香川セミナー

– 対称行列のペアの類数について –

中川 仁

2001年12月8日

目標 整数係数 n 次対称行列のペアの類数に関する J. Morales の結果を解説する．

目 次

1 n 次対称行列のペア

$x = (x_1, x_2)$ を整数係数の n 次対称行列のペアとする．$\Gamma = GL_n(\mathbb{Z})$ とおく．二つのペア $x = (x_1, x_2)$ と $y = (y_1, y_2)$ に対して，$\gamma \in \Gamma$ で，$y_1 = \gamma x_1 {}^t\gamma$ かつ $y_2 = \gamma x_2 {}^t\gamma$ を満たすものが存在するとき，x と y は**同値**であるという．

$x = (x_1, x_2)$ に対して，u, v を変数とする 2 元 n 次形式 $\Phi_x(u, v)$ を

$$\Phi_x(u, v) = \det(ux_1 + vx_2)$$

によって定義する．Φ_x は整数係数の 2 元 n 次形式である．x と y が同値ならば，明らかに，$\Phi_x = \Phi_y$ である．そこで，与えられた 2 元 n 次形式 Φ に対して，$\Phi_x = \Phi$ となるようなペア x の同値類の個数はいくつあるかという問題が考えられる．

Morales は代数体の整数環に係数を持つ非退化対称行列のペアを扱ったが，ここでは，$\mathbb{Z}$ に係数を持つ非退化対称行列のペアに限定する．$\Phi(1, 0) \neq 0$, $\Phi(0, 1) \neq 0$ とする．次を仮定する．

$$(\mathrm{H}_1) \quad \Phi\text{は重根を持たない．}$$

$A = \mathbb{Q}[T]/(\Phi(T, 1))$, $\theta = T \bmod (\Phi(T, 1))$ とおく．

今，$x = (x_1, x_2)$ を $\Phi_x = \Phi$ を満たす整数係数の非退化 n 次行列のペアとする．$V = \mathbb{Q}^n$ を有理数を成分とする n 次元縦ベクトル全体のなすベクトル空間とする．$M = \mathbb{Z}^n$ を整数を成分とするベクトルのなす V の格子とする．A の V 上の表現 $\rho = \rho_x$ を

$$\rho(\theta)v = -x_1^{-1}x_2 v, \quad v \in V$$

によって定義する．$\rho(\theta)$ の固有多項式は $\Phi(T, 1)$ の定数倍であり，仮定 (H1) より，それは $\rho(\theta)$ の $\mathbb{Q}$ 上の最小多項式と一致する．V は ρ によって，ランク 1 の自由 A–加群になる．これを V_x で表す．

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \; \ldots, \; e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

とおく．$v_0 \in V_x$ を $V_x = \rho(A)v_0$ となるようにとる．

$$\begin{aligned} \mathfrak{a} = \mathfrak{a}_x &= \{\alpha \in A \,|\, \rho(\alpha)v_0 \in M\}, \\ \Lambda = \Lambda_x &= \{\lambda \in A \,|\, \rho(\lambda)M \subset M\} \end{aligned}$$

とおけば，$\mathfrak{a}$ は A の格子であり，Λ は A の整環である．さらに，$\Lambda = \{\lambda \in A \,|\, \lambda\mathfrak{a} \subset \mathfrak{a}\}$ を満たす．すなわち，$\mathfrak{a}$ は proper Λ–イデアルである．$\rho = \rho_x$ によって，M は Λ-加群になる．これを M_x で表す．

$\hat{\Lambda} = \{\alpha \in A \,|\, \mathrm{tr}_{A/\mathbb{Q}}(\alpha\Lambda) \subset \mathbb{Z}\}$ とおく．

補題 1.1. $\mathrm{tr}_{A/\mathbb{Q}}$ によって，同型

$$\mathrm{Hom}_\Lambda(M_x, \hat{\Lambda}) \cong \mathrm{Hom}_\mathbb{Z}(M_x, \mathbb{Z})$$

