ガロア表現の基礎 I

山内 卓也 (大阪府立大学)

今回のサマースクールに登場する主なガロア表現は

(i) 代数体の絶対ガロア群の ℓ 進表現, 整 ℓ 進表現, 法 ℓ 表現

(ii) 局所体 ($\mathbb{Q}_p$ の有限次拡大) の絶対ガロア群の ℓ 進表現, 整 ℓ 進表現, 法 ℓ 表現

(iii) Artin 表現

(iv) "大きな"環を係数とするガロア群の表現

である. 本稿では主に (i),(ii) のガロア表現を中心にそれらの定義および簡単な性質を紹介する. 講演では時間の都合で (iii) には触れることはできなかったがサマースクールの後半の内容と関連する重要な表現達である[1]. (iv) に関しては深くは立ち入らないが, どのような場面でそのような表現が登場するかを早足に紹介した. 関連する今井氏や落合氏の原稿を読む動機となることを期待したい.

本稿を読むために必要な予備知識は [9] で十分である. 本稿に続く [4] ではガロア表現に付随する不変量の１つである L-関数が紹介され, それに纏わる話が展開されている. 併せて参照されたい.

Contents

[1] Artin 表現だけは何かを調べる道具というよりもその保型性に興味が注がれているため, これについても, あまり詳しく述べなかった. ただし, その保型性の証明には肥田理論や楕円保型形式に付随するガロア表現の性質が用いられることなどを考えると, Artin 表現は今回学ぶ ℓ 進表現およびその変形理論の研究の枠組みに入っている.

1. 副有限群の線形表現

Γを副有限群, Rを局所コンパクトな位相環[2], および, MをR上の有限階数自由加群とする. MにはRの位相が誘導する位相が入る. MからMへの連続写像全体の成す集合$\mathrm{Map}(M,M)$にはコンパクト開位相[3] が入り, $\mathrm{Aut}_R(M)$にその制限位相を入れる. このとき連続準同型射

$$\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M)$$

のことをΓの線形表現とよぶことにする. MのR上の階数をnとし, そのR上基底を固定すると, R係数の一般線形群に値をとる表現

$$\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M) \simeq \mathrm{GL}_n(R) := \{g \in \mathrm{M}_n(R) |\ \det(g) \in R^\times\}$$

が得られる[4]. 表現ρを与えることとΓがR線形に作用する有限階数自由R加群Mを与えることは同じである. 本報告集では, これらの表示方法を, 場合に応じて適宜使い分ける.

本稿では, 主に, Γが数論的な体Kの絶対ガロア群$G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$の場合を考える. より詳しくこのサマースクールでは, 体Kとして代数体, 局所体などを想定し, Rはℓ進体$\mathbb{Q}_\ell$, ℓ進整数環$\mathbb{Z}_\ell$, 有限体$\mathbb{F}_\ell$およびそれらを係数とする有限生成代数($\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$, $\mathbb{Z}_\ell[[X]], \ldots$)やBanach 代数などを想定している. 先に述べたようにG_Kのいくつかの表現を紹介するがそれらをまとめてガロア表現ということにする.

次節に入る前に線形表現に関する一般的事項や操作について復習しておく. 本報告集ではこれらの知識は仮定されて話が進められている.

定義 1-1. 記号は上の通りする. $\rho_1, \rho_2 : \Gamma \longrightarrow \mathrm{Aut}_R(M)$を$\Gamma$の表現とする. このとき, ρ_1とρ_2が**同値 (equivalent)** とはある$t \in \mathrm{Aut}_R(M)$が存在して, $\rho_1(g) = t\rho_2(g)t^{-1},\ g \in \Gamma$が成り立つときをいう. この場合, $\rho_1 \sim \rho_2$などと書いたりする. 自由R加群Mの基底を固定することで, 表現のトレースを考えることができる:

$$\mathrm{tr}\rho_i : \Gamma \xrightarrow{\rho_i} \mathrm{Aut}_R(M) \simeq \mathrm{GL}_n(R) \xrightarrow{\mathrm{tr}} R,\ i = 1, 2.$$

これはMのR上の基底の取り方に依らない. 表現ρ_1, ρ_2が同値であるとき, 両者のトレースは等しくなるが, 比較的緩やかな仮定の下でこの逆も成立することを後で示す(命題2-2-6と命題2-4-1を参照).

---

[2]位相環とは下部構造が位相空間の構造を持ち, この位相に関して環としてのすべての演算が連続であるもの. 位相空間Xが局所コンパクトであるとは, Xの各点がコンパクトな近傍を少なくとも1つもつときをいう.

[3]X, Yを位相空間とし, $\mathrm{Map}(X, Y)$をXからYへの連続写像全体の成す集合とする. Xのコンパクト集合AとYの開集合Bに対して, $W(A, B) := \{f \in \mathrm{Map}(X, Y) |\ f(A) \subset B\}$とおく. このような$W(A, B)$全体で生成される$\mathrm{Map}(X, Y)$上の位相を**コンパクト開位相**という.

[4]このサマースクールではこのようなGL_n型のガロア表現しか扱わないが, Mにある構造$*$を付けて, $\mathrm{Aut}_R(M)$のところを

$$\mathrm{Aut}_R(M, *) = \{f \in \mathrm{Aut}_R(M) |\ f\text{は}*\text{を保つ}\}$$

に代えると自然に線形代数群Gに値をもつガロア表現が得られる. このような代数群Gとしては, GSp_{2n}, $\mathrm{GO}(n)$, $\mathrm{GU}(n, m)$などが挙げられる. また, ガロア群の線形化とその変形が今回の勉強目的なのでサマースクール 2004 ([17]) で扱っているような型のガロア表現はここでは扱わない.

定義 1-2. Γ の表現 $\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M)$ と正規部分群 $H \subset \Gamma$ が与えられたとき, M の H 不変部分 $M^H := \{m \in M \mid$ 任意の $h \in H$ に対して, $\rho(h)m = m\}$ は Γ/H が作用する R 部分加群である. これに対応する表現を ρ_H とかく:

$$\rho_H : .\Gamma/H \longrightarrow \mathrm{Aut}_R(M^H).$$

これに対して, H 余不変部分 M/M^H に対応する Γ/H の表現を ρ^H と表す.

定義 1-3.(1) $\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M)$ を Γ の表現とする. このとき, R 代数 R' に対して, ρ の R' への係数拡大を $\rho_{R'}$ によって表す. これは, 表現空間が $M \otimes_R R'$ であり, 作用は $m \otimes r' \in M \otimes_R R'$ に対して,

$$\rho_{R'}(m \otimes r') = \rho(m) \otimes r'$$

によって与えられる表現である.
(2) $\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M)$ を Γ の表現とする. ρ が**既約**であるとは, ρ の表現空間 M が 0 と M 以外の Γ 不変 R 部分加群を持つときを言う.
(3) K を体とし, V を K 上の有限次ベクトル空間とする. $\rho : \Gamma \longrightarrow \mathrm{Aut}_K(V)$ を Γ の表現とする. ρ が**絶対既約**であるとは, 任意の K の有限次拡大 L に対して, ρ_L が既約であるときをいう.

定義 1-4. (1) Γ の表現 $\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M)$ が与えられたとき, R 加群 M の m 次の直和 $\bigoplus_r M$, テンソル積 $\bigotimes_r M$, 対称積 $\mathrm{Sym}^r_R M$, 外積 $\bigwedge^r_R M$ に対応する表現をそれぞれ, $\oplus^r\rho,\ \otimes^m\rho, \mathrm{Sym}^m\rho,\ \wedge^r\rho$ と表すことにする. 特に, M の R 上の階数を n とするとき,

$$\det\rho := \wedge^n\rho$$

のことを ρ の**判別式**という. 基底を固定して, $\mathrm{Aut}_R(M) \simeq \mathrm{GL}_n(R)$ と同一視するとき, ρ の判別式は 1 次元表現 $\Gamma \xrightarrow{\rho} \mathrm{Aut}_R(M) \simeq \mathrm{GL}_n(R) \xrightarrow{\det} R^\times$ に他ならない. ただし, この $\det$ は行列の判別式を取るという対応である.

また, M の双対 $M^\vee := \mathrm{Hom}_R(M, R)$ に対応する表現を $\rho^\vee$ で表し, **反傾表現 (contragredient representation)** という. 作用は, $\phi \in M^\vee$, $\gamma \in \Gamma$ に対して,

$$\gamma\phi(m) := \phi(\gamma^{-1}m),\ m \in M$$

によって与えられる.

1 次元の表現 $\chi : \Gamma \longrightarrow R^\times$ の整数冪 $\chi^n,\ n \in \mathbb{Z}$ と ρ とのテンソル積 $\rho \otimes \chi^n$ を ρ の χ による n **回捻り**という.
(2) 二つの Γ の表現 $\rho_i : \Gamma \longrightarrow \mathrm{Aut}_R(M_i), i = 1, 2$ が与えられたとき, $M_1 \oplus_R M_2,\ M_1 \otimes_R M_2$ に対応する表現を $\rho_1 \oplus \rho_2,\ \rho_1 \otimes \rho_2$ と表す.

特に, Γ の表現 $\rho : \Gamma \longrightarrow \mathrm{Aut}_R(M)$ に対して, $\mathrm{End}_R(M) = M^\vee \otimes_R M$ なので, これに対応する表現を $\mathrm{ad}\rho := \rho^\vee \otimes \rho$ と表し, ρ の**随伴表現 (adjoint representation)** という. 作用は, $\phi \in \mathrm{End}_R(M)$, $\gamma \in \Gamma$ に対して,

$$\gamma\phi(m) := \gamma\phi(\gamma^{-1}m),\ m \in M$$

によって与えられる.

2. 代数体の絶対ガロア群の線形表現

2.1. **分岐と不分岐.** この節では K は代数体とし, p や ℓ は素数とする. Σ_K によって K の有限素点全体の集合を表す. L を K の正規拡大 (無限次拡大でもよい) とし, その整数環を $\mathcal{O}_L$ と書く. このときガロア群 $\mathrm{Gal}(L/K)$ は副有限群であり, このことから Krull 位相に関してコンパクトな位相群であることがわかる (cf. [9]). v を K の有限素点とし, v の上にある L の素点 w をとる. このとき, $D_{L,v} = \{\sigma \in \mathrm{Gal}(L/K) |\ \sigma(w) = w\}$ のことを v **での分解群**という. $D_{L,v}$ は w の取り方に依存しているが, そのずれは $\mathrm{Gal}(L/K)$ の中で互いに共役となる. このとき, よく知られているように全射

$$D_{L,v} \longrightarrow \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v),\ \sigma \mapsto \sigma \bmod w$$

が存在する. ただし, $\mathbb{F}_w := \mathcal{O}_L/w$ は w の剰余体とする. この写像の核を $I_{L,v}$ と書き, v **での惰性群**という:

$$1 \longrightarrow I_{L,v} \longrightarrow D_{L,v} \longrightarrow \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v) \longrightarrow 1.$$

ガロア群 $\mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$ には

$\mathrm{Frob}_v(x) = x^{\sharp\mathbb{F}_v},\ x \in \mathbb{F}_w$ という標準的な元 Frob_v が存在し, これを**フロベニウス置換 (元)** という[5]. これを上の全射で $D_{L,v}$ へ持ち上げたものも Frob_v と書くことにする.

このとき, $I_{L,v} = \{1\}$ ならば L は v で**不分岐**であるといい, そうでないならば, L は v で**分岐する**という. L が v で不分岐である場合は Frob_v の持ち上げは一意的に決まる.

S を K の有限素点から成る有限集合とし, K_S を S に含まれない Σ_K の各素点で不分岐な K の代数拡大で最大のものとする (S の外不分岐最大拡大という). 上の議論を $L = K_S$ として考えたとき, $v \notin S$ ならば, v は K_S で不分岐であり, Frob_v は $D_{K_S,v}$ の中で一意に定まる. しかし, $D_{K_S,v}$ の G_{K_S} への埋め込みが, v の上にある K_S の素点 w の取り方に依存しているので, Frob_v も同様に w の取り方に依存する.

定義 2-1-1. R を位相環, M を位相 R 加群とする[6]. v を K の有限素点とし, $I_v := I_{\overline{K},v}$ とおく. G_K の連続な線形表現 $\rho : G_K \longrightarrow \mathrm{Aut}_R(M)$ が v で**不分岐**であるとは, $\rho(I_v) = \{1\}$ となるときをいい, そうならないとき, ρ は v **で分岐する**という. これらの性質は I_v の定義 (即ち, w の取り方) に依らない.

ρ の核に対応する K のガロア拡大を $K_{S_\rho} := \overline{K}^{\mathrm{Ker}\rho}$ とすると, K_{S_ρ} で分岐する素点の集合 S_ρ は ρ が分岐するような素点と丁度一致する. 上の脚注 6 で説明したように 1 点 $\{\mathrm{id}_M\}$ は $\mathrm{Aut}_R(M)$ の閉集合なので, $\mathrm{Ker}\rho$ は正規部分群かつ閉集合. 従って, (無限次) ガロア対応により ([9] の定理 1.12 を参照), $G_K/\mathrm{Ker}\rho \simeq \mathrm{Gal}(K_{S_\rho}/K)$ を得る. そして準同型定理よ

---

[5] 数論的フロベニウス元とも呼ばれる.

[6] ここでは, 位相加群の定義に Hausdorff 性も含める. そうすると, $\mathrm{Aut}_R(M)$ は Hausdorff になり (cf. [21] の p.170 の定理 30.2*-(2)), 特に, $\mathrm{Aut}_R(M)$ の任意の点は閉集合である.

