1 - x) \equiv a (\mathrm{mod}\ I)$. 同様に $z \equiv b (\mathrm{mod}\ I)$ であるから写像を $z + I \cap J \mapsto (a + I, b + J)$ で定める.

有限アーベル群の構造定理についての復習をしたいがその前に整理すべき内容をかく.

注 4. (1) 位数という言葉は色々な使われ方がされていることに注意. a を群 G の位数 n の元としたとき, G の巡回部分群 $\langle a \rangle$ の位数は n であって $\langle a \rangle = \{1, a, a^2, ..., a^{n-1}\}$ である.
(2) a を位数 n の有限群 G の元とする. このとき a の位数は n の約数であり $a^n = 1$ である. ただちに, 有限群の元の位数も有限なのがわかる.
(3) a を群 G の位数 n の元とすると $a^m = 1 \Leftrightarrow n | m$ が成り立つ. $(Proof)$ $(\Leftarrow)$ ある $q \in \mathbb{Z}$ があって $m = nq$ より $a^m = (a^n)^q = 1$. $(\Rightarrow) a^m = 1$ とする. $\exists q, r$ があって $m = nq + r (0 \le r < n)$ で $a^m = a^{nq+r} = a^r = 1$. n は $a^n = 1$ となる最小の整数だから $r = 0$ で $n | m$.

注 5. 次の事実も確かめておく方がよいと思われる.
(4) *Abel* 群 G において位数が有限な元全体 H は G の部分群になる. なぜなら $a, b \in H$ の位数を m, n とする. $(ab)^{mn} = (a^m)^n (b^n)^m = 1,\ (a^{-1})^m = (a^m)^{-1} = 1$ より $ab, a^{-1} \in H$.
(5) G を位数 n の有限群, $a \in G$ とする. このとき $(i)\ G = \langle a \rangle \Leftrightarrow (ii)\ ord(a) = n$

補題 5. p は素数, $r \in \mathbb{N}, G$ は有限アーベル群で $|G| = p^r$ とする. このとき $\exists n \in \mathbb{N} \exists r_1, ..., r_n \in \mathbb{N}$ が存在し $r_1 + \cdots + r_n = r$ であって

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{r_n}\mathbb{Z}$$

である. このようにアーベル群の基本定理は G が p 冪のときに帰着する.

証明. rに関する帰納法で示す. $r=1$の場合, $0\neq x\in G$をとる. 注(2)より$ord(x)$は$|G|=p$の約数なので$ord(x)=1$又はpであるが$ord(x)=1$は$x=0$なので矛盾するから$ord(x)=p$. よって$G=\{x,2x,...,px=0\}\cong\mathbb{Z}/p\mathbb{Z}$. さて$r\geq 2$とし$|G|=p^e(e<r)$のとき補題は正しいとせよ. Gの中で位数最大の元をaとし$p^{r_1}=ord(a)$とする. もし$r_1=r$なら$G\cong\mathbb{Z}/p^r\mathbb{Z}$であるので$r_1<r$とする. $H=\langle a\rangle=\{ka|k=0,1,...,p^{r_1}-1\}\subsetneq G$とおく. ここで$b'\in G-H$をとる. 注(2)の「$a$を位数$n$の$\sim a^n=1$である」の箇所によって$|G|=p^r$であったのだから当然$p^rb'=0\in H$である. そこで$p^\ell b'\in H$となる最小の$\ell\in\mathbb{N}$をとる. 改めて$b:=p^{\ell-1}b'$とおくとその定義によって$b\notin H,\ pb\in H=\{ka|k\in\mathbb{N}\}$. よって$pb=ka$となる$k\in\mathbb{N}$をとる. もし$gcd(p,k)=1$とすれば$pb=ka$が$\langle a\rangle$を生成し$(H=\langle a\rangle=\langle pb\rangle)$, よって$ord(a)=ord(pb)\Leftrightarrow r_1=ord(b)-1$. これは$ord(b)>r_1$となり$a$が位数最大の元であることに矛盾する. よって$k$は$p$の倍数でありある$m\in\mathbb{N}$があって$k=pm$とかける.
すると$0=pb-ka=p(b-ma):=pc(c=b-ma$とおく$)$であるが, $pc=0$となり注(2)によってcの位数はp(素数)である. $b\notin H=\langle a\rangle$より$c\neq 0$. これより$N:=\langle c\rangle\cong\mathbb{Z}/p\mathbb{Z}$とおけ$N\lhd G$から$G'=G/N$とできる. $\pi:G\to G'$を自然な全射とすると$\pi(a)\neq 0$で$ord(\pi(a))=ord(a)$. $H'=\langle\pi(a)\rangle\subset G'$とおくと$\pi|_H:H\xrightarrow{\cong}H'\lhd G'$である. aはGの位数最大の元だからそれと同じ位数をもつ$\pi(a)$はG'の位数最大の元となる. 注(1)によって$H'\cong\mathbb{Z}/p^{r_1}\mathbb{Z}$であり次の$M'\subsetneq G$に対する帰納法の仮定(真部分集合なので)より

$$G'\cong H'\oplus\underbrace{\mathbb{Z}/p^{t_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p^{t_m}\mathbb{Z}}_{M'とおく}$$

とかける. すなわち$G'=H'\oplus M'$である. $M=\pi^{-1}(M')$とする. $\pi|_H:H\xrightarrow{\cong}H'$で$H\cap M=\{0\}$より$G=H\oplus M$である. Mもp群で再びMに帰納法の仮定を用いればMはp冪の巡回群の直和の形にかけて結論を得る. なお$H\cap M=\{0\}$は$\langle\pi(a)\rangle\cap M'=\{0\}$より$\langle a\rangle\cap M\subset\mathrm{Ker}\,\pi=\langle c\rangle$で$\langle a\rangle\cap M\subset\langle a\rangle\cap\langle c\rangle=\{0\}$から.

□

命題 8. Gを有限アーベル群とする. ある$n,r_1,...,r_n\in\mathbb{N}$と素数$p_1,...,p_n$があって$G\cong\mathbb{Z}/{p_1}^{r_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/{p_n}^{r_n}\mathbb{Z}$とかける. これは次のように, $e_1,...,e_n\geq 2$があって$G\cong\mathbb{Z}/e_1\mathbb{Z}\times\cdots\times\mathbb{Z}/e_n\mathbb{Z}$(ただし$\forall i=1,...,n-1$に対して$e_i|e_{i+1}$)と直和分解できるという様にもかける.

証明. $|G|$の約数である素数pをとりPをGの$pSyllow$群とする. つまり$|G|=p^rm$とすると$|P|=p^r$である.

$$H=\{x\in G|gcd(p,ord(x))=1\}$$

と定義するとHはGの部分群でありまた注(2)より$H\cap P=\{0\}$である. $gcd(p^r,m)=1$より$p^rs+mt=1$となる$s,t\in\mathbb{Z}$が存在する. $\forall x\in G$に対し$x_1:=mtx, x_2:=p^rsx$とおくと注(2)によって$p^rx_1=p^rm(tx)=0,\ mx_2=p^rm(sx)=0$である. 第二式より$x_2\in H$である. $ord(x_1)\neq 1$ならば$|\langle x_1\rangle|=p^e(\exists e\in\mathbb{N}_+)$である. x_1を含む$pSyllow$群P'をとるとPとP'は共役であるがGは$Abel$群なのでP'とPは一致する. なぜなら, $\exists g\in G; P'=g+P+(-g)=P$. よって$x=x_1+x_2\in P+H$. $G=P+H$で$P\cap H=\{0\}$, またGが$Abel$群なので$P,H\lhd G$より$P\oplus H$である. PはGの位数p冪の部分群なので前補題が適用できる. $|G|=p^rm$と仮定していたのであるがPは位数がp冪のGの部分群を全て含み, Hは位数がpと互いに素な部分群を全て含むことから以下の命題(1)によって証明は終わる. また以下の命題(2)にも留意すべきである. □

定義 11. 群 G の部分群 H は適当な部分群 K をとると $G = H \times K$ となるとき G の直積因子という. G が自身と $\{1\}$ 以外に直積因子を持たないとき G は直既約であるという.

命題 9. (1) $m = m_1 m_2 (m_1$ と m_2 は互いに素$) \Rightarrow G \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_1\mathbb{Z}$. (2) ある n があって $m = p^n$ と表せるなら G は直既約である.

証明. (1) は明らか. (2) を示す. $m = p^n$ とし $\mathbb{Z}/m\mathbb{Z} = A \times B (A, B \neq \{0\})$ とする. A, B は双方位数 p の部分群 A_1, B_1 を含む. $A \cap B = \{0\}$ より $A_1 \neq B_1$ であるが, すると巡回群 $\mathbb{Z}/m\mathbb{Z}$ が位数 p の部分群を 2 つもち矛盾. "$1, a, a^2$...の同じ長さの異なる列"というのはありえない. □

命題 10. p を素数とし有限群 G に対して $|G| = p^2$ なら G は *Abel* 群で $G \cong \mathbb{Z}/p^2\mathbb{Z}$ か $G \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ である.

証明. G が *Abel* 群でないとすると $Z(G) \subsetneq G$. $p^2 = |G| = |Z(G)| + \sum_{|C_i|>1} |C_i| (C_i$ は G 上の共役類) で各 $|C_i|$ は $|G|$ の約数である. $|C_i| = p$ または p^2 であるが $1 \in Z(G)$ より当然 $|C_i| = p$ である. $Z(G) \lhd G$ より $Z(G)$ は $|G| = p^2$ の約数で類等式によって $|Z(G)|$ は p の倍数であるので $|Z(G)| = p$. よって $|G/Z(G)| = p$ より $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$. つまり $a \in G, a \notin Z(G)$ をとれば $G/Z(G)$ は $aZ(G)$ で生成される巡回群. よって任意の $x \in G$ は

$$x = a^i z (\exists i \in \mathbb{N},\ \exists z \in Z(G))$$

$z \in Z(G)$ より $az = za$ で $ax = a^i(az) = a^i(za) = xa$ であるから $x \in Z(G)$. $G \subseteq Z(G)$ となり矛盾したから $G = Z(G)$. *Abel* 群の構造定理より終わる. □

補題 6 (Syllow)**.** $|G| = p^r m, (p, m) = 1$ のとき
(1) $|P| = p^r$ という部分群 P が存在し, この極大 p 群 P を *pSyllow* 群と呼ぶ.
(2) P, P' が *pSyllow* 群ならば互いに共役で $\exists a \in G; P' = aPa^{-1}$ である.
(3) *pSyllow* 群の個数を k とすると $k \equiv 1 (\mathrm{mod}\ p)$
$N_G(P) = \{a \in G | aPa^{-1} = P\}$ とおくと $N_G(P)$ は G の部分群で $P \subset N_G(P)$. $Y = \{P' | P'$ は G の *pSyllow* 群 $\}$ とし $a \in G$ を $aP'a^{-1} \in Y$ のように Y に作用させる. この時 $Orb_G(P') := \{aP'a^{-1} | a \in G\} = Y$ だった. また $Stab_G(P') = N_G(P')$ で $k = |Y| = |G/N_G(P')|$ だった. 単純に *pSyllow* 群の個数 k は $|G|$ の約数であり k は m の約数である. 簡単に次の事実を導く.

命題 11. p, q を素数 $(p > q)$ とし $|G| = pq$ の有限群 G に対して P は G の *pSyllow* 群で Q は G の *qSyllow* 群とすると (1) $G = PQ, P \cap Q = \{1\}$ (2) $P \lhd G$

証明. (1) $x \in P \cap Q, x \neq 1$ と仮定すると $ord(x)$ は $|P| = p$ かつ $|Q| = q$ の 0 でない約数なので $ord(x) = p = q$(矛盾). よって $P \cap Q = \{1\}$. $P \cong \mathbb{Z}/p\mathbb{Z}, Q \cong \mathbb{Z}/q\mathbb{Z}$ より $P = \langle a \rangle = \{a^i | i = 0, 1, ..., p-1\}, Q = \langle b \rangle = \{b^j | j = 0, 1, ..., q-1\}$ とかける. $i_1, i_2 \in \{0, 1, ..., p-1\},\ j_1, j_2 \in \{0, 1, ..., q-1\}$ について $P \cap Q = \{1\}$ により

$$a^{i_1} b^{j_1} = a^{i_2} b^{j_2} \Rightarrow i_1 = i_2,\ j_1 = j_2$$

これより $X = \{a^i b^j | 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$ とおくと $|X| = pq$. $X \subset PQ \subset G$ より $X = PQ = G$. (2) P の共役類の個数を k とすると $k \equiv 1 (\mathrm{mod}\ p)$ であり k は q の約数である. $k \leq q < p$ より $k = 1$. $g \in G$ に対し gPg^{-1} は *pSyllow* 群であるが G の *pSyllow* 群は 1 個なので $gPg^{-1} = P \Leftrightarrow P \lhd G$. □

系 1. p,q,G,P,Q は前命題と同じとする. $p \not\equiv 1 (\mathrm{mod}\ q)$ と仮定すると G は *Abel* 群で $G = P \times Q \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$ である.

証明. G の $qSylow$ 群の個数を ℓとする. $\ell \equiv 1 (\mathrm{mod}\ q)$ で ℓは p の約数. $\ell \neq 1$ とすると $\ell = p$ で $\ell \equiv p \not\equiv 1$ で直ちに矛盾. よって $\ell = 1$. 前命題と同様 $Q \triangleleft G$ であり $G = PQ, P \cap Q = \{1\}$ より $G \cong P \times Q$ である. □

定義 12. 集合 E で定義される自由群を定義し, 与えられた群を生成系と基本関係により表示することを考える. 各元$\alpha \in E$ に対して $E^+ = \{{x_\alpha}^{+1} | \alpha \in E\}, E^- = \{{x_\alpha}^{-1} | \alpha \in E\}$ とおく. ${x_{\alpha_i}}^{\epsilon_i} \in E^+ \cup E^-$とし $w = {x_{\alpha_1}}^{\epsilon_1} \cdots {x_{\alpha_n}}^{\epsilon_n}$(ただし$\epsilon_i = \pm 1$ で ${x_\alpha}^{+1}$と ${x_\alpha}^{-1}$は隣合わない.) を語という. $n = l(w)$ を w の長さという. $l(w) = 0$ なる $w = w_0$がただ一つ存在するとしこの語を空語という. E から作られる語全体の集合 W の元 $w_1 = {x_{\alpha_1}}^{\epsilon_1} \cdots {x_{\alpha_n}}^{\epsilon_n}, w_2 = {x_{\beta_1}}^{\delta_1} \cdots {x_{\beta_m}}^{\delta_m} (\epsilon_i, \delta_j = \pm 1)$ に対し $w_1 w_2 = {x_{\alpha_1}}^{\epsilon_1} \cdots {x_{\alpha_n}}^{\epsilon_n} {x_{\beta_1}}^{\delta_1} \cdots {x_{\beta_m}}^{\delta_m}$とし, また$\alpha_n = \beta_1, \epsilon_n = -\delta_1$のときに ${x_{\alpha_n}}^{\epsilon_n} {x_{\beta_1}}^{\delta_1}$を消去するとする. これを簡約という. W は結合法則を満たし, 単位元は空語であり逆元があり群をなし群 W を E を生成系とする自由群という. $|E|$ を階数という. ${x_\alpha}^{r\epsilon} = {x_\alpha}^{\epsilon} \cdots {x_\alpha}^{\epsilon}$とかくから ${x_{\alpha_i}}^{\epsilon_i}$の$\epsilon_i$は ± 1 ではなく勝手な整数という意味でかくことがある.

注 6. G を群, E を集合, $\sigma : E \to G$ を写像, W を E を生成系とする自由群とする. $\sigma(\alpha) = g_\alpha (\alpha \in E)$ とし$\varphi_0 : E \to G; x_\alpha \mapsto g_\alpha$を定める. φ_0は一意に準同型$\varphi : W \to G$ に拡張される. これは $w = {x_{\alpha_1}}^{\epsilon_1} \cdots {x_{\alpha_n}}^{\epsilon_n}$に対し$\varphi(w) = {g_{\alpha_1}}^{\epsilon_1} \cdots {g_{\alpha_n}}^{\epsilon_n}$とすれば$\varphi(x_\alpha) = \varphi_0(x_\alpha) = g_\alpha$による. W を群 G を生成系とする n 変数自由群とすれば, σは恒等写像ゆえ$\varphi_0(x_g) = g$ である. すると全射準同型な$\varphi : W \to G; \varphi({x_{g_1}}^{\epsilon_1} \cdots {x_{g_n}}^{\epsilon_n}) = {g_1}^{\epsilon_1} \cdots {g_n}^{\epsilon_n}$が存在する.

$$\begin{array}{ccc} E & \longrightarrow & W \\ & \searrow^{\varphi_0} \quad \cup & \downarrow \exists! \varphi \\ & & G \end{array} \tag{1.4}$$

命題 12. G を群とし $S \subset G$ とする. $N = \langle \{xyx^{-1} | x \in G, y \in S\} \rangle$ は S を含む最小の G の正規部分群である.

定義 13. F_nを n 変数 $\boldsymbol{x} = (x_1, ..., x_n)$ の自由群, $R_1(\boldsymbol{x}), ..., R_m(\boldsymbol{x}) \in F_n$とする.

$$N := \langle \{gR_i(\boldsymbol{x})g^{-1} | g \in F_n, i = 1, ..., m\} \rangle$$

は前命題より $R_1(\boldsymbol{x}), ..., R_m(\boldsymbol{x})$ を含む F_nの最小の正規部分群である. $G = F_n/N$ を $\langle x_1, ..., x_n | R_1(\boldsymbol{x}) = 1, ..., R_m(\boldsymbol{x}) = 1 \rangle$ とかき生成元 $x_1, ..., x_n$と基本関係 $R_1(\boldsymbol{x}) = 1, ..., R_m(\boldsymbol{x}) = 1$ で定義された群という.

注 7. このような群 F_n/N は N が最小の正規部分群であるので「ある生成元を持ち, それが与えられた基本関係を満たすような群の中で最大のもの」である. 例えば 3 次対称群は $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$で生成され$\sigma^3 = \tau^2 = \sigma\tau\sigma\tau = 1$ の関係式を満たすが自明な群 $\{1\}$ に対しても$\sigma = \tau = 1$ として同じ関係式を満たしてしまう. F_n/N とは関係式を満たす群で最大のものであるので意味がある定義である.

命題 13. G を群とする. $R(\boldsymbol{x})$ が語で $y_1, ..., y_n \in G$ なら $x_1, ..., x_n$ に $y_1, ..., y_n$ を代入した $R(\boldsymbol{y}) \in G$ を考えられる. G は n 個の生成元 $y_1, .., y_n$ を持ち, 関係式 $R_1(y_1, ..., y_n) = \cdots = R_m(y_1, ..., y_n) = 1_G$ を持つとする. $K = \langle x_1, ..., x_n | R_1(\boldsymbol{x}) = ... = R_m(\boldsymbol{x}) = 1 \rangle$ とする. このとき全射準同型 $\phi : K \to G; x_1 \mapsto y_1, ..., x_n \mapsto y_m$ となるものが存在する.

証明. (6) より準同型 $\varphi : F_n \to G$ で $\varphi(x_1) = y_1, ..., \varphi(x_n) = y_n$ となるものがある. G は $y_1, ..., y_n$ で生成されているからこれは全射. また $R_1(\boldsymbol{x}), ..., R_m(\boldsymbol{x}) \in \mathrm{Ker}\varphi \lhd F_n$ で $N \subset \mathrm{Ker}\varphi$. 準同型定理より $\pi : F_n \to K$ を自然な全射とするとき $\exists! \phi : K \to G; \varphi = \phi \circ \pi$. φ 全射より ϕ は全射で明らかに $\phi(x_i) = y_i$. □

命題 14. $K = \langle x, y | x^3 = y^2 = yxyx = 1 \rangle$ とする. $K \cong \mathfrak{S}_3 \cong D_3$.

証明. $\mathfrak{S}_3$ は σ, τ で生成されるので前命題 (13) より全射 $\phi : K \to \mathfrak{S}_3$ で $\phi(x) = \sigma, \phi(y) = \tau$ となるものがある. $|\mathfrak{S}_3| = 6$ より $|K| \leq 6$ が分かれば ϕ は全射より $|K| = 6$ であり ϕ は同型.
$xy = yx^2$ なので $\cdots xy \cdots$ における xy を yx^2 に変えることで y の左に x が来ないようにかける. よって K の任意の元は $y^i x^j (i = 0, 1\ j = 0, 1, 2)$ とかける. よって $|K| \leq 6$. 二面体群については $|D_3| = 6$ で同じ議論で終わる. □

命題 15. p, q は素数とする. $p > q$ とし G は位数 pq の有限群, P, Q をそれぞれ G の $pSylow$ 群と $qSylow$ 群とすると, $G = PQ, P \cap Q = \{1_G\}, P \lhd G$ であった. $p \not\equiv 1 (\mathrm{mod}\ q)$ の時 $G \cong P \times Q$ だったが $p \equiv 1$ とする. $P \cong \mathbb{Z}/p\mathbb{Z}, Q \cong \mathbb{Z}/q\mathbb{Z}$ であった所, ここでは a, b をそれぞれ (巡回群) P, Q の生成元とする. すると $b^q = 1$ である. ($\because$ 注 4.(2))
$Abel$ 群とすると基本定理を使えば良いので G は非 $Abel$ 群とする. 以上の設定で, (1) $bab^{-1} = a^r, 2 \leq r \leq p-1$ となる r が存在し $r^q \equiv 1 (\mathrm{mod}\ p)$ である.
(2) $G = \langle a, b | a^p = b^q = 1, bab^{-1} = a^r \rangle$ である.

証明. $P \lhd G$ で $pSylow$ 群の個数は 1 つだったので $bPb^{-1} = P$ より, $bab^{-1} \in bPb^{-1} = P (= \langle a \rangle = \{1, a, ..., a^{p-1}\}$. よって $1 \leq r \leq p-1$ のある r があって $bab^{-1} = a^r$. $bab^{-1} = a$ だと G が $Abel$ 群となるので $r \geq 2$. ここで $a^{r^k} = b^k a b^{-k}$ が成り立つ. なぜなら $k+1$ の時も $b^{k+1} a b^{-k-1} = b(b^k a b^{-k}) b^{-1} = b a^{r^k} b^{-1} = (bab^{-1})^{r^k} = a^{r^{k+1}}$ と成り立つから. $k = q$ とすると $b^q = 1$ より $a^{r^q} = b^q a b^{-q} = a$. a は P の生成元としたことによってこれはすなわち, $a^{r^q - 1} = 1$ が $P (\cong \mathbb{Z}/p\mathbb{Z})$ で成り立つ. 従って $r^q - 1 \equiv 0 (\mathrm{mod}\ p)$ である. ($a^n = 1$ となる $\min n$ を位数と呼んだ)
(2) (14) の証明を僅かに一般的に書き直せばいい. $|G| \leq pq$ を示せばよい. $ba = a^r b$ より G' の任意の元は $a^i b^j (0 \leq i < p, 0 \leq j < q)$ の形に表せる. よって $|G| \leq pq$. □

命題 16. 上の設定の続きではあるが $q = 2, p \geq 3$ とし $|G| = 2p$ であるとすると G は二面体群に同型である. $G \cong D_n$ である.

証明. 前命題より

$$G \cong \langle a, b | a^p = b^2 = 1, bab^{-1} = a^r \rangle,\ \exists r((2 \leq r < p) \wedge r^2 \equiv 1 (\mathrm{mod}\ p))$$

$(r-1)(r+1)$ は p の倍数である. 明らかに $r-1$ は p の倍数ではないので $r+1 = p$. $\therefore bab^{-1} = a^{p-1} = a^{-1}$. $abab^{-1} = 1$ であるが $b^{-1} = b$ より $(ab)^2 = 1$.

$$\langle a, b | a^p = b^2 = (ab)^2 = 1 \rangle \cong D_{2p}$$

□

注 8 (行列表示)**.**

$$a = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix},\ b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

とおくと, a が回転角$\frac{2\pi}{n}$の回転を表し b が鏡映変換を表すように二面体群は a と b で生成される. 基本関係 $ab = ba^{-1}(abab = 1)$ より $b = b^{-1} = aba$ と左から a で始まる書き方をして

$$D_n \cong \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle = \{e, a, a^2, ..., a^{n-1}, b, ab, a^2b, ..., a^{n-1}b\},\ |D_n| = 2n$$

定義 14. 四元数体 $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$ としこの元同士の和は $1, i, j, k$ を基底とする $\mathbb{R}$ 上の 4 次元線型空間として定め積は

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

となるよう定める. $x = a+bi+cj+dk$ に対し$\bar{x} = a-bi-cj-dk$, $|x|^2 = x\bar{x} = a^2+b^2+c^2+d^2$ とおくと $x\frac{\bar{x}}{|x|^2} = 1$ より $x^{-1} = \frac{\bar{x}}{|x|^2}$. 逆元が存在し $\mathbb{H}$ は非可換体である. これをハミルトンの四元数体という. 四元数群 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$ は積で群となる. 次において $a = i, b = j$ とおけば

$$Q_8 = \langle a, b | a^4 = 1, a^2 = b^2, ba = a^3b \rangle$$

一般四元数群については

$$Q_{4n} = \langle a, b | a^{2n} = 1, a^n = b^2, ab = ba^{-1} \rangle$$

数学的事実 1. 有限非可換体は存在しない. また $\mathbb{R}$ を含む非可換体を含めた体で $\mathbb{R}$ 上有限次元線型空間であるものは $\mathbb{C}, \mathbb{H}$ のみに限る.

問 1. H を G の部分群とする. $[G : H] := |G/H| = 2$ ならば $H \triangleleft G$ である.

証明. 次の b を取る. $b \in G, b \notin H$. $[G : H] = 2$ より $H \sqcup bH = G$ である. $H \sqcup Hb = G$ でもあるから $bH = Hb$ であり $H \triangleleft G$. □

問 2. 単位元でない任意の $x \in G$ に対し $x^2 = 1$ であれば G は *Abel* 群である.

証明. 任意に $x, y \in G$ を取る. $(xy)^2 = 1$ より $(xy)^{-1} = xy$ より $yx = xy$. □

命題 17. 正方形の合同群は $D_8 = \langle a, b | a^4 = b^2 = 1, (ab)^2 = 1 \rangle$ である. $Q_8 = \langle a, b | a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1} \rangle$ であるが, $|G| = 8$ の非可換群は D_8か Q_8と同型である. なお G が *Abel* 群の時は n 次巡回群を C_nとかくと $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$と同型.

注 9. G が以下のいずれかを満たせば G は *Abel* 群である.
(1) G が巡回群であるとき.
(2) $G = \langle x, y | xy = yx \rangle$ のとき.
(3) G の中心を $Z(G)$ とかくとき $G/Z(G)$ は巡回群のとき.
(4) 単位元を除く全ての元の位数が 2 であるとき. (3) だけ示す. $G/Z(G)$ での $x \in G$ を代表元とする剰余類を $[x]$ とかくことにし $x, y \in G$ を任意に取る. $G/Z(G)$ は巡回群 (cyclic group) だからその生成元の一つを $[g]$ とすると $[x] = [g]^m, [y] = [g]^n (m, n \in \mathbb{Z})$ とかける. $a, b \in Z(G)$ とし $x = (g^m)a, y = (g^n)b$. a, b は G の任意の元と可換なので $xy = (g^m)a(g^n)b = g^{m+n}ab,\ yx = g^{m+n}ab$ より $xy = yx$.

証明. 注 9(1) より G の中で位数が最大の元 a を取ると $ord\ a = 8$ なら G は巡回群であるから *Abel* 群であり仮定に反するので $ord\ a = 4$ 又は 2 である. 注 9(4) より $ord\ a = 4$ であることもわかった. そこで $A := \langle a \rangle = \{1, a, a^2, a^3\}$ とおく. $[G : A] = 8/4 = 2$ より $A \lhd G$ である.
$\exists b(b \in G \wedge b \notin A)$ とすると $A \lhd G$ より $b^{-1}Ab = A$ であるから, $b^{-1}ab = a^i (\exists i = 0, 1, 2, 3)$ とかける. $i = 0$ なら $b^{-1}ab = 1 \Leftrightarrow a = 1$ となり反する. $i = 1$ なら G は *Abel* 群となる.
$i = 2$ なら $1 = a^4 = (b^{-1}ab)^2 = b^{-1}a^2b \Leftrightarrow a^2 = 1$ となりこれも $ord\ a = 4$ に反する.
よって $i = 3,\ ab = ba^3$である.
$|G|$ の位数は 8 で位数最大の元の位数は 4 なので $ord\ b = 2$ 又は 4. $ord\ b = 2$ の場合 $b^2 = 1, b = b^{-1}$ より $bab = a^3 = a^{-1}$ より $(ab)^2 = 1$ だから G は二面体群に同型. $ord\ b = 4$ の場合 $G \cong Q_8$. ($\because\ b^4 = 1$ とすると $b^2 = a^2 = -1$.) $G = \{\pm 1, \pm a, \pm b, \pm ab\}$ と表される. □

注 10. 表示 (representation) にはいくつかあって, $Q_8 = \langle a, b | a^4 = b^3 = 1, ba = ab^2 \rangle$ には $a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b \mapsto \begin{pmatrix} -e^{\pi i/3} & 0 \\ 0 & -e^{-\pi i/3} \end{pmatrix}$ とおいて $\langle a, b | a^6 = 1, a^3 = b^2, ab = ba^{-1} \rangle$ には $a \mapsto \begin{pmatrix} e^{\pi i/3} & 0 \\ 0 & e^{-\pi i/3} \end{pmatrix}$, $b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ と対応させられる.

命題 18.
(1) p を 3 以上の素数とする. $p + 1$ 次の対称群の位数 p の元の個数と *pSylow* 群の個数を求めよ.
(2) (1) で求めた *pSylow* 群の個数と *sylow* の定理からどのような合同式を得るか.

証明. (1) 一般に素数位数の群は巡回群より位数が素数 p となる (対称群の元としての) 置換は巡回置換のみ. $p + 1$ 個の文字から p 個の文字を選ぶのは $p + 1$ 通りで選んだ p 個の文字による巡回置換は $(p - 1)!$通りだから $(p + 1)(p - 1)!$. また, 対称群 S_{p+1}の位数は $(p + 1)!$ なので S_{p+1}の *pSylow* 群の位数は p. すなわち各 *pSylow* 群は巡回群でその元とは単位元と $p - 1$ 個の位数 p の元である. もし位数 p の共通元があったら 2 つの *pSylow* 部分群は一致してしまうので相異なる *pSylow* 群に含まれる共通元は単位元しかないことが分かる. 以上より位数 p の元が $(p + 1)(p - 1)!$こあり, 一つの *pSylow* 群には $p - 1$ 個の位数 p の元があるため, *pSylow* 群の個数は

$$\frac{(p + 1)(p - 1)!}{(p - 1)} = (p + 1)(p - 2)!$$

(2) $(p - 1)(p - 2)! \equiv 1 (\mathrm{mod} p)$ である. これより $(p - 2)! \equiv 1 (\mathrm{mod} p), (p - 1)! \equiv p - 1 \equiv -1 (\mathrm{mod} p)$. これはウィルソンの定理と呼ばれる. □

補題 7 (次で G が *Abel* 群のときに使う)**.** A, B を G の部分群とする. $|G| = |A||B|, gcd(|A|, |B|) = 1$ のとき $G = AB, A \cap B = \{1\}$ が成り立つ. $x \in A \cap B$ とする.
$ord\ x || A|, ord\ x || B|$ であるが $|A|$ と $|B|$ は互いに素なので $x = 1_G$.

命題 19. 位数 12 の非可換群 G は $D_{12}, Q_{12}, 4$ 次交代群 A_4のいずれかと同型である.
なお G が位数 12 の *Abel* 群の場合をまず考えると, G の 2*sylow* 群 H と 3*sylow* 群 K が存在する. ($|G| = 12 = 2^2 \cdot 3$ ということなので $|H| = 4, |K| = 3$). 前補題より $G \cong H \times K$. $H \cong C_4$ 又は $H \cong C_2 \times C_2$である. $K \cong C_3$であるので $G \cong C_4 \times C_3 \cong C_{12}$又は $G \cong C_2 \times C_6$.
次の主張 1 がまず大事である.

証明. (*Claim*1) p, q を異なる素数とし $|G| = p^2 q$ とする.
P, Q を G の $pSylow$ 群, Q を G の $qSylow$ 群とすると $P \triangleleft G$ または $Q \triangleleft G$ である.
(*Proof*) Q が G の正規部分群ではないとして $P \triangleleft G$ となることを示す. なお, 以下の下線部が指示するように相異なる $qSylow$ 群の共通元は単位元のみであることは前命題 (18) での言及と同様.
G の部分集合 S の中心化群とは $C_G(S) = \{g \in G | sg = gs(\forall s \in S)\}$ で S の正規化群とは $N_G(S) = \{g \in G | gS = Sg\}$ だった. この定義は, g が正規化群の元のとき $s \neq t$ となるような s, t も含めて $gs = tg$ が成り立つということであるから, $s \in S$ に対して $gs = sg$ となるような g 全体の集合という中心化群の定義とは違うことに注意. $N_Q = N_G(Q)$ とかくことにすると $[G : N_Q] | p^2$, $[G : N_Q] \equiv 1 (\mathrm{mod}\, q)$.(なぜなら $Sylow$ の定理から $qSylow$ 群の個数 $|G/N_G(Q)|$ は q を法として 1 に等しい.) $[G : N_Q] = 1$ とすると正規化群の定義よりこれは $Q \triangleleft G$ ということなので仮定に反するから $[G : N_Q] = p$ または $[G : N_Q] = p^2$.
$[G : N_Q] = p^2$のとき, 各 $sylow$ 群に番号をつけるようにかくと G には $qSylow$ 群 $Q_i (1 \leq i \leq p^2)$ が存在して$\underline{Q_i \cap Q_j = \{e\} (i \neq j)}$, $P \cap Q_i = \{e\}$ である. よって,

$$|Q_1 \cup \cdots \cup Q_{p^2}| = p^2(q-1) + 1 = p^2 q - (p^2 - 1)$$

(p^2という $qSylow$ 群の個数と単位元の個数 1 を引いた各 $qSylloy$ 群の位数 $q-1$ をかけて集合の元の数を数えた.)
よって

$$P \cup Q_1 \cup \cdots \cup Q_{p^2} = G$$

これより, もし P'が P と相異なる $pSylow$ 群であるならば $x \in P' \backslash P$ はある $Q_i (1 \leq i \leq p^2)$ に属するから, $ord\ x$ は (P'に由来する)p^2と q の約数になる. すなわち $x = e$ となって矛盾.
従って $P \triangleleft G$ が成り立つ.
最後に使う必要に迫られ用いた次の主張が正しいことも記しておく.
(*Claim*2) P を群 G の $pSylow$ 群とする. P が唯一の $pSylow$ 群 $\Leftrightarrow P \triangleleft G$.
$\because P \triangleleft G \Leftrightarrow G$ での P の共役部分群は全て $P \Leftrightarrow G$ の全ての $pSylow$ 群は P に一致.
次に $[G : N_Q] = p$ の場合を考える. $sylow$ の定理より $p \equiv 1 (\mathrm{mod} q)$ で $p = 1 + \ell q (\exists \ell > 0)$ と表せる. $N_P = N_G(P)$ とかくと $sylow$ の定理より $[G : N_P] \equiv 1 (\mathrm{mod} p)$ かつ $[G : N_P] | q$ である.
もし $[G : N_P] = q$ であるなら, $q = 1 + kp (\exists k > 0)$ から

$$p = 1 + \ell q = 1 + \ell(1 + kp) = (1 + \ell) + \ell k p > p$$

となり矛盾. よって $[G : N_P] = 1$ の場合しかなくこれはすなわち $P \triangleleft G$ である. (*Claim*1) の証明終. □

定義 15. 準同型 $\mathrm{sgn} : \mathfrak{S}_n \to \{1, -1\}$ に対して置換$\sigma \in \mathfrak{S}_n$は $\mathrm{sgn}\sigma = 1$ なら偶置換, -1 なら奇置換という. $A_n := \mathrm{Ker}(\mathrm{sgn})$ と定めこれを交代群という. 交代群とは偶置換全体である.

定理 2 (再喝)**.** $|G| = 12$ の非可換群 G は $A_4, D_6 \cong \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}, \langle a, b | a^4 = b^3 = 1, a^{-1}ba = b^2 \rangle$ のいずれかに同型.

注 11. 上定理の証明と位数 4 の群 G の分類において登場するクラインの四元数群 V は A_4に対する正規部分群であり, 単位元以外の元の位数は 2 である. 位数は p^2の形なので $Abel$ 群

であるが次のように書き下してみると良い.

$$A_4 = \{(123), (132), (124), (142), (134), (143), (234), (243), e, (12)(34), (13)(24), (14)(23)\}$$

であるが命題18と同様に考えると, A_4において$(i_1i_2i_3)$という形の巡回置換の数は$\{1,2,3,4\}$から3つ数字を選ぶ事の選び方の数4と3つの数字の巡回置換の数2の積8であり, それとクラインの四元数群の元4個があり計12こである. よってA_4には位数4の元はない. D_6にも位数4の元はない. しかし上定理の最後のような群には位数4の元aがある. このように同型であるか否かを判断することができる. 位数6の元の存在性によってA_4とD_6が同型でないことも分かる.

定義 16. 群Gから自身への自己同型写像とは$\phi : G \to G$のことである. 自己同型全体がなす集合は写像の合成に関して群をなしGの自己同型群といい, $\mathrm{Aut}(G)$とかく. 群の圏などある種の圏では自己同型を内部自己同型とそうでない外部自己同型の二つに区別することがある.
群Gの内部自己同型とは$a \in G$による共役な作用である. 即ち, 作用$\phi_a : G \to G; g \mapsto aga^{-1}$のことであり, 内部自己同型全体$\mathrm{Inn}(G)$は$\mathrm{Aut}(G)$の正規部分群である.

証明. H, KをそれぞれGの$2syllow$部分群, $3syllow$部分群とする. (6)より$|H| = 2^2$なのでHは$Abel$群. Hが位数4の元を持てば注4より$H \cong \mathbb{Z}/4\mathbb{Z}$. さらに注4より$H$が位数4の元を持たなければ単位元以外の元の位数は2である. すると, $(1 \neq)a \neq b \in H$に対して当然$ab \neq a, b$であり$ab = 1$なら$b = a^{-1} = a$(位数2なので)となり矛盾. よって$ab \neq 1$で$H = \{1, a, b, ab\}$(クラインの四元数群; $H_1 = \{1, a\}, H_2 = \{1, b\}$とすれば$H_1 \cap H_2 = \{1\}$で$H$は可換群, $H = H_1H_2$より$H \cong H_1 \times H_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)
$[G : N_G(K)]$は$[G : K] = 12/3 = 4$の約数のいずれかであるからKの共役群の個数は$1, 2$または4. $2 \not\equiv 1(\mathrm{mod}3)$より1または4であるが, 今$H$だけが$G$の正規部分群である場合を考えると1の可能性も除外される.
改めてHだけが正規部分群であるとし, $K_1, ..., K_4$をKの共役とする. ($Claim1$)により$K \triangleleft G$または$H \triangleleft G$であり, 両方ともそうであるなら$G \cong \mathbb{Z}/12\mathbb{Z}$か$G \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$である. また後で$K$だけが正規部分群の場合も考える.)
群Gは共役により集合$\{K_1, ..., K_4\}$に作用しこれは推移的な作用である. $\phi : G \to \mathfrak{S}_4$をこの作用による置換表現とする. つまり$gK_ig^{-1} = K_{\phi(g)(i)}(i = 1, 2, 3, 4)$である. $4 = K$の共役の数$= (G : N_G(K_i)) \leq (G : K_i) = 4$より$N_G(K_i) = K_i$. $g \in \mathrm{Ker}\phi$とすると$gK_ig^{-1} = K_i(i = 1, 2, 3, 4) \Leftrightarrow g \in \cap_{i=1}^4 N_G(K_i) = \cap_{i=1}^4 K_i = \{1\}$. よって$\phi$は単射.
$|K_i| = 3$は素数なので$i \neq j$に対し$K_i \cap K_j = \{1\}$. よって$S := \cup_{i=1}^4 (K_i \backslash \{1\})$とおくと$|S| = 2 \times 4 = 8$で$S$の元の位数はすべて3である. $|S| = 8$よりSで生成されるGの部分群Fの位数は8以上. $|F|$は$|G| = 12$の約数なので$|F| = 12$すなわち$F = G$. よってGは位数3の元のみで生成される. ϕは単射なので$g \in G$が位数3の元なら$\phi(g) \in \mathfrak{S}_4$も位数3の元. $\mathfrak{S}_4$の位数3の元は$(i_1i_2i_3)$の形の巡回置換のみでこれらはすべてA_4の元であるから$G \subset \phi(G) \subset A_4$. $|A_4| = 12$より$A_4 = \phi(G)$. また$G \cong A_4$である.
次にKだけが正規部分群であるとき, $h \in H$に対して$\mathrm{Aut}(K)$の元$\phi_h : K \to K$を$\phi_h(k) = hkh^{-1}$と定める. (つまり内部自己同型) $K = \mathbb{Z}/3\mathbb{Z}$. $\psi \in \mathrm{Aut}(K)$とするとKの位数3の元は$1, 2$なので$\psi(1) = 1, 2$. $f : K \ni k \mapsto 2k \in K$は準同型で$f$は同型. よって$\psi(1) = 2$となる同

型ψがある. 任意の$\psi \in \mathrm{Aut}(K)$ は K の生成元 1 の像で定まるので $\mathrm{Aut}(K) \cong \{1,2\}$(この群の演算は $\mathbb{Z}/3\mathbb{Z}$ の通常の演算) で $\mathrm{Aut}(K) \cong \mathbb{Z}/2\mathbb{Z}$. さて$\phi_H(\subseteq \mathrm{Aut}(K))$ が自明 (恒等写像) であるなら $\forall h \in H, k \in K$ に対し $hkh^{-1} = k$ で $H \triangleleft G$ であるので矛盾. $|\mathbb{Z}/2\mathbb{Z}| = 2$ でありこれより小さい 1 の可能性が除外されたので$\phi_H = \mathbb{Z}/2\mathbb{Z}$ である. そして以下, $H \cong \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ の場合について.
(a) $H \cong \mathbb{Z}/4\mathbb{Z}$ のとき.
$H = \langle a \rangle, K = \langle b \rangle$ とする. 今は K だけが正規部分群という下故の既述のϕ_Hの非自明性 (又は G の非可換性) より $ab \neq ba$ で$\phi_H = \mathbb{Z}/2\mathbb{Z}$ だから $aba^{-1} = b^2$. ($K \ni k \mapsto hkh^{-1} \in K$ は単に写像の対応を指していて, 今この式の右辺が行き先 K のうちであり得るのは b, b^2のどちらか. もし 1 なら $b = 1$ となり不合理.) G は a, b で生成されていて $a^4 = b^3 = 1, ab = b^2a$ より命題 (13) より全射準同型 $\langle x, y | x^4 = y^3 = 1, xy = y^2x \rangle \to G$ で $x \mapsto a, y \mapsto b$ となるものが存在する. 左辺の位数は 12 なのは各自確かめることとし, よって同型.
(b) $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ のとき.
$K = \langle \upsilon \rangle$ とする. $f : K \to \mathrm{Aut}(H)$ の核 $\mathrm{Ker}(f)$ の元 $1 \neq \upsilon \in K$, $w \in H$ に対して $w\upsilon w^{-1} = \upsilon$ 即ち $w\upsilon w^{-1} = \upsilon$. H の元がすべてυと可換なら G が非可換群であるのに反するから $b \in H$ で $b\upsilon b^{-1} = \upsilon^2$となるものがある. また $b \notin \langle w \rangle$ より $H \cong \langle b \rangle \times \langle w \rangle$. $a = w\upsilon$とおくと w とυは可換である事より

$$a^2 = w^2\upsilon^2 = \upsilon^2 \neq 1,\ a^3 = w^3\upsilon^3 = w \neq 1,\ a^6 = w^6\upsilon^6 = 1$$

(可換なことは $a^2 = (w\upsilon)^2 = w\upsilon w\upsilon = w^2\upsilon^2$と使った. また$\upsilon$の位数は 3 の約数なので 2 であることはない.) よって a の位数は 6 である. また $a^3 = w$ より $w \in \langle a \rangle$. $\langle a, b \rangle \supset \langle a \rangle, H$ なので, $|\langle a, b \rangle|$ は $6, 4$ の倍数. よって $G = \langle a, b \rangle$.
D_6は位数 12 の群で二つの元 t, r で生成され関係式は $t^6 = r^2 = 1, rtr^{-1} = t^{-1}$であるが,

$$bab^{-1} = bw\upsilon b^{-1} = wb\upsilon b^{-1} = w\upsilon^2 = \upsilon^2 w = a^{-1}$$

最後の等号は$\upsilon^2 wa = \upsilon^2 w^2 \upsilon = \upsilon^3 = 1$ による. つまり a, b は D_6の生成元と同じ関係式を満たす. 従って (13) により全射準同型な

$$L = \langle x, y | x^6 = y^2 = 1, yxy^{-1} = x^{-1} \rangle \to D_6$$

が存在する. 全射なので $|L| \geq 12$ であるが L の任意の元は $x = y^2x$ で $y^i x^j$ ($i = 0, 1,\ j = 0, ..., 5$) の形に表されるので $|L| \leq 12$. よって $|L| = 12, L \cong D_6$である. また包含全射準同型写像 $L \to G$ が存在し $|L| = |G| = 12$ より $G \cong L \cong D_6$なので $G \cong D_6$. □

注 12. p を素数として位数 p^2の群は C_{p^2}か $C_p \times C_p$に同型であるということによって位数 4 の群 H が (a) と (b) の二つの場合に分けられた. ではこれを以下で示す.
(*Claim*4) G を位数 p^2, A, B を位数 p の G の部分群とし $A \neq B$ であるとすると $A \cap B = \{1\}, G = AB$ である.
($\because$) $A \cap B \leq A$ より $|A \cap B|$ は p の約数なので $|A \cap B| = 1, p$. もし p なら $A \cap B = A$ なので $A \subset B$ である. $|A| = |B|$ より $A = B$ となり矛盾. よって $|A \cap B| = 1$ より $A \cap B = \{1\}$. $|AB| = |A||B|/|A \cap B| = p^2 = |G|$ より $G = AB$.
G を位数 p^2の群とすると G の元の位数は $1, p, p^2$のいずれか. 位数 p^2の元が存在すれば $G \cong$

C_{p^2}である. G は位数 p^2の元を持たないとしそのとき $G \cong C_p \times C_p$であることを言う. その仮定の下 G の単位元以外の元の位数は p である. G の $a \neq 1$ を取り a で生成される部分群を A とし, 次に元 $b \in G, b \notin A$ を取り b で生成される部分群を B とおく. a, b の位数は p なので $|A| = |B| = p$. *Claim* 4 より $A \cap B = \{1\}, G = AB$ であるが $|G| = p^2$より G は *Abel* 群だから $A, B \lhd G$ より $G \cong A \times B \cong C_p \times C_p$.

命題 20. $|G| = 4$ の群は C_4またはクラインの四元群 V に同型である. $V = \{1, a, b, ab\}$ は単位元以外の元の位数は全て 2 である *Abel* 群である. なお位数 p^2の p 群 G は *Abel* 群である.
($\because$) p 群 G の中心 $Z(G)$ の位数は p の倍数であるので $Z(G) \ni a \neq 1$ を取れる. a の位数は p または p^2であるがもし $ord\ a = p^2$なら注 9 より $G = \langle a \rangle$ で G は *Abel* 群である. $ord\ a = p$ のとき $H = \langle a \rangle$ とおく. このとき $H \subset Z(G)$ で G/H の位数は $p^2/p = p$ になり素数位数の群は巡回群であることから巡回群. よって G は *Abel* 群. 最後に用いた主張をかくと
(*Claim*3) G の正規部分群 N が G の中心に含まれ G/N が巡回群であるならば G は *Abel* 群.

命題 21. $|G| = 15$ の有限群 G は $\mathbb{Z}/15\mathbb{Z}$ に同型であるか.

証明. H, K をそれぞれ G の 3*syllow* 群, 5*syllow* 群とする. $|H| = 3, |K| = 5$ は素数より其々は巡回群すなわち $H \cong \mathbb{Z}/3\mathbb{Z}, K \cong \mathbb{Z}/5\mathbb{Z}$. 其々の *syllow* 群の個数を s, t とおくと $s \equiv 1(\mathrm{mod}3), t \equiv 1(\mathrm{mod}5)$. $H \subset N_G(H), K \subset N_G(K)$ なので $[G : N_G(H)], [G : N_G(K)]$ は其々 $[G : H] = 15/3 = 5$, $[G : K] = 3$ の約数. これらは素数なので s, t は $1, 5$ および $1, 3$ である. 上の *syllow* の定理より $s = t = 1$. よって $H, K \lhd G$. $|H \cap K|$ は $|H|, |K|$ の約数より 1 である. すなわち $H \cap K = \{1\}$. $H, K \lhd G$ より HK は G の部分群である. $H, K \subset HK$ より $|HK|$ は 15 の倍数. $|HK| \leq 15$ より $HK = G$. (部分群の位数が全体の群 G の位数と等しいならその部分群は G に一致する)
$H \cap K = \{1\}$ より $G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. 中国剰余より $G \cong \mathbb{Z}/15\mathbb{Z}$. □

注 13. $H \lhd N_G(H)$ であり, $N_G(H)$ は H を正規部分群として含むような G の部分群の中で最大のもの. $\forall g \in N_G(H)$ に対し $gH = Hg$ より $H \lhd N_G(H)$. $H \lhd N \subset G$ となる部分群 N があれば $N \subset N_G(H)$ を示す. $\forall x \in N$ に対して $H \lhd N$ より $xH = Hx$ より $x \in N_G(H)$. よって $N \subset N_G(H)$.

補題 8. $N \lhd G, H \leq G$ とする. このとき (1)$NH \leq G$ (2)$N \lhd NH, N \cap H \lhd H$ が成立.
(3)$HN/N \cong H/H \cap N; hN \mapsto h(H \cap N)$

証明. (1)$\forall x, y \in NH$ に対し $x = nh, y = n'h'$とする. $N \lhd G, h \in H \subset G$ より $xy = nhn'h' = n(hn'h^{-1})hh' \in NH$. $x^{-1} = h^{-1}n^{-1} \in Hn' = n'H$(これも $n' \in N, N \lhd G$ より). よって $NH \leq G$ である. (2)$N = N1_H \subset NH$ は明らかに NH の部分群であり $\forall x \in NH$ に対し $x \in G$ より $xNx^{-1} \subset N$. また $\forall h \in H$ に対し $h(N \cap H)h^{-1} = hNh^{-1} \cap hHh^{-1} = N \cap H$ よりすなわち $N \cap H \lhd H$. (3)$N \lhd G$ より G/N が定義され f を $f : G \to G/N; x \mapsto xN$ と定める. f の制限 $f' : H \to G/N; x \mapsto xN$ の像は $\mathrm{Im}f' = HN/N$ であり $\mathrm{Ker}f' = H \cap N$. f'は自然な準同型 f の制限なので準同型である. よって f'に対して準同型定理より $H/H \cap N \cong HN/N$.

□

補題 9. $K \lhd G, K \subset H \Rightarrow K \lhd H$.

命題 22 (ツァッセンハウス)**.** H, K を G の部分群, $H' \lhd H, K' \lhd K$ とする. このとき

$$H'(H \cap K)/H'(H \cap K') \cong K'(H \cap K)/K'(H' \cap K)$$

証明. $\forall x \in H'(H \cap K) \subset H$ に対し $xH'x^{-1} = H'$が成り立つ.(∵ $x \in H, H' \lhd H$.) よって

$$H' \lhd H'(H \cap K) \tag{1.5}$$

$H' \lhd H$ で補題より $H'(H \cap K)$ は H の部分群である. また $H \cap K \subset H'(H \cap K) \subset H \lhd N_G(H)$. (1.5) より $H' \cap K \lhd H'(H \cap K) \cap K \subset H \cap K$. 一方 $x \in H \cap K$ なら $x = 1x \in H'(H \cap K)$ より $H'(H \cap K) \cap K = H \cap K$. また前補題より $H' \cap K \lhd H \cap K$ である. さて

$$H' \cap K \lhd H \cap K \Rightarrow H'(H' \cap K) \lhd H'(H \cap K)$$

である. これは $H \lhd I$ かつ $H' \lhd H \Rightarrow H'H \lhd H'I$ ということであるが何故成り立つかは次でいうように明らか. すなわち仮定より $ihi^{-1} \in H, hh'h^{-1} \in H'$でありこの時 $h'ih'h(h'i)^{-1} \in H'H$. なぜなら $h'\underline{ih'hi^{-1}}h'^{-1}$における下線部は $\exists h_* \in H$ とかけるからである.
$H'(H' \cap K) = H' \lhd H'(H \cap K)$ であり同型定理より

$$(H \cap K)/(H' \cap K) \cong H'(H \cap K)/H'(H' \cap K) = H'(H \cap K)/H'$$

同様のことを K, K'と H, H'を入れ替えて行うと $K'(H \cap K') = K' \lhd K'(H \cap K)$ で

$$(H \cap K)/(H \cap K') \cong K'(H \cap K)/K'$$

である. そこで $f : (H \cap K)/(H' \cap K) \xrightarrow{\cong} H'(H \cap K)/H'$, $g : (H \cap K)/(H \cap K') \xrightarrow{\cong} K'(H \cap K)/K'$ とおく. $(H \cap K')(H' \cap K)/(H' \cap K) \subset (H \cap K)/(H' \cap K)$ であり

$$f((H \cap K')(H' \cap K)/(H' \cap K)) = H'(H \cap K')/H' \tag{1.6}$$

である. $H' \cap K \lhd H \cap K$ と $H \cap K' \lhd H \cap K$ より, $(H \cap K')(H' \cap K) \lhd H \cap K$ なので全射準同型を作って

$$(H \cap K')(H' \cap K)/(H' \cap K) \lhd (H \cap K)/(H' \cap K)$$

これと (1.6) より

$$H'(H\cap K')\lhd H'(H\cap K)$$

を得る. 同様に

$$K'(H'\cap K)\lhd K'(H\cap K)$$

である. 次の二つの可換図式 (互いに H,H' と K,K' を取り替えたもの)

$$\begin{array}{ccc}(H\cap K)/(H'\cap K) & \xrightarrow{f} & H'(H\cap K)/H'\\ \downarrow & & \downarrow\\ (H\cap K)/(H\cap K')(H'\cap K) & \longrightarrow & H'(H\cap K)/H'(H\cap K')\end{array}$$

$$\begin{array}{ccc}(H\cap K)/(H\cap K') & \xrightarrow{g} & K'(H\cap K)/K'\\ \downarrow & & \downarrow\\ (H\cap K)/(H\cap K')(H'\cap K) & \longrightarrow & K'(H\cap K)/K'(H'\cap K)\end{array}$$

より $H'(H\cap K)/H'(H\cap K')\cong K'(H\cap K)/K'(H'\cap K)$ を得る. □

定義 17. $G_0,G_1,...,G_n$ は G の部分群で $G=G_0\supset G_1\supset\cdots\supset G_n=\{1\}$ を満たしかつ $G_{i-1}\rhd G_i(i=1,2,...,n)$ を満たすものを

$$G=G_0\rhd G_1\rhd\cdots\rhd G_n=\{1\} \tag{1.7}$$

とかき正規列という. さらに (1.7) が $i=1,2,...,n$ に対し (1)$G_{i-1}\neq G_i$ (2)$G_{i-1}\rhd N\rhd G_i$ となるような N(ただし $G_{i-1}\supsetneq N\supsetneq G_i$) が存在しない
の二条件を満たすとき (1.7) を組成列という. すなわち (1.7) が組成列であるとは正規列であって各 G_{i-1}/G_i は単純群すなわち正規部分群が $\{1\}$ と自身のみであることを指す. なお (2) の条件を細分できないという.

定義 18.

$$G=G_0\rhd G_1\rhd\cdots\rhd G_n=\{1\} \tag{1.8}$$

$$G=H_0\rhd H_1\rhd\cdots\rhd H_\ell=\{1\} \tag{1.9}$$

はいずれも正規列とする.
(同値) まず $n=\ell$ でありある置換 $\sigma:\{1,...,n\}\to\{1,...,n\}$ が存在し $H_{\sigma(i)-1}/H_{\sigma(i)}\cong G_{i-1}/G_i$ が成立するときに (1.8 と (1.9) は同値であるという.
(細分) ある単射 $f:\{0,1,...,n\}\to\{0,1,...,\ell\}$ が存在し
$(i)\forall i,j(0\le i<j\le n\Rightarrow f(i)<f(j))$
$(ii)H_{f(i)}=G_i(\forall i=0,1,...,n)$ が成立するときに (1.9) は (1.8) の細分であるという. すなわち (1.9) が (1.8) の細分であるとは (1.8) の途中にいくつかの項を適当に挿入することによって (1.9) を得られるということである.

命題 23. 二つの正規列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_\ell = \{1\} \tag{1.10}$$

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{1\} \tag{1.11}$$

がある. 上の二つの正規列の細分で同値なものが存在する. これをシュライヤーの細分定理という.

証明. $0 \le i \le \ell, 0 \le j \le m$ に対し ${G_i}^j = G_i(G_{i-1} \cap H_j)$, ${H_j}^i = H_j(G_i \cap H_{j-1})$ とおく.
$G = H_0, G_i \subset G_{i-1}$より直ちに ${G_i}^0 = G_i(G_{i-1} \cap H_0) = G_{i-1}(i \ge 1)$ でありまた ${G_i}^m = G_i(G_{i-1} \cap H_m) = G_i$であるから正規列 (1.10) の細分が次のように取れる.

$$\begin{aligned} G = {G_1}^0 \supset {G_1}^1 \supset {G_1}^2 \supset \cdots \supset {G_1}^{m-1} \supset {G_1}^m = G_1 = {G_2}^0 \supset {G_2}^1 \supset \cdots \supset {G_{i-1}}^m = G_{i-1} = {G_i}^0 \\ \supset {G_i}^1 \supset \cdots \supset {G_i}^m \supset \cdots \supset {G_\ell}^m = \{1\} \end{aligned} \tag{1.12}$$

同様に (1.11) の細分が次のように取れる.

$$G = {H_1}^0 \supset {H_1}^1 \supset \cdots \supset {H_1}^{\ell-1} \supset {H_1}^\ell = H_1 = {H_2}^0 \supset {H_2}^1 \supset \cdots \supset {H_m}^\ell = \{1\} \tag{1.13}$$

どちらの細分も長さは ℓm であるから後は同値であることの条件のもう一方も成り立つことを示す. これは上記ツァッセンハウスの補題において $K \rhd K'$ を $G_{i-1} \rhd G_i$, $H \rhd H'$ を $H_{j-1} \rhd H_j$ に置き換えて適用することにより

$${G_i}^{j-1}/{G_i}^j = G_i(G_{i-1} \cap H_{j-1})/G_i(G_{i-1} \cap H_j) \cong H_j(G_{i-1} \cap H_{j-1})/H_j(G_i \cap H_{j-1}) = {H_j}^{i-1}/{H_j}^i$$

従って (1.12) と (1.13) は同値である. □

命題 24 (ジョルダンヘルダー)**.** (1.10), (1.11) は組成列であるとすると $\ell = m$ であり同値である. すなわち同じ群 G に対する存在する任意の組成列は同値である. 例えば $\{1\} \lhd \mathbb{Z}_3 \lhd \mathbb{Z}_6$ と $\{1\} \lhd \mathbb{Z}_2 \lhd \mathbb{Z}_6$に対し $\mathbb{Z}_6/\mathbb{Z}_3 \cong \mathbb{Z}_2, \mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_3$.

証明. シュライヤーの細分定理より (1.10), (1.11) の各細分 $1', 2'$で同値なものが存在し, (1.10) のその細分 $1'$を $G = G'_0 \rhd G'_1 \rhd \cdots \rhd G'_n = \{1\}$ とする. $i \in \{1, ..., \ell\}$ に対する $G_{i-1} \rhd G_i$について考えるとある $s(i), t(i)(0 \le s(i) < t(i) \le n)$ があって $G_{i-1} = G'_{s(i)} \rhd \cdots \rhd G'_{t(i)} = G_i$とすると $s(i) < k \le t(i)$ なる k に対し $G'_k \lhd G_{i-1}$である. よって $G'_k/G_i \lhd G_{i-1}/G_i$であり G_{i-1}/G_iは単純群なので $G'_k = G_i$または G_{i-1}である.
$2'$を $G = H'_0 \rhd \cdots \rhd H'_n = \{1\}$とすると同値性よりある置換 (permutation)σが存在し, $G'_{k-1}/G'_k \cong H'_{\sigma(k)-1}/H'_{\sigma(k)}$. 組成列なので定義 (17) より $1'$は真の細分ではなく $\{G'_{i-1}/G'_i\}$ は $\{G_{i-1}/G_i\}$ に単位群をいくつか付け加えただけであり $2'$も同様である. したがって $G'_{k-1} = G'_k$となるすべての k と, 対応するすべての$\sigma(k)$ を添字とする G'_kと $H'_{\sigma(k)}$を $1', 2'$から取り除くと長さが等しい組成列となる. このようにして作った組成列 $1'', 2''$はそれぞれ $1, 2$ に一致して特に $\ell = m$ で 1 と 2 は同値である.
このように, 二つの異なる長さの列から得た同値な細分は, もとの組成列という条件によって同じ数の単位群を並び合わせて得たものとして構成されるのでそれらの単位群列を取り除いてできる二つの組成列は同じ長さである. □

問 3. 有限 *Abel* 群 G が単純群で $G \neq \{1\}$ ならば p を素数として $G \cong \mathbb{Z}/p\mathbb{Z}$ である.

証明. G が有限 *Abel* 群のとき $G \cong \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/{p_r}^{e_r}\mathbb{Z}$ とかける. もし $r \geq 2$ なら G が単純群に反するので $G \cong \mathbb{Z}/p^e\mathbb{Z}$ である. $G = \langle g \rangle$ としもし $e \geq 2$ なら $pg \neq 0$ となり $G \neq \langle pg \rangle \triangleleft G$ で反する. □

定義 19. G を群, $a, b \in G$ とする. $[a,b] = aba^{-1}b^{-1}$ としこれを a, b の交換子という. ただし $a^{-1}b^{-1}ab$ とする教科書もある. G の中で $\{[a,b] | a, b \in G\}$ を含む最小の群を $[G,G]$ とかき G の交換子群という.

命題 25. $[G,G]$ の元は r を自然数として $[a_1,b_1][a_2,b_2]\cdots[a_r,b_r]$ という形全体の集合を H とすると $[G,G] = H$.

証明. 明らかに $H \subset [G,G]$. $[a,b][b,a] = aba^{-1}b^{-1}bab^{-1}a^{-1} = 1$ より $[b,a] = [a,b]^{-1}$ より H は群である. 明らかに $H \supset \{[a,b] | a, b \in G\}$ と G の定義より $H \supset [G,G]$. よって $H = [G,G]$. □

命題 26. $H \triangleleft G$ とする. このとき G/H は *Abel* 群 $\Leftrightarrow H \supset [G,G]$ である.

注 14. 一般に $N \triangleleft G$ に対し, G/N が *Abel* $\Leftrightarrow \forall a, b \in G; (aN)(bN) = (bN)(aN) \Leftrightarrow abN = baN$

証明. まず, $[G,G] \triangleleft G$ であることを言い $G/[G,G]$ が *Abel* 群であることを示す. そこで $\forall c \in G$ に対し

$$c[G,G]c^{-1} = [G,G]$$

を示す. $c[a,b]c^{-1} = caba^{-1}b^{-1}c^{-1} = (cac^{-1})(cbc^{-1})(ca^{-1}c^{-1})(cb^{-1}c^{-1}) = [cac^{-1}, cbc^{-1}] \in [G,G]$. これより任意の $a, b, c \in G$ に対して

$$c[a_1,b_1]\cdots[a_r,b_r]c^{-1} = [ca_1c^{-1}, cb_1c^{-1}]\cdots[ca_rc^{-1}, cb_rc^{-1}] \in [G,G]$$

でありよって $c[G,G]c^{-1} \subset [G,G]$ である. すなわち $[G,G] \subset c^{-1}[G,G]c$ であり c を c^{-1} に置き換えれば $c[G,G]c^{-1} \supset [G,G]$ でもありこれで示せた.
次に $G/[G,G]$ が *Abel* を言う. $ab[G,G] \ni ab[b^{-1},a^{-1}] = abb^{-1}a^{-1}ba = ba$ より, $ba[G,G] \subset ab[G,G]$. 逆の包含関係も成り立ち, $ab[G,G] = ba[G,G]$ である. a, b は G の任意の元であったので $G/[G,G]$ は *Abel*.
($\Rightarrow$)G/H は *Abel* とすると任意の $a, b \in G$ に対し $abH = baH$ で特に $a^{-1}b^{-1}H = b^{-1}a^{-1}H$. すなわち $aba^{-1}b^{-1}H = H$ で $[a,b]H = H$. よって $[a,b] \in H$ であり $[G,G] \subset H$ がいえた.
($\Leftarrow$)$[G,G] \subset H$ とすると自然な全射 $\psi : G/[G,G] \to G/H$ があって $G/[G,G]$ は *Abel* なので $\psi(G/[G,G]) = G/H$ も *Abel* 群である. □

定義 20. G が可解群であるとは, ある正規列 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ で $\forall i = 1, 2, ..., n$ に対し G_{i-1}/G_i が *Abel* 群になるようなものが存在することである. そのような正規列をアーベル的正規列という.

命題 27. G を群とし $N_0 = G$, $N_{i+1} = [N_i, N_i] (i = 0, 1, ...)$ とおく. G が可解群 $\Leftrightarrow \exists m \in \mathbb{N}\ N_m = \{1\}$ が成り立つ.

証明. $\Leftarrow$ は $i = 0, 1, ..., n$ に対して $G_i = N_i$とおけば $G/[G,G], N_1/N_2(= N_1/[N_1,N_1]), ...$ は *Abel* であり G は可解である. $\Rightarrow$ を示す. アーベル的正規列

$$G = G_0 \rhd \cdots \rhd G_n = \{1\}$$

をとる. G_0/G_1は *Abel* なので前命題より $G_1 \supset [G_0, G_0] = N_1$である.
今, $G_i \supset N_i$まで示されたとして $G_{i+1} \supset N_{i+1}$を示す. すると G_i/G_{i+1}は *Abel* なので $G_{i+1} \supset [G_i, G_i] \supset [N_i, N_i] = N_{i+1}$である. よって, $N_n \subset G_n = \{1\}$ から $N_n = \{1\}$. 示せた. □

命題 28. 有限群 G が可解群ならば任意の正規列 $G = H_0 \rhd H_1 \rhd \cdots \rhd H_\ell = \{1\}$ に対してある素数 $p_1, ..., p_n$が存在して $H_{i-1}/H_i \cong \mathbb{Z}/p_i\mathbb{Z}(\forall i = 1, 2, ..., \ell)$ となる. すなわち有限群 G が可解となる $\Leftrightarrow$ 組成因子 $\{H_{i-1}/H_i\}(i = 1, ..., \ell)$ がすべて素数位数の群となることである.

証明. 素数位数の群は *Abel* 群なので $\Leftarrow$ は明らか. 最初の主張である $\Rightarrow$ を証明する. アーベル的正規列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

をとる. $G_{i-1} \rhd G_i$の細分を $G_{i-1} = N_0 \rhd N_1 \rhd \cdots \rhd N_r = G_i$とし, $N_{j-1}/N_j \cong \mathbb{Z}/q_i\mathbb{Z}$ (q_iは素数, $j = 1, 2, ..., r$) を示せばよい. アーベル的正規列であるので基本定理より, $p_1, ..., p_r$ を素数として

$$G_{j-1}/G_j \cong \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/{p_r}^{e_r}\mathbb{Z}$$

と表せる. よってある正規列

$$G_{j-1} = K_0 \rhd \cdots \rhd K_r = G_j$$

であって $K_{k-1}/K_k \cong \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}(k = 1, 2, ..., r)$となるものが必ず存在する. したがって $G_{j-1}/G_j \cong \mathbb{Z}/p^e\mathbb{Z}(\exists e \in \mathbb{N})$ の場合に証明すればよいことがわかった. そこで, $\mathbb{Z}/p^e\mathbb{Z} \supset p\mathbb{Z}/p^e\mathbb{Z} \supset \cdots \supset p^e\mathbb{Z}/p^e\mathbb{Z}$ に対応したような *Abel* 群の列

$$G_{j-1}/G_j = L_0 \supset L_1 \supset \cdots \supset L_e = \{1\}$$

があって, $k \in \{0, 1, ..., e\}$ に対し $N_k = G_jL_k$とおけば, $G_{j-1} \rhd L_k$と $G_{j-1} \rhd G_j$より $G_{j-1} \rhd N_k$であり,

$$G_{j-1} = N_0 \rhd N_1 \rhd \cdots \rhd N_e = G_j$$

$$N_{k-1}/N_k \cong G_jL_{k-1}/G_jL_k \cong p^{k-1}\mathbb{Z}/p^k\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$$

よって示せた. □

補題 10 (同型定理)**.** (1) $H \leq G,\ N \lhd G \Rightarrow HN/N \cong H/H \cap N$
(2) $i = 1, 2$ に対し $N_i \lhd G,\ N_1 \subset N_2 \Rightarrow N_2/N_1 \lhd G/N_1$であって $(G/N1)/(N_2/N_1) \cong G/N_2$

命題 29. G を可解群とする. このとき (1) G の部分群 H も可解群 (2) $H \lhd G \Rightarrow G/H$ も可解群である.

証明. (1) アーベル的正規列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\} \tag{1.14}$$

をとる. $H_i = H \cap G_i$ とおくと

$$H = H_0 \supset H_1 \supset \cdots \supset H_r = \{1\}$$

という部分列がある. $G_{i-1} \rhd G_i$ゆえ $G_{i-1} \subset N_G(G_i)$ だから $H_{i-1} \subset N_G(H_i)$ である. 実際に $x \in H_{i-1}, h \in H_i$とすると $xhx^{-1} \in H \cap G_i = H_i$. ($H$ に含まれるのは自明であるが G_{i-1}ではなく G_iに含まれるのは, $\forall a \in G_{i-1}, \forall h \in G_i; aha^{-1} \in G_i$という $G_{i-1} \subset N_G(G_i)$ の条件からである.) $H_i \lhd H_{i-1}$. また $H_{i-1}G_i$は G_{i-1}の部分群で $H_{i-1} \cap G_i = H_i$, そして第二同型定理より,

$$G_{i-1}/G_i \supset H_{i-1}G_i/G_i \cong H_{i-1}/H_{i-1} \cap G_i = H_{i-1}/H_i$$

よって H_{i-1}/H_iは *Abel* 群である. よって H は可解群である.
$f_i : H_{i-1}/H_i \to G_{i-1}/G_i$に対して $\mathrm{Ker} f_i = G_i \cap H_{i-1} = H_i$より f_iは単射でありこの f_iを通して $H_{i-1}/H_i \subset G_{i-1}/G_i$を考えると H_{i-1}/H_iは *Abel* 群である.
(2) $H \lhd G$ の仮定より $G'_i = G_iH$ は G の部分群. アーベル的正規列 (1.14) から G の部分群の列

$$G = G'_0 \supset G'_1 \supset \cdots \supset G'_r = H$$

がある. さらに, $G'_i \lhd G'_{i-1}$である. なぜなら $g \in G_{i-1}, g' \in G_i,\ h, h' \in H$ とし $G_i \lhd G_{i-1}, H \lhd G$ より,

$$g(g'h')g^{-1} = (gg'g^{-1})(gh'g^{-1}) \in G_iH = G'_i$$

$$h(g'h')h^{-1} = g'(g'^{-1}hg')h'h^{-1} \overset{g'^{-1}hg' \in H}{\in} G_iH = G'_i$$

すなわち $G'_i \lhd G_{i-1}$かつ $G'_i \lhd H$ なので $G'_i \lhd G_{i-1}H = G'_{i-1}$である. なお $A \lhd B, A \lhd C \Rightarrow A \lhd BC$ は明らか. そこで$\overline{G}_i = G'_i/H (1 \leq i \leq r)$ とおくと前補題より$\overline{G}_i \lhd \overline{G}_{i-1}$であり,

$$G/H = \overline{G}_0 \rhd \overline{G}_1 \rhd \cdots \rhd \overline{G}_r = \{\overline{e}\}$$

を取れる. また

$$\overline{G}_{i-1}/\overline{G}_i \cong G'_{i-1}/G'_i \cong G_{i-1}H/G_iH \cong G_{i-1}/G_{i-1} \cap G_iH$$

$G_i \subset G_{i-1} \cap G_iH$ より全射準同型な$\pi : G_{i-1}/G_i \to G_{i-1}/G_{i-1} \cap G_iH$ が存在し, $\pi(G_{i-1}/G_i) = \overline{G}_{i-1}/\overline{G}_i$も *Abel* である. よってアーベル的正規列であることが分かった. □

命題 30. G を群とする. $N \lhd G$ で N と G/N が可解群ならば G も可解群である.