が引き起こされる．

[証明]　$(\alpha, \beta) \longmapsto \mathrm{tr}_{A/\mathbb{Q}}\,\alpha\beta$ は $\mathbb{Q}$–ベクトル空間 A 上の非退化双 1 次形式である．これから，$\mathrm{Hom}_\Lambda(M_x, \hat{\Lambda}) \ni \varphi \longmapsto \mathrm{tr}_{A/\mathbb{Q}} \circ \varphi$ は同型 $\mathrm{Hom}_\Lambda(M_x, \hat{\Lambda}) \cong \mathrm{Hom}_\mathbb{Z}(M_x, \mathbb{Z})$ を引き起こすことがわかる．　□

補題 1.2. Λ-双線形形式 $B_x : M_x \times M_x \longrightarrow \hat{\Lambda}$ が存在して，

$$x_1 = (\mathrm{tr}_{A/\mathbb{Q}}\, B_x(e_i, e_j)), \quad x_2 = -(\mathrm{tr}_{A/\mathbb{Q}}\, \theta B_x(e_i, e_j))$$

を満たす．

[証明]　$u \in M_x$ とする．補題 1.1 より，$\varphi_u \in \mathrm{Hom}_\Lambda(M, \hat{\Lambda})$ で

$$(\mathrm{tr}_{A/\mathbb{Q}} \circ \varphi_u)(v) = {}^t u x_1 v \quad (v \in M_x) \tag{1.1}$$

を満たすものが存在する．φ_u は Λ-準同型であるから，

$$\begin{aligned}
\mathrm{tr}_{A/\mathbb{Q}}(\theta\varphi_u(v)) &= \mathrm{tr}_{A/\mathbb{Q}}\,\varphi_u(\rho(\theta)v) \\
&= (\mathrm{tr}_{A/\mathbb{Q}}\circ\varphi_u)(\rho(t)v) \\
&= {}^t\!ux_1\rho(t)v = {}^t\!ux_1(-x_1^{-1}x_2v) \\
&= -{}^t\!ux_2v \quad (v\in M_x).
\end{aligned} \tag{1.2}$$

一方，

$$\begin{aligned}
\mathrm{tr}_{A/\mathbb{Q}}(\varphi_{\rho(\theta)u}(v)) &= (\mathrm{tr}_{A/\mathbb{Q}}\circ\varphi_{\rho(\theta)u})(v) \\
&= {}^t(\rho(\theta)u)x_1v = {}^t(-x_1^{-1}x_2u)x_1v \\
&= -{}^t\!ux_2v \quad (v\in M_x).
\end{aligned}$$

よって，$\mathrm{tr}_{A/\mathbb{Q}}(\varphi_{\rho(\theta)u}(v)) = \mathrm{tr}_{A/\mathbb{Q}}(\theta\varphi_u(v))$ を得る．補題 1.1 より，

$$\varphi_{\rho(\theta)u}(v) = \theta\varphi_u(v) \quad (\forall u, v\in M_x)$$

を得る．よって，任意の $\lambda\in\Lambda$ に対して，

$$\varphi_{\rho(\lambda)u}(v) = \lambda\varphi_u(v) = \varphi_u(\rho(\lambda)v) \quad (\forall u, v\in M_x).$$

したがって，$B_x(u,v) = \varphi_u(v)$ とおけば，$B_x : M_x\times M_x \longrightarrow \hat{\Lambda}$ は Λ-双線形形式である．(1.1), (1.2) よりこれが求めるものである． □

$\mathfrak{j} = \Lambda + \theta\Lambda$ とおけば，$\mathfrak{j}$, $\hat{\mathfrak{j}}$ は A の Λ-部分加群である．$B_x(e_i,e_j)\in\hat{\lambda}$ かつ $\theta B_x(e_i,e_j)\in\hat{\lambda}$ より，$B_x(e_i,e_j)\in\hat{\lambda}\cap\theta^{-1}\hat{\Lambda} = \hat{\mathfrak{j}}$ である．$M_x = \rho(\mathfrak{a})v_0$ であるから，$\alpha_1,\ldots,\alpha_n\in\mathfrak{a}$ を $\rho(\alpha_i)v_0 = e_i$ にとれば，$\mathfrak{a} = [\alpha_1,\ldots,\alpha_n]$ である．さらに，$\beta = \beta_x = B_x(v_0,v_0)$ とおけば，

