Hasse norm principle and representations over finite prime fields

北海道大学　大学院理学研究院数学部門　沖　泰裕
Yasuhiro Oki
Department of Mathematics, Faculty of Science,
Hokkaido University

概要

本稿では, 代数的整数論の古典的な問題の 1 つである Hasse ノルム原理について解説する. また, 著者が得た Hasse ノルム原理における結果について, 有限素体上の表現との関係を中心に紹介する.

1　Hasse 原理と Hasse ノルム原理 (HNP)

本稿では, k を代数体, すなわち有理数体 $\mathbb{Q}$ の有限次拡大体とする. X を k 上の代数多様体 (ここでは, 完備性は仮定しない) とする. X の k-有理点からなる集合 $X(k)$ について理解することは, 整数論において古くから考えられてきた問題の 1 つである. その中でも, 現在では Hasse 原理の成否が重要な問題の 1 つとされている.

定義 1.1. X を k 上の代数多様体とする. X に対して **Hasse 原理** (または**局所大域原理**) が成り立つとは, 任意の v に対し $X(k_v) \neq \emptyset$ ならば $X(k) \neq \emptyset$ が成り立つことである. ここで, v は k の素点であり, k_v は k の v による完備化である.

$k = \mathbb{Q}$ のとき, k_v は p 進数体 $\mathbb{Q}_p$ または実数体 $\mathbb{R}$ のいずれかである. k が一般の場合はこれらの有限次拡大となる.

Hasse 原理に関する最も古典的な結果は次の通りである. ここで, $\mathbb{P}^n$ は k 上の n 次元射影空間を表す.

定理 1.2 (Hasse–Minkowski)**.** X を滑らかな quadric とする. すなわち,

$$X = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid a_0 x_0^2 + \cdots + a_n x_0^2 = 0\} \quad (a_0, \ldots, a_n \in k)$$

で定義される非特異代数多様体とする．このとき, X に対する Hasse 原理が成り立つ.

一方で, Hasse 原理は必ずしも成り立つとは限らないことが知られている.

定理 1.3 (Selmer)**.**

$$X := \{(x : y : z) \in \mathbb{P}^3 \mid 3x^3 + 4y^3 + 5z^3 = 0\}$$

とおくと, X に対する Hasse 原理は成り立たない.

証明は [雪江 13, 定理 5.5.1] を参照せよ.

次に, Hasse ノルム原理について説明する．そのために, いくつかの対象を導入する.

- k_v が $\mathbb{Q}_p$ の有限次拡大となるような素点を k の有限素点と呼ぶ．v が有限素点のとき, k_v の整閉な局所閉部分環がただ 1 つ存在する．これを O_v で表す.
- k のイデール群とは, 以下で定義される (位相) 群のことである:

$$\mathbb{A}_k^\times := \left\{ (x_v)_v \in \prod_v k_v^\times \;\middle|\; \text{有限個の素点を除いて } x_v \in O_v^\times \right\}.$$

定義 1.4. K/k を有限次拡大とする.

$$Ш(K/k) := (k^\times \cap \mathrm{N}_{K/k}(\mathbb{A}_K^\times))/\,\mathrm{N}_{K/k}(K^\times)$$

とおく．$Ш(K/k) = \{1\}$ となるとき, K/k に対する **Hasse ノルム原理** (以下, HNP) が成り立つという.

$Ш(K/k) = \{1\}$ であるためには, 任意の $a \in k^\times$ に対し以下の同値が成り立つことが必要十分である:

$$a \in \mathrm{N}_{K/k}(K^\times) \iff \text{任意の } v \text{ に対し } a \in \mathrm{N}_{(K\otimes_k k_v)/k_v}((K \otimes_k k_v)^\times).$$

すなわち, HNP とは, 代数体の有限次拡大に付随する大域的なノルム写像と局所的なノルム写像との「ずれ」について扱う問題である.

最後に, HNP と Hasse 原理の関係について説明する．K/k を有限次拡大とする．$a \in k^\times$ に対し,

$$X_{K/k}^{(a)} := \{x \in K^\times \mid \mathrm{N}_{K/k}(x) = a\}$$

とおく．ここで, $\mathrm{N}_{K/k}$ は K/k に付随するノルム写像である．この集合は, $[K : k]$ 次元アフィン空間の部分代数多様体とみなすことができる．一方,

$$T_{K/k} := X_{K/k}^{(1)}$$

とおくと, これは k 上の代数的トーラスである. $T_{K/k}$ を K/k に付随するノルム 1 トーラスと呼ぶ. このとき, 次が成り立つ.