証明. アーベル的正規列である

$$N = N_0 \rhd \cdots \rhd N_k = \{1\}$$

$$G/N = M_0 \rhd \cdots \rhd M_\ell = \{1\}$$

が存在する. $g : G \to G/N$ を自然な全射とし $G_i = g^{-1}(M_i)$ $(i = 0, 1, ..., \ell)$, $G_{\ell+j} = N_j$ $(j = 0, 1, ..., k)$ とおくと

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_\ell = N \rhd G_{\ell+1} = N_1 \rhd \cdots \rhd G_{\ell+k} = N_k = \{1\}$$

となる. $i = 1, 2, ..., \ell$に対して $G_{i-1}/G_i \cong M_{i-1}/M_i$でありこれは *Abel* 群なので G は可解群である. □

命題 31. $G_1, ..., G_n$を可解群とする. それらの直積群 $G_1 \times \cdots \times G_n$も可解群である.

証明. $n = 2$ のとき $G = G_1 \times G_2$, $N = G_2$とすると $N \lhd G$, $G/N \cong G_1$より前命題ゆえ G は可解. $n + 1$ の時に関しても, n の時に成り立つと仮定すると $n = 2$ の場合と同様に前命題の適用によって本命題が成立する. □

定義 21. G を群とする. ある正規列

$$G = G_0 \rhd \cdots \rhd G_n = \{1\}$$

で任意の $i = 1, 2, ..., n$ に対し $G_{i-1}/G_i \subset Z(G/G_i)$ を満たすものが存在するとき G を冪零群という. G が冪零群であるとき, また同値な定義が採用されたときに例えば上のような減少列を (降) 中心列という. (昇) 中心列もある. 中心列はアーベル的正規列であるので冪零群は明らかに可解群である. G の真部分群 $H \subsetneq G$ に対し $H \subsetneq K \subsetneq G$ となる G の部分群 K が存在しないとき, H は極大部分群という.

例 1. G をアーベル群とすると

$$\{1\} = G_1 \lhd G_0 = G$$

は $G/\{1\} \cong G \subset Z(G)$ より冪零群である.

命題 32. G を冪零群とする.
(1) H は G の部分群とすると H は冪零群である.
(2) $H \lhd G$ とすると G/H も冪零群である.

証明. 中心列を部分群に制限した場合が (1) で剰余群に制限した場合が (2) であるがどちらもまた中心列である. □

命題 33. $G_1, ..., G_n$が冪零群ならば $G_1 \times \cdots \times G_n$も冪零群である.

証明. $n = 2$ の場合を示せば十分である. そこで G_1, G_2を改めて G, H とかき各正規列を

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_\ell = \{1\}$$

とおくと仮定より $G_{i-1}/G_i \subset Z(G/G_i)$, $H_{j-1}/H_j \subset Z(H/H_j)$. ここで $G \times H_{j-1}/G \times H_j \cong H_{j-1}/H_j \subset Z(H/H_j) \cong Z(G \times H/G \times H_j)$ である. これにより, $N = G \times H$, $N_j = G \times H_j$ $(j = 0, 1, ..., \ell)$, $N_{\ell+i} = G_i \times \{1\}$ $(i = 1, 2, ..., n)$ とおくと

$$N = N_0 \rhd N_1 \rhd \cdots \rhd N_\ell \cong G \rhd \cdots \rhd N_{\ell+n} = \{1\}$$

は中心列である. □

注 15. 群 G の中心 $Z(G)$ とは $Z(G) = \{a \in G | \forall b \in G$ に対し $ab = ba\}$ であり $Z(G) \lhd G$. $N_G(H) = \{a \in G | aHa^{-1} = H\}$.

命題 34. G を冪零群とし $H \subsetneq G$ を部分群とする.
(1) $H \subsetneq N_G(H)$ である. ただし $N_G(H) = \{a \in G | aHa^{-1} = H\}$ である.
(2) $H \subsetneq G$ が極大部分群ならば $H \lhd G$ が成り立つ.

証明. $h \in H$ のとき $hH = H = Hh$ より $h \in N_G(H)$. よって $H \subseteq N_G(H)$ である. 中心列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

をとる. $G_i \subset H, G_{i-1} \not\subset H$ となるある $i \in \{1, 2, ..., n\}$ が存在する. 任意に $a \in G_{i-1}, b \in H$ を取る. $G_{i-1}/G_i \subset Z(G/G_i)$ より $\overline{a} = aG_i, \overline{b} = bG_i$ とおくと中心の定義から

$$\overline{a}\overline{b} = \overline{b}\overline{a}$$

よって $\overline{a}\overline{b}\overline{a}^{-1}\overline{b}^{-1} = \overline{1} \in G_{i-1}/G_i$ である. これは即ち左辺が G_i の元であることを意味する為 $aba^{-1}b^{-1}$ が G_i の元であることが分かった. よって $[a, b] = aba^{-1}b^{-1} \in G_i \subset H$, $b^{-1} \in H$ より $aba^{-1} \in H$ である. よって $aHa^{-1} \subset H$ であり逆の包含関係も同様に示せるので $aHa^{-1} = H$. よって $a \in N_G(H)$ で $a \in G_{i-1}$ は任意であったから $G_{i-1} \subset N_G(H)$. $H \subset N_G(H)$ は自明であり, もし $H = N_G(H)$ なら $G_{i-1} \not\subset H$ に反するので示せた.
(2) を示す. H を極大部分群とする. $H \subsetneq N_G(H)$ で H は極大なので $N_G(H) = G$ つまり任意の $a \in G$ に対し $aHa^{-1} = H$. 即ち $H \lhd G$. □

命題 35. ある自然数 r を使って位数が p^r とかける p 群 G は冪零群である.

証明. r に関する帰納法で示す. $r = 1$ のとき $G \cong \mathbb{Z}/p\mathbb{Z}$ で G は *Abel* 群より $Z(G) = G$ なので $G = G_0 \rhd G_1 = \{1\}$ が中心列となり G は冪零群.$(*)$ $r \geq 2$ とし $r - 1$ の場合まで主張は正しいとする. もし $Z(G) = G$ なら G は *Abel* 群で $(*)$ であるので G は冪零群. よって $Z(G) \subsetneq G$ とする. $G_0 = G$, $G_1 = Z(G)$ とする. $Z(G) \lhd G$ より $G_1 \lhd G_0$, また $|Z(G)| = p^s (\exists s < r)$ である. 類等式

$$|G| = |Z(G)| + \sum_{|C_i| \geq 2} |C_i|$$

において $|C_i|$ は p の倍数なので $|Z(G)|$ は p の倍数で $s \geq 1$ である. 従って帰納法の仮定から $Z(G)$ は冪零群である. $G/Z(G)$ も G より位数の小さい p 群なので冪零群. $G \cong G/Z(G) \times Z(G)$ も命題 (33) より冪零群である. □

補題 11. $N \lhd G$, p は素数で P は G の *pSylow* 群とする. $P \subset N$ ならば $G = NN_G(P)$ である.

証明. $\supset$ は自明なので $\subset$ を示す. $P \subset N$ より P は N の $pSyllow$ 群でもある. aPa^{-1}は P の共役な N の $pSyllow$ 群. $syllow$ の定理よりある $b \in N$ が存在して $bPb^{-1} = aPa^{-1}$. すなわち $b^{-1}a \in N_G(P)$ であるから $a = b(b^{-1}a) \in NN_G(P)$. □

命題 36. G を有限群とするとき以下は同値である.
(1) G は冪零群
(2) G の任意の極大部分群は正規部分群
(3) $|G|$ の任意の素因数 p に対し G の $pSyllow$ 群は G の正規部分群
(4) $|G| = {p_1}^{e_1} \cdots {p_r}^{e_r}$ とし G の $p_iSyllow$ 群を $P_i(i = 1, 2, ..., r)$ とすると $G \cong P_1 \times \cdots \times P_r$ となる.

証明. (1) $\Rightarrow$ (2) は示している. (1) $\Rightarrow$ (3) : P を G の $pSyllow$ 群とする. もし $N_G(P) = G$ なら $P \triangleleft G$ より G は p 群なので G はまた冪零群である. (3) が成り立たないように $N_G(P) \subsetneq G$ と仮定する. G は有限群なので $N_G(P) \subset N \subsetneq G$ となる極大部分群 N があり, 命題 (34) より $N \triangleleft G$ であり前補題から $G = NN_G(P)$. $N_G(P) \subset N$ から $NN_G(P) = N$ なので $G = N$ となり矛盾した. (3) $\Rightarrow$ (4) : $P_i \triangleleft G(i = 1, 2, ..., r)$ とすると $H = P_1P_2 \cdots P_r$は部分群をなす. $P_i \cap P_j(i \neq j)$ の元は位数は ${p_i}^{e_i}$の約数かつ ${p_j}^{e_j}$の約数であるから 1 で $P_i \cap P_j = \{1\}$. よって $P_1P_2 \cdots P_i \cap P_{i+1} = \{1\}(i = 1, 2, ..., r-1)$. よって $H = P_1 \times \cdots \times P_r$であり, 位数の比較から $H = G$. (4) $\Rightarrow$ (1) : 各 P_i は冪零群であり $G \cong P_1 \times \cdots \times P_r$も冪零群である. □

次のページ以降ではジョルダン・ヘルダーの定理を違った見方により再び示し, また素因数分解の一意性との関わりを述べる.

補題 12. G は組成列をもつ群としそれを

$$\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$$

とする. $\forall K \lhd G$ に対し

$$\{1\} = K \cap G_n \lhd K \cap G_{n-1} \lhd \cdots \lhd K \cap G_0 = K$$

は組成列である.

証明. $\forall i$ に対して $K \cap G_{i+1} \lhd K \cap G_i$であることと $K \cap G_i / K \cap G_{i+1}$が単純群であることを示せばよい. まず前者をいう. $x \in K \cap G_i, g \in K \cap G_{i+1}$とすると, それぞれ $K \lhd G, G_{i+1} \lhd G_i$ なので $xgx^{-1} \in K, xgx^{-1} \in G_{i+1}$. よって $xgx^{-1} \in K \cap G_{i+1}$より,

$$K \cap G_{i+1} \lhd K \cap G_i$$

である. 後者を示す. G_i/G_{i+1}は単純群より G_{i+1}は G_iの最大の正規部分群 $\Leftrightarrow G_{i+1}$を含む G_i の正規部分群は G_{i+1}と G_i. ここで, 自然な全射 $G \to G/K$ の制限 $G_i \to G_i/K$ の核を考えると $K \cap G_i \lhd G_i$である. さて,

$$G_{i+1} \lhd (K \cap G_i)G_{i+1} \lhd G_i$$

が成り立つ. 最初の $\lhd$ は $\forall kg \in (K \cap G_i)G_{i+1}$に対して, $kgG_{i+1}g^{-1}k^{-1} = kG_{i+1}k^{-1} \subset G_{i+1}$であることによる. 次の $\lhd$ は $\forall g_i \in G_i$に対して,

$$g(K \cap G_i)G_{i+1}g^{-1} \overset{K\cap G_i \lhd G_i}{=} (K \cap G_i)gG_{i+1}g^{-1} \overset{G_{i+1}\lhd G_i}{\subset} (K \cap G_i)G_{i+1}$$

であることによる. よって,

$$(K \cap G_i)G_{i+1} = G_{i+1} \text{または } G_i$$

であり, 同型定理より

$$(K \cap G_i)G_{i+1}/G_{i+1} \cong (K \cap G_i)/(K \cap G_i \cap G_{i+1}) = K \cap G_i/K \cap G_{i+1}$$

よって, もし $(K \cap G_i)G_{i+1} = G_{i+1}$なら $K \cap G_i = K \cap G_{i+1}$で明らかに命題の列は組成列. また $(K \cap G_i)G_{i+1} = G_i$のときは

$$G_i/G_{i+1} \cong K \cap G_i/K \cap G_{i+1}$$

なので後者が示せた. □

命題 37 (ジョルダン・ヘルダーの定理)**.** G を群とする. するといかなる異なる G の組成列も同じ長さであり,

$$\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$$

$$\{1\} = H_n \lhd H_{n-1} \lhd \cdots \lhd H_0 = G$$

という組成列に対してある置換 τが存在して $G_i/G_{i+1} \cong H_{\tau(i)}/H_{\tau(i)+1}$.

例 2. 巡回群 C_{12} は *3* つの組成列

$$C_1 \lhd C_2 \lhd C_6 \lhd C_{12},\ C_1 \lhd C_2 \lhd C_4 \lhd C_{12},\ C_1 \lhd C_3 \lhd C_6 \lhd C_{12}$$

をもちどれも同じ長さであり組成因子 $\{C_2, C_3, C_2\}, \{C_2, C_2, C_3\}, \{C_3, C_2, C_2\}$ は要素の順番を入れ替えると同じである.

証明. まず $m = n$ を帰納法で示す. $n-1$ まで正しいとする.

$$\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G\ (\forall i \text{ で } G_i \neq G_{i+1})$$

$$\{1\} = H_m \lhd H_{m-1} \lhd \cdots \lhd H_0 = G\ (\forall i \text{ で } H_i \neq H_{i+1})$$

を長さがそれぞれ n, m の G の組成列とする. $G_1 = H_1$のとき, 長さ $n-1$ の G_1の組成列に対し帰納法の仮定を使うと $n-1 = m-1$ が成り立つから $G_1 \neq H_1$の場合を考える. G_1 と H_1 は共に G の最大の正規部分群より $H_1 \underset{\neq}{\lhd} G_1H_1 \lhd G$ より $G_1H_1 = G$.

$$G_1H_1/H_1 = G/H_1 \cong G_1/H_1 \cap G_1$$

であり G/H_1は単純なので $G_1/H_1 \cap G_1$も単純$^{(*)}$である. 前補題より, H_1の組成列

$$\{1\} = H_1 \cap G_1 \lhd \cdots \lhd H_1 \cap G_0 = H_1$$

があり H_1を削いでせいぜい長さ $n-1$ の組成列

$$\{1\} = H_1 \cap G_n \lhd \cdots \lhd H_1 \cap G_1$$

がある. $(*)$ より

$$\{1\} = H_1 \cap G_n \lhd \cdots \lhd H_1 \cap G_1 \lhd G_1$$

も組成列であり,

$$\{1\} = G_n \lhd \cdots \lhd G_1$$

という長さ $n-1$ の G_1の組成列もあったので帰納法の仮定より前後者同じ長さである. $G_1 \neq H_1$ゆえ $G_1 \neq H_1 \cap G_1$だから, これはすなわち上の一見長さ n の方は次の長さ $n-1$ の

$$\{1\} = K_n \lhd \cdots \lhd K_3 \lhd K_2 = H_1 \cap G_1 \lhd K_1 = G_1 \tag{1.15}$$

である. なお $\exists\alpha[G_i/G_{i+1} \cong K_{\alpha(i)}/K_{\alpha(i)+1} (i = 1, 2, ..., n-1)]$. すると

$$G = G_0 \rhd \cdots \rhd G_n = \{1\}$$

$$G = K_0 \rhd G_1 = K_1 \rhd K_2 = H_1 \cap G_1 \rhd K_3 \rhd \cdots \rhd K_n = \{1\}$$

は長さ n の G の組成列でなお $G_i/G_{i+1} \cong K_{\alpha(i)}/K_{\alpha(i)+1} (i = 0, ..., n-1)$ を満たす. 前補題より

$$H_1 \cap G_1 \rhd \cdots \rhd H_m \cap G_1 = \{1\}$$

という組成列があり, また (1.15) より長さ $n-2$ の $H_1 \cap G_1$ に対する組成列も存在する.
よって帰納法の仮定よりこれも長さ $n-2$ である. $H_1/H_1 \cap G_1 \cong H_1G_1/G_1 = G_0/G_1$ なので $H_1/H_1 \cap G_1$ は単純であるから,

$$H_1 \rhd H_1 \cap G_1 \rhd \cdots \rhd H_m \cap G_1 = \{1\}$$

は長さ $n-1$ の H_1 の組成列である. よって帰納法の仮定から

$$H_1 \rhd H_2 \rhd \cdots \rhd H_m = \{1\}$$

も長さ $n-1$ であるので $m-1 = n-1$. $m = n$ である.
次に, 組成因子が順序を除いて一意であることを帰納法で示す.

$$H_1 \rhd H_1 \cap G_1 \rhd H_2 \cap G_1 \rhd \cdots \rhd H_n \cap G_1 = \{1\}$$

という長さ $n-1$ の組成列において $L_1 = H_1, L_2 = H_1 \cap G_1$ などとおくと長さ n の G の組成列

$$G = H_0 \rhd H_1 \rhd \cdots H_n = \{1\}$$

$$G = L_0 \rhd L_1 \rhd \cdots \rhd L_n = \{1\}$$

を得る. 長さ $n-1$ に対しての帰納法の仮定による $H_i/H_{i+1} \cong L_{\beta(i)}/L_{\beta(i)+1} (i = 0, 1, ..., n-1)$ はここで $\{1, ..., n-1\}$ の置換 β を $\beta(0) = 0$ とすることで $\{0, ..., n\}$ に拡げられていることに注意.
$K_2 = L_2 = H_1 \cap G_1$ としたので G の組成列

$$G \rhd G_1 \rhd H_1 \cap G_1 \rhd K_3 \rhd \cdots \rhd K_n = \{1\}$$

$$G \rhd H_1 \rhd H_1 \cap G_1 \rhd L_3 \rhd \cdots \rhd L_n = \{1\}$$

がある. $H_1 \cap G_1$ から列が始まると見るとそれに対して帰納法の仮定から,

$$K_i/K_{i+1} \cong L_{\gamma(i)}/L_{\gamma(i)+1} \ (i = 2, 3, ..., n-1)$$

を満たす $\{2, 3, ..., n-1\}$ の置換 γ が存在する. さらに同型 $G/G_1 \cong H_1/H_1 \cap G_1, G/H_1 \cong G_1/H_1 \cap G_1$ により γ は

$$\gamma(0) = 1, \ \gamma(1) = 0$$

と定めることで

$$K_0 = G = L_0, \ K_1 = G_1, \ L_1 = H_1, \ K_2 = L_2 = H_1 \cap G_1$$

より

$$K_i/K_{i+1} \cong L_{\gamma(i)}/L_{\gamma(i)+1} \ (i = 0, 1, ..., n-1)$$

を得る. 以上より $\forall i = 0, 1, ..., n-1$ に対し

$$K_i/K_{i+1} \cong L_{\gamma(i)}/L_{\gamma(i)+1}, \ G_i/G_{i+1} \cong K_{\alpha(i)}/K_{\alpha(i)+1}, \ H_i/H_{i+1} \cong L_{\beta(i)}/L_{\beta(i)+1}$$

で $\tau := \beta^{-1}\gamma\alpha$ とおくと

$$G_i/G_{i+1} \cong H_{\tau(i)}/H_{\tau(i)+1}$$

がいえたので, 本証明の最初の導入部分における二つの G の組成列の同値性が示せた. □

系 2. n を正の整数とする. 相異なる素数 $p_1, p_2, ..., p_k$ と正の整数 $r_1, ..., r_k$ があって $n = {p_1}^{r_1} \cdots {p_k}^{r_k}$ が成り立つ. また表示は一意である.

証明. G を位数 n の巡回群とし $G = \langle g \rangle$ とする. すると G の任意の部分群は正規部分群で, n を割り切る最大の整数を $d(\neq n)$ とし, そして G_1 を位数 d の G の唯一の部分群とする. $G_1 \lhd G$ であり G/G_1 は単純な巡回群である. (巡回群なのは n/d が素数だからであるが, 単純であることがいま効く.) 同様の操作を巡回部分群 G_1 に対してすることによって次の組成列

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{1\}$$

を得る. 各 G_i/G_{i+1} の位数は素数 $p_i (i = 0, 1, ..., m-1)$ なので

$$n = |G| = |G/G_1||G_1| = |G/G_1||G_1/G_2| \cdots |G_{m-1}/G_m||G_m| = p_0 p_1 \cdots p_{m-1}$$

ジョルダンヘルダーの定理より, G の組成列は一意的であるので素因数分解の一意性も従う. □

G が冪零群とは正規列

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

であって $G_{i+1}/G_i \subset Z(G/G_i) (i = 0, ..., n-1)$ が満たされることであった. このときの列を中心列といった. 次の命題はこの冪零群の定義と同値な事柄である.

命題 38. (1) G は冪零群
(2) $\delta^0(G) := G, \delta^i(G) := [\delta^{i-1}(G), G] (i \geq 1)$ と定義すると列

$$G = \delta^0(G) \supset \delta^1(G) \supset \cdots \supset \delta^i(G) \supset \cdots$$

は有限の長さで単位群に達し, $\exists m; \delta^m(G) = \{1\}$ である.
(3) $Z_0(G) := \{1\}, Z_{i+1}(G)/Z_i(G) := Z(G/Z_i(G)) (i \geq 0)$ と定義すると列

$$\{1\} = Z_0(G) \subset Z_1(G) \subset \cdots \subset Z_i(G) \subset \cdots$$

は有限の長さで元の群に達し, $\exists n; Z_n(G) = G$ である.

証明. (3) $\Rightarrow$ (1) は冪零群の定義より成立. (1) $\Rightarrow$ (3) : G の中心列

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_n = G$$

をとる. $H_i \subset Z_i(G) \equiv Z_i (\forall i \geq 0)$ を示せば上の n が $Z_n(G) = G$ を満たすことになりよい. $i = 0$ のとき成立し, $i-1$ のときも $H_{i-1} \subset Z_{i-1}$ が正しいとする. 自然な写像 $\pi : G/H_{i-1} \to G/Z_{i-1}$ を考える. 中心列ゆえ $H_i/H_{i-1} \subset Z(G/H_{i-1})$ より,

$$\pi(H_i/H_{i-1}) \subset Z(G/Z_{i-1}) \equiv Z_i/Z_{i-1}$$

である. よって π の定義より $H_i \subset Z_i$ である.
(2) $\Rightarrow$ (1) : 一般に $H \lhd G$ に対して

$$H/[H, G] \subset Z(G/[H, G])$$

である. よって$\delta^i(G) \triangleleft G$ をいえば$^{(*)}$, 後はこの一般的性質から

$$G/[G,G] \subset Z(G/[G,G]),\ [G,G]/[[G,G],G] \subset Z(G/[[G,G],G]), ...$$

であるのですなわち (3) の列は中心列である. では $(*)$ を示す. $i = 0$ なら $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G,G]$ で成り立つ. $i-1$ まで正しいとすると $\forall g \in G, \forall x \in \delta^{i-1}(G)$ に対し, $gxg^{-1} \in \delta^{i-1}(G)$ だから $\forall g,h \in G, x \in \delta^{i-1}(G)$ に対して $g[h,x]g^{-1} \in [G, \delta^{i-1}(G)]$. 逆元をとって $g[x,h]g^{-1} \in [\delta^{i-1}(G), G] \equiv \delta^i(G)$. よって i のときも成り立つ.
(1) $\Rightarrow$ (2) : 中心列 $\{G_i\}_{0 \leq i < n}$に対し$\delta^i(G) \subset G_{n-i}$を示せば, $\delta^n(G) \subset G_0 = \{1\}$ より示せたことになる. 帰納法によって示す. $i = 0$ のときは明らか. i のときが正しいとし $i+1$ のときを考える. $\delta^{i+1}(G) := [\delta^i(G), G] \subset [G_{n-i}, G]$. (1) の仮定より $G_{n-i}/G_{n-i-1} \subset Z(G/G_{n-i-1})$ により,

$$[G_{n-i}, G] \subset G_{n-i-1}$$

である. よって $\delta^{i+1}(G) \subset G_{n-(i+1)}$. □

定義 22. H を G の部分群とする. G の任意の自己同型 f に対し $f(H) = H$ であるとき H は特性部分群 (*characteristic subgroup*) であるといい, H *char* G とかく. g を固定し $G \ni x \mapsto gxg^{-1} \in G$ の共役写像を内部自己同型といい特性部分群は正規部分群である. f の定義域を特性部分群 H に制限した f_Hは H の内部自己同型である.

命題 39. G を群とし, H, K を G の部分群とする. (1) H は K の特性群, K は G の特性群としたとき H は G の特性群. (2) H は K の特性群, $K \triangleleft G$ としたとき $H \triangleleft G$.

証明. (1) ϕを G の自己同型とすると$\phi(K) = K$ で$\phi|_K$は K の自己同型. H は K の特性群より$\phi|_K(H) = H$ であるがこれは$\phi(H) = H$ でもある. (2) K の自己同型写像は $g \in G$ を固定して$\phi|_K : k \mapsto gkg^{-1}$で定まる. これは $K \triangleleft G$ より良定義である. H は K の特性群より制限 $\phi|_H : h \mapsto ghg^{-1}$に関して $gHg^{-1} \subset H$ を満たすから $H \triangleleft G$. □

問 4. 有限群は組成列をもつことを示せ.

証明. G は有限群なので可能な限り長い正規部分群の列 $\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$ をとれる. もし $\forall i$ に対する G_i/G_{i+1}が単純でないなら $G_i \rhd N \rhd G_{i+1}$となる $N \neq G_i, G_{i+1}$が存在するのでこれは最大の長さの列をとったことに反する. よって組成列である. □

問 5. 無限巡回群 G は組成列をもたないことを示せ.

証明. $G = \langle g \rangle, |g| < \infty$ とする. 組成列 $\{1\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$ があるとする. もし $n = 1$ なら $\{1\} = G_1 \triangleleft G$ より G は単純であるが G は例えば $\langle g^2 \rangle \triangleleft G$ という真正規部分群をもつので反する. $n \geq 2$ であり組成列は $G_{n-1} \neq \{1\}, G$ を含む. 即ち G_{n-1}は自明でない G の正規部分群で $\exists k \in \mathbb{N}; G_{n-1} = \langle g^k \rangle$. しかし G_{n-1}は巡回群なので単純でない. 組成列であることに反する. □

問 6. $GL_n(\mathbb{R})$ は正規部分群列をもつが組成列はもたない.

証明. まず, End(V) で V 上の線型変換全体とする. n 次元 $\mathbb{R}$ 上線型空間 V に対する $GL_n(V) = \{f \in \mathrm{End}(V) | \exists g \in \mathrm{End}(V); f \circ g = id\}$ と $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) | \det A \neq 0\}$ は同型である.

$$\{1\} \lhd Z(GL_n(\mathbb{R})) \lhd SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$$

は正規部分群列であるが組成列はもたない. これは無限巡回群と同型な $GL_n(\mathbb{R})$ の正規部分群 $\{kE_n | k \in \mathbb{R}\}$ が存在するため. 単純群は自身も自明群ではない. □

問 7. 一般二面体群 $D_{2n} = \{a, b | a^n = b^2 = 1, b^{-1}ab = a^{-1}\}$ について, D_{2n}は可解であるか.

証明. G が可解群であることの同値な定義はいくつかあったがその一つは正規列

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

であって G_{i+1}/G_iはアーベル群であることである. 回転 a に対する $\langle a \rangle$ は正規部分群なので

$$\{1\} \lhd \langle a \rangle \lhd D_{2n}$$

があり $D_{2n}/\langle a \rangle$ は位数 2 の巡回群. 任意の巡回群はアーベル群なのでよって可解. □

問 8. $D_6 = \{a, b | a^3 = b^2 = 1, b^{-1}ab = a^{-1}\}$ は冪零ではないことを示せ.

証明. 一般に D_{2n}に対し n が奇数のとき, 2 が位数 $2n$ を割る最大の 2 の冪なため位数 2 の部分群が *syllow* 群であり, 2*syllow* 群 P_2の個数 n_2は 3 である. $n_2 \equiv 1 (\mathrm{mod} 2)$. 有限冪零群は任意の p に対する p*Syllow* 群の直積群と同型なので冪零ではない.
[1], P.68 によれば二面体群 D_{2n}は $\langle a | a^n = 1 \rangle$ を正規部分群としてもつとある. これにより $n_2 = 1, 3$ は *syllow* の定理でもってしても可能性が残るが 1 の場合はないことになる. もし $n_2 = 1$ なら 2*yllow* 群 P_2の個数はただ一つであり $P_2 \lhd D_6$となり $P_2 = \langle a | a^3 = 1 \rangle$ であるが P_2に位数 3 の元は存在しないので矛盾. □

定義 23. $G := G^{(0)}, G^{(n+1)} := [G^{(n)}, G^{(n)}] (n \geq 0)$ とかくと $G^{(n)} \lhd G$ であった. 特にある非負整数 n が存在して $G^{(n)} = \{1\}$ となるとき G は可解群といい, またそのような最小の整数 n を G のランクといい $d(G)$ とかく. 例えば単位群でないアーベル群はランク 1 の可解群である.
$G_{(0)} := G$, $G_{(n)} := [G_{(n-1)}, G] (n \geq 0)$ とかくと $G_{(n)} \lhd G$ であった. $G_{(n)} = \{1\}$ を満たす非負整数 n が存在するとき G を冪零群, またそのような最小の n を G のクラスといい $c(G)$ とかく. 単位群でないアーベル群はクラス 1 の冪零群である.

問 9. 冪零な四元数群 Q_8 のクラスは 2 であることを示せ.

証明. Q_8 の中心列は

$$\{1\} = G_2 \lhd G_1 = \{\pm 1\} \lhd G_0 = Q_8$$

実際に中心列であることを示す. G_1は Q_8の中心であり中心は常に正規部分群ゆえ $G_1 \lhd Q_8$より正規列である. $G_1/G_2 \cong \{\pm 1\} \subset Z(G/G_2) \cong \{\pm 1\}$である. また $G_0/G_1 \cong G/Z(G)$ で $|G/Z(G)| = 4$ でかつもし巡回群なら, 命題 (20) 中の (*Claim*3) より Q_8がアーベル群となるので, そうではない. よって $G/Z(G)$ はラインの四元群. よって可換性を含意するので $G/Z(G) \subset Z(G/Z(G))$ が成り立つ. またこの中心列はこれ以上長さが短くなるとすれば Q_8はアーベル群となるのでそれはない. □

補題 13. p を素数とし, H を有限群 G の p 部分群であって $p|[G:H]$ を満たすものとする. このとき $p|[G:H] \Rightarrow p|[N_G(H):H]$.

証明. $|G| = p^\alpha m, (p,m) = 1$ とし $|H| = p^\beta$(ただし $p|[G:H]$ より$\beta \leq \alpha$) とする. *syllow* の定理より H を含む G の *psyllow* 群 $K(|K| = p^\alpha)$ が存在する. よって $H \leq N_K(H)$, また $N_K(H) \leq N_G(H)$ より $H \lneq N_G(H)$ でありこれは $p|[N_G(H):H]$ を意味する. なお *syllow* の定理が効いている所は $H \leq N_K(H)$ の所もで, ここは次の G を K に置き換えることで言える.

H が G の部分群であるときに, H を正規部分群として含むような最大の G の部分群が $N_G(H)$

□

補題 14 ([1])**.** G を冪零群とする. G の正規部分群 $N \neq \{1\}$ に対し

$$N \cap Z(G) \neq \{1\}$$

が成り立つ.

証明. $\pi : G \to G/Z(G)$ を自然な準同型とする. $\pi(N) = \{1\}$ なら $N \subset Z(G)$ で $N \cap Z(G) \neq \{1\}$. よって$\pi(N) \neq \{1\}$ とする. 冪零群 G の中心は $\{1\}$ ではないから $|G/Z(G)| < |G|$. よって $n \in N$ で$\pi(n) \neq 1$ かつ$\pi(n) \in Z(G/Z(G))$ となるものが存在. $\pi(n) \neq 1$ より $n \notin Z(G)$ でつまり $\exists g \in G; gn \neq ng$. $\pi[n,g] = [\pi(n), \pi(g)] \overset{n \text{ の性質}}{=} 1$ より $[n,g] = ngn^{-1}g^{-1} \in Z(G)$. よって $1 \neq n(gn^{-1}g^{-1}) \in N \cap Z(G)$ である. □

注 16. G が有限群でないときはこの限りではない. 反例として

$$G = \bigcup_{n \geq 1} U(p,n)$$

をみる. $Z(U(p,n))$ は, 対角線上には$\overline{1}$が並び $(1,n)$ にある $\mathbb{F}_p$の元を除いて$\overline{0}$がしきつめられたような上三角行列からなる, 乗法での位数 p の巡回群である. もはや無限 p 群 G の中心 $Z(G) = Z(\cup_{n\geq 1} U(p,n)) \subset Z(\lim_{n\to\infty} U(p,n)) = \begin{pmatrix} \ddots & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix}$ より $Z(G) = \{1\}$.

問 10. G を位数 16 の群とする. また G は位数 4 の元 g をもつとすると $\langle g^2 \rangle \triangleleft G$ であることを示せ.

証明. もし $\langle g \rangle \triangleleft G$ なら, $\langle g^2 \rangle$ もまた G の正規部分群である. なぜなら $\langle g^2 \rangle$ は G の特性群である.
($\because$ $\langle g \rangle$ の任意の自己同型 f をとると $f : g^i \mapsto g^j \in G$ より $f((g^2)^i) = f(g^i)^2 = (g^j)^2 \in \langle g^2 \rangle$.) 次に, $\langle g \rangle$ が G の正規部分群でないときは $\langle g \rangle$ の正規化群

$$H = \{h \in G; h\langle g \rangle = \langle g \rangle h\}$$

の位数は 8 である. 実際, H は G の部分群より $|H| = 1, 2, 4, 8, 16$ で $|H| \geq |\langle g \rangle|$ より $|H| = 4, 8, 16$. 16 とすると $\langle g \rangle \triangleleft G$ となるから違う. $|H| = 4$ なら g の位数が 4 より $H = \langle g \rangle$ であるがこれは前補題に矛盾する. $\langle g^2 \rangle$ が H における特性群であることを示せばよい. そのとき $\langle g^2 \rangle$ は, 指数 2 の G の正規部分群 H に対する特性群である.
我々は H が位数 8 の群, $\langle g \rangle$ が位数 4 の群のときに $\langle g^2 \rangle$ は H での特性群であることを示せばよい. もし H がアーベル群なら $H \cong C_8, \langle g \rangle \times C_2$ でありどちらの場合についても特性群となる. もし H がアーベル群でないなら, $|Z(H)| = 2$ ($\because$ 中心の位数は $|H|$ を割り切る. もし $4, 8$ なら $|H/Z(H)| = 2, 1$ となり素数位数より $H/Z(H)$ は巡回群なので H がアーベル群になってしまう.) G が p 群ゆえ冪零なので前補題より中心は H の自明でない任意の正規部分群と共通部分をもち, $\langle g^2 \rangle$ は $\langle g \rangle \triangleleft H$ の唯一の位数 2 の部分群なので $Z(H) = \langle g^2 \rangle$. 常に $Z(H)$ は H での特性部分群であるから示せた. □

問 11. P を有限群 G の $pSyllow$ 群とすると, $N_G(N_G(P)) = N_G(P)$ である. すなわちもし H が $N_G(P)$ に含まれるような G の部分群であるとき $N_G(H) = H$ である.

証明. $N_G(H)$ を $N(H)$ とかくことにし, $H \subset N(H)$ は自明なので逆を示すために $\forall x \in N(H)$ をとると $xHx^{-1} = H$. $P \subset N(P) \subset H$ より $xPx^{-1} \subset xHx^{-1} = H$ なので P と xPx^{-1} は共に H の $pSyllow$ 群である. H に対する $syllow$ の定理より $\exists y \in H; xPx^{-1} = yPy^{-1}$ となる. $y^{-1}xP(y^{-1}x)^{-1} = P$ より $y^{-1}x \in N(P) \subset H$ なので $x \in yH = H$ である. □

問 12. (12) における次の命題を示せ. G を群とする. H と K を任意の有限部分群とすると

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

なおもし $K \triangleleft G$ の仮定があるのならこれは同型定理に帰着される.

証明. $f : H \times K \ni (h, k) \mapsto hk \in HK$ と定めると f は全射より $|HK| \leq |H \times K| < \infty$. よって HK は有限群である. $h_1k_1, ..., h_dk_d$ を HK の異なる元とすると $H \times K$ は $f^{-1}(h_ik_i), i = 1, 2, ..., d$ の直和で表せる. 集合 $f^{-1}(hk) = \{(hg, g^{-1}k) | g \in H \cap K\}$ に対し $|f^{-1}(hk)| = |H \cap K|$ より, $|H \times K| = d|H \cap K|$. d とは $|HK|$ のことであり $|H \times K| = |H||K|$ よりよい. □

問 13 (Cauchy)**.** 素数 p を $|G|$ の約数とするとき G は位数 p の元をもつことを示せ.

証明. P を G の $pSyllow$ 群とし $1 \neq x \in P$ をとる. すると x の位数は p 冪であり $ordx = p^k$ とかける. $ord\ x^{p^{k-1}} = p$ である. □

定義 24. ここでは G が p 群であるとは G の任意の元の位数が p 冪であることとせよ. p 群に関連するこれまでの命題では G が有限群のときを扱っていたので次系を意識することはなかったが補足的に注意しておく.

系 3. 有限群 G は p 群であることと G の位数が p 冪であることは同値である.

証明. もし G の位数が p 冪でないならそれは異なる素数 q で割り切れる. そして前命題より G は位数 q の元をもつ. しかしこれは p 群であることに矛盾. 逆も明らか. □

例 3. $U(p,n)$ を有限体 $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ 上の $n \times n$ 上三角行列であって対角線上には$\overline{1}$が並ぶものとする. $|U(p,n)| = p^{n(n-1)/2}$, また $U(p,n)$ は p 群である.

$$G = \bigcup_{n \geq 1} U(p,n)$$

は任意の元の位数が p 冪の無限 p 群であるが $|G|$ は p 冪ではない.

問 14. G を位数 231 の群とする. n_pで $pSylow$ 群の個数をかくとする.
(1) $11syllow$ 群 M はただ一つである.
(2) n_7を求めよ.
(3) P を $3syllow$ 群, L を $7syllow$ 群とする. $N = PL$ は位数 21 の部分群をなす.
(4) N は正規部分群である.
(5) $G = MN$ と表せるか.
(6) $M \subset Z(G)$ である.

証明. (1)$231 = 11 \cdot 3 \cdot 7$. $n_{11} \equiv 1 (\mathrm{mod}\ 11), n_{11} | 21$ より $n_{11} = 1$. (2) 同様に $n_7 = 1$. (3)$n_7 = 1$ より $L \lhd G$ である. $pl \in PL$ とすると $(pl)^{-1} = l^{-1}p^{-1}$で $\forall g \in G$ に対し $gL = Lg$ より $l^{-1}p^{-1} \in Lp^{-1} = p^{-1}L$, $\exists l'; l^{-1}p^{-1} = p^{-1}l'$. つまり逆元も PL に含まれる. また $plp'l' \in PL$ も L の正規部分群性から $lp' = p'l''$より, $p(lp')l' = p(p'l'')l' \in PL$ と示せる. PL は部分群である.
$|P| = 3, |L| = 7, P \cap L = \{1\}$ より $|PL| = |P||L|/|P \cap L| = 21$.
(4) 正規化群 $N_G(N)$ を考える. これは G の部分群なのでその位数は $|G|$ の約数である. $N \subset N_G(N)$ より $|N_G(N)| \geq 21$. $|N_G(N)| > 21$ を示せば $|N_G(N)| = 231$ となり証明は終わる.
$|N_G(N)| > 21$ つまり $N_G(N) \neq N$ をいうために $N_G(N)$ に属し N には属さない元の存在を示せばよい. 中心の元を一つ挙げる. $Cauchy$ より G は位数 3 の元 g をもつ. M は唯一の $11syllow$ 群なので $M \lhd G$ で $M = \langle m \rangle$ とする. $gM = Mg$, よって $gm = m^l g$ において $l = 1$ を示す. $ord\ g = 3$ より $m = g^3 m g^{-3} = g^2(gmg^{-1})g^{-2} = g^2 m^l g^{-2} = g(gm^l g^{-1})g^{-1} = g(m^{l^2})g^{-1} = m^{l^3}$. $l^3 \equiv 1 (\mathrm{mod} 11)$ より $l = 1$. (5)$N \lhd G$ より MN は群である. $|M| = 11, |N| = 21$ より $M \cap N = \{1\}$ で $|MN| = 231$. よって $G = MN$ である. (6) もし $m \in M, n \in N$ なら M の正規部分群性から $mnm^{-1}n^{-1} \in M \cap N = \{1\}, mn = mn$ より M は N と可換. M は G と可換であることを言うために $G = MN$ を使う. 任意の $g \in G$ は $g = m'n'$ とかけ $gm = m'n'm = mm'n' = mg$ より M は G と可換. □

問 15. 位数 200 の群は単純群ではない.

証明. $5syllow$ 群の個数 $n_5 \equiv 1 (\mathrm{mod}\ 5)$ で 8 を割り切る. よって $n_5 = 1$ で $5syllow$ 群は正規部分群となる. □

問 16. $|G| = p^2 q, (p,q) = 1$ のとき G は正規 $pSylow$ 群と正規 $qSylow$ 群をもつことを示せ.

証明. $p, qSylow$ 群がただ一つ存在することを否定するとし, $n_p, n_q > 1$ とする. まず G の位数 q の元の数を数える. もし $qSylow$ 群の位数が q ならそれは巡回群で単位元でない任意の元によって生成される. よって一つの G の $qSylow$ 群には位数 q の元 $q-1$ こがある. もし y が位数 q なら y が生成する巡回群は $qSylow$ 群でどんな異なる $qSylow$ 群も自明な共通部分しかもたない.(もし位数 q の共通元があれば異なる部分群ではなくなるため.) よって

位数 q の元の数は $n_q(q-1)$. $n_q|p^2$であるが $n_q = 1$ とすると仮定に反するため n_qは p または p^2である. $n_q = p^2$のとき, G の中で位数 q でない元の数は $p^2q - p^2(q-1) = p^2$である. 一方で, $|P| = p^2$であり P の任意の元は位数 q でない. よって $pSyllow$ 群はただ一つであるから仮定に矛盾した. 次に $n_q = p$ のとき $n_q \equiv 1 (\mathrm{mod}\ q)$ より $p > q$ である. $n_p|q, q$ は素数なので $n_p = 1$ または q である. $n_p \equiv 1 (\mathrm{mod}\ p)$ であり $q \equiv 1 (\mathrm{mod}\ p)$ なら $q > p$ を意味しこれは矛盾. よって $n_p = 1$ であるが仮定に矛盾した. □

問 17. G を位数 59 以下の群とする. もし G が単純群なら $|G|$ は素数であることを示せ.

証明. $|G| = pq$ のときは G は単純ではないのだった. $k > 0$ としてこれは $|G| = p^k m, (m, p) = 1, m < p$ のときに拡張される. 実際 n_pは m を割り切るが $n_p \equiv 1 (\mathrm{mod}\ p)$ よりもし $n_p \neq 1$ なら $n_p \geq p + 1 > m$ だが $n_p|m$ に反する. よって位数 $12, 24, 30, 36, 40, 45, 48, 56$ の群が単純ではないことを示す. $|G| = 45 = 5 \cdot 3^2$は $|G| = p^2q$ の形なので単純でない. $|G| = 40$ のとき $n_5 \equiv 1 (\mathrm{mod}\ 5)$ で n_5は 8 を割り切るため $n_5 = 1$ で正規 $5syllow$ 群をもつ. $|G| = 56 = 2^3 \cdot 7$ のとき $n_7 \equiv 1 (\mathrm{mod}\ 7)$ で 8 を割り切る. もし $n_7 = 1$ なら G は単純でなく $n_7 = 8$ なら位数 7 の元は $6 \cdot 8 = 48$ こあり, 位数 7 でない元は G の中に 8 こしかないがこれは $2syllow$ 群 P_2 が $|P_2| = 8$ であるのに反する.(つまりこのとき P_2の個数は唯一つとなり G は単純でない.) 同様に $|G| = 12$ のときは $n_3 \equiv 1 (\mathrm{mod}\ 3), n_3|4$ より $n_3 = 1, 4$ である. $n_3 = 1$ なら G は単純でなく $n_3 = 4$ なら位数 3 の元の数は $4 \cdot 2 = 8$ である. 残りの 4 つの元は $2syllow$ 群 P_2 に含まれ $|P_2| = 4$ であるから矛盾. 位数 $24, 30, 36, 48$ の群については独立に解決するしかない. 位数 $30 = 2 \cdot 3 \cdot 5$ の単純群が存在するとする. $n_3 = 1 (\mathrm{mod}\ 3), n_3|10$ より $n_3 = 1, 10$. G は単純群なので $n_3 = 10$. よって G は異なる 10 この $3syllow$ 群をもち各 $3syllow$ 群は位数 3 の元を 2 こ含む. よって G には位数 3 の元を少なくとも 20 こ存在する. $n_5 = 1 (\mathrm{mod}\ 5), n_5|6$ より $n_5 = 6$. よって G には位数 5 の元を 24 こは存在する. $|G| = 30$ なので矛盾した. $syllow$ の定理より位数 24 の群は単純群でない. 自明でない準同型$\phi : G \to \mathfrak{S}_k; g \mapsto \begin{pmatrix} P_1 & P_2 & \cdots & P_k \\ gP_1g^{-1} & gP_2g^{-1} & \cdots & gP_kg^{-1} \end{pmatrix}$を定める. これは $\mathrm{Syl}_k(G)$ への G の作用 $G \times \mathrm{Syl}_k(G) \to \mathrm{Syl}_k(G)$ の置換表現であるが $syllow$ 群は互いに共役であるため推移的な作用である.
$|G| = 2^3 \cdot 3, 2^4 \cdot 3$ のとき $2syllow$ 群の個数が 1 なら単純でないからよい. 個数を 3 とすると $G \to \mathfrak{S}_3$への非自明な準同型があり $|G| > S_3$より全単射ではない. よって $\{1\}, G \neq \mathrm{Ker}\ \phi \lhd G$ ($G \neq \mathrm{Ker}\ \phi$なのはもし, $syllow$ 群の個数が 1 であれば $\mathfrak{S}_k$の元は恒等置換となり $\forall g \in G$ に対し $G \ni g \mapsto 1 \in \mathfrak{S}_k$となるからである.) であり G は単純でない. $|G| = 2^2 \cdot 3^2$ に対しては $3syllow$ 群の個数を考える. 1 ならよくて 4 とすると非自明な準同型 $G \to \mathfrak{S}_4$があり同様に G は単純でない. □

注 17 (burnside)**.** p, q を素数とし a, b を非負整数とする. $|G| = p^a q^b$である群 G は可解である. 位数 59 以下の群は可解, 特に単純ではない.

命題 40. p, q を相異なる素数とし $|G| = pq$ とする. G は単純でない. また, もし $q \neq 1 (\mathrm{mod}\ p)$ なら $pSyllow$ 群の個数は 1 である. もし $q \neq 1 (\mathrm{mod}\ p), p \neq 1 (\mathrm{mod}\ q)$ なら G は巡回群である.

証明. 最後を示す. $pSyllow$ 群を $P, qSyllow$ 群を Q とする. $P, Q \lhd G$ であり P, Q は巡回群より $P = \langle x \rangle, Q = \langle y \rangle$ とかく. $xyx^{-1}y^{-1} \in P \cap Q = \{1\}$ より $xy = yx$. よって $(xy)^n = x^n y^n$が成り立ちこれにより xy の位数は pq である. $G = \langle xy \rangle$. □

問 18. G を位数 105 の非アーベル群とする. $|Z(G)| \neq 7$ を示せ.

証明. $|Z(G)| = 7$ とすると $|G|/|Z(G)| = 15$ より $G/Z(G)$ は位数 $15 = 3 \cdot 5$ の群. 前命題より $G/Z(G)$ は巡回群より G はアーベル群である. □

定義 25. 群 G に対して G から G への同型写像を G の自己同型といいその全体を $\mathrm{Aut}(G) = \{f : G \to G | f \text{ は自己同型 }\}$ とかく. $\mathrm{Aut}(G)$ は写像の合成について群をなすため G の自己同型群という.

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{m \in \mathbb{Z}/n\mathbb{Z}; 1 \leq m \leq n-1, gcd(n,m) = 1\}$$

を定義すると, これは位数 $\varphi(n)$ の群をなす. ただし $\varphi(n)$ はオイラー関数である.

証明. 群であることを示す. $gcd(m,n) = gcd(m'n) = 1$ となる任意の $m, m' \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ に対して $gcd(mm', n) = 1$ より $m \cdot m' = mm' \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. よって乗法に関して閉じている. この乗法における結合法則は自明で単位元も存在. 逆元の存在をいう. 任意の $m \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ に対し $gcd(m,n) = 1$ よりある整数 x, y で $mx + ny = 1$ となるものが存在する. $gcd(x,n) = 1$ より $m^{-1} = x \in (\mathbb{Z}/n\mathbb{Z})^{\times}$なので群である. □

定義 26. G を群とし $x \in G$ とする. $\forall g \in G$ に対し$\theta_g : G \to G$ を $x \mapsto gxg^{-1}$で定めるとθ_g は G 上の自己同型となる. これを G の内部自己同型というのだった. また $\mathrm{Inn}(G) = \{\theta_g : G \to G\}$ は $\mathrm{Aut}(G)$ に対する部分群であり G の内部自己同型群という. 部分群であることは $\forall g, h \in G$ に対し $x \mapsto hxh^{-1} \mapsto g(hxh^{-1})g^{-1} = ghx(gh)^{-1}$ より$\theta_g\theta_h = \theta_{gh}$, また$\theta_g{}^{-1} = \theta_{g^{-1}}$ による.

補題 15. $\mathrm{Aut}(C_n) \cong (C_n)^{\times}$である.

証明. 任意の$\sigma \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対し$\sigma(1) = m$ とするとσは同型写像なので m は $\mathbb{Z}/n\mathbb{Z}$ の生成元である. なぜならもしそうでないとすると $\mathrm{Im}(\sigma) = \langle m \rangle \neq \mathbb{Z}/n\mathbb{Z}$ であるがこれはσが同型であることに矛盾. このとき $gcd(m,n) = 1$ より $f : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$を$\sigma \mapsto \sigma(1)$ で定める. このとき, f は同型である. 実際, 任意の$\sigma, \tau \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対し, $\sigma(1) = m, \tau(1) = m'$とすると $f(\sigma\tau) = ((\sigma\tau))(1) = \sigma(m') = m'\sigma(1) = mm' = m \cdot m' = f(\sigma)f(\tau)$ となるので f は準同型である. 次に f が単射であることを示す. $f(\sigma) = f(\tau)$ とすると$\sigma(1) = \tau(1)$. 任意の $k \in \mathbb{Z}$ に対し$\sigma(k) = k\sigma(1) = k\tau(1) = \tau(k)$ より$\sigma = \tau$. また f の全射性を示す為に任意の $m \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ に対し$\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}; k \mapsto mk$ を定める. するとσは $\mathbb{Z}/n\mathbb{Z}$ 上の同型写像でありすなわち $\sigma \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ より f は全射である. ではσの同型性を示す. $k = \ell$であれば $n|(mk - m\ell)$ だから $mk = m\ell$となりσは良定義である. なお f は代表元に対する写像でないので良定義は関係ない. 任意の $k, \ell \in \mathbb{Z}/n\mathbb{Z}$ に対し,

$$\sigma(k + \ell) = m(k + \ell) = mk + m\ell = \sigma(k) + \sigma(\ell)$$

よりσは準同型. 任意の$\ell \in \mathbb{Z}/n\mathbb{Z}$に対し, $gcd(m,n) = 1$ より $mx+ny = 1$ となるある $x, y \in \mathbb{Z}$があるので, $mx\ell + ny\ell = \ell$である. 従って$\sigma(x\ell) = mx\ell = \ell$より$\sigma$は全射. 次に, $\sigma(k) = \sigma(\ell)$ とすると $mk = m\ell$であるが両辺に上の x による乗法を演算させれば $k = \ell$となる. よってσは単射. □

補題 16. n が互いに素な自然数 $n_1, ..., n_r$ を用いて $n = n_1 \cdots n_r$ とかけるとするとき,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times$$

となる.

証明. [5] より引用した. □

定義 27. G, H を群とする. $\cdot$ は $G \times H$ 上での以下の諸条件を満たすときの演算を表すとする. $\forall g \in G, \forall h \in H$ に対しある $g \cdot h \in H$ が一意に定まり,
(1) $\forall g, g' \in G, \forall h \in H$ に対して $g \cdot (g' \cdot h) = (gg') \cdot h$
(2) $\forall h \in H$ に対して $1 \cdot x = x$
(3) $\forall g \in G, \forall h, h' \in H$ に対して, $g \cdot (hh') = (g \cdot h)(g \cdot h')$
が成り立つとき, G は H に作用するといった.

命題 41. 群 G から群 H への作用を考えることと準同型 $G \to \mathrm{Aut}(H)$ を考えることは等価である. これは群 G の集合 X への作用を与えることと群の置換表現を与えることが等価であったことへの類似である. 群の集合への作用と同様, 自明な準同型 $G \ni g \mapsto id_H \in \mathrm{Aut}(H)$ に対応する G の H への作用を自明な作用という.

証明. G が H に作用しているとしそれを $G \times H \to H$ とする. すると $\forall g \in G$ に対し $\sigma_g : H \to H$ を $h \mapsto g \cdot h$ で定めることが可能である. このとき, $\sigma_g \in \mathrm{Aut}(H)$ である. なぜなら作用の定義 (3) より σ_g は準同型. また, $\sigma_g \sigma_{g^{-1}} = id_H$ の逆写像の存在より σ_g は全単射だからである. よって $\sigma : G \to \mathrm{Aut}(H); g \mapsto \sigma_g$ を定めると, 作用の定義 (1) より $\sigma(gg') = \sigma(g)\sigma(g')$ で準同型である.

$$\sigma(gg')(h) = \sigma_{gg'}(h) = gg' \cdot h,\ \sigma(g)\sigma(g')(h) = \sigma_g\sigma_{g'}(h) = \sigma_g(g' \cdot h) = g \cdot (g' \cdot h)$$

逆に, 準同型 $\sigma : G \to \mathrm{Aut}(H)$ が存在するとき, $\forall g \in G, \forall h \in H$ に対し, $g \cdot h := \sigma_g(h)$ と定義することで G が H に作用する. □

定義 28. K を群, $\sigma : K \to \mathrm{Aut}(H)$ を準同型とする. 集合としての直積 $G = H \times K$ 上に $\forall (h, k), (h', k') \in G$ とし, $(h, k) \cdot (h', k') := (h\sigma_k(h'), kk')$ と演算を定義する. すると G はこの演算に関し群であり, H と K の半直積群 (semidirect product) といい $G = H \rtimes_\sigma K$ とかく. 作用 $\sigma_k : K \times H \to H$ に対応する σ を略記して $G = H \rtimes K$ ともかく. $\sigma_k(h') = k \cdot h'$ が $k \cdot h' = h'$ という自明な作用であるとき, $H \rtimes K = H \times K$.

定義 29. G を群とし, H, K を G の部分群とし, また $G = HK, H \lhd G, H \cap K = \{1\}$ とする. このとき G を H と K の内部半直積群 (interior semiproduct) といって $G = H \dot{\rtimes} K$ とかき, 事実としてこれは K の H への共役作用に対応する $\sigma : K \to \mathrm{Aut}(H)$ に関する半直積群と同型である.

補題 17 (半直積群の表示)**.** K, N を $K = \langle Y \mid S \rangle$, $N = \langle X \mid R \rangle$ と表示が与えれた群とし, 準同型 $\sigma : N \to \mathrm{Aut}(K)$ が存在するとする. 任意の $x \in X, y \in Y$ に対して, $\sigma(x)(y) \in K$ を Y の語で書き表わしたものを $w_{x,y}$ とする.

$$T := \{x^{-1}yxw_{x,y}{}^{-1} \mid x \in X, y \in Y\}$$

とおくと

$$K \rtimes_\sigma N = \langle X \cup Y \mid R \cup S \cup T \rangle$$

となる.

証明. [5] より引用した. □

命題 42. 位数 105 の群 G を分類せよ.

証明. もしアーベル群なら $G \cong \mathbb{Z}/105\mathbb{Z}$ である. $105 = 3 \cdot 5 \cdot 7$ で 7*syllow* 群がある. これが正規部分群でないと仮定する. $n_7 | 15, n_7 = 1 (\mathrm{mod}\ 7)$ より 7*syllow* 群は 15 こ存在するので位数 7 の元が $15 \cdot 6 = 90$ こある. このとき 5*syllow* 群は正規部分群である. なぜなら正規でないとすると, それは 1 こではなく 21 こ存在するので位数 5 の元が $21 \cdot 4 = 84$ こあるから $84 + 90 > 105$ となり矛盾. また 3*syllow* 群も正規部分群である. なぜなら正規でないとするとそれは 7 こ存在し, 位数 3 の元が $7 \cdot 2 = 14$ こある. 位数 5 の元が 4 こあることが分かっているので $90 + 14 + 4 > 105$ となり矛盾. よって, 7*syllow* 群が正規でないと仮定したとき位数 15 の正規部分群が存在する ($\because\ gp_5g^{-1} \in P_5, gp_3g^{-1} \in P_3$のとき $gp_5p_3g^{-1} \in P_5P_3$) ことで $G \cong C_{15} \rtimes C_7$であるが $\mathrm{Aut}(C_{15}) \cong C_2 \times C_4 (\not\cong C_8)$ には位数 7 の元がないので半直積は自明, すなわち群準同型$\varphi : C_7 \to \mathrm{Aut}(C_{15})$ は C_7の任意の元を C_{15}上の恒等自己同型写像に対応させるものとなり $G \cong C_{15} \times C_7 \cong C_{105}$. よって G はアーベル群でありつまり任意の部分群が正規部分群であるので最初の仮定に反する.
以下, 正規 7*syllow* 群を N とする. すると G/N が定義され, 短完全列

$$\{1\} \to N \to G \to G/N \to \{1\}$$

において $|N| = 7, |G/N| = 15$ は互いに素なので分裂する. よって G/N と同型な部分群 H が存在して $G \cong N \rtimes H, N \cong C_7, H \cong C_{15}$である. (以下の注意における逆のようなことも成り立つ.)
非自明な半直積を誘導する準同型$\varphi : H \to \mathrm{Aut}(N)$ を定めると H の生成元 y に対応すべき非自明な $\mathrm{Aut}(N) \cong C_6$の元として考えられるのは, その元の位数が 15 の約数でなければならないから N の生成元を x とするとき, $x \mapsto x^2$しかありえない.

$$x \mapsto x^2 \mapsto x^4 \mapsto x$$

この写像としての元の位数は 3 であり唯一の 15 の約数となっている. 以下の他の対応は 15 の約数でない.

$$x \mapsto x^3 \mapsto x^2 \mapsto x^6 \mapsto x^4 \mapsto x^5 \mapsto x$$

$$x \mapsto x^4 \mapsto x$$

$$x \mapsto x^5 \mapsto x^4 \mapsto x^6 \mapsto x^2 \mapsto x^3 \mapsto x$$

$$x \mapsto x^6 \mapsto x$$

よって非自明な半直積は補題 (17) より

$$G = \langle x, y | x^7 = y^{15} = y^{-1}xyx^{-2} = 1 \rangle$$

のみ. $\langle y^3\rangle = Z(G)$ より $xy^3 = y^3x = a$ とおく. $y^5 = b$ とおくと関係式より $a^{35} = 1, b^3 = 1$ で, $b^{-1}ab = y^{-5}(y^3x)y^5 = (y^{-2}xy^2)y^3 = (y^{-1}x^2y)y^3 = (y^{-1}xy)^2y^3 = x^4y^3 = x^{11}y^{33} = a^{11}$なので

$$G = \langle a, b | a^{35} = b^3 = 1, b^{-1}ab = a^{11}\rangle$$

とも表示できる. また

$$G = \langle C_5 \times \langle x, y\rangle | x^7 = y^3 = 1, y^{-1}xy = x^2\rangle$$

である. □

注 18. 半直積群 $G \cong K \rtimes H$ に対して分裂拡大

$$1 \to K \xrightarrow{\tau} G \xrightarrow{\pi} N \to 1$$

が存在する.

証明. 自然な準同型$\tau : K \to G, \pi : G \to N$ を $k \mapsto (k, 1)$ と $(k, n) \mapsto n$ で定めると

$$1 \to K \xrightarrow{\tau} G \xrightarrow{\pi} N \to 1$$

を得る. $s : N \to G$ を $n \mapsto (1, n)$ により定めれば$\pi \circ s = id_N$なのでこの系列は分裂する. □

問 19. $K = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ の自己同型群 $\mathrm{Aut}(K)$ は $\mathbb{Z}/2\mathbb{Z}$ に同型であり $\mathrm{Aut}(K)$ の元を $f : 1 \mapsto 3$ とすると $\mathrm{Aut}(K) = \{id, f\}$ である. $N = \mathbb{Z}/2\mathbb{Z} = \{1, t\}$ に対して非自明な準同型 $\sigma : N \ni t \mapsto f \in \mathrm{Aut}(K)$ を定める. このとき $G = K \rtimes H$ の表示をかけ.

証明. $K = \langle s | s^4 = 1\rangle$ とする. ただし, K は加法群であるが表示は同型対応 $K \ni k \mapsto s^k \in K$ によって乗法群として表されているとした. $G = K \rtimes N$ という書き表し方は N から K へ作用していると思え, t の s への作用は f の定義より$\sigma(t)(s) = s^3$だから $G = \langle s, t |\ s^4 = t^2 = t^{-1}sts^{-3} = 1\rangle$. □

注 19. [5] では位数 n の乗法巡回群から位数 m の加法巡回群への準同型を構成することで正二面体群 D_{2n}の更なる一般化といえるような位数 mn の非可換群を作っている.

問 20. P を p 群とする. A を P における極大可換正規部分群とする. このとき, $C_P(A) = A$.

証明. $A \lhd P$ より $C := C_P(A) \lhd P$ である. $C \neq A$ と仮定すると $C' = C/A \neq 1$ より C' は $P' = P/A$ の非自明な正規部分群である. よって $C' \cap Z(P') \neq 1$ より $U' = U/A \subset C' \cap Z(P')$ であって, $|U'| = p, U' \lhd P/A$ となるような巡回群 U'が存在する. 従って U は P での可換正規部分群であって $A \subset U$. これは A の極大性に矛盾した. □

問 21. $A \lhd P, A = C_P(A)$ ならば $|P : A|\,|\,(|A| - 1)!$である.

証明. A の単位元ではない元全体の集合を X とおく. $A \lhd P, pxp^{-1} = 1 \Leftrightarrow x = 1$ より, X には単位元 1 がないので自明な置換を考えることなく P から X への共役への作用 $P \times X \to X$ を与えられる. $f : P \ni p \mapsto \begin{pmatrix} x_1 & \cdots & x_n \\ px_1p^{-1} & \cdots & px_np^{-1} \end{pmatrix} \in Sym(X)$ において, $x \in X$ が $p \in P$ での共役作用で不変なことと $p \in C_P(x)$ が同値なので $\mathrm{Ker}(f) = \{p \in P | \forall x \in X$ に対し $p \in C_P(x)\}$ である. $p \in \cap_{x\in X} C_P(x) = \cap_{x\in X, x\in\{1\}} C_P(x) = \cap_{x\in X} C_p(x) \cap P = C_P(A) = A$ より $\mathrm{Ker}(f) = A$. よって同型定理より $P/A \cong Sym(X)$ なので $|P : A|\,|\,|Sym(X)|$. $|Sym(X)| = (|A| - 1)!$. □

問 22. G を位数 m のアーベル群とする. n が m を割り切れば G は位数 n の部分群を持つことを示せ.

証明. m を割り切る素数 p を選ぶ. *Cauchy* より $ord\ a = p$ であるような $a \in G$ が存在する. $N = \langle a \rangle$ とし $Q = G/N$ とおくと $|Q| = m/p$ であり, 位数 n/p の Q の部分群 H がある. G の部分群 HN が求める群である. □

問 23. G を群とし $\mathrm{Aut}(G)$ をその自己同型群とする. $\mathrm{Aut}(G)$ が巡回群ならば G はアーベル群であることを示せ.

証明. $\mathrm{Aut}(G)$ の部分群 $\mathrm{Inn}(G)$ も巡回群である. $\mathrm{Inn}(G) \cong G/Z(G)$ より $G/Z(G)$ も巡回群で G はアーベル群である. 次のように背理法で示すことも可能である. $x, y \in G$ であって x, yxy^{-1} は可換でないように取れる. なぜなら G を非可換群と仮定すると $xz \neq zx$ となる z が存在し, $x := y^{-1}zy, yxy^{-1} := z$ と取れるからである. $\mathrm{Aut}(G)$ は巡回群なのである自然数 n があって $f^n = C_x \in \mathrm{Aut}(G)$ とかけ, これは $C_x(z) = xzx^{-1}$ を満たす. またある自然数 m があって $f^m = C_y, C_y(z) = yzy^{-1}$. C_x と C_y は可換なので, $C_xC_y(x) = C_yC_x(x) = C_y(x) \Leftrightarrow yxy^{-1} = xyxy^{-1}x^{-1} \Leftrightarrow (yxy^{-1})x = x(yxy^{-1})$. よって矛盾した. □

問 24. G を $|G| = n$ の有限群とする. $\mathrm{Aut}(G)$ が巡回群となる必要十分条件は $n = 4$ または $n = 2^m p^k$(ただし $m = 0, 1$, p は奇素数, $k \geq 0$) である. $n = 4$ については $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ではないものとする.

証明. (16) から従う. $G \cong C_2 \times \cdots \times C_2 \times \mathbb{Z}/p^k\mathbb{Z}$ のような場合も考え得るがその自己同型群は巡回群即ちただ一つの生成元から生成される群とはならない. 例えば $k = 0$ であって $G \cong C_2 \times C_2$ の場合, $\mathrm{Aut}(C_2 \times C_2) \cong D_6 = \langle x, y | x^3 = y^2 = 1, xy = yx^2 \rangle \cong S_3$ である. D_6 が三次対称群に同型であることはよい. よって生成元は唯一ではない. $C_2 \times C_2$ は $\mathbb{Z}/2\mathbb{Z}$ 上の線形空間なので $\mathrm{Aut}(C_2 \times C_2) = GL_2(C_2)$. $\mathbb{Z}/2\mathbb{Z}$ 上の 2 次正則行列全体がなす非可換群 $GL_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ は S_3 に同型. 何故なら一般に位数 6 の非可換群 $G \cong S_3$ だからである. *Cauchy* より G には位数 2 の H と位数 3 の K がある. $[G : K] = 2$ より $K \lhd G$. もし $H \lhd G$ なら $G = HK, H \cap K = \{1\}, \forall h \in H, k \in K; hkh^{-1}k^{-1} \in H \cap K$ より G が非可換群に矛盾. よって H は G の正規部分群でない. G の gH への作用が誘導する ($\therefore \mathrm{Ker}(f) \subset H$) 全射準同型 $f : G \to S_3 = \langle (1, 2), (1, 2, 3) \rangle$(一般に $S_n = \langle (1, 2), (1, ..., n) \rangle$) に対して $\mathrm{Ker}(f) \neq H$ より $\mathrm{Ker}(f) = \{1\}$. よって f は単射より $G \cong S_3$. □

補題 18. $\delta^0(G) = G, \delta^1(G) = D^1(G) = [G, G], \delta^2(G) = [G, \delta^1(G)], ..., \delta^i(G) = [G, \delta^{i-1}(G)]$ と定めたとき, 次が成り立つ.
(1) $\delta^i(G) \lhd G$, (2) $\delta^i(G) \subset \delta^{i-1}(G)$, (3) $\delta^{i-1}(G)/\delta^i(G) \subset Z(G/\delta^i(G))$

証明. (1) $i = 1$ のとき成立. i による帰納法で示すことができる. 又, 証明は既述. (2) $x \in G, y \in \delta^{i-1}(G)$ とすると $\delta^{i-1}(G) \lhd G$ より $[x, y] \in \delta^{i-1}(G)$. $[x, y] \in \delta^i(G)$ より $\delta^i(G) \subset \delta^{i-1}(G)$. (3) $\forall y \in \delta^{i-1}(G)$ に対し $x' = x\delta^i(G), y' = y\delta^i(G)$ とおくと $x'y'x'^{-1}y'^{-1} = [x, y]\delta^i(G) = \delta^i(G) = 1' \in G/\delta^i(G)$ なので $x'y' = y'x'$. 即ち $y' \in Z(G/\delta^i(G))$ である. □

問 25. $N \lhd G$ とする. $\forall i$ について $N\delta^i(G) = \delta^i(G)N$ を示せ.

証明. 前補題 (1) より$\delta^i(G) \triangleleft G$ であるが勝手な $N \triangleleft G$ に対し $N \subset \delta^i(G)$ なら $N \triangleleft G$ より $N \triangleleft \delta^i(G)$ で$\delta^i(G) \subset N$ なら$\delta^i(G) \triangleleft N$ であるから $\forall i$ について $N\delta^i(G) = \delta^i(G)N$ である. □

問 26. $G/Z(G)$ が冪零ならば G も冪零である.

証明. まず降中心列における$\delta^i(G/N) = N\delta^i(G)/N$ を示す. $i = 0$ の時は

$$\delta^0(G/N) = G/N,\ N\delta^0(G)/N = NG/N \overset{N\triangleleft G}{=} GN/N \cong G/G \cap N = G/N$$

より良い. k の時まで成立するとする.

$$\delta^{k+1}(G/N) = [G/N, \delta^k(G/N)] = [G/N, N\delta^k(G)/N] = \langle [xN, yN] | xN \in G/N, yN \in \delta^k(G/N) \rangle$$

ここで $y \in \delta^k(G)$ である. 何故なら $N\delta^k(G) = \delta^k(G)N$ なので $yN \in N\delta^k(G)/N \Leftrightarrow \exists y' \in \delta^k(G) \exists n \in N\ s.t.\ yN = y'nN$ であり即ち $y \in \delta^k(G)$. よって,

$$\langle [xN, yN] | x \in G, y \in \delta^k(G) \rangle = [G, \delta^k(G)]N \subset N\delta^{k+1}(G)/N$$

が成り立つ. これで一方の包含関係が示せた. 次に k まで正しい即ち $N\delta^k(G)/N = \delta^k(G/N)$ として逆の包含 $N\delta^{k+1}(G)/N \subset \delta^{k+1}(G/N)$ を示す. $\delta^{k+1}(G)$ の生成元に注目する為 $x \in G, y \in \delta^k(G)$ とする. このとき $yN \in N\delta^k(G)/N = \delta^k(G/N)$ より $[x, y]N = [xN, yN] \in [G/N, \delta^k(G/N)] = \delta^{k+1}(G/N)$.
次に $G/Z(G)$ を冪零群とすると, ある n に対して$\delta^n(G/Z(G)) = \{1\}$ が成り立つ. $\delta^i(G/N) = \delta^i(G)N/N$ において N を $Z(G)$ とおくと$\delta^n(G)Z(G)/Z(G) = \{1\}$. よって$\delta^n(G) \subset Z(G)$ であり $\delta^{n+1}(G) = [G, \delta^n(G)] = \{1\}$. $\delta^\ell(G) = \{1\}$ となるような番号 ℓが存在したので G は冪零群となる. □

定義 30. G の極大部分群全体の交叉を G の Frattini 部分群といい $\phi(G)$ とかく. $\phi(G)$ は明らかに G の正規部分群である. 何故なら特性群であることが次のように分かるからである. f を G 上の任意の自己同型とする. もし M が G の極大群なら $f(M)$ も G の極大群なので $f(\phi(G)) = f(\cap M) = \cap f(M) = \phi(G)$ である. 更に次も成り立つ.

命題 43. $\phi(G)$ は冪零群である.

