# 有限代数的数とその計算例

山本 修司 (慶應義塾大学)

## 1 イントロダクション

本稿では論文 [6] に基づいて有限代数的数の理論を説明し, いくつかの計算例を挙げる. 講演では「素数の分解法則」, すなわち与えられた ($\mathbb{Q}$ 上 Galois な) 代数体において完全分解する素数を線型回帰数列によって記述する定理を中心に述べたが, これについては別のところで ($S$ 整数への精密化も合わせて) 日本語の解説を書いた[1]. そこで重複を避けるために, 本稿ではこれらに関する解説は最小限に留め, 有限代数的数の計算例, とくに重さ 1 のモジュラー形式と関係する例と, それらに関する若干の考察を紹介することを中心にする. なおこれらの計算例の多くは田坂浩二氏によるものであり, 考察は同氏と筆者とで遂行中の共同研究に基づく.

## 2 有限代数的数

有限代数的数は J. Rosen によって導入された概念である. ここではその二通りの特徴づけを簡単に復習する. 詳細については [4] や [6] を参照されたい.

**定義 2.1.** $\mathbb{Q}$ 代数 $\mathcal{A}$ を

$$\mathcal{A} := \prod_p \mathbb{F}_p \Big/ \bigoplus_p \mathbb{F}_p \cong \mathbb{Q} \otimes_{\mathbb{Z}} \prod_p \mathbb{F}_p$$

で定義する. ただし直積や直和における $p$ はそれぞれ全ての素数をわたる.

記号を濫用して, 直積の元 $(a_p)_p \in \prod_p \mathbb{F}_p$ で代表される $\mathcal{A}$ の元を, しばしば同じ記号で $(a_p)_p \in \mathcal{A}$ と表す. $(a_p)_p, (b_p)_p \in \mathcal{A}$ が一致するのは, ほとんど (=有限個を除く) 全ての素数 $p$ において $a_p = b_p$ が成り立つときである. またこれより, ほとんど全ての素数 $p$ において $a_p \in \mathbb{F}_p$ が与えられれば $(a_p)_p \in \mathcal{A}$ は定義されることに注意する.

有限代数的数全体は $\mathcal{A}$ の部分 $\mathbb{Q}$ 代数をなす. その一つ目の特徴づけ (以下ではそれを定義として採用する) は, Galois 群上の関数環を使って記述される. 以下, $L/\mathbb{Q}$ を有限次 Galois 拡大とし, その Galois 群を $G$ と書く.

**定義 2.2.** (1) $G$ 上の $L$ 値関数全体のなす環 $\mathrm{Fun}(G, L)$ において, 群 $G$ の作用を

$$(\sigma g)(\tau) := \sigma\big(g(\sigma^{-1}\tau\sigma)\big) \quad (\sigma, \tau \in G,\ g \in \mathrm{Fun}(G, L))$$

と定義し, その不変元のなす部分環を

$$A(L) := \mathrm{Fun}(G, L)^G = \big\{ g \colon G \to L \;\big|\; \sigma g = g\ (\forall \sigma \in G) \big\}$$

と表す.

[1] 2023 早稲田整数論研究集会の報告集に収録予定.

(2) $L/\mathbb{Q}$ で不分岐な素数 $p$ に対し, その上の素イデアル $\mathfrak{p}$ を一つとり, 付随する Frobenius 自己同型を $\phi_{\mathfrak{p}} \in G$ で表す. すると任意の $g \in A(L)$ に対して $\mathrm{ev}(g) \in \mathcal{A}$ が

$$\mathrm{ev}(g) := \big(g(\phi_{\mathfrak{p}}) \bmod \mathfrak{p}\big)_p$$

と定義される (この定義の整合性については [6] の §2.3 および §2.5 を参照されたい).
(3) 上で定義された写像 $\mathrm{ev}\colon A(L) \to \mathcal{A}$ は $\mathbb{Q}$ 代数の単射準同型である. その像を

$$\mathcal{P}_L^{\mathcal{A}} := \mathrm{ev}\big(A(L)\big) \subset \mathcal{A}$$

と表し, その元を ($L$ 上定義された) 有限代数的数という.

有限代数的数の二つ目の特徴づけは, 線型回帰数列を用いて与えられる.

**定義 2.3.** (1) 有理係数のモニック多項式 $f(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Q}[x]$ に対し, $f$ を特性多項式とする線型漸化式を満たす有理数列全体の空間を

$$\mathrm{Rec}(f;\mathbb{Q}) := \left\{ (a_m)_m \in \prod_{m\geq 0} \mathbb{Q} \;\middle|\; a_m + c_1 a_{m-1} + \cdots + c_d a_{m-d} = 0 \ (\forall m \geq d) \right\}$$

で表す.
(2) $\mathbb{Q}$ 線型写像 $r_f\colon \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{A}$ を

$$r_f\big((a_m)_m\big) := (a_p \bmod p)_p$$

と定義する (一般項 $a_m$ の分母を割る素数は, たかだか $f$ の係数 $c_1, \ldots, c_d$ および数列の初期値 $a_0, \ldots, a_{d-1}$ の分母を割る素数のみであり, それら有限個の素数 $p$ を除いて $a_p \bmod p \in \mathbb{F}_p$ は定まる).

