可換な行列と単因子論

@Metachick_2021

2026 年 5 月 7 日

1　証明の準備

【補題 1.1】

R を単位的可換環とする。$M_1, M_2, \ldots, M_m$ および $N_1, N_2, \ldots, N_n$ を R-加群とする。このとき、以下の R-加群としての同型が成立する。

$$\operatorname{Hom}_R\left(\bigoplus_{i=1}^{m} M_i, \bigoplus_{j=1}^{n} N_j\right) \cong \bigoplus_{i=1}^{m}\bigoplus_{j=1}^{n} \operatorname{Hom}_R(M_i, N_j)$$

証明　$p_k \colon \bigoplus_j N_j \to N_k$ を射影、$\iota_k \colon N_k \to \bigoplus_j N_j$ を包含写像とする。まず、以下を示す。

$$\operatorname{Hom}_R\left(M, \bigoplus_{j=1}^{n} N_j\right) \cong \bigoplus_{j=1}^{n} \operatorname{Hom}_R(M, N_j)$$

$F : \operatorname{Hom}_R(M, \bigoplus_j N_j) \to \bigoplus_j \operatorname{Hom}_R(M, N_j)$ を $F(\phi) = (p_1 \circ \phi, p_2 \circ \phi, \ldots, p_n \circ \phi)$ で定めれば、これは R-線形写像である。また、$(f_1, f_2, \ldots, f_n) \in \bigoplus_j \operatorname{Hom}_R(M, N_j)$ が与えられたとき、$G(f_1, \ldots, f_n)(m) = \sum_{j=1}^{n} \iota_j(f_j(m))$ と定義すれば、これが F の逆写像となることが直ちに確認できるから、同型であることがわかる。全く同様にして、

$$\operatorname{Hom}_R\left(\bigoplus_{i=1}^{m} M_i, N\right) \cong \bigoplus_{i=1}^{m} \operatorname{Hom}_R(M_i, N)$$

も従う。以上の議論を組み合わせることで、

$$\operatorname{Hom}_R\left(\bigoplus_{i=1}^{m} M_i, \bigoplus_{j=1}^{n} N_j\right) \cong \bigoplus_{i=1}^{m} \operatorname{Hom}_R\left(M_i, \bigoplus_{j=1}^{n} N_j\right) \cong \bigoplus_{i=1}^{m}\left(\bigoplus_{j=1}^{n} \operatorname{Hom}_R(M_i, N_j)\right)$$

と変形できるから、示したかった同型が得られた。　□

V を n 次元複素ベクトル空間、$A \in M_n(\mathbb{C})$ を線型変換とする。V の基底を $\{e_1, \ldots, e_n\}$ と固定し、多項式の作用を $f(x) \cdot v = f(A)v$ と定義することで、V を $\mathbb{C}[x]$-加群とみなす。また、$\mathbb{C}[x]^n$ を成分が複素係数多項式である n 次元列ベクトル全体のなす自由 $\mathbb{C}[x]$-加群とし、その標準基底を $\{u_1, \ldots, u_n\}$ とする。

【補題 1.2】

$\mathbb{C}[x]$-加群として、以下の同型が成立する。

$$V \cong \mathbb{C}[x]^n/(xE-A)\mathbb{C}[x]^n$$

ここで、$(xE-A)\mathbb{C}[x]^n$ は行列 $xE-A$ の列ベクトルたちが生成する $\mathbb{C}[x]^n$ の部分加群である。

証明　全射 $\pi : \mathbb{C}[x]^n \to V$ を、各標準基底 u_j に対して $\pi(u_j) = e_j$ となるように $\mathbb{C}[x]$-線型に拡張して定義する。以下、$\operatorname{Ker}\pi = \operatorname{Im}(xE-A)$ を示す。