り, ρ はこの群を経由する:

$$\begin{tikzcd} G_K \arrow[rr, "\rho"] \arrow[dr, "\pi"'] & & \mathrm{Aut}_R(M) \\ & \mathrm{Gal}(K_{S_\rho}/K) \arrow[ur, "\widetilde{\rho}"'] & \end{tikzcd}$$

ただし, 自然な射影 π は $\sigma \mapsto \sigma|_{K_{S_\rho}}$ で与えられる. $v \notin S_\rho$ ならば, $\mathrm{Frob}_v \in D_{K_{S_\rho},v}$ は一意的に定まるので $\widetilde{\rho}(\mathrm{Frob}_v)$ を考えることができる. Frob_v の住んでいる場所は正確には $\mathrm{Gal}(K_{S_\rho}/K)$ であり, G_K ではない. しかし, 事あるごとに $\widetilde{\rho}$ と書いて議論するのは面倒なので, $\widetilde{\rho}(\mathrm{Frob}_v)$ を $\rho(\mathrm{Frob}_v)$ と表すことにする.

上でも説明したように, $\rho(\mathrm{Frob}_v)$ は v の上の K_{S_ρ} の素点 w の選び方に依存している. 素点 w の選び方を換えると, ある元 $g \in G_K$ が存在して, 対応するフロベニウス元が $g\mathrm{Frob}_v g^{-1}$ となる. これを ρ で (正確には $\widetilde{\rho}$ で) 写すと,

$$\rho(g\mathrm{Frob}_v g^{-1}) = \rho(g)\rho(\mathrm{Frob}_v)\rho(g)^{-1} \overset{\text{共役}}{\sim} \rho(\mathrm{Frob}_v)$$

となる. これより, $\rho(\mathrm{Frob}_v)$ のトレースや行列式は w の取り方にも依らず一意的に定まることがわかる. 後で見るように ρ はこれらの値で特徴付けられる.

2.2. ℓ **進表現.** E を $\mathbb{Q}_\ell$ の有限次拡大, $\mathcal{O}_E$ をその整数環とし, V を E 上の有限次ベクトル空間とする. V の零元 0 の開近傍系を V の $\mathcal{O}_E$ 格子[7]で定義することによって, V に位相を入れる. このとき, 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_E(V)$ のことを ℓ **進表現**と呼ぶ. ただし, $\mathrm{Aut}_E(V)$ には V の連続自己写像の成す集合 $\mathrm{Map}(V, V)$ のコンパクト開位相から定まる制限位相を入れている. V の基底を固定することで同型 $\mathrm{Aut}_E(V) \simeq \mathrm{GL}_n(E)$, $(n = \dim_E V)$ を得るが, この同型は $\mathrm{GL}_n(E)$ に E のノルムが誘導する位相を入れると, 位相同型を与える. 実は E が $\mathbb{Q}_\ell$ 上無限次拡大でも, ρ の像はある $\mathbb{Q}_\ell$ の有限次拡大に係数をとる (定理 2.2.8). 従って, ℓ 進表現の係数体 E が影響しない問題を扱う場合は V は $\overline{\mathbb{Q}}_\ell$ 上のベクトル空間となっていることがよくあることを注意しておく. 以下では ℓ 進表現の代表的な例を与える.

例 2-2-1. 1 の ℓ 冪等分点の成す群 $\mu_{\ell^n}(\overline{K}) := \{x \in \overline{K} |\ x^{\ell^n} = 1\} \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ が定める射影系 $\{\mu_{\ell^{n+1}}(\overline{K}) \xrightarrow{\ell\text{乗}} \mu_{\ell^n}(\overline{K})\}_n$ の極限

$$\mathbb{Z}_\ell(1) := \varprojlim_{\ell\text{乗}} \mu_{\ell^n}(\overline{K}) \simeq \mathbb{Z}_\ell$$

を考える. G_K の $\mu_{\ell^n}(\overline{K})$ への作用は射影系の射 (ℓ 乗写像) と可換なので, G_K は $\mathbb{Z}_\ell(1)$ にも作用する. この作用から得られる 1 次元連続表現

$$\chi_\ell : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell(1)) \simeq \mathbb{Z}_\ell^\times$$

のことを ℓ **進円分指標**という. 連続性は明らかである (命題 2-3-2 を参照). χ_ℓ の $\mathbb{Q}_\ell$ への係数拡大も同様に χ_ℓ で表す. 整数 i を固定したとき, 下部構造が $\mathbb{Z}_\ell$ で, G_K が χ_ℓ^i を経由して作用している加群を $\mathbb{Z}_\ell(i)$ と書いて**第 i Tate 捻り (i-th Tate Twist)** と呼ぶ. 先ほど同様,

[7] V の $\mathcal{O}_E$ 部分加群 T であって, $T \otimes_{\mathcal{O}_E} E = V$ となるもの.

$\mathbb{Q}_\ell(i) := \mathbb{Z}_\ell(i) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ のこともそう呼ぶことにする. フロベニウス自己同型 $\mathrm{Frob}_p,\ p \neq \ell$ は $\mathbb{Z}_\ell(i)$ または $\mathbb{Q}_\ell(i)$ に p^i 倍写像として作用する. すなわち, $\chi_\ell^i(\mathrm{Frob}_p) = p^i$.

整数 i と ℓ 進表現 (ρ, V) に対して, $V(i)$ は下部構造が V で, G_K が $\rho \otimes \chi_\ell^i$ を経由して作用している加群を表し, V の第 i Tate 捻りと呼ばれる.

ヘンゼルの補題より, $\mu_{\ell-1}(\mathbb{Q}_\ell) \subset \mathbb{Z}_\ell^\times$ である. これより, 同型 $\mathbb{Z}_\ell^\times \simeq \mu_{\ell-1} \times (1 + \ell\mathbb{Z}_\ell)$ を用いて, ℓ 進円分指標 χ_ℓ を $\chi_\ell = \omega_\ell \chi_{\ell,1},\ \omega_\ell : G_K \longrightarrow \mu_{\ell-1},\ \chi_{\ell,1} : G_K \longrightarrow 1 + \ell\mathbb{Z}_\ell$ と分解できる. ω_ℓ のことを **Teichmüller 指標**という. この指標は後で述べる法 ℓ 円分指標の Teichmüller lift になっている.

例 2-2-2. $\log_\ell : (1 + \ell\mathbb{Z}_\ell) \xrightarrow{\sim} \ell\mathbb{Z}_\ell,\ x \mapsto \displaystyle\sum_{n \geq 1} \frac{(1-x)^n}{n}$ を ℓ 進対数関数とする. このとき,

$$\rho : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell),\ g \mapsto \rho(g) = \begin{pmatrix} 1 & \log_\ell \chi_{\ell,1}(g) \\ 0 & 1 \end{pmatrix}$$

は可約だが半単純ではない表現である. また, その像は明らかに有限ではない.

例 2-2-3. K を代数体, E を $\mathbb{P}_K^2 \ni [x : y : z]$ 内で Weierstrass 方程式

$$zy^2 + a_1xyz + a_3z^2y = x^3 + a_2zx^2 + a_4z^2x + a_6z^3, a_1, a_3, a_2, a_4, a_6 \in K$$

によって, 定義される K 上の楕円曲線とする. 簡単のため適当に座標変換をして係数はすべて $\mathcal{O}_K$ に入っていると仮定しておく. K を含む体 L に対して,

$$E(L) := \{[x : y : z] \in \mathbb{P}^2(L) |\ zy^2 + a_1xyz + a_3z^2y = x^3 + a_2zx^2 + a_4z^2x + a_6z^3\}$$

は $O_E := [0 : 1 : 0]$ を単位元とするアーベル群である (群構造に関しては [16] の 3 章を見よ). このとき, ℓ^n-等分点の成す群 $E[\ell^n](\overline{K}) = \{P \in E(\overline{K}) |\ \ell^n P = O\} \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{\oplus 2}$ が定める射影系 $\{E[\ell^{n+1}](\overline{K}) \xrightarrow{\ell 倍} E[\ell^n](\overline{K})\}_n$ の極限

$$T_\ell(E) := \varprojlim_{\ell\ 倍} E[\ell^n](\overline{K}) \simeq \mathbb{Z}_\ell^{\oplus 2}$$

のことを ℓ **進テート加群** (**ℓ-adic Tate module**) という. $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ とおき, ℓ **進有理テート加群** (**ℓ-adic rational Tate module**) という . $V_\ell(E)$ は $\mathbb{Q}_\ell$ 上 2 次元のベクトル空間である. 射影系の射である ℓ 倍射は K 上定義された代数的な射なので, これは G_K の $E[\ell^n]$ への作用と G_K 同変である. よって, G_K は $T_\ell(E)$ および $V_\ell(E)$ にも作用する. この作用によって, 連続準同型写像

$$\rho_{E,\ell} : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Q}_\ell)$$

を得る. 連続性は $V_\ell(E)$ が G_K 不変な格子 $T_\ell(E)$ を持つことから明らかに従う (命題 2-3-2 を見よ). 次元が g のアーベル多様体 A に対しても同様に有理 ℓ 進 Tate 加群 $V_\ell(A)$ を考えることができ, それは $\mathbb{Q}_\ell$ 上 $2g$ 次元のベクトル空間となる.

素数 $p \neq \ell$ の上にある K の素点 v に対して, $\mathbb{F}_v$ をその剰余体とする. 素点 v が E の判別式 $D_E (\in \mathcal{O}_K)$ を割らないとき $\rho_{E,\ell}$ は v で不分岐であることが知られている (cf. [16] の命題 5.1). この場合, $\rho_{E,\ell}(\mathrm{Frob}_v)$ を考えることができるが, この作用 (又はその表現行列) を

一般に理解することは難しい. しかし, そのトレースや行列式はわかりやすいものになっており, それぞれ

$$\det(\rho_{E,\ell}(\mathrm{Frob}_v)) = \chi_\ell(\mathrm{Frob}_v) = \sharp\mathbb{F}_v,\ \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_v)) = \sharp\mathbb{F}_v + 1 - \sharp\widetilde{E}(\mathbb{F}_v)$$

となっている ([16] の 5 章を参照). ただし, $\widetilde{E}$ は E の v での還元を表す. ここで注目すべきはこれらの値が ℓ によらないということである. 背景には 4 節で説明する厳整合系や三枝氏によって解説されるエタールコホモロジー理論がある ([7]).

注意 2-2-4. ℓ 進表現を具体的に作るには G_K の構造を理解していなければならない. しかし, G_K の構造は完全に知られておらず, それ故に, 楕円曲線やアーベル多様体のテート加群などの幾何的起源のつく対象を扱わなければ ℓ 進表現の例を系統的に構成することができない.

より一般に, 代数体 K 上定義された代数多様体が与えられたとき, そこから G_K の ℓ 進表現を構成する「機械」が存在する. それが Grothendieck によって発明されたエタールコホモロジーである (三枝氏の原稿 [7] 参照).

一般に, ℓ 進表現は像が有限とも限らないし, 半単純とも限らない (例 2-2-2). 従って, 次のように与えられた ℓ 進表現の半単純化を構成することは有効である.

定義 2-2-5. 有限次元 E ベクトル空間 V に G_K が作用しているとする. このとき, V の $E[G_K]$ 加群としての減少列

$$V_0 = V \supset V_1 \supset \cdots \supset V_t = \{0\}$$

で各 $V_i/V_{i+1},\ i = 0, \ldots, t-1$ が単純 $E[G_K]$ 加群となるものがとれる (ジョルダン-ヘルダーの定理). このような減少列から定まる $\{V_i/V_{i+1}\}_{i=0}^{t-1}$ は順番と同型を除いて一意に定まる. このとき, 半単純 $E[G_K]$ 加群

$$V^{\mathrm{ss}} := \bigoplus_{i=0}^{t-1} V_i/V_{i+1}$$

のことを V の**半単純化**とよぶ. ℓ 進表現 (ρ, V) の半単純化を ρ^{ss} によって表すことにする. このとき, ρ が v で不分岐ならば, $\mathrm{tr}\rho(\mathrm{Frob}_v) = \mathrm{tr}\rho^{\mathrm{ss}}(\mathrm{Frob}_v)$, $\det\rho(\mathrm{Frob}_v) = \det\rho^{\mathrm{ss}}(\mathrm{Frob}_v)$ 等が成り立つ. また, ρ が既約ならば明らかに $\rho^{\mathrm{ss}} = \rho$ が成立.

一般にガロア表現が同値であるかどうか判定することは難しいが, その半単純化はトレースで特徴付けることができる. この事実は [4] で登場する Chebotarev の密度定理と半単純加群の一般論から導かれる.

命題 2-2-6. 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_E(V)$ の分岐素点の成す集合 S_ρ は有限集合であると仮定する. このとき, ρ の半単純化 ρ^{ss} は $\mathrm{tr}\rho(\mathrm{Frob}_v),\ v \in \Sigma_K \setminus S_\rho$ の値で一意的に決まる.

証明. 分岐する素点が有限個である二つの連続表現 $\rho, \rho' : G_K \longrightarrow \mathrm{Aut}_E(V)$ が

$$\mathrm{tr}(\rho(\mathrm{Frob}_v)) = \mathrm{tr}(\rho'(\mathrm{Frob}_v)), \forall v \in \Sigma_K \setminus S,\ S := S_\rho \cup S_{\rho'}$$

を満たすとき, $\rho \sim \rho'$ を示せば良い. そのためにまずこの仮定から,

$$(*)\ \mathrm{tr}\rho(g) = \mathrm{tr}\rho'(g), \forall g \in G_K$$

が成立することを示す.

$$H = G_K/(\mathrm{Ker}\rho \cap \mathrm{Ker}\rho')$$

とおくと, ρ, ρ' は H を経由する. ここで, 次の包含関係を考える:

$$F := \{h \in H |\ \exists v \in \Sigma_K \setminus S \text{ such that } h = \mathrm{Frob}_v\} \subset \{h \in H |\ \mathrm{tr}\rho(h) = \mathrm{tr}\rho'(h)\} \subset H$$

中央の集合は H の閉集合である[8]. H に対応する代数体は S の外不分岐なので, H に Chebotarev の密度定理を適用すると, F は H の中に稠密に入っているので, 閉包をとることで, 主張 $(*)$ を得る. あとは次の命題を $A = E[G_K]$ と $M = V$ に適用することで, $\rho \sim \rho'$ を得る. □

命題 2-2-7 k を標数 $p \geq 0$ の体, A を k-代数とし, M, M' を k 上有限次元の半単純 A 加群とする. もし $p > 0$ ならば, $p > \max\{\dim_k(M), \dim_k(M')\}$ を仮定する. このとき,

$$\mathrm{tr}_M(a) = \mathrm{tr}_{M'}(a), \forall a \in A$$

が成り立つとき, M と M' は A 加群として同型である. ただし, $\mathrm{tr}_M(a)$ は k ベクトル空間 M への a の作用の表現行列のトレースを表す.