$$B_x(M_x, M_x) = \beta\mathfrak{a}^2 \subset \hat{\mathfrak{j}}.$$

補題 1.3. $y = (y_1, y_2)$ を $x = (x_1,x_2)$ と同値なペアとすれば，$c\in A^\times$ が存在して，$\Lambda_y = \Lambda_x$, $\mathfrak{a}_y = c^{-1}\mathfrak{a}_x$, $\beta_y = c^2\beta_x$.

[証明] $y_k = \gamma x_k{}^t\gamma$, $k=1,2$, $\gamma\in\Gamma$ とする．そのとき，

$$\rho_y(\theta) = -y_1^{-1}y_2 = -(\gamma x_1{}^t\gamma)^{-1}\gamma x_2{}^t\gamma = -{}^t\gamma^{-1}x_1^{-1}x_2{}^t\gamma = {}^t\gamma^{-1}\rho_x(\theta){}^t\gamma.$$

よって，任意の $\alpha\in A$ に対して，$\rho_y(\alpha) = {}^t\gamma^{-1}\rho_x(\alpha){}^t\gamma$．したがって，$f : V_y \longrightarrow V_x$ を，$f(a) = {}^t\gamma a$, $a\in V_y$ によって定義すれば，f は A-加群としての同型である．$\Phi_y = \Phi_x$ は明らか．$f(M_y) = {}^t\gamma M_y = M_x$ であるから，

$$\begin{aligned}
\Lambda_y &= \{\lambda\in A\,|\,\rho_y(\lambda)M_y\subset M_y\} \\
&= \{\lambda\in A\,|\,\rho_x(\lambda)M_x\subset M_x\} = \Lambda_x.
\end{aligned}$$

$v'_0 \in V_y$ を $V_y = \rho_y(A)v'_0$ となるようにとる．$c \in A$ を $f(v'_0) = \rho_x(c)v_0$ となるようにとる．そのとき，対応 $a \longmapsto \rho_y(a)v'_0$，$f$, および対応 $\rho_x(a)v_0 \longmapsto a$ はそれぞれ A-加群の同型 $A \cong V_y$, $V_y \cong V_x$, $V_x \cong A$ を与えるから，これらの合成 $a \longmapsto ac$ は A から A への A-加群としての同型を与える．よって，$c \in A^\times$ である．

$$
\begin{aligned}
\mathfrak{a}_y &= \{\alpha \in A \mid \rho_y(\alpha)v'_0 \in M_y\} \\
&= \{\alpha \in A \mid \rho_x(c\alpha)v_0 \in M_x\} = c^{-1}\mathfrak{a}_x.
\end{aligned}
$$

$B' : M_y \times M_y \longrightarrow \hat{\Lambda}$ を $B'(u, v) = B_x(f(u), f(v))$, $u, v \in M_y$ によって定義すれば，B' は Λ–双線形である．実際，

$$
\begin{aligned}
B'(\rho_y(\lambda)u, \rho_y(\mu)v) &= B_x(f(\rho_y(\lambda)u), f(\rho_y(\mu)v)) = B_x(\rho_x(\lambda)f(u), \rho_x(\mu)f(v)) \\
&= \lambda\mu B_x(f(u), f(v)) = \lambda\mu B'(u, v).
\end{aligned}
$$

また，容易に，

$$
\begin{aligned}
(\mathrm{tr}_{A/\mathbb{Q}}\, B'(e_i, e_j)) &= (\mathrm{tr}_{A/\mathbb{Q}}\, B_x(f(e_i), f(e_j))\,) \\
&= \gamma(\mathrm{tr}_{A/\mathbb{Q}}\, B_x(e_i, e_j)){}^t\gamma = \gamma x_1{}^t\gamma = y_1, \\
-(\mathrm{tr}_{A/\mathbb{Q}}\, \theta B'(e_i, e_j)) &= -(\mathrm{tr}_{A/\mathbb{Q}}\, \theta B_x(f(e_i), f(e_j))\,) \\
&= -\gamma(\mathrm{tr}_{A/\mathbb{Q}}\, \theta B_x(e_i, e_j)){}^t\gamma = \gamma x_2{}^t\gamma = y_2
\end{aligned}
$$

