# 院試に役立つ代数の命題

浦川

2024 年 8 月 2 日

**定義 0.1** とくに断りのない限り $p$ : 素数, $G$ : 群, $R$ : 単位的環, $K$ : 体, $I$ : イデアル

## 1 群論

**命題 1.1** $N$, $H$ は $G$ の正規部分群で $N \cap H = \{1\}$, $NH = G$ を満たす. このとき, $G \cong N \times H$ が成り立つ.

**証明**. $N$, $H$ は $G$ の正規部分群であることより $nhn^{-1}h^{-1} \in N \cap H = \{1\}$ が従うので $hn = nh$ である. すると $f : N \times H \to G : f(n,h) = nh$ が群準同型として well-defined であり, $NH = G$ より全射となる. $N \cap H = \{1\}$ から単射性も従うので $f$ は同型である. □

**命題 1.2** $N$, $H$ は $G$ の部分群で $N \triangleleft G$, $N \cap H = \{1\}$, $NH = G$ を満たす. このとき, $G \cong N \rtimes H$ が成り立つ. ここで $N \rtimes H$ は内部半直積であり, $H \to \mathrm{Aut}(N) : h \mapsto (n \mapsto hnh^{-1})$ である.

**証明**. 内部半直積における積の定め方から, $f : N \times H \to G : f(n,h) = nh$ が群準同型として well-defined であり, $NH = G$ より全射となる. $N \cap H = \{1\}$ から単射性も従うので $f$ は同型である. □

**命題 1.3** (中国剰余定理) $m$, $n$ は正整数であるとする. $(m,n) = 1$ ならば, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

**証明**. $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} : f(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z})$ は群準同型として well-defined であり, $(m,n) = 1$ より単射となる. 両辺の位数が等しいので同型. □

**命題 1.4** (部分群の積) $H$, $N \subset G$: 部分群
$N \triangleleft G \Rightarrow HN \subset G$ は部分群. また $HN = NH$.
$N \triangleleft G$ かつ $H \triangleleft G \Rightarrow NH \triangleleft G$.

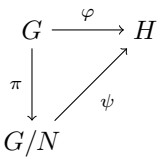
**証明**. $NH$ は空ではなく $N \triangleleft G$ だから, 任意の $hn, h'n' \in NH$ に対して $(hn)(h'n')^{-1} = hnn'^{-1}h'^{-1} = (h(nn'^{-1})h^{-1})(hh'^{-1}) \in NH$. また任意の $h \in H$ に対し $hNh^{-1} = N$ より $hN = Nh$ なので $HN = NH$. さらに $H \triangleleft G$ なら $gHNg^{-1} = gHg^{-1}gNg^{-1} = HN$ なので正規. □

**注意 1.5** 準同型定理は射の一意性まで保証している.

**命題 1.6** (部分群の積に関する準同型定理) $H$, $N \subset G$: 部分群で $N \triangleleft G$. このとき $HN/H \cong N/H \cap N$.

**証明**. $N \triangleleft G$ より前命題から $HN$ は部分群. 自然な射影 $HN \to N/H \cap N$ の核は $H$ なので, 準同型定理より主張を得る. □

**命題 1.7** 下図が可換になるような $\psi : G/N \to H$ が存在 $\Leftrightarrow N \subset \ker \varphi$




**証明**. ($\Rightarrow$) 任意の $n \in N$ は $\varphi(n) = \psi \circ \pi(n) = \psi(1) = 1$.
($\Leftarrow$) $\psi : G/N \to H : \psi(gN) = \varphi(g)$ が well-defined になる. □

**命題 1.8** 指数 2 の部分群は正規部分群.

**証明**. $H \subset G$ を指数 2 の部分群とする. $g \in H$ なら $gHg^{-1} = H$ という等式は明らかである. $g \notin H$ なら $gH \neq H$ なので, $g$ は $G$ の $H$ による左剰余類分解 $G = H \sqcup gH$ を導く. 一方 $Hg \neq H$ でもあるので, 右剰余類分解 $G = H \sqcup Hg$ をも導く. この 2 つの式の比較により $gH = Hg$ を得る. □

**命題 1.9** 群 $G$ の指数 $n$ の正規部分群は $nG := \{g^n \mid g \in G\}$ を含む.

**証明**. 指数 $n$ の正規部分群を $H$ とする. $|G/H| = n$ である. よって任意の $g \in G$ に対して $(gH)^n = H$ となる. これは $g^n \in H$ を意味する. □

**命題 1.10** (Abel 群の場合の指数 $n$ の部分群の求め方) $G$ : Abel 群とする.

1. 前命題のように任意の指数 $n$ の部分群が $nG$ を含むことを示す.
2. $G/nG$ を簡単な群に表示する.
3. $G$ の指数 $n$ の部分群は $G/nG$ の指数 $n$ の部分群と 1 対 1 対応することを示す.
4. $G/nG$ の部分群を全て調べる.

