概均質ベクトル空間論の発展（第30回整数論サマースクール報告集、写真なし）

谷口, 隆 ; 杉山, 和成 ; 石塚, 裕大 ; 佐藤, 文広 ; 都築, 正男 ; Thorne, Frank ; 鈴木, 雄太 ; 伊吹山, 知義 ; 鈴木, 美裕 ; 佐野, 薫 ; 山本, 修司

(Citation)
第30回整数論サマースクール報告集「概均質ベクトル空間論の発展」:1-421

(Issue Date)
2024-01-31

(Resource Type)
conference proceedings

(Version)
Version of Record

(JaLCDOI)
https://doi.org/10.24546/0100486229

(URL)
https://hdl.handle.net/20.500.14094/0100486229

有理軌道，整軌道の解釈

石塚　裕大（九州大学 IMI）

概要

いくつかの概均質ベクトル空間の体上の軌道，あるいは $\mathbb{Z}$ 上の軌道が代数による自然な解釈を持つことを概説する．これは [鈴木雄], [Thorne], [鈴木美] で扱われるような，体の数え上げを軌道の数え上げに帰着する場面で利用される．また体上の軌道の解釈は [佐野] で取り扱われる楕円曲線の Selmer 群の軌道解釈の雛形ともなっている．

簡単のため，この章では K は完全体とする．前節と同様に $K^2 \otimes K^2 \otimes K^3$ や $K^2 \otimes \mathrm{Sym}^2 K^3$ などの空間を，K を省略して $2 \otimes 2 \otimes 3$ や $2 \otimes \mathrm{Sym}^2 3$ のように略記することがある．

1　有理軌道の解釈：Wright–Yukie 理論

いくつかの概均質ベクトル空間について，その軌道に射影空間の点集合を対応させ，体 k 上の分離代数と体 k 上の軌道（有理軌道）との間に対応を見出すことができる．これは Wright–Yukie [WY92] を筆頭としたいくつかの論文によって実行された．今節では，このうち代表的なものについて概観する．

1.1　二元三次形式と三次代数

まず [谷口 1, 谷口 2] から次の命題を思い出す．

命題 1.1　次の集合の間に自然な対応がある．

- 体 K 上の三次分離代数の同型類．
- $V(K) = \mathrm{Sym}^3 K^2$ の非退化な元（つまり $P(x) \neq 0$）の部分集合 $V'(K)$ についての $G(K) = \mathrm{GL}_1(K) \times \mathrm{GL}_2(K)$ 軌道．

初等的な証明が [谷口 1] に，ガロアコホモロジーを使った証明が [谷口 2] にある．ここでは後者について簡単に復習しておこう．

1.1.1 三次分離代数とガロアコホモロジー

まず三次分離代数の同型類をガロアコホモロジーで解釈する命題を復習しよう．

命題 1.2 K 上の三次分離代数の同型類は $H^1(K, \mathfrak{S}_3)$ と自然に全単射を持つ．

実際，K 上の三次分離代数 L は $L \otimes_K \overline{K}$ が $K^3 \otimes_K \overline{K} \cong \overline{K}^3$ に同型になるような K 代数だった [谷口 1, 定義 1.4]．この同型を $\rho_L \colon L \otimes_K \overline{K} \to K^3 \otimes_K \overline{K}$ とおくと，

$$c_L(\sigma) = \rho_L^{-1} \rho_L^{\sigma}$$

で定義される写像

$$c_L \colon \Gamma_K = \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\overline{K}\text{-alg}}(\overline{K}^3)$$

は $\mathrm{Aut}_{\overline{K}\text{-alg}}(\overline{K}^3)$ に値を取る 1-コサイクルになる（[谷口 2, §1.4] 参照．1-コサイクルの定義は [谷口 2, 定義 1.5] を参照）．いま [谷口 1, 命題 1.6] によると

$$\mathrm{Aut}_{\overline{K}\text{-alg}}(\overline{K}^3) = \mathrm{Aut}_{K\text{-alg}}(K^3) \cong \mathfrak{S}_3$$

であるから，

$$c_L \in H^1(K, \mathrm{Aut}_{\overline{K}\text{-alg}}(\overline{K}^3)) \cong H^1(K, \mathfrak{S}_3)$$

がわかる．これが全単射を与えるのである [谷口 2, 補題 1.12]．別にこの対応は n 次分離代数でもよい．

1.1.2 非退化軌道とガロアコホモロジー

次に軌道と $H^1(K, \mathfrak{S}_3)$ との対応を見ておこう．写像 $G(\overline{K}) \to V'(\overline{K})$ を $g \mapsto gw_0$ で定める．これは全射であり（V の概均質性），「核」は固定部分群

$$G_{w_0}(\overline{K}) = \{g \in G(\overline{K}) \mid gw_0 = w_0\}$$

である．これから「短完全列」

$$1 \longrightarrow G_{w_0}(\overline{K}) \longrightarrow G(\overline{K}) \longrightarrow V'(\overline{K}) \longrightarrow 1$$

が得られ,「長完全列」

$$1 \longrightarrow G_{w_0}(K) \longrightarrow G(K) \longrightarrow V'(K) \longrightarrow H^1(K, G_{w_0}) \longrightarrow H^1(K, G)$$

ができる．つまり

$$G(K) \setminus V'(K) \overset{1:1}{\leftrightarrow} \mathrm{Ker}(H^1(K, G_{w_0}) \to H^1(K, G))$$

である [谷口 2, 定理 1.11]．ここまでは概均質ベクトル空間での一般論であり，$V'(K)$ の代わりに $G(\overline{K})w_0 \cap V(K)$ を考えることで概均質空間でない場合にも拡張できる．

いま $V = \mathrm{Sym}^3 2, G = \mathrm{GL}_1 \times \mathrm{GL}_2$ である特殊事情を利用して，より状況を絞り込める：