証明. 証明は付録 (5 節) で与えられる. □

問 2-2-7-1 命題 2-2-6 の条件「S_ρ は有限集合...」の部分を「S_ρ は解析的密度 0 の集合...」にかえても成立するかどうか考えよ (これは [4] の 1 節をみれば成立することがわかる. これより, [20] で扱うような無限個の素点で分岐するようなガロア表現もトレースの値で特徴付けられることがわかる).

定理 2-2-8. 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(V)$ の像は $\mathrm{Aut}_E(V_E)$ に入る. ただし, E は $\mathbb{Q}_\ell$ の有限次拡大で V_E は G_K 不変な V の E 部分空間で $\dim_E V_E = \dim_{\overline{\mathbb{Q}}_\ell} V$ となるものである.

証明. 簡単のため, V の基底 $\{e_i\}$ を固定して, $\mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(V) \simeq \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ と同一視しておく.

$$\mathrm{Im}\rho = \bigcup_{E'/\mathbb{Q}_\ell:\text{有限次拡大}} \mathrm{Im}\rho \cap \mathrm{GL}_n(E')$$

と表示すると, $\mathrm{Im}\rho \cap \mathrm{GL}_n(E')$ は閉集合であり, 右辺の合併は可算無限集合をわたる. 今, $\mathrm{Im}\rho$ はコンパクトなので, 完備距離空間である. 従って, ベールのカテゴリー定理 (Baire category theorem) [9]より少なくとも１つの E' に対して, $\mathrm{Im}\rho \cap \mathrm{GL}_n(E')$ は開集合を含む. よって, $H := \mathrm{Im}\rho \cap \mathrm{GL}_n(E')$ も開集合である. 従って $G_K/\rho^{-1}(H)$ は有限集合だから, そ

[8]連続写像 $H \longrightarrow E \times E,\ h \mapsto (\mathrm{tr}\rho(h), \mathrm{tr}\rho'(h))$ による閉集合 $\Delta_E = \{(x,x) \in E \times E\}$ の逆像だから.

[9]位相空間 X がベール空間であるとは X の可算個の稠密開集合の共通部分は X の中で稠密であるときをいう. ベールの (第一) カテゴリー定理はすべての完備距離空間はベール空間であることを主張し, これより, 空でない完備距離空間が可算個の閉部分集合の合併集合としてかけるとき, 少なくとも１つの閉集合は開集合を含むことがわかる.

の代表系を $\{g_i\}_{i=1}^r$ とし, $\rho(g_i), 1 \leq i \leq r$ のすべての行列成分を E' に添加した体を E とするとこれは E' 上の有限次拡大なので特に $\mathbb{Q}_\ell$ 上の有限次拡大. よって, $\mathrm{Im}\rho \subset \mathrm{GL}_n(E)$ である. あとは $V_E = \bigoplus_i Ee_i$ とおけばよい. □

2.3. **整 ℓ 進表現.** E を $\mathbb{Q}_\ell$ の有限次拡大, $\mathcal{O}$ を E の整数環, π を $\mathcal{O}$ の素元とする. T を $\mathcal{O}$ 上階数 n となる自由加群とし, 指数有限な部分 $\mathcal{O}$ 加群によって, T に位相を入れる. このとき, 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T)$ のことを整 ℓ 進表現と呼ぶ. ただし, $\mathrm{Aut}_{\mathcal{O}}(T)$ には $\mathrm{Map}(T, T)$ のコンパクト開位相からの制限位相を入れる. これは, $\mathcal{O}$ が誘導する位相を備えた位相群 $\mathrm{GL}_n(\mathcal{O})$ と位相同型である.

定理 2-3-1. G_K は有限次 E-ベクトル空間 V に連続に作用しているとき, V の G_K-安定な格子, 即ち, 有限階数自由 $\mathcal{O}$ 加群 T で $T \otimes_{\mathcal{O}} E \simeq V$ となるものが存在する.

証明. $\{e_\lambda\}_\lambda$ を V の基底とし, $T_0 = \bigoplus_\lambda \mathcal{O}e_\lambda$ とおく. T_0 は V の格子である. ここから, G_K-安定な格子を作る. $\rho : G_K \longrightarrow \mathrm{Aut}_E(V)$ を G_K の V への作用が引き起こす連続表現とする. V の局所コンパクト性から $\mathrm{Aut}_{\mathcal{O}}(T_0)$ は $\mathrm{Aut}_E(V)$ は開部分群である. よって, ρ による T_0 の逆像 $H = \{g \in G_K |\ \rho(g)T_0 = T_0\}$ は G_K の開部分群であるので, $[G_K : H]$ は有限である. G_K/H の完全代表系を $\{\gamma_i\}_{i=1}^t$ とする. $T := \sum_{i=1}^t \gamma_i T_0$ とおけば, これが求めるものとなる. 実際, $G_K = \coprod_{i=1}^t \gamma_i H$ なので, 任意の $g \in G_K$ と $\gamma_i, 1 \leq i \leq t$ に対して, $g\gamma_i = \gamma_{k_i}h,\ h \in H,\ 1 \leq k_i \leq t$ と書ける ($\{k_1, \ldots, k_t\} = \{1, \ldots, t\}$). よって,

$$\rho(g)T = \sum_{i=1}^t \rho(g\gamma_i)T_0 = \sum_{i=1}^t \rho(\gamma_{k_i})\rho(h)T_0 = \sum_{i=1}^t \rho(\gamma_{k_i})T_0 = T.$$

□

実は, ℓ 進表現の格子の存在はその連続性と同値であることが簡単にわかる.

命題 2-3-2. V を有限次 E-ベクトル空間とし, $\rho : G_K \longrightarrow \mathrm{Aut}_E(V)$ を群準同型射とする. このとき, ρ が連続, 即ち ℓ 進表現であることと V の G_K-安定な格子が存在することは同値である.

証明. 連続性がそのような格子の存在を導くのは定理 2-3-1 で見た. 逆に, G_K-安定な格子 T が存在したとする. 対応する表現を $\rho' : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_E}(T)$ とすると, $\rho' \otimes_{\mathcal{O}_E} E = \rho$ なので, $\mathrm{Im}\rho \simeq \mathrm{Im}\rho'$ だから, $\mathrm{Im}\rho \subset \mathrm{Aut}_{\mathcal{O}_E}(T)$ としてよい. π を $\mathcal{O}_E$ の素元とし, $n \geq 1$ に対して $U_n := \mathrm{Ker}(\mathrm{Aut}_{\mathcal{O}_E}(T) \overset{\mathrm{mod}\ \pi^n}{\longrightarrow} \mathrm{Aut}_{\mathcal{O}_E/\pi^n\mathcal{O}_E}(T/\pi^nT))$ とおく. U_n は $\mathrm{Aut}_{\mathcal{O}_E}(T)$ の正規部分群であり, 単位元 $1 = \mathrm{id}_T$ の開近傍系を定める. このとき, $G_K/\rho^{-1}(U_n) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_E}(T)/U_n$ より右辺は有限群だから, 左辺も有限群. 従って, G_K の (正規) 部分群 $\rho^{-1}(U_n)$ は G_K の開集合. 任意の $\mathrm{Aut}_{\mathcal{O}_E}(T)$ の開集合は $gU_n,\ g \in \mathrm{Aut}_{\mathcal{O}_E}(T),\ n \geq 1$ の形で生成されるので, それらの引き戻しも開集合. よって, ρ は連続. □

定理 2-3-1 は圏論の言葉を用いると次の様に表現できる.

系 2-3-3. $\mathrm{Rep}_E(G_K)$ を G_K が連続に作用する有限次元 E 加群の成す圏, $\mathrm{Rep}_{\mathcal{O}}(G_K)$ を G_K が連続に作用する有限階数自由 $\mathcal{O}$ 加群の成す圏とする. このとき,

$$\mathrm{Rep}_{\mathcal{O}}(G_K) \longrightarrow \mathrm{Rep}_E(G_K), T \mapsto T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

は**本質的に全射 (essentially surjective)**[10].

例 2-3-4. E/K を楕円曲線とし, $T_\ell(E)$ を ℓ 進テート加群とする (cf. 例 2-2-3). このとき,

$$\rho_\ell : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$$

は整 ℓ 進表現である. 例 2-2-1 で紹介した ℓ 進円分指標 $\chi_\ell : G_K \longrightarrow \mathbb{Z}_\ell^\times$ (やその冪) も整 ℓ 進表現である.

例 2-3-5. X/K を K 上の滑らかな射影的代数多様体とする. このとき,

$$T_\ell := H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_\ell)/(\text{torsion})\ (0 \leq i \leq 2\mathrm{dim}X)$$

は有限階数の自由 $\mathbb{Z}_\ell$ 加群である (cf. 三枝氏の稿). G_K の T_ℓ への作用は整 ℓ 進表現を誘導する.

2.4. **法 ℓ 表現.** $\mathbb{F}$ を位数 ℓ の有限体 $\mathbb{F}_\ell$ の有限次拡大とする ($\mathbb{F}$ は $\mathbb{F}_\ell$ の代数拡大でもよい). $\mathbb{F}$ には離散位相を入れて位相体とみなす. $\overline{V}$ を $\mathbb{F}$ 上の n 次ベクトル空間とする. このとき, 連続表現 $\overline{\rho} : G_K \longrightarrow \mathrm{Aut}_{\mathbb{F}}(\overline{V})$ のことを**法 ℓ 表現**と呼ぶ. $\mathrm{Aut}_{\mathbb{F}}(\overline{V})$ には, コンパクト開位相を入れる. これは, $\mathrm{Aut}_{\mathbb{F}}(\overline{V}) \simeq \mathrm{GL}_n(\mathbb{F})$ とみなすとき, 右辺に離散位相をいれたものと一致する.

法 ℓ 表現は, 次の様に ℓ 進表現および整 ℓ 進表現と関係している. $\rho : G_K \longrightarrow \mathrm{Aut}_E(V)$ を ℓ 進表現とする. このとき, 定理 2-3-1 より, V の G_K 不変 $\mathcal{O}_E$ 格子 T が存在する. このとき,

$$\overline{\rho} : G_K \xrightarrow{\rho} \mathrm{Aut}_{\mathcal{O}_E}(T) \xrightarrow{\mathrm{mod}\ m_E} \mathrm{Aut}_{\mathcal{O}_E/m_E}(T/m_ET)$$

は法 ℓ 表現である. $\overline{\rho}$ のことを ρ の**還元**という. $\overline{\rho}$ は V の格子の取り方に依存しているので標準的な構成ではないがその半単純化 $\overline{\rho}^{ss}$ は格子の取り方によらない (命題 2-4-1 から従う).

整 ℓ 進表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T)$ が与えられると, 係数環 $\mathcal{O}$ の極大イデアル m の冪で還元することによって, ガロア表現の射影系 $\{\overline{\rho}_n : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}/m^n}(\overline{V}_n)\}_n$ を得る. ただし, $\overline{V}_n = V \otimes_{\mathcal{O}} \mathcal{O}/m^n$ とし, ここには離散位相を入れる. 特に $n = 1$ のときは, 法 ℓ 表現

[10]つまり, $\mathrm{Rep}_E(G_K)$ のすべての対象はこの対応による $\mathrm{Rep}_{\mathcal{O}}(G_K)$ のある対象の像と同値である.

$\overline{\rho} = \overline{\rho}_1 : G_K \longrightarrow \mathrm{Aut}_{\mathbb{F}}(\overline{V}_1)$ となっている:

$$\begin{tikzcd}
G_K \arrow[r, "\rho"] \arrow[dr, "\overline{\rho}_n"] \arrow[ddr, "\overline{\rho}:=\overline{\rho}_1"'] & \mathrm{Aut}_{\mathcal{O}}(T) \arrow[d, "\mathrm{mod}\ m^n"] \\
& \mathrm{Aut}_{\mathcal{O}/m^n}(\overline{V}_n) \arrow[d, "\mathrm{mod}\ m"] \\
& \mathrm{Aut}_{\mathbb{F}}(\overline{V}_1)
\end{tikzcd}$$

ただし, $\mathbb{F} := \mathcal{O}/m$. 逆に, ガロア表現の射影系 $\{\rho_n : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}/m^n}(\overline{V}_n)\}_n$ が与えられたとき, 極限をとることで整 ℓ 進表現を構成することができる. すなわち, ガロア表現の射影系と整 ℓ 進表現を考えることは同じである:

$$\left\{\begin{array}{l} \text{整}\,\ell\,\text{進表現} \\ \rho : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(V) \end{array}\right\} \longleftrightarrow \left\{\begin{array}{l} \text{ガロア表現の射影系} \\ \{(\rho_n, \overline{V}_n)\}_n \end{array}\right\}$$

$$\rho = \varprojlim_n \rho_n \longleftrightarrow \{\rho \otimes_{\mathcal{O}} \mathcal{O}/m^n\}_n = \{\rho_n\}_n.$$

このような理解は無限個の素点で分岐する ℓ 進表現の構成においても本質的に重要な役割を果たしている [20].

この節の最後に法 ℓ 表現の同値性判定法を与える.

命題 2-4-1. 法 ℓ 表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{F}}(V)$ の分岐素点の和集合を S とする. 像は有限なので S は有限集合である. このとき, ρ の半単純化 ρ^{ss} は $\mathrm{tr}\wedge^i\rho(\mathrm{Frob}_v),\ v \in \Sigma_K \setminus S,\ i = 1, \ldots, n$ の値で一意的に決まる. 特に, ρ が既約かつ $\ell > \dim_{\mathbb{F}}(V)$ ならば, トレースの値だけで ρ は決まる.