**証明**. 1. は $G$ が Abel なので任意の部分群が正規であることから従う.
2. は有限 Abel 群の基本定理や中国剰余定理などを使うとよい.
3. は準同型定理の部分群の対応から, $G/nG$ の部分群と $G$ の $nG$ を含む部分群は 1 対 1 対応する. すると第三同型定理より, $H \subset G$ が指数 $n$ の部分群 $\Leftrightarrow n = |G/H| = |(G/nG)/(H/nG)| = (G/nG)/\pi(H)$
$\Leftrightarrow \pi(H) \subset G/nG$ が指数 $n$ の部分群
となる.
4. は位数で絞り込んでいくと良い. □

**命題 1.11** 共役類は同値類

**証明**. 略 □

**命題 1.12** (作用に関する Lagrange の定理) $G \curvearrowright X$, $x \in X$ とする. $G_x$ を $x$ の安定化群, $Gx$ を $x$ の軌道とする. このとき, $(G : G_x) = |Gx|$, $|G| < \infty$ なら $|G|/|G_x| = |Gx|$. とくにこの作用が $G$ の部分群の集合に対する共役作用ならば, (部分群 $H$ の共役の個数)$= (G : N_G(H))$, $|G| < \infty$ ならこの右辺は $|G|/|N_G(H)$ である.

**証明**. $G_x \subset G$ は部分群であり, $G/G_x \to Gx : gG_x \mapsto gx$ は全単射であるから Lagrange の定理より主張を得る. 後半は前半の特別な場合. □

**命題 1.13** (類等式の性質) 類等式 $|G| = \sum |C(x)|$ の右辺について次が成り立つ.

1. 少なくとも 1 回 1 が現れる.
2. 1 が現れる回数は $|Z(G)|$ に等しい.
3. 現れる数は全て $|G|$ の約数である.

**証明**. 中心の元はそれ自身の 1 元集合で 1 つの共役類をなすことから 2. を得る. 中心は単位元を含むことから 1. を得る. 3. は前命題より従う. □

**命題 1.14** $G/Z(G)$ が巡回群ならば $G$ は Abel 群.

**証明**. $G/Z(G) = \langle xZ(G) \rangle$ とすれば, $G$ の任意の元 $g$ はある $h \in Z(G)$ を用いて $g = x^n h$ と表せる. $x^n h$ という形の元は $h \in Z(G)$ より可換である. □

**命題 1.15** $G$ の内部自己同型群を $\mathrm{Inn}(G) := \{\phi_g : h \mapsto ghg^{-1}\}$ で表す. $G/Z(G) \cong \mathrm{Inn}(G)$ である.

**証明**. $G \to \mathrm{Inn}(G)$ を $g \mapsto \phi_g$ で定めると, これは全射準同型であり, その核は $Z(G)$ である. □

**命題 1.16** (可解性) $G$: 可解 $\overset{def}{\Leftrightarrow}$ Abel 正規列が有限 $\Leftrightarrow$ $D_n(G) = \{1\}$ なる $n$ が存在する.
ここで Abel 正規列とは $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ s.t. $G_{i+1} \triangleleft G_i$ かつ $G_i/G_{i+1}$ : Abel であり, また $D_n(G) := [D_{n-1}(G), D_{n-1}(G)]$.

**証明**. $D_n(G)$ の列は Abel 正規列になることから従う. □

**命題 1.17** (可解性) $G$:Abel なら可解

**証明**. $G \supset \{1\}$ は Abel 正規列. □

**命題 1.18** $N \triangleleft G$ とするとき, $G$: 可解 $\Leftrightarrow$ $N$, $G/N$: 可解

**証明**. $\pi : G \to G/N$ を自然な射影とする. $N$ の Abel 正規列を $N = N_0 \supset N_1 \supset \cdots \supset N_m = \{1\}$, $G/N$ の Abel 正規列を $G/N = (G/N)_0 \supset (G/N)_1 \supset \cdots \supset (G/N)_n = \{1\}$ としたとき, $G = \pi^{-1}((G/N)_0) \supset \pi^{-1}((G/N)_1) \supset \cdots \supset \pi^{-1}((G/N)_n) = N = N_0 \supset N_1 \supset \cdots \supset N_m = \{1\}$ は $G$ の Abel 正規列となる. □

**命題 1.19** (冪零性) $G$: 冪零群 $\overset{def}{\Leftrightarrow}$ 中心列が有限 $\Leftrightarrow Z_n(G) = \{1\}$ なる $n$ が存在する.
ここで中心列とは $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ s.t. $G_{i+1} \triangleleft G$ かつ $G_i/G_{i+1} \subset Z(G/G_{i+1})$ であり, また $Z_n(G) := [G, Z_{n-1}(G)]$

**証明**. $Z_n(G)$ の列は中心列になることから従う. □

**注意 1.20** $D_n(G) \subset Z_n(G)$ なので冪零なら可解である. また Abel 群は $Z_1(G) = [G, G] = \{1\}$ なので冪零 (よって可解) である.

**命題 1.21** $p$ 群の中心は非自明.

**証明**. 背理法. 自明であるとすると類等式が $p^n = |G| = 1 + (p$ の倍数) となるので矛盾. □

**命題 1.22** $p$ 群は冪零

**証明**. $|G| = p^n$ とし, $n$ に関する帰納法. $n = 0$ のときはあきらか. $n \geq 1$ とする. 前命題より中心は非自明だから $|G/Z(G)| < |G|$ である. よって帰納法の仮定より $G/Z(G)$ の中心列は停留する. これを $G/Z(G) = G'_0 \supset G'_1 \supset \cdots \supset G'_n = \{1\}$ とする. $\pi : G \to G/Z(G)$ を自然な射影として $G_i = \pi^{-1}(G'_i)$, および $G_{n+1} = \{1\}$ とすれば $G_i$ は中心列をなす. □