(1) [谷口 2, 命題 1.6] から，$H^1(K, \mathrm{GL}_n) = \{1\}$ である．すると

$$H^1(K, G) = H^1(K, \mathrm{GL}_1 \times \mathrm{GL}_2) \cong H^1(K, \mathrm{GL}_1) \times H^1(K, \mathrm{GL}_2) = \{1\}.$$

したがって $\mathrm{Ker}(H^1(K, G_{w_0}) \to H^1(K, G)) = H^1(K, G_{w_0})$ となる．

(2) $T \coloneqq \mathrm{Ker}(G \to \mathrm{GL}(V))$ とおくと，$G_{w_0} \cong \mathfrak{S}_3 \times T$ である．したがって $H^1(K, G_{w_0}) \cong H^1(K, \mathfrak{S}_3) \times H^1(K, T)$ である．

(3) $T = \{(t^{-2}, tI_2) \mid t \in K^*\}$ と特定される（I_2 はサイズ 2 の単位行列）．特に $T \cong \mathrm{GL}_1$ であるから，再び Hilbert 90 から $H^1(K, T) = \{1\}$ である．

これから, $G(K)\backslash V'(K)$ は $H^1(K, \mathfrak{S}_3)$ と自然に全単射を持つ．(2) の $G_{w_0} \cong \mathfrak{S}_3 \times T$ についても少し深入りしておこう．

(2.1) $G_{w_0}(K)$ は $Z_{w_0}(K) = W_0 = \{(1:0), (0:1), (1:1)\}$ に右から作用する．したがって群準同型 $\pi_0 \colon G_{w_0} \to \mathrm{Aut}(W_0) \cong \mathfrak{S}_3$ が誘導される．

(2.2) $\mathrm{Ker}(\pi_0) = T$ である．実際 W_0 の各点を固定するから $g = (g_1, g_2)$ について g_2 はスカラー行列であり，w_0 を固定することから g_1 が決定される．

(2.3) π_0 は分裂する：つまり単射準同型 $\iota_0 \colon \mathrm{Aut}(W_0) \hookrightarrow G_{w_0}(K)$ であって，$\pi_0 \circ \iota_0$ が恒等写像になるものが存在する [Yuk, Lemma 13.15].

(2.4) T は中心 $Z(G)$ に入る．つまり T の各元は G の任意の元と可換である．

これらを合わせると，写像

$$G_{w_0} \to \mathfrak{S}_3 \times T; g \mapsto (\pi_0(g), g\iota_0(\pi_0(g))^{-1})$$

が同型を与えることが以下のようにして（純粋に群論的に）わかる．

- well-defined: π_0 の核が T だから $g\iota_0(\pi_0(g))^{-1}$ は T の要素である．
- 全射：$(s,t) \in \mathfrak{S}_3 \times T$ について $\iota(s)t \in G_{w_0}$ を考えれば良い．
- 群準同型：$g_2\iota_0(\pi_0(g_2))^{-1}$ は T の要素だから G の要素と可換であり，

$$\begin{aligned} g_1\iota_0(\pi_0(g_1))^{-1} \cdot g_2\iota_0(\pi_0(g_2))^{-1} &= g_1 \cdot g_2\iota_0(\pi_0(g_2))^{-1} \cdot \iota_0(\pi_0(g_1))^{-1} \\ &= (g_1g_2) \cdot \iota_0(\pi_0(g_1g_2))^{-1} \end{aligned}$$

  となるので従う．
- 単射性: $\pi_0(g) = 1$ から $g \in T$ であり，このとき $g\iota_0(\pi_0(g))^{-1} = g$ であることから従う．

1.2 三元二次形式のペアと四次代数

さて，この節のメインである次を紹介しよう．

命題 1.3 次の集合の間に自然な対応がある．

- 体 K 上の四次分離代数の同型類．
- $V(K) = K^2 \otimes \mathrm{Sym}^2 K^3$ の非退化な元（つまり $P(x) \neq 0$）の部分集合 $V'(K)$ についての $G(K) = \mathrm{GL}_2(K) \times \mathrm{GL}_3(K)$ 軌道．

実はこの命題を証明するだけならば，前節のガロアコホモロジーによる抽象的な証明で素早くできてしまう．実際，$H^1(K, \mathfrak{S}_4)$ が四次分離代数の同型類に対応することは命題 1.2 と同様である．軌道側では，特殊事情にあたる部分 (1)∼(3) を一つ一つ証明していけばよい：

(1) Hilbert の定理 90 から，

$$H^1(K, G) = H^1(K, \mathrm{GL}_2 \times \mathrm{GL}_3) \cong H^1(K, \mathrm{GL}_2) \times H^1(K, \mathrm{GL}_3) = \{1\}.$$

  したがって $\mathrm{Ker}(H^1(K, G_{w_0}) \to H^1(K, G)) = H^1(K, G_{w_0})$ となる．

(2) $T \coloneqq \mathrm{Ker}(G \to \mathrm{GL}(V))$ とおくと，$G_{w_0} \cong \mathfrak{S}_4 \times T$ である．したがって $H^1(K, G_{w_0}) \cong H^1(K, \mathfrak{S}_4) \times H^1(K, T)$ である．

(3) $T = \{(t^{-3}I_2, tI_3) \mid t \in K^*\}$ と特定される．特に $T \cong \mathrm{GL}_1$ であるから，再び Hilbert 90 から $H^1(K, T) = \{1\}$ である．したがって $H^1(K, G_{w_0}) \cong$

$H^1(K, \mathfrak{S}_4)$.

