# 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」

2019年9月6日 ～ 9月10日

於 山形県酒田市

# まえがき

2019 年度第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」は 2019 年 9 月 6 日 (金) から 9 月 10 日 (火) まで山形県酒田市にて行われました．講演を東北公益文科大学公益ホール (酒田市公益研修センター)，宵の時間 (若手中心の発表の時間) および宿泊をかんぽの宿酒田にて行い，昼も夜も参加者の熱気に満ちたサマースクールとなりました．この報告集は，講演および当日 Web (https://sites.google.com/view/ntss2019/home) 上で配布したレジメをもとに，講演者の方々にご執筆いただいた原稿を収録しています．Web にある講演全体の参考文献も本報告集とともにご活用下さい．また，１日目と２日目の夕食後に行われた宵の時間の講演スライドも講演者全８名分収録しました．

今回のテーマである構成的ガロア逆問題と不変体の有理性問題は整数論および代数幾何学における重要な主題の１つとして研究されてきました．当該分野の第一人者である J-P. Serre 氏の研究をふまえながら，数論的，代数幾何的，数論幾何的視点が交錯する研究の展開・躍動の様子を皆さんに体感いただけたことは，大きな意義があったと感じています．

講義は前半 (１，２，３日目) の基本と後半 (４，５日目) の発展からなります．基本では，ガロア理論続論としてガロアコホモロジーやガロア群の計算，不変体の有理性問題における種々の定義とその具体例，ガロア逆問題に関する解説が行われました．サマースクールらしく，各講演者からは証明のアイデアや要点の解説がありました．有限単純群の分類問題の歴史的な経緯を含んだ解説もお願いすることができました．発展では，解析数論と体の同型問題，ガロア拡大の具体的構成と何が出来るのか，有限単純群に対するガロア逆問題，代数的トーラスの有理性問題，ノルム１トーラスとハッセノルム原理，不分岐ブラウアー群，3 次不分岐コホモロジー群と GAP による計算，野性 McKay 対応など，より発展的な内容，研究のさらなる展開についての解説がありました．内容の詰まり過ぎた時間設定と世話人の無茶振りの要求に丁寧かつ完璧にご対応下さった講演者の皆様に感謝申し上げます．

サマースクールの企画・運営にあたって多くの方々から助言・協力を頂きました．伊吹山知義先生，青木宏樹先生には運営に関して大変有益な助言をいただきました．角皆宏先生，木村巌先生，田坂浩二先生には過去のサマースクールを踏まえた情報をご教示いただきました．当日会場でホワイトボード (実際は銀板でした) やお茶の係りとして手伝ってくれた東京理科大学の関川隆太郎さん，皆川祐太朗さん，吉崎彪雅さん，新潟大学の池田愛輝さん，大泉佑太さん，半内広貴さん，本田涼真さんにも感謝を述べたいと思います．

本サマースクールは以下の科学研究費から援助を受けています．
基盤研究 (S) 16H06336 (研究代表者：金子昌信)
基盤研究 (B) 18H01112 (研究代表者：安田健彦)
基盤研究 (C) 15K04798 (研究代表者：木田雅成)　18K03253 (研究代表者：角皆宏)
18K03259 (研究代表者：藤井俊)　19K03418 (研究代表者：星明考)
19K03429 (研究代表者：青木宏樹)　19K03447 (研究代表者：北山秀隆)
若手研究 19K14512 (研究代表者：谷本祥)
特別研究員奨励費 17J01827 (研究代表者：佐久川憲児)
また，これらの一部によって本報告集も印刷されていることを付け加えます．

伝統ある整数論サマースクールを継承し，日本の整数論のこれからの発展に少しでも寄与できたのでしたら大変嬉しく思います．参加者の皆様，本当にありがとうございました．

世話人：小松亨 (東京理科大学)，星明考 (新潟大学)，北山秀隆 (和歌山大学)

# 第27回整数論サマースクール
# 「構成的ガロア逆問題と不変体の有理性問題」

日時　2019年9月6日（金）～10日（火）
場所　山形県酒田市　東北公益文科大学公益ホール・かんぽの宿酒田
世話人　小松亨（東京理科大学），星明考（新潟大学），北山秀隆（和歌山大学）

プログラム

9月6日（金）
14:30 – 16:30　藤井俊（島根大学）
ガロア理論続論
17:30 – 18:45　深作亮也（九州大学）
ガロア群の計算
20:00 – 21:30　宵の時間

9月7日（土）
09:00 – 10:30　金井和貴（新潟大学）
不変体の有理性問題 (1)
10:45 – 12:15　長谷川寿人（新潟大学）
不変体の有理性問題 (2)
13:30 – 14:00　山崎愛一（京都大学）
Flabby resolution の GAP による計算
14:15 – 15:30　星明考（新潟大学）
半単項式作用と有理性問題
15:45 – 17:15　木田雅成（東京理科大学）
冪根を含まない体のクンマー理論について
17:30 – 18:45　角皆宏（上智大学）
複比の体での有理性問題
20:00 – 21:30　宵の時間

9月8日（日）
09:00 – 10:30　田中康彦（大分大学）
有限単純群の分類問題について
10:45 – 12:15　佐久川憲児（京都大学）
ガロワの逆問題と剛性の方法について
13:30 – 19:00　自由討論

9 月 9 日（月）

09:00 – 10:30　岡崎龍太郎
The simplest cubic fields are non-isomorphic to each other
— exposition of ideas

10:45 – 12:15　角皆宏（上智大学）
ガロア群の構成問題の明示解の活用
～ 明示的な多項式があると出来ること ～

13:30 – 14:15　佐久川憲児（京都大学）
$\mathrm{PSL}_2(\mathbf{F}_l)$ に対するガロワの逆問題について

15:00 – 16:00　長谷川寿人（新潟大学）
Rationality problem for algebraic tori

16:15 – 17:15　金井和貴（新潟大学）
Norm one tori and Hasse norm principle

17:30 – 18:45　谷本祥（熊本大学）
不分岐 Brauer 群と不変体の有理性問題

20:00 – 21:00　今後の SS

9 月 10 日（火）

09:00 – 10:30　星明考（新潟大学）
3 次不分岐コホモロジー群とネーター問題

10:30 – 10:45　山崎愛一（京都大学）
3 次不分岐コホモロジー群の GAP による計算

11:00 – 12:30　安田健彦（東北大学）
野生 McKay 対応概説 –数論的視点と最新成果–

参加者リスト（75 名，敬称略，所属は参加申請時のもの）

| | | | |
|---|---|---|---|
| 東北大学 | 安田健彦 | 新潟大学 | 星明考 |
| | 丹野真人 | | 金井和貴 |
| | 石澤夏希 | | 長谷川寿人 |
| | 常盤裕太 | | 池田愛輝 |
| | 尾上耕佑 | | 半内広貴 |
| 東北学院大学 | 佐藤篤 | | 大泉佑太 |
| 一関高専 | 佐藤一樹 | | 本田涼真 |
| 東京大学 | 岡崎龍太郎 | 富山大学 | 木村巌 |
| | 小田部秀介 | 名古屋大学 | 舘野荘平 |
| | 沖泰裕 | | 武田渉 |
| 東京工業大学 | 色川怜未 | | 藤井大輔 |
| | 湯山孝雄 | | 中森幸佑 |
| | 成田承基 | | 寺島拓人 |
| | 畑佐悠太 | 名古屋文理大学 | 齋藤正顕 |
| 東京理科大学 | 木田雅成 | 名古屋工業大学 | 水澤靖 |
| | 小松亨 | | 山本康太 |
| | 青木宏樹 | 名城大学 | 植松哲也 |
| | 加塩朋和 | 愛知県立大学 | 田坂浩二 |
| | 野村次郎 | 豊田高専 | 筒石奈央 |
| | 國府田玄基 | 京都大学 | 山崎愛一 |
| | 岡野凌大 | | 佐久川憲児 |
| | 関川隆太郎 | | 石塚裕大 |
| | 吉崎彪雅 | | 伊藤和広 |
| | 皆川祐太朗 | 大阪大学 | 伊吹山知義 |
| | 田中雄大 | | 厳冬 |
| 東京電機大学 | 植木潤 | | 山本貴大 |
| 慶應義塾大学 | 片岡武典 | | 片岡周太 |
| | 松村英樹 | | 後藤倫 |
| | 臺信直人 | | 藤盛公太 |
| | 後藤有輝 | 和歌山大学 | 北山秀隆 |
| 早稲田大学 | 青木琢哉 | 広島大学 | 上野卓 |
| | 隈川直貴 | 島根大学 | 藤井俊 |
| | 木村昭太郎 | 九州大学 | 深作亮也 |
| 日本大学 | 下元数馬 | 九州産業大学 | 高田芽味 |
| 上智大学 | 角皆宏 | 大分大学 | 田中康彦 |
| 千葉大学 | 小林俊幸 | 熊本大学 | 谷本祥 |
| 川崎医療福祉大学 | 兵藤史武 | IIC パートナーズ | 小川紘平 |
| 津田塾大学 | 原隆 | | |

# 目次

# ガロア理論続論

藤井 俊 (島根大学)

## 1 序

本稿は, 2019 年度整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」における筆者の講演レジュメに加筆・修正したものである. ここでは, ガロア理論および体の加法群, 乗法群へのガロア群の作用, コホモロジー群の導入および基礎となる性質の解説, Hilbert の定理 90 および Kummer 理論について述べる. ガロア理論の続きという立場であるため, 代数と名のつく入門書の内容は仮定する. 想定しているのは永尾 [2] 程度の内容である.

体論については, 桂 [1] の第 3 章を参考にした. 群のコホモロジーについては, Neukirch–Schmidt–Wingberg [4] の Chapter I を参考にした. Cassels–Frölich [3] の Chapter IV も, 要領よくまとまっており, 最初に学ぶにはおすすめである. [4] の Chapter I は, [3] の Chapter IV, V をより詳しくしたものといえるだろう.

有限群のコホモロジーの基本的な命題については, なるべく証明をつけることにして, 初めて学ぶ際の参考になることを目標とした. また, 筆者は特段コホモロジーに詳しいわけではない. 一人の group cohomology user による解説であることを, ご承知いただきたい. コホモロジーの勉強では, まずコホモロジーを使ってみる, ということが大事であるように筆者には考えられる.

レジュメにはなかったものであるが, 離散加群係数の副有限群のコホモロジー, ガロア・コホモロジーの性質を証明抜きで入れた.

## 2 ガロア群の体の加法群への作用

### 2.1 ガロア理論

本稿では体は可換体を意味するものとする.

**定理 1** (ガロア理論の基本定理)**.** $F$ を体とし, $K/F$ を有限次ガロア拡大, すなわち分離かつ正規拡大とする. $G = \mathrm{Gal}(K/F)$ を $K/F$ のガロア群とする. $K/F$ の中間体 $M$ に対して $G$ の部分群

$$H_M = \{g \in G \mid g(x) = x,\ \forall x \in M\}$$

を対応させ, $G$ の部分群 $H$ に対して中間体

$$K^H = \{x \in K \mid h(x) = x,\ \forall h \in H\}$$

を対応させることは, $K/F$ の中間体と $G$ の部分群の間の互いに逆写像となる一対一対応を与える.

## 2.2 指標の独立性

以下, 体 $K$ の乗法群を $K^\times$ で表す. また, わかりづらく感じる人もいるかもしれないが, ガロア群の元 $g$ の体の元 $x$ への作用は, 写像のように $g(x)$ と表すこととする.

**命題 1** (指標の独立性)**.** $S$ を半群, $K$ を体とする. $\chi_1, \cdots, \chi_m$ を $S$ から $K^\times$ への全て異なる準同型とする. $a_1, \cdots, a_m \in K$ とする. もし, 任意の $s \in S$ に対して $a_1\chi_1(s) + \cdots + a_m\chi_m(s) = 0$ ならば, $a_1 = \cdots = a_m = 0$ である.

Proof. 主張が成り立たないとし, 矛盾を導く. すなわち, 任意の $s \in S$ に対して $a_1\chi_1(s) + \cdots + a_m\chi_m(s) = 0$ であるような $(0, \cdots, 0) \neq (a_1, \cdots, a_m) \in K^m$ が存在するとする. $a_i = 0$ となるものは省いても良いので, $a_i \neq 0$ $(1 \leq i \leq m)$ とする. さらに, $m$ をこのような $(a_1, \cdots, a_m)$ が存在するような最小のものとする.

$m = 1$ とせよ. $a_1 \neq 0$, $\chi_1(s) \neq 0$ より $a_1\chi_1(s) \neq 0$ なので, これは矛盾である. よって $m \geq 2$ である. 任意の $s \in S$ に対して, $a_1\chi_1(s) + \cdots + a_m\chi_m(s) = 0$ とせよ. $t \in S$ をとり, $s$ の代わりに $st$ を代入すると

$$a_1\chi_1(ts) + \cdots + a_m\chi_m(ts) = a_1\chi_1(t)\chi_1(s) + \cdots + a_m\chi_m(t)\chi_m(s) = 0$$

となる. ここで, $\chi_1 \neq \chi_m$ なので, $\chi_1(t) \neq \chi_m(t)$ となる $t \in S$ が存在する. そこで, 最初の式を $\chi_m(t)$ 倍して二つ目の式から引くと,

$$0 = a_i(\chi_1(t) - \chi_m(t))\chi_1(s) + \cdots + a_{m-1}(\chi_{m-1}(t) - \chi_m(t))\chi_{m-1}(s)$$

となるが, $t$ の取り方から $a_1(\chi_1(t) - \chi_m(t)) \neq 0$ であるため, $m$ の最小性に反する. よって矛盾である. □

**命題 2** (デデキントの補題)**.** $K, L$ を体とし, $\sigma_1, \cdots, \sigma_m : K \to L$ をすべて異なる環準同型とする. $b_1, \cdots, b_m \in L$ とする. もし, 任意の $a \in K$ に対して $\sigma_1(a)b_1 + \cdots + \sigma_m(a)b_m = 0$ ならば, $b_1 = \cdots = b_m = 0$ である.

Proof. $1 \leq i \leq m$ に対して, $\chi_i(a) = \sigma_i(a)$ とおけば, 指標の独立性より従う. □

**命題 3** (トレースの非退化性)**.** $K/F$ を $n$ 次分離拡大とし, $\mathrm{Tr}_{K/F} : K \to F$ をトレースとする. このとき,

$$K \times K \to F,\ (a, b) \mapsto \mathrm{Tr}_{K/F}(ab)$$

は $F$ 上の非退化な双線型形式である.

PROOF. $F$ 上の双線型形式であることはトレースの定義から従う. $\overline{F}$ を $F$ の代数閉包とし, $\sigma_1, \cdots, \sigma_n : K \hookrightarrow \overline{F}$ を $K$ の $F$ 同型全体とする. $b \in K$, $b \neq 0$ とすると,

$$\mathrm{Tr}_{K/F}(ab) = \sigma_1(a)\sigma_1(b) + \cdots + \sigma_n(a)\sigma_n(b)$$

なので, デデキントの補題より $\mathrm{Tr}_{K/F}(ab) \neq 0$ となる $a \in K$ が存在する. よって非退化性が従う. □

## 2.3 体の加法群へのガロア作用, 正規底定理

$K/F$ を有限次ガロア拡大とし, $G = \mathrm{Gal}(K/F)$ とする. ガロア理論の基本定理より, ガロア群 $G$ を知ること, および $G$ の体 $K$ への作用を知ることは, 重要な研究の一つである. まずは $G$ の $K$ への作用について調べる. $K$ は $G$ が作用する $F$ 線型空間なので, $F$ 上 $G$ の群環

$$F[G] = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \;\middle|\; a_\sigma \in F \right\}$$

上の加群である.

**定理 2** (正規底定理)**.** $F[G]$ 加群として $K \simeq F[G]$ である. すなわち, $\{\sigma(\theta) \mid \sigma \in G\}$ が $K$ の $F$ 上の基底となる $\theta \in K$ が存在する.

PROOF. $F$ が有限体の場合と無限体の場合に分けて証明する. まずは $F$ が有限体の場合に示す. このとき, ある素数 $p$ があり, $F$ は $q = p^r$ $(r \geq 1)$ 元体 $\mathbb{F}_q$ とみなせる. また, $[K : F] = n$ とすれば, $K = \mathbb{F}_{q^n}$ であり, $\varphi(a) = a^q$ $(a \in K)$ を $q$ 乗フロベニウスとすると, $G = \langle \varphi \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ である. ここで, $K$ を $Xa = \varphi(a)$ によって多項式環 $F[X]$ 上の加群と見る. $K$ は有限であることから, $K$ は有限生成捻れ $F[X]$ 加群である. このとき, $F[X]$ 加群の構造定理より, 非負整数 $r$ とモニック多項式 $f_1(X), \cdots, f_r(X) \in F[X]$ が存在し, $f_i(X) \mid f_{i+1}(X)$ $(1 \leq i \leq r-1)$,

$$n = \sum_{i=1}^{r} \deg f_i$$

かつ

$$K \simeq \bigoplus_{i=1}^{r} F[X]/(f_i(X))$$

が成り立つ. $f_r(X)$ はフロベニウス $\varphi$ の最小多項式であることに注意する. $1, \varphi, \cdots, \varphi^{n-1}$ はすべて異なり, $\varphi^n = 1$ なので, デデキントの補題より $\varphi$ の最小多項式は $X^n - 1$ である. したがって, $r = 1$, $f_r(X) = f_1(X) = X^n - 1$ となり,

$$K \simeq F[X]/(X^n - 1) \simeq F[G]$$

である.

次に $F$ が無限体である場合に示す. $[K : F] = n$ とする.

**命題 4.** $G = \{\sigma_1 = 1, \sigma_2, \cdots, \sigma_n\}$, $u_1, \cdots, u_n \in K$ とする. このとき, $u_1, \cdots, u_n$ が $K$ の $F$ 上の基底であるための必要十分条件は, $\Delta(u_1, \cdots, u_n) = \det(\sigma_j(u_i)) \neq 0$ となることである[1].

PROOF. まずは $\Delta(u_1, \cdots, u_n) \neq 0$ ならば, $u_1, \cdots, v_n$ が基底であることを示す. $a_1, \cdots, a_n \in F$ に対して, $a_1 v_1 + \cdots + a_n v_n = 0$ とせよ. このとき, 任意の $1 \leq j \leq n$ に対して

$$a_1 \sigma_j(v_1) + \cdots + a_n \sigma_j(v_n) = 0$$

である. よって, $j$ を動かして連立一次方程式と見れば, 係数行列の行列式は $\Delta(v_1, \cdots, v_n) \neq 0$ なので, $a_1 = \cdots = a_n = 0$ でなくてはならない. よって, $v_1, \cdots, v_n$ は基底である.

次に, $u_1, \cdots, u_n$ が $K$ の基底ならば, $\Delta(u_1, \cdots, u_n) \neq 0$ を示す. $T = (\mathrm{Tr}_{K/F}(u_i u_j))$ とする. トレースが定める双線型形式は非退化であるため, $u_1, \cdots, u_n$ が基底であることから $T$ は正則行列である. このとき,

$$\begin{aligned} \det T &= \det(\sum_{k=1}^{n} \sigma_k(u_i u_j)) \\ &= \det(\sigma_j(u_i))^2 = \Delta(\sigma_j(u_i))^2 \end{aligned}$$

であることと, $\det T \neq 0$ より $\Delta(u_1, \cdots, u_n) \neq 0$ である. □

$G$ の各元 $\sigma_1 = 1, \sigma_2, \cdots, \sigma_n$ に対して不定元 $X_{\sigma_1}, X_{\sigma_2}, \cdots, X_{\sigma_n}$ をとり, 行列式

$$f(X_{\sigma_1}, \cdots, X_{\sigma_n}) = \det(X_{\sigma_i^{-1}\sigma_j})$$

を考える. $f(0, \cdots, 0) = 0$, $f(1, 0, \cdots, 0) = 1$ より, $f(X_{\sigma_1}, \cdots, X_{\sigma_n})$ は定数ではない. $u_1, \cdots, u_n$ を $K$ の一つの基底とすると, $\det(\sigma_j(u_i)) \neq 0$ より変数変換

$$X_{\sigma_i} = \sigma_i(u_1)x_1 + \cdots + \sigma_i(u_n)x_n, \ 1 \leq i \leq n$$

が定義され,

$$F(X_{\sigma_1} \cdots, X_{\sigma_n}) = g(x_1, \cdots, g_n)$$

とすれば, $g(x_1, \cdots, x_n)$ も定数ではない. 定数でない 1 変数方程式は解を有限個しか持たないことから, $F$ が無限体であることより,

$$g(a_1, \cdots, a_n) \neq 0$$

となる $a_1, \cdots, a_n \in F$ が存在する. ここで,

$$\theta = a_1 u_1 + \cdots + a_n u_n$$

[1] ガロア拡大でなくても, 有限次分離拡大で成立する.

とおけば, $\{\sigma_1(\theta), \cdots, \sigma_n(\theta)\}$ は $K$ の基底となる. $c_1, \cdots, c_n \in F$ に対して,

$$c_1\sigma_1(\theta) + \cdots + c_n\sigma_n(\theta) = 0$$

とせよ. このとき, 任意の $1 \leq i \leq n$ に対して

$$c_1\sigma_i^{-1}\sigma_1(\theta) + \cdots + c_n\sigma_i^{-1}\sigma_n(\theta) = 0$$

であるため, $c_1, \cdots, c_n$ は斉次形連立一次方程式の解である. 係数行列の行列式を計算すると

$$\begin{aligned}\det(\sigma_i^{-1}\sigma_j(\theta)) &= \det(\sum_{t=1}^{n} a_t\sigma_i^{-1}\sigma_j(u_t)) \\ &= \det(X_{\sigma_i^{-1}\sigma_j})|_{X_{\sigma_k}=a_1\sigma_k(u_1)+\cdots+a_n\sigma_k(u_n) \text{ for } 1\leq k\leq n} \\ &= g(a_1, \cdots, a_n) \neq 0\end{aligned}$$

となり, $c_1 = \cdots = c_n = 0$ がしたがう. よって, $\sigma_1(\theta), \cdots, \sigma_n(\theta)$ は一次独立であり, したがって $K$ の $F$ 上の基底である. 以上より,

$$F[G] \to K,\ \sum_{\sigma} a_\sigma\sigma \mapsto \sum_{\sigma} a_\sigma\sigma(\theta)$$

は $F[G]$ 加群の同型写像である. □

ガロア理論と正規底定理により,

- 体として $K^G = \{a \in K \mid \sigma(a) = a,\ \forall\sigma \in G\} = F$.
- $F[G]$ 加群として $K \simeq F[G]$.

であることが分かった. 特に, $F[G]$ 加群としての構造は, この上なく理解できていることになる. ガロア群は体 $K$ に付随する様々な対象に作用する. 例えば, $K$ の乗法群 $K^\times$ へガロア群 $G$ は作用する. ガロア理論より $(K^\times)^G = \{a \in K^\times \mid \sigma(a) = a,\ \forall\sigma \in G\} = F^\times$ であるが, $K^\times$ の $G$ 加群としての構造は, 簡単に理解できるものではない. では, $G$ 加群 $K^\times$ の理解を進めるためには, 何を研究すればよいのだろうか? その一つの答えが, コホモロジーである.

# 3 群のコホモロジー

## 3.1 加群の一般論を少々

$G$ を有限群とする. 本稿では, $G$ の作用は左作用を表すこととする. また, ガロア群の体の元への作用と異なる表記となるが, $\sigma \in G$ の元 $a$ への作用は, $\sigma a$ と表すことにする. まずは, 加群の一般論について, 記号の確認, 同意を行う.

**定義 1** ($G$ 加群について)**.** $G$ を有限群とする.

(1) $G$ 加群 $A$ と $G$ の部分群 $H$ に対して,

$$A^H = \{a \in A \mid ha = a,\ \forall h \in H\}$$

を $A$ の $H$ 不変部分加群という.

(2) $G$ 集合 $X$ と $G$ 加群 $A$ に対して, $X$ から $A$ への写像のなす加群

$$\mathrm{Map}(X, A) = \{f \mid f : X \to A :\ \text{map}\}$$

への $G$ の作用を,

$$(\sigma f)(x) = \sigma f(\sigma^{-1}x),\ (f \in \mathrm{Map}(X, A),\ x \in X,\ \sigma \in G)$$

で定義[2] すれば, $\mathrm{Map}(X, A)$ は $G$ 加群である. また, $A, B$ を $G$ 加群とするとき, $A$ から $B$ への準同型加群

$$\mathrm{Hom}(A, B) = \{f \mid f : A \to B :\ \text{group hom.}\}$$

は, $\mathrm{Map}(A, B)$ の $G$ 部分加群をなす.

**定義 2** (完全系列と複体)**.** $n \in \mathbb{Z}$ に対して, 加群 $A_n$ および射 $f_n : A_{n-1} \to A_n$ $(n \in \mathbb{Z})$ があるとする. このとき, 加群と射の列

$$\cdots \overset{f_{-1}}{\to} A_{-1} \overset{f_0}{\to} A_0 \overset{f_1}{\to} A_1 \overset{f_2}{\to} \cdots \overset{f_{n-1}}{\to} A_{n-1} \overset{f_n}{\to} A_n \overset{f_{n+1}}{\to} \cdots$$

が得られる.

(1) 任意の $n \in \mathbb{Z}$ に対して, $\mathrm{Im}f_{n-1} = \mathrm{Ker}f_n$ であるとき, 上の列を完全系列という. 特に, 3 つの加群 $A, B, C$ に対して,

$$0 \to A \to B \to C \to 0$$

が完全系列のとき, 短完全系列であると言ったりする.

(2) 任意の $n \in \mathbb{Z}$ に対して, $\mathrm{Im}f_{n-1} \subseteq \mathrm{Ker}f_n$ であるとき, つまり, $f_n \circ f_{n-1} = 0$ のとき, 上の列を複体という.

[2]恥ずかしながら, 筆者が初めてこの作用を見たとき, 妙なものに感じた. 後になって, 関数 $y = f(x)$ への $(a, b) \in \mathbb{R}^2$ による平行移動は $y = f(x - a) + b$ であることを思い出して, 納得することができた.

## 3.2 群のコホモロジーの定義

再び $G$ を有限群とする. $n \in \mathbb{Z}_{\geq 1}$ に対して, $G^n$ を $G$ の $n$ 個の直積とする. $G^n$ は各成分への作用によって $G$ 集合である. すなわち, $\sigma \in G$, $(\sigma_1, \cdots, \sigma_n) \in G^n$ に対して,

$$\sigma(\sigma_1, \cdots, \sigma_n) = (\sigma\sigma_1, \cdots, \sigma\sigma_n)$$

として作用する.

**定義 3.** $n \in \mathbb{Z}_{\geq 1}$ とする.

(1) $G$ 加群 $A$ に対して, $X^n = X^n(G, A) = \mathrm{Map}(G^{n+1}, A)$ とする.

(2) $\partial^n : X^{n-1} \to X^n$ を, $x \in X^{n-1}$ に対して

$$\partial^n(x)(\sigma_0, \cdots, \sigma_n) = \sum_{i=0}^{n} (-1)^i x(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_n)$$

で定める. ここで, $\hat{\sigma}$ は成分 $\sigma$ を除くことを意味する.

(3) $\partial^0 : A \to X^0$ を, $a \in A$ に対して, 定数写像 $\partial^0(a)(\sigma_0) = a$ を対応させる写像で定める.

**命題 5.** $A, X^n$ $(n \in \mathbb{Z}_{\geq 0})$ および射 $\partial^n$ からなる列

$$0 \to A \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} \cdots \xrightarrow{\partial^{n-1}} X^{n-1} \xrightarrow{\partial^n} X^n \xrightarrow{\partial^{n+1}} \cdots$$

は完全系列である.

Proof. まずは複体であることを示す.

$$\begin{aligned} \partial^1 \circ \partial^0(a)(\sigma_0, \sigma_1) &= \partial^0(a)(\sigma_0) - \partial^0(a)(\sigma_1) \\ &= a - a = 0 \end{aligned}$$

より, $\partial^1 \circ \partial^0 = 0$ である. $n \geq 1$, $x \in X^{n-1}$ とせよ. このとき,

$$\begin{aligned} \partial^{n+1} \circ \partial^n(x)(\sigma_0, \cdots, \sigma_{n+1}) &= \sum_{i=0}^{n+1} (-1)^i \partial^n(x)(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_{n+1}) \\ &= \sum_{i=0}^{n+1} \left\{ \sum_{j<i} (-1)^i (-1)^j x(\sigma_0, \cdots, \hat{\sigma_j}, \cdots, \hat{\sigma_i}, \cdots, \sigma_{n+1}) \right. \\ &\quad \left. + \sum_{j>i} (-1)^i (-1)^{j-1} x(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \hat{\sigma_j}, \cdots, \sigma_{n+1}) \right\} \\ &= \sum_{0 \leq j < i \leq n+1} (-1)^i (-1)^j x(\sigma_0, \cdots, \hat{\sigma_j}, \cdots, \hat{\sigma_i}, \cdots, \sigma_{n+1}) \\ &\quad + \sum_{0 \leq j < i \leq n+1} (-1)^j (-1)^{i-1} x(\sigma_0, \cdots, \hat{\sigma_j}, \cdots, \hat{\sigma_i}, \cdots, \sigma_{n+1}) \end{aligned}$$

であり, 同じ範囲で符号を変えて和を取っているので, $\partial^{n+1}\circ\partial^n=0$ がしたがう.

次に完全系列であることを示す. アーベル群としての射の列 $\{D^n \mid n\in\mathbb{Z}_{\geq -1}\}$ を, 次のように定める. $n=-1$ のとき,

$$D^{-1}:X^0\to A,\ D^{-1}(x)=x(1)$$

とし, $n\geq 0$ のとき,

$$D^n:X^{n+1}\to X^n,\ D^n(x)(\sigma_0,\cdots,\sigma_n)=x(1,\sigma_0,\cdots,\sigma_n)$$

とする. このとき, $n\geq 0$ に対して

$$D^n\circ\partial^{n+1}+\partial^n\circ D^{n-1}=id_{X^n}$$

が成り立つことを確かめる. $n=0$ のとき, $x\in X^0$ に対して,

$$\begin{aligned}(D^0\circ\partial^1+\partial^0\circ D^{-1})(x)(\sigma_0)&=D^0\circ\partial^1(x)(\sigma_0)+\partial^0\circ D^{-1}(x)(\sigma_0)\\&=\partial^1(x)(1,\sigma_0)+x(1)\\&=x(\sigma_0)-x(1)+x(1)\\&=x(\sigma_0)\end{aligned}$$

であり, $n\geq 1$, $x\in X^n$ のとき,

$$\begin{aligned}(D^n\circ\partial^{n+1}+\partial^n\circ D^{n-1})(x)(\sigma_0,\cdots,\sigma_n)&=D^n\circ\partial^{n+1}(x)(\sigma_0,\cdots,\sigma_n)\\&\quad+\partial^n\circ D^{n-1}(x)(\sigma_0,\cdots,\sigma_n)\\&=\partial^{n+1}(x)(1,\sigma_0,\cdots,\sigma_n)\\&\quad+\sum_{i=0}^{n}(-1)^iD^{n-1}(x)(\sigma_0,\cdots,\hat{\sigma_i},\cdots,\sigma_n)\\&=x(\sigma_0,\cdots,\sigma_n)+\sum_{i=0}^{n}(-1)^{i+1}x(1,\sigma_0,\cdots,\hat{\sigma_i},\cdots,\sigma_n)\\&\quad+\sum_{i=0}^{n}(-1)^ix(1,\sigma_0,\cdots,\hat{\sigma_i},\cdots,\sigma_n)\\&=x(\sigma_0,\cdots,\sigma_n)\end{aligned}$$

なので成り立つ. $x\in\mathrm{Ker}(\partial^{n+1})$ とすると,

$$x=(D^n\circ\partial^{n+1}+\partial^n\circ D^{n-1})(x)=\partial^n\circ D^{n-1}(x)\in\mathrm{Im}(\partial^n)$$

より

$$\mathrm{Ker}(\partial^{n+1})=\mathrm{Im}(\partial^n)$$

がしたがう. よって完全系列である. □

完全系列

$$0 \to A \overset{\partial^0}{\to} X^0 \overset{\partial^1}{\to} X^1 \overset{\partial^2}{\to} \cdots \overset{\partial^{n-1}}{\to} X^{n-1} \overset{\partial^n}{\to} X^n \overset{\partial^{n+1}}{\to} \cdots$$

の各項の $G$ 不変部分加群をとる.

$$0 \to A^G \overset{\partial^0}{\to} (X^0)^G \overset{\partial^1}{\to} (X^1)^G \overset{\partial^2}{\to} \cdots \overset{\partial^{n-1}}{\to} (X^{n-1})^G \overset{\partial^n}{\to} (X^n)^G \overset{\partial^{n+1}}{\to} \cdots,$$

ここで, $X^n = X^n(G, A)$ としていた. この列は完全であるとは限らないが, 複体にはなっている.

**定義 4** (cochain, cocycle, coboundary)**.** $n \in \mathbb{Z}_{\geq 0}$ とする.

(1) $C^n(G, A) := (X^n)^G = X^n(G, A)^G$ を $n$-cochain といい, 複体

$$C^0(G, A) \overset{\partial^1}{\to} C^1(G, A) \overset{\partial^2}{\to} \cdots \overset{\partial^{n-1}}{\to} C^{n-1}(G, A) \overset{\partial^n}{\to} C^n(G, A) \overset{\partial^{n+1}}{\to} \cdots$$

を cochain 複体という.

(2) $Z^n(G, A) := \mathrm{Ker}(C^n(G, A) \overset{\partial^{n+1}}{\to} C^{n+1}(G, A))$ を, $n$-cocycle という.

(3) $B^0(G, A) = 0$ とし, $n \geq 1$ に対して $B^n(G, A) := \mathrm{Im}(C^{n-1}(G, A) \overset{\partial^n}{\to} C^n(G, A))$ を, $n$-coboundary という.

cochain は複体をなしているため, $B^n(G, A) \subseteq Z^n(G, A)$ である. 話が抽象的なものばかりだったので, 具体的な計算もしておこう.

• $C^0(G, A)$ の計算. $f \in C^0(G, A)$ のとき,

(1) $f : G \to A$,

(2) 任意の $\sigma, \sigma_0 \in G$ に対して $f(\sigma\sigma_0) = \sigma f(\sigma_0)$,

を満たしている. (2) より, 任意の $\sigma \in G$ に対して $f(\sigma) = \sigma f(1)$ なので, $f$ は $f(1)$ で決まり, また逆に $a \in A$ から $f(1) = a$ として $f$ が決まる. よって, 同型

$$C^0(G, A) \simeq A,\ f \mapsto f(1)$$

が成り立つ.

**命題 6.** $C^0(G, A) = A$. □

**定義 5** ($G$ 加群 $A$ のコホモロジー群)**.** $G$ を有限群とし, $A$ を $G$ 加群とする. $n \in \mathbb{Z}_{\geq 0}$ に対して,

$$H^n(G, A) = Z^n(G, A)/B^n(G, A)$$

を $G$ の $A$ 係数の $n$ 次コホモロジー群という.

定義より, $H^n(G,A)$ は, cochain 複体がどの程度完全系列から離れているかを表現するものであり, $G$ 加群 $A$ の不変量でもある. コホモロジー群がどのようなものか, 具体的にいくつか計算してみよう.

• $H^0(G,A)$ の計算. $B^0(G,A)=0$ と定義していたので, $H^0(G,A)=Z^0(G,A)/B^0(G,A)=Z^0(G,A)$ である. $f\in Z^0(G,A)$ のとき,

(1) $f:G\to A$,

(2) 任意の $\sigma_0\in G$ に対して, $f(\sigma_0)=\sigma_0 f(1)$,

(3) 任意の $\sigma_0,\sigma_1\in G$ に対して, $f(\sigma_0)-f(\sigma_1)=0$,

を満たしている. (2), (3) より, 任意の $\sigma_0\in G$ に対して, $\sigma_0 f(1)=f(\sigma_0)=f(1)$ なので, $f$ は定数写像であり, かつ $f(1)\in A^G$ である. したがって, 射 $Z^0(G,A)\to A^G,\ f\mapsto f(1)$ が定義され, $A^G\to Z^0(G,A),\ a\mapsto f_a,\ f_a(\sigma_0)=a\ (\sigma_0\in G)$ は逆写像である. 以上より, $H^0(G,A)=A^G$ である.

**命題 7.** $H^0(G,A)=A^G$. □

• $H^1(G,A)$ の計算. $H^1(G,A)=Z^1(G,A)/B^1(G,A)$ であったので, $Z^1(G,A)$ と $B^1(G,A)$ を計算する. $f\in Z^1(G,A)$ のとき,

(1) $f:G^2\to A$,

(2) 任意の $\sigma,\sigma_0,\sigma_1\in G$ に対して, $f(\sigma\sigma_0,\sigma\sigma_1)=\sigma f(\sigma_0,\sigma_1)$,

(3) 任意の $\sigma_0,\sigma_1,\sigma_2\in G$ に対して, $f(\sigma_1,\sigma_2)-f(\sigma_0,\sigma_2)+f(\sigma_0,\sigma_1)=0$,

を満たす. (3) の式を少し変形すると, $\sigma_0 f(1,\sigma_0^{-1}\sigma_2)=\sigma_0 f(1,\sigma_0^{-1}\sigma_1)+\sigma_1 f(1,\sigma_1^{-1}\sigma_2)$ となり, 両辺に $\sigma_0^{-1}$ を作用し, 改めて $\sigma=\sigma_0^{-1}\sigma_1$, $\tau=\sigma_1^{-1}\sigma_2$ とすれば,

$$f(1,\sigma\tau)=f(1,\sigma)+\sigma f(1,\tau)$$

を得る. $Z^1(G,A)$ の元はこの方程式で特徴付けられる, すなわち,

$$Z^1(G,A)=\{f\in C^1(G,A)\mid f(1,\sigma\tau)=f(1,\sigma)+\sigma f(1,\tau),\ \sigma,\tau\in G\}$$

である.

次に, $B^1(G,A)$ を計算する. $g\in B^1(G,A)$ のとき,

(1) $g:G^2\to A$,

(2) ある $h\in C^0(G,A)$ があって, 任意の $\sigma_0,\sigma_1\in G$ に対して $g(\sigma_0,\sigma_1)=h(\sigma_0)-h(\sigma_1)$,

(3) 任意の $\sigma_0 \in G$ に対して, $h(\sigma_0) = \sigma_0 h(1)$.

を満たす. (2), (3) より,

$$g(\sigma_0, \sigma_1) = h(\sigma_0) - h(\sigma_1) = \sigma_0 h(1) - \sigma_0 h(\sigma_0^{-1}\sigma_1) = \sigma_0 g(1, \sigma_0^{-1}\sigma_1)$$

がしたがう. よって, $\sigma = \sigma_0^{-1}\sigma_1$ とすれば,

$$g(1, \sigma) = h(1) - h(\sigma) = (1 - \sigma)h(1)$$

となり, $C^0(G, A) = A$ より $B^1(G, A)$ の元はこの方程式で特徴付けられる. すなわち,

$$B^1(G, A) = \{g \in Z^1(G, A) \mid \exists a \in A \text{ s.t. } g(1, \sigma) = (1 - \sigma)a,\ \sigma \in G\}$$

である.

さて, $C^1(G, A)$ の元は 2 変数関数であるが, $G$ 写像であることを用いれば, 上の計算のように, 定義域を $\{1\} \times G$ に制限して, 1 つ変数を減らして考えれば良いことがわかる. したがって,

$$\begin{aligned} Z^1(G, A) &\simeq \{f \in \mathrm{Map}(G, A) \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau),\ \sigma, \tau \in G\}, \\ B^1(G, A) &\simeq \{g \in \mathrm{Map}(G, A) \mid \exists a \in A \text{ s.t. } g(\sigma) = (1 - \sigma)a,\ \sigma \in G\} \end{aligned}$$

が成り立つ. 右辺のように, 1 つ変数を減らした表現を非斉次形という. $Z^1(G, A)$ の方程式を, 交差準同型 (crossed homomorphism) という. $A = A^G$, すなわち $A$ に $G$ が自明に作用しているとする. このとき, 交差準同型は準同型 $f(\sigma\tau) = f(\sigma) + f(\tau)$ に他ならない. さらに, $B^1(G, A) = 0$ より, $H^1(G, A) = \mathrm{Hom}(G, A)$ が成り立つ.

**命題 8.** (1) $H^1(G, A) \simeq \dfrac{\{f \in \mathrm{Map}(G, A) \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau),\ \sigma, \tau \in G\}}{\{g \in \mathrm{Map}(G, A) \mid \exists a \in A \text{ s.t. } g(\sigma) = (1 - \sigma)a,\ \sigma \in G\}}$.
(2) $A = A^G$ ならば, $H^1(G, A) = \mathrm{Hom}(G, A)$. □

- $H^2(G, A)$ の計算. $f \in Z^2(G, A)$ とする. このとき,

(1) $f : G^3 \to A$,

(2) 任意の $\sigma, \sigma_0, \sigma_1, \sigma_2 \in G$ に対して, $f(\sigma\sigma_0, \sigma\sigma_1, \sigma\sigma_2) = \sigma f(\sigma_0, \sigma_1, \sigma_2)$ が成り立つ,

(3) 任意の $\sigma_0, \sigma_1, \sigma_2, \sigma_3 \in G$ に対して, $f(\sigma_1, \sigma_2, \sigma_3) - f(\sigma_0, \sigma_2, \sigma_3) + f(\sigma_0, \sigma_1, \sigma_3) - f(\sigma_0, \sigma_1, \sigma_2) = 0$ が成り立つ.

1 次の場合と同じように, 1 変数減らして考えてみる. (2), (3) より,

$$\begin{aligned} 0 =& \sigma_0^{-1}\sigma_1 f(1, \sigma_1^{-1}\sigma_2, \sigma_1^{-1}\sigma_3) - f(1, \sigma_0^{-1}\sigma_2, \sigma_0^{-1}\sigma_3) \\ &+ f(1, \sigma_0^{-1}\sigma_1, \sigma_0^{-1}\sigma_3) - f(1, \sigma_0^{-1}\sigma_1, \sigma_0^{-1}\sigma_2) \end{aligned}$$

である. $\tau_1 = \sigma_0^{-1}\sigma_1,\ \tau_2 = \sigma_1^{-1}\sigma_2,\ \tau_3 = \sigma_2^{-1}\sigma_3$ とすれば, 上の方程式は

$$\tau_1 f(1,\tau_2,\tau_2\tau_3) - f(1,\tau_1\tau_2,\tau_1\tau_2\tau_3) + f(1,\tau_1,\tau_1\tau_2\tau_3) - f(1,\tau_1,\tau_1\tau_2) = 0$$

となる. 複雑な方程式であるが, [4] の p.12 および p.18 の非斉次化の対応より, $f \in C^2(G,A)$ に対して, $f_0 : G^2 \to A$ を $f_0(\sigma,\tau) = f(1,\sigma,\sigma\tau)$ と定義すると, 方程式

$$\tau_1 f_0(\tau_2,\tau_3) - f_0(\tau_1\tau_2,\tau_3) + f_0(\tau_1,\tau_2\tau_3) - f_0(\tau_1,\tau_2) = 0 \quad \text{(2-cocycle)}$$

に変換できる. この方程式を 2-cocycle 条件と呼ぶことが多い.

次に $g \in B^2(G,A)$ とする. このとき,

(1) $g : G^3 \to A$,

(2) 任意の $\sigma,\sigma_0,\sigma_1,\sigma_2 \in G$ に対して, $g(\sigma\sigma_0,\sigma\sigma_1,\sigma\sigma_2) = \sigma g(\sigma_0,\sigma_1,\sigma_2)$ が成り立つ,

(3) $h \in C^1(G,A)$ が存在し, $g(\sigma_0,\sigma_1,\sigma_2) = h(\sigma_1,\sigma_2) - h(\sigma_0,\sigma_2) + h(\sigma_0,\sigma_1)$ である,

が成り立つ. (2), (3) より,

$$g(1,\sigma_0^{-1}\sigma_1,\sigma_0^{-1}\sigma_2) = \sigma_0^{-1}\sigma_1 h(1,\sigma_1^{-1}\sigma_2) - h(1,\sigma_0^{-1}\sigma_2) + h(1,\sigma_0^{-1}\sigma_1)$$

であり, $\tau_1 = \sigma_0^{-1}\sigma_1,\ \tau_2 = \sigma_1^{-1}\sigma_2$ とすれば, 方程式

$$g(1,\tau_1,\tau_1\tau_2) = \tau_1 h(1,\tau_2) - h(1,\tau_1\tau_2) + h(1,\tau_1)$$

を得る. $h \in C^1(G,A)$ の非斉次化 $h_0$ は $h_0(\tau) = h(1,\tau)$ なので, 方程式は

$$g_0(\tau_1,\tau_2) = \tau_1 h_0(\tau_2) - h_0(\tau_1\tau_2) + h_0(\tau_1) \quad \text{(2-coboundary)}$$

と書き換えられる. 以上より,

$$Z^2(G,A) \simeq \{f_0 \in \mathrm{Map}(G^2,A) \mid f_0 \text{は 2-cocycle を満たす}\},$$
$$B^2(G,A) \simeq \{g_0 \in \mathrm{Map}(G^2,A) \mid g_0 \text{は 2-coboundary を満たす}\}$$

である.

**命題 9.** $H^2(G,A) \simeq \dfrac{\{f_0 \in \mathrm{Map}(G^2,A) \mid f_0 \text{は 2-cocycle を満たす}\}}{\{g_0 \in \mathrm{Map}(G^2,A) \mid g_0 \text{は 2-coboundary を満たす}\}}$. □

ここまでで, $0,1,2$ 次のコホモロジー群の記述を行なった[3]. $n \geq 3$ に対しても複雑になってゆくが, cocycle, coboundary の方程式を求めることで $H^n(G,A)$ の記述が得られる. 注意として, cocycle, coboundary の満たす方程式は, コホモロジー群を表現したり, 方程式を通じてコホモロジー群の性格を理解するためには役立つが, 実際にコホモロジー群を計算するにはあまり役には立たない. コホモロジー群の計算では, 定義に従えば計算できる対象を知ること, すでに計算されているコホモロジー群から相対的に計算をすること, が常套手段である. 以降, その方法について少し説明したい.

[3]筆者は, 群のコホモロジーは, $n = 0,1,2$ の場合が特に大事であると思っている.

## 3.3 群のコホモロジーの長完全系列

この小節でも $G$ は有限群とする.

**命題 10.** $A, B$ を $G$ 加群とする. 射 $f : A \to B$ に対して, コホモロジー群の射

$$f : H^n(G, A) \to H^n(G, B)$$

が定まる. さらに, $f$ が同型であれば, 任意の $n$ について $f : H^n(G, A) \to H^n(G, B)$ も同型である.

Proof. 射 $f : A \to B$ は射

$$f : X^n(G, A) \to X^n(G, B),\ x \mapsto f \circ x$$

を誘導し, $f$ が $G$ 加群の射であることから, $x \in C^n(G, A), \sigma \in G$ に対して

$$f \circ x(\sigma\sigma_0, \cdots, \sigma\sigma_n) = f(\sigma x(\sigma_0, \cdots, \sigma_n)) = \sigma(f \circ x(\sigma_0, \cdots, \sigma_n))$$

より, $f : C^n(G, A) \to C^n(G, B)$ が誘導される. $x \in Z^n(G, A)$ とせよ. このとき,

$$\begin{aligned}
\partial^{n+1}(f \circ x)(\sigma_0, \cdots, \sigma_n) &= \sum_{i=0}^{n} (-1)^i (f \circ x)(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_n) \\
&= f\left(\sum_{i=0}^{n} (-1)^i x(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_n)\right) \\
&= f(\partial^{n+1}(x)(\sigma_0, \cdots, \sigma_n)) \\
&= f(0) = 0
\end{aligned}$$

より $f \circ x \in Z^n(G, B)$ であり, $x \in B^{n-1}(G, A)$ に対して,

$$\begin{aligned}
f \circ \partial^n(x)(\sigma_0, \cdots, \sigma_n) &= f\left(\sum_{i=0}^{n} (-1)^i x(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_n)\right) \\
&= \sum_{i=0}^{n} (-1)^i f \circ x(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_n) \\
&= \partial^n(f \circ x)(\sigma_0, \cdots, \sigma_n)
\end{aligned}$$

より $f \circ \partial^n(x) \in B^n(G, B)$ である. 以上より, $f$ はコホモロジー群の射 $f : H^n(G, A) \to H^n(G, B)$ を誘導する. $g$ が $f$ の逆写像であるとき, $g$ はコホモロジー群においても $f$ の逆写像を誘導する. □

**定理 3** (コホモロジー群の長完全系列)**.** $A, B, C$ を $G$ 加群とし, 短完全系列

$$0 \to A \to B \to C \to 0$$

があるとする. このとき, 任意の $n \in \mathbb{Z}_{\geq 0}$ に対して, 射

$$H^n(G, C) \xrightarrow{\delta} H^{n+1}(G, A)$$

が存在し,

$$\begin{array}{rcccccc}
0 & \to & H^0(G,A) & \to & H^0(G,B) & \to & H^0(G,C) \\
 & \xrightarrow{\delta} & H^1(G,A) & \to & H^1(G,B) & \to & H^1(G,C) \\
 & \xrightarrow{\delta} & H^2(G,A) & \to & H^2(G,B) & \to & H^2(G,C) \\
 & \xrightarrow{\delta} & \cdots & & & & \\
 & \cdots & & & & & \\
 & \xrightarrow{\delta} & H^n(G,A) & \to & H^n(G,B) & \to & H^n(G,C) \\
 & \xrightarrow{\delta} & \cdots & & & &
\end{array}$$

は完全系列をなす. $\delta$ を連結準同型という.