証明. ρ, ρ' を法 ℓ 表現とし, $\mathrm{tr}\wedge^i\rho(\mathrm{Frob}_v) = \mathrm{tr}\wedge^i\rho'(\mathrm{Frob}_v),\ v \in \Sigma_K \setminus S_\rho \cup S_{\rho'},\ i = 1, \ldots, n$ が成り立つと仮定すると, Chebotarev の密度定理から, この等式は任意の G_K の元に対しても成立することがわかる. これより, 問題が次の命題に帰着された. □

命題 2-4-2. k を標数 $p > 0$ の体, A を k-代数とし, M, M' を k 上有限次元の半単純 A 加群とする. $\dim_k(M) = \dim_k(M') =: n$ と仮定する. このとき,

$$\mathrm{tr}_{\wedge^i M}(a) = \mathrm{tr}_{\wedge^i M'}(a), \forall a \in A,\ \forall i = 1, \ldots, n$$

が成り立つならば (この条件は $a \in A$ の固有多項式が一致するということと同じ), M と M' は A 加群として同型である.

証明. 証明は付録 (5 節) で与えられる. □

例 2-4-3. G_K の $\mu_\ell(\overline{K}) \simeq \mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_\ell$ への作用が定める 1 次元法 ℓ 表現

$$\overline{\chi}_\ell : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Z}/\ell\mathbb{Z}}(\mu_\ell(\overline{K})) \simeq \mathbb{F}_\ell^\times$$

のことを**法 ℓ 円分指標**という. これは整 ℓ 表現 χ_ℓ の還元になっている.

例 2-4-4. 例 2-2-3 でみたように G_K は楕円曲線 E の ℓ 等分点の成す群 $E[\ell](\overline{K})$ に作用する．これが定める表現

$$\overline{\rho}_{E,\ell} : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Z}/\ell\mathbb{Z}}(E[\ell](\overline{K})) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

は法 ℓ 表現であり, 例 2-3-4 の整 ℓ 進表現の還元となっている．

問 2-4-5. K を代数体とする．このとき, 1 次元連続表現 $\rho : G_K \longrightarrow \overline{\mathbb{F}}_\ell^\times$ が有限指標と法 ℓ 円分指標の冪との積で表せることを示せ (ヒント: G_K のコンパクト性から $\mathrm{Im}\rho$ は有限群, また 1 次元なのでアーベル商を経由することから, ρ はある巡回群 $(\mathbb{Z}/N\mathbb{Z})^\times$ を経由．あとは $N = \ell^t M$, $p \nmid M$ と分けて考えればよい．像の標数が ℓ なので $t = 1$ となることに注意).

2.5. **大きな環を係数にもつガロア表現.** h 変数の $\mathbb{Z}_p$ 係数形式冪級数環 $\Lambda = \mathbb{Z}_p[[T_1, \ldots, T_h]]$ を考える．環 Λ に極大イデアル $(p, T_1, \ldots, T_h)$ の冪を零元の開近傍系とすることによって位相を入れる．Λ のように大きな環を係数に持つような場面がガロア表現の変形理論で登場する．以下にそのことを簡単にみる．

S を代数体 K の素点から成る有限集合とし, $G_{K,S}$ を K の S 外不分岐最大拡大のガロア群とする．法 p 表現 $\overline{\rho} : G_{K,S} \longrightarrow \mathrm{GL}_n(\mathbb{F}_p)$ を考える．剰余体が $\mathbb{F}_p$ である完備ネーター局所代数 (A, m_A) と連続表現 $\rho : G_{K,S} \longrightarrow \mathrm{GL}_n(A)$ の組 (ρ, A) で, 次の可換図式を満たすもののことを $\overline{\rho}$ の**持ち上げ (lift)** という:

$$\begin{tikzcd} G_{K,S} \arrow[r, "\rho"] \arrow[dr, "\overline{\rho}"'] & \mathrm{GL}_n(A) \arrow[d, "\mathrm{mod}\ m_A"] \\ & \mathrm{GL}_n(\mathbb{F}_p) \end{tikzcd}$$

このような持ち上げの普遍性を満たす “最大の” A を $\overline{\rho}$ の普遍変形環と呼び, $R(\overline{\rho})$ と表し, また対応する普遍表現を ρ^{univ} と表す．つまり, A への任意の持ち上げ ρ に対して, 環準同型 $R(\overline{\rho}) \overset{\iota}{\longrightarrow} A$ が存在して, 次の可換図式が成立する:

$$\begin{tikzcd} G_{K,S} \arrow[r, "\rho^{\mathrm{univ}}"] \arrow[dr, "\rho"] \arrow[ddr, "\overline{\rho}"'] & \mathrm{GL}_n(R(\overline{\rho})) \arrow[d, "\iota"] \\ & \mathrm{GL}_n(A) \arrow[d, "\mathrm{mod}\ m_A"] \\ & \mathrm{GL}_n(\mathbb{F}_p) \end{tikzcd}$$

この環を取り巻く詳細な研究は Mazur が (肥田理論からの動機を受けて) 行っており, Mazur の変形理論として定着している．普遍変形環はいつでも存在するわけではないが, $\overline{\rho}$ の条件によっていつ存在するかはよくわかっている．この環は Λ/I (I は Λ の閉イデアル) の形をしており, その Krull 次元 $\leq h$ は $\overline{\rho}$ に付随する随伴表現のガロアコホモロジーを用いて計算される．変形環については今井 直毅氏によって解説されるが, 佐藤 周友氏によるガロアコホモロジーの概説も併せて参照されたい．またその動機となった肥田理論については落合 理氏によって紹介がなされる [10].

普遍変形環を幾何的に扱う試みも進んでいる．$R(\overline{\rho})$ から剛解析的空間 (rigid analytic space)$\mathfrak{X}$ を付随させる手続きが存在し, その E 値点 $\mathfrak{X}(E)$, (E は $\mathbb{Q}_p$ の有限次拡大) は $\overline{\rho}$ の変形である E 上の p 進表現全体を与えている．そのような p 進表現 ρ が保型的であるような点が剛解析空間 $\mathfrak{X}$ の中でどのように分布しているかを調べることは, ガロア表現の変形を理解する上で非常に重要である．これに関連する話題は佐々木 秀氏, 山上 敦士氏によって解説される．

2.6. **Artin 表現.** K を $\mathbb{Q}$ の有限次拡大とし, V を $\mathbb{C}$ 上の有限次ベクトル空間とする．このとき, 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{C}}(V)$ のことを **Artin 表現**と呼ぶ．右辺には今までと同様に, コンパクト開位相の制限位相を入れる．いま, V の基底を固定すると, $\mathrm{Aut}_{\mathbb{C}}(V) \simeq \mathrm{GL}_n(\mathbb{C}) \subset M_n(\mathbb{C}) \simeq \mathbb{C}^{n^2}$ を得る．これにより, $\mathrm{Aut}_{\mathbb{C}}(V)$ には $\mathbb{C}^{n^2}$ の通常の距離空間としての位相の制限位相が入るが, これはコンパクト開位相と一致する．

連続性に加えて, 既約性を仮定したり, $\rho(c)$, (c 複素共役) の形に条件を付けたりする場合がある．例えば, 2 次の Artin 表現 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$ には連続性に加えて既約性を課すことが多い．さらに, ρ が奇 (odd), つまり, $\det(\rho(c)) = -1$ を仮定すると, この表現は重さ 1, Neben-type 保型形式に付随するガロア表現と同値であると予想されている[11].

定理 2-6-1. 記号は上のものと同じであるとする．このとき, 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{C}}(V)$ の像は有限.

証明. G_K を一般の副有限群に変えても同様に成立. 証明を一言で述べると, 「G_K のコンパクト性と両者の位相が整合しないため」となる.

V の基底を固定し, $\mathrm{Aut}_{\mathbb{C}}(V)$ と $\mathrm{GL}_n(\mathbb{C})$ を同一視して話を進める．$\mathrm{GL}_n(\mathbb{C}) \supset B^\circ$ を中心 I_n(単位元), 半径 $\dfrac{1}{2}$ の開球とする．このとき, $\rho^{-1}(B^\circ)$ は開集合であり, 単位元を含むので, G_K の開部分群 H で $\rho(H) \subset B^\circ$ となっているものがとれる．このとき, $\rho(H) = \{I_n\}$ を示す (副有限群の位相から $[G : H] < \infty$ なので, 主張を得る).

$\rho(H) \ni T \neq I_n$ が存在したとする．$M_n(\mathbb{C}) = \mathrm{End}(\mathbb{C}^n)$ によって, 作用素ノルム $|| \cdot ||$ を $\mathrm{GL}_n(\mathbb{C})$ に入れる．この位相と元の位相は同じである．T の固有値がすべて 1 のとき, Jordan 分解により, $||T^N - I_n|| > \dfrac{1}{2}$ を満たす整数 N が取れる．そうでないときは, T の固有値 α で, $|\alpha^N - 1| > \dfrac{1}{2}$ を満たす整数 N が取れる．よって, $T^N \notin B^\circ$ なので矛盾. □

この定理より Artin 表現を考える場合, 係数体にあらかじめ離散位相を入れて議論しても何もかわらないことがわかる.

系 2-6-2. 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{C}}(V)$ は半単純表現である．また, ρ が分岐する K の素点は有限個である.

命題 2-6-3. 連続表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{C}}(V)$ の分岐素点の成す集合を S_ρ とおく (系 2-6-2 より $\sharp S_\rho < \infty$)．このとき, ρ は $\mathrm{tr}\rho(\mathrm{Frob}_v)$, $v \in \Sigma_K \setminus S_\rho$ の値で一意的に決まる．ただし, $\mathrm{tr}\rho(\mathrm{Frob}_v)$ は行列 $\rho(\mathrm{Frob}_v)$ のトレースを意味する.

---

[11] $K = \mathbb{Q}$ の場合, 多くの研究の後、$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{C})$ に対する Artin 予想は Khare と Wintenberger による Serre 予想の解決の系として, 現在では完全に解決されている.

証明. 二つの連続表現 $\rho, \rho' : G_K \longrightarrow \mathrm{Aut}_{\mathbb{C}}(V)$ が $\mathrm{tr}(\rho(\mathrm{Frob}_v)) = \mathrm{tr}(\rho'(\mathrm{Frob}_v)), \forall v \in \Sigma_K \setminus S_\rho \cup S_{\rho'}$ を満たすとき, $\rho \sim \rho'$ を示せば良い. ρ, ρ' の像に対応する K の拡大体の合併を L とすると, L/K 有限次拡大でその分岐素点の集合は $S := S_\rho \cup S_{\rho'}$ に含まれる. L/K に Chebotarev の密度定理を適用すると, 各 $\sigma \in \mathrm{Gal}(L/K)$ に対して, $v \in \Sigma_K \setminus S$ が存在して, $\mathrm{Frob}_v = \sigma$ となる. よって, $\mathrm{tr}(\rho(\sigma)) = \mathrm{tr}(\rho'(\sigma)), \forall \sigma \in \mathrm{Gal}(L/K)$ が成り立つので, 有限群の線形表現の一般論 (cf. [13], p.17 の定理 3) から, $\rho \sim \rho'$ を得る. $\square$

例 2-6-3. L を多項式 $F(x) = x^3 + ax + b, a, b \in \mathbb{Q}$ の分解体で, そのガロア群が 3 次対称群 $\mathfrak{S}_3 = \langle \sigma, \tau | \ \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ と同型であるものとする. $\iota : \mathfrak{S}_3 \longrightarrow \mathrm{GL}_2(\mathbb{C})$ を

$$\iota(\sigma) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}, \ \iota(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

によって定義する. ただし, $\zeta_3 = e^{\frac{2\pi\sqrt{-1}}{3}}$. このとき,

$$\rho : G_{\mathbb{Q}} \overset{L\text{ への制限}}{\longrightarrow} \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_3 \overset{\iota}{\longrightarrow} \mathrm{GL}_2(\mathbb{C})$$

は 2 次元 (既約)Artin 表現である. $F(x)$ の判別式が負ならば, $\det\rho(c) = \det\iota(\tau) = -1$ が成り立つ. $F(x)$ の判別式が正ならば, ρ は **Maass 形式 (Maass form)** と対応するであろうと期待されている (cf. [18]).

問 2-6-4. $K = \mathbb{Q}(\sqrt{-47})$ の Hilbert 類体を H とする.
(1) K の類数が 5 であること, 及び, H は多項式 $F(x) = x^5 - x^4 + x^3 + x^2 - 2x + 1$ の分解体 K_F であることを示せ ([22] を参照). また, $\mathrm{Gal}(H/\mathbb{Q}) \simeq D_5$ であることも示せ.
(2) $A = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 12 \end{pmatrix}$, $B = \begin{pmatrix} 3 & \frac{1}{2} \\ \frac{1}{2} & 4 \end{pmatrix}$, $C = \begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & 6 \end{pmatrix}$ に対応するテータ級数をそれぞれ $\theta_A, \theta_B, \theta_C$ とおく: $\theta_A(\tau) = \sum_{m,n \in \mathbb{Z}} q^{m^2+mn+12n^2}$, $\theta_B(\tau) = \sum_{m,n \in \mathbb{Z}} q^{3m^2+mn+4n^2}$, $\theta_C(\tau) = \sum_{m,n \in \mathbb{Z}} q^{2m^2+mn+6n^2}$. このとき,

$$f(\tau) := \theta_A(\tau) - \Big(\frac{1+\sqrt{5}}{2}\Big)\theta_B(\tau) - \Big(\frac{1-\sqrt{5}}{2}\Big)\theta_C(\tau) \in S_1(\Gamma_0(47), \chi), \ \chi = \Big(\frac{-47}{*}\Big)$$

であることを示せ. また, f は正規化された Hecke 固有尖点形式になっていることも示せ (テータ級数に関しては [11] の 6 章をそれが正規化された Hecke 固有尖点形式になることは [1] の p.204 をそれぞれ参照).
(3) $D_5 = \langle \sigma, \tau \rangle | \ \sigma^5 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ と表示するとき, σ を $\begin{pmatrix} \zeta_5 & 0 \\ 0 & \zeta_5^{-1} \end{pmatrix}$, τ を $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ に対応させることで例 2-6-3 のようにして $\mathrm{Gal}(H/\mathbb{Q})$ の Artin 表現 ρ を得る. ρ が f に付随するガロア表現 ρ_f(cf. [4], [5]) と同値であることを認めて, 多項式 F の法 p 還元の分解法則を f の p 番目のフーリエ係数の言葉で記述せよ.