**定理 2.4** (cf. [6, Theorem 2.9])**.** 多項式 $f(x)$ が $L$ において 1 次式の積に分解するとき, $r_f\colon \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{A}$ の像は $\mathcal{P}_L^{\mathcal{A}}$ に含まれる. さらに $f(x)$ が拡大 $L/\mathbb{Q}$ における正規底の最小多項式であるならば, $r_f\colon \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{P}_L^{\mathcal{A}}$ は全単射である.

**注意 2.5.** 与えられた有理数列 $(a_m)_m$ から $(a_p \bmod p)_p \in \mathcal{A}$ が定まっているとき, それが $\mathcal{A}$ において 0 でないことを証明するのはしばしば困難である. 例えば, 有限多重ゼータ値

$$\zeta_{\mathcal{A}}(k_1, \ldots, k_r) := \left( \sum_{0<n_1<\cdots<n_r<p} \frac{1}{n_1^{k_1} \cdots n_r^{k_r}} \bmod p \right)_p \in \mathcal{A}$$

は近年盛んに研究されている対象であるが, その中に (自明な $r = 0$ の場合を除いて) 0 でないものが存在することは証明されていない (cf. [7]). この種の問題の難しさに鑑みれば, 定義 2.2 の写像 $\mathrm{ev}\colon A(L) \to \mathcal{A}$ や定理 2.4 の後半における $r_f\colon \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{A}$ の単射性は著しい事実というべきである.

定理 2.4 を通じて, Galois 拡大 $L/\mathbb{Q}$ に付随する環 $A(L) = \mathrm{Fun}(G, L)^G$ に含まれる数論的な情報を, $\mathrm{Rec}(f;\mathbb{Q})$ に属する数列を使って記述することができる. 例えば次の定理が直ちに得られる:

**定理 2.6** (cf. [6, Theorem 1.1])**.** 有限次 Galois 拡大 $L/\mathbb{Q}$ に対し, 線型漸化式を満たす有理数列 $(a_m)_{m\geq 0}$ が存在して, ほとんど全ての素数 $p$ に対して

$$a_p \equiv \begin{cases} 1 \pmod{p} & (p \text{ が } L/\mathbb{Q} \text{ で完全分解するとき}), \\ 0 \pmod{p} & (\text{それ以外のとき}) \end{cases}$$

を満たす.

なおこの定理において除外された有限個の例外素数を具体的に決定することは重要であるが, $\mathbb{Q}$ 代数 $\mathcal{A}$ の中で理論を考える限りそれは達成されない. この問題は, 素数の有限集合 $S$ に対し, 有限代数的数の理論を $\mathbb{Q}$ 上から $S$ 整数環 $\mathbb{Z}_S$ 上に精密化することで解決される. 詳細は [6, §4] を参照されたい.

## 3 計算例

**例 3.1.** $L = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ とおく.

$$f(x) = x^6 + 3x^5 + 12x^4 + 25x^3 + 60x^2 + 51x + 127$$

とおくと, その根は $L/\mathbb{Q}$ における正規底をなす. 数列 $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ を初期値

$$(a_0, \ldots, a_5) = \left(-\frac{1}{3}, 1, 0, -\frac{10}{3}, 7, -20\right)$$

で定義すると, ほとんど全ての素数 $p$ に対して

$$a_p \equiv \begin{cases} 1 \pmod{p} & (p \text{ が } L/\mathbb{Q} \text{ で完全分解するとき}), \\ 0 \pmod{p} & (\text{それ以外のとき}) \end{cases}$$

が成り立つ (なお [6, §4] の方法を用いると, 例外素数はたかだか $p = 2, 3, 5, 11$ のみであることが分かる). また同じ漸化式を満たす数列 $(a'_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ を

$$(a'_0, \ldots, a'_5) = (0, 2, -4, -3, 20, -40)$$

で定め, 数列 $(b_m)_m$ を

$$\sum_{m\geq 0} b_m q^m = q \prod_{n\geq 1} (1-q^{6n})(1-q^{18n})$$

で定めると, ほとんど全ての素数 $p$ に対して

$$a'_p \equiv b_p \pmod{p}$$

が成り立つ. 言い換えると, $\mathcal{A}$ において $(a'_p \bmod p)_p = (b_p \bmod p)_p$ が成り立つ.

後者の例は, 重さ 1 の newform $\eta(6z)\eta(18z)$ $(q = e^{2\pi i z})$ と $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_3$ の既約 2 次元表現 $\rho$ との間に $b_p = \mathrm{Tr}\,\rho(\phi_{\mathfrak{p}})$ なる関係がある事実に基づく (cf. [1, §1.1.1]). 以下に同様の現象を三例挙げる. ただしこれらは数値実験で発見されたもので, 証明は (原理的には可能なはずだが) 行っていない.