がわかる．よって，$B' = B_y$ である．$e'_i = \rho_y(\alpha_i c^{-1})v'_0$, $i = 1, \ldots, n$ とおけば，$f(e'_i) = \rho_x(\alpha_i)v_0 = e_i$ である．よって，$\alpha_1 c^{-1}, \ldots, \alpha_n c^{-1}$ は $\mathfrak{a}_y$ の基底である．B_y は Λ–双線形だから，$B_y(e'_i, e'_j) = \alpha_i\alpha_j c^{-2} B_y(v'_0, v'_0)$ である．一方，$B_y = B'$ より，

$$
B_y(e'_i, e'_j) = B_x(f(e'_i), f(e'_j)) = B_x(e_i, e_j) = \alpha_i\alpha_j B_x(v_0, v_0).
$$

よって，$\beta_y = c^2\beta_x$ を得る． $\square$

補題 1.4. $a_0 = \Phi(1, 0)$, $\mathfrak{J} = \mathcal{O}_A + \theta\mathcal{O}_A$ とおくと，$a_0^{-1}(N\mathfrak{J})^{-1}\Phi(T, 1)$ は $\mathbb{Z}[T]$ の原始的多項式である．

[証明] p を素数として，$A_p = A \otimes_{\mathbb{Q}} \mathbb{Q}_p$, $\mathfrak{J}_p = \mathfrak{J} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ とかく．$\mathcal{O}_{A_p}$ を A_p の極大整環とすれば，$\mathcal{O}_{A_p} = \mathcal{O}_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$ である．$\varphi(T) = a_0^{-1}\Phi(T, 1)$ は θ の $\mathbb{Q}_p$ 上の固有多項式であり，$\mathfrak{J}_p = \mathcal{O}_{A_p} + \theta\mathcal{O}_{A_p}$ である．次の二つの場合がある．

(a) θ または θ^{-1} は $\mathcal{O}_{A_p}$ の元である．

(b) θ, θ^{-1} のどちらも $\mathcal{O}_{A_p}$ の元でない．

(a) の場合は，$\theta \in \mathcal{O}_{A_p}$ ならば，$\varphi(T) \in \mathbb{Z}_p[T]$ であり，$\mathfrak{J}_p = \mathcal{O}_{A_p}$ であるから，$N_{A_p/\mathbb{Q}_p}(\mathfrak{J}_p)\mathbb{Z}_p = \mathbb{Z}_p$ である．すなわち，$N_{A/\mathbb{Q}}(\mathfrak{J})$ は $\mathbb{Z}_p$ の単数である．$\theta^{-1} \in \mathcal{O}_{A_p}$ ならば，$\mathfrak{J}_p = \theta\mathcal{O}_{A_p}$ であるから，$N_{A_p/\mathbb{Q}_p}(\mathfrak{J}_p)^{-1}\mathbb{Z}_p = N_{A_p/\mathbb{Q}_p}(\theta^{-1})\mathbb{Z}_p$ である．した

がって，$N_{A/\mathbb{Q}}(\mathfrak{J})^{-1}T^n\varphi(T^{-1})$ は $\theta^{-1}\in\mathcal{O}_{A_p}$ の固有多項式であるから，$\mathbb{Z}_p[T]$ の原始的多項式である．よって，$N_{A/\mathbb{Q}}(\mathfrak{J})^{-1}\varphi(T)$ もそうである．
(b) の場合は，$\mathbb{Q}_p$-algebra として，$A_p=A_1\oplus A_2$, $\theta=(\theta_1,\theta_2)$, $\theta_1\in\mathcal{O}_{A_1}$, $\theta_2^{-1}\in\mathcal{O}_{A_2}$, と分解できる．$\varphi_i(T)$ を θ_i の $\mathbb{Q}_p$ 上の固有多項式として，$\mathfrak{J}_i=\mathcal{O}_{A_i}+\theta_i\mathcal{O}_{A_i}$, $i=1,2$ とおく．(a) より，$N_{A_i/\mathbb{Q}_p}(\mathfrak{J}_i)^{-1}\varphi_i(T)$ は $\mathbb{Z}_p[T]$ の原始的多項式である．$\mathcal{O}_{A_p}=\mathcal{O}_{A_1}\oplus\mathcal{O}_{A_2}$, $\mathfrak{J}_p=\mathfrak{J}_1\oplus\mathfrak{J}_2$ であるから，