- 任意の $a \in k^\times$ に対し, $X^{(a)}_{K/k}$ は $T_{K/k}$-torsor である. 逆に, 任意の $T_{K/k}$-torsor は $X^{(a)}_{K/k}$ の形で表される.
- $a, a' \in k^\times$ において, $X^{(a)}_{K/k} \cong X^{(a')}_{K/k} \iff a^{-1}a' \in \mathrm{N}_{K/k}(K^\times)$ が成り立つ.
- $a \in k^\times$ に対し, $X^{(a)}_{K/k}(k) \neq \emptyset \iff a \in \mathrm{N}_{K/k}(K^\times)$ が成り立つ.

特に, 以下の同型が成り立つ:

$$k^\times / \mathrm{N}_{K/k}(K^\times) \cong H^1(k, T_{K/k}).$$

同様の主張は k を k_v に, K を $K \otimes_k k_v$ に置き換えても成り立つ. 従って, 次が得られる.

定理 1.5 ([Ono63, p. 70], [PR94, p. 307])**.** K/k を有限次拡大とする. このとき, 同型

$$Ш(K/k) \cong Ш^1(k, T_{K/k})$$

が存在する. ここで, $Ш^1(k, T_{K/k})$ は $T_{K/k}$ の Tate–Shafarevich 群であり, 次で定義される 1 次 Galois コホモロジー群 $H^1(k, T_{K/k})$ の部分群である:

$$Ш^1(k, T_{K/k}) := \mathrm{Ker}\left(H^1(k, T_{K/k}) \xrightarrow{(\mathrm{Res}_{k_v/k})_v} \prod_v H^1(k_v, T_{K/k}) \right).$$

特に, 以下は同値である.

(i) K/k に対する HNP が成り立つ.
(ii) 任意の $a \in k^\times$ に対し, $X^{(a)}_{K/k}$ に対する Hasse 原理が成り立つ.

2 HNP に関する先行研究と主定理

まず, HNP に関する先行研究について紹介する. HNP の最も古典的な結果は, Hasse による以下の結果である.

定理 2.1 ([Has31])**.** (i) K/k が巡回拡大のとき, $Ш(K/k) = \{1\}$ が成り立つ.
(ii) $Ш(\mathbb{Q}(\sqrt{-39}, \sqrt{-3})) \cong \mathbb{Z}/2$ が成り立つ.

定理 2.1 (i) は, 代数的整数論における基本的な結果の 1 つである大域類体論の証明にも現れる. 一方, 定理 2.1 (ii) より HNP は一般には成り立たないことが分かる.

上記の結果は, 後に Tate によって Galois 拡大の場合に一般化された.

命題 2.2 ([Tat67, p. 198])**.** K/k を有限次 Galois 拡大とする. G の分解群からなる集合を $\mathcal{D}$ とするとき, 同型

$$Ш(K/k) \cong \mathrm{Coker}\left(\widehat{H}^{-3}(G,\mathbb{Z}) \to \bigoplus_{D\in\mathcal{D}} \widehat{H}^{-3}(D,\mathbb{Z})\right)$$

が存在する. ここで, $\widehat{H}^i$ は i 次 Tate コホモロジー群である.

考える有限次拡大が Galois でない場合にも, いくつかの結果が存在する. ここでは, 拡大次数を指定したときの結果について言及する. その他の結果については [金井 20] などを参照せよ.

命題 2.3 (Bartels, [Bar81, Lemma 4])**.** K/k を代数体の素数次拡大とすると, $Ш(K/k) = \{1\}$ が成り立つ.

$[K:k]$ が小さい場合についても $Ш(K/k)$ の構造が完全に決定されている. 例えば, $[K:k] = 4$ のときは以下の結果が知られている.

命題 2.4 (Kunyavskii, [Kun84, Proposition 1])**.** K/k を代数体の 4 次拡大とする. $\widetilde{K}/k$ を K/k の Galois 閉包とし, $G := \mathrm{Gal}(\widetilde{K}/k)$ とおく. このとき, $Ш(K/k) = \{1\}$ ならば $G \cong (\mathbb{Z}/2)^2$ または $G \cong A_4$ (4 次交代群) が成り立つ. 逆に, $G \cong (\mathbb{Z}/2)$ または $G \cong A_4$ であるとき, 以下の同型が存在する:

$$Ш(K/k) \cong \begin{cases} \{1\} & (\text{ある } \widetilde{K}/k \text{ の分解群が } (\mathbb{Z}/2)^2 \text{ を含む}); \\ \mathbb{Z}/2 & (\text{その他}). \end{cases}$$

注意 2.5. 定理 2.1 (ii) の拡大 $\mathbb{Q}(\sqrt{-39},\sqrt{-3})/\mathbb{Q}$ は同型

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{-39},\sqrt{-3})/\mathbb{Q}) \cong (\mathbb{Z}/2)^2$$

を満たし, すべての分解群は巡回群となる. 後者は平方剰余の相互法則より従う.