**命題 1.23** (位数 $p^2$) 位数 $p^2$ の群は Abel 群

**証明**. $G = Z(G)$ を示す. $p$ 群の中心は非自明なのでその位数は $p$ か $p^2$. $|Z(G)| = p$ とすると $G/Z(G)$ が位数 $p$, 従って巡回群となるので 1.14 より $G$ が Abel となり矛盾. □

**命題 1.24** (位数 $pq$) 位数 $pq$ ($p < q$ はともに素数) の群は単純でない. とくに $p \not\equiv 1 \bmod q$ なら巡回群である.

**証明**. Sylow$p$ 部分群 $H \cong \mathbb{Z}/p\mathbb{Z}$ と Sylow$q$ 部分群 $K \cong \mathbb{Z}/q\mathbb{Z}$ が存在して, Sylow$q$ 部分群は共役の個数が 1 しかありえないため正規である. よって単純でない. $p \not\equiv 1 \bmod q$ なら Sylow$p$ 部分群も正規となり, 位数の比

較から $H \cap K = \{1\}$ および $G = HK$ を得るので 1.1 および中国剰余定理から $G \cong H \times K \cong \mathbb{Z}/pq\mathbb{Z}$, とくに $G$ は巡回群. □

**命題 1.25** (位数 $p^2q$) 位数 $p^2q$ の群の Sylow$p$ 部分群, Sylow$q$ 部分群の少なくともどちらか一方は正規. よってとくに単純でない.

**証明**. $p > q$ ならば Sylow の定理より Sylow$p$ 部分群が正規である. $q > p$ のとき, Sylow$q$ 部分群が正規でないならば, Sylow$p$ 部分群が正規となることを示す. Sylow$p$ 部分群が正規でないときその共役は $q$ 個存在する. □

**命題 1.26** (位数 60 未満) 位数 $n$ $(n < 60)$ の群は単純でない.

**証明**. 素数位数と平方位数の群は可換なので考えなくてよい. また $p$ 群は中心 (正規部分群) が非自明なので単純でない. 前に述べた命題より位数 $pq$, $p^2q$ の群は単純でない. すると残るは位数 24, 30, 36, 40, 42, 48, 54, 56 の群である. □

**命題 1.27** $G \setminus Z(G)$ は 1 つの共役類.

**証明**. 任意の $g \in G$ に対して $g(G \setminus Z(G))g^{-1} = G \setminus Z(G)$ を示せばよい. $x \in G \setminus Z(G)$, $g \in G$ に対し $y := gxg^{-1} \in Z(G)$ なら $gx = yg = gy$ なので $G \setminus Z(G) \ni x = y \in Z(G)$ となり矛盾. よって任意の $g \in G$ に対して $g(G \setminus Z(G))g^{-1} \subset G \setminus Z(G)$. 任意の $g \in G$ に対して $gG = Gg = G$ なので $G$ による $G$ への共役作用は推移的である. よってとくに $x \in G \setminus Z(G)$ に対し, ある $y$, $g \in G$ があり $x = gyg^{-1}$ である. ここでもし $y \in Z(G)$ なら再び $G \setminus Z(G) \ni x = y \in Z(G)$ となり矛盾. よって $G$ の $G \setminus Z(G)$ に対する作用は推移的である. よって $G \setminus Z(G)$ は 1 つの共役類をなす. □

**命題 1.28** (剰余類に対する置換表現の核) $H \subset G$ : 指数 $n$ の部分群, $X = \{gH \mid g \in G\}$ を $H$ による剰余類とする. $X$ に対して左から $g$ の元をかけることによる作用 $G \curvearrowright X$ を考え, その置換表現を $\varphi : G \to S_n$ とする. このとき, $\ker\varphi = \cap_{g\in G} gHg^{-1}$ である. よってとくに, $\ker\varphi \subset H$.

**証明**.

$$\begin{aligned} h \in \ker\varphi &\Leftrightarrow \forall g \in G, hgH = gH \\ &\Leftrightarrow \forall g \in G, g^{-1}hgH = H \\ &\Leftrightarrow \forall g \in G, g^{-1}hg \in H \\ &\Leftrightarrow \forall g \in G, h \in gHg^{-1} \\ &\Leftrightarrow \forall g \in \cap_{g\in G} gHg^{-1}. \end{aligned}$$

□

**注意 1.29** このことは, 指数有限の部分群があればそれと同じかより小さな正規部分群 ($\ker\varphi$) が存在することを主張している. それは自明な正規部分群かもしれないが, 指数 $n$ を十分小さくとれば $n! < |G|$ となりうるので, $\varphi : G \to S_n$ が単射でなくなり, $\ker\varphi$ が自明でなくなることがある.