(2) の $G_{w_0} \cong \mathfrak{S}_4 \times T$ も，二元三次形式とまったく同様に証明できる．(2.1) 群準同型 $\pi_0 \colon G_{w_0} \to \mathrm{Aut}(W_0) \cong \mathfrak{S}_4$ が定まり，(2.2) 核が T に一致し，(2.3) 単射 $\iota_0 \colon \mathrm{Aut}(W_0) \to G_{w_0}$ で $\pi_0 \circ \iota_0$ が恒等射になるものが見つかる [Yuk, Proposition 14.18]．さらに (2.4) T は $Z(G)$ に入ることから，全く同様にして同型

$$G \to \mathfrak{S}_4 \times T; g \mapsto (\pi_0(g), g\iota_0(\pi_0(g))^{-1})$$

が定義できる．

1.2.1 具体的な対応

抽象的にはこれで対応が理解できたが，せっかくなのでより具体的に理解してみよう．

例 1.4 K 上の四次方程式

$$f(u) \coloneqq u^4 + bu^3 + cu^2 + du + e = 0 \ (b, c, d, e \in K)$$

を考える．重根がないことは仮定するが，別に既約性は仮定しない．このとき

$$R_f \coloneqq K[u]/(u^4 + bu^3 + cu^2 + du + e)$$

で四次分離代数ができる（K は完全体であることに注意）．

一方，四次多項式 f を次のように分解できる：

$$\begin{cases} v - u^2 = 0, \\ v^2 + buv + cv + du + e = 0. \end{cases}$$

これらは二元二次の多項式なので，斉次化をすると三元二次形式のペアができる：

$$\begin{cases} A_f(u, v, w) = vw - u^2, \\ B_f(u, v, w) = v^2 + buv + cvw + duw + ew^2. \end{cases}$$

このとき，$x_f = (A_f, B_f)$ について対応する四次分離代数は R_f である．なお $Z_x(\overline{K})$ は，$f(u) = 0$ の根 u_i $(1 \leq i \leq 4)$ について $P_i = (u_i : u_i^2 : 1)$ と記述される．

この対応はモニックな二元三次形式 $x(u, v) = u^3 + bu^2v + cuv^2 + dv^3$ について，対応する分離代数が $K[u]/(x(u, 1))$ で与えられることと対応している．

1.2.2 三次レゾルベント体

上の例を深掘りしてみよう．四次多項式 f から定まる $x_f = (A_f, B_f)$ について，$f_{x_f}(u,v) = 4\det(uM_A + vM_B)$ によって二元三次形式が定義されたことを思い出そう．二元三次形式は三次分離代数に対応するはずだが，この三次分離代数と，四次分離代数 R_f の関係はなにかあるだろうか．

簡単のため，f を K 上で既約な多項式としよう．すると R_f は K の四次拡大体になり，f の根 $\alpha \in \overline{K}$ について $K(\alpha)$ に同型になる．α の共役を $\alpha_0 = \alpha, \alpha_1, \alpha_2, \alpha_3$ としたとき，

$$\begin{aligned}\beta_1 &= \alpha_0\alpha_1 + \alpha_2\alpha_3,\\ \beta_2 &= \alpha_0\alpha_2 + \alpha_1\alpha_3,\\ \beta_3 &= \alpha_0\alpha_3 + \alpha_1\alpha_2\end{aligned}$$

を根とする三次多項式

$$c_f(u) = (x-\beta_1)(x-\beta_2)(x-\beta_3)$$

は K 上で定義される．この方程式 c_f を f の**三次レゾルベント** *cubic resolvent* といい，対応する三次分離代数 $C_f = K[u]/(c_f(u))$ が f_{x_f} にも対応することがわかる．$K(\alpha_0)$ の Galois 閉包 $K(\alpha_0,\alpha_1,\alpha_2,\alpha_3)$ が K の $\mathfrak{S}_4$-拡大なら，$K = K(\beta_1)$ は D_8-不変部分体に対応する[*1]．

幾何的に見てみよう．$f_{x_f}(u,v)$ の自明でない根 $(s,t) \neq (0,0)$ を取ると，三元二次形式 $F = sA_f + tB_f$ は対応する行列の階数が下がる．前章 [石塚] でも事実として述べたように，行列の階数は 2 までしか下がらず，対応する二次曲線 $Z_F(\overline{K})$ は二本の直線の和集合になる．

$$Z_{x_f}(\overline{K}) = \{P_i = (\alpha_i : \alpha_i^2 : 1) \mid 0 \le i \le 3\}$$

であることを思い出すと，$Z_{x_f}(\overline{K})$ を通る二本の直線の和集合は，

$$\begin{aligned}C_1 &= (P_0, P_1 \text{ を通る直線}) \cup (P_2, P_3 \text{ を通る直線}),\\ C_2 &= (P_0, P_2 \text{ を通る直線}) \cup (P_1, P_3 \text{ を通る直線}),\\ C_3 &= (P_0, P_3 \text{ を通る直線}) \cup (P_1, P_2 \text{ を通る直線})\end{aligned}$$

[*1] より一般の設定で，レゾルベントを考えることもできる（[SM85]）．f の根たちの多項式 $\beta = F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ を取り，Galois 群 G での固定部分群を H とおく．$\sigma \in G/H$ についての $X - \sigma(\beta)$ を掛けると，基礎体 K 係数の多項式が得られる．これがレゾルベント $R_{f,F}(X)$ である．なお，$K(\beta)$ は一般には H-不変部分体になるとは限らない．

の 3 つあるが，C_1, C_2, C_3 がそれぞれ $\beta_1, \beta_2, \beta_3$ に対応するわけである．

なお，f が既約であるとき，c_f がいつ既約になるかも決定できる．$K(\alpha)$ の Galois 閉包 $K(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ について，$\mathrm{Gal}(K(\alpha_0, \alpha_1, \alpha_2, \alpha_3)/K)$ が四次対称群 $\mathfrak{S}_4$ もしくは交代群 $\mathfrak{A}_4$ なら三次レゾルベント c_f は既約になり，それ以外は c_f は既約にならないことがわかる．R_x が四次拡大体に，かつ c_f が既約な三次多項式になる場合は**強既約** *strongly irreducible* と呼ばれ，[鈴木雄] で扱う対象になる．

1.3 Wright–Yukie の理論から

Wright–Yukie [WY92] では，いくつかの概均質ベクトル空間の開軌道に入る元 $x \in V'(K)$ について，点の集合 $Z_x \subseteq \mathbb{P}^n$ を対応させるなどして，分離代数との対応を論じている．いくつかの例を見てみよう．