Proof. 任意の $n \in \mathbb{Z}_{\geq 0}$ に対して, $n$-cochain の列

$$0 \to C^n(G, A) \to C^n(G, B) \to C^n(G, C) \to 0 \ \cdots \ (*)$$

が完全系列であることを示す. そのために, $n$-cochain の非斉次化を調べる. $M$ を $G$ 加群とする. 1 次, 2 次コホモロジーの計算でも述べていたように, $n$-cochain は $\{1\} \times G^n$ での値で決まる. すなわち, $x \in C^n(G, M)$ に対して,

$$x(\sigma_0, \cdots, \sigma_n) = \sigma_0 x(1, \sigma_0^{-1}\sigma_1, \cdots, \sigma_0^{-1}\sigma_n)$$

で関数 $x$ が定まる. このことから, 任意の $G$ 加群 $M$ に対して, アーベル群としての同一視

$$\begin{aligned}
C^n(G, M) &= \prod_{(\sigma_1, \cdots, \sigma_n) \in G^n} M, \\
x(1, \sigma_1 \cdots, \sigma_n) &= m_{(\sigma_1, \cdots, \sigma_n)}
\end{aligned}$$

ができる. したがって, もし $0 \to A \to B \to C \to 0$ が完全系列であれば,

$$0 \to \prod_{(\sigma_1, \cdots, \sigma_n) \in G^n} A \to \prod_{(\sigma_1, \cdots, \sigma_n) \in G^n} B \to \prod_{(\sigma_1, \cdots, \sigma_n) \in G^n} C \to 0$$

もまた完全系列である. 以上より, $(*)$ は完全系列である.

$n$-cochain の完全系列 $(*)$ より,

$$\frac{C^n(G, A)}{B^n(G, A)} \to \frac{C^n(G, B)}{B^n(G, B)} \to \frac{C^n(G, C)}{B^n(G, C)} \to 0$$

と

$$0 \to Z^{n+1}(G, A) \to Z^{n+1}(G, B) \to Z^{n+1}(G, C)$$

は完全系列である. また, $\partial^{n+1}$ による完全可換図式

$$\begin{array}{ccccccc} & & \dfrac{C^n(G,A)}{B^n(G,A)} & \longrightarrow & \dfrac{C^n(G,B)}{B^n(G,B)} & \longrightarrow & \dfrac{C^n(G,C)}{B^n(G,C)} \longrightarrow 0 \\ & & {\scriptstyle \partial^{n+1}}\downarrow & & {\scriptstyle \partial^{n+1}}\downarrow & & {\scriptstyle \partial^{n+1}}\downarrow \\ 0 & \longrightarrow & Z^{n+1}(G,A) & \longrightarrow & Z^{n+1}(G,B) & \longrightarrow & Z^{n+1}(G,C) \end{array}$$

において, 縦写像の核は $n$ 次コホモロジー, 余核は $n+1$ 次コホモロジーである. 以上まとめると, 蛇の補題より,

$$\begin{array}{ccccc} H^n(G,A) & \to & H^n(G,B) & \to & H^n(G,C) \\ \xrightarrow{\delta} H^{n+1}(G,A) & \to & H^{n+1}(G,B) & \to & H^{n+1}(G,C) \end{array}$$

が完全系列となる射 $\delta$ が存在する. □

蛇の補題と次の可換図式を参考に, 0 次から 1 次への連結準同型 $H^0(G,C) \xrightarrow{\delta} H^1(G,A)$ を具体的に求めておこう. 一般に, $C^0(G,M) = M$, $H^0(G,M) = M^G$, $\partial^1(m)(\sigma) = (1-\sigma)m$ であることに注意する.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \xrightarrow{\delta} & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C^0(G,A) & \longrightarrow & C^0(G,B) & \longrightarrow & C^0(G,C) & \longrightarrow & 0 \\ & & {\scriptstyle \partial^1}\downarrow & & {\scriptstyle \partial^1}\downarrow & & {\scriptstyle \partial^1}\downarrow & & \\ 0 & \longrightarrow & Z^1(G,A) & \longrightarrow & Z^1(G,B) & \longrightarrow & Z^1(G,C) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & \xrightarrow{\delta} & H^1(G,A) & \longrightarrow & H^1(G,B) & \longrightarrow & H^1(G,C) & & \end{array}$$

$c \in H^0(G,C) = C^G$ とせよ. $C = B/A$ なので, $c = b \bmod A$ となる $b \in B$ が存在する. このとき, 任意の $\sigma \in G$ に対して $\sigma(c) = c$ より,

$$\partial^1(b)(\sigma) = (1-\sigma)b = b - \sigma(b) \in A$$

であり, $\delta(c) = \partial^1(b)$ である. というわけで, 全射 $B \to C$ がよくわかっていれば, 連結準同型 $H^0(G,C) \xrightarrow{\delta} H^1(G,A)$ もわかりやすいものである.

# 4 Hilbert の定理 90 と Kummer 理論

## 4.1 Hilbert の定理 90

ガロア群のコホモロジーにおける最も大きな結果の一つである, Hilbert の定理 90 を示す.

**定理 4** (Hilbert の定理 90)**.** $K/F$ を有限次ガロア拡大とし, $G = \mathrm{Gal}(K/F)$ とする. このとき,

$$H^1(G, K^\times) = 0$$

が成り立つ.

Proof. $H^1(G, K^\times) = Z^1(G, K^\times)/B^1(G, K^\times)$ であったので, $Z^1(G, K^\times) \subseteq B^1(G, K^\times)$ であることを示せばよい. 非斉次形での表現

$$Z^1(G, K^\times) = \{f \in \mathrm{Map}(G, K^\times) \mid f(\sigma\tau) = f(\sigma)\sigma(f(\tau)),\ \sigma, \tau \in G\},$$
$$B^1(G, K^\times) = \{g \in Z^1(G, K^\times) \mid \exists \beta \in K^\times \text{ s.t. } g(\sigma) = \beta\sigma(\beta)^{-1},\ \sigma \in G\}$$

を用いる. $f \in Z^1(G, K^\times)$ とせよ. また, $\alpha \in K^\times$, $\sigma \in G$ をとる. このとき,

$$\begin{aligned} f(\sigma)\sigma\left(\sum_{\tau\in G} f(\tau)\tau(\alpha)\right) &= \sum_\tau f(\sigma)\sigma(f(\tau))\sigma\tau(\alpha) \\ &= \sum_\tau f(\sigma\tau)\sigma\tau(\alpha) \\ &= \sum_\tau f(\tau)\tau(\alpha) \end{aligned}$$

を得る. デデキントの補題と $f(\tau) \in K^\times$ より, $\sum_\tau f(\tau)\tau(\alpha) \neq 0$ となる $\alpha \in K^\times$ が存在する. したがって, $\beta = \sum_\tau f(\tau)\tau(\alpha) \neq 0$ とおけば,

$$f(\sigma) = \beta\sigma(\beta)^{-1}$$

より, $f \in B^1(G, K^\times)$ である. □

## 4.2 一般線型群に対する Hilbert の定理 90

この小節のみ, 非アーベル・コホモロジーについて述べたい. $G$ を有限群とする. $G$ の作用を持つ群を $G$ 群とよぶ. 非斉次形での 1 次コホモロジー群の類似として, 1 次の非アーベル・コホモロジーを定義する.

**定義 6** (1 次の非アーベル・コホモロジー)**.** $G$ を群, $A$ を $G$ 群とする. $G$ の $A$ 係数の 1-cocycle を

$$Z^1(G, A) = \{f \in \mathrm{Map}(G, A) \mid f(\sigma\tau) = f(\sigma)\sigma f(\tau),\ \sigma, \tau \in G\}$$

とし, $f, g \in Z^1(G, A)$ に対して,

$$f \sim g \overset{\text{def}}{\iff} \exists a \in A \text{ s.t. } f(\sigma) = ag(\sigma)(\sigma a)^{-1},\ \sigma \in G$$

で同値関係 $\sim$ を定義する. 商集合

$$H^1(G,A) = Z^1(G,A)/\sim$$

を, $G$ の $A$ 係数の 1 次コホモロジーという. 任意の $f \in Z^1(G,A)$ が恒等写像 $f(\sigma) = 1$ ($\sigma \in G$) と同値なとき, すなわち, $f(\sigma) = a(\sigma a)^{-1}$ となる $a \in A$ が存在するとき, $H^1(G,A) = 1$ と表す.

体 $K$ に対して $GL_n(K)$ を, $K$ 成分の $n$ 次一般線型群とする. $K/F$ がガロア拡大のとき, ガロア群 $G$ は $(a_{ij}) \in GL_n(K)$ へ, 成分ごとに作用する.

**命題 11** (一般線型群に対する Hilbert の定理 90)**.** $K/F$ を有限次ガロア拡大とし, $G = \mathrm{Gal}(K/F)$ とする. 任意の $n \in \mathbb{Z}_{\geq 1}$ に対して, $H^1(G, GL_n(K)) = 1$ である. すなわち, $f \in Z^1(G, GL_n(K))$ ならば, $f(\sigma) = B(\sigma B)^{-1}$ となる $B \in GL_n(K)$ が存在する.

Proof. $f \in Z^1(G, GL_n(K))$ とし, $A \in GL_n(K)$ とする. このとき,

$$\begin{aligned} f(\sigma)\sigma\left(\sum_{\tau\in G} f(\tau)\tau(A)\right) &= \sum_{\tau} f(\sigma)\sigma f(\tau)\sigma\tau(A) \\ &= \sum_{\tau} f(\sigma\tau)\sigma\tau(A) \\ &= \sum_{\tau} f(\tau)\tau(A) \end{aligned}$$

である. したがって, $\sum_\tau f(\tau)\tau(A)$ が正則行列となる $A \in GL_n(K)$ が存在すれば, $B = \sum_\tau f(\tau)\tau(A)$ として定理が成立する.

$x \in K^n$ に対して $b(x) = \sum_\tau f(\tau)\tau(x)$ とする. $\phi : K^n \to K$ を線型汎関数で, 任意の $x \in K^n$ に対して $\phi(b(x)) = 0$ を満たすものとする. このとき, 任意の $\alpha \in K$ に対して,

$$\begin{aligned} 0 &= \phi(b(\alpha x)) \\ &= \sum_{\tau} \phi(f(\tau)\tau(\alpha x)) \\ &= \sum_{\tau} \phi(f(\tau)\tau(x))\tau(\alpha) \end{aligned}$$

となる. $\phi(f(\tau)\tau(x)) \in K$ なので, デデキントの補題より, 任意の $\tau \in G$, $x \in K^n$ に対して $\phi(f(\tau)\tau(x)) = 0$ となる. そこで, 任意の $x \in K^n$ に対して, $y = \tau^{-1}f(\tau)^{-1}x \in K^n$ とすれば, $0 = \phi(f(\tau)\tau y) = \phi(x)$ となり, $\phi = 0$ である. したがって, $K^n = \langle b(x) \mid x \in K^n \rangle$ である.

$a_1, \cdots, a_n \in K^n$ を $b(a_1), \cdots, b(a_n)$ が $K^n$ の基底となるようにとり, $A = (a_1 \ \cdots \ a_n)$ とする. $A$ は正則行列であることに注意する.

$$b(A) = b(a_1 \ \cdots \ a_n) = (b(a_1) \ \cdots \ b(a_n))$$

より $b(A)$ は正則であり,

$$b(A) = \sum_{\tau} f(\tau)\tau(A)$$

でもあるので, $A$ が求める正則行列である. □

## 4.3 Kummer 理論

Hilbert の定理 90 の応用として, Kummer 理論を紹介する. $n \in \mathbb{Z}_{\geq 1}$ に対して, $\mu_n$ を 1 の $n$ 乗根のなす群とする. 体 $F$ の標数は $n$ と素とし, $\mu_n \subseteq F$ とする.

**定理 5** (Kummer 理論)**.** $K/F$ を有限次アーベル拡大, $G = \mathrm{Gal}(K/F)$ とする. さらに, $G$ の指数を $n$ とする. すなわち, $G$ の元の位数の最大値が $n$ であるとする. このとき, 標準的な同型

$$G \simeq \mathrm{Hom}\left(\frac{(K^\times)^n \cap F^\times}{(F^\times)^n}, \mu_n\right)$$

が存在する.

Kummer 理論の結論は, 標準的な同型

$$\frac{(K^\times)^n \cap F^\times}{(F^\times)^n} \simeq \mathrm{Hom}(G, \mu_n)$$

や, 非退化双線型形式

$$G \times \left(\frac{(K^\times)^n \cap F^\times}{(F^\times)^n}\right) \to \mu_n$$

という形でも述べられる.

Proof. 短完全系列

$$0 \to \mu_n \to K^\times \overset{a \mapsto a^n}{\to} (K^\times)^n \to 0$$

に対して, コホモロジー群の長完全系列を取ると, 0 次, 1 次の項として完全系列

$$\begin{aligned} 0 \ &\to \ H^0(G, \mu_n) \ \to \ H^0(G, K^\times) \ \to \ H^0(G, (K^\times)^n) \\ &\overset{\delta}{\to} \ H^1(G, \mu_n) \ \to \ H^1(G, K^\times) \end{aligned}$$

を得る. これらのコホモロジー群を調べる. まず, 仮定より $\mu_n \subseteq F$ であるので,

$$H^0(G, \mu_n) = \mu_n^G = \mu_n, \ H^1(G, \mu_n) = \mathrm{Hom}(G, \mu_n)$$

である. 次に, ガロア理論と Hilbert の定理 90 より,

$$H^0(G, K^\times) = F^\times, \ H^1(G, K^\times) = 0, \ H^0(G, (K^\times)^n) = (K^\times)^n \cap F^\times$$

である. これらより, 完全系列

$$0 \to \mu_n \to F^\times \overset{a \mapsto a^n}{\to} (K^\times)^n \cap F^\times \overset{\delta}{\to} \mathrm{Hom}(G, \mu_n) \to 0$$

が得られる. したがって, 同型

$$\frac{(K^\times)^n \cap F^\times}{(F^\times)^n} \overset{\delta}{\simeq} \mathrm{Hom}(G, \mu_n)$$

が成り立つ. この同型は, $G$ と $\frac{(K^\times)^n \cap F^\times}{(F^\times)^n}$ が互いに双対の関係にあることを示している. また, 連結準同型 $\delta$ は, $\alpha \in (K^\times)^n \cap F^\times$ に対して $\alpha$ の $n$ 乗根 $\sqrt[n]{\alpha}$ をとり,

$$\delta(\alpha(F^\times)^n) = f_\alpha,\ f_\alpha(\sigma) = \frac{\sqrt[n]{\alpha}}{\sigma(\sqrt[n]{\alpha})}$$

で与えられる. これは $\sqrt[n]{\alpha}$ の取り方に依らない. □

# 5 いくつかの話題

この章では, 後々のために知っておいた方がいいかな, というような話題を紹介する. ただし, 難易度に応じて, 証明はしたりしなかったりする.

## 5.1 コホモロジーの well-defined 性

$G$ を有限群とする. アーベル群 $X$ と言うときは, 常に自明な $G$ の作用を持つとする.

**定理 6.** $A$ を $G$ 加群とし, $n \in \mathbb{Z}_{\geq 0}$ に対して $\mathfrak{H}^n(G, A)$ を $G$ 加群からアーベル群への関手で, 以下を満たすものとする.

(1) $\mathfrak{H}^0(G, A) = A^G$,

(2) $0 \to A \to B \to C \to 0$ を任意の $G$ 加群の短完全系列とするとき, 任意の $n \geq 0$ に対して,

$$\begin{array}{rcccccc} 0 & \to & \mathfrak{H}^0(G,A) & \to & \mathfrak{H}^0(G,B) & \to & \mathfrak{H}^0(G,C) \\ & \overset{\gamma}{\to} & \mathfrak{H}^1(G,A) & \to & \mathfrak{H}^1(G,B) & \to & \mathfrak{H}^1(G,C) \\ & \overset{\gamma}{\to} & \mathfrak{H}^2(G,A) & \to & \mathfrak{H}^2(G,B) & \to & \mathfrak{H}^2(G,C) \\ & \overset{\gamma}{\to} & \cdots & & & & \\ & \cdots & & & & & \\ & \overset{\gamma}{\to} & \mathfrak{H}^n(G,A) & \to & \mathfrak{H}^n(G,B) & \to & \mathfrak{H}^n(G,C) \\ & \overset{\gamma}{\to} & \cdots & & & & \end{array}$$

が完全系列となる射 $\mathfrak{H}^n(G, C) \overset{\gamma}{\to} \mathfrak{H}^{n+1}(G, A)$ が存在する.

(3) 任意のアーベル群 $X$, 任意の $n \geq 1$ に対して, $\mathfrak{H}^n(G, \mathrm{Hom}(\mathbb{Z}[G], X)) = 0$.

このとき, 任意の $G$ 加群 $A$ と任意の $n \geq 0$ に対して

$$H^n(G, A) \simeq \mathfrak{H}^n(G, A)$$

が成り立つ.

本稿で紹介した複体以外からも, 群のコホモロジーを作ることができることを, 上記の定理は示している. つまり, 群のコホモロジーは普遍性によって特徴づけられ, 本稿ではコホモロジーの一つの構成法を紹介した, ということになる.

## 5.2 巡回群のコホモロジー

$G = \langle \sigma \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ を位数 $n$ の巡回群とする. $G$ 加群 $A$ と $a \in A$ に対して,

$$Na = \sum_{i=0}^{n-1} \sigma^i a \in A$$

をノルムオペレーターとし, $A[N] = \{a \in A \mid Na = 0\}$ とする.

**命題 12.** $A$ を $G$ 加群とするとき,

$$H^1(G, A) \simeq \frac{A[N]}{(1-\sigma)A},\ f \mapsto f(\sigma)$$

が成り立つ. ただし, $f : G \to A$ は非斉次形の 1-cocycle である.

Proof. $f \in Z^1(G, A)$ とせよ. このとき,

$$Nf(\sigma) = \sum_{i=0}^{n-1} \sigma^i f(\sigma) = \sum_{i=0}^{n-1} (f(\sigma^{i+1}) - f(\sigma^i)) = 0$$

より, $f(\sigma) \in A[N]$ である. また, $a \in A[N]$ とせよ. $g_a(\sigma) = a$ とし, 帰納的に $g_a(\sigma^{i+1}) = g_a(\sigma^i) + \sigma^i a$ と定める. $i \leq j,\ i \equiv j \bmod n$ のとき, $j = i + kn$ とすると,

$$\begin{aligned} g_a(\sigma^j) &= g_a(\sigma^{i+kn}) \\ &= g_a(\sigma^{i+(k-1)n+n-1}) + \sigma^{n-1}a \\ &= \cdots \\ &= g_a(\sigma^{i+(k-1)n}) + (\sigma^{n-1} + \sigma^{n-2} + \cdots + \sigma + 1)a \\ &= g_a(\sigma^{i+(k-1)n}) \\ &= \cdots \\ &= g_a(\sigma^i) \end{aligned}$$

より, $g_a : G \to A$ は well-defined である. また, 定義より $g_a \in Z^1(G, A)$ である. ゆえに同型

$$Z^1(G, A) \simeq A[N],\ f \leftrightarrow f(\sigma)$$

が成り立つ. また, $f \in B^1(G, A) \Leftrightarrow \exists a \in A \text{ s.t. } f(\sigma) = (1-\sigma)a$ なので, 同型

$$H^1(G, A) \simeq \frac{A[N]}{(1-\sigma)A}$$

が成り立つ. この同型は $G$ の生成元 $\sigma$ を決めるごとに定まるもので, 標準的なものではないことに注意する. □

**系 1** (巡回拡大の Hilbert の定理 90)**.** $K/F$ を $n$ 次の巡回拡大とし, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ とする. このとき, $\alpha \in K^\times$ に対して, $N_{K/F}\alpha = 1$ ならば, $\alpha = \beta\sigma(\beta)^{-1}$ となる $\beta \in K^\times$ が存在する.

$\sigma^n = 1$ より, 任意の $G$ 加群 $A$ に対して $N(1-\sigma)A = (1-\sigma)NA = 0$ である. すなわち,

$$A \overset{1-\sigma}{\to} A \overset{N}{\to} A,$$
$$A \overset{N}{\to} A \overset{1-\sigma}{\to} A,$$

は複体をなす. この複体のコホモロジーを

$$\hat{H}^{-1}(G, A) = \frac{A[N]}{(1-\sigma)A},$$
$$\hat{H}^{0}(G, A) = \frac{A^G}{NA},$$

とおき, これらを, $-1, 0$ 次の Tate cohomology という[4]. 上で示したように, $\hat{H}^{-1}(G, A) \simeq H^1(G, A)$ である.

**命題 13.** $G = \langle\sigma\rangle$ を位数 $n$ の巡回群, $0 \to A \to B \to C \to 0$ を $G$ 加群の短完全系列とする. このとき, 次の 6 項

$$\begin{array}{ccccc} \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & \longrightarrow & \hat{H}^0(G,C) \\ {\scriptstyle\delta_1}\uparrow & & & & \downarrow{\scriptstyle\delta_{-1}} \\ \hat{H}^{-1}(G,C) & \longleftarrow & \hat{H}^{-1}(G,B) & \longleftarrow & \hat{H}^{-1}(G,A) \end{array}$$

が完全系列となる連結準同型 $\delta_1, \delta_{-1}$ が存在する.

証明は蛇の補題の練習問題程度なので, もし気になれば各自で考えてみよ. という感じで, 証明自体は簡単であるが, $H^1(G, A) \simeq \hat{H}^{-1}(G, A)$ であることと, コホモロジーの well-defined 性より次の重要な結論が得られる.

**定理 7** (巡回群のコホモロジーの決定)**.** $G$ を位数 $n$ の巡回群とする. このとき,

$$H^i(G, A) \simeq \begin{cases} A^G & (i = 0), \\ \hat{H}^0(G, A) & (i \neq 0,\ i:\ \text{even}), \\ \hat{H}^{-1}(G, A) & (i:\ \text{odd}) \end{cases}$$

が成り立つ. □

[4] $(1-\sigma)A$ を $\sum_{\sigma\in G}(1-\sigma)A$ に置き換えれば, 任意の有限群 $G$ と任意の $G$ 加群 $A$ に対して, $\hat{H}^0(G, A)$, $\hat{H}^{-1}(G, A)$ が定義される. Tate cohomology は, $\hat{H}^{-1}$ と $\hat{H}^0$ を接着剤として, homology と cohomology をつないだものである.

# 6 ガロア・コホモロジー

この章では, 簡単にガロア・コホモロジーを紹介する. 詳しくは [4] などを参照してほしい.

## 6.1 副有限群

**定義 7** (副有限群)**.** 群 $G$ が副有限群 (profinite group) であるとは, ある有限群の射影系 $\{G_i \mid i \in I\}$ が存在して,

$$G \simeq \varprojlim_{i \in I} G_i$$

となることである. 有限群に離散位相を導入することにより, 副有限群 $G$ は直積位相により位相群となる.

副有限群には, 純位相的な特徴付けがある.

**命題 14.** 次が成り立つ.
(1) $G$ が副有限群 $\Leftrightarrow$ $G$ は Hausdorff, compact, totally disconnected な位相群.
(2) $G$ の開正規部分群全体 $\{H_t \mid t \in T\}$ は, $G$ の一つの単位元の基本近傍系をなす.
(3) 自然な射影は, 位相群の同型

$$G \simeq \varprojlim_{t \in T} G/H_t,\ g \mapsto (gH_t)_t$$

を引き起こす.

$F$ を体, $\overline{F}$ を $F$ の分離閉包とし, $G_F = \mathrm{Gal}(\overline{F}/F)$ を $F$ の絶対ガロア群とする.

**命題 15.** $F$ を体とする. このとき, $\mathfrak{F}_F$ を $F$ の有限次ガロア拡大全体とすると, 同型

$$G_F \simeq \varprojlim_{F' \in \mathfrak{F}_F} \mathrm{Gal}(F'/F)$$

が成り立ち, よって $G_F$ は副有限群である. 射影極限はガロア群の自然な全射に関してとる. $G_F$ の位相を Krull 位相という. また,

$$\{\mathrm{Gal}(\overline{F}/F') \mid F' \in \mathfrak{F}_F\}$$

は, 単位元の基本近傍系である.

## 6.2 副有限群のコホモロジー

$G$ を副有限群とする. 位相 $G$ 加群 $M$ の位相は, 離散位相であるとする.

$$X^i(G, M) = \mathrm{Map}_c(G^{i+1}, M) = \{\varphi : G^{i+1} \to M \ :\ \text{連続}\,\}$$

を, $G$ の $i$ 個直積から $M$ への連続写像のなす加群とし,

$$C^i(G,M) = X^i(G,M)^G$$

とする. ここで, 右上の $G$ は $G$ 不変部分加群を示す. 有限群の場合と同様に複体

$$C^0(G,M) \to C^1(G,M) \to \cdots \to C^i(G,M) \to \cdots$$

が得られるので, コホモロジー $H^i(G,M)$ $(i \geq 0)$ が定義される. 位相を考慮すること以外, 有限群のコホモロジーと同じであることに注意する.

$H$ を $G$ の閉正規部分群全体とする.

$$\pi_H : G \to G/H,\ g \mapsto gH$$

を自然な全射とする. $G/H$ は副有限群であり, $M$ の $H$ 不変部分加群 $M^H$ は $G/H$ 加群であるため, $G/H$ のコホモロジー群

$$H^i(G/H, M^H)$$

が定義される. $f \in C^i(G/H, M^H)$ とせよ. 可換図式

$$\begin{array}{ccc} G^{i+1} & \xrightarrow{f\circ\pi_H} & M \\ {\scriptstyle \pi_H}\downarrow & & \uparrow{\scriptstyle \text{inclusion}} \\ (G/H)^{i+1} & \xrightarrow{f} & M^H \end{array}$$

から, 写像

$$\inf_H : H^i(G/H, M^H) \to H^i(G,M),\ \overline{f} \mapsto \overline{f \circ \pi_H}$$

が定義される. $\inf_H$ を膨張写像 (inflation map) という.

また, 定義域を制限することにより, 写像

$$\mathrm{res}_H : H^i(G,M) \to H^i(H,M),\ \overline{f} \mapsto \overline{f|_{H^{i+1}}}$$

が定義される. $\mathrm{res}_H$ を制限写像 (restriction map) という.

**命題 16.** $G$ を副有限群とし, $H_t$ $(t \in T)$ を $G$ の開正規部分群全体とする. $M$ を離散 $G$ 加群とする. $i \in \mathbb{Z}_{\geq 0}$ とする. 次が成り立つ.
(1) $\{H^i(G/H_t, M^{H_t}) \mid t \in T\}$ は膨張写像によって帰納系をなす.
(2) 膨張写像は同型

$$\varinjlim_{t\in T} H^i(G/H_t, M^{H_t}) \simeq H^i(G,M)$$

を引き起こす.
(3) $0 \to A \to B \to C \to 0$ を離散 $G$ 加群の短完全系列とすると, 任意の $n \in \mathbb{Z}_{\geq 0}$ に対して, 射

$$H^n(G, C) \overset{\delta}{\to} H^{n+1}(G, A)$$

が存在し,

$$\begin{array}{rcccccc}
0 & \to & H^0(G,A) & \to & H^0(G,B) & \to & H^0(G,C) \\
 & \overset{\delta}{\to} & H^1(G,A) & \to & H^1(G,B) & \to & H^1(G,C) \\
 & \overset{\delta}{\to} & H^2(G,A) & \to & H^2(G,B) & \to & H^2(G,C) \\
 & \overset{\delta}{\to} & \cdots & & & & \\
 & \cdots & & & & & \\
 & \overset{\delta}{\to} & H^n(G,A) & \to & H^n(G,B) & \to & H^n(G,C) \\
 & \overset{\delta}{\to} & \cdots & & & &
\end{array}$$

は完全系列をなす.
(4) (膨張–制限完全系列) $H$ を $G$ を閉正規部部群とするとき, 完全系列

$$0 \to H^1(G/H, M^H) \overset{\inf_H}{\to} H^1(G, M) \overset{\mathrm{res}_H}{\to} H^1(H, M)$$

が成り立つ.

## 6.3 ガロア・コホモロジー, Hilbert の定理 90 と Kummer 理論

$F$ を体とする. $\overline{F}$ を $F$ の分離閉包とする. また, $n$ を $F$ の標数と素な正整数とする. $\overline{F}^\times$ は離散位相で考える.

**定義 8** (ガロア・コホモロジー)**.** $i \in \mathbb{Z}_{\geq 0}$ と離散 $G_F$ 加群 $M$ に対して,

$$H^i(F, M) = H^i(G_F, M)$$

を $M$ のガロア・コホモロジーという.

**定理 8** (Hilbert の定理 90)**.** $H^1(F, \overline{F}^\times) = 0$

Proof. いろいろ認めてしまえば証明は簡単であるので, ここで書くこととしよう. $\mathfrak{F}_F$ を $F$ の有限次ガロア拡大全体とすると,

$$H^1(F, \overline{F}^\times) \simeq \varinjlim_{F' \in \mathfrak{F}_F} H^1(\mathrm{Gal}(F'/F), F'^\times) = 0$$

である. □

**定理 9** (Kummer 理論)**.** $\mu_n \subseteq \overline{F}$ を 1 の $n$ 乗根のなす群とし, $\mu_n \subseteq F$ とする. $F^{(n)}$ を, $F$ の全ての $n$ 次巡回拡大の合成体とする. このとき, pairing

$$\mathrm{Gal}(F^{(n)}/F) \times F^\times/(F^\times)^n \to \mu_n,\ (\sigma, a(F^\times)^n) \mapsto \frac{\sqrt[n]{a}}{\sigma(\sqrt[n]{a})}$$

は非退化である.

$\mathrm{Gal}(F^{(n)}/F)$ は compact, $F^\times/(F^\times)^n$ は discrete であることに注意しよう. これもいろいろ認めてしまえば証明は簡単なので, ここで書くことにしよう.

Proof. 短完全系列

$$0 \to \mu_n \to \overline{F}^\times \overset{a\mapsto a^n}{\to} \overline{F}^\times \to 0$$

に対して, コホモロジー群の長完全系列を取ると, 0 次, 1 次の項として完全系列

$$\begin{array}{ccccc} 0 & \to & H^0(F,\mu_n) & \to & H^0(F,\overline{F}^\times) \quad \to \quad H^0(F,\overline{F}^\times) \\ & \overset{\delta}{\to} & H^1(F,\mu_n) & \to & H^1(F,\overline{F}^\times) \end{array}$$

を得る. これらのコホモロジー群を調べる. まず, 位相群 $A, B$ に対して, $\mathrm{Hom}_c(A,B)$ を $A$ から $B$ への連続準同型全体とする (compact–open 位相が入る). 仮定より $\mu_n \subseteq F$ であるので,

$$H^0(F,\mu_n) = \mu_n^{G_F} = \mu_n,$$

であり,

$$H^1(F,\mu_n) = \mathrm{Hom}_c(G_F,\mu_n) = \mathrm{Hom}_c(G_F/G_F^n[G_F,G_F],\mu_n) = \mathrm{Hom}_c(\mathrm{Gal}(F^{(n)}/F),\mu_n)$$

である. 次に, ガロア理論と Hilbert の定理 90 より,

$$H^0(F,\overline{F}^\times) = F^\times,\ H^1(F,\overline{F}^\times) = 0,$$

である. 以上より, 完全系列

$$0 \to \mu_n \to F^\times \overset{a\mapsto a^n}{\to} F^\times \overset{\delta}{\to} \mathrm{Hom}_c(\mathrm{Gal}(F^{(n)}/F),\mu_n) \to 0$$

から同型

$$F^\times/(F^\times)^n \overset{\delta}{\simeq} \mathrm{Hom}_c(\mathrm{Gal}(F^{(n)}/F),\mu_n)$$

が成り立つ. この同型は, $\mathrm{Gal}(F^{(n)}/F)$ と $F^\times/(F^\times)^n$ が互いに双対の関係にあることを示している. また, 連結準同型 $\delta$ は, $\alpha \in F^\times$ に対して $\alpha$ の $n$ 乗根 $\sqrt[n]{\alpha}$ をとり,

$$\delta(\alpha(F^\times)^n) = f_\alpha,\ f_\alpha(\sigma) = \frac{\sqrt[n]{\alpha}}{\sigma(\sqrt[n]{\alpha})}$$

で与えられる. これは $\sqrt[n]{\alpha}$ の取り方に依らない. □

# References

[1] 桂 利行, 代数学 III 体とガロア理論, 東京大学出版会 (2017).

[2] 永尾 汎, 代数学, 朝倉書店 (1983).

[3] Edited by J. W. S. Cassels and A. Frölich, Algebraic number theory, Second Edition, London Mathematical Society (2010).

[4] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields. Second edition. Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2008. xvi+825 pp.

# ガロア群の計算

深作亮也
九州大学 数理学研究院

**概要**

計算代数システム Magma には多項式のガロア群を計算するためのパッケージ `GaloisGroup` が組み込まれている．本稿では, Magma をインストールした計算機において, `GaloisGroup` を利用し, どのようにガロア群を計算できるのかを紹介する．

## 1 計算代数システム Magma

計算代数システムは計算機上で数学構造を計算するためのソフトウェアであり, 計算機代数システムや数式処理システムとも呼ばれる．また, 多くの計算代数システムには “グレブナー基底計算” や “多変数多項式イデアルの準素分解” や “限量子消去” などといった記号的に数学対象を扱うための計算手法が組み込まれている．Magma は計算代数システムの一つであり, Windows OS や Mac OS や Linux OS で動作する．

Magma はシドニー大学で開発されており, ライセンスを US $1100 で購入できる (購入時にはインストールする計算機の OS と MAC アドレスをシドニー大学に申請する)．シドニー大学はライセンス料を Magma の研究開発費に充てており, シドニー大学内外から発表された最新の研究成果を Magma に組み込んできた．

計算代数システムとして Mathematica や Maple も挙げることができる．Mathematica では, 一階述語論理式の簡単化手法 “限量記号消去” を `Reduce`, `Resolve` パッケージで利用できる．また, Maple では富士通研究所が開発する `SyNRAC` パッケージや, 著者が開発する `CGSQE` パッケージ等で “限量記号消去” を利用できる．Magma にこうしたパッケージは存在しない．しかし, Magma には様々な代数構造を計算するためのパッケージが組み込まれている．こうした点が Magma の大きな特徴であり, 利点である．例えば, Magma には入力された多項式のガロア群を計算するパッケージ `GaloisGroup` が組み込まれており, 高次多項式のガロア群までも計算できる．そして, Mathematica や Maple は組込関数としてガロア群計算パッケージを持っていない．

一方, Magma には Mathematica, Maple や一般プログラミング言語 Java, C に比べて敷居が高いという側面もある．例えば, Mathematica や Maple は変数に関して型を宣言せずにプログラミングできる．Magma では, [Magma] の通り, 型を定義していない変数に関する処理でエラーを発生させる．型宣言はプログラミングの初歩的なバグを減らすため, プログラミングにとっての利点の一つではあるが, プログラミング初心者にはハードルとなる．また, Magma は代数構造の計算を対象としているので, 型宣言では有限体, 一変数多項式環, 多変数多項式環のような代数構造も扱う．従って, 一般プログラミング言語 Java, C より必要とされる知識も多い．本稿では Magma の基本文法や型宣言等を紹介した後にガロア群の計算手順を紹介する．

# 2 MAGMA における基本的操作

MAGMA をデフォルトの場所にインストールした Mac OS や Linux OS のターミナル上で “magma” を実行すると, 以下のように MAGMA が立ち上がる (デフォルト以外にインストールした場合はバッシュファイル “.bashrc” 等にパスを追加しなければならない).

```
fukasaku:~$ magma
Magma V2.24-5     Tue Jun 25 2019 20:12:41 on fukasaku [Seed = 3086543668]
Type ? for help.  Type <Ctrl>-D to quit.
>
```

本節では MAGMA の基本文法や型宣言などを紹介する.

## 2.1 基本文法

基本的な演算については, 下記の MAGMA の実行画面のように, 他の計算代数システムや一般プログラミング言語と基本的には同様であり, コマンド末尾にはセミコロン “;” をつける. また, “//” で行のコメントアウト, “/* */” で範囲のコメントアウトができる.

```
> 1+1;      // 足し算
2
> 1-2;      /* 引き算 */
-1
> 2*3;      // 掛け算
6
> 2^3;      // 2 の 3 乗
8
> 5 div 3; // 5 の 3 による商
1
> 5 mod 3; // 5 の 3 による剰余
2
> $1;       // 1 つ前の出力
2
```

上記の通り, $1 や $2 で 1 つ前の出力や 2 つ前の出力を参照することもできる. また, 変数代入は下記のようにコロンイコール “:=” を利用して行う.

```
> a1 := 2*3; a2 := 2^3; // a1 に 2*3 の結果を, a2 に 2^3 の結果を代入
> a1 + a2;
14
```

また, リスト構造等も利用できる.

```
> a := [2*3, 2^3];          // a にリスト [2*3, 2^3] を代入
> a[1] + a[2];              // リスト a の第 1 要素と第 2 要素の足し算
14
> a := [1..30];             // a をリスト [1, 2, ..., 30] に置き換える
> #a;                       // a の要素の個数
30
```

代入済みの変数に新たな代入を行えば変数は変化するが, if 文や for 文 も実行できる.

```
> for i in [11..20] do // i = 11, 12, ..., 20 に対して
for> if i eq 15 then   // i = 15 ならば,
for|if> print i;       // i の値を出力する
for|if> end if;
for> end for;
15
```

本小節を MAGMA 言語で記述されたファイルの読み込みパッケージ load で締めくくる. 例えば, テキストファイル “for.txt” に以下を記述する.

```
/* for.txt: 15 から 20 までの素数を表示する */
for i in [15..20] do // i = 15, 16, ..., 20 に対して
  if IsPrime(i) then // i が素数ならば
    print i;         // i の値を出力する
  end if;
end for;
```

ファイル “for.txt” を MAGMA で読み込むと, 以下のように, 上から順に実行する.

```
> load "ファイルに関するパス/for.txt" // ‘‘for.txt’’ の読み込み
Loading "./for.txt"
17
19
```

load の他にも iload でファイルを読み込むこともできる. iload はインタラクティブにファイルを読み込むことができ, 講演等でデモンストレーションを行う際に扱いやすい. また, 上記 “for.txt” のような入力ファイルを用意すれば, 以下のように端末上から実験等を行うこともできる. また, MATHEMATICA や MAPLE 等と同様に, 自動で実験を行うようなスクリプトを書くこともできる. 従って, いくつかの実験を行いたい場合でも, ユーザーはその実験に関する入力ファイルたちを用意し, スクリプトファイルを実行すれば, 自動で計算を行うこともできる.

```
fukasaku:~$ magma < ファイルに関するパス/for.txt > for.log
fukasaku:~$
```

上記では “for.txt” を MAGMA に読み込ませ, その結果を “for.log” に書き込ませる作業を端末上で行っており, 以下が記述された “for.log” が生成される.

```
Magma V2.24-5     Wed Jul 24 2019 16:39:01 on RyoyanoAir [Seed = 2432026327]
Type ? for help.  Type <Ctrl>-D to quit.
17
19

Total time: 0.440 seconds, Total memory usage: 32.09MB
```

## 2.2 変数の型

MAGMA における変数操作には型宣言が必要である. 例えば, 一変数多項式の展開において型宣言を与えないと, 以下のようなエラーが出てしまい, 結果を得ることができない.

```
> (x+3)*(x+21);

>> (x+3)*(x+21);
    ^
User error: Identifier 'x' has not been declared or assigned
```

x に関する宣言がないため, エラーが出ている. そこで一変数整数係数多項式環 $\mathbb{Q}[x]$ を PR に代入することで x の型宣言を行う. この宣言を行えば, 先ほどの展開が可能となる.

```
> PR<x> := PolynomialAlgebra(Rationals()); // PR := \mathbb{Q}[x]
> (x+3)*(x+21);
x^2 + 24*x + 63
```

また, 多項式の判別式は以下のように計算できる.

```
> f := x^2 + 24*x + 63; d := Discriminant(f); d;
324
```

判別式が平方数かどうかを因数分解パッケージ Factorization で確かめると, 以下エラーが出る.

```
> Factorization(d);

>> Factorization(d);
                ^
Runtime error in 'Factorization': Bad argument types
Argument types given: FldRatElt
```

そこで, d の型 (つまり, 何の要素とみなされているか) をパッケージ Parent によって確認する.

```
> Parent(d); // d を含む集合
Rational Field
```

d が有理数とみなされていることがわかる. これは d が有理数係数多項式の判別式であるため, 起こったことである. そこで d を整数環の元であると明示的に記述し, 因数分解を行うと, 因数分解の結果が $2^2 \cdot 3^4$ であり, 判別式 d が平方数であることがわかる.

```
> Factorization(IntegerRing()!d);
[ <2, 2>, <3, 4> ]
```

このように Magma では計算対象の属する集合を意識する必要がある. 一方で, 次節の通り, Magma はガロア群を計算するための力強く, 有効で, 強力な道具の一つである.

# 3 Magma におけるガロア群の計算

Magma を使えば, 自動的にガロア群も計算できる. 本節では [Jensen-Ledet-Yui, Section 2] の内容も参照しながら, Magma によるガロア群の計算手順を紹介する.

## 3.1 3 次多項式のガロア群の計算

3 次既約多項式のガロア群は対称群 $S_3$ (位数 $6 = 3!$) もしくは巡回群 $C_3$ (位数 3) であるが ([Jensen-Ledet-Yui, §2.1]), 既約多項式 $f_1(x) = x^3 + 23x^2 + 21x + 15 \in \mathbb{Q}[x]$ のガロア群がどちらなのかを Magma の関数 GaloisGroup で計算してみる.

```
> PR<x> := PolynomialAlgebra(Rationals()); // PR := \mathbb{Q}[x]
> f1 := x^3+23*x^2+21*x+15;     // f_1(x) := x^3 + 23 x^2 + 21 x +15
> Gf1 := GaloisGroup(f1); Gf1;
Symmetric group Gf1 acting on a set of cardinality 3
Order = 6 = 2 * 3
```

上記計算結果から $f_1$ のガロア群は対称群であることがわかる. ちなみに, ガロア群 Gf1 の位数には以下のようにバックスラッシュでアクセスできる.

```
> Gf1‘Order;
6
```

以下定理 ([Jensen-Ledet-Yui, Theorem 2.2.1]) から, ガロア群計算の結果を検算する.

**定理 1** 既約な $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$ を考える. このとき, ガロア群 $\mathrm{Gal}(f/\mathbb{Q})$ は

$$\mathrm{Gal}(f/\mathbb{Q}) \simeq \begin{cases} S_3 & (d(f) \notin (\mathbb{Q}^\star)^2) \\ C_3 & (d(f) \in (\mathbb{Q}^\star)^2) \end{cases},$$

ただし, $d(f)$ は $f$ の判別式であり, $(\mathbb{Q}^\star)^2 = \{a^2 : a \in \mathbb{Q} \setminus \{0\}\}$ である.

定理 1 の通り, 判別式が平方数かどうかで検算できるので, 判別式の因数分解を計算して確認する.

```
> Factorization(Integers()!Discriminant(f1));
[ <2, 5>, <3, 1>, <5, 1>, <853, 1> ]
```

因数分解の結果から, 判別式は非平方数であることがわかる. 従って, 定理 1 から `GaloisGroup(f1)` の計算結果は正しいことが従う. 次に, 既約多項式 $f_2(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ のガロア群を Magma で計算してみる.

```
> f2 := x^3-3*x+1;
> Gf2 := GaloisGroup(f2); Gf2;
Permutation group Gf2 acting on a set of cardinality 3
Order = 3
    (1, 2, 3)
```

`Gf2` の位数は 3 であり, `Gf2` は巡回群であることがわかる. この結果も検算する.

```
> Factorization(Integers()!Discriminant(f2));
[ <3, 4> ]
```

判別式は平方数なので, 定理 1 から `GaloisGroup(f2)` の計算結果は正しいことが従う.

## 3.2 4 次多項式のガロア群の計算

4 次既約多項式のガロア群は対称群 $S_4$ (位数 $24 = 4!$), 交代群 $A_4$ (位数 $12 = 4!/2$), クラインの 4 元群 $V_4$ (位数 4), 二面体群 $D_4$ (位数 $8 = 2 \cdot 4$), もしくは巡回群 $C_4$ (位数 4) である ([Jensen-Ledet-Yui, §2.2]). 本小節では, まず, 既約多項式 $f_3(x) = x^4 + 23x^3 + 21x^2 + 12x + 3 \in \mathbb{Q}[x]$ のガロア群を Magma で計算してみる (後で行う検算で係数を利用するため, 係数から多項式を定義する). そして, 前小節と同様に検算を行う.

```
> a3 := 23; a2 := 21; a1 := 12; a0 := 2;
> f3 := x^4 + a3*x^3 + a2*x^2 +a1*x + a0;
> Gf3 := GaloisGroup(f3); Gf3;
Symmetric group Gf3 acting on a set of cardinality 4
Order = 24 = 2^3 * 3
```

ガロア群は位数 24 の対称群であることがわかった. 以下定理 ([Jensen-Ledet-Yui, Theorem 2.2.2 - Theorem 2.2.3]) を利用して, この結果に関して検算する.

**定理 2** $\mathbb{Q}$ 上において既約な多項式 $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$ を考え,

$$g = x^3 - a_2x^2 + (a_1a_3 - 4a_0)x - (a_0a_3^2 - 4a_0a_2 + a_1^2)$$

とする. $L$ を $g$ の $K$ 上分離体, $m$ を次数 $[L : K]$ とする. このとき, $m = 1, 2, 3$ もしくは 6 で,

$$\mathrm{Gal}(f/\mathbb{Q}) \simeq \begin{cases} S_4 & (m = 6) \\ A_4 & (m = 3) \\ V_4 & (m = 1) \\ D_4 \text{ or } C_4 & (m = 2) \end{cases}$$

が満たされる. $m = 2$ を仮定する. このとき, $g$ は $\mathbb{Q}$ 上可約である. ここで, $g$ の因数分解を

$$g = (x - r)(x^2 + sx + t)$$

で与える, ただし $x^2 + sx + t$ は $\mathbb{Q}$ 上において既約である. $L = K(\sqrt{s^2 - 4t})$ とする. このとき

$$\mathrm{Gal}(f/\mathbb{Q}) \simeq C_4 \quad \Leftrightarrow \quad \{x \in L : x^2 - rx + a_0 = 0\}, \{x \in L : x^2 - a_1x + (a_2 - r) = 0\} \neq \emptyset.$$

まず, 定理 2 の $g$ に対応する g3 を a3, a2, a1, a0 から構成する. そして, 3 次多項式 g3 のガロア群を GaloisGroup で計算することで, 位数を計算する.

```
> g3 := x^3 - a2*x + (a1*a3 - 4*a0)*x - (a0*a3^2 - 4*a0*a2 + a1^2);
> Gg3 := GaloisGroup(g3); Gg3;
Symmetric group Gg3 acting on a set of cardinality 3
Order = 6 = 2 * 3
```

g3 のガロア群の位数は 6 なので, 定理 2 の次数 $m$ は 6 である ([桂, 系 1.7.12]). 従って, 定理 2 前半から本小節の GaloisGroup(f3) の結果も正しい. 次に, 既約多項式 $f_4(x) = x^4 + 2x^3 + 2x^2 + x + 3 \in \mathbb{Q}[x]$ のガロア群を MAGMA で計算してみる.

```
> a3 := 2; a2 := 2; a1 := 1; a0 := 3;
> f4 := x^4 + a3*x^3 + a2*x^2 +a1*x + a0;
> Gf4 := GaloisGroup(f4); Gf4;
Permutation group Gf4 acting on a set of cardinality 4
Order = 8 = 2^3
    (1, 2)(3, 4)
    (1, 4)
```

従って, ガロア群は位数 8 の二面体群である. 先ほどと同様に定理 2 で検算する.

```
> g4 := x^3 - a2*x + (a1*a3 - 4*a0)*x - (a0*a3^2 - 4*a0*a2 + a1^2);
> Gg4 := GaloisGroup(g4); Gg4;
Permutation group Gg4 acting on a set of cardinality 3
Order = 2
    (1, 2)
```

g3 のガロア群の位数は 2 なので定理 2 の次数 $m$ は 2 である ([桂, 系 1.7.12]). 従って, 定理 2 から $f_4$ のガロア群は $D_4$ もしくは $C_4$ であることがわかる. 定理 2 後半から GaloisGroup(f4) の結果を検算する. まずは g4 を有理数係数多項式として因数分解する.

```
> Fg4 := Factorization(g4); Fg4; // 因数分解
[
    <x - 1, 1>,
    <x^2 + x - 11, 1>
]
```

次に $x-r$ に関する多項式 g41 と $x^2+sx+t$ に関する多項式 g42 への代入を for と if で行う.

```
> // x - r, x^2 + sx + t の抽出
> for i in [1..#Fg4] do
for> if Degree(Fg4[i][1]) eq 1 then
for|if> g41 := Fg4[i][1];
for|if> else
for|if> g42 := Fg4[i][1];
for|if> end if;
for> end for;
```

g41 と g42 の係数に関するリストを以下のように与える.

```
> // 係数リストの構築
> Cg41 := []; Cg42 := [];
> for i in [0..1] do
for> Cg41[i+1] := Coefficient(g41, i);
for> end for;
> for i in [0..2] do
for> Cg42[i+1] := Coefficient(g42, i);
for> end for;
```

g41 と g42 の係数に関するリスト Cg41 と Cg42 を利用して r, s, t に係数を代入する.

```
> // r, s, t への係数代入
> r := -Cg41[1+0];
> s := Cg42[1+1];
> t := Cg42[1+0];
```

ext を使って, L に拡張体 $\mathbb{Q}(\sqrt{s^2-t})$ を代入する.

```
> // L への拡張体 \mathbb{Q}(\sqrt{s^2-4t}) の代入
> L := ext<Rationals() | x^2-(s^2-4*t)>;
```

HasRoot を使って, L における根の存在判定を行う.

```
> // L における根の存在判定
> HasRoot(x^2-r*x+a0, L);
false
> HasRoot(x^2+a1*x+(a2-r), L);
false
```

従って, 定理 2 後半から GaloisGroup(f4) の結果は正しいことが保証される.