$$N_{A_p/\mathbb{Q}_p}(\mathfrak{J}_p)^{-1}\varphi(T)=N_{A_1/\mathbb{Q}_p}(\mathfrak{J}_1)^{-1}\varphi_1(T)N_{A_2/\mathbb{Q}_p}(\mathfrak{J}_2)^{-1}\varphi_2(T)$$

はガウスの補題によって $\mathbb{Z}_p[T]$ の原始的多項式である．これがすべての素数 p について成り立つから，$N_{A/\mathbb{Q}}(\mathfrak{J})^{-1}\varphi(T)$ は $\mathbb{Z}[T]$ の原始的多項式である． $\square$

さらに，Morales は次を仮定する．

(H$_2$) Φは原始的である．

(H$_3$) Λは weakly self-dual である．

ここで，Λ が weakly self-dual であるとは，任意の proper Λ–イデアルが可逆 Λ–イデアルであることを意味する．これは，$\hat{\Lambda}$ が可逆 Λ–イデアルであることと同値である (Fröhlich)．これらの仮定の下で，実は $\beta\mathfrak{a}^2=\hat{\mathfrak{j}}$ が成り立つことを示そう．

命題 1.5. 仮定 (H$_1$), (H$_2$), (H$_3$) のもとで，$\beta_x\mathfrak{a}_x^2=\hat{\mathfrak{j}}$ が成り立つ．また，$\mathfrak{j}$ は可逆 Λ–イデアルである．

［証明］ $|a_0|=|\det x_1|=(\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}):x_1(M))$ である． $\mathbb{Z}$-加群の単射準同型の列

$$M\overset{B_x}{\hookrightarrow}\mathrm{Hom}_\Lambda(M,\hat{\mathfrak{j}})\hookrightarrow\mathrm{Hom}_\Lambda(M,\hat{\Lambda})\overset{\mathrm{tr}_{A/\mathbb{Q}}}{\cong}\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$$

と

$$\begin{array}{ccc} B_x(M) & \subset & \mathrm{Hom}_\Lambda(M,\hat{\Lambda}) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{tr}_{A/\mathbb{Q}}} \\ x_1(M) & \subset & \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}) \end{array}$$

から，

$$\begin{aligned}|a_0|=|\det x_1| &= (\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}):x_1(M))\\ &= (\mathrm{Hom}_\Lambda(M,\hat{\Lambda}):B_x(M))\\ &= (\mathrm{Hom}_\Lambda(M,\hat{\Lambda}):\mathrm{Hom}_\Lambda(M,\hat{\mathfrak{j}}))(\mathrm{Hom}_\Lambda(M,\hat{\mathfrak{j}}):B_x(M)).\end{aligned}$$

$M=\rho(\mathfrak{a})v_0$, $\mathfrak{a}=\mathfrak{a}_x$ は proper Λ-イデアルとかける．仮定 (H$_3$) より，Λ は weakly self-dual であるから，proper Λ-イデアル $\mathfrak{a}$ は可逆 Λ-イデアルである．したがって，各素数 p に対して，$\mathfrak{a}_p=\alpha_p\Lambda_p$ である．よって，$M_p=\rho(\Lambda_p)v_p$, $v_p=\rho(\alpha_p)v_0$ であ