例 1.5（[谷口 1, §3.1]） K の標数は 2 でないとする．$V = K, G = \mathrm{GL}_1$ とし，$\lambda \cdot x = \lambda^2 x$ で作用を定める．すると，$G(K) \setminus V'(K)$ は二次分離代数の同型類と対応する．

例 1.6（[WY92, §2]） $V = 4 \otimes \bigwedge^2 5, G = \mathrm{GL}_4 \times \mathrm{GL}_5$ とする．これは五元二次交代形式の四つ組，あるいは五次交代行列の四つ組と考えられる．G の作用は $2 \otimes \mathrm{Sym}^2 3$ の場合と同様に入れると，概均質ベクトル空間になる．このとき $G(K) \setminus V'(K)$ は五次分離代数の同型類と対応する．この場合には，Z_x として $\mathbb{P}^3$ の五点を対応させる．

例 1.7（[谷口 1, §3.3]） すでに見た内容ではあるが，異なる表現が同じ分離代数をパラメータ付けしていることがある．$V = \mathrm{Sym}^2 2, G = \mathrm{GL}_1 \times \mathrm{GL}_2$ とすれば，$G(K) \setminus V'(K)$ は二次分離代数の同型類と対応する．Z_x としては，二元二次形式 $x(u, v)$ の零点集合を対応させる．これは $\overline{K}$ 上では二点になる．

例 1.8（[WY92, §3]） 三元二次形式の対 $x \in 2 \otimes \mathrm{Sym}^2 3$ について $f_x \in \mathrm{Sym}^3 2$ を考えることが，幾何的にも代数的にも意味を持つことをこれまでに紹介した．この写像は $g = (g_2, g_3) \in \mathrm{GL}_2 \times \mathrm{GL}_3$ を $g' = (\det(g_3)^2, g_2) \in \mathrm{GL}_1 \times \mathrm{GL}_2$ に送ることで，$f_{gx} = g' f_x$ となり，「同変」な写像になっている．このような表現の間の同変な写像はほかにもある．

$V = 2 \otimes 2 \otimes 2, G = \mathrm{GL}_2^3$ とする．

$$K^2 \otimes K^2 \otimes K^2 = (K^2 \otimes K^2) \oplus (K^2 \otimes K^2)$$

であるから，$V(K)$ の要素は 2×2 の行列 2 つ組 $x=(M_1,M_2)$ と思うことができる．すると，$f_x(u,v)=\det(M_1u+M_2v)$ は二元二次形式であり，$g=(g_1,g_2,g_3)\in G(K)$ について $g'=(\det g_2 \det g_3, g_1)\in \mathrm{GL}_1(K)\times\mathrm{GL}_2(K)$ とすると，$f_{gx}=g'f_x$ である．

ただし，この場合 $G(K)\setminus V'(K)$ としては同じ二次分離代数の同型類を対応させるので，軌道を代数で解釈すると恒等写像になってしまう．

例 1.9（[WY92, §3]） $V=2\otimes 3\otimes 3, G=\mathrm{GL}_2\times\mathrm{GL}_3^2$ とする．$V(K)$ の要素は 3×3 の行列 2 つ組 $x=(M_1,M_2)$ と思うことができる．すると，$f_x(u,v)=\det(M_1u+M_2v)\in \mathrm{Sym}^3 2$ である．

この場合も，$G(K)\setminus V'(K)$ としては同じ三次分離代数の同型類を対応させる．

別の論文に目を向ければ，K 上の四元数環や八元数環の同型類と対応する軌道が取り扱われている．前者は [Yuk, Section 11], 後者については [Yuk, Section 20] および [WYZ00] を参照のこと．

2 整軌道の解釈：高次合成則

Wright–Yukie 理論は分離代数と有理軌道との対応であった．これと対比すると，Bhargava による高次合成則は n 次環と整数上の軌道（整軌道）との対応にしたものと考えられる．ポイントはレゾルベント構造と，極大性が局所条件であることである．この節のより詳細な解説は [谷口 11] を参照のこと．

2.1 n 次環と基本判別式

まず n 次環の定義から始めよう．これは n 次代数の整数環類似になっている．

定義 2.1 $n\geq 2$ について，可換環 R が n **次環** *n-ic ring* とは，アーベル群として $R\cong\mathbb{Z}^n$ であることである．

例 2.2 いくつかの例を挙げておく．

- $R=\mathbb{Z}^n, \mathbb{Z}[x]/(x^n)$ は n 次環である．
- $K/\mathbb{Q}$ を n 次拡大とすると，整環 $\mathcal{O}\subseteq K$ は n 次環である．
- R,S を r,s 次環とすれば $R\times S$ は $r+s$ 次環である．また，$n\geq 1$ について $R_n=\mathbb{Z}+nR$ も r 次環となる．

たとえば $R = \mathbb{Z}[\sqrt{2}]$ は二次環．その部分環 $R_2 = \mathbb{Z}[2\sqrt{2}]$ は整環で，やはり二次環．その直積 $\mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[2\sqrt{2}]$ は四次環である．

より一般に，R_0 を可換環，R を R_0 代数とするとき，R が n 次の R 代数とは，R_0 加群として $R \cong R_0^n$ であることとする．R_0 が体 K のときは，K 上の n 次分離代数は n 次 K 代数であるが，逆は成立しない．

n 次環で分離代数にあたるものを定義するため，跡写像 $\mathrm{Tr} = \mathrm{Tr}_{R/\mathbb{Z}} \colon R \to \mathbb{Z}$ を考えよう．これは $r \in R$ について，$\times r \colon R \to R$ を n 次行列表示したときのトレースのことである．

定義 2.3　R を n 次環，$(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ を $\mathbb{Z}$ 基底とする．R の**判別式** *discriminant* を，$\mathrm{Disc}(R) \coloneqq \det(\mathrm{Tr}(\alpha_i\alpha_j))_{0\le i,j\le n-1}$ で定義する．

判別式は R の $\mathbb{Z}$ 基底の取り方に依存しない．これは

$$(\beta_0, \beta_1, \ldots, \beta_{n-1}) = (\alpha_0, \ldots, \alpha_{n-1})g \ (g \in \mathrm{GL}_n(\mathbb{Z}))$$