3. 局所体の絶対ガロア群の線形表現

ℓ を素数とし, 以下固定する. K を代数体とする. 各素数 p の上の素点 $v \in \Sigma_K$ ごとに埋め込み $\overline{K} \hookrightarrow \overline{K_v}$ を固定する. これにより, 閉埋め込み

$$G_{K_v} := \mathrm{Gal}(\overline{K_v}/K_v) \hookrightarrow G_K,\ \sigma \mapsto \sigma|_{\overline{K}}$$

を得る. G_K の中で G_{K_v} は G_K の v での分解群 $D_{K,v}$ と同一視される (cf. 2.1 節). また, 埋め込みの取り替えは G_K の部分群として互いに共役となる. いま, G_K の ℓ 進表現 $\rho : G_K \longrightarrow \mathrm{Aut}_E(V)$ が与えられたとき, その G_{K_v} への制限 $\rho|_{G_{K_v}}$ を考えることで, 大域体の絶対ガロア群の表現から自然に局所体の絶対ガロア群の表現が得られる. このようにして, 大域体のガロア表現を局所的に調べることができる. 素点 v が ℓ を割らない場合は比較的易しく調べる道具も揃っている. 素点 v が ℓ を割る場合は [8] で登場する p 進 Hodge 理論を用いて調べることができる.

3.1. **局所体の絶対ガロア群の ℓ 進表現, 整 ℓ 進表現, 法 ℓ 表現.** 素数 ℓ を固定し, $p \neq \ell$ を素数とする. 以下, この節では K を $\mathbb{Q}_p$ の有限次拡大, E を $\mathbb{Q}_\ell$ の有限次拡大とする. K の剰余体を $\mathbb{F}$ とする. 2-1 節で見たように全射 $G_K \longrightarrow G_{\mathbb{F}}$ の核を I_K と書く:

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow G_{\mathbb{F}} \longrightarrow 1$$

[9] の 3 節で述べられているように $I_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{ur}}),\ K^{\mathrm{ur}} = \bigcup_{p \nmid n} K(\zeta_n)$ である. ただし, $\zeta_n \in \overline{K}$ は 1 の原始 n 乗根である. 先に進む前に, G_K や I_K の構造について, もう少し詳しく復習しておく. K の素元 π を固定し, $K^{\mathrm{tm}} := \bigcup_{p \nmid n} K^{\mathrm{ur}}(\pi^{\frac{1}{n}})$ を K の**最大馴分岐拡大** **(maximal tamely ramified extension)** とすると, 対応するガロア群の列が正規列となるような体拡大の列

$$K \subset K^{\mathrm{ur}} \subset K^{\mathrm{tm}} \subset \overline{K}$$

$$G_K \supset I_K \supset P_K \supset \{1\}$$

を得る. I_K の最大副 p 部分群 $P_K := \mathrm{Gal}(\overline{K}/K^{\mathrm{tm}})$ のことを**暴惰性群 (wild inertia)** といい, その商 $I^t := I_K/P_K = \mathrm{Gal}(K^{\mathrm{tm}}/K^{\mathrm{ur}})$ のことを**馴惰性群 (tame inertia group)** という. このとき次の可換図式を得る (横は完全列である):

$$\begin{tikzcd}
1 \arrow[r] & I_K \arrow[r] \arrow[d] & G_K \arrow[r] \arrow[d] & G_{\mathbb{F}} \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & I^t \arrow[r] & G_K/I_P = \mathrm{Gal}(K^{\mathrm{tm}}/K) \arrow[r] & G_{\mathbb{F}} \arrow[r] & 1
\end{tikzcd}$$

また,

$$I^t = \varprojlim_{p \nmid n} \mathrm{Gal}(K^{\mathrm{ur}}(\pi^{\frac{1}{n}})/K^{\mathrm{ur}}) \simeq \varprojlim_{p \nmid n} \mathbb{Z}/n\mathbb{Z}(1) = \prod_{\text{素数 } r \neq p} \mathbb{Z}_r(1)$$

なので, I^t の位相的生成元 τ と $G_{\mathbb{F}}$ の位相的生成元の G_K/P_K への持ち上げ σ は関係式

$$\sigma\tau\sigma^{-1} = \tau^{\chi_\ell(\tau)}$$

を (G_K/P_K の中で) 満たす.

復習はこの辺りで止め, 本題に入る. G_K の連続表現 $\rho : G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K) \longrightarrow \mathrm{Aut}_E(V)$ のことを大域体の場合と同様に ℓ 進表現と呼ぶ. 整 ℓ 進表現や法 ℓ 進表現も同様に定義される.

三枝氏の稿 [7] でも説明されているが, ℓ 進表現 V がエタールコホモロジーを通して代数多様体 X から得られている時 (例えば, 例 2-2-3), V には X の性質が反映されている. Grothendieck はSGA 7-I において K 上のアーベル多様体 A の還元の様子は対応する ℓ 進表現 $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ の性質に完全に焼き直すことができることを示した. これらすべての性質は ℓ 進表現の惰性群への制限 $\rho|_{I_p}$ によって統制される. その動機となったのが次の定理である. この定理は [15] の Appendix で証明されている. 実際には, もう少し一般の設定でも成立するが, それについてはSGA 7-I の Deligne の解説 [2] を参照されたい.

定理 3-1-1.(Grothendieck のモノドロミー定理[12]) $v \not| \ell$ のとき, $\rho(I_K)$ の元はすべて擬冪単行列 (quasi-unipotent matrix) である[13].

証明. $\mathcal{O}_E$ を E の整数環, π を素元とする. D_v はコンパクトなので, ρ の連続性から $\mathrm{Im}\rho$ はコンパクト. よって, ある整数 $a_1, \ldots, a_r \geq 0$ と点 $x_1, \ldots, x_r \in \mathrm{GL}_n(E)$ が存在して, $\mathrm{Im}\rho = \bigcup_{i=1}^r (x_i + \pi^{a_i}\mathrm{M}_n(\mathcal{O}_E))$ とできる. 右辺は $\mathrm{GL}_n(\mathcal{O}_E)$ 上指数有限なので, K の有限次拡大 L をとれば, $\rho|_{G_L}$ は $\mathrm{GL}_n(\mathcal{O}_E)$ に含まれると仮定してよい. 整数 $k \geq 1$ に対して, $I_n + \pi^k\mathrm{M}_n(\mathcal{O}_E)$ は $\mathrm{GL}_n(\mathcal{O}_E)$ の中で指数有限なので, さらに, L の有限次拡大 M をとれば, すべての元 $g \in \rho(G_M)$ は $g \equiv I_n \bmod \pi^k$ を満たすと仮定してよい.

よって, 最初から $\mathrm{Im}\rho$ の任意の元 g は $g \in I_n + \pi^k\mathrm{M}_n(\mathcal{O}_E)$ を満たすとしてよい. この条件より, $\mathrm{Im}\rho$ は副 ℓ 群であることがわかる. 以下では, $\mathrm{Im}\rho$ の勝手な元は冪単行列であること示す. P_K を I_K の最大副 p 群とするとき, $\rho(P_K) = \{I_n\}$ だから, $\rho|_{I_K}$ は $I^t := I_K/P_K$ を経由する. $\mathbb{F}$ を K の剰余体とし, 次の完全列

$$1 \longrightarrow I^t = \mathrm{Gal}(K^{\mathrm{tm}}/K^{\mathrm{ur}}) \longrightarrow \mathrm{Gal}(K^{\mathrm{tm}}/K) \longrightarrow \mathrm{Gal}(K^{\mathrm{ur}}/K) = G_{\mathbb{F}} \longrightarrow 1$$

を考えると, $G_{\mathbb{F}} \ni t$ は $s \in \mathrm{Gal}(K^{\mathrm{tm}}/K^{\mathrm{ur}})$ に共役に作用し[14], $\mathrm{Gal}(K^{\mathrm{tm}}/K)$ の中で ℓ 進円分指標 $\chi_\ell : G_{\mathbb{F}} \longrightarrow \mathbb{Z}_\ell^*$ を用いて, $tst^{-1} = s^{\chi_\ell(t)}$ と表せる (cf. [9]). これより, $\rho(tst^{-1}) = \rho(s^{\chi_\ell(t)}) = \rho(s)^{\chi_\ell(t)}$ を得る (最後の等式には ρ の連続性を用いている).

$X = \log\rho(s)$ とおく,

$$X \overset{\text{共役}}{\sim} \rho(t)X\rho(t)^{-1} = \log\rho(s)^{\chi_\ell(t)} = \chi_\ell(t)X.$$

$a_i(X)$ を X の固有値達のなす i 次対称関数とすると,

$$a_i(X) = a_i(\chi_\ell(t)X) = \chi_\ell(t)^i a_i(X)$$

[12]Grothendieck の有限性定理とも呼ばれる.

[13]正方行列 A が擬冪単行列であるとは, ある整数 $m, n \geq 1$ が存在して, $(A^m - I)^n = 0$ となるときをいう. ただし, I は単位行列. これはすべての固有値が 1 の冪根になることと同じである.

[14]$G_{\mathbb{F}} = \mathrm{Gal}(K^{\mathrm{ur}}/K)$ の元を K^{ur} に一旦延長させてから $\mathrm{Gal}(K^{\mathrm{tm}}/K^{\mathrm{ur}})$ に内部自己準同型として作用させる.

が成り立つ．いま K の剰余体 $\mathbb{F}$ は有限体なので，χ_ℓ の像は無限群．従って，各 i ごとに $\chi_\ell(t)^i \neq 1$ となる t がとれる．よって，$a_i(X)=0,\ i \geq 0$．よって，X の固有値はすべて 0 なので，$X^n=0$．最初の所でとった整数 k を $\exp\log\rho(s)=\rho(s)$ が成り立つ様に予め十分大きくとっておくと，$\rho(s)=\exp X=\displaystyle\sum_{j=0}^{n-1}\frac{X^j}{j!}$ となり，冪単行列であることがわかる． □

命題 3-1-2. $p \neq \ell$ のとき，$\rho(P_K)$ は有限群.

証明. G_K はコンパクトなので，K を有限次拡大 L で取り替えることにより，$\mathrm{Im}\rho|_{G_L}$ は副 ℓ 群 に含まれていると仮定してよい．一方，$\rho|_{G_L}(P_K\cap G_L)$ は副 p 群なので，自明な群となる．$[G_K,G_L]<\infty$ なので，$\rho(P_K)$ は有限群である． □

注意 3-1-3.(1) $p=\ell$ のとき，多くの場合，$\rho(P_K)$ の元は擬冪単行列 (quasi-unipotent matrix) にはならない．例えば，ρ がエタールコホモロジーを通して代数幾何多様体から得られる場合などは決してそうはならない．実際，P_K は有限群と $\mathbb{Z}_p$ の直積群の形にかいたとき，$\mathbb{Z}_p$ の位相的生成群 γ を 1 つ固定し，$\log_p\rho(\gamma^a)$ が意味をもつように十分大きな正整数 a をとると，$\dfrac{\log_p\rho(\gamma^a)}{\log_p\chi_p(\gamma^a)}$ の固有値は ρ の**一般化された Hodge-Tate 重み**と一致する (中村氏の稿 [8] を参照).

(2) 定理 3-1-1 の直前でも説明したように局所体の絶対ガロア群の ℓ 進表現の惰性群への制限は，それが幾何的性質を反映しているということから，リーマン面の基本群の表現 (モノドロミー表現) の類似と思われている．例えば，$\{X_z\}_z$ を開円板 $D:=\{z\in\mathbb{C}|\ |z|<1\}$ 上のリーマン面の族で，$z\in D\setminus\{0\}$ でのファイバーは種数 1 の複素トーラスになっているものとする．$z=0$ のファイバー X_0 がどのような (位相幾何的) 振る舞いをしているかどうかは位相的基本群 $\pi_1^{\mathrm{top}}(D\setminus\{0\},z)=\langle\gamma_0\rangle\simeq\mathbb{Z}$ の 1 次ホモロジー群 $H_1(X_z,\mathbb{Z})\simeq\mathbb{Z}^{\oplus 2}$ への作用で決まる．ただし，γ_0 は点 z を基点として，0 を一周する道である．よって，$z=0$ のまわりでの (整) モノドロミー表現

$$\rho_z^{\mathrm{top}}:\pi_1^{\mathrm{top}}(D\setminus\{0\},z)\longrightarrow \mathrm{Aut}_{\mathbb{Z},\,\text{向き}}(H_1(X_z,\mathbb{Z}))=\mathrm{SL}_2(\mathbb{Z}).$$

を得る．γ_0 の作用の表現行列を $x=0$ でのまわりのモノドロミー行列という (cf. [3] の第 II 部 4 章)．モノドロミー行列が自明なら X_0 は種数 1 の複素トーラスであるが，そうでない場合，X_0 は退化した複素トーラス (の組み合わせ) となる．

この表現 ρ_z^{top} はガロア表現側では次のような状況に対応している．$E_{\mathbb{Q}_p}$ を $\mathbb{Q}_p$ 上の楕円曲線とし，$E_{\mathbb{Q}_p^{\mathrm{ur}}}$ を $\mathbb{Q}_p^{\mathrm{ur}}$ への基底変換とする．$\mathbb{Q}_p^{\mathrm{ur}}$ の整数環を $\mathbb{Z}_p^{\mathrm{ur}}$ とする．その極大イデアルは有理素数 p で生成される．$E_{\mathbb{Q}_p^{\mathrm{ur}}}$ の $\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}}$ 上の Néron モデルを $\mathcal{E}$ とする (cf. [16] の Appendix C を参照)．$\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}}$ は二点 $\{(p),(0)\}$ からなり，それらは，$p_0=\mathrm{Spec}\,\overline{\mathbb{F}}_p,\ p_1=\mathrm{Spec}\,\mathbb{Q}_p^{\mathrm{ur}}$ にそれぞれ対応する．$\mathcal{E}$ は $\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}}$ 上の代数曲線の (数論的な) 族と思うことができ，Spec $\mathbb{Z}_p^{\mathrm{ur}}\setminus\{p_0\}=\{p_1\}$ 上のファイバーは楕円曲線 $E_{\mathbb{Q}_p^{\mathrm{ur}}}$ である．p_0 でのファイバーの幾何的様子は数論的基本群

$$\pi_1(\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}}\setminus\{p_0\})=\pi_1(\mathrm{Spec}\,\mathbb{Q}_p^{\mathrm{ur}})=\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ur}})=I_{\mathbb{Q}_p}$$

の $T_\ell(\mathcal{E}_{p_1}) = T_\ell(E_{\mathbb{Q}_p^{\mathrm{ur}}})$ への作用で決まる:

$$\rho_\ell : I_{\mathbb{Q}_p} \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(T_\ell(E_{\mathbb{Q}_p^{\mathrm{ur}}})).$$

さらに, ρ_ℓ を $\mathbb{Q}_p^{\mathrm{ur}}$ の適当な有限次拡大の絶対ガロア群に制限すればこの射は $I_{\mathbb{Q}_p}$ の最大副 ℓ 商 $\mathbb{Z}_\ell(1)$ を経由し, この位相的生成元の適当な冪がモノドロミー行列を定めたのであった.