$\operatorname{Im}(xE-A) \subseteq \operatorname{Ker}\pi$ を示そう。行列 $xE-A$ の第 j 列を $\mathbf{c}_j(x)$ とすると、これは $\mathbf{c}_j(x) = xu_j - \sum_{i=1}^n a_{ij}u_i$ と書ける。これを π で送ると、

$$\pi(\mathbf{c}_j(x)) = Ae_j - \sum_{i=1}^n a_{ij}e_i$$

となる。$Ae_j = \sum_{i=1}^n a_{ij}e_i$ であるから、$\pi(\mathbf{c}_j(x)) = \mathbf{0}$ が成り立つ。したがって、$(xE-A)\mathbb{C}[x]^n \subseteq \operatorname{Ker}\pi$ である。

次に、$\operatorname{Ker}\pi \subseteq \operatorname{Im}(xE-A)$ を示す。$\mathbf{f}(x) \in \operatorname{Ker}\pi$ とする。行列 $xE-A$ は x について 1 次であり、その最高次係数は単位行列 E である。E は可換環 $\mathbb{C}[x]$ 上で可逆であるから、除法の原理により、

$$\mathbf{f}(x) = (xE-A)\mathbf{Q}(x) + \mathbf{r}$$

を満たす $\mathbf{Q}(x) \in \mathbb{C}[x]^n$ および複素定数ベクトル $\mathbf{r} \in \mathbb{C}^n$ が一意に存在する。この両辺に π を施すと、

$$\pi(\mathbf{f}(x)) = \mathbf{0} + \pi(\mathbf{r}) = \pi(\mathbf{r})$$

となる。$\mathbf{f}(x) \in \operatorname{Ker}\pi$ より $\pi(\mathbf{r}) = \mathbf{0}$ である。$\mathbf{r}$ は定数ベクトルであるから、$\mathbf{r} = \sum_{j=1}^n r_j u_j$ $(r_j \in \mathbb{C})$ とおくと、

$$\pi(\mathbf{r}) = \sum_{j=1}^n r_j e_j = \mathbf{0}$$

が成り立つ。$\{e_j\}$ は V の基底であり線型独立であるため、すべての r_j は 0 である。すなわち $\mathbf{r} = \mathbf{0}$ となる。ゆえに $\mathbf{f}(x) = (xE-A)\mathbf{Q}(x) \in \operatorname{Im}(xE-A)$ が示された。

最後に、準同型定理により $\mathbb{C}[x]^n/\operatorname{Ker}\pi \cong \operatorname{Im}(\pi) = V$ が成り立ち、結論を得る。 □

【補題 1.3】

$f, g \in \mathbb{C}[x]$ を 0 でない多項式とする。このとき、$\mathbb{C}[x]$-加群として以下の同型が成り立つ。

$$\mathrm{Hom}_{\mathbb{C}[x]}(\mathbb{C}[x]/(f), \mathbb{C}[x]/(g)) \cong \mathbb{C}[x]/(\gcd(f,g))$$

また、この線型空間の $\mathbb{C}$ 上の次元は $\deg(\gcd(f,g))$ である。

証明　$R = \mathbb{C}[x]$ とおき、$d = \gcd(f,g)$ とする。R-加群の準同型 $\phi \in \mathrm{Hom}_R(R/(f), R/(g))$ は、生成元 $\bar{1}$ の行き先 $\phi(\bar{1}) = \bar{a}$ $(a \in R)$ によって完全に決定される。この対応が well-defined であるためには、元の環において $f \cdot 1 \equiv 0 \pmod f$ であることから、

$$f \cdot \bar{a} = \bar{0} \quad \text{in } R/(g)$$

すなわち、$fa \in (g)$ であることが必要十分である。これは $fa = kg$ となる $k \in R$ が存在することを意味する。ここで $f = df_1, g = dg_1$ とおくと、$\gcd(f_1, g_1) = 1$ である。式 $df_1 a = kdg_1$ の両辺を d で割ると $f_1 a = kg_1$ を得る。$\gcd(f_1, g_1) = 1$ より a は g_1 の倍数、すなわち $a \in (g_1)$ でなければならない。逆に、$a \in (g_1)$ のとき、$fa \in (g)$ である。したがって、$\phi(\bar{1})$ として取り得る値の集合は、剰余環 $R/(g)$ 内のイデアル $(g_1)/(g)$ である。