と取り替えたとき，

$$\begin{aligned}\det(\mathrm{Tr}(\beta_i\beta_j))_{0\le i,j\le n-1} &= \det\left({}^t g \det(\mathrm{Tr}(\alpha_i\alpha_j))_{0\le i,j\le n-1} g\right)\\ &= \det(g)^2 \det(\mathrm{Tr}(\alpha_i\alpha_j))_{0\le i,j\le n-1}\end{aligned}$$

となるが，$g \in \mathrm{GL}_n(\mathbb{Z})$ について $\det(g)^2 = 1$ だからである．なお一般の R_0 上では，判別式は R_0^{*2} 倍を除いてのみ定義される．

例 2.4　先に挙げた例のいくつかで見てみる．

- $\mathrm{Disc}(\mathbb{Z}^n) = 1, \mathrm{Disc}(\mathbb{Z}[x]/(x^n)) = 0.$
- n 次拡大 $K/\mathbb{Q}$ の整数環 $\mathcal{O}_K \subseteq K$ については $\mathrm{Disc}(\mathcal{O}_K)$ が K の判別式 $\mathrm{Disc}(K)$ の定義であった．
- $\mathrm{Disc}(R \times S) = \mathrm{Disc}(R)\,\mathrm{Disc}(S).$
- R の $\mathbb{Z}$ 基底を $\omega_0 = 1, \omega_1, \omega_2, \ldots, \omega_{n-1}$ とすると（命題 2.5 参照），$R_k = \mathbb{Z} + kR$ の $\mathbb{Z}$ 基底は $\omega_0 = 1, k\omega_1, k\omega_2, \ldots, k\omega_{n-1}$ である．すると $\mathrm{Disc}(R_k) = k^{2(n-1)}\,\mathrm{Disc}(R)$ である．

$\mathrm{Disc}(R) \neq 0$ であるような n 次環を非退化 nondegenerate な n 次環と呼ぶ．これは分離代数の整数版である．

2.1.1 小さな次数の環の分類

つぎに $n = 1, 2$ の場合を調べておこう．そのために次の補題を用意しておく．

命題 2.5（[谷口 11, 補題 2.1]） n 次環 R の $\mathbb{Z}$ 基底の一つとして，R の単位元 1_R を取ることができる．つまり $R/\mathbb{Z}\cdot 1_R$ は自由加群.

証明 もし $r \in R$ と $n \geq 2$ で $nr = 1_R$ となるものが見つかると，r で生成される部分環 $\mathbb{Z}[r] \subseteq R$ は $\mathbb{Z}[1/n]$ に同型で，有限生成でない $\mathbb{Z}$ 加群になる．これは Noether 環の有限生成加群の部分加群が有限生成であることに矛盾する． □

$n = 1$: $R = \mathbb{Z}1_R$ は $\mathbb{Z}$ に標準的に同型になる．

$n = 2$: $R = \mathbb{Z}1_R + \mathbb{Z}\tau$ とおく．$\tau^2 = a\tau + b$ と表示できるが，τ の代わりに $\tau - m$ を考えることで，$a = 0, 1$ としてよい．このような m の取り方は一つしかない．

(1) $a = 0$ のとき：$R \cong \mathbb{Z}[u]/(u^2 - b)$ で，$\mathrm{Disc}(R) = 4b$.
(2) $a = 1$ のとき：$R \cong \mathbb{Z}[u]/(u^2 - u - b)$ で，$\mathrm{Disc}(R) = 4b + 1$.

すると，二次環 R から $\mathrm{Disc}(R)$ を与える写像は，同型類からの全単射であることがわかる．

命題 2.6 次の対象の間に，自然な全単射が存在する：

- 二次環の同型類.
- $d \in \mathbb{Z}$ であって，$d \equiv 0, 1 \pmod 4$ であるようなもの.

注意 2.7 なお，R の $\mathbb{Z}$-基底 $1_R, \tau'$ であって $\tau'^2 = a'\tau' + b'$ $(a' = 0, 1)$ を満たすものは τ のほかに $a - \tau$ が存在する．$\tau, a - \tau$ は同じ方程式を満たすので，$\tau \mapsto a - \tau$ は 2 次環の自己同型 $R \to R$ を誘導する．

この自己同型の存在は少し厄介なので，$\mathbb{Z}$ 加群としての同型 $\iota\colon R/\mathbb{Z}1_R \cong \mathbb{Z}\tau \xrightarrow{\cong} \mathbb{Z}$ のデータを加えた (S, ι) の組を考えることがある（向き付き二次環 oriented quadratic ring と呼ぶ）．詳しくは [谷口 11], [Bha04a] 参照.

2.2 Levi–Delone–Faddeev 対応

さて，いよいよ本論の一つである次の対応を紹介しよう．

定理 2.8（Levi [Lev14], Delone–Faddeev [DF64], ...） 次の対象の間に，自然な全単射が存在する：

- 三次環の同型類.
- 軌道の集合 $\mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{Sym}^3 \mathbb{Z}^2$.

ただし，$g = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ は f に

$$(gf)(u,v) = \frac{1}{\det g} f(pu+rv, qu+sv)$$

で作用する.

この構成のあらすじを紹介する．三次環 R の $\mathbb{Z}$-基底 $1_R, \omega, \theta$ を取る．このとき適当な $m_1, m_2 \in \mathbb{Z}$ について ω, θ を $\omega - m_1, \theta - m_2$ に取り替えると，$\omega\theta \in \mathbb{Z}1_R$ としてよい．この操作（正規化）は二次環において τ を $\tau - m$ に取り替えた操作に対応する.