**命題 1.30** (指数最小の部分群は正規) $G$：有限群, $H \subset G$：指数最小の部分群なら, $H \triangleleft G$.

**証明**. $H$ がある準同型の核となることを示す. 指数の最小性から, 指数は $|G|$ の最小の素因数 $p$ である. $X$ に対して左から $g$ の元をかけることによる作用 $G \curvearrowright X$ を考え, その置換表現を $\varphi : G \to S_p$ とする. このとき前命題より, $\ker\varphi = \cap_{g\in G} gHg^{-1}$ である. よってとくに, $\ker\varphi \subset H$.

ところで, $\mathrm{Im}\varphi$ は $S_p$ の部分群であることより $|\mathrm{Im}\varphi|$ は $|S_p| = p!$ の約数である. 一方, 準同型定理より $|\mathrm{Im}\varphi|$ は $|G|$ の約数である. これらと $p$ の最小性から, $|\mathrm{Im}\varphi| = 1, p$ である. とくに, $|\mathrm{Im}\varphi| \leq p$ である. すると上の包含関係ともあわせて

$$p \geq \mathrm{Im}\varphi = \frac{|G|}{|\ker\varphi|} \geq \frac{|G|}{|H|} = p$$

を得る. よって $\ker\varphi = H$ である. □

**注意 1.31** 単純群の定義は「非自明な正規部分群を持たない」であったが, 有限単純群の場合, 前命題から「非自明な部分群を持たない」ことと同値であることが分かる. ゆえに有限単純群はかなり強い意味で「単純」である. 実際, 有限群が非自明な部分群をもてば, そのうち指数最小の部分群は前命題より正規となる. よって有限単純群は非自明な部分群を持ちえない.

なお有限性の仮定を外すと指数が素数であることが言えないので, 証明中 $|\mathrm{Im}\varphi| \leq p$ が一般には成り立たなくなる.

# 2 加群論

**命題 2.1** (可換環上の有限階数自由加群における Cayley-Hamilton の定理) $N = (a_{ij}) \in M_n(R)$, $p_N(x) = \det(xI_n - N) \in R[x]$ とする. このとき, $p_N(N) = 0$ が成り立つ.

**証明**. $N$ を $R^n$ の加群準同型 $R^n \to R^n$ とみなす. $Ne_j = \sum_{i=1}^n a_{ij}e_i$ である.
$R'[N] \subset \mathrm{End}R^n$ を $I_n$ のスカラー倍と $N$ で生成される可換部分環とする. $R'[N]$ の $\mathrm{End}R^n$ への作用を, $Nx$ は通常の積, また $\lambda \in R$ については $\lambda x = \lambda I_n x$ で定めることにより, $R'[N]$ の $\mathrm{End}R^n$ への作用として $Ne_j = \sum_{i=1}^n a_{ij}e_i$ をえる. よって $0 = \sum_{i=1}^n (N\delta_{ij} - a_{ij})e_i \cdots (1)$ となる. $\Delta = (N\delta_{ij} - a_{ij})$ とすると, $\Delta$ は $R'[N]$ の元を成分に持つ行列とみなせる.
ここで $R[x] \to R'[N]$ ; $x \mapsto N$ は準同型である. この準同型により $R[x] \ni p_N(x) = \det(xI_n - N) \mapsto \det(N\delta_{ij} - a_{ij}) = \det\Delta$ である. よって $\det\Delta = 0$ ならば $p_N(N) = 0$ が成り立つことになる. $\det\Delta = 0$ を, 任意の $k$ に対して $(\det\Delta)e_k = 0$ が成り立つことを示すことによって証明する.
$\Delta' = (b_{ij})$ を $\Delta$ の余因子行列とする. $\Delta'\Delta = \Delta\Delta' = (\det\Delta)I_n$ である. これより, (1) を $b_{jk}$ にかけて $j$ につ

いて和を取ると,

$$\begin{aligned}0 &= \sum_{j=1}^{n} b_{jk} \sum_{i=1}^{n} (N\delta_{ij} - a_{ij})e_i \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} (N\delta_{ij} - a_{ij})b_{jk}e_i \\ &= \sum_{i=1}^{n} ((\det \Delta)\delta_{ik})e_i \\ &= (\det \Delta)e_k\end{aligned}$$

となるため, 主張を得る. □

**命題 2.2** $M$ : $R$ 加群, $v = {}^t(u_1, \ldots, u_n) \in M^n$, $T \in M_n(R)$ とする. もし $Tv = 0$ なら, 任意の $i$ で $(\det T)u_i = 0$ である.