命題 2.4 は, 4 次拡大 K/k に対する HNP の成否が K/k の Galois 閉包の Galois 群と分解群によって特徴づけられることを意味する. 同様の結果は, $[K:k] = 6$ のとき Drakokhrust および Platonov ([DP87]) によって, $d \leq 16$ のとき星明考氏, 金井和貴氏および山﨑愛一氏 ([HKY22], [HKY23], [HKY24]) によって与えられている.

注意 2.6. [DP87], [HKY22], [HKY23], [HKY24] では, Galois 群の分類を用いて個別に計算を行う手法をとっている. さらに, [HKY22], [HKY23], [HKY24] ではそれらの

計算の大半を計算機で行っている. したがって, 次数が大きい場合に彼らの手法を適用することは容易でない.

以下, 有限アーベル群 A および素数 p に対し,

$$A[p^\infty] := \{a \in A \mid \text{ある } n \in \mathbb{Z}_{>0} \text{ に対し } p^n a = 0\}$$

とおく. 著者は, K/k の拡大次数が square-free な素因子 p をもち, Galois 閉包の Galois 群の p-Sylow 部分群が正規であるような場合に $Ш(K/k)[p^\infty]$ の構造について群論的な記述を与えた. いま, 有限群 G およびその部分群 H に対し, 以下の記号を用いる:

- $[H, G]$: H の元と G の元の交換子で生成される部分群;
- $N_G(H)$: H の G における正規化群;
- $Z_G(H)$: H の G における中心化群.

定理 2.7 ([Oki23])**.** K/k を代数体の有限次拡大とする. $\widetilde{K}/k$ を K/k の Galois 閉包とし, $G := \mathrm{Gal}(\widetilde{K}/k)$, $H := \mathrm{Gal}(\widetilde{K}/K)$ とおく. 以下 2 つを仮定する:

- $[K : k] \in p\mathbb{Z} \setminus p^2\mathbb{Z}$;
- G の p-Sylow 部分群 S_p は G の正規部分群である.

このとき, $Ш(K/k)[p^\infty] \neq \{1\}$ ならば次が成り立つ:

(a) $S_p \cong (\mathbb{Z}/p)^2$;
(b) $[S_p, G] = S_p$;
(c) $N_G(S_p \cap H) = Z_G(S_p \cap H)$.

逆に, (a), (b), (c) がすべて成り立つとき, 以下の同型が存在する:

$$Ш(K/k)[p^\infty] \cong \begin{cases} \{1\} & (\text{ある } \widetilde{K}/k \text{ の分解群が } S_p \text{ を含む}); \\ \mathbb{Z}/p & (\text{その他}). \end{cases}$$

定理 2.7 より, HNP が成り立たないような新たな例も得られる.

系 2.8 ([Oki23])**.** p, ℓ を $2 < \ell \mid p^2 - 1$ が成り立つような素数とする. d を平方因子をもたないような $p\ell$ の倍数とする. このとき, 任意の代数体 k に対し, 次数 d の拡大 K/k で HNP が成り立たないものが存在する.

注意 2.9. 系 2.8 に現れる K/k は Galois でない. すなわち, K/k が d 次 Galois 拡大

ならば $Ш(K/k) = \{1\}$ が成り立つ. この結果は Gurak によって証明されたものである ([Gur78]).

3 Poitou–Tate 双対性

以下の記号を用いる.

- $\mathbb{G}_m := \operatorname{Spec} k[t, t^{-1}]$ を k 上の乗法群スキームとする.
- K/k を有限次拡大, T を K 上のトーラスとするとき, $\operatorname{Res}_{K/k} T$ を T の k 上への Weil 制限とする. すなわち, k-代数 R に対し

$$(\operatorname{Res}_{K/k} T)(R) := T(R \otimes_k K)$$

で定義される k 上のトーラスである.

例 3.1. K/k を有限次拡大とするとき,

$$T_{K/k} = \operatorname{Ker}(\mathrm{N}_{K/k} \colon \operatorname{Res}_{K/k} \mathbb{G}_{m,K} \to \mathbb{G}_m)$$

である. ここで, $\operatorname{Res}_{K/k}$ は K/k に関する Weil 制限である. 特に, 以下の完全列を得る:

$$1 \to T_{K/k} \to \operatorname{Res}_{K/k} \mathbb{G}_{m,K} \xrightarrow{\mathrm{N}_{K/k}} \mathbb{G}_m \to 1. \tag{1}$$

定義 3.2. T を k 上のトーラスとするとき,

$$X^*(T) := \operatorname{Hom}_{\overline{k}\text{-group}}(T \otimes_k \overline{k}, \mathbb{G}_{m,\overline{k}})$$

とする. これは (離散位相に関して) 連続な $\operatorname{Gal}(\overline{k}/k)$-作用をもつ有限生成自由アーベル群である. $X^*(T)$ を T の**指標群**とよぶ.