証明. P を $\phi(G)$ の $pSylow$ 群とする. 任意の $x \in \phi(G)$ に対し $x^{-1}Px$ も $\phi(G)$ の $pSylow$ 群でありある $y \in \phi(G)$ に対し $x^{-1}Px = y^{-1}Py$ が成り立つので $xy^{-1} \in N_G(P), x \in N_G(P)\phi(G)$. よって $G = N_G(P)\phi(G)$ であるが $G = N_G(P)$ 即ち $\forall g \in G; gP = Pg, P \lhd G$(なぜなら, もしそうでなければ M を $N_G(P) \subset M : G$ の極大群とすれば$\phi(G) \subset M$ より $G = M$ となり矛盾.) で $\phi(G)$ の $pSylow$ 群は唯一である. $\phi(G)$ は極大な $pSylow$ 群の共通部分という定義だった. $\phi(G)$ はある $pSylow$ 群の直積とみなせ冪零である. □

2 Linear Algebras

2.1 [9] 第 4 章

解 1. $\mathbb{K}^n$の部分空間 $W_1 = \{\langle \boldsymbol{w}_1, ..., \boldsymbol{w}_k \rangle\}, W_2 = \{\langle \boldsymbol{w}'_1, ..., \boldsymbol{w}'_\ell \rangle\}$ に対し

$$\boldsymbol{b} \in W_1 \cap W_2$$

$\Leftrightarrow \exists x_i, y_j \in \mathbb{K}(1 \leq i \leq k, 1 \leq j \leq \ell)\ s.t.\ x_1\boldsymbol{w}_1 + \cdots + x_k\boldsymbol{w}_k = y_1\boldsymbol{w}'_1 + \cdots + y_\ell\boldsymbol{w}_\ell = \boldsymbol{b}$
$\Leftrightarrow A = \begin{pmatrix} \boldsymbol{w}_1 & \cdots & \boldsymbol{w}_k \end{pmatrix} \in M_{n\times m}(\mathbb{K}), B = \begin{pmatrix} \boldsymbol{w}'_1 & \cdots & \boldsymbol{w}'_\ell \end{pmatrix} \in M_{n\times \ell}(\mathbb{K})$ に対し, $\begin{pmatrix} A & \boldsymbol{b} \end{pmatrix}$ と $\begin{pmatrix} B & \boldsymbol{b} \end{pmatrix}$ を拡大係数行列とする 2 つの連立一次方程式 $\begin{pmatrix} A & \boldsymbol{b} \end{pmatrix}\hat{\boldsymbol{x}} = \boldsymbol{0}$ (ただし $\hat{\boldsymbol{x}} = \begin{pmatrix} x_1 & \cdots & x_k & -1 \end{pmatrix}^t$, $\hat{\boldsymbol{y}}$ も同様に $\begin{pmatrix} B & \boldsymbol{b} \end{pmatrix}\hat{\boldsymbol{y}} = \boldsymbol{0}$) が解を持つ.

$$\Leftrightarrow \begin{pmatrix} A & O & \boldsymbol{b} \\ O & B & \boldsymbol{b} \end{pmatrix} \text{を拡大係数行列とする連立一次方程式が解を持つ.} \begin{pmatrix} 1 & -1 & 0 & 0 & p \\ 2 & 1 & 0 & 0 & q \\ 0 & 3 & 0 & 0 & r \\ 4 & -3 & 0 & 0 & s \\ 0 & 0 & 0 & -1 & p \\ 0 & 0 & 1 & -9 & q \\ 0 & 0 & -5 & -1 & r \\ 0 & 0 & -2 & -4 & s \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 1 & -1 & 0 & 0 & p \\ 2 & 1 & 0 & 0 & q \\ 0 & 3 & 0 & 0 & r \\ 0 & -5 & 0 & 0 & s-2q \\ 0 & 0 & 0 & -1 & p \\ 0 & 0 & 1 & -9 & q \\ 0 & 0 & -5 & 0 & r-p \\ 0 & 0 & -2 & 0 & -4p+s \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 & 0 & 2/3p - 1/3q + 1/3r \\ 1 & 0 & 0 & 0 & 1/3(p+q) \\ 0 & 1 & 0 & 0 & 1/3r \\ 0 & 0 & 0 & 0 & 5/3r + s - 2q \\ 0 & 0 & 0 & 1 & -p \\ 0 & 0 & 1 & 0 & -9p + q \\ 0 & 0 & 0 & 0 & r - 46p + 5q \\ 0 & 0 & 0 & 0 & -22p + s + 2q \end{pmatrix}.$$

定理 [5.2] より $\begin{cases} 2p - q + r = 0 \\ 5/3r + s - 2q = 0 \\ r - 46p + 5q = 0 \\ -22p + s + 2q = 0 \end{cases}$ を解く. $\hat{A} = \begin{pmatrix} 2 & -1 & 1 & 0 \\ 0 & -2 & 5/3 & 1 \\ -46 & 5 & 1 & 0 \\ -22 & 2 & 0 & 1 \end{pmatrix}\begin{pmatrix} p \\ q \\ r \\ s \end{pmatrix} = 0$ において, これは [9].54 での考察より拡大係数行列$\hat{A}$に左基本変形をしても方程式は同値であるから

$$\hat{A} \rightarrow \begin{pmatrix} 2 & -1 & 1 & 0 \\ -4 & 0 & -1/3 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & -3 & 4 & 0 \end{pmatrix} \text{とし} \begin{cases} 2p - q + r = 0 \\ -4p - 1/3r + s = 0 \\ r - s = 0 \\ -3q + 4r = 0 \end{cases} \text{を解くと } \boldsymbol{b} = \begin{pmatrix} p \\ q \\ r \\ s \end{pmatrix} = r\begin{pmatrix} 1 \\ 8 \\ 6 \\ 6 \end{pmatrix}.$$

問 27. $W_1 = \langle a_1 \rangle, W_2 = \langle a_2, a_3 \rangle, a_1 = \begin{pmatrix} a & 1 & 1 & 1 \end{pmatrix}^t$, $a_2 = \begin{pmatrix} 1 & a & 1 & 1 \end{pmatrix}^t$, $a_3 = \begin{pmatrix} 1 & 1 & a & 1 \end{pmatrix}^t$ と

する. $W_1 \cap W_2$の次元は$a \neq 1$の時$0, a = 1$の時1である. $\because \begin{pmatrix} a & 0 & 0 & p \\ 1 & 0 & 0 & q \\ 1 & 0 & 0 & r \\ 1 & 0 & 0 & s \\ 0 & 1 & 1 & p \\ 0 & a & 1 & q \\ 0 & 1 & 6a & r \\ 0 & 1 & 1 & s \end{pmatrix} \overset{a\neq 1}{\to} \begin{pmatrix} 0 & 0 & 0 & p-qa \\ 1 & 0 & 0 & q \\ 0 & 0 & 0 & r-q \\ 0 & 0 & 0 & s-q \\ 0 & 1 & 1 & p \\ 0 & 0 & 1 & \frac{pa-q}{-1+a} \\ 0 & 1 & 0 & \frac{-p+q}{-1+a} \\ 0 & 0 & 0 & s-p \end{pmatrix} \to$

$\begin{pmatrix} 0 & 0 & 0 & p-qa \\ 1 & 0 & 0 & q \\ 0 & 0 & 0 & r-q \\ 0 & 0 & 0 & s-q \\ 0 & 0 & 0 & p+\frac{pa-q}{1-a}+\frac{-p+q}{1-a} \\ 0 & 0 & 1 & \frac{pa-q}{-1+a} \\ 0 & 1 & 0 & \frac{-p+q}{-1+a} \\ 0 & 0 & 0 & s-p \end{pmatrix}$, 解を持つ条件と$a \neq 1$より$p = q = r = s = 0$. よって

$$W_1 \cap W_2 = \{\mathbf{0}\}$$

解 2. $\begin{pmatrix} 1 & 2 & 1 & 3 \\ 1 & 3 & 2 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0$を満たす$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = x_3 \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} -9 \\ 3 \\ 0 \\ 1 \end{pmatrix}$より$W_1 = \left\langle \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -9 \\ 3 \\ 0 \\ 1 \end{pmatrix} \right\rangle$. 同様に$W_2 = \left\langle \begin{pmatrix} 1 \\ 2 \\ -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ -2 \\ 1 \end{pmatrix} \right\rangle$であり$W_1 + W_2$は上の 4 つのベクトル$\{\boldsymbol{a}_i\}_{1\leq i\leq 4}$で生成される. それらが基底であるかは線形独立の定義即ち$\{\boldsymbol{a}_i\}_i$が線形独立

$$:\Leftrightarrow \boldsymbol{a}_1 x + \boldsymbol{a}_2 y + \boldsymbol{a}_3 z + \boldsymbol{a}_4 w = 0 \text{ なら } x = y = z = w = 0$$

を見る. $\begin{pmatrix} 1 & 0 & 1 & -9 \\ 2 & 5 & -1 & 3 \\ -2 & -2 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 & -9 \\ 3 & 0 & 0 & -11 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$より$\begin{cases} x + z - 9w = 0 \\ 3x - 11w = 0 \\ y + w = 0 \end{cases}$ となるが一次独立でないことが分かる. そこで$\begin{pmatrix} 0 & 1 & -9 \\ 5 & -1 & 3 \\ -2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$を考えるとこの列ベクトルらは線形独立だから次元は 3 である.

解 3. $\boldsymbol{a}_k$をAのk番目の列ベクトルとする. $j_1, ..., j_t \in \{1, ..., m\}$に対し$\boldsymbol{a}_{j_1}, ..., \boldsymbol{a}_{j_t}$を$A$の線型独立な列ベクトルとする. $E_{ij} \in M_{mn}(\mathbb{K})$を$(i, j)$成分が 1 でそれ以外が 0 の行列とする.
すると$X_{ij} = L_A(E_{ij})$はj番目の列ベクトルが$\boldsymbol{a}_i$, それ以外の列ベクトルが$\mathbf{0}$の行列であ

る. $\{X_{ij}\}$ (ただし $i \in \{j_1, ..., j_t\}, j \in \{1, ..., n\}$) は $M_{\ell n}(\mathbb{K})$ において線型独立なので, $\mathrm{rank} L_A = \dim \mathrm{im}(L_A) = n\,\mathrm{rank}(A)$ である. $\mathrm{rank}(A)$ は一般に A の線型独立な列ベクトルの個数に等しいことはよい.

解 4. $A \in M_{\ell m}, B \in M_{mn}$に対し $r(A)+r(B)-m \leq r(AB)$ を示す. $\mathrm{Ker}(A) = \{\boldsymbol{x} \in \mathbb{K}^m; A\boldsymbol{x} = \boldsymbol{0}\}$ とおくと一般に $r(A) = m - \dim(\mathrm{Ker}(A))$ が成り立つ. これより, $r(AB) = \dim(AB[\mathbb{K}^n]) = \dim(B[\mathbb{K}^n]) - \dim(\mathrm{Ker}(A) \cap B[\mathbb{K}^n]) \geq \dim(B[\mathbb{K}^n]) - \dim(\mathrm{Ker}(A)) = r(B)+r(A)-m$. また $r(AB) = \dim(\mathrm{Im}(AB[\mathbb{K}^n])) \leq \dim(\mathrm{Im}(A[\mathbb{K}^m])) = r(A)$ で同様に $r(AB) \leq r(B)$ より $r(AB) \leq \min\{r(A), r(B)\}$ である.

解 5. $A, B \in M_{mn}$に対し $r(A+B) \leq r(A) + r(B)$ が成り立つ. A, B の列ベクトルの極大線型独立系をそれぞれ $\boldsymbol{a}_1, ..., \boldsymbol{a}_r$と $\boldsymbol{b}_1, ..., \boldsymbol{b}_s$とすると $A+B$ の任意の列ベクトルは和空間の定義より $\boldsymbol{a}_1, ...\boldsymbol{a}_r, \boldsymbol{b}_1, ..., \boldsymbol{b}_s$の線型結合でかける. $r(A+B) \geq s+r+1$ 特に $r(A+B) = s+r+1$ と仮定し次の $\boldsymbol{c}_1, ..., \boldsymbol{c}_{s+r+1}$を $A+B$の線型独立な列ベクトルとして $\begin{cases} \boldsymbol{c}_1 = k_1\boldsymbol{a}_1 + \cdots + k_r\boldsymbol{a}_r + k_{r+1}\boldsymbol{b}_1 + \cdots + k_{r+s}\boldsymbol{b}_s \\ \vdots \\ \boldsymbol{c}_{s+r+1} = k'_1\boldsymbol{a}_1 + \cdots + k'_r\boldsymbol{a}_r + k'_{r+1}\boldsymbol{b}_1 + \cdots + k'_{r+s}\boldsymbol{b}_s \end{cases}$ を考えると連立方程式が $s+r+1$ 個あるのに対して解は $r+s$ 個だから $\{\boldsymbol{c}_i\}_{1 \leq i \leq s+r+1}$の線型独立であることに反する. 即ち $r(A+B) \leq s+r = r(A)+r(B)$.

解 6. $m < n$ とし $A \in M_{mn}, B \in M_{nm}$に対し BA は正則でない. $n = \dim(\mathrm{Ker}(A)) + r(A)$ かつ $r(A) \leq m < n$ ($r(A) \leq m$ は行列の階数は線型独立な行ベクトルの本数 = 線型独立な列ベクトルの本数を表すので.) より $\dim(\mathrm{Ker}(A)) > 0$ であり, $\dim(\mathrm{Ker}(A)) \leq \dim(\mathrm{Ker}(BA))$ より $\dim(\mathrm{Ker}(BA)) > 0$ 即ち BA は単射でないので正則でない. 必要条件として B, A が共に正則のとき AB が正則なので $r(A) = r(B) = m$ かつ, もし次が $\boldsymbol{0}$ でない元を持つなら $\mathrm{Ker}(AB) = \{\boldsymbol{0}\}$ に反するので $B[\mathbb{K}^m] \cap \mathrm{Ker}(A) = \{\boldsymbol{0}\}$.

解 7. 任意の線形写像 $T : M_{nn}(\mathbb{K}) \to \mathbb{K}$ はある $A \in M_{nn}(\mathbb{K})$ により, $T(X) = tr(AX)$ とかける. M_{nn}の次元は n^2で基底は (i, j) 成分を 1 としそれ以外を 0 とする $\{E_{ij}\}_{1 \leq i,j \leq n}$である. T は M_{nn} の基底の像により決定され, 後に書く事から $T(E_{ij}) = a_{ji}, A = (a_{ij})$ とすればよい. またこのように定めた A は唯一である. 実際 $A = (a_{ij}), B = (b_{ij}) \in M_{nn}$に対し $tr(AX) = tr(BX)$ とし $X = E_{ij}$のとき $tr(AE_{ij}) = tr\begin{pmatrix} 0 & \cdots & a_{1i} & \cdots & 0 \\ & \cdots & & \cdots & \\ 0 & \cdots & a_{ni} & \cdots & 0 \end{pmatrix} = a_{ji} = b_{ji}$より $A = B$ である.

解 8. $[-\pi, \pi]$ 上の連続関数 $f(x)$ に対し $\|f-g\|^2 = \int |f(x)-g(x)|^2\,dx$ を最小にする有限フーリエ級数 $g(x) = a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx)$ を求める. $I = I(a_0, a_1, ..., a_n, b_1, ..., b_n) = \|f-g\|^2 = \int_{-\pi}^{\pi} |f(x) - (a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx))|^2\,dx$

$$= \int_{-\pi}^{\pi} \left[f(x)^2 - 2f(x)(a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx)) + (a_0 + \sum_{k=1}^n (a_k \cos kx + b_k \sin kx))^2 \right] dx$$

が最小となる必要条件は各変数の偏分が 0 となることである.

$$\frac{\partial I}{\partial a_0} = -2 \int f(x) + 4\pi a_0 + 2 \int (\sum_{k=1}^n (a_k \cos kx + b_k \sin kx)) = 0$$

$\forall n \in \mathbb{Z}$ に対し $\int_{-\pi}^{\pi} \sin nx\, dx = \int_{-\pi}^{\pi} \cos nx\, dx = 0$ より

$$a_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x)\, dx$$

また, $k \in \{1, 2, ..., n\}$ に対し

$$0 = \frac{\partial I}{\partial a_k} = \int \left[-2f(x) \cos kx + 2a_0 \cos kx + 2 \sum_{k=1}^{n} (a_k \cos kx + b_k \sin kx) \cos kx \right] dx$$

において $\forall n, m \in \mathbb{Z}$ に対し $\int_{-\pi}^{\pi} \cos nx \cos mx\, dx = \pi(if\ n = m), 0(if\ n \neq m)$, $\int_{-\pi}^{\pi} \sin nx \cos mx\, dx = 0$ なので

$$2\pi a_k - 2 \int_{-\pi}^{\pi} f(x) \cos kx\, dx = 0 \Leftrightarrow a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos kx$$

また $\int_{-\pi}^{\pi} \sin nx \sin mx\, dx = \pi(if\ n = m), 0(if\ n \neq m)$ より $b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin kx\, dx$ である.

解 9. $f : U \to V$ を線型写像とする. U の基底ベクトルの f で写した先が V の基底ベクトルでどう表されるかをみる. $T(1), T(x), T(x^2)$ は $2x^2 + 2/3, -4/3x, 2/3x^2 + 2/5$ より $T \leftrightarrow \begin{pmatrix} \frac{2}{3} & 0 & \frac{2}{5} \\ 0 & -\frac{4}{3} & 0 \\ 2 & 0 & \frac{2}{3} \end{pmatrix}$ である. また $S(1) = -1, S(f(x)) = S(x) = -x + 1, S(x^2) = -x^2 + 2x$ より $S \leftrightarrow \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & -1 \end{pmatrix}$ である. 任意の線形写像 $f : \mathbb{R}^N \ni \boldsymbol{x} \mapsto f(\boldsymbol{x}) \in \mathbb{R}^M$ に対しある $A \in \mathbb{R}^{M \times N}$ が存在して $f(\boldsymbol{x}) = A\boldsymbol{x}$ を満たすことの具体例である.

$$\begin{pmatrix} T(1) & T(x) & T(x^2) \end{pmatrix} = \begin{pmatrix} \frac{2}{3} + 2x^2 & -\frac{4}{3}x & \frac{2}{5} + \frac{2}{3}x^2 \end{pmatrix} = \begin{pmatrix} 1 & x & x^2 \end{pmatrix} \begin{pmatrix} \frac{2}{3} & 0 & \frac{2}{5} \\ 0 & -\frac{4}{3} & 0 \\ 2 & 0 & \frac{2}{3} \end{pmatrix}$$

$$\begin{pmatrix} S(1) & S(x) & S(x^2) \end{pmatrix} = \begin{pmatrix} 1 & x & x^2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & -1 \end{pmatrix}$$

解 10. (1), (2) 明らかに内積の公理を満たす. 実数係数 n 次以下多項式全体 $P_n(\mathbb{R})$ に $(f, g) = \int_0^{\infty} e^{-x} f(x) g(x) dx$ で内積が定義できることはこの広義積分が収束することをいえればよい. 道草を食うが $(f, f) = 0 \Leftrightarrow 0$ が成り立つかどうかが公理の中では肝心である. $\Leftarrow$ は明らかだが $\Rightarrow$ は自明ではない. 例えば $(f, g) = \int_0^{\infty} e^{x} f(x) g(x)$ とすれば $(f, f) = 0 \Rightarrow f = e^{-\frac{x}{2}} \notin P_n(\mathbb{R})$ となってしまう.
任意の自然数について $\int_0^{\infty} e^{-x} x^m\, dx$ が収束することを示す. $\lim_{x \to \infty} e^{-x} x^{m+2} = 0$ より十分大きい $R > 0$ を取ると $\forall x \in [R, \infty)$ において

$$e^{-x} x^m < \frac{1}{x^2}$$

である. よって

$$\int_R^{R'} e^{-x} x^m\, dx < \int_R^{R'} \frac{1}{x^2}\, dx = -\frac{1}{R'} + \frac{1}{R} < \frac{1}{R'}$$

最左辺は x について単調増加するがそれが $R' \in [R, \infty)$ によらず有界なので広義積分 $\int_R^\infty e^{-x}x^m\,dx$ は収束する.
(3) ラゲール多項式の直交性についての問いである. $L_k(x) = \sum_{i=0}^k (-1)^i{}_kC_i \frac{x^i}{i!}$ は

$$x\frac{d^2}{dx^2}L_k(x) + (1-x)\frac{d}{dx}L_k(x) + kL_k(x) = 0$$

を満たす. ここで $\frac{d}{dx}(e^{-x}x\frac{d}{dx}L_k(x)) = e^{-x}(x\frac{d^2}{dx^2}L_k(x)+(1-x)\frac{d}{dx}L_k(x))$ より, $e^x\frac{d}{dx}(e^{-x}x\frac{d}{dx}L_k(x)) = -kL_k(x)$ 即ち $\frac{d}{dx}(xe^{-x}\frac{d}{dx}L_k(x)) + e^{-x}kL_k(x) = 0$. よって

$$L_\ell(x)\frac{d}{dx}(xe^{-x}\frac{d}{dx}L_k(x)) + L_\ell(x)e^{-x}kL_k(x) = 0$$

$$L_k(x)\frac{d}{dx}(xe^{-x}\frac{d}{dx}L_\ell(x)) + L_k(x)e^{-x}\ell L_\ell(x) = 0$$

よって

$$\int_0^\infty L_\ell(x)\frac{d}{dx}(xe^{-x}\frac{d}{dx}L_k(x)) - \int_0^\infty L_k(x)\frac{d}{dx}(xe^{-x}\frac{d}{dx}L_\ell(x)) + (k-\ell)\int_0^\infty e^{-x}L_k(x)L_\ell(x)\,dx = 0$$

部分積分を行うことで, $L_k(x) = \sum_{i=0}^k (-1)^i{}_kC_i\frac{x^i}{i!}$ の表示は得ているとして $\frac{(x\text{ の有限次多項式})}{e^x} \to 0 (x \to \infty)$ より $k \neq \ell$ ならば上記の内積のもと,

$$(L_k(x), L_\ell(x)) = 0$$

となる. 次に $\int_0^\infty e^{-x}L_k(x)L_k(x)dx$ の計算をする. $L_k(x)$ の母関数は $g(t,x) = \sum_{k=0}^\infty t^kL_k(x) = \frac{1}{1-t}e^{-\frac{xt}{1-t}}, g(s,x) = \sum_{\ell=0}^\infty s^\ell L_\ell(x) = \frac{1}{1-s}e^{-\frac{xs}{1-s}}$ を満たす. すると

$$\int_0^\infty g(t,x)g(s,x)e^{-x}dx = \sum_{k=0}^\infty\sum_{\ell=0}^\infty t^ks^\ell\int_0^\infty L_k(x)L_\ell(x)e^{-x}dx$$

(左辺) $= \int_0^\infty \frac{1}{(1-t)(1-s)}e^{-(\frac{t}{1-t}+\frac{s}{1-s}+1)x}\,dx = \frac{1}{(1-t)(1-s)}\int_0^\infty e^{\frac{ts-1}{(1-t)(1-s)}x}dx = \frac{1}{1-ts}$. ここで $f(z) = \frac{1}{1-z}$ を考えると $f(z) = f(0)+f'(0)z+\frac{f''(0)}{2!}z^2+... = 1+z+z^2+z^3+...$ より $\frac{1}{1-ts} = 1+ts+(ts)^2+... = \sum_{n=0}^\infty t^ns^n$ である. 即ち

$$\int_0^\infty g(t,x)g(s,x)e^{-x}dx = \sum_{n=0}^\infty t^ns^n$$

右辺は又

$$\sum_{k=0}^\infty\sum_{\ell=0}^\infty t^ks^\ell\int_0^\infty L_k(x)L_\ell(x)e^{-x}dx \overset{n=k=\ell\text{のとき}}{=} \sum_{n=0}^\infty t^ns^n(L_n(x), L_n(x))$$

よって

$$(L_n(x), L_n(x)) = 1$$

が成り立つ.

解 11. $A = \begin{pmatrix} \boldsymbol{a}_1 & \cdots & \boldsymbol{a}_n \end{pmatrix} \in GL_n(\mathbb{R})$ とすると $\boldsymbol{a}_1, ..., \boldsymbol{a}_n$ は基底なので正規直交基底 $\boldsymbol{u}_1, ..., \boldsymbol{u}_n$ を各 $k(1 \leq k \leq n)$ に対し $\langle \boldsymbol{a}_1, ..., \boldsymbol{a}_k \rangle = \langle \boldsymbol{u}_1, ..., \boldsymbol{u}_k \rangle$ となるように取れるから $\boldsymbol{a}_k = t_{k,1}\boldsymbol{u}_1 + t_{k,2}\boldsymbol{u}_2 + \cdots + t_{k,k}\boldsymbol{u}_k$ と表せる. $\boldsymbol{t}_k = \begin{pmatrix} t_{k,1} \\ t_{k,2} \\ \vdots \\ t_{k,k} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$ とおくと基底の変換行列 $\boldsymbol{t} = \begin{pmatrix} \boldsymbol{t}_1 & \cdots & \boldsymbol{t}_n \end{pmatrix}$ は上三角行列. 正規直交列ベクトルがなす $\begin{pmatrix} \boldsymbol{u}_1 & \cdots & \boldsymbol{u}_n \end{pmatrix}$ は直交行列であり $A = UT$.

解 12. (イ) 任意の $\upsilon = \sum_{j=1}^n a_j e_j \in V$ に対し $f_i(e_i) = \delta_{ij}$ より $f_i(\upsilon) = \sum_{j=1}^n a_j f_i(e_j) = a_i$. 勝手な $f \in V^*$ に対して $f(e_i) = b_i \in \mathbb{R}(1 \leq i \leq n)$ とすると $\upsilon = \sum_{i=1}^n a_i e_i \in V$ について $f(\upsilon) = \sum_{i=1}^n a_i f(e_i) = \sum_{i=1}^n a_i b_i$ である. $g = \sum_{i=1}^n b_i f_i \in V^*$ とすると $g(\upsilon) = \sum_{i=1}^n b_i f_i(\upsilon) = \sum_{i=1}^n a_i b_i = f(\upsilon)$. υ は任意だったから $f = g = \sum_{i=1}^n b_i f_i$. また $f \in V^*$ は任意だったから V^* は $f_1, ..., f_n$ を生成系とすることがわかる. そこで $\sum_{i=1}^n b_i f_i = 0$ とすると $0 = (\sum_{i=1}^n b_i f_i)(\sum_{j=1}^n a_j e_j) = (b_1 f_1 + \cdots + b_n f_n)(a_1 e_1 + \cdots + a_n e_n)$, $f_i(e_j) = \delta_{ij}$ の定義より $\sum_{i=1}^n b_i a_i = 0$. 任意の $\upsilon \in V$ に対し成り立つので特に $e_i(1 \leq i \leq n)$ とすることで, $(b_1 f_1 + \cdots + b_n f_n)e_i = b_i = 0$. 即ち $(f_i)_i$ は V^* の基底.

(ロ) $a \in \mathbb{K}^n = M_{n1}(\mathbb{K})$ に対する $a^t \in M_{1n}(\mathbb{K})$ 倍写像を $f_a : \mathbb{K}^n \to \mathbb{K}$ とかくと写像 $\mathbb{K}^n \to (\mathbb{K}^n)^*; a \mapsto f_a$ は同型である. n 次元線型空間 V の基底が定まることと同型 $\mathbb{K}^n \to V$ が定まることは等しいので $g_E : \mathbb{K}^n \to V, g_F : \mathbb{K}^m \to W$, $g_{E^*} : \mathbb{K}^n \to V^*, g_{F^*} : \mathbb{K}^m \to W^*$ をそれぞれ基底 E, F と双対基底 E^*, F^* が定める同型とする. $h : \mathbb{K}^n \to (\mathbb{K}^n)^*$ と $h' : \mathbb{K}^m \to (\mathbb{K}^m)^*$ を $a \mapsto f_a$ で定めたような同型写像とする. $h' = (g_F)^* \circ g_{F^*}, h = (g_E)^* \circ g_{E^*}$: (注) であり

$$\begin{array}{ccc} W^* & \xrightarrow{f^*} & V^* \\ {\scriptstyle (g_F)^*}\downarrow & & \downarrow{\scriptstyle (g_E)^*} \\ (K^m)^* & \xrightarrow[f_{A^*}]{} & (K^n)^* \\ \uparrow{\scriptstyle h'} & & \uparrow{\scriptstyle h} \\ K^m & \xrightarrow[f_{A^t}]{} & K^n \end{array} \tag{2.1}$$

は可換図式であるので帰結を得る.

(注) : $\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = a \in \mathbb{K}^m$ を勝手にとったとき

$$h'(a) = g_F^* \circ g_{F^*}(a)$$

が成り立つ. なぜなら左辺は a^t 倍写像 f_{a^t}. 右辺は $g_F^*(a_1 f_1^* + \cdots + a_m f_m^*) = a_1 g_F^*(f_1^*) + \cdots a_m g_F^*(f_m^*) =$

$a_1 f_{(1\cdots 0)} + \cdots a_m f_{(0\cdots 1)} = f_{\boldsymbol{a}_1{}^t} + \cdots + f_{\boldsymbol{a}_m{}^t}$(ただし, $\boldsymbol{a}_i = \begin{pmatrix} 0 \\ \vdots \\ a_i \\ \vdots \\ 0 \end{pmatrix}$) であるからである. 次に, 可換図式における上部方形の中の可換性を示す必要がある. まず, 一般に線型写像 $f : V \to W, g : W \to U$ に対して $(g \circ f)^* = f^* \circ g^*$という補題を認めよ. さて $f : V \to W$ を同様の写像とし次が成り立つことを示せば補題の適用より上部方形の中の可換性が示される.

$$f \circ g_E \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = g_F \circ f_A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

左辺は

$$f(c_1 e_1 + \cdots c_n e_n) = c_1 f(e_1) + \cdots + c_n f(e_n)$$

である. 右辺は

$$g_F \left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \right) = g_F \left(\begin{pmatrix} a_{11}c_1 + \cdots + a_{1n}c_n \\ \vdots \\ a_{m1}c_1 + \cdots + a_{mn}c_n \end{pmatrix} \right) = (a_{11}c_1 + \cdots + a_{1n}c_n) f_1 + \cdots + (a_{m1}c_1 + \cdots + a_{mn}c_n) f_m$$

である. 表現行列の定義である

$$\begin{pmatrix} f(e_1) & \cdots & f(e_n) \end{pmatrix} = \begin{pmatrix} f_1 & \cdots & f_m \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

より左辺と右辺は一致する. 最後に下部方形の可換性を確かめるため, $b \in \mathbb{K}^n$に対する線型形式 $(f_A)^*(h'(a))(b) = h(f_{A^t}(a))(b) \in \mathbb{K}$ を示す. 左辺は $h'(a)(f_A b) = f_{a^t}(f_A b) = f_{a^t A} b$ であり, 右辺は $n \times 1$ 行列 $A^t a$ に h が作用して $(A^t a)^t$倍写像となりそれが b に作用して $\mathbb{K}$ の元となるので, $f_{a^t A} b$ である.

(ハ) 任意の $x \in V$ に対し $x' : V^* \ni f \mapsto f(x) \in \mathbb{K}$. $\tau : V \ni x \mapsto x' \in V^{**}$は単射線型である. τが線型であること即ち $x, y \in V, a \in \mathbb{K}$ としたとき$\tau(x + y) = \tau(x) + \tau(y)$ と$\tau(ax) = a\tau(x)$ を示す. $\forall f \in V^*$に対し $(x + y)'(f) = (x' + y')(f)$ を言えば良い. 左辺は $f(x + y)$ である. 右辺は $(x' + y')(f) = x'(f) + y'(f) = f(x) + f(y) = f(x + y)$. また $(ax)'(f) = f(ax) = af(x) = (ax')(f)$ である. よってτは線型. 次に$\tau : V \ni x \mapsto x' \in V^{**}$は単射であることを示すために $\mathrm{Ker}(\tau) = \{0\}$ を言う. 勝手な $0 \neq x \in \mathrm{Ker}(\tau)$ を取る. $f \in V^*$で $f(x) = 1$ となるものがあるが $f(x) = x'(f) = (\tau(x))(f) = 0$ より矛盾. よって $\mathrm{Ker}(\tau) = \{0\}$ よりτは単射.

全射性を示す. τの単射性より $x \in V$ と$\tau(x) \in V^{**}$を同一視して $V = \tau(V) \subset V^{**}$とみなすこととする. V が有限次元のとき $\dim(V) = \dim(V^*) = \dim(V^{**})$ より $V \cong V^{**}$.

解 13. (イ)$[x_1] = [y_1], [x_2] = [y_2]$ のとき $(x_1 + x_2) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2) \in W$ より $[x_1 + x_2] = [y_1 + y_2]$ より V/W 上の和の演算は良定義であり $cx_1 - cy_1 = c(x_1 - y_1) \in W$ よ

り $[cx_1]=[cy_1]$ よりスカラー倍の演算も代表元の取り方に依らず良定義. この二つの演算で線型空間となることは明らか. 明らかに $\forall[x_1],[x_2]\in V/W$ に対し $[c_1x_1+c_2x_2]=c_1[x_1]+c_2[x_2]$ となる. (ロ)$\forall[x]\in V/W$ に対し $[x]=(c_1e_1+\cdots+c_ne_n)+W=(c_{r+1}e_{r+1}+\cdots+c_ne_n)+W=c_{r+1}(e_{r+1}+W)+\cdots+c_n(e_n+W)$. $\sum_{i=r+1}^{n}c_i(e_i+W)=\sum_{i=r+1}^{n}d_i(e_i+W)$ とすると $\sum_{i=r+1}^{n}(c_i-d_i)e_i\in W$ より $c_{r+1}=d_{r+1}=0,...,c_n=d_n=0$ で一意的に表せる. よって $\langle e_{r+1}+W,...,e_n+W\rangle$ は V/W の基底で $i\in\{r+1,...,n\};e_i+W=[e_i]$. (ハ) まず, $(*)\forall w\in W;\hat{T}(x+W)=\hat{T}(x+w+W)\Leftrightarrow[Tx]=[T(x+w)]$ を示す. $[T(x+w)]\overset{T\text{は線型}}{=}[T(x)+T(w)]\overset{T(W)\subset W}{=}[Tx]$. 次に$\hat{T}$が線型であることを示す. $\hat{T}([x]+[y])=\hat{T}((x+W)+(y+W))\overset{(*)}{=}\hat{T}((x+y)+W)=[T(x+y)]=T(x+y)+W=T(x)+W+T(y)+W=\hat{T}[x]+\hat{T}[y]$. 次に良定義であることを示す. つまり $[x_1]=[y_1],[x_2]=[y_2]$ のとき$\hat{T}[x_1+x_2]=\hat{T}[y_1+y_2],\hat{T}[cx_1]=\hat{T}[cy_1]$ であるかどうかである. $[T(x_1+x_2)]=[T(x_1)]+[T(x_2)]$. $T(x_1)+W=T(y_1)+W\Leftrightarrow T(x_1-y_1)\in W$ を言えればよいが, $x_1-y_1\in W$ と T 不変より $T(x_1-y_1)\in W$. また $[T(cx_1)]=[T(cy_1)]$ も明らか.

(ニ)$\begin{pmatrix}T(e_1)&\cdots&T(e_n)\end{pmatrix}=\begin{pmatrix}e_1&\cdots&e_n\end{pmatrix}\begin{pmatrix}x_{11}&&\\&\ddots&\\&&x_{nn}\end{pmatrix}$ における (x_{ij}) を T の基底 $e_1,...,e_n$に関する表現行列といった. $V\cong W\oplus V/W$ であり $W,V/W$ は共に T 不変なので命題の主張が成り立つ. なぜなら $T_W(W)\subset W$ より $\begin{pmatrix}e_1&\cdots&e_n\end{pmatrix}\begin{pmatrix}x_{11}\\\vdots\\x_{n1}\end{pmatrix},...,\begin{pmatrix}e_1&\cdots&e_n\end{pmatrix}\begin{pmatrix}x_{1r}\\\vdots\\x_{nr}\end{pmatrix}\in\mathrm{span}(e_1,...,e_r)$ ゆえに $x_{ij}=0(r+1\le i\le n,1\le j\le r)$. よって $j\in\{1,...,r\}$ に対し $T_W(e_j)=\sum_{i=1}^{r}x_{ij}e_i$より, T の E に関する表現行列における $(x_{ij})_{1\le i,j\le r}=A_0$である. 同様に$\hat{T}(V/W)\subset V/W$ より $\begin{pmatrix}[e_1]&\cdots&[e_n]\end{pmatrix}\begin{pmatrix}x_{11}\\\vdots\\x_{n1}\end{pmatrix},...,\begin{pmatrix}[e_1]&\cdots&[e_n]\end{pmatrix}\begin{pmatrix}x_{1,n-r}\\\vdots\\x_{n,n-r}\end{pmatrix}\in\mathrm{span}([e_{r+1}],...,[e_n])$ なので $j\in\{r+1,...,n\}$ に対し $T_{V/W}([e_j])=\sum_{i=r+1}^{n}x_{ij}[e_i]$. よって $(x_{ij})_{r+1\le i,j\le n}=\tilde{A}$である.

2.2 速修線形代数学

ベクトルないし線型空間の元を太文字表記にすることは今後特にない. $\mathbb{R}$ と $\mathbb{C}$ を統一的に $\mathbb{K}$ で表し特に指定しない限りは V は $\mathbb{K}$ 上の線型空間とする.

定義 31. $a_1, ..., a_k \in V$ が V を生成する (generate) 又は張る (span) とは

$$\forall x \in V\ \exists \lambda_1, ..., \lambda_k \in \mathbb{K}\ s.t.\ x = \sum_{i=1}^{k} \lambda_i a_i \Leftrightarrow V = \{\sum_{i=1}^{k} \lambda_i a_i | \lambda_1, ..., \lambda_k \in \mathbb{K}\}$$

このとき $V = \langle a_1, ..., a_k \rangle$ とかく.

定義 32. $e_1, ..., e_n \in V$ が V の基底 (basis, base) であるとは $e_1, ..., e_n$ が線型独立であってそれらが V を生成することである. 例えば $\mathbb{K}[x] \ni P(X) = a_m X^m + ... + a_1 x + a_0$ の基底は $1, X, ..., X^m$ である. $E = \langle e_1, ..., e_n \rangle$ を V の基底としたとき V は $\mathbb{K}^n$ に線型同型である.

なぜなら $\varphi_E : V \ni x = \sum_{i=1}^{n} x_i e_i \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ とすれば φ は以下のように同型だからである.

$a, b \in \mathbb{K}, y = \sum_{i=1}^{n} y_i e_i$ を V の任意の元とすると

$$\varphi(ax + by) = \begin{pmatrix} ax_1 + by_1 \\ \vdots \\ ax_n + by_n \end{pmatrix} = a\varphi(x) + b\varphi(y)$$

単射性を示すため $\mathrm{Ker}(\varphi) = \{0\}$ をいう. $0 = \varphi(x)$ なる x を考えると $x_1, ..., x_n = 0$ より $x = 0$ よりいえた. 全射性は, 任意の $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$ に対してある $x := \sum_{i=1}^{n} x_i e_i \in V$ が存在するのでいえた.

命題 44. 次の内容を基底の延長定理と呼ぶことにする. V を線型空間とし $e_1, ..., e_r \in V$ が独立ならば $\langle e_1, ..., e_r, e_{r+1}, ..., e_n \rangle$ が V の基底となるような $e_{r+1}, ..., e_n \in V$ が存在する.

定義 33. V の基底が含むベクトルの数 n を V の次元といい $\dim V = n$ とかく. 基底の取り方に n はよらない.

命題 45. [9], 103, 定理 [3.9] $V \cong \mathbb{K}^n$ において n 個より多くの元全体は線型従属である.

証明. $a_1, ..., a_m \in \mathbb{K}^n$ $(m > n)$ に対して $A := \begin{pmatrix} a_1 & \cdots & a_m \end{pmatrix} \in M_{nm}$ とおく. $m > n$ なので
第 2 章, [5.6] より $A\boldsymbol{x} = 0$ が非自明な解 $\boldsymbol{x}' \neq \boldsymbol{0}$(なお自明な解とは $\boldsymbol{x} = \boldsymbol{0}$ のこと) があることがわかる. もし A^{-1} が存在すれば $\boldsymbol{x}' = \boldsymbol{0}$ となり矛盾するので $a_1, ..., a_m$ は線型従属である. 証明終. なお, 対偶を取ると $a_1, ..., a_m$ が独立ならば $m \leq n$ である. □

定義 34 (基底の変換行列)**.** $E = \langle e_1, ..., e_n \rangle$ と $F = \langle f_1, ..., f_n \rangle$ を V の基底とする. このとき任意の $a \in V$ はある x_i そして $y_j (1 \leq i, j \leq n)$ が存在して $a = \sum_{i=1}^{n} x_i e_i = \sum_{j=1}^{n} y_j f_j$ とかける. す

るとある n 次正則行列 $P=(p_{ij})$ が存在して, $\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=P\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$ となる. この行列 P を基底の変換 $E\to F$ の行列という. P が存在する理由は, $\varphi\circ\psi^{-1}:\mathbb{K}^n\to\mathbb{K}^n$が線型写像であり, 任意の線型写像は行列 (この場合 n 次正則行列) で表せるからである.

$$\begin{pmatrix}e_1 & \cdots & e_n\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\sum_{i=1}^{n}x_ie_i=\sum_{j=1}^{n}y_jf_j=\begin{pmatrix}f_1 & \cdots & f_n\end{pmatrix}\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$$

より

$$\begin{pmatrix}e_1 & \cdots & e_n\end{pmatrix}\begin{pmatrix}p_{11} & \cdots & p_{1n}\\ & \ddots & \\ p_{n1} & \cdots & p_{nn}\end{pmatrix}=\begin{pmatrix}f_1 & \cdots & f_n\end{pmatrix}\Leftrightarrow f_j=\sum_{i=1}^{n}p_{ij}e_i\ (1\le j\le n)$$

逆に, V の基底 E と n 次正則行列 $P=(p_{ij})$ に対し $f_j(1\le j\le n)$ をこのように定めると $\langle f_1,...,f_n\rangle$ は V の基底である.

例 4. $\mathbb{K}^n$の単位ベクトルを並べた基底を $E_0=\langle e_1,...,e_n\rangle$ とかく. また異なる基底 $F=\langle p_1,...,p_n\rangle$ に対して $E_0\to F$ の行列は上の関係式より $P=\begin{pmatrix}p_1 & \cdots & p_n\end{pmatrix}$である.

命題 46.

$$\boldsymbol{p}_1,...,\boldsymbol{p}_n\in\mathbb{K}^n\text{は線型独立}\Leftrightarrow\begin{pmatrix}\boldsymbol{p}_1 & \cdots & \boldsymbol{p}_n\end{pmatrix}\text{は正則行列}$$

命題 47. 線型写像 $T:V\to\mathrm{Im}(T)$ に対して $V/\mathrm{Ker}(T)\cong\mathrm{Im}(T)$ が成り立つ.

$$0\to\mathrm{Ker}(T)\to V\to\mathrm{Im}(T)\to 0$$

は完全 (exact) であるという. 一般に $f_i:V_i\to V_{i+1}$を $\mathbb{K}$ 上の線型写像とし任意の i に対して $\mathrm{Im}(f_i)\subset\mathrm{Ker}(f_{i+1})\Leftrightarrow f_{i+1}\circ f_i=0$ が成り立つとき

$$V_*:V_1\overset{f_1}{\to}V_2\overset{f_2}{\to}V_3\to\cdots$$

を複体 (complex) といい V_*は完全であると呼ぶ. 複体 V_*について $H^i(V_*)=\mathrm{Ker}(f_i)/\mathrm{Im}(f_{i-1})$ を V_* の i 番目のコホモロジーという.

例 5. $W_1,W_2\subset V$ を部分空間とするとき $W_1+W_2\cong W_1\oplus W_2/W_1\cap W_2$である. $W_1\oplus W_2$は自然な埋め込み (canonical imbedding) によって $V\oplus V$ の部分空間とみなしている.

証明. $r:=\dim(W_1\cap W_2)$ とおき $\dim W_1=r+s,\dim W_2=r+t$ とする. 即ち $\dim(W_1\oplus W_2)=2r+s+t$ で

$\langle a_1,...,a_r\rangle$ を $W_1\cap W_2$の基底, $\langle a_1,...,a_r,b_1,...,b_s\rangle$ を W_1の基底, $\langle a_1,...,a_r,c_1,...,c_t\rangle$ を W_2の基底

とする. ただし, 各 b_jと c_kは互いに従属であるとし, 基底の延長定理を使った.
$E:\langle a_1,...,a_r,b_1,...,b_s,c_1,...,c_t\rangle$ は W_1+W_2の基底であることを示す. $\forall x\in W_1,\forall y\in W_2$に対

し, $x = \sum_{i=1}^{r} \alpha_i a_i + \sum_{j=1}^{s} \beta_j b_j$及び$y = \sum_{i=1}^{r} \alpha'_i a_i + \sum_{k=1}^{t} \gamma_k c_k$とかけ, $W_1 + W_2$の任意の元は定義より $x + y$ の形にかける. そして $x + y = \sum(\alpha + \alpha')a_i + \sum \beta_j b_j + \sum \gamma_k c_k$は E が $W_1 + W_2$の生成系であることを意味する. 線型独立であることを示すためには

$$\sum \alpha_i ai + \sum \beta_j b_j + \sum \gamma_k c_k = 0 \Rightarrow \alpha_i = \beta_j = \gamma_k = 0$$

をいえばよい.

$$W_1 \ni \sum \alpha_i a_i + \sum \beta_j b_j = -\sum \gamma_k c_k \in W_2$$

より上のベクトルはどちらも $W_1 \cap W_2$の元である. $\langle a_1, ..., a_r \rangle$ は $W_1 \cap W_2$の基底だったので$\sum \beta_j b_j = 0$であり$\langle b_1, ..., b_s \rangle$は一次独立であるように取ったので$\forall j; \beta_j = 0$である. よって

$$W_1 \cap W_2 \ni \sum \alpha_i a_i = -\sum \gamma_k c_k \in W_1$$

より $\forall k; \gamma_k = 0$ である. 最後に, $\langle a_1, ..., a_r \rangle$ の一次独立性から $\forall i; \alpha_i = 0$ がわかる.
まず, $W_1 \cap W_2 \hookrightarrow W_1 \oplus W_2; x \mapsto (x, x)$ を定める. また $W_1 \oplus W_2 \xrightarrow{T} W_1 + W_2; x \oplus y = (x, y) \mapsto x - y$ を定めるとこれは明らかに全射である.

$$\mathrm{Ker}(T) = \{x \oplus y |\ x - y = 0, x \in W_1, y \in W_2\} = \{x \oplus x \in W_1 \cap W_2\} \cong \{x \in W_1 \cap W_2\} = W_1 \cap W_2$$

準同型定理より, $W_1 \oplus W_2 / W_1 \cap W_2 \cong W_1 + W_2$が成り立つ. □

定義 35 (表現行列)**.** $T : V \to V'$を線型写像とし $E = \langle e_1, ..., e_n \rangle$ を V の基底, $E' = \langle e'_1, ..., e'_m \rangle$ を V' の基底とする.

$$\begin{array}{ccc} x = \sum_{j=1}^{n} x_j e_j \in V & \xrightarrow{T} & V' \ni Tx = \sum_{i=1}^{m} y_i e'_i \\ \downarrow{\scriptstyle \varphi_E} & \circlearrowright & \downarrow{\scriptstyle \varphi_{E'}} \\ (x_1 \ \cdots \ x_n)^t \in \mathbb{K}^n & \xrightarrow[T_A]{} & \mathbb{K}^m \ni (y_1 \ \cdots \ y_m)^t \end{array} \tag{2.2}$$

が可換となるように正則行列 $A = (a_{ij}) \in M_{mn}$を定める. そのような A を T の表現行列という. 図式より A は基底の取り方に依存することがわかる. また V と V'の両方で基底の取り替えを行ったときに行列はどのような関係式を満たすかについても重要である.
V の基底 $F = \langle f_1, ..., f_n \rangle$ と V'の基底 $F' = \langle f'_1, ..., f'_m \rangle$ についても新たにそれぞれ$\varphi_F : V \to \mathbb{K}^n, \varphi_{F'} : V \to \mathbb{K}^m$によって定め, V と V'で基底の変換 $E \to F$ と $E' \to F'$を行いそれらの正則行列を P, Q とする. 即ち

$$f_k = \sum_{j=1}^{n} p_{jk} e_j,\ f'_\ell = \sum_{i=1}^{m} q_{i\ell} e'_i$$

$T : V \to V'$の E, E’ に関する表現行列を A とし F, F'に関する表現行列を B とする. このとき

$$B = Q^{-1} A P$$

が成り立つ. $\boldsymbol{x} = \sum_{j=1}^{n} x_j \boldsymbol{e}_j \in V,\ T\boldsymbol{x} = \sum_{i=1}^{m} y_i \boldsymbol{e}'_i \in V'$ に対して

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \varphi_{E'} \circ T(\boldsymbol{x}) = T_A \varphi_E(\boldsymbol{x}) = \begin{pmatrix} \boldsymbol{a}_1 & \cdots & \boldsymbol{a}_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

を満たすような$\begin{pmatrix}\boldsymbol{a}_1 & \cdots & \boldsymbol{a}_n\end{pmatrix}$を$T$の行列$(a_{ij})$といった. そして以下の関係式が重要である.

$$Te_j = \sum_{i=1}^{m} a_{ij}e'_i \tag{2.3}$$

ではこれを導いてみる. ϵ_jをj番目の成分が1の単位ベクトル$\epsilon_j := \begin{pmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{pmatrix}$で定義される$\mathbb{K}^n$の元とする. また同じく$\epsilon'_i := \begin{pmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{pmatrix} \in \mathbb{K}^m$と定義する. 明らかに$\varphi_E^{-1}(\epsilon_j) = e_j$が成り立つ.
そして図式の可換性によって

$$A\epsilon_j = \underbrace{\begin{pmatrix}a_{1j}\\ \vdots\\ a_{mj}\end{pmatrix}}_{\boldsymbol{a}_j\text{つまり }A\text{ の第 }j\text{ 列}} = \varphi_{E'} \circ Te_j$$

である. そこで$Te_j = \varphi_{E'}^{-1}(\boldsymbol{a}_j) =: \sum_{i=1}^{m} y_i e'_i$とおく(1)と (これは, Vの各基底ベクトルを写した先ではどのような一次結合で表せるのかを定めたということ)

$$\boldsymbol{a}_j = \varphi_{E'}(\sum_{i=1}^{m} y_i e'_i) = \sum_{i=1}^{m} y_i \varphi_{E'}(e'_i) = \sum_{i=1}^{m} y_i \epsilon'_i = \begin{pmatrix}y_1\\ \vdots\\ y_m\end{pmatrix}$$

と(2)なる. (1), (2) より (2.3) の関係式が成り立つことは明らか.

命題 48 (116 ページ,[5.1])**.** 補足を行う. V, V'をn次元, m次元線型空間とする. $V \xrightarrow{T} \mathrm{Im}(T) \hookrightarrow V'$と思うことにする. すると基底の延長定理により $\mathrm{Im}(T)$ の基底 $\langle e'_1, ..., e'_r\rangle$ に対し V'の基底 $E' : \langle e'_1, ..., e'_r, \exists e'_{r+1}, ..., \exists e'_m\rangle$ とする. $V \to \mathrm{Im}(T)$ は全射であるので任意の $e'_i (1 \le i \le r)$ に対しある e_iがあって, $Te_i = e'_i$が成り立つことに注意.
主張 1) $e_1, ..., e_r$が線型独立である.
$\sum_{i=1}^{r} x_i e_i = 0$ としこれを示す. $0 = T0 = T(\sum_{i=1}^{r} x_i e_i) \overset{T\text{ は線型}}{=} \sum x_i Te_i = \sum_{i=1}^{r} x_i e'_i$であり $\langle e'_1, ..., e'_r\rangle$ は独立系だから $x_i = 0\ (1 \le i \le r)$ である. 次元定理より $\dim \mathrm{Ker}(T) = n - r$ であり $\mathrm{Ker}(T)$ の基底 $\langle e_{r+1}, ..., e_n\rangle$ をとる.(*)
主張 2) $E := \langle e_1, ..., e_r, e_{r+1}, ..., e_n\rangle$ は V の基底をなす.
これを示すため $\sum_{i=1}^{n} x_i e_i$とする.

$$0 = T0 = T(\sum_{i=1}^{r} x_i e_i + \sum_{i=r+1}^{n} x_i e_i) = \sum_{i=1}^{r} x_i Te_i + T(\sum_{i=r+1}^{n} x_i e_i) \overset{(*)}{=} \sum_{i=1}^{r} x_i e'_i$$

であり, よって一次独立性から

$$x_1 = \cdots = x_r = 0$$

である. よってもとの式は $\sum_{i=r+1}^{n} x_i e_i$ となるが $x_{r+1} = \cdots = x_n = 0$ もわかる.

主張 3) さて, 線型写像 T の E, E' に関する行列は標準形 $\begin{pmatrix} E_r & O \\ O & O \end{pmatrix} \in M_{mn}$ である.

証明.

$$\begin{array}{ccccc} V & \xrightarrow{T} & \mathrm{Im}(T) & \hookrightarrow & V' \\ \downarrow{\scriptstyle \varphi_E} & \circlearrowright & \downarrow{\scriptstyle \varphi_{E'}} & & \\ \mathbb{K}^n & \xrightarrow[A|_{\langle e'_1,\ldots,e'_r\rangle}]{} & \mathbb{K}^r & \hookrightarrow \begin{pmatrix} E_r \\ O_{m-r} \end{pmatrix} & \mathbb{K}^m \end{array} \tag{2.4}$$

(2.3) より $Te_j = \sum_{i=1}^{m} a_{ij} e'_j$ である. よって

$$1 \le j \le r \text{ に対しては } e'_j = Te_j = \sum_{i=1}^{m} a_{ij} e'_j \text{ より } a_{ij} = \delta_{ij}$$

$$r+1 \le j \le n \text{ に対しては } 0 = Te_j = \sum_{i=1}^{m} a_{ij} e'_i \text{ より } a_{ij} = 0$$

□

定義 36. 線型写像 T に対し $\mathrm{rank}(T) := \dim \mathrm{Im}(T)$ と定める.

命題 49 (116 ページ,[5.2])**.** V, V' の基底 E, E' に関する $T : V \to V'$ の行列を A とすると $\mathrm{rank}(T) = \mathrm{rank}(A)$ が成り立つ.

証明. 表現行列が標準形となるような, V, V' の特別な基底 F, F' に関するものを $B := \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$ とすると, これについては明らかに成立. 一方, 基底の変換 $E \to F, E' \to F'$ の行列を P, Q として $B = Q^{-1}AP$ であるが一般の表現行列 A についても $\mathrm{rank}(A) = \mathrm{rank}(B) = r$ より良い. □

命題 50 (121 ページ,[6.1])**.** 任意の $x, y \in V$ に対し $|(x, y)| \le \|x\| \, \|y\|$ が成り立つ.

証明. $y = \mathbf{0}$ なら明らかなので $y \neq \mathbf{0}$ とする. 勝手に $\lambda \in \mathbb{K}$ をとる.

$$\begin{aligned} 0 \le \|x + \lambda y\|^2 & \\ &= (x + \lambda y, x + \lambda y) = (x, x) + \lambda(y, x) + \overline{\lambda}(x, y) + \lambda\overline{\lambda}(y, y) \\ &= \|x\|^2 + \lambda\overline{(x, y)} + \overline{\lambda}(x, y) + |\lambda|^2\|y\|^2 \\ &= \|x\|^2 + 2Re(\lambda\overline{(x, y)}) + |\lambda|^2\|y\|^2 \end{aligned}$$

任意の λ に対してこれが成り立つので特に $\lambda = -\frac{(x,y)}{\|y\|^2}$ とすると, $0 \le \|x\|^2 - \frac{|(x,y)|^2}{\|y\|^2}$ を得る. □

注 20. 前命題より, $V \times V \ni (x,y) \mapsto (x,y) \in \mathbb{C}$ は連続である. なぜなら n を十分大きくすると $x_n \to x \in V$ すなわち $\|x_n - x\| \to 0$ ならば

$$|(x_n, y) - (x, y)| = |(x_n - x, y)| \leq \|x_n - x\| \, \|y\| \to 0$$

定義 37. $\boldsymbol{e}_1, ..., \boldsymbol{e}_r \in V$ は $(\boldsymbol{e}_i, \boldsymbol{e}_j) = \delta_{ij}$のときに正規直交系 (ONS) といい, さらに V の基底であるときに正規直交基底 (ONB) という.

命題 51 (Schmidt の直交化法)**.** $e_1, .., e_r$が V の正規直交系であるならある $e_{r+1}, ..., e_n \in V$ が存在して $\langle e_1, ..., e_r, e_{r+1}, ..., e_n \rangle$ は正規直交基底となる.

証明. $a \in V$ が $e_1, ..., e_r$の一次結合でかけないとき $a' := a - \sum_{i=1}^{r} (a, e_i) e_i$とおけば $i \in \{1, ..., r\}$ に対し $(a', e_i) = 0$ であり $e_{r+1} = \frac{a'}{\|a'\|}$と定義すれば $e_1, ..., e_{r+1}$はまた正規直交系である. e_{r+2}, e_{r+3}と繰り返し定義すればいずれは正規直交基底を取れる. □

定義 38. W を V の部分空間とする. $W^{\perp} = \{x \in V | \, \forall y \in W; (x, y) = 0\}$ を W の直交補空間という. 明らかに $V \cong W \oplus W^{\perp}$である.

命題 52 (125 ページ,[6.6])**.** $T : V \to V$ をユニタリー変換とする. E を T の ONB としたとき, T の E に関する行列 A はユニタリー行列である. 逆に, T のある ONB の E に関する行列 A がユニタリー行列のとき, T はユニタリー変換である.

証明. [9], 124 ページよりφ^{-1}, φ は計量同型$^{(*)}$である.
A がユニタリー行列と $(A\boldsymbol{x}, A\boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{y})$(内積を保つ) とは同値であることは重要事項であろう.

$$(A^* A\varphi(x), \varphi(y))_{\mathbb{K}^n} = (A\varphi(x), A\varphi(y))_{\mathbb{K}^n} \overset{(*)}{=} (Tx, Ty)_V$$

において最左辺は $A^* A = E$ ならば

$$(\varphi(x), \varphi(y))_{\mathbb{K}^n} \overset{(*)}{=} (x, y)_V$$

□

定義 39. $\mathbb{K} = \mathbb{C}$ とする. 線型変換 $T : V \to V$ に対しある $x \neq \mathbf{0}$, ある$\alpha \in \mathbb{K}$ が存在して $Tx = \alpha x$ を満たすときαを T の固有値といい, x をαに対する T の固有ベクトルという. $W_\alpha := \mathrm{Ker}(\alpha \mathrm{id}_V - T) = \{x \in V | \, Tx = \alpha x\} \subset V$ をαに対する T の固有空間という. そして $A \in M_{nn}(\mathbb{C})$ を線型変換 $\mathbb{C}^n \to \mathbb{C}^n$と思って同様に A の固有値や固有ベクトルなどを定義する.

定義 40. $A = (a_{ij})$ とする. $\Phi_A(\alpha) := |\alpha I - A| = \begin{vmatrix} \alpha - a_{11} & -a_{12} & \cdots & & -a_{1n} \\ -a_{21} & \alpha - a_{22} & \cdots & & \\ & & \ddots & & \\ & & & \ddots & \\ -a_{n1} & & \cdots & \cdots & \alpha - a_{nn} \end{vmatrix}$ を A の n 次固有多項式という. αが A の固有値 $\Leftrightarrow \exists x \neq \mathbf{0}; (\alpha I - A)x = \mathbf{0} \Leftrightarrow \Phi_A(\alpha) = 0$ である. 一般に$\Phi_A(\alpha) = (\alpha - \alpha_1)^{m_1} \cdots (\alpha - \alpha_k)^{m_k}$と因数分解できる. ただし, $\forall i, j (i \neq j \to \alpha_i \neq \alpha_j)$ かつ $m_1 + \cdots + m_k = n$ とした.

注 21. 先に重要事項を述べる. $T : V \to V$ を線型変換としそれを表現する n 次正則行列を A とする. A の固有値αに対する固有空間を W_αとするとき,

$$
\begin{aligned}
A \text{ が対角化可能} \quad &\Leftrightarrow \quad \text{各固有値}\alpha\text{の重複度が各固有空間の次元} \dim W_\alpha \text{に等しい} \\
&\Leftrightarrow \quad \text{相異なる固有値の各固有空間の次元の総和が} n \text{に等しい (132 ページ, [1.2])} \\
&\text{i.e.} \quad V = \bigoplus_\lambda W_\lambda
\end{aligned}
$$

注 22. V, V'を $\mathbb{K}$ 線型空間とし $V \times V'$に和とスカラー倍を $(x, x') + (y, y') = (x + y, x' + y'), \lambda(x, x') = (\lambda x, \lambda x')$ で定めて出来る線型空間を $V \oplus V'$とかき V と V'の直和という. より一般に $(V_i)_{i\in I}$に対しても, $\{(x_1, x_2)\}$ を x_1, x_2という二つのベクトルから生成される集合を表すものとした上で

$$
\bigoplus_{i\in I} V_i = \{\{(x_i)_{i\in I} \in \prod_{i\in I} V_i\}\} = \{\sum_{i\in I} a_i x_i \mid a_i \in \mathbb{K},\ a_1, a_2, ...\text{は有限個以外 } 0\}
$$

によって線型空間の直和を定義する.

注 23. αが T の固有値であることとαが A の固有値であることは同値である. なぜなら図式の可換性より $Tx = \alpha x \Leftrightarrow A\varphi(x) = \alpha\varphi(x) = \varphi(\alpha x)$ であるから.

注 24. $\alpha_1, ..., \alpha_k$を T の相異なる固有値とする. 任意の $i \in \{1, ..., k\}$ に対し $x_i \in W_{\alpha_i}\backslash\{\mathbf{0}\}$ と定める. このとき $x_1, ..., x_k$は一次独立である. 131 ページ, [1.1] を参照せよ.

注 25 (132 ページ,[1.2])**.** 固有空間 W_αは V の $\{\mathbf{0}\}$ でない T 安定空間であることからも, もし $V = \bigoplus_{j=1}^k W_{\alpha_j}$であるなら, 以下の可換図式において T の行列 A とは

$$
A = \begin{pmatrix} A|_1 & O & O & O \\ O & A|_2 & O & O \\ O & O & \ddots & O \\ O & O & O & A|_k \end{pmatrix},\ \text{ただし},\ A|_i = \begin{pmatrix} \alpha_i & & 0 \\ & \ddots & \\ 0 & & \alpha_i \end{pmatrix} (1 \le i \le k)
$$

とかける. 行列 A における対角線上の $A|_i$の順番は V の適当な基底 $E = \langle e_1, ..., e_n\rangle$ をなす列ベクトル $e_1, ..., e_n$の順序によっている.

$$
\begin{array}{ccc}
W_{\alpha_1} \oplus \cdots \oplus W_{\alpha_k} & \xrightarrow{\quad T \quad} & W_{\alpha_1} \oplus \cdots \oplus W_{\alpha_k} \\
\Big\downarrow{\scriptstyle \varphi_E} & \cup & \Big\downarrow{\scriptstyle \varphi_E} \\
\mathbb{C}^n \cong \mathbb{C}^{m_1} \oplus \cdots \oplus \mathbb{C}^{m_k} \oplus \cdots \oplus \mathbb{C}^{m_k} & \xrightarrow[A]{} & \mathbb{C}^{m_1} \oplus \cdots \oplus \mathbb{C}^{m_k} \cong \mathbb{C}^n
\end{array} \tag{2.5}
$$

証明. [1.2] を示す. ($\Rightarrow$) 仮定より, 適当な基底 E を選べば T の E に関する行列は $A =$

$\begin{pmatrix} \beta_1 & & 0 \\ & \ddots & \\ 0 & & \beta_n \end{pmatrix}$ である. $A = \varphi_E \circ T \circ \varphi_E^{-1}$ より

$$\varphi_E \circ T(e_i) = \varphi_E T \varphi_E^{-1} \varphi_E(e_i) = A\varphi_E(e_i) = A\boldsymbol{\epsilon}_i \equiv \begin{pmatrix} \beta_1 & & 0 \\ & \ddots & \\ 0 & & \beta_n \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \beta_i \boldsymbol{\epsilon}_i = \varphi(\beta_i e_i)$$

よって

$$Te_i = \beta_i e_i$$

であるから e_i は T の固有値β_iに対する固有ベクトルである. これと (24), そして任意の $x \in V$ は $x = \sum_{i=1}^{n} \underset{\text{各 } i \text{ に対してある } j \text{ があって } x_i e_i \in W_{\alpha_j} \text{である.}}{x_i e_i}$ とかけたので, $\bigoplus_{j=1}^{k} W_{\alpha_j} = V$.

($\Leftarrow$) $m_j := \dim W_{\alpha_j}$ $(1 \leq j \leq k)$ とおき $E_j = \langle e_{j,1}, ..., e_{j,m_j} \rangle$ を W_{α_j}の基底としよう. そして仮定により

$$m_1 + \cdots + m_k = n$$

である. まずこのとき

$$E = \langle e_{1,1}, ..., e_{1,m_1}, e_{2,1}, ..., e_{2,m_2}, \cdots, e_{k,1}, ..., e_{k,m_k} \rangle$$

は V の基底となることを確かめよ. そして線型写像 T の定義域を各固有空間に制限したときを考えると各 $j \in \{1, ..., k\}$ に対し

$$Te_{j,\ell} = \alpha_j e_{j\ell} \ \ (1 \leq \ell \leq m_j)$$

が成り立ち,

$$\begin{array}{ccc} W_{\alpha_j} & \xrightarrow{T|_{W_{\alpha_j}}} & W_{\alpha_j} \\ {\scriptstyle \varphi_{E_j}}\downarrow & \circlearrowright & \downarrow{\scriptstyle \varphi_{E_j}} \\ \mathbb{C}^{m_j} & \xrightarrow[A|_j]{} & \mathbb{C}^{m_j} \end{array} \tag{2.6}$$

が可換となる. ここで $T|_{W_{\alpha_j}}$ の表現行列 $A|_j$ は $A|_j = \begin{pmatrix} \alpha_j & & 0 \\ & \ddots & \\ 0 & & \alpha_j \end{pmatrix}$ である. 以下にこれを示す.

任意の $x \in W_{\alpha_j}$ は $x = \sum_{\ell=1}^{m_j} x_\ell e_{j,\ell}$ とかける. 以前と同じく $\epsilon_\ell := \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ と定める.

$$\varphi_{E_j}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_{m_j} \end{pmatrix} = \sum_{\ell=1}^{m_j} x_\ell \epsilon_\ell$$

$A|_j = \varphi_{E_j} T \varphi_{E_j}^{-1}$ より (*)

$$A|_j \begin{pmatrix} x_1 \\ \vdots \\ x_{m_j} \end{pmatrix} = A|_j \varphi_{E_j}(\sum_\ell x_\ell e_{j,\ell}) = \sum_\ell x_\ell \varphi_{E_j} \circ \varphi_{E_j}^{-1} A|_j \varphi_{E_j}(e_{j,\ell}) \overset{(*)}{=} \sum_\ell x_\ell \varphi_{E_j} T(e_{j,\ell})$$

$$= \sum_\ell x_\ell \alpha_j \varphi_{E_j}(e_{j,\ell}) = \begin{pmatrix} \alpha_j & & 0 \\ & \ddots & \\ 0 & & \alpha_j \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{m_j} \end{pmatrix}$$

□

注 **26** (119 ページ)**.**

$T : V \to V$ を線型写像, $\varphi_E : V \cong \mathbb{C}^n$ で定まる V の基底を E, A を T の行列

$S : U \to U$ を線型写像, $\varphi_F : U \cong \mathbb{C}^m$ で定まる U の基底を F, B を S の行列

とし $T \oplus S : V \oplus U \to V \oplus U; x \oplus y \mapsto Tx \oplus Sy$ を定める. すると $T \oplus S$ の行列 $R \in M_{n+m}(\mathbb{C})$ は $\begin{pmatrix} A & O \\ O & B \end{pmatrix}$ である.

定義 41. V を計量空間とし $T : V \to V$ を $\mathbb{K}$ 上の線型変換とする. 124 ページの簡単な考察より, V の任意の正規直交基底 E に関する T の行列 A に対して

$$(Tx, y)_V = (A\varphi_E(x), \varphi_E(y))_{\mathbb{K}^n}$$

が成り立つ. $(T^*x, y) = (x, Ty)$ により定まる $T^* : V \to V$ を T の共役 (adjoint) といいその行列は A^* である. 実際

$$(A^*\varphi(x), \varphi(y)) = (\varphi(x))^t (A^*)^t \overline{\varphi(y)} = (\varphi(x), A\varphi(y))$$

命題 53. A を正規行列 (i.e. $A^*A = AA^*$) とし $W \subset V$ を部分空間とする. W が A 安定 ($\forall x \in W; Ax \in W$) であるなら $W^\perp$ は A^* 安定である.

証明. 任意に $y \in W^\perp$ を取ると $\forall x \in W$ に対し $(x, y) = 0$ である. よって仮定より $\forall z \in W$ に対し, $(z, A^*y) = (Az, y) = 0$. すなわち $A^*y \in W^\perp$ がいえた. □

命題 54. αを正規行列 A の固有値とするとき固有空間 W_αは A 安定であり A^*安定でもある. 前命題と $(W_\alpha^*)^* = W_\alpha$から $W_\alpha{}^\perp$も A 不変かつ A^*不変.

証明. 任意の $x \in W_\alpha$に対し $Ax = \alpha x \in W_\alpha$($\because A(Ax) = \alpha(Ax)$ より.) なので A 不変である. また

$$A(A^*x) = A^*(Ax) = A^*(\alpha x) = \alpha A^* x$$

より $A^*x \in W_\alpha$がいえたので W_αは A^*不変である. □

命題 55 (139 ページ,[2.1])**.** A, B を n 次正方行列で互いに可換であるとする. このとき A の任意の固有値λに対しある B の固有値μと共通の固有ベクトル $x \neq \mathbf{0}$ が少なくとも一つ存在する.

$$\forall\lambda\exists x \neq \mathbf{0}(Ax = \lambda x \to \exists\mu(Bx = \mu x))$$

注 27. 量子力学の枠組みでは, 可観測量としての演算子は自己共役 (エルミート変換の一般化) であることが要請される. 自己共役演算子$\hat{A}, \hat{B}$が可換であるときは, 本命題とは裏腹に$\hat{A}, \hat{B}$の全ての固有ベクトルを同時固有ベクトル (もしくは同時固有状態という) として取れることを以下に示す. その際には少し後で述べる, まだ証明していない定理を使うがご容赦願いたい. 古典力学では二つの物理量を同時に測定できるが, 量子力学の範疇ではその為には物理量に対応する演算子$\hat{A}, \hat{B}$が可換でなければならないということである. 次の証明はいつしかの自主ゼミの場で私が与えたものをまた引っ張り出してきたものである.

証明. 以下, 本来なら無限次元の固有空間を有限次元と考えるなど議論に曖昧さが残っている点があることに注意すると共に, 巨大な行列を適宜イメージするとよい.
$\hat{A}$の固有値αに対する固有空間 W_αを考える. W_αの正規直交系を $\{|n\rangle ; n \in \{1, ..., m\}\}$ とする.

$$\hat{A}\hat{B}|n\rangle = \hat{B}\hat{A}|n\rangle = a\hat{B}|n\rangle \quad (\forall |n\rangle)$$

よって $\hat{B}|n\rangle$ は固有値αに対する$\hat{A}$の固有状態ベクトルであるので, $\hat{B}|k\rangle$ は W_αの基底を用いて一次結合でかける.

$$\hat{B}|k\rangle = \sum_n {c_n}^{(k)} |n\rangle$$

$\{|n\rangle\}(1 \leq n \leq m)$ を並べた行列を $P = \begin{pmatrix} |1\rangle & \cdots & |m\rangle \end{pmatrix}$ とすると

$$\hat{B}P = PM \quad \text{ただし } M := \begin{pmatrix} {c_1}^{(1)} & {c_1}^{(2)} & \cdots & {c_1}^{(m)} \\ \vdots & \vdots & \ddots & \vdots \\ {c_m}^{(1)} & {c_m}^{(2)} & \cdots & {c_m}^{(m)} \end{pmatrix} \in M_{mm}(\mathbb{C})$$

同様に他の固有値$\alpha', \alpha'', ...$についても

$$P' = \begin{pmatrix} |1\rangle' & \cdots & |p\rangle' \end{pmatrix} \text{に対し} \hat{B}P' = P'M'$$

$$M' := \begin{pmatrix} {d_1}^{(1)} & {d_1}^{(2)} & \cdots & {d_1}^{(p)} \\ \vdots & \vdots & \ddots & \vdots \\ {d_p}^{(1)} & {d_p}^{(2)} & \cdots & {d_p}^{(p)} \end{pmatrix} \in M_{pp}(\mathbb{C})$$

$$\vdots$$

とおく. 次に行列 $\mathbb{P} = \begin{pmatrix} P & P' & \cdots & P'^{\cdots'} \end{pmatrix}$ という, 線型独立な固有ベクトルを同じ固有値に対する固有ベクトルは隣り合う順番に並べた行列を定義すると

$$\hat{B}\,\mathbb{P} = \mathbb{P}\begin{pmatrix} M & & & O \\ & M' & & \\ & & \ddots & \\ O & & & M'^{\cdots'} \end{pmatrix}$$

である. W_αの元 $|1\rangle, ..., |m\rangle$ と $W_{\alpha'}$の元 $|1\rangle', ..., |p\rangle'$ と, ...とは独立でそれらを合わせたものは全体の空間の基底であることから $\mathbb{P}$ は正則なので,

$$\mathbb{P}^{-1}\hat{B}\,\mathbb{P} = \begin{pmatrix} M & & & O \\ & M' & & \\ & & \ddots & \\ O & & & M'^{\cdots'} \end{pmatrix}$$

が成り立つ. $\hat{B}$が自己共役演算子即ちエルミート行列として考え $\mathbb{P}$ はユニタリー行列より $(\mathbb{P}^{-1}\hat{B}\mathbb{P})^* = \mathbb{P}\hat{B}\mathbb{P}$ なので $\mathbb{P}^{-1}\hat{B}\mathbb{P}$ はエルミート行列である. よって, 対角成分の行列 $M, M', ...$ もエルミート行列である. 即ち適当なユニタリー行列 Q で対角化可能なので $Q^{-1}MQ$ は対角行列となり, $M', M'', ...$に対しても同様に適当な $Q', Q'', ...$を用いて対角行列にできる. ここまでの議論によると行列 $Q, Q', ...Q'^{\cdots'}$ を対角線上に並べてできる行列を $\mathbb{Q}$ とすると $\mathbb{Q}^{-1}(\mathbb{P}^{-1}B\mathbb{P})\mathbb{Q}$ は対角行列となることが分かる. 即ち $\mathbb{P}\mathbb{Q}$ は$\hat{B}$の対角化行列である. また $\mathbb{P}\mathbb{Q}$ は$\hat{A}$の正規直交系をなす固有状態ベクトルらを並べた行列 $\mathbb{P}$ を $\mathbb{Q}$ で列基本変形したものであるから, $\mathbb{P}\mathbb{Q}$ の各列ベクトルも$\hat{A}$の線型独立な固有ベクトルゆえ 133 ページ, [1.2]′の仮定を満たし$\hat{A}$の対角化行列でもある. $\hat{A}\hat{B} = \hat{B}\hat{A}$なら$\hat{A}$と$\hat{B}$は同時対角化可能で, $\hat{A}, \hat{B}$の任意の固有ベクトルは同時固有ベクトルとして取れる. □

上命題を基礎として, 以下が成り立つ.