## 3.3 5 次多項式のガロア群の計算

次数 5 の対称群 $S_5$ の可移部分群は対称群 $S_5$ (位数 $120 = 5!$), 交代群 $A_5$ (位数 $60 = 5!/2$), Frobenius 群 $F_{20}$ (位数 20), 二面体群 $D_5$ (位数 $10 = 2 \cdot 5$), もしくは巡回群 $C_5$ (位数 5) である ([Jensen-Ledet-Yui, §2.3]). 本小節では, 既約多項式 $f_5(x) = x^5 + 12x + 3 \in \mathbb{Q}[x]$ のガロア群を計算し, その結果を検算する.

```
> a := 120; b := 64;
> f5 := x^5 + a*x + b;
> Gf5 := GaloisGroup(f5); Gf5;
Permutation group Gf5 acting on a set of cardinality 5
Order = 20 = 2^2 * 5
    (1, 4, 2, 5)
    (1, 2)(4, 5)
    (1, 2, 5, 3, 4)
```

ガロア群は位数 20 の Frobenius 群 $F_{20}$ であることがわかる. 以下定理 ([Jensen-Ledet-Yui, Theorem 2.3.4]) を利用して, この結果に関して検算する.

**定理 3** $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$ を既約とする. $a = 0$ のとき $\mathrm{Gal}(f/\mathbb{Q}) \simeq F_{20}$. そうでないとき $\mathrm{Gal}(f/\mathbb{Q}) \simeq D_5$ *(*もしくは $F_{20}$*)* であることと以下 *(i), (ii)* が満たされることは等価である*:*

*(i)* $d(f) \in (\mathbb{Q}^\star)^2$ *(*もしくは $\notin (\mathbb{Q}^\star)^2$*)*

*(ii)* 係数 $a$, $b$ が $\lambda \neq 1$, $\mu \neq 0$ なる $\lambda, \mu \in \mathbb{Q}$ に対して以下を満たす:

$$a = \frac{5^5 \lambda \mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)}, \quad b = a\mu.$$

判別式が平方数かどうかを, 判別式の因数分解を計算して確認する.

```
> Factorization(Integers()!Discriminant(f5));
[ <2, 23>, <5, 6>, <7, 2> ]
```

因数分解の結果から, 判別式は非平方数であることがわかる. (ii) を満たすような $\lambda, \mu \in \mathbb{Q}$ が存在するかどうかを判定するために変数 `l`, `m` に関する 2 変数多項式環 `Rf5` を与える.

```
> Rf5<l,m> := PolynomialAlgebra(Rationals(),2);
```

さらに (ii) に関連する多項式を構成する.

```
> p1 := a*((l-1)^4*(l^2-6*l+25)) - 5^5*l*m^4;
> p2 := a*m - b;
```

`p2` の変数は `m` のみなので MAGMA の一変数多項式の係数体 (ここでは $\mathbb{Q}$) に属する根を計算するための関数 `Roots` を使うことができる. しかし, その前に `p2` を一変数多項式に型変換する必要がある. `IsUnivariate` は入力が一変数多項式かどうかを判定する. 一変数多項式の場合, 真偽値 `true` と 一変数多項式表現を与える (そうでない場合, 真偽値 `false` が返ってくる). この一変数多項式表現を利用することで根計算関数 `Roots` を利用する.

```
> boolean, p2 := IsUnivariate(p2); p2;
120*x - 64
> R2 := Roots(p2); R2;
[ <8/15, 1> ]
```

根に関するリスト `R2` も利用して, `p1` を一変数多項式に変換し, その有理数根を計算する.

```
> p1 := Evaluate(p1,[l,R2[1][1]]); boolean, p1 := IsUnivariate(p1);
> Roots(p1);
[ <5/3, 1> ]
```

`p1` の因数分解を行えば上記の正当性もわかる.

```
> Factorization(p1);
[
  <$.1 - 5/3, 1>,
  <$.1^5 - 25/3*$.1^4 + 370/9*$.1^3 - 1930/27*$.1^2 + 4525/81*$.1 - 15, 1>
]
```

上記検算と定理 3 から既約多項式 $f_5(x) = x^5 + 12x + 3 \in \mathbb{Q}[x]$ のガロア群は $F_{20}$ である.

## 4 まとめ

本稿では計算機 (特に計算代数システム Magma) におけるガロア群の計算方法を紹介した. 最後に, 代数構造に関するデータベース LMFDB (詳細: [LMFDB] 参照) を紹介したい. このデータベースでは様々な多項式のガロア群もデータベース化し, 紹介している. 特に, 各ガロア群の性質等もデータベース化している. そして, こうしたデータは Magma や Gap によって計算されている.

## 参考文献

[桂] 桂利行: 大学数学の入門 3, 代数学 III, 体とガロア理論. 東京大学出会, 2005.

[Jensen-Ledet-Yui] Jensen, C. U., Ledet, A. and Yui, N.: Generic polynomials, Constructive aspects of the inverse Galois problem. Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, Cambridge. 2002

[LMFDB] LMFDB - The L-functions and Modular Forms Database. `http://www.lmfdb.org/`

[Magma] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system, I, The user language. Journal of Symbolic Computation, 24, pp. 235 - 265. 1997.

# 不変体の有理性問題 (1)

金井 和貴　(新潟大学)

**概要**

本稿は第 27 回整数論サマースクール「構成的ガロアの逆問題と不変体の有理性問題」における講演「不変体の有理性問題 (1)」のレジュメである．本講演ではまず，ガロアの逆問題と不変体の有理性問題の関係を述べる．その後生成的多項式の定義を与え，有理性を弱めた安定有理性とレトラクト有理性の導入し，最後に実例として $\mathbb{Q}$ 上の巡回群に対する不変体の有理性問題を取り扱う．その過程において後の講演において必要となる事柄の準備を行う．

## 1　ガロアの逆問題とネーター問題

ガロア理論において，与えられた代数方程式から生ずる体の拡大のガロア群を求めることは基本的な問題である．これを順方向の問題と捉え，ガロアの逆問題は次のような形で提起される．

問題 **1.1** (ガロアの逆問題)**.** 与えられた有限群 $G$ に対して，体 $k$ 上のガロア拡大 $L/k$ であって，そのガロア群が $G$ と同型となるものは存在するか？

$k = \mathbb{Q}$ とすれば，「絶対ガロア群 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ の商群としてどのような有限群があらわれるか？」を問うており，これは現代の代数的整数論においても最も重要な問題の一つであると考えられる．

ネーターは 1913 年に報文 [Noe1913] において，次の問題を提起した (論文としては [Noe1917])．

問題 **1.2** (ネーター問題)**.** 有限群 $G$ が体 $k$ 上の有理関数体 $k(x_g \mid g \in G)$ に左正則作用するとき，すなわち $h(x_g) = x_{hg}$ $(\forall h, g \in G)$ とするとき，$k(x_g \mid g \in G)$ の $G$ による不変体 $k(G) := k(x_g \mid g \in G)^G$ は $k$ 上有理的 (純超越的) か？

ネーター問題が肯定解が得られれば，$k$ 同型写像 $\phi : k(\mathbf{t}) \to k(G)$ が存在し，$G$ 拡大 $k(x_g \mid g \in G)/k(G)$ の定義多項式の $\phi$ による引き戻し $f(\mathbf{t}; X) \in k(\mathbf{t})[X]$ が $k(\mathbf{t})$ 上の $G$ 拡大を与える．ここで，$\mathbf{t} := (t_1, \ldots, t_n)$ は $k$ 上 $|G|$ 個の独立変数の組である．

さらに，$k$ がヒルベルト体であれば，ヒルベルトの既約性定理から，$\mathbf{t}$ の $k$ 上の特殊化 $\mathbf{a} \in k^n$ で $\mathrm{Gal}(f(\mathbf{a}; X)/k) \simeq G$ となるものが無限個存在する (詳しくは 2 節で述べる)．

すなわち，体 $k$ と有限群 $G$ に対して

$$\text{ネーター問題が肯定的} \Longrightarrow \text{ガロアの逆問題が肯定的}$$

が成立するのである．

## 2　ヒルベルトの既約性定理と生成的多項式

この節において断りがない限り，$k$ を体，$G$ を有限群とし，$k$ 上 $n$ 個の独立変数の組を $\mathbf{t} = (t_1, \ldots, t_n)$ とし, $k(\mathbf{t})$ を $k$ 上の $n$ 変数有理関数体とする．また証明に関しては [JLY02] の 3 章を見よ．

まず，ヒルベルト体の定義からはじめよう．

定義 **2.1** (ヒルベルト体)**.** 以下の条件を満たす体 $k$ をヒルベルト体と呼ぶ：

- 有限個の $k(\mathbf{t})$ 既約多項式 $f_1(\mathbf{t}; X), \ldots, f_r(\mathbf{t}; X) \in k(\mathbf{t})[X]$ と，有限個の 0 でない多項式 $g_1(\mathbf{t}), \ldots, g_s(\mathbf{t}) \in k[\mathbf{t}]$ を任意に取る．このとき，特殊化 $\mathbf{a} \in k^n$ で次を満たすものが存在する：
  (i) $f_1(\mathbf{a}; X), \ldots, f_r(\mathbf{a}; X) \in k[X]$ が全て定義され $k$ 上既約
  (ii) $g_1(\mathbf{a}), \ldots, g_s(\mathbf{a}) \in k$ が全て 0 にならない

ヒルベルト体において次の定理が成立する．

定理 **2.2.** $k$ をヒルベルト体とし, $f(\mathbf{t}; x) \in k(\mathbf{t})[X]$ を既約であるとする．このとき，$f(\mathbf{t}; X)$ の特殊化 $\mathbf{a} \in k^n$ で $f(\mathbf{a}; X)$ が定義され既約となり，

$$\mathrm{Gal}(f(\mathbf{t}; X)/k(\mathbf{t})) \simeq \mathrm{Gal}(f(\mathbf{a}; X)/k)$$

を満たすものが無限に存在する．

定義から有限体や代数閉体はヒルベルト体ではないことがわかる．また，ヘンゼル体もヒルベルト体ではないことが知られている．すなわち，$\mathfrak{p}$ 進体や形式的べき級数体はヒルベルト体ではない．

次のヒルベルトによる結果が基本的かつ重要である．

定理 **2.3** (Hilbert [Hil1892])**.** 有理数体 $\mathbb{Q}$ はヒルベルト体である．

また，次が成立する．

命題 **2.4.** ヒルベルト体の有限次分離拡大はヒルベルト体である．

系 **2.5.** 代数体はヒルベルト体である．

次に生成的 $G/k$ 多項式を定義する．

定義 **2.6** (生成的 $G/k$ 多項式)**.** $k$ を無限体，$G$ を有限群とする．このとき $f(\mathbf{t}; X) \in k(\mathbf{t})[X]$ が以下の条件を満たすとき，$f(\mathbf{t}; X)$ を生成的 $G/k$ 多項式と呼ぶ.

(i) $f(\mathbf{t}; X)$ の $k(\mathbf{t})$ 上の最小分解体は $k(\mathbf{t})$ 上の $G$ 拡大である．
(ii) $K \supset k$ とする．$L$ を任意の $K$ 上の $G$ 拡大とする．このとき，$\mathbf{t}$ の $k$ 上の特殊化 $\mathbf{a} \in K^n$

で，$f(\mathbf{a};X)$ の $K$ 上の最小分解体が $L$ となるものが存在する．

注意 **2.7.** 生成的多項式は既約でなくてもよい。

生成的多項式が定義された [DeM83] において，以下の性質は定義に含まれていたが，2001 年に Kemper によって示され不要となった．

定理 **2.8** (Kemper [Kem01])**.** $k$ を無限体，$G$ を有限群とする．生成的 $G/k$ 多項式 $f(\mathbf{t};X) \in k(\mathbf{t})[X]$ は次の性質を持つ：

- $H$ を $G$ の部分群とする．$K \supset k$ とし，$M$ を任意の $K$ 上の $H$ 拡大とする．このとき，$M$ が最小分解体となるような $\mathbf{t}$ の $k$ 上の特殊化 $\mathbf{a}$ が存在する．

定理 **2.9** (Kuyk [Kuy64])**.** ネーター問題が肯定的であるとする．このとき, $k$ 同型写像 $\phi : k(\mathbf{t}) \to k(G)$ が存在し, $G$ 拡大 $k(x_g \mid g \in G)/k(G)$ の定義多項式の $\phi$ による引き戻し $f(\mathbf{t};X) \in k(\mathbf{t})[X]$ は生成的 $G/k$ 多項式である．

すなわち，ネーター問題の肯定解から得られる $G/k$ 多項式は無限個の $G$ 拡大の例を与えるだけでなく，ガロアの逆問題に対しての最上の解答を与えることがわかる．

例 **2.10** (Shanks の多項式)**.** 次の 3 次多項式は Shanks 多項式と呼ばれており，生成的 $C_3/\mathbb{Q}$ 多項式である (これは本サマースクールにおいて角皆氏，岡崎氏の講演においても扱われる)．

$$f(t;X) = X^3 - tX^2 + (t-3)X + 1$$

## 3　種々の有理性問題

有理性問題はネーター問題を一般化した問題であり，以下のように定義される．

問題 **3.1** (不変体の有理性問題)**.** $G$ を有限群，$k$ を体とし，$G$ は $k$ に自明に作用するとする．$F$ を $k$ の有限生成拡大とし，$G$ は $F$ に自己同型として作用しているとする (すなわち，$G \leq \mathrm{Aut}_k(F)$. このような作用付きの体を以降 $G$ 体と呼ぶ)．このとき，$G$ による $F$ の不変体 $F^G$ は $k$ 上有理的か？

すなわち、同じ有限群 $G$ に対しても $F$ への作用の仕方によって様々な有理性問題が考えられる．1 変数有理関数体の場合は Lüroth の定理により常に肯定的である．また，ネーター問題は $F = k(x_g \mid g \in G)$ とし，$G$ の $F$ への作用を左正則作用によって定めたときに対応し，定理 2.9 は次のように一般化される．

定理 **3.2** (Kemper-Mattig [KM00])**.** 有理関数体 $F = k(x_1, \ldots, x_n)$ に対する有限群 $G$ の作用が基礎体 $k$ には自明に作用し，変数に対しては線型に作用するとする．この作用に対する有理性問題が肯定的であるとする．このとき，$k$ 同型写像 $\phi : k(\mathbf{t}) \to F^G$ が存在し, $G$ 拡大 $F/F^G$ の定義多

項式の $\phi$ による引き戻し $f(\mathbf{t};X)\in k(\mathbf{t})[X]$ は生成的 $G/k$ 多項式である.

例 **3.3** ($V_4$ の線型作用に関する有理性問題)**.** $G$ がクラインの四元群 $V_4\simeq C_2\times C_2$ であり, 体 $k$ は標数が 2 ではない体とする. このとき, $k(x_1,x_2)$ への $G=\langle\sigma,\tau\rangle$ の作用が

$$\sigma:\begin{cases} x_1\mapsto -x_1\\ x_2\mapsto x_2\end{cases},\quad \tau:\begin{cases} x_1\mapsto x_1\\ x_2\mapsto -x_2\end{cases}$$

で与えられているとする. この作用は

$$\sigma\mapsto\begin{pmatrix}-1&0\\0&1\end{pmatrix},\quad \tau\mapsto\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

によって, $GL(2,k)$ に表現される. このとき,

$$k(x_1,x_2)^{\langle\sigma,\tau\rangle}=k(x_1^2,x_2^2)$$

となる. 実際 ($\supset$) は明らかであり,

$$[k(x_1,x_2):k(x_1,x_2)^{\langle\sigma,\tau\rangle}]=4,\quad [k(x_1,x_2):k(x_1^2,x_2^2)]\le 4$$

より等号が成立する. $\mathbb{Q}(x_1^2,x_2^2)$ 上 $\mathbb{Q}(x_1,x_2)$ は

$$(X^2-x_1^2)(X^2-x_2^2)$$

の最小分解体であるから, $k$ 同型写像 $\phi:k(t_1,t_2)\to k(x_1,x_2)^{V_4}$ による引き戻しは

$$(X^2-t_1)(X^2-t_2)$$

となり, これは生成的 $V_4/k$ 多項式である.

例 **3.4** ($C_4$ と $D_4$ の線型作用に関する有理性問題)**.** $k$ を標数が 2 ではない体とする. $G$ を位数 8 の二面体群 $G=D_4=\langle\sigma,\tau\mid\sigma^4=\tau^2=1,\tau\sigma\tau=\sigma^{-1}\rangle$, $H\le G$ を位数 4 の巡回群 $H=C_4=\langle\sigma\rangle$ とする. このとき, $k(x_1,x_2)$ への作用を

$$\sigma:\begin{cases} x_1\mapsto -x_2\\ x_2\mapsto x_1\end{cases},\quad \tau:\begin{cases} x_1\mapsto x_2\\ x_2\mapsto x_1\end{cases}$$

で与えられているとする. この作用は

$$\sigma\mapsto\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad \tau\mapsto\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

によって, $GL(2,k)$ に表現される. $G\rhd V_4$ であり,

$$V_4\simeq\langle\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix}\rangle$$

であるから,

$$G/V_4\simeq\langle\overline{\begin{pmatrix}0&1\\1&0\end{pmatrix}}\rangle$$

となる．ここで

$$\begin{cases} a = x_1^2 x_2^2 \\ b = x_1^2 + x_2^2 \\ c = x_1 x_2 (x_1^2 - x_2^2) \end{cases}$$

と置くと，

$$\begin{aligned} k(x_1, x_2)^G &= (k(x_1, x_2)^{V_4})^{G/V_4} \\ &= k(x_1^2, x_2^2)^{\overline{\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle}} \\ &= k(x_1^2 x_2^2, x_1^2 + x_2^2) \\ &= k(a, b) \end{aligned}$$

となる．したがって，$k(x_1, x_2)^G$ は $k$ 上有理的である．ここで，$k(x_1, x_2)^H$ は $k(x_1, x_2)^G$ の二次拡大である．また，

$$\sigma(c) = (-x_2) x_1 (x_2^2 - x_1^2) = x_1 x_2 (x_1^2 - x_2^2) = c$$

であり，$c \in k(x_1, x_2)^H$ である．さらに，$\tau(c) = -c$ より $c \notin k(x_1, x_2)^G$ となる．したがって，

$$k(x_1, x_2)^G \subsetneq k(a, b, c) \subset k(x_1, x_2)^H$$

かつ

$$[k(x_1, x_2)^H : k(x_1, x_2)^G] = 2$$

であるから，

$$k(x_1, x_2)^H = k(a, b, c)$$

を得る．ここで，

$$c^2 = x_1^2 x_2^2 (x_1^2 - x_2^2)^2 = a(b^2 - 4a) = ab^2 - 4a^2$$

より

$$\left(\frac{c}{a}\right)^2 = a \left(\frac{b}{a}\right)^2 - 4$$

であるから，$C := c/a, B := b/a$ と置けば

$$a = \frac{C^2 + 4}{B^2}$$

となる．したがって

$$\begin{aligned} k(x_1, x_2)^H &= k(a, b, c) \\ &= k(B, C) \\ &= k\left(\frac{x_1^2 + x_2^2}{x_1^2 x_2^2}, \frac{x_1^2 - x_2^2}{x_1 x_2}\right) \end{aligned}$$

を得る．すなわち，$k(x_1, x_2)^H$ も $k$ 上有理的となる．

$x_1, x_2$ を根に持つ多項式

$$f(X) = (X^2 - x_1^2)(X^2 - x_2^2) = X^4 - (x_1^2 + x_2^2)X^2 + x_1^2 x_2^2 = X^4 - bX^2 + a$$

を考えると，$k(x_1, x_2)$ は $k(x_1, x_2)^G$ 上 $f(X)$ の最小分解体となる．$f(X)$ の $k$ 同型写像 $\phi : k(t_1, t_2) \to k(x_1, x_2)^G = k(a, b)$ による引き戻しは

$$f(X) = X^4 - t_2 X^2 + t_1$$

となり，これは生成的 $D_4/k$ 多項式となる．また，

$$a = \frac{C^2 + 4}{B^2}, \quad b = aB = \frac{C^2 + 4}{B}$$

であるから，$k(x_1, x_2)^H$ 上では

$$f(X) = X^4 - \frac{C^2 + 4}{B} X^2 + \frac{C^2 + 4}{B^2}$$

となり，$f(X)$ の最小分解体は同様に $k(x_1, x_2)$ となる．したがって，$k$ 同型写像 $\phi : k(t_1, t_2) \to k(x_1, x_2)^H = k(B, C)$ による引き戻しは

$$f(X) = X^4 - \frac{t_2^2 + 4}{t_1} X^2 + \frac{t_2^2 + 4}{t_1^2}$$

となり，これは生成的 $C_4/k$ 多項式となる．

例 **3.5** ($C_2$ の非線型作用に対する有理性問題)**.** 非線形な作用に対しての有理性問題の肯定解から得られる定義方程式には，生成的ではないものが存在する．

$C_2 = \langle \sigma \rangle$ の $\mathbb{Q}(x)$ に対しての作用を

$$\sigma(x) = \frac{1}{x}$$

により定義する．このとき，

$$\mathbb{Q}(x)^{\langle \sigma \rangle} = \mathbb{Q}\left(x + \frac{1}{x}\right)$$

となる．実際 $x + (1/x)$ は $\sigma$ 作用で不変であり，$x$ の $\mathbb{Q}\left(x + (1/x)\right)$ 上の最小多項式は

$$f(X) = X^2 - \left(x + \frac{1}{x}\right) X + 1$$

となる．したがって，$f$ の $k$ 同型写像 $\phi : \mathbb{Q}(t) \to \mathbb{Q}(x)^{\langle \sigma \rangle}$ による引き戻しは

$$f(t; X) = X^2 - tX + 1$$

となる．しかしながら，$f(t; X)$ は $\mathbb{Q}$ 上生成的ではない．なぜならば，$f(t; X)$ の判別式は $D = t^2 - 4$ であるから，$t$ に有理数 $p/q$ を代入すると，

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}\left(\sqrt{\frac{p^2}{q^2} - 4}\right) = \mathbb{Q}\left(\sqrt{p^2 - 4q^2}\right)$$

となる．したがって，根号の中が $\pmod 4$ で 3 なることはない．これは $f(t;X)$ が $C_2/\mathbb{Q}$ 生成的ではないことを意味する．

有理性問題をより超越次数の低い拡大に帰着する方法として，“No-name Lemma” と呼ばれる次の補題が重要である (証明は長谷川氏の講演において行う)．

補題 **3.6** (No-name Lemma)．$F$ を忠実な $G$ 体とし，$V$ を $F$ 上の線形空間とし，$G$ は $V$ に線型に作用しているとする．また，$W$ を $V$ の忠実な $F[G]$ 部分加群とする．このとき，$F(V)^G$ は $F(W)^G$ 上有理的である．

有限群 $G$ は常に適当な対称群の部分群であると見なせることに注意すれば次が成立する．

系 **3.7.** 有限群を $G \leq S_n$, $k$ を体とする．$n$ 変数有理関数体 $F = k(x_1, \ldots, x_n)$ に $G$ が変数の置換として $\sigma(x_i) = x_{\sigma(i)}$ $(\forall g \in G)$ のように作用しているとする．このとき，$F$ のこの作用に関する不変体の有理性問題が肯定的ならば，$k$ 上の $G$ に対するネーター問題，すなわち $k$ 上の $|G|$ 変数有理関数体の左正則作用に関する不変体の有理性問題は肯定的である．

証明．まず，$G$ は $\mathrm{GL}(n,\mathbb{Z})$ に置換として表現されるから，この表現空間を $W$ とする．$G$ の置換表現は既約であり，$G$ の任意の既約表現は左正則表現の直既約分解に現れる．したがって，左正則作用の表現空間を $V$ とすれば，$W$ は $V$ の忠実な $K[G]$ 部分加群, No-name Lemma により $K(V)^G$ は $K(W)^G$ 上有理的である．したがって，$k$ 上の $n$ 変数有理関数体の置換作用に関する不変体の有理性問題が肯定的ならば，$k$ 上の $G$ に対するネーター問題，すなわち $k$ 上の $|G|$ 変数有理関数体の左正則作用に関する不変体の有理性問題は肯定的となる． □

例 **3.8** ($S_n$ のネーター問題)．$G \simeq S_n$ と体 $k$ のネーター問題を考える．系 3.7 を用いれば，$n$ 変数有理関数体の置換作用に関する有理性問題に帰着され，$n$ 変数有理関数体 $k(x_1, \ldots, x_n)$ に対する作用は，$\sigma \in G$ に対して $\sigma(x_i) = x_{\sigma(i)}$ となる．このとき，

$$k(x_1, \ldots, x_n)^G = k(e_1, \ldots, e_n)$$

となる．ここで，$e_i$ は $i$ 次基本対称式とする．すなわち

$$\begin{aligned} e_1 &= x_1 + x_2 + \cdots + x_n, \\ e_2 &= x_1x_2 + x_2x_3 + \cdots + x_nx_1, \\ &\vdots \\ e_n &= x_1x_2\cdots x_n. \end{aligned}$$

従って，$k(x_1, \ldots, x_n)^{S_n}$ は $k$ 上有理的である．また，$k$ 同型写像 $\phi : k(t_0, \ldots, t_{n-1}) \to k(x_1, \ldots, x_n)^{S_n}$ による $k(x_1, \ldots, x_n)/k(x_1, \ldots, x_n)^G$ の定義多項式の引き戻しは生成的 $S_n/k$ 多項式

$$X^n + t_{n-1}X^{n-1} + \cdots + t_1X + t_0$$

となる．

# 4　安定有理性とレトラクト有理性

有理的であるかを調べることは一般に非常に難しい．したがってこれを弱くした概念が考えられてきた．本節ではそれらの定義を与え，その関係を述べる．以下断りがない限り $G$ を有限群とし，$G$ は基礎体 $k$ に自明に作用しているものとし，$k$ は無限体とする．

定義 **4.1** (安定有理的，レトラクト有理的，単有理的)．$F$ を $k$ 上有限生成な体とする．

- $F$ が $k$ 上安定有理的 $\overset{\text{def}}{\Leftrightarrow}$ $G$ 不変な $F$ 上代数的独立な元 $s_1, \ldots, s_r$ で $F(s_1, \ldots, s_r)$ が $k$ 上有理的となるものが存在する．
- $F$ が $k$ 上レトラクト有理的 $\overset{\text{def}}{\Leftrightarrow}$ $F$ の部分 $k$ 代数 $R$ で以下の条件を満たすものが存在する：
  (i) $F = Q(R)$. ここで $Q(R)$ は $R$ の商体を表す．
  (ii) $f \in k[x_1, \ldots, x_n]$ と $k$ 代数の準同型

$$\phi : R \to k[x_1, \ldots, x_n][1/f], \quad \psi : k[x_1, \ldots, x_n][1/f] \to R$$

  で $\psi \circ \phi = \mathrm{Id}_R$ を満たすものが存在する．このとき，$R$ は $k[x_1, \ldots, x_n][1/f]$ のレトラクトであると言う．
- $F$ が $k$ 上単有理的 $\overset{\text{def}}{\Leftrightarrow}$ $F$ は $k$ 上有理的な体 $E$ の部分体となる．

上記の有理性の間には，

$$\text{“有理的”} \Longrightarrow \text{“安定有理的”} \Longrightarrow \text{“レトラクト有理的”} \Longrightarrow \text{“単有理的”}$$

が成り立つ．

“有理的 $\Rightarrow$ 安定有理的” は明らか．“レトラクト有理的 $\Rightarrow$ 単有理的” は $R \hookrightarrow k[x_1, \ldots, x_n][1/f]$ より $F \hookrightarrow k(x_1, \ldots, x_n)$ となることから成り立つ．

従って以降は，“安定有理的 $\Rightarrow$ レトラクト有理的” を示すことに注力する．

注意 **4.2.** 各 “$\Rightarrow$” の逆向きは成立しない．

- $F = \mathbb{Q}(x, y, t), x^2 + 3y^2 = t^3 - 2$ とすると $F$ は $\mathbb{Q}$ 上非有理的であるが，$F(x_1, x_2, x_3)$ は有理的，すなわち $F$ は安定有理的 (Beauville, Colliot-Thélène, Sunsuc, Swinnerton-Dyer [BCTSSD85]).
- $\mathbb{Q}(C_{47})$ は $\mathbb{Q}$ 上非安定有理的であるが，$\mathbb{Q}$ 上レトラクト有理的 (Saltman 1984 [Sal84]).
- $\mathbb{Q}(C_8)$ は $\mathbb{Q}$ 上非レトラクト有理的であるが，$\mathbb{Q}$ 上単有理的 (Saltman 1982 [Sal82]).

定義 **4.3** (安定同型)．$F, F'$ を $k$ 上有限生成な体とする．以下の条件を満たすとき $F$ と $F'$ は $k$ 上安定同型であるといい，$F \overset{\text{stab}}{\sim} F'$ で表す：

$G$ 不変な $F$ 上代数的独立な元 $x_1, \ldots, x_n$ と $G$ 不変な $F'$ 上代数的独立な元 $y_1, \ldots, y_m$ で，$G$

作用込みの同型

$$F(x_1,\dots,x_n) \simeq F^{'}(y_1,\dots,y_m)$$

が成立するものが存在する.

以下の補題が重要となる.

補題 **4.4** (Swan の補題 [Swa69, Lemma 8]). $K$ を $G$ 体とし，$K$ の有限生成部分 $k$ 代数 $R, S$ が $G$ の作用で閉じており，$Q(R) = Q(S)$ であるとする．このとき，$r \in R^G$, $s \in S^G$ が存在して，$R[1/r] = S[1/s]$ となる.

証明. $S = k[a_1, a_2, \dots, a_n]$ とする．このとき，$Q(R) = Q(S)$ であるから，$a_i = x_i/c_i$ $(x_i, c_i \in R)$ とかける．$c = c_1c_2 \dots c_n, r = \prod_{\sigma\in G} \sigma(c)$ とおくと，$r \in R^G$ であり，$S \subset R[1/r]$ である．同様の議論により，$R[1/r] \subset S[1/s]$ となる $s \in S^G$ がとれる．よって，$R[1/s][1/r] = S[1/s]$ である．一方，$S \subset R[1/r]$ から $s = t/r^n$ となる $t \in R, n \in \mathbb{N}$ がとれる．このとき，$t = sr^n$ で $s, r$ はともに $G$ 不変な元であるから，とくに $t \in R^G$ である．すると，

$$R\left[\frac{1}{s}\right]\left[\frac{1}{r}\right] = R\left[\frac{1}{rt}\right]$$

であるから，$R[1/rt] = S[1/s]$ が得られる．ここで，$t, r \in R^G$ より $rt \in R^G$ である． □

レトラクトについて以下のことを注意しておく.

注意 **4.5.**

$$\phi : R \to S, \quad \psi : S \to R$$

で $\psi \circ \phi = \mathrm{Id}_R$ を満たすものが存在するとき，$\phi$ は単射であるから $\phi(r) \neq 0$ であり，

$$\phi : R[1/r] \to S[1/\phi(r)], \quad \psi : S[1/\phi(r)] \to R[1/r]$$

は $\psi \circ \phi = \mathrm{Id}_{R[1/r]}$ を満たすように自然に延長することができる．すなわち，$R[1/r]$ は $S[1/\phi(r)]$ のレトラクトとなる.

定理 **4.6.** $F, F^{'}$ を $k$ 上有限生成な体とする.

(i) $F$ と $F^{'}$ が $k$ 上安定同型であるとする．このとき，

$$F \text{ が } k \text{ 上レトラクト有理的} \iff F^{'} \text{ が } k \text{ 上レトラクト有理的.}$$

(ii) $F$ が $k$ 上安定有理的ならば $F$ はレトラクト有理的.

証明. (i) $F$ が $k$ 上レトラクト有理的 $\Longrightarrow F^{'}$ が $k$ 上レトラクト有理的を示せば十分．まず，$F$ と $F^{'}$ が安定同型であるから，

$$F(x_1,\dots,x_n) \simeq F^{'}(y_1,\dots,y_m)$$

となる有限個の代数的独立な元 $x_1,\ldots,x_n$ と $y_1,\ldots,y_m$ が存在する．この同型を通じて，$F(x_1,\ldots,x_n)$ と $F^{'}(y_1,\ldots,y_m)$ を同一視する．このとき，$F$ がレトラクト有理的であることにより存在する $k$ 代数を $R_0$ として，$R := R_0[x_1,\ldots,x_n]$ を考えれば，$R$ は $k[x_1,\ldots,x_n][x_{n+1},\ldots,x_{n'}][1/f]$ のレトラクトとなり，$F(x_1,\ldots,x_n)$ は $k$ 上レトラクト有理的となる．したがって，$F^{'}(y_1,\ldots,y_m)$ は $k$ 上レトラクト有理的となる．

すなわち，$F^{'}(y_1,\ldots,y_m)$ が $k$ 上レトラクト有理的であるとき，$F^{'}$ が $k$ 上レトラクト有理的となることを示せば良い．

まず，$F^{'}$ の有限生成部分 $k$ 代数 $A$ で $Q(A) = F^{'}$ を満たすものをとる．このとき，

$$Q(R) = Q(A[y_1,\ldots,y_m])$$

であるから，Swan の補題より $r \in R$, $t \in A[y_1,\ldots,y_m]$ が存在して，

$$R[1/r] = A[y_1,\ldots,y_m][1/t] \tag{1}$$

とできる (Swan の補題において $G$ を自明群とすれば適用できる)．$F^{'}$ は無限体であるから，$A$ の位数も無限である．従って，$A$ 代数の写像

$$\psi : A[y_1,\ldots,y_m] \longrightarrow A$$

で $a := \psi(t) \neq 0$ となるものが存在する．このとき $a \in R[1/r]$ より，$a = s/r^e$ となる $s \in R$ が存在し，(1) より

$$A[1/a][y_1,\ldots,y_n][1/t] = R[1/r][1/a] = R[1/rs]$$

が成立する．$a = \psi(t)$ だから $\psi$ は

$$\psi : A[y_1,\ldots,y_n][1/t] \longrightarrow A[1/a]$$

に延長され，さらに

$$\psi : R[1/rs] = A[1/a][y_1,\ldots,y_n][1/t] \longrightarrow A[1/a]$$

に延長すれば，$R[1/rs]$ は $A[1/a]$ のレトラクトとなる．

ここで，$R$ は $k[x_1,\ldots,x_n][x_{n+1},\ldots,x_{n'}][1/f]$ のレトラクトであるから，注意 4.5 から，$R[1/rs]$ が $k[x_1,\ldots,x_{n'}][1/f\psi^{'}(rs)]$ のレトラクトとなる

$$\phi^{'} : R[1/rs] \to k[x_1,\ldots,x_{n'}][1/f\phi^{'}(rs)],\ \psi^{'} : k[x_1,\ldots,x_{n'}][1/f\phi^{'}(rs)] \to R[1/rs]$$

が存在する．すなわち，

$$A[1/a] \overset{\psi}{\leftrightarrows} R[1/rs] \overset{\psi^{'}}{\leftrightarrows} k[x_1,\ldots,x_{n'}][1/f\phi^{'}(rs)]$$

$\psi$ と $\psi^{'}$ を合成することにより，$A[1/a]$ は $k[x_1,\ldots,x_{n'}][1/f\phi^{'}(rs)]$ のレトラクトとなる．$Q(A[1/a]) = F^{'}$ であったから，$F^{'}$ は $k$ 上レトラクト有理的となる．

(ii) $F$ が $k$ 上安定有理的であるとすると

$$F \overset{\text{stab}}{\sim} F(t_1, \ldots, t_n) \simeq k(s_1, \ldots, s_m)$$

より $F \overset{\text{stab}}{\sim} k$ となる．$k$ は明らかにレトラクト有理的であり，(i) より安定同型でレトラクト有理性は保たれるから，$F$ はレトラクト有理的である． □

ネーター問題に対するレトラクト有理性はガロアの逆問題において非常に重要な意味をもつことが次の定理からわかる．

定理 **4.7** (Saltman [Sal82], DeMeyer [DeM83])**.** $k$ を無限体，$G$ を有限群とする．このとき，以下は同値：

(i) $k(G)$ はレトラクト有理的.
(ii) 生成的 $G/k$ 多項式が存在する．

定理 2.9 は有理的であれば定義多項式が生成的であることを述べていたが，実際には有理的を弱めたレトラクト有理的でさえあれば十分である．

## 5 巡回群に対する不変体の有理性問題

この節では標数 0 の体上の巡回群に対するネーター問題を扱う．以下，$k$ を標数 0 の体，$G = C_n = \langle\sigma\rangle$ が $n$ 変数有理関数体 $F := k(x_0, \ldots, x_{n-1})$ に対して，変数には $\sigma(x_i) = x_{i+1}$，$k$ には自明に作用しているとする．ここで変数の添え字は mod $n$ で考える．

$\mathbb{Q}$ 上 $C_n$ に対してのネーター問題は必ずしも有理的ではないことを 2 節において注意したが，基礎体が 1 のべき根を含むときは大きく状況が変わり，次の定理が成立する (証明は増田 [Mas55] によるもの).

定理 **5.1** (Fischer [Fis15])**.** $k' := k(\zeta_n), F' := k'(x_0, \ldots, x_{n-1})$ とし，$k'$ に $C_n$ は自明に作用しているとする．このとき，${F'}^{C_n}$ は $k'$ 上有理的である．

証明**.** まず,

$$F'^{\langle\sigma\rangle} = F^{\langle\sigma\rangle}(\zeta_n)$$

であることを示す．($\supset$) は明らかであるが，$F^{\langle\sigma\rangle}(\zeta_n) \cap F = F^{\langle\sigma\rangle}$ であるから,

$$[F' : F^{\langle\sigma\rangle}(\zeta_n)] = [F : F^{\langle\sigma\rangle}] = [F' : F'^{\langle\sigma\rangle}]$$

より，両者の $F'$ からの拡大次数が等しくなり，等号が成立する．

ラグランジュレゾルベント

$$y_j := \sum_{i=0}^{n-1} \zeta_n^{-ij} x_i$$

を用いて，超越基底を具体的に与えることにより，$F^{'\langle\sigma\rangle}$ が $k^{'}$ 上有理的になることを示す．

$$c_{j,k} := \frac{y_j y_k}{y_{j+k}} \quad (0 \leq j,k \leq n-1)$$

と置く．$y_j, c_{j,k}$ についても添え字は mod $n$ で考える．このとき，

$$\sigma(y_j) = \sum_{i=0}^{n-1} \zeta_n^{-ij}\sigma(x_i) = \sum_{i=0}^{n-1} \zeta_n^{-ij} x_{i+1} = \sum_{i'=0}^{n-1} \zeta_n^{-j(i'-1)} x_{i'} = \zeta_n^j \sum_{i'=0}^{n-1} \zeta_n^{-i'j} x_{i'} = \zeta_n^j y_j$$

が成立する．したがって，

$$\sigma(c_{j,k}) = \frac{\zeta_n^j y_j \zeta_n^k y_k}{\zeta_n^{j+k} y_{j+k}} = \frac{y_j y_k}{y_{j+k}} = c_{j,k}$$

となり，$c_{j,k} \in F^{'\langle\sigma\rangle}$ がわかる．

また，

$$c_{j,k} = \frac{c_{1,j}c_{1,j+1}\cdots c_{1,j+k-1}}{c_{1,1}c_{1,2}\cdots c_{1,k-1}}$$

が成立することにより，

$$k^{'}(c_{j,k} \mid 0 \leq j,k \leq n-1) = k^{'}(c_{1,0}, c_{1,2}, \ldots, c_{1,n-1}) \subset F^{'\langle\sigma\rangle}$$

となる．ここで $M^{'} := k^{'}(c_{1,0}, c_{1,2}, \ldots, c_{1,n-1})$ と置くと，

$$c_{1,0}c_{1,1}\cdots c_{1,n-1} = \frac{y_1 y_0}{y_1}\frac{y_1 y_1}{y_2}\frac{y_1 y_2}{y_3}\cdots\frac{y_1 y_{n-1}}{y_0} = y_1^n$$

より，$y_1$ の $M^{'}$ 上の最小多項式は

$$X^n - c_{1,0}c_{1,1}\cdots c_{1,n-1}$$

となる．したがって，

$$[M^{'}(y_1) : M^{'}] = n$$

である．ここで

$$y_2 = \frac{y_1^2}{c_{1,1}}, y_3 = \frac{y_1 y_2}{c_{1,2}}, \ldots, y_0 = \frac{y_1 y_{n-1}}{c_{1,n-1}}$$

であるから

$$M^{'}(y_1) = M^{'}(y_1, \ldots, y_n) = F^{'}$$

となる．したがって $[F^{'} : M^{'}] = n$ と $M^{'} \subset F^{'\langle\sigma\rangle}$ より，

$$F^{'\langle\sigma\rangle} = M^{'} = k^{'}(c_{1,0}, c_{1,1}, \cdots, c_{1,n-1})$$

となる．$F^{'\langle\sigma\rangle}$ の $k^{'}$ 上の超越基底は $c_{1,1}, c_{1,2}, \cdots, c_{1,n}$ であり，$k^{'}$ 上有理的であることに他ならない． □

増田は基礎体に 1 のべき根を付け加えた体における超越基底を基礎体上に “降下” させる方法を与えた．

定理 **5.2** (増田 [Mas55]). $f_1, \ldots, f_t \in F^{'\langle\sigma\rangle}$ で次の条件を満たすものが存在するとする：

(i) $F^{'\langle\sigma\rangle} = k^{'}([f_i]_{\mathrm{conj}} \mid 1 \leq i \leq t)$.
(ii) $\sum_{i=1}^{t} \iota(f_i) = n$

ただし，$[f]_{\mathrm{conj}} := \{f \text{ の } F^{\langle\sigma\rangle} \text{上の共役 }\}, \iota(f) = \#[f]_{\mathrm{conj}}$ とする．このとき $F^{\langle\sigma\rangle}$ は $k$ 上有理的.
特に，$k^{'} \cap F^{\langle\sigma\rangle}(f_i)$ の $k$ 上の正規底 $\omega_{i,1}, \ldots, \omega_{i,\iota(f_i)}$ に対して

$$f_i = \sum_{j=1}^{\iota(f_i)} \omega_{i,j} m_{j,i} \quad (m_{j,i} \in F^{'\langle\sigma\rangle})$$

ならば，$F^{\langle\sigma\rangle}$ の超越基底は $\{m_{j,i} \mid 1 \leq i \leq t, 1 \leq j \leq \iota(f_i)\}$ となる.

注意 **5.3.** 逆向きは明らかに成立する.

証明. $f_1, \ldots, f_t$ が仮定を満たすとする．$k_i^{'} := k^{'} \cap F^{\langle\sigma\rangle}(f_i)$ と置く．このとき，

$$F^{\langle\sigma\rangle}k_i^{'} \subset F^{\langle\sigma\rangle}(f_i) \subset F^{'\langle\sigma\rangle} = F^{\langle\sigma\rangle}(\zeta_n)$$

となり，$k^{'}F^{\langle\sigma\rangle}k_i^{'} = F^{\langle\sigma\rangle}(\zeta_n)$ が成り立つ．また，

$$k^{'} \cap (F^{\langle\sigma\rangle}k_i^{'}) = k_i^{'}, \quad k^{'} \cap (F^{\langle\sigma\rangle}(f_i)) = k_i^{'}$$

である．$F^{\langle\sigma\rangle}k_i^{'}$ と $F^{\langle\sigma\rangle}(f_i)$ は $\zeta_n$ を付け加えれば $F^{'\langle\sigma\rangle}$ となる．ここで

$$[F^{'\langle\sigma\rangle} : F^{\langle\sigma\rangle}k_i^{'}] = \frac{[k^{'} : k]}{[k^{'} \cap (F^{\langle\sigma\rangle}k_i^{'}) : k]} = \frac{[k^{'} : k]}{[k^{'} \cap (F^{\langle\sigma\rangle}(f_i)) : k]} = [F^{'\langle\sigma\rangle} : F^{\langle\sigma\rangle}(f_i)]$$

となり，

$$F^{\langle\sigma\rangle}(f_i) = F^{\langle\sigma\rangle}k_i^{'}$$

が成立する．したがって

$$\mathrm{Gal}(F^{\langle\sigma\rangle}(f_i)/F^{\langle\sigma\rangle}) \simeq \mathrm{Gal}(k_i/k) \tag{2}$$

となる．仮定 (i) と，$f_i$ の $F^{\langle\sigma\rangle}$ 上の共役は $k$ 上 $m_{1,i}, \ldots, m_{\iota(f_i),i}$ によって書けることから

$$F^{'\langle\sigma\rangle} = k^{'}([f_i]_{\mathrm{conj}} \mid 1 \leq i \leq t) = k^{'}(m_{j,i} \mid 1 \leq i \leq t, 1 \leq j \leq \iota(f_i))$$

となる．ここで，$M := k(m_{j,i} \mid 1 \leq i \leq t, 1 \leq j \leq \iota(f_i))$ とすれば，

$$M(\zeta_n) = k^{'}(m_{j,i} \mid 1 \leq i \leq t, 1 \leq j \leq \iota(f_i)) = F^{'\langle\sigma\rangle}$$

より，

$$[F^{'\langle\sigma\rangle} : F^{\langle\sigma\rangle}][F^{\langle\sigma\rangle} : M] = [F^{'\langle\sigma\rangle} : M] \leq [k^{'} : k]$$

となり，(2) より $[F^{'\langle\sigma\rangle} : F^{\langle\sigma\rangle}] = [k^{'} : k]$ であるから $[F^{\langle\sigma\rangle} : M] = 1$ となる．したがって

$$F^{\langle\sigma\rangle} = M = k(m_{j,i} \mid 1 \leq i \leq t, 1 \leq j \leq \iota(f_i))$$

となる．仮定 (ii) から $\#\{m_{j,i}\} = n$ であるから，$F^{\langle\sigma\rangle}$ は $k$ 上有理的. □

増田は実際に $f_i$ を求めることにより次を示した.

系 **5.4** (増田 [Mas55]). $p \leq 11$ に対して，$\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上有理的.

証明. $f_1 = c_{1,0}$ とし，$p = 3, 5, 7, 11$ に対して，それぞれ $f_2 = c_{1,1}, c_{1,2}, c_{1,3}, c_{1,2}$ とすれば

$$\mathbb{Q}(\zeta_p)(x_0, \ldots, x_{p-1})^{C_p} = \mathbb{Q}(\zeta_p)([c_{1,0}]_{\mathrm{conj}}, [f_2]_{\mathrm{conj}}), \iota(f_2) = p - 1 \tag{3}$$

が成立する．ここでは $p = 3$ のときのみ確かめる.