**例 3.2.** 以下のように数列 $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ および $(b_m)_m$ を定めると, $\mathcal{A}$ において $(a_p \bmod p)_p = (b_p \bmod p)_p$ が成り立つ:

$$\text{(i)}\quad \begin{cases} f(x) = x^6 + x^5 + 4x^4 + x^3 + 2x^2 - 2x + 1, \\ (a_0, \ldots, a_5) = (0, 2, 3, -4, -7, 15), \\ \sum_m b_m q^m = \eta(z)\eta(23z). \end{cases}$$

$$\text{(ii)}\quad \begin{cases} f(x) = x^6 + x^5 + 2x^4 + 3x^3 + 2x^2 + x + 1, \\ (a_0, \ldots, a_5) = (0, 2, -2, -1, 0, 4), \\ \sum_m b_m q^m = \eta(2z)\eta(22z). \end{cases}$$

$$\text{(iii)}\quad \begin{cases} f(x) = x^8 + 3x^7 + 4x^6 + 3x^5 + 3x^4 + 3x^3 + 4x^2 + 3x + 1, \\ (a_0, \ldots, a_7) = (0, 2, 0, 0, -2, 0, 2, -8), \\ \sum_m b_m q^m = \eta(3z)\eta(21z). \end{cases}$$

上の例を観察すると, いずれも初期値において $a_0 = 0$, $a_1 = 2$ が成り立っている. これは偶然ではなく, 一般的に成り立つ事実である (証明は難しくはないが, 割愛する):

**命題 3.3.** $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ が例 3.2 と同様の意味で重さ 1 の newform と対応しているとする. またモニック多項式 $f(x) \in \mathbb{Q}[x]$ は既約であり, $f(x)$ の根の和は 0 でないとする. すると $a_0 = 0$, $a_1 = 2$ が成り立つ.

重さ 2 以上のモジュラー形式に関して, その $p$ 番目の係数が満たす合同式がいろいろな例で指摘 (予想または証明) されている. 例えば

$$\sum_{m\geq 0} a_m q^m = \eta(4z)^6 \quad (\text{重さ } 3),$$
$$\sum_{m\geq 0} b_m q^m = \eta(2z)^4\eta(4z)^4 \quad (\text{重さ } 4)$$

に対して

$$a_p \equiv {}_3F_2\left(\begin{matrix}\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1\end{matrix}; 1\right)_{p-1} \pmod{p^2} \quad (p \geq 5),$$
$$b_p \equiv {}_4F_3\left(\begin{matrix}\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \\ 1, 1, 1\end{matrix}; 1\right)_{p-1} \pmod{p^3} \quad (p \geq 7)$$

が成り立つ ([3, Theorem 4 (1)], [2, Theorem 1]). ここで

$${}_rF_s\left(\begin{matrix}\alpha_1, \ldots, \alpha_r \\ \beta_1, \ldots, \beta_s\end{matrix}; x\right)_N := \sum_{n=0}^{N} \frac{(\alpha_1)_n \cdots (\alpha_r)_n}{(\beta_1)_n \cdots (\beta_s)_n} \frac{x^n}{n!}$$

は超幾何級数を有限項で打ち切った和 (truncated hypergeometric series) を表す.

我々の重さ 1 の例も, このような現象に連なるものとみなすことができると思うが, さてこれらを包括する理論があるとしたら, どのようなものだろうか.

## 謝辞

第 15 回福岡数論研究集会において講演の機会をくださった世話人の皆様に謝意を表します. また共同研究 [6] に迎えてくださった Julian Rosen 氏, 竹山美宏氏, 田坂浩二氏に感謝します. 計算機実験の結果を記載することを許可してくださった田坂氏には重ねて感謝します. 本研究は JSPS 科研費 JP18H05233, JP21K03185 の助成を受けたものです.

## 参考文献

[1] T. Hiramatsu and S. Saito, An introduction to non-abelian class field theory, Ser. Number Theory Appl., 13, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2017, xii+175 pp.

[2] L. Long, F.-T. Tu, N. Yui and W. Zudilin, Supercongruences for rigid hypergeometric Calabi-Yau threefolds, Adv. Math. **393** (2021), Paper No. 108058, 49 pp.

[3] E. Mortenson, Supercongruences for truncated ${}_{n+1}F_n$ hypergeometric series with applications to certain weight three newforms, Proc. Amer. Math. Soc. **133** (2005), no. 2, 321–330.

[4] J. Rosen, A finite analogue of the ring of algebraic numbers, J. Number Theory **208** (2020), 59–71.

[5] J. Rosen, Sequential periods of the crystalline Frobenius, preprint, arXiv:1805.01885.

[6] J. Rosen, Y. Takeyama, K. Tasaka and S. Yamamoto, The ring of finite algebraic numbers and its application to the law of decomposition of primes, preprint, arXiv:2208.11381.

[7] S. Seki, Regular primes, non-Wieferich primes, and finite multiple zeta values of level $N$, preprint, arXiv:2310.06809.