る．このとき，$\psi \in \mathrm{Hom}_{\Lambda_p}(M_p, \hat{\Lambda}_p)$ に対して，$\psi(v_p) \in \hat{\Lambda}_p$ を対応させることによって，同型

$$\mathrm{Hom}_{\Lambda_p}(M_p, \hat{\Lambda}_p) \cong \hat{\Lambda}_p$$

を得る．この同型は，$\mathrm{Hom}_{\Lambda_p}(M_p, \hat{\mathfrak{j}}_p) \cong \hat{\mathfrak{j}}_p$，および $B_x(M_p) \cong B_x(M_p, M_p)$ を引き起こす．ゆえに，

$$(\mathrm{Hom}_{\Lambda_p}(M_p, \hat{\Lambda}_p) : \mathrm{Hom}_{\Lambda_p}(M_p, \hat{\mathfrak{j}}_p)) = (\hat{\Lambda}_p : \hat{\mathfrak{j}}_p),$$
$$(\mathrm{Hom}_{\Lambda_p}(M_p, \hat{\mathfrak{j}}_p) : B_x(M_p)) = (\hat{\mathfrak{j}}_p : B_x(M_p, M_p))$$

を得る．これがすべての素数 p について成り立つから，

$$(\mathrm{Hom}_{\Lambda}(M, \hat{\Lambda}) : \mathrm{Hom}_{\Lambda}(M, \hat{\mathfrak{j}})) = (\hat{\Lambda} : \hat{\mathfrak{j}}),$$
$$(\mathrm{Hom}_{\Lambda}(M, \hat{\mathfrak{j}}) : B_x(M)) = (\hat{\mathfrak{j}} : B_x(M, M))$$

を得る．また，$(\hat{\Lambda} : \hat{\mathfrak{j}}) = (\mathfrak{j} : \Lambda)$ が成り立つ．したがって，

$$|\det x_1| = (\mathfrak{j} : \Lambda)(\hat{\mathfrak{j}} : B_x(M, M)) \tag{1.3}$$

を得る．$(\mathfrak{j} : \Lambda) = |\det x_1|$ を示せば証明が完成する．まず，(1.3) より，

$$(\mathfrak{j} : \Lambda) | \det x_1 \tag{1.4}$$

である．一方，

$$(\mathcal{O}_A \mathfrak{j} : \mathfrak{j})(\mathfrak{j} : \Lambda) = (\mathcal{O}_A \mathfrak{j} : \Lambda) = (\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A)(\mathcal{O}_A : \Lambda)$$

より，

$$\frac{(\mathfrak{j} : \Lambda)}{(\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A)} = \frac{(\mathcal{O}_A : \Lambda)}{(\mathcal{O}_A \mathfrak{j} : \mathfrak{j})}$$

を得る．この右辺は，Fröhlich の不変量であり，それは自然数である．Fröhlich の定理によって，$\mathfrak{j}$ が可逆 Λ-イデアルであるための必要十分条件は，その値が 1 であることである．特に，

$$(\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A) | (\mathfrak{j} : \Lambda) \tag{1.5}$$

である．ここで，$(\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A)^{-1} = N_{A/\mathbb{Q}}(\mathcal{O}_A \mathfrak{j})$ である．$\mathcal{O}_A \mathfrak{j} = \mathcal{O}_A + \theta \mathcal{O}_A = \mathfrak{J}$ であるから，補題 1.4 より，

$$(\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A)(\det x_1)^{-1} \Phi(T, 1)$$

は $\mathbb{Z}[T]$ の原始的多項式である．仮定 H_2 より，$\Phi(T, 1)$ は原始的多項式であるから，

$$\det x_1 | (\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A) \tag{1.6}$$

を得る．(1.5), (1.6) より，$\det x_1 | (\mathfrak{j} : \Lambda)$ を得る．これと (1.4) から，$(\mathfrak{j} : \Lambda) = |\det x_1|$，したがって，$B_x(M, M) = \hat{\mathfrak{j}}$ を得る．また，$(\mathcal{O}_A \mathfrak{j} : \mathcal{O}_A) = |\det x_1| = (\mathfrak{j} : \Lambda)$，したがって，$(\mathcal{O}_A : \Lambda)(\mathcal{O}_A \mathfrak{j} : \mathfrak{j})^{-1} = 1$ が成り立つから，Fröhlich の定理により，$\mathfrak{j}$ は可逆 Λ-イデアルである． □