K/k を有限次拡大, T を K 上のトーラスとする. K を含む k 上の Galois 拡大体 $\widetilde{K}$ をとり, $G := \operatorname{Gal}(\widetilde{K}/k)$, $H := \operatorname{Gal}(\widetilde{K}/K)$ とおく. このとき, G-加群としての同型

$$X^*(\operatorname{Res}_{K/k} T) \cong \operatorname{Ind}_H^G X^*(T) := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} X^*(T)$$

が存在する. 特に, $X^*(\operatorname{Res}_{K/k} \mathbb{G}_m) \cong \mathbb{Z}[G/H]$ が成り立つ. また, 次の補題も得られる.

補題 3.3. K/k を代数体の有限次拡大とする. $\widetilde{K}/k$ を K/k の Galois 閉包とし, $G := \operatorname{Gal}(\widetilde{K}/k)$, $H := \operatorname{Gal}(\widetilde{K}/K)$ とおく. このとき, (1) は完全列

$$0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to X^*(T_{K/k}) \to 0$$

を誘導する.

定義 3.4. A を $\mathrm{Gal}(\overline{k}/k)$-加群とするとき,

$$Ш^i(k,A) := \mathrm{Ker}\left(H^i(k,A) \to \prod_v H^i(k_v,A)\right)$$

を A の i 次 Tate–Shafarevich 群とよぶ. ここで, v は k の素点である.

定理 1.5 の同型の右辺は, より扱いやすい対象に書き換えることができる.

命題 3.5 (Poitou–Tate 双対性; [PR94, Theorem 6.10])**.** T を k 上のトーラスとするとき, 同型

$$Ш^1(k,T) \cong Ш^2(k,X^*(T))^\vee$$

が存在する. ここで, $(-)^\vee$ は Pontryagin 双対である.

定理 1.5 と命題 3.5 をまとめると, 以下の主張が従う.

系 3.6. K/k を有限次拡大とするとき, 同型

$$Ш(K/k) \cong Ш^2(k,X^*(T_{K/k}))^\vee$$

が存在する.

さらに, 系 3.6 内の同型の右辺は, 有限群のコホモロジーによって記述することができる.

命題 3.7. K/k を代数体の有限次拡大とし, $\widetilde{K}/k$ を K/k の Galois 閉包とする. $G := \mathrm{Gal}(\widetilde{K}/k)$ とおくと, $\mathrm{Gal}(\overline{k}/k)$ の $X^*(T_{K/k})$ への作用は G を経由する. さらに, G に対応する有限次 Galois 拡大の分解群からなる集合を $\mathcal{D}$ とおくと, 自然な同型

$$Ш^2(k,X^*(T_{K/k})) \cong Ш^2_{\mathcal{D}}(G,X^*(T_{K/k}))$$

が存在する. ただし, 右辺は準同型

$$(\mathrm{Res}_{G/D})_{D\in\mathcal{D}} \colon H^2(G,X^*(T_{K/k})) \to \bigoplus_{D\in\mathcal{D}} H^2(D,X^*(T_{K/k}))$$

の核で定義される.

4　定理 2.7 の証明の概略

補題 4.1. p を素数, K/k を代数体の有限次拡大体とし, $\widetilde{K}/k$ を K/k の Galois 閉包とする. 以下を仮定する:

(1) $[K:k] \in p\mathbb{Z} \setminus p^2\mathbb{Z}$;
(2) $G := \mathrm{Gal}(\widetilde{K}/k)$ の p-Sylow 部分群 S_p は G の正規部分群である.

このとき, S_p は $\mathbb{Z}/p$ の有限個の直積と同型である. さらに, ある G の部分群 G' が存在して, 次の 2 つの条件を満たす.

(i) $G = S_p \rtimes G'$;
(ii) H を K に対応する G の部分群とするとき, G' の部分群 H' が存在して $H = (S_p \cap H) \rtimes H'$ が成り立つ.

Proof. S_p に関する主張は, 仮定 (1) より $(S_p : S_p \cap H) = p$ が成り立つことおよび $N^G(S_p \cap H) = \{1\}$ から従う. また, (i) については仮定 (2) および Schur–Zassenhaus の定理から従う.

以下, (i) の同型を取り替えて, (ii) が成り立つようにできることを示す. 自然な同型 $G' \cong G/S_p$ により HS_p/S_p に対応する G' の部分群を H' とおく. このとき, G の部分群 H の積構造は 1-コサイクル $H' \to S_p/(S_p \cap H)$ を定める. 一方, H' と $S_p/(S_p \cap H)$ は位数が互いに素であることから, $H^1(H', S_p/(S_p \cap H)) = 0$ が従う. ゆえに, ある $s \in S_p$ が存在して $sHs^{-1} = (S_p \cap H) \rtimes H'$ となる. 主張はこの事実から直ちに従う. ■

補題 4.1 により, 定理 2.7 における G から位数が p と互いに素な有限群 G' の $\mathbb{F}_p$ 上の有限次元表現が自然に定まる.