$[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ である．$\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_3/\mathbb{Q}))$ を非自明な元とすると $\tau(\zeta_3) = \zeta_3^2$ となる．したがって

$$\tau(y_1) = y_2, \tau(y_2) = y_1$$

となる．よって

$$\tau(c_{1,1}) = \tau\left(\frac{y_1^2}{y_2}\right) = \frac{y_2^2}{y_1} = c_{2,2} = \frac{c_{1,2}c_{1,0}}{c_{1,1}}.$$

$c_{1,0}$ は $\tau$ により不変であるから，$p = 3$ のとき (3) が成り立っていることがわかる. □

例 **5.5** ($k(x_0, x_1, x_2)^{C_3}$ の超越基底). $k$ を標数 3 ではない体とする．$k$ が 1 のべき根を含むときは定理 5.1 より，超越基底は $c_{1,0}, c_{1,1}, c_{1,2}$ となるから，$k$ が 1 のべき根を含まないとする.

$k(x_0, x_1, x_2)^{C_3}$ の超越基底 $m_{1,1}, m_{2,1}, m_{2,2}$ を求める．$m_{1,1} = c_{1,0}$ は良い．$c_{1,1} = m_{2,1}\zeta_3 + m_{2,2}\zeta_3^2$ から $m_{2,1}, m_{2,2}$ を求める際，$c_{1,1} = y_1^2/y_2$ の分子分母に $y_1$ を掛けておくと，分母から $\zeta_3$ がなくなり，幾分計算が容易になる．$\zeta_3^2 + \zeta_3 + 1 = 0$ に注意し直接求めれば以下を得る：

$$\begin{aligned} m_{1,1} &= x_0 + x_1 + x_2, \\ m_{2,1} &= -\frac{x_0^3 + x_1^3 + x_2^3 + 6x_0x_1x_2 - 3(x_0^2x_1 + x_1^2x_2 + x_2^2x_0)}{x_0^2 + x_1^2 + x_2^2 - (x_2x_0 + x_0x_1 + x_1x_2)}, \\ m_{2,2} &= -\frac{x_0^3 + x_1^3 + x_2^3 + 6x_0x_1x_2 - 3(x_0x_1^2 + x_1x_2^2 + x_2x_0^2)}{x_0^2 + x_1^2 + x_2^2 - (x_2x_0 + x_0x_1 + x_1x_2)}. \end{aligned}$$

また，上式において，

$$x_0^3 + x_1^3 + x_2^3 = (x_0 + x_1 + x_2)(x_0^2 + x_1^2 + x_2^2 - x_0x_1 - x_1x_2 - x_2x_0) + 3x_0x_1x_2$$

であることを用いれば，

$$m_{2,2} = -m_{1,1} - 3\frac{x_0x_1^2 + x_1x_2^2 + x_2x_0^2 - 3x_0x_1x_2}{x_0^2 + x_1^2 + x_2^2 - (x_0x_1 + x_1x_2 + x_2x_0)}$$

となることがわかる．$m_{2,1}$ ついても同様に

$$m_{2,1} = -m_{1,1} - 3\frac{x_0^2x_1 + x_1^2x_2 + x_2^2x_0 - 3x_0x_1x_2}{x_0^2 + x_1^2 + x_2^2 - (x_0x_1 + x_1x_2 + x_2x_0)}$$

となる．したがって，より簡明な超越基底

$$s = x_0 + x_1 + x_2,$$
$$t = \frac{x_0x_1^2 + x_1x_2^2 + x_2x_0^2 - 3x_0x_1x_2}{x_0^2 + x_1^2 + x_2^2 - (x_0x_1 + x_1x_2 + x_2x_0)},$$
$$u = \frac{x_0^2x_1 + x_1^2x_2 + x_2^2x_0 - 3x_0x_1x_2}{x_0^2 + x_1^2 + x_2^2 - (x_0x_1 + x_1x_2 + x_2x_0)}$$

を得ることができる．$k$ の標数が 3 の場合でも $t$ と $u$ は独立であり，標数に関わらず $k(x_0, x_1, x_2)^{C_3}$ の超越基底となり，増田の公式と呼ばれている (しかしながら，[Mas55] で上記の超越基底が記載されている p.62 の最後の行には誤植があり，$t$ と $u$ にあたる式が同じ式になってしまっている．実際は分子が異なる式となり上記の $t$ と $u$ になる)．

以下証明なしに巡回群に対しての $\mathbb{Q}$ 上のネーター問題について知られている結果を列挙する．長谷川氏の講演においては，$G$ 格子の理論を用いて $\mathbb{Q}(C_8)$ のネーター問題が否定的であることを示すことを注意しておく．

Swan は増田の結果 [Mas55], [Mas68] を受け，はじめてネーター問題の反例を与えた．

定理 **5.6** (Swan [Swa69], Voskresenskii [Vos70])**.**

(i) $\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的であるならば，$\alpha \in \mathbb{Z}[\zeta_{p-1}]$ で $N_{\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}(\alpha)}(\alpha) = \pm p$ を満たすものが存在する．

(ii) (Swan [Swa69, Theorem 1]) $\mathbb{Q}(C_{47}), \mathbb{Q}(C_{167}), \mathbb{Q}(C_{233})$ は $\mathbb{Q}$ 上非有理的．

(iii) (Voskresenskii [Vos70, Theorem 2]) $\mathbb{Q}(C_{47})$, $\mathbb{Q}(C_{167})$, $\mathbb{Q}(C_{359})$, $\mathbb{Q}(C_{383})$, $\mathbb{Q}(C_{479})$, $\mathbb{Q}(C_{503})$, $\mathbb{Q}(C_{719})$ は $\mathbb{Q}$ 上非有理的．

定理 **5.7** (Voskresenskii [Vos71, Theorem 1])**.** $\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的であることと，$\alpha \in \mathbb{Z}[\zeta_{p-1}]$ で $N_{\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}}(\alpha) = \pm p$ を満たすものが存在することは同値である．

この結果から $\mathbb{Q}(\zeta_{p-1})$ の類数が 1 ならば $\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上有理的であることがわかる．

遠藤と宮田は，増田と Swan の方法を改良しネーター問題に大きな進展をもたらした．

定理 **5.8** (遠藤-宮田 [EM73, Theorem 2.3])**.** $G_1, G_2$ を有限群，$k$ を標数 0 の体とする．$k(G_1)$ と $k(G_2)$ が共に $k$ 上有理的 (resp. 安定有理的) ならば，$k(G_1 \times G_2)$ は $k$ 上有理的 (resp. 安定有理的)．

注意 **5.9.** Kang-Plans は [KP09, Theorem 1.3] において上記の結果が任意の体に対して正しいことを示した．

定理 **5.10** (遠藤-宮田 [EM73, Proposition 3.2])**.** $p$ を奇素数, $k$ を標数 0 の体とする．$k$ が $\zeta_p + \zeta_p^{-1}$ を含むとき，任意の自然数 $l$ に対して $k(C_{p^l})$ は $k$ 上有理的．特に，$\mathbb{Q}(C_{3^l})$ は $\mathbb{Q}$ 上有理的．

定理 **5.11** (遠藤-宮田 [EM73, Proposition 3.4, Corollary 3.10])**.**

(i) $p \leq 43$ と $p = 61, 67, 71$ に対して，$\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上有理的.
(ii) $p = 5, 7$ に対して，$\mathbb{Q}(C_{p^2})$ は $\mathbb{Q}$ 上有理的.
(iii) $l \geq 3$ に対して，$\mathbb{Q}(C_{2^l})$ は $\mathbb{Q}$ 上非有理的.

定理 **5.12** (遠藤-宮田 [EM73, Theorem 4.4])．$G$ を奇数位数の有限アーベル群，$k$ を標数 0 の体とする．このとき，自然数 $m$ で $k(G^m)$ が $k$ 上有理的となるものが存在する.

定理 **5.13** (遠藤-宮田 [EM73, Theorem 4.6])．$G$ を有限アーベル群とする．このとき，$\mathbb{Q}(G)$ が $\mathbb{Q}$ 上有理的となることと $\mathbb{Q}(G)$ が $\mathbb{Q}$ 上安定有理的となることは同値である.

Lenstra は [Len74] において，アーベル群のネーター問題が肯定的であるための必要十分条件を与えた.

定理 **5.14** (Lenstra [Len74, Main Theorem, Remark 5.7])．$k$ を体, $G$ を有限群とする．$k_{cyc}$ を $k$ の代数閉包に含まれる $k$ の最大円分拡大とする．$k \subset K \subset k_{cyc}$ とし，$\rho_K = \mathrm{Gal}(K/k) = \langle \tau_k \rangle$ が有限巡回群と仮定する．$p$ を $k$ の標数と異なる奇素数とし，$s \geq 1$ を整数とする．$\mathfrak{a}_K(p^s)$ を以下で定義された $\mathbb{Z}[\rho_K]$ のイデアルとする:

$$\mathfrak{a}_K(p^s) = \begin{cases} \mathbb{Z}[\rho_K] & (K \neq k(\zeta_p^s)) \\ (\tau_k - t, p) & (K = k(\zeta_p^s), \text{ここで } t \in \mathbb{Z} \text{ は } \tau_k(\zeta_p) = \zeta_p^t \text{を満たすとする}) \end{cases}$$

また，$\mathfrak{a}_K(G) = \prod_{p,s} \mathfrak{a}_K(p^s)^{m(G,p,s)}$ とする．ここで $m(G,p,s) = \dim_{\mathbb{Z}/p\mathbb{Z}}(p^{(s-1)}G/p^sG)$．このとき，以下は同値：

(i) $k(G)$ は $k$ 上有理的.
(ii) $k(G)$ は $k$ 上安定有理的.
(iii) $k \subset K \subset k_{cyc}$, $\mathbb{Z}[\rho_K]$ のイデアル $\mathfrak{a}_K(G)$ が単項イデアル．また $k$ の標数が 2 でないとき，$k(\zeta_{r(G)})/k$ は巡回拡大．ここで $r(G)$ は $G$ の指数を割る 2 の最大べきとする.

定理 **5.15** (Lenstra [Len74, Corollary 7.2])．以下は同値:

(i) $\mathbb{Q}(C_n)$ は $\mathbb{Q}$ 上有理的.
(ii) 任意の体 $k$ に対して $k(C_n)$ は $k$ 上有理的.
(iii) $p^s \,||\, n$ に対して $\mathbb{Q}(C_{p^s})$ は $\mathbb{Q}$ 上有理的.
(iv) $8 \nmid n$ かつ，任意の $p^s \,||\, n$ に対して $\alpha \in \mathbb{Z}[\zeta_{\phi(p^s)}]$ で $N_{\mathbb{Q}(\zeta_{\phi(p^s)})/\mathbb{Q}}(\alpha) = \pm p$.

定理 **5.16** (Lenstra [Len80, Proposition 4])．$p$ を素数とし，$s \geq 2$ の整数とする．このとき，$\mathbb{Q}(C_{p^s})$ が $\mathbb{Q}$ 上有理的であることと $p^s \in \{2^2, 3^m, 5^2, 7^2 \mid m \geq 2\}$ であることは同値.

遠藤-宮田 [EM73] では定理 5.8 を用いて，$p < 2000$ に対して $\mathbb{Q}(C_p)$ の $\mathbb{Q}$ 上の有理性を確かめている．また，星 [Hos15] では，$p < 20000$(2262 個) に対して $\mathbb{Q}(C_p)$ の $\mathbb{Q}$ 上の有理性を計算ソフト PARI/GP を用いて確かめている．その結果 17 個の有理的なケース ($p \leq 43, p = 61, 67, 71$) と 46 個の不明なケースを除きすべて $\mathbb{Q}$ 上非有理的であることがわかった.

最終的には Plans [Pla17] により $\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的になるケースが完全に決定された．

定理 **5.17** (Plans [Pla17, Theorem 1.1])．$p$ を素数とする．このとき，$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的であることと $p \leq 43, p = 61, 67, 71$ であることは同値である．

定理 5.15，定理 5.16，定理 5.17 を合わせて次を得る．

系 **5.18** (Plans [Pla17, Corollary 1.2])．$n$ を正整数とする．このとき，$\mathbb{Q}(C_n)$ が $\mathbb{Q}$ 上有理的であることと $n$ が

$$2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71$$

を割ることは同値である．ここで $m \geq 0$ である整数とする．

標数 $p$ に対しては以下の結果が知られていることを注意しておく：

定理 **5.19** (国吉 [Kun54, Kun55, Kun56])．$G$ を $p$ 群, $k$ を標数 $p$ の体とする．このとき，$k(G)$ は $k$ 上有理的．

しかしながら，一般に非アーベル群に対してのネーター問題は非常に難しく十分な結果が得られていない．例えば交代群 $A_n (n \geq 6)$ に対してのネーター問題は未解決である．

## 参考文献


[BCTSSD85] A. Beauville, J.-L. Colliot-Thélène, J.-J. Sunsuc, P. Swinnerton-Dyer, *Variétés stablement rationelles non rationelles*, Ann. Math. **121** (1985), 283–318.

[DeM83] F. R. DeMeyer, *Generic polynomials*, J. Algebra **84** (1983), 441–448.

[EM73] S. Endo, T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973), 7–26.

[Fis15] E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linear Transformationen*, Nachr. Königl. Ges. Wiss. Göttingen (1915), 77–80.

[Hil1892] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.

[Hos15] A. Hoshi, *On Noether's problem for cyclic groups of prime order*, Proc. Japan Akad. Ser. A **91** (2015), 39–44.

[HK10] A. Hoshi, M. Kang, *Twisted symmetric group actions*, Pacific J. Math. **248** (2010), 285–304.

[JLY02] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials, constructiveaspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, **45**, Cambridge University Press, Cambridge, (2002).

[KP09] M. Kang, B. Plans *Reduction theorems for Noether problem*, Proc. Amer. Math. Soc. **137** (2009), 1867–1874.

[Kem96] G. Kemper, *A constructive approach to Noether's problem*, Manuscripta Math. **90** (1996), 343–363.

[Kem01] G. Kemper, *Generic polynomals are descent-generic*, Manuscripta Math. **105** (2001), 139–141.

[KM00] G. Kemper, E. Mattig, *Generic polynomial with few parameters*, J. Symboric Comp. **30** (2000), 843–857.

[Kun54] H. Kuniyoshi, *On purely-transcendency of a certain field*, Tohoku Math. J. (2) **6** (1954), 101–108.

[Kun55] H. Kuniyoshi, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955), 65–67.

[Kun56] H. Kuniyoshi, *Certain subfields of rational function fields*, Proceedings of the international symposium on algebraic number theory, Tokyo&Nikko, 1955, 241–243, Science Council of Japan, Tokyo, 1956.

[Kuy64] W. Kuyk, *On a theorem of E. Noether*, Nederl. Akad. Wetensch. Proc. Ser. A. **67** (1964), 32–39.

[Len74] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325.

[Len80] H. W. Lenstra, Jr., *Rational functions invariant under a cyclic group*, Proceedings of the Queen's Number Theory Conference, 1979 (Kingston, Ont., 1979). pp.91–99, Queen's Papers in Pure and Appl. Math., 54, Queen's Univ., Kingston, Ont., 1980.

[Mas55] K. Masuda, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955), 59–63.

[Mas68] K. Masuda, *Application of theory of the group of classes of projective modules to existence problem of independent parameters of invariant*, J. Math. Soc. Japan **20** (1968) 223–232.

[Noe1917] E. Noether, *Gleichungen mit vorgeschriebener Gruppe* (German), Math. Ann. **78** (1917), 221–229.

[Noe1913] E. Noether, *Rationale Funktionenkörper* (German), Jber. Deutsch. Math. Verein **22** (1913), 316–319.

[Pla17] B. Plans, *On Noether's rationality problem for cyclic groups over* $\mathbb{Q}$, Proc. Amer. Math. Soc. **145** (2017), 2407–2409.

[Sal82] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.

[Sal84] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984), 165–215.

[Swa69] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent.

Math. **7** (1969), 148–158.

[Vos70] V. E. Voskresenskii, *On the question of the structure of the subfield of invariants of a cyclic group of the automorphisms of the field* $\mathbb{Q}(x_1, \ldots, x_n)$ (Russian), Izv. Akad. Nauk SSSR Ser. Mat **34** (1970), 366–375. English translation: Math. USSR-Izv. **4** (1970), 371–380.

[Vos71] V. E. Voskresenskii, *Rationality of certain algebraic tori* (Russian), Izv. Akad. Nauk SSSR Ser. Mat **35** (1971), 1037–1046. English translation: Math. USSR-Izv. **5** (1971), 1049–1056.

[Vos73] V. E. Voskresenskii, *Fields of invariants of abelian groups* (Russian), Uspekh Mat. Nauk **28** (1973), 77–102. English translation: Russian Math. Surveys **28** (1973), 79–105.

# 不変体の有理性問題 (2)

長谷川　寿人 (新潟大学)

本稿は第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」における講演「不変体の有理性問題 (2)」の原稿です．本講演では代数的トーラスの関数体の有理性問題と，それを用いたネーター問題の否定解の構成を中心に解説を行います．代数的トーラスの関数体の有理性問題を考える上では，$G$ 格子の理論が非常に重要な役割を果たします．本稿では，まず $G$ 格子の基本的な性質について確認した後，$G$ 格子と代数的トーラスの関数体の有理性問題との関係性について述べます．さらにその結果を用いて，位数 8 の巡回群 $C_8$ に対する $\mathbb{Q}$ 上のネーター問題が否定的であることを示します．

以下，$G$ は有限群であるとする．また，体は有限生成かつ無限体であると仮定する．

## 1　$G$ 格子

**定義** ($G$ 格子)**.** 有限生成 $\mathbb{Z}[G]$ 加群 $M$ で $\mathbb{Z}$ 上自由加群であるものを $G$ **格子**という．

**定義** (置換格子，安定置換格子，可逆格子，flabby，coflabby)**.** $M$ を $G$ 格子とする．

- $M$ の $\mathbb{Z}$ 基底を適当にとれば $G$ の作用が基底の置換を引き起こすとき，$M$ を**置換格子**という．
- ある置換格子 $P$，$P'$ が存在して $M \oplus P' \simeq P$ となるとき，$M$ を**安定置換格子**という．
- ある $G$ 格子 $M'$ と置換格子 $P$ が存在して $M \oplus M' \simeq P$ となるとき，$M$ を**可逆格子**であるという．
- 任意の $G$ の部分群 $H$ に対して $\widehat{H}^{-1}(H, M) = 0$ となるとき，$M$ は **flabby** であるという．
- 任意の $G$ の部分群 $H$ に対して $H^1(H, M) = 0$ となるとき，$M$ は **coflabby** であるという．

**例.** • $\mathbb{Z}[G] = \bigoplus_{\sigma \in G} \mathbb{Z}u_\sigma$ は $\tau \in G$ が $\tau \cdot u_\sigma = u_{\tau\sigma}$ で作用する $G$ 格子である．

• $H$ を $G$ の部分群とし，$G = \sigma_1 H \cup \sigma_2 H \cup \cdots \cup \sigma_n H$ を $G$ の $H$ による左剰余類分解とする．このとき，$\mathbb{Z}[G/H] = \bigoplus_{i=1}^{n} \mathbb{Z}u_{\sigma_i H}$ は $\tau \in G$ が $\tau \cdot u_{\sigma_i H} = u_{\tau\sigma_i H}$ で作用する $G$ 格子である．

• $M^\circ = \mathrm{Hom}(M, \mathbb{Z})$ とする．このとき $M^\circ$ は $\tau \in G$ が $f \in M^\circ$ に対し $(\tau \cdot f)(m) = \tau^{-1} f(\tau m)$ と作用する $G$ 格子である．これを $M$ の**双対格子**という．このとき，$(M^\circ)^\circ \simeq M$ が成り立つ．また，置換格子 $P$ の双対格子 $P^\circ$ もまた置換格子である．

**注意.** $M$ が置換格子であるとき，$G$ が置換で作用する $M$ の基底をとり，その $G$ の作用の安定化群を考えることで，$M$ は $G$ の部分群 $H_1, H_2, \ldots, H_n$ を用いて $M \simeq \bigoplus_{i=1}^{n} \mathbb{Z}[G/H_i]$ とかける．

**命題 1.1.** $M$ を $G$ 格子とする．$M$ が置換格子ならば $M$ は flabby かつ coflabby である．

**証明.** $M$ は $G$ の部分群 $H$ を用いて $\mathbb{Z}[G/H]$ の直和の形でかける．したがって $\mathbb{Z}[G/H]$ が flabby かつ coflabby であることを示せば十分である．これは Shapiro の補題より $\hat{H}^{\pm 1}(G, \mathbb{Z}[G/H]) \simeq \hat{H}^{\pm 1}(H, \mathbb{Z}) = 0$ であることから従う． □

$G$ 格子 $M$ に対して，以下の性質が成り立つ：
$M$ が置換格子 $\Longrightarrow$ 安定置換格子 $\Longrightarrow$ 可逆格子 $\Longrightarrow$ flabby かつ coflabby．最後に関しては，$M$ が可逆格子であるとき $M \oplus M'$ が置換格子でとなる $G$ 格子 $M'$ がとれ，命題 1.1 より $\hat{H}^{\pm 1}(G, M \oplus M') = \hat{H}^{\pm 1}(G, M) \oplus \hat{H}^{\pm 1}(G, M') = 0$ であることから従う．

$G$ 格子全体のカテゴリーに対して同値関係 $\sim$ を次のように定義する：
$G$ 格子 $M_1$，$M_2$ に対して，

$$M_1 \sim M_2 \iff \text{置換格子 } P_1, P_2 \text{が存在して } M_1 \oplus P_1 \simeq M_2 \oplus P_2.$$

演算を $[M_1] + [M_2] = [M_1 \oplus M_2]$ により定義すると，$\{G \text{ 格子全体のカテゴリー }\}/\sim$ は可換モノイドとなる．

このとき安定置換格子と可逆格子の定義は次のように言い換えることができる．

- $M$ は安定置換格子である $\iff [M] = 0$.
- $M$ は可逆格子である $\iff [M]$ は上のモノイドの可逆元である．

**補題 1.2.** $0 \to L \to M \xrightarrow{\pi} N \to 0$ を $G$ 格子の完全系列，$I$ を可逆格子とし，$f$ を $I$ から $N$ への $G$ 格子の準同型写像 $f : I \to N$ とする．このとき，任意の $G$ の部分群 $H$ に対して $\pi|_{M^H} M^H \to N^H$ が全射ならば，$f$ は $M$ に持ち上げられる，すなわち $f = \pi \circ f'$ となる $G$ 格子の準同型写像 $f' : I \to M$ が存在する．

**証明.** (以下の証明は [Arn81, Theorem 3.1] によるものである．)

3 つの step に分けて示そう．

step 1:$G$ の部分群 $H$ に対し $I = \mathbb{Z}[G/H]$ となる場合．このとき $u_H, \sigma_1(u_H), \sigma_2(u_H), \ldots, \sigma_n(u_H)$ が $I$ の $\mathbb{Z}$ 基底である．ここで，$G$ の左剰余類分解を $G = H \cup \sigma_1 H \cup \cdots \cup \sigma_n H$．$f$ が $G$ 格子の準同型写像であることから $f(u_H) \in N^H$ である．したがって，$\pi(m) = f(u_H)$ となる $m \in M^H$ がとれる．そこで，$f' : I \to M$ を $f'(\sigma_i(u_H)) = \sigma_i \cdot m$ と定義すれば，これが $f$ の $M$ への持ち上げとなる．

step 2 : $I$ が置換格子である場合．このとき $I$ は $\mathbb{Z}[G/H]$ という形の置換格子の直和となるから，それぞれの直和因子に対して step 1 を用いればよい．

step 3 : $I$ が可逆格子である場合．$I$ に対して，$I \oplus I'$ が置換格子になるような $G$ 格子 $I'$ をとり，$\bar{f} : I \oplus I' \to N$ を $\bar{f}(x, y) = f(x)$ で定義する．step 2 より，$\bar{f}$ の $M$ への持ち上げ $\varphi : I \oplus I' \to M$ がとれるから，$f'(x) = \varphi(x, 0)$ と定義すれば，これが $f$ の $M$ への持ち上げとなる． □

**命題 1.3.** $G$ 格子の完全系列

$$0 \to L \to M \xrightarrow{\pi} N \to 0 \qquad (*)$$

で $L$ が coflabby，$N$ が可逆格子であるとき，$(*)$ は分裂する．

**証明.** 任意の $G$ の部分群 $H$ に対し，完全系列 $(*)$ のコホモロジーの長完全列を考えることにより

$$\cdots \to M^H \to N^H \to H^1(H, L) = 0$$

であるから $\pi|_{M^H}$ は全射である．よって補題 1.2 より $N$ 上の恒等写像 $\mathrm{id}_N : N \to N$ の $M$ への持ち上げが得られ，これが完全系列 $(*)$ の分裂を与える． □

$G$ 格子全体のカテゴリーに対する重要な不変量である flabby 類の定義をしよう．

**定理 1.4** ([EM74, Lemma 1.1])**.** $G$ 格子 $M$ に対して，置換格子 $P$，flabby な $G$ 格子 $F$ が存在して，

$$0 \to M \to P \to F \to 0$$

が完全系列となる．この完全系列を $M$ の **flabby resolution** という．

**証明.** $0 \to C \to Q \xrightarrow{\pi} M^\circ \to 0$ が完全系列となるような置換格子 $Q$，$G$ 格子 $C$ で $\pi$ が次の条件をみたすように取れることを示そう : $G$ の任意の部分群 $H \leq G$ に対し，$\pi|_{Q^H} : Q^H \to M^{\circ H}$ が全射になる．ここで $M^\circ = \mathrm{Hom}(M, \mathbb{Z})$ は $M$ の双対格子である．実際，$Q^H = \mathbb{Z}[G/H]^{\oplus n_H}$ で自然数 $n_H$ を十分大きくとれば，$Q^H \to M^{\circ H}$ が全射となるようにできる．$Q = \bigoplus_{H \leq G} \mathbb{Z}[G/H]^{\oplus n_H}$，$\pi : Q \to M$ を上で定まるものとし，$C = \mathrm{Ker}\ \pi$ とすると完全系列 $0 \to C \to Q \xrightarrow{\pi} M^\circ \to 0 \cdots (*)$ が得られる．任意の $G$ の部分群 $H$ に対し，$(*)$ に対してコホモロジーの長完全列を考えると

$$\cdots \to Q^H \xrightarrow{\pi|_{Q^H}} M^{\circ H} \to H^1(H, C) \to H^1(H, Q) = 0$$

であり，$\pi|_{Q^H}$ は全射であることから $H^1(H, C) = 0$ となる．よって $C$ は coflabby である．

したがって $P = Q^\circ, F = C^\circ$ ととればよい． □

$G$ 格子 $M$ に対して，$[F]$ は一意的に定まる．これを，$M$ の **flabby 類**といい，$[M]^{fl}$ とかく．

**注意.** $G$ 格子 $M$ の flabby 類は，類 $[M]$ に対する不変量になっている．実際，$M_1,\ M_2 \in [M]$ とすると，$M_1 \oplus P_1 \simeq M_2 \oplus P_2$ となる置換格子 $P_1, P_2$ がとれる．$M_1 \oplus P_1,\ M_2 \oplus P_2$ の flabby resolution をそれぞれ $0 \to M_1 \oplus P_1 \to Q_1 \to F_1 \to 0,\ 0 \to M_2 \oplus P_2 \to Q_2 \to F_2 \to 0$ ($Q_1,\ Q_2$ は置換格子，$F_1,\ F_2$ は flabby な $G$ 格子) とする．このとき上の flabby resolution の双対を考えると，図式

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & & & & & F_2^\circ & & \\ & & & & & & \downarrow & & \\ & & & & & & Q_2^\circ & & \\ & & & & & & \downarrow & & \\ 0 & \to & F_1^\circ & \to & Q_1^\circ & \to & (M_1 \oplus F_1)^\circ & \to & 0 \\ & & & & & & \downarrow & & \\ & & & & & & 0 & & \end{array}$$

が得られる．これに対して pullback(3.1 節参照) を考えることで，

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & F_2^\circ & = & F_2^\circ & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & F_1^\circ & \to & E & \longrightarrow & Q_2^\circ & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & F_1^\circ & \to & Q_1^\circ & \to & (M_1 \oplus F_1)^\circ & \to & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

が得られる．命題 1.3 から 2 行目と 2 列目の完全系列は分裂するから，$F_1^\circ \oplus Q_2^\circ \simeq E \simeq F_2^\circ \oplus Q_1^\circ$ となる．よって $[F_1^\circ \oplus Q_2^\circ] = [F_2^\circ \oplus Q_1^\circ]$ で，$Q_1^\circ, Q_2^\circ$ が置換格子であることに注意すると，$[F_1^\circ] = [F_2^\circ]$ となる．これより両辺の双対をとれば $[F_1] = [F_2]$ となるから，$[M_1]^{fl} = [M_2]^{fl}$ となる．以上のことから $M$ の類の代表元のとり方によらず $[M]^{fl}$ が定まる．

flabby 類に関する性質について述べる．

**命題 1.5.** (1) $M$ が可逆格子のとき，$[M]^{fl} = -[M]$ である．
(2) $0 \to L \to M \to N \to 0$ を $G$ 格子の完全系列とし，$N$ が可逆格子であるとする．このとき，$[M]^{fl} = [L]^{fl} + [N]^{fl}$ である．

**証明.** (1) $M$ は可逆格子であるから，$M \oplus M' \simeq Q$ となる可逆格子 $M'$ と置換格子 $P$ が存在する．このとき，$M$ の flabby resolution として $0 \to M \to P \to M' \to 0$ を自然にとることができる．すると，$[M] + [M'] = 0$ であるから，$[M]^{fl} = [M'] = -[M]$ が得られる．

(2) $0 \to L \to P \to F \to 0$ を $L$ の flabby resolution とし，図式

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ 0 & \to & L & \to & M & \to & N & \to & 0 \\ & & \downarrow & & & & & & \\ & & P & & & & & & \\ & & \downarrow & & & & & & \\ & & F & & & & & & \\ & & \downarrow & & & & & & \\ & & 0 & & & & & & \end{array}$$

に対して pushout(3.1 節参照) を考えて次の図式が得られる：

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & L & \to & M & \to & N & \to & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \to & P & \to & X & \to & N & \to & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & F & = & F & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array}$$

$N$ は可逆格子だから，定理 1.3 から 2 行目の完全系列は分裂する．よって，$X \simeq P \oplus N$ である．また $N$ は可逆格子より $N \oplus N' \simeq Q$ となる可逆格子 $N'$ と置換格子 $Q$ が存在する．このとき $X \oplus N' = P \oplus N \oplus N' = P \oplus Q$ は置換格子であるから上の図式の 2 列目に $N'$ を直和することにより，$M$ の flabby resolution として $0 \to M \to P \oplus Q \to F \oplus N' \to 0$ が得られる．(1) の証明中の議論から $[N]^{fl} = [N']$ であることに注意すると $[M]^{fl} = [F \oplus N'] = [F] + [N'] = [L]^{fl} + [N]^{fl}$ を得る． □

**命題 1.6.** $M_1, M_2$ を $G$ 格子としたとき，以下は同値である：
(i) $[M_1]^{fl} = [M_2]^{fl}$.
(ii) $0 \to M_1 \to E \to P_1 \to 0,\ 0 \to M_2 \to E \to P_2 \to 0$ が完全系列となるような $G$ 格子 $E$ と置換格子 $P_1, P_2$ が存在する．

**証明.** (i) $\Longrightarrow$(ii)：仮定より $[M_1]^{fl} = [M_2]^{fl}$ であるから，$M_1$ と $M_2$ の flabby resolution として完全系列 $0 \to M_1 \to P_1 \to F \to 0,\ 0 \to M_2 \to P_2 \to F \to 0$ ($P_1, P_2$ は置換格子，$F$ は flabby な $G$ 格子) が得られる．

図式

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ & & & & & & M_2 & & \\ & & & & & & \downarrow & & \\ & & & & & & P_2 & & \\ & & & & & & \downarrow & & \\ 0 & \to & M_1 & \to & P_1 & \longrightarrow & F & \to & 0 \\ & & & & & & \downarrow & & \\ & & & & & & 0 & & \end{array}$$

に対して pullback(3.1 節参照) を考えることで,

$$\begin{array}{ccccccccc} & & & & & & 0 & & 0 \\ & & & & & & \downarrow & & \downarrow \\ & & & & & & M_2 & = & M_2 \\ & & & & & & \downarrow & & \downarrow \\ 0 & \to & M_1 & \longrightarrow & E & \longrightarrow & P_2 & \to & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & M_1 & \to & P_1 & \longrightarrow & F & \to & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

が得られる.

(ii) $\Longrightarrow$ (i) : (ii) の完全系列において，$P_1, P_2$ は置換格子であるから，とくに可逆格子である．そこで，命題 1.5(2) を適用すると

$$[E]^{fl} = [M_1]^{fl} + [P_1]^{fl} = [M_1]^{fl}$$
$$[E]^{fl} = [M_2]^{fl} + [P_2]^{fl} = [M_2]^{fl}$$

が得られる．よって，$[M_1]^{fl} = [M_2]^{fl}$ である． □

## 2 $G$ 格子と代数的トーラスの有理性

$K/k$ をガロア群が $G$ のガロア拡大，$M = \sum_{i=1}^{n} \mathbb{Z}u_i$ を $G$ 格子とする．$K[M] = K[{x_1}^{\pm 1}, {x_2}^{\pm 1}, \ldots, {x_n}^{\pm 1}]$ とし，$G$ の元 $\sigma \in G$ が $M$ に $\sigma u_i = \sum_{j=1}^{n} a_{ij}u_j$ $(a_{ij} \in \mathbb{Z})$ と作用するとき，$K[M]$ の元には $\sigma(\alpha x_i) = \sigma(\alpha)\prod_{j=1}^{n} {x_j}^{a_{ij}}$ $(\alpha \in K)$ と乗法的に作用するものとする．このとき $K[M]$ の商体を $K(M) = Q(K[M])$ とし，$G$ の作用は自然に延長したものとする．このとき $K(M)^G$ は $k$ 上の代数的トーラスの関数体となる (代数的トーラスの基本事項は本整数論サマースクール「Rationality problem for algebraic tori」を参照)．本節では，代数的トーラスの関数体の有理性問題について考えていく．

**補題 2.1** (Swan の補題 [Swa69, Lemma 8])**.** $K$ を $G$ が作用する体とし，$K$ の有限生成部分 $k$ 代数 $R, S$ が $G$ の作用で閉じており $Q(R) = Q(S)$ であるとする．このとき $r \in R^G$, $s \in S^G$ が存在して $R[1/r] = S[1/s]$ となる．

**証明.** $S = k[a_1, a_2, \ldots, a_n]$ とする．このとき $Q(R) = Q(S)$ であるから，$a_i = x_i/c_i$, $(x_i, c_i \in R)$ とかける．$c = c_1 c_2 \ldots c_n, r = \prod_{\sigma \in G} \sigma(c)$ とおくと，$r \in R^G$ であり $S \subset R[1/r]$ である．同様の議論により $R[1/r] \subset S[1/s]$ となる $s \in S^G$ がとれる．よって $R[1/s][1/r] = S[1/s]$ である．一方 $S \subset R[1/r]$ から $s = t/r^n$ となる $t \in R, n \in \mathbb{N}$ がとれる．このとき，$t = sr^n$ で $s, r$ はともに $G$ 不変な元であるから，とくに $t \in R^G$ である．すると

$$R\left[\frac{1}{s}\right]\left[\frac{1}{r}\right] = R\left[\frac{1}{rt}\right]$$

であるから $R[1/rt] = S[1/s]$ が得られる．ここで $t, r \in R^G$ より $rt \in R^G$ である． □

**定理 2.2** (Hilbert の定理 90)**.** $K/k$ をガロア拡大とし，$G = \mathrm{Gal}(K/k)$ とする．このとき $H^1(G, \mathrm{GL}_n(K)) = 0$ である．

Hilbert の定理 90 の応用として，次の非常に有用な定理が得られる．

**命題 2.3** ([EM73, Proposition 1.1])**.** $K$ を忠実に $G$ が作用する体，$V = \oplus_{i=1}^n K u_i$ を $K$ 線型空間とし，$G$ が $V$ に半線型作用，すなわち $\sigma \in G$ が $K(V) = K(u_1, u_2, \ldots, u_n)$ に対し

$$\sigma(a u_i) = \sigma(a) \sum_{j=1}^{n} a_{ij}(\sigma) u_j \ (a, a_{ij}(\sigma) \in K)$$

と作用しているとする．このとき，$K(u_1, u_2, \ldots, u_n)^G$ は $K^G$ 上有理的である．

**証明.** $\{u_1, u_2, \ldots, u_n\}$ を $V$ の基底とする．このとき，

$$\sigma \cdot \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} & a_{ij}(\sigma) & \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}, \quad \begin{pmatrix} & a_{ij}(\sigma) & \end{pmatrix} \in \mathrm{GL}_n(K)$$

である．$f : G \to \mathrm{GL}_n(K)$ を $\sigma \mapsto (a_{ij}(\sigma))$ と定めると，任意の $\sigma, \tau \in G$ に対して

$$\begin{aligned}
\sigma\tau \cdot \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} &= \sigma \cdot \begin{pmatrix} & a_{ij}(\tau) & \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \\
&= \begin{pmatrix} & a_{ij}(\sigma) & \end{pmatrix} \begin{pmatrix} & \sigma \cdot a_{ij}(\tau) & \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \\
&= f(\sigma)\big(\sigma \cdot f(\tau)\big) \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}
\end{aligned}$$

となるから，$f(\sigma\tau) = f(\sigma)\big(\sigma \cdot f(\tau)\big)$ となり $f$ は 1 コサイクルになる．すると，Hilbert の定理 90(定理 2.2) から，任意の $\sigma \in G$ に対して

$$f(\sigma) = \sigma(P)^{-1}P$$

となる $P \in \mathrm{GL}_n(K)$ が存在する．ここで

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = P \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

とおくと，任意の $\sigma \in G$ に対して

$$\sigma \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \sigma \cdot P \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \sigma(P) \left\{ \sigma \cdot \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \right\} = \sigma(P) f(\sigma) \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = P \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

であるから，$\sigma \cdot v_i = v_i$ $(i = 1, 2 \ldots, n)$ となる．よって $K(V)^G = K(u_1, u_2, \ldots, u_n)^G = K(v_1, v_2, \ldots, v_n)^G = K^G(v_1, v_2, \ldots, v_n)$ となり，$K(V)^G$ は $K^G$ 上有理的である． □

この定理の系として，次の重要な結果が得られる．

**系 2.4.** $P$ が置換格子のとき，$K(P)^G$ は $K^G$ 上有理的である．

**系 2.5** (No-Name Lemma)**.** $W$ を $V$ の忠実な $K[G]$ 部分加群とする．このとき，$K(V)^G$ は $K(W)^G$ 上有理的である．

**証明.** 命題 2.3 で $K$ を $K(W)$ ととればよい. □

**定理 2.6** ([Len74, Proposition 1.5]). $K/k$ をガロア拡大で $G = \mathrm{Gal}(K/k)$ とし，$M, M'$ を $G$ 格子，$N$ を可逆格子とし，$0 \to M' \to M \to N \to 0$ が完全系列であるとする．このとき，$K(M) \simeq K(M' \oplus N)$ である．とくに，$K(M)^G \simeq K(M' \oplus N)^G$.

**証明.** 完全系列

$$0 \to K(M')^\times \to K(M')^\times \cdot M \xrightarrow{\pi} N \to 0 \qquad (*)$$

を考える．ここで $\pi(\lambda m) = m \mod M'$, $\lambda \in K(M')^\times, m \in M$. Hilbert の定理 90 (定理 2.2) から，任意の $G$ の部分群 $H$ に対し $H^1(H, K(M')^\times) = 0$ であるから，$K(M')^\times$ は coflabby である．よって命題 1.3 より完全系列 $(*)$ は分裂する．この分裂を与える写像 $N \to K(M') \cdot M \subset K(M)^\times$ から，$K(M' \oplus N) \simeq K(M)$ が得られる． □

**系 2.7.** $N$ が置換格子のとき，$K(M)^G$ は $K(M')^G$ 上有理的である.

**証明.** $N$ が置換格子であるとき，定理 2.6 より $K(M)^G \simeq K(M' \oplus N)^G = K(M')(N)^G$ である．補題 2.4 より $K(M')(N)^G$ は $K(M')^G$ 上有理的であるから，$K(M)^G$ は $K(M')^G$ 上有理的である． □

本稿の主定理である代数的トーラスの関数体の有理性問題と $G$ 格子との関係について述べる．そこで必要となる補題を 1 つ用意しておく.

**補題 2.8.** $K$ を忠実に $G$ が作用する体とし，$L/K$ を体の拡大とする．このとき $L^G$ が $K^G$ 上有理的であるならば，$K$ 上代数的独立な元 $x_1, x_2, \ldots, x_n$ が存在して $L = K(x_1, x_2, \ldots, x_n)$ とかける.

**証明.** $L^G$ が $K^G$ 上有理的であることから，$K^G$ 上代数的独立な $L^G$ の元 $x_1, x_2 \ldots, x_n$ が存在して，$F^G = K^G(x_1, x_2, \ldots, x_n)$ とかける．このとき，$K/K^G$ は代数拡大であるから，$x_1, x_2 \ldots, x_n$ は $K$ 上代数的独立でもある．ここで，$F = K(x_1, x_2 \ldots, x_n)$ とすると，$L^G \subset F \subset L$ であるから，$F^G = L^G$ である．さらに $[L : L^G] = |G| = [F : F^G]$ であるから，上と合わせて $L = E = K(x_1, x_2 \ldots, x_n)$ が得られる． □

**定理 2.9** ([Vos74, Theorem 2]). $K/k$ をガロア拡大，$G = \mathrm{Gal}(K/k)$ とし，$M_1, M_2$ を $G$ 格子とする．このとき，以下は同値である：
(i) $K(M_1), K(M_2)$ は $K$ 上安定同型である，
(ii) $[M_1]^{fl} = [M_2]^{fl}$.

**証明.** (ii) $\Longrightarrow$ (i) : 仮定より $[M_1]^{fl} = [M_2]^{fl}$ であるから，命題 1.6 より $M_1, M_2$ の flabby resolution を $0 \to M_1 \to E \to P_1 \to 0$, $0 \to M_2 \to E \to P_2 \to 0$（$E$ は $G$ 格子，$P_1, P_2$ は置換格子）ととることができる．すると定理 2.6 より $K(M_1 \oplus P_1) \simeq_K K(E) \simeq_K K(M_2 \oplus P_2)$ となるから $K(M_1)$ と $K(M_2)$ は $K$ 上安定同型である．よって $K(M_1)^G, K(M_2)^G$ は $K^G = k$ 上安定同型である．(i) $\Longrightarrow$ (ii) : 仮定より $K(M_1), K(M_2)$ が $K$ 上安定同型であることから，$K$ 上代数的独立な元 $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n$ が存在して

$$K(M_1)(x_1, x_2, \ldots, x_m) \simeq K(M_2)(y_1, y_2, \ldots, y_n)$$

となる．$R_1 = K[M_1][x_1, x_2, \ldots, x_m]$, $R_2 = K[M_2][y_1, y_2, \ldots, y_n]$ とおくと，$Q(R_1) \simeq Q(R_2)$ であるから，Swan の補題 (補題 2.1) より $R_1[1/r_1] \simeq R_2[1/r_2]$ となる $r_1 \in R_1^G, r_2 \in R_2^G$ がとれる．ここで，$U(R)$ で $R$ の単数群を表すものとする．すると完全系列 $1 \to U(R_1) \to U(R_1[1/r_1]) \to P_1 \to 0$ が得られる．ここで，$P_1$ は置換格子である．$U(R_1) \simeq K^\times \times M_1$ であるから，

$$1 \to K^\times \times M_1 \to U\left(R_1\left[\frac{1}{r_1}\right]\right) \to P_1 \to 0$$

が得られる．これより $1 \to M_1 \to U\left(R_1\left[1/r_1\right]\right)/K^\times \to P_1 \to 0$ を得る．同様にして $1 \to M_2 \to U\left(R_2\left[1/r_2\right]\right)/K^\times \to P_2 \to 0$ が得られ，$U\left(R_1\left[1/r_1\right]\right)/K^\times \simeq U\left(R_2\left[1/r_2\right]\right)/K^\times$ であるから，命題 1.6 より $[M_1]^{fl} = [M_2]^{fl}$ である． □

上の定理から，代数的トーラスの関数体が安定有理的であることは次のように特徴づけられる．

**系 2.10** ([EM73, Theorem 1.6])**.** $K/k$ をガロア拡大，$G = \mathrm{Gal}(K/k)$ とし，$M$ を $G$ 格子とする．このとき，以下は同値である：
(i) $K(M)^G$ は $k$ 上安定有理的である．
(ii) $[M]^{fl} = 0$ である．

**証明.** (i) $\Longrightarrow$ (ii) : $K(M)^G$ は $k = K^G$ 上安定有理的である．すると補題 2.8 から $K(M)$ と $K$ は $K$ 上安定有理的である．よって定理 2.9 より $[M]^{fl} = 0$ である．

(ii) $\Longrightarrow$ (i) : 定理 2.9 から $K(M)$ は $K$ と $K$ 上安定同型であるから $K(M)^G$ は $k = K^G$ 上安定有理的である． □

また，代数的トーラスの関数体がレトラクト有理的であることは次のように特徴づけられる．

**定理 2.11** ([Sal84, Theorem 3.14])**.** $K/k$ をガロア拡大，$G = \mathrm{Gal}(K/k)$ とし，$M$ を $G$ 格子とする．このとき，以下は同値である：
(i) $K(M)^G$ は $k$ 上レトラクト有理的である，
(ii) $[M]^{fl}$ は可逆である．

**証明.** (ii) $\Longrightarrow$ (i) : 仮定より $[M]^{fl}$ が可逆であるから，$M$ の flabby resolution として $0 \to M \to P \to F \to 0$（$P$ は置換格子，$F$ は可逆格子）をとることができる．すると，定理 2.6 より $K(P)^G \simeq K(M \oplus F)^G$ であり，$K(P)^G$ は $k$ 上有理的であることから，$K(M \oplus F)^G = K(M)(F)^G$ は $k$ 上有理的である．とくに $K(M)(F)^G$ は $k$ 上レトラクト有理的であるから，下の補題 2.12 により $K(M)^G$ も $k$ 上レトラクト有理的である．

(i) $\Longrightarrow$ (ii) : (以下の証明は [Yam12, Theorem 2.10] によるものである．)

仮定より $K(M)^G$ が $k$ 上レトラクト有理的であることから，次の条件をみたす有限生成 $k$ 代数 $B$ が存在する：

・ $B$ の商体 $Q(B)$ は $K(M)^G$ である，

・ $k$ 上代数的独立な元 $x_1, x_2 \ldots, x_n$ と $h \in k[x_1, x_2, \ldots, x_n]$ が存在して，

$$B \underset{\psi}{\overset{\varphi}{\rightleftarrows}} k[x_1, x_2, \ldots, x_n]\left[\frac{1}{h}\right]$$

で $\psi \circ \varphi = \mathrm{id}_B$ となる $k$ 準同型写像 $\varphi, \psi$ が存在する．

このとき，$Q(K \otimes B) = K(M) = Q(K[M])$ である．ここで補題 2.1 より，$f \in K[M]^G$, $g \in (K \otimes B)^G$ が存在して，

$$K[M]\left[\frac{1}{f}\right] = (K \otimes B)\left[\frac{1}{g}\right]$$

となる．ここで，$h$ の $K[x_1, x_2, \ldots, x_n]$ での既約分解を $h = h_1^{\lambda_1} h_2^{\lambda_2} \cdots h_r^{\lambda_r}$ ($\lambda_1, \lambda_2, \ldots, \lambda_r$ は自然数で，$h_1, h_2, \ldots, h_r$ はそれぞれ互いに素) とし，$\varphi(g) = \tilde{h}/h_1^{\alpha_1} h_2^{\alpha_2} \cdots h_r^{\alpha_r}$　($\alpha_1, \alpha_2, \ldots, \alpha_r$ は自然数で，$\tilde{h} \in K[x_1, x_2, \ldots, x_n]$ は $h_1, h_2, \ldots, h_r$ とそれぞれ互いに素) とすると，$\varphi, \psi$ は $K$ 準同型写像 $\varphi : (K \otimes B)[1/g] \to K[x_1, x_2, \ldots, x_n][1/h\tilde{h}], \psi : K[x_1, x_2, \ldots, x_n][1/h\tilde{h}] \to (K \otimes B)[1/g]$ に延長でき，$\psi \circ \varphi = \mathrm{id}_{(K \otimes B)[1/g]}$ である．ここで，$R = K[M][1/f], S = (K \otimes B)[1/g]$ とすると，$U(R) = U(S)$ である．上の $\varphi, \psi$ から $G$ 格子 $U(S)/K^\times$ は置換格子 $U(K[x_1, x_2 \ldots, x_n][1/h\tilde{h}])/K^\times$ の直和因子になる．よって $U(S)/K^\times$ は可逆格子であるから，ある $G$ 格子 $I$ が存在して，$U(S)/K^\times \oplus I$ は置換格子になる．このとき，完全系列 $1 \to U(R) \to U(R[1/f]) \to Q \to 0$ が得られ，$Q$ は置換格子である．これより，

$$1 \to M \to U\left(R\left[\frac{1}{f}\right]\right)/K^\times \oplus I \to Q \oplus I \to 0$$

が得られ，$U(R[1/f])/K^\times \oplus I = U(S)/K^\times \oplus I$ は置換格子である．よって，これが $M$ の flabby resolution であることから $[M]^{fl} = [Q \oplus I] = [I]$ となり $[M]^{fl}$ は可逆である．　□

**補題 2.12.** $F$ を忠実に $G$ が作用する体で，$M$ を $G$ 格子とする．このとき $F(M)^G$ が $k$ 上レトラクト有理的であるならば，$F^G$ も $k$ 上レトラクト有理的である．

**証明.** $F(M)^G$ が $k$ 上レトラクト有理的であるから，次の条件をみたす有限生成 $k$ 代数 $R$ が存在する：

・ $R$ の商体 $Q(R)$ は $F(M)^G$ である，

・ $k$ 上代数的独立な元 $x_1, x_2 \ldots, x_n$ と $f \in k[x_1, x_2, \ldots, x_n]$ が存在して，

$$R \underset{\psi}{\overset{\varphi}{\rightleftarrows}} k[x_1, x_2, \ldots, x_n]\left[\frac{1}{f}\right] \tag{$*$}$$

で $\psi \circ \varphi = \mathrm{id}_R$ となる $k$ 準同型写像 $\varphi, \psi$ が存在する．

ここで，$A = F[M]^G$ とおき，$A = K^G S$ となる $A$ の有限生成部分 $k$ 代数 $S$ を $Q(S \cap K^G) = K^G$ となるようにとる．このとき，$Q(R) = Q(S) = Q(A) = F(M)^G$ であることに注意すると，補題 2.1 より，

$$R\left[\frac{1}{r}\right] = S\left[\frac{1}{s}\right] = A\left[\frac{1}{a}\right]$$

となる $r \in R^G, s \in S^G, a \in A^G$ が存在する．すると，$(*)$ は

$$S\left[\frac{1}{s}\right] = R\left[\frac{1}{r}\right] \underset{\psi}{\overset{\varphi}{\rightleftarrows}} k[x_1, x_2, \ldots, x_n]\left[\frac{1}{f'}\right] \tag{$**$}$$

に延長できる．ここで $\alpha : A \to F^G$ を $\alpha(s) \neq 0$ となるような $k$ 代数の準同型写像とし，それを自然に $\alpha : A[1/s] \to F^G$ に延長し，$S' = \alpha(S[1/s])$ とする．このとき，$S \cap K^G = \alpha(S \cap K^G) \subset S' \subset K^G = Q(S \cap K^G)$ により，$Q(S') = K^G$ が得られる．補題 2.1 を用いると，$S' \subset S[1/s']$ となる $s' \in S \cap K^G$ がとれる．すると，$(**)$ は

$$S\left[\frac{1}{ss'}\right] \underset{\psi}{\overset{\varphi}{\rightleftarrows}} k[x_1, x_2, \ldots, x_n]\left[\frac{1}{f''}\right] \tag{$***$}$$

に延長できる．一方 $\alpha$ は $k$ 上恒等写像であるから，

$$S'\left[\frac{1}{s'}\right] \underset{\alpha}{\overset{\beta}{\rightleftarrows}} S\left[\frac{1}{ss'}\right] \subset A\left[\frac{1}{s}\right]$$

が得られる．ここで，$\beta : S'[1/s'] \to S[1/ss']$ は自然な埋め込みである．よって $(***)$ と合わせると

$$S'\left[\frac{1}{s'}\right] \underset{\alpha\circ\psi}{\overset{\varphi\circ\beta}{\rightleftarrows}} k[x_1, x_2, \ldots, x_n]\left[\frac{1}{f''}\right]$$

が得られ，$(\alpha \circ \psi) \circ (\varphi \circ \beta) = \mathrm{id}$ である．以上より $F^G$ は $k$ 上レトラクト有理的である． □

以上をまとめると，次のようになる：

・$K(M)^G$ が $k$ 上有理的である $\Longleftarrow$ $M$ が置換格子である (系 2.4).