**証明**. 2.1 より, 固有多項式 $f(x) = \det(xI_n - T)$ について $f(x)$ は $M^n$ 上で 0 である. これと仮定を合わせ

$$\begin{aligned}0 &= f(T)(v) \\ &= T^n v - (\mathrm{tr}T)T^{n-1}(v) + \cdots + (-1)^n(\det T)v \\ &= (-1)^n(\det T)v\end{aligned}$$

である. よって $(\det T)v = 0$. これは任意の $i$ で $(\det T)u_i = 0$ であることを意味する. □

**命題 2.3** $B$ : 可換環, $A \subset B$ : 部分環とする. $B$ が $A$ 加群として有限生成なら, $B$ は $A$ 上整である.

**証明**. 任意に $b \in B$ をとる. $B$ の $A$ 上の生成系 $(1 =)e_1, e_2, \ldots, e_n$ を 1 つ固定する. $be_i = \sum_{j=1}^{n} a_{ij}e_j$ であるとすると, $0 = \sum_{j=0}^{n}(b\delta_{ij} - a_{ij})e_j$ である. $\cdots(1)$
$A = (a_{ij})$, $B = bI_n - A = (b_{ij})$, $v = {}^t(e_1, \ldots, e_n) \in B^n$ とおく. また, $B$ の余因子行列を $B' = (b'_{ij})$ とおく. すると $BB' = B'B = (\det(bI_n - A))I_n$ である. $\cdots(2)$
(1) より $Bv = 0$ なので, $B'B$ を $v$ にかけたときの第一成分は 0. 一方 (2) よりこの第一成分は $\det(bI_n - A)e_1 = \det(bI_n - A)$ である. よって $\det(bI_n - A) = 0$ である. 左辺は $b$ についての monic な多項式なので主張を得る. □

# 3 環論

**命題 3.1** (中国剰余定理) 可換環 $R$ の $n$ 個のイデアル $I$, $J$ が $I + J = R$ を満たすとする.

1. $I \cap J = IJ$
2. $R/(I \cap J) \cong R/I \oplus R/J$

**証明**. (1) $IJ \subset I \cap J$ は明らか. 逆は $1 = a + b$ なる $a \in I$, $b \in J$ があることを用いて任意の $r \in I \cap J$ に対し $r = ar + br$ とすればよい.
(2) $f : R \to R/I \oplus R/J : r \mapsto (r + I, r + J)$ とするとこれは準同型. 全射性は $bx + ay \mapsto (x + I, y + J)$ より従う. $\ker f = I \cap J$ より準同型定理から主張を得る. □

**注意 3.2** 2 個以上のイデアルに対して使う場合は, どの 2 つも互いに素なイデアルであることが適用の条件になる.

**命題 3.3** $R$ : PID, $x$, $y \in R$ の最大公約元を $d$ とする. このとき, ある $a$, $b \in R$ があり $ax + by = d$ である. とくに $x$, $y$ が互いに素なら, $ax + by = 1$ となる $a$, $b \in R$ が存在する.

**証明**. 一般の PID なのである $z \in R$ があり $(x, y) = (z)$. $x$, $y \in (z)$ なので $z$ は $x$, $y$ の公約元. $z \in (x, y)$ より $ax + by = z$ なる $a$, $b \in R$ が存在するため, $z'$ が $x$, $y$ の公約元なら $z'$ は $z$ の約元である. ゆえに $z = d$. □

**命題 3.4** (行列環の両側イデアル) $R$ : 可換環, $M_n(R)$ : $n$ 次正方行列環とする. $R$ : 体のとき, $M_n(R)$ の任意の両側イデアルは自明, すなわち $M_n(R)$ は単純環. $R = \mathbb{Z}$ のとき, $M_n(\mathbb{Z})$ の任意の両側イデアル $I$ はある正整数 $d$ があり $M_n(d\mathbb{Z})$ をふくむ. とくに $M_n(\mathbb{Z})/I$ は有限環.

**証明**. $E_{ij} \in M_n(R)$ を $(i, j)$ 成分が 1 でそれ以外は 0 の行列とする. 一般に, $A \in M_n(R)$ に対して $E_{is}AE_{tj}$ は $(i, j)$ 成分が $A$ の $(s, t)$ 成分に等しく, それ以外は 0 であるような行列である. $0 \neq I \subset M_n(R)$ を両側イデアルとすると, ある成分 $(s, t)$ が $d \neq 0$ であるような行列 $A \in I$ が取れる. 両側イデアルなので, 任意の $(i, j)$ に対して $dE_{ij} = E_{is}AE_{tj} \in I$ である.
ここでもし $R$ が体なら, $E_{ij} = d^{-1}dE_{ij} = d^{-1}E_{is}AE_{tj} \in I$ である. 任意の行列は $E_{ij}$ の一次結合なので, これより $I$ は任意の行列を含む. 以上より $R$ が体なら 0 でない両側イデアルは $M_n(R)$ に一致する. すなわち体上の行列環の任意の両側イデアルは自明である.
一方, $R = \mathbb{Z}$ ならば $dE_{ij} \in I$ より $M_n(d\mathbb{Z}) \subset I$ である. よって $M_n(\mathbb{Z})/I$ の位数は $M_n(\mathbb{Z})/M_n(d\mathbb{Z}) \cong M_n(\mathbb{Z}/d\mathbb{Z})$ の位数より小さい. とくに有限環. □

**命題 3.5** (素イデアルの上昇定理) $A \subset B$ : 部分環, $B$ は $A$ 上整であるとする. このとき, $I \subset A$ : 素イデアルなら, $J \subset B$ : 素イデアルがあり, $A \cap J = I$ となる.