写像 $\Psi\colon \mathrm{Hom}_R(R/(f), R/(g)) \to (g_1)/(g)$ を $\Psi(\phi) = \phi(\bar{1})$ と定めると、これは R-加群の同型となる。さらに、全射準同型 $\psi\colon R \to (g_1)/(g)$ を $\psi(r) = \overline{rg_1}$ で定めると、その核は

$$rg_1 \in (g) \iff rg_1 = m(dg_1) \iff r = md$$

より $\mathrm{Ker}(\psi) = (d)$ である。準同型定理により、

$$\mathrm{Hom}_R(R/(f), R/(g)) \cong (g_1)/(g) \cong R/(d) = R/(\gcd(f,g))$$

が示された。$\mathbb{C}$ 上の次元については、多項式環の剰余環 $R/(d)$ の基底が $\{\bar{1}, \bar{x}, \ldots, \bar{x}^{\deg d - 1}\}$ で与えられることから、$\dim_{\mathbb{C}} R/(d) = \deg d = \deg(\gcd(f,g))$ となる。　□

2　主張とその証明

【命題 2.1】行列の中心化群の次元

V を n 次元複素ベクトル空間とする。$A \in M_n(\mathbb{C})$ の特性行列 $tE - A$ の単因子を $d_1(x), \ldots, d_n(x)$ とする。ただし、各 i について、$d_i \mid d_{i+1}$ かつモニックである。このとき、A と可換な行列全体の成す $\mathbb{C}$ 線型空間 $Z(A)$ の次元は以下で与えられる。

$$\dim_{\mathbb{C}} Z(A) = \sum_{k=1}^{n} (2n - 2k + 1) \deg d_k(x)$$

証明　A と可換な $B \in M_n(\mathbb{C})$ は、$\mathbb{C}[x]$-加群としての自己準同型写像 $\phi \in \mathrm{End}_{\mathbb{C}[x]}(V)$ と一対一に対応する。実際、$\phi(Av) = \phi(x \cdot v) = x \cdot \phi(v) = A\phi(v)$ より $AB = BA$ である。逆に B が A と可換なら、任意の $f(A)$ とも可換であり、ϕ は $\mathbb{C}[x]$-線型となる。したがって、求める次元は $\dim_{\mathbb{C}} \mathrm{End}_{\mathbb{C}[x]}(V)$ に等しい。

補題 2 より $V \cong \mathbb{C}[x]^n / \mathrm{Im}(xE - A)$ である。$xE - A$ を Smith 標準形に変形すると、

$$V \cong \mathbb{C}[x]^n / \mathrm{Im}(\mathrm{diag}(d_1(x), \ldots, d_n(x))) \cong \bigoplus_{i=1}^{n} \mathbb{C}[x]/(d_i(x))$$

となる。補題 1 より、

$$\mathrm{End}_{\mathbb{C}[x]}(V) \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{n} \mathrm{Hom}_{\mathbb{C}[x]} \left(\mathbb{C}[x]/(d_i(x)), \mathbb{C}[x]/(d_j(x))\right)$$

である。補題 3 より、各成分は $\mathbb{C}[x]/(\gcd(d_i, d_j))$ に同型である。$i \leq j$ のとき $d_i \mid d_j$ なので $\gcd(d_i, d_j) = d_{\min\{i,j\}}$ である。この $\mathbb{C}$ 上の次元は $\deg d_{\min\{i,j\}}(x)$ であるから、

$$\dim_{\mathbb{C}} Z(A) = \sum_{i=1}^{n} \sum_{j=1}^{n} \deg d_{\min\{i,j\}}(x)$$

を計算すれば良い。$\min(i, j) = k$ となるペア (i, j) の個数を数えると、これは $2n - 2k + 1$ 個である（主客転倒)。これらを合計して、

$$\dim_{\mathbb{C}} Z(A) = \sum_{k=1}^{n} (2n - 2k + 1) \deg d_k(x)$$

を得る。 $\square$