命題 56 (141 ページ)**.** A と B が互いに可換なら適当なユニタリー行列 U によって U^*AU, U^*BU は同時に上三角行列にできる.

特に, 正方行列 A に対して適当なユニタリー行列 U が存在して $U^{-1}AU = \begin{pmatrix} \alpha_1 & & * \\ & \ddots & \\ O & & \alpha_n \end{pmatrix}$ と

なる.

証明. V の n 個の異なる安定部分空間にそれぞれ $T : V \to V$ を制限すれば 119 ページ, (6) より各 i について $T_A|_{W_i}$は i 次上三角行列であるから T_Aは上三角行列となる. T_Bも同様に上三角行列となる. 共通する固有ベクトル $\boldsymbol{u}_i \in W_i(s.t.\ (\boldsymbol{u}_i, \boldsymbol{u}_{i-1}) = 0$ であって $\|\boldsymbol{u}_i\| = 1)$ を並べたユニタリー行列 U に対して $U^{-1}AU = T_A$である. T_A, T_Bの対角線上には固有値$\lambda_1, ..., \lambda_n$や$\mu_1, ..., \mu_n$がある. □

命題 57 (141 ページ, [2.4]')**.**

$$A \text{ が正規行列} \Rightarrow \text{適当なユニタリー行列 } U \text{ が存在して } U^*AU \text{ が対角行列}$$

[9] では $TT^* = T^*T$ であるとき T, T^*は可換より前定理を用いてその表現行列 A, A^*が上三角行列となることから直ちに導いている. これより特にエルミート行列はユニタリー行列で対角化可能である.

証明. ϵ_j $(1 \le j \le n)$ は単位列ベクトルとする.
$\mathbb{C}^n \cong V = W_{\alpha_1} \oplus {W_{\alpha_1}}^{\perp}$に応じて

$$\langle e_1, ..., e_{m_1} \rangle : W_{\alpha_1} \text{の } ONB \quad \langle e_{m_1+1}, ..., e_n \rangle : {W_{\alpha_1}}^{\perp} \text{の } ONB$$

$$E = \langle e_1, ..., e_{m_1}, e_{m_1+1}, ..., e_n \rangle \text{ を } V \text{ の } ONB$$

とする.

$$\text{ユニタリーな } U_1 := \begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} \text{は基底の変換行列 } \langle \epsilon_1, ..., \epsilon_n \rangle \to E$$

である. なぜなら任意の $V \ni x = \sum_{j=1}^{n} x_j \epsilon_j = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$はまた

$$x = \sum_{i=1}^{n} y_i e_i = \begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} =: U_1 \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

と表せるからである. (基底の取り替え行列とは, 線型空間の元を 2 つの基底によってそれぞれの一次結合で表したときの成分の間に成り立つ関係式を与えるようなものであった.)
任意の $x \in V = W_{\alpha_1} \oplus {W_{\alpha_1}}^{\perp}$は

$$\begin{aligned} x &= \sum_{i=1}^{m_1} y_i e_i + \sum_{i=m_1+1}^{n} y_i e_i \ (=: x' + x'' \text{とおく}. \ x' \in W_{\alpha_1}, x' \in {W_{\alpha_1}}^{\perp}) \\ &= U_1 \begin{pmatrix} y_1 \\ \vdots \\ y_{m_1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + U_1 \begin{pmatrix} 0 \\ \vdots \\ 0 \\ y_{m_1+1} \\ \vdots \\ y_n \end{pmatrix} \left(:= U_1 \begin{pmatrix} y^{(1)} \\ \mathbf{0} \end{pmatrix} + U_1 \begin{pmatrix} \mathbf{0} \\ y^{(2)} \end{pmatrix} \text{とおく}.\right) \end{aligned}$$

$$Ax = Ax' + Ax'' = AU_1 \begin{pmatrix} y^{(1)} \\ \mathbf{0} \end{pmatrix} + AU_1 \begin{pmatrix} \mathbf{0} \\ y^{(2)} \end{pmatrix}$$

α_1は x'に対する固有値なので

$$Ax' = \alpha_1 x' = \alpha_1 U_1 \begin{pmatrix} y^{(1)} \\ \mathbf{0} \end{pmatrix} = \alpha_1 U_1 \begin{pmatrix} I_{m_1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} y^{(1)} \\ y^{(2)} \end{pmatrix}$$

$$Ax'' = AU_1\begin{pmatrix}\mathbf{0}\\ \hline y^{(2)}\end{pmatrix} = AU_1\begin{pmatrix}\mathbf{0} & \mathbf{0}\\ \mathbf{0} & I_{n-m_1}\end{pmatrix}\begin{pmatrix}y^{(1)}\\ y^{(2)}\end{pmatrix}$$

$$= \begin{pmatrix}\mathbf{0} & *_1\\ \mathbf{0} & *_2\end{pmatrix}\begin{pmatrix}y^{(1)}\\ y^{(2)}\end{pmatrix} \text{かつ } Ax'' \in {W_{\alpha_1}}^{\perp} = \left\{\begin{pmatrix}\mathbf{0}\\ \hline y^{(2)}\end{pmatrix} \mid y^{(2)}\text{は任意}\right\} \text{より},$$

$$Ax'' = \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ \mathbf{0} & *_2\end{pmatrix}\begin{pmatrix}y^{(1)}\\ y^{(2)}\end{pmatrix}$$

である. したがって

$$\begin{aligned} Ax &= Ax' + Ax'' \\ &= U_1\begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & \exists A_1\end{pmatrix}\begin{pmatrix}y^{(1)}\\ y^{(2)}\end{pmatrix} \\ &= U_1\begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix}{U_1}^{-1}x \quad (\text{ただし } U_1A_1 = *_2) \end{aligned}$$

よって

$${U_1}^{-1}Ax = \begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix}{U_1}^{-1}x \text{ において } x := U_1\begin{pmatrix}y^{(1)}\\ \hline y^{(2)}\end{pmatrix}$$

と定めると

$${U_1}^{-1}AU_1 = \begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix}$$

がわかる.

(主張) 正規行列 A とユニタリー行列 U に対し $U^{-1}AU$ は正規である.

$(U^{-1}AU)^*(U^{-1}AU) = U^*A^*UU^{-1}AU = U^*A^*AU = U^*AA^*U = U^*AUU^{-1}A^*U = (U^{-1}AU)(U^{-1}AU)^*$ より明らか. よって

$$\begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix}^*\begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix} = \begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix}\begin{pmatrix}\alpha_1 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1\end{pmatrix}^*$$

$$\Leftrightarrow \begin{pmatrix}|\alpha_1|^2 I_{m_1} & \mathbf{0}\\ \mathbf{0} & {A_1}^*A_1\end{pmatrix} = \begin{pmatrix}|\alpha_1|^2 I_{m_1} & \mathbf{0}\\ \mathbf{0} & A_1{A_1}^*\end{pmatrix}$$

よって $n-1$ 以下の場合の帰納法の仮定より, A_1は正規であるからある適当なユニタリー行列 $U_2 \in M_{n-m_1}(\mathbb{C})$ があって

$${U_2}^*A_1U_2 = \begin{pmatrix}\beta_1 & & 0\\ & \ddots & \\ 0 & & \beta_{n-m_1}\end{pmatrix} \quad (\text{各}\beta_i(1 \le i \le n-m_1) \text{ は } A_1\text{の固有値})$$

とできる. そこで $U := U_1 \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0} & U_2 \end{pmatrix}$ とおくと

$$\begin{aligned} U^*AU &= \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0} & {U_2}^* \end{pmatrix} \begin{pmatrix} \alpha_1 I & \mathbf{0} \\ \mathbf{0} & A_1 \end{pmatrix} \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0} & U_2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_1 I & \mathbf{0} \\ \mathbf{0} & {U_2}^* A_1 U_2 \end{pmatrix} \end{aligned}$$

証明終. また $\beta_1, ..., \beta_{n-m_1}$ は A の α_1 以外の固有値全体として与えられていたことになる. □

系 4 ([2.5]). V をユニタリー空間とし $T : V \to V$ を正規変換とする. T の相異なる固有値 $\beta_1, ..., \beta_k$ に対する固有ベクトルは直交し $V = W_{\beta_1} \oplus \cdots \oplus W_{\beta_k}$ である.

証明. β_i の重複度を $m_i (1 \le i \le k)$ とする. 前定理より T の固有ベクトルだけからなる V の正規直交基底 $E = \langle e_1, ..., e_n \rangle$ が存在し, $\langle e_1, ..., e_{m_1} \rangle$ は W_{β_1} の正規直交基底, $\cdots$, $\langle e_{n-(m_r-1)}, ..., e_n \rangle$ は W_{β_k} の正規直交基底である. よって正しい. □

命題 58 (139 ページ). エルミート行列 A の固有値 $\alpha_1, ..., \alpha_n$ はすべて実数である. なぜなら $A^* = A$ のとき $A^*A = AA^* = A^2$ より A は正規行列であるから適当なユニタリー行列 U があって $D := U^*AU = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}$ だがこれの共役転置をとって $D^* = \begin{pmatrix} \overline{\alpha_1} & & \\ & \ddots & \\ & & \overline{\alpha_n} \end{pmatrix}$ であることより. また, 次は A をユニタリー行列とすると

$$\begin{pmatrix} |\alpha_1|^2 & & \\ & \ddots & \\ & & |\alpha_n|^2 \end{pmatrix} = DD^* = (U^*AU)(U^*AU)^* = U^*AUU^*A^*U = E$$

より $|\alpha_1|^2 = \cdots = |\alpha_n|^2 = 1$ を満たす.

注 28 (145 ページ). T が正規変換であるとき T のスペクトル分解が一意に定まるので

T がエルミート変換 $\Leftrightarrow$ T の固有値が全て実数, T がユニタリー変換 $\Leftrightarrow$ 固有値が全て絶対値 1

が示される.

解 14 (94 ページ)**.** 例えば $M_{mn} \ni A = \begin{pmatrix} a & O \\ O & O \end{pmatrix} \sim F_{mn}(1)$ というように各同値類の元は行列基本変形をすることで標準形 $F_{mn}(r)(0 \leq r \leq \min\{m,n\})$ となる. $|M_{mn}/\sim| = 1 + \min\{m,n\}$ である.

解 15 (106 ページ)**.** $E = \langle e_1, e_2, e_3\rangle \to F = \langle f_1, f_2, f_3\rangle$ の行列 P は $(e_1\ e_2\ e_3)P = (f_1\ f_2\ f_3)$ を満たす. $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 3 & 4 & 3 \\ -1 & 1 & -2 \\ 4 & 8 & 6 \end{pmatrix} = \begin{pmatrix} 1/2 & -1 & 1/2 \\ 1/2 & 0 & -1/2 \\ -1/2 & 1 & 1/2 \end{pmatrix} \begin{pmatrix} 3 & 4 & 3 \\ -1 & 1 & -2 \\ 4 & 8 & 6 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 9 & 10 & 13 \\ -1 & -4 & -3 \\ -1 & 6 & -1 \end{pmatrix}$

解 16 (107 ページ)**.** $E \to F$ の行列を P とすると $(e_1\ e_2)P = (f_1\ f_2)$ より $\begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ -1 & -2 \end{pmatrix}$ を満たし $P = \begin{pmatrix} -1 & -1 \\ 1 & 2 \end{pmatrix}$ である.

解 17 (108 ページ)**.** (イ)59 ページ, [5.5] より $\{(x_i) | \sum_{i=1}^n x_i = 0, x_i \in \mathbb{K}\}$ は $\mathbb{K}^n$の次元 $n-1$ の部分空間である. 未知数が n こあり 59 ページでいう係数行列のランクが 1 より, 斉次方程式の任意の解が $n-1$ この解ベクトルの一次結合でかける即ち解空間の次元が $n-1$ であることが定理 [5.5] から直ぐに言えるということである.
(ロ)$W = \{(x_i)\, | x_{p+1} = x_{p+2} = \cdots = x_n = 0 (1 \leq p \leq n)\}$ が解空間である斉次方程式

$$\begin{pmatrix} 0 & \cdots & 0 & \underset{(1,p+1)\text{ 成分}}{1} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ & & & & & & \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_p \\ x_{p+1} \\ x_{p+2} \\ \vdots \\ x_n \end{pmatrix} = \mathbf{0}$$

において係数行列のランクは $n-p$(独立な列ベクトルの本数から明らか) であるので部分空間の次元は $n-(n-p) = p$ である. 他にも, 部分空間の定義によるとここでは $\mathbb{K}^n$の演算が W 上でも閉じることを示してもよい. なお次元の数は $\forall \boldsymbol{x} = x_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} + \cdots + x_p \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ より p であり連立方程式系の理論を援用しなくてもよい.
(ハ) $\boldsymbol{x} = \epsilon_i, \boldsymbol{y} = \epsilon_j (i \neq j)$ のとき $\boldsymbol{x} + \boldsymbol{y} \notin \{(x_i) | \sum_{i=1}^n {x_i}^2 = 1\}$ より部分空間でない. (ニ) さて $\boldsymbol{a} = a_1\epsilon_1 + \cdots + a_n\epsilon_n$とすると $(\boldsymbol{a}, \boldsymbol{x}) = 0 \Leftrightarrow \boldsymbol{a}^t\overline{\boldsymbol{x}} = 0$ i.e $\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} \begin{pmatrix} \overline{x_1} \\ \vdots \\ \overline{x_n} \end{pmatrix} = 0$ である. 問

いの空間はこの方程式の解空間であるから部分空間であり, 次元は方程式における未知数の数 – 係数行列のランクである. よって $\boldsymbol{a}=\boldsymbol{0}$ なら $n, \boldsymbol{a}\neq\boldsymbol{0}$ なら $n-1$ である.

解 18. (イ) 反例を与える. n 次非正則行列全体の空間の元から $\boldsymbol{a}=(\epsilon_1\ \cdots\ \epsilon_{n-1}\ \boldsymbol{0})$, $\boldsymbol{b}=(\boldsymbol{0}\ \cdots\ \boldsymbol{0}\ \epsilon_n)$ を取ると $\boldsymbol{a}+\boldsymbol{b}$ は単位行列で正則である. (ロ)$AX_1=X_1B, AX_2=X_2B$ となる X_1, X_2 に対して $A(X_1+X_2)=(X_1+X_2)B$ かつ $A(aX_1)=(aX_1)B$ より部分空間である.
(ハ) 反例を与える. $A=\begin{pmatrix}0&1\\0&0\end{pmatrix}, B=\begin{pmatrix}0&0\\1&0\end{pmatrix}$ とすると $k\in\mathbb{N}$ について $(A+B)^k=A+B : k$ は奇数, $E_2 : k$ は偶数なので部分空間をなさない. スカラー倍については $A^k=O$ となる k があるなら $(aA)^k=O$ より演算は閉じる. (ニ) 部分空間でない.

例 6 (114 ページ,118 ページ)**.** V の元 $\{x_n\}$ の項 $x_0, x_1, ...$は (すなわち数列 $\{x_n\}$ は) 等式

$$x_{n+k}+a_{k-1}x_{n+k-1}+\cdots+a_1x_{n+1}+a_0x_n=0,\ n\geq 0$$

より始めの k 項によって定まる. よって同型$\varphi : V\to\mathbb{K}^k$を $\{x_n\}\mapsto(x_0\ x_1\cdots\ x_{k-1})$ で定められる. 次の $e_i\in\mathbb{K}^k(0\leq i\leq k-1)$ を V の元とみると

$$e_0=(1,0,0,...,0)\quad e_1=(0,1,0,...,0)\qquad e_{k-1}=(0,0,...,1)$$

$\langle e_0,...,e_{k-1}\rangle$ は V の基底をなす. 各 $e_i(0\leq i\leq k-1)$ に対する $T(e_i)$ が終域の基底 (今の場合は同じ基底)
ではどのような一次結合で表せるのかを調べることで得る k 本の列ベクトルを並べること で T の表現行列 A がわかる. $A=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\&&&&\\0&0&\cdots&0&1\\-a_0&-a_1&\cdots&-a_{k-2}&-a_{k-1}\end{pmatrix}$ は $A\begin{pmatrix}x_0\\x_1\\\vdots\\x_{k-1}\end{pmatrix}=\begin{pmatrix}x_1\\x_2\\\vdots\\x_k\end{pmatrix}$ を満たす. この A は

$$\frac{d^ky}{dx^k}+a_{k-1}\frac{d^{k-1}y}{dx^{k-1}}+\cdots+a_1\frac{dy}{dx}+a_0y=0$$

の解空間の元に対する $D : y\mapsto\frac{dy}{dx}$の行列でもある.
上の数列空間 V は, $k=2, a_0=2, a_1=-3$ とすると $x_{n+2}-3x_{n+1}+2x_n=0$ を満たす $\{x_n\}$ 全体である. 上述より $A=\begin{pmatrix}0&1\\-2&3\end{pmatrix}$ であり T の $\langle f_0,f_1\rangle$ に関する行列は式 (5) より $P^{-1}AP=\begin{pmatrix}1&0\\0&2\end{pmatrix}$ なので $Tf_0=f_0, Tf_1=2f_1$(T の固有値を求めているということ) である. T は項を一つずらす線型変換であったので $f_0=\{1\}, f_1=\{2^n\}$. V の任意の数列は $\{x_n\}=\{\alpha+\beta 2^n\}$ である. 項を一つずらす線型変換を考えることで数列の一般項が求められた. また同じ解法で

$$\frac{d^2y}{dx^2}-3\frac{dy}{dx}+2y=0$$

の任意の解は $f(x)=\alpha e^x+\beta e^{2x}$である.

例 7 (137 ページ)**.** 上例において固有方程式$\Phi_A(x)=\begin{vmatrix}x&-1\\2&x-3\end{vmatrix}=x(x-3)+2=0$ より $f_0:=\{1\}, f_1:=\{2^n\}$ という固有ベクトルを探せ $\langle f_0,f_1\rangle$ は V の基底であるから V の任意の元は $\{\alpha+\beta 2^n\}$ とかけた. 固有方程式が重解を持つときはこの解法は適用できない. 重解を持つ場合はジョルダン標準形の構造的理解が必要である. 195 ページを参照せよ.

2.3 [9] 第 5 章

解 19 (138 ページ)**.** $\Phi_A(x) = (x-1)(x-2)(x-3) = 0$ より固有値は $1, 2, 3$ である. 固有値 1 に対する固有ベクトルを求める. $\begin{pmatrix} -5 & 6 & 4 \\ -7 & 8 & 4 \\ -2 & 2 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Leftrightarrow \begin{pmatrix} -6 & 6 & 4 \\ -7 & 7 & 4 \\ -2 & 2 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \mathbf{0}$ において左から行基本変形をしても方程式は同値であるので $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & -1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \mathbf{0}$ であるので固有ベクトルは他にも色々あるが $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ である. 同様に固有値 $2, 3$ に対する固有ベクトルも求めてそれらを並べてできる $P = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$ が対角化行列である. $P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. なお, 対角化できる必要十分条件としての各固有空間の次元の和が線型変換 $f_A : V \to V$ の V の次元 (今は 3) に一致することは, 相異なる 3 つの固有値を求めた時点で固有ベクトルは $\mathbf{0}$ ではないことに注意すれば満たされていることがわかる.

(ロ)$\Phi_A(x) = x(x-1)^2$である. 固有値 1 に対する固有空間が 2 次元なら対角化可能であり 1 次元なら対角化できない. 重要な点として

固有空間の次元が固有値の重複度より大きいことはない. 例えば今の場合では固有空間の次元が 3 次元となることはない. $\begin{pmatrix} -1 & 0 & 2 \\ -1 & 1 & 1 \\ -1 & 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 1\begin{pmatrix} x \\ y \\ z \end{pmatrix} \Leftrightarrow \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \mathbf{0}$. これを満たす x, y, z の組で独立なものとして (異なる固有値に対する固有ベクトルは常に一次独立だが同じ固有値に対してもそのように取ることで対角化できる. そしてそのように取れる状況が固有空間の次元が固有値の重複度に等しい状況である. 本問における $W_1 = \{k(1\ 1\ 1)^t + \ell(0\ 1\ 0)^t; s, t \in \mathbb{K}\}$ より $\dim W_1 = 2$ のように.) $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ を取る. 固有値 0 に対する固有ベクトルは $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ と取る. $P = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ は A を $P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ と対角化する.

(ハ) 対角化可能である.

解 20.

$$(イ)\ y'' - 5y' + 6y = 0$$

105 ページに, k 階斉次線形微分方程式の解空間 V は k 次元であり基底は $\langle f_0, ..., f_{k-1}\rangle s.t.\ \frac{d^j f_i(x)}{dx^j}(0) = \delta_{ij}$であることが記されている. よって

$$y(0) = 1, y'(0) = 0 \text{ を満たす解を } \boldsymbol{e}_1 \text{とし, } y(0) = 0, y'(0) = 1 \text{ を満たす解を } \boldsymbol{e}_2$$

$$\therefore\ \ \boldsymbol{e}_1(x) = 1,\ \boldsymbol{e}_2 = x$$

とすると $E = \langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle$ は $y'' - 5y' + 6y = 0$ の解空間の基底となる. この両辺を微分すると $y''' - 5y'' + 6y' = 0$ であるがこれは $(y')'' - 5(y')' + 6(y') = 0$ と思うと y'も同じ微分方程式の解であることがわかる. よって $\boldsymbol{e}_1'$ と $\boldsymbol{e}_2'$も微分方程式を満たす. E は解空間の基底なので $\boldsymbol{e}_1'$ と $\boldsymbol{e}_2'$は $\boldsymbol{e}_1, \boldsymbol{e}_2$の線型結合としてかける.
以下, 表現行列を見る為その係数を求める. $\boldsymbol{e}_1, \boldsymbol{e}_2$は解なので

$$(\boldsymbol{e}_1')'(0) = 5\boldsymbol{e}_1'(0) - 6\boldsymbol{e}_1(0) = -6 \quad (\boldsymbol{e}_2')'(0) = 5\boldsymbol{e}_2'(0) - 6\boldsymbol{e}_2(0) = -6$$

よって,

$$\boldsymbol{e}_1'(x) = 0\boldsymbol{e}_1 - 6\boldsymbol{e}_2, \quad \boldsymbol{e}_2'(x) = 1\boldsymbol{e}_1 + 5\boldsymbol{e}_2$$

である. $T : V \ni y \mapsto y' \in V$ の基底 E に関する行列を $A = (a_{ij})$ とすると 114 ページの

$$T\boldsymbol{e}_j' = a_{1j}\boldsymbol{e}_1' + \cdots + a_{mj}\boldsymbol{e}_m'$$

が今

$$T(\boldsymbol{e}_j) = \boldsymbol{e}_j' = a_{1j}\boldsymbol{e}_1 + a_{2j}\boldsymbol{e}_2 \ (1 \leq j \leq 2)$$

に当たる訳だから $A = \begin{pmatrix} 0 & 1 \\ -6 & 5 \end{pmatrix}$ である. $\Phi_A(x) = (x-2)(x-3)$ より固有値は $2, 3$ で A は対角化可能である. ゆえに各固有値に対する固有ベクトルらは基底をなす. $Ty = y' = 2y$ となる y が固有値 2 に対する固有ベクトルであり, $y = e^{2x}$を取ろう. なお, この固有空間は $\{ae^{2x}; a \in \mathbb{R}\}$ である. また固有値 3 に対する固有ベクトル e^{3x}を取ろう. 微分方程式の一般解は, 解空間はこれらの固有ベクトルとしての解を基底にもつので, $se^{2x} + te^{3x}$ $(s, t \in \mathbb{R})$ である.

$$(ロ)\ y''' - 7y' + 6y = 0$$

この微分方程式の解 $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$ *s.t.*

$$\boldsymbol{e}_1(0) = 1, \boldsymbol{e}_1'(0) = \boldsymbol{e}_1''(0) = 0, \quad \boldsymbol{e}_2'(0) = 1, \boldsymbol{e}_2(0) = \boldsymbol{e}_2''(0) = 0, \quad \boldsymbol{e}_3'''(0) = 1, \boldsymbol{e}_3(0) = \boldsymbol{e}_3'(0) = 0$$

は解空間の基底をなす. $\boldsymbol{e}_1', \boldsymbol{e}_2', \boldsymbol{e}_3'$も解である.

$$(\boldsymbol{e}_1')''(0) = 7\boldsymbol{e}_1'(0) - 6\boldsymbol{e}_1(0) = -6, \ (\boldsymbol{e}_2')'' = 7\boldsymbol{e}_2'(0) - 6\boldsymbol{e}_2(0) = 7, \ (\boldsymbol{e}_3')'' = 7\boldsymbol{e}_3' - 6\boldsymbol{e}_3 = 0$$

これと $\boldsymbol{e}_i^{(j)}$ $(j = 0, 1, 2\ 1 \leq i \leq 3)$ の初期値より

$$\boldsymbol{e}_1' = 0\boldsymbol{e}_1 + 0\boldsymbol{e}_2 - 6\boldsymbol{e}_3, \ \boldsymbol{e}_2' = 1\boldsymbol{e}_1 + 0\boldsymbol{e}_2 + 7\boldsymbol{e}_3, \ \boldsymbol{e}_3' = 0\boldsymbol{e}_1 + 1\boldsymbol{e}_2 + 0\boldsymbol{e}_3$$

よって基底 $\langle \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3 \rangle$ に関する T *s.t.*$T(\boldsymbol{e}_i) = \boldsymbol{e}_i'$の行列は

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -6 & 7 & 0 \end{pmatrix}$$

である. $\Phi_A(x) = (x-1)(x-2)(x+3)$ より A は対角化可能である. この微分方程式の一般解は s, t, u を任意定数として $se^x + te^{2x} + ue^{-3x}$である.

注 29. これまで求めてきた行列 A はコンパニオン行列といわれる. 問いでは地道に A を求めたが一般論から微分方程式を見た瞬間にみてとれる.

$$x_{n+k} + a_{k-1}x_{n+k-1} + \cdots + a_1 x_{n+1} + a_0 x_n = 0\ (n \geq 0)$$

$$\Leftrightarrow \begin{pmatrix} x_{n+1} \\ x_{n+2} \\ \vdots \\ x_{n+k-1} \\ x_{n+k} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix} \begin{pmatrix} x_n \\ x_{n+1} \\ \vdots \\ x_{n+k-2} \\ x_{n+k-1} \end{pmatrix}$$

$$\Leftrightarrow \boldsymbol{x}_n = \begin{pmatrix} x_n \\ x_{n+1} \\ \vdots \\ x_{n+k-1} \end{pmatrix} \text{に対し } \boldsymbol{x}_{n+1} = A\boldsymbol{x}_n, \quad A \text{ は } f : \{x_n\} \mapsto \{x_{n+1}\} \text{ の行列}$$

$$\frac{d^k y(x)}{dx^k} + a_{k-1}\frac{d^{k-1}y(x)}{dx^{k-1}} + \cdots + a_1 \frac{dy(x)}{dx} + a_0 y(x) = 0$$

$$\Leftrightarrow \frac{d}{dx}\begin{pmatrix} y(x) \\ y'(x) \\ \vdots \\ y^{(k-2)}(x) \\ y^{(k-1)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix} \underbrace{\begin{pmatrix} y(x) \\ y'(x) \\ \vdots \\ y^{(k-2)}(x) \\ y^{(k-1)}(x) \end{pmatrix}}_{\boldsymbol{F}(x)}$$

A の固有値λ_iに対する固有ベクトル $\boldsymbol{U}_i = \begin{pmatrix} u_{i,0} \\ u_{i,1} \\ \vdots \\ u_{i,k-1} \end{pmatrix}$ としたとき, ベクトル値関数

$$\boldsymbol{Y}(x) = \sum_i c_i e^{\lambda_i x} \boldsymbol{U}_i$$

が微分方程式 $\frac{d\boldsymbol{Y}(x)}{dx} = A\boldsymbol{Y}(x)\,;\boldsymbol{Y}(x) = \begin{pmatrix} y(x) \\ y''(x) \\ \vdots \\ y^{(k-1)}(x) \end{pmatrix}$ の解である.

問 28. $x_{n+2} - 3x_{n+1} + 2x_n = 0 (n \geq 0), x_0 = 3, x_1 = 2, x_2 = 6$ で定まる数列 $\{x_n\}$ に対しコンパニオン行列 A の固有ベクトルを求めることで x_{16}を求めよ.

解 21 (143 ページ)**.** $A = \begin{pmatrix} a & i \\ i & a \end{pmatrix}$ は $A^*A = AA^*$(ただし $A^* = \overline{A}^t$) を満たし正規なのでユニタリー行列によって対角化できる. その際は列ベクトルの固有ベクトルは正規直交基底となるよ

うにユニタリー行列を作る. $\Phi_A(x) = \begin{vmatrix} x-a & -i \\ -i & x-a \end{vmatrix} = x^2-2ax+a^2+1 = (x-a-i)(x-a+i)$ より固有値は $a \pm i$. $\begin{pmatrix} \mp ix+iy \\ ix \mp iy \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ つまり $\begin{pmatrix} \mp i & i \\ i & \mp i \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}$ より, $y = \pm x$ であり固有ベクトルは $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ と $\frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix}$ と取ろう. $U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ が A の対角化行列である.

命題 59 (147 ページ)**.** 任意の線型変換 T に対し T^*T は半正値エルミート変換である.

証明.

$$(T^*Tx, y) = (Tx, Ty) = (x, T^*Ty)$$

より T^*T はエルミート変換である. T^*T が半正値であるすなわち固有値が全て非負であることは $\forall x \neq 0$ に対し (T^*Tx, x) が非負であることと同値であるからこれを示す. そして $(T^*Tx, x) = (Tx, Tx) = \|Tx\|^2 \geq 0$ より明らか. T が正則なら $Tx \neq 0$ より $(T^*Tx, x) > 0$ となるから T^*T は正値. □

命題 60. 正則なユニタリー変換 T は正値エルミート変換 H とユニタリー変換 U を用いて $T = HU$ と一意にかける. 正則な実線型変換 T は正値対称変換と直交変換の積として一意にかける.

証明. 前命題より $H = \sqrt{TT^*}$ とすると H は正値エルミート変換である. $U = H^{-1}T$ とすれば

$$UU^* = H^{-1}TT^*H^{-1} = H^{-1}H^2H^{-1} = I$$

より U はユニタリー変換である. もし $T = H_1U_1$ ともかけたとしたら $H_1 = HUU_1{}^{-1}, H_1 = H_1{}^* = (U_1{}^{-1})^*U^*H^*$ より $H_1{}^2 = HUU_1{}^{-1}(U_1{}^{-1})^*U^*H^* = HH^* = H^2$ なので $H = H_1$. □

定義 42. $A = (a_{ij})$ を n 次実対称行列とし変数 $x_1, ..., x_n$ に関する実係数多項式 $\boldsymbol{x}^tA\boldsymbol{x} = (A\boldsymbol{x}, \boldsymbol{x}) = \sum_{i,j=1}^n a_{ij}x_ix_j$ を二次形式という.

命題 61 (154 ページ)**.** 二次形式 $F(\boldsymbol{x}) = A[\boldsymbol{x}](A = (a_{ij})$ は $a_{ij} = a_{ji}$ より実対称行列であり直交行列で対角化できる) に対し, 適当な直交行列 P を取って $\boldsymbol{x} = P\boldsymbol{y}$ とすれば

$$F(\boldsymbol{x}) = G(\boldsymbol{y}) = P^tAP[\boldsymbol{y}] = \boldsymbol{y}^tP^tAP\boldsymbol{y} = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix}\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \alpha_1{y_1}^2 + \cdots + \alpha_n{y_n}^2$$

$\alpha_1, ..., \alpha_n$ は重複を込めた A の固有値である. 固有値全体 $\subset \mathbb{R}$ に対して

$$\alpha_1, ..., \alpha_p > 0, \quad \alpha_{p+1}, ..., \alpha_{p+q} < 0$$

と正項の数を p, 負項の数を q としまた

$$\alpha_{p+q+1} = \alpha_{p+q+2} = \cdots = \alpha_n = 0$$

とおこう. 組 p, q は $r(A) = p + q$ を満たす数である.

$$P^tAP = \begin{pmatrix} \alpha_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \alpha_p & & & & & & \\ & & & \alpha_{p+1} & & & & & \\ & & & & \ddots & & & & \\ & & & & & \alpha_{p+q} & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{pmatrix}$$

変数を $y_i = \frac{1}{\sqrt{\alpha_i}} z_i (1 \leq i \leq p),\ y_j = \frac{1}{\sqrt{-\alpha_j}} z_j (p+1 \leq j \leq p+q)$ と変えて

$$G(\boldsymbol{y}) = {z_1}^2 + \cdots + {z_p}^2 - {z_{p+1}}^2 - \cdots - {z_{p+q}}^2$$

となる. これをシルベスター標準形という. 標準形は一意に定まる. つまり $\boldsymbol{x} = P\boldsymbol{y}$ の P の取り方に依らず p と q は一定である.

注 30. 「直交行列で対角化可能」という内容においては行列の言葉ではなく線型空間の言葉で言い直したときに基底の取り方が関わって対角化する直交行列が一意に存在する訳ではないことに今更ながら注意しておく.

証明. 70 ページ, 系 [5.6] より $p > s$ と仮定すると自明でない解 $\boldsymbol{x}' = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ を持つので矛盾を導く. また $p < s$ としても矛盾を導く必要があるように思われる. □

定義 43.

$$\forall \boldsymbol{x} \neq 0; F(\boldsymbol{x}) = A[\boldsymbol{x}] \overset{A \text{ はエルミート}}{=} (A\boldsymbol{x}, \boldsymbol{x}) > 0 \Leftrightarrow A \text{ の固有値が全て正 i.e. } p = n$$

のとき二次形式 $F(\boldsymbol{x})$ は正値という.

命題 62. A_k を k 次首座小行列と呼ぶ.

$$A[\boldsymbol{x}] = \boldsymbol{x}^t A\boldsymbol{x} \text{ が正値} \Leftrightarrow \forall k \in \{1, 2, ..., n\}; |A_k| > 0$$

証明. A が正値行列であるために B が正値行列であることを示しているが, これは一般に B が正値 $\Rightarrow A = P^tBP$ が正値であるからである. なぜなら $\boldsymbol{x}^tA\boldsymbol{x} = \boldsymbol{x}^tP^tBP\boldsymbol{x} = (P\boldsymbol{x})^tB(P\boldsymbol{x}) > 0$. □

系 5.

$$A[\boldsymbol{x}] \text{ が負値} \Leftrightarrow \forall k \in \{1, 2, ..., n\}; (-1)^k |A_k| > 0$$

補題 19. (61) における実対称行列 A と P に対し正則行列 P' を

$$P' := P \begin{pmatrix} \frac{1}{\sqrt{\alpha_1}} & & & & & & & \\ & \ddots & & & & & & \\ & & \frac{1}{\sqrt{\alpha_p}} & & & & & \\ & & & \frac{1}{\sqrt{-\alpha_{p+1}}} & & & & \\ & & & & \ddots & & & \\ & & & & & \frac{1}{\sqrt{-\alpha_{p+q}}} & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix}$$

と定義すると

$$P'^t A P' = \begin{pmatrix} I_p & & \\ & -I_q & \\ & & O \end{pmatrix}$$

となる. ここで, n 次対称行列 A が正値行列であるなら前定理 (156 ページ, 定理 [4.3]) より A の任意の固有値が正であるので $p = n$ $(q = 0)$ となり, 上のように適当な正則行列 P' を選ぶことで

$$P'^t A P' = I_n$$

と出来る.

解 22 (158 ページ)**.** 正値対称行列 A は正値実対称行列である. 前補題より, 正値対称行列 A に対して適当な正則行列 Q を取ると $Q^t A Q = I$ となる. $R := Q^{-1}$ に対して $A = Q^{t-1} Q^{-1} = R^t R$. 正則行列の逆行列も正則なので R は正則. 第 4 章末問題 11 より U を直交行列, P を上三角行列として $R = UT$ とかける. $A = P^t U^t U P = P^t P$ が成り立つ.

解 23 (158 ページ)**.** (イ) 平方根がないから $x' = x+y, y' = x-y$ とする. $x'^2 = x^2+y^2+2xy, y'^2 = x^2 + y^2 - 2xy$. $x'^2 - y'^2 = 4xy$ などとして

$$F = \frac{1}{4}x'^2 - \frac{1}{4}y'^2 + x'z + x'u + zu$$

また x, y に対して x', y' という変換を考えたように $z' = z + u, u' = z - u$ とすると

$$F = \frac{1}{4}x'^2 - \frac{1}{4}y'^2 + x'z' + \frac{1}{4}(z'^2 - u'^2) \overset{x'\text{に関して平方完成}}{=} \frac{1}{4}(x' + 2z')^2 - \frac{3}{4}z'^2 - \frac{1}{4}y'^2 - \frac{1}{4}u'^2$$

正項と負項の数をみて符号は $(1, 3)$ である. あるいは

$$F = \frac{1}{4}(x' + 2(u + z))^2 - (u + z)^2 - \frac{1}{4}y'^2 + zu$$

とまず x'について平方完成してから $u' = u + z, z' = u - z$ とおいて

$$F = \frac{1}{4}(x' + 2u')^2 - u'^2 - \frac{1}{4}y'^2 + \frac{1}{4}(u'^2 - z'^2)$$

より符号は $(1,3)$ である. このように (p,q) は一定である.
(ロ) どの変数の順番で平方完成しても符号は一定. x について平方完成すると

$$F = (x+y-z+u)^2 + 3y^2 + 3z^2 - 2u^2 + 6yz + 2zu$$

y について平方完成すると

$$F = (x+y-z+u)^2 + 3(y+z)^2 - 2u^2 + 2zu$$

u について平方完成すると

$$F = (x+y-z+u)^2 + 3(y+z)^2 - 2(u-\frac{z}{2})^2 + \frac{1}{2}z^2$$

符号は $(3,1)$ である.

解 24 (165 ページ)**.** 線織面とは直線の合併集合で表される曲面, 即ち曲面に含まれる任意の点 s に対し s を通る直線が存在する曲面である. ググってみた写真からは一葉双曲面上の任意の点が 2 種類の母線の交点として存在している様子が理解できる. 二つの母線に対して母線の方程式が同じなら一致するか平行であって違う種類なら交点を持つ.

$$\frac{{x_1}^2}{(\frac{d}{a_1})^2} + \frac{{x_2}^2}{(\frac{d}{a_2})^2} - \frac{{x_3}^2}{(\frac{d}{a_3})^2} = 1$$

$$\Leftrightarrow (\frac{x_1}{\frac{d}{a_1}} - \frac{x_3}{\frac{d}{a_3}})(\frac{x_1}{\frac{d}{a_1}} + \frac{x_3}{\frac{d}{a_3}}) = (1 - \frac{x_2}{\frac{d}{a_2}})(1 + \frac{x_2}{\frac{d}{a_2}})$$

が一葉双曲面の方程式である. $t \neq 0$ として

$$(\frac{x_1}{\frac{d}{a_1}} - \frac{x_3}{\frac{d}{a_3}}) : (1 - \frac{x_2}{\frac{d}{a_2}}) = (1 + \frac{x_2}{\frac{d}{a_2}}) : (\frac{x_1}{\frac{d}{a_1}} + \frac{x_3}{\frac{d}{a_3}}) = t : 1$$

$$\Leftrightarrow \begin{cases} 1). \frac{x_1}{d/a_1} - \frac{x_3}{d/a_3} = t(1 - \frac{x_2}{d/a_2}) \\ 2). 1 + \frac{x_2}{d/a_2} = t(\frac{x_1}{d/a_1} + \frac{x_3}{d/a_3}) \end{cases}$$

平面 1) の法線ベクトルは $\begin{pmatrix} \frac{a_1}{d} \\ \frac{a_2}{d}t \\ -\frac{a_3}{d} \end{pmatrix}$, 平面 2) の法線ベクトルは $\begin{pmatrix} \frac{a_1}{d}t \\ -\frac{a_2}{d} \\ \frac{a_3}{d}t \end{pmatrix}$ でありこれらの法線ベクトルと (空間的距離を無視すれば) 直交するベクトルが, 平面の交線 (一葉双曲面をなす母線) の方向ベクトルである. これは外積を用いて計算でき $\frac{1}{d^2}\begin{pmatrix} a_2a_3(1-t^2) \\ 2a_1a_3t \\ (t^2+1)a_1a_2 \end{pmatrix} \neq \mathbf{0}$ である. よって母線の方程式の一つは方向ベクトルと通る点がわかれば決まって

$$\frac{x_1}{\frac{a_2a_3}{d^2}(1-t^2)} = \frac{x_2 - \frac{d}{a_2}}{\frac{2a_1a_3}{d^2}t} = \frac{x_3}{\frac{a_1a_2}{d^2}(t^2+1)}$$

である. 異なる母線を求めるため $s \neq 0$ を任意の実数として

$$(\frac{x_1}{\frac{d}{a_1}} - \frac{x_3}{\frac{d}{a_3}}) : (1 + \frac{x_2}{\frac{d}{a_2}}) = (1 - \frac{x_2}{\frac{d}{a_2}}) : (\frac{x_1}{\frac{d}{a_1}} + \frac{x_3}{\frac{d}{a_3}}) = s : 1$$

$$\Leftrightarrow \begin{cases} 3).\frac{x_1}{d/a_1} - \frac{x_3}{d/a_3} = s(1 + \frac{x_2}{d/a_2}) \\ 4).1 - \frac{x_2}{d/a_2} = s(\frac{x_1}{d/a_1} + \frac{x_3}{d/a_3}) \end{cases}$$

3) の法線ベクトルは $\begin{pmatrix} \frac{a_1}{d} \\ -s\frac{a_2}{d} \\ -\frac{a_3}{d} \end{pmatrix}$, 4) の法線ベクトルは $\begin{pmatrix} s\frac{a_1}{d} \\ \frac{a_2}{d} \\ s\frac{a_3}{d} \end{pmatrix}$ であり, 母線の方向ベクトルは

$\frac{1}{d^2}\begin{pmatrix} (1-s^2)a_2a_3 \\ -2sa_1a_3 \\ (1+s^2)a_1a_2 \end{pmatrix} \neq \mathbf{0}(\because a_i > 0, s \neq 0)$ より母線の方程式は

$$\frac{x_1}{\frac{a_2a_3}{d^2}(1-s^2)} = \frac{x_2 - \frac{d}{a_2}}{-\frac{2a_1a_3}{d^2}s} = \frac{x_3}{\frac{a_1a_2}{d^2}(s^2+1)}$$

である. 次に双曲放物面 ${a_1}^2{x_1}^2 - {a_2}^2{x_2}^2 = b'x_3, b' \neq 0$ の母線方程式を求める. $t \neq 0$ を任意の実数とし双曲放物面の方程式と同値な連立式

$$\begin{cases} a_1x_1 - a_2x_2 = t \\ a_1x_1 + a_2x_2 = \frac{b'x_3}{t} \end{cases} \Leftrightarrow \begin{cases} a_1x_1 = \frac{1}{2}(t + \frac{b'x_3}{t}) \\ a_2x_2 = \frac{1}{2}(\frac{b'x_3}{t} - t) \end{cases}$$

を考える. $\begin{pmatrix} a_1 \\ -a_2 \\ 0 \end{pmatrix} \times \begin{pmatrix} a_1 \\ a_2 \\ -\frac{b'}{t} \end{pmatrix} = \begin{pmatrix} \frac{a_2b'}{t} \\ \frac{b'a_1}{t} \\ 2a_1a_2 \end{pmatrix}$ が母線の方向ベクトルより母線の方程式の一つは $\frac{x_1}{a_2b'/t} =$

$\frac{x_2}{a_1b'/t} = \frac{x_3}{2a_1a_2}$ である. s を 0 を除く任意の実数とし双曲放物面と同値な連立式 $\begin{cases} a_1x_1 - a_2x_2 = \frac{b'x_3}{s} \\ a_1x_1 + a_2x_2 = s \end{cases}$ からは母線の方程式 $\frac{x_1}{a_2b'/s} = \frac{x_2}{-a_1b'/s} = \frac{x_3}{2a_1a_2}$ を得る.

注 31. 柱面, 楕円錐面, 上の二曲面以外の二葉双曲面などの二次曲面は直線を含まない.

ある行列に対して対角化はできないが, 標準的な行列にできることが応用の際に重要となることがある. $\mathbb{K}$ を代数的閉体とし任意の $\mathbb{K}$ 正方行列はジョルダン標準形に相似であることもこの延長線にある話題である. ここでは $\mathbb{K}=\mathbb{R}$ とし最も大事な直交行列の標準化と余力ができたらその応用について述べる.

命題 63. *n 次直交行列 A に対して適当な直交行列 Q を取ると*

$$Q^{-1}AQ = Q^tAQ = \begin{pmatrix} Q_1 & & & & & & \\ & \ddots & & & & & \\ & & Q_m & & & & \\ & & & \pm 1 & & & \\ & & & & \ddots & & \\ & & & & & \pm 1 & \end{pmatrix},\quad Q_i = \begin{pmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{pmatrix}\ (\theta_i \neq 2\pi k, k\in\mathbb{Z})$$

A の固有方程式$\Phi_A(x)$ の重複を込めた複素数解全体 S があり, S の内の r この実数解全体が $\{\pm 1, ..., \pm 1\}$ になる. S の内の虚数解 (ただし複素数解で実数でないもの) は $e^{\theta i}$とその共役 $e^{-\theta i}$である. これらの全体 $\{e^{\theta_1 i}, e^{-\theta_1 i}, ..., e^{\theta_m i}, e^{-\theta_m i}\}$ が上の $Q_1, ..., Q_m$と対応する.

注 32. *任意の n 次実正方行列 A に対し, 適当な実正則行列 P を選ぶと*

$$B = P^{-1}AP = \begin{pmatrix} B_1 & & & & & * & \\ O & B_2 & & & & & \\ \vdots & & \ddots & & & & \\ O & O & \cdots & B_k & & & \\ & & & & \beta_1 & & \\ & & & & & \ddots & \\ O & & & & & & \beta_\ell \end{pmatrix},\quad B_j = \begin{pmatrix} a_j & b_j \\ -b_j & a_j \end{pmatrix}\ (a_j, b_j \in \mathbb{R}, b_j \neq 0)$$

と対角線上の並べ替えを除いてできる. ただし, $\alpha_j = a_j + ib_j, \overline{\alpha_j} = a_j - ib_j$は A の虚固有値 (代数学の基本定理より 234 ページ, [2.7] より固有方程式の虚数解に対してその複素共役も虚数解である), $\beta_1, ..., \beta_\ell$は A の実固有値である.

証明. *n に関する帰納法で示す. もし A に実固有値β_ℓが存在すれば, βに対する固有ベクトルυ_1と独立なようにυ_2, そしてそれらと独立なように$\upsilon_3, ..., \upsilon_n$を取れ ($\upsilon_2, ..., \upsilon_n$は何か A の固有ベクトルのように見えてしまったら誤りで単なる基底の延長定理により保証されるベクトルらである.) 正則行列 $R := \begin{pmatrix}\upsilon_1 & \cdots & \upsilon_n\end{pmatrix}$を作り $R^{-1}AR = \begin{pmatrix} A' & * \\ \boldsymbol{o} & \beta_\ell \end{pmatrix}$(ただし $\boldsymbol{o} = \begin{pmatrix}0 & 0 & \cdots & 0\end{pmatrix}$) とできる.(その際$\epsilon_n{}^t(R^{-1}AR) = \epsilon_n{}^t\beta_\ell$を示せ.) よって $n-1$ 次に帰着され良い. よって A に実固有値がない場合を考える. $\alpha_j = a_j + ib_j (b_j \neq 0)$ が A の固有値, その固有ベクトル p_jのとき$\overline{\alpha_j}$も$\overline{p_j}$を固有ベクトルとする固有値である. p_jと$\overline{p_j}$は独立である.*
なぜなら $cp_j + d\overline{p_j} = o \Rightarrow c = d = 0$ である. 実際, 左辺に A をかけると $c\alpha p = -d\overline{\alpha p}$より $\overline{c\alpha p} = -\overline{d}\alpha p = \frac{|d|^2}{c}\overline{\alpha p}$, 固有ベクトル $p \neq o$ より $|c|^2 = |d|^2$.
もし従属なら$\overline{p_j} = kp_j$となる k があり直ちに $k = \pm 1$. $k = -1$ 即ち $p_j = -\overline{p_j}$のとき $(c-d)p_j = o$ より $c = d$. $c(\alpha p_j + \overline{\alpha p_j}) = o$ は $cp_j(\alpha - \overline{\alpha}) = o$ ということでありαは実数となっては設定

に矛盾するから $c=0$. $k=1$ 即ち $p_j=\overline{p_j}$のときも $cp_j(\alpha-\overline{\alpha})=o$ から $c=0$ である.
$q_{1,j}=\frac{p_j+\overline{p_j}}{2}, q_{2,j}=\frac{p_j-\overline{p_j}}{2i}$とおくとそれらは実ベクトルで $p_j=q_{1,j}+iq_{2,j}, \overline{p_j}=q_{1,j}-iq_{2,j}$より独立である. $Aq_{1,j}=aq_{1,j}-bq_{2,j}, Aq_{2,j}=bq_{1,j}+aq_{2,j}$. $q_{1,j}, q_{2,j}$を第一列, 第二列とする実正則行列 Q をとって $B:=Q^{-1}AQ$ とする. $B\epsilon_1=Q^{-1}AQ\epsilon_1=Q^{-1}Aq_{1,j}=Q^{-1}(aq_{1,j}-bq_{2,j})=a\epsilon_1-b\epsilon_2$, $B\epsilon_2=Q^{-1}AQ\epsilon_2=Q^{-1}Aq_{2,j}=Q^{-1}(bq_{1,j}+aq_{2,j})=b\epsilon_1+a\epsilon_2$であるので, B の第一列と第二列は明らかになり

$$B=\begin{pmatrix} a & b & * \\ -b & a & \\ 0 & 0 & B' \end{pmatrix}$$

である. B' は $n-2$ 次で帰納法の仮定より適当な実正則行列 R' を選んで $R'^{-1}B'R'$ は命題の標準形になる. $R:=\begin{pmatrix} I_2 & O \\ O & R' \end{pmatrix}, P:=QR$ と定義すれば, いま B を B_1 として

$$P^{-1}AP=R^{-1}Q^{-1}AQR=R^{-1}BR=\begin{pmatrix} I_2 & O \\ O & R'^{-1} \end{pmatrix}\begin{pmatrix} a & b & * \\ -b & a & \\ 0 & 0 & B' \end{pmatrix}\begin{pmatrix} I_2 & O \\ O & R'^{-1} \end{pmatrix}$$

より n の場合も成り立つ. □

解 25 (170 ページ)**.** 群論的意味 $T=Z_\varphi Y_\theta Z_\psi$が成り立つことを認めると $T^{-1}={Z_\psi}^{-1}{Y_\theta}^{-1}{Z_\varphi}^{-1}$ でありこれが $Z_{\pi-\psi}Y_\theta Z_{\pi-\varphi}$と等しいこと即ち

$$Y_\theta Z_\psi Z_{\pi-\psi}Y_\theta Z_{\pi-\varphi}Z_\varphi=(Y_\theta Z_\psi Z_{\pi-\psi})^2=E$$

を示す. $Z_\psi Z_{\pi-\psi}=\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$であって

$$(Y_\theta Z_\psi Z_{\pi-\psi})^2=\left(\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right)^2=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

より示せた.

解 26 (170 ページ)**.** (イ)$0\le\theta\le\pi$より$\theta=\frac{\pi}{4}$. $\psi=0$ であり $\cos\varphi=\frac{1}{2}, \sin\varphi=\frac{\sqrt{3}}{2}$より $\varphi=\frac{\pi}{3}$である. 回転角αは$\cos\alpha=\frac{3\sqrt{2}-2}{8}, 0<\alpha<\pi$で定まる. (ロ)$\theta=\frac{\pi}{3}, \varphi=\psi=\frac{\pi}{4}$であり $\cos\alpha=-\frac{1}{4}, \pi<\alpha<\frac{3}{2}\pi$.
三次元の回転行列は各軸周りの回転を 12 通り考えられるある順にかけることで表せる. X 軸周りの回転は$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=X_\theta\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, y 軸周りの回転は$Y_\theta=\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}$, z 軸

周りの回転は $Z_\theta = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$ とおけば三次元の空間内の回転は

$$Z_\gamma Y_\beta X_\alpha = \begin{pmatrix} \cos\beta\cos\gamma & \sin\alpha\sin\beta\cos\gamma - \cos\alpha\sin\gamma & \cos\alpha\sin\beta\cos\gamma + \sin\alpha\sin\gamma \\ \cos\beta\sin\gamma & \sin\alpha\sin\beta\sin\gamma + \cos\alpha\cos\gamma & \cos\alpha\sin\beta\sin\gamma - \sin\alpha\cos\gamma \\ -\sin\beta & \sin\alpha\cos\beta & \cos\alpha\cos\beta \end{pmatrix}$$

でかかれたりまた

$$Z_\alpha Y_\beta Z_\gamma = \begin{pmatrix} \cos\alpha\cos\beta\cos\gamma - \sin\alpha\sin\gamma & -\cos\alpha\cos\beta\sin\gamma - \sin\alpha\cos\gamma & \cos\alpha\sin\beta \\ \sin\alpha\cos\beta\cos\gamma + \cos\alpha\sin\gamma & -\sin\alpha\cos\beta\sin\gamma + \cos\alpha\cos\gamma & \sin\alpha\sin\beta \\ -\sin\beta\cos\gamma & \sin\beta\sin\gamma & \cos\beta \end{pmatrix}$$

を [9] では取り上げている.

解 27. (ハ) 与えられた行列を A としその固有値を求める. $\Phi_A(x) = \begin{vmatrix} x+3 & 2 & 2 & -1 \\ -2 & x-3 & -2 & 0 \\ x & 1 & x & 0 \\ x^2+x-2 & 2x-2 & 2x-2 & 0 \end{vmatrix} =$
$\begin{vmatrix} -2 & x-3 & -2 \\ x & 1 & x \\ x^2+x-2 & 2x-2 & 2x-2 \end{vmatrix} = \begin{vmatrix} -x^2+3x-2 & x-3 & -x^2+3x-2 \\ 0 & 1 & 0 \\ -x^2+3x-2 & 2x-2 & -2x^2+4x-2 \end{vmatrix} = \begin{vmatrix} -x^2+3x-2 & -x^2+3x-2 \\ 0 & -x^2+x \end{vmatrix} =$
$\begin{vmatrix} -x^2+3x-2 & 0 \\ 0 & -x^2+x \end{vmatrix} = x(x-1)^2(x-2)$ であるので固有値λは $0, 1, 2$ である. まず 0 に対する固有ベクトルを計算する. 固有値 1 に対しては独立な固有ベクトルを 2 個存在することが問題文から示唆される. $A\boldsymbol{x} = \lambda\boldsymbol{x}$ が自明でない解 $\boldsymbol{x}$ を持つ $\Leftrightarrow$ $(\lambda E - A)\boldsymbol{x} = \boldsymbol{0}$ が解 $\boldsymbol{x} \neq \boldsymbol{o}$ を持つなので

$$\begin{pmatrix} 3 & 2 & 2 & -1 \\ -2 & -3 & -2 & 0 \\ -3 & -1 & -2 & 1 \\ 4 & 2 & 2 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \boldsymbol{0}$$

行基本変形して $\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \boldsymbol{0}$ を満たす $\boldsymbol{x}$ は $\begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix}$ である. 同様に固有値 1, 2 に対する固有ベクトルを計算して $P = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -2 \\ -1 & 0 & -1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$

解 28. 対称行列, エルミート行列に対する対角化行列をそれぞれ P や U でかくことにする. 独立な固有ベクトルはノルム 1 にする必要 (必要十分) がある. (イ) 満足する行列の一つに

は $P=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&-1\\0&\sqrt{2}&0\\1&0&1\end{pmatrix}$ (ロ)$P=\begin{pmatrix}1/\sqrt{2}&1/\sqrt{3}&1/\sqrt{6}\\-1/\sqrt{2}&1/\sqrt{3}&1/\sqrt{6}\\0&1/\sqrt{3}&-2/\sqrt{6}\end{pmatrix}$ (ハ)$P=\begin{pmatrix}-1/2&1/\sqrt{2}&1/2\\1/2&1/\sqrt{2}&-1/2\\1/\sqrt{2}&0&1/\sqrt{2}\end{pmatrix}$

(ニ)$P=\begin{pmatrix}\frac{1}{2\sqrt{2}}&\frac{1}{2\sqrt{2}}&\frac{\sqrt{3}}{2}\\\frac{\sqrt{3}}{2\sqrt{2}}&\frac{\sqrt{3}}{2\sqrt{2}}&-\frac{1}{2}\\\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\end{pmatrix}$ (ホ)$\begin{vmatrix}x-3&-i&1\\i&x-5&-i\\1&i&x-3\end{vmatrix}=(x-2)(x-3)(x-6)$ より$\lambda=2,3,6$ で ある. 2 に対する固有ベクトルでノルム 1 のものを計算する.

$$\begin{pmatrix}-1&-i&1\\i&-3&-i\\1&i&-1\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\mathbf{0}$$

を満たす$\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}1\\0\\1\end{pmatrix}$を規格化すると$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\end{pmatrix}$. $\lambda=3$ については$\frac{1}{\sqrt{3}}\begin{pmatrix}-i\\1\\i\end{pmatrix}$を取る等して U を作 る (へ) 固有方程式は

$$\begin{vmatrix}x-a&-i&-1&i\\i&x-a&-i&-1\\-1&i&x-a&-i\\-i&-1&i&x-a\end{vmatrix}$$

$$\overset{\text{第一列を第三列に加え, 第二列を第四列に加える}}{=}\begin{vmatrix}x-a&-i&x-a-1&0\\i&x-a&0&x-a-1\\-1&i&x-a-1&0\\-i&-1&0&x-a-1\end{vmatrix}$$

$$\overset{\text{第四行}\times(-1)\text{ を第二行に加え, 第三行も同じく}}{=}\begin{vmatrix}x-a+1&-2i&0&0\\2i&x-a+1&0&0\\-1&i&x-a-1&0\\-i&-1&0&x-a-1\end{vmatrix}$$

$$\begin{vmatrix}A&O\\C&D\end{vmatrix}\overset{=|A||D|}{=}\begin{vmatrix}x-a+1&-2i\\2i&x-a+1\end{vmatrix}\begin{vmatrix}x-a-1&0\\0&x-a-1\end{vmatrix}=(x-a+3)(x-a-1)^3$$

$a+1$ に対する正規直交基底をなす固有ベクトルは 3 個存在することが必要十分である.

一つには $U=\begin{pmatrix}1/2&1/\sqrt{2}&0&1/2\\i/2&0&1/\sqrt{2}&-i/2\\-1/2&1/\sqrt{2}&0&-1/2\\-i/2&0&1/\sqrt{2}&i/2\end{pmatrix}$ となる.

(ト)n 次行列 A に対して n が偶数か奇数かで場合分けせよ. 今 n を偶数とすると固有方程式 $\Phi_A(x)=|xE-A|$

$$\overset{i\text{ 行}\times x\text{ を }n-i+1\text{ 行に加える}}{=}\begin{vmatrix} x & 0 & \cdots & 0 & 0 & \cdots & 0 & -1 \\ 0 & x & \cdots & 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & x & -1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & x^2-1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & x^2-1 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ x^2-1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \end{vmatrix}$$

$$\overset{80\text{ ページ,[2.3] で行の置換}}{=}(-1)^{\frac{n(n-1)}{2}}\begin{vmatrix} x^2-1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ 0 & x^2-1 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & x^2-1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & x & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & x & \cdots & 0 & 0 & \cdots & -1 & 0 \\ x & 0 & \cdots & 0 & 0 & \cdots & 0 & -1 \end{vmatrix} = (-1)^{\frac{n(n-1)}{2}}(-1)^{\frac{n}{2}}(x-1)^{\frac{n}{2}}(x+1)^{\frac{n}{2}}$$

であるから固有値は 1 と -1 である. 固有値 1 に対する $\frac{n}{2}$ 本の独立な固有ベクトルを計算する.

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & -1 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & -1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & -1 & \cdots & 0 & 0 & \cdots & 1 & 0 \\ -1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n/2} \\ x_{n/2+1} \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} = \mathbf{0}$$

を解くと一つには, $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\\vdots\\0\\0\\\vdots\\0\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\\vdots\\0\\0\\\vdots\\1\\0\end{pmatrix}, ..., \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\\vdots\\1\\1\\\vdots\\0\\0\end{pmatrix}$ であろう. 固有値 -1 に対する $n/2$ 本の独立な

固有ベクトルは, $\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\0\\\vdots\\0\\0\\\vdots\\0\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}0\\-1\\\vdots\\0\\0\\\vdots\\1\\0\end{pmatrix}, ..., \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\\vdots\\-1\\1\\\vdots\\0\\0\end{pmatrix}$ として上に挙げたベクトル $\boldsymbol{u}_i(1 \leq i \leq n)$ に対し $U = \begin{pmatrix}\boldsymbol{u}_1 & \cdots & \boldsymbol{u}_n\end{pmatrix}$ とおけば U は直交行列で A を対角化する.

n が奇数の場合, $\Phi_A(x) = |xE - A| = (-1)^{\frac{(n^2-1)}{2}}(x-1)^{\frac{n+1}{2}}(x+1)^{\frac{n-1}{2}}$ となる. n が偶数の時と同様にし, 固有値 1 に対する $\frac{(n+1)}{2}$ 本の正規直交基底をなす固有ベクトルで独立なものを計算すると

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\\vdots\\0\\0\\0\\\vdots\\0\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\\vdots\\0\\0\\0\\\vdots\\1\\0\end{pmatrix}, ..., \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\\vdots\\1\\0\\1\\\vdots\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\\vdots\\0\\1\\0\\\vdots\\0\\0\end{pmatrix}$$

であり固有値 -1 に対する $\frac{(n-1)}{2}$ 本の正規直交基底をなす固有ベクトルは

$$\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\0\\\vdots\\0\\0\\0\\\vdots\\0\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}0\\-1\\\vdots\\0\\0\\0\\\vdots\\1\\0\end{pmatrix}, ..., \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\\vdots\\-1\\0\\1\\\vdots\\0\\0\end{pmatrix}$$

となり以上の列ベクトルを並べて直交行列 U を作る.

解 29.

$$(イ)\exists k\ s.t.\ T^k = O \Leftrightarrow \forall n\ s.t. T^n = O$$

これは三角化を使うと示せることはご存知の通りである. T の n 次行列を A とする. 任意の正方行列は適当なユニタリー行列 U を用いて三角化にすることができる. $\alpha_1, ..., \alpha_n$ を A の

固有値とする. $U^{-1}AU = \begin{pmatrix} \alpha_1 & & * \\ & \ddots & \\ O & & \alpha_n \end{pmatrix}$ の両辺を k 乗し $U^{-1}A^kU = \begin{pmatrix} {\alpha_1}^k & & * \\ & \ddots & \\ O & & {\alpha_n}^k \end{pmatrix} = O$ よ
り各固有値は 0 である. よって $U^{-1}A^nA = O$ であって $U \neq O$ より $A^n = O$ である.

(ロ) T が冪零変換 $\Leftrightarrow$ T の固有値が全て 0

(イ) ですでに示している. T の行列 A の対角線には A の固有値が並ぶこれは T の固有値に対応している.

注 33. 以下, 別証明とその準備

命題 64. $A \in M_n(\mathbb{C})$ の固有値を$\lambda_1, ..., \lambda_n$とする. $\mathbb{C}$ 係数多項式 $p(X) = a_0 + a_1X + \cdots a_mX^m$に対し $p(A)$ の固有値は $p(\lambda_1), ..., p(\lambda_n)$ である.

証明. 適当なユニタリー行列 P があって $P^{-1}AP = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ となる.

$$\begin{aligned} P^{-1}p(A)P &= P^{-1}(a_0E_n + a_1A + \cdots + a_mA^m)P \\ &= a_0E_n + a_1B + \cdots + a_mB^m \\ &= \begin{pmatrix} a_0 & & \\ & \ddots & \\ & & a_0 \end{pmatrix} + \begin{pmatrix} a_1\lambda_1 & & * \\ & \ddots & \\ & & a_1\lambda_n \end{pmatrix} + \cdots + \begin{pmatrix} a_m{\lambda_1}^m & & * \\ & \ddots & \\ & & a_m{\lambda_n}^m \end{pmatrix} = \begin{pmatrix} p(\lambda_1) & & * \\ & \ddots & \\ & & p(\lambda_n) \end{pmatrix} \end{aligned}$$

よって相似変換では固有値も不変なので $p(A)$ の固有値は $p(\lambda_1), ..., p(\lambda_n)$ である. 簡単な例としてある $m \in \mathbb{N}$ に対し $A^m = E_n$なら A の固有値の m 乗は 1 であることが分かる. なぜなら $p(A) = A^m$の固有値は${\lambda_1}^m, ..., {\lambda_n}^m = 1$. □

命題 65. $A \in M_n(\mathbb{C})$ に対する固有方程式$\Phi_A(x) = |xE_n - A|$ について$\Phi_A(A) = O$ である.

解 30. $A^m = O$ なる m で最小のものを取ると $A^{m-1} \neq O$. α_iを A の成分で定まる数とし $\Phi_A(A) = A^n + \alpha_1A^{n-1} + \alpha_2A^{n-2} + \cdots + \alpha_{n-1}A + \alpha_nE_n = O$ が成り立つ. 両辺に A^{m-1}をかけると$\alpha_nA^{m-1} = O$ より$\alpha_n = 0$ であり順に$\alpha_{n-1} = 0, ..., \alpha_1 = 0$ を得るから $A^n = O$ である.

解 31. $\mathbb{K} = \mathbb{C}$ のときの証明は量子力学の言葉で与えた. 本問は $\mathbb{K} = \mathbb{R}$ の場合でありやはり A の任意の固有空間は B 不変であることが効く. αを A の固有値とする. $AB = BA$ より $A(B\boldsymbol{x}) = B\alpha\boldsymbol{x} = \alpha(B\boldsymbol{x})$ なので $B\boldsymbol{x}$ もαに対する固有ベクトルであり A の固有空間 W_α は B 不変ということである. 実対称行列 A は直交行列で対角化可能である. A の固有値 $\alpha_1, ..., \alpha_n$, 対応する固有空間を $W_{\alpha_1}, ..., W_{\alpha_n}$とすると $V = W_{\alpha_1} \oplus \cdots \oplus W_{\alpha_n}$である. ただし A の線型変換 T に対して定義されている線型空間とした. B を各 W_{α_i}に制限することを考える. B も実対称行列なので B を W_{α_i}に制限した写像 S の行列も実対称行列であるから, それも W_{α_i}の正規直交基底を並べた行列によって対角化できる. 各 W_{α_i}におけるこのような正規直交基底を集めたものは V の基底をなし, それを並べて出来る P は A と B を同時対角化する.

解 32. (イ) $A = -A^t$のとき A を交代行列という. 交代行列は正規なのである直交行列 U で対角化出来るので $D := U^{-1}AU = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}$ となる. $D^t = U^{-1}(-A)U = \begin{pmatrix} \overline{\alpha_1} & & \\ & \ddots & \\ & & \overline{\alpha_n} \end{pmatrix}$ より$\alpha_i = -\overline{\alpha_i}$であるから実交代行列の固有値は純虚数または 0 である. (ロ) 実交代行列のランクは偶数である. 実行列の固有方程式は $\mathbb{R}$ 上の多項式なので代数学の基本定理よりαが固有値なら$\overline{\alpha}$も固有方程式の解であり, $\boldsymbol{x}$ がαに対する固有ベクトルなら $A\overline{\boldsymbol{x}} = \overline{A\boldsymbol{x}} = \overline{\alpha\boldsymbol{x}}$より $\overline{\boldsymbol{x}}$は$\overline{\alpha}$に対する固有ベクトルである. 逆も明らかでよって次の固有空間は一致する.

$$\dim W_\alpha = \dim W_{\overline{\alpha}}$$

実交代行列の 0 でない固有値は純虚数であるから 0 以外の固有値に対する固有空間の次元を全て足すとそれは $\sum_i 2\dim W_{\alpha_i}$で偶数. 一般に対角化可能な行列 A について $r(A)$ は A のノンゼロの固有値の数に等しいから示せた.

注 34. n 次正方行列 A に対し, $r(A)$ は A の重複度を込めたノンゼロの固有値の数以上である. 特に A が対角化できるとき等号が成り立つ.

証明. $\mathrm{Ker}(A) = \{v \in \mathbb{C}^n | Av = \mathbf{0}\}$ とかく. このvは固有値 0 に対する固有ベクトルとみれるので (即ち $\mathrm{Ker}(A) = W_0$) $\dim \mathrm{Ker}(A) \leq$ 重複度を込めたゼロ固有値の数. $r(A) = n - \dim \mathrm{Ker}(A) \geq$ ノンゼロの固有値の数である. A が対角化可能なときの必要十分条件 (すなわち, 各固有空間の次元がその固有値の重複度に一致する) より $\dim W_0$は固有値 0 の重複度と等しいので等号が成立する. 以下, 別証明である. 対角化可能行列 A に対しある正則行列 P があって $B = P^{-1}AP$ と対角化. $A = PBP^{-1}$. P は正則であるから $r(A) = r(B) =$ ノンゼロの A の固有値の数である. □

解 33. (イ, ロ, ハ) $B = (b_{ij}) = U^*AU = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ O & & \lambda_n \end{pmatrix}$ に対し

$$BB^* = U^*AU(U^*AU)^* = U^*AA^*U$$

よって

$$\mathrm{tr}(BB^*) = \mathrm{tr}(U^*AA^*U) \overset{\text{トレースはユニタリー変換で不変}}{=} \mathrm{tr}(AA^*) = \sum_{i,j=1}^n |a_{ij}|^2$$

$$\sum_{i,j=1}^n |a_{ij}|^2 = \sum_{i,j=1}^n |b_{ij}|^2 \geq \sum_{i=1}^n |b_{ii}|^2 = \sum_{i=1}^n |\lambda_i|^2$$

等号が成り立つ必要十分条件は B が対角行列であることだから A がユニタリー行列で対角化でき即ち A が正規行列であること.