位相幾何	数論幾何
$D = \{z \in \mathbb{C} \mid \lvert z\rvert < 1\}$	$\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}}$
原点 0	$p_0 = \mathrm{Spec}\,\overline{\mathbb{F}}_p$
$\pi_1^{\mathrm{top}}(D \setminus \{0\}, z) \simeq \mathbb{Z} \ni \gamma_0$	$\pi_1(\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}} \setminus \{p_0\}) = I_{\mathbb{Q}_p}$ の最大副 ℓ 商 $\mathbb{Z}_\ell(1) \ni \gamma$
$\{X_t\}_{t\in D}$	$\mathcal{E}_{\mathrm{Spec}\,\mathbb{Z}_p^{\mathrm{ur}}}$
$H_1(X_z, \mathbb{Z}) \simeq \mathbb{Z}^{\oplus 2}$	$T_\ell(\mathcal{E}_{p_1}) = T_\ell(E_{\mathbb{Q}_p^{\mathrm{ur}}}) \simeq \mathbb{Z}_\ell^{\oplus 2}$

3.2. **Weil-Deligne 表現.** この節では Grothendieck のモノドロミー定理の応用として, Weil 群の表現と Weil-Deligne 表現との対応を与える. これは局所 Langlands 対応の記述に必要とされる. Langlands 対応の詳細やそれに纏わる話については吉田氏の稿を参照. また三枝氏の稿の 3 節にも解説がある.

ℓ と p 素数とし, $K/\mathbb{Q}_p, E/\mathbb{Q}_\ell$ をそれぞれ局所体とする. $\mathbb{F}$ を K の剰余体とし, $q := \sharp\mathbb{F}$ をその位数とする. このとき, 完全列

$$1 \longrightarrow I_K \longrightarrow G_K \xrightarrow{\iota} G_{\mathbb{F}} \longrightarrow 1$$

を思い出す. 位相的生成元 $\mathrm{Frob}_q \in G_{\mathbb{F}} \simeq \widehat{\mathbb{Z}}$ を固定し, その $\mathbb{Z}$-span $\mathrm{Frob}_q^{\mathbb{Z}} = \{\mathrm{Frob}_q^n \mid n \in \mathbb{Z}\}$ の ι による逆像を W_K と書き, K の **Weil 群**という:

$$1 \longrightarrow I_K \longrightarrow W_K \xrightarrow{\iota} \mathrm{Frob}_q^{\mathbb{Z}} \simeq \mathbb{Z} \longrightarrow 1.$$

$\mathbb{Z}$ は $G_{\mathbb{F}} \simeq \widehat{\mathbb{Z}}$ の中で稠密なので, W_K は G_K の稠密部分群であることがわかる.

$1 \in \mathbb{Z}$ に対応する W_K の元 Φ をひとつ取り固定すると, Weil 群 W_K は $W_K = \coprod_{n\in\mathbb{Z}} \Phi^n I_K$ と書ける. 惰性群 I_K には G_K からの誘導位相が入っておりこれにより, (W_K を I_K の可算個のコピーと思うことで)W_K に位相を入れる.

有限次元 E ベクトル空間 V を考え, 勝手な ℓ 進表現 $\rho : G_K \longrightarrow \mathrm{Aut}(V)$ から W_K の連続表現を次のように対応させる.

先ず, 非自明な連続準同型 $t_\ell : I_K \longrightarrow \mathbb{Q}_\ell$ を考える. I_K はコンパクトなので適当な $c \in \mathbb{Q}_\ell$ が存在して, $c \cdot t_\ell(I_K) = \mathbb{Z}_\ell$ とできる. 実際, $\mathrm{Im}\,t_\ell$ は副 ℓ 群なので, P_K を K の最大副 p 部分群とすると, $p \neq \ell$ なので t_ℓ は $I^t := I_K/P_K$ を経由する. ここで, 同型

$$I_K/P_K \simeq \prod_{\text{素数 } r\neq p} \mathbb{Z}_r(1)$$

を思い出すと ([9]), t_ℓ は副 ℓ 群 $\mathbb{Z}_\ell(1)$ を経由するので, t_ℓ は $\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_\ell(1), \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ の非ゼロ元に対応. このことから上述のことがわかる.

そこで, 非自明な連続準同型 $t_\ell : I_K \longrightarrow \mathbb{Q}_\ell$ を固定し, $c \in \mathbb{Q}_\ell$ で $c \cdot t_\ell(I_K) = \mathbb{Z}_\ell$ なるものを取っておく[15]. さらに, $\gamma^c \in I_K$ を $1 \in \mathbb{Z}_\ell = c \cdot t_\ell(I_K)$ に対応する元とする.

以下この節の終わりまでは $p \neq \ell$ と仮定する. すると, Grothendieck のモノドロミー定理 (定理 3-1-1) の証明と P_K の ρ による像は有限であることから (命題 3-1-2), I_K の正規開部分群 I' をとれば $\rho(I')$ は副 ℓ 群である. よって, $\rho|_{I'}$ は I_K/P_K の副 ℓ 群を経由するので $\sigma \in I'$ に対して $\sigma = \gamma^{c\cdot t_\ell(\sigma)}$ と表される. 特に, $\gamma^{c\cdot t_\ell(\gamma)} = \gamma^1 = \gamma$ となる. よって,

$$\rho(\sigma) = \rho(\gamma^{c\cdot t_\ell(\sigma)}) = \rho(\gamma)^{c\cdot t_\ell(\sigma)} = \exp(t_\ell(\sigma)N),\ N = c\log(\rho(\gamma)).$$

定理 3-1 より, N は巾零行列であった.

上で説明したように, W_K の元は $\Phi^n\sigma, n \in \mathbb{Z}, \sigma \in I_K$ と一意的に書ける. そこで, ρ に対して, W_K の表現 r を

$$r(\Phi^n\sigma) := \rho(\Phi^n\sigma)\exp(-t_\ell(\sigma)N)$$

で定める. $\sigma \in I'$ に対して,

$$r(\sigma) = \rho(\sigma)\exp(-t_\ell(\sigma)N) = \rho(\sigma)\exp(-\log\rho(\gamma)^{ct_\ell(\sigma)}) = \rho(\sigma)\exp(-\log\rho(\sigma)) = 1$$

なので, $r(I)$ は有限群である. また $g \in W_K, \sigma \in I_K$ に対して関係式,

$$g\sigma g^{-1} = \sigma^{\chi_\ell(g)} \bmod P_K$$

から, $t_\ell(g\sigma g^{-1}) = \chi_\ell(g)t_\ell(\sigma)$. 任意の $g \in W_K$ に対して,

$$\begin{aligned}\rho(g)N\rho(g)^{-1} = \rho(g)(c\log(\rho(\gamma)))\rho(g)^{-1} &= \log(\rho(g\gamma^c g^{-1})))\\ &= \log\rho(\gamma^{ct_\ell(g\gamma^c g^{-1})}) = \log\rho(\gamma^{c\chi_\ell(g)}) = \chi_\ell(g)N\end{aligned}$$

を得る. よって, 定義から

$$r(g)Nr(g)^{-1} = \chi_\ell(g)N,\ g \in W_K$$

を得る. 簡単に確認できることではあるが, r は Φ や t_ℓ の取り方に依らない.

定義 3-2-1.$K/\mathbb{Q}_p$ を有限次拡大, その剰余体の位数を q とする. Ω を標数 0 の代数閉体とし, V を Ω 上の有限次元ベクトル空間とする. このとき, **Weil-Deligne 表現**/Ω とは K の Weil 群 W_K のスムーズ表現 $r : W_K \longrightarrow \mathrm{Aut}_\Omega(V)$ [16] と $N \in \mathrm{End}_\Omega(V)$ との組で, $g = \Phi^n\sigma, n \in \mathbb{Z}, \sigma \in I_K$ と表すとき

$$r(g)Nr(g)^{-1} = q^nN$$

を満たすものとして定義する[17].

---

[15]K の素元 π を固定し, π の ℓ^n 乗根の成す系 $\{\pi^{\frac{1}{\ell^n}}\}_n$ に I_t を $\sigma \mapsto \frac{\sigma(\pi^{\frac{1}{\ell^n}})}{\pi^{\frac{1}{\ell^n}}}$ によって作用させることで, 全射連続準同型 $I^t \longrightarrow \mathbb{Z}_\ell(1) \simeq \mathbb{Z}_\ell$ を得る. t_ℓ としてはこの準同型をとればよい.

[16]任意の V の元 v に対し, その固定化部分群 $\{\sigma \in W_K |\ r(\sigma)v = v\}$ は W_K の開集合.

[17]三枝氏や吉田氏の稿ではフロベニウス元 は幾何的フロベニウス元 $\mathrm{Frob}_q^{\mathrm{geom}} : x \mapsto x^{\frac{1}{q}}$ を意味するので, $r(g)Nr(g)^{-1} = q^{-n}N$ となり q の冪の符号が変わることに注意.

定理 3-2-2. $\ell \neq p$ のとき, 次の圏の間に 1 対 1 の対応が存在:

$$\left\{\begin{array}{l}\text{Weil 群 } W_K \text{ の連続表現}/\overline{\mathbb{Q}}_\ell \\ \rho : W_K \longrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(V)\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{l}\text{Weil-Deligne 表現}/\overline{\mathbb{Q}}_\ell \\ (r, N)\end{array}\right\}$$

証明. 右から左への対応は $\sigma \in W_K$ に対して,

$$\rho(\sigma) = r(\sigma)\exp(t_\ell(\sigma)N)$$

とおけばよい. 左から右への対応は定義 3-2-1 の直前で説明した構成を ρ に適用すればよい. □

例 3-2-3.(1) Ω を標数 0 の代数閉体とする. $n \in \mathbb{Z}$ に対して, $\omega_n(\Phi) = q^{-n},\ \omega_n(I_K) = 1$ を満たす指標 $\omega_n : W_K \longrightarrow \Omega^\times$ は 1 次元の Weil 群の表現を与える.

(2) Ω を標数 0 の代数閉体. $V = \Omega^n$ の標準基底を $\{e_i\}_{i=0}^{n-1}$ とする. このとき,

$$r(\Phi)e_i = \omega_i(\Phi)e_i,\ Ne_i = e_{i+1}, i = 0, \ldots, n-2,\ Ne_{n-1} = 0$$

を満たし, $\Phi^n\sigma,\ \sigma \in I_K$ に対して,

$$r(\Phi^n\sigma) = r(\Phi^n)\exp(t_\ell(\sigma)N)$$

となる表現 r を $\mathrm{sp}(n)$ で表し, **特殊表現 (special representation)** という.

Weil-Deligne 表現 (r, N) の像 $\mathrm{Im}(r)$ は惰性群 I_K とフロベニウス元の持ち上げ Φ で決まる. さらに, 惰性群の像は有限なので $\mathrm{Im}\, r$ は位相によらない代数的な群であることがわかる. 従って, 任意の体同型 $\iota : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \Omega$ に対して,

$$\left\{ \text{Weil-Deligne 連続表現}/\overline{\mathbb{Q}}_\ell \right\} \overset{1:1}{\longleftrightarrow} \left\{ \text{Weil-Deligne 表現}/\Omega \right\}, V \mapsto V \otimes_\iota \Omega$$

が成り立つ.

注意 3-2-4.(1) W_K は G_K の稠密部分群なので対応

$$\left\{ \ell \text{ 進表現}/\overline{\mathbb{Q}}_\ell \right\} \hookrightarrow \left\{ \text{Weil 群 } W_K \text{ の表現}/\overline{\mathbb{Q}}_\ell \right\}, \rho \mapsto \rho|_{W_K}$$

は像への 1:1 対応を与える. W_K の表現 r が G_K の表現に延長されることと $r(\Phi)$ のすべての固有値が ℓ 進単数であることは同値.

(2) W_K は局所副有限群[18]であり, コンパクトではない. よって, W_K の連続表現 r の像が必ずしも有限になるとは限らない. しかし, 適当な指標 ω_s で捻ると, $r \otimes \omega_s^{-1}$ の像は有限となる. ただし, ω_s は $\omega_s(I_K) = 1,\ \omega_s(\Phi) = q^{-s},\ s \in \mathbb{C}$ を満たす W_K の指標 (q^{-s} は $\mathbb{C}$ の元として考えておいて, 体同型で $\overline{\mathbb{Q}}_\ell$ などに写す).

(3) $\ell = p$ のときは定理 3-2-2 に類似する対応は Fontaine の関手 $\mathrm{D}_{\mathrm{pst}}$ を用いて, 構成される (cf. [6]). ただし対応は 1:1 でなくなる.

[18]副有限開集合を含む位相群をそう呼ぶ.