**証明**. むずい □

**命題 3.6** (環の自己同型群の求め方の例) $\mathrm{Aut}(R)$ を求める手順の例：

1. $R$ を多項式環またはその剰余環として表す.
2. 元を分かりやすい形に表示する.
3. $\mathrm{Aut}(R)$ の元を任意に 1 つ取り, 変数の行先を決定する.
4. 必要があれば $R$ の可逆元を求めたり多項式環をベクトル空間とみなして一次独立性などを用いて自己同型の形を絞り込む.

**命題 3.7** (Eisenstein の既約判定法) $A$：UFD とする. $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$ に対し, ある素元 $p$ が存在して $p \nmid a_0$, $p \mid a_1, \ldots, a_n$, $p^2 \nmid a_n$ なら, $f$ は既約である.

**証明**. 背理法. $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$, $h(x) = c_0x^{n-m} + c_1x^{n-m-1} + \cdots + c_{n-m-1}$ により $f(x) = g(x)h(x)$ であったとする. $a_n = b_mc_{n-m}$ だが, $p^2 \nmid a_n$ よりどちらか一方のみが $p$ の倍元. $b_m$ が $p$ の倍元としても一般性を失わない. $a_{n-1} = b_{m-1}c_{n-m} + b_mc_{n-m-1}$ であるが, 仮定と $c_{n-m}$ が $p$ の倍元ではなく $b_m$ が $p$ の倍元であることから $b_{m-1}$ が $p$ の倍元である. これを続けていくことにより, $b_0$ まで $p$ の倍元となって $p \nmid a_0 (= b_0c_0)$ に矛盾. □

**注意 3.8** 上記の証明では示せていないが, 一般に Eisenstein の既約判定法ではその商体上での既約性まで言える.

**命題 3.9** $K[x]$：体上の多項式環とする. 2 次式 $f(x) \in K[x]$ が生成する単項イデアル $(f(x))$ による剰余環 $K[x]/(f(x))$ について, 以下が成り立つ:

$$K[x]/(f(x)) = \begin{cases} K[x]/(x^2) & (f \text{ が重根を持つとき}) \\ K \times K & (f \text{ が相異なる 2 つの根を持つとき}) \\ K[\alpha] = K(\alpha) & (f \text{ が既約であるとき.} \alpha \text{は代数閉包上での根}) \end{cases}$$

**証明**. $f$ が既約なときは 4.10 より.

$K$ 上で $f(x) = (x-a)(x-b)$ と分解されるとき, $a \neq b$ なら $(x-a) - (x-b) = b - a \in (K[x])^\times$ よりイデアルとして $(x-a) + (x-b) = K[x]$ であるから, 中国剰余定理及び $x \mapsto a, b$ とする準同型によって

$$K[x]/(f(x)) \cong K[x]/(x-a) \times K[x]/(x-b) \cong K \times K$$

となる.

$a = b$ なら, 代入写像 $K[x] \to K[x]/(x^2) : x \mapsto x + a$ の核が $((x-a)^2) = (f(x))$ であることより従う. □

**注意 3.10** 上の命題は $f$ が $n$ 次式のときも既約分解を適切に行うことで同様なことが成り立つ.

**命題 3.11** (位数 $n$ の環の分類における基本的な手法) $R$ は位数 $n$ の環とする.
まず $\mathbb{Z}$ からの自然な環準同型 $\mathbb{Z} \to R : m \mapsto m1_R$ の核を考察する. 準同型定理よりその核の位数 $k$ は $n$ の約数になる.
$k = n$ なら位数の比較によりただちに $\mathbb{Z}/n\mathbb{Z} \cong R$ が従う.
そうでないときも, この準同型によって $R$ を自然に $\mathbb{Z}/k\mathbb{Z}$-代数とみなせるので, 加群としての議論が可能である. とくに $k$ が素数ならばベクトル空間としての議論が可能である.

# 4 体論

**注意 4.1** 体の 2 つの元が共役とは, 最小多項式を共有することである.

**命題 4.2** 体からの準同型は単射.

**証明**. $f$ を体からの準同型, $f(x) = 0$ とするとき, もし $x \neq 0$ なら $x^{-1}$ が存在するので $1 = f(1) = f(x^{-1}x) = f(x^{-1})f(x) = 0$ となり矛盾. □

**命題 4.3** 有限体の乗法群は巡回群.

**証明**. 有限体の乗法群 $G$ は有限 Abel 群なので, 有限 Abel 群の基本定理より $G \cong \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_n\mathbb{Z}$, ただし $e_i \mid e_{i+1}$ である. $n = 1$ を示せばよい. $x^{e_1} = 1$ となる元 $x$ は, 右辺では $\mathbb{Z}/e_1\mathbb{Z} \times (e_2/e_1)\mathbb{Z}/e_2\mathbb{Z} \times \cdots \times (e_n/e_1)\mathbb{Z}/e_n\mathbb{Z}$ に属す元全てである. これは $e_1(e_2/(e_2/e_1)) \cdots (e_n/(e_n/e_1)) = e_1^{2n-1}$ 個存在する. しかし $x^{e_1} = 1$ となる元は高々 $e_1$ 個しかないため, $n = 1$ である. □

**命題 4.4** (Artin の定理, あるいは Dedekind の定理) $\sigma_i : G \to K^\times$ $(i = 1, \ldots, n)$ は相異なる $n$ 個の群準同型とする. このとき, $\sigma_i, \ldots, \sigma_n$ は一次独立である.