解 34. エルミート行列 A に対しあるユニタリー行列 U があって $U^*AU = \begin{pmatrix} \lambda_1 & & O \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ と

なる.

$$\boldsymbol{x}^t A\overline{\boldsymbol{x}} = \boldsymbol{x}^t UU^* AUU^*\overline{\boldsymbol{x}} = \boldsymbol{y}^t \begin{pmatrix} \lambda_1 & & O \\ & \ddots & \\ O & & \lambda_n \end{pmatrix} \overline{\boldsymbol{y}} \quad \boldsymbol{y}^t := \boldsymbol{x}^t U$$

$\alpha = \max \lambda_i$, $\beta = \min \lambda_i$とおくと任意の $\boldsymbol{x}$ に対し

$$\boldsymbol{x}^t A\overline{\boldsymbol{x}} \leq \boldsymbol{y}^t \begin{pmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{pmatrix} \overline{\boldsymbol{y}} = \alpha \boldsymbol{y}^t \overline{\boldsymbol{y}} = \alpha \boldsymbol{x}^t UU^* \overline{\boldsymbol{x}} = \alpha \|\boldsymbol{x}\|^2$$

同様に $\forall i; \lambda_i = \beta$とすると

$$\beta \|\boldsymbol{x}\|^2 \leq \boldsymbol{x}^t A\overline{\boldsymbol{x}} \leq \alpha \|\boldsymbol{x}\|^2$$

ここで $\boldsymbol{x} = \boldsymbol{\epsilon}_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ とすれば

$$\beta \leq a_{ii} \leq \alpha$$

である.

解 35. (イ) $x^2 + 2y^2 + 3z^2 + 2xy - 2xz + 2yz = (x + y - z)^2 + y^2 + 2z^2 + 4yz = (x + y - z)^2 + (y + 2z)^2 - 2z^2 = (x + y - z)^2 + (y + 2z)^2 - (\sqrt{2}z)^2$. (ロ) $(x + y)^2 + y^2 - z^2 - u^2 - 2yz + 2yu - 6zu = (x + y)^2 + (y - z + u)^2 - 2z^2 - 4zu - 2u^2 = (x + y)^2 + (y - z + u)^2 - (\sqrt{2}z + \sqrt{2}u)^2$と各変数を順に平方完成する.

解 36. 行列 X^2の (i, i) 成分は

$$\begin{pmatrix} x_{i1} & x_{i2} & \cdots & x_{in} \end{pmatrix} \begin{pmatrix} x_{1i} \\ x_{2i} \\ \vdots \\ x_{ni} \end{pmatrix} = {x_{ii}}^2 + \sum_{k \neq i} x_{ik} x_{ki}$$

$$\mathrm{tr}(X^2) = \sum_{i=1}^{n} ({x_{ii}}^2 + \sum_{k \neq i}^{n} x_{ik} x_{ki}) = \sum_{i=1}^{n} {x_{ii}}^2 + \sum_j \sum_{k \neq j} x_{jk} x_{kj}$$

$$= \sum_{i=1}^{n} {x_{ii}}^2 + 2 \sum_j \sum_{k>j} x_{jk} x_{kj} = \sum_{i=1}^{n} {x_{ii}}^2 + \sum_j \sum_{k>j} \frac{1}{2} \left((x_{jk} + x_{kj})^2 - (x_{jk} - x_{kj})^2 \right)$$

よって正の項数は $n + \{1 + 2 + \cdots + (n-2) + (n-1)\} = \frac{n^2+n}{2}$, 負の項数は$\frac{n^2-n}{2}$である.

解 37. A を n 次行列とし n に関する帰納法で示す. $n = 1$ のとき明らかに成立. $n - 1$ のとき正しいと仮定する. $A = \begin{pmatrix} A_0 & \boldsymbol{b} \\ \boldsymbol{b}^* & a_{nn} \end{pmatrix}$とおくと A が正値エルミートならば A_0も正値エルミート

である. 実際, $A^* = \begin{pmatrix} {A_0}^* & \boldsymbol{b} \\ \boldsymbol{b}^* & \overline{a_{nn}} \end{pmatrix}$ より $A^* = A$ のとき ${A_0}^* = A_0$である. また $\boldsymbol{x} \in \mathbb{C}^{n-1}, \boldsymbol{x} \neq \boldsymbol{0}$ に対し

$$\boldsymbol{x}^t A_0 \overline{\boldsymbol{x}} = \begin{pmatrix} \boldsymbol{x}^t & 0 \end{pmatrix} \begin{pmatrix} A_0 & \boldsymbol{b} \\ \boldsymbol{b}^* & a_{nn} \end{pmatrix} \begin{pmatrix} \overline{\boldsymbol{x}} \\ 0 \end{pmatrix} \underset{A \text{ は正値}}{>} 0$$

であるからである. 146 ページ, [2.9] より正値エルミート行列はすべての固有値が正より, すべての固有値の積と等しい行列式の値が正である. よって一般に正値エルミート行列は正則であり逆行列が存在する. A_0は正則. また A_0が正値エルミートのとき, ${A_0}^{-1}$も正値エルミートである. 実際 $({A_0}^{-1})^* = ((A_0)^*)^{-1} = (A_0)^{-1}$よりエルミート. また任意の $\boldsymbol{x}, \boldsymbol{y} := \overline{(A_0)^{-1}}\boldsymbol{x}$ に対して

$$\boldsymbol{x}^t (A_0)^{-1} \overline{\boldsymbol{x}} = \boldsymbol{y}^t (A_0)^* (A_0)^{-1} A_0 \overline{\boldsymbol{y}} = \boldsymbol{y}^t A_0 \overline{\boldsymbol{y}}$$

であるからである. ここで

$$A = \begin{pmatrix} A_0 & \boldsymbol{b} \\ \boldsymbol{b}^* & a_{nn} \end{pmatrix} = \begin{pmatrix} A_0 & \boldsymbol{0} \\ \boldsymbol{b}^* & a_{nn} - \boldsymbol{b}^* (A_0)^{-1} \boldsymbol{b} \end{pmatrix} \begin{pmatrix} E_{n-1} & (A_0)^{-1}\boldsymbol{b} \\ \boldsymbol{0}^t & 1 \end{pmatrix}$$

において行列式を取る. 以上で色々示したことで次の最初の不等号で帰納法の仮定を使える.

$$\det A = \det A_0 (a_{nn} - \boldsymbol{b}^* (A_0)^{-1} \boldsymbol{b}) \leq a_{11} \cdots a_{nn} - \det A_0 (\boldsymbol{b}^* (A_0)^{-1} \boldsymbol{b}) \leq a_{11} \cdots a_{nn}$$

等号が成り立つ為には $\det A_0 = a_{11} \cdots a_{n-1,n-1}, \boldsymbol{b}^* (A_0)^{-1} \boldsymbol{b} = 0$ が必要十分で帰納法の仮定よりこれは A_0が対角行列であること及び $\boldsymbol{b} = \boldsymbol{0}$ と同値. よって A は対角行列. 即ち n の場合の等号成立の必要十分条件も A が対角行列であることである.

解 38. もし A が正則でないなら $|A| = 0$ より明らか. A は正則行列とする. 任意の A に対し $A^t\overline{A}$は正値エルミートである. 実際

$$(A^t \overline{A})^* = A^t \overline{A}$$

であり

$$(A^t \overline{A} \boldsymbol{x}, \boldsymbol{x}) = (A^t \overline{A} \boldsymbol{x})^t \overline{\boldsymbol{x}} = \boldsymbol{x}^t A^* A \overline{\boldsymbol{x}} = (\overline{A}\boldsymbol{x}, \overline{A}\boldsymbol{x}) = \|\overline{A}\boldsymbol{x}\|^2 > 0$$

であるから. ($\because$ A は正則より $\|\overline{A}\boldsymbol{x}\|^2 \neq 0, \forall \boldsymbol{x} \neq \boldsymbol{0}$)

$$A^t \overline{A} = \begin{pmatrix} \boldsymbol{a}_1 {}^t\overline{\boldsymbol{a}_1} & \cdots & \boldsymbol{a}_1 {}^t\overline{\boldsymbol{a}_n} \\ & \ddots & \\ \boldsymbol{a}_n {}^t\overline{\boldsymbol{a}_1} & \cdots & \boldsymbol{a}_n {}^t\overline{\boldsymbol{a}_n} \end{pmatrix} = \begin{pmatrix} (\boldsymbol{a}_1, \boldsymbol{a}_1) & \cdots & (\boldsymbol{a}_1, \boldsymbol{a}_n) \\ & \ddots & \\ (\boldsymbol{a}_n, \boldsymbol{a}_1) & \cdots & (\boldsymbol{a}_n, \boldsymbol{a}_n) \end{pmatrix}$$

より $(A^t\overline{A})_{i,i} = (\boldsymbol{a}_i, \boldsymbol{a}_i)$. 前問より $\det A^t\overline{A} \leq \|\boldsymbol{a}_1\|^2 \cdots \|\boldsymbol{a}_n\|^2$が成立. ここで

$$\det A^t \overline{A} = \det A^t \det \overline{A} = \det A \overline{\det A} = |\det A|^2$$

なので示せた. 等号成立条件は $A^t\overline{A}$が対角行列即ち $(\boldsymbol{a}_i, \boldsymbol{a}_j) = k\delta_{ij}, k \in \mathbb{C}$ である.

注 35. $A \in M_n(\mathbb{C})$ に対して $\det \overline{A} = \overline{\det A}$である. またユニタリー行列式は絶対値 1 の複素数である. なぜなら

$$\begin{aligned}
\det A^* &= \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) A^*_{1\sigma(1)} \cdots A^*_{n\sigma(n)} \\
&= \sum_{\sigma} \operatorname{sgn}(\sigma) \overline{A^t_{1\sigma(1)}} \cdots \overline{A^t_{1\sigma(1)}} \\
&= \overline{\sum_{\sigma} \operatorname{sgn}(\sigma) A^t_{1\sigma(1)} \cdots A^t_{n\sigma(n)}} = \overline{\det A^t}
\end{aligned}$$

より

$$\overline{\det A} = \det \overline{A}^t = \det \overline{A}$$

U をユニタリー行列とすると

$$1 = \det E = \det(U^* U) = \det U^* \det U = \overline{\det U^t} \det U = |\det U|^2$$

より.

2.4 [9] 第 6 章

解 39 (179 ページ)**.** (イ) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & (x-2)^2 \end{pmatrix}$ (ロ) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-3)(x-2)^2 \end{pmatrix}$

解 40 (183 ページ)**.** 任意の $\mathbb{C}$ 正方行列 A と A^tとは相似であることを示す. [1.8] より $xE-A$ と $xE-A^t$が対等であることを示す. $xE-A$ の単因子標準形を $J(x)$ とすると適当な可逆行列 $P(x), Q(x)$ が存在して

$$P(x)(xE-A)Q(x) = J(x)$$

となる. よって

$$Q(x)^t(xE-A^t)P(x)^t = J(x) = P(x)(xE-A)Q(x)$$

$$xE-A^t = (Q(x)^t)^{-1}P(x)(xE-A)Q(x)(P(x)^t)^{-1}$$

明らかに $(Q(x)^t)^{-1}P(x), Q(x)(P(x)^t)^{-1}$は可逆行列である.

注 36. 行列の相似性は係数体の取り方によらない. 即ち $\mathbb{L}$ を体 $\mathbb{K}$ を含む体とするとき, 行列 A, B が $\mathbb{K}$ 相似であることと $\mathbb{L}$ 相似であることは同値である. よって与えられた二つの行列の相似性を判定するときはそれらの行列を代数閉体, 特に $\mathbb{C}$ 上の行列としジョルダン標準形を計算できる. さて上の別解を以下で与える. $J = P^{-1}AP$ を任意の $A \in M_n(\mathbb{C})$ のジョルダン標準形とする. 両辺の転置を取ると $J^t = P^tA^t(P^{-1})^t$より J^tと A^tは相似である. 相似という関係は同値関係なので任意のジョルダン標準形 $J \in M_m$に対して J と J^tが相似であることを各ジョルダンセルについて示す. $R = (r_{ij}) \in M_m$を $i+j = m+1$ のとき成分 1, $i+j \neq m+1$ のとき成分 0 の行列とするとこれは $R^{-1} = R$ を満たし可逆で $J^t = RJR$ である.

解 41. (イ)[9]181 ページ, 定理 [1.8] を認めると $xE-A$ と $xE-B$ の単因子は $1, (x-1)^2$であり等しいので A と B は相似であることが分かる. $B = P^{-1}AP$ となる $P = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$が求められたのでここに記録しておく.

(ロ)$AP = PB \Leftrightarrow \begin{cases} A\boldsymbol{p}_1 = \boldsymbol{0} \\ A\boldsymbol{p}_2 = \boldsymbol{p}_1 \\ A\boldsymbol{p}_3 = \boldsymbol{p}_2 \end{cases}$ であることを利用する. $P = \begin{pmatrix} \boldsymbol{p}_1 & \boldsymbol{p}_2 & \boldsymbol{p}_3 \end{pmatrix}$の探求作業を軽快に行うその準備として $A\boldsymbol{x} = \boldsymbol{b} := \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$が解をもつ必要十分条件を調べる.

$$\begin{pmatrix} 4 & -1 & 1 & b_1 \\ 8 & -2 & 2 & b_2 \\ -6 & 1 & -2 & b_3 \end{pmatrix} \overset{rankA \text{ が判明するまで行基本変形, この場合 } rankA=2}{\rightarrow} \begin{pmatrix} 4 & -1 & 1 & b_1 \\ 0 & 0 & 0 & b_2-2b_1 \\ -6 & 1 & -2 & b_3 \end{pmatrix}$$

よって

$$b_2 = 2b_1$$

のとき $A\boldsymbol{x} = \boldsymbol{b}$ は解をもつ. そのような $\boldsymbol{b}$ に対して, $\boldsymbol{x}$ は s を任意定数として

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} s \\ 2s - 2b_1 - b_3 \\ -2s - b_1 - b_3 \end{pmatrix}$$

とかける.

$$\begin{cases} A\boldsymbol{p}_1 = \boldsymbol{0} \\ A\boldsymbol{p}_2 = \boldsymbol{p}_1 \\ A\boldsymbol{p}_3 = \boldsymbol{p}_2 \end{cases}$$

が解をもつように注意して $\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3$ を選ぶと

$$\boldsymbol{p}_1 = \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}$$

$$\boldsymbol{p}_2 = \begin{pmatrix} s \\ 2s \\ -2s + 1 \end{pmatrix} \overset{s=1 \text{ と選ぶ}}{=} \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$$

$$\boldsymbol{p}_3 = \begin{pmatrix} s' \\ 2s' - 1 \\ -2s' \end{pmatrix} \overset{s'=1 \text{ と選ぶ}}{=} \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix}$$

よって一意性をもたないものの変換行列 P は

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 1 \\ -2 & -1 & -2 \end{pmatrix}$$

が挙げられる. $B = P^{-1}AP$ を満たす A, B が与えられたとき P を計算するこの方法は, ジョルダン標準形への変換行列を計算するときに同様に使われる. また本問の B は A のジョルダン標準形である.

解 42 (191 ページ)**.**

$$\text{イ}. \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} P = \begin{pmatrix} -1 & -1/2 & -2 \\ -2 & -1 & -3 \\ 2 & 0 & 2 \end{pmatrix} \quad \text{ロ}. J = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} P = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

解 43 (196 ページ)**.** $T : y \mapsto \frac{dy}{dx}$の行列は$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -4 & 0 & 3 \end{pmatrix}$でこの固有値は 1 と -2 (重複度 2) より $y = \alpha e^{-x} + \beta e^{2x} + \gamma x e^{2x}$

解 44 (201 ページ)**.** (イ) 与えられた行列を A とする. $|xE-A| = \begin{vmatrix} x+2 & 1 & 2 & -1 \\ -5 & x-3 & -4 & 1 \\ -1 & 0 & x-1 & 1 \\ 3 & 1 & 2 & x-2 \end{vmatrix} =$

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

$$(x-1) \begin{vmatrix} x-1 & 0 & 0 \\ -7 & x-3 & -4 \\ 3 & 1 & x+1 \end{vmatrix} = (x-1)^4$$

$$A - E_4 = \begin{pmatrix} -3 & -1 & -2 & 1 \\ 5 & 2 & 4 & -1 \\ 1 & 0 & 0 & -1 \\ -3 & -1 & -2 & 1 \end{pmatrix} \to \begin{pmatrix} -3 & -1 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

なので $r_1(1) = \mathrm{rank}(A - 1E) = 2$. $r_2(1) = \mathrm{rank}(A - 1E)^2 = 1, r_3(1) = \mathrm{rank}(A - 1E)^3 = 0$. m 次ジョルダンセル $J_m(\lambda_i)$ の個数を $c_m(\lambda_i)$ とかくと終節で述べる定理 A より

$$c_m(1) = 0 \ (m \geq 5), \ c_1(1) + 2c_2(1) + 3c_3(1) + 4c_4(1) = 4$$

定理 B より

$$c_1(1) = r_0(1) - 2r_1(1) + r_2(1) = 4 - 2 \times 2 + 1 = 1$$

$$c_2(1) = r_1(1) - 2r_2(1) + r_3(1) = 2 - 2 \times 1 + 0 = 0$$

$$c_3(1) = r_2(1) - 2r_3(1) + r_4(1) = 1 - 2 \times 0 + 0 = 1$$

$$c_4(1) = 0$$

よって

$$J = P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = J_1(1) \oplus J_3(1)$$

または

$$J = P'^{-1}AP' = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = J_3(1) \oplus J_1(1)$$

変換行列 P を計算するには $AP = PJ$ を第一に利用することが賢明である. 正則行列 $P = \begin{pmatrix} \boldsymbol{p}_1 & \boldsymbol{p}_2 & \boldsymbol{p}_3 & \boldsymbol{p}_4 \end{pmatrix}$ とおく. $AP = PJ$ であって $J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ であるから,

$$\begin{cases} A\boldsymbol{p}_1 = \boldsymbol{p}_1 \\ A\boldsymbol{p}_2 = \boldsymbol{p}_2 \\ A\boldsymbol{p}_3 = \boldsymbol{p}_2 + \boldsymbol{p}_3 \\ A\boldsymbol{p}_4 = \boldsymbol{p}_3 + \boldsymbol{p}_4 \end{cases} \Leftrightarrow \begin{cases} (A-E)\boldsymbol{p}_1 = \boldsymbol{0} \\ (A-E)\boldsymbol{p}_2 = \boldsymbol{0} \\ (A-E)\boldsymbol{p}_3 = \boldsymbol{p}_2 \\ (A-E)\boldsymbol{p}_4 = \boldsymbol{p}_3 \end{cases}$$

を満たす一次独立な $\boldsymbol{p}_1, ..., \boldsymbol{p}_4$ を探せばよい. なぜ独立性が要求されるかは, P が正則であるから. ここでこの探求作業を効率よくするために,

$\boldsymbol{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$ とし

$$(A-E)\boldsymbol{x} = \boldsymbol{b} \Leftrightarrow \begin{pmatrix} A-E & \boldsymbol{b} \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ -1 \end{pmatrix} = \boldsymbol{0}$$

が $\boldsymbol{x}$ についての解を持つ必要十分条件 (57 ページ, [5.2]) を求める.

$$\begin{pmatrix} A-E & \boldsymbol{b} \end{pmatrix} = \begin{pmatrix} -3 & -1 & -2 & 1 & b_1 \\ 5 & 2 & 4 & -1 & b_2 \\ 1 & 0 & 0 & -1 & b_3 \\ -3 & -1 & -2 & 1 & b_4 \end{pmatrix} \overset{rank(A-E) \text{ が判明するまで行基本変形をする}}{\rightarrow} \begin{pmatrix} -3 & -1 & -2 & 1 & b_1 \\ -1 & 0 & 0 & 1 & 2b_1 + b_2 \\ 1 & 0 & 0 & -1 & b_3 \\ -3 & -1 & -2 & 1 & b_4 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} -3 & -1 & -2 & 1 & b_1 \\ -1 & 0 & 0 & 1 & 2b_1 + b_2 \\ 1 & 0 & 0 & -1 & b_3 \\ 0 & 0 & 0 & 0 & b_4 - b_1 \end{pmatrix} \rightarrow \begin{pmatrix} -3 & -1 & -2 & 1 & b_1 \\ -1 & 0 & 0 & 1 & 2b_1 + b_2 \\ 0 & 0 & 0 & 0 & 2b_1 + b_2 + b_3 \\ 0 & 0 & 0 & 0 & b_4 - b_1 \end{pmatrix}$$

よって,

$$(A-E)\boldsymbol{x} = \boldsymbol{b} \text{ が解を持つ} \Leftrightarrow 2b_1 + b_2 + b_3 = 0 \text{ かつ } b_4 - b_1 = 0 \qquad (2.7)$$

この条件を満たす $\boldsymbol{b}$ に対し解 $\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ は (2.7) より

$$(A-E)\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} b_1 \\ -b_3 - 2b_1 \\ b_3 \\ b_1 \end{pmatrix} \text{ i.e. } \begin{pmatrix} -3 & -1 & -2 & 1 \\ 5 & 2 & 4 & -1 \\ 1 & 0 & 0 & -1 \\ -3 & -1 & -2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} b_1 \\ -b_3 - 2b_1 \\ b_3 \\ b_1 \end{pmatrix}$$

$$\Leftrightarrow \quad \begin{cases} -3x_1 - x_2 - 2x_3 + x_4 = b_1 \\ 5x_1 + 2x_2 + 4x_3 - x_4 = -b_3 - 2b_1 \\ x_1 - x_4 = b_3 \\ -3x_1 - x_2 - 2x_3 + x_4 = b_1 \end{cases}$$

$$\overset{x_3=t,x_4=s}{\rightarrow} \quad \begin{cases} x_1 = s + b_3 \\ x_2 = -2s - 2t - 3b_3 - b_1 \\ x_3 = t \\ x_4 = s \end{cases}$$

よって $\boldsymbol{b}$ に対して $\boldsymbol{x}$ は s, t を任意の実数として

$$\boldsymbol{x} = \begin{pmatrix} s + b_3 \\ -2s - 2t - 3b_3 - b_1 \\ t \\ s \end{pmatrix} \tag{2.8}$$

とかける. 以下, $\boldsymbol{p}_2$と $\boldsymbol{p}_3$を探すときにはこのことを意識する.

$$(A - E)\boldsymbol{p}_3 = \boldsymbol{p}_2$$

が解を持つように

$$\boldsymbol{p}_2 = \begin{pmatrix} -1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$$

と選ぶ. すると s, t を任意の実数として

$$\boldsymbol{p}_3 = \begin{pmatrix} s \\ 1 - 2s - 2t \\ t \\ s \end{pmatrix}$$

とかける. $(A - E)\boldsymbol{p}_4 = \boldsymbol{p}_3$も成り立つように考える必要があるので (2.7) から $s = 1, t = 1$ (特に t を方程式から要求されるように選んだ) とおき,

$$\boldsymbol{p}_3 = \begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix}$$

と選ぼう. $(A - E)\boldsymbol{p}_4 = \boldsymbol{p}_3$において (2.8) より

$$\boldsymbol{p}_4 = \begin{pmatrix} s' + 1 \\ -2s' - 2t' - 4 \\ t' \\ s' \end{pmatrix}$$

とかけ, $\boldsymbol{p}_2$と $\boldsymbol{p}_3$と $\boldsymbol{p}_4$が独立となるように任意定数 s', t'を定め

$$\boldsymbol{p}_4 = \begin{pmatrix} 1 \\ -4 \\ 0 \\ 0 \end{pmatrix}$$

と選ぼう. 次に $(A-E)\boldsymbol{p}_1 = \boldsymbol{0}$ が成り立つように (2.8) より

$$\boldsymbol{p}_1 = \begin{pmatrix} s''' \\ -2s''' - 2t''' \\ t''' \\ s''' \end{pmatrix} = \begin{pmatrix} 0 \\ -2 \\ 1 \\ 0 \end{pmatrix}$$

と選ぶ. よって

$$P = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 2 & -3 & -4 \\ -1 & 0 & 1 & 0 \\ 1 & -1 & 1 & 0 \end{pmatrix}$$

という変換行列を探すことができた. 変換行列は一意ではないことに注意せよ. 検算すると確かに

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = P^{-1}AP$$

となっている.

注 37. 変換行列 P *s.t.* $B = P^{-1}AP$ は, $\exists C$ *s.t.* $[A, C] = O$ のとき

$$(CP)^{-1}A(CP) = B$$

なので一意ではない.

解 45. (ロ) $|A - xE| = \begin{vmatrix} 1-x & -1 & -1 & -1 \\ 1 & 2-x & 2 & 1 \\ -1 & 0 & -x & 0 \\ 1 & -1 & -1 & -1-x \end{vmatrix} = \begin{vmatrix} -x & -1 & 0 & -1 \\ 2 & 2-x & x & 1 \\ -1 & 0 & -x & 0 \\ 0 & 0 & 0x & \end{vmatrix} = x \begin{vmatrix} -x & -1 & 0 \\ 1 & 2-x & 0 \\ -1 & 0 & -x \end{vmatrix} =$
$-x^2(x-1)^2$. まず$\lambda_1 = 0$ に対する $J_m(0)$ の個数 $c_m(0)$ を計算しようと思う. $r_0(0) = 4,\ r_1(0) = rank(A - 0E) = 3,\ r_2(0) = rank(A - 0E)^2 = 2$ である.
定理 A より

$$c_m(0) = 0\ (m \geq 3),\ c_1(0) + 2c_2(0) = 2$$

定理 B より

$$c_1(0) = r_0(0) - 2r_1(0) + r_2(0) = 4 - 2 \times 3 + 2 = 0$$

$$c_2(0) = 1$$

次に$\lambda_2 = 1$ に対する $J_m(1)$ の個数 $c_m(1)$ を計算しよう.

$$(A-E)^2 = \begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & -2 & -2 \\ 1 & 1 & 2 & 1 \\ -2 & 0 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 \end{pmatrix} \text{より } rank(A-E)^2 = 2$$

$r_1(1) = rank(A-E) = 3,\ r_2(1) = rank(A-E)^2 = 2.$
定理 A より

$$c_m(1) = 0\ if m \geq 3,\ c_1(1) + 2c_2(1) = 2$$

定理 B より

$$c_1(1) = r_0(1) - 2r_1(1) + r_2(1) = 4 - 2 \times 3 + 2 = 0,\ c_2(1) = 1$$

よって

$$J = P^{-1}AP = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = J_2(0) \oplus J_2(1)$$

または

$$J = P'^{-1}AP' = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = J_2(1) \oplus J_2(0)$$

解 46. (ハ) $A = \begin{pmatrix} 0 & -1 & -1 & 0 \\ 6 & 3 & 4 & -2 \\ -5 & -1 & -1 & 2 \\ -1 & -1 & -1 & 1 \end{pmatrix}$ に対し$\Phi_A(x) = |xE - A| = \begin{vmatrix} x & 1 & 1 & 0 \\ -6 & x-3 & -4 & 2 \\ 5 & 1 & x+2 & -2 \\ 1 & 1 & 1 & x-1 \end{vmatrix} =$
$(x+1)(x-1)^3$. $\lambda_1 = -1$ に対する $J_m(-1)$ の個数を計算する.

$$r_0(-1) = 4,\ r_1(-1) = rank(A+E) = 3,\ r_2(-1) = rank((A+E)^2) = 3$$

である. 定理 A より

$$c_m(-1) = 0\ if m \geq 2,\ c_1(-1) = 1$$

定理 B より

$$c_1(-1) = r_0(-1) - 2r_1(-1) + r_2(-1) = 4 - 2 \times 3 + 3 = 1$$

であるがこれはもうすでに求まってあった. $\lambda_2 = 1$ に対する $J_m(1)$ の個数を計算する.

$$r_0(1) = 4,\ r_1(1) = rank(A-E) = 2,\ r_2(1) = rank((A-E)^2) = 1,\ r_3(1) = rank((A-E)^3) = 1$$

である. 定理 A により

$$c_m(1) = 0\ if m \geq 4,\ c_1(1) + 2c_2(1) + 3c_3(1) = 3$$

定理 B により

$$c_1(1) = r_0(1) - 2r_1(1) + r_2(1) = 4 - 2 \times 2 + 1 = 1$$

$$c_2(1) = r_1(1) - 2r_2(1) + r_3(1) = 2 - 2 \times 1 + 1 = 1$$

最後に, $c_3(1) = 0$ である. ジョルダン標準形は並び方を除いて一意であり

$$J = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

である. (ニ) も同様に J を求めて次に P を計算できる.

解 47.

$$A = \begin{pmatrix} \alpha & b & c \\ 0 & \alpha & a \\ 0 & 0 & \alpha \end{pmatrix}$$

のジョルダン標準形を求める. $|A - xE| = -(x - \alpha)^3$である. 定理 A, B より

$$c_m(\alpha) = 0 if m \geq 4,\ c_1(\alpha) + 2c_2(\alpha) + 3c_3(\alpha) = 3$$

$$c_1(\alpha) = r_0(\alpha) - 2r_1(\alpha) + r_2(\alpha)$$

$$c_2(\alpha) = r_1(\alpha) - 2r_2(\alpha) + r_3(\alpha)$$

ここで次のランクを計算すると

$$r_1(\alpha) = rank(A - \alpha E) = \begin{cases} 2 & (a \neq 0, b \neq 0) \\ 1 & (\text{「}a = 0, b \neq 0\text{」または「}a \neq 0, b = 0\text{」または「}a = 0, b = 0, c \neq 0\text{」}) \end{cases}$$

$$r_2(\alpha) = rank(A - \alpha E)^2 = \begin{cases} 1 & (a \neq 0, b \neq 0) \\ 0 & (a = 0\ or\ b = 0) \end{cases} \qquad r_3(\alpha) = 0$$

なので

$$if\ a \neq 0, b \neq 0\ ;\ c_1(\alpha) = 3 - 2 \times 2 + 1 = 0,\ c_2(\alpha) = 2 - 2 \times 1 = 0,\ c_3(\alpha) = 1 \text{ で } J = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$$

$$if\ a = 0\ or\ b = 0 \text{ただし} a = b = 0 \text{の時に限り} c \neq 0\ ;\ c_1(\alpha) = 1,\ c_2(\alpha) = 1,\ c_3(\alpha) = 0 \text{で} J = \begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

$$if\ a = b = c = 0\ ;\ J = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

解 48. 復習から始めると $f : V \to W$ の表現行列 $A \in M_{mn}(\mathbb{K})$ は V, W の基底 $E = \langle e_1, ..., e_n \rangle$ と $F = \langle f_1, ..., f_m \rangle$ の取り方に依存する. $\mathbb{K}$ 多項式全体 $P_2(\mathbb{K})$ の基底を上手く選ぶことで T_bの行列をジョルダン標準形にすることができる. まず標準基底 $E = \langle 1, x, x^2 \rangle$ で T_bを表すと

$$\begin{pmatrix} T_b(1) & T_b(x) & T_b(x^2) \end{pmatrix} = \begin{pmatrix} 1 & x+b & (x+b)^2 \end{pmatrix} = \begin{pmatrix} 1 & x & x^2 \end{pmatrix} \begin{pmatrix} 1 & b & b^2 \\ 0 & 1 & 2b \\ 0 & 0 & 1 \end{pmatrix}$$

より $A = \begin{pmatrix} 1 & b & b^2 \\ 0 & 1 & 2b \\ 0 & 0 & 1 \end{pmatrix}$ である. $b \neq 0$ であり前問からそのジョルダン行列は $J = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ となる. $P_2(\mathbb{K})$ 上の線型変換の基底として固有値 1 (代数的重複度 3) に対応する広義固有ベクトルを選んだ場合の表現行列が J である. $W_3 = \{x | (A-E)^3 x = 0\}$ の基底は $F = \langle 2b^2, 2bx, x^2 - bx \rangle$ ということであり

$$\begin{pmatrix} 2b^2 & 2bx + 2b^2 & x^2 + bx \end{pmatrix} = \begin{pmatrix} 2b^2 & 2bx & x^2 - bx \end{pmatrix} J$$

を満たす. 基底の取り替え行列 $P_{E \to F}$ は $AP = PJ$ を利用して求められる $P = \begin{pmatrix} 2b^2 & 0 & 0 \\ 0 & 2b & -b \\ 0 & 0 & 1 \end{pmatrix}$ (ただし, 分母がある有理数が現れないように任意定数を便宜上選んだ) なので

$$\begin{pmatrix} 2b^2 & 2bx & x^2 - bx \end{pmatrix} = \begin{pmatrix} 1 & x & x^2 \end{pmatrix} \begin{pmatrix} 2b^2 & 0 & 0 \\ 0 & 2b & -b \\ 0 & 0 & 1 \end{pmatrix}$$

と変換後の基底がその実体としてのベクトルが不変である為に計算される.

解 49. $J = P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ より $A^n = PJ^nP^{-1}$, $J^n = \begin{pmatrix} 1 & n & \frac{1}{2}n(n-1) \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$ で計算する.

注 38. 固有多項式とケーリーハミルトンの定理による 2 次と 3 次行列の n 乗計算について考えよ.

解 50. (イ) A のジョルダン標準形を J とするとある正則行列 P があって

$$J = P^{-1}AP = \begin{pmatrix} J_1(\alpha_1) & & & & & & \\ & \ddots & J_{m_1}(\alpha_1) & & & & \\ & & & \ddots & & & \\ & & & & J_1(\alpha_n) & & \\ & & & & & \ddots & \\ & & & & & & J_{m_n}(\alpha_n) \end{pmatrix}$$

とかける. m_1は $J_i(\alpha_1)$ の番号 i の中で最も大きいものと並べておく. A が対角行列に相似であることを示すには全てのジョルダンセルの次数が 1 であればよい.

$$0 \leq k < m_1 - 1 \text{ のとき } J_{m_1}(\alpha_1)^k = \begin{pmatrix} {\alpha_1}^k & k{\alpha_1}^{k-1} & \cdots & 1 & & 0 \\ & {\alpha_1}^k & \ddots & \ddots & & \\ & & \ddots & \ddots & & 1 \\ & & & \ddots & \ddots & \vdots \\ & & & & \ddots & k{\alpha_1}^{k-1} \\ O & & & & & {\alpha_1}^k \end{pmatrix}$$

でありもし $m_1 \geq 2$ ならそのとき $J_{m_1}(\alpha_1)^k = E$ に反するので $m_1 = 1$ である. その他の固有値α_nに対するジョルダンセル $J_{m_n}(\alpha_n)$ についても同様.
(ロ) $A^k = O$, $A \neq O$ ならば A は対角行列に相似ではない. なぜなら重複を込めた A の固有値$\alpha_1, ..., \alpha_n$が全て 0 であるからである.

解 51. $r \leq n$ とし n 次行列 A の相異なる固有値を$\lambda_1, ..., \lambda_r$とおく. A のジョルダン標準形 $P^{-1}AP$ の固有値λ_1に対するジョルダンセルの最大次数を ℓとおき, $P^{-1}AP$ に含まれる固有値λ_1に対する k 次ジョルダンセルの個数を s_kと $(1 \leq k \leq \ell)$ とする. P の列を交換することでジョルダンセルの順序を交換できるので同じ固有値に対するジョルダンセルは連続して並んでいるとしてよい. λ_iに対するジョルダンセルを対角線上に並べた行列を $J(\lambda_i)$ とし, その次数を n_iと $(1 \leq i \leq r)$ とおく. このとき明らかに

$$J(\lambda_i) = \bigoplus_{m \geq 1} (J_m(\lambda_i) \oplus \cdots \oplus J_m(\lambda_i))$$

$$n_1 = s_1 + 2s_2 + 3s_3 + \cdots + \ell s_\ell$$

$$P^{-1}AP = \begin{pmatrix} J(\lambda_1) & & \\ & \ddots & \\ & & J(\lambda_r) \end{pmatrix}$$

である. ここで

$$J_k(\lambda_1) - \lambda_1 E = J_k(0) = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}$$

のランクは $k-1$ 即ち

$$k - \operatorname{rank}(J_k(\lambda_1) - \lambda_1 E) = 1$$

$J(\lambda_1)$ の各ジョルダンセルに対し上式が成り立つので

$$n_1 = \operatorname{rank}(J(\lambda_1) - \lambda_1 E) = s_1 + s_2 + \cdots + s_\ell$$

である. $i \geq 2$ のときは $J(\lambda_1) - \lambda_1 E$ は正則より

$$n_i - \operatorname{rank}(J(\lambda_i) - \lambda_1 E) = 0$$

であるので

$$\mathrm{rank}(A-\lambda_1 E) = n - n_1 + \mathrm{rank}(J(\lambda_1)-\lambda_1 E) = n - (s_1 + \cdots + s_\ell)$$

$$\Leftrightarrow n - \mathrm{rank}(A-\lambda_1 E) = n - \mathrm{rank}(J-\lambda_1 E) = s_1 + s_2 + \cdots + s_\ell$$

である. よって$\lambda_1 = 0,\ s_1 + \cdots + s_\ell = s$ とおくことで題意は示せた.

この問いは重要であるので本稿の終節「ジョルダン標準形の存在一意」で述べる i 次ジョルダンセルの個数を特定する公式と関連してまとめておく. この問いを俯瞰すると以下の命題の主張が意味するところとなり, それはつまり A の λ に対するジョルダンセルの個数は λ の固有空間 $W_\lambda = \ker(A-\lambda E)$ の次元に等しい.「ジョルダン標準形の存在一意」では A の固有値と重複度を求め, A の各固有値 λ と自然数 k に対して $\mathrm{rank}(A-\lambda E)^k$を計算し, それによって i 次ジョルダンセルの個数が特定できることを述べた. 上の問いのように, $\mathrm{rank}(A-\lambda E) = n - \dim\ker(A-\lambda E)$ を計算しても λ に対するジョルダンセルの個数 (の総数) が分かるだけで i 次ジョルダンセルの各個数まで分からないと A のジョルダン標準形は判明しない. よってさらなる公式的等式の探求が求められる.

解 52. n 次 $\mathbb{K}$ 正方行列 A に対し, $f(A) = O$ となる多項式 f が存在する. 実際, $M_n(\mathbb{K})$ は n^2 次元なので, n^2+1 個の $E, A, A^2, ..., A^{n^2}$の間には自明でない関係

$$a_0 A^{n^2} + a_1 A^{n^2-1} + \cdots + a_{n^2-1}A + a_{n^2}E = O$$

が存在する. これより

$$a_{n^2}E = -a_{n^2-1}A - \cdots - a_0 A^{n^2}$$

両辺に $A^{-1}(a_{n^2})^{-1}$をかけると

$$A^{-1} = -(a_{n^2})^{-1}(a_{n^2-1}E + \cdots + a_0 A^{n^2-1})$$

である.

補題 20. 任意の正方行列 $A \in M(\mathbb{C})$ に対して次を満たす正方行列 $S, N \in M(\mathbb{C})$ が一意的に存在する. これを A の加法的ジョルダン分解という.
(1) $A = S + N,\ SN = NS$
(2) S は対角行列に相似
(3) N は冪零行列
(4) S, N はともに A の多項式

証明. A の相異なる固有値を$\alpha_1, ..., \alpha_k$とし A のジョルダン標準形 $J = P^{-1}AP = J_1 \oplus J_2 \oplus \cdots \oplus J_k$ を考える. $i \in \{1, ..., k\}$ に対し $S_i := \alpha_i E,\ N_i := J_i - \alpha_i E$ と定義する. $S_0 := S_1 \oplus S_2 \oplus \cdots \oplus S_k,\ N_0 := N_1 \oplus N_2 \oplus \cdots \oplus N_k,\ S := PS_0P^{-1},\ N := PN_0P^{-1}$とおくと S, N が (1) から (4) を満たす. □

解 53. A の加法的ジョルダン分解を $A = S + N$ とする. S の固有値は A の固有値なので S は正則である. よって $U := S^{-1}N + E$ とおけば S, U は諸条件を満たす. なぜなら $A = S + N = S + (SU - S) = SU = US$ より (1) は成立し (2), (4) は明らか. $U - E = S^{-1}N$ が冪零である

ことを示す. $U-E$ が冪零でないと仮定すると冪零行列の行列式は 0 なので $|S^{-1}N| \neq 0$ であるがこれは $|S^{-1}N| = |S^{-1}|\,|N| = 0$ に矛盾する.
一意性を示す. もし (S', U') も乗法的ジョルダン分解であるなら, $N' := S'(U'-E)$ と定めると (S', N') は A の加法的ジョルダン分解である.

$$\because\ S'+N' = S'+S'(U'-E) = S'U' = A$$

$N := S(U-E)$ とおくと (S, N) についても同様に A の加法的ジョルダン分解なのでその一意性より $S = S', N = N'$ である. 特に A が実行列ならば S, U も実行列であることを示す. A を乗法的ジョルダン分解すると $\overline{A} = A = SU = US$. $(\overline{S}, \overline{U})$ もまたそうなるので一意性より $S = \overline{S}$ が成立し, S は実行列である.

命題 66. $d_1, ..., d_r \in \mathbb{N},\ r = \mathrm{rank}(A),\ d_{i-1} | d_i\ (2 \leq i \leq r)$ とする. 任意の正方整数行列 A に対しある正則整数行列 P, Q が存在して

$$B := PAQ = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

この標準形は一意的である.

解 54 (整数行列の単因子)**.** 基本変形を起こす行列 P, Q を適当に定義すればよい. $A = O$ なら $r = 0$ の場合であり自明. $A \neq O$ とすると A のある (i, j) 成分は 0 でないので第 1 行と第 i 行を交換し第 1 列と第 j 列を交換することで $a_{11} \neq 0$ とする. 次に $(1, 1)$ をかなめとし第 1 行, 第 1 列を P, Q をそれぞれ左右からかけて掃き出す. 次数が 1 つ下がった行列に順に同様の操作をすると B を得る. 一意性は積 $d_1 \cdots d_r$ が第 i 次小行列式全ての最大公約数であることより保証される.

問 29. $\forall A$: 正則整数行列 $\exists B$: 正則整数行列, $\exists R$: 正則整数上三角行列で対角成分は正

$$s.t.\ AB = R$$

証明. 前命題において A は次のユニモジュラー行列による基本変形で上の $B = PAQ$ になった.
(1) A の行 (列) を交換
(2) A のある行 (列) の整数倍を他の行に加える
(3) A のある行 (列) を ± 1 倍する
(1), (2), (3) を起こす行列 P を考えると, $AQ = P^{-1}B$ は上三角で対角成分は 0 より大きい整数行列である. □

2.5 [9] 第 3 章

解 55. (イ) $X=(x_{ij})$ を n 次行列としたとき $\det A=\sum_\sigma \mathrm{sgn}(\sigma)\prod_{i=1}^n a_{i\sigma(i)}$ より

$$D_{n+1}(a_n,a_{n-1},...,a_0) = \begin{vmatrix} x & -1 & 0 & \cdots & 0 & 0 \\ 0 & x & -1 & \cdots & 0 & 0 \\ 0 & 0 & x & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & -1 & 0 \\ 0 & 0 & 0 & \cdots & x & -1 \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \end{vmatrix}$$

$$= x\begin{vmatrix} x & -1 & \cdots & 0 & 0 \\ 0 & x & \vdots & \vdots & \\ \vdots & \vdots & -1 & 0 & \\ 0 & 0 & x & -1 & \\ a_{n-1} & a_{n-2} & a_1 & a_0 & \end{vmatrix} + (-1)^{n+2}a_n \begin{vmatrix} -1 & 0 & 0 & 0 & \\ x & -1 & 0 & 0 & \\ 0 & x & -1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & -1 & 0 & \\ 0 & 0 & \cdots & x & -1 \end{vmatrix}$$

$D_{n+1}(a_n,a_{n-1},...,a_0)=xD_n(a_{n-1},...,a_0)+(-1)^{n+2}a_n(-1)^n=xD_n(a_{n-1},...,a_0)+a_n=x(xD_{n-1}(a_{n-2},...,a_0)+a_{n-1})+a_n=D_{n-1}(a_{n-2},...,a_0)x^2+a_{n-1}x+a_n=...=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n.$

(ロ) 系 2.5, 定理 2.6 より $\begin{vmatrix} x & a_1 & a_2 & \cdots & a_n \\ a_1 & x & a_2 & \cdots & a_n \\ a_1 & a_2 & x & \cdots & a_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & x \end{vmatrix} = \begin{vmatrix} x & a_1 & a_2 & \cdots & a_{n-1} & x+a_1+\cdots+a_n \\ a_1 & x & a_2 & \cdots & a_{n-1} & x+a_1+\cdots+a_n \\ a_1 & a_2 & x & \cdots & a_{n-1} & x+a_1+\cdots+a_n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & x & x+a_1\cdots+a_n \\ a_1 & a_2 & a_3 & \cdots & a_n & x+a_1+\cdots+a_n \end{vmatrix} =$

$$(\textstyle\sum_{i=1}^n a_i+x)\begin{vmatrix} x & a_1 & a_2 & \cdots & a_{n-1} & 1 \\ a_1 & x & a_2 & \cdots & a_{n-1} & 1 \\ a_1 & a_2 & x & \cdots & a_{n-1} & 1 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ a_1 & a_2 & a_3 & \cdots & x & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n & 1 \end{vmatrix} = (\textstyle\sum_{i=1}^n a_i+x)\begin{vmatrix} x & a_1 & a_2 & \cdots & a_{n-1} & 1 \\ a_1-x & x-a_1 & 0 & \cdots & 0 & 0 \\ a_1-x & a_2-a_1 & x-a_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1-x & a_2-a_1 & a_3-a_2 & \cdots & x-a_{n-1} & 0 \\ a_1-x & a_2-a_1 & a_3-a_2 & \cdots & a_n-a_{n-1} & 0 \end{vmatrix}$$

$$\overset{\text{余因子展開}}{=} (-1)^{n+2}(\textstyle\sum_{i=1}^n a_i+x)\begin{vmatrix} a_1-x & x-a_1 & 0 & \cdots & 0 \\ a_1-x & a_2-a_1 & x-a_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1-x & a_2-a_1 & a_3-a_2 & \cdots & x-a_{n-1} \\ a_1-x & a_2-a_1 & a_3-a_2 & \cdots & a_n-a_{n-1} \end{vmatrix}$$

$j=n,n-1,...,2$ に対して第 j 列に $1,2,...,j-1$ 列を全て足すと, $(-1)^n(\sum_{i=1}^n a_i+x)\begin{vmatrix} a_1-x & 0 & 0 & \cdots & 0 \\ a_1-x & a_2-x & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1-x & a_2-x & a_3-x & \cdots & 0 \\ a_1-x & a_2-x & a_3-x & \cdots & a_n-x \end{vmatrix} =$

$(-1)^n(\sum_{i=1}^n a_i + x)\prod_{i=1}^n(a_i - x) = (\sum_{i=1}^n a_i + x)\prod_{i=1}^n(x - a_i)$ である.
(ハ) 与えられた正方行列式の次数を n とし D_n とかくと $D_n = (1+x^2)D_{n-1} - x(x(1+x^2)^{n-2}) = (1+x^2)\{(1+x^2)D_{n-2} - x^2(1+x^2)^{n-3}\} - x^2(1+x^2)^{n-2} = (1+x^2)^2D_{n-2} - 2x^2(1+x^2)^{n-2} = \cdots = (1+x^2)^n - (n-1)x^2(1+x^2)^{n-2}$. (ニ) $\begin{vmatrix} 0 & a^2 & b^2 & 1 \\ 0 & -a^2 & c^2-a^2 & 1 \\ 0 & c^2-b^2 & -b^2 & 1 \\ 1 & 0 & 0 & 0 \end{vmatrix} = -\begin{vmatrix} a^2 & b^2 & 1 \\ -a^2 & c^2-a^2 & 1 \\ c^2-b^2 & -b^2 & 1 \end{vmatrix} = (c^2-a^2-b^2)^2 - 4a^2b^2 = (a^2+b^2-c^2)^2 - 4a^2b^2 = (a^2+b^2-2ab-c^2)(a^2+b^2+2ab-c^2) = -(a+b+c)(-a+b+c)(a-b+c)(a+b-c)$.

解 56. (イ) 左辺 $= a\begin{vmatrix} a & b & c \\ -d & 0 & f \\ -e & -f & 0 \end{vmatrix} - b\begin{vmatrix} a & b & c \\ 0 & d & e \\ -e & -f & 0 \end{vmatrix} + c\begin{vmatrix} a & b & c \\ 0 & d & e \\ -d & 0 & f \end{vmatrix} = a(-bef + cdf + af^2) - b(-be^2 + cde + aef) + c(adf - bed + cd^2) =$ 右辺. (ロ) $|A| = |A^t| = |-A| = (-1)^n|A|$ より n が奇数のとき $|A| = 0$ である. A が偶数次ならば $|A|$ は多項式 $P(a_{ij})(1 \le i, j \le n)$ を用いて $|A| = P^2$ と表せる.

解 57. $\alpha_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}(1 \le k \le n)$ とおく. $\begin{vmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & x_1 & \cdots & x_{n-2} \\ & & & \ddots & \\ x_1 & x_2 & x_3 & \cdots & x_0 \end{vmatrix}$ において $j \in \{2, ..., n\}$ に対し第 j 列の${\alpha_k}^{j-1}$倍を第 1 列に加えることで左辺は $x_0 + \alpha_k x_1 + \cdots {\alpha_k}^{n-1}x_{n-1}$ で割れる. ($\because {\alpha_k}^n = 1$) よって左辺は右辺の倍数であり, 左辺の多項式 $P(x_0, ..., x_{n-1})$ の x_{n-1}^n の係数は$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & 1 & 2 & \cdots & n-2 & n-1 \end{pmatrix} = (-1)^{n+1}$. 右辺の x_{n-1}^n の係数である $\prod_{k=1}^n \alpha_k^{n-1}$ は α_k を指数関数を使って表すことで容易に $(-1)^{n+1}$ であり係数が等しい. このような状況では左辺と右辺は等しい.

問 30. $\omega_n = e^{\frac{2i\pi}{n}}$ は 1 の原始 n 乗根とする.

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_n & {\omega_n}^2 & \cdots & {\omega_n}^{n-1} \\ 1 & {\omega_n}^2 & {\omega_n}^4 & \cdots & {\omega_n}^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & {\omega_n}^{n-1} & {\omega_n}^{2(n-1)} & \cdots & {\omega_n}^{(n-1)^2} \end{pmatrix}^{-1} = \frac{1}{n}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & {\omega_n}^{-1} & {\omega_n}^{-2} & \cdots & {\omega_n}^{-(n-1)} \\ 1 & {\omega_n}^{-2} & {\omega_n}^{-4} & \cdots & {\omega_n}^{-2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & {\omega_n}^{-(n-1)} & {\omega_n}^{-2(n-1)} & \cdots & {\omega_n}^{-(n-1)^2} \end{pmatrix}$$

を示せ.

解 58. 前解より $\begin{vmatrix} x & i & 1 & -i \\ -i & x & i & 1 \\ 1 & -i & x & i \\ i & 1 & -i & x \end{vmatrix} = (x+1)^3(x-3)$

解 59. $\begin{pmatrix} 1 & x_1 & \cdots & {x_1}^{n-1} \\ 1 & x_2 & \cdots & {x_2}^{n-1} \\ & & \cdots & \\ 1 & x_n & \cdots & {x_n}^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$ においてヴァルデモンド行列式は 0 でないので n 個の点 $(x_i, y_i)(1 \leq i \leq n)$ があるとき $(a_0 \cdots a_{n-1})^t$ は一意に定まる.

解 60. 拡大係数行列に対し行基本変形しても連立方程式は同値. $\begin{pmatrix} a & -b & -a & b & 1 \\ b & a & -b & -a & 0 \\ c & -d & c & -d & 0 \\ d & c & d & c & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ u \\ -1 \end{pmatrix} =$

$0, \begin{cases} (a + b^2/a)(x - z) - 1 = 0 \\ b(x - z) + a(y - u) = 0 \\ (c + d^2/c)(x + z) = 0 \\ d(x + z) + c(y + u) = 0 \end{cases}$ より $x \neq -z$ とすると $c = d = 0$ で矛盾なので $x = -z = \frac{a}{2(a^2+b^2)}$ であり $y = -u = \frac{-b}{2(a^2+b^2)}$ である.

解 61. 直線 $l_i : a_i x + b_i y + c_i = 0$ とし $A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$ とする. 少なくとも 2 直線が並行で直線の交点を結んで三角形はできない場合と 1 点で交わる場合に 3 直線は三角形を作らない.

前者の必要十分条件を考える. l_i と l_j が平行であるとは $a_i b_j - a_j b_i = 0$ であり $a_1 b_2 - a_2 b_1 = 0, a_2 b_3 - a_3 b_2 = 0, a_3 b_1 - a_1 b_3 = 0$ の少なくとも一つが成りたつ. (なお全て成立 $\Leftrightarrow$ 全ての直線が並行 $\Leftrightarrow \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = c_3 \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} - c_2 \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} + c_1 \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} = 0$ が成立.) $(a_1 b_2 - a_2 b_1)(a_2 b_3 - a_3 b_2)(a_3 b_1 - a_1 b_3) = 0 \Leftrightarrow \Delta_{13}\Delta_{23}\Delta_{33} = 0$. 後者の必要十分条件については唯一の交点を (λ, μ) とすると $A \begin{pmatrix} \lambda \\ \mu \\ -1 \end{pmatrix} = 0$ が成立. もし A^{-1} が存在するなら矛盾するので $\det A = 0$ が必要十分である.

解 62. 空間にある 4 点 $P_i(x_i, y_i, z_i)$ が同一平面上にある必要条件は $\begin{vmatrix} x_4 & y_4 & z_4 & 1 \\ x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \end{vmatrix} = 0$ である. なぜならこれは $\begin{vmatrix} x_1 - x_4 & y_1 - y_4 & z_1 - z_4 \\ x_2 - x_4 & y_2 - y_4 & z_2 - z_4 \\ x_3 - x_4 & y_3 - y_4 & z_3 - z_4 \end{vmatrix} = 0$ と同値でこれは $P_1, ..., P_4$ が同一平面

上にあることを意味する. 次に題意を示す. もし $\begin{vmatrix} x & y & z & 1 \\ x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \end{vmatrix} = 0$ ならば空間内の任意の $P(x,y,z)$ に対し P_1, P_2, P_3, P が同一平面上に存在するので P_1, P_2, P_3 が同一直線上に存在し矛盾. よって恒等的に 0 ではなく, $(x,y,z) = (x_i, y_i, z_i)$ のとき行列式は 0 となりすなわち各 P_i はこの平面の方程式を満たす平面上に存在する.

解 63. n 次正方行列 A, B に対し $|AB| = |A||B|$ である. $|A||A^{-1}| = 1$ かつ A, A^{-1} が整数行列なので $|A| = \pm 1$. 逆に $|A| = \pm 1$ のとき $A^{-1} = \frac{1}{|A|}\tilde{A}$($\tilde{A}$ は A の余因子行列, 系 [3.3]) より $A^{-1} = \pm\tilde{A} \Leftrightarrow a_{ij}^{-1} = \pm\tilde{a_{ji}}$. A が正則整数行列であったとするとこの関係式より A^{-1} も整数行列である.

解 64. (イ)$(A_\sigma)_{\sigma(j),j} = 1, (A_\sigma)_{\sigma(j)\text{ でない},j} = 0$ の定義より各行に 1 が一つありそれ以外の成分が 0 の行列であるので A_σ は正規直交ベクトルを並べた直交行列. (ロ)$\tau = \begin{pmatrix} 1 & \cdots & n \\ j_1 & \cdots & j_n \end{pmatrix}, \sigma = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix}$ とする. $\sigma\tau = \begin{pmatrix} 1 & \cdots & k & \cdots & n \\ i_{j_1} & \cdots & i_{j_k} & \cdots & i_{j_n} \end{pmatrix}$ である. 各 (i,j) 成分が等しいことすなわち $(A_{\sigma\tau})_{ij} = \sum_{k=1}^n (A_\sigma)_{ik}(A_\tau)_{kj}$ を示す. $i \equiv i_{j_k}, j \equiv k$ のときは行列 A_σ の定義より $(A_{\sigma\tau})_{ij}$ は 1 である. そこで, $\sum_{k=1}^n (A_\sigma)_{ik}(A_\tau)_{kj} = (A_\sigma)_{i_{j_k},1}(A_\tau)_{1,k} + \cdots + (A_\sigma)_{i_{j_k},n}(A_\tau)_{n,k} = 1$ を示す. 左辺の各項に注目すると $(A_\tau)_{\tau(k),k}$ の 1 を除いて 0 であるので $(A_\sigma)_{i_{j_k},\tau(k)} = 1$ を示せばよい. そしてこれはその左辺 $= (A_\sigma)_{\sigma(j_k),j_k}$ なので成り立つ. $i \not\equiv i_{j_k}, j \not\equiv k$ に対しても (i,j) 成分は 0 で等しい. (次のように書くとなお良い. $A_\sigma = (a_{ij}), A_\tau = (b_{ij})$ とする. $(A_\sigma A_\tau)_{i,k} = \sum_{j=1}^n a_{ij}b_{jk} = \sum_{j=1}^n a_{ij}\delta_{j,\tau(k)} = a_{i,\tau(k)} = \delta_{i,\sigma\tau(k)}$ より.) (ハ) まず $\Rightarrow$ を示す. $\mathrm{sgn}(\sigma) = 1$ であって $\det A_\sigma = -1$ と仮定する. σ, τ が偶置換のとき $\det A_{\sigma\tau} = (-1)(-1)$ であるが, $\det A_{\sigma\tau} = -1$ なので矛盾. $\Leftarrow$ は $\Rightarrow$ の対偶を取れば $\Rightarrow$ が成立するかどうかに帰着する.

解 65 (77 ページ)**.** n 文字の置換がなす群を S_n とかく. $\sigma \in S_n$ を互換とする. $\pi : S_n \ni \tau \mapsto \sigma\tau \in S_n$ は全単射. 全射性は明らか. 単射であることを示す. $\sigma\tau_1 = \sigma\tau_2$ なら σ を左から作用させて $\tau_1 = \tau_2$ よりこれも明らか. この写像は偶置換を奇置換に, 奇置換を偶置換にする. なぜなら τ を k この互換の積としたとき (任意の置換は互換の積で表せるのだった. その表す方にはもちろん一意性はないが互換の数が奇数が偶数であるかは τ によって決まっている. この事実により $\mathrm{sgn} : S_n \to \{1, -1\}$ が良定義である.) に $\sigma\tau$ は $k+1$ この互換の積であるからである. よって偶置換と奇置換はこの写像 π により S_n の間を写り合うので $\frac{n!}{2}$.

解 66 (77 ページ)**.** 互換 $\begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ k_1 & \cdots & j & \cdots & i & \cdots & k_n \end{pmatrix}$ を σ_{ij} でかくと $n = 2k$ のとき与えられた置換は順番は気にせず $\sigma_{1,2k}\sigma_{2,2k-1}\cdots\sigma_{k,k+1}$ であり答えは $(-1)^k$. $n = 2k+1$ のとき $\sigma_{1,2k}\sigma_{2,2k-1}\cdots\sigma_{k,k+2}$ よりこれも $(-1)^k$.

解 67 (79 ページ)**.** $a_{ij} = \begin{cases} a_i & (i+j = n+1) \\ 0 & (i+j \neq n+1) \end{cases}$ で定義された行列が A である. $|A| := \sum_\sigma \mathrm{sgn}(\sigma) a_{1\sigma(1)}\cdots a_{n\sigma(n)} = \mathrm{sgn}(\sigma_0)a_1\cdots a_n$ で

$$\sigma_0 := \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$$

である. よって行列式は (66) より

$$\sum_{\sigma} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \mathrm{sgn}(\sigma_0) a_1 \cdots a_n = (-1)^k a_1 \cdots a_n$$

である. このように行列式の定義に基づいた計算ができることは重要である. 例えば 2, 3 次正方行列式もその置換を考えて計算できたい. 自明な例で申し訳ないが $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = (+1)a_{11}a_{22} - a_{12}a_{21}$ における 2 つの置換は $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ というようにである.

2.6 [9] 第 2 章

解 68. (イ) 拡大係数行列に行基本変形を施しても方程式は同値なので $\begin{pmatrix} 1 & 2 & -1 & 3 & -2 & 1 \\ 2 & 4 & 1 & 3 & -3 & 2 \\ -1 & -2 & 2 & -4 & -1 & 1 \\ 3 & 6 & 0 & 6 & -5 & 3 \end{pmatrix} \to$

$$\begin{pmatrix} 1 & 2 & -1 & 3 & -2 & 1 \\ 0 & 0 & 0 & 0 & 5 & -3 \\ 0 & 0 & 1 & -1 & -3 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ -1 \end{pmatrix} = 0 \Leftrightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1/5 \\ 0 \\ -3/5 \end{pmatrix} + s \begin{pmatrix} -2 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

解 69. P^{-1} をまず計算. P が行基本変形だけで単位行列になることと P が正則であることは同値. $\begin{pmatrix} 1 & 3 & 2 & 1 & 0 & 0 \\ -1 & -2 & -1 & 0 & 1 & 0 \\ 2 & 4 & 3 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & -2 & -1 & 1 \\ 0 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{pmatrix}$ より $P^{-1}AP$ を計算し $A^n =$

$$P(P^{-1}AP)^nP^{-1} = \begin{pmatrix} 1 & 3 & 2 \\ -1 & -2 & -1 \\ 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 2^n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} -2 & -1 & 1 \\ 1 & -1 & -1 \\ 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} -2^{n+1}+3 & -2^n-3 & 2^n-3 \\ 2^{n+1}-2 & 2^n+2 & -2^n+2 \\ -2^{n+2}+4 & -2^{n+1}-4 & 2^{n+1}-4 \end{pmatrix}.$$

解 70. $x = 1$ ならば階数は 1 である. 正則行列を左から掛けても (行基本変形をしても) 階数は変わらないことに注意. 与えられた行列の第 2...n 列は互いに明らかに線型独立なので階数が $n-1 \Leftrightarrow$ 第一列が第 2...第 n 列の線型結合でかける即ち $\begin{pmatrix} 1 \\ x \\ x \\ \vdots \\ x \end{pmatrix} = c_1 \begin{pmatrix} x-1 \\ 1-x \\ 0 \\ \vdots \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} x-1 \\ 0 \\ 1-x \\ \vdots \\ 0 \end{pmatrix} +$

$$\cdots + c_{n-1} \begin{pmatrix} x-1 \\ 0 \\ 0 \\ \vdots \\ 1-x \end{pmatrix} \Leftrightarrow c_i = \frac{x}{1-x} (1 \le i \le n-1), -x = \frac{1}{n-1}.$$ また $x \neq 1$ かつ $x \neq \frac{-1}{n-1}$ のとき階数は n である.

解 71. 問いに於いて n 次正方行列 A は正則でないと仮定する. 一般に $A \in M_{mn}$, 一次方程式 $A\boldsymbol{x} = \boldsymbol{0}$ の解全体 V とし $r(A) = r$ とすると V は $n-r$ 個の線型独立なベクトルを持ち V の任意の元はこれらの線型結合として書ける. 系として $n > m$ なら $A\boldsymbol{x} = \boldsymbol{0}$ が自明でない解を持つことと, $n = m$ (未知数 n, 方程式の数 m が一致する) ならば $A\boldsymbol{x} = \boldsymbol{0}$ が自明でない解を持つ $\Leftrightarrow A$ が正則でないことを得る. ゆえに, 自明でない解を $\boldsymbol{x}_0 = (x_1\ x_2 \cdots x_n)^t$ とおける. すると $A\boldsymbol{x} = \boldsymbol{0} \Leftrightarrow x_j = -\frac{1}{a_{jj}}(a_{j,1}x_1 + \cdots + a_{j,n}x_n)$ より $\boldsymbol{x}_0$ で最も絶対値が大きい成分を x_j とすると $|x_j| \le \frac{1}{|a_{j,j}|}(a_{j,1} + \cdots + a_{j,n})|x_j| < |x_j|$. 矛盾したので A は正則.

解 72. (イ) $A^{-1} = A^{k-1}$である. (ロ)A が正則であるとすると矛盾する. (ハ) $A^k = O$ となるある k が存在するならば A は正則でない. なぜなら $(A^{-1})^k A^k = O$ となってしまう. 行列の乗法は任意の行列に対しては可換ではないが成り立つ例もあり, $(E-A)(E+A+\cdots+A^{k-1}) = (E+A+\cdots+A^{k-1})(E-A) = E-A^k = E$ より $(E-A)^{-1} = E+A+\cdots+A^{k-1}$. 同様に $(E+A)(E-A+\cdots+(-1)^{k-1}A^{k-1}) = E-A+\cdots+(-1)^{k-1}A^{k-1}+A+\cdots+(-1)^{k-2}A^{k-1}+(-1)^{k-1}A^k = E$.

解 73. $X = (x_{ij}), Y = (y_{ij})$ とすると $tr(XY) = \sum_{i=1}^n (\sum_{j=1}^n x_{ij}y_{ji}), tr(YX) = \sum_{i=1}^n (\sum_{j=1}^n y_{ij}x_{ji}) = \sum_{j=1}^n (\sum_{i=1}^n x_{ij}y_{ji}) = \sum_{i=1}^n \sum_{j=1}^n x_{ij}y_{ji}$より $tr(XY-YX) = O$. もし問いの X, Y が存在するなら矛盾する.

解 74. $A \in M_{lm}, B \in M_{mn}$のとき $r(AB) \leq \min\{r(A), r(B)\}$ を示す. 第 4 章の章末を見よ.

解 75. $a_i x + b_i y + c_i z = d_i (1 \leq i \leq 3)$ に対してある 2 平面のみが平行である場合と 3 平面が平行である場合はこの方程式系が解を持たない. もし 3 平面が 1 点を共有つまり 3 本の法線ベクトルが一次独立である場合は方程式系は唯一の解を持つ. 3 平面が一つの直線を共有する時は方程式系は無限個の解を持つ. 問いは最後者の場合が満たす条件について訊いている

$$\cdot \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ -1 \end{pmatrix} = \mathbf{0}$$

における拡大係数行列$\tilde{A}$について $r(A) = r(\tilde{A}) \Leftrightarrow$ 方程式系が解を持つ.([9]P.59) もし $r(A) = r(\tilde{A}) = 3$ であれば 3 平面の共有点が求められ $r(A) = r(\tilde{A}) = 2$ であれば$\tilde{A}\begin{pmatrix} x & y & z & -1 \end{pmatrix}^t = \mathbf{0}$ から未知数 3 の方程式 2 つを等価的に得て共有する直線の式を未知数の一つを任意定数扱いして表記できる.
$r(A) = r(\tilde{A}) = 1$ となることは例えば $a_1x + b_1y + c_1z = d_1$ と $a_2x + b_2y + c_2z = d_2$が同じ平面を表すことになるのでない.

解 76. (イ)$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{b}{a^2+b^2} \\ \frac{-b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$より $a = b = 0$ でない限り正則. (ロ) 行列の和, 積, 逆行列が複素数の和, 積, 逆数と対応することは明らか. (ハ) $\alpha = a + bi = r(\cos\theta + i\sin\theta)$ で明らか.

解 77. (イ) 仮定より $P^tP = E$ で $P + E$ は正則である. $A^t = ((P-E)(P+E)^{-1})^t = ((P+E)^{-1})^t(P-E)^t = ((P+E)^t)^{-1}(P^t - E) = (P^t + P^tP)^{-1}(P^t - P^tP) = (P^t(E+P))^{-1}(P^t(E-P)) = (E+P)^{-1}(P^t)^{-1}P^t(E-P) = -(E+P)^{-1}(P-E)$. ここで

$$(P-E)(P+E) = (P+E)(P-E)$$

について $(P+E)^{-1}$ が存在するので

$$(P+E)^{-1}(P-E)(P+E)(P+E)^{-1} = (P+E)^{-1}(P+E)(P-E)(P+E)^{-1}$$

よって, $-A^t = A$ が成立する. (ロ) $A = (P+E)^{-1}(P-E)$ より $(E-A)(P+E) = P+E-(P-E)(P+E)^{-1}(P+E) = 2E$ であるので $E-A$ は正則である. (ハ) $(E+A)(E-A)^{-1} = (E-P+P+A)\frac{1}{2}(P+E) = \frac{1}{2}(E-P)(E+P) + \frac{1}{2}P(P+E) + \frac{1}{2}A(P+E) = \frac{1}{2}(E-P^2) + \frac{1}{2}(P^2+P) + \frac{1}{2}(P-E) = P$.

解 78. $A^*A = AA^* \Leftrightarrow$ 任意の x に対し $\|Ax\| = \|A^*x\|$ を示す. そこで任意の x に対して $\|Ax\| = \|A^*x\|$ であることと任意の x, y に対して $(Ax, Ay) = (A^*x, A^*y)$ が同値であることをいえば, $A^*A(x, y) = AA^*(x, y) \Leftrightarrow (Ax, Ay) = (A^*x, A^*y)$ より良い. 改めて

$$\|Ax\| = \|A^*x\| \Leftrightarrow (Ax, Ay) = (A^*x, A^*y)$$

を示す.

$$\|A^*(x+y)\| = \|Ax\|^2 + (A^*x, A^*y) + \overline{(A^*x, A^*y)} + \|Ay\|^2$$

$$\|A(x+y)\| = \|Ax\|^2 + (Ax, Ay) + \overline{(Ax, Ay)} + \|Ay\|^2$$

($\Rightarrow$) 上より (A^*x, A^*y) と (Ax, Ay) の実部は等しく x を ix に置き換えると虚部も等しいことがわかる.
($\Leftarrow$) まず $(Ax, Ay) = (A^*x, A^*y)$ ならば $A^*A = AA^*$をいう. これは次のように明らかである.

$$(x, (A^*A - AA^*)y) = (x, A^*Ay) - (x, AA^*y) = (Ax, Ay) - (A^*x, A^*y) = 0$$

次に $A^*A = AA^*$ならば $\|Ax\| = \|A^*x\|$ をいう. これは次のように明らか.

$$\|A^*x\|^2 = (A^*x, A^*x) = (\overline{A}^t x, \overline{A}^t x) = x^t(\overline{A}A^t)\overline{x} = x^t A^t \overline{A}\overline{x} = (Ax, Ax) = \|Ax\|^2$$

解 79. $[X, Y] = XY - YX = -[X, Y]^t$を示せばよい. X, Y が交代行列のとき $-[X, Y]^t = -(Y^tX^t - X^tY^t) = -(YX - XY) = [X, Y]$. (ハ)$X + Y \leftrightarrow \boldsymbol{x} + \boldsymbol{y}$ と $cX \leftrightarrow c\boldsymbol{x}$ は明らかである. $[X, Y] \leftrightarrow \boldsymbol{x} \times \boldsymbol{y}, X\boldsymbol{y} = \boldsymbol{x} \times \boldsymbol{y}$ も成り立つ. (ニ) 対応 $\mathbb{R}^3 \ni \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{pmatrix} \in$ (三次実対称行列全体)
によって示す等式はヤコビ恒等式に置き換わる.

解 80. (イ) $\Rightarrow$ (ロ) は非負行列の積が閉じていることから明らかであり逆を示す. $A\boldsymbol{x} = \boldsymbol{0}$ とする. このとき $A(-\boldsymbol{x}) = \boldsymbol{0}$ で条件より $\boldsymbol{x}$ と $-\boldsymbol{x}$ は非負ベクトルゆえ $\boldsymbol{x} = \boldsymbol{0}$. n 次正方行列 A に対して $A\boldsymbol{x} = \boldsymbol{0}$ が自明でない解を持つ $\Leftrightarrow$ A は正則でないので, A はいま正則である. A^{-1}が非負行列でないと仮定する. ある単位ベクトル $\boldsymbol{e}_j$に対し $A^{-1}\boldsymbol{e}_j$は非負ベクトルではない. (ロ) の対偶と $\boldsymbol{e}_j = AA^{-1}\boldsymbol{e}_j$より矛盾している. よって A^{-1}は非負行列である.

解 81. (イ) $\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1j} \\ \vdots \\ \sum_{j=1}^n a_{nj} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ より. (ロ) $\sum_{j=1}^n a_{ij} = 1, \sum_{j=1}^n b_{ij} = 1 (1 \le i \le n)$ ならば $\sum_{j=1}^n (AB)_{ij} = 1 (1 \le i \le n)$ を示す. $\sum_{j=1}^n (AB)_{ij} = \sum_{j=1}^n (a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}) = (a_{i1}b_{11} + a_{i2}b_{21} + \cdots + a_{in}b_{n1}) + \cdots + (a_{i1}b_{1n} + a_{i2}b_{2n} + \cdots + a_{in}b_{nn}) = a_{i1}(b_{11} + \cdots + b_{1n}) + a_{i2}(b_{21} + \cdots + b_{2n}) + \cdots + a_{in}(b_{n1} + \cdots + b_{nn}) = 1$ である.

解 82 (34 ページ)**.** $A \in M_{lm}(\mathbb{C}), B, C \in M_{mn}(\mathbb{C})$ とする. $A(B+C) = \begin{pmatrix} \sum_{k=1}^m a_{1k}(b_{k1} + c_{k1}) & \cdots & \sum_{k=1}^m a_{1k}(b_{kn} + c_{kn}) \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^m a_{lk}(b_{k1} + c_{k1}) & \cdots & \sum_{k=1}^m a_{lk}(b_{kn} + c_{kn}) \end{pmatrix}$

$\overset{\mathbb{C} \text{ 上の分配法則}}{=} \begin{pmatrix} \sum_{k=1}^m a_{1k}b_{k1} & \cdots & \sum_{k=1}^m a_{1k}b_{kn} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^m a_{lk}c_{k1} & \cdots & \sum_{k=1}^m a_{lk}c_{kn} \end{pmatrix} + \begin{pmatrix} \sum_{k=1}^m a_{1k}c_{k1} & \cdots & \sum_{k=1}^m a_{1k}c_{kn} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^m a_{lk}b_{k1} & \cdots & \sum_{k=1}^m a_{lk}b_{kn} \end{pmatrix} = AB + AC.$ 他
の等式の証明は略す.