定義 3-2-5. Weil-Deligne 表現 (r, N) に対する L 関数を

$$L(r,s) := \det(1 - q^{-s}\rho(\Phi)|(\mathrm{Ker}N)^{I_K})^{-1}$$

で定義する．ここで，s は複素変数である．例えば，

$$L(\omega_n, s) = (1 - q^{-(s+n)})^{-1},\ L(\mathrm{sp}(n), s) = (1 - q^{-(s+n-1)})^{-1}.$$

定義 3-2-6. (r, N) を W_K の Weil-Deligne 表現とする．このとき，r の**フロベニウス半単純化 (Frobenius semisimplification)** r^{ss} を次の用に定義する: $r(\Phi)$ をジョルダン分解することで，$r(\Phi)$ を半単純行列 T と冪単行列 U の積で表す．このとき，$g = \Phi^n\sigma \in W_K,\ \sigma \in I_K,\ n \in \mathbb{Z}$ に対して，

$$r^{\mathrm{ss}}(g) := T^n r(\sigma)$$

と定義する．$r = r^{\mathrm{ss}}$ のとき，r は**フロベニウス半単純**であるという．

注意 3-2-7.(1) Weil-Deligne 表現 (r, N) に対して，$N = 0$ であることと，r が潜在的に不分岐，つまり K の有限次拡大 L が存在して，$r|_{W_L}$ は不分岐であることとは同値.

(2) 与えられた ℓ 進表現に付随する Weil-Deligne 表現を求めるのは容易ではない．例えば，例 2-2-3 の楕円曲線に付随する ℓ 進表現を考えたとき，その Weil-Deligne 表現を理解することと楕円曲線の幾何的様子を理解することは同じである．三枝氏の稿 [7] に内容に富む計算例が沢山あるので参照されたい．

4. ガロア表現の族

代数体 K に対して，Σ_K で K の有限素点全体の成す集合を表す．ℓ 進表現 ρ とその不分岐素点 $v \in \Sigma_K$ に対して，$P_{v,\rho}(T) := \det(1 - \rho(\mathrm{Frob}_v)T)$ とおく．

定義 4-1. ℓ 進表現 ρ が**有理的 (rational)** であるとは，Σ_K のある有限集合 S が存在して，次を満たすときを言う:

(i) ρ は $\Sigma_K \setminus S$ の任意の素点で不分岐

(ii) 任意の素点 $v \notin S$ (無限素点も込める) に対して，$P_{v,\rho}(T)$ は $\mathbb{Q}$ 係数多項式
さらに，

(ii)$'$ $P_{v,\rho}(T)$ は $\mathbb{Z}$ 係数多項式

を満たすとき，ρ は**整 (integral)** であるという．

定義 4-2. ℓ, ℓ' を素数とし，$\rho : G_K \longrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(V)$ および $\rho' : G_K \longrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}_{\ell'}}(V')$ をそれぞれ ℓ 進表現，ℓ' 進表現とし，ともに有理的であると仮定する．

このとき，ρ, ρ' が**整合的 (compatible)** であるとはある有限集合 $S \subset \Sigma_K$ が存在して，ρ, ρ' は共に S の外で不分岐かつ

$$P_{v,\rho}(T) = P_{v,\rho'}(T),\ \forall v \in \Sigma_K \setminus S$$

が成り立つときを言う．

定義 4-3. ℓ 進表現の成す系 $(\rho_\ell)_\ell$ が**整合系 (compatible system)** であるとは任意の 2 つの素数 ℓ, ℓ' に対して, $\rho_\ell, \rho_{\ell'}$ が整合的であるときをいう.

さらに, ある有限集合 $S \subset \Sigma_K$ が存在して次の条件を満たすとき, $(\rho_\ell)_\ell$ は**厳整合系 (strictly compatible system)** であると言う:

(i) すべての素点 $v \in \Sigma_K \setminus S \cup \{v \in \Sigma_K |\ v|\ell\}$ に対して, ρ_ℓ は v で不分岐かつ $P_{v,\rho_\ell}(T)$ は有理数係数をもつ.

(ii) 素数 ℓ, ℓ' に対して, $P_{v,\rho_\ell}(T) = P_{v,\rho_{\ell'}}(T),\ \forall v \in \Sigma_K \setminus S \cup \{v \in \Sigma_K |\ v|\ell\ell'\}$

(i),(ii) をみたす最小の S のことを $(\rho_\ell)_\ell$ の**例外集合 (exceptional set)** という.

例 4-4. (a) ℓ 進円分指標の成す系 $(\chi_\ell)_\ell$ は厳整合系を成し, その例外集合は空集合である.

(b) 例 2-2-3 楕円曲線のテート加群に付随するガロア表現の成す系 $(\rho_{E,\ell})_\ell$ は厳整合系を成す. 例外集合は E が悪い還元を持つような素点と丁度一致する. これは、Neron-Ogg-Shafarevich の良還元判定法からわかる (cf. [16] の定理 7.1 を参照). アーベル多様体の場合も同様である.

(c) X を $\mathbb{Q}_p$ 上の非特異射影的代数多様体とする. X に対して, ある $\operatorname{Spec}\mathbb{Z}_p$ 上のスキーム $\mathfrak{X}$ が存在して, $\mathfrak{X}$ の生成的繊維 (generic fiber) $\mathfrak{X} \times_{\operatorname{Spec}\mathbb{Z}_p} \operatorname{Spec}\mathbb{Q}_p$ が X と同型で, $\mathfrak{X}$ の特殊繊維 (special fiber) $\mathfrak{X} \times_{\operatorname{Spec}\mathbb{Z}_p} \operatorname{Spec}\mathbb{F}_p$ が $\mathbb{F}_p$ 上の非特異射影的代数多様体であるとき, X は ℓ で**良還元 (good reduction)** をもつという.

今度は X は $\mathbb{Q}$ 上の非特異射影的代数多様体とする. X が p で良還元をもつとは $X_{\mathbb{Q}_p} := X \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}_p$ がそうなるときをいう. $X/\mathbb{Q}$ に対して, $\operatorname{Spec}\mathbb{Z}$ 上の平坦スキーム $\mathfrak{X}/\operatorname{Spec}\mathbb{Z}$ でその生成的繊維が X と同型なものが存在する. さらに, $\operatorname{Spec}\mathbb{Z}$ の (空でない) 開集合 U で $\mathfrak{X}_U \longrightarrow U$ は滑らかであるものが存在する (cf. [7] の系 3.26). このとき, 各 $0 \le i \le 2\dim X$ に対して, エタールコホモロジー $V_i := H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)^\vee$ を取ることで, $G_\mathbb{Q}$ が連続に作用する有限次 $\mathbb{Q}_\ell$ ベクトル空間を得る. これより, ガロア表現

$$\rho_{i,\ell} : G_\mathbb{Q} \longrightarrow \operatorname{Aut}_{\mathbb{Q}_\ell}(V_i)$$

を, さらには, 厳整合系 $(\rho_{i,\ell})_\ell$ を得る. この系が厳整合系であることは Weil 予想から従う (cf. [7]). また, この系の例外集合は $\operatorname{Spec}\mathbb{Z} \setminus U$ にはいることがわかる. これは固有平滑底変換定理により. $V_i|_{G_{\mathbb{Q}_p}} \simeq H^i_{\text{ét}}(\mathfrak{X}_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_\ell) \simeq H^i_{\text{ét}}(\mathfrak{X}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$ が成り立つことから従う (cf. [7] の系 3.25 を参照).

注意 4-5. (a) 厳整合系を最初に考案・考察したのは谷山豊であると思われる [19]. 谷山は Weil の意味で (A_0) 型のイデール類群の指標から G_K^{ab} の ℓ 進表現からなる厳整合系を付随させ、また逆にそのような系から (A_0) 型のイデール類群の指標を対応させた. 一見, 本質的には Weil が考案していてもおかしくないのではないかと疑うのも自然ではあるが, [19] の Math.review を幸運にも Weil が書いていてそこには「At this point the author takes a step involving what is perhaps the most original idea of the whole paper; he considers any system (M_ℓ) of ℓ-adic representations of $\mathfrak{g}$, all of the same degree (ℓ ranging over all

primes) satisfying the same set of conditions.」という文章が書かれてある．Weil が辛口であることを思い出すと, Weil も思いも寄らなかったのではないかと推測できる．
(b) 代数体の絶対ガロア群の "良い" ℓ 進表現 ρ は適当な厳整合系 $(\rho'_{\ell'})_{\ell'}$ に埋め込めると期待されている．つまり, $\rho'_\ell \sim \rho$. また代数体の絶対ガロア群の "良い" 法 ℓ 表現は厳整合系に埋め込める ℓ 進表現の還元になることが期待されている．

最近のガロア表現の保型性の証明では実際にこのことを証明することで, Wiles 以降飛躍的に進歩した議論を展開させている (安田正大氏, 吉田輝義氏の講演・原稿を参照).

この節の最後に整合系に埋め込むことができない有理的 ℓ 進表現の具体例を紹介する．
例 4-6. $H = \left(\dfrac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q}\cdot 1 + \mathbb{Q}\cdot i + \mathbb{Q}\cdot j + \mathbb{Q}\cdot ij,\ i^2 = j^2 = -1, ij = -ji$ を 2 と ∞ のみで分岐する $\mathbb{Q}$ 上の 4 元数体とする．よく知られているように $H_\ell := H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ は $\ell = 2, \infty$ のときは斜体となり, それ以外では $\mathrm{M}_2(\mathbb{Q}_\ell)$ と同型となる．$G = \{\pm 1, \pm i, \pm j, \pm ij\}$ を 4 元数群 (quaternion group) とする．$K = \mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{3})})$ とおくとき, $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ がわかる．これは Dedekind によって与えられた例である．このとき, $\ell > 2$ に対して

$$\rho_\ell : G_{\mathbb{Q}} \overset{K\ \text{への制限}}{\longrightarrow} \mathrm{Gal}(K/\mathbb{Q}) \simeq G \hookrightarrow H^\times \hookrightarrow (H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times \simeq \mathrm{GL}_2(\mathbb{Q}_\ell)$$

は既約な有理的 ℓ 進表現であることがわかる (既約性は次のように確認できる．埋め込み $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ を固定し, ρ_ℓ の $\mathbb{C}$ への係数拡大を考えると, これは Artin 表現である．よって, 可約ならば半単純性から像がアーベル群となり矛盾).

ここで適当に有理的 2 進表現 $\rho_2 : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_2)$ を持ってきて, $\{\rho_\ell\}_\ell$ を整合系にできるかどうか考えてみる．

そのような有理的 2 進表現 ρ_2 が存在したと仮定すると, ρ_2 は $\rho_\ell(\ell \neq 2)$ と整合的でなければならない．ここで埋め込み $\mathbb{Q}_2 \hookrightarrow \mathbb{C}, \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ を固定し, ρ_2, ρ_ℓ の $\mathbb{C}$ への係数拡大を $\rho_{2,\mathbb{C}}, \rho_{\ell,\mathbb{C}}$ と書く．これらの表現は像が有限なので Artin 表現である．表現 ρ_2 と ρ_ℓ は整合的なので, 命題 2-6-3 から $\rho_{2,\mathbb{C}} \sim \rho_{\ell,\mathbb{C}}$ である．また, これらの表現の像は有限群 G と同型で係数拡大しても変わらないものなので, 特に, 群準同型

$$r : G \simeq \mathrm{Im}\rho_2 \subset \mathrm{GL}_2(\mathbb{Q}_2)$$

を得る．群準同型 r の像は $\mathrm{M}_2(\mathbb{Q}_2)$ に入るので, r をこの中で $\mathbb{Q}_2$ 線形に拡張すれば群環 $\mathbb{Q}_2[G]$ から $\mathrm{M}_2(\mathbb{Q}_2)$ への $\mathbb{Q}_2$ 線形写像 r^* を得る．さらに r^* は $\mathbb{Q}_2$ 多元環としての射であることが直接計算から分かる．明らかに, r^* の像は $H \otimes_{\mathbb{Q}} \mathbb{Q}_2$ と同型であり, これと $\mathrm{M}_2(\mathbb{Q}_2)$ との $\mathbb{Q}_2$ 上のベクトル空間としての次元を比較すると, $H \otimes_{\mathbb{Q}} \mathbb{Q}_2 \simeq \mathrm{M}_2(\mathbb{Q}_2)$ を得る．しかし, H は 2 で分岐するので矛盾．これは上記 $\rho_\ell,\ \ell > 2$ はどうやっても整合系には埋め込めないことを示している．このような現象は Artin 表現に特有のものと思われる (注意 4-5 の (b) を参照).

問 4-7. ([14] の I-12 の問 3) 例 4-6 を参考にして, 与えられた有理的 ℓ 進表現 ρ_ℓ に対して, ρ_ℓ と整合的な有理的 ℓ' 進表現 $\rho_{\ell'}(\ell' \neq \ell)$ が存在するかどうか考えよ (∞ と ℓ' で分岐する四元数体を用いる．[12] の定理 5.1 にそのような四元数体の例が書いてある).

5. 付録

この付録では命題 2-2-7 と命題 2-4-2 の証明を与える． 証明はブルバキの８章の命題 3(p.136) に沿って行う．そのためにいくつかの準備を行う．

A を単位元をもつ可換環とし, A 加群 M に対して, $\mathrm{End}(M)$ を M の加法群としての自己準同型全体のなす環, $\mathrm{End}_A(M)$ を M の A-自己準同型全体のなす環とする． また, $B_M = \{f \in \mathrm{End}(M) |\ fg = gf, \forall g \in \mathrm{End}_A(M)\}$ とおく[19]. A の元を M の A-自己準同型とみることで, $A \longrightarrow B_M$ を得る．この像を A_M と書き, この対応による, $a \in A$ の像を a_M と書く．

命題 5-1. A を単位元をもつ可換環とし, $F_i, i \in I$ を A 加群の族とし, 各メンバーは互いに同型であるとする $(F_i \simeq F_j,\ i, j \in I)$. $M = \bigoplus_i F_i$ とおき, i をひとつ固定し, $F = F_i$ とおく．このとき, 対応

$$B_M \longrightarrow B_F, b \mapsto b|_F$$

は全射.