**証明**. $n$ にかんする帰納法.
$n = 1$ のときは $a_1\sigma_1 = 0$ なら $a_1 = a_1\sigma_1(1) = 0$ よりたしかに一次独立である.
$n > 1$ とし, $n - 1$ まで一次独立と仮定する. $\sum_{i=1}^{n} a_i\sigma_i = 0$ とする. 任意の $g \in G$ に対し

$$a_1\sigma_1(g) + \cdots + a_n\sigma_n(g) = 0 \cdots (1)$$

である. $a_n = 0$ なら帰納法の仮定より直ちに主張が従う. ここから背理法を用いる. $a_n \neq 0$ と仮定する. すると適切にスカラー倍すればよいので $a_n = 1$ と仮定してよい. $\sigma_{n-1} \neq \sigma_n$ よりある $h \in G$ が存在して $\sigma_{n-1}(h) \neq \sigma_n(h)$ である. (1) に $hg$ を代入したものは

$$a_1\sigma_1(h)\sigma_1(g) + \cdots + a_{n-1}\sigma_{n-1}(h)\sigma_{n-1}(g) + \sigma_n(h)\sigma_n(g) = 0$$

であるが, この両辺を $\sigma_n(h)$ で割ることで

$$a_1\frac{\sigma_1(h)}{\sigma_n(h)}\sigma_1(g) + \cdots + a_{n-1}\frac{\sigma_{n-1}(h)}{\sigma_n(h)}\sigma_{n-1}(g) + \sigma_n(g) = 0$$

をえる. ここに (1) を代入することで

$$a_1\left(\frac{\sigma_1(h)}{\sigma_n(h)}-1\right)\sigma_1(g)+\cdots+a_{n-1}\left(\frac{\sigma_{n-1}(h)}{\sigma_n(h)}-1\right)\sigma_{n-1}(g)=0$$

を得る. $\frac{\sigma_{n-1}(h)}{\sigma_n(h)}-1\neq 0$ だから, これは非自明な $n-1$ 個の $\sigma$ の線形関係であり, 従って帰納法の仮定から $a_1=\cdots=a_{n-1}=0$ である. よって $a_n\sigma_n=0$ を得るが, 1 を代入することで $a_n=0$ となり, 背理法の仮定に矛盾. よって示された. □

**命題 4.5** $L/K$ : 体の拡大, $f(x)\in K[x]$ : 既約かつ monic な多項式で $\alpha\in L$, $f(\alpha)=0$ とする. このとき, $f(x)$ は $\alpha$ の最小多項式である.

**証明**. $\alpha$ を根に持ち, かつその次数が $\deg f$ 以下の monic な多項式が存在したとする. このうち次数が最小のものを取り, それを $g\in K[x]$ とする. 仮定より $f$ は既約なので, $f=g$ であるか, $f$ を $g$ で割ったとき余りが生じる. 後者の場合, $f(\alpha)=g(\alpha)=0$ なので, この余りもまた $\alpha$ を根に持つ多項式である. この余りをその最高次の係数でわることで, $g$ より次数が小さな $\alpha$ を根に持つ monic な多項式が得られる. しかしそれは $g$ の取り方に矛盾する. よって $f=g$ しかありえない. これは $f$ の次数の最小性を意味する. □

**命題 4.6** 標数 0 の体, および有限体の任意の代数拡大は分離拡大, すなわち完全体である. **よって, このような体の拡大が** Galois **拡大かどうかを判定する場合には正規性の確認だけを行えばよい**.

**証明**. □

**命題 4.7** (分離拡大の推移性) $L/M/K$ がいずれも代数拡大であるとき, 次は同値:

1. $L/K$ : 分離拡大
2. $L/M$, $M/K$ : 分離拡大

**証明**. □

**注意 4.8** 分離性は推移するが, 正規性は推移しないので Galois 拡大は推移しない.
例えば, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ はいずれも Galois 拡大だが, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は Galois 拡大ではない.

**命題 4.9** $f$ は $K$ 上の多項式であるとする. $f$ の最小分解体を $L$ とするとき, $L/K$ は正規拡大. **よって, 正規性をいうためには最小分解体であることを示せばよい**.

**証明**. $f$ を既約多項式の積で書くと, それぞれの既約因子は最小多項式である. $f$ の根が全て $L$ に入っているため, 各既約因子たる最小多項式も $L$ 上で 1 次式の積に分解する. □

**命題 4.10** $L/K$ は代数拡大で, $\alpha \in L$ の最小多項式を $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ とする. このとき, $\beta \in L$ が $f(x)$ の根なら, 次が成り立つ:

1. $K(\beta) \cong K[\beta] \cong K[x]/(f(x))$
2. $\{1, \alpha, \ldots, \alpha^{n-1}\}$ は $K(a)$ の $K$ の基底である. **よってとくに, 単拡大の拡大次数はその生成元の最小多項式の次数に等しい**.