解 83 (42 ページ)**.** (1)$\overline{AB} = \overline{A}\,\overline{B}$である. $E = \overline{E} = \overline{AA^{-1}} = \overline{A}\overline{A^{-1}}$より$\overline{A}^{-1} = \overline{A^{-1}}$. よって A が正則ならば$\overline{A}$も正則である. $E = E^t = (AA^{-1})^t = (A^{-1})^t A^t$ より $(A^t)^{-1} = (A^{-1})^t$. (2) 正方行列 A が正則であることと $\det A \neq 0$ は同値.

解 84 (48 ページ)**.** 行の入れ替えの操作はある行の定数倍と, ある行に他の行の定数倍を加えることでできる. 即ち (左 2) と (左 3), (右 2) と (右 3) で基本変形が指すことはできる. なぜなら $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \to \begin{pmatrix} a_1+b_1 & \cdots & a_n+b_n \\ b_1 & \cdots & b_n \end{pmatrix} \to \begin{pmatrix} a_1+b_1 & \cdots & a_n+b_n \\ -a_1 & \cdots & -a_n \end{pmatrix} \to \begin{pmatrix} b_1 & \cdots & b_n \\ a_1 & \cdots & a_n \end{pmatrix}$

解 85 (62 ページ)**.** (1) 明らか. (2)$\|x+y\|^2 = (x+y, x+y) = (x,x) + (x,y) + (y,x) + (y,y) = \|x\|^2 + \|y\|^2$. x, y が実ベクトルのとき $(x,y) = (y,x)$ より $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ のとき $0 = 2(x,y)$ すなわち $(x,y) = 0$. もし x, y が複素ベクトルなら $(x,y) + (y,x) = (x,y) + \overline{(x,y)} = 2Re(x,y)$ より $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ のとき $Re(x,y) = 0$ である. つまり任意の x, y に対する $(x,y) = 0$ は導かれない. よって次のような, x と y と直交しない例がある.

$$x = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix},\ y = \begin{pmatrix} iy_1 \\ iy_2 \\ \vdots \\ iy_n \end{pmatrix}\ x_i, y_j \in \mathbb{R}$$

解 86 (63 ページ)**.** x, y が実ベクトルなら $(x,y) = (y,x)$ より.

注 39 (65 ページ)**.** イ, ニの同値性は明快な証明であると思った. $A = \begin{pmatrix} \boldsymbol{a}_1 & \cdots & \boldsymbol{a}_n \end{pmatrix}$, $A^t = \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_n \end{pmatrix}$ に対して

$$A^t\overline{A} = \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_n \end{pmatrix} \begin{pmatrix} \overline{\boldsymbol{a}_1} & \cdots & \overline{\boldsymbol{a}_n} \end{pmatrix} = \begin{pmatrix} (\boldsymbol{a}_1, \boldsymbol{a}_1) & \cdots & (\boldsymbol{a}_1, \boldsymbol{a}_n) \\ & \ddots & \\ (\boldsymbol{a}_n, \boldsymbol{a}_1) & \cdots & (\boldsymbol{a}_n, \boldsymbol{a}_n) \end{pmatrix}$$

解 87 (65 ページ)**.** [6.4](1)(ニ) より, 求める二次直交群の第一列と第二列を $\boldsymbol{a} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$, $\boldsymbol{b} = \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix}$ とおくと $(\boldsymbol{a}, \boldsymbol{b}) = \cos(\theta - \varphi) = 0$ であるので $n \in \mathbb{Z}$ として$\varphi = \theta + \frac{\pi}{2} + n\pi$. よって二次直交行列は次の行列の列を逆にしたものも含めて

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

である.

(2) 任意の正方行列 $A \in M_{mn}$に対し $M = A^*A$ は $M^* = A^*A = M$ よりエルミート行列であり AA^*もまた同様. 対角成分が非負であることを示すため $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$, $A^* = \overline{A^t} =$

$\begin{pmatrix} \overline{a_{11}} & \cdots & \overline{a_{m1}} \\ & \ddots & \\ \overline{a_{1n}} & \cdots & \overline{a_{mn}} \end{pmatrix}$ とおく. $(A^*A)_{i,i} = \overline{a_{1i}}a_{1i} + \overline{a_{2i}}a_{2i} + \cdots + \overline{a_{mi}}a_{mi} = \sum_{j=1}^{m} |a_{ji}|^2$ である.

$a_{ji} = a_j + b_j i (a_j, b_j \in \mathbb{R}, 1 \leq j \leq m)$ とおくと $(A^*A)_{i,i} = \sum_{j=1}^{m} \overline{a_{ji}}a_{ji} = \sum_{j=1}^{m} {a_j}^2 + {b_j}^2 \geq 0$. AA^* もまた同様.

2.7 [9] 第 1 章

解 88. 点 A, B を結ぶ線分上の点の位置ベクトルは $t\boldsymbol{a} + s\boldsymbol{b}(t, s \geq 0, t + s = 1)$ と一意にかける.
そして三角形 ABC の境界含む内部の点は $t\boldsymbol{a} + s\boldsymbol{b} + r\boldsymbol{c}(t + s + r = 1, t, s, r \geq 0)$ と一意にかけることも示せる. これを一般化した命題平面上の凸多角形 $A_1A_2 \cdots A_n$の境界含む内部の点の位置ベクトルは $t_1\boldsymbol{a}_1 + \cdots + t_n\boldsymbol{a}_n(\sum_{i=1}^{n} t_i = 1, t_i \geq 0)$ と一意にかけることとその逆を示す. 凸 n 多角形は $n-2$ 個の三角形に分割され例えば三角形 $A_kA_{k+1}A_{k+2}$の内部の点の位置ベクトルは $t_k\boldsymbol{a}_k + t_{k+1}\boldsymbol{a}_{k+1} + t_{k+2}\boldsymbol{a}_{k+2}(t_k, t_{k+1}, t_{k+2}$はそれぞれ非負で和は 1) とかけ $k = 1, ..., n-2$ に対しても同様. 逆を示す. $n-1$ まで正しいとして帰納法を使う. $\boldsymbol{p} = t_1\boldsymbol{a}_1 + \cdots + t_n\boldsymbol{a}_n(t_1 + \cdots + t_n = 1, t_i \geq 0)$ とかけるとする. $t_n = 1$ なら $\boldsymbol{p} = \boldsymbol{a}_n$で良いから $t_n < 1$ とし $i \in \{1, ..., n-1\}$ に対し $s_i = \frac{t_i}{1-t_n}$とおくと $s_1 + \cdots + s_{n-1} = 1, s_i \geq 0$ より帰納法の仮定から $\boldsymbol{b} := \sum_{j=1}^{n-1} s_j\boldsymbol{a}_j$を位置ベクトルとする B は凸 $A_1 \cdots A_{n-1}$の境界含む内部に存在. $\boldsymbol{p} = (1 - t_n)\boldsymbol{b} + t_n\boldsymbol{a}_n$なので P は線分 BA_n上に存在する. B, A_nは凸 $A_1 \cdots A_n$の内部にあるので P も内部に存在する. よって n のときも成り立つ.

解 89. $x_1y_2 - x_2y_1 + x(y_1 - y_2) + y(x_2 - x_1) = 0$ は $(x_1, y_1), (x_2, y_2)$ を通る直線の方程式である. 実際 $x_1 \neq x_2$のとき $y = \frac{y_2-y_1}{x_2-x_1}x + \frac{x_2y_1-x_1y_2}{x_2-x_1}$. $x_1 = x_2$のとき $x(y_1 - y_2) - x_1(y_1 - y_2) = (x - x_1)(y_1 - y_2) = 0$ で P_1, P_2は異なるので $y_1 \neq y_2$より $x - x_1 = 0$ が直線の式である.

解 90. 平面上, 原点を通る任意の直線 $\ell : y = \tan\theta x$ に関する折り返しは $\mathbb{R}^2$の線型変換 T を引き起こす. $T(\boldsymbol{x}) = L\boldsymbol{x}$ となる L を考える. まず $\begin{pmatrix} r\cos(\alpha+\theta) \\ r\sin(\alpha+\theta) \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} r\cos\alpha \\ r\sin\alpha \end{pmatrix}$ より原点中心の回転行列は $R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$である. 直線 ℓに関する折り返しは原点を中心に $-\theta$回転し次に (x, y) を $(x, -y)$ に写し最後に原点を中心にθ回転することと同じなので行列の演算に反映すると $L_\theta = R_\theta f_{x\mapsto -x}R_{-\theta} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$である.

解 91. 前問の直線 $y = \tan\theta x$ と $y = \tan(-\theta)x$ に関する折り返しに対応する行列を用いる. 問いの主張とは点 $\begin{pmatrix} r\cos\alpha \\ r\sin\alpha \end{pmatrix} \in \mathbb{R}^2$に対して

$$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}\begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ -\sin 2\theta & -\cos 2\theta \end{pmatrix}\begin{pmatrix} r\cos\alpha \\ r\sin\alpha \end{pmatrix} = \begin{pmatrix} r\cos(\alpha+4\theta) \\ r\sin(\alpha+4\theta) \end{pmatrix}$$

が成り立つことである. これは実際に成り立つ.

補題 21 ([9], 19 及び 22)**.** 原点を $\boldsymbol{0}$ とする. 点 $\boldsymbol{x} \in \mathbb{R}^3$から単位方向ベクトルが $\boldsymbol{a}$ の直線に下ろした垂線の足を $\boldsymbol{y}$ とする. この変換 $f : \mathbb{R}^3 \ni \boldsymbol{x} \mapsto \boldsymbol{y} \in \mathbb{R}^3$は $\boldsymbol{y} = f(\boldsymbol{x}) = (\boldsymbol{a}, \boldsymbol{x})\boldsymbol{a}$ とかけ射影変換と呼ばれる. このとき f は線型変換である. そして, $\boldsymbol{a}$ が単位方向ベクトルでなく方向ベクトルのとき $\boldsymbol{y} = f(\boldsymbol{x}) = \frac{(\boldsymbol{a},\boldsymbol{x})}{(\boldsymbol{a},\boldsymbol{a})}\boldsymbol{a}$ である.

注 40. 点 $\boldsymbol{x} \in \mathbb{R}^3$から xy 平面に下ろした垂線の足を $\boldsymbol{y}$ とする. 図を書けば対応 $f : \mathbb{R}^3 \ni \boldsymbol{x} \mapsto \boldsymbol{y} \in \mathbb{R}^3$は明らかに $\boldsymbol{y} = (\boldsymbol{x}, \boldsymbol{e}_x)\boldsymbol{e}_x + (\boldsymbol{x}, \boldsymbol{e}_y)\boldsymbol{e}_y$かつ $\boldsymbol{y} = \boldsymbol{x} - (\boldsymbol{x}, \boldsymbol{e}_z)\boldsymbol{e}_z$を満たすことが分かる. f は線型写像である. なぜなら $f(a\boldsymbol{x}_1 + b\boldsymbol{x}_2) = af(\boldsymbol{x}_1) + bf(\boldsymbol{x}_2)$ が成り立つからである. 実際,

$$(\text{左辺}) = a\boldsymbol{x}_1 + b\boldsymbol{x}_2 - (a\boldsymbol{x}_1 + b\boldsymbol{x}_2, \boldsymbol{e}_z)\boldsymbol{e}_z = a\boldsymbol{x}_1 + b\boldsymbol{x}_2 - a(\boldsymbol{x}_1, \boldsymbol{e}_z)\boldsymbol{e}_z - b(\boldsymbol{x}_2, \boldsymbol{e}_z)\boldsymbol{e}_z$$

$$(\text{右辺}) = a(\boldsymbol{x}_1 - (\boldsymbol{x}_1, \boldsymbol{e}_z)\boldsymbol{e}_z) + b(\boldsymbol{x}_2 - (\boldsymbol{x}_2, \boldsymbol{e}_z)\boldsymbol{e}_z)$$

解 92. 平面の方程式 $ax + by + cz = 0$ において $\boldsymbol{a} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \boldsymbol{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$とおく. この平面に関する折り返しは $\mathbb{R}^3$の線型変換でありその変換公式を求めるのであるが, まず線型変換であることは, $\boldsymbol{x}$ に対する平面に関する折り返しを表す行列は平面への正射影ベクトルを $\boldsymbol{x}'$とすると $\boldsymbol{x}$ を $2\boldsymbol{x}' + (-\boldsymbol{x})$ へ変換するような行列であり, $\boldsymbol{x} \mapsto \boldsymbol{x}'$を表す射影変換は線型変換であって恒等変換 $\boldsymbol{x} \mapsto \boldsymbol{x}$ も線型変換であるのでその加法で得るものも線型変換であることより示される. [9], 22, 式 (5) で与えられている $\boldsymbol{x} \mapsto \boldsymbol{x}'$の変換行列を用いて求める折り返しを表す行列は

$$\boldsymbol{x} \mapsto 2\boldsymbol{x}' - \boldsymbol{x} = 2\left(\boldsymbol{x} - \frac{(\boldsymbol{a}, \boldsymbol{x})}{(\boldsymbol{a}, \boldsymbol{a})}\boldsymbol{a}\right) - \boldsymbol{x} = \boldsymbol{x} - \frac{2(\boldsymbol{a}, \boldsymbol{x})}{(\boldsymbol{a}, \boldsymbol{a})}\boldsymbol{a}$$

という変換を与える.

解 93. (イ) S とそれぞれの座標軸との交点は $(\frac{d}{a}, 0, 0), (0, \frac{d}{b}, 0), (0, 0, \frac{d}{c})$. 求める四面体の体積は $\frac{1}{3}|\frac{1}{2}\frac{d}{a}\frac{d}{b}\|\frac{d}{c}| = \frac{|d|^3}{6|abc|}$. (ロ)(イ) の四面体の底面の面積がいま求める三角形の面積である. 四面体の高さ即ち原点と S との距離を求めればよい. 原点を通り S と直交する直線は, S の方程式から平面 S の法線ベクトルが $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ なので k を任意の実数として $\boldsymbol{0} + k\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ である. これと S との交点 $\boldsymbol{h}$ は, $a(ka) + b(kb) + c(kc) = d$ より $k = \frac{d}{a^2+b^2+c^2}$で, $\boldsymbol{h} = \begin{pmatrix} \frac{ad}{a^2+b^2+c^2} \\ \frac{bd}{a^2+b^2+c^2} \\ \frac{cd}{a^2+b^2+c^2} \end{pmatrix}$ である. よって原点と S との間の距離は $\|\boldsymbol{h}\| = \frac{|d|}{\sqrt{a^2+b^2+c^2}}$. 三角形の面積を T とすると, $\frac{1}{3}\,T\frac{|d|}{\sqrt{a^2+b^2+c^2}} = \frac{|d|^3}{6|abc|}$ より $T = \frac{d^2\sqrt{a^2+b^2+c^2}}{2|abc|}$である.

解 94. (イ) 点 O, B, C を通る平面と A との距離は $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ が張る平行六面体を, $\boldsymbol{b}$ と $\boldsymbol{c}$ が定める面を底面とみたときの高さに当たる. そしてこれは [9], 25 及び 26 より $\frac{|\det(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})|}{\|\boldsymbol{b}\times\boldsymbol{c}\|}$である. (ロ) 点 A, B, C が決める ($\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ が決める, ではないことに注意.) 平行四辺形を BC を底辺とみたときの高さが, 直線 BC と点 A との距離である. 平行四辺形の面積は $\|\vec{CA} \times \vec{CB}\| = \|(\boldsymbol{a}-\boldsymbol{c})\times(\boldsymbol{b}-\boldsymbol{c})\| = \|(\boldsymbol{a}-\boldsymbol{b})\times(\boldsymbol{c}-\boldsymbol{b})\|$. 最後の等号が成り立つことは $\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ とかいたとき外積の分配法則により左辺は $\|\boldsymbol{a}\times\boldsymbol{c}-\boldsymbol{a}\times\boldsymbol{b}-\boldsymbol{b}\times\boldsymbol{c}+\boldsymbol{b}\times\boldsymbol{b}\|$, 右辺が $\boldsymbol{a}\times\boldsymbol{b}-\boldsymbol{a}\times\boldsymbol{c}-\boldsymbol{c}\times\boldsymbol{b}+\boldsymbol{c}\times\boldsymbol{c}$ で $\boldsymbol{b}\times\boldsymbol{b} = \boldsymbol{c}\times\boldsymbol{c} = 0$ より.

解 95. $\begin{pmatrix}(\boldsymbol{a},\boldsymbol{a}) & (\boldsymbol{a},\boldsymbol{b}) & (\boldsymbol{a},\boldsymbol{c})\\ (\boldsymbol{b},\boldsymbol{a}) & (\boldsymbol{b},\boldsymbol{b}) & (\boldsymbol{b},\boldsymbol{c})\\ (\boldsymbol{c},\boldsymbol{a}) & (\boldsymbol{c},\boldsymbol{b}) & (\boldsymbol{c},\boldsymbol{c})\end{pmatrix} = \begin{pmatrix}a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{pmatrix}\begin{pmatrix}a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{pmatrix}$ において $\det A^t = \det A$ より与式の左辺は $\det^2\begin{pmatrix}\boldsymbol{a} & \boldsymbol{b} & \boldsymbol{c}\end{pmatrix}$.

解 96. 辺の長さが全て 1 の平行六面体の体積 $|\det(\boldsymbol{x}\ \boldsymbol{y}\ \boldsymbol{z})|$ が最大となるのは平行六面体が立方体のときである.

解 97. もし $a = 0 \in V^3$ なら e_1 は通常のノルム 1 の V^3 の任意の元とし $a \neq 0$ のとき $e_1 = \frac{a}{\|a\|}$ とおく. e_1 と直交しノルム 1 の e_2 を, e_1 と b が線型独立なときは e_1 と b の張る平面上のベクトルから (e_1 と b が生成する V^2 の部分空間の元として) 選び, e_1 と b が線型従属なときは勝手に選び, $e_3 = e_1 \times e_2$ とおく. このとき

$$a = a_1e_1,\ b = b_1e_1 + b_2e_2,\ c = c_1e_1 + c_2e_2 + c_3e_3$$

である.

$$(a\times b)\times c = (a_1b_2e_1\times e_2)\times(c_1e_1+c_2e_2+c_3e_3) = a_1b_2c_1e_3\times e_1+a_1b_2c_2e_3\times e_2 = a_1b_2c_1e_2-a_1b_2c_2e_1$$

最後の等号は

$$e_3 \times e_1 = e_2,\ e_3 \times e_2 = -e_1$$

ということであるがこれは $e_3 \times e_1 = -(e_2 \times e_1) \times e_1 = -\{(e_2, e_1)e_1 - (e_1, e_1)e_2\}$ からも確かめられる. また (イ) の右辺と左辺は一致する. そして次が成り立つ.

$$\begin{aligned}(a \times b) \times c + (b \times c) \times a + (c \times a) \times b &\\ &= -(b, c)a + (a, c)b - (c, a)b + (b, a)c - (a, b)c + (c, b)a\\ &= (-(b, c) + (c, b))a + ((a, c) - (c, a))b + ((b, a) - (a, b))c = 0\end{aligned}$$

解 98 (13 ページ)**.** 任意の二つの平面に対し, その両方と直交する平面が存在する. すなわち任意の二平面の各法線ベクトルに対しても平行な平面が存在することを示す. 各法線ベクトルを $\boldsymbol{a}, \boldsymbol{b}$ として $\boldsymbol{a}$ と $\boldsymbol{b}$ が線型独立なら平面 : $t\boldsymbol{a} + s\boldsymbol{b}(t, s \in \mathbb{R})$ とこれに平行な平面が上の性質を満たす. もし $\boldsymbol{a}$ と $\boldsymbol{b}$ が線型独立でないなら (平行なら), $\boldsymbol{a}, \boldsymbol{c}$ が線型独立となるような $\boldsymbol{c}$ を任意にとって, 平面 : $t'\boldsymbol{a} + s'\boldsymbol{c}(t', s' \in \mathbb{R})$ とこれに平行な平面が上の性質を満たす.

解 99 (19 ページ)**.** この変換 T は $T\boldsymbol{p} = -\boldsymbol{p}$ を満たし明らかに線型写像である. 対応する行列は $\begin{pmatrix}-p\\ -q\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}p\\ q\end{pmatrix}$ より $-E_2$ である.

解 100 (19 ページ)**.** $\boldsymbol{x} = \begin{pmatrix}x\\ y\end{pmatrix}$ とおく.

$$\frac{ax + by}{a^2 + b^2}\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}a^2 & ab\\ ab & b^2\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} = T\begin{pmatrix}x\\ y\end{pmatrix}$$

である.

解 101 (19 ページ)**.** 3 つの内容は射影子の物理的意味から明らかである. 以下内積に関係する計算を簡単にするため $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x} \in \mathbb{R}^2$の場合を考える. (イ) $(\boldsymbol{a}, T\boldsymbol{x}) = (\boldsymbol{a}, \frac{(\boldsymbol{a},\boldsymbol{x})}{(\boldsymbol{a},\boldsymbol{a})}\boldsymbol{a}) \overset{\mathbb{R}^2\text{上の内積}}{=} \frac{(\boldsymbol{a},\boldsymbol{x})}{(\boldsymbol{a},\boldsymbol{a})}(\boldsymbol{a},\boldsymbol{a}) = (\boldsymbol{a},\boldsymbol{x})$ より $T^2\boldsymbol{x} = TT\boldsymbol{x} = \frac{(\boldsymbol{a},T\boldsymbol{x})}{(\boldsymbol{a},\boldsymbol{a})}\boldsymbol{a} = T\boldsymbol{x}$ となる. (ロ)$(\boldsymbol{a}, S\boldsymbol{x}) = (\boldsymbol{a}, \frac{(\boldsymbol{b},\boldsymbol{x})}{(\boldsymbol{b},\boldsymbol{b})}\boldsymbol{b}) \overset{(\boldsymbol{a},\boldsymbol{b})=0}{=} 0$ である. これより $(TS)\boldsymbol{x} = T(S\boldsymbol{x}) = \frac{(\boldsymbol{a},S\boldsymbol{x})}{(\boldsymbol{a},\boldsymbol{a})}\boldsymbol{a} = \boldsymbol{0}$ より. また $ST(\boldsymbol{x}) = S(T\boldsymbol{x}) = \boldsymbol{0}$ も成り立つ. (ハ)T の行列は前問より $M_T = \frac{1}{a^2+b^2}\begin{pmatrix} a^2 & ab \\ ab & b^2 \end{pmatrix}$ である. $\boldsymbol{a} = \begin{pmatrix} a \\ b \end{pmatrix}$とおくと $\boldsymbol{b} = \begin{pmatrix} -b \\ a \end{pmatrix}$とかけるので S の行列は $M_S = \frac{1}{a^2+b^2}\begin{pmatrix} b^2 & -ab \\ -ab & a^2 \end{pmatrix}$である. $M_T + M_S = E_2$. 線型写像なので $T\boldsymbol{x} + S\boldsymbol{x} = (M_T + M_S)\boldsymbol{x} = \boldsymbol{x}$.

解 102 (22 ページ)**.** 各空間的意味は (イ)y 軸に関して対称移動させる変換 (ロ)x 軸の周りに α回転する変換 (ハ) 直線 $x = y = z$ の周りに (y 軸から x 軸の方向に)$\frac{2}{3}\pi$点を回転させる. $\boldsymbol{a}$ への射影変換 T の行列は$\begin{pmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix}$であることは明らか.

解 103 (23 ページ)**.** (イ) $\boldsymbol{a} \in \mathbb{R}^3$に対する $T^2 = T$ は $\boldsymbol{a} \in \mathbb{R}^2$のときの証明と同様. 22 ページの (5) より $S\boldsymbol{x} = \boldsymbol{x} - T\boldsymbol{x}$ であるから $S^2\boldsymbol{x} = S(\boldsymbol{x} - T\boldsymbol{x}) = S\boldsymbol{x} - S(T\boldsymbol{x}) = S\boldsymbol{x} - (T\boldsymbol{x} - T^2\boldsymbol{x}) = S\boldsymbol{x}$ より $S^2 = S$ が成り立つ. (ロ)$TS\boldsymbol{x} = T\boldsymbol{x} - T^2\boldsymbol{x} = \boldsymbol{0}, ST\boldsymbol{x} = S(T\boldsymbol{x}) = T\boldsymbol{x} - T^2\boldsymbol{x} = \boldsymbol{0}$.

休憩所 次の内容を QR 分解という.

任意の正則行列 P はユニタリー行列 U, 上三角行列 T を用いて $P = UT$ とかける.

次を右極分解といい, また左極分解とは $M = PU$ とかけることを指す. M が正則なら表し方は一意.

任意の複素正方 [正則] 行列 M はユニタリー行列 U, 半正値 [正値] エルミート行列 P を用いて $M = UP$

任意の実正方 [正則] 行列 M は直交行列 U, 半正値 [正値] 実対称行列 P を用いて $M = UP$

正則行列 A を下三角行列 L と上三角行列 U の積として $A = LU$ とかくことを LU 分解という.

A が LU 分解可能である必要十分条件は $1 \leq \forall k \leq n$ に対し $|A_k| \neq 0$ となることである.

実正値対称行列 A に対し対角要素が全て正の下三角行列 L を用いて $A = LL^t$とかける.

2.8 [9] 第 7 章と関連する解析学

解 104 (205 ページ)**.** (1) $\boldsymbol{a}(t) = \begin{pmatrix} a_1(t) \\ a_2(t) \\ a_3(t) \end{pmatrix}$, $\boldsymbol{b}(t) = \begin{pmatrix} b_1(t) \\ b_2(t) \\ b_3(t) \end{pmatrix}$ とおく. (2) $(\boldsymbol{x}(t), \boldsymbol{x}'(t)) = (\boldsymbol{x}(t))^t \boldsymbol{x}'(t)$ は 0 となることをいう. $\|x(t)\| = const$ より $(x(t))^t x(t) = const$ の両辺を t で微分して $(x'(t))^t x(t) + (x(t))^t x'(t) = 0$. $k = (x(t))^t x'(t) \in \mathbb{R}$ とおくと $2k = 0$ より $k = 0$. よって示せた. (3) $A(t) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$ とすると $A'(0) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ で交代行列となっている. A を n 次直交行列とすると

$$A(t)^t A(t) = E_n$$

$$(A'(t))^t A(t) + A(t)^t A'(t) = 0$$

よって, $A'(0)^t + A'(0) = 0$ より $A'(0)$ は交代行列である.

定義 44. $n \geq 1$ に対する f_n と f を Ω 上の関数とする. 任意の $x \in \Omega$ に対し

$$\forall \epsilon > 0 \; \exists N(\epsilon) \; \forall n \; (n \geq N \to |f_n(x) - f(x)| < \epsilon$$

であるとき関数列 $\{f_n\}_n$ は f に一様収束するという.

命題 67. (1) 冪級数 $\sum_{n=0}^{\infty} c_n x^n$ が $x = x_0 (\neq 0)$ で収束すれば,
$0 < r < |x_0|$ を満たす任意の r に対して $\sum_{n=0}^{\infty} c_n x^n$ は閉区間 $[-r, r]$ で一様収束かつ絶対収束する. そして, $\sum_{n=0}^{\infty} c_n x^n$ は $[-r, r]$ で x の連続関数を表す.
(2) $\sum_{n=0}^{\infty} c_n x^n$ が $x = x_0 (\neq 0)$ で発散すれば, $|x_0| < |x|$ を満たす任意の x に対して
$\sum_{n=0}^{\infty} c_n x^n$ は発散する.

証明. $\sum_{n=0}^{\infty} c_n {x_0}^n$ は収束するから, $\lim_{n\to\infty} c_n {x_0}^n = 0$ である. ゆえに $\{c_n {x_0}^n\}_n$ は有界である. すなわち

$$n \geq 0 \text{ に対し } |c_n {x_0}^n| \leq M$$

を満たす 正数 M が存在する. 仮定より $0 < r < |x_0|, |x| < r$ であり,

$$|c_n x_n| = |c_n {x_0}^n| \left|\frac{x}{x_0}\right|^n \leq M \left|\frac{r}{x_0}\right|^n$$

である. $|\frac{r}{x_0}| < 1$ だから, $\sum_{n=0}^{\infty} M \left|\frac{r}{x_0}\right|^n$ は収束する. ワイエルシュトラスの判定法より, $\sum_{n=0}^{\infty} c_n x^n$ は $[-r, r]$ で一様絶対収束する. $c_n x^n$ は x の連続関数であり「連続関数を項とする級数 $\sum_{n=1}^{\infty} f_n$ が s に一様収束するとき, s は連続」$^{(*)}$なので $s := \sum_{n=0}^{\infty} c_n x^n$ は連続である. □

補題 22. (2.9) において使用する. Ω 上で定義された関数列 $\{f_n\}_n$ が f に一様収束することと $\lim_{n\to\infty} \|f_n - f\| = 0$ とは同値である.

命題 68. 前命題の証明における $(*)$ は次から明らか. Ω 上で定義された連続関数の列 $\{f_n\}$ が f に一様収束するなら, f は連続関数である.

証明. 点 $x_0 \in \Omega$を任意に固定する. f_nは f に一様収束するので前補題より

$$\forall \epsilon > 0 \exists N \in \mathbb{N} \forall n (n \geq N \to \|f_n - f\| < \frac{\epsilon}{3}) \tag{2.9}$$

f_Nは x_0で連続なので次が成り立つ.

$$\exists \delta > 0 \, (|x - x_0| < \delta \wedge x \in \Omega \to |f_N(x) - f_N(x_0)| < \frac{\epsilon}{3})$$

いま, $x \in \Omega$を任意に取り $|x - x_0| < \delta$とすると

$$f(x) - f(x_0)| \leq \|f(x) - f_N(x)| + |f_N(x) - f_N(x_0)| + |f_N(x_0) - f(x)| \leq 3\frac{\epsilon}{3} = \epsilon$$

が成り立つ. よって f は連続関数である. □

定義 45 (収束半径)**.** べき級数 $\sum_{n=0}^{\infty} c_n x^n$に対して

$$\rho = \sup\{r = |x_0|; \sum_{n=0}^{\infty} c_n {x_0}^n \text{は収束する}\}$$

とおくと $0 \leq \rho \leq \infty$ であって, 次の (1), (2) が成立する.
(1)$|x| < \rho$ならば $\sum_{n=0}^{\infty} c_n x^n$は収束する.
(2)$|x| > \rho$ならば $\sum_{n=0}^{\infty} c_n x^n$は発散する.
このρを冪級数 $\sum_{n=0}^{\infty} c_n x^n$の収束半径といい, $\{x \,|\, |x| < \rho\}$ をその収束円という.

証明. (2) はρの定義からそうである. (1) を示す. $|x| < \rho$よりρの定義から $|x| < |x_0| \leq \rho$, $\sum_{n=0}^{\infty} c_n {x_0}^n$ は収束するというような x_0が存在する. よって前定理から $\sum_{n=0}^{\infty} c_n x^n$は収束する. □

命題 69 (コーシー・アダマールの公式)**.** $\sum_{n=0}^{\infty} c_n a_n$の収束半径を$\rho$とすると

$$\rho = 1/\limsup_{n\to\infty} |c_n|^{1/n}$$

補題 23. 有界数列 $\{a_n\}_{n=1,2...}$に対して, $A_n = \{a_n, a_{n+1}, ...\}, \alpha_n = \inf A_n, \beta_n = \sup A_n$ $(n \geq 1)$ とする. このとき次が成り立つ.
・$\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n \leq \cdots \leq \beta_n \leq \cdots \leq \beta_1$
・数列 $\{\alpha_n\}, \{\beta_n\}$ は収束し, $\lim_{n\to\infty} \alpha_n \leq \lim_{n\to\infty} \beta_n$
極限 $\lim_{n\to\infty} \alpha_n$および $\lim_{n\to\infty} \beta_n$を数列 $\{a_n\}$ の下極限および上極限といい, $\liminf_{n\to\infty} a_n$および $\limsup_{n\to\infty} a_n$と表す. これらは実数の公理により存在する. 有界数列 $\{a_n\}$ が収束する必要条件は $\liminf_{n\to\infty} a_n = \limsup_{n\to\infty} a_n$が満たされることである.

ここで, 数列 $\{a_n\}$ が与えられたとき以下が成立する.
(1) ある$\beta \in \mathbb{R}$ が$\limsup_{n\to\infty} a_n$と一致するための条件十分条件は, 次が成立することである.
(∗) 任意の$\epsilon > 0$ に対して, $\{n; a_n \geq \beta + \epsilon\}$ は有限集合で, $\{n; a_n > \beta - \epsilon\}$ は無限集合である.
(2) ある$\alpha \in \mathbb{R}$ が$\liminf_{n\to\infty} a_n$と一致するための必要十分条件は次が成立することである.
(∗) 任意の$\epsilon > 0$ に対して, $\{n; a_n \leq \alpha - \epsilon\}$ は有限集合で, $\{n; a_n < \alpha + \epsilon\}$ は無限集合である.

証明. ご連絡は@societah までお願い致します. □

証明. $0 < \limsup_{n\to\infty}|c_n|^{1/n} = \beta < \infty$ の場合を証明する. 前補題より任意の$\epsilon > 0$ に対して $\{n; |c_n|^{1/n} \geq \beta + \epsilon\}$ は有限集合で, $\{n; |c_n|^{1/n} > \beta - \epsilon\}$ は無限集合である.
$|x| < \frac{1}{\beta}$とし, $|x| < \frac{1}{\beta+2\epsilon} < \frac{1}{\beta}$を満たす正数$\epsilon$をとる. この正数$\epsilon$に対して上に述べたことの前半を用いると, ある番号 N があって

$$n \geq N \text{ ならば } |c_n|^{1/n} < \beta + \epsilon$$

が成り立つ. よって, $n \geq N$ ならば

$$|c_n x^n| = |c_n||x|^n \leq (\beta+\epsilon)^n \left(\frac{1}{\beta+2\epsilon}\right)^n = \left(\frac{\beta+\epsilon}{\beta+2\epsilon}\right)^n$$

ここで $\left|\frac{\beta+\epsilon}{\beta+2\epsilon}\right| < 1$ だから, $\sum_{n=N}^{\infty}\left(\frac{\beta+\epsilon}{\beta+2\epsilon}\right)^n$ は収束する. よって, $\sum_{n=N}^{\infty} c_n x^n$も収束し, $\sum_{n=0}^{\infty} c_n x^n$も収束する.
次に $|x| > \frac{1}{\beta}$とする. すると, $|x| > \frac{1}{\beta-\epsilon} > \frac{1}{\beta}$を満たす正数$\epsilon$が存在する. はじめに述べたことの後半箇所から, $|c_n|^{1/n} > \beta - \epsilon$を満たす n が無限に存在する. すなわち $|c_n x^n| = |c_n||x^n| > (\beta-\epsilon)^n\left(\frac{1}{\beta-\epsilon}\right)^n = 1$ を満たす n が無限に存在する. よって $\lim_{n\to\infty} c_n x^n = 0$ は成り立たないから $\sum_{n=0}^{\infty} c_n x^n$は収束しない.
以上から $\sum_{n=0}^{\infty} c_n x^n$は $|x| < \frac{1}{\beta}$のとき収束し, $|x| > \frac{1}{\beta}$のとき発散する. ゆえに$\frac{1}{\beta}$が収束半径の値である. □

補題 24. $a_n \neq 0$ とする. $\sum_{n=1}^{\infty} a_n$において $\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| = r$ が存在し, $r < 1$ であれば $\sum_{n=1}^{\infty} a_n$は絶対収束する. また $r > 1$ ならば $\sum_{n=1}^{\infty} a_n$は発散する.

命題 70. $\sum_{n=0}^{\infty} c_n x^n$において, $\lim_{n\to\infty}|c_n/c_{n+1}|$ が存在すれば, これは収束半径の値に等しい.

証明. $\alpha = \lim_{n\to\infty}\left|\frac{c_n}{c_{n+1}}\right|$ とおく.$x \neq 0$ として,

$$\lim_{n\to\infty}\left|\frac{c_{n+1}x^{n+1}}{c_n x^n}\right| = \lim_{n\to\infty}\left|\frac{c_{n+1}}{c_n}\right||x| = \frac{|x|}{\alpha}$$

よって, 級数 $\sum_{n=0}^{\infty} c_n x^n$は $|x| < \alpha$のとき収束して $|x| > \alpha$のとき発散する. すなわちαは収束半径. □

命題 71 (収束半径)**.** $z \in \mathbb{C}$ と点 $z_0 \in \mathbb{C}$, 複素数列 $\{a_n\}$ に対して定まる $f(z) = \sum_{n=0}^{\infty} a_n(z-z_0)^n$ を冪級数という. この冪級数に対して R_0 $(0 \leq R_0 \leq \infty)$ を

$$\frac{1}{R_0} = \lim_{n\to\infty}\sup|a_n|^{1/n}$$

で定義する. このとき以下が成り立つ.
(1) 任意の $R < R_0$に対して冪級数は閉円板$\overline{\Delta}(z_0, R) = \{|z-z_0| \leq R\}$ 上で一様絶対収束する.
(2) $|z-z_0| > R_0$であれば冪級数は z において発散する.

証明. $0 < R_0 < \infty$ の場合を考える. まず (1) を示す. $0 < R_0 < R$ を満たす R を任意にとる. 任意の $n \geq N$ に対して $|a_n|^{1/n} \leq \frac{2}{R+R_0}$となるようなある N が存在する. $|z-z_0| \leq R$ を満たす $z \in \mathbb{C}$ に対して

$$|a_n||z-z_0|^n \leq \left(\frac{2R}{R+R_0}\right)^n (n \geq N)$$

であり

$$\sum_{n=0}^{\infty}\left(\frac{2R}{R+R_0}\right)^n = \frac{R_0+R}{R_0-R} < \infty$$

であることを考えるとワイエルシュトラスの判定法より冪級数 f(z) は $\overline{\Delta}(z_0, R)$ 上で一様絶対収束する.
次に (2) を示す. $|z-z_0| > R_0$を満たす $z \in \mathbb{C}$ を任意にとる. R を $|z-z_0| > R > R_0$を満たすようにとる. ここで, $|a_{n_j}|^{1/n_j} \geq 1/R$ かつ $n_j \to \infty (j \to \infty)$ となるような n_jが存在する.
このとき

$$|a_{n_j}||z-z_0|^{n_j} \geq \frac{1}{R^{n_j}}|z-z_0|^{n_j} > 1$$

である. よって冪級数は発散する. □

定義 46. 上の定理における非負整数 R_0 を冪級数の収束半径という.

命題 72 (208 ページ)**.** $A \in M_n(\mathbb{C})$ に対する

$$\exp(A) := \sum_{p=0}^{\infty}\frac{1}{p!}A^p$$

という級数は収束する.

証明. A のジョルダン標準形を $J = P^{-1}AP$ とすると

$$\sum_{p=0}^{k}\frac{1}{p!}A^p = P\left(\sum_{p=0}^{k}\frac{1}{p!}J^p\right)P^{-1}$$

なので, $\exp(J)$ が収束するならば$\exp(A)$ が収束するのでジョルダンセルに対する行列の指数関数 $\exp(J_m(\alpha))$ の収束性を考える.

$$\exp(J_m(\alpha)) = e^{\alpha}\begin{pmatrix} 1 & 1 & \frac{1}{2} & \frac{1}{6} & \cdots & \frac{1}{(m-1)!} \\ & \ddots & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & & & \frac{1}{6} \\ & & & \ddots & & \frac{1}{2} \\ & & & & \ddots & 1 \\ & & & & & 1 \end{pmatrix}$$

となるのでよい. もしくは $A \in M_{mn}(\mathbb{C})$ に対してノルム $\|A\|_2$を定義して

$$\|\sum_{k=0}^{\infty}\frac{1}{k!}A_2^k\| \leq \sum_{k=0}^{\infty}\frac{1}{k!}\|A\|_2^k = \exp(\|A\|_2)$$

より, $\exp(A)$ は絶対収束するから. □

命題 73 (209 ページ)**.** 行列 X, Y が可換なら

$$e^{X+Y} = e^X\, e^Y$$

であり, 特に $Y = -X$ とおくと $e^{-X} = (e^X)^{-1}$である.

証明. 別解 (88) □

命題 74 (210 ページ)**.** $\det U = 1$ を満たす任意の直交行列 U に対しある交代行列 $X(X^t = -X)$ が存在して $U = \exp(X)$ となる. 直交変換の理論や力学的な回転群 (特に微小な回転を起こす群) の話は, n 次元空間でのある軸に関する回転又は鏡映の後にある軸に関する回転についてだけに留まらず, 高速フーリエ変換や微分幾何学にも通じているそうでこの命題と並んで重要であると思う.

問 31. (イ) $\exp(X) = \begin{pmatrix}1&0\\0&1\end{pmatrix}+\begin{pmatrix}0&1\\1&0\end{pmatrix}+\frac{1}{2!}\begin{pmatrix}1&0\\0&1\end{pmatrix}+\frac{1}{3!}\begin{pmatrix}0&1\\1&0\end{pmatrix}+\cdots+ = \begin{pmatrix}1+\frac{1}{2!}+\frac{1}{4!}+\cdots & 1+\frac{1}{3!}+\frac{1}{5!}+\cdots\\ 1+\frac{1}{3!}+\frac{1}{5!}+\cdots & 1+\frac{1}{2!}+\frac{1}{4!}+\cdots\end{pmatrix} = \begin{pmatrix}\frac{1}{2}\sum_{n=0}^{\infty}\frac{1+(-1)^n}{n!} & \frac{1}{2}\sum_{n=0}^{\infty}\frac{1+(-1)^{n-1}}{n!}\\ \frac{1}{2}\sum_{n=0}^{\infty}\frac{1+(-1)^{n-1}}{n!} & \frac{1}{2}\sum_{n=0}^{\infty}\frac{1+(-1)^n}{n!}\end{pmatrix} = \begin{pmatrix}\frac{1}{2}(e+e^{-1}) & \frac{1}{2}(e-e^{-1})\\ \frac{1}{2}(e-e^{-1}) & \frac{1}{2}(e+e^{-1})\end{pmatrix}$

(ロ) $\exp(J) = \exp\begin{pmatrix}-1&0&0\\0&1&0\\0&0&2\end{pmatrix} = \begin{pmatrix}\sum_{k=0}^{\infty}\frac{(-1)^k}{k!} & 0 & 0\\ 0 & \sum_{k=0}^{\infty}\frac{1}{k!} & 0\\ 0 & 0 & \sum_{k=0}^{\infty}\frac{2^k}{k!}\end{pmatrix} = \begin{pmatrix}e^{-1}&0&0\\0&e&0\\0&0&e^2\end{pmatrix}$. $\exp(X) = P\exp(J)P^{-1} = \begin{pmatrix}1&1&2\\-1&0&1\\1&1&1\end{pmatrix}\begin{pmatrix}e^{-1}&0&0\\0&e&0\\0&0&e^2\end{pmatrix}\begin{pmatrix}1&-1&-1\\-2&1&3\\1&0&-1\end{pmatrix}$. (ハ) も同様に X のジョルダン標準形をまず計算する.

問 32. 211 ページの注意で定数係数 n 階微分方程式が 1 階微分方程式系に帰着され, 例 2 の方法で解けることが記されている. いま解く微分方程式系 $\begin{cases}x_1'(t) = x_1(t) + 2x_2(t)\\ x_2'(t) = 3x_1(t) - x_2(t) - 3x_3(t)\\ x_3'(t) = -x_1(t) + 2x_2(t) + 2x_3(t)\end{cases}$ もある 3 階微分方程式と同値であることが分かる. それを 1 階微分方程式系として考えることで考察する対象が簡単になったといえる. $A = \begin{pmatrix}1&2&0\\3&-1&-3\\-1&2&2\end{pmatrix}$ は前問の (ロ) の行列であり

$$\exp(tA) = P\exp(tJ)P^{-1} = \begin{pmatrix}1&1&2\\-1&0&1\\1&1&1\end{pmatrix}\begin{pmatrix}e^{-t}&0&0\\0&e^{t}&0\\0&0&e^{2t}\end{pmatrix}\begin{pmatrix}1&-1&-1\\-2&1&3\\1&0&-1\end{pmatrix}$$

命題 75 (213 ページ,[2.6] と 214 ページ)**.** $\|A\|_1$ が 1) ~ 4) の性質を持つことを確かめる. 2) においては $A, B \in M_{mn}$ とし 4) においては $A = (a_{ij}) \in M_{mn}(\mathbb{R})$, $B = (b_{ij}) \in M_{np}$ とする. 1) は明らかである. 2) は $|a_{ij} + b_{ij}| \le |a_{ij}| + |b_{ij}|$ より成り立つ. 3) も明らか. 4) 即ち

$$\sum_{i=1}^{m}\sum_{j=1}^{p}|\sum_{k=1}^{n}a_{ik}b_{kj}| \le (\sum_{i=1}^{m}\sum_{k=1}^{n}|a_{ik}|)(\sum_{j=1}^{p}\sum_{k=1}^{n}|b_{kj}|)$$

も成り立つ.
$\|A\|_2 := \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}|a_{ij}|^2}$ が性質を満たすことを確かめる.
1) は明らか. 3) は $\|cA\|_2 = \sqrt{\sum_{i,j}|ca_{ij}|^2} = |c|\sqrt{\sum_{i,j}|a_{ij}|} = |c|\|A\|_2$ より. $A, B \in M_n(\mathbb{R})$ とし

て 2) を示す.

$$\begin{aligned}
\|A+B\|_2^2 &= \sum_{i,j}^{n} |a_{ij}+b_{ij}|^2 \leq \sum_{i,j}^{n} (|a_{ij}|+|b_{ij}|)(|a_{ij}+b_{ij}|) \\
&= \sum_{i,j}^{n} |a_{ij}|\,|a_{ij}+b_{ij}| + \sum_{i,j}^{n} |b_{ij}|\,|a_{ij}+b_{ij}| \\
&\underset{(\sum_i^n x_i y_i)^2 \leq (\sum_i^n x_i{}^2)(\sum_i^n y_i{}^2)}{\leq} \sqrt{\sum_{i,j}^{n} |a_{ij}|^2}\sqrt{\sum_{i,j}^{n} |a_{ij}+b_{ij}|^2} + \sqrt{\sum_{i,j}^{n} |b_{ij}|^2}\sqrt{\sum_{i,j}^{n} |a_{ij}+b_{ij}|^2} \\
&= \|A\|_2\|A+B\|_2 + \|B\|_2\|A+B\|_2 = (\|A\|_2+\|B\|_2)\|A+B\|_2
\end{aligned}$$

よって $\|A+B\| = 0$ なら 2) では等号が成立するので $\|A+B\|_2 > 0$ の場合を考えると

$$\|A+B\|_2 < \|A\|_2 + \|B\|_2$$

である. 4) を示す. $C = AB = (c_{ij})$ とおく.

$$|c_{ij}|^2 = |\sum_k^n a_{ik}b_{kj}|^2 \leq (\sum_k^n |a_{ik}||b_{kj}|)^2 \leq (\sum_k^n |a_{ik}|^2)(\sum_k^n |b_{kj}|^2)$$

ここで i, j について総和を取ると

$$\|AB\|_2^2 = \sum_i^n \sum_j^n |c_{ij}|^2 \leq \|A\|_2^2\|B\|_2^2$$

であるので示すことができた. $\|A\|_0$が性質 1) から 4) を満たすことは略す.

問 33.

$$\mathrm{tr}(AA^*) = \mathrm{tr}(A^*A) = \sum_{i,j=1}^{n} |a_{ij}|^2$$

を示す.

$$(\text{左辺}) = \mathrm{tr}\begin{pmatrix} a_{11} & & a_{1n} \\ & \ddots & \\ a_{m1} & & a_{mn} \end{pmatrix}\begin{pmatrix} \overline{a_{11}} & & \overline{a_{m1}} \\ & \ddots & \\ \overline{a_{1n}} & & \overline{a_{mn}} \end{pmatrix} = (\text{右辺})$$

より成り立つ. 作用素ノルム $\|A\|_0 := \sup_{\|\boldsymbol{x}\|_2=1, \boldsymbol{x}\in\mathbb{R}^n} \|A\boldsymbol{x}\|_2$に対して

$$\|A\|_0^2 = A^*A \text{ の最大固有値}$$

を示す. A^*A は半正値エルミートよりあるユニタリー行列 U が存在して

$$U^{-1}A^*AU = \begin{pmatrix} {\alpha_1}^2 & & \\ & \ddots & \\ & & {\alpha_n}^2 \end{pmatrix},\ {\alpha_1}^2 \leq \cdots \leq {\alpha_n}^2$$

とかける. エルミート行列の固有値は非負であることを使った. $\boldsymbol{x}$ *s.t.* $\|\boldsymbol{x}\|_2 = 1$ に対し $\boldsymbol{y} := U^{-1}\boldsymbol{x} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ とおけば

$$(*) : (\boldsymbol{y}, \boldsymbol{y}) = (U^*\boldsymbol{x}, U^*\boldsymbol{x}) \overset{U^*U=E}{=} (\boldsymbol{x}, \boldsymbol{x}) = 1$$

よって

$$\begin{aligned} \|A\boldsymbol{x}\|_2^2 &= (A\boldsymbol{x}, A\boldsymbol{x}) = (A^*A\boldsymbol{x}, \boldsymbol{x}) = (A^*AU\boldsymbol{y}, U\boldsymbol{y}) \\ &= (U^*(A^*AU)\boldsymbol{y}, \boldsymbol{y}) \overset{(*)}{=} \sum_i^n {\alpha_i}^2 \leq {\alpha_n}^2 \end{aligned}$$

次より結論を得る.

$$\|A\|_0^2 = \left(\sup_{\|\boldsymbol{x}\|_2=1, \boldsymbol{x}\in\mathbb{R}^n} \|A\boldsymbol{x}\|_2 \right)^2 = {\alpha_n}^2$$

問 34. $\|A\|_1 \geq \|A\|_2$はよい. $\|A\|_2 \geq \|A\|_0$を示す. その為には $\|A\|_2 \geq \|A\boldsymbol{x}\|_2$であることを示せばよい. これは

$$\begin{aligned} \|A\boldsymbol{x}\|_2^2 &\overset{\|\cdot\|_2\text{の定義}}{=} \sum_i^n |\sum_j^n a_{ij}x_j|^2 \leq \sum_i^n (\sum_j^n |a_{ij}||x_j|)^2 \\ &\overset{\text{Cauchy, Schwarz}}{\leq} \sum_i^n (\sum_j^n |a_{ij}|^2)(\sum_j^n |x_j|^2) \\ &= \|A\|_2^2 \|\boldsymbol{x}\|_2^2 \end{aligned}$$

すなわち

$$\|A\boldsymbol{x}\|_2 \leq \|A\|_2 \, \|\boldsymbol{x}\|_2$$

及び $\|\boldsymbol{x}\|_2 = 1$ より成り立つ. 最後に

$$\|A\|_0 \geq \frac{1}{n^2}\|A\|_1$$

の成立を確かめたい. (33) の設定を用いる. $\mathrm{tr} : M_n(\mathbb{C}) \to \mathbb{C}$ はユニタリー変換で不変なので

$$\mathrm{tr}(A^*A) = \mathrm{tr}(U^*A^*AU) = \sum_{i=1}^n {\alpha_i}^2 = \sum_{i,j=1}^n |a_{ij}|^2$$

ここで $\|A\|_0^2 = (A^*A$ の最大固有値 ${\alpha_n}^2)$ であることを (33) で示したので証明すべきは次の不等式

$$\frac{1}{n^2}\sum_{i,j=1}^n |a_{ij}| \leq \alpha_n$$

である. いま分かっていることは

$$\sum_{i,j=1}^n |a_{ij}|^2 \leq n{\alpha_n}^2$$

である. Cauchy, Shwartz の不等式 $(\sum_i x_i y_i)^2 \leq \sum_i x_i^2 \sum_i y_i^2$ において $x_i \leftarrow |a_{ij}|$, $y_i \leftarrow 1$ を代入すると

$$\left(\sum_{i,j} |a_{ij}| \right)^2 \leq \sum_i |a_{ij}|^2 n^2 \leq n^3 {\alpha_n}^2$$

よって, 予定していたよりも強い

$$\frac{1}{n^{\frac{3}{2}}} \sum_{i,j=1}^{n} |a_{ij}| \leq \alpha_n$$

を示すことができた.

注 41 ($A \in M_n(\mathbb{R})$ に対しては成り立つ不等式を思い付いた)**.**

$$\|A\|_2 \geq \frac{1}{n} \|A\|_1$$

を示す. チェビシェフの不等式において $y_i := x_i (1 \leq i \leq n)$ とおくと各 x_iの大小関係は無視してよく

$$\frac{1}{n^2} \sum_{i=1}^{n^2} {x_i}^2 \geq \left(\frac{1}{n^2} \sum_{i=1}^{n^2} x_i \right)^2 \Rightarrow \frac{1}{n} \sqrt{\sum_{i=1}^{n^2} |x_i|^2} \geq \frac{1}{n^2} \sum_{i=1}^{n^2} |x_i|$$

が成り立つ. $x_i \leftarrow a_{ij}$ (x_iの番号 i が a_{ij}の番号 (i, j) に対応) として示せた.

注 42.

$$\|A\|_0 \leq \|A\|_2 \leq \sqrt{n} \|A\|_0$$

も成り立つことを証明することに成功した. $\|A\|_2 \leq \sqrt{n}\|A\|_0$は

$$\sqrt{\sum_{i,j}^{n} |a_{ij}|^2} \leq \sqrt{n}\, \alpha_n \Leftrightarrow \sum_{i,j=1}^{n} |a_{ij}|^2 \leq n\, {\alpha_n}^2$$

に帰着するが, これは前問より成り立つ.

命題 76. 正の正方行列 A は次を満たす正の固有値αを持つ. αを A のフロベニウス根という.
(イ) αの代数的重複度は 1 即ち単純特性根であり, 固有値αに対する正の固有ベクトル $\boldsymbol{u}$ が存在する.
(ロ) A の正の固有ベクトルは全て $\boldsymbol{u}$ の定数倍である. 即ちαを除く固有値に対する正の固有ベクトルは存在しない.
(ハ) A のαでない任意の固有値βに対して $|\beta| < \alpha$である.
(ニ) A^tのフロベニウス根は A のフロベニウス根に等しい.

証明. 証明をステップ毎に処理する. 有界な単調増加実数列は収束することや$\mathbb{R}^N$の部分空間 $\{\boldsymbol{x} \in \mathbb{R}^N \mid \|\boldsymbol{x}\| = 1\}$ において任意の点列が収束する部分列を持つ (i.e.点列コンパクト) ことを利用するなど面白い. □

命題 77 (222 ページ)**.** 非負の正方行列 A は次を満たす A の固有値αが存在する.
(イ) αは非負であり, A の任意の固有値βに対して $|\beta| < \alpha$
(ロ) αに対する非負固有ベクトルが存在する.

証明. 複素数値関数 $a_1(t), ..., a_n(t)$ (*s.t.* 各 $a_i(t)t = t_0$で連続) を係数にもつ多項式 $f(t, X) = X^n + a_1(t)X^{n-1} + \cdots + a_n(t)$ の根 α *s.t.* $f(t_0, \alpha) = 0$ に対して

$$\forall \epsilon > 0\ \exists \delta > 0\ \forall t\ (|t_0 - t| < \delta \to \exists \alpha(t)(f(t, \alpha(t)) = 0 \wedge |\alpha - \alpha(t)| < \epsilon))$$

が成り立つことから A の任意の固有値αは $A(t)$ の固有値$\alpha(t)$ の $t \to \infty$ の極限として存在する. □

章末問題

解 105. 曲率は曲線の曲がり具合の指標であることを表した数式が$\kappa(s) = \lim_{\Delta s \to 0} \frac{\Delta \theta}{\Delta s}$ (定義上の$\kappa(s) := \|\boldsymbol{a}_1'(s)\|$ も空間的に意味をもっていることが理解できる) であることの直観的な理解が先んじて重要である. 接線ベクトルを $\boldsymbol{a}_1, \boldsymbol{a}_1 + \Delta \boldsymbol{a}_1$とすれば

$$\lim_{\Delta s \to 0} \frac{\boldsymbol{a}_1 \times \Delta \boldsymbol{a}_1}{\Delta s} = \boldsymbol{a}_1 \times \boldsymbol{a}_1' \underset{\boldsymbol{a}_1' = \kappa \boldsymbol{a}_2}{=} \kappa \boldsymbol{a}_3$$

$\boldsymbol{x}$ と $\boldsymbol{y}$ がなす角をθとすると $\|\boldsymbol{x} \times \boldsymbol{y}\| = \|\boldsymbol{x}\|\,\|\boldsymbol{y}\| \sin\theta$より,

$$\|\boldsymbol{a}_1 \times \Delta \boldsymbol{a}_1\| \underset{\boldsymbol{a}_1 \times \boldsymbol{a}_1 = \boldsymbol{o}}{=} \|\boldsymbol{a}_1 \times (\boldsymbol{a}_1 + \Delta \boldsymbol{a}_1)\| \underset{\text{その二つの接戦ベクトルがなす角は}\Delta\theta}{=} \sin \Delta\theta$$

である. 即ち

$$\kappa \underset{\|\boldsymbol{a}_3\| = 1}{=} \|\kappa \boldsymbol{a}_3\| = \lim_{\Delta s \to 0} \frac{\sin \Delta\theta}{\Delta s} = \lim_{\Delta s \to 0} \frac{\Delta \theta}{\Delta s}$$

より成り立つ. 以下, 概要を把握せよ.
主法線ベクトル $\boldsymbol{a}_2(s) := \frac{1}{\kappa(s)} \boldsymbol{a}_1'(s)$ とは各点での曲がる向きの方向ベクトルを表しその定義より $\|\boldsymbol{a}_2(s)\| = 1$ を満たす. 従法線ベクトル $\boldsymbol{a}_3 := \boldsymbol{a}_1 \times \boldsymbol{a}_2$は

$$\boldsymbol{a}_3'(s) = -\tau(s) \boldsymbol{a}_2(s)$$

を満たし, この結び付ける$\tau(s)$ は曲線の捩率 (れいりつ, torsion) という. $-\tau(s)$ は各点において曲がる方向ベクトルが進行方向に対して左回りまたは右回りに捩れ (ねじれ) ていく分を表す指標で, それが実際に $\boldsymbol{a}_2(s)$ という瞬間での曲がる向きへのベクトルにかけられて $\boldsymbol{a}_3$の極小幅での変化率と結び付いている. 捩率がない例とは平面上の円 (半径を $a + \frac{b^2}{a}$ としよう) であり, ある例とは螺旋 ($\boldsymbol{x}(s) = \begin{pmatrix} a\cos s \\ a \sin s \\ bs \end{pmatrix}$, $\dot{\boldsymbol{x}}(s) = \begin{pmatrix} -a \sin s \\ a \cos s \\ b \end{pmatrix}$, $\|\dot{\boldsymbol{x}}(s)\| = \sqrt{a^2 + b^2}$ とする) であり, 両者は曲率は等しいが捩率の有無で決定的に異なる曲線となっている. なお, 螺旋の捩率は一定であることも確かめられるがこれも空間的な意味をもって理解できるだろう.
さて

$$\tau(s) = \lim_{\Delta s \to 0} \frac{\Delta \varphi}{\Delta s}$$

を示す.

$$\lim_{\Delta s \to 0} \frac{\boldsymbol{a}_3 \times \Delta \boldsymbol{a}_3}{\Delta s} = \boldsymbol{a}_3 \times \boldsymbol{a}_3' = \boldsymbol{a}_3 \times (-\tau(s) \boldsymbol{a}_2(s)) = -\tau(s) \boldsymbol{a}_1(s)$$

また

$$\|\boldsymbol{a}_3 \times \Delta\boldsymbol{a}_3\| = \|\boldsymbol{a}_3 \times (\boldsymbol{a}_3 + \Delta\boldsymbol{a}_3)\| = \sin\Delta\varphi$$

より

$$\tau(s) = \|\tau(s)\boldsymbol{a}_1(s)\| = \lim_{\Delta s\to 0}\frac{\sin\Delta\varphi}{\Delta s} = \lim_{\Delta s\to 0}\frac{\Delta\varphi}{\Delta s}$$

である. また, $\Delta\psi^2 = \Delta\theta^2 + \Delta\varphi^2$の関係がある. これはフルネ・セレの公式の第二列ベクトルより成り立つ. この演習問題に対して内積を用いた別解も考えてみよ.

解 106 (別解)**.** 曲率の定義は

$$\kappa(s) = \|\boldsymbol{a}_1'(s)\| = \|x''(s)\|$$

である. $a_1(s) = x'(s)$ と $a_1(s+\Delta s) = x'(s+\Delta s)$ の接戦のなす角$\Delta\theta$について

$$(x'(s), x'(s+\Delta s)) = \|x'(s)\|\,\|x'(s+\Delta s)\|\cos\Delta\theta$$

が成り立つ. また

$$\kappa(s)^2 = \lim_{\Delta s\to 0}\left\|\frac{x'(s+\Delta s) - x'(s)}{\Delta s}\right\|^2$$

より

$$\begin{aligned}\|x'(s+\Delta s) - x'(s)\|^2 &= (x'(s+\Delta s) - x'(s),\ x'(s+\Delta s) - x'(s))\\ &= \|x'(s+\Delta s)\|^2 + \|x'(s)\|^2 - 2\|x'(s)\|\|x'(s+\Delta s)\|\cos\Delta\theta\end{aligned}$$

近似式 $f(x) = f(0) + f'(0)x + \frac{1}{2}f''(y)x^2$ $(0 < y < x)$ を $\cos\Delta\theta$に適用すると

$$\cos\Delta\theta = 1 - \frac{1}{2}(\Delta\theta)^2\cos y,\quad \text{ただし } 0 < y < \Delta\theta$$

である. $\|x'(s)\| = 1$ であるので

$$\|x'(s+\Delta s) - x'(s)\|^2 = (\Delta\theta)^2\cos y$$

$$\kappa(s)^2 = \lim_{\Delta s\to 0}(\frac{\Delta\theta}{\Delta s})^2\cos y = \lim_{\Delta s\to 0}(\frac{\Delta\theta}{\Delta s})^2$$

解 107. もし B が正則行列だったら相似変換で固有多項式などが不変で $AB = B^{-1}(BA)B$ より AB と BA の特性方程式は等しい. B が正則行列でないときは $B(t) = B + tE_n$が十分小さい $t \neq 0$ で可逆であることから (B をジョルダン標準形 $P^{-1}BP$ にするように $B(t)$ の左から P^{-1}, 右から P をかける) 同様に $AB(t) = B(t)^{-1}(B(t)A)B(t)$ より$\Phi_{AB(t)} = \Phi_{B(t)A}$だから $t\to\infty$ の極限をとればよい.
十分小さい t に対して $B(t) = B + tE$ が可逆であることの理由は次の方が良いか. B が可逆でないとき (i.e. 固有値に 0 を含む) は十分小さい t に対して $B(t) = B + tE$ の固有値に 0 は含まれない (i.e. 可逆である)

解 108. $X=\begin{pmatrix}a & b\\ c & -a\end{pmatrix}$ に対し $J=P^{-1}XP=\begin{pmatrix}-\sqrt{a^2+bc} & 0\\ 0 & \sqrt{a^2+bc}\end{pmatrix}$, $P=\begin{pmatrix}\frac{a-\sqrt{a^2+bc}}{c} & \frac{a+\sqrt{a^2+bc}}{c}\\ 1 & 1\end{pmatrix}$ である. $\alpha:=\sqrt{|a^2+bc|}$ とおく. $\alpha\neq 0$, $a^2+bc>0$ ならば行列指数関数の定義より $P\exp(J)P^{-1}=\begin{pmatrix}\frac{a-\alpha}{c} & \frac{a+\alpha}{c}\\ 1 & 1\end{pmatrix}\begin{pmatrix}e^{-\alpha} & 0\\ 0 & e^{\alpha}\end{pmatrix}\begin{pmatrix}-\frac{c}{2\alpha} & \frac{1}{2}(\frac{a}{\alpha}+1)\\ \frac{c}{2\alpha} & \frac{1}{2}(1-\frac{a}{\alpha})\end{pmatrix}=\begin{pmatrix}\cosh\alpha+\frac{a}{\alpha}\sinh\alpha & \frac{b}{\alpha}\sinh\alpha\\ \frac{c}{\alpha}\sinh\alpha & \cosh\alpha-\frac{a}{\alpha}\sinh\alpha\end{pmatrix}$ となる.

$$e^{-\alpha}=\cosh\alpha-\sinh\alpha,\quad e^{\alpha}=\cosh\alpha+\sinh\alpha$$

を用いた. $a^2+bc<0$ の場合については, $\alpha=\sqrt{-(a^2+bc)}=i\sqrt{a^2+bc}$ に注意する. すると $P\exp(J)P^{-1}=\begin{pmatrix}\frac{a+i\alpha}{c} & \frac{a-i\alpha}{c}\\ 1 & 1\end{pmatrix}\begin{pmatrix}e^{i\alpha} & 0\\ 0 & e^{-i\alpha}\end{pmatrix}\begin{pmatrix}-\frac{c}{2\alpha}i & \frac{1}{2}\left(1-\frac{a}{i\alpha}\right)\\ \frac{c}{2\alpha}i & \frac{1}{2}\left(1+\frac{a}{i\alpha}\right)\end{pmatrix}=\begin{pmatrix}\cos\alpha+\frac{a}{\alpha}\sin\alpha & \frac{b}{\alpha}\sin\alpha\\ \frac{c}{\alpha}\sin\alpha & \cos\alpha-\frac{a}{\alpha}\sin\alpha\end{pmatrix}$ と計算される.

解 109. $\lim_{p\to\infty}(E+\frac{1}{p}A)^p=\exp(A)$ が成り立つ. $B_p:=\left(E+\frac{A}{p}\right)^p$ とおくと

$$B_p=E+A+\frac{A^2}{2!}(1-\frac{1}{p})+\cdots+\frac{A^p}{p!}(1-\frac{1}{p})(1-\frac{2}{p})\cdots(1-\frac{p-1}{p})\leq E+A+\frac{A^2}{2!}+\cdots+\frac{A^p}{p!}$$

と評価できる. $\exp(A)\leq\left(E+\frac{A}{p}\right)^{p+1}$ を示すことはできないか考えたが, 無理そうだった. そこで以下の解法を取る. A のジョルダン標準形 $J=P^{-1}AP=\begin{pmatrix}J_1 & & \\ & \ddots & \\ & & J_s\end{pmatrix}$ を考え, 各ジョルダンセル $J_i=\begin{pmatrix}\lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1\\ & & & \lambda_i\end{pmatrix}$ について命題の内容が成り立つか検討する. 即ちあるジョルダンセルを改めて $A\in M_n(\mathbb{C})$ とし $A=\begin{pmatrix}\lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1\\ & & & \lambda\end{pmatrix}=\lambda E_n+N$, $N=\begin{pmatrix}0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1\\ & & & 0\end{pmatrix}$ とする. このとき $\ell\geq n$ なら $(N_n)^{\ell}=O$ である. ジョルダンセルの場合に命題の主張が成り立つならば一般の行列の場合にも成り立つ. なぜなら $P\exp(J)P^{-1}=\exp(A)$ であり,

$$\lim_{p\to\infty}(E+\frac{1}{p}J)^p=\exp(J)\Rightarrow\lim_{p\to\infty}(E+\frac{1}{p}A)^p=P\exp(J)P^{-1}=\exp(A)$$

なので. そして

$$(E+\frac{A}{p})^p=\left((1+\frac{\lambda}{p})E+\frac{N}{p}\right)^p=(1+\frac{\lambda}{p})^pE+{}_pC_1(1+\frac{\lambda}{p})^{p-1}\frac{N}{p}+\cdots+{}_pC_{n-1}(1+\frac{\lambda}{p})^{p-n+1}(\frac{N}{p})^{n-1}+O+\cdots+O$$

ここで, 第一項は $(1+\frac{\lambda}{p})^pE\to e^{\lambda}E$, 第二項は $p\frac{(1+\lambda/p)^p}{1+\lambda/p}\frac{N}{p}\to e^{\lambda}N$, 第三項は $\frac{1}{2}e^{\lambda}N^2$ となるので結果,

$$\lim_{p\to\infty}(E+\frac{A}{p})^p=e^{\lambda}(E+N+\cdots+\frac{1}{(n-1)!}N^{n-1})\underset{(*)}{=}\exp(A)$$

最後の等号 $(*)$ については $\exp(A)$ の定義と次を確認せよ.

$$N^2 = \begin{pmatrix} 0 & 0 & 1 & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & \ddots & 0 \\ & & & & 0 \end{pmatrix}, \ \dots, \ N^{n-1} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

$$\exp(A) = \exp(J_n(\lambda)) = \begin{pmatrix} e^\lambda & e^\lambda & \frac{e^\lambda}{2} & \frac{e^\lambda}{6} & \cdots & \frac{e^\lambda}{(n-1)!} \\ & \ddots & & & & \vdots \\ & & \ddots & & & \frac{e^\lambda}{6} \\ & & & \ddots & \ddots & \frac{e^\lambda}{2} \\ & & & & \ddots & e^\lambda \\ & & & & & e^\lambda \end{pmatrix}$$

解 110 (別解)**.** 行列ノルム $\|\cdot\|$ の性質だけを用いる. 一般の $A \in M_n(\mathbb{C})$ に対し

$$\begin{aligned} \left\| \left(E + \frac{A}{p}\right)^p - \exp(A) \right\| &= \left\| \sum_{k=0}^{p} {}_pC_k \frac{A^k}{p^k} - \sum_{k=0}^{\infty} \frac{A^k}{k!} \right\| = \left\| \sum_{k=0}^{p} \frac{A^k}{k!} \left(\frac{p!}{(p-k)!p^k} - 1 \right) - \sum_{k=p+1}^{\infty} \frac{A^k}{k!} \right\| \\ &\leq \sum_{k=0}^{p} \frac{\|A^k\|}{k!} \left| \frac{p!}{(p-k)!p^k} - 1 \right| + \sum_{k=p+1}^{\infty} \frac{\|A^k\|}{k!} \end{aligned}$$

ここで, 任意の k, p $(0 \leq k \leq p)$ について $\frac{p!}{(p-k)!p^k} - 1 \leq 0$ である. $(p-k)!p^k \geq 0$ であり $p! - (p-k)!p^k \leq p! - p!p^k \leq 0$ より. よって

$$\leq \sum_{k=0}^{p} \frac{\|A\|^k}{k!} \left(1 - \frac{p!}{(p-k)!p^k} \right) + \sum_{k=p+1}^{\infty} \frac{\|A^k\|}{k!} = \sum_{k=0}^{\infty} \frac{\|A\|^k}{k!} - \sum_{k=0}^{p} \frac{{}_pC_k}{p^k} \|A\|^k$$

$$= \exp(\|A\|) - \left(1 + \frac{\|A\|}{p}\right)^p \ (\text{数の級数}) \overset{p\to\infty}{\to} 0$$

よって, [9], 213 ページの (10) により

$$\left(E + \frac{A}{p}\right)^p \overset{p\to\infty}{\to} \exp(A)$$

となる.

命題 78. 任意の正方行列 X に対し

$$\cos(X) := \sum_{p=0}^{\infty} \frac{(-1)^n}{(2n)!} X^{2n}, \ \ \sin(X) := \sum_{p=0}^{\infty} \frac{(-1)^n}{(2n+1)!} X^{2n+1}$$

は収束する. 以下のステップを取る.

補題 25 (コーシー, アダマール)**.** 冪級数 $\sum_{n=0}^{\infty} a_n(z-z_0)^n$ $(z, z_0 \in \mathbb{C})$ に対してある K が存在し

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| = K$$

となるとする. このとき冪級数の収束半径 R は

$$R = \frac{1}{K}$$

である. $K = 0$ なら冪級数は収束し $R = \infty$ とかき, K が発散するなら $R = 0$ であり冪級数は $z = z_0$以外の任意の点で発散する.

補題 26. 複素冪級数 $\sum_{n=0}^{\infty} a_n x^n$の収束半径を R とする. もし $\|A\| < R$ ならば冪級数 $\sum_{n=0}^{\infty} a_n A^n$ は収束する. ただし $A \in M(\mathbb{C})$ とし A に対して定まるノルム $\|A\|$ は作用素ノルム $\|\cdot\|_0$としておく.