・$K(M)^G$ が $k$ 上安定有理的である $\Longleftrightarrow$ $[M]^{fl} = 0$ (定理 2.10).

・$K(M)^G$ が $k$ 上レトラクト有理的である $\Longleftrightarrow$ $[M]^{fl}$ が可逆 (定理 2.11).

**例.** $\mathbb{Q}(C_8)$ が $\mathbb{Q}$ 上有理的でないことを示そう．$C_8 = \langle\sigma\rangle$ とし，$\mathbb{Q}(C_8) = \mathbb{Q}(x_i \mid i = 0, 1, \ldots, 7)^{\langle\sigma\rangle}$ である．ここで $\sigma(x_i) = x_{i+1}$ である．

$$\begin{aligned} y_1 &= x_0 - x_4,\ y_1' = x_0 + x_4 \\ y_2 &= x_1 - x_5,\ y_2' = x_1 + x_5 \\ y_3 &= x_2 - x_6,\ y_3' = x_2 + x_6 \\ y_4 &= x_3 - x_7,\ y_4' = x_3 + x_7 \end{aligned}$$

とおくと，$\mathbb{Q}(C_8) = \mathbb{Q}(y_1, y_2, y_3, y_4, y_1', y_2', y_3', y_4')^{\langle\sigma\rangle}$ となる．ここで，$z = y_1' - y_2' + y_3' - y_4'$ とおくと，定理 2.3 より

$$\begin{aligned} \mathbb{Q}(C_8) &= \mathbb{Q}(y_1, y_2, y_3, y_4, y_1', y_2', y_3', y_4', z)^{\langle\sigma\rangle} \\ &= \mathbb{Q}(y_1, y_2, y_3, y_4, z)(y_1', y_2', y_3', y_4')^{\langle\sigma\rangle} \\ &= \mathbb{Q}(y_1, y_2, y_3, y_4, z)^{\langle\sigma\rangle}(z_1, z_2, z_3, z_4) \end{aligned}$$

となる $\sigma$ 不変な元 $z_1, z_2, z_3, z_4$ がとれる．

以下 $\mathbb{Q}(y_1, y_2, y_3, y_4, z)^{\langle\sigma\rangle}$ が非レトラクト有理的であることを示そう．$\zeta$ を 1 の原始 8 乗根とし，$\pi = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle\tau_t \mid t = 0, 1, \ldots, 7\rangle = \langle\tau_3, \tau_5\rangle \simeq C_2 \times C_2$ とする．ただし，$\tau_t : \zeta \mapsto \zeta^t$.

ここで，

$$\begin{aligned} Y_1 &= y_1 + \zeta^7 y_2 + \zeta^6 y_3 + \zeta^5 y_4 \\ Y_3 &= y_1 + \zeta^5 y_2 + \zeta^2 y_3 + \zeta^7 y_4 \\ Y_5 &= y_1 + \zeta^3 y_2 + \zeta^6 y_3 + \zeta y_4 \\ Y_7 &= y_1 + \zeta y_2 + \zeta^2 y_3 + \zeta^3 y_4 \\ Y_4 &= z \end{aligned}$$

とおくと，$\mathbb{Q}(C_8) = \mathbb{Q}(\zeta)^{\pi}(Y_1, Y_3, Y_4, Y_5, Y_7)^{\langle\sigma\rangle} = \mathbb{Q}(\zeta)(Y_1, Y_3, Y_4, Y_5, Y_7)^{\langle\sigma\rangle\times\pi}$ となる．このとき，$\sigma, \tau_t$ の $Y_i$ への作用は

$$\sigma : Y_i \mapsto \zeta^i Y_i,\quad \tau_t : Y_i \mapsto Y_{ti}$$

となる．ここで

$$C_1 = \frac{Y_3}{Y_1^3},\ C_2 = \frac{Y_5}{Y_1^2 Y_3},\ C_3 = \frac{Y_7}{Y_1^2 Y_5},\ C_4 = \frac{1}{Y_1 Y_7},\ C_5 = \frac{Y_4}{Y_1^4}$$

とすると，$\langle C_1, C_2, C_3, C_4, C_5\rangle$ は $\sigma$ の作用で不変であり，

$$\mathbb{Q}(\zeta)(Y_1, Y_3, Y_4, Y_5, Y_7)^{\langle\sigma\rangle\times\pi} = (\mathbb{Q}(\zeta)(Y_1, Y_3, Y_4, Y_5, Y_7)^{\langle\sigma\rangle})^{\pi} = \mathbb{Q}(\zeta)(C_1, C_2, C_3, C_4, C_5)^{\pi} = \mathbb{Q}(\zeta)(M)^{\pi}$$

となる．ここで，$M$ は $C_1, C_2, C_3, C_4, C_5$ から生成される $\pi$ 格子である．(本来は $\pi$ 格子 $M$ は加法的に書くべきであるが，今回は話の都合上乗法的に書いていることに注意する．) すると，$\tau_3, \tau_5$ の $C_i$ への作用は

$$\tau_3 : C_1 \mapsto \frac{C_2C_3C_4}{C_1^2},\ C_2 \mapsto \frac{C_2C_3}{C_1},\ C_3 \mapsto \frac{C_2C_4}{C_1},\ C_4 \mapsto \frac{C_3C_4}{C_1},\ C5 \mapsto \frac{C_2C_3C_4C_5}{C_1^3}$$
$$\tau_5 : C_1 \mapsto \frac{C_3^2C_4}{C_1C_2},\ C_2 \mapsto \frac{C_3C_4^2}{C_1C_2},\ C_3 \mapsto \frac{C_3C_4}{C_2},\ C_4 \mapsto \frac{C_3C_4}{C_1},\ C_5 \mapsto \frac{C_3^2C_4^2C_5}{C_1^2C_2^2}$$

となるから，$\tau_3, \tau_5$ の作用の $C_1, C_2, C_3, C_4, C_5$ に関する表現行列は

$$\left\langle \begin{pmatrix} -2 & 1 & 1 & 1 & 0 \\ -1 & 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 1 & 0 \\ -3 & 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 & 2 & 1 & 0 \\ -1 & -1 & 1 & 2 & 0 \\ 0 & -1 & 1 & 1 & 0 \\ -1 & 0 & 1 & 1 & 0 \\ -2 & -2 & 2 & 2 & 1 \end{pmatrix} \right\rangle$$

となる．ここで任意の $\pi$ の部分群 $\pi'$ に対し $H^1(\pi', M)$ を計算することで $M$ は coflabby であることがわかる ($G$ 格子のコホモロジーの計算法については 3.2 節を参照)．また $\hat{H}^1(\pi, M)$ を計算すると $\hat{H}^1(\pi, M') \simeq \mathbb{Z}/2\mathbb{Z}$ であることがわかるから，とくに $M$ は flabby でない．

ここで $M$ の flabby resolution を $0 \to M \to P \to F \to 0$ とし，$F$ が可逆格子であるとすると，$M$ は coflabby あるから命題 1.3 より $P \simeq M \oplus F$ となり $M$ が可逆格子である．しかし，これは $M$ は flabby でないことから矛盾である．したがって $F$ は可逆格子ではないから，$[M]^{fl}$ は可逆でないからよって，定理 2.10 から $\mathbb{Q}(\zeta)(M)^\pi$ は $\mathbb{Q}$ 上レトラクト有理的でない．

以上のことから $\mathbb{Q}(C_8)$ が $\mathbb{Q}$ 上レトラクト有理的ではないから，とくに有理的でもないことがわかる．

# 3 Appendix

## 3.1 Pushout，Pullback

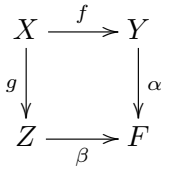
ここでは，$R$ を環とする．

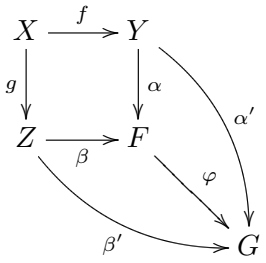
**定義** (pushout)**.** $f : X \to Y, g : X \to Z$ を $R$ 加群の準同型写像とする．このとき，$f, g$ の *pushout* とは，$R$ 加群 $F$ と $R$ 加群の準同型写像 $\alpha : Y \to F, \beta : Z \to F$ で次の条件をみたすものをいう：

・$\alpha \circ f = \beta \circ g$.

・$R$ 加群 $G$ と $R$ 準同型写像 $\alpha' : Y \to G, \beta : Z \to G$ が $\alpha' \quad \circ f = \beta' \circ g$ をみたすとき，$R$ 準同型写像 $\varphi : F \to G$ で $\alpha' = \varphi \circ \alpha, \beta' = \varphi \circ \beta$ をみたすものがただ 1 つ存在する．

**命題 3.1.** $f : X \to Y, g : X \to Z$ を $R$ 加群の準同型写像とし，$T = \{(f(x), -g(x)) \in Y \oplus Z \mid$




$x \in X\}$ とする．このとき，$(Y \oplus Z)/T$ と $\alpha(y) = (y, 0) + T, \beta(z) = (0, z) + T$ は $f, g$ の pushout である．

**証明.** $\alpha \circ f(x) = (f(x), 0) + T$, $\beta \circ g(x) = (0, g(x)) + T$ であるから，$\alpha \circ f = \beta \circ g$ が得られる．また，$R$ 加群 $G$ と $R$ 準同型写像 $\alpha' : Y \to G, \beta : Z \to G$ が $\alpha' \circ f = \beta' \circ g$ があったとき，$\varphi : F \to G$ を $\varphi((y, z) + T) = \alpha'(y) + \beta'(z)$ と定義すると，これは well-defined であり，$\alpha' = \varphi \circ \alpha, \beta' = \varphi \circ \beta$ であることが確認できる．また，$\psi : F \to G$ も $\alpha' = \psi \circ \alpha, \beta' = \psi \circ \beta$ をみたすとすると，$\varphi \circ \alpha = \psi \circ \alpha, \varphi \circ \beta = \psi \circ \beta$ であるから，

$$\psi((y, z) + T) = \psi(\alpha(y) + \beta(z) + T) = \varphi(\alpha(y) + \beta(z) + T) = \varphi((y, z) + T)$$

より，$\psi = \varphi$ が得られる． □

2 つの $R$ 加群の完全系列 $0 \to L \to M \to N \to 0, 0 \to L \to M' \to N' \to 0$ に対し pushout を考えることにより，次の完全系列の可換図式が得られる：

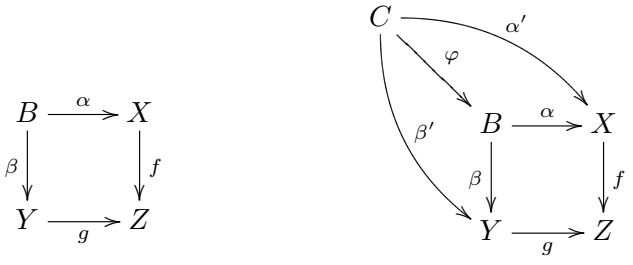
$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & L & \longrightarrow & M & \to & N & \to & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \to & M' & \to & F & \to & N & \to & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & N' & = & N' & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

**定義** (pullback)**.** $f : X \to Z, g : y \to Z$ を $R$ 加群の準同型写像とする．このとき，$f, g$ の *pullback* とは，$R$ 加群 $B$ と $R$ 加群の準同型写像 $\alpha : B \to X, \beta : B \to Y$ で次の条件をみたすものをいう：

・$f \circ \alpha = g \circ \beta$.

・$R$ 加群 $C$ と $R$ 準同型写像 $\alpha' : C \to X, \beta : C \to Y$ が $f \circ \alpha' = g \circ \beta'$ をみたすとき，$R$ 準同型写像 $\varphi : C \to B$ で $\alpha' = \alpha \circ \varphi, \beta' = \beta \circ \varphi$ をみたすものがただ 1 つ存在する．

**命題 3.2.** $f : X \to Z, g : y \to Z$ を $R$ 加群の準同型写像とする．このとき，$B = \{(x, y) \in X \times Y \mid f(x) = g(y)\}$ と $\alpha((x, y)) = x, \beta((x, y)) = y$ は $f, g$ の pullback である．




**証明.** 写像の定め方から $f \circ \alpha = g \circ \beta$ である．また，$R$ 加群 $C$ と $R$ 準同型写像 $\alpha' : C \to X, \beta : C \to Y$ が $f \circ \alpha' = g \circ \beta'$ を満たすとき，$\varphi : B \to C$ を $\varphi(c) = (\alpha'(c), \beta'(c))$ と定義すると，これは well-defined であり，$\alpha' = \alpha \circ \varphi, \beta' = \beta \circ \varphi$ であることが確認できる．また，$\psi : B \to C$ も $\alpha' = \alpha \circ \varphi, \beta' = \beta \circ \varphi$ をみたすとすると，$\varphi \circ \alpha = \psi \circ \alpha, \varphi \circ \beta = \psi \circ \beta$ であるから，$\psi = \varphi$ が得られる． □

2 つの $R$ 加群の完全系列 $0 \to L \to M \to N \to 0, 0 \to L' \to M' \to N \to 0$ に対し pullback を考えることにより，次の完全系列の可換図式が得られる：

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & L' & = & L' & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \to & L & \to & Y & \to & M' & \to & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \to & L & \to & M & \to & N & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

## 3.2 コホモロジー $(\hat{H}^{-1}, H^0, H^1)$ の計算法

ここでは，$G$ を有限群とし，$M$ を $\mathbb{Z}[G]$ 加群とする．

**定義** (テイトコホモロジー)**.** トレース写像 $T_G : M \to M$ を

$$T_G(m) = \sum_{g \in G} g \cdot m$$

とする．0 コサイクル，$-1$ コサイクルを

$$\begin{cases} \hat{Z}^{-1}(G, M) = \mathrm{Ker}(T_G), \\ \hat{Z}^0(G, M) = M^G \end{cases}$$

0 コバウンダリー，$-1$ コバウンダリーを

$$\begin{cases} \hat{B}^{-1}(G,M) = \sum_{g\in G}\{g\cdot m - m \mid m \in M\}, \\ \hat{B}^{0}(G,M) = \mathrm{Im}(T_G) \end{cases}$$

と定義する．このとき $n$ **次テイトコホモロジー**を

$$\hat{H}^n(G,M) = \begin{cases} H^n(G,M)\ (n \geq 1), \\ \hat{Z}^0(G,M)/\hat{B}^0(G,M)\ (n=0), \\ \hat{Z}^{-1}(G,M)/\hat{B}^{-1}(G,M)\ (n=-1), \\ H_{-n-1}(G,M)\ (n \leq -2) \end{cases}$$

で定義する．ここで $H_n$ は $n$ 次ホモロジー群である．

$G = \langle g_1, g_2, \ldots, g_r \rangle$，$M = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \oplus \cdots \oplus \mathbb{Z}u_n$ ($u_1, u_2, \ldots, u_n$ は $M$ の $\mathbb{Z}$ 基底) とする．

$H^1(G,M)$ を計算するには，$B^1(G,M)$ を $\mathbb{Z}$ 加群とみなして，$C^1(G,M)$ における単因子を計算すればよい．

$f \in Z^1(G,M)$ をとる．このとき 1 コサイクル条件から，任意の $G$ の元 $\sigma, \tau$ に対し $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$ が成り立つから，$f$ は $f(g_1), f(g_2), \ldots, f(g_r)$ の値によって決まる．すると，$Z^1(G,M)$ の $\mathbb{Z}$ 基底として，$f_{ij}(g_i) = m_j, f_{ij}(g_k) = 0\ (k \neq i)$ がとれる．ここで，$B^1(G,M) = \mathrm{Im}\ d^0 = \{d^0(m) \mid m \in M\}$ の $\mathbb{Z}$ 上の生成系として $d^0(u_1), d^0(u_2), \ldots, d^0(u_n)$ がとれる．このとき，

$$\begin{pmatrix} d^0(u_1) & d^0(u_2) & \cdots & d^0(u_n) \end{pmatrix} = \left(\begin{array}{c|c|c|c} g_1 - 1 & g_2 - 1 & \cdots & g_r - 1 \end{array}\right) \begin{pmatrix} & f_{ij} & \end{pmatrix}$$

であるから，

$$\left(\begin{array}{c|c|c|c} g_1 - 1 & g_2 - 1 & \cdots & g_r - 1 \end{array}\right)$$

の単因子を計算すればよい．

$H^0(G,M)$ を計算するためには，$\sum_{g\in G} g$ の単因子を計算すればよい．

$\hat{H}^{-1}(G,M)$ を計算するためには，$\hat{B}^{-1}(G,M)$ を $\mathbb{Z}$ 加群とみなして，$M$ における単因子を計算すればよい．任意の $m \in M$, $\sigma, \tau \in G$ に対し，$(\sigma\tau)m - m = \sigma(\tau m) - \tau m + \tau m - m \in \mathrm{Im}\ (\sigma - 1) + \mathrm{Im}\ (\tau - 1)$ となることから，$\hat{B}^{-1}(G,M) = \sum_{i=1}^{r} \mathrm{Im}\ (g_i - 1)$ となる．よって，$\sum_{i=1}^{r} \mathrm{Im}\ (g_i - 1)$ の単因子を計算すればよい．これは，行列表示をすると

$$\left(\begin{array}{c} g_1 - 1 \\ \hline g_2 - 1 \\ \hline \vdots \\ \hline g_r - 1 \end{array}\right)$$

となる．

## 参考文献


[Arn81] J. E. Arnold, Jr., *Homological algebra based on permutation modules*, J. Algebra **70** (1981) 250–260.

[EM73] S. Endo, T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973) 7–26.

[EM74] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85104.

[Len74] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974) 299–325.

[Lor05] M. Lorenz, *Multiplicative invariant theory*, Encyclopaedia Math. Sci., vol. 135, Springer-Verlag, Berlin, 2005.

[Sal84] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984) 165–215.

[Swa69] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969) 148–158.

[Vos74] Voskresenski, V. E. *Stable equivalence of algebraic tori*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974) 3–10.

[Yam12] A. Yamasaki, *Negative solutions to three-dimensional monomial Noether problem*, J. Algebra **370** (2012) 46–78.

# Flabby resolution の GAP による計算

山崎愛一

2019 年 9 月 7 日

## 目次



## 1 $GL(n,\mathbb{Z})$ の有限部分群

この章と次の章は, 私と星明考さんとの共著論文 [HY] の結果と計算機によるその具体的な計算例を主に扱う.

### 1.1 $n \leq 6$ のときの $GL(n,\mathbb{Z})$ の有限部分群の表の整備

各自然数 $n$ に対して, 共役でない $GL(n,\mathbb{Z})$ の有限部分群は有限個しかない. $n \leq 6$ のとき, 共役でない $GL(n,\mathbb{Q})$ の有限部分群の個数, 共役でない $GL(n,\mathbb{Z})$ の有限部分群の個数は次の表の通りである.

([BBNWZ78, PS00] 参照).

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $GL(n,\mathbb{Q})$ の有限部分群の個数 | 2 | 10 | 32 | 227 | 955 | 7103 |
| $GL(n,\mathbb{Z})$ の有限部分群の個数 | 2 | 13 | 73 | 710 | 6079 | 85308 |

.

$GL(4,\mathbb{Z})$ までの有限部分群の共役類については, [BBNWZ78] に完全な分類表が載っていて, 各共役類に番号付けがされている. また, 数式処理ソフト GAP には, 指定した番号の群を呼び出す組み込み関数が用意されている. `MatGroupZClass(n,i,j,k)` は番号 ($i$,$j$,$k$,$l$) に対応する群を返す.

しかし $GL(5,\mathbb{Z})$, $GL(6,\mathbb{Z})$ についてはそういうものが見当たらなかった. GAP の carat パッケージで一応 $GL(6,\mathbb{Z})$ まで扱えるようにはなっているが, crystcat パッケージで $GL(4,\mathbb{Z})$ の有限部分群を番号で指定するようなことは carat パッケージではできない. そこで私は $GL(5,\mathbb{Z})$,$GL(6,\mathbb{Z})$ について crystcat パッケージでやっているように分類表を整備し, 計算機上で呼び出せるようにした. 私は,carat パッケージ内の carat-2.1b1/tables/qcatalog.tar.gz を解凍してできる $GL(1,\mathbb{Q})$ から $GL(6,\mathbb{Q})$ までの有限部分群の表を用いて各群の生成元の一覧表を作った. qcatalog.tar.gz 内の qcatalog/data1 から qcatalog/data6 までが有限部分群の一覧で, qcatalog/dim1/フォルダから qcatalog/dim6/フォルダの中に各群の生成元等のデータが入っている. 私は perl でスクリプトを書いてそれらの表を整理した. cryst1.gap から cryst6.gap という名前のファイルで, それぞれ $GL(1,\mathbb{Q})$ から $GL(6,\mathbb{Q})$ の有限部分群の一覧が GAP で読めるリストの形になっている. このファイルは
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/GLnQ.zip` からダウンロードできる. これらのファイルを生成したときの perl スクリプトは
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/crystlst.pl` からダウンロードできる. 私が最初にこの作業をしたのが 2007 年 11 月ごろで, その当時の carat パッケージ (バージョン 2.1) での $GL(6,\mathbb{Q})$ の一覧表で, 同じ群が重複して数えられていたのを見つけた. (現在では修正されている).

次に整数行列からなる有限群 $G$ の $GL(n,\mathbb{Q})$ 共役類から $GL(n,\mathbb{Z})$ 共役類のリストを作る GAP パッケージ carat の関数 `ZClassRepsQClass(G)` を用いて, $GL(n,\mathbb{Z})$ の有限部分群の表を作った. cryst1.txt から cryst6.txt という名前のテキストファイルで,
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/crystdat.zip` からダウンロードできる.

$GL(n,\mathbb{Z})$ の有限部分群が与えられたとき, その群の $\mathbb{Q}$-共役類および $\mathbb{Z}$-共役類を [$n$,$m$], および [$n$,$m$,$l$] の形で表すことにする. $n$ は行列の次数,$m$ は qcatalog/data$n$ および cryst$n$.gap の $m$ 番目の $\mathbb{Q}$-共役類, $l$ は `ZClassRepsQClass(G)` の $l$ 番目の $\mathbb{Z}$-共役類を表すものとする. $G$ からその群の $\mathbb{Q}$-共役類および $\mathbb{Z}$-共役類を求めるプログラムを作った. gap 版は caratnumber.gap, magma 版は caratnumber.magma で, どちらも
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/` からダウンロードできる.
すなわち, それぞれ
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/caratnumber.gap`
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/caratnumber.magma`
からダウンロードできる. GAP 版は ubuntu linux 12.04LTS 上で GAP4.4.12 でプログラムした. (その後少し修正を加えることで現在では ubuntu linux 18.04LTS 上の GAP4.9.3 でも動くようになっている). 生成元の表以外に, 行列の特性多項式の表および $-1,0,1$ 次の Tate コホモロジーの表も用いている. そのた

め,crystdat.zip も解凍しておく必要がある.

例えば,G が各行各列に 0 でない成分が一つずつあって ±1 であるようなもの全体からなる 6 次の群 (位数 $6! \times 2^6$) の例を示す. gap の場合,

```
gap> Read("caratnumber.gap");
gap> CaratQClassNumber(G);
[ 6, 2773 ]
gap> CaratZClassNumber(G);
[ 6, 2773, 1 ]
```

magma の場合,

```
> load"caratnumber.magma";
Loading "caratnumber.magma"
Loading "cryst1.txt"
Loading "cryst2.txt"
Loading "cryst3.txt"
Loading "cryst4.txt"
Loading "cryst5.txt"
Loading "cryst6.txt"
Loading "caratchpol.txt"
Loading "H1cryst.txt"
Loading "carat2crystcat.txt"
> CaratQClassNumber(G);
[ 6, 2773 ]
> CaratZClassNumber(G);
[ 6, 2773, 1 ]
```

逆に, 指定された群番号を持つ群を構成するには, caratnumber.gap 又は caratnumber.magma を読み込んだ状態で, gap ならば

```
gap> G:=CaratMatGroupZClass(6,2773,1);
```

magma ならば

```
> G:=CaratMatGroupZClass(6,2773,1);
```

とすればよい. どちらも実際に入力するのは

```
G:=CaratMatGroupZClass(6,2773,1);
```

の部分だけである.

## 1.2 直既約分解の一意性の成否

**定義 1.** $G$ を $GL(n,\mathbb{Z})$ の有限部分群とする．対応する rank $n$ の $G$-格子 $M_G$ を次のように定義する．$\{u_1,\dots,u_n\}$ を $\mathbb{Z}$-基底とし, $\sigma=[a_{i,j}]\in G$ に対して $\sigma(u_i)=\sum_{j=1}^{n}a_{i,j}u_j$ で $\sigma$ の作用を定める．

**定義 2.** $M$ を $G$-格子とする．$M=M_1\oplus M_2$ の形に二つの $G$-格子の直和に書けるとき直可約, そうでないとき直既約であるという．$M$ が $\mathbb{Z}$-加群として $M=M_1\oplus M_2$ の形に書けて $M_1,M_2$ のうち少なくとも一方が $M$ の部分 $G$-格子になっているとき可約, そうでないとき既約であるという．

$M$ が既約ならば直既約であるが, 逆は必ずしも成り立たない．

**例 1.** $GL(2,\mathbb{Z})$ の位数 *2* の二つの部分群 $G_1=\left\langle\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\rangle$, $G_2=\left\langle\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\rangle$ を考える．それぞれ群番号 *(GAP ID)* は *(2,2,1,1), (2,2,1,2)* である．二つの群は $\mathbb{Q}$ 共役 *(*すなわち $GL(2,\mathbb{Q})$ の中で共役*)* だが, $\mathbb{Z}$ 共役でない *(*すなわち $GL(2,\mathbb{Z})$ の中で共役でない*)*. 対応する $G_1$-格子 $M_{G_1}$ については可約かつ直可約である．しかし $G_2$-格子 $M_{G_2}$ については, 可約だが直可約ではない．

$n\le 6$ について, $M_G$ の直既約分解がどうなっているかを計算機を用いて調べた．$G$ を $GL(n,\mathbb{Z})$ の有限部分群, $M_G$ を対応する $G$-格子とする．$n\le 4$ のときは $M_G$ は一意的に直既約分解できる．一方 $n\ge 5$ では $M_G$ が二通りに直既約分解できる場合がある．計算結果は,$n\le 4$ のときのデータは
`https://www.math.kyoto-u.ac.jp/~yamasaki/MultInvField/Glattice.dat`
からダウンロードできる．$n=5$ のときのデータは
`https://www.math.kyoto-u.ac.jp/~yamasaki/MultInvField/Glattice5.dat`
から,$n=6$ のときのデータは
`https://www.math.kyoto-u.ac.jp/~yamasaki/MultInvField/Glattice6.dat`
からそれぞれダウンロードできる．

**例 2.** $GL(5,\mathbb{Z})$ の有限部分群 $G$ で $M_G$ が二通りに直既約分解できるものは全部で *11* 個ある．いずれも $M_G\simeq M_1\oplus M_2\simeq N_1\oplus N_2$, rank $M_1=4$, rank $M_2=1$, rank $N_1=3$, rank $N_2=2$ の形に二通りに直既約分解できる．

$$X=\left(\begin{array}{cccc|c}0&1&0&1&0\\1&0&0&1&0\\0&0&0&1&0\\0&0&-1&-1&0\\\hline 0&0&0&0&1\end{array}\right),\quad Y=\left(\begin{array}{cccc|c}1&0&0&0&0\\0&1&0&0&0\\0&0&0&-1&0\\0&0&-1&0&0\\\hline 0&0&0&0&1\end{array}\right).$$

とおく．*5* 次の単位行列を $I$ と書く．このとき *11* 個の群は下表の通りである．

| $G$ | $CARAT\ ID$ | 生成元 |
|---|---|---|
| $S_3 \times C_2 \simeq D_6$ | $(5, 188, 4)$ | $\langle X^2, XY, -I\rangle$ |
| $C_2 \times C_6$ | $(5, 189, 4)$ | $\langle X, -I\rangle$ |
| $D_6$ | $(5, 190, 6)$ | $\langle -X, Y\rangle$ |
| $D_6$ | $(5, 191, 6)$ | $\langle -X, XY\rangle$ |
| $D_6$ | $(5, 192, 6)$ | $\langle X, Y\rangle$ |
| $D_6$ | $(5, 193, 4)$ | $\langle X, -Y\rangle$ |
| $D_6 \times C_2$ | $(5, 205, 6)$ | $\langle X, Y, -I\rangle$ |
| $S_3$ | $(5, 218, 8)$ | $\langle X^2, XY\rangle$ |
| $S_3$ | $(5, 219, 8)$ | $\langle X^2, -XY\rangle$ |
| $C_6$ | $(5, 220, 4)$ | $\langle X\rangle$ |
| $C_6$ | $(5, 221, 4)$ | $\langle -X\rangle$ |

このとき,$X, Y$ の行列の形から $M_G$ は rank 4 と rank 1 の $G$-格子の直和に分かれることがわかる. 一方で $P = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ とおくと,

$$P^{-1}XP = \left(\begin{array}{ccc|cc} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right), \quad P^{-1}YP = \left(\begin{array}{ccc|cc} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

となり,$M_G$ は rank 3 と rank 2 の $G$-格子の直和にも分かれることがわかる.

*GAP* 上で $n = 5$ のときのデータ `Glattice5.dat` を読み込んで, $M_G$ が rank $4+1$ にも rank $3+2$ にも直和分解できる *11* 個の $G$ の *CARAT ID* を確かめることもできる.

```
gap> Read("Glattice5.dat");
gap> Intersection(e41,e32);
[ [ 5, 188, 4 ], [ 5, 189, 4 ], [ 5, 190, 6 ], [ 5, 191, 6 ], [ 5, 192, 6 ],
  [ 5, 193, 4 ], [ 5, 205, 6 ], [ 5, 218, 8 ], [ 5, 219, 8 ], [ 5, 220, 4 ],
  [ 5, 221, 4 ] ]
```

$M_G$ が rank $4+1$ に直和分解できる $G$ の *CARAT ID* のリストが `e41`, $M_G$ が rank $3+2$ に直和分解できる $G$ の *CARAT ID* のリストが `e32` なので, 二つのリストの *intersection* を取ることにより, 両方に属する *11* 個の $G$ の *CARAT ID* が得られる.

## 2 rank 5 以下の $G$-格子の flabby 類の可逆性

### 2.1 rank $2, 3$ のとき (Voskresenskii, Kunyavskii)

rank 2 の $G$-格子の flabby 類は Voskresens によってすべて 0 であることが示された [Vos67].

rank 3 の $G$-格子の flabby 類の可逆性は Kunyavskii によって解かれた [Kun90]. $G$ が下表の 15 個の群のどれかであれば flabby 類は可逆でないが, それ以外であれば 0 である.

[Kun90] と [HY] では行列の作用を縦に見るか横に見るかが逆になっているため $G$ の転置をとる必要がある.

| ${}^tG$ in [Kun90] | GAP ID | $G$ |
|---|---|---|
| $U_1$ | $(3,3,1,3)$ | $C_2^2$ |
| $U_2$ | $(3,3,3,3)$ | $C_2^3$ |
| $U_3$ | $(3,4,4,2)$ | $D_4$ |
| $U_4$ | $(3,4,6,3)$ | $D_4$ |
| $U_5$ | $(3,7,1,2)$ | $A_4$ |
| $U_6$ | $(3,4,7,2)$ | $D_4 \times C_2$ |
| $U_7$ | $(3,7,2,2)$ | $A_4 \times C_2$ |
| $U_8$ | $(3,7,3,3)$ | $S_4$ |
| $U_9$ | $(3,7,3,2)$ | $S_4$ |
| $U_{10}$ | $(3,7,4,2)$ | $S_4$ |
| $U_{11}$ | $(3,7,5,3)$ | $S_4 \times C_2$ |
| $U_{12}$ | $(3,7,5,2)$ | $S_4 \times C_2$ |
| $W_1$ | $(3,4,3,2)$ | $C_4 \times C_2$ |
| $W_2$ | $(3,3,3,4)$ | $C_2^3$ |
| $W_3$ | $(3,7,2,3)$ | $A_4 \times C_2$ |

## 2.2 rank $4,5$ のときの計算プログラム

そこで rank $4,5$ の $G$-格子すべてについて flabby class$[M_G]^{fl}$ が 0 になるか可逆になるかを決定した。そのための GAP のプログラムは gap 版は FlabbyResolution.gap で,
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/FlabbyResolution.gap`
からダウンロードできる. (その後プログラムに改良を加えたものが FlabbyResolutionFromBase.gap で,
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbNorm1Tori/FlabbyResolutionFromBase.gap`

からダウンロードできる).

## 2.3 flabby resolution の構成

$G$ を $GL(n,\mathbb{Z})$ の有限部分群, $M = M_G$ を対応する $G$-格子とする. $M$ の flabby resolution $0 \to M \to P \to F \to 0$ で rank $F$ がなるべく小さいものを求めたい. $0 \to Q \to R \to M^\circ \to 0$ を $M^\circ = \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ の coflabby resolution とする. すなわち $R$ は置換格子で $Q$ は coflabby とする. この完全系列の双対写像 $0 \to M \to \mathrm{Hom}_{\mathbb{Z}}(R,\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(Q,\mathbb{Z}) \to 0$ を取ることにより $M$ の flabby resolution を得る.

そこで $M^\circ$ の coflabby resolution を構成することを考える. $P^\circ$ を置換 $G$-格子, $P^\circ \xrightarrow{f} M^\circ$ を $G$-準同形とする. $G$ の部分群 $H$ に対し,

$$(P^\circ)^H \xrightarrow{f|_{(P^\circ)^H}} (M^\circ)^H \to 0 \text{ は完全系列} \tag{1}$$

が成り立つとする. このとき $\widehat{H}^0(H,P^\circ) \to \widehat{H}^0(H,M^\circ)$ は全射になる. $Q = \ker f$ とおくと,$\widehat{H}^1(H,Q) = 0$ が成り立つ. $M^\circ$ の coflabby resolution を得るためには置換 $G$-格子 $P^\circ$ と $G$ 準同形 $f$ で (1) が $G$ のすべての部分群 $H$ に対して成り立つようなものを構成できれば十分である.

$Q = \ker f$ の rank をなるべく小さくしたいのであるが, そのためにはなるべく小さな rank の置換 $G$-格子 $P^\circ$ を構成できればよい. いろいろ工夫して $P^\circ$ が小さくなるように GAP 上でプログラムを組んで, flabby resolution が計算機上で計算できるようにした.
`FlabbyResolution(G)` は $M_G$ の flabby resolution を返す:
`FlabbyResolution(G).actionP` は $P$ への $G$ の作用の行列表現を返す;

`FlabbyResolution(G).actionF` は $F$ への $G$ の作用の行列表現を返す;
`FlabbyResolution(G).injection` は単射 $\iota : M_G \to P$ の行列表現を返す;
`FlabbyResolution(G).surjection` は全射 $\phi : P \to F$ の行列表現を返す.

**例 3.** $G = \left\langle \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right) \right\rangle \simeq C_3$ のとき, $[M_G]^{fl} = 0$ であることが以下の計算により示される.

```
Read("FlabbyResolution.gap");

gap> G:=Group([[[0,1],[-1,-1]]]);
Group([ [ [ 0, 1 ], [ -1, -1 ] ] ])
gap> FlabbyResolution(G);
rec( injection := [ [ 1, 0, -1 ], [ 0, -1, 1 ] ],
  surjection := [ [ 1 ], [ 1 ], [ 1 ] ],
  actionP := Group([ [ [ 0, 0, 1 ], [ 1, 0, 0 ], [ 0, 1, 0 ] ] ]),
  actionF := Group([ [ [ 1 ] ] ]) )
gap> FlabbyResolution(G).actionF; # F is trivial of rank 1
Group([ [ [ 1 ] ] ]) )
```

この計算で得られた *flabby resolution*

$$0 \to M_G \to P \to F \to 0$$

で $P$ と $F$ の rank はそれぞれ *3,1* である. $M_G$,$P$,$F$ の基底をそれぞれ $\{m_1, m_2\}$,$\{p_1, p_2, p_3\}$,$\{f_1\}$ とおく. $G$ の生成元 $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ を $\sigma$ とおく.
$\sigma$ の $P$ への作用の行列表現は $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $F$ への作用の行列表現は $\left(1\right)$ である. すなわち,$P$ には基底の置換作用 $p_1 \mapsto p_3 \mapsto p_2 \mapsto p_1$ として作用し, $F$ には自明に作用する. 単射 $\iota : M_G \to P$ の行列表現は $\left(\begin{smallmatrix} 1 & 0 & -1 \\ 0 & -1 & 1 \end{smallmatrix}\right)$, 全射 $\phi : P \to F$ の行列表現は $\left(\begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix}\right)$ である. すなわち $\iota(m_1) = p_1 - p_3, \iota(m_2) = -p_2 + p_3$, $\phi(p_i) = f_1\,(i = 1, 2, 3)$ である.

## 2.4 $[M_G]^{fl}$ の可逆性

$[M_G]^{fl}$ が可逆かどうか決定するのは比較的簡単である. 次の補題を用いる.

**補題 1** ([Len74, Proposition 1.1, Proposition 1.2] および [Swa83, Section 8])**.** $E$ を可逆 $G$-格子とする. そのとき
(i) $E$ は *flabby* かつ *coflabby*.
(ii) $C$ が *coflabby* $G$-格子のとき, 任意の *short exact sequence* $0 \to C \to N \to E \to 0$ は分裂する.

$G$-格子 $M$ が与えられたとき, まず $M$ の flabby resolution

$$0 \to M \to P \to F \to 0$$

を取る. もし $F$ が coflabby でなければ $[M]^{fl}$ は可逆ではない. $F$ が coflabby のとき,$F$ の flabby resolution

$$0 \to F \xrightarrow{\iota} Q \to E \to 0. \tag{2}$$

を取る. このとき補題 1 より $[M]^{fl}$ が可逆 $\Leftrightarrow$ $F$ が可逆 $\Leftrightarrow$ (2) が分裂する. 従って $[M]^{fl}$ が可逆かどうか判定するためには (2) が分裂するかどうかすなわち $\pi : Q \to F$ で $\pi \circ \iota = \mathrm{id}_F$ が成り立つような $\pi$ が存在するかどうかを調べればよい. これは整数係数の連立一次方程式に帰着されるので計算機上で実行できる.

`IsInvertibleF(G)` は $[M_G]^{fl}$ が可逆かどうかを返す.

## 2.5 $[M_G]^{fl} = 0$ の可能性

$[M_G]^{fl}$ が可逆とする. 直既約置換 $G$-格子の各同型類は $G$ の部分群 $H$ の共役類と一対一に次のように対応する. $H \leftrightarrow \mathbb{Z}[G/H]$. $H_1, \ldots, H_r$ を,$G$ の部分群の共役類を, GAP の関数 `ConjugacyClassesSubgroups2(G)` が返す順番と同じ順番に並べたものとする. (`ConjugacyClassesSubgroups2(G)` は GAP のバージョンが同じであれば特定の $G$ に対していつも同じ値を返すが, GAP のバージョンが異なれば返す値も異なってくる. [HY] では GAP 4.4.12 で計算している.). $[F] = 0$ とする. $x_{r+1} = \pm 1$ に対して, $(\bigoplus_{i=1}^{r} \mathbb{Z}[G/H_i]^{\oplus x_i}) \oplus F^{\oplus x_{r+1}} \simeq \bigoplus_{i=1}^{r} \mathbb{Z}[G/H_i]^{\oplus y_i}$. が成り立つ. $a_i = x_i - y_i$,$b_1 = x_{r+1}$ とおくと $b_1 = \pm 1$,

$$\bigoplus_{i=1}^{r} \mathbb{Z}[G/H_i]^{\oplus a_i} \simeq F^{\oplus(-b_1)}. \tag{3}$$

が成り立つ.

いくつかの不変量を計算することにより, $a_1, \ldots, a_r, b_1$ の可能性を絞ることができる.

`PossibilityOfStablyPermutationF(G)` は $a_1, \ldots, a_r, b_1$ の値の可能性を返す. $\mathcal{L} = \{l_1, \ldots, l_s\}$ が返ってきたとき, $a_1, \ldots, a_r, b_1$ の値は必ず $l_1, \ldots, l_s$ の $\mathbb{Z}$ 係数一次結合でなければならない.

**例 4.** rank 4 の代数的トーラスで $G$ の *GAP ID* が *(4,31,1,3)* と *(4,31,1,4)* の場合を計算する. どちらの場合も $G$ の位数は *20* である.

```
Read("FlabbyResolution.gap");

gap> G:=MatGroupZClass(4,31,1,3);; # G=F20
gap> Rank(FlabbyResolution(G).actionF.1); # F is of rank 16
16
gap> IsInvertibleF(G);
true
gap> List(ConjugacyClassesSubgroups2(G),x->StructureDescription(Representative(x)));
[ "1", "C2", "C4", "C5", "D10", "C5 : C4" ]
gap> PossibilityOfStablyPermutationF(G); # checking [M]^{fl}: non-zero
[ [ 1, 1, 0, 1, -1, 0, -2 ] ]

gap> G:=MatGroupZClass(4,31,1,4);; # G=F20
gap> Rank(FlabbyResolution(G).actionF.1); # F is of rank 16
16
gap> IsInvertibleF(G);
true
gap> List(ConjugacyClassesSubgroups2(G),x->StructureDescription(Representative(x)));
```

```
[ "1", "C2", "C4", "C5", "D10", "C5 : C4" ]
gap> PossibilityOfStablyPermutationF(G); # checking [M]^{fl}: non-zero
[ [ 1, 1, 0, 1, -1, 0, -2 ] ]
```

$[M_G]^{fl}$ は可逆だが 0 ではない．これは rank 3 の *Kunyavskii* の結果には現れなかった現象である．

## 2.6 $[M_G]^{fl} = 0$ の証明

具体的に (3) の同型写像を構成できれば $[M_G]^{fl} = 0$ の証明ができる．しかし $G$ によっては (3) の両辺の rank がかなり大きくなってしまうので, 工夫して計算量を減らす必要がある．rank 5 までの代数的トーラスの中で一番大変だったのは $G$ の CARAT ID が (5,946,4) の場合で, (3) の両辺の rank が 88 にもなる．

この場合は GAP での計算だけでは同型写像を構成することはまず不可能で, C 言語による並列計算 (OpenMP) で計算機を何日間も動かした結果やっと同型写像が得られた．[HY] にはこの同型写像を構成するためのデータが具体的に書いてあるので, それを使えば $[M_G]^{fl} = 0$ が成り立つことの検算ができる．ただし, そのときの GAP のバージョンは 4.4.12 でなければならない．(GAP のバージョンが異なれば `ConjugacyClassesSubgroups2(G)` の値が変わり, 構成すべき同型写像の表現行列の具体的な形も変わってしまうからである).

## 2.7 rank $= 4, 5$ のときの結果

$T$ を rank 4 または 5 の代数的トーラスとする．対応する $G$-格子 $M$ が直可約なとき $M = M_1 \bigoplus M_2$ と書いたとき, 少なくとも一方は rank が 2 以下である．rank $M_2 = 2$ とすると, $[M]^{fl} = [M_1]^{fl}$ が成り立つ．従って $M$ が直可約なときはより rank が小さい場合に帰着される．$M$ が直既約の場合が本質的である．

rank 4 の直既約な $GL(4, \mathbb{Z})$ の有限部分群は全部で 295 個ある．rank 5 の直既約な $GL(5, \mathbb{Z})$ の有限部分群は全部で 1452 個ある．

**定理 1.** rank 4 の直既約 $G$-格子について, $[M_G]^{fl}$ は可逆だが 0 でないのは次の 7 つの場合だけである．

| *GAP ID* | *G* | *GAP ID* | *G* |
|---|---|---|---|
| $(4, 31, 1, 3)$ | $F_{20}$ | $(4, 31, 5, 2)$ | $S_5$ |
| $(4, 31, 1, 4)$ | $F_{20}$ | $(4, 31, 7, 2)$ | $C_2 \times S_5$ |
| $(4, 31, 2, 2)$ | $C_2 \times F_{20}$ | $(4, 33, 2, 1)$ | $C_3 \rtimes C_8$ |
| $(4, 31, 4, 2)$ | $S_5$ | | |

また,$[M_G]^{fl}$ が可逆でないものは全部で *152* 個ある．

**定理 2.** rank 5 の直既約 $G$-格子について, $[M_G]^{fl}$ は可逆だが 0 でないのは存在しない．$[M_G]^{fl}$ が可逆でないものは全部で *1141* 個ある．

[HY] には $L(M)^G$ が retract rational でないときの $G$ の群番号のリストが載っているが, 量が膨大になるのでここでは省略している．

また FlabbyResolution.gap にはここでは紹介していない関数がたくさんあり, それらも [HY] では解説している．

# 3　必要なソフトのインストール方法

## 3.1　linux への GAP 4.4.12 のインストール

筆者は ubuntu linux 12.04LTS, 18.04LTS 上で GAP 4.4.12 をインストールした. ほかのバージョンやディストリビューションの linux でも (あるいは macOS でも) 動く可能性があるが, 筆者は検証していない.