まず, 定理 2.7 のうち $\dim_{\mathbb{F}_p} S_p \neq 2$ の場合は次より従う.

定理 4.2. 有限次拡大 K/k は素数 p に関して条件 (a), (b) を満たすとする. 同型 $\mathrm{Gal}(\widetilde{K}/k) \cong S_p \rtimes G'$ を補題 4.1 の通りとする. $\dim_{\mathbb{F}_p} S_p \neq 2$ ならば, 等式

$$Ш^2(k, X^*(T_{K/k}))[p^\infty] = 0$$

が成り立つ.

Proof. $\mathrm{Gal}(\widetilde{K}/k)$ の唯一の p-Sylow 部分群 $S_p \rtimes \{1\}$ に対応する $\widetilde{K}/k$ の中間体を K_0

で表す. また, $\mathrm{Res}_{K_0/k}$ と $\mathrm{Cor}_{K_0/k}$ をそれぞれ Galois コホモロジーにおける K_0/k に付随する制限写像と corestriction 写像とする. このとき,

$$\mathrm{Cor}_{K_0/k} \circ \mathrm{Res}_{K_0/k} = [K_0 : k]$$

である ([NSW00, (1.5.7) Corollary]). K_0 の定義より $[K_0 : k]$ は p と互いに素であるから, $\mathrm{Res}_{K_0/k}$ は単射

$$Ш^2(k, X^*(T_{K/k}))[p^\infty] \hookrightarrow Ш^2(K_0, X^*(T_{K/k}))$$

を誘導する. 一方, K と K_0 の定義から, d 個の K_0 の p 次 Galois 拡大 $K_1, \ldots, K_d$ および K_0-代数としての同型 $K \otimes_k K_0 \cong \prod_{i=1}^d K_i$ が存在する. 特に,

$$T_{K/k} \otimes_k K_0 \cong \mathrm{Ker}\left((\mathrm{N}_{K_i/k})_i \colon \prod_{i=1}^d \mathrm{Res}_{K_i/K_0} \mathbb{G}_{m,K_i} \to \mathbb{G}_{m,K_0} \right)$$

が成り立つ. また, $\widetilde{K}$ の定義より $K_1, \ldots, K_d$ の合成体は $\widetilde{K}$ に一致する. いま, 仮定より

$$[K_1 \cdots K_d : K_0] = [\widetilde{K} : K_0] = p^{\dim_{\mathbb{F}_p}(S_p)} \neq p^2$$

であるから, 主張は以下の命題 4.3 より従う. ■

命題 4.3 ([BLP19, Theorem 8.5])**.** $K_1, \ldots, K_d$ を k の p 次 Galois 拡大とし,

$$T := \mathrm{Ker}\left((\mathrm{N}_{K_i/k})_i \colon \prod_{i=1}^d \mathrm{Res}_{K_i/k} \mathbb{G}_{m,K_i} \to \mathbb{G}_m \right)$$

とおく. $[K_1 \cdots K_d : k] \neq p^2$ ならば

$$Ш^2(k, X^*(T)) = 0$$

が成り立つ.

注意 4.4. 命題 4.3 で現れるトーラスは**多重ノルム 1 トーラス**と呼ばれるものである.

命題 4.3 において, 仮定 $[K_1 \cdots K_d : k] = p^2$ を外すことは不可能である. 実際, $d = 3$ のときは $Ш^2(k, X^*(T)) \cong \mathbb{Z}/p$ が成り立つ. そのため, $\dim_{\mathbb{F}_p} S_p = 2$ のときはより繊細な議論が必要である.

定理 2.7 のうち $\dim_{\mathbb{F}_p} S_p = 2$ の場合は次より従う.

定理 4.5. p を素数, K/k を代数体の有限次拡大体, $\widetilde{K}/k$ を K/k の Galois 閉包とする. $G := \mathrm{Gal}(\widetilde{K}/k)$, $H := \mathrm{Gal}(\widetilde{K}/K)$ とおく. 以下を仮定する:

(a) $[K:k] \in p\mathbb{Z} \setminus p^2\mathbb{Z}$;
(b) $G := \mathrm{Gal}(\widetilde{K}/k)$ の p-Sylow 部分群 S_p は**位数** p^2 の正規部分群である.