注意 1.6. 仮定 (H_3) から，$\hat{\Lambda}$ は可逆 Λ-イデアルであり，$\mathfrak{j}$ も可逆 Λ-イデアルであることから，$\hat{\mathfrak{j}} = \mathfrak{j}^{-1}\hat{\Lambda}$ も可逆 Λ-イデアルである．

I_Λ によって A の可逆 Λ–イデアルのなす乗法群を表し，

$$\begin{aligned}
S &= \{(\mathfrak{a}, \beta) \in I_\Lambda \times A^\times \,|\, \beta\mathfrak{a}^2 = \hat{\mathfrak{j}},\ a_0 D_A N_{A/\mathbb{Q}}\,\beta > 0\}, \\
A_+^\times &= \{\alpha \in A^\times \,|\, N_{A/\mathbb{Q}}\,\alpha > 0\}, \\
G &= \{(\mathfrak{b}, \xi) \in I_\Lambda \times A_+^\times \,|\, \xi\mathfrak{b}^2 = \Lambda\}, \\
G_0 &= \{(\xi^{-1}\Lambda, \xi^2) \,|\, \xi \in A^\times\} \\
G_1 &= \{(\xi^{-1}\Lambda, \xi^2) \,|\, \xi \in A_+^\times\}
\end{aligned}$$

とおく．G_1, G_0 は群 G の部分群であり，容易にわかるように，

$$(G : G_1) = |{}_2\mathrm{Pic}^+(\Lambda)||\Lambda^{(1)}/(\Lambda^{(1)})^2|.$$

ここで，

$$\begin{aligned}
\mathrm{Pic}^+(\Lambda) &= I_\Lambda/\{\xi\Lambda \,|\, \xi \in A_+^\times\}, \\
{}_2\mathrm{Pic}^+(\Lambda) &= \{c \in \mathrm{Pic}^+(\Lambda) \,|\, c^2 = 1\}, \\
\Lambda^{(1)} &= \{\varepsilon \in \Lambda^\times \,|\, N_{A/\mathbb{Q}}\,\varepsilon = 1\}
\end{aligned}$$

とおいた．実際，$\varepsilon \longmapsto (\Lambda, \varepsilon)$ および $(\mathfrak{b}, \xi) \longmapsto [\mathfrak{b}]$ によって，

$$1 \longrightarrow \Lambda^{(1)}/(\Lambda^{(1)})^2 \longrightarrow G/G_1 \longrightarrow {}_2\mathrm{Pic}^+(\Lambda) \longrightarrow 1$$

は完全系列である．

[証明] $(\mathfrak{b}, \xi) \in G$, $(\eta^{-1}\Lambda, \eta^2) \in G_1$ とすれば，$(\mathfrak{b}, \xi)(\eta^{-1}\Lambda, \eta^2) = (\eta^{-1}\mathfrak{b}, \xi\eta^2)$, $[\eta^{-1}\mathfrak{b}] = [\mathfrak{b}]$ であるから，$(\mathfrak{b}, \xi) \longmapsto [\mathfrak{b}]$ は $h : G/G_1 \longrightarrow {}_2\mathrm{Pic}^+(\Lambda)$ を引き起こす．$[\mathfrak{b}] \in {}_2\mathrm{Pic}^+(\Lambda)$ とすれば，ある $\xi \in A_+^\times$ について，$\xi\mathfrak{b}^2 = \Lambda$ であるから，$(\mathfrak{b}, \xi) \in G$ であり，h は全射である．$(\mathfrak{b}, \xi)G_1 \in \ker h$ とする．ある $\eta \in A_+^\times$ について，$\mathfrak{b} = \eta\Lambda$ であるから，$\xi\eta^2\Lambda = \Lambda$, $\xi\eta^2 = \varepsilon \in \Lambda^\times$ である．$\xi \in A_+^\times$ より，$\varepsilon \in \Lambda^{(1)}$ である．よって，$(\mathfrak{b}, \xi)G_1 = (\eta\Lambda, \varepsilon\eta^{-2})G_1 = (\Lambda, \varepsilon)G_1$ である．$\varepsilon \longmapsto (\Lambda, \varepsilon)$ は明らかに，$\Lambda^{(1)}/(\Lambda^{(1)})^2 \longrightarrow G/G_1$ を引き起こす．$(\Lambda, \varepsilon) \in G_1$ とすれば，ある $\xi \in A_+^\times$ について $(\Lambda, \varepsilon) = (\xi^{-1}\Lambda, \xi^2)$ であるから，$\xi \in \Lambda^\times \cap A_+^\times = \Lambda^{(1)}$, $\varepsilon = \xi^2 \in (\Lambda^{(1)})^2$ である． □