`http://www.gap-system.org/Releases/4.4.12.html` から必要なファイル gap4r4p12.tar.gz, packages-2012_07_27-09_32_UTC.tar.gz, xtom1r1p4.tar.gz をダウンロードする. たとえば ∼/Downloads のフォルダにダウンロードしたとする.

ここではホームフォルダ ∼/にインストールするものとして説明する. ホームフォルダに移動して gap4r4p12.tar.gz を解凍する.

```
cd
tar xvzf ~/Downloads/gap4r4p12.tar.gz
```

gap4r4 のフォルダが作成され, その下にファイルが展開される.

そして

```
cd ~/gap4r4/pkg
tar xvzf ~/Downloads/packages-2012_07_27-09_32_UTC.tar.gz
```

を実行する.

```
cd
tar xvzf ~/Downloads/xtom1r1p4.tar.gz
```

を実行する.

gap のフォルダに移動して GAP をコンパイルする. すなわち

```
cd ~/gap4r4
./configure
make
```

を実行する. ”Please install m4 or build without GMP.”というメッセージが表示された場合は m4 をインストールする. すなわち

```
sudo apt install m4
```

を実行する. パスワードを尋ねられたら,ubuntu の場合は自分のログインパスワードを入力する. そして,GAP のコンパイルをやりなおす.

GAP が正しくコンパイルされたならば

```
~/gap4r4/bin/gap.sh
```

を実行すると GAP が立ち上がるはずである. カレントフォルダがどこであっても

```
gap4.4.12
```

と入力するだけで GAP 4.4.12 が立ち上がるように設定するには bin/gap.sh を path の通ったフォルダ (/usr/local/bin など) にコピーすればよい.

```
sudo cp bin/gap.sh /usr/local/bin/gap4.4.12
```

パスワードを尋ねられたら,ubuntu の場合は自分のログインパスワードを入力する.

## 3.2 GAP のパッケージのインストール

GAP のパッケージによってはさらにインストールをしないと使えないものがる. 例えば nq はコンパイルが必要である. カレントフォルダが GAP をインストールしたフォルダにあるとして, nq をコンパイルするには次のようにすればよい.

```
cd /gap4r4/pkg/nq-2.3
./configure
make
```

ほかのパッケージについても, まず該当するパッケージのフォルダに移動してから README ファイルを読んでそこに書いてある通りにインストール作業をすればよい.

## 3.3 carat のインストール

carat のインストールはほかのパッケージと比べて少し複雑な上に, 場合によっては設定を変更する必要があるので解説する.

まず

```
https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbAlgTori/RatProbAlgTori.zip
```

をダウンロードする. たとえば ~/Downloads のフォルダにダウンロードしたとする.

ホームフォルダに移動して RatProbAlgTori.zip を解凍する.

```
cd
unzip ~/Downloads/RatProbAlgTori.zip
```

RatProbAlgTori のフォルダが作成され, その下にファイルが展開される.

RatProbAlgTori のフォルダに移動して, BuildPackages.sh に実行権限を与える. すなわち

```
cd ~/RatProbAlgTori
chmod +x BuildCarat.sh
```

を実行する.

~/gap4r8/pkg に移動して BuildCarat.sh を実行する. すなわち

```
cd ~/gap4r8/pkg
```

```
~/RatProbAlgTori/BuildCarat.sh
```

## 3.4 caratnumber のインストール

`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/` から caratnumber.gap と crystdat.zip をダウンロードする.

自分が GAP のプログラムをよく保存するフォルダ (例えば ~/data/gap/など) に caratnumber.gap をコピーし, crystdat.zip を解凍する.

そのフォルダに移動して GAP を起動して,

```
gap> Read("caratnumber.gap");
```

とすれば caratnumber が使えるようになる.

## 3.5 より新しいバージョンの GAP の場合

GAP 4.4.12 は長く使われていたバージョンで安定しているので GAP 4.4.12 をインストールする手順を今まで説明した.

GAP 4.4.12 までと GAP 4.5 以降ではかなり変更されている部分がある. GAP 4.5, 4.6 は不安定であったが, 最近のバージョンではまた安定してきている. ここでは GAP 4.9.3 を例にインストール手順を説明する.

`https://www.gap-system.org/Releases/4.9.3.html` から gap-4.9.3.tar.gz をダウンロードする. たとえば ~/Downloads のフォルダにダウンロードしたとする.

ここではホームフォルダ ~/にインストールするものとして説明する. ホームフォルダに移動して gap-4.9.3.tar.gz を解凍する.

```
cd
tar xvzf ~/Downloads/gap-4.9.3.tar.gz
```

gap-4.9.3 のフォルダが作成され, その下にファイルが展開される.

gap のフォルダに移動して GAP をコンパイルする. すなわち

```
cd ~/gap-4.9.3
./configure
make
```

を実行する. "Please install m4 or build without GMP."というメッセージが表示された場合は m4 をインストールする. すなわち

```
sudo apt install m4
```

を実行する. パスワードを尋ねられたら,ubuntu の場合は自分のログインパスワードを入力する. そして,GAP のコンパイルをやりなおす.

~/gap-4.9.3/pkg に移動する. そして ~/gap-4.9.3/bin/BuildPackages.sh を実行してパッケージをまとめてインストールする. すなわち

```
cd ~/gap-4.9.3/pkg
../bin/BuildPackages.sh
```

を実行する.

```
https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbAlgTori/RatProbAlgTori.zip
```

をダウンロードする. たとえば ∼/Downloads のフォルダにダウンロードしたとする.
ホームフォルダに移動して RatProbAlgTori.zip を解凍する.

```
cd
unzip ~/Downloads/RatProbAlgTori.zip
```

RatProbAlgTori のフォルダが作成され, その下にファイルが展開される.
RatProbAlgTori のフォルダに移動して, BuildPackages.sh に実行権限を与える. すなわち

```
cd ~/RatProbAlgTori
chmod +x BuildCarat.sh
```

を実行する.
∼/gap-4.9.3/pkg に移動して BuildCarat.sh を実行する. すなわち

```
cd ~/gap-4.9.3/pkg
~/RatProbAlgTori/BuildCarat.sh
```

## 参考文献


[BBNWZ78] H. Brown, R. Bülow, J. Neubüser, H. Wondratschek, H. Zassenhaus. *Crystallographic Groups of Four-Dimensional Space*, John Wiley, New York, 1978.

[Bro82] K. S. Brown, *Cohomology of Groups*, Grad. Texts in Math., vol. 87, Springer-Verlag, 1972.

[Carat] J. Opgenorth, W. Plesken, T. Schulz, CARAT, GAP 4 package, version 2.2.3 (2018), based on CARAT 2.1b1; available at `https://www.math.uni-bielefeld.de/~gaehler/gap45/packages.php`.

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. (http://www.gap-system.org).

[HY] A. Hoshi and A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. 248 (2017) no. 1176, v+215 pp., arXiv: 1210.4525.

[Kun90] B. E. Kunyavskii, *Three-dimensional algebraic tori*, Selecta Math. Soviet. **9** (1990) 1–21.

[Len74] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974) 299–325.

[PS00] W. Plesken, T. Schulz, *Counting crystallographic groups in low dimensions*, Exp. Math. **9** (2000) 407–411.

[Swa83] R. G. Swan, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (Bryn Mawr,

Pa., 1982), 21–40, Springer, New York-Berlin, 1983.

[Vos67] V. E. Voskresenskii, *On two-dimensional algebraic tori II*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967) 711–716; translation in Math. USSR-Izv. **1** (1967) 691–696.

# 半単項式作用と有理性問題

新潟大学理学部　星 明考
Akinari Hoshi, Department of Mathematics, Niigata University [1]

**概要**　この原稿は第 27 回整数論サマースクール (2019 年 9 月) の講演のレジメです．この講演では，半単項式作用の概念を導入し，その不変体の有理性問題に関する結果を (ほとんど証明なしに) 紹介していきます．

**謝辞.** 10 回目の参加の今回は，世話人としての参加でした．世話人の一人として，参加して下さった皆様に心より感謝申し上げます．また，これまで重要な示唆と数多くのアドバイスを下さった Ming-chang Kang 氏，遠藤静男氏にこの場を借りて御礼申し上げます．

## 目 次



## 1　半単項式作用と不変体の有理性問題

### 1.1　基本的な定義と例

**定義 1.1.** $K/k$, $L/k$ を体の有限生成な拡大とする．
(1) $K$ が $k$ 上**有理的** (rational over $k$, $k$-rational) であるとは，$K$ が $k$ 上純超越的であること．すなわち，$K \simeq k(x_1, \ldots, x_n)$ ; $k$ 上の $n$ 変数有理関数体．
(2) $K$ が $k$ **上安定有理的** (stably $k$-rational) とは，$K$ 上代数的独立な元 $y_1, \ldots, y_m$ に対して，$K(y_1, \ldots, y_m)$ が $k$ 上有理的であること．
(3) $K$ と $L$ が**安定 $k$ 同型** (stably $k$-isomorphic) であるとは，$K$ 上代数的独立な元 $y_1, \ldots, y_m$ と $L$ 上代数的独立な元 $z_1, \ldots, z_n$ に対して，$K(y_1, \ldots, y_m)$ と $L(z_1, \ldots, z_n)$ が $k$ 同型となること．
(4) $k$ が無限体のとき，$K$ が $k$ **上レトラクト有理的** (retract $k$-rational) とは，$k$ 代数 (整域)$A \subset K$ が存在して，(i) $K$ は $A$ の商体 ; (ii) $f \in k[x_1, \ldots, x_n]$ と $k$ 代数の準同型 $\varphi\colon A \to k[x_1, \ldots, x_n][1/f]$, $\psi\colon k[x_1, \ldots, x_n][1/f] \to A$ が存在し，$\psi \circ \varphi = 1_A$，をみたすこと．
(5) $K$ が $k$ **上単有理的** ($k$-unirational) とは，$K$ が $k$ 上有理的な体の部分体となること．

無限体 $k$ に対して，“$k$ 上有理的”⇒“$k$ 上安定有理的”⇒ “$k$ 上レトラクト有理的”⇒“$k$ 上単有理的”となる．

[1] 本研究は科研費 19K03418 の助成を受けています．

**定義 1.2.** $k$ を体，$K/k$ を有限次拡大，$K(x_1,\dots,x_n)$ を $K$ 上の $n$ 変数有理関数体とする．$G \leq \mathrm{Aut}_k(K(x_1,\dots,x_n))$ を有限部分群とする．
(1) $G$ の $K(x_1,\dots,x_n)$ への作用が**半単項式作用** (quasi-monomial action) であるとは，次の条件をみたすこと：
(i) $\sigma(K) \subset K$ $(\sigma \in G)$;
(ii) $K^G = k$. ただし，$K^G$ は $K$ の $G$ 作用による不変体 ;
(iii) $\sigma \in G$ と $1 \leq j \leq n$ に対して，

$$\sigma(x_j) = c_j(\sigma) \prod_{i=1}^{n} x_i^{a_{ij}} \tag{1}$$

ただし，$c_j(\sigma) \in K^\times$ かつ $[a_{ij}]_{1\leq i,j\leq n} \in GL_n(\mathbb{Z})$.
(2) 半単項式作用は，すべての $c_j(\sigma) = 1$ となるとき，**純半単項式作用** (purely quasi-monomial action) という．
(3) 半単項式作用は，$G$ の $K$ への作用が自明，すなわち $k = K$ のとき，**単項式作用** (monomial action) という．
(4) 半単項式作用は，純半単項式作用かつ単項式作用であるとき，**純単項式作用** (purely monomial action) という．

定義から，次の関係となる：

$$\begin{array}{ccc} \text{半単項式作用} & \Leftarrow & \text{純半単項式作用} \\ \Uparrow & & \Uparrow \\ \text{単項式作用} & \Leftarrow & \text{純単項式作用.} \end{array}$$

代数幾何学や不変式論において，多くの有理性問題が生じるが，我々は以下の枠組みで考える：

**問題 1.3** (**半単項式作用の不変体の有理性問題**)**.** $K/k$ を体の拡大，有限群 $G$ の $K(x_1,\dots,x_n)$ への作用を半単項式作用とする．このとき，$K(x_1,\dots,x_n)^G$ は $k$ 上有理的となるか？

この問題はネーター問題，代数的トーラスの有理性問題をも含んでいる (例 1.4 参照)． 有理性問題に関する概説は，Swan [Swa83], Manin–Tsfasman [MT86], Colliot-Thélène–Sansuc [CTS07] を参照. 基本事項 (Galois cohomology, Galois descent, Brauer group など) に対しては，Serre [Ser79, Ser02], Knus-Merkurjev-Rost-Tignol [KMRT98], Gille-Szamuely [GS06], Berhuy [Ber10] を参照のこと．

**例 1.4** (**典型的な半単項式作用の不変体の例**)**.**
(1) **(ネーター問題)**. $G$ が $K(x_1,\dots,x_n)$ に変数 $x_1,\dots,x_n$ には置換として作用し，$K$ には自明に作用するとき $(k = K)$，不変体 $k(x_1,\dots,x_n)^G$ の $k$ 上の有理性問題は**ネーター問題** (Noether's problem) とよばれる．ネーター問題については 2 節で論じる．
(2) **(代数的トーラスの有理性問題)**. $G \simeq \mathrm{Gal}(K/k)$ の $K(x_1,\dots,x_n)$ への作用が純半単項式のとき，不変体 $K(x_1,\dots,x_n)^G$ は $K$ で分裂する $k$ 上の代数的トーラスの関数体となる (Voskresenskii [Vos98, Chapter 2] 参照). 代数的トーラスの有理性問題については 3 節で論じる.
(3) **(Severi-Brauer 多様体の有理性問題)**. $G \simeq \mathrm{Gal}(K/k)$ とする．各 $\sigma \in G$ に対して，$a_\sigma \in GL_{n+1}(K)$ をとり，$GL_{n+1}(K) \to PGL_{n+1}(K), a_\sigma \mapsto \bar{a}_\sigma$ とする．有理関数体 $K(y_0, y_1, \dots, y_n)$ と $K(x_1, \dots, x_n)$ $(x_i = y_i/y_0\ (1 \leq i \leq n))$ を考える．各 $\sigma \in G$ に対して，$a_\sigma$ は $K(y_0, y_1, \dots, y_n)$ と $K(x_1, \dots, x_n)$ の $G$ 同変自己同型を誘導する．さらに，$\gamma : G \to PGL_n(K)$, $\gamma(\sigma) = \bar{a}_\sigma$ を 1 コサイクルとする：$\gamma(\sigma\tau) = \gamma(\sigma) \cdot \sigma(\gamma(\tau))$. すると $G$ は $K(x_1,\dots,x_n)$ への作用を誘導し，その不変体 $F_{n,k}(\gamma) = K(x_1,\dots,x_n)^G$ は $\gamma$ に付随する $k$ 上 $n$ 次 Severi-Brauer 多様体の関数体となる．$F_{n,k}(\gamma)$ は**ブラウアー体** (Brauer-field) とよばれる (Roquette [Roq63, Roq64], Kang [Kan90] 参照). $F_{n,k}(\gamma)$

はコホモロジー類 $[\gamma] \in H^1(G, PGL_n(K))$ できまり ($\gamma' \sim \gamma$ (コホモロガス) $\Rightarrow F_{n,k}(\gamma) \simeq_k F_{n,k}(\gamma')$), $k$ 上有理的 $\Leftrightarrow$ $k$ 上単有理的，となる (Serre [Ser79, page 160] 参照). さらに，$a_\sigma$ が単項行列 (0 でない元が各行各列に 1 つ) のとき，$G$ の $K(x_1, \ldots, x_n)$ への作用は半単項式作用となる．

**記号の説明.** $S_n$, $A_n$, $D_n$, $C_n$ で $n$ 次対称群，$n$ 次交代群，$n$ 次二面体群，$n$ 次巡回群をあらわす. (それぞれ，位数 $n!$, $n!/2$, $2n$, $n$)

## 1.2 単項式作用の不変体の有理性問題

2 次元の単項式作用の不変体の有理性問題は Hajja [Haj87] によって肯定的に解かれた：

**定理 1.5** (Hajja [Haj87]). 有限群 $G$ の $k(x_1, x_2)$ への作用を単項式作用とする．このとき，$k(x_1, x_2)^G$ は $k$ 上有理的.

3 次元の場合，純単項式作用の不変体の有理性問題は肯定的に解かれている．実際，1 つの場合を除き，Hajja-Kang [HK92], [HK92] によって肯定的に解決された．星-陸名 [HR08] は残った 1 つの場合も肯定的であることを示した：

**定理 1.6** (Hajja-Kang [HK92, HK94], 星-陸名 [HR08]). 有限群 $G$ の $k(x_1, x_2, x_3)$ への作用を純単項式作用とする．このとき，$k(x_1, x_2, x_3)^G$ は $k$ 上有理的.

半単項式作用に付随した群準同型 $\rho_{\underline{x}} : G \to GL_n(\mathbb{Z})$ を以下のように定義する：

**定義 1.7** (準同型 $\rho_{\underline{x}}$). 有限群 $G$ の $K(x_1, \ldots, x_n)$ への作用を半単項式作用とする (定義 1.2 (1) (i), (ii), (iii) をみたす). 群準同型 $\rho_{\underline{x}} : G \to GL_n(\mathbb{Z})$ を $\rho_{\underline{x}}(\sigma) = [a_{ij}]_{1 \le i,j \le n} \in GL_n(\mathbb{Z})$ ($\sigma \in G$) によって定義する．ただし，$[a_{ij}]_{1 \le i,j \le n}$ は定義 1.2 (1) (iii) における $\sigma(x_j) = c_j(\sigma) \prod_{1 \le i \le n} x_i^{a_{ij}}$.

有限群 $G$ の $K(x_1, \ldots, x_n)$ への半単項式作用に対して，次の命題により，$G \le GL_n(\mathbb{Z})$ と仮定しても一般性を失わないことがわかる.

**命題 1.8** (星-Kang-北山 [HKK14, Proposition 1.12]). 有限群 $G$ の $K(x_1, \ldots, x_n)$ への作用を半単項式作用とする．正規部分群 $N \lhd G$ が存在して，次の条件をみたす：
(i) $K(x_1, \ldots, x_n)^N = K^N(y_1, \ldots, y_n)$ で $y_i$ は $a x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ ($a \in K^\times, e_i \in \mathbb{Z}$) の形 (さらに，作用が純半単項式作用のときは，$a = 1$ とできる),
(ii) $G/N$ の $K^N(y_1, \ldots, y_n)$ への作用は半単項式作用；
(iii) $\rho_{\underline{y}} : G/N \to GL_n(\mathbb{Z})$ は単射．ただし，$\rho_{\underline{y}}$ は定義 1.7 における $\rho_{\underline{y}}$.

3 次元の単項式作用による $k(x_1, x_2, x_3)^G$ の有理性問題は $G \le GL_3(\mathbb{Z})$ の共役類できまる．有限部分群 $G \le GL_3(\mathbb{Z})$ の共役類 ($\mathbb{Z}$-class) $[G]$ は 73 個ある．Brown-Bülow-Neubüser-Wondratschek-Zassenhaus [BBNWZ78, Table 1] にしたがって，$[G] = [G_{i,j,k}]$ を $GL_3(\mathbb{Z})$ の $i$ 番目の crystal system ($1 \le i \le 7$) で，$j$ 番目の $\mathbb{Q}$-class の中の $k$ 番目 $\mathbb{Z}$-class をあらわす.

$$\mathcal{N} := \{[G_{1,2,1}], [G_{2,3,1}], [G_{3,1,1}], [G_{3,3,1}], [G_{4,2,1}], [G_{4,2,2}], [G_{4,3,1}], [G_{4,4,1}]\}$$

とおく．$\mathcal{N}$ の元は，それぞれ，$C_2$, $(C_2)^2$ $(C_2)^2$, $(C_2)^3$, $C_4$, $C_4$, $C_4 \times C_2$, $D_4$ に同型である．2 つの群 $G = G_{1,2,1}, G_{4,2,2} \in \mathcal{N}$ に対して，$k(x_1, x_2, x_3)^G$ の有理性問題は否定解をもちえること，そして有理的であるための必要十分条件が Saltman [Sal00] と Kang [Kan04] によってそれぞれあたえられた.

**定理 1.9** (Saltman [Sal00, Theorem 0.1], Kang [Kan05, Theorem 4.4] も参照)**.**
体 $k$ を char $k \neq 2$ とする．$G_{1,2,1} = \langle\sigma\rangle \simeq C_2$ の $k(x_1, x_2, x_3)$ への作用を

$$\sigma : x_1 \ \mapsto \ \frac{a_1}{x_1},\ x_2 \ \mapsto \ \frac{a_2}{x_2},\ x_3 \ \mapsto \ \frac{a_3}{x_3}, \quad a_i \in k^\times,\ 1 \leq i \leq 3$$

とする．このとき，$k(x_1, x_2, x_3)^{G_{1,2,1}}$ は $k$ 上非有理的 $\Leftrightarrow$ $[k(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3}) : k] = 8$. さらに，$k(x_1, x_2, x_3)^{G_{1,2,1}}$ が $k$ 上非有理的ならば $k$ 上非レトラクト有理的.

**定理 1.10** (Kang [Kan04, Theorem 1.8])**.** $G_{4,2,2} = \langle\sigma\rangle \simeq C_4$ の $k(x_1, x_2, x_3)$ への作用を

$$\sigma : x_1 \ \mapsto \ x_2 \ \mapsto \ x_3 \ \mapsto \ \frac{c}{x_1x_2x_3} \ \mapsto \ x_1, \quad c \in k^\times$$

とする．このとき，$k(x_1, x_2, x_3)^{G_{4,2,2}}$ は $k$ 上非有理的 $\Leftrightarrow$ 次の 4 条件のうち少なくとも 1 つが成立：(i) char $k = 2$; (ii) $c \in k^2$; (iii) $-4c \in k^4$; (iv) $-1 \in k^2$. さらに，$k(x_1, x_2, x_3)^{G_{4,2,2}}$ が $k$ 上非有理的ならば $k$ 上非レトラクト有理的.

3 次元の単項式作用の不変体の有理性問題は，1 つの場合 $G_{7,1,1} \simeq A_4$ を除き，解決された：

**定理 1.11** (星-北山-山崎 [HKY11], 山崎 [Yam12])**.** 体 $k$ を char $k \neq 2$ とし，有限群 $G \leq GL_3(\mathbb{Z})$ の $k(x_1, x_2, x_3)$ への作用を単項式作用とする.
(1) (星-北山-山崎 [HKY11]) $G \notin \mathcal{N}$ かつ $G \notin [G_{7,1,1}]$ ならば $k(x_1, x_2, x_3)^G$ は $k$ 上有理的；
(2) (山崎 [Yam12]) $G \in \mathcal{N}$ ならば定義 1.2 における $k$ と $c_j(\sigma)$ によっては，$k(x_1, x_2, x_3)^G$ は $k$ 上非有理的となる．さらに，$k(x_1, x_2, x_3)^G$ は $k$ 上非有理的ならば $k$ 上非レトラクト有理的．実際，各 $G \in \mathcal{N}$ に対して，$k(x_1, x_2, x_3)^G$ が $k$ 上有理的となるための必要十分条件を $k$ と $c_j(\sigma)$ の条件としてあたえることができる.

(1) の例外 $G_{7,1,1} = \langle\tau, \lambda, \sigma\rangle \simeq A_4$ の場合，有理性問題は次の場合に帰着できる：

$$\tau : x_1 \ \mapsto \ \frac{a}{x_1},\ x_2 \ \mapsto \ \varepsilon\frac{a}{x_2},\ x_3 \ \mapsto \ \varepsilon x_3, \qquad \lambda : x_1 \ \mapsto \ \varepsilon\frac{a}{x_1},\ x_2 \ \mapsto \ \varepsilon x_2,\ x_3 \ \mapsto \ \frac{a}{x_3},$$
$$\sigma : x_1 \ \mapsto \ x_2,\ x_2 \ \mapsto \ x_3,\ x_3 \ \mapsto \ x_1$$

$a \in k^\times$, $\varepsilon = \pm 1$. 次の定理は，(1) の例外に対して，部分的な解をあたえる．しかしながら，$\varepsilon = -1$ かつ $[k(\sqrt{a}, \sqrt{-1}) : k] = 4$ の場合には，$k(x_1, x_2, x_3)^{G_{7,1,1}}$ の有理性問題は未解決となっている.

**定理 1.12** (星-北山-山崎 [HKY11, Theorem 1.7])**.** 体 $k$ を char $k \neq 2$ とする.
(1) $\varepsilon = 1$ ならば $k(x_1, x_2, x_3)^{G_{7,1,1}}$ は $k$ 上有理的；
(2) $\varepsilon = -1$ かつ $[k(\sqrt{a}, \sqrt{-1}) : k] \leq 2$ ならば $k(x_1, x_2, x_3)^{G_{7,1,1}}$ は $k$ 上有理的.

定理 1.11 と定理 1.12 から次がえられる：

**定理 1.13** (星-北山-山崎 [HKY11, Theorem 1.8])**.** 体 $k$ を char $k \neq 2$ とし，有限群 $G$ の $k(x_1, x_2, x_3)$ への作用を単項式作用とする．このとき，$L = k(\sqrt{a})$ $(a \in k^\times)$ が存在して，$L(x_1, x_2, x_3)^G$ は $L$ 上有理的となる．とくに，$k$ が 2 次閉体ならば $k(x_1, x_2, x_3)^G$ は $k$ 上有理的.

**注意 1.14.** Prokhorov [Pro10, Theorem 5.1] は定理 1.13 を $k = L = \mathbb{C}$ のとき，代数幾何学の手法 (Segre embedding など) によって証明した.

## 1.3 半単項式作用の不変体の有理性問題

主に，星-Kang-北山 [HKK14] による 5 次元以下の半単項式作用の不変体に関する結果を紹介する．一般に，不変体 $K(x_1,\dots,x_n)^G$ は $k$ 上単有理的とも限らなくなる．

**命題 1.15** (星-Kang-北山 [HKK14, Proposition 1.13])**.**
(1) 有限群 $G$ の $K(x)$ への作用を純半単項式作用とする．このとき，$K(x)^G$ は $k$ 上有理的.
(2) 有限群 $G$ の $K(x)$ への作用を半単項式作用とする．このとき，$K(x)^G$ は次の場合を除いて $k$ 上有理的：正規部分群 $N \lhd G$ が存在して，(i) $G/N = \langle\sigma\rangle \simeq C_2$; (ii) $K(x)^N = k(\alpha)(y)$ $(\alpha^2 = a \in K^\times)$, $\sigma(\alpha) = -\alpha$ ($\operatorname{char} k \neq 2$ のとき), $\alpha^2+\alpha = a \in K$, $\sigma(\alpha) = \alpha+1$ ($\operatorname{char} k = 2$ のとき); かつ (iii) $\sigma\cdot y = b/y$ $(b \in k^\times)$.

例外の場合，$K(x)^G = k(\alpha)(y)^{G/N}$ は $k$ 上有理的 $\Leftrightarrow$ ノルム剰余 2 記号 $(a,b)_k = 0$ ($\operatorname{char} k \neq 2$ のとき), $[a,b)_k = 0$ ($\operatorname{char} k = 2$ のとき).

さらに，$K(x)^G$ が $k$ 上非有理的ならばブラウアー群 $\operatorname{Br}(k)$ は非自明かつ $K(x)^G$ は $k$ 上非単有理的.

ノルム剰余 2 記号 $(a,b)_k$ と $[a,b)_k$ については [Dra83, Chapter 11] 参照.

**定理 1.16** (星-Kang-北山 [HKK14, Theorem 1.14])**.** 有限群 $G$ の $K(x,y)$ への作用を純半単項式作用とする.

$$N = \{\sigma \in G : \sigma(x) = x,\ \sigma(y) = y\},\ H = \{\sigma \in G : \sigma(\alpha) = \alpha \text{ for all } \alpha \in K\}$$

とする．このとき，$K(x,y)^G$ は次の場合を除いて，$k$ 上有理的:(1) $\operatorname{char} k \neq 2$ かつ (2) $(G/N, HN/N) \simeq (C_4, C_2)$ または $(D_4, C_2)$.

より詳細には，例外の場合，$u, v \in k(x,y)$ が存在して，以下をみたす：
$k(x,y)^{HN/N} = k(u,v)$ (よって $K(x,y)^{HN/N} = K(u,v)$);
(i) $(G/N, HN/N) \simeq (C_4, C_2)$ のとき，$K^N = k(\sqrt{a})$ $(a \in k\backslash k^2)$, $G/N = \langle\sigma\rangle \simeq C_4$ で，$\sigma$ の $K^N(u,v)$ への作用は $\sigma : \sqrt{a} \mapsto -\sqrt{a}$, $u \mapsto \dfrac{1}{u}$, $v \mapsto -\dfrac{1}{v}$;
(ii) $(G/N, HN/N) \simeq (D_4, C_2)$ のとき，$K^N = k(\sqrt{a}, \sqrt{b})$ は $k$ の 4 次拡大 $(a, b \in k\backslash k^2)$, $G/N = \langle\sigma,\tau\rangle \simeq D_4$ で $\sigma$ と $\tau$ の $K^N(u,v)$ への作用は $\sigma : \sqrt{a} \mapsto -\sqrt{a}$, $\sqrt{b} \mapsto \sqrt{b}$, $u \mapsto \dfrac{1}{u}$, $v \mapsto -\dfrac{1}{v}$, $\tau : \sqrt{a} \mapsto \sqrt{a}$, $\sqrt{b} \mapsto -\sqrt{b}$, $u \mapsto u$, $v \mapsto -v$. さらに,
(i) の場合，$K(x,y)^G$ は $k$ 上有理的 $\Leftrightarrow$ ノルム剰余 2 記号 $(a,-1)_k = 0$.
(ii) の場合, $K(x,y)^G$ は $k$ 上有理的 $\Leftrightarrow$ ノルム剰余 2 記号 $(a,-b)_k = 0$.

さらに，$K(x,y)^G$ は $k$ 上非有理的ならば $\operatorname{Br}(k)$ は非自明かつ $K(x,y)^G$ は $k$ 上非単有理的.

Saltman [Sal90a, Section 3] は不変体とガロア理論の埋め込み問題の関係を議論している．定理 1.16 の例外は埋め込み問題の視点から表現すると以下のようになる.

**命題 1.17** (星-Kang-北山 [HKK14, Proposition 4.3])**.** 体 $k$ を $\operatorname{char} k \neq 2$ とする.
(1) $a \in k\backslash k^2$, $K = k(\sqrt{a})$，$G = \langle\sigma\rangle$ の $K(u,v)$ への作用を以下とする：

$$\sigma : \sqrt{a} \mapsto -\sqrt{a},\ u \mapsto \frac{1}{u},\ v \mapsto -\frac{1}{v}.$$

このとき，$K(u,v)^G$ は $k$ 上有理的 $\Leftrightarrow$ $\operatorname{Gal}(L/k) \simeq C_4$ なるガロア拡大 $L/k$ が存在して，$K \subset L$.
(2) $K = k(\sqrt{a}, \sqrt{b})$, $a, b \in k\backslash k^2$, $[K:k] = 4$, $G = \langle\sigma,\tau\rangle$ の $K(u,v)$ への作用を以下とする：

$$\sigma : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto \sqrt{b},\ u \mapsto \frac{1}{u},\ v \mapsto -\frac{1}{v},$$
$$\tau : \sqrt{a} \mapsto \sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b},\ u \mapsto u,\ v \mapsto -v.$$

このとき，$K(u,v)^G$ は $k$ 上有理的 $\Leftrightarrow$ $\operatorname{Gal}(L/k) \simeq D_4$ なるガロア拡大 $L/k$ が存在して，$K \subset L$.

定理 1.16 の例外 (ii) の場合の例をあたえる．

**例 1.18** (星-Kang-北山 [HKK14, Example 4.4])．体 $k$ を $\mathrm{char}\ k \neq 2$，$K = k(\sqrt{a}, \sqrt{b})$, $[K : k] = 4$ とする．次の $D_4 = \langle \sigma, \tau \rangle$ の $K(x, y)$ への純半単項式作用を考える：

$$\sigma_a : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto \sqrt{b},\ x \mapsto y,\ y \mapsto \frac{1}{x},$$
$$\sigma_b : \sqrt{a} \mapsto \sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b},\ x \mapsto y,\ y \mapsto \frac{1}{x},$$
$$\sigma_{ab} : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b},\ x \mapsto y,\ y \mapsto \frac{1}{x},$$
$$\tau_a : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto \sqrt{b},\ x \mapsto y,\ y \mapsto x,$$
$$\tau_b : \sqrt{a} \mapsto \sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b},\ x \mapsto y,\ y \mapsto x,$$
$$\tau_{ab} : \sqrt{a} \mapsto -\sqrt{a},\ \sqrt{b} \mapsto -\sqrt{b},\ x \mapsto y,\ y \mapsto x.$$

不変体 $L_{a,b} = K(x, y)^{\langle \sigma_a, \tau_b \rangle}$ に対して，以下が成り立つ：
(1) $L_{a,b}$ は $k$ 上有理的 $\Leftrightarrow$ $L_{a,ab}$ は $k$ 上有理的 $\Leftrightarrow$ $(a, -b)_k = 0$;
(2) $L_{b,a}$ は $k$ 上有理的 $\Leftrightarrow$ $L_{b,ab}$ は $k$ 上有理的 $\Leftrightarrow$ $(b, -a)_k = 0$;
(3) $L_{ab,a}$ は $k$ 上有理的 $\Leftrightarrow$ $L_{ab,b}$ は $k$ 上有理的 $\Leftrightarrow$ $(a, b)_k = 0$.

とくに，$\sqrt{-1} \in k$ ならば (1),(2),(3) の有理性は一致する．(全て同じ条件 $(a, b)_k = 0$ となる)

一方で，$k = \mathbb{Q}$ のとき，$p \equiv 1 \pmod 4$ なる素数 $p$ に対して，$K = \mathbb{Q}(\sqrt{-1}, \sqrt{p})$ とすれば，$(-1, -p)_{\mathbb{Q}} = (-1, -1)_{\mathbb{Q}} \neq 0$ より $L_{a,b}$, $L_{a,ab}$ は $\mathbb{Q}$ 上非有理的となるが，$L_{b,a}$, $L_{b,ab}$, $L_{ab,a}$, $L_{ab,b}$ は $\mathbb{Q}$ 上有理的である．

次は半単項式作用を言い換えたものである：

**定義 1.19.** $G$ を有限群とする．$G$ **格子** ($G$-lattice) $M$ とは，有限性生成 $\mathbb{Z}[G]$ 加群でアーベル群として $\mathbb{Z}$ 自由であるもの ($M = \bigoplus_{1 \leq i \leq n} \mathbb{Z} \cdot x_i$)．$K/k$ を体の拡大，$G$ は $K$ に作用し $K^G = k$ とする．$G$ の $K(x_1, \ldots, x_n)$ への純半単項式作用とは $\sigma \cdot x_j = c_j(\sigma) \prod_{1 \leq i \leq n} x_i^{a_{ij}} \in K(x_1, \ldots, x_n)$．ただし，$\sigma \cdot x_j = \sum_{1 \leq i \leq n} a_{ij} x_i \in M$ とする．$K(M)$ の $G$ 作用による不変体を $K(M)^G$ とかく．

$M = M_1 \oplus M_2$ が直可約のとき，$G$ の $k(M)$ への純単項式作用は，$k(M) = K(M_2)$, $K = k(M_1)$ とみなすことによって $K(M_2)$ への純半単項式作用とみなすことができる．実際，定理 1.16 を用いて，$G$ 格子 $M$ の $\mathbb{Z}$ 階数が 4 で直可約のとき，$k(M)^G$ は $k$ 上有理的であることが示せる．

$\mathbb{Z}$ 階数が 4 の $G$ 格子は 710 個あり，そのうち直可約なものは 415 個である．

**定理 1.20** (星-Kang-北山 [HKK14, Theorem 1.16])．$G$ を有限群，$M$ を $G$ 格子で $\mathrm{rank}_{\mathbb{Z}} M = 4$ とする．$G$ の $k(M)$ への作用は純単項式作用とする．$M$ が直可約 ($\mathbb{Z}[G]$ 加群として $M = M_1 \oplus M_2$, $1 \leq \mathrm{rank}_{\mathbb{Z}} M_1 \leq 3$) ならば $k(M)^G$ は $k$ 上有理的．

**命題 1.21** (星-Kang-北山 [HKK14, Proposition 5.2])．$G$ を有限群，$M$ を $G$ 格子とする．$\mathbb{Z}$ 階数が 5 の $G$ 格子 $M$ に対して，$\mathbb{Z}[G]$ 加群として $M = M_1 \oplus M_2 \oplus M_3$ ($\mathrm{rank}_{\mathbb{Z}} M_1 = \mathrm{rank}_{\mathbb{Z}} M_2 = 2$, $\mathrm{rank}_{\mathbb{Z}} M_3 = 1$) と仮定する．$G$ の $k(M)$ への作用が純単項式作用ならば $k(M)^G$ は $k$ 上有理的．

**定理 1.22** (星-Kang-北山 [HKK14, Theorem 6.2, Theorem 6.4])．$G$ を有限群，$M$ を $G$ 格子とする．次を仮定する：(i) $\mathbb{Z}[G]$ 加群として $M = M_1 \oplus M_2$ ($\mathrm{rank}_{\mathbb{Z}} M_1 = 3$, $\mathrm{rank}_{\mathbb{Z}} M_2 = 2$); (ii) $M_1$ または $M_2$ は忠実 $G$ 格子．$G$ の $k(M)$ への作用を純単項式作用とする．このとき，$k(M)^G$ は次の場合を除いて $k$ 上有理的：$\mathrm{char}\, k \neq 2$, $G = \langle \sigma, \tau \rangle \simeq D_4$, $M_1 = \bigoplus_{1 \leq i \leq 3} \mathbb{Z} x_i$, $M_2 = \bigoplus_{1 \leq j \leq 2} \mathbb{Z} y_j$, $\sigma : x_1 \leftrightarrow x_2$, $x_3 \mapsto -x_1 - x_2 - x_3$, $y_1 \mapsto y_2 \mapsto -y_1$, $\tau : x_1 \leftrightarrow x_3$, $x_2 \mapsto -x_1 - x_2 - x_3$, $y_1 \leftrightarrow y_2$．ただし，$M$ の $\mathbb{Z}[G]$ 加群の表示と作用を加法的にあらわした．

例外の場合は，$k(M)^G$ は $k$ 上非レトラクト有理的となる．とくに，$G=\langle\sigma,\tau\rangle\simeq D_4$ の $k(x_1,x_2,x_3,x_4,x_5)$ への作用が純単項式作用

$$\sigma: x_1\mapsto x_2,\ x_2\mapsto x_1,\ x_3\mapsto \frac{1}{x_1x_2x_3},\ x_4\mapsto x_5,\ x_5\mapsto \frac{1}{x_4},$$
$$\tau: x_1\mapsto x_3,\ x_2\mapsto \frac{1}{x_1x_2x_3},\ x_3\mapsto x_1,\ x_4\mapsto x_5,\ x_5\mapsto x_4,$$

ならば $k(x_1,x_2,x_3,x_4,x_5)^G$ は $k$ 上非レトラクト有理的.

**注意 1.23.** 定理 1.22 の例外の場合 $G\simeq D_4$ は，$k(M)^G$ が代数閉体 $k$ 上でも非レトラクト有理的な純単項式作用の例をあたえている (定理 1.6, 定理 1.13 参照).

定理 1.22 の例外の場合は次の 4 次元の作用に帰着できる (定理 2.17 も参照)：

**定理 1.24** (星-Kang-北山 [HKK14, Theorem 6.3])**.** 体 $k$ を char $k\neq 2$ とする．$G=\langle\rho\rangle\simeq C_2$ の $k(x_1,x_2,x_3,x_4)$ への $k$ 自己同型としての作用が

$$\rho: x_1\mapsto -x_1,\ x_2\mapsto \frac{x_4}{x_2},\ x_3\mapsto \frac{(x_4-1)(x_4-x_1^2)}{x_3},\ x_4\mapsto x_4$$

ならば $k(x_1,x_2,x_3,x_4)^G$ は $k$ 上非レトラクト有理的.

## 2　不変体の有理性問題と不分岐ブラウアー群

### 2.1　ネーター問題：正則作用による不変体の有理性問題

有限群 $G$ が有理関数体 $k(x_g:g\in G)$ に変数の置換 $h(x_g)=x_{hg}$ $(g,h\in G)$ によって，$k$ 自己同型として作用しているとする．この作用による不変体 $k(x_g:g\in G)^G=\{f\in k(x_g:g\in G):\sigma(f)=f\ (\sigma\in G)\}$ を $k(G)$ とかく．($k(x_g:g\in G)/k(G)$ は $G$ ガロア拡大となる)

**ネーター問題** (Noether's problem) とは，$k(G)$ が $k$ 上有理的 (純超越的) かを問う問題である．今回の金井和貴さん，長谷川寿人さんの講義でも紹介があったように，この問題はガロア逆問題，生成的 $G$ 拡大の存在，生成的 $G$ トーサーの存在と深い関わりがある (Swan [Swa83], Manin-Tsfasman [MT86], Colliot-Thélène–Sansuc [CTS07], Serre [GMS03, pages 86–92] 参照)．例えば，Saltman [Sal82a, Sal82b] は次を示した (Jensen-Ledet-Yui [JLY02, Chapter 5] も参照):

**定理 2.1** (Saltman [Sal82a, Sal82b] 参照)**.** $G$ を有限群，$k$ を無限体とする．次は同値：
(1) $k(G)$ は $k$ 上レトラクト有理的 ;
(2) $G$ は $k$ 上の lifting property をみたす ;
(3) $k$ 上の生成的 $G$ 拡大 ( 生成的 $G$ 多項式 ) が存在する.

ネーター問題に対して，知られていることをいくつか述べる：

**定理 2.2** (Fischer [Fis15], see also Swan [Swa83, Theorem 6.1])**.** $G$ をアーベル群とし，その指数を $e$ とする．$k$ が 1 の $e$ 乗根を含むならば $k(G)$ は $k$ 上有理的．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的.

国吉 [Kun54, Kun55, Kun56] は $p$ 群に対して次を示した ([Kun56], Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, 参照).

**定理 2.3** (国吉 [Kun54, Kun55, Kun56])**.** $k$ を標数 $p>0$ の体，$G$ を $p$ 群とする．このとき，$k(G)$ は $k$ 上有理的.

Swan [Swa69] は，増田 [Mas55, Mas68] の方法を発展させて，$\mathbb{Q}(C_{47})$ は $\mathbb{Q}$ 上非有理的であることを示し，ネーター問題の最初の反例をあたえた．Voskresenskii, 遠藤-宮田など多くの努力のあと，アーベル群に対するネーター問題は Lenstra [Len74] によって解かれた (Swan [Swa83] 参照)．

一方で，非可換群に対するネーター問題はその多くがよく分かっていない．例えば，以下のような結果が知られている：

**定理 2.4** (Chu-Kang [CK01])．$G$ を位数 $\leq p^4$ の $p$ 群，その指数を $e$ とする．$k$ が 1 の $e$ 乗根を含むならば $k(G)$ は $k$ 上有理的．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的．

**定理 2.5** (Serre [GMS03, Chapter IX])．有限群 $G$ を 2 シロー群が位数 8 以上の巡回群または位数 16 の一般四元数群 $Q_{16}$ とする．このとき，$\mathbb{Q}(G)$ は $\mathbb{Q}$ 上非有理的．

**定理 2.6** (Chu-Hu-Kang-Prokhorov [CHKP08])．$G$ を位数 32 の群，その指数を $e$ とする．$k$ が 1 の $e$ 乗根を含むならば $k(G)$ は $k$ 上有理的．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的．

位数が 64 の群 $G$ に対しては，$\mathbb{C}(G)$ が $\mathbb{C}$ 上非有理的になることがある (Chu-Hu-Kang-Kunyavskii [CHKK10] 参照)．$K$ が $k$ 上非有理的であることを示すには，双有理不変量の計算が有効となる．以下，その不変量の 1 つとして不分岐ブラウアー群 $\mathrm{Br}_{\mathrm{nr}}(K/k)$ と，それに関連した結果を紹介する．

## 2.2 ネーター問題の不変体の不分岐ブラウアー群

不分岐ブラウアー群 $\mathrm{Br}_{\mathrm{nr}}(K/k)$ の概念は Saltman [Sal84a] によって導入された：

**定義 2.7** (Saltman [Sal84a, Definition 3.1], [Sal85, page 56])．$k \subset K$ を体の拡大とする．$K$ の $k$ 上の**不分岐ブラウアー群** (unramified Brauer group) $\mathrm{Br}_{\mathrm{nr}}(K/k)$ とは，

$$\mathrm{Br}_{\mathrm{nr}}(K/k) = \bigcap_R \mathrm{Image}\{\mathrm{Br}(R) \to \mathrm{Br}(K)\}.$$

ただし，$\mathrm{Br}(R) \to \mathrm{Br}(K)$ は自然な埋め込み，$R$ は $k \subset R \subset K = Q(R)$ なる離散付置環をうごく．

**補題 2.8** (Saltman [Sal84a], [Sal85, Proposition 1.8], [Sal87])．$k$ を無限体，体 $K$ を $k$ 上レトラクト有理的とする．このとき，自然な射 $\mathrm{Br}(k) \to \mathrm{Br}(K)$ は同型 $\mathrm{Br}(k) \xrightarrow{\sim} \mathrm{Br}_{\mathrm{nr}}(K)$ を誘導する．とくに，$k = \overline{k}$ かつ $K$ は $k$ 上レトラクト有理的ならば $\mathrm{Br}_{\mathrm{nr}}(K) = 0$.