補題 4.1 より $S_p \cong (\mathbb{Z}/p)^2$ であり, G の部分群の列 $H' < G'$ が存在して $G = S_p \rtimes G'$ および $H = (S_p \cap H) \rtimes H'$ が成り立つ. いま, S_p を G' の 2 次元 $\mathbb{F}_p$-表現とみなし, $L := S_p \cap H$ を S_p の 1 次元部分空間とみなす. このとき, $Ш^2(k, X^*(T_{K/k}))[p^\infty] \neq 0$ ならば次が成り立つ:

(B) L の G' における固定部分群 $\mathrm{Stab}_{G'}(L)$ は L の pointwise stabilizer $\mathrm{Fix}_{G'}(L)$ に一致する (一般には $\mathrm{Fix}_{G'}(L) \subset \mathrm{Stab}_{G'}(L)$ である);
(C) $S_p^{G'} = \{0\}$ が成り立つ.

逆に, (B), (C) がともに成り立つとき, 次の同型が存在する:

$$Ш^2(k, X^*(T_{K/k}))[p^\infty] \cong \begin{cases} 0 & (\text{ある } \widetilde{K}/k \text{ の分解群が } S_p \text{ を含む}); \\ \mathbb{Z}/p & (\text{その他}). \end{cases}$$

Proof. $\mathcal{D}$ を $\widetilde{K}/k$ の分解群からなる集合とする. 命題 3.7 より, $Ш^2(k, X^*(T_{K/k}))$ を $Ш^2_{\mathcal{D}}(G, X^*(T_{K/k}))$ に置き換えた主張を示せばよい. $\mathcal{D}$ のある元が S_p を含むときは, 制限写像

$$\mathrm{Res}_{G/S_p} \colon H^2(G, X^*(T_{K/k}))[p^\infty] \to H^2(S_p, X^*(T_{K/k}))$$

が単射であることから, $Ш^2_{\mathcal{D}}(G, X^*(T_{K/k}))[p^\infty] = 0$ が従う. 以降, $\mathcal{D}$ に含まれるすべての G の部分群は S_p を含まないとする. いま, G の部分群 HS_p に対応する $\widetilde{K}/k$ の中間体を K_0 とおくと, これは K/k の中間体である. よって, K/K_0 に関するノルム写像は k 上のトーラスの完全列

$$1 \to \mathrm{Res}_{K_0/k} T_{K/K_0} \to T_{K/k} \xrightarrow{\mathrm{N}_{K/K_0}} T_{K_0/k} \to 1$$

を誘導する. この完全列の指標群の G-係数群コホモロジーを取ることで, 完全列

$$H^1(G, X^*(T_{K/k})) \to H^1(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0})) \to H^2(G, X^*(T_{K_0/k}))$$
$$\xrightarrow{\widehat{\mathrm{N}}_{K/K_0}} H^2(G, X^*(T_{K/k})) \to H^2(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0}))$$

を得る. ここで, $Ш^2_{\mathcal{D}}(G, X^*(T_{K/k}))$ の $\widehat{\mathrm{N}}_{K/K_0}$ による逆像を M とおくと, 次の完全列が従う:

$$H^1(G, X^*(T_{K/k}))[p^\infty] \to H^1(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0}))[p^\infty] \xrightarrow{\delta} M[p^\infty]$$
$$\xrightarrow{\widehat{\mathrm{N}}_{K/K_0}} Ш^2_{\mathcal{D}}(G, X^*(T_{K/k}))[p^\infty] \to Ш^2_{\mathcal{D}}(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0}))[p^\infty].$$

以降, G' の部分群 G'' および G''-安定な S_p の部分空間 S' に対し,

$$I_{G''}(S') := \{gs - s \in S' \mid g \in G'', s \in S'\}$$

とおく. 簡単な計算から,

$$H^1(G, X^*(T_{K/k}))[p^\infty] = 0,$$
$$H^1(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0}))[p^\infty] \cong (S_p/(L + I_{H'}(S_p)))^\vee$$

が分かる. よって, δ は単射である. 一方, $[K : K_0] = p$ は素数であるから, 命題 2.3 と命題 3.7 より

$$Ш^2_{\mathcal{D}_{HS_p}}(HS_p, X^*(T_{K/K_0})) = 0$$

となる. ここで, $\mathcal{D}_{HS_p} := \{D \cap HS_p \mid D \in \mathcal{D}\}$ である. 従って, Shapiro の補題より

$$Ш^2_{\mathcal{D}}(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0})) = 0$$

が成り立つ. 以上より, 完全列

$$0 \to (S_p/(L + I_{H'}(S_p)))^\vee \to M[p^\infty] \to Ш^2_{\mathcal{D}}(G, X^*(T_{K/k}))[p^\infty] \to 0$$

を得る. このとき, 次の同型を示せばよい.

$$M[p^\infty] \cong \frac{(S_p/(I_{H'}(S_p) + I_{\mathrm{Stab}_{G'}(L)}(L)))^\vee}{(S_p/I_{G'}(S_p))^\vee}. \tag{2}$$

実際, 上の同型が正しいとすると, 同型

$$Ш^2_{\mathcal{D}}(G, X^*(T_{K/k})) \cong \begin{cases} \mathbb{Z}/p & ((\mathrm{B}), (\mathrm{C}) \text{ がともに成立する}); \\ 0 & (\text{それ以外}) \end{cases}$$

が得られ, 主張の証明が完了する. ここで, $\mathrm{Stab}_{G'}(L) = \mathrm{Fix}_{G'}(L)$ かつ S_p が H'-表現として自明でない場合に, H' の $\mathbb{F}_p$-表現 S_p に対して Maschke の定理を用いる.