するとある $a,b,c,d,k,\ell,m \in \mathbb{Z}$ を用いて次のように環構造を記述できる：

$$\begin{cases} \omega\theta = k, \\ \omega^2 = \ell - b\omega + a\theta, \\ \theta^2 = m - d\omega + c\theta. \end{cases}$$

種明かしをすると，この場合には $au^3 + bu^2v + cuv^2 + dv^3$ を対応させるのである．k, ℓ, m が決まらないように見えるが，結合法則によって $\omega^2 \cdot \theta = \omega \cdot \omega\theta, \omega \cdot \theta^2 = \omega\theta \cdot \theta$ であり，この係数を比較すると

$$k = -ad,\ \ell = -ac,\ m = -bd$$

が従う[*2]．ω, θ の取替が $\mathrm{GL}_2(\mathbb{Z})$ 作用に対応する.

なお，有理軌道と比べて代数群 $\mathrm{GL}_1 \times \mathrm{GL}_2$ と作用が変わってしまったように見えるが，$(g_1, g_2) \in \mathrm{GL}_1 \times \mathrm{GL}_2$ の作用は今回の作用の $g_1 \det(g_2) I_2 \cdot g_2 \in \mathrm{GL}_2(\mathbb{Z})$ の作用に一致するので，軌道自体は一致している.

[*2] この 1_R の係数がほかの係数から一意的に決定される現象は $n \geq 4$ についての n 次環でも成り立つ ([KY04, Lemma 2]).

2.3 四次環の高次合成則：レゾルベント構造

四次環に移ろう．このまま四次環の同型類が $\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3$ の $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ 軌道に対応すると言いたいところだが，それでは足りないのである．

前節の四次分離代数の場合，三元二次形式のペア $x = (A, B) \in K^2 \otimes \mathrm{Sym}^2 K^3$ から二元三次形式 $f_x(u, v) = 4\det(M_A u + M_B v) \in \mathrm{Sym}^3 K^2$ を構成でき，それが「三次レゾルベント代数」とでも呼ぶべき三次分離代数に対応していた．Bhargava [Bha04c] によれば，この三次レゾルベント代数の整数版である三次レゾルベント環を導入することが必要だったのである．

2.3.1 形式 Galois 閉包

四次分離代数が $\mathfrak{S}_4$ を Galois 群に持つとき，三次レゾルベントを考えるに当たっては，まず Galois 閉包が活躍していた．そこで Galois 閉包の形式化を考える．

定義 2.9（[Bha04c], cf. [BSat14]） n 次環 R の形式 Galois 閉包 formal Galois closure とは，次のようにして構成される環 $\overline{R}$ である．

(1) n^n 次環 $R^{\otimes n}$ を考え，$r \in R$ と $1 \le i \le n$ について

$$\sigma_i(r) = 1_R \otimes 1_R \otimes \cdots \otimes \overset{i}{\hat{r}} \otimes \ldots 1_R$$

とおく．これは環準同型 $R \to R^{\otimes n}$ を定める．

(2) n^n 次環 $R^{\otimes n}$ のイデアルで，$r \in R$ について

$$\sigma_1(r) + \sigma_2(r) + \cdots + \sigma_n(r) - \mathrm{Tr}(r) 1_R^{\otimes n}$$

で生成されるものを I_R とおく．

(3) ある整数 $m \ge 2$ について $mr \in I_R$ となるような $r \in R^{\otimes n}$ 全体を J_R とおく．これもイデアルである．

(4) $\overline{R} \coloneqq R^{\otimes n}/J_R$ とする．

大雑把に言うと，$r \in R$ について $r^n - a_1 r^{n-1} + \cdots \pm a_n = 0$ となるなら，$\sigma_1(r), \ldots, \sigma_n(r)$ たちの k 次対称式が a_k となるような環である．また $\sigma_i(r)$ の像たちは，$\overline{R}$ における「r の共役」にあたる．$R^{\otimes n}$ には成分の入れ替えで $\mathfrak{S}_n$ が作用し，

I_R, J_R はその作用で不変であるから，$\overline{R}$ についても $\mathfrak{S}_n$ が作用することになる．これが Galois 群の代わりになる．そして R が非退化なら，$\overline{R}$ は $n!$ 次環になる．

注意 2.10（[BSat14]） 退化している場合は状況が異なってくる．実際 $n = 4$ の場合で $R = \mathbb{Z}[x, y, z]/(x^2, y^2, z^2, xy, yz, zx)$ とおくと，$\overline{R}$ は 32 次環になると証明されている [BSat14, §9]．このことの応用として，J_R で割る今回の定義では，形式 Galois 閉包の構成が底変換と可換でないことがわかる [BSat14, Remark 7]．したがってレゾルベント環の定義は別の定義が必要になる [Bha04c, §3.9].

[BSat14] では別の定義を採用している．この場合は底変換と可換だが，$\overline{R}$ には torsion が入ってきて，一般には m 次環にならない．この点は鈴木雄太氏にご指摘いただいた．

2.3.2 三次レゾルベント環

三次レゾルベント環では，α について $\beta = \alpha_0\alpha_1 + \alpha_2\alpha_3$ のような元を考えることが重要だった．いま Galois 閉包にあたる環と R の元の共役ができたので，形式的に真似して写像を構成しよう．

非退化な四次環 Q について，**三次レゾルベント写像** *cubic resolvent map* $\widetilde{\phi}_{4,3}\colon Q \to \overline{Q}$ を次で定義する：

$$\begin{aligned}\widetilde{\phi}_{4,3}(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha) + \sigma_3(\alpha)\sigma_4(\alpha)\\ &= \alpha\otimes\alpha\otimes 1_R\otimes 1_R + 1_R\otimes 1_R\otimes\alpha\otimes\alpha.\end{aligned}$$

注意として，これは R 加群の準同型ではなく，いわゆる二次写像になっている．また像は $D_4 = \langle(12), (34), (13)(24)\rangle \subsetneq \mathfrak{S}_4$ について不変であり，したがって $\overline{Q}^{D_4}$ に属する．