証明. 実は単射であることもわかるが必要ないので省略する．まず, 上の対応は well-defined であることを示す．F は M の直和因子なので, F への射影子 $p : M \longrightarrow M$ をとると, 明らかに, p は A-自己準同型. よって, $b \in B_M$ に対して, 定義より, $bp = pb$ だから,

$$b|_F(F) = bp(M) = pb(M) \subset p(M) = F$$

なので, $b|_F \in \mathrm{End}(F)$. $f \in \mathrm{End}_A(F)$ を取り,$g : M \longrightarrow M$ を $g|_F = f$, それ以外では 0 と定めると, $x \in F$ に対して, $b_F f(x) = bg(x) = gb(x) = fb_F(x)$. よって, $b|_F \in B_F$.

仮定より, 各 $j \in I$ に対して, 同型射 $f_j : F \xrightarrow{\sim} F_j \subset M$ が存在する．$b' \in B_F$ をとると, $b_j = f_j b' f_j^{-1}$ は B_{F_j} の元. 実際, $g' \in \mathrm{End}_A(F_j)$ は $g' = f_i g f_j^{-1},\ g \in \mathrm{End}_A(F)$ とかけるので,

$$b_j g' = (f_j b' f_j^{-1})(f_i g f_j^{-1}) = f_j b' g f_j^{-1} = f_j g b' f_j^{-1} = f_j g f_j^{-1} f_i b' f_j^{-1} = g' b_j$$

だからよい.

ここで, $b \in \mathrm{End}(M)$ を $b(x) = b_j(x),\ x \in F_j$ と定めると, このような b は一意的にきまる. ここで, $b \in B_M$ が成り立つことを確認する．$c \in \mathrm{End}_A(M)$ をとり, 単位元 $1_M \in \mathrm{End}_A(M)$ を F_j への射影子 p_j を用いて, $1_M = \displaystyle\sum_j p_j$ と分解しておく.

このとき, $x \in F_k$ に対して, $x_k = f_k(y)$ なる $y_k \in F$ をとっておくと,

$$cb(x) = cb_k(x) = cb_k f_k(y) = cf_k b'(y)$$

および, 分解 $b = b \cdot 1_M = \displaystyle\sum_j b_j p_j$ を用いて,

$$bc(x) = \sum_j b_j p_j c f_k(y) = \sum_j f_j b' f_j^{-1} p_j c f_k(y)$$

[19] B_M は M の再交換団と呼ばれる.

を得る．ここで，$f_j^{-1}p_jcf_k$ は $\mathrm{End}_A(F)$ なので，b' と交換可能．よって，

$$bc(x) = \sum_j p_jcf_kb'(y) = cf_kb'(y) = cb(x).$$

線形性より，すべての $x \in M$ に対して，この等式が成り立つので，$b \in B_M$ である． □

定理 5-2. A を単位元をもつ可換環，M を半単純 A 加群とし，$b \in B_M$ をとる．このとき，M の任意の有限列 $x_1, \ldots, x_n$ に対して，$ax_i = b(x_i),\ i = 1, \ldots, n$ を満たす $a \in A$ が存在する．

証明. 各 i に対して，M から M の n 個の直和 M^n の第 i 成分への上への同型を $f_i : M \longrightarrow M^n$ とおき，その像を M_i とおく．各 $b \in B_M$ に対して，$b_i := f_ibf_i^{-1} \in B_{M_i}$ が成立する．このとき，$b' \in \mathrm{End}(M^n)$ を $b'(x) = b_i(x),\ x \in M_i$ と定めると，命題 5-1 より，$b' \in B_{M^n}$ であって，その M_i への制限が b_i と一致するものが存在し，，$b'f_i = f_ib$ がすべての i について成立．

M は半単純 A 加群なので M^n もそう．よって，$x := (x_i)_i = \sum_i f_ix_i \in M^n$ に対して，Ax は M^n の直和因子．命題 5-1 の証明の 1 から 5 行目をみると，Ax は B_{M^n} 加群であることがわかる．よって，$b'(Ax) \subset Ax$ なので，$a \in A$ であって，$ax = b'(x)$ が成り立つものが存在するから，

$$(ax_i)_i = ax = b'(x) = \sum_i b'f_ix_i = \sum_i f_ibx_i = (bx_i)_i$$

が成り立つ．よって，$ax_i = bx_i,\ i = 1, \ldots, n$. □

系 5-3. M を半単純 A 加群とし，左 $\mathrm{End}_A(M)$ 加群として，M は有限生成であると仮定する．このとき，$B_M = A_M$ が成り立つ．

証明. $b \in B_M$ をとる．左 $\mathrm{End}_A(M)$ 加群としての M の生成系を $x_1, \ldots, x_n$ とすると，定理 5-2 から，ある $a_M \in A_M$ が存在して，$a_Mx_i = b(x_i),\ i = 1, \ldots, n$ を満たす．ここで，すべての元 $x \in M$ は $x = \sum_{i=1}^n g_i(x_i),\ g_i \in \mathrm{End}_A(M)$ とかけるので，$a_M, b \in B_M$ であることから，

$$a_M(x) = a_M\sum_{i=1}^n g_i(x_i) = \sum_{i=1}^n g_ia_M(x_i) = \sum_{i=1}^n g_ib(x_i) = b\sum_{i=1}^n g_i(x_i) = b(x).$$

よって，$B_M \subset A_M$ なので結論を得る． □

系 5-4. $M_1, \ldots, M_n$ を単純 A 加群とし，互いに同型ではないと仮定する．$M = \bigoplus_i M_i$ とおき，各 M_i は左 $\mathrm{End}_A(M_i)$ 加群として有限生成であると仮定．このとき，A の n 個の元 $a_1, \ldots, a_n$ に対して，ある $a \in A$ が存在して，

$$a_M|_{M_i} = (a_i)_{M_i}$$

が成立する[20].

[20]記号が紛らわしいが，$(a_i)_{M_i}$ は $A \longrightarrow \mathrm{End}_A(M_i)$ による $a_i \in A$ の像である．

証明. 半単純加群 M と $((a_i)_{M_i})_i \in \mathrm{End}_A(M^n)$ に系 5-3 を適用すればよい. $\square$

以上で準備が整ったので命題 2-2-7 と命題 2-4-2 を証明する.

命題 2-2-7 の証明. 記号を復習すると, A は体 k 上の代数で, M, M' は k 上有限次な A 単純加群であり, k が正標数であるならば, $\mathrm{char}(k) > \max\{\dim_k(M), \dim_k(M')\}$ という仮定を設けていた. このとき, $\mathrm{tr}_M(a) = \mathrm{tr}_{M'}(a)$, $\forall a \in A$ のとき, M と M' が同型であることを示す.

$\mathfrak{S}$ で半単純 A 加群の同型類の成す圏とする ($\mathfrak{S}$ は半単純圏となる). $\mathfrak{S}$ の対象 λ に対して, M の半単純 A 因子で λ に属する (λ はある半単純加群の同型類) ものを M_λ と書き, その重複度を $n_\lambda \in \mathbb{Z}_{\geq 0}$ で表す. M' に関しても同様に, M'_λ, n'_λ を定義する.

このとき, $\mathfrak{S}$ の対象からなる有限集合 H が存在して,

$$M = \bigoplus_{\lambda \in H} n_\lambda M_\lambda,\ M' = \bigoplus_{\lambda \in H} n'_\lambda M'_\lambda$$

と表せる.

M(resp. M') は A 上有限生成でもあるので, 左 $\mathrm{End}_A(M)$ 加群 (resp. 左 $\mathrm{End}_A(M')$ 加群) としても有限生成.

各 $\lambda \in H$ に対して, その代表系である単純 A 加群を N_λ を一つとり固定しておく. もし, $n_\lambda \neq 0$ かつ $n'_\lambda \neq 0$ ならば,

$$M_\lambda \simeq N_\lambda \simeq M'_\lambda$$

であり,

$$\mathrm{tr}_{M_\lambda}(a) = \mathrm{tr}_{N_\lambda}(a) = \mathrm{tr}_{M'_\lambda}(a),\ a \in A$$

が成り立つことを注意しておく.

このとき, $1 \in A$ と $\bigoplus_{\lambda \in H} N_\lambda$ に対して, 系 5-4 を適用することで, $c \in A$ で $c_{N_\lambda} = 1$ かつ $c_{N_\mu} = 0,\ \mu \neq \lambda$ を満たすものがとれる. 仮定より, $\mathrm{tr}_M(c) = \mathrm{tr}_{M'}(c)$ が成立するので, これは

$$(n_\lambda - n'_\lambda)\mathrm{tr}_{N_\lambda}(1) = 0$$

を導く. ここで, N_λ は 0 でないと仮定してよいので, もし, k の標数が 0 ならば, $\mathrm{tr}_{N_\lambda}(1) = \dim_k(M_\lambda) = \dim_k(M'_\lambda)$ は $k^\times$ の元である. よって, $n_\lambda = n'_\lambda$. もし, k の標数 p が正ならば, 仮定より, それは $p > d := \max\{\dim_k(M), \dim_k(M')\}$ を満たしているので, 同様に $\mathrm{tr}_{N_\lambda}(1) \in k^\times$. よって,

$$n_\lambda - n'_\lambda \equiv 0 \bmod p$$

が成り立つ. 一方, $0 \leq |n_\lambda - n'_\lambda| \leq d$ なので, $n_\lambda - n'_\lambda = 0$ を得る.

命題 2-4-2 の証明. 記号は上のものと同じであるとする. すると, 上記証明から M, M' はそれぞれ

$$M = L_1 \oplus M_1^{\oplus p},\ M = L'_1 \oplus M_1'^{\oplus p}$$

の形をしていることがわかる. ただし, L_1, L'_1, M_1, M'_1 は半単純 A 加群で, A 加群として $L_1 \simeq L'_1$ である. 各 $a \in A$ の $M_1^{\oplus p}$, $M_1'^{\oplus p}$ への作用の固有多項式はそれぞれ,

$$F(a,T)^p,\ F'_1(a,T)^p \in k[T]$$

の形をしており, 仮定から $F(a,T)^p = F_1'(a,T)^p$ である. k の標数は p だから, これより, $F(a,T) = F_1'(a,T)$ を得る. もし $M_1 \neq 0$ ならば, $F(a,T) = F_1'(a,T), a \in A$, $\dim_k(M_1) = \dim_k(M_1')$ という仮定が成立することから同じことを何度も繰り返すことができて, M, M' は

$$M = L_r \oplus M_r^{\oplus p^r},\ M' = L_r' \oplus M_r'^{\oplus p^r},\ L_r \simeq L_r'$$

という形になることがわかる. しかし, M, M' は k 上有限次元なのでこの操作はどこかで止まり, ある r に対して, $M_r = 0, M_r' = 0$ となる. よって, 結論を得る.

6. 謝辞

サマースクールを共に企画してくださいました落合理, 千田雅隆両氏と多岐にわたりご協力くださいました森山知則, 山上敦士両氏に感謝申し上げます. また, 小林真一さん, 山崎隆雄さん, および, 田口雄一郎先生にはセールの本の演習問題の解答や整合系に関連する話題をいくつも教えていただきました. 特に記して感謝申し上げます.

References

[1] J. A. Antoniadis, Diedergruppe und Reziprozitatsgesetz, J. Reine Angew. Math. 377 (1987), 197–209.
[2] P. Deligne, Résumé des premiers exposés de A. Grothendieck, Groupes de monodromie en geometrie algebrique. I. Seminaire de Geometrie Algebrique du Bois-Marie 1967–1969 (SGA 7 I). pp. 1–24.
[3] 飯高茂, 上野健爾, 浪川幸彦, デカルトの精神と代数幾何, 日本評論社.
[4] 千田 雅隆, ガロア表現の基礎 II, 本報告集.
[5] P. Deligne and J-P. Serre, Formes modulaires de poids 1. Annales scientifiques de l'Ecole Normale Superieure, Ser. 4, 7 no. 4 (1974), p. 507-530.
[6] J-M. Fontaine, Représentations l-adiques potentiellement semi-stables, Exposé VIII, Astérisque 1994, 224, périodes p-adiques, seminaire de Bures, 1988.
[7] 三枝洋一, エタールコホモロジー入門, 本報告集.
[8] 中村 健太郎, p-進ホッジ理論, 本報告集.
[9] 落合 理, プレサマースクール-数論的な体の絶対ガロア群の構造への道先案内-, 本報告集.
[10] 落合 理, 肥田理論概説, 本報告集.
[11] A. Ogg, Modular forms and Dirichlet series, 1969, Benjamin New York.
[12] A. Pizer, An algorithm for computing modular forms on $\Gamma_0(N)$. J. Algebra 64 (1980), no. 2, 340–390.
[13] J-P. Serre, Linear representations of finite groups. Translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg.
[14] J-P. Serre, Abelian l-adic representations and elliptic curves. With the collaboration of Willem Kuyk and John Labute. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. xxiv+184 pp.
[15] J-P. Serre and J. Tate, Good reduction of abelian varieties. Ann. of Math. (2) 88 1968 492–517.
[16] J. Silverman, Arithmetic of Elliptic curves, GTM 106.
[17] 第 12 回整数論サマースクール「基本群とガロア表現」.
[18] P. Sarnak, Maass cusp forms with integer coefficients. A panorama of number theory or the view from Baker's garden (Zurich, 1999), 121–127.
[19] Y. Taniyama, L-functions of number fields and zeta functions of abelian varieties. J. Math. Soc. Japan 9 1957 330–366.
[20] 冨山 恭敬, 無限個の素点で分岐する既約な p 進表現の構成について, 本報告集.

[21] 内田 伏一, 集合と位相, 裳華房.

[22] 山本 芳彦, 数論入門 2, 岩波講座, 現代数学への入門.

[23] A. Weil, On a certain type of characters of the idele-class group of an algebraic number-field. Proceedings of the international symposium on algebraic number theory, Tokyo and Nikko, 1955, pp. 1-7.