最後に, 同型 (2) の証明について説明する. $[K_0 : k] = \ell \notin p\mathbb{Z}$ であることから, 補題 3.3 のコホモロジーより誘導される連結準同型

$$H^2(G, X^*(T_{K/k})) \to H^3(G, \mathbb{Z})$$

の核は $H^2(G, X^*(T_{K/k}))[p^\infty]$ を含む. よって, $H'[p^\infty]$ は補題 3.3 および Shapiro の補題から得られる準同型

$$H^2(H, \mathbb{Z}) \cong H^2(G, \mathbb{Z}[G/H]) \to H^2(G, X^*(T_{K/k}))$$

の像に含まれる. この事実と $\mathrm{Ind}_{HS_p}^{G} X^*(T_{K/K_0})$ および $X^*(T_{K_0/k})$ に対する Mackey 分解を組み合わせて, すべての $D \in \mathcal{D}$ に対して可換図式

$$\begin{array}{ccc} H^1(G, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0}))[p^\infty] & \xrightarrow{\delta} & H^2(G, X^*(T_{K_0/k}))[p^\infty] \\ \downarrow{\scriptstyle \mathrm{Res}_{G/D}} & & \downarrow{\scriptstyle \mathrm{Res}_{G/D}} \\ H^1(D, X^*(\mathrm{Res}_{K_0/k} T_{K/K_0}))[p^\infty] & \xrightarrow{\delta} & H^2(D, X^*(T_{K_0/k}))[p^\infty] \end{array}$$

を詳細に調べることで (2) を証明することができる. 詳しくは [Oki23, Section 4.2] を参照せよ. ■

5 系 2.8 の証明の概略

補題 5.1. p を 3 でない素数, ℓ を奇素数かつ $p^2 - 1$ の約数とする. $G' := \mathbb{Z}/\ell$ とするとき, 以下を満たす G' の 2 次元 $\mathbb{F}_p$-表現 S_p が存在する:

(i) $S_p^{G'} = \{0\}$;
(ii) G' の作用で安定でない S_p の 1 次元部分空間が存在する.

Proof. 準同型

$$G' \to \mathrm{GL}_2(\mathbb{F}_p);\ 1 \bmod \ell \mapsto \begin{cases} \mathrm{diag}(\zeta_\ell, \zeta_\ell^{-1}) & (p \equiv 1 \bmod \ell), \\ \begin{pmatrix} 0 & -1 \\ 1 & \zeta_\ell + \zeta_\ell^p \end{pmatrix} & (p \equiv -1 \bmod \ell) \end{cases}$$

に対応する 2 次元 $\mathbb{F}_p$-表現を S_p とすればよい. ■

補題 5.2. p を素数, G' を有限可解群, S_p を G' の有限次元 $\mathbb{F}_p$-表現とする. $G := S_p \rtimes G'$ とおくとき, Galois 群が G と同型であるような有限次 Galois 拡大 $\widetilde{K}/k$ であって, すべての $\widetilde{K}/k$ の分解群が巡回群であるようなものが存在する.

Proof. S_p はアーベル群であるから, 定義より G は可解群である. よって, 主張は Shafarevich による可解群に対する Galois 逆問題の証明から従う ([NSW00, Chapter IX, §6] を参照). ■

系 *2.8* の証明. $d' = d/p \in \mathbb{Z}_{>0}$ とし, $G' := \mathbb{Z}/d'$ とおく. 全射 $\pi\colon G' \twoheadrightarrow \mathbb{Z}/\ell$ を固定し, 補題 5.1 の条件 (i), (ii) を満たすような $\mathbb{Z}/\ell$ の 2 次元 $\mathbb{F}_p$-表現 S_p をとる. ここで, $\mathbb{Z}/\ell$ の作用で安定でない S_p の 1 次元部分空間 L を 1 つとる. また, S_p を π に