次に三次不変環 cubic invariant ring $R^{\mathrm{inv}}(Q)$ を，$\mathbb{Z}$ 上 $\mathrm{Im}(\widetilde{\phi}_{4,3}(Q))$ で生成される $\overline{Q}$ の部分環とする．非自明なことだが，これは三次環になる．ところが，一般には $\mathrm{Disc}(R^{\mathrm{inv}}(Q)) \neq \mathrm{Disc}(Q)$ である．形式のレベルでは $\mathrm{Disc}(A, B) = \mathrm{Disc}(f_{A,B})$ であるにも関わらずだ．したがって $R^{\mathrm{inv}}(Q)$ ではない環を対応させる必要がある．そこで，最終的な定義は以下のようになる：

定義 2.11（[Bha04c, Definition 8]） 非退化な四次環 Q の**三次レゾルベント環** *cubic resolvent ring* とは，三次環 $C \subseteq \overline{Q}^{D_4} \otimes \mathbb{Q}$ であって，$C \supseteq R^{\mathrm{inv}}(Q)$ となり，なおかつ $\mathrm{Disc}(C) = \mathrm{Disc}(Q)$ となるもののことである．

つまり $\mathrm{Disc}(Q) = \mathrm{Disc}(C)$ であって，三次レゾルベント写像 $\widetilde{\phi}_{4,3}$ が $Q \to C$ という写像として定義できるということである（この定義は非退化の場合のみ）．この定義を導入すると，めでたく軌道との対応が構成できる．

定理 2.12（[Bha04c, Theorem 1]） 次の集合の間に，判別式を保つ全単射が存在する：

- 非退化な四次環 Q, 三次環 C および三次レゾルベント写像 $\widetilde{\phi}_{4,3} : Q \to C$ の組 $(Q, C, \widetilde{\phi}_{4,3})$ の同型類.
- 相対不変式 P が消えない軌道の集合 $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z}) \setminus (\mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3)'$.

片方の構成だけを具体的に見ておこう．$\widetilde{\phi}_{4,3}(r+m)$ を計算してみると，

$$\begin{aligned}\widetilde{\phi}_{4,3}(r+m) &= (r+m)\otimes(r+m)\otimes 1\otimes 1 + 1\otimes 1\otimes(r+m)\otimes(r+m)\\ &= r\otimes r\otimes 1\otimes 1 + 1\otimes 1\otimes r\otimes r + m(\sigma_1(r)+\sigma_2(r)+\sigma_3(r)+\sigma_4(r)) + 2m^2\\ &\equiv \widetilde{\phi}_{4,3}(r) + m\,\mathrm{Tr}(r) + 2m^2\end{aligned}$$

となるため，$C/\mathbb{Z}1_C$ の類は変わらない．したがって $\widetilde{\phi}_{4,3}$ は $\phi_{4,3}\colon Q/\mathbb{Z}1_Q \to C/\mathbb{Z}1_C$ を誘導するが，$Q/\mathbb{Z}1_Q \cong \mathbb{Z}^3, C/\mathbb{Z}1_C \cong \mathbb{Z}^2$ から，この $\phi_{4,3}$ が三元二次形式のペアとして表示できるのである．また退化した場合にも，「Disc が四次環 Q と一致して，二次写像 $\phi_{4,3}\colon Q/\mathbb{Z}1_Q \to C/\mathbb{Z}1_C$ が定義できる三次環 C」とレゾルベント環の定義を取り替えることで拡張できる．詳細は元論文 [Bha04c] を参照してほしい．

2.3.3 三次レゾルベント環の個数

ところで，上のように定義すると，与えられた四次環について三次レゾルベント環が一つあるかどうかもわからないが，実際には必ず一つ以上はあることがわかる．その前に用語を一つ定義する．

R を非退化な n 次環としたとき，その内容 content を

$$\mathrm{ct}(R) \coloneqq \max_{m\in\mathbb{Z}}(\exists R' : n\text{ 次環}, R = \mathbb{Z} + mR')$$

として定義する．

この定義は見た目ほど難しいものではない．R' の整基底を $1_{R'} = 1_R, \alpha_1, \ldots, \alpha_{n-1}$ とすると，$R = \mathbb{Z} + mR'$ の整基底は $1_{R'} = 1_R, m\alpha_1, \ldots, m\alpha_{n-1}$ である．R' の構造

定数 $c_{i,j}^k$ を

$$\alpha_i\alpha_j = c_{i,j}^0 + \sum_{1\le k\le n-1} c_{i,j}^k \alpha_k$$

とすると，R の構造定数は

$$(m\alpha_i)(m\alpha_j) = m^2 c_{i,j}^0 + \sum_{1\le k\le n-1} m c_{i,j}^k (m\alpha_k)$$

からすべて m の倍数になる．逆に R の構造定数たちがすべて m の倍数なら，1_R 以外の基底を $1/m$ 倍して，$R = \mathbb{Z} + mR'$ となる環 R' を構成できる．したがって，$\mathrm{ct}(Q)$ は構造定数の最大公約数である．

事実 2.13（[Bha04c, Corollary 4]） 非退化な四次環 Q について，その三次レゾルベント環は $\sigma_1(\mathrm{ct}(Q)) = \sum_{d|\mathrm{ct}(Q)} d$ 個だけ存在する．特に，一つ以上は三次レゾルベント環が存在する．

また，$\mathrm{ct}(Q) = 1$ のときは $R^{\mathrm{inv}}(Q)$ が唯一の三次レゾルベント環になることが証明されている [Bha04c, Corollary 18].