証明. まず

$$\|A\| \le a \Rightarrow \|A^n\| \le a^n$$

をいう. これは $\|A^n\|_0 := \sup_{\|x\|=1}\|AA^{n-1}x\|_2 \le a\|A^{n-1}\|_0 \le \cdots \le a^n$より成立する. 部分列 $\sum_{n=0}^{n} a_n A^n$がコーシー列となることをいえば, $\sum_{n=0}^{\infty} a_n A^n$は収束することがわかる. そこで $r > q$ として

$$\|\sum_{n=0}^{r} a_n A^n - \sum_{n=0}^{q} a_n A^n\| = \|\sum_{n=q}^{r} a_n A^n\| \le \sum_{n=q}^{r}\|a_n A^n\|$$

である. なお最後の不等式は [9], 213 ページのノルムの性質 [2.6](2) による. さらに冒頭の事実より

$$\lim_{r,q\to\infty}\sum_{n=q}^{r}\|a_n A^n\| \le \lim_{r,q\to\infty}\sum_{n=q}^{r}|a_n|\,\|A\|^n$$

となり, 仮定の $\|A\| < r$ かつ $\sum_{n=0}^{\infty} a_n x^n$の収束半径 R が $R < r$ なら収束することから

$$\lim_{q,r\to\infty}\sum_{n=r}^{q}\|a_n A^n\| \to 0$$

が成り立つ. よって部分列はコーシー列であり, 空間 $M(\mathbb{C})$ は完備だから部分列がコーシー列ならば収束する. □

解 111. $\sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}\theta^{2n}$の収束半径は ∞ である. 任意の $X \in M_n(\mathbb{C})$ に対して $\|X\| < \infty$ より補題から $\cos(X)$ と $\sin(X)$ は収束する. 関係式 $\exp(X) = \cos(X) + i\sin(X)$ を満たす.

解 112. $A \in M_n(\mathbb{C})$ が冪零行列であることと A の固有値が全て 0 であることは同値. そこで A が冪零でない即ちある 0 でない固有値 α を A は持つと仮定する. すると $\frac{1}{\alpha}A$ は 1 を固有値にもつ (i.e. $\exists \boldsymbol{x} \neq \boldsymbol{0}; \frac{1}{\alpha}A\boldsymbol{x} = \boldsymbol{x}$) ので $\sum_{p=0}^{\infty}\frac{1}{\alpha^p}A^p$は収束しない. なぜならもし収束するとすると $K = \sum_{p=0}^{\infty}\frac{1}{\alpha^p}A^p\boldsymbol{x}$ もある一定の行列になるが $K = \boldsymbol{x}E + \boldsymbol{x} + \cdots +$ は収束しないからである. また仮定より十分大きい p に対しては $\|A^p\|^{1/p} < |\alpha|$ となる. よって $r^p := \frac{|\alpha|^p}{|\alpha^p|}$で定義すると $r^p < 1$ であり,

$$\|\frac{1}{\alpha^p}A^p\| \le r^p < 1$$

が成り立つ.

$$\sum_{p=0}^{\infty} \|\frac{1}{\alpha^p}A^p\| \leq \sum_{p=0}^{\infty} r^p = \frac{1}{1-r}$$

より絶対収束する. 絶対収束するならば収束する. これは矛盾する.

解 113. $\rho(A)$ を A の最大固有値としてかく. ペロン・フロベニウスの定理より, 任意の A の固有値 βに対して $|\beta| < \alpha$なので $\alpha = \rho(A) \geq 0$ である. $\rho > \alpha$のとき $\frac{1}{\rho}A$ の固有値は 0 以上 1 より小さいから (「絶対値は 1 より小さい」ではない)

$$(\rho E - A)^{-1} = \left(\rho(E - \frac{A}{\rho})\right)^{-1} = \frac{1}{\rho}\left(E + \frac{A}{\rho} + (\frac{A}{\rho})^2 + \cdots\right) \geq O$$

逆に, $B := (\rho E - A)^{-1} \geq O$ とする. αに対する A の非負固有ベクトル $\boldsymbol{u}$ が存在し

$$B\boldsymbol{u} = (\rho E - A)^{-1}\boldsymbol{u} = \frac{1}{\rho}\left(E + \frac{A}{\rho} + (\frac{A}{\rho})^2 + \cdots\right)\boldsymbol{u} = \frac{1}{\rho - \rho(A)}\boldsymbol{u}$$

非負行列と非負固有ベクトルの積も非負であるので $\rho > \alpha$が成り立つ.

補題 27. λ を $|\lambda| < 1$ を満たす数とする. $\lim_{p\to\infty} \lambda^p = 0$ が成り立つ.

証明. 微積分学におけるϵN 論法で示せ. □

解 114. 成分が全て 1 の列ベクトル $\boldsymbol{u}$ を A のフロベニウス根 1 に対する唯一の固有ベクトル (i.e. 1 に対する固有空間の次元は 1) としてかく. $\boldsymbol{u}$ を第一列にもつ正則行列 $U = \begin{pmatrix}\boldsymbol{u} & * & \cdots & *\end{pmatrix}$を適当に選べば $U^{-1}AU = \begin{pmatrix}1 & \boldsymbol{0}^t \\ \boldsymbol{0} & A_1\end{pmatrix}$となり, またペロン・フロベニウスの定理より A_1の固有値の絶対値は 1 より小さい. $|\lambda_i| < 1$ *s.t.* $A_1\boldsymbol{x} = \lambda_i\boldsymbol{x}$ のとき $A_1^p\boldsymbol{x} = \lambda_i^p\boldsymbol{x}$ であり, 固有値が全て 0 ならば冪零行列であることから補題 (27) より $\lim_{p\to\infty} A_1^p = O$ である. よって

$$\lim_{p\to\infty} U^{-1}A^pU = \lim_{p\to\infty}\begin{pmatrix}1 & \boldsymbol{0}^t \\ \boldsymbol{0} & A_1\end{pmatrix}^p = \begin{pmatrix}1 & \boldsymbol{0}^t \\ \boldsymbol{0} & O\end{pmatrix}$$

$U^{-1} := \begin{pmatrix}b_1 & b_2 & \cdots & b_n \\ * & * & \cdots & * \\ \vdots & & & \vdots \\ * & * & \cdots & *\end{pmatrix}$とおくと $\lim_{p\to\infty} A^p = U\begin{pmatrix}1 & \boldsymbol{0}^t \\ \boldsymbol{0} & O\end{pmatrix}U^{-1} = B$ となる. A, B が確率行列なら AB も確率行列なので B は確率行列である.

$A \in M_3(\mathbb{R})$ とすると確かに $\begin{pmatrix}1 & u_{12} & u_{13} \\ 1 & u_{22} & u_{23} \\ 1 & u_{32} & u_{33}\end{pmatrix}\begin{pmatrix}1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}b_1 & b_2 & b_3 \\ u'_{21} & u'_{22} & u'_{23} \\ u'_{31} & u'_{32} & u'_{33}\end{pmatrix} = \begin{pmatrix}b_1 & b_2 & b_3 \\ b_1 & b_2 & b_3 \\ b_1 & b_2 & b_3\end{pmatrix}$と計算できる. A が対称行列ならそれを無限回かけてできる B も対称行列なので $b_1 = b_2 = \cdots = b_n$ より B の各成分は $1/n$ である.

注 43. 上問の明快な解説を記録する. $A = (a_{ij}) \in M_n(\mathbb{R})$ $(s.t.\ a_{ij} > 0,\ \sum_{j=1}^{n} a_{ij} = 1)$ はペロン・フロベニウスの定理より固有空間の次元が 1 である固有値 1 と, その他の絶対値 1 未満の固有値を持つ. よって A のジョルダン標準形 $U^{-1}AU$ のジョルダンセルは, 一つのセルは

$$\begin{pmatrix} 1 \end{pmatrix}$$

であって, その他は

$$\lambda E_k + N$$

という形 (ただし $|\lambda| < 1$) をしている. $U^{-1}A^nU = (U^{-1}AU)^n$もこのセルを用いて

$$\begin{pmatrix} 1 \end{pmatrix}$$

と

$$(\lambda E_k + N)^n = \sum_{i=0}^{n} {}_nC_i \lambda^{n-i} N^i$$

というセルの直和になる. また $N^i = 0\ (if\ i \geq k)$ なので

$$(\lambda E_k + N)^n = \lambda^n E_k + \lambda^{n-1}{}_nC_1 N + \cdots + \lambda^{n-k+1}{}_nC_{k-1} N^{k-1}$$

であり, $E_k, N, N^2, ..., N^{k-1}$の係数は$\lambda^{n-j}{}_nC_j$; $(j = 0, 1, ..., k-1)$ は $n \to \infty$ のとき 0 に収束する. これより,

$$\lim_{n\to\infty} U^{-1}A^nU = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = R$$

ここで R のランクは 1 なので URU^{-1}のランクも 1 である. A の各成分が正なので URU^{-1} の各成分は 0 以上 (0 より大きい, ではないことは極限を考慮せよ.) で A^nは確率行列より URU^{-1}も確率行列である. ランクが 1 より

$$B := URU^{-1} = \begin{pmatrix} p_1 & \cdots & p_n \\ \vdots & & \vdots \\ p_1 & \cdots & p_n \end{pmatrix},\ p_1, ..., p_n \geq 0,\ \sum_{i=1}^{n} p_i = 1$$

2.9 [9] 多項式

命題 79. $\mathbb{K}$ 係数多項式 $f(x), g(x)$ の最大公約数 $d(x)$, 最小公倍数 $m(x)$ に対して

$$d(x)m(x) = cf(x)g(x),\ 0 \neq c \in \mathbb{K}$$

解 115. [9], 227 ページ, [1.4] を用いる.

解 116.

$$R(f,g) = {a_0}^m {b_0}^n \prod_{i,j=1}^{n,m} (\alpha_i - \beta_j)$$

を示せば, $f(x)$ と $g(x)$ が共通の零点をもつことと $R(f,g) = 0$ は同値であることが分かるのでこれを示す. まず

$$V(x_1, ..., x_n) := \begin{vmatrix} {x_1}^{n-1} & {x_2}^{n-1} & \cdots & {x_n}^{n-1} \\ {x_1}^{n-2} & {x_2}^{n-2} & \cdots & {x_n}^{n-2} \\ \vdots & & & \vdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{vmatrix} = \prod_{i,j=1}^{n} (x_i - x_j)$$

である. 設定より

$$\begin{cases} a_0{\beta_i}^{n+k} + a_1{\beta_i}^{n-1+k} + \cdots + a_{n-1}{\beta_i}^{1+k} + a_n{\beta_i}^k = {\beta_i}^k f(\beta_i) \\ a_0{\alpha_i}^{n+k} + a_1{\alpha_i}^{n-1+k} + \cdots + a_{n-1}{\alpha_i}^{1+k} + a_n{\alpha_i}^k = 0 \\ b_0{\beta_i}^{m+k} + b_1{\beta_i}^{m-1+k} + \cdots + b_{m-1}{\beta_i}^{1+k} + b_m{\beta_i}^k = 0 \\ b_0{\alpha_i}^{m+k} + b_1{\alpha_i}^{m-1+k} + \cdots + b_{m-1}{\alpha_i}^{1+k} + b_m{\alpha_1}^k = {\alpha_i}^k g(\alpha_i) \end{cases}$$

であるから

$$R(f,g)V(\beta_1, ..., \beta_m, \alpha_1, ..., \alpha_n)$$

$$= \begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & \cdots & a_n & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & \cdots & b_m & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix} \begin{vmatrix} {\beta_1}^{n+m-1} & \cdots & {\beta_m}^{n+m-1} & {\alpha_1}^{n+m-1} & \cdots & {\alpha}^{n+m-1} \\ {\beta_1}^{n+m-2} & \cdots & {\beta_m}^{n+m-2} & {\alpha_1}^{n+m-2} & \cdots & {\alpha_n}^{n+m-2} \\ \vdots & & & & & \vdots \\ \beta_1 & \cdots & \beta_m & \alpha_1 & \cdots & \alpha_n \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{vmatrix}$$

$$\underset{\det AB = \det A \det B}{=} \begin{vmatrix} {\beta_1}^{m-1} f(\beta_1) & \cdots & {\beta_m}^{m-1} f(\beta_m) & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ f(\beta_1) & \cdots & f(\beta_m) & 0 & \cdots & 0 \\ 0 & \cdots & 0 & {\alpha_1}^{n-1} g(\alpha_1) & \cdots & {\alpha_n}^{n-1} g(\alpha_n) \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & g(\alpha_1) & \cdots & g(\alpha_n) \end{vmatrix}$$

これに対して $\det(\boldsymbol{x}_1 \cdots\ c\boldsymbol{x}_i\ \cdots\ \boldsymbol{x}_\ell) = c\det(\boldsymbol{x}_1 \cdots\ \boldsymbol{x}_i \cdots \boldsymbol{x}_\ell)$ と $\begin{vmatrix} A & O \\ O & B \end{vmatrix} = |A|\,|B|$ という行列式の性質より

$$(\text{上式}) = f(\beta_1)\cdots f(\beta_m)g(\alpha_1)\cdots g(\alpha_n)V(\beta_1,...,\beta_m)V(\alpha_1,...,\alpha_n)$$

よって

$$R(f,g)V(\alpha_1,...,\alpha_n)V(\beta_1,...,\beta_m)\prod_{i,j}(\beta_i-\alpha_j) = a_0^m\prod_{i,j}(\beta_i-\alpha_j)b_0^n\prod_{i,j}(\alpha_i-\beta_j)V(\beta_1,...,\beta_m)V(\alpha_1,...,\alpha_n)$$

より結論を得る. 前式は次の (i), (ii) より成り立つ.

$$(i)\ V(\beta_1,...,\beta_m,\alpha_1,...,\alpha_n) = V(\beta_1,...,\beta_m)V(\alpha_1,...,\alpha_n)\prod_{i,j}(\beta_i-\alpha_j)$$

$$(ii)\ a_0^m\prod_{i,j}(\beta_i-\alpha_j) = f(\beta_1)\cdots f(\beta_m)$$

$\mathbb{C}$ の範囲では n 次 $\mathbb{K}$ 係数多項式は一次式の積に因数分解され, $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ であるので

$$(\text{右辺}) = \{a_0(\beta_1-\alpha_1)\cdots(\beta_1-\alpha_n)\}\cdots\{a_0(\beta_m-\alpha_1)\cdots(\beta_m-\alpha_n)\} = a_0^m\prod_{i,j}(\beta_i-\alpha_j) = (\text{左辺})$$

同様に

$$b_0^n\prod_{i,j}(\alpha_i-\beta_j) = g(\alpha_1)\cdots g(\alpha_n)$$

である. 以上より

$$R(f,g) = a_0^m b_0^n\prod_{i,j}(\alpha_i-\beta_j)$$

解 117.

$$R(f,f') = (-1)^{\frac{n(n-1)}{2}}a_0^{2n-1}D(f)$$

の誤植に注意する. また n 変数の差積とは $\Delta(x_1,...,x_n) = \prod_{i<j}(x_j-x_i) = \{(x_n-x_{n-1})(x_n-x_{n-2})\cdots(x_n-x_1)\}\cdots\{(x_3-x_2)(x_3-x_1)\}\{(x_2-x_1)\}$ で定められる.
n 次多項式 $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$ に対する導関数は $g(x) = a_0\sum_{i=1}^n(x-\alpha_1)\cdots(x\ \hat{-}\ \alpha_i)\cdots(x-\alpha_n)$ であるので

$$g(\alpha_i) = a_0\prod_{j\neq i}(\alpha_i-\alpha_j)$$

である. 前問より x に関する n 次多項式 f, m 次多項式 g に対する終結式について

$$R(f,g) = a_0^m\prod_{i=1}^n g(\alpha_i)\left(= (-1)^{mn}b_0^n\prod_{j=1}^m f(\beta_j)\right)$$

であり, g を f' とすると

$$R(f,g) = a_0^{n-1}\prod_{i=1}^n a_0\prod_{j\neq i}(\alpha_i-\alpha_j) = (-1)^{\frac{n(n-1)}{2}}a_0^{2n-1}\left(\prod_{i<j}(\alpha_j-\alpha_i)\right)^2$$

である. 結論を得た. 最後の等号において例として $n = 3$ なら $\prod_i \prod_{j\neq i}(\alpha_i - \alpha_j) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) = -((\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1))^2$ と検算して確かめてみると良い.

命題 80. n^2個の変数 x_{ij}の斉次一次多項式として n 次行列式 $\det(x_{ij})$ は $\mathbb{C}$ 上既約である.

証明. ここで多項式 $h(x)$ が既約であるとは $h(x) = f(x)g(x)$ ならば $f(x)$ または $g(x)$ が定数または $h(x)$ の定数倍であることを指す. 既約の概念は環論を勉強するとより一般化される. n^2変数多項式 $\det(x_{ij})$ が既約であることを示すため,

$$\det(x_{ij}) = f(x_{11}, ..., x_{1n}, \cdots, x_{n1}, ..., x_{nn})g(x_{11}, ..., x_{1n}, \cdots, x_{n1}, ..., x_{nn})$$

とかけたとする. 第 1 行のみを変数と思うと $\det(x_{ij})$ は n 変数斉次一次式より f が x_{11}を含めば行列式の定義より g は x_{1j} $(1 \leq j \leq n)$ を含まない. よって f は x_{1j}を含む. 第 j 列を変数と思えば g は x_{ij} $(1 \leq i \leq n)$ を含まないから定数である. □

命題 81. 斉次多項式の約数は斉次多項式である.

解 118. $f = gh$ とし, g, h の項のうちで総次数が最高のものの和を p, q, 総次数が最小のものの和を r, s $(p, q, r, s \neq 0)$ とおけば, f の最高次の項の和は pq であり最低次の項の和は rs である. 命題の主張は $pq = rs \Rightarrow p = r$ かつ $q = s$ であるが $pq = rs$ であるとし $p = r$ であって $q \neq s$ とすると矛盾するので $q = s$ である.

解 119. 対称式の因数分解に関する問題である.

$$(x + y + z)^3 - x^3 - y^3 - z^3 = 3(x + y)(y + z)(z + x)$$

$$(x + y + z)^5 - x^5 - y^5 - z^5 = 5(x + y)(y + z)(z + x)(x^2 + y^2 + z^2 + xy + yz + zx)$$

左辺を $P(x, y, z)$ とおくと x のみを変数とみて $P(x)$ に $-y$ を代入すると $P(-y) = 0$ より $P(x)$ は $x+y$ を因数に持ち, 同様に y や z のみを変数と思うと $P(x, y, z)$ は $(x+y)(y+z)(z+x)$ を因数に持つ.

解 120. $f(x) = P(x)(x - \alpha) + r = Q(x)(x - \beta) + s$ のとき $f(x) = R(x)(x - \alpha)(x - \beta) + ax + b$ とかいたときの a と b の値は

$$a = \frac{r - s}{\alpha - \beta}, \quad b = \frac{\alpha s - \beta r}{\alpha - \beta}$$

解 121. $x_1, ..., x_n$に関する基本対称式を $s_1, ..., s_n$とかく. $\alpha_1, ..., \alpha_n$を根にもつモニック多項式を $f(x) = \prod_{i=1}^n (x - \alpha_i) := x^n + a_1 x^{n-1} + \cdots + a_n$とおけば

$$a_i = (-1)^i s_i \tag{2.10}$$

が成り立つ.

$$\frac{f'(x)}{f(x)} = \sum_{i=1}^n \frac{1}{x - \alpha_i} = \sum_{i=1}^n \left(\frac{1}{x} + \frac{\alpha_i}{x^2} + \cdots + \frac{\alpha_i^k}{x^{k+1}} + \frac{\alpha_i^{k+1}}{x^{k+1}(x - \alpha_i)} \right) = \frac{n}{x} + \frac{t_1}{x^2} + \cdots + \frac{t_k}{x^{k+1}} + \frac{g(x)}{x^{k+1} f(x)}$$

である. ただし $g(x)$ は次数 $n-1$ 以下の x に関する多項式であり k は任意の自然数である. $f'(x) =$ (右辺)$f(x)$ を書き直した次式における x^{n-k-1}の係数比較

$$nx^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1} = (x^n + a_1x^{n-1} + \cdots + a_n)\left(\frac{n}{x} + \frac{t_1}{x^2} + \cdots + \frac{t^k}{x^{k+1}} + \frac{g(x)}{x^{k+1}f(x)}\right)$$

をすると

$$if\ 1 \leq k \leq n\ ;\ (n-k)a_k = na_k + t_1a_{k-1} + \cdots + t_{k-1}a_1 + t_k$$

$$if\ k \geq n\ ;\ 0 = t_{k-n}a_n + t_{k-n+1}a_{n-1} + \cdots + t_{k-1}a_1 + t_k$$

となる. (2.10) により題意の

$$if\ 1 \leq k \leq n\ ;\ 0 = t_k - t_{k-1}s_1 + t_{k-2}s_2 - \cdots + (-1)^{k-1}t_1s_{k-1} + (-1)^k ks_k$$

$$if\ k > n\ ;\ 0 = t_k - t_{k-1}s_1 + \cdots + (-1)^n t_{k-n}s_n = 0$$

を得る.

2.10 [9] ユークリッド幾何学の公理

定義 47. 集合 $(S) \neq \emptyset$, V : n 次元実計量空間の組 $((S), V)$ が次を満たすとき $((S), V)$ を n 次元ユークリッド空間という.
(i) $\forall P, Q \in (S)\ \exists a \in V\ ;\ a = (\overrightarrow{PQ})$
(ii) $\forall P \in (S)\ \forall a \in V\ \exists! Q \in (S)\ ;\ (\overrightarrow{PQ}) = a$
(iii) $a = (\overrightarrow{PQ})$, $b = (\overrightarrow{QR})$ ならば $a + b = (\overrightarrow{PR})$
(S) の元を点といい, V の元をベクトルという. また V を (S) に付随するベクトル空間という.

命題 82. (iii) より $(\overrightarrow{PP}) + (\overrightarrow{PP}) = (\overrightarrow{PP})$. (iii) より $(\overrightarrow{PQ}) + (\overrightarrow{QP}) = (\overrightarrow{PP}) = \mathbf{0}$ なので $-(\overrightarrow{PQ}) = (\overrightarrow{QP})$ が成り立つ.

定義 48. ユークリッド空間が同型であることを次で定める.

$$((S), V) \cong ((S'), V') :\Leftrightarrow \text{集合 } (S) \cong (S') \text{ かつ計量同型写像 } f : V \cong V' \text{が存在する}$$

命題 83. 任意の 2 つの n 次元ユークリッド空間は同型である. i.e. $((S), V) \cong ((S'), V')$

証明. V と V'は同じ次元の計量空間であるから計量同型 $f : V \to V'$が存在する. $(S) \cong (S')$ は次のように示せる.
$(step1)$ $a \in V$ に対し $f(a) = a' \in V'$が対応する.
$(step2)$ $\forall P_0 \in (S), \forall P'_0 \in (S')$ を取る.
$(step3)$ (i) により $\forall P \in (S)$ に対し $\exists a[a = (\overrightarrow{P_0P})]$
$(step4)$ (ii) により任意に取った $P'_0 \in (S')$ と $\exists f(a) =: a' \in V'$に対してただ一つの $P' \in (S')$ が存在して次のように論理式を満たす. (i.e.$\exists! P' \in (S')[(\overrightarrow{P'_0P'}) = a' = f((\overrightarrow{P_0P}))]$)
まず g を $g : (S) \ni P \mapsto P' \in (S')$ で定めると g は写像の公理を満たし写像である. なぜなら任意に (S) の元 P に対してただ一つの g による送り先 $P' \in (S')$ があるからである. 次に g は全単射であることを示して集合としての同型 $(S) \cong (S')$ をいう. g は単射であるという為には任意の $P_1, P_2 \in (S)$ に対し $g(P_1) = g(P_2) \to P_1 = P_2$を示せばよい.
上ステップより勝手な P_0, P'_0, P_1をとりそれらに対してある唯一の P'_1が存在して

$$(\overrightarrow{P'_0P'_1}) = f(\overrightarrow{P_0P_1})$$

を満たす. この等号は V のベクトルと V'のベクトルを同一視していることによる等号である. 論理学における論証の手法として先に存在量化子 $\exists$ が束縛する変数 t を考え, 次に全称量化子 $\forall$ が束縛する x に t を当てはめたりや, $\forall x[P(x)]$ が与えられたときに妥当な推論として $\forall x[P(x)] \to P(u)$ ($\forall$ 除去という) を得るなどのものがあるがそのようにし, ここでも次を満たす $P'_2 \in (S')$ が存在する.

$$(\overrightarrow{P'_0P'_2}) = f(\overrightarrow{P_0P_2})$$

$g(P_1) = g(P_2)$ 即ち $P'_1 = P'_2$であるから

$$f(\overrightarrow{P_0P_1}) = f(\overrightarrow{P_0P_2})$$

となる. f は全単射より逆写像 f^{-1}が存在し,

$$(\overrightarrow{P_0P_1}) = (\overrightarrow{P_0P_2})$$

である. (ii) における唯一性は P_1と P_2は一致するということを意味する. よって g は単射である. $g : (S') \ni P' \mapsto P \in (S)$ も単射であることを対称的な議論によって示せるので g は全単射である. □

定義 49 (平たい部分空間)**.** $((S), V)$ を n 次元ユークリッド空間とする. $(S) \supset (A) \neq \varnothing$に対し V の r 次元部分空間 W があって次を満たすとき $((A), W)$ は $((S), V)$ の r 次元平たい部分空間という.
(イ) $P, Q \in (A) \to (\overrightarrow{PQ}) \in W$
(ロ) $P \in (A), Q \in (S), (\overrightarrow{PQ}) \in W \to Q \in (A)$

命題 84. W は一意である. また平たい部分空間 $((A), W)$ は r 次元ユークリッド空間である.

証明. W の一意性を示すため $((A), W)$ と $((A), X)$ が共に平たい部分空間であるとする. $W \subset X$ を示せば議論は対称なので $W = X$ といえる. $\forall a \in W$ というベクトルを取る. $((S), V)$ はユークリッド空間であるのでその公理より

$$\forall P \in (A) \text{ に対し } \exists! Q \in (S) \text{ が存在して } (\overrightarrow{PQ}) = a$$

である. (ロ) により $Q \in (A)$ がいえる. (イ) により $(\overrightarrow{PQ}) \in X$ なので $W \subset X$ である.
$((A), W)$ はユークリッド空間であることを示す.

$$(i)\ \forall P, Q \in (A) \text{ に対してある } a \in W \text{ が存在して } (\overrightarrow{PQ}) = a$$

これは成り立つ. なぜなら (イ) より $(\overrightarrow{PQ}) \in W$ でありこれを $a := (\overrightarrow{PQ})$ とすればいい.

$$(ii)\ \forall P \in (A)\ \forall a \in W \text{ に対し } \exists! Q \in (A)[(\overrightarrow{PQ}) = a]$$

$Q \in (S)$ を動かして勝手な a を $a = (\overrightarrow{PQ}) \in W$ として取る.
すると (ロ) より $Q \in (A)$ である. Q の一意性は $((S), V)$ がユークリッド空間なので $((S), V)$ における一意性より保証される. (iii) も $((S), V)$ がユークリッド空間であることによる. □

命題 85 (242 ページ)**.** 点 $P_1 \in (S)$ と $W \subset V$ に対し

$$\exists!(A)\ [\text{平たい部分空間として } ((A), W) \subset ((S), V) \wedge P_1 \in (A)]$$

が成り立つ. なぜなら $(A) := \{P \mid P \in (S),\ (\overrightarrow{P_1P}) \in W\}$ とおけばよい. $P_1 \in (A)$ はベクトル空間の零元の存在より成り立つ. 次に $((A), W)$ が平たい部分空間であることを示す. (ロ) を示すため $(\overrightarrow{P_1P}) \in W, Q \in (S), (\overrightarrow{PQ}) \in W$ とする. $(\overrightarrow{P_1Q}) - (\overrightarrow{P_1P}) \in W$ より $(\overrightarrow{P_1Q}) \in W$ でありこれは $Q \in (A)$ を意味する. よって (ロ) が示せた. (イ) を満たすことをいうため, $P, Q \in (A)$ とする. すると $(\overrightarrow{P_1P}), (\overrightarrow{P_1Q}) \in W$ である. ベクトル空間の公理より $(\overrightarrow{PQ}) = (\overrightarrow{P_1Q}) - (\overrightarrow{P_1P}) \in W$ なので (イ) も示せた.

定義 50. 二つの平たい部分空間は, 付随する V の部分空間の一方が他方に含まれるとき, 平行であるという.

定義 51. Cauchy, Schwartz の不等式より, $(\overrightarrow{PQ}) = \boldsymbol{a} \neq \boldsymbol{0}, (\overrightarrow{PR}) = \boldsymbol{b} \neq \boldsymbol{0}$ に対して

$$\cos\theta = \frac{(\boldsymbol{a}, \boldsymbol{b})}{\|\boldsymbol{a}\| \, | \, \|\boldsymbol{b}\|}$$

で定まる$\theta \in [0, \pi]$ を線分 PQ, PR のなす角といい$\angle QPR$ とかく.

問 35. $((S), V)$ が存在するのでそれに対して定まる n 次元ユークリッド空間 $(A) = \{P \mid P \in (S),\ (\overrightarrow{P_1P}) = t(\overrightarrow{P_1P_2}) + s(\overrightarrow{P_1P_3}),\ t, s \in \mathbb{R}\}$ という平面での余弦定理を示す. $P_1, P_2, P_3 \in (A)$ に対し

$$\begin{aligned} \|(\overrightarrow{P_1P_2})\|^2 &\overset{\text{ユークリッド空間の公理}}{=} \|(\overrightarrow{P_3P_2}) - (\overrightarrow{P_3P_1})\|^2 \\ &= \Big((\overrightarrow{P_3P_2}) - (\overrightarrow{P_3P_1}),\ (\overrightarrow{P_3P_2}) - (\overrightarrow{P_3P_1})\Big) \\ &= \|(\overrightarrow{P_3P_2})\|^2 + \|(\overrightarrow{P_3P_1})\|^2 - 2\|(\overrightarrow{P_3P_2})\| \, \|(\overrightarrow{P_3P_1})\| \cos\theta \end{aligned}$$

三平方の定理とは$\theta = \frac{\pi}{2}$のときの特別な場合を指す. なお, ピタゴラスの定理の逆とは $P_1, P_2, P_3 \in (A)$ に対して $\|(\overrightarrow{P_1P_2})\|^2 + \|(\overrightarrow{P_1P_3})\|^2 = \|(\overrightarrow{P_2P_3})\|^2$が成り立つとき$\angle P_2P_1P_3 = \frac{\pi}{2}$であることを指す.

定義 52. $r = 2$ の場合に同一直線上にない 3 点を通る平面の一意存在を考えたときは独立の概念は定めていなかったが, 例として $r = 2$ のとき P_0, P_1, P_2が独立であるとはその 3 点を通る直線が存在しないということである. 一般的に $r + 1$ 個の点 $P_0, P_1, ..., P_r$が $(r - 1)$ 次元平たい部分空間に含まれないとき, それらは独立であるという. $P_0, P_1, ..., P_r$が独立なとき $(\overrightarrow{P_0P_i}) = \boldsymbol{a}_i$ $(1 \leq i \leq r)$ として

$$\{P \mid (\overrightarrow{P_0P}) = \sum_{i=1}^{r} t_i \boldsymbol{a}_i,\ 0 \leq t_i \leq 1\}$$

を $P_0P_1, P_0P_2, ..., P_0P_r$を辺とする r 次元平行体という. 2 次元平行体は平行四辺形といい, 3 次元平行体は平行六面体という. 直方体とは平行六面体であって $\cos\angle P_1P_0P_2 = \cos\angle P_1P_0P_3 = \cos\angle P_2P_0P_3 = 0$ を満たすものであり, 立方体とは直方体であって $\forall i, j \in \{1, 2, 3\}(\|\overrightarrow{P_0P_i})\| = \|(\overrightarrow{P_0P_j})\|)$ を満たすものである. 平行体の体積を $\det(\boldsymbol{a}_i, \boldsymbol{a}_j)^{\frac{1}{2}}$で定める.

定義 53. n 次元ユークリッド空間 (S) の正規直交座標系 $(O; E), (O'; E')$ に対して基底の変換行列 $E = \langle \boldsymbol{e}_1, ..., \boldsymbol{e}_n \rangle \to E' = \langle \boldsymbol{e}'_1, ..., \boldsymbol{e}'_n \rangle$ を $A = (a_{ij})$ とすると A は直交行列である. なぜなら

$$\boldsymbol{e}'_j = \sum_{i=1}^{n} a_{ij} \boldsymbol{e}_i$$

$$(\boldsymbol{e}'_m, \boldsymbol{e}'_n) = (\sum_{i=1}^{n} a_{im}\boldsymbol{e}_i, \sum_{\ell=1}^{n} a_{\ell n}\boldsymbol{e}_\ell) = \sum_{i}^{n}\sum_{\ell}^{n} a_{im}a_{\ell n}(\boldsymbol{e}_i, \boldsymbol{e}_\ell) = \sum_{i=1}^{n} a_{im}a_{in} = \delta_{m,n}$$

よって $A^t = (a'_{ij}) \in M_n(\mathbb{R})$ とすると

$$\sum_{i=1}^{n} a'_{mi}a_{in} = \delta_{m,n}$$

より

$$A^tA = E_n$$

であるからである. $\det A = 1$ のとき $(O;E),(O';E')$ は同じ向きといい $\det A = -1$ のとき違う向きという. 直交基底全体がなす集合に関係 $\sim$ を $E \sim E' :\Leftrightarrow \det A = 1$ で定義すると「右手系」とそうでない「左手系」に類別される. 多様体に対しても向き付けを考えられる. 即ち多様体は局所的にはユークリッド空間と同相なので局所的な向つきを定め, 次にそれを連続的に移動して全局的な向き付けを与えられる. しかし一般に全局的な向き付けができる訳ではなく, メビウスの輪や射影平面はできない.

定義 54. (S) 上の座標系の向きを保つ合同変換を (S) の運動という.

問 36. $((S),V)$ を n 次元ユークリッド空間とする. $((S),V)$ 上の合同変換とは [9] では $g:(S)\to(S)$ が全単射であって $f:V\to V$ が計量同型 (i.e. $\boldsymbol{x},\boldsymbol{y}\in V$ に対し $(\boldsymbol{x},\boldsymbol{y}) = (f(\boldsymbol{x}),f(\boldsymbol{y}))$) であることをいう. 合同変換は 2 点間の距離を変えないことを示す. $\rho(P,Q):(S)\times(S)\ni(P,Q)\mapsto \|(\overrightarrow{PQ})\|\in\mathbb{R}$ とかくと, $\|\boldsymbol{x}\| = \sqrt{(\boldsymbol{x},\boldsymbol{x})}$ (内積からノルムを定義, $\boldsymbol{x} = (\overrightarrow{PQ})$) より

$$\rho(P,Q) = \|(\overrightarrow{PQ})\| \overset{f\text{が計量同型}}{=} \|f(\overrightarrow{PQ})\| = \|\overrightarrow{g(P)g(Q)}\| = \rho(g(P),g(Q))$$

逆に二点間の距離を変えない即ち上式より $\|\boldsymbol{x}\| = \|f(\boldsymbol{x})\|$ であるならば $(\boldsymbol{x},\boldsymbol{y}) = \frac{1}{2}(\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}\|^2 - \|\boldsymbol{b}\|^2)$ と, f の等長変換性からくる $\|f(\boldsymbol{x})+f(\boldsymbol{y})\| = \|\boldsymbol{x}+\boldsymbol{y}\|$ より g は合同変換である.

命題 86. n 次元ユークリッド空間 $((S),V)$ の r 次元部分空間 $((A),W)$ と $P_1\in(S)$ に対し, P_1 を含み, (A) に平行な r 次元部分空間が一意的に存在する.

$$(A)\subset(S), P_1\in(S) \text{ に対し } \exists!((B),W')\subset((S),V)\ [P_1\in(B)\wedge (A)\text{ と }(B)\text{ は平行}]$$

解 122. $((A),W)\subset((S),V)$ と $P_1\in(S)$ に対し $(B) := \{P \mid P\in(S),(\overrightarrow{P_1P})\in W\}$ と定めると (85) より W は一意なので (A) と (B) は平行であること即ち $W = W'$が成り立つ.

解 123. $((S),V^n)$ を全体のユークリッド空間とする. 前問で $r=1$ の場合より二次元ユークリッド空間における直線 $((A),W)$ とその上にない一点 $P_1\in(B)$ が与えられたときに P_1を通る平行線 $((B),W')$ が存在する. 余弦定理よりいわゆる錯覚の原理が示せることより三角形の内角の和は π である.

解 124. $n=3, r=1$ とすると確かに

$$((A),W_1^r)\subset((S),V^n) \text{ と } P_0\notin(A) \text{ に対し } \exists!((B),W_2^{r+1})[P_0,((A),W_1^r)\in((B),W_2^{r+1})]$$

を満たす (B) は $W_2 := \{t(\overrightarrow{P_0P}) + \boldsymbol{a} \mid P\in(A), t\in\mathbb{R}, \boldsymbol{a}\in W_1\}$ を付随するベクトル空間とした集合である.

解 125. $(\Rightarrow)$ は平たい部分空間の公理 (イ) より成り立つ.

解 126. 全体 $((S),V)$ をユークリッド空間とする.
$(S_1),(S_2)\subset(S)$ とする. W_1,W_2をベクトル部分空間とする. 一般に $(A) := ((S_1),W_1), B = ((S_2),W_2)$ に対して生成される部分空間は

$$(A)\vee(B) = ((S_1),\ \{\langle(\overrightarrow{S_1S_2})\rangle\} + W_1 + W_2)$$

である. $\because$ $V[\cdot] : \mathcal{P}(((S), V)) \ni (C) \mapsto W \in \mathcal{P}(V)$ を付随するベクトル空間をとるものとしてかく. $(A) \vee (B)$ は (A) と (B) を共に含む部分空間なので

$$V[(A) \vee (B)] \supset \{\langle(\overrightarrow{S_1 S_2})\rangle\} + W_1 + W_2$$

が成り立つ. 逆に $\{\langle(\overrightarrow{S_1 S_2})\rangle\} + W_1 + W_2$ は $(A) = ((S_1), W_1)$ を含み (S_2) も含むので

$$(A) \vee (B) \subset ((S_1), \{\langle(\overrightarrow{S_1 S_2})\rangle\} + W_1 + W_2\})$$

すなわち

$$V[(A) \vee (B)] \subset \{\langle(\overrightarrow{S_1 S_2})\rangle\} + W_1 + W_2\}$$

より逆の包含も成り立つ. (イ) と (ロ) の次元に関する関係式は付随するベクトル空間の次元の話に帰着して考えることで成立を確かめることができる. そのためには $(A) \cap (B) \neq \varnothing$ のときに対して

$$V[(A) \cap (B)] = W_1 \cap W_2$$

$$V[(A) \vee (B)] = W_1 + W_2$$

を示せばよい.

解 127. n 次元ユークリッド空間 V における二つの座標系 $(O; \boldsymbol{e}_1, ..., \boldsymbol{e}_n)$, $(O'; \boldsymbol{e}'_1, ..., \boldsymbol{e}'_n)$ を与える.

$$O' \underset{(O;\boldsymbol{e}_i) \text{ による座標}}{\leftrightarrow} (a_1, ..., a_n), \quad O \underset{(O;\boldsymbol{e}_i) \text{ による座標}}{\leftrightarrow} (0, ..., 0)$$

$$(\boldsymbol{e}'_1, ..., \boldsymbol{e}'_n) = (\boldsymbol{e}_1, ..., \boldsymbol{e}_n)T, \ \ T = (t_{ij})$$

とする. $P \in V$ に対し

$$\begin{aligned} P \quad &\underset{(O;\boldsymbol{e}_i)}{\leftrightarrow} \quad (x_1, ..., x_n) \\ &\underset{(O';\boldsymbol{e}'_i)}{\leftrightarrow} \quad (x'_1, ..., x'_n) \end{aligned}$$

とする. $(\overrightarrow{OP}) = (\overrightarrow{OO'}) + (\overrightarrow{O'P})$ であるから

$$\sum_i x_i \boldsymbol{e}_i = \sum_i a_i \boldsymbol{e}_i + \sum_i x'_i \boldsymbol{e}'_i = \sum_i a_i b \boldsymbol{e}_i + \sum_i \sum_j x'_i t_{ji} \boldsymbol{e}_j$$

従って

$$x_i = \sum_j t_{ij} x'_j + a_i \quad (1 \leq i \leq n) \Leftrightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = T \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} + \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

2.11 [9] 群および体の公理

問 37. 分配法則より $a(0+0) = a0 + a0$. よって $a0 = 0$. また $(0+0)a = 0a + 0a$ より $0a = 0$ である. $ab = 0$ ならば $a = 0$ または $b = 0$ を示す. $a \neq 0$ ならば左から a^{-1} をかけると $b = 0$ であり $b \neq 0$ ならば右から b^{-1} をかけて $a = 0$ である. 即ち $a = 0$ または $b = 0$ といわざるを得ない.

問 38 (252 ページ)**.** 直観的に成り立つことは想像されるものの困難な任意の実数に対する関係についての問いである. *http://www2.math.kyushu-u.ac.jp/~hara/lectures/07/realnumbers.pdf* を参照されたい.

解 128. p を素数とし $m, n \in \mathbb{Z}$ に対し $p \mid m - n \Leftrightarrow: m \sim n$ と定めると $\sim$ は $\mathbb{Z}$ 上の同値関係である. なぜなら $m \sim m$ が成り立ち, $m \sim n$ ならば $n \sim m$ が成り立つ. また $m \sim n$ かつ $n \sim \ell$ (i.e.$\exists k, k' \in \mathbb{Z}; m - n = kp, n - \ell = k'\ell$) ならば $m \sim \ell$ (i.e.$m - \ell = (k + k')p$) も成り立つ. $\mathbb{F}_p$上に加法と乗法を問いのように定めることは良定義であることを示す. 加法については代表元の取り方によらない即ち

$$[m] = [m'], [n] = [n'] \Rightarrow [m + n] = [m' + n']$$

ことは明らかである. $\exists k, \ell \in \mathbb{Z}; m' - m = kp, n' - n = \ell p$ のとき $(m' + n') - (m + n) = (k + \ell)p$ より. 乗法についても代表元の取り方によらない即ち

$$[m] = [m'], [n] = [n'] \Rightarrow [mn] = [m'n']$$

ことは明らかである. なぜなら $m'n' - mn = (m + kp)(n + \ell p) - mn = (m\ell + nk + k\ell p)p$ より $[mn] = [m'n']$ である. 加法に関して可換群である. 次に分配法則

$[m]([n] + [\ell]) = [m][n] + [m][\ell]$, もう一方は $\mathbb{F}_p$が可換群であるからこれをいえば十分

も (左辺) $= [m(n + \ell)]$, (右辺) $= [mn + m\ell] = [m(n + \ell)]$ より満たす. $[m] \in \mathbb{F}_p$に対する逆元は $[-m]$ で加法に関する零元 $0 = [0]$ である. また乗法に関する単位元 $1 = [1]$ であり, $[m] \in \mathbb{F}_p$に対する逆元 $[x]$ がもし存在したらそれは $[m][x] = [1]$ を満たし, $mx \sim 1$ より $\exists k \in \mathbb{Z}; mx - 1 = kp$ より $x = \frac{1}{m}(kp + 1)$ と表される. よって体の公理における乗法に関して零元 [0] 以外に対しては逆元が存在することも満たす.
$|\mathbb{F}_p| = p$ であることは $m \sim n$ の定義より. 標数が p であることは, $[m] \in \mathbb{F}_p$に対して $\min\{i \mid [i][m] = [0]\} = p$ より.

解 129. 埋め込み写像 $\mathbb{Q} \ni mn^{-1} \hookrightarrow m1(n1)^{-1} \in \mathbb{K}$ が存在する. なぜなら, $1 \in \mathbb{K}$ に対して加法の演算を繰り返すことで $\mathbb{K} \ni n \geq 1$ であり逆元 $-n \in \mathbb{K}$ の存在がいえる. 次に $\mathbb{K} \ni n \hookrightarrow n \in \mathbb{Z}$ の対応を作る. $\mathbb{K}$ の乗法の演算により $n, m \in \mathbb{K}$ に対して $mn^{-1} \in \mathbb{K}$ がいえて $\mathbb{Q} \ni mn^{-1} \hookrightarrow mn^{-1} \in \mathbb{K}$ が存在する.

解 130. $(0, 1) \subset \mathbb{R}$ と $\mathbb{N}$ の間には全単射が存在しない. $\mathbb{N}$ から $(0, 1)$ への全射が存在しないことを示せば十分である. 全射 $f : \mathbb{N} \to (0, 1)$ が存在したと仮定する. 各 $n \in \mathbb{N}$ に対し

て $f(n) \in (0,1)$ を十進無限小数で表してこれを順番に並べると

$$\begin{aligned} f(1) &= 0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots \\ f(2) &= 0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots \\ &\vdots \\ f(n) &= 0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots \end{aligned}$$

ただし, この表記は有限小数で終了するものは 0 が続いているとみなし 9 が無限に続くときは例えば $0.1 = 0.099\cdots$ とみなすことで一意である. 対角線にある $a_{11}, a_{22}, ..., a_{nn}, ...$ に対して

$$b_n := \begin{cases} 1 & (if\ a_{nn} \neq 1) \\ 9 & (if\ a_{nn} = 1) \end{cases}$$

と定義する. そして

$$b := 0.b_1b_2b_3\cdots b_n\cdots \in (0,1)$$

と定義する. すると $f(n)$ と b は小数第 n 位が違うので $f(n) \neq b$ である. n を 1 から ∞ まで走らせることで f は全射ではないことがわかる. これは矛盾している.

解 131. 正の実数 a を勝手にとり, $a_1^k < a < b_1^k$ なる有理数 a_1 と b_1 をとる. もし $\left(\frac{a_1+b_1}{2}\right)^k \leq a$ なら a は b_1 よりも a_1 に近く ($\mathbb{Q}$ は距離空間なので「近い」は妥当な言葉と思われる), $a_2 := a_1$, $b_2 := \frac{a_1+b_1}{2}$ と定める. $\left(\frac{a_1+b_1}{2}\right)^k > a$ なら $a_2 := \frac{a_1+b_1}{2}$, $b_2 := b_1$ と定める. 同様に a_n, b_n ($n \geq 1$) を定めて有理数列 $(a_n)_n, (b_n)_n$ を作ればこれはコーシー列であり収束先 $x := \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ が存在する. 作り方により x は $x^k = a$ を満たす.

解 132. $\mathbb{R} \subsetneq \mathbb{K} \subset \mathbb{C}$ とすると任意の $\alpha \in \mathbb{K}$ は $a, b \in \mathbb{R}$ として $\alpha = a + bi$ (ただし $b \neq 0$) とかける. $\mathbb{K}$ は体より加法と乗法の逆元の存在 (ただし零元に対する乗法の逆元は存在しない) と四則演算が閉じることから $i = b^{-1}(\alpha - a) \in \mathbb{K}$. よって $\mathbb{C} \subset \mathbb{K}$ より $\mathbb{K} = \mathbb{C}$ である. $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{R}$ を満たす $\mathbb{K}$ は無限個存在することについては私も代数学を勉強したい.

2.12 再修ジョルダン標準形

2.12.1 f 安定部分空間

定義 55. ベクトル空間 V の線型変換 $f : V \to V$ を考える. 部分空間 $U \subset V$ が f 安定部分空間であるとは

$$f(U) \subset U$$

であることをいう.

例 8. $U := \{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 | x = y = z\}$ として f を $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}$ で定めると U は安定部分空間ではない.

定理 3. V を有限次元ベクトル空間とし $e_1, ..., e_n$ をその基底とする. 部分空間 $U := L(e_1, ..., e_r)$ と線型変換 $f : V \to V$ に対し
U は f の安定部分空間 $\Leftrightarrow$ f の $e_1, ..., e_n$ に関する表現行列は以下の形

$$A \in M_{r\times r}, B \in M_{r\times(n-r)}, D \in M_{n-r} \text{は任意 } s.t \begin{pmatrix} A & B \\ O & D \end{pmatrix}$$

さらに, $f|_U : U \to U$ の $e_1, ..., e_r$ に関する表現行列は A となる.

証明. f の $e_1, ..., e_n$ に関する表現行列を $X = (x_{ij})_{1\le i\le n, 1\le j\le n} \in M_{nn}$ とおく. すなわち

$$[f(e_1)\cdots f(e_n)] = [e_1\cdots e_n]\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & a_{n1} & \cdots & x_{nn} \end{pmatrix}$$

$$= \left[[e_1\cdots e_n]\begin{pmatrix} x_{11} \\ \vdots \\ x_{n1} \end{pmatrix} \cdots\cdots [e_1\cdots e_n]\begin{pmatrix} x_{1n} \\ \vdots \\ x_{nn} \end{pmatrix} \right]$$

とかける. よって

$$f(U) = f(L(e_1\cdots e_r)) = L(f(e_1)\cdots f(e_r))$$

$$= L\left(\left[[e_1\cdots e_n]\begin{pmatrix} x_{11} \\ \vdots \\ x_{n1} \end{pmatrix} \cdots\cdots [e_1\cdots e_n]\begin{pmatrix} x_{1n} \\ \vdots \\ x_{nn} \end{pmatrix} \right]\right) \subset U := L(e_1\cdots e_r)$$

これより $x_{ij} = 0$ (ただし $r+1 \le i \le n, 1 \le j \le r$) これは表現行列を命題の形に定めることを意味する.
さらにこのとき

$$f|_U(\boldsymbol{e}_j) = \sum_{i=1}^{n} x_{ij}\boldsymbol{e}_i \underset{r+1\le i\le n, 1\le j\le r}{=} \sum_{i=1}^{r} x_{ij}\boldsymbol{e}_i \ (1 \le j \le r)$$

であり $A = (x_{ij})_{1\le i\le r, 1\le j\le r}$ が $f|_U$ の $e_1, ..., e_r$ に関する表現行列となる. □

定理 4. V をベクトル空間とする. 直和分解 $V = U_1 \oplus U_2$と U_1の基底 $e_1, ..., e_r, U_2$の基底 $e_{r+1}, ..., e_n$が与えられている.

補題 28. $e_1, ..., e_n$は V の基底である.

線型変換 $f : V \to V$ に対し U_1, U_2は f の安定部分空間 $\Leftrightarrow$ f の $e_1, ..., e_n$に関する表現行列は以下のようなものである

$$\begin{pmatrix} A & O_1 \\ O_2 & D \end{pmatrix}$$

($A \in M_{rr}, D \in M_{n-r}$は任意 $O_1 \in M_{r\times(n-r)}, O_2 \in M_{(n-r)\times r}$はゼロ行列) さらにこの時 $f|_{U_1} : U_1 \to U_1$の $e_1, ..., e_r$に関する表現行列は A で $f|_{U_2} : U_2 \to U_2$の $e_{r+1}, ..., e_n$に関する表現行列は D.

証明. 上と同様の手続きによって帰結を得る. 同様にして,

$$f(U_1) \subset U_1 \Leftrightarrow L\left((\boldsymbol{e}_1 \cdots \boldsymbol{e}_n)\begin{pmatrix} x_{11} \\ \vdots \\ x_{n1} \end{pmatrix}, ..., (\boldsymbol{e}_1 \cdots \boldsymbol{e}_n)\begin{pmatrix} x_{1r} \\ \vdots \\ x_{nr} \end{pmatrix}\right) \in L(\boldsymbol{e}_1, ..., \boldsymbol{e}_r)$$

$$f(U_2) \subset U_2 \Leftrightarrow L\left((\boldsymbol{e}_1 \cdots \boldsymbol{e}_n)\begin{pmatrix} x_{1(r+1)} \\ \vdots \\ x_{n(r+1)} \end{pmatrix}, ..., (\boldsymbol{e}_1 \cdots \boldsymbol{e}_n)\begin{pmatrix} x_{1n} \\ \vdots \\ x_{nn} \end{pmatrix}\right) \in L(\boldsymbol{e}_{r+1}, ..., \boldsymbol{e}_n)$$

である. 従って, $r+1 \leq i \leq n$ かつ $1 \leq j \leq r$, $1 \leq i \leq r$ かつ $r+1 \leq j \leq n$ のとき $x_{ij} = 0$
よって命題のように表現行列を定める. □

注 44. 上では A は $r \times r$ 行列だが前提を変えることで表現行列を対角行列にすることができる.

V を n 次元ベクトル空間としその基底を $e_1, ..., e_n$とする. $U_i := L(e_i)$ とする. このとき $V = U_1 \oplus \cdots \oplus U_n$であり線型変換 $f : V \to V$ に対し (1), (2) は同値

(1)$U_1, ..., U_n$はすべて f の安定部分空間

(2)f の $e_1, ..., e_n$に関する表現行列は対角行列である.

定義 56 (一般固有空間)**.** A を n 次正方行列としλは A の固有値とする. λに属する A の固有空間を V_λ とする. このとき

$$W_\lambda := \{\boldsymbol{v} \in \mathbb{C}^n \,|(A - \lambda I_n)^n \boldsymbol{v} = \boldsymbol{0}\}$$

を λに属する A の一般固有空間という. 明らかに $V_\lambda \subseteq W_\lambda$である.

定義 57. V を $\mathbb{C}$ 上のベクトル空間, $f : V \to V$ を線型変換とする.
f がベキ零であるとは $m \underset{\text{十分大}}{>>} 0$ をとると, $f^m = f \circ f \circ \cdots \circ f = 0$ すなわち $\forall v \in V$ に対し $f^m v = 0$ となることである.
V の部分空間 W が f 安定であるとは $f(W) \subseteq W$ となることである.

定理 5. W_λは f_A 安定である. ただし f_Aとは $f_A : \mathbb{C}^n \ni v \mapsto Av \in \mathbb{C}^n$であるような写像である.

証明. $(A-\lambda I)^n A = A(A-\lambda I)^n$ が成り立つ. $v \in W_\lambda$ならば $(A-\lambda I)^n v = 0A$ である. $(A-\lambda I)^n Av = A(A-\lambda I)^n v = 0$ より $f_A(v) = Av \in W_\lambda$ である. $\therefore f_A(W_\lambda) \subseteq W_\lambda$. □

定理 6 (フィッティングの補題)**.**
V を有限次元ベクトル空間とし $f : V \to V$ を線形変換とする.V のある部分空間 W', W''が存在してそれは以下を満たす.
(1)W', W''は f 安定
(2)$V = W' \oplus W''$
(3)$f|'_W$はベキ零
(4)$f|''_W$は同型写像

証明. Kerを N, Im を R とかくことにする.
$i \geq 1$ とし任意に $v \in N(f^i)$ をとる.$f^{i+1}(v) = f(f^i(v)) = f(0) = 0$ から $v \in N(f^{i+1}), f(v) \in N(f^i)$ $\therefore N(f^i) \subseteq N(f^{i+1}), N(f^i)$ は f 安定である.
一方任意の $w \in R(f^i)$ をとると $\exists v \in V; w = f^i(v)$ すると $w \in R(f^i(v))$ でさらに $f(w) = f^{i+1}(v) = f^i(f(v))$ だから $f(w) \in R(f^i)$
$\therefore R(f^i) \subseteq R(f^{i-1}), R(f^i)$ は f 安定である.
そこで以下の f 安定部分空間の列が存在する.

$$\{0\} \subseteq N(f) \subseteq N(f^2) \subseteq \cdots \subseteq N(f^i) \subseteq N(f^{i+1}) \subseteq \cdots$$

$$V \supseteq R(f) \supseteq R(f^2) \supseteq \cdots \supseteq R(f^i) \supseteq R(f^{i+1}) \cdots$$

V が有限次元だから $m >> 0$ をとると必ず

$$N(f^m) = N(f^{m+1}) = \cdots, \quad R(f^m) = R(f^{m+1}) = \cdots$$

となる.
そこで $W' = N(f^m), W'' = R(f^m)$ とおく.任意に $v \in V$ をとる.$f^m(v) \in R(f^m) = R(f^{2m})$ だから $\exists w \in V; f^m(v) = f^{2m}(w)$ である.
このとき $f^m(v - f^m(w)) = 0 \Leftrightarrow v - f^m(v) \in N(f^m) = W'$ そして

$$v = (v - f^m(v)) + f^m(v) \in W' + W''$$

となっている.
ここで $w \in W' \cap W''$とすると $w \in W''$だから $v \in V; w = f^m(v)$ であるが $w \in W'$でもあったから $f^m(f^m(v)) = 0$ となり

$$v \in N(f^{2m}) = W'$$

である. よって

$$w = f^m(v) = 0$$

これより $W' \cap W'' = \{0\} \Leftrightarrow V = W' \oplus W''$である. (2) が示せた.
任意の $w \in W'$に対して $(f|_{W'})^m(w) = 0$ より $(f|_{W'})^m(w) = 0$ であるから (3) が示せた.
$f|''_W$は全射である. なぜなら $w \in W''$なら $w \in R(f^{m+1})$ だから $\exists v \in V; w = f^{m+1}(v) =$

$f(f^m(v))$ とかける. $f^m(v) \in W''$だから $f|''_W : W'' \to W''$は全射の必要十分条件を満たす

$f|''_W$は単射である.「線形写像 f に対して $N(f) = \{0\} \Leftrightarrow f$ は単射」を使う.
$w \in N(f|''_W)$ とすると $w \in W''$なので $\exists v \in V; w = f^m(v)$ とかける. $f(w) = f(f^m(v)) = f^{m+1}(v) = 0$ である. これから $v \in N(f^{m+1}) = N(f^m)$ で, よって $w = f^m(v) = 0$ である. □

フィッティングの補題はジョルダン標準形の存在の証明に用いる.

2.12.2 ジョルダン標準形の存在一意

定義 58. 自然数 r と複素数αに対して $J_r(\alpha) = \begin{pmatrix} \alpha & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}$ と定める. $J_r(\alpha)$ を固有値 αの r 次ジョルダンセルという.

定義 59. いくつかのジョルダンセルを対角線上に並べた n 次正方行列

$$\begin{pmatrix} J_{r_1}(\alpha_1) & & & & \\ & J_{r_2}(\alpha_2) & & & 0 \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & J_{r_m}(\alpha_m) \end{pmatrix}$$

をジョルダン標準形行列という.

定理 7. 任意の n 次正方行列 A に対し正則行列 P を適当にとれば $P^{-1}AP$ はジョルダン標準形行列となる.

次を示せばよい.
$(*)V$ は n 次元ベクトル空間で $f : V \to V$ を線形変換とする. このとき V の基底 $\{v_1, \cdots, v_n\}$ をうまくとると $\{v_1, \cdots, v_n\}$ に関する表現行列 f_Aはジョルダン標準形となる.
なぜそう問題をかえられるのかの証明
$f_A : \mathbb{C}^n \ni v \mapsto Av \in \mathbb{C}^n$を考える. もし $(*)$ を認めれば, $\mathbb{C}^n$の基底 $\{v_1, \cdots, v_n\}$ を適当にとると f_A の表現行列はジョルダン標準形行列となる. よって

$$\begin{pmatrix} f_A(v_1) & f_A(v_2) & \cdots & f_A(v_n) \end{pmatrix} = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} J$$

$$\begin{pmatrix} Av_1 & \cdots & Av_n \end{pmatrix} = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} J$$

$$AP = PJ \qquad (P := \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix})$$

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

さらに, 問題は定理 A と定理 B により V を f 安定部分空間として直既約分解した状態に帰着される.

定義 60. V を線型空間, $f : V \to V$ を線形変換とする.
(1) 部分空間 $W \subset V$ が f 安定 $:\Leftrightarrow f(W) \subset W$. $f|_W : W \to W$ は線形変換である.
(2)V が f 直既約 $:\Leftrightarrow V = W_1 \oplus W_2$, W_1, W_2は f 安定部分空間であるなら $W_1 = \{\mathbf{0}\}$ または $W_2 = \{\mathbf{0}\}$
(3)V の f 直既約分解とは $V = W_1 \oplus \cdots \oplus W_r$ (各 W_iは f 安定で $f|_{W_i}$直既約) という形に表す

ことをいう.
(4)f の固有値αに属する一般固有空間 W_αを次で定義する

$$W_\alpha = \{\boldsymbol{v} \in V \mid \exists n \in \mathbb{N}\ s.t.\ (f - \alpha \mathrm{id}_V)^n(\boldsymbol{v}) = \boldsymbol{0}$$

(5)f が冪零変換 $:\Leftrightarrow \exists n \in \mathbb{N}\ s.t. f^n = 0$

以下, V は n 次元 $\mathbb{C}$ 上有限次元ベクトル空間で $f : V \to V$ を線形変換とする.

定理 8 (定理 A)**.**

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_r \text{ (各 } W_i \text{は } f \text{ 安定部分空間として直既約)}$$

と表すことができる. 線型空間としての V 以外にも PID 上の有限生成加群である場合にも直既約分解可能であり, 各直既約加群は構造の基本単位として自然に考察対象となる.

証明.

$$\mathcal{F} := \left\{ W \mid W \text{は} V \text{の} f \text{安定部分空間で} f \text{安定部分空間として直既約な部分空間の直和として表せない} \right\}$$

とおく.
$\mathcal{F} \neq \emptyset$ と仮定する. $W \in \mathcal{F}$ を $\dim W$ が最小となるようにとれる.
ここで W 自身は f 安定部分空間として直既約でない. :

$$\exists W' \exists W'' \neq \{0\} : V \text{の} f \text{安定部分空間}\quad s.t.\ W = W' \oplus W''$$

このとき $W' \subsetneq W, W'' \subsetneq W$ なので $\dim W' < \dim W,\ \dim W'' < \dim W$ である.
よって $\dim W$ の最小性から $W' \notin \mathcal{F}, W'' \notin \mathcal{F}$.
すなわち, W', W''は直既約分解できる. W'_iと W''_jは直既約な部分空間として

$$W' = W'_1 \oplus \cdots \oplus W'_r$$

$$W'' = W''_1 \oplus \cdots \oplus W''_s$$

だが $W = W'_1 \oplus \cdots \oplus W'_r \oplus W''_1 \oplus \cdots \oplus W''_s$となり $W \in \mathcal{F}$ に反する. □

注 45. あるいは, 次のように有限次元 $\mathbb{C}$ ベクトル空間 V 上の線形変換 $f : V \to V$ に対し, 必ず f 直既約分解が存在することをいうことも出来る.
V が f 直既約であれば証明することはない. f 直既約でなければ $V = V_1 \oplus V_2,\ V_i \neq \{\boldsymbol{0}\}$ は f 安定の形にかける. 次に V_iが f 直既約でなければ分解し続けていけば V は有限次元より有限回で f 直既約分解される.

定理 9 (定理 B)**.**
$V = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ (各 W_iは f 安定部分空間として直既約) とする.
$i = 1, \cdots, r$ に対して $w_{i,1}, w_{i,2}, \cdots, w_{i,n_i}$は W_iの基底とし, この基底に関する $f|_{W_i} : W_i \to W_i$ の表現行列を A_i とする.
このとき

$$w_{1,1}, \cdots, w_{1,n_1}\ , w_{2,1}, \cdots, w_{2,n_2},\ \ , \cdots\ \ w_{r,1}, \cdots, w_{r,n_r}$$

は V の基底となり, この基底に関する f の表現行列は

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_r \end{pmatrix}$$

となる.

証明. 前節「安定部分空間」での命題より成り立つ. □

この $A_1, \cdots, A_r$ がキレイになるように W_i の基底の取り方を考えるという流れである. 途中,
V が f 安定部分空間として直既約分解 $V = W_1 \oplus \cdots \oplus W_r$ できるので, そのような時まず $f|_{W_i}$ の固有値はただ一つの固有値 α_i をもち, W_i は $f|_{W_i}$ の固有値 α_i に属する一般固有空間と一致することを示すのである. 次に, W_i の基底の取り方をうまくすれば, $f|_{W_i}$ の表現行列がジョルダンセル $J_{\dim_{\mathbb{C}} W_i}(\alpha_i)$ となる. このことは冪零変換と極小生成系を導入し, 中山の補題の特別な場合によって示される. 定理 C により $W_1, \cdots, W_r$ の基底の和集合に関する f の表現行列にはジョルダンセル $J_{\dim_{\mathbb{C}} W_i}(\alpha_i)$ が並ぶことになり, キレイなジョルダン標準形行列を与える.

問 39. 一般固有空間 W_α は固有空間 V_α を含む V の f 安定部分空間であることを示せ.
解. 含むこと, 部分空間となること, f 安定であることの順にかく.
$\boldsymbol{v} \in V_\alpha \Rightarrow (f - \alpha\mathrm{id})^1(\boldsymbol{v}) = \boldsymbol{0} \Rightarrow \boldsymbol{v} \in W_\alpha. c \in \mathbb{C}, \boldsymbol{u}, \boldsymbol{v} \in W_\alpha \Rightarrow \exists m, n \in \mathbb{N}\ s.t.\ (f - \alpha\mathrm{id})^m(\boldsymbol{u}), (f - \alpha\mathrm{id})^n(\boldsymbol{v}) = \boldsymbol{0} \Rightarrow (f - \alpha\mathrm{id})^n(c\boldsymbol{v}) = \boldsymbol{0}$
$\exists m + n;\ (f - \alpha\mathrm{id})^{\max(m+n)}(\boldsymbol{u} + \boldsymbol{v}) = \boldsymbol{0},\ (f - \alpha\mathrm{id})^n(f(\boldsymbol{v})) = f(f - \alpha\mathrm{id})^n(\boldsymbol{v}) = f(\boldsymbol{0}) = \boldsymbol{0}$

命題 87. f を n 次元クトル空間 V 上の冪零変換 $f : V \to V$ とする. このとき $f^n = 0$ となる (冪零変換の定義において十分大きな N に対して $f^N = 0$ であるが N としてギリギリ空間の次元を取れる.)
$\because$
$V \supset f(V) \supset f^2(V) \supset \cdots \supset \{\boldsymbol{0}\}$ においていつか $=$ になったらそれ以降全て $=$ となる. よって $f^N = 0$ となる最小の N をとると

$$V \supsetneq f(V) \supsetneq f^2(V) \supsetneq \cdots \supsetneq f^N(V) = \{\boldsymbol{0}\}$$

となっている. $\supsetneq$ の個数は $\dim_{\mathbb{C}} V$ を超えられないから $N \leq n$ である.

定理 10 (フィッティングの補題)**.** 有限次元 $\mathbb{C}$ ベクトル空間 V 上の線形変換 $f : V \to V$ を考える.

$$V = V_1 \oplus V_2,\ V_1, V_2 \text{は } f \text{ 安定部分空間},\ f|_{V_1} \text{は冪零},\ f|_{V_2} \text{は同型}$$

を満たす V_1, V_2 が存在する.

系 6. V が f 直既約 (f 安定部分空間として直既約) $\Rightarrow$ f は冪零または同型写像である.

証明. $\exists W' \exists W'' : V$ の f 安定部分空間 $s.t.$
$V = W' \oplus W''$
$f|_{W'}$は冪零
$f|_{W''}$は同型
とかける. V が f 直既約なので $W' = \{\mathbf{0}\}$ または $W'' = \{\mathbf{0}\}$ である.
$W' = \{\mathbf{0}\}$ ならば $V = W''$なので f は同型, $W'' = \{\mathbf{0}\}$ ならば $V = W'$なので f は冪零となる
□

定理 11. $\mathbb{C}$ ベクトル空間 V 上の線形変換 $f : V \to V$ に対し, V の f 直既約分解を一つとり

$$V = V_1 \oplus \cdots \oplus V_r$$

とする. このとき各 $1 \leq i \leq r$ に対し, 制限 $f|_{V_i} : V_i \to V_i$はただ一つの固有値λ_iをもち, V_iはλ_iに属する V_i内での一般固有空間

$$\{\boldsymbol{v} \in V_i | \exists n \in \mathbb{N}\ s.t.(f - \lambda_i \mathrm{id})^n(\boldsymbol{v})\} = \mathbf{0}$$

と一致する.

このことはV_iが f 直既約であることから, 次の命題のように
一つの V_iに注目して次が成り立てば示されることになる.

定理 12. $\mathbb{C}$ ベクトル空間 V 上の線形変換 $f : V \to V$ を考える. V が f 直既約のとき, f はただ一つの固有値αをもち, $V = W_\alpha$(αに属する一般固有空間) となる.

証明. $\mathbb{K} = \mathbb{C}$ なので, 固有多項式は必ず根αを持つ. まず

$$V \text{ が } f \text{ 直既約} \Rightarrow V \text{ が } (f - \alpha\mathrm{id}) \text{ 直既約 } (*)$$

であることに注意したい. つまり, 仮定から V は $(f - \alpha\mathrm{id})$ 直既約である. よって, $f - \alpha\mathrm{id}$ は冪零または同型.
ここで, $g := f - \alpha\mathrm{id}_\mathrm{V}$ とおき V は g 直既約である. α に属する f の固有ベクトル υ をとると g の定義から $\upsilon \in \mathrm{Ker}(g)$. よって $\mathrm{Ker}(g) \neq \{\mathbf{0}\}$. よって g は同型ではなく冪零であるから, ある $r > 0$ があって $g^r = 0$ である. またすでに述べたように $g^n = 0$ となる. したがって

$$W_\alpha = \{\upsilon \in V | (f - \alpha\mathrm{id}_\mathrm{V})^n(\upsilon) = 0\} \overset{g^n=0}{=} V$$

□

注 46. $(*)$ は V の f 安定部分空間での直和分解と V の $(f - \alpha\mathrm{id})$ 安定部分空間での直和分解が対応し, 既約性も対応するから. となると, 示すべきは部分空間 $\mathrm{W} \subset \mathrm{V}$ に対し

$$W \text{ は } f \text{ 安定部分空間} \Leftrightarrow W \text{ は } (f - \alpha\mathrm{id}) \text{ 安定部分空間}$$

といえる.
$\because$
$f(W) \subset W \Rightarrow (f - \alpha\mathrm{id})(\mathrm{W}) = \{\mathrm{f(w)} - \alpha\mathrm{w} | \mathrm{w} \in \mathrm{W}\} \subset \mathrm{f(W)} + \alpha(\mathrm{W}) \subset \mathrm{W} + \mathrm{W} = \mathrm{W}$ より

$$W \subset V \text{ が } f \text{ 安定} \Rightarrow W \subset V \text{ が } (f - \alpha\mathrm{id}) \text{ 安定}$$

をいったことになる.

注 47. αがただ一つの固有値であることを示す. 別の固有値βを持つとする. このとき

$$0 \neq \exists \boldsymbol{v} \in V \ s.t. \ f(\boldsymbol{v}) = \beta \boldsymbol{v}$$

だが一方で $V = W_\alpha$なので

$$(f - \alpha \mathrm{id})^n(\boldsymbol{v}) = (\beta - \alpha)^n \boldsymbol{v} = \boldsymbol{0}$$

となり $\beta = \alpha$である.

以下, V は f 安定空間とする.

定義 61. r 個のベクトルを$\upsilon_1, \cdots, \upsilon_r \in V$ とおく.
$\langle \upsilon_1, \cdots, \upsilon_r \rangle := \{\upsilon \in V \mid \upsilon = \sum_{i=1}^{n} a_i \upsilon_i (a_i \in \mathbb{C}\}$ とおく. $V = \langle \upsilon_1, \cdots, \upsilon_r \rangle$ のとき$\upsilon_1, \cdots, \upsilon_r$は V の生成系という. また

$$\begin{aligned} V &= \left\langle \{f^i(\upsilon_j)\} \mid 0 \leq i \in \mathbb{Z},\ 1 \leq j \leq r \} \right\rangle \\ &= \Big\langle \upsilon_1, \cdots, \upsilon_r \\ &\quad f(\upsilon_1), \cdots,\ f(\upsilon_r) \\ &\quad f^2(\upsilon_1), \cdots,\ f^2(\upsilon_r) \\ &\quad f^3(\upsilon_1), \cdots,\ f^3(\upsilon_r) \\ &\quad \cdots \\ &\quad \cdots \Big\rangle \end{aligned}$$

となるとき, $\upsilon_1, \cdots, \upsilon_r$は V の f 生成系であるという.

例 9. $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ とおく. $f_A(e_2) = Ae_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1$なので

$$\mathbb{C}^2 = \langle e_1, e_2 \rangle = \langle f_A(e_2), e_2 \rangle$$

である. よって $\{e_2\}$ は $\mathbb{C}^2$の f_A 生成系である.
また $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$とおくと $f_B(e_1) = e_2$となり $\{e_1\}$ は f_B 生成系.

定義 62. $V = \langle \upsilon_1, \cdots, \upsilon_r \rangle (\upsilon_1, \cdots, \upsilon_r$が V の f 生成系) であって, $\upsilon_1, \cdots, \upsilon_r$のどの一つのベクトルを除いても V の f 生成系とはならないとき, $\upsilon_1, \cdots, \upsilon_r$は V の極小 f 生成系であるという.