**定理 2.9** (Bogomolov [Bog88, Theorem 3.1], Saltman [Sal90b, Theorem 12])．$G$ を有限群，代数閉体 $k$ を $\mathrm{char}\ k = 0$ または $\mathrm{char}\ k = p \nmid |G|$ とする．このとき，$\mathrm{Br}_{\mathrm{nr}}(k(G)/k)$ は次の $B_0(G)$ と同型：

$$B_0(G) = \bigcap_A \mathrm{Ker}\{\mathrm{res} : H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(A, \mathbb{Q}/\mathbb{Z})\}.$$

ただし，$A$ は巡回群または 2 つの巡回群の直積である $G$ の部分群をうごく．

$B_0(G) \leq H^2(G, \mathbb{Q}/\mathbb{Z}) \simeq M(G)$, $M(G)$ は $G$ の Schur multiplier であることから，$B_0(G)$ は $G$ の **Bogomolov multiplier** ともよばれる (Karpilovsky [Kar87], Kunyavskii [Kun10] 参照)．定理 2.9 から，$k$ が代数閉体かつ $\gcd\{|G|, \mathrm{char}\, k\} = 1$ のとき，$B_0(G)$ と $\mathrm{Br}_{\mathrm{nr}}(k(G)/k)$ をとくに区別しないことにする．不分岐ブラウアー群 $B_0(G)$ をもちいて，Saltman と Bogomolov は代数閉体 $k$ 上のネーター問題の反例を構成した：

**定理 2.10** (Saltman [Sal84a], Bogomolov [Bog88])．$p$ を素数，$k$ を代数閉体で $\mathrm{char}\ k \neq p$ とする．
(1) (Saltman) 位数 $p^9$ の $p$ 群 $G$ が存在して，$B_0(G) \neq 0$．とくに，$k(G)$ は $k$ 上非有理的．
(2) (Bogomolov) 位数 $p^6$ の $p$ 群 $G$ が存在して，$B_0(G) \neq 0$．とくに，$k(G)$ は $k$ 上非有理的．

さらに，Bogomolov [Bog88, Lemma 5.6] は $G$ が位数 $\leq p^5$ の $p$ 群ならば $B_0(G) = 0$ を主張していたが，2012 年になって，これは間違いであることが分かった．この続きは，4 日目の谷本祥さんの講演および 5 日目の講演者の講演で解説される．

## 2.3 単項式作用の不変体の不分岐ブラウアー群

$k$ を体，$G$ を有限群，$\rho : G \to GL(V)$ を $G$ の忠実表現とする．ただし，$V$ は $k$ 上有限次元ベクトル空間．$G$ は有理関数体 $k(V)$ に作用し，不変体 $k(V)^G$ の有理性問題を考える．No-name Lemma (宮田 [Miy71, Remark 3] 参照) により，$k(G)$ は $k(V)^G$ 上有理的となる．特に，$k(G)$ と $k(V)$ は安定 $k$ 同型である．このような事情から，$k(V)^G$ の $k$ 上の有理性問題もまた**ネーター問題** (Noether's problem) とよばれることがある．(安定有理性を問うことをネーター問題と呼ぶこともある)

$M$ を $\mathbb{Z}$ 階数が $n$ の $G$ 格子 (有限生成 $\mathbb{Z}[G]$ 加群 $\simeq \mathbb{Z}^n$) とする．$G$ の $k(M) = k(x_1, \dots, x_n)$ への単項式作用は，**乗法的作用** (multiplicative action) ともよばれる．乗法的作用による不変体 $k(M)^G = k(x_1, \dots, x_n)^G$ は**乗法的不変体** (multiplicative invariant field) とよばれる．

$G$ 格子 $M$ が $M = \oplus_{g \in G} \mathbb{Z} \cdot x_g$, $h \cdot x_g = x_{hg}$ $(h, g \in G)$ のとき，$k(M) = k(x_g : g \in G)$ かつ $k(M)^G = k(G)$ となり，不変体の有理性問題はネーター問題となる (1 節参照)．$G$ の正則表現 $G \to GL(V_{\mathrm{reg}})$ に対して，$k(G) = k(V_{\mathrm{reg}})^G$ であるから，ネーター問題とは $G$ の正則作用による不変体の有理性問題のことである．

不変体 $k(V)^G$ の有理性問題は，乗法的不変体 $k(M)^G$ の有理性問題に帰着されることが多い (Chu-Hu-Kang-Kunyavskii [CHKK10], 星-北山-山崎 [HKY11, Example 13.7], 定理 2.17 参照)．

以下，単項式作用による不変体 $k(M)^G$ (乗法的作用) を考える．$G$ 格子 $M$ はすべての $\sigma \in G \setminus \{1\}$ に対して，ある $x \in M$ が存在して，$\sigma \cdot x \neq x$ となるとき，**忠実** (faithful) という．定義 1.7 の群準同型 $\rho_{\underline{x}} : G \to GL_n(\mathbb{Z})$ に対して，命題 1.8 から，$\rho_{\underline{x}}$ は単射としてよい．すなわち，$G \leq GL_n(\mathbb{Z})$ と仮定してよい．このとき，対応する $G$ 格子 $M$ は忠実である．

$GL_n(\mathbb{Z})$ の共役有限部分群のリストは，$n \leq 4$ に対しては，Brown-Bülow-Neubüser-Wondratschek-Zassenhaus [BBNWZ78] や GAP [GAP], $n = 5, 6$ に対しては，CARAT [CARAT] から手に入る (Plesken-Schulz [PS00], 星-山崎 [HY17, Chapter 3] 参照)．とくに，共役有限部分群 $G \leq GL_n(\mathbb{Z})$ ($\mathbb{Z}$ 階数が $n$ の忠実 $G$ 格子 $M$) の個数は以下となる：

| $\mathrm{rank}_{\mathbb{Z}} M = n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $G$ 格子 $M$ の個数 | 2 | 13 | 73 | 710 | 6079 | 85308 |

**定義 2.11** ($\mu$ 拡大)**.** $k$ を体，$\mu \leq k^\times$ を $k$ の $n$ 乗根全体とする．$G$ 格子 $M$ の **$\mu$ 拡大** ($\mu$-extension) とは，$\mathbb{Z}[G]$ 加群の完全系列 $(\alpha) : 1 \to \mu \to M_\alpha \to M \to 0$ のこと．ただし，$G$ は $\mu$ に自明作用とする．$M_\alpha$ を $M$ の $\mu$ 拡大ともいう．アーベル群としては，$M_\alpha = \mu \oplus M$ であるが，$\mathbb{Z}[G]$ 加群としては，$(\alpha)$ が分裂するとき以外は，そうはならないことに注意しておく．

$G$ の $k_\alpha(M) = k(x_1, \dots, x_n)$ への作用を $\sigma \cdot x_i = \varepsilon_i(\sigma) \prod_{1 \leq j \leq n} x_j^{a_{ij}}$ によって定義する．ただし，$\sigma \cdot x_i = \varepsilon_i(\sigma) + \sum_{1 \leq j \leq n} a_{ij}\, x_j$ $(\varepsilon_i(\sigma) \in \mu)$ とする．これは，単項式作用 (1 節, Hajja-Kang [HK92] も参照) である．また，**捩れ乗法的作用** (twisted multiplicative action) とよばれることもある．このとき，不変体 $k_\alpha(M)^G = k(x_1, \dots, x_n)^G$ は**捩れ乗法的不変体** (twisted multiplicative invariant field) とよばれる (Saltman [Sal90b] 参照)．特に，$\mu$ 拡大 $(\alpha) : 1 \to \mu \to M_\alpha \to M \to 0$ が分裂するとき，$k_\alpha(M) = k(M)$ であり，捩れ乗法的作用 (単項式作用) は，単に乗法的作用 (純単項式作用) となる．

$G$ の忠実線形表現 $G \to GL(V)$ に対して，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(V)^G) \simeq B_0(G)$ である．$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(V)^G)$ に対する Bogomolov の公式 (定理 2.9) は，Saltman [Sal90b] によって，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}_\alpha(M)^G)$ に拡張された：

**定理 2.12** (Saltman [Sal90b, Theorem 12])**.** $k$ を標数 0 の代数閉体，$G$ を有限群，$M$ を忠実 $G$ 格子，$(\alpha) : 1 \to \mu \to M_\alpha \to M \to 0$ を $\mu$ 拡大，$H^2(G, \mu) \to H^2(G, M_\alpha)$ は単射と仮定する．このとき，

$$\mathrm{Br}_{\mathrm{nr}}(k_\alpha(M)^G) = \bigcap_A \mathrm{Ker}\{\mathrm{res} : H^2(G, M_\alpha) \to H^2(A, M_\alpha)\}.$$

ただし，$A$ は巡回群または 2 つの巡回群の直積である $G$ の部分群をうごく．とくに，$\mu$ 拡大 $(\alpha)$ が分裂するとき，$\mathrm{Br}_{\mathrm{nr}}(k(M)^G) \simeq B_0(G) \oplus \bigcap_A \mathrm{Ker}\{\mathrm{res} : H^2(G, M) \to H^2(A, M)\}$ となる．

Saltman [Sal90b, page 536] によって，$\mathrm{Br}_{\mathrm{nr}}(k_\alpha(M)^G) \leq H^2(G, M_\alpha)$. そこで，$\mathrm{Br}_{\mathrm{nr}}(k_\alpha(M)^G)$ を $H^2_{\mathrm{nr}}(G, M_\alpha)$ ともかく (Saltman [Sal90b], 星-Kang-山崎 [HKY, Definition 2.3] 参照).

**定義 2.13** ($H^2_{\mathrm{nr}}(G, \mathbb{Q}/\mathbb{Z})$, $H^2_{\mathrm{nr}}(G, M)$)**.** $\mu$ 拡大 $(\alpha) : 1 \to \mu \to M_\alpha \to M \to 0$ は分裂すると仮定する．自然な写像 $H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, M_\alpha)$ は単射で，$H^2(G, \mathbb{Q}/\mathbb{Z})$, $H^2(G, M) \leq H^2(G, M_\alpha)$ とみなせるから，$H^2_{\mathrm{nr}}(G, \mathbb{Q}/\mathbb{Z}) = H^2(G, \mathbb{Q}/\mathbb{Z}) \cap \mathrm{Br}_{\mathrm{nr}}(k_\alpha(M)^G)$, $H^2_{\mathrm{nr}}(G, M) = H^2(G, M) \cap \mathrm{Br}_{\mathrm{nr}}(k_\alpha(M)^G)$ と定義する．これより，$\mathrm{Br}_{\mathrm{nr}}(k_\alpha(M)^G) = H^2_{\mathrm{nr}}(G, \mathbb{Q}/\mathbb{Z}) \oplus H^2_{\mathrm{nr}}(G, M)$ である．定理 2.9 と定理 2.12 より，$H^2_{\mathrm{nr}}(G, \mathbb{Q}/\mathbb{Z}) \simeq B_0(G)$ かつ $H^2_{\mathrm{nr}}(G, M) \simeq \bigcap_A \mathrm{Ker}\{\mathrm{res} : H^2(G, M) \to H^2(A, M)\}$ であった．

Barge [Bar89], [Bar97] によって，以下が知られている：

**定理 2.14** (Barge [Bar89, Theorem II.7])**.** $G$ を有限群とする．次は同値：
(1) $G$ のすべてのシロー群は巡回群または 2 つの巡回群の直積；
(2) すべての $G$ 格子 $M$ に対して，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) = 0$.

**定理 2.15** (Barge [Bar97, Theorem IV-1])**.** $G$ を有限群とする．次は同値：
(1) $G$ のすべてのシロー群は巡回群；
(2) すべての $G$ 格子 $M$ とすべての $\mathbb{Z}[G]$ 加群の完全系列 $\alpha : 0 \to \mathbb{C}^\times \to M_\alpha \to M \to 0$ に対して，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}_\alpha(M)^G) = 0$.

$G$ 加群 $M$ が $\mathrm{rank}_{\mathbb{Z}} M \leq 3$ の場合，定理 1.6 (Hajja-Kang [HK92, HK94], 星-陸名 [HR08]) から $\mathbb{C}(M)^G$ は $\mathbb{C}$ 上有理的であり，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) = 0$ となる．

次の定理 2.16 は，$\mathrm{rank}_{\mathbb{Z}} M \leq 6$ なる $M$ に対して，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$ となる場合の分類をあたえている．($\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0 \Rightarrow \mathbb{C}(M)^G$ は $\mathbb{C}$ 上非レトラクト有理的，補題 2.8 参照)

**記号の説明.** $C_n$, $D_n$, $QD_{8n}$, $Q_{8n}$ で $n$ 次巡回群，$n$ 次二面体群 (位数 $2n$), 位数 $16n$ の準二面体群，位数 $16n$ の一般四元数群をあらわす.

**定理 2.16** (星-Kang-山崎 [HKY, Theorem 1.10])**.** $G$ を有限群，$M$ を $G$ 格子とする．
(1) $\mathrm{rank}_{\mathbb{Z}} M \leq 3$ ならば $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) = 0$.
(2) $\mathrm{rank}_{\mathbb{Z}} M = 4$ のとき，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0 \Leftrightarrow M$ は表 1 の 5 個の $G$ 格子. さらに，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$ ならば $B_0(G) = 0$ かつ $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) = H^2_{\mathrm{nr}}(G, M)$.
(3) $\mathrm{rank}_{\mathbb{Z}} M = 5$ のとき，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0 \Leftrightarrow M$ は [HKY, Table 2] の 46 個の $G$ 格子. さらに，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$ ならば $B_0(G) = 0$ かつ $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) = H^2_{\mathrm{nr}}(G, M)$.
(4) $\mathrm{rank}_{\mathbb{Z}} M = 6$ のとき，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0 \Leftrightarrow M$ は [HKY, Table 3] の 1073 個の $G$ 格子. さらに，24 個の例外 ($B_0(G) = \mathbb{Z}/2\mathbb{Z}$) を除いて，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$ ならば $B_0(G) = 0$ かつ $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) = H^2_{\mathrm{nr}}(G, M)$. (24 個の例外のうち，22 個は $H^2_{\mathrm{nr}}(G, M) = 0$.)

| $G(n, i)$ | $G$ | GAP ID | $B_0(G)$ | $H^2_{\mathrm{nr}}(G, M)$ |
|---|---|---|---|---|
| $(8, 3)$ | $D_4$ | $(4, 12, 4, 12)$ | 0 | $\mathbb{Z}/2\mathbb{Z}$ |
| $(8, 4)$ | $Q_8$ | $(4, 32, 1, 2)$ | 0 | $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ |
| $(16, 8)$ | $QD_8$ | $(4, 32, 3, 2)$ | 0 | $\mathbb{Z}/2\mathbb{Z}$ |
| $(24, 3)$ | $SL_2(\mathbb{F}_3)$ | $(4, 33, 3, 1)$ | 0 | $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ |
| $(48, 29)$ | $GL_2(\mathbb{F}_3)$ | $(4, 33, 6, 1)$ | 0 | $\mathbb{Z}/2\mathbb{Z}$ |

表 1: $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$ となる $\mathrm{rank}_{\mathbb{Z}} M = 4$ の 5 つの $G$ 格子 $M$

定理 2.16 をまとめると以下のようになる：

| $\mathrm{rank}_{\mathbb{Z}} M = n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $G$ 格子 $M$ の数 | 2 | 13 | 73 | 710 | 6079 | 85308 |
| $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$ となる $G$ 格子 $M$ の数 | 0 | 0 | 0 | 5 | 46 | 1073 |

**定理 2.17** (星-Kang-山崎 [HKY, Theorem 4.4])**.** 次の体 $K$ は互いに安定 $\mathbb{C}$ 同型である：
(1) $K = \mathbb{C}(G)$. ただし，$G$ は位数 64 の 2 群で 16 番目の同質族 $\Phi_{16}$ に属する (Chu-Hu-Kang-Kunyavskii [CHKK10, Theorem 1.8] の 9 つの群を参照 );
(2) $K = \mathbb{C}(x_1, x_2, x_3, x_4)^{D_4}$. ただし，$D_4 = \langle \sigma, \tau \rangle$ の $\mathbb{C}(x_1, x_2, x_3, x_4)$ への作用は純単項式作用

$$\sigma : x_1 \mapsto x_2x_3, x_2 \mapsto x_1x_3, x_3 \mapsto x_4, x_4 \mapsto \frac{1}{x_3},$$
$$\tau : x_1 \mapsto \frac{1}{x_2}, x_2 \mapsto \frac{1}{x_1}, x_3 \mapsto \frac{1}{x_4}, x_4 \mapsto \frac{1}{x_3}$$

(定理 2.16，表 1 参照);
(3) $K = \mathbb{C}(y_1, y_2, y_3, y_4, y_5)^{D_4}$. ただし，$D_4 = \langle \sigma, \tau \rangle$ の $\mathbb{C}(y_1, y_2, y_3, y_4, y_5)$ への作用は純単項式作用

$$\sigma : y_1 \mapsto y_2, y_2 \mapsto y_1, y_3 \mapsto \frac{1}{y_1y_2y_3}, y_4 \mapsto y_5, y_5 \mapsto \frac{1}{y_4},$$
$$\tau : y_1 \mapsto y_3, y_2 \mapsto \frac{1}{y_1y_2y_3}, y_3 \mapsto y_1, y_4 \mapsto y_5, y_5 \mapsto y_4$$

(定理 1.22 参照);
(4) $K = \mathbb{C}(z_1, z_2, z_3, z_4)^{C_2 \times C_2}$. ただし，$C_2 \times C_2 = \langle \sigma, \tau \rangle$ の $\mathbb{C}(z_1, z_2, z_3, z_4)$ への作用は単項式作用

$$\sigma : z_1 \mapsto z_2, z_2 \mapsto z_1, z_3 \mapsto \frac{1}{z_1z_2z_3}, z_4 \mapsto \frac{-1}{z_4},$$
$$\tau : z_1 \mapsto z_3, z_2 \mapsto \frac{1}{z_1z_2z_3}, z_3 \mapsto z_1, z_4 \mapsto -z_4$$

(星-Kang-北山 [HKK14, Proof of Theorem 6.4] 参照 );
(5) $K = \mathbb{C}(w_1, w_2, w_3, w_4)^{C_2}$. ただし，$C_2 = \langle \sigma \rangle$ の $\mathbb{C}(w_1, w_2, w_3, w_4)$ への作用は

$$\sigma : w_1 \mapsto -w_1, w_2 \mapsto \frac{w_4}{w_2}, w_3 \mapsto \frac{(w_4 - 1)(w_4 - w_1^2)}{w_3}, w_4 \mapsto w_4$$

(定理 1.24 参照).

特に，(1)–(5) の体 $K$ に対して，$H^i_{\mathrm{nr}}(K, \mathbb{Q}/\mathbb{Z})$ はすべて等しく，$\mathrm{Br}_{\mathrm{nr}}(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

定理 2.16 にて，$\mathrm{rank}_{\mathbb{Z}} M \leq 6$ かつ $H^2_{\mathrm{nr}}(G, M) \neq 0$ となる群 $G$ は，すべて非可換群かつ可解群である．星-Kang-山崎 [HKY] は，$H^2_{\mathrm{nr}}(G, M) \neq 0$ (したがって $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0$) となるアーベル群 $G$ および非可解群 $G$ と $G$ 格子 $M$ をそれぞれ次のようにあたえている：

**定理 2.18** (星-Kang-山崎 [HKY, Theorem 6.1])**.** $G \simeq (C_2)^n \leq GL_7(\mathbb{Z})$ を位数 $2^n$ の基本アーベル群，$M$ を付随する $\mathbb{Z}$ 階数 7 の $G$ 格子とする．このとき，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^G) \neq 0 \Leftrightarrow G$ は [HKY, Theorem 6.1] の 9 個の群 $G_1, \ldots, G_9 \simeq (C_2)^3 \leq GL_7(\mathbb{Z})$ と共役．さらに，$\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^{G_i}) = H^2_{\mathrm{nr}}(G_i, M) \simeq \mathbb{Z}/2\mathbb{Z}$ $(1 \leq i \leq 8)$ かつ $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(M)^{G_9}) = H^2_{\mathrm{nr}}(G_9, M) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

**定理 2.19** (星-Kang-山崎 [HKY, Theorem 6.2])**.** $A_6$ を 6 次交代群とする．$A_6 \simeq PSL_2(\mathbb{F}_9)$ をつうじて，可移部分群 $A_6 \leq S_{10}$ とみなす．$N = \oplus_{1 \leq i \leq 10} \mathbb{Z} \cdot x_i$ を $\sigma \cdot x_i = x_{\sigma(i)}$ $(\sigma \in S_{10})$ によって定義された $S_{10}$ 格子の作用を $A_6$ に制限してえられる $A_6$ 格子，$M = N/(\mathbb{Z} \cdot \sum_{i=1}^{10} x_i)$ $(\mathrm{rank}_{\mathbb{Z}} M = 9)$ とする．このとき，$\mathbb{Q}$ 共役ではあるが $\mathbb{Z}$ 共役ではない $A_6$ 格子 $M = M_1, M_2, \ldots, M_6$ が存在して，

$$H^2_{\mathrm{nr}}(A_6, M_1) \simeq H^2_{\mathrm{nr}}(A_6, M_3) \simeq \mathbb{Z}/2\mathbb{Z}, \quad H^2_{\mathrm{nr}}(A_6, M_i) = 0 \ (i = 2, 4, 5, 6).$$

特に，$\mathbb{C}(M_1)^{A_6}$ と $\mathbb{C}(M_3)^{A_6}$ は $\mathbb{C}$ 上非レトラクト有理的．さらに，$M_1$ と $M_3$ は次のようにして Tate コホモロジー群で区別できる：

$$H^1(A_6, M_1) = 0, \qquad \widehat{H}^{-1}(A_6, M_1) = \mathbb{Z}/10\mathbb{Z},$$
$$H^1(A_6, M_3) = \mathbb{Z}/5\mathbb{Z}, \qquad \widehat{H}^{-1}(A_6, M_3) = \mathbb{Z}/2\mathbb{Z}.$$

定理 2.16 (2) (表 1) の 3 つの群 $G = D_4, Q_8, QD_8$ に対する $G$ 格子 $M$ は次のように一般化された：

**定理 2.20** (星-Kang-山崎 [HKY, Theorem 7.2])．$G = \langle \sigma, \tau : \sigma^{4n} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle \simeq D_{4n}$ $(n \geq 1)$ を位数 $8n$ の二面体群とする．$M$ を [HKY, Definition 7.1] の $\mathbb{Z}$ 階数 $2n+2$ の $G$ 格子とする．このとき，$H^2_{\mathrm{nr}}(G, M) \simeq \mathbb{Z}/2\mathbb{Z}$. とくに，$\mathbb{C}(M)^G$ は $\mathbb{C}$ 上非レトラクト有理的.

**定理 2.21** (星-Kang-山崎 [HKY, Theorem 7.5])．
(1) $G = \langle \sigma, \tau : \sigma^{8n} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{4n-1} \rangle \simeq QD_{8n}$ $(n \geq 1)$ を位数 $16n$ の準二面体群とする．$M$ を [HKY, Definition 7.4] の $\mathbb{Z}$ 階数 $4n$ の $G$ 格子とする．このとき，$H^2_{\mathrm{nr}}(G, M) \simeq \mathbb{Z}/2\mathbb{Z}$. とくに，$\mathbb{C}(M)^G$ は $\mathbb{C}$ 上非レトラクト有理的.
(2) $\widehat{G} = \langle \sigma^2, \sigma\tau \rangle \simeq Q_{8n} \leq G$ を位数 $8n$ の一般四元数群とする．$\widehat{M} = \mathrm{Res}^G_{\widehat{G}}(M)$ を [HKY, Definition 7.4] の $\mathbb{Z}$ 階数 $4n$ の $\widehat{G}$ 格子とする．このとき，$H^2_{\mathrm{nr}}(\widehat{G}, \widehat{M}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. とくに，$\mathbb{C}(\widehat{M})^{\widehat{G}}$ は $\mathbb{C}$ 上非レトラクト有理的.

以下は，$H^2_{\mathrm{nr}}(G, M) \simeq \mathbb{Z}/p\mathbb{Z}$ となる例である：

**定理 2.22** (星-Kang-山崎 [HKY, Theorem 7.7])．$p$ を奇素数，$G = \langle \sigma, \tau : \sigma^{p^2} = \tau^p = 1, \tau^{-1}\sigma\tau = \sigma^{p+1} \rangle \simeq C_{p^2} \rtimes C_p$ とする．$M$ を [HKY, Definition 7.6] の $\mathbb{Z}$ 階数 $p(p-1)$ の $G$ 格子とする．このとき，$H^2_{\mathrm{nr}}(G, M) \simeq \mathbb{Z}/p\mathbb{Z}$. とくに，$\mathbb{C}(M)^G$ は $\mathbb{C}$ 上非レトラクト有理的.

## 3　代数的トーラスの有理性問題

体 $L$ を体 $k$ のガロア拡大，$G = \mathrm{Gal}(L/k)$，$M = \bigoplus_{1 \leq i \leq n} \mathbb{Z} \cdot u_i$ を $\mathbb{Z}$ 基底 $\{u_1, \ldots, u_n\}$ の $G$ 格子 (有限生成 $\mathbb{Z}[G]$ 加群 $\simeq \mathbb{Z}^n$) とする．有限群 $G$ の有理関数体 $L(x_1, \ldots, x_n)$ への作用を

$$\sigma(x_i) = \prod_{j=1}^{n} x_j^{a_{ij}}, \quad 1 \leq i \leq n \tag{2}$$

とおく．ただし，$\sigma(u_i) = \sum_{j=1}^n a_{ij} u_j$ $(\sigma \in G,\, a_{ij} \in \mathbb{Z})$. この $G$ の作用をともなった体 $L(x_1, \ldots, x_n)$ を $L(M)$ とかく．

1 節の式 (1) の定義とは異なっている (“転置の関係” となっている) ことに注意してほしい．これは，次のような対応と適合するように作用の定義を変更したものである．$T$ を**代数的 $k$ トーラス** (algebraic torus over $k$, algebraic $k$-torus) とする．すなわち，$k$ 上の代数群で $T \otimes_k \overline{k} \simeq (\mathbb{G}_{m,\overline{k}})^n$; $k$ 上の分裂トーラス $(\mathbb{G}_{m,k})^n$ の $k$-form．このとき，有限次ガロア拡大 $L/k$ ($T$ の分解体 $K$) が存在して，$T \otimes_k L \simeq (\mathbb{G}_{m,L})^n$ となる．このとき，$G$ 格子の圏は $L$ で分裂する代数的 $k$ トーラスの圏と反同値となる (小野 [Ono61, Section 1.2], Voskresenskii [Vos98, page 27, Example 6], Knus-Merkurjev-Rost-Tignol [KMRT98, Proposition 20.17] 参照). 実際，$T$ を代数的 $k$ トーラスとすると，$T$ の指標加群 $X(T) = \mathrm{Hom}(T, \mathbb{G}_m)$ は $G$ 格子となる．逆に，$G$ 格子 $M$ に対して，$L$ で分裂する代数的 $k$ トーラス $T$ が存在して，$G$ 格子として $X(T) \simeq M$ となる．このとき，不変体 $L(M)^G$ は代数的 $k$ トーラス $T$ の関数体とみなせる．$T$ は関数体 $k(T) \simeq L(M)^G$ が $k$ 上 (安定, レトラクト) 有理的のとき，$k$ 上 (安定, レトラクト) 有理的という．また，$T$ は ($L(M)^G$ は) $k$ 上単有理的となる ([Vos98, page 40, Example 21] 参照). $n$ 次元代数的 $k$ トーラスから，ガロア降下および $\mathrm{Aut}(\mathbb{G}_m^n) = GL_n(\mathbb{Z})$ を通じて，集合 $H^1(\mathcal{G}, GL_n(\mathbb{Z}))$ へ全単射がある．ただし，$\mathcal{G} = \mathrm{Gal}(k_{\mathrm{s}}/k)$. $n$ 次元代数的 $k$ トーラスは整数表現 $h : \mathcal{G} \to GL_n(\mathbb{Z})$ によって共役を除いて一意的に決まる．ただし，$h(\mathcal{G}) \leq GL_n(\mathbb{Z})$ は有限部分群 ([Vos98, page 57, Section 4.9] 参照).

$K/k$ を体の $n$ 次分離拡大，$L/k$ を $K/k$ のガロア閉包，$G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$ とする．ガロア群 $G$ は可移部分群 $G \leq S_n$ とみなせる．次の $\mathbb{Z}[G]$ 加群の完全系列がある：

$$0 \longrightarrow I_{G/H} \longrightarrow \mathbb{Z}[G/H] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

ただし，$\varepsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$, $\sum_{i=1}^n a_i e_i \mapsto \sum_{i=1}^n a_i$, は添加写像 (augmentation map), $e_i = g_i H$ は $\mathbb{Z}[G/H]$ の $\mathbb{Z}$ 基底．双対をとれば，次の完全系列をえる：

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G/H] \longrightarrow J_{G/H} \longrightarrow 0.$$

とくに，$J_{G/H} = \mathrm{Hom}_{\mathbb{Z}}(I_{G/H}, \mathbb{Z})$ は $\mathbb{Z}$ 階数 $n-1$ の $G$ 格子で**シュバレー加群** (Chevalley module) とよばれる．さらに，代数的 $k$ トーラスの完全系列

$$1 \longrightarrow R^{(1)}_{K/k}(\mathbb{G}_{m,K}) \longrightarrow R_{K/k}(\mathbb{G}_{m,K}) \overset{N_{K/k}}{\longrightarrow} \mathbb{G}_m \longrightarrow 1$$

をえる．ここで，$R_{K/k}(\mathbb{G}_{m,K})$ は拡大 $K/k$ による乗法群 $\mathbb{G}_{m,K}$ の Weil 制限，$R^{(1)}_{K/k}(\mathbb{G}_{m,K})$ は $K/k$ のノルム 1 トーラスで指標加群 $X(R^{(1)}_{K/k}(\mathbb{G}_{m,K})) \simeq J_{G/H}$ である．このとき，$J_{G/H} = \oplus_{1 \le i \le n-1} \mathbb{Z} x_i$ とすれば，$G$ の $L(J_{G/H}) = L(x_1, \ldots, x_{n-1})$ への作用は式 (2) に他ならない．

1 次元代数的 $k$ トーラス ($\mathbb{G}_m$ および $[L:k]=2$ に対する $R^{(1)}_{L/k}(\mathbb{G}_m)$) は $k$ 上有理的である．2 次元および 3 次元代数的 $k$ トーラスの双有理分類はそれぞれ Voskresenskii [Vos67] および Kunyavskii [Kun90] によって完成された：

**定理 3.1** (Voskresenskii [Vos67], Kunyavskii [Kun90])．$k$ を体とする．
(1) (Voskresenskii [Vos67]) すべての 2 次元代数的 $k$ トーラスは $k$ 上有理的．特に，$G \simeq \mathrm{Gal}(K/k)$ の純半単項式作用による不変体 $K(x_1, x_2)^G$ は $k$ 上有理的．
(2) (Kunyavskii [Kun90], Kang [Kan12, Section 1] も参照) すべての 3 次元代数的 $k$ トーラスは [Kun90, Theorem 1] の 15 の例外を除いて $k$ 上有理的．15 の例外は $k$ 上非レトラクト有理的．

4 次元代数的 $k$ トーラスのうち，安定 (レトラクト) 有理的なものは星-山崎 [HY17] によって分類された．$GL_4(\mathbb{Z})$ の有限部分群の共役類は 227 個の $\mathbb{Q}$-class の中に 710 個の $\mathbb{Z}$-class がある．

**定理 3.2** (星-山崎 [HY17, Theorem 1.8])．$L/k$ を体のガロア拡大，有限部分群 $G \simeq \mathrm{Gal}(L/k) \le GL_4(\mathbb{Z})$ は $L(x_1, x_2, x_3, x_4)$ に式 (2) によって作用するとする．
(i) $L(x_1, x_2, x_3, x_4)^G$ は $k$ 上安定有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 2, 3, 4] に含まれない 487 個の群と共役．
(ii) $L(x_1, x_2, x_3, x_4)^G$ は $k$ 上非安定有理的かつレトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Table 2] の 7 個の群と共役．
(iii) $L(x_1, x_2, x_3, x_4)^G$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 3, 4] の 216 個の群と共役．

5 次元代数的 $k$ トーラスのうち，安定 (レトラクト) 有理的なものは，星-山崎 [HY17] によって分類された．$GL_5(\mathbb{Z})$ の有限部分群の共役類は 955 個の $\mathbb{Q}$-class の中に 6079 個の $\mathbb{Z}$-class がある．

**定理 3.3** (星-山崎 [HY17, Theorem 1.11])．$L/k$ を体のガロア拡大，有限部分群 $G \simeq \mathrm{Gal}(L/k) \le GL_4(\mathbb{Z})$ は $L(x_1, x_2, x_3, x_4)$ に式 (2) によって作用するとする．
(i) $L(x_1, x_2, x_3, x_4, x_5)^G$ は $k$ 上安定有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 11, 12, 13, 14, 15] に含まれない 3051 個の群と共役．
(ii) $L(x_1, x_2, x_3, x_4, x_5)^G$ は $k$ 上非安定有理的かつレトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Table 11] の 25 個の群と共役．
(iii) $L(x_1, x_2, x_3, x_4, x_5)^G$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 12, 13, 14, 15] の 3003 個の群と共役．

ノルム 1 トーラス $R^{(1)}_{K/k}(\mathbb{G}_m)$ の場合には，より多くの研究がある ([EM75], [CTS77], [Hür84], [CTS87], [LeB95], [CK00], [LL00], [Flo], [End11], [HY17], [HY], [HHY] 参照)．以下で，ノルム 1 トーラス $R^{(1)}_{K/k}(\mathbb{G}_m)$ の有理性問題に関して，知られている結果を紹介していく：

$K/k$ がガロア拡大のとき．

**定理 3.4.** $K/k$ を体のガロア拡大，$G = \mathrm{Gal}(K/k)$ とする．
(1) (遠藤-宮田 [EM75, Theorem 1.5], Saltman [Sal84b, Theorem 3.14])
$R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $G$ のすべてのシロー群は巡回群．
(2) (遠藤-宮田 [EM75, Theorem 2.3]) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上安定有理的 $\Leftrightarrow$ $G = C_m$ または $G = C_n \times \langle \sigma, \tau : \sigma^k = \tau^{2^d} = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ $(d \geq 1, k \geq 3,\ n, k$ は奇数で $\gcd\{n, k\} = 1)$.

$K/k$ が非ガロア拡大のとき．$L/k$ を $K/k$ のガロア閉包，$G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$ とする．

**定理 3.5** (遠藤 [End11, Theorem 2.1])．$G = \mathrm{Gal}(L/k)$ をべき零群とする．このとき，$R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上非レトラクト有理的．

**定理 3.6** (遠藤 [End11, Theorem 3.1])．$G = \mathrm{Gal}(L/k)$ のすべてのシロー群は巡回群とする．このとき，$R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上レトラクト有理的で，次は同値：
(i) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上安定有理的；
(ii) $G = D_n$ ($n \geq 3$ は奇数) または $G = C_m \times D_n$ ($m, n \geq 3$ は奇数, $\gcd\{m, n\} = 1$, $H = \mathrm{Gal}(L/K) \leq D_n$ は位数 2);
(iii) $H = C_2$, $G \simeq C_r \rtimes H$, $r \geq 3$ は奇数，$H$ は $C_r$ に非自明に作用する．

**定理 3.7** (遠藤 [End11, Theorem 4.1], see also [End11, Remark 4.2])．$\mathrm{Gal}(L/k) = S_n$ $(n \geq 3)$, $\mathrm{Gal}(L/K) = S_{n-1}$ は $S_n$ の 1 点固定群とする．
(1) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $n$ は素数；
(2) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上 ( 安定 ) 有理的 $\Leftrightarrow$ $n = 3$.

**定理 3.8** (遠藤 [End11, Theorem 4.4])．$\mathrm{Gal}(L/k) = A_n$ $(n \geq 4)$, $\mathrm{Gal}(L/K) = A_{n-1}$ は $A_n$ の 1 点固定群とする
(1) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $n$ は素数.
(2) ある $t \geq 1$ が存在して，$[R^{(1)}_{K/k}(\mathbb{G}_m)]^{(t)}$ は $k$ 上安定有理的 $\Leftrightarrow$ $n = 5$. ただし，$[R^{(1)}_{K/k}(\mathbb{G}_m)]^{(t)}$ は $R^{(1)}_{K/k}(\mathbb{G}_m)$ の $t$ 個の直積をあらわす.

$F_{20} \simeq C_5 \rtimes C_4$ を位数 20 のフロベニウス群とする．定理 3.2 より，以下がえられる,

**定理 3.9** (星-山崎 [HY17, Theorem 1.9])．$K/k$ を体の 5 次分離拡大，$L/k$ を $K/k$ のガロア閉包とする．可移部分群 $G = \mathrm{Gal}(L/k) \leq S_5$ は $L(x_1, x_2, x_3, x_4)$ に式 (2) によって作用し，$H = \mathrm{Gal}(L/K)$ は $G$ の 1 点固定群とする．
(1) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上安定有理的 $\Leftrightarrow$ $G \simeq C_5$, $D_5$, $A_5$;
(2) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上非安定有理的かつレトラクト有理的 $\Leftrightarrow$ $G \simeq F_{20}$, $S_5$.

定理 3.9 は $A_5$ の場合を除いてすでに得られていた (定理 3.4, 定理 3.6, 定理 3.7, 定理 3.8 参照). $A_5$ に対する，$R^{(1)}_{K/k}(\mathbb{G}_m)$ の安定有理性は遠藤 [End11, Remark 4.6] によって問題とされていた．定理 3.8 と定理 3.9 より，以下がえられる：

**系 3.10** (星-山崎 [HY17, Corollary 1.10])．$K/k$ を体の非ガロアな $n$ 次分離拡大，$L/k$ を $K/k$ のガロア閉包とする．$\mathrm{Gal}(L/k) = A_n$ $(n \geq 4)$, $\mathrm{Gal}(L/K) = A_{n-1}$ は $A_n$ の 1 点固定群とする．このとき，$R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上安定有理的 $\Leftrightarrow$ $n = 5$.

**定理 3.11** (星-山崎 [HY17, Theorem 1.13])．$K/k$ を体の 6 次分離拡大，$L/k$ を $K/k$ のガロア閉包とする．可移部分群 $G = \mathrm{Gal}(L/k) \leq S_6$ は $L(x_1, x_2, x_3, x_4, x_5)$ に式 (2) によって作用し，$H = \mathrm{Gal}(L/K)$ は $G$ の 1 点固定群とする．このとき，$R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上安定有理的 $\Leftrightarrow$ $G \simeq C_6$, $S_3$, $D_6$. さらに，$R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上非安定有理的ならば $k$ 上非レトラクト有理的.

この節で $k$ 上安定有理的と判定できたとき，実際に $k$ 上有理的かどうかは，ほとんどの場合よく分からない．これについては，以下の予想がある (Voskresenskii [Vos98, Chapter 2] 参照)：

**予想 3.12 (Voskresenskii 予想).** $k$ 上安定有理的な代数的 $k$ トーラスは $k$ 上有理的である．

さらに，$[K:k]=n\leq 15$ に対して，安定 (レトラクト) 有理的な $n-1$ 次元のノルム 1 トーラス $T=R^{(1)}_{K/k}(\mathbb{G}_m)$ の分類は，1 つの例外 $G\simeq 9T27\simeq PSL_2(\mathbb{F}_8)$ の安定有理性を除いて，星-山崎 [HY] ($n$ が素数または $n\leq 10$) と長谷川-星-山崎 [HHY] ($n=12,14,15$) によってあたえられた．

詳細は，長谷川寿人さんの 4 日目の講演で紹介される予定．

## 参考文献


[Bar89] J. Barge, *Cohomologie des groupes et corps d'invariants multiplicatifs*, Math. Ann. **283** (1989) 519–528.

[Bar97] J. Barge, *Cohomologie des groupes et corps d'invariants multiplicatifs tordus*, Comment. Math. Helv. **72** (1997) 1–15.

[Ber10] G. Berhuy, *An introduction to Galois cohomology and its applications*, With a foreword by Jean-Pierre Tignol. London Mathematical Society Lecture Note Series, 377. Cambridge University Press, Cambridge, 2010.

[Bog88] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Math. USSR Izv. **30** (1988) 455–485.

[BBNWZ78] H. Brown, R. Bülow, J. Neubüser, H. Wondratschek, H. Zassenhaus. *Crystallographic Groups of Four-Dimensional Space*, John Wiley, New York, 1978.

[CARAT] J. Opgenorth, W. Plesken, T. Schulz, CARAT, GAP 4 package, version 2.1b1, 2008, available from `http://wwwb.math.rwth-aachen.de/carat/`.

[CHKK10] H. Chu, S.-J. Hu, M. Kang, B. E. Kunyavskii, *Noether's problem and the unramified Brauer groups for groups of order* 64, Int. Math. Res. Not. IMRN **2010**, 2329–2366.

[CHKP08] H. Chu, S.-J. Hu, M. Kang, Y. G. Prokhorov, *Noether's problem for groups of order* 32, J. Algebra **320** (2008) 3022–3035.

[CK01] H. Chu, M. Kang, *Rationality of p-group actions*, J. Algebra **237** (2001) 673–690.

[CTS77] J.-L. Colliot-Thélène, J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. (4) **10** (1977) 175–229.

[CTS87] J.-L. Colliot-Thélène, J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: Applications*, J. Algebra **106** (1987) 148–205.

[CTS07] J.-L. Colliot-Thélène, J.-J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups* (*with special regards to the Brauer groups*), in "Proc. International Conference, Mumbai, 2004" edited by V. Mehta, Narosa Publishing House, 2007.

[CK00] A. Cortella, B. Kunyavskii, *Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000) 771–793.

[Dra83] P. K. Draxl, *Skew fields*, London Math. Soc. Lecture Note Series vol. 81, Cambridge Univ. Press, Cambridge, 1983.

[End11] S. Endo, *The rationality problem for norm one tori*, Nagoya Math. J. **202** (2011) 83–106.

[EM75] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85–104. Corrigenda: Nagoya Math. J. **79** (1980) 187–190.

[Fis15] E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen*, Nachr. Königl. Ges. Wiss. Göttingen (1915) 77–80.

[Flo] M. Florence, *Non rationality of some norm-one tori*, preprint (2006).

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. (http://www.gap-system.org).

[GMS03] S. Garibaldi, A. Merkurjev, J-P. Serre, *Cohomological invariants in Galois cohomology*, AMS Univ. Lecture Series, vol.28, Amer. Math. Soc., Providence, RI, 2003.

[GS06] P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, 101. Cambridge University Press, Cambridge, 2006.

[Haj87] M. Hajja, *Rationality of finite groups of monomial automorphisms of* $K(x, y)$, J. Algebra **109** (1987) 46–51.

[HK92] M. Hajja, M. Kang, *Finite group actions on rational function fields*, J. Algebra **149** (1992) 139–154.

[HK94] M. Hajja, M. Kang, *Three-dimensional purely monomial group actions*, J. Algebra **170** (1994) 805–860.

[HHY] S. Hasegawa, A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori in small dimensions*, to appear in Math. Comp., arXiv:1811.02145.

[HKK14] A. Hoshi, M. Kang, H. Kitayama, *Quasi-monomial actions and some 4-dimensional rationality problems*, J. Algebra **403** (2014) 363–400.

[HKY] A. Hoshi, M. Kang, A. Yamasaki, *Multiplicative invariant fields of dimension* $\leq 6$, arXiv:1609.04142.

[HKY11] A. Hoshi, H. Kitayama, A. Yamasaki, *Rationality problem of three-dimensional monomial group actions*, J. Algebra **341** (2011) 45–108.

[HR08] A. Hoshi, Y. Rikuna, *Rationality problem of three-dimensional purely monomial group actions: the last case*, Math. Comp. **77** (2008) 1823–1829.

[HY17] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. 248 (2017) no. 1176, v+215 pp.

[HY] A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori*, 12 pages. arXiv:1811.01676.

[Hür84] W. Hürlimann, *On algebraic tori of norm type*, Comment. Math. Helv. **59** (1984) 539–549.

[JLY02] C. U. Jensen, A. Ledet, N. Yui, *Generic polynomials*, Constructive aspects of the inverse Galois problem. Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, Cambridge, 2002.

[Kan90] M. Kang, *Constructions of Brauer-Severi varieties and norm hypersurfaces*, Canadian J. Math. **42** (1990) 230–238.

[Kan04] M. Kang, *Rationality problem of* $\mathrm{GL}_4$ *group actions*, Adv. Math. **181** (2004) 321–352.

[Kan05] M. Kang, *Some group actions on* $K(x_1, x_2, x_3)$, Israel J. Math. **146** (2005) 77–92.

[Kan12] M. Kang, *Retract rational fields*, J. Algebra **349** (2012) 22–37.

[Kar87] G. Karpilovsky, *The Schur Multiplier*, London Math. Soc. Monographs, vol.2, Oxford Univ. Press, 1987.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions*, With a preface in French by J. Tits. American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998.

[Kun54] H. Kuniyoshi, *On purely-transcendency of a certain field*, Tohoku Math. J. (2) **6** (1954) 101–108.

[Kun55] H. Kuniyoshi, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955) 65–67.

[Kun56] H. Kuniyoshi, *Certain subfields of rational function fields*, Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, 241–243, Science Council of Japan, Tokyo, 1956.

[Kun90] B. E. Kunyavskii, *Three-dimensional algebraic tori*, (Russian) Translated in Selecta Math. Soviet. **9** (1990) 1–21. Investigations in number theory (Russian), 90–111, Saratov. Gos. Univ., Saratov, 1987.

[Kun10] B. E. Kunyavskii, *The Bogomolov multiplier of finite simple groups*, Cohomological and geometric approaches to rationality problems, 209–217, Progr. Math., 282, Birkhäuser Boston, Inc., Boston, MA, 2010.

[LeB95] L. Le Bruyn, *Generic norm one tori*, Nieuw Arch. Wisk. (4) **13** (1995) 401–407.

[LL00] N. Lemire, M. Lorenz, *On certain lattices associated with generic division algebras*, J. Group Theory **3** (2000) 385–405.

[Len74] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974) 299–325.

[MT86] Y. I. Manin, M. A. Tsfasman, *Rational varieties: algebra, geometry and arithmetric*, Russian Math. Survey **41** (1986) 51–116.

[Mas55] K. Masuda, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955) 59–63.

[Mas68] K. Masuda, *Application of theory of the group of classes of projective modules to existence problem of independent parameters of invariant*, J. Math. Soc. Japan **20** (1968) 223–232.

[Miy71] T. Miyata, *Invariants of certain groups. I*, Nagoya Math. J. **41** (1971) 69–73.

[Ono61] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961) 101–139.

[PS00] W. Plesken, T. Schulz, *Counting crystallographic groups in low dimension*, Exp. Math. **9** (2000) 407–411.

[Pro10] Y. G. Prokhorov, *Fields of invariants of finite linear groups*, in "Cohomological and geometric approaches to rationality problems", edited by F. Bogomolov and Y. Tschinkel, Progress in Math. vol. 282, Birkhäuser, Boston, 2010.

[Roq63] P. Roquette, *On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras*, Math. Ann. **150** (1963) 411–439.

[Roq64] P. Roquette, *Isomorphisms of generic splitting fields of simple algebras*, J. Reine Angew. Math. **214/215** (1964) 207–226.

[Sal82a] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982) 250–283.

[Sal82b] D. J. Saltman, *Generic structures and field theory*, Algebraists' homage: papers in ring theory and related topics (New Haven, Conn., 1981), pp. 127–134, Contemp. Math., 13, Amer. Math. Soc., Providence, R.I., 1982.

[Sal84a] D. J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984) 71–84.

[Sal84b] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984) 165–215.

[Sal85] D. J. Saltman, *The Brauer group and the center of generic matrices*, J. Algebra **97** (1985) 53–67.

[Sal87] D. J. Saltman, *Multiplicative field invariants*, J. Algebra **106** (1987) 221–238.

[Sal90a] D. J. Saltman, *Twisted multiplicative field invariants, Noether's problem and Galois extensions*, J. Algebra **131** (1990) 535–558.

[Sal90b] D. J. Saltman, *Multiplicative field invariants and the Brauer group*, J. Algebra **133** (1990) 533–544.

[Sal00] D. J. Saltman, *A nonrational field, answering a question of Hajja*, Algebra and number theory, Lecture Notes in Pure and Appl. Math., 208, 263–271, Dekker, New York, 2000.

[Ser79] J-P. Serre, *Local fields*, Springer GTM vol. 67, Springer-Verlag, Berlin, 1979.

[Ser02] J-P. Serre, *Galois cohomology*, Translated from the French by Patrick Ion and revised by the author. Corrected reprint of the 1997 English edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002

[Swa69] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969) 148–158.

[Swa83] R. G. Swan, *Noether's problem in Galois theory*, in "Emmy Noether in Bryn Mawr", edited by B. Srinivasan and J. Sally, Springer-Verlag, Berlin, 1983, pp. 21–40.

[Vos67] V. E. Voskresenskii, *On two-dimensional algebraic tori II* Math. USSR Izv. **1** (1967) 691–696.

[Vos98] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, Translated from the Russian manuscript by Boris Kunyavskii, Translations of Mathematical Monographs, 179. American Mathematical Society, Providence, RI, 1998.

[Yam12] A. Yamasaki, *Negative solutions to three-dimensional monomial Noether problem*, J. Algebra **370** (2012) 46–78.