2.3.4 極大性

関連する概念である極大性について考えておく．n 次環 R について，別の n 次環 R' で $R' \supsetneq R$ となるものが見つからないとき，R は**極大** *maximal* であるという．

例 2.14 n 次環 R について $R_m = \mathbb{Z} + mR$ とすると $m \ge 2$ なら $R \supsetneq R_m$ である．したがって $\mathrm{ct}(R) > 1$ であれば R は極大ではない．極大なら $\mathrm{ct}(R) = 1$ である．

例 2.15 n 次体 $K/\mathbb{Q}$ について，その整数環 $\mathcal{O}_K$ は極大である．このことと前小小節の結果を合わせると，$\mathcal{O}_K$ の三次レゾルベント環は $R^{\mathrm{inv}}(\mathcal{O}_K)$ 唯一に定まることがわかる．

ところで，n 次 $\mathbb{Z}_p$ 代数 R についても類似の条件を考えられる．別の n 次 $\mathbb{Z}_p$ 代数 R' で $R' \supsetneq R$ となるものが見つからないとき，R は n 次 $\mathbb{Z}_p$ 代数として極大 maximal であるという．そして n 次環 R について，$R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ が n 次 $\mathbb{Z}_p$ 代数として極大であるとき，R は p **で極大** *maximal at* p であるという．

事実として，以下がわかる：

- n 次環 R が極大であることは，すべての素数 p について p で極大であることと同値.
- 四次環 R が p で極大であることは，対応する点 $x \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3$ の $\bmod p^2$ の合同条件で定義される [Bha04c, §4].
- 非退化な n 次環 R が極大なら，R は整数環の直積である.

特に，強既約な $x \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2 \mathbb{Z}^3$ の軌道であって，上記の $\bmod p^2$ の合同条件を満たすものを数えることは，Galois 群が $\mathfrak{S}_4$ になる四次体を数えることに対応することがわかる.

2.4 その他の高次合成則

Wright–Yukie 理論のときのように，ほかのいくつかの表現についてその整軌道の解釈が知られている.

例 2.16（[Bha08]） $V(\mathbb{Z}) = \mathbb{Z}^4 \otimes \bigwedge^2 \mathbb{Z}^5, G(\mathbb{Z}) = \mathrm{GL}_4(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z})$ とすると，次の 2 つの集合の間に，判別式を保つ全単射が存在する：

- 五次環 Q，六次レゾルベント環 S と六次レゾルベント写像 $\widetilde{\phi}_{5,6} \colon Q \to C$ の同型類.
- 整軌道の集合 $G(\mathbb{Z}) \setminus V(\mathbb{Z})$.

この対応は五次体の数え上げに用いられている.

例 2.17（[Bha04b]） $V(\mathbb{Z}) = \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3, G(\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})^2$ とする．このとき次の 2 つの集合の間に，判別式を保つ全単射が存在する：

- 三次環 C とその “分数イデアル” I, I' の三つ組 (C, I, I') で，$II' \subseteq C, N(I)N(I') = 1$ を満たすものの同値類.
- 整軌道の集合 $G(\mathbb{Z}) \setminus V(\mathbb{Z})$.

これを利用すると，三次体のイデアル類群を軌道として解釈できる．また，前節で考えた同変な写像 $x = (M_1, M_2) \mapsto f_x(u, v) = \det(M_1 u + M_2 v)$ について代数側で解釈すると，(C, I, I') から C だけを抽出する写像になっている．有理軌道では見られなかった現象である.

なおこの三次環の場合の類似として，$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ の軌道についても「二次環＋特定の条件を満たす分数イデアル三つ」の同値類という解釈が見つかるほか，$\mathrm{Sym}^2 \mathbb{Z}^2$ の軌道も「二次環＋分数イデアル」の同値類という解釈が見つかる [Bha04a]．特に後者は退化した環にも拡張できるという意味で，いわゆる Gauss の合成則の拡張になっている．

しかし注 2.7 で見た「向き付けられた二次環」を考える必要が出たり，「向き付きのイデアル」や上記の同値関係を定義したりと，定義すべき内容が非常に多くなってしまうので，ここでは割愛する．

参考文献

[Bha04a] M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. *Ann. Math.* **158** (2004), 217–250.

[Bha04b] M. Bhargava, Higher composition laws II: On cubic analogues of Gauss composition. *Ann. Math.* **159** (2004), 865–886.

[Bha04c] M. Bhargava, Higher composition laws III: The parametrization of quartic rings. *Ann. Math.* **159** (2004), 1329–1360.

[Bha08] M. Bhargava, Higher composition laws IV: The parametrization of quintic rings. *Ann. Math.* **167** (2008), 53–94.

[BSat14] M. Bhargava and M. Satriano, On a notion of “Galois closure” for extensions of rings. *J. Eur. Math. Soc.* **16** (2014), no.9, 1881–1913.

[DF64] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, vol.10, American Mathematical Society, 1964.

[KY04] A. C. Kable and A. Yukie, A construction of quintic rings, *Nagoya Math. J.* **173** (2004), 163–203.

[Lev14] F. Levi, Kubische zahlkörper und binäre kubische formen klassen, Ber. S̈achs. Akad. Wiss. Leipzig, Math.-Naturwiss **66**(1914), 26–37.

[SM85] L. Soicher and J. McKay, Computing Galois Groups over the Rationals, J. Number Th. **20** (1985) 273–281.

[WY92] D. Wright and A. Yukie, *Prehomogeneous vector spaces and field extensions*, Inv. Math. **110** (1992), 283–314.

[WYZ00] D. Witte, A. Yukie and R. Zierau, Prehomogeneous vector spaces and Ergodic theory II, Trans. Amer. Math. Soc. **352** (2000), 1687–1708.

[Yuk] A. Yukie, Rational orbit decomposition of prehomogeneous vector spaces. Available from https://www.math.kyoto-u.ac.jp/˜yukie/.

[石塚] 石塚裕大，三元二次形式のペアと射影空間の幾何．**本報告集**，2023.

[佐野] 佐野薫，余正則空間と楕円曲線のセルマー群．**本報告集**，2023.

[鈴木美] 鈴木美裕，保型形式付き概均質ゼータ関数．**本報告集**，2023.

[鈴木雄] 鈴木雄太，整数軌道の数え上げ：数の幾何と平均法．**本報告集**，2023.

[谷口 11] 谷口隆，高次合成則入門．**数理解析研究所講究録別冊 B25** (2011), 211–253.

[谷口 1] 谷口隆，例で学ぶ概均質ベクトル空間．**本報告集**，2023.

[谷口 2] 谷口隆，本論のための準備．**本報告集**，2023.

[Thorne] F. Thorne，Counting integral orbits : Zeta function method．**本報告集**，2023.