また，群 G は集合 S に

$$(\mathfrak{b}, \xi)(\mathfrak{a}, \beta) = (\mathfrak{a}\mathfrak{b}, \beta\xi), \quad (\mathfrak{b}, \xi) \in G, (\mathfrak{a}, \beta) \in S$$

によって作用する．$[\mathfrak{a}]$ によって，$\mathfrak{a}$ の狭義イデアル類を表す．$\beta_0 \in A^\times$ を $N_{A/\mathbb{Q}}\,\beta_0$ が $a_0 D_A$ と同じ符号になるようにとる．

定理 1.7 (J. Morales). 仮定 $(\mathrm{H}_1), (\mathrm{H}_2), (\mathrm{H}_3)$ を満たすような Φ, Λ が与えられとき，$\Phi_x = \Phi$, $\Lambda_x = \Lambda$ を満たすようなペア x が存在するための必要十分条件は，$S \neq \emptyset$ である．これは，$[\hat{\mathfrak{j}}] \in [(\beta_0)]\mathrm{Pic}^+(\Lambda)^2$ と同値である．

定理 1.8 (J. Morales). $S \neq \emptyset$ のとき，$x \longmapsto (\mathfrak{a}_x, \beta_x)$ は $\Phi_x = \Phi,\ \Lambda_x = \Lambda$ を満たすようなペア x の同値類の集合から，$G_0 \backslash S$ への全単射を引き起こす．特に，そのようなペア x の同値類の個数は,

$$\frac{1}{(G_0 : G_1)} |\Lambda^{(1)}/(\Lambda^{(1)})^2|\,|_2\mathrm{Pic}^+(\Lambda)|$$

に等しい．ここで,

$$(G_0 : G_1) = \begin{cases} 1, & n\,\text{が奇数または，}A\,\text{が総虚代数体の直和のとき,} \\ 2, & \text{それ以外のとき.} \end{cases}$$

[証明]　G は S に transitive に作用するから,

$$|G_0 \backslash S| = (G : G_0) = \frac{(G : G_1)}{(G_0 : G_1)} = \frac{1}{(G_0 : G_1)} |\Lambda^{(1)}/(\Lambda^{(1)})^2|\,|_2\mathrm{Pic}^+(\Lambda)|.$$

n が奇数ならば，$(\xi^{-1}\Lambda, \xi^2) = ((-\xi)^{-1}\Lambda, (-\xi)^2)$ であり，ξ または $-\xi$ は $A_+^\times$ に属するから，$G_0 = G_1$ である．A が総虚代数体の直和ならば，$A^\times = A_+^\times$ であるから，$G_0 = G_1$ である．n が偶数であって，A は総虚代数体の直和でないとする．そのとき，$\xi \in A^\times$ で $N_{A/\mathbb{Q}}\xi < 0$ となるものがとれる．もし，$(\xi^{-1}\Lambda, \xi^2) \in G_0$ が G_1 に属したとすれば，$(\xi^{-1}\Lambda, \xi^2) = (\eta^{-1}\Lambda, \eta^2)$, $\eta \in A_+^\times$ となるが，$\xi^2 = \eta^2$ より，$\xi = \pm\eta$ となって， $N_{A/\mathbb{Q}}\xi < 0$ に矛盾する．よって，この場合には，$G_0 \supsetneq G_1$ であり，指数 $(G_0 : G_1)$ は明らかに 2 である． □