より G' の $\mathbb{F}_p$-表現とみなし, $G := S_p \rtimes G'$ とおく. このとき, 補題 5.2 より, Galois 群が G と同型 Galois 拡大 $\widetilde{K}/k$ で, すべての $\widetilde{K}/k$ の分解群が巡回群であるようなものが存在する. いま, $H := L \rtimes \{0\}$ とおき, K を H に対応する $\widetilde{K}/k$ の中間体とする. このとき, 定義から $[K : k] = d$ である. また, $S_p^{G'} = \{0\}$ より $[S_p, G] = S_p$ であり, K/k の Galois 閉包は $\widetilde{K}$ に一致する. さらに, $S_p \cap H = H = L \rtimes \{1\}$ より, $N_G(S_p \cap H) = Z_G(S_p \cap H)$ が成り立つ. 一方, $\widetilde{K}/k$ の分解群は巡回群であるから, 定理 2.7 より, $Ш(K/k)[p^\infty] \cong \mathbb{Z}/p$ を得る. 特に, $Ш(K/k) \neq \{1\}$ であるから, 主張が示された. ■

注意 5.3. 系 2.8 の証明で構成した拡大 K/k について, $Ш(K/k) = Ш(K/k)[p^\infty]$ となることが証明できる. 特に, $Ш(K/k) \cong \mathbb{Z}/p$ が成り立つ. また, 以下に示す通り, d が小さい数の場合は先行研究の一部を復元している.

(i) $d = 6$ のとき, $p = 2$ および $\ell = 3$ とすると, 系 2.8 の条件が成り立つ. このとき, G は 4 次交代群と同型である. この場合に $Ш(K/k) \cong \mathbb{Z}/2$ が成り立つことは [DP87, §10] で証明されている.

(ii) $d = 15$ のとき, $p = 5$ および $\ell = 3$ とすると, 系 2.8 の条件が成り立つ. このとき, G は transitive group と呼ばれる対象のうち $15T9$ と同型である. この場合に $Ш(K/k) \cong \mathbb{Z}/5$ が成り立つことは [HKY22, Theorem 1.18] で証明されている.

謝辞. 2024 年度 RIMS 共同研究 (公開型)「表現論と調和解析のひろがり」にて講演の機会を与えてくださった, プログラム委員の田中 雄一郎先生に感謝申し上げます. また, 本研究は JSPS 科研費 (22KJ0041) の助成を受けて実施されました.

参考文献

[Bar81] H. J. Bartels, *Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen*, J. Alg. **70** (1981), 179–199.

[BLP19] E. Bayer-Fluckiger, T.-Y. Lee, R. Parimala, *Hasse principle for multi-norm equations*, Adv. Math. **356** (2019), 106818.

[Bro82] K. Brown, *Cohomology of groups*, Grad. Texts in Math., 87, Springer-Verlag, New York-Berlin, 1982.

[DP87] Y. A. Drakokhrust, V. P. Platonov, *The Hasse norm principle for algebraic*

number fields (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), 946–968; translation in Math. USSR-Izv. **29** (1987), 299–322.

[EM75] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975), 85–104.

[Gur78] S. Gurak, *On the Hasse norm principle*, J. Angew. Math. **299**/**300** (1978), 16–27.

[Has31] H. Hasse, *Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol*, Nschrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1931), 64–69.

[HKY22] A. Hoshi, K. Kanai, A. Yamasaki, *Norm one tori and Hasse norm principle*, Math. Comput. **91** (2022), 2431–2458.

[HKY23] A. Hoshi, K. Kanai, A. Yamasaki, *Norm one tori and Hasse norm principle, II: Degree* 12 *case*, J. Number Theory **244** (2023), 84–110.

[HKY24] A. Hoshi, K. Kanai, A. Yamasaki, *Norm one tori and Hasse norm principle III: Degree* 16 *case*, preprint, arXiv:2404.01362, 2024.

[NSW00] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Springer Verlag, 2000.

[Kun84] B. E. Kunyavskii, *Arithmetic properties of three-dimensional algebraic tori*, in: Integral Lattices and Finite Linear Groups, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **116** (1982), 102–107, 163 (Russian); translation in J. Sov. Math. **26** (1984), 1898–1901.

[Oki23] Y. Oki, *The Hasse norm principle for some non-Galois extensions of square-free degree*, preprint, arXiv:2307.12550, 2023.

[Ono63] T. Ono, *On Tamagawa numbers of algebraic tori*, Ann. Math. (2) **78** (1963), 47–73.

[PR94] V. P. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, Pure and applied mathematics, 139, Academic Press, 1994.

[Tat67] J. Tate, *Global class field theory*, Algebraic Number Theory, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union, Edited by J. W. S. Cassels and F. Flölich, 162–203,

Academic Press, London; Thompson Book Co., Inc., Washington, D.C. 1967.
[金井 20] 金井 和貴, Norm one tori and Hasse norm principle, 第 27 回整数論サマースクール報告集「構成的ガロア逆問題と不変体の有理性問題」(2020), 239–254.
[雪江 13] 雪江 明彦, 整数論 2 代数的整数論の基礎, 日本評論社, 2013.