**証明**. □

**命題 4.11** $L/K$ : Galois 拡大, $\alpha, \beta \in L$ : 共役とする.

1. 任意の $\mathrm{Gal}(L/K)$ の元は $L$ の $K$ 上の生成元を生成元に写す.
2. $\sigma(\alpha) = \beta$ となるような $\sigma \in \mathrm{Gal}(L/K)$ が存在する.

**証明**. □

**命題 4.12** 有限体 $\mathbb{F}_q$ から有限体 $\mathbb{F}_{q^n}$ への拡大は巡回拡大で, その Galois 群は $\mathrm{Frob}_q$ で生成される.

**証明**. □

**命題 4.13** $\zeta$ を 1 の原始 $n$ 乗根とする. 円分体 ($n$ 分体) $\mathbb{Q}(\zeta)$ について, $\mathbb{Q}(\zeta)/\mathbb{Q}$ は Galois 拡大であり, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ である.

**証明**. □

**命題 4.14** $\zeta_n$ で 1 の原始 $n$ 乗根を表すことにし, 正整数 $n$, $m$ は $\mathrm{GCD}(n, m) = 1$ であるとする. このとき, 次が成り立つ:

1. $\mathbb{Q}(\zeta_{nm}) = \mathbb{Q}(\zeta_n, \zeta_m)$, $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$
2. $\mathrm{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q})$

**証明**. □

**命題 4.15** (Galois 拡大の推進定理) $L/K$ : 体の拡大, $M$, $N$ : 中間体, $L = MN$, $M \cap N = K$ なら, 次が成り立つ :

1. $M/K$ が有限次 Galois 拡大なら $L/N$ も有限次 Galois 拡大で $\mathrm{Gal}(L/N) \cong \mathrm{Gal}(M/K)$ である.
2. $M/K$, $N/K$ が有限次 Galois 拡大なら $L/K$ も有限次 Galois 拡大で $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$ である.

**証明.** □

**命題 4.16** (中間体を求める手順) $L/K$ : 体の拡大, この中間体を求める手順の例 :

1. $L/K$ が Galois 拡大かどうかを調べる. もし Galois 拡大でなければここでの方法が使えないので別の方法を取る.
   (a) $K$ が標数 0 か有限体なら, 4.6 より分離性が従う. そうでなければ定義通り任意の元の最小多項式が分離多項式であることを示すか, 4.7 を用いて分離拡大を繰り返して得られる拡大であることを示す.
   (b) 正規性は 4.9 より生成元の最小多項式を求め, それ (の積) の最小分解体になっていることを示せばよい. なお最小多項式であることを示すためには 4.5 より得られた式が既約かつ monic であることを示せばよく, 既約性は Eisenstein の判定法 (3.7) を用いればよい.
2. $L$ の $K$ 上の生成元を求める. 可能な限り生成元は簡単なものに取り換えておく.
3. あとで Galois 群を決定するときのために, 拡大次数を求めておく (拡大次数と Galois 群の位数は一致する). 4.10 より, 拡大次数は単拡大ならその生成元の最小多項式の次数に等しいので最小多項式を求めたら良い. たとえば $L = K(a, b)$ などであれば $[L : K] = [K(a, b) : K] = [K(a, b) : K(a)][K(a) : K]$ であることに注意しなければならないから, この場合だと $b$ については $K(a)$ 上の最小多項式を求めておくべきである. 既約性の証明は Eisenstein の判定法が有効.
4. Galois 群を求める. Galois 群の元は生成元の行先で決まるため, 生成元の行先を全て列挙してしまえば原理的には終わる. しかし群構造が知りたいので, Galois 群の生成元がどのような写像になるかに注目するとスジが良い. このとき, 共役でない元は互いに移り合わない (最小多項式を共有する元どうしが移りあう) ことに注意.
5. 4 での生成元などの考察や 3 で求めた位数の考察などから, 同型になりそうな群を引っ張ってきて同型を構成する.
6. 5 で Galois 群と同型になった群の部分群を全て求める. Sylow の定理が役に立つこともある.
7. その部分群による不変体を調べる. たとえば部分群 $H$ が $H = \langle\sigma\rangle$ であって $\sigma$ は生成元 $(a, b)$ を $(a, -b)$ に移すのであれば, $a$ を不変にするということなのでその不変体は $K(a)$ である. $(a, b)$ を $(-a, -b)$ に移すのであれば, 不変体は符号の影響を受けない $K(ab)$ や $K(a/b)$ であることが期待される. 中間体は例えば $K(a, b)/K$ なら $K(a \pm b)$, $K(ab)$, $K(a/b)$, $K(a)$, $K(b)$, $K(a \pm b)$, $K(ab, a/b)$ で大体は尽くされる.
8. このようにして全ての不変体を決定すれば Galois の基本定理よりそれが $L/K$ の全ての中間体である.

## 参考文献


[1] 雪江明彦　代数学 1　日本評論社　2010
[2] 雪江明彦　代数学 2　日本評論社　2010
[3] 雪江明彦　代数学 3　日本評論社　2010
[4] 永田雅宜　復刻版　大学院への代数学演習　現代数学社　2021