定理 13 (中山の補題の特別な場合)**.**
f は V 上の冪零変換とする. このとき

$$\{\upsilon_1, \cdots, \upsilon_r\} \text{ が } V \text{ の } f \text{ 生成系である} \Leftrightarrow V = \langle \upsilon_1, \cdots, \upsilon_r \rangle + \mathrm{Im} f$$

証明. $\Rightarrow$)

$$\begin{aligned} V &= \langle \{f^i(\upsilon_j)\} \mid 0 \leq i \in \mathbb{Z}\ j = 1, \cdots, r \} \rangle \\ &= \langle \upsilon_1, \cdots, \upsilon_r \rangle + \langle \{f^i(\upsilon_j) \mid 1 \leq i,\ j = 1, \cdots, r\} \rangle \end{aligned}$$

$i \geq 1$ のとき $f(f^{i-1}(\upsilon_j)) \in \mathrm{Im} f$ なので

$$V \subseteq \langle \upsilon_1, \cdots, \upsilon_r \rangle + \mathrm{Im} f \underset{f: V \to V}{\subseteq} V$$

よって

$$V = \langle \upsilon_1, \cdots, \upsilon_r \rangle + \mathrm{Im} f$$

⇐)
任意に$v \in V$をとると

$$v = (\sum_{j=1}^{r} a_{0j} v_j) + f(w_1) \ (a_{0j} \in \mathbb{C}, w_1 \in V)$$

とかける. w_iはVの元なので

$$w_1 = (\sum_{j=1}^{r} a_{1j} v_j) + f(w_2) \ (a_{1j} \in \mathbb{C}, w_2 \in V)$$

とかける. このとき

$$v = (\sum_{j=1}^{r} a_{0j} v_j) + f(\sum_{j=1}^{r} a_{1j} v_j) + f^2(w_2)$$

$$w_2 = (\sum_{j=1}^{r} a_{2j} v_j) + f(w_3) \ (a_{2j} \in \mathbb{C}, w_3 \in V)$$

とおき

$$v = \left(\sum_{i=0}^{2} \sum_{j=1}^{r} a_{ij} f^i(v_j) \right) + f^3(w_3)$$

議論を繰り返して任意の$N \geq 1$に対して

$$v = \left(\sum_{i=0}^{N-1} \sum_{j=1}^{r} a_{ij} f^i(v_j) \right) + f^N(w_N) \ (a_{ij} \in \mathbb{C}, \ w_N \in V)$$

fは冪零変換なので十分大きいNに対して

$$v = \sum_{i \geq 0} \sum_{j=1}^{r} a_{ij} f^i(v_j)$$

□

注 48. 中山の補題は可換環論で扱われる.

系 7. ベクトル空間 V 上の冪零変換 $f : V \to V$ を考える. $f(V)$ の基底を一組とり$\upsilon_1, \cdots, \upsilon_m$ とおき,
基底を延長し V の基底$\upsilon_1, \cdots, \upsilon_m, a_1, \cdots, a_r$をとる. このとき $S = \{a_1, \cdots, a_r\}$ は V の極小 f 生成系となる.

証明. $V = \mathbb{K}\upsilon_1 \oplus \cdots \oplus \mathbb{K}\upsilon_m \oplus \mathbb{K}a_1 \oplus \cdots \oplus \mathbb{K}a_r = f(V) \oplus \langle a_1, \cdots, a_r \rangle$ が成り立つ.
特に, $V = f(V) + \langle a_1, \cdots, a_r \rangle$ であり, 中山の補題より S は V の f 生成系である. 次に極小 f 生成系であることをいう. 実際 $S_0 \subsetneq S$ であれば

$$\dim_{\mathbb{K}}(f(V) + L(a_i \mid a_i \in S_0)) \leq \dim_{\mathbb{K}} f(V) + \dim_{\mathbb{K}} L(a_i \mid a_i \in S_0) < \dim_{\mathbb{K}} f(V) + |S| = \dim_{\mathbb{K}} V$$

となり,

$$f(V) + L(a_i \mid a_i \in S_0) \subsetneq V$$

よって中山の補題より S_0は V の f 生成系でない. すなわち S は極小 f 生成系である. □

補題 29. ベクトル 空間 V と, その有限次元部分空間 $U_1, \cdots, U_r \subset V$ に対して, 以下は全て同値となる. 以下の一つ (よって全て) が成り立つとき, 和空間 $U_1 + \cdots + U_r$は直和であるといい,
$U_1 + \cdots + U_r = U_1 \oplus \cdots \oplus U_r$と表す.
(1) 各 $i = 1, \cdots, r-1$ について $(U_1 + \cdots + U_i) + U_{i+1} = (U_1 + \cdots + U_i) \oplus U_{i+1}$
(2)$f : U_1 \times \cdots \times U_r \to U_1 + \cdots + U_r;\ (a_1, \cdots, a_r) \mapsto a_1 + \cdots + a_r$は同型
(3) 各 $i = 1, 2, \cdots, r-1$ に対して $(U_1 + \cdots U_i) \cap U_{i+1} = \{\mathbf{0}\}$
(4) $\dim(U_1 + \cdots + U_r) = \dim U_1 + \cdots + \dim U_r$
(5)$U_1 + \cdots U_r$の各ベクトルを $a_1 + \cdots + a_r$ $(a_i \in U_i)$ の形にかくのは 1 通りだけである.
(6)$a_1 + \cdots + a_r = \mathbf{0}$ $(a_i \in U_i) \Rightarrow a_1 = \cdots = a_r = \mathbf{0}$

証明. $r = 2$ の時を言えば十分である. □

次の定理を示すのが目先の目標である.

定理 14. ベクトル空間 V 上の冪零変換 $f : V \to V$ を考える. このとき以下は同値.
(1) V が f 直既約
(2) $\dim_{\mathbb{K}} V - \dim_{\mathbb{K}} f(V) = 1$
またこれが成り立つとき

$$\text{ベクトル } \boldsymbol{a} \in V,\ \boldsymbol{a} \notin f(V)$$

を満たす任意のベクトル $\boldsymbol{a}$ をとれば $S = \{\boldsymbol{a}\}$ は V の極小 f 生成系を与える.

証明. (1) ⇒ (2)
$\dim V = \dim f(V)$ と仮定すると $f^k(V) = V$ $(\forall k \in \mathbb{N})$ なので冪零変換であることに矛盾する.
よって $r := \dim V - \dim f(V) \geq 1$ である. 上の系通りに
・$f(V)$ の基底を一組とって$\upsilon_1, \cdots, \upsilon_m$とおき, 基底を延長して
・V の基底$\upsilon_1, \cdots, \upsilon_m, a_1, \cdots, a_r$をとる.

a_1の取り方は $a_1 \notin f(V)$ でさえあればどの元でも良い.

$\because\ a_i \notin f(V) \Rightarrow L(v_1, \cdots, v_m, a_1) \supsetneq f(V) \Rightarrow \dim L(v_1, \cdots, v_m, a_1) > \dim f(V) = m \Rightarrow$
$v_1, \cdots, v_m, a_1$は一次独立である. $v_1, \cdots, v_m, a_1$から再び基底の延長をしていく.

以下の議論のため, 次の取り方をする.

$$m_a := \min\{k \in \mathbb{N} \mid f^k(a) = \mathbf{0}\} \text{ とおき, } V - f(V) \text{ の中で } m_a \text{が最小となる}$$

$$a \in V - f(V) \text{ のうちの一つを } a_1 \text{とおく.}$$

以下 $r \geq 2$ として矛盾を導く. 具体的には

$$V_1 := L(a_1, f(a_1), f^2(a_1), \cdots)$$

$$V_2 := L(a_2, \cdots, a_r, f(a_2), \cdots, f(a_r), f^2(a_2), \cdots, f^2(a_r), \cdots)$$

とおくと V_1, V_2が f 安定部分空間で $V = V_1 \oplus V_2$ となることをいう. これが言えると V が f 直既約であることと矛盾する. まず $V = V_1 + V_2$ を示す. $a_1, \cdots, a_r$は f 生成系なので, 中山の補題より

$$V = L(a_1, a_2, \cdots, a_r) + f(V)$$

である. $V_1 + V_2 = L(a_1, \cdots a_r, f(a_1), \cdots, f(a_r), f^2(a_1), \cdots, f^2(a_r), \cdots) = V$
なので $V = V_1 + V_2$. さて $V_1 + V_2 = V_1 \oplus V_2$ をいう.
補題より

$$v_1 + v_2 = \mathbf{0}\ (v_i \in V_i) \Rightarrow v_1 = v_2 = \mathbf{0}$$

を言えばよい.

$$v_1 = \sum_{j=0}^{m_{a_1}-1} c_{1j} f^j(a_1),\ v_2 = \sum_{i=2}^{r} \sum_{j=0}^{m_{a_i}-1} c_{ij} f^j(a_i)\ (c_{**} \in \mathbb{K})$$

とかけるから仮定は

$$\sum_{i=1}^{r} \sum_{j=0}^{m_{a_i}-1} c_{ij} f^j(a_i) = \mathbf{0}$$

ここで

$$j_0 := \min\{j \mid \exists i\ s.t.\ c_{ij} \neq 0\}$$

とおくと

$$\sum_{i=1}^{r} \sum_{j=j_0}^{m_{a_i}-1} c_{ij} f^j(a_i) = f^{j_0}\left(\sum_{i=1}^{r} \sum_{j=j_0}^{m_{a_i}-1} c_{ij} f^{j-j_0}(a_i)\right) = \mathbf{0}$$

かける. 上式に於いて $f^{j_0}(*)$ の中身 $\in V - f(V)$ が成り立つことを認めると m_{a_1}の最小性より

$$\min\{j \mid \exists i\ s.t.\ c_{ij} \neq 0\} = j_0 \geq m_{a_1},\ \text{つまり任意の } i(1 \leq i \leq r) \text{ に対し } c_{i0} = \cdots = c_{i(m_{a_1}-1)} = 0$$

となる. 特に $c_{10} = \cdots = c_{1(m_{a_1}-1)} = 0$ だから

$$v_1 = \sum_{j=0}^{m_{a_1}-1} c_{1j} f^j(a_1) = \mathbf{0}$$

となり, $v_2 = \mathbf{0} - v_1 = \mathbf{0}$ なので題意を得た.
さて示すべきこと ($f^{j_0}(*)$ の中身が $V - f(V)$ の元であること) を示す. まず

$$\sum_{i=1}^{r} \sum_{j=j_0}^{m_{a_i}-1} c_{ij} f^{j-j_0}(a_i) = \sum_{i=1}^{r} c_{ij_0} a_i + f(V) \text{ に属するベクトル}$$

の形なので

$$\sum_{i=1}^{r} \sum_{j=j_0}^{m_{a_i}-1} c_{ij} f^{j-j_0}(a_i) \in f(V) \Leftrightarrow \sum_{i=1}^{r} c_{ij_0} a_i \in f(V)$$

である. よって

$$\sum_{i=1}^{r} c_{ij_0} a_i \notin f(V)$$

を示せば良い. j_0の取り方より $\exists i \ s.t. \ c_{ij_0} \neq 0$. よって $\sum_{i=1}^{r} c_{ij_0} a_i \neq \mathbf{0}$($\because a_1, \cdots, a_r$は一次独立より. もし $a_1, ..., a_r$が従属だったら $c_{ij_0} \neq 0$ となる番号 i があっても $\sum_{i=1} c_{ij_0} a_i = \mathbf{0}$ となることがある) である.

$$\mathbf{0} \neq \sum_{i=1}^{r} c_{ij_0} a_i \in L(a_1, \cdots, a_r)$$

$\sum_{i=1}^{r} c_{ij_0} a_i \in f(V)$ と仮定すると, $f(V) \cap L(a_1, \cdots, a_r)$ が非零ベクトル $\sum_{i=1}^{r} c_{ij_0} a_i$ を含む. しかしこれは下の補題 (1) の $V = f(V) \oplus L(a_1, \cdots, a_r)$ ($\because \{a_1, \cdots, a_r\}$ は V の極小 f 生成系なので系の仮定を満たす) に矛盾する. □

授業でやった流れでも (1) ⇒ (2) が成り立つことを確かめることにしたいと思う. 使う条件と背理法の順番が違うだけで, 証明は全く差し変わりない.

補題 30. $\{v_1, \cdots, v_r\}$ が V の極小 f 生成系ならば次が成り立つ.
(1) $V = \langle v_1, \cdots, v_r \rangle \oplus \mathrm{Im} f$
(2) $r = \dim V - \mathrm{rank} f$

証明. (1) $\langle v_1, \cdots v_r \rangle \cap \mathrm{Im} f = \{\mathbf{0}\}$ を示す.
そこで $\mathbf{0} \neq \exists w \in \langle v_1, \cdots v_r \rangle \cap \mathrm{Im} f$ とせよ. すると $\exists v \in V$ s.t. $w = f(v)$. 一方で $w = c_1 v_1 + \cdots + c_r v_r$ $(c_i \in \mathbb{C})$ とかける. $w \neq \mathbf{0}$ なので, $c_1, \cdots, c_r$ のいずれかは $\mathbf{0}$ ではない. 必要ならば番号を付け替えて $c_i \neq \mathbf{0}$ として良い.

$$\begin{aligned} v_r &= \frac{1}{c_r}\{f(v) - c_1 v_1 - \cdots - c_{r-1} v_{r-1}\} \\ &= -\frac{c_1}{c_r} v_1 - \cdots - \frac{c_{r-1}}{c_r} v_{r-1} + f(\frac{1}{c_r} v) \\ &\in \langle v_1, \cdots, v_{r-1} \rangle + \mathrm{Im} f \end{aligned}$$

これより

$$V = \langle v_1, \cdots, v_{r-1}, v_r \rangle + \mathrm{Im} f = \langle v_1, \cdots, v_{r-1} \rangle + \mathrm{Im} f$$

よって $\{v_1, \cdots, v_{r-1}\}$ は V の f 生成系であるがこれは $\{v_1, \cdots, v_r\}$ の極小性に矛盾する. □

定理 15. f を V 上の線形な冪零変換とし, V が f 安定空間として直既約であるとする. このとき

$$\exists u \in V \ s.t. \ V = \langle u, f(u), f^2(u), \cdots \rangle$$

よって $\dim V - \mathrm{rank} f = 1$ がこのとき成り立つ.

証明. $\forall v \in V$ に対して, $m(v) := \min\{i \geq 0 \mid f^i(v) = 0\}$ とおく. f が冪零ならば f は全射ではないので $v \notin \mathrm{Im} f$ となるような v を取れる. ($\because$ 冪零より $\exists m \forall v \in V \ f^m(v) = \mathbf{0}$. $f(V) = V$ と仮定すると $f^m(V) = \mathbf{0}$ より $V = \mathbf{0}$ となってしまう)

$$t := \min\{m(v) \mid v \in V, v \notin \mathrm{Im} f\}$$

とおく. $v \notin \mathrm{Im} f$ ならば $v \neq 0$ なので $m(v) > 0$ ゆえ $t > 0$.
ここで $t = m(u)$ となる $u \in V \backslash \mathrm{Im} f$ をとる.

$$V \supsetneq \langle u, f(u), f^2(u), \cdots \rangle \text{ として矛盾を導く.}$$

すなわち, u だけでは V を f 生成できないと仮定するのである. 実は u のみで V を f 生成系できるというのが流れである. 背理法は複数回用いるが, 次の仮定が本筋の仮定である.
$\{u, v_1, v_2, \cdots, v_r\}$ が V の極小 f 生成系となるように $v_1, \cdots, v_r \in V (r \geq 1)$ がとれるとする.

$$W_1 := \langle u, f(u), f^2(u), \cdots, f^{t-1}(u) \rangle$$

$$W_2 := \left\langle \{f^i(v_j) \mid 0 \leq i < m(v_j) \ j = 1, \cdots, r \right\rangle$$

とおく. 明らかに $V = W_1 + W_2$ である. もし $W_1 \cap W_2 = \{\mathbf{0}\}$ ならば $V = W_1 \oplus W_2$ となり V が f 直既約であることに反する. よって, $\mathbf{0} \neq \exists w \in W_1 \oplus W_2$ を取れる.
このとき

$$w = \sum_{i=0}^{t-1} c_i f^i(u),\ w = \sum_{j=1}^{r} \sum_{i=0}^{m(\upsilon_j)-1} d_{ij} f^i(\upsilon_j)$$

と表せる. そこで

$$s := \min\left\{ i \mid c_i, d_{i1}, d_{i2}, \cdots, d_{ir} \text{のどれかが } 0 \text{ でない} \right\}$$

と定める. $c_0, c_1, \cdots, c_{t-1}$のうち少なくとも一つは 0 でないので $s \leq t-1$ であり, またその定義から $i < s$ ならば $c_i = d_{i1} = d_{i2} = \cdots = d_{ir} = 0$ である. よって,

$$\sum_{i=s}^{t-1} c_i f^i(u) = \sum_{j=1}^{r} \sum_{i=s}^{m(\upsilon_j)-1} d_{ij} f^i(\upsilon_j)$$

$$f^s\left(\sum_{i=s}^{t-1} c_i f^{i-s}(u)\right) = f^s\left(\sum_{j=1}^{r} \sum_{i=s}^{m(\upsilon_j)-1} d_{ij} f^{i-s}(\upsilon_j)\right)$$

従って, $\delta := \sum_{i=s}^{t-1} c_i f^{i-s}(u) - \sum_{j=1}^{r} \sum_{i=s}^{m(\upsilon_j)-1} d_{ij} f^{i-s}(\upsilon_j)$ とおくと, $f^s(\delta) = 0$ となるが.
t の最小性から$\delta \in \mathrm{Im} f$ となる.
これから次は何がわかるかを調べる.
ここで, $c_s, d_{s1}, d_{s2}, \cdots, d_{sr}$ のどれかが 0 でないことに注意. $c_s \neq 0$ ならば,

$$\delta = c_s u + c_{s+1} f(u) + \cdots + c_{t-1} f^{t-s-1}(u)$$

$$-d_{s1}\upsilon_1 - \cdots - d_{sr}\upsilon_r - \sum_{j=1}^{r} \sum_{i=s+1}^{m(\upsilon_j)-1} d_{ij} f^{i-s}(\upsilon_j)$$

より, $u \in \langle \upsilon_1, \cdots, \upsilon_r \rangle + \mathrm{Im} f$ を得る.
よって,

$$V = \langle u, \upsilon_1, \cdots, \upsilon_r \rangle + \mathrm{Im}\ f = \langle \upsilon_1, \cdots, \upsilon_r \rangle + \mathrm{Im}\ f$$

となるので $\{\upsilon_1, \cdots, \upsilon_r\}$ が V の生成系となってしまうが, これは $\{u, \upsilon_1, \cdots, \upsilon_r\}$ が V の極小 f 生成系であることに矛盾. よって $c_s = 0$ である. 次に, $d_{sj} \neq 0 (1 \leq j \leq r)$ ならば必要なら番号を付け替えて $d_{s1} \neq 0$ とすると $\upsilon_1 \in \langle u, \upsilon_2, \cdots, \upsilon_r \rangle + \mathrm{Im} f$ となり, これは $\{u, \upsilon_2, \cdots, \upsilon_r\}$ が V の f 生成系であることを意味するから $\{u, \upsilon_1, ..., \upsilon_r\}$ の極小性に反する
. □

定義 63. 自然数 r と複素数αに対して $J_r(\alpha) = \begin{pmatrix} \alpha & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}$ と定める. $J_r(\alpha)$ を固有値 αの r 次ジョルダンセルという.

定義 64. いくつかのジョルダンセルを対角線上に並べた n 次正方行列

$$\begin{pmatrix} J_{r_1}(\alpha_1) & & & & \\ & J_{r_2}(\alpha_2) & & & 0 \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & J_{r_m}(\alpha_m) \end{pmatrix}$$

を n 次のジョルダンの標準形行列という.

定理 16. 任意の n 次正方行列はあるジョルダン標準形行列に相似である.

補題 31. 線形変換 $f : V \to V$ を考える.
$r := \dim_{\mathbb{C}} V$ とおく. さらに V は f 安定空間として直既約としαは f の固有値とする.
$g := f - \alpha id_V$ とおく. この時 $\mathbf{0} \neq \upsilon \in V$ を適当に取ると,
$\{\upsilon, g(\upsilon), g^2(\upsilon), \cdots, g^{r-1}(\upsilon)\}$ は V の基底となり,
$\{\upsilon, g(\upsilon), g^2(\upsilon), \cdots, g^{r-1}(\upsilon)\}$ に関する f の表現行列は $J_r(\alpha)$ である.

証明. この状況では $V = W_\alpha$であった. ただし W_αはαに属する一般固有空間である. V は g 安定空間としても直既約で g は V 上冪零である. すでに示したように,

$$\mathbf{0} \neq \exists \upsilon \in V \ s.t. \ V = \langle \upsilon, g(\upsilon), g^2(\upsilon), \cdots \rangle$$

ここで $g^m(\upsilon) = 0$ なる $m \geq 1$ を最小に取る.

$$\underline{Claim}\ \upsilon, g(\upsilon), \cdots, g^{m-1}(\upsilon) \text{ は 1 次独立}$$

これが正しいとせよ. すると,
$\upsilon(:= \upsilon_1), g(\upsilon)(:= \upsilon_2), \cdots, g^{m-1}(\upsilon)(:= \upsilon_m)$ は V の基底となるので, $m = r$

$$f(\upsilon_i) = f(g^{i-1}(\upsilon)) = (g + \alpha id_V)(g^{i-1}(\upsilon))$$

$$= g(g^{i-1}(\upsilon)) + \alpha id_V(g^{i-1}(\upsilon)) = g^i(\upsilon) + \alpha g^{i-1}(\upsilon)$$

$$= \upsilon_{i+1} + \alpha \upsilon_i \text{ (ただし} \upsilon_{m+1} = 0 \text{ と約束する)}$$

これより

$$\begin{pmatrix} f(\upsilon_m) & \cdots & f(\upsilon_2) & f(\upsilon_1) \end{pmatrix} = \begin{pmatrix} \upsilon_m & \cdots & \upsilon_2 & \upsilon_1 \end{pmatrix} \begin{pmatrix} \alpha & 1 & & 0 \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}$$

であり f の表現行列は $J_r(\alpha)$ であるので補題は成り立つ.
Claim を示す.
証明

$$c_0v + c_1g(v) + c_2g^2(v) + \cdots + c_{m-1}g^{m-1}(v) = 0 \ (c_i \in \mathbb{C})$$

とすると

$$g^{m-1}(c_0v + c_1g(v) + \cdots + c_{m-1}g^{m-1}(v) = g^{m-1}(\mathbf{0}) = \mathbf{0}$$

$$c_0g^{m-1}(v) + c_1g^m(v) + \cdots + c_{m-1}g^{2m-2}(v) = \mathbf{0}$$

m の取り方より $c_0 = 0$.
よって

$$c_1g(v) + c_2g^2(v) + \cdots + c_{m-1}g^{m-1}(v) = \mathbf{0}$$

となり, また g^{m-2}を作用させて $c_1 = 0$ を導く. これを繰り返し $c_0, \cdots, c_{m-1}$の 1 次独立性がわかる. □

ジョルダンの定理の証明
A は n 次 正方行列とし, $f := f_A : \mathbb{C}^n \ni v \mapsto Av \in \mathbb{C}^n$ とおく.
$V \simeq \mathbb{C}^n = W_1 \oplus W_2 \oplus \cdots \oplus W_m$ と表す. ただし各 W_iは f 安定空間として直既約な部分空間とできる. α_iを $f|_{W_i} : W_i \to W_i$ の固有値とすると, この状況では W_iは $W_i = W_{\alpha_i}$ という一般固有空間と一致する. $r_i = \dim W_i$ とおくと,
上の補題より W_iの適当な基底 $\{v_{i,1}, v_{i,2} \cdots v_{i,r_i}\}$ に関する $f|_{W_i}$の表現行列は $J_{r_i}(\alpha_i)$ である.
すると

$$\{v_{1,1}, \cdots, v_{1,r_1}, v_{2,1}, \cdots, v_{2,r_2}, \cdots\cdots, v_{m,1}, \cdots, v_{m,r_m}$$

は V の基底となりこの基底に関して f を表現すると

$$J := \begin{pmatrix} J_{r_1}(\alpha_1) & & & & \\ & J_{r_2}(\alpha_2) & & & \mathbf{0} \\ & & \ddots & & \\ & & & \ddots & \\ \mathbf{0} & & & & J_{r_m}(\alpha_m) \end{pmatrix}$$

となる. すなわち正則行列

$$P := \begin{pmatrix} v_{1,1} & \cdots & v_{1,r_1} & \cdots & \cdots & v_{m,1} & \cdots & v_{m,r_m} \end{pmatrix}$$

とおくと

$$PJ = \begin{pmatrix} f(v_{1,1}) & \cdots & f(v_{1,r_1}) & \cdots & \cdots & f(v_{m,1}) & \cdots & f(v_{m,r_m}) \end{pmatrix}$$

$$PJ = \begin{pmatrix} Av_{1,1} & \cdots & Av_{1,r_1} & \cdots & Av_{m,1} & \cdots & Av_{m,r_m} \end{pmatrix} = AP$$

$$J = P^{-1}AP \tag{2.11}$$

ジョルダン標準形の求め方

$\begin{pmatrix} A_1 & & O \\ & \ddots & \\ O & & A_r \end{pmatrix}$ を $A_1 \oplus \cdots \oplus A_r$ とかくことにする. 以下 A は n 次正方行列とする. $\lambda_1, \cdots, \lambda_r$ を A の異なる固有値全体とし, A の固有方程式を

$$\chi_A(x) = (x-\lambda_1)^{n_1}(x-\lambda_2)^{n_2}\cdots(x-\lambda_r)^{n_r} \ (i \neq j \text{ ならば} \lambda_i \neq \lambda_j)$$

とおく.
このとき

$$\underset{n_i\text{次行列}}{J_i} = \bigoplus_{m=1,2,\ldots} \left(\underset{\text{この個数を } c_m(\lambda_i) \text{ とおく}}{J_m(\lambda_i) \oplus \cdots \oplus J_m(\lambda_i)} \right)$$

とすると A のジョルダン標準形を J とすると $J = J_1 \oplus J_2 \cdots \oplus J_r$ と表せる.

定理 17.

$$n_i = \sum_{m=1,2,\ldots} m c_m(\lambda_i)$$

である. よって $m > n_i$ ならば $c_m(\lambda_i) = 0$.

定義 65. $r_m(\lambda_i) := \operatorname{rank}(A - \lambda_i I_n)^m$ と定める. n 次単位行列の階数は n ということもあり $r_0(\lambda_i) := n$ と約束する.

定理 18.

$$c_m(\lambda_i) = r_{m-1}(\lambda_i) - 2r_m(\lambda_i) + r_{m+1}(\lambda_i)$$

が成り立つ. 右辺は行列 A で決まるので, 左辺のジョルダンセルの情報も A だけで決まり, ジョルダン標準形は一意に定まることがわかる. 相似な行列の固有値は等しくジョルダンセルの個数が A のみで決まるからジョルダン標準形は一意である.

証明. まずある正則行列 P があって $P^{-1}AP = J$ となる.
すると

$$P^{-1}(A-\lambda_i I_n)^m P = (J-\lambda_i I_n)^m \text{ より } r_m(\lambda_i) = \operatorname{rank}(J-\lambda_i I_n)^m$$

($\because$ 正則行列をかけてもランクは変わらない) ここで

$$J_j - \lambda_i I_{n_j} = \begin{pmatrix} \lambda_j-\lambda_i & & & * \\ & \lambda_j-\lambda_i & & \\ & & \ddots & \\ O & & & \lambda_j-\lambda_i \end{pmatrix}$$

$$|J_j - \lambda_i I_{n_j}| = (\lambda_j-\lambda_i)^{n_j} \underset{i\neq j \text{ の時}}{\neq} 0$$

であるから $j \neq i$ の時 $J_j - \lambda_i I_{n_j}$ は正則, すると $(J_j - \lambda_i I_{n_j})^m$ も正則

つまり

$$i \neq j \text{ の時 } \operatorname{rank}(J_j - \lambda_i I_{n_j})^m = n_j$$

よって

$$r_m(\lambda_i) = n_1 + \cdots + n_{i-1} + n_{i+1} + \cdots + n_r + \mathrm{rank}(J_i - \lambda_i I_{n_i})^m$$

となり,

$$r_m(\lambda_i) = n - n_i + \mathrm{rank}(J_i - \lambda_i I_{n_i})^m \tag{2.12}$$

である.

$$J_i - \lambda_i I_{n_i} = \bigoplus_{k=1}^{n_i} \Bigg(\underbrace{(J_k(\lambda_i) - \lambda_i I_k) \oplus \cdots \oplus (J_k(\lambda_i) - \lambda_i I_k)}_{c_k(\lambda_i)\text{ 個}} \Bigg)$$

$$= \bigoplus_{k=1}^{n_i} \Bigg(\underbrace{J_k(0) \oplus \cdots \oplus J_k(0)}_{c_k(\lambda_i)\text{ 個}} \Bigg)$$

$$(J_i - \lambda_i I_{n_i})^m = \bigoplus_{k=1}^{n_i} (J_k(0) \oplus \cdots \oplus J_k(0))^m$$

$$= \bigoplus_{k=1}^{n_i} \Bigg(\underbrace{J_k(0)^m \oplus \cdots \oplus J_k(0)^m}_{c_k(\lambda_i)\text{ 個}} \Bigg)$$

よって,

$$\mathrm{rank}(J_i - \lambda_i I_{n_i})^m = \sum_{k=1}^{n_i} c_k(\lambda_i) \mathrm{rank} J_k(0)^m$$

である.

$$J_k(0) = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ & 0 & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix},\ J_k(0)^2 = \begin{pmatrix} 0 & 0 & 1 & \cdots & 0 \\ & 0 & 0 & \ddots & \\ & & 0 & \ddots & 1 \\ & & & \ddots & 0 \\ & & & & 0 \end{pmatrix},\ J_k(0)^k = 0$$

であるから

$$\mathrm{rank} J_k(0)^m = k - m (m \leq k-1 \text{ の時}),\ 0 (m \geq k \text{ の時})$$

となり

$$\mathrm{rank}(J_i - \lambda_i I_{n_i})^m = \sum_{k \geq m+1} c_k(\lambda_i)(k-m)$$

(2.12) に代入し, $r_m(\lambda_i) = n - n_i + \sum_{k \geq m+1}^{\infty} c_k(\lambda_i)(k-m)$. これより

$$r_{m-1}(\lambda_i) - 2r_m(\lambda_i) + r_{m+1}(\lambda_i)$$

$$= \sum_{k=m+2}^{\infty} c_k(\lambda_i)\{(k-m+1) - 2(k-m) + (k-m-1)\} - 2c_{m+1}(\lambda_i)(m+1-m) + c_m(\lambda_i)(m-m+1) + c_{m+1}(\lambda_i)(m+1-m+1)$$

$$= c_m(\lambda_i)$$

□

定理 19 (定理 A)**.**

$$\sum_{m=1}^{n_i} m \cdot c_m(\lambda_i) = n_i,\ \ c_m(\lambda_i) = 0\ (if\ m > n_i)$$

定理 20 (定理 B)**.**

$$c_m(\lambda_i) = r_{m-1}(\lambda_i) - 2r_m(\lambda_i) + r_{m+1}(\lambda_i)$$

これらを使いジョルダンセルの情報についての連立方程式を解いて任意の正方行列のジョルダン標準形を求めることができる.

例 10.

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

定理 A より,

$$c_m(1) = 0\ if\ m \geq 2.\ c_1(1) = 1$$

$$c_m(2) = 0\ if\ m \geq 3.\ c_1(2) + 2c_2(2) = 2.$$

定理 B より

$$c_1(2) = r_0(2) - 2r_1(2) + r_2(2)$$

$$A - 2I = \begin{pmatrix} -1 & 2 & 2 \\ 0 & 0 & 1 \\ -1 & 2 & 0 \end{pmatrix}.\ r_1(2) = 2.$$

$$(A-2I)^2 = \begin{pmatrix} -1 & 2 & 0 \\ -1 & 2 & 0 \\ 1 & -2 & 0 \end{pmatrix}.\ r_2(2) = 1.$$

$r_0(2) = 3$ であるから, $c_1(2) = 3 - 2 \times\ 2\ + 1 = 0$ となる. そして $c_2(2) = 1$ も求まる. よって

$$J_A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} = J_1(1) \oplus J_2(2)$$

例 11. $A = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 1 & 2 & 0 & 2 \\ 3 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ とする. $\chi_A(x) = (x-1)^2(x-2)^2$.

定理 A より, $c_m(1) = 0\ if\ m \geq 3.\ c_1(1) + 2c_2(1) = 2.$

$c_m(2) = 0\ if\ m \geq 3.\ c_1(2) + 2c_2(2) = 2.$

定理 B より

$$c_1(1) = r_0(1) - 2r_1(1) + r_2(1)$$

$$c_1(2) = r_0(2) - 2r_1(2) + r_2(2)$$

$$A - I = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 1 & 1 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \ r_1(1) = 3.$$

$$(A - I)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \ r_2(1) = 2.$$

$$c_1(1) = 4 - 2 \cdot \ 3 \ + 2 = 0. \ c_2(1) = 1.$$

$\cdots$ とやり, $c_1(2) = 2$, $c_2(2) = 0$. よって

$$J_A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

例 12. $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -2 & 7 & -9 & 5 \end{pmatrix}$ のジョルダン標準形を求める. $\chi_A(x) = (x-2)(x-1)^3$.

$$J_A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

$\begin{pmatrix} -2 & 7 & 2 & -3 \\ -1 & 4 & 1 & -2 \\ -2 & 9 & 2 & -4 \\ -2 & 8 & 2 & -4 \end{pmatrix}$ のジョルダン標準形は $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

単因子を導入した方法

有理標準形を経由した方法『ジョルダン標準形』, 韓太舜・伊里正夫

定理 21 (有理標準形)**.** n 次正方行列 A は適当な正則行列 S を用いて

$$S^{-1}AS = \begin{pmatrix} C_1 & & O \\ & C_2 & \\ & & \ddots \\ O & & C_t \end{pmatrix}$$

の形のブロック対角行列にできる. 各ブロック $C_i (i = 1, ..., t)$ は n_i次のコンパニオン行列

$$C_i = \begin{pmatrix} 0 & \cdots & \cdots & 0 & {a_0}^{(i)} \\ 1 & 0 & \cdots & 0 & {a_1}^{(i)} \\ & 1 & \ddots & \vdots & \vdots \\ & & \ddots & 0 & \vdots \\ O & & & 1 & {a_{n_i-1}}^{(i)} \end{pmatrix} \tag{2.13}$$

であり, C_{j+1}の最小多項式は C_j の最小多項式を割り切る. $(j = 1, ..., t-1)$ (2.13) の形の行列を有理標準形といい A に対し一意的に定まる. また相似な行列の有理標準形は一致し, 逆に有利標準形が一致するならば 2 つの行列は相似である.

が成り立つとせよ.

証明. n 次行列 A の有理標準形 $S^{-1}AS = C_1 \oplus \cdots \oplus C_t$が (2.13) のように定められたとする. $C_1, \cdots, C_t$の最小多項式を$\varphi_1(x), \varphi_t(x)$ とする ($\varphi_i(x)$ の次数は m_i). まず最初のコンパニオン行列　C_1 に対して, C_1の全ての異なる固有値を$\lambda_1, ..., \lambda_l$として$\varphi_1(x) = x^{m_1} - a_{m_1-1}x^{m_1-1} - \cdots - a_1x - a_0$ を

$$\varphi_1(x) = (x - \lambda_1)^{p_1} \cdots (x - \lambda_l)^{p_l} \ (p_1 + \cdots + p_l = m_1)$$

とおく. 次に固有値 λ_1に対し $m_1 \times p_1$行列 ${U_1}^{(1)}$を

$${u_{ij}}^{(1)} = \binom{i-1}{p_1-j} {\lambda_1}^{i+j-p_1-1} \ (i = 1, ..., m_1; j = 1, ..., p_1)$$

を (i, j) 成分とする行列として定義する. ただし $\binom{k}{l}$ は $l > k$ または $l < 0$ の時は 0 と約束す

る. これを行列表示すると

$$U_1{}^{(1)} = \begin{pmatrix} 0 & \cdots & 0 & 1_{(1,p_1)\text{ 成分}} \\ \vdots & & 1 & \lambda_1 \\ \vdots & & & {\lambda_1}^2 \\ 0 & 1 & \cdots & {\lambda_1}^{p_1-2} \\ 1_{(1,p_1)\text{ 成分}} & \binom{p_1-1}{p_1-2}\lambda_1 & \cdots & {\lambda_1}^{p_1-1} \\ \binom{p_1}{p_1-1}\lambda_1 & \binom{p_1}{p_1-2}{\lambda_1}^2 & \cdots & {\lambda_1}^{p_1} \\ \vdots & \vdots & & \vdots \\ \binom{m_1-1}{p_1-1}{\lambda_1}^{m_1-p_1}{}_{(1,m_1)\text{ 成分}} & \binom{m_1-1}{p_1-2}{\lambda_1}^{m_1-p_1+1} & \cdots & {\lambda_1}^{m_1-1} \end{pmatrix}$$

すると

$$\underline{Claim}\ {C_1}^T {U_1}^{(1)} = {U_1}^{(1)} J^T(p_1, \lambda_1)$$

が成り立つとせよ. ただし ${C_1}^T$ は C_1 の転置行列, ${J^T}_{p_1}(\lambda_1)$ はジョルダンセル $J_{p_1}(\lambda_1)$ の転置行列である.
他の固有値 $\lambda_2, \cdots, \lambda_l$に対しても同様にして得られる $m_1 \times p_k$行列を ${U_k}^{(1)}$ $(k = 2, ..., l)$ とすれば

$${C_1}^T {U_k}^{(1)} = {U_k}^{(1)} {J^T}_{p_k}(\lambda_k)\ (k = 2, ..., l)$$

$k = 1, ..., l$ の場合をまとめると

$${C_1}^T U^{(1)} = U^{(1)} J^{(1)T}$$

$$U^{(1)} = [{U_1}^{(1)}, {U_2}^{(1)}, \cdots, {U_l}^{(1)}]$$

$$J^{(1)T} = J^T_{p_1}(\lambda_1) \oplus \cdots \oplus J^T_{p_l}(\lambda_l)$$

となる. $U^{(1)}$は ${U_1}^{(1)}, \cdots {U_l}^{(1)}$をこの順に並べた m_1 次正方行列である. 同様に他のコンパニオン行列 $C_2, \cdots, C_t$ に対しても行い, m_2次行列 $U^{(2)}, J^{(2)T}$から m_t次行列 $U^{(t)}, J^{(t)T}$を作り

$$U = U^{(1)} \oplus U^{(2)} \oplus \cdots \oplus U^{(t)}$$

とおくと, U は n 次正方行列で

$$U^{-1} \begin{pmatrix} {C_1}^T & & & O \\ & {C_2}^T & & \\ & & \ddots & \\ O & & & {C_t}^T \end{pmatrix} U = \begin{pmatrix} J^{(1)T} & & & O \\ & J^{(2)T} & & \\ & & \ddots & \\ O & & & J^{(t)T} \end{pmatrix}$$

となる. ただし, $\underline{Claim}$ U は正則すなわち $U^{(1)}, \cdots, U^{(t)}$ が正則となることは正しいとせよ.
両辺の転置をとって

$$U^T \begin{pmatrix} C_1 & & & O \\ & C_2 & & \\ & & \ddots & \\ O & & & C_t \end{pmatrix} (U^T)^{-1} = \begin{pmatrix} J^{(1)} & & & O \\ & J^{(2)} & & \\ & & \ddots & \\ O & & & J^{(t)} \end{pmatrix}$$

に $C_1 \oplus \cdots \oplus C_t = S^{-1}AS$ を代入すれば $R = S(U^T)^{-1}$ とおくことで

$$R^{-1}AR = J^{(1)} \oplus \cdots \oplus J^{(t)}$$

を得る. よって有理標準形を経由して任意の正方行列がジョルダン標準形と相似であることがわかった. □

応用例

数列の収束と同様に行列の列についても考える.

定義 66. 複素 $m \times n$ 行列の列 $A^{(k)} = (a_{ij}{}^{(k)}), k = 1, 2, ...(1 \leq i \leq m, 1 \leq j \leq n)$ がある. ある複素 $m \times n$ 行列 $A = (a_{ij})$ が存在して, 任意の i, j に対し

$$\lim_{k\to\infty} a_{ij}{}^{(k)} = a_{ij},\ 1 \leq i \leq m,\ 1 \leq j \leq n$$

が成り立つとき, 列 $A^{(k)}$は A に収束するといい $\lim_{k\to\infty} A^{(k)} = A$ とかく.

ここで, $m \times n$ 行列 $A = a_(ij) \in M_{m,n}(\mathbb{C})$ に対してその 2 乗ノルム $\|A\|_2$を

$$\|A\|_2 = \sqrt{\sum_{1\leq i\leq m, 1\leq j\leq n} |a_{ij}|^2} = \sqrt{\mathrm{tr}A^*A}$$

で定義する

補題 32. $A^{(k)}, A \in M_{m,n}(\mathbb{C}), k = 1, 2...$とし P, Q をそれぞれ m 次, n 次 の正則行列とする. このとき

$$\lim_{k\to\infty} A^{(k)} = A \Leftrightarrow \lim_{k\to\infty} PA^{(k)}Q = PAQ \tag{2.14}$$

証明.

$$\|PA^{(k)}Q - PAQ\|_2 \leq \|P\|_2\|A^{(k)} - A\|_2\|Q\|_2$$
$$\|A^{(k)} - A\|_2 \leq \|P_2^{-1}\|PA^{(k)}Q - PAQ\|_2\|Q^{-1}\|_2$$

□

ジョルダンセルを l 乗した行列はどんなものであるかみてみると

$$J_m(\alpha)^l = \begin{cases} \begin{pmatrix} \alpha^l & l\alpha^{l-1} & \frac{l}{2}(l-1)\alpha^{l-2} & \cdots & {}_lC_{m-1}\alpha^{l-m+1} \\ & \alpha^l & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & \frac{l}{2}(l-1)\alpha^{l-2} \\ & & & \ddots & l\alpha^{l-1} \\ O & & & & \alpha^l \end{pmatrix} & l \geq m-1 \text{ のとき} \\ \begin{pmatrix} \alpha^l & l\alpha^{l-1} & \cdots & 1 & 0 \\ & \alpha^l & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & \ddots & \ddots & \vdots \\ & & & & \ddots & l\alpha^{l-1} \\ O & & & & & \alpha^l \end{pmatrix} & 0 \leq l < m-1 \text{ のとき} \end{cases} \tag{2.15}$$

定理 22. $A \in M_n(\mathbb{C})$ に対し $\lim_{k\to\infty} A^k$が存在するための必要十分条件は, A の任意の固有値 λに対し $|\lambda| < 1$ が成り立つことである. スペクトル半径ρを使うと$\rho(\lambda) < 1$ のことであり, また次の証明より明らかに$\rho(\lambda) < 1 \Leftrightarrow \lim_{k\to\infty} A^k = O$ である.

証明. $P^{-1}AP = J_A = \oplus_i J_i$を A のジョルダン標準形, J_i をジョルダン細胞とする. (2.14) より $\lim_{k\to\infty} A^k$が存在するためには $P^{-1}A^kP = \oplus_i J_i{}^k$ ゆえ, すべての i について $\lim_{k\to\infty} J_i{}^k$ が存在することが必要十分である. そこで $\lim_{k\to\infty} J_m(\alpha)^k$ について考える. $J_m(\alpha)$ は上 (2.15) で与えれるから,
$\lim_{k\to\infty} J_m(\alpha)^k$ が存在するには, $\lim_{k\to\infty} \alpha^k$ が存在すること, すなわち $|\alpha| < 1$ か$\alpha = 1$ であることが必要十分.
$|\alpha| < 1$ ならば

$$\lim_{k\to\infty} {}_kC_{m-1}\alpha^{k-m+1} = 0$$

より $\lim_{k\to\infty} J_m(\alpha)^k = 0$ は m によらず成り立つ. $\alpha = 1$ の時 $m \geq 2$ なら

$$J_m(\alpha)^k = \begin{pmatrix} 1 & k & & * \\ & \ddots & \ddots & \\ & & \ddots & k \\ O & & & 1 \end{pmatrix}$$

ゆえ極限は存在しない. □

定義 67. $A \in M_n(\mathbb{C})$ に対し

$$\rho(A) = \max\{|\alpha|; \alpha は A は固有値\}$$

を A のスペクトル半径という.

定理 23. 冪級数 $\sum_{k=0}^{\infty} c_k z^k$ $(z \in \mathbb{C})$ の収束半径を r とすると $A \in M_n(\mathbb{C})$ に対して

$$\rho(A) = 0 または \rho(A) < r ならば \sum_{k=0}^{\infty} c_k A^k は収束.$$

$$\rho(A) > r ならば \sum_{k=0}^{\infty} c_k A^k は発散.$$

証明. $\rho(A) = 0$ なら

$$A = \begin{pmatrix} 0 & & * \\ & \ddots & \\ & & 0 \end{pmatrix}$$

より A は冪零行列なので冪級数は有限和になるから収束する.
$P^{-1}AP = J_A = \bigoplus_i J_i$を A のジョルダン標準形, J_iをジョルダンセルとすると

$$\sum_{k=0}^{l} c_k A^k = \sum_{k=0}^{l} c_k (PJ_AP^{-1})^k = P(\sum_{k=0}^{l} c_k {J_A}^k)P^{-1}$$

$$= P\left(\bigoplus_i (\sum_k c_k J_i{}^k)\right) P^{-1}$$

なので全ての i に対し $\sum_{k=0}^{\infty} c_k {J_i}^k$ が収束するすることが必要である. そこで一般に $\sum_{k=0}^{\infty} c_k J(\alpha;m)^k$ の収束を調べる. $J(\alpha;m) = \alpha I_m + N, N = J(0;m)$ で $N^m = 0$ だから,

$$\sum_{k=0}^{l} c_k J(\alpha;m)^k = \sum_{k=0}^{l} c_k (\alpha I_m + N)^k = \sum_{k=0}^{l} c_k \left(\sum_{j=0}^{k} {}_kC_j \alpha^{k-j} N^j \right)$$

$$= \sum_{j=0}^{m-1} \left(\sum_{k\geq j}^{l} {}_kC_j c_k \alpha^{k-j} \right) N^j$$

$$= \sum_{j=0}^{m-1} \left(\frac{1}{j!} \sum_{k\geq j}^{l} \frac{k!}{(k-j)!} c_k \alpha^{k-j} \right) N^j$$

従って

$$\sum_{k=0}^{\infty} c_k J(\alpha;m)^k \text{が収束} \Leftrightarrow \forall j = 0,1,...,m-1 \text{ に対して} \sum_{k\geq j}^{\infty} \frac{k!}{(k-j)!} c_k \alpha^{k-j} \text{が全て収束}$$

となることがわかる. (行列が出ない形に帰着できた.)
$\sum_{k\geq j}^{\infty} \frac{k!}{(k-j)!} c_k z^{k-j}$ は $\sum_{k=0}^{\infty} c_k z^k$ を j 回項別微分した級数なので元の級数と同じ収束半径 r をもつ. よって題意が成り立つ. □

命題 88. $A \in M_n(\mathbb{C})$ とする.
(1)$\| \exp A \|_2 \leq \exp \|A\|_2$
(2)$B \in M_n(\mathbb{C})$ で $AB = BA$ が成り立つならば, $\exp(A+B) = \exp A \exp B$

証明. (1)

$$\| \sum_{k=0}^{\infty} \frac{1}{k!} A^k \|_2 \leq \sum_{k=0}^{\infty} \frac{1}{k!} \|A^k\|_2 \leq \sum_{k=0}^{\infty} \frac{1}{k!} \|A\|_2{}^k = \exp \|A\|_2$$

(2)

$$\|(\sum_{k=0}^{2N} \frac{A^k}{k!})(\sum_{k=0}^{2N} \frac{B^k}{k!}) - \sum_{k=0}^{2N} \frac{1}{k!}(A+B)^k\|_2 \to 0 \ (N \to \infty)$$

をいえばよい.
claim
$A, B \in M_n$ で $AB = BA$ のとき

$$(A+B)^k = \sum_{j=0}^{k} {}_kC_j A^{k-j} B^j$$

が成り立つことを正しいとせよ. すると

$$\sum_{k=0}^{2N} \frac{1}{k!}(A+B)^k = \sum_{k=0}^{2N} \frac{1}{k!} \sum_{j=0}^{k} {}_kC_j A^{k-j} B^j = \sum_{k=0}^{2N} \sum_{j=0}^{k} \frac{1}{(k-j)!\,j!} A^{k-j} B^j$$

$$= \sum_{\substack{0\le p+q\le 2N \\ p,q\ge 0}} \frac{A^p}{p!}\frac{B^q}{q!}$$

したがって

$$\|\sum_{k=0}^{2N}\frac{A^k}{k!}\sum_{k=0}^{2N}\frac{B^k}{k!} - \sum_{k=0}^{2N}\frac{1}{k!}(A+B)^k\|_2$$
$$= \|\sum_{\substack{p+q>2N \\ 0\le p,q\le 2N}} \frac{A^p}{p!}\frac{B^q}{q!}\|_2 \le \sum_{\substack{p+q>2N \\ 0\le p,q\le 2N}} \frac{\|A\|_2{}^p}{p!}\frac{\|B\|_2{}^q}{q!}$$

最後の項の数は $N(2N+1)$ である. p,q の一方は N より大きいので $p!q! \ge N!$だから

$$\max(\|A\|_2, \|B\|_2, 1) = \psi$$

とすれば

$$\sum_{\substack{p+q>2N \\ 0\le p,q\le 2N}} \frac{\|A\|_2{}^p}{p!}\frac{\|B\|_2{}^q}{q!} \le \frac{N(2N+1)}{N!}\psi^{4N} \to 0(N\to\infty)$$

よって $\exp(A+B) = \exp A \exp B$. □

2.13 [2] 第 1 章

問 40 (1.1.7)**.** $f : A \to B$ を写像とする. f が全射であることと任意の $S \subset B$ に対して $f(f^{-1}(S)) = S$ は同値である.

証明. ($\Rightarrow$) 任意に $x \in f(f^{-1}(S))$ を取るとある $y \in f^{-1}(S)$ が存在して $x = f(y)$ である. すると $x = f(y) \in S$. よって $f(f^{-1}(S)) \subset S$ である. 逆に任意に $x \in S$ を取り $S \subset f(f^{-1}(S))$ を示す. f は全射なのである $y \in A$ が存在して $f(y) = x \in S$ となる. よって $y \in f^{-1}(S)$ であり $x = f(y) \in f(f^{-1}(S))$. よって $S \subset f(f^{-1}(S))$ が成り立つ. □

問 41. 任意の部分集合 $S \subset B$ に対して $f^{-1}(f(f^{-1}(S))) = f^{-1}(S)$ である.

証明. 任意に $x \in f^{-1}(f(f^{-1}(S)))$ を取る. すると, ある $y \in f(f^{-1}(S))$ が存在して $f^{-1}(y) = x$ である. $y = f(x) \in f(f^{-1}(S))$ となる. もし $x \notin f^{-1}(S)$ と仮定すると $f(x) \in f(f^{-1}(S))$ に矛盾するので $x \in f^{-1}(S)$ である. よって $\subset$ は示せた. 逆に任意に $x \in f^{-1}(S)$ を取ると $f(x) \in f(f^{-1}(S))$ で $x \in f^{-1}(f(f^{-1}(S)))$ である. □

問 42. (1) A, B を空でない集合とする. A の部分集合 S と単射写像 $f : S \to B$ の組 (S, f) の集合を X とする. $(S_1, f_1), (S_2, f_2) \in X$ に対し $S_1 \subset S_2$ で f_2が f_1の拡張であるとき, $(S_1, f_1) \le (S_2, f_2)$ と定める. これは X 上の順序である. X に極大元が存在することを示せ.
(2) (S_0, f_0) が X の極大元なら, (a) $S_0 = A$ または (b) $f_0(S_0) = B$ を示せ.

解 133. (1) X は順序集合の定義を満たす. また X の任意の全順序 (無限) 部分集合 $\mathcal{X}_k = \{(S_i, f_i) \mid i \in \mathbb{N}, \min_k \le i \le \max_k\} \subset X$ ($\max_k \le \infty$) の上界は, $(S_{\max_k}, f_{\max_k}) \in X$ として存在する. よってツォルンの補題より X は極大元をもつ. (2) $f : A \to B$ が単射なら (S_0, f_0) の極大条件より $S_0 = A$ である. もし $f : A \to B$ が単射でないなら X の極大元 (S_0, f_0) が定める $f_0 : S_0 \to B$ は全射でもある. すなわち $f_0(S_0) = B$ である. 極大元の存在をいうために同値なトゥーキーの補題を用いてもよい.

2.14 [2] 第 2 章

解 134 (2.1.1)**.** 単位元は 1 である. G の任意の元に対して逆元が存在することが群であることの必要条件であるが, $\neg\exists 0^{-1}(0\cdot 0^{-1}=1)$ である.

解 135 (2.1.2)**.** 単位元は $0\in\mathbb{R}$ である. 任意の元に対して逆元が存在するか否かをみる. 仮に群であると仮定すると, $\exists a^{-1}\in\mathbb{R}\ s.t.\ a\circ a^{-1}=a+a^{-1}+aa^{-1}=0$. このとき $a^{-1}=\frac{-a}{a+1}$ である.
$a=-1$ は逆元を持たないので群ではない.

解 136 (2.1.3)**.** $\mathfrak{S}_3$の乗法表については$\sigma\in\{$ 縦においた置換全体 $X\},\tau\in\{$ 横においた置換全体 $Y\}$ に対し$\tau\sigma\in\{(X,Y)\}$ というように読む.

解 137 (2.1.4)**.** 結合法則とは $A,B,C\in G$ に対して $(AB)C=A(BC)$ というものであるからまず $((ab)c)d=(ab)(cd)$ である. また $A\leftarrow a,B\leftarrow b,C\leftarrow cd$ として $(ab)(cd)=a(b(cd))$. 最後に, $a(b(cd))=a((bc)d)$ が成り立つ.

解 138 (2.1.6)**.** (1) 確かに$\sigma_1^{-1}\sigma_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ となる.

解 139 (2.3.2)**.** $\mathrm{Sp}(2n)=\{g\in G:g^t\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}\}\subset GL_{2n}(\mathbb{R})$ は部分群であることを示す. $g_1,g_2\in\mathrm{Sp}(2n)$ が $g_1^{-1}g_2\in\mathrm{Sp}(2n)$ を満たすことをみる. 定義より

$$g_2^t\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g_2=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix},\quad g_1^{-1}\begin{pmatrix}0&-I_n\\I_n&0\end{pmatrix}g_1^*=\begin{pmatrix}0&-I_n\\I_n&0\end{pmatrix}$$

である. よって

$$\begin{cases}g_2^t=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g_2^{-1}\begin{pmatrix}0&-I_n\\I_n&0\end{pmatrix}\\ g_1^*=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g_1\begin{pmatrix}0&-I_n\\I_n&0\end{pmatrix}\end{cases}$$

これを用いると

$$\begin{aligned}&(g_1^{-1}g_2)^t\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}(g_1^{-1}g_2)=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}\\ \Leftrightarrow&\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g_2^{-1}\begin{pmatrix}0&-I_n\\I_n&0\end{pmatrix}\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g_1\begin{pmatrix}0&-I_n\\I_n&0\end{pmatrix}\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}g_1^{-1}g_2=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}\\ \Leftrightarrow&\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}=\begin{pmatrix}0&I_n\\-I_n&0\end{pmatrix}\end{aligned}$$

解 140 (2.3.3)**.** $U(n)=\{g\in G:g^*g=I_n\}$ の任意の元 $g_1,g_2\in U(n)$ に対し $g_1^{-1}g_2\in U(n)$ が満たされることを示す. すなわち

$$(g_1^{-1}g_2)^*(g_1^{-1}g_2)=I_n\Leftrightarrow g_2^*(g_1^{-1})^*g_1^{-1}g_2=I_n$$

を示す. これは $(g_1^{-1})^*=g_1,\ g_2^*g_2=I_n$より成り立つ.

解 141 (2.3.4)**.** (1) $G = GL_n(\mathbb{R})$ の部分集合 B が部分群であることを示す. 任意に $m = \begin{pmatrix} b_{11} & & O \\ & \ddots & \\ b_{n1} & & b_{nn} \end{pmatrix}, n = \begin{pmatrix} b'_{11} & & O \\ & \ddots & \\ b'_{n1} & & b'_{nn} \end{pmatrix}$ をとり, $m^{-1}n = \begin{pmatrix} \frac{1}{b_{11}} & & O \\ & \ddots & \\ * & & \frac{1}{b_{nn}} \end{pmatrix}\begin{pmatrix} b'_{11} & & O \\ & \ddots & \\ b'_{n1} & & b'_{nn} \end{pmatrix} = \begin{pmatrix} \frac{b'_{11}}{b_{11}} & & O \\ & \ddots & \\ * & & \frac{b'_{nn}}{b_{nn}} \end{pmatrix} \in B$ より B は $GL_n(\mathbb{R})$ の部分群である. (2) $\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$ より可換群でない.

解 142 (2.3.5)**.** 任意に $x, y \in \mathbb{R}_>$ を取ると $x^{-1}y = \frac{y}{x} \in \mathbb{R}_>$ より $\mathbb{R}^\times$ の部分群.

解 143 (2.3.6)**.** 単位元 $0 \notin \mathbb{R}_>$ より部分群ではない.

解 144 (2.3.7)**.** 群 H が巡回群であることを示す為には H の任意の元がある固定した元 h の冪としてかけることをいう必要がある. $z \in H$ とすると $h_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ $(k = 0, 1, ..., n-1)$ である. 部分群であることは $x, y \in H$ に対し $(x^{-1}y)^n = (x^n)^{-1}y^n = 1^{-1}1 = 1$ より $x^{-1}y \in H$ より. 巡回群であることを示すために $k \in \{0, ..., n-1\}$ を任意に取り, $h \in H$ を固定する. $(h^k)^n = (h^n)^k = 1$ より $h^k \in H$ すなわち $\langle h\rangle \subset H$. $h_0, ..., h_{n-1}$ は相異なり $\langle h\rangle$ の位数は n. よって $H = \langle h\rangle$ である.

解 145 (2.3.8)**.** (1) $\mathfrak{S}_3$ は巡回群ではない. 巡回群ならばアーベル群なので, その対偶よりアーベル群でないことを示す. 実際, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$ は可換でない. また, 元の位数に注目することもできる. $\mathfrak{S}_3$ がもし巡回群なら 6 つの任意の元に対しある $\sigma \in \mathfrak{S}_3$ が存在して $\sigma^6 = 1$ を満たす. $e, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$ はそれぞれ $\sigma_1 = 1, \sigma_2^2 = 1, \sigma_3^2 = 1, \sigma_4^3 = 1, \sigma_5^3 = 1, \sigma_6^2 = 1$ より矛盾している.
(2) もし $(\mathbb{Q}, +)$ が g を生成元とする巡回群なら任意の $\mathbb{Q}$ の元が g の冪 $(g^1 = g + 0, g^n = g + g^{n-1}; n \geq 1$ とかく) でかけるので, $\exists n \in \mathbb{N}\,(\frac{g}{5} = g^n = ng)$ これは矛盾している. (3) $(\mathbb{R}, +)$ が g を生成元とする巡回群と仮定する. このとき $\pi g \in \mathbb{R}$ に対し $\pi g = ng$ となる $n \in \mathbb{N}$ が存在する. これは矛盾. (4) $(\mathbb{Q}^\times, \times)$ が g を生成元とする巡回群であると仮定する. 任意の $\mathbb{Q}^\times$ の元が g の冪でかけるので, ある正整数 n が存在して $-1 = g^n$ を満たす. $1 = (-1)^2 = g^{2n}$ より g の位数は有限である. よって $\mathbb{Q}^\times = \langle g\rangle$ の位数 $|\langle g\rangle|$ も有限であるが, $|\mathbb{Q}^\times| = \infty$ より矛盾している.
(5) $\mathbb{Z} \times \mathbb{Z}$ が (a, b) を生成元とする巡回群であると仮定する. するとある整数 n, m が存在して $n(a, b) = (na, nb) = (1, 0)$, $m(a, b) = (ma, mb) = (0, 1)$ を満たす. $na = 1$ かつ $nb = 0$ より $b = 0$. $mb = 1$ に矛盾する.

解 146 (2.3.9)**.** (1) $\mathfrak{S}_n$ は $\sigma_1 = (1\,2), ..., \sigma_{n-1} = (n-1\,n)$ で生成される. これは対称群の任意の元は互換の積でかけるということである. $\supset$ は明らかなので $\mathfrak{S}_n \subset \langle (1\,2), ..., (n-1\,n)\rangle := H$ であることを示す. $k \geq 1$ とし互換 $(i\,i+k) \in \mathfrak{S}_n$ を任意に取る. $k = 1$ のとき $(i\,i+1) \in H$ より成り立つ. $(i\,i+k) \in H$ とすると, $(i\,i+k+1) = (i\,i+k)(i+k\,i+k+1)(i\,i+k) \in H$ より $k+1$ の時も成り立つ. よって $\mathfrak{S}_n = H$ である.
(2) $\mathfrak{S}_n = \langle \sigma, \tau \mid \sigma = (12\cdots n), \tau = (12)\rangle$ であることを言う. その為に

$$\mathfrak{S}_n = \langle (1\,2), ..., (n-1\,n)\rangle \subset \langle \sigma, \tau\rangle =: H$$

を示し逆の包含は明らかなので等しいことがわかる. よって任意の互換が

$$(i\,i+k) \in H, \;\; k \geq 1$$

を満たすことを示す. k に関する帰納法を用いる.
$k=1$ のとき $(i\,i+1)=\sigma^{i-1}\tau\sigma^{-(i-1)}(i\geq 1)$ より, $\forall i$ に対し $(i\,i+1)\in H$ が成り立つ. (1) と同様に $(i\,i+k+1)=(i\,i+k)(i+k\,i+k+1)(i\,i+k)$ において k の場合に成り立つことを仮定すると $k+1$ の場合も成り立つ.

解 147 (2.4.4)**.** $\overline{1},\overline{2},...,\overline{p^n}$ という $|\mathbb{Z}/p^n\mathbb{Z}|=p^n$ このうち p の倍数は $p^n/p=p^{n-1}$ こあるので

$$|(\mathbb{Z}/p^n\mathbb{Z})^\times|=p^n-p^{n-1}$$

である.

解 148 (2.4.5)**.** $x^{35d}=1_G$ を満たす最小の d が x^{35} の位数である. $x^{35d}=1\Leftrightarrow 60|35d\Leftrightarrow 12|3d\Leftrightarrow 12|d$ より $d=12$.

解 149 (2.4.6)**.** 前問と同様にして, $d|nm$ であることと $(x^n)^m=1$ は同値である.

$$d|nm\Leftrightarrow \frac{d}{gcd(d,n)}|\frac{n}{gcd(d,n)}m\Leftrightarrow \frac{d}{gcd(d,n)}|m$$

解 150 (2.4.7)**.** 体 $\mathbb{Z}/5\mathbb{Z},\mathbb{Z}/7\mathbb{Z}$ の生成元は加法群 $\mathbb{Z}/5\mathbb{Z},\mathbb{Z}/7\mathbb{Z}$ のそれとは違うことに注意.

解 151 (2.4.8)**.** 単位元の位数は 2 ではないので問題文が不正確である. 任意の $a,b\in G$ に対して $(ab)(ab)=(ab)^2=1, a^2=1, b^2=1$ より $(ab)^{-1}=ab, a^{-1}=a, b^{-1}=b$ である.
$ab=(ab)^{-1}=b^{-1}a^{-1}=ba$ より G は可換群である.

解 152 (2.4.9)**.** (1) g,h の位数は $4,6$. $gh=\begin{pmatrix}1&0\\1&1\end{pmatrix}$ の位数は $(gh)^n=\begin{pmatrix}1&0\\n&1\end{pmatrix}$ より ∞ である.

解 153 (2.4.10)**.** (1) G は可換群なので $(ab)^n=a^nb^n$ が成り立つ. a と b の位数は有限なので ab の位数は有限である. (2) H を G の有限位数の元全体の集合とする. 任意に $a,b\in H$ を取ると a は位数有限なのである正整数 $n<\infty$ が存在して $a^n=1$ を満たす. $(a^{-1})^n=(a^n)^{-1}=1$ より a^{-1} の位数は n の約数より有限. (1) より $a^{-1}b\in H$ である.

解 154 (2.5.1)**.** 略解にあるように群準同型 $\phi:G\to H$ の定め方について G を生成する S の ϕ による行き先を $\phi(x^i)=y^i$ $(\forall i\in\mathbb{Z})$ と定めて良定義であるのは (1) のある条件を満たす必要十分性があるときである. $x^{i_1-i_2}=0$ より $m|i_1-i_2$ つまり $i_1-i_2=km$ となる $k\in\mathbb{Z}$ が存在する.
$x^{i_1}=x^{i_2}$ を満たす任意の i_1,i_2 に対し $y^{i_1}=y^{i_2}$ より m が n の倍数であることが必要十分である. x,y をそれぞれ G,H の生成元とする. m が n の倍数とし, $\forall i\in\mathbb{Z}$ に対し $\phi:G\to H$ を $\phi(x^i)=y^i$ で定めると準同型であることを示す.

$\phi(x_1^i+m\mathbb{Z})\phi(x_2^i+m\mathbb{Z}):=(y_1^i+n\mathbb{Z})(y_2^i+n\mathbb{Z})$, $\phi((x_1^i+m\mathbb{Z})(x_2^i+m\mathbb{Z}))=\phi((x_1x_2)^i+m\mathbb{Z})=(y_1y_2)^i+n\mathbb{Z}$

などとかくのは ϕ の準同型性を示す為にそれを使っていたりで誤答である.

$$\phi(1_G)=\phi(x^m)=y^m=y^{\ell n}=1_H$$

が成り立つ. しかしここから $\phi(1_G1_G)=\phi(1_G)\phi(1_G)$ が成り立つから, ϕ は準同型であるとは言えない. そこで略解にあるように 66 ページ, 命題 [2.10.5] を適用する.

$$\pi_1:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$$

は群準同型であり, 自然な全射を

$$\pi_2 : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

で定める. すると命題 [2.10.5] より

$$\text{群準同型}\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \text{ が存在} \Leftrightarrow m\mathbb{Z} \subset \mathrm{Ker}(\pi_1) = n\mathbb{Z}$$

すなわち, m が n の倍数であることと準同型$\phi : G \to H$ が存在することは同値である.

解 155 (2.5.2)**.** G は可換群なので, $g_1, g_2 \in G$ に対し$\phi_n(g_1g_2) = (g_1g_2)^n = g_1^n g_2^n = \phi_n(g_1)\phi_n(g_2)$ より準同型である.

解 156. (1) $\phi : G \to H$ を準同型, $g \in G$ の位数を有限とする. g の位数は n なので$\phi(g^n) = \phi(1_G) = 1_H$なので$\phi(g^n) = \phi(g)^n = 1_H$より$\phi(g)$ の位数は n の約数である. (2) (1) より$\phi(g)$ の位数を m とし, ある $k \in \mathbb{N}$ が存在して $km = n$ とかける. $\phi(g^m) = \phi(g)^m = 1_H$. これと$\phi(g^n) = 1_H\phi$は単射だから $g^m = g^n = 1_G$が成り立つ. よってある $k \in \mathbb{N}$ があって $m = k'n$ である. $kk'n = n$ より $k = 1, k' = 1$ より $m = n$ である. すなわち$\phi(g)$ の位数は g の位数と等しい.

解 157 (2.5.4)**.** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ は可換群であり $\mathbb{Z}/4\mathbb{Z}$ なので任意の可換群 G と H は $|G| = |H|$ のとき同型であるとは限らない. 本問は元の位数に注目すると, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ の単位元以外は位数 2 であり, $\mathbb{Z}/4\mathbb{Z}$ は位数 4 の元 $1, 3$ が存在する. もし$\phi : G \to H$ が同型写像なら前問より元の位数を保つので矛盾する.

解 158 (2.5.6)**.** (1) A, B は $GL_2(\mathbb{R})$ で共役である. ある $P \in GL_2(\mathbb{R})$ が存在して $B = PAP^{-1}$を満たすことを言う. 実際に $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$がある. (2) A, B が $SL_2(\mathbb{R})$ で共役であると仮定すると $\exists P \in SL_2(\mathbb{R})(B = PAP^{-1})$ である. $P = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}$とおき $BP = PA$ より $P = \begin{pmatrix} 0 & p_{12} \\ p_{12} & p_{22} \end{pmatrix}$より $\det P = 1$ に矛盾. (3) ある $P \in SL_2(\mathbb{C})$ があって $B = PAP^{-1}$となることを示す. $P = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$に対して $BP = PA$ である.

解 159 (2.5.7)**.** $\phi : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$を次のように定める. $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対し f は単射準同型なので $f(1) \in \mathbb{Z}/n\mathbb{Z}$ は [2.5.3] より位数 n の元である. 即ちある n と互いに素な整数 m が存在して $f(1) = m\ (mod\ n)$ を満たす. これよりϕを$\phi : f \mapsto f(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$で定められる. すると$\phi$は準同型である. なぜなら $f, g \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対して

$$f(1) = m\ (mod\ n),\ \ g(1) = m'\ (mod\ n)$$

とおくと$\phi(fg) = \phi(f)\phi(g)$ が成り立つからである. 実際, (左辺) $= fg(1) = f(m'\ mod\ n) = m'f(1\ mod\ n) = m'm\ (mod\ n)$ で (右辺) $= \phi(f)\phi(g) = f(1)g(1) = mm'\ (mod\ n)$ である. ϕは単射かつ全射であることも示せるから, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$である.
(1) $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$ であり, 上の記号をϕをΦとして転用すると

$$\Phi^{-1} : (\mathbb{Z}/n\mathbb{Z})^\times \ni \bar{k} \mapsto \phi_{\bar{k}} \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

上における説明から, $\phi_{\overline{k}}$は $\mathbb{Z}/n\mathbb{Z}$ の元に対する n と互いに素な$\overline{k}$倍写像である. よって$\phi_{\overline{2}}$または$\phi_{\overline{3}}$または$\phi_{\overline{4}}$を生成元とする巡回群としての $\mathbb{Z}/4\mathbb{Z}$ となる. (3) $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^2$であることを示す. $\phi_k : \mathbb{Z}/8\mathbb{Z} \ni x \mapsto kx \in \mathbb{Z}/8\mathbb{Z}$ は準同型写像である. 巡回群 $\mathbb{Z}/8\mathbb{Z}$ の生成元は $1, 3, 5, 7$ なのでϕ_kが自己同型 $\Leftrightarrow \phi_k \in \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ となるためには$\phi_k(1) = 1, 3, 5, 7$ でなければならない. よって $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) = \{\phi_1, \phi_3, \phi_5, \phi_7\}$ である.

$$(\phi_3)^2(1) = 1 \text{ より} \phi_3 \text{の位数は } 2,\ (\phi_5)^2 = (\phi_7)^2 = 1_{\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})}$$

なので, この位数 4 の自己同型群は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ に同型である. $\overline{k}$を単に k とかいた. (4) も同様.
略解中の注意の補足をすると, $\phi_k \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ より $x \in \mathbb{Z}/n\mathbb{Z}$ に対して$\phi_k(x) = kx$ となる k がある. (なぜなら $\langle x \rangle = \mathbb{Z}/n\mathbb{Z}$ であるから) $G = \mathbb{Z}/n\mathbb{Z}$ は巡回群より可換群なので, [2.5.2] より $\phi_k : x \mapsto x^k \equiv kx$ は準同型である. さらに, 一般には生成元は一意的でないからこの写像は生成元の取り方によらず良定義であることは示す必要があるがこれは明らかである.

注 49 ([3],122 ページ)**.** 互いに素な整数 $n_1, ..., n_r$を用いて $n = n_1 \cdots n_r$のとき, $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \cdots (\mathbb{Z}/n_r\mathbb{Z})^\times$が成り立つ.

参考文献

[1] 森田康夫, 代数概論, 裳華房

[2] 雪江明彦, 代数学 1 群論入門, 日本評論社

[3] 佐藤隆夫, シローの定理, 近代科学社

[4] 堀田良之, 代数入門－群と加群, 裳華房

[5] 佐藤隆夫, 群の表示, 近代科学社

[6] J.S.Milne,Group Theory,https://www.jmilne.org/math/CourseNotes/GT.pdf

[7] Hans Kurzweil,Bernd Stellmacher,The Theory of Finite Groups An Introduction

[8] http://www1.spms.ntu.edu.sg/ frederique/chap1.pdf

[9] 齋藤正彦, 線型代数入門, 東京大学出版会

[10] http://www2.math.kyushu-u.ac.jp/ hara/lectures/07/realnumbers.pdf 微積分学と関連が深い実数の構成に詳しい資料です。