Akinari Hoshi
Department of Mathematics
Niigata University
8050 Ikarashi 2-no-cho
Nishi-ku, Niigata, 950-2181
Japan
E-mail: `hoshi@math.sc.niigata-u.ac.jp`
Web: `http://mathweb.sc.niigata-u.ac.jp/~hoshi/`

# 冪根を含まない体のクンマー理論について*

木田雅成

**概 要**

第 27 回サマースクールでの講演の報告である．代数的トーラスを使って，冪根のない体にクンマー理論を拡張することを解説した．

## 1 理論的な枠組み

$k$ を体とする．$\bar{k}$ を $k$ の分離閉包とし，一つ固定する．$m$ を $k$ の標数と互いに素な 2 以上の整数とする．$k^\times$ が 1 の $m$ 乗根の群 $\mu_m$ を含むと仮定する．完全系列

$$1 \longrightarrow \mu_m \longrightarrow \bar{k}^\times \overset{m\text{ 乗写像}}{\longrightarrow} \bar{k}^\times \longrightarrow 1$$

から，ガロア・コホモロジーをとることによって，

$$\begin{array}{ccccc} 1 & \longrightarrow & k^\times/(k^\times)^m & \longrightarrow & \mathrm{H}^1(k,\mu_m) \\ & & & & \| \\ & & & & \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k),\mu_m) \end{array} \longrightarrow \begin{array}{c} \mathrm{H}^1(k,\bar{k}^\times) \\ \| \\ 1 \end{array}$$

がヒルベルトの定理 90 によって得られ，

$$k^\times/(k^\times)^m \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k),\mu_m)$$

というクンマー双対が得られるというのが古典的なクンマー理論である．これから $k$ の任意の $m$ 次巡回拡大がある $a \in k^\times$ を使って，$k(\sqrt[m]{a})$ と書けることが導かれる．このクンマー理論が代数学，数論に多くの応用を持つことは周知の通りである．

この古典的な場合を乗法群 $\mathbb{G}_{m,k}$ のクンマー理論だと考えて，それを次のような枠組みで一般化することを考えよう．$k$ を体として $G/k$ を可換な代数群とする．まず

(P1)　$m$ 次巡回自己同種写像 $\lambda/k : G \longrightarrow G$ が存在する

*この研究は文部科学省科学研究費補助金基盤研究 (C) (No.15K04798) の援助をうけて行われています．

ことを仮定すると，完全系列

$$1 \longrightarrow \ker(\lambda) \longrightarrow G \xrightarrow{\lambda} G \longrightarrow 1$$

が得られる．ガロア・コホモロジーをとると，

$$1 \longrightarrow G(k)/\lambda G(k) \longrightarrow \mathrm{H}^1(k, \ker(\lambda)(\bar{k})) \longrightarrow \mathrm{H}^1(k, G(\bar{k}))[\lambda]$$

が導かれる．ここで $\mathrm{H}^1(k, G(\bar{k}))[\lambda]$ は $\lambda$ が $\mathrm{H}^1(k, G(\bar{k}))$ に引き起こす自己準同型の核である．ここでさらに

$$\text{(P2)} \quad \ker(\lambda)(\bar{k}) = \ker(\lambda)(k)$$

ならば

$$\mathrm{H}^1(k, \ker(\lambda)(\bar{k})) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker(\lambda)(\bar{k}))$$

となる．さらに

$$\text{(P3) 弱ヒルベルト 90} \quad \mathrm{H}^1(k, G(\bar{k}))[\lambda] = 1$$

が成り立てば，最終的にクンマー双対

$$G(k)/\lambda G(k) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker(\lambda)(\bar{k}))$$

を得ることができる．この同型はコホモロジーの連結準同型から誘導されるものであり，具体的には次のように与えられる．$P \in G(k)$ に対し，$\lambda(Q) = P$ をみたす $Q \in G(\bar{k})$ を選び，$P$ に対応する指標 $\chi_P \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker(\lambda)(\bar{k}))$ を $\tau \in \mathrm{Gal}(\bar{k}/k)$ に対し，$\chi_P(\tau) = Q^{\tau-1}$ とする．これから，古典的な場合と同様に，$k$ の任意の $m$ 次巡回拡大は $k(Q) = k(\lambda^{-1}(P))$ の形に書けることがわかる．もし体 $k$ が冪根を含まないようにとれれば，冪根を含まない体についてもクンマー理論が成り立つことになる．

これまで，中心的に研究されてきたのは代数群 $G$ が代数的トーラスの場合で，次の場合に，拡大体 $K/k$ をうまく選ぶと，上記の (P1),(P2),(P3) が成り立つことがわかっている．

(i) ([10]). 乗法群の Weil 制限 $R_{K/k}\mathbb{G}_m$.

(ii) ([13]). $M$ を $K/k$ の中間体とするとき，相対ノルム $N_{K/M} : K^\times \longrightarrow M^\times$ が誘導する写像の核

$$\ker(N_{K/M} : R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m).$$

(ii) で $M = k$ とするとき，上のトーラスは $R^{(1)}_{K/k}\mathbb{G}_m$ になり，この場合が [5] で研究された場合である．また，$K/k$ が 2 次拡大で，このトーラスが 1 次元の場合が小松 [15] あるいは小川 [20] で調べられ，一連の研究の発端となった場合である．これらの先行研究については最後の節でまとめて述べることにする．

# 2　クンマー理論

この節では，前節で述べた条件 (P1), (P2), (P3) がみたされるような状況をどのようにして作り出すかを解説する．(P1), (P2) をみたす $\lambda$ を作るのが問題である．(P3) に関してはこれが成り立つような代数的トーラスをとるということで解決する．

一般に $T$ を体 $k$ 上定義された代数的トーラスとし，$k$ のガロア拡大体 $K$ で分解するとする．すなわち，$T \times K \cong \mathbb{G}_{m,K}^{\dim T}$. このとき，$T$ の指標加群 $\widehat{T} = \mathrm{Hom}_{K\text{-gr}}(T \times_k K, \mathbb{G}_{m,K})$ は，階数 $\dim T$ の自由 $\mathbb{Z}$ 加群で $G = \mathrm{Gal}(K/k)$ が作用する．$T$ の自己同種写像 $\lambda$ を見つけたければ，その双対である $\widehat{T}$ の $G$ 自己準同型でその余核が有限になるものを見つければよい．したがって，$\widehat{T}$ を計算して，その $G$ 自己準同型を計算しなければならない．この部分はどのような $T$ をとるかに関わらず必要な計算である．

以下では $T$ として，$R^{(1)}_{K/k}\mathbb{G}_m$ をとり，[13] にしたがって，冪根の含まれない体のクンマー理論の定理を紹介し，(P1), (P2), (P3) をどのように示すかの概要を示そう．

整数 $n$ に対して $R(n)$ で $n$ の 1 以外の約数全体をあらわす．

**定理 2.1.** $m$ を 1 より大きい整数とし，$n$ を $m$ と互いに素な $\varphi(m)$ の約数とする．

次数が $n-2$ 次以下の整係数多項式

$$\mathscr{P}(t) = c_1 + c_2 t + \cdots + c_{n-s-1}t^{n-2} \in \mathbb{Z}[t] \tag{2.1}$$

と，$R(n)$ の部分集合 $R$ と，$R$ の元を添字にもつ，2つごとに互いに素な整数 $m_r\,(r \in R)$ が存在して以下の条件をみたすとする．

*(i)* $n = \mathrm{lcm}\{r \mid r \in R\}$;

*(ii)* $\displaystyle\prod_{r\in R} m_r = m$;

*(iii)* $r \in R$ なら，同型

$$\mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \cong \mathbb{Z}/m_r\mathbb{Z} \tag{2.2}$$

が成り立つ．

*(iv)* $r \in R(n)\backslash R$ なら

$$\mathscr{P}(\zeta_r) \in \mathbb{Z}[\zeta_r]^\times \tag{2.3}$$

が成り立つ．

$k$ を標数が $m$ と互いに素な体で，環準同型 (2.2) が群同型

$$\nu_k \,:\, \mathrm{Gal}(k(\zeta_m)/k) \xrightarrow{\sim} \langle \zeta_r \bmod \ \mathscr{P}(\zeta_r) \mid r \in R\rangle \tag{2.4}$$

を誘導するようなものとする．$K = k(\zeta_m)$ とし，$T = R^{(1)}_{K/k}\mathbb{G}_m$ とする．

これらの条件のもとで，$T$ の次数 $m$ の巡回自己同種写像 $\lambda$ で，条件 $\ker\lambda(\bar{k}) = \ker\lambda(k)$ をみたすものが存在し，$\lambda$ に付随する完全系列

$$1 \longrightarrow \ker\lambda \longrightarrow T \xrightarrow{\lambda} T \longrightarrow 1$$

はクンマー双対

$$\kappa_k \ : \ T(k)/\lambda T(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda(\bar{k})). \tag{2.5}$$

を誘導する．

**証明の概要**. 拡大 $K/k$ はあとで具体的にその定め方をみることにして，まず一般に $K/k$ が巡回拡大のときに $T = R^{(1)}_{K/k}\mathbb{G}_m$ の指標加群 $\widehat{T}$ の自己同型環を計算する．$G = \mathrm{Gal}(k/k) = \langle\tau\rangle$ とする．$\widehat{T} = \mathrm{Hom}(\ker\varepsilon, \mathbb{Z})$ であることが知られている．ここで $\varepsilon : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ は augumentaion map である．$\ker\varepsilon$ の基底として $\tau^i - \tau^{i-1}$ $(i = 1, \ldots, n-1)$ をとると，行列の形で計算する．$[K:k]-1$ 次行列

$$S = \begin{bmatrix} -1 & -1 & \cdots\cdots & -1 \\ 1 & 0 & \cdots\cdots & \\ 0 & 1 & 0 & \cdots\cdots \\ & \cdots\cdots\cdots & & \\ 0 & 0 & \ldots & 1 \quad 0 \end{bmatrix}$$

で定義すると，$G = \mathrm{Gal}(K/k)$ として，

$$\mathrm{End}_G(\widehat{T}) \cong \mathbb{Z}[S]$$

となることがわかる．したがって，求める $\widehat{T}$ の自己同型は (2.1) の形の多項式 $\mathscr{P}(t)$ を使って，$\Lambda = \mathscr{P}(S)$ とかける．$\Lambda$ の余核を計算すると，

$$\mathrm{Coker}\Lambda \cong \bigoplus_{r\in R(n)} \mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \tag{2.6}$$

となることがわかる．定理の条件 (iii), (iv) により，余核は $\oplus_{r\in R}\mathbb{Z}/m_r\mathbb{Z}$ に同型であり，(ii) と $m_r$ たちが互いに素であることから，この群は位数 $m$ の巡回群になる．$\lambda$ を $\Lambda$ に対応する $\mathrm{End}(T)$ の元とすると，$\lambda$ は $k$ 上定義された次数 $m$ の巡回同種写像となり (P1) がみたされる．

ここで基礎体 $k$ を次のように決める．標数が $m$ と素な体 $k_0$ をとり，$K_0 = k_0(\zeta_m)$ とおく．$\mathrm{Gal}(K_0/k_0)$ を $(\mathbb{Z}/m\mathbb{Z})^\times$ の部分群と同一視する．このとき，この部分群が十分大きくなるように $k_0$ をとっておく．(2.2) の同型での $\zeta_r$ の像を $\sigma_r$ とする．$\sigma_r$ $(r \in R)$ が $\oplus_{r\in R}(\mathbb{Z}/m_r\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times$ において生成する部分群を $H$ とする．すべての $r$ が $n$ の約数であることに注意すると，(i) から，$H$ の位数は $n$ になる．$k = K_0^H$ とし，$K = k(\zeta_m)$ とすれば，(2.4) をみたす拡大体 $K/k$ がとれたことになる．$n = [K:k]$ であって $n \mid \varphi(m)$ をみたしている．

$\lambda$ が (P2) をみたすことを示すために，(2.6) を使って，$\Lambda$ の余核を具体的に計算する．法 $m$ での座標がわかるので，それから $\lambda$ の核の具体的な表示がえられる．これから (P2) が成り立つ．

(P3) は次のように示される．完全系列

$$1 \longrightarrow \ker\lambda \longrightarrow T \xrightarrow{\lambda} T \longrightarrow 1$$

のガロア・コホモロジーをとると，

$$T(k) \xrightarrow{\lambda} T(k) \longrightarrow \mathrm{H}^1(k, \ker\lambda) \longrightarrow \ker\Big(\lambda : \mathrm{H}^1(k,T) \longrightarrow \mathrm{H}^1(k,T)\Big).$$

一方，完全系列

$$1 \longrightarrow T \longrightarrow R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/k}} \mathbb{G}_{m,k} \longrightarrow 1$$

から，

$$R_{K/k}\mathbb{G}_m(k) \xrightarrow{N_{K/k}} \mathbb{G}_{m,k}(k) \longrightarrow \mathrm{H}^1(k,T) \longrightarrow \mathrm{H}^1(k, R_{K/k}\mathbb{G}_m) \text{ (完全).}$$

Shapiro の補題とヒルベルトの定理 90 から，

$$\mathrm{H}^1(k, R_{K/k}\mathbb{G}_m) \cong \mathrm{H}^1(K, \mathbb{G}_{m,K}) = 1.$$

標準的な同型 $R_{K/k}\mathbb{G}_m(k) \cong K^\times$ のもとで，

$$\mathrm{H}^1(k,T) \cong k^\times / N_{K/k}K^\times.$$

右辺は $[K : k]$ 乗で消える群である．一方 $m = \deg\lambda$ は $n$ と互いに素だから，$\mathrm{H}^1(k,T)[\lambda] = 1$ をえる． □

補注 2.2. 条件 (2.2) から，$\mathscr{P}(\zeta_r)$ の生成する単項イデアルは剰余標数が相異なる次数 1 の素イデアルの積にならなくてはいけない．特に $m_r$ および $m$ は平方因子を持たない．

補注 2.3. この定理をスキーム理論を使って述べたものが [26] にある．特に核の決定に関しては同論文 Remark 3.5 が明快な記述を与えているようである．

この定理から，同型 (2.5) が成り立つような $[k(\zeta_m) : k] = n$ をみたす体 $k$ 上の $m$ 次巡回拡大が全てクンマー拡大としてえられることになる．それらは $T(k)$ の元でパラメータづけされていると考えると，$T(k) \cong \ker(N_{K/k} : K^\times \longrightarrow k^\times)$ だから $k$ 上の $n$ 個のパラメータ（そのパラメータには 1 つの関係式がはいる）を含む多項式で定義されることになる．これからわかるように，代数的トーラスの次元が小さいほど，パラメータの個数は少なくなる．その方向に議論をすすめると，相対ノルムのトーラスを使った [13] になる．

いろいろな都合があって，論文 [13] にしたがって，定理を述べたが，$R_{K/k}\mathbb{G}_m$ を使った [10] が一番定式化が素直で，証明も簡明である．

## 3 いくつかの例

この節では定理 2.1 が成立するような例をいくつかあげる．

例 3.1 (2 次降下 [5, Example 6.1]). $m$ を平方因子を持たない正の奇数とする．$n = 2$ とする．$R(2) = R = \{2\}$ とする．$\mathscr{P}(t) = \dfrac{m+1}{2} + \dfrac{1-m}{2}t \in \mathbb{Z}[t]$ とすると，$\mathscr{P}(-1) = m$ であるから (2.2) は

$$\mathbb{Z}[-1]/\mathscr{P}(-1)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$$

となる．$K = \mathbb{Q}(\zeta_m)$ とし，$H = \langle -1 \bmod m \rangle$ の固定体 $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ を $k$ ととって，$T = R^{(1)}_{K/k}\mathbb{G}_m$ とする．$T$ は 1 次元トーラスになる．$\mathscr{P}(S) = m$ であるから，$\lambda$ は $T$ の $m$ 乗写像である．よってこのトーラス $T$ に関してクンマー双対が成立する．これが小松 [15]，小川 [20] で扱われた場合である．最大実部分体上で generic 巡回多項式を簡単な形で書いた [22] もこの文脈で理解される．

$1, \sqrt{d} = (\zeta_m^2 - \zeta_m^{-2})$ を基底にとって，$T$ 上の $m$ 乗写像を計算すると，本質的にチェエビシェフ多項式が座標に現れる．

例えば $m = 3$ とすると，$k = \mathbb{Q}$ となり，クンマー拡大を定義する多項式が $(u_1 : u_2) \in \mathbb{P}^1(\mathbb{Q})$ をパラメータとして

$$4x^3 - 3x = \frac{u_1^2 - 3u_2^2}{u_1^2 + 3u_2^2}$$

と求められる．(詳細については [5, Example 6.1] を見よ)．パラメータ $u_1, u_2$ に $\mathbb{Q}$ の元を代入すれば $\mathbb{Q}$ 上の巡回 3 次拡大が得られ，逆に任意の $\mathbb{Q}$ 上の巡回 3 次拡大はこの形で得られる．

例 3.2 (基礎体として有理数体が取れる場合). 例 3.1 の $m = 3$ の場合以外にも，次の場合には基礎体として $\mathbb{Q}$ が取れることがわかる．すべて，$R = \{m-1\}$ ととればよい．

| $\mathscr{P}(t)$ | $m$ |
|---|---|
| $2t+1$ | 5 |
| $t+2$ | 7 |
| $2t^3 - t^2 + t$ | 11 |

例 3.3 ($|R| \geq 2$ の場合 [13, Example 4.4]). $n = 6$ とする．$R(6) \supset R = \{3, 6\}$ をとる．多項式 $\mathscr{P}(t) = t^4 + t^3 + 2t^2 + 3t + 2$ は

$$\mathscr{P}(-1) = 1, \quad \mathscr{P}(\zeta_3) = 2\zeta_3 + 1, \quad \mathscr{P}(\zeta_6) = 4\zeta_6 - 1$$

をみたすから，

$$\mathbb{Z}[\zeta_3]/(2\zeta_3 + 1) \cong \mathbb{Z}/3\mathbb{Z}, \qquad \zeta_3 \mapsto 1,$$

$$\mathbb{Z}[\zeta_6]/(4\zeta_6 - 1) \cong \mathbb{Z}/13\mathbb{Z}, \qquad \zeta_6 \mapsto 10.$$

となり定理 2.1 の諸条件がみたされる．$k$ を $\mathbb{Q}(\zeta_{39})$ の部分体で $\zeta_{39} \mapsto \zeta_{39}^{10}$ で固定されるものとする．計算により $x^4 + x^3 - 11x^2 + 9x + 3$ が $k$ の定義多項式であることがわかる．$\mathscr{P}(t)$ できまる $T = R^{(1)}_{\mathbb{Q}(\zeta_{39})/k}\mathbb{G}_m$ の同種写像の逆像により，4 次体 $k$ を含む体上の 39 次巡回拡大がすべてえられる．

このようなクンマー拡大では，体の生成元 $Q = \lambda^{-1}(P)$ へのガロア群の作用は $Q$ に $\ker\lambda$ の元をかけることで得られる．これを利用すると，$Q$ の座標を根に持つような多項式を具体的に計算することができる．詳細は [7] をみよ．

# 4　クンマー拡大の数論

古典的なクンマー拡大は単純な生成元をもち，そのガロア作用も 1 の冪根のかけ算という形でよくわかる．このことから，特に基礎体が代数体である場合に，その数論的な性質が詳しく調べられ，クンマー拡大は代数拡大体の構成において基本的なツールになっている．これらが，われわれのクンマー理論の場合にどのように一般化されるかをみるのがこの節の目的である．

## 4.1　分岐の記述

$k$ を代数体とする．クンマー拡大 $k(\sqrt[n]{a})/k$ で $n$ または $a$ をわる $k$ の素イデアル以外は不分岐であることはよく知られている．$n$ が素数の場合は Hecke の理論として知られる詳細な分岐理論がある（例えば [1, Theorem 10.2.9] を見よ）．

トーラスを使ったクンマー拡大の場合も，$P \in T(k)$ に対応するクンマー拡大 $k(\lambda^{-1}(P))$ においては，標準的な同一視で $P \in K^\times$ とみたときに，$P$ または $m$ をわる $k$ の素イデアルしか分岐しないことが示されている ([10, Proposition 6.3])．

Hecke の理論に対応する分岐理論は 1 次元のノルムトーラスの場合に小松 [15] で研究が行われた．一般の場合は，小野 [21] のアイディアに基づいて，局所体上のトーラスの指標加群にフィルター付けを行い，それを使って，局所体の巡回拡大の導手の付値を求めることができる．詳細は島倉 [23] を見ていただきたい．

## 4.2　Artin map

ふたたび $k$ を代数体とする．クンマー拡大 $k(\sqrt[n]{a})/k$ の Artin 写像は具体的に計算することができる ([1, Proposition 5.4.1])．

$\mathbb{Q}$ 上の巡回 3 次拡大を 1 次元のノルムトーラスからくるクンマー拡大とみて，Artin map を計算したのが，小松 [16] である．

## 4.3 Equivariant Kummer theory

$k_0$ を通常の $m$ 次のクンマー理論が成り立つ体とする．このとき $k_0$ の任意の拡大体 $k$ でクンマー理論が成り立つ．$k/k_0$ がガロア拡大であれば $\mathrm{Gal}(k/k_0)$ が $k^\times/(k^\times)^m$ に作用し，この作用で不変な部分空間に対応するクンマー拡大は $k_0$ 上のガロア拡大になる．これが節題の equivariant Kummer theory である ([2, Theorem 1.26]).

$k/k_0$ をその次数が $m$ と素なアーベル拡大にとると，$\mathrm{Gal}(k/k_0)$ の指標で $k^\times/(k^\times)^m$ を固有空間に分解できる．この場合に，上の定理の特別な場合が [1, Theorem 5.3.5 (1)] にのっている．この定理の一般化を使って $\mathbb{Q}$ 上のいろいろな metacyclic 拡大を構成したのが [19] である．ここで群 $G$ が metacyclic であるとは，$G$ が巡回群の巡回群による拡大になること，すなわち，ある $u, v \in \mathbb{N}$ に対して完全系列

$$1 \longrightarrow C_u \longrightarrow G \longrightarrow C_v \longrightarrow 1$$

が存在することである．上記の論文 [19] では，クンマー理論で構成した体を冪根を含まない体に落とす際に，トレイスが使われている．これは [1, Theorem 5.3.5 (2)] を素直にならった構成だが，トレイスを使うとクンマー生成元のもつ乗法的な情報が欠落してしまう．

そこで，トーラスを使ったクンマー理論を使って metacyclic 拡大を構成する試みを行ったのが [12] である．(2.5) にあらわれる，$T(k)/\lambda T(k)$ を上と同様にアーベル群の作用で不変部分空間にわける．適用範囲が狭くなるものの，metacyclic 拡大が Kummer 拡大として得られ，しかもその部分体の情報を含んだ形で得られる．とくに $\mathbb{Q}$ 上のクンマー理論が存在する $m = 3, 5, 7, 11$ に対して，二面体群 $D_m$ やフロベニウス群 $F_{m(m-1)}$ などの群をガロア群にもつ拡大体がクンマー拡大で実現される．日韓シンポジウムの報告集に掲載された [11] にこの方法で計算した $S_3$ クンマー多項式の例がある．

## 4.4 代数的トーラスを楕円曲線に取り替える

代数的トーラス $T$ を他の代数群に取り替えることは容易に思いつくアイディアであろう．たとえば楕円曲線に取り替えると，自己同種写像だけを考えていても，虚数乗法を持たない場合は巡回拡大がえられない．一般の同種写像を考えて，クンマー拡大を作ることは例えば [14] や [9] で行われている．[18] はその先駆的仕事である．[14] では次のような形の単射準同型が得られている．

$$E_{a,b}(\mathbb{Q})/\phi^*(E^*_{a,b}(\mathbb{Q})) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker \lambda^*(\mathbb{Q})).$$

くわしい説明はしないが，$E_{a,b}, E^*_{a,b}$ はパラメータ $a, b$ をもつ楕円曲線，$\lambda^*, \phi^*$ はある同種写像である．この単射の左辺は弱モーデル・ヴェイユの定理から有限群で，右辺の群のほんの一部の情報しかもっていない．同論文では，パラメータ $a, b$ を動かすことにより，右辺の群の情報を回復している．

[18] や [9] では，楕円曲線を使った metacyclic 拡大の構成についても述べられている．

# 5 いくつかの課題

以上の節で，現在までの研究を振り返ったので，これをふまえて，いくつか今後の課題を述べよう．

## 5.1 クンマー生成元を求める

通常のクンマー拡大では， Lagrange resolvent を使って，$K = k(\sqrt[m]{a})$ となる $a \in k^\times$ が求められる ([1, Theorem 5.3.5 (4)])．それでは，巡回拡大 $K/k$ が巡回同種写像 $\lambda$ に関するクンマー拡大であることがわかっているとき，$K = k(\lambda^{-1}(P))$ をみたす $P \in T(k)$ を求めるにはどうすればよいか．

Artin map が一般の場合にも計算できれば，[1, Section 5.4] で説明されている方法が使えるかもしれない．

## 5.2 イデアル類群の鏡映定理

イデアル類群の鏡映定理というのは Scholz によって証明された，$\mathbb{Q}(\sqrt{d})$ と $\mathbb{Q}(\sqrt{-3d})$ のイデアル類群の 3-rank の関係を与える定理である ([27, Theorem 10.10])．その証明にはクンマー理論，ガロア理論，類体論が三位一体で使われる．この場合には $\mathbb{Q}(\sqrt{-3})$ が円分体であるから，クンマー理論が使えるわけだが，ここで前節までで説明したクンマー理論を使ったらどうなるだろう．別の体の組であったり，3-rank ではなく 5-rank であったりというふうに拡張できるだろうか．[4] の拡張や簡単な証明が得られたりするだろうか．

[20] の第 4 節にも同様の問題がのっている．この節にはいろいろな課題がのっているがどれも手付かずであろうと推測される．

## 5.3 代数群を取りかえる

まず，これまで研究されてきた代数的トーラス以外の代数的トーラスをとると，クンマー理論の適用範囲は広がるだろうか．$R^{(1)}_{K/k}\mathbb{G}_m$ と $R_{K/k}\mathbb{G}_m$ では適用範囲が変わらないことが [10, Section 6] で示されている．[17] にリストのある 2 次元や 3 次元の代数的トーラスに限って具体的に調べてみてもよいかもしれない．また自己同種写像だけでなく，一般の同種写像についても調べる価値があるかもしれない．

4.4 節で述べたように代数群をアーベル多様体に取りかえるのも一つのアイディアである．楕円曲線だけを考えていると，大きい核を持つ同種写像が得られない

ので，高次元のものも考える必要があろう．その場合でも弱モーデル・ヴェイユの定理があるので，なんらかの族を考える必要がある．ただし，実際に巡回多項式を計算することなどは容易ではないであろう．

究極には可換代数群だけではなく，非可換代数群も考えてはどうだろうか．クンマー双対の定式化をどうすればよいのか，私にはよくわからないが，非可換なガロア群をもつ拡大が，クンマー拡大として得られれば，とてもおもしろいのではないだろうか．

## 6　先行研究に関する覚書

昔から，クンマー理論を冪根のない体に拡張しようとする試みはいろいろあるようだが，それらをすべて調べ上げ，解説するのは私の手に余る．ここでは第2節で解説した研究に直接つながるものだけを覚書風に書いておくことにとどめる．

まずあげなければいけないのは小松 [15] である．橋本・三宅 [3] の仕事をうけて，最大実部分体上で簡明な形の generic 巡回方程式を作った陸名 [22] の仕事を「2次降下」クンマー理論として定式化したのがこの小松さんの仕事である．私は，そのころ活発に研究されていた generic 多項式に関するいろいろな結果の素晴らしさは別にして，証明の中で使われる巧妙な式変形，華麗な変数変換に，かなり近寄りがたい印象を受けていた．小松さんの仕事を知ったとき（それは確か立命館大学での小規模な研究集会の時であったと記憶する），「こういう風にやる方法もあるのか」と蒙を啓かれる思いだった．小松さん自身は巡回多項式への興味が強かったと思うが，私は初めから体の理論としてのクンマー理論の一般化を考える方に興味があった．そのような意識を共有していたのが，阪大の小川さんだったように思われる．残念ながら彼のこの方面の論文は [20] しかない．以上が2002年の出来事である．

その後，私は2003年10月から2004年7月にかけて文部科学省長期在外研究員として，ローマに滞在した．ホストの Schoof さんのもとで非常に楽しい滞在であったが，その間，小松さんの仕事を高次元に拡張することを考えた．高次元の代数群に関する知識はほとんどないに等しかったので，小野先生の [21] などを読みながら，手探りで拡張を探った．はじめは，小松さんのやり方を踏襲して，冪乗写像を使っていて，巡回同種写像が必要なことがすぐには気づかなかった．同種写像を双対である指標加群に構成することができると，あとはいろいろな計算が，自分でも驚くほど順調に進み，その結果としてできあがったのが [5] である．帰国後2004年の数理研の研究集会での講演の記録が [6] である．

小川さんや小松さんの定式化を群スキームの枠組みで拡張したのが，諏訪さんの [24] で，2004年の上記の数理研の研究集会でも，その内容を講演している．その後，諏訪さんは，今回紹介した定理を含めて，それらを環上に一般化した理論を群スキームの洗練された言葉で書いたものを論文にしている ([25], [26] など)．幾

何の達者な方には私の論文よりも諏訪さんの論文の方が読みやすいであろう.

**謝辞** このサマースクールで講演の機会をいただけたことに対し，世話人の皆様に深く感謝します．2015年には完成稿ができていたにもかかわらず，諸事情からお蔵入りになりかけていた [13] を出版するきっかけにもなったことを記しておきます.

# 参考文献

[1] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 2000.

[2] P. Guillot, *A gentle course in local class field theory*, Cambridge University Press, Cambridge, 2018.

[3] K.-I. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications (Kyoto, 1997), Dev. Math., vol. 2, Kluwer Acad. Publ., Dordrecht, 1999, pp. 165–181.

[4] M. Imaoka and Y. Kishi, *On dihedral extensions and Frobenius extensions*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 195–220.

[5] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447.

[6] ———, **ノルム・トーラスのクンマー理論**, 数理解析研究所講究録 (2005), no. 1451, 237–242, Algebraic number theory and related topics (Japanese) (Kyoto, 2004).

[7] ———, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 102–113.

[8] ———, **冪根を含まない体のクンマー理論について**, 第5回北陸数論研究集会報告集, 2006, pp. 87–94.

[9] ———, $D_5$ **拡大のクンマー理論**, 早稲田大学整数論研究集会2008報告集, 2008, pp. 51–62.

[10] ———, *Descent Kummer theory via Weil restriction of multiplicative groups*, J. Number Theory **130** (2010), no. 3, 639–659.

[11] ———, *A Kummer theoretic construction of an $S_3$-polynomial with given quadratic subfield*, Interdiscip. Inform. Sci. **16** (2010), no. 1, 17–20.

[12] ———, *On metacyclic extensions*, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 339–353.

[13] ———, *Algebraic extensions attached to algebraic tori of relative norm*, to appear in SUT Journal of Math. (2019).

[14] M. Kida, Y. Rikuna, and A. Sato, *Classifying Brumer's quintic polynomials by weak Mordell-Weil groups*, Int. J. Number Theory **6** (2010), no. 3, 691–704.

[15] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), no. 3, 265–279.

[16] ———, *Cyclic cubic field with explicit Artin symbols*, Tokyo J. Math. **30** (2007), no. 1, 169–178.

[17] B. Kunyavskiĭ and J.-J. Sansuc, *Réduction des groupes algébriques commutatifs*, J. Math. Soc. Japan **53** (2001), no. 2, 457–483.

[18] O. Lecacheux, *Constructions de polynômes génériques à groupe de Galois résoluble*, Acta Arith. **86** (1998), no. 3, 207–216.

[19] S. Nakano and M. Sase, *A note on the construction of metacyclic extensions*, Tokyo J. Math. **25** (2002), no. 1, 197–203.

[20] H. Ogawa, *Quadratic reduction of multiplicative group and its applications*, 数理解析研究所講究録 (2003), no. 1324, 217–224, Algebraic number theory and related topics (Japanese) (Kyoto, 2002).

[21] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961), 101–139.

[22] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2215–2218 (electronic).

[23] M. Shimakura, *Ramification in Kummer extensions arising from algebraic tori*, Bull. Aust. Math. Soc. **96** (2017), no. 2, 196–204.

[24] N. Suwa, *Twisted Kummer and Kummer-Artin-Schreier theorems*, Tohoku Math. J. (2) **60** (2008), no. 2, 183–218.

[25] ———, *Around Kummer theories*, Algebraic number theory and related topics 2007, RIMS Kôkyûroku Bessatsu, B12, Res. Inst. Math. Sci. (RIMS), Kyoto, 2009, pp. 115–148.

[26] ———, *Kummer theories for algebraic tori and normal basis problem*, Tokyo J. Math. **39** (2017), no. 3, 827–862.

[27] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

木田雅成
東京理科大学理学部第一部数学科
〒 162-8601 新宿区神楽坂 1-3
E-mail: kida@rs.tus.ac.jp
(2019 年 9 月 7 日講演)

# 複比の体での有理性問題

角皆 宏

本稿では、Noether 問題から派生する有理性問題の一つとして、複比の体での有理性問題での有理性問題について紹介する。複比への置換の作用の計算法や、5 次・6 次の場合の結果やそれから得られる生成的多項式、また、複比の体での有理性問題と Noether 問題との関係について触れる。

## 1. 有理性問題と生成的多項式

$k$ を無限体（本稿では専ら標数 0 の場合を扱う）とし、$G$ を有限群とする。体 $k$ 上で群 $G$ に関する Noether 問題が肯定的であるとき、群 $G$ に関する $k$ 上の生成的多項式が得られるのであった。

有理関数体 $k(\boldsymbol{x}) = k(x_1, \ldots, x_n)$ への $G$ の作用として、変数への置換作用と限らない一般の作用を考えた場合の有理性問題「固定体 $k(\boldsymbol{x})^G$ は $k$ 上有理的（純超越的）か？」を考えた場合、これが肯定的であれば $k$ 上の助変数付き $G$ 多項式を得るが、一般には生成的とは限らない。

**例 1.1.** 有理数体 $\boldsymbol{Q}$ 上で 8 次巡回群 $G = C_8$ に関する有理性問題を考える。$\boldsymbol{Q}$ 上の生成的 $C_8$ 多項式が存在しないことが知られている (Wang [W], Lenstra [Len])。従って、8 つの変数を巡環する $C_8$ 作用に関する Noether 問題は、$\boldsymbol{Q}$ 上では否定的である。（勿論、$\boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}(\sqrt{-1}, \sqrt{2})$ 上では Noether 問題は肯定的で、$\boldsymbol{Q}(\zeta_8)$ 上の生成的 $C_8$ 多項式は $X^8 - t$ である。）しかしながら、$\boldsymbol{Q}$ 上で固定体が有理的になるような $C_8$ 作用も知られている（橋本-星-陸名 [HHR, Theorem 6.2]）：2 変数有理関数体 $\boldsymbol{Q}(x, y)$ への $C_8 = \langle\alpha\rangle$ の作用を

$$\alpha : x \longmapsto y, \qquad y \longmapsto \frac{1+x}{1-x}$$

で定めるとき、固定体 $\boldsymbol{Q}(x, y)^{\langle\alpha\rangle}$ は $\boldsymbol{Q}$ 上有理的である。これより 2 助変数の $\boldsymbol{Q}$ 上の $C_8$ 多項式が得られるが、それは $\boldsymbol{Q}$ 上生成的ではない。

とは言え、置換作用と限らない一般の作用の場合でも、生成的多項式が得られることはある。

**定理 1** (Kemper-Mattig[KM], Theorem 3)**.** $K$ を体、有限群 $G$ が有理関数体 $K(x_1, \ldots, x_n)$ に変数の置換で作用しているとし、$F$ が $K(x_1, \ldots, x_n)/K$ の $G$ 安定な中間体で、$G$ の $F$ への作用が忠実であるとする。固定体 $F^G$ が $K$ 上純超越的であるとき、$G$ に対する $K$ 上の生成的多項式が存在する。

$\varphi_1, \ldots, \varphi_m \in F^G$ を minimal basis とし、$G$ 安定な有限集合 $\mathcal{M} \subset F$ で $F = F^G(\mathcal{M})$ なるものを選んで、

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in F^G[X]$$

とすると、$f(X) = g(\varphi_1, \ldots, \varphi_m, X)$ となる $g \in K(t_1, \ldots, t_m)[X]$ があって、$g$ は $G$ に対する $K$ 上の生成的多項式である。

[KM, Theorem 7] にもあるように、これが適用できる典型例の一つは忠実線型作用の場合である。$n$ 変数有理関数体 $F = k(x_1, \ldots, x_n)$ の 部分 $k$ 線型空間 $V = \bigoplus_{i=1}^{n} kx_i$ 上への $G$ の忠実な線型作用が与えられているとき、$V$ の $k$ 上の対称テンソル代数 $T(V) =$

第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」報告集原稿.

$\bigoplus_{i\geq 0}\mathrm{Sym}^i V \simeq k[x_1,\ldots,x_n]$、さらにその商体 $\mathrm{Frac}(T(V)) \simeq k(x_1,\ldots,x_n) = F$ にも $G$ が自然に作用する。そこで、固定体 $F^G$ が $k$ 上有理的であると、上記の定理が適用できて生成的多項式が得られる。

本稿では、他の典型例として、複比の体への群作用を考える。

## 2. 複比の体

$k$ 上の $n$ 変数有理関数体 $L = L_n := k(x_1,\ldots,x_n)$ を考える。$L$ には $n$ 次対称群 $\mathfrak{S}_n$ が変数の添字の置換で作用している：$\sigma(x_i) = x_{\sigma(i)}$. 一方、$L$ には $k$ 上の 2 次の射影一般線型群 $\mathrm{PGL}(2,k)$ が一次分数変換で作用する：

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x_i := \frac{ax_i + b}{cx_i + d} \qquad (i = 1,\ldots,n).$$

各変数について同様に作用することから、この両者の作用は可換である。従って、$\mathrm{PGL}(2,k)$ の作用に関する $L$ の固定体 $K = K_n = L^{\mathrm{PGL}(2,k)}$ にも $\mathfrak{S}_n$ が作用する。$n \geq 5$ のとき、この作用が忠実になる（注 1 参照）。そこで、$\mathfrak{S}_n$ の部分群 $G$ の $K$ への作用の固定体 $K^G$ の有理性を考えよう、というのである。これは定理 1 に適合（$K$ が定理での $F$ に相当）するので、$K^G$ が有理的であれば、生成的 $G$ 多項式が得られることになる。

ところで、定理 1 では $F$ が有理的であることは必要ないが、この場合は $K$ 自身が再び有理的であるので、有理関数体 $K$ への一般の（非線型な）作用に関する有理性問題とも見られる。実際、$K$ は変数 $x_i$ たちの複比

$$\frac{x_i - x_j}{x_i - x_l} \Big/ \frac{x_k - x_j}{x_k - x_l}$$

で生成され、$(n-3)$ 変数有理関数体と同型である：

$$\begin{aligned} K &= k\left( \frac{x_i - x_j}{x_i - x_l} \Big/ \frac{x_k - x_j}{x_k - x_l} \,\middle|\, 1 \leq i,j,k,l \leq n, \text{全て相異なる} \right) \\ &= k\left( \frac{x_i - x_{n-2}}{x_i - x_n} \Big/ \frac{x_{n-1} - x_{n-2}}{x_{n-1} - x_n} \,\middle|\, 1 \leq i \leq n-3 \right). \end{aligned}$$

$(n-3)$ 変数有理関数体と見るときの生成系の取り方は色々あるが、考えている群の作用に合わせた取り方をすると計算がしやすい。次節で触れる。

**注 1.** $n = 4$ のときには、$K$ への $\mathfrak{S}_4$ の作用は忠実ではない。実際、

$$K = k(\lambda), \qquad \lambda := \frac{x_1 - x_2}{x_1 - x_3} \Big/ \frac{x_4 - x_2}{x_4 - x_3}$$

であり、$\lambda$ は $V_4 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \lhd \mathfrak{S}_4$ で固定されるので、$\mathfrak{S}_4$ の作用は $\mathfrak{S}_4 \longrightarrow \mathfrak{S}_4/V_4 \simeq \mathfrak{S}_3$ を経由する。1 変数なので、Lüroth の定理により固定体はすべて有理的である。この $\mathfrak{S}_3$ 作用による $\lambda$ の軌道は、

$$\mathrm{Orb}_{\mathfrak{S}_3}(\lambda) = \left\{ \lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\}$$

である。尚、このとき、$\mathfrak{A}_4$ の作用は、$\mathfrak{A}_4 \longrightarrow \mathfrak{A}_4/V_4 \simeq \mathfrak{A}_3 = C_3$ を経由し、その軌道は

$$\mathrm{Orb}_{C_3}(\lambda) = \left\{ \lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda} \right\}$$

で、この $C_3$ 作用から得られる多項式

$$\prod_{w \in \mathrm{Orb}_{C_3}(\lambda)} (X - w) = X^3 - tX^2 + (t-3)X + 1$$

（ここに、$t = \dfrac{1 - 3\lambda + \lambda^3}{\lambda(1-\lambda)}$）は Shanks の巡回 3 次多項式 [S] に他ならない。

## 3. 複比の体への置換群の作用の計算

$n$ 変数の複比の体 $K = K_n$ は、$(n-3)$ 個の代数的独立な複比で生成される有理関数体で、例えば生成元として次の $y_i$ $(i = 1, \ldots, n-3)$ が取れる：

$$y_i := \frac{x_i - x_{n-2}}{x_i - x_n} \Big/ \frac{x_{n-1} - x_{n-2}}{x_{n-1} - x_n}$$

この $y_i$ たちへの $\sigma \in \mathfrak{S}_n$ の作用を計算したい。勿論

$$\sigma(y_i) = \frac{x_{\sigma(i)} - x_{\sigma(n-2)}}{x_{\sigma(i)} - x_{\sigma(n)}} \Big/ \frac{x_{\sigma(n-1)} - x_{\sigma(n-2)}}{x_{\sigma(n-1)} - x_{\sigma(n)}} \in K = k(y_1, \ldots, y_{n-3})$$

であるから、$\sigma(y_i)$ を $y_1, \ldots, y_{n-3}$ で表わすべく、これらの関係式から $x_1, \ldots, x_n$ を消去すればよいのであるが、幾何的な背景を考えて、より簡明に計算する方法がある。

複比の体 $K = L^{\mathrm{PGL}(2,k)}$ は $(\mathbf{P}^1)^n \smallsetminus \Delta$ 上の $\mathrm{PGL}(2,k)$ 不変な有理関数体であり、従って、$\mathcal{M}_{0,n} = ((\mathbf{P}^1)^n \smallsetminus \Delta)/\mathrm{PGL}(2)$ の $k$ 上の関数体であった。点 $(x_1, \ldots, x_n) \in (\mathbf{P}^1)^n \smallsetminus \Delta$ の $\mathrm{PGL}(2)$ 作用による同値類を $[x_1, \ldots, x_n] = (x_1, \ldots, x_n) \bmod \mathrm{PGL}(2)$ と書くとき、複比 $y_i$ は次で定まる関数と見ることができる：点 $P = [x_1, \ldots, x_n] \in \mathcal{M}_{0,n}$ に対し、$P = (*, \ldots, *, 0, 1, \infty) \bmod \mathrm{PGL}(2)$ の形の代表元が唯一に定まるので、その第 $i$ 成分への射影を $y_i$ とする。即ち、$P = [x_1, \ldots, x_n] = [y_1, \ldots, y_{n-3}, 0, 1, \infty]$ により定まる。

$$\begin{array}{rccccc} y_i : & \mathcal{M}_{0,n} = ((\mathbf{P}^1)^n \smallsetminus \Delta)/\mathrm{PGL}(2) & \xrightarrow{\sim} & (\mathbf{P}^1 \smallsetminus \{0,1,\infty\})^{n-3} \smallsetminus \Delta & \xrightarrow{\mathrm{pr}_i} & \mathbf{P}^1 \\ & [x_1, \ldots, x_n] = [y_1, \ldots, y_{n-3}, 0, 1, \infty] & \longmapsto & (y_1, \ldots, y_{n-3}) & \longmapsto & y_i \end{array}$$

さて、$\sigma \in \mathfrak{S}_n$ の $x_i$ への置換作用 $\sigma(x_i) = x_{\sigma(i)}$ は、$x_i$ を $(\mathbf{P}^1)^n \smallsetminus \Delta$ 上の座標関数 $x_i : (\mathbf{P}^1)^n \smallsetminus \Delta \xrightarrow{\mathrm{pr}_i} \mathbf{P}^1$ と見做すとき、$\sigma(x_i) = x_i \circ \sigma^{-1}$ と書ける。ここに、$\mathfrak{S}_n$ は $(\mathbf{P}^1)^n \smallsetminus \Delta$ に成分の入れ替えで（左から）作用するものとする。（非可換群の作用を扱いたいので、作用の右左には充分注意を払う必要がある。）従って、$P = [x_1, \ldots, x_n] = [y_1, \ldots, y_{n-3}, 0, 1, \infty]$ に対し、$\sigma^{-1}(P) = [x_{\sigma(1)}, \ldots, x_{\sigma(n)}] = [y_{\sigma(1)}, \ldots, y_{\sigma(n)}]$（ここに、$y_{n-2} = 0, y_{n-1} = 1, y_n = \infty$ とおいた）を $[*, \ldots, *, 0, 1, \infty]$ の形に再正規化した際の第 $i$ 成分として $\sigma(y_i)$ が得られる：

$$\sigma^{-1}(P) = [x_{\sigma(1)}, \ldots, x_{\sigma(n)}] = [\sigma(y_1), \ldots, \sigma(y_{n-3}), 0, 1, \infty]$$

**例 3.1.** $n = 5$ として、$P = [x_1, x_2, x_3, x_4, x_5] = [y_1, y_2, 0, 1, \infty]$ により $y_1, y_2$ を定める。正規化の際の一次分数変換は $\xi \longmapsto \dfrac{\xi - x_3}{\xi - x_5} \Big/ \dfrac{x_4 - x_3}{x_4 - x_5}$ であるので、

$$y_1 = \frac{x_1 - x_3}{x_1 - x_5} \Big/ \frac{x_4 - x_3}{x_4 - x_5}\ , \qquad y_2 = \frac{x_2 - x_3}{x_2 - x_5} \Big/ \frac{x_4 - x_3}{x_4 - x_5}$$

であり、これが複比の体 $F$ の生成元である：$F = k(y_1, y_2)$. 5 次巡換 $\alpha = (1\ 2\ 3\ 4\ 5) \in \mathfrak{S}_5$ の作用は次のようにして求められる：

$$\alpha^{-1}(P) = [y_2, 0, 1, \infty, y_1] = \left[\frac{y_2 - 1}{y_2 - y_1}, \frac{1}{y_1}, 0, 1, \infty\right]$$

（ここに正規化は $\xi \longmapsto \dfrac{\xi - 1}{\xi - y_1}$ による）であるから、

$$\alpha(y_1) = \frac{y_2 - 1}{y_2 - y_1}\ , \qquad \alpha(y_2) = \frac{1}{y_1}\ .$$

**例 3.2.** $n \geq 5$ に対し、

$$P = [x_1, \ldots, x_n] = [0, y_1 \cdots y_{n-3}, y_1 \cdots y_{n-2}, \ldots, y_1 y_2, y_1, 1, \infty]$$

により定まる $y_1, \ldots, y_{n-3}$ を取ることもしばしばある。これは幾何的には、$\mathcal{M}_{0,n}$ の標準的な接基点に対応するものと捉えられる（例えば伊原 [Ih], 角皆 [T1] など）。変換 $\xi \longmapsto (y_1 \cdots y_{i-1})^{-1}\xi$ により再正規化すると、$P = [0, \ldots, y_i, 1, \ldots, \infty]$ となるので、

$$y_i = \frac{x_{n-1-i} - x_1}{x_{n-1-i} - x_n} \Big/ \frac{x_{n-i} - x_1}{x_{n-i} - x_n}$$

であり、$F = k(y_1, y_1y_2, \ldots, y_1\cdots y_{n-3}) = k(y_1, \cdots, y_{n-3})$ であるので、これも複比の体 $F$ の生成系になる。例えば、$n = 5$ のとき、$\alpha = (1\ 2\ 3\ 4\ 5) \in \mathfrak{S}_5$ の作用は次のようにして求められる：

$$\alpha^{-1}(P) = \alpha^{-1}([0, y_1y_2, y_1, 1, \infty]) = [y_1y_2, y_1, 1, \infty, 0] = [0, 1-y_2, 1-y_1y_2, 1, \infty]$$

（ここに正規化は $\xi \longmapsto \dfrac{\xi - y_1y_2}{\xi}$ による）であるから、

$$\alpha(y_1) = 1 - y_1y_2\ , \qquad \alpha(y_2) = \frac{1-y_2}{1-y_1y_2}\ .$$

となる。

次節・次々節では、橋本-角皆 [HT1, HT2] の結果を中心に、$\boldsymbol{Q}$ 上で $n = 5, 6$ の場合の複比の体に関する固定体の有理性問題の結果を紹介する。多くの場合は、具体的な計算により固定体の生成系を得ることによって、肯定的な結果を得ている。群によって計算や得られる多項式が簡潔になるものとそうでもないものとがある。簡潔な多項式は代数的整数論などへの応用も大きいので、本稿では簡潔になる場合（つまり凄くうまく行っている場合）を中心に紹介する。

## 4. 複比の体の有理性問題：5 次の場合

5 次対称群 $\mathfrak{S}_5$ の可移部分群の共役類は次の表に挙げる 5 個である (cf. [B-MK, HT1])。

| [B-MK] | 位数 | 偶奇 | 構造 | 生成元 |
|---|---|---|---|---|
| ${}_5T_1$ | 5 | + | $C_5 \simeq \boldsymbol{Z}/5\boldsymbol{Z}$ | $\alpha$ |
| ${}_5T_2$ | 10 | + | $D_5 \simeq \{\pm 1\} \ltimes \boldsymbol{Z}/5\boldsymbol{Z}$ | $\alpha, \beta$ |
| ${}_5T_3$ | 20 | | $F_{20} \simeq (\boldsymbol{Z}/5\boldsymbol{Z})^\times \ltimes \boldsymbol{Z}/5\boldsymbol{Z}$ | $\alpha, \gamma$ |
| ${}_5T_4$ | 60 | + | $\mathfrak{A}_5$ | $D_5, \omega$ |
| ${}_5T_5$ | 120 | | $\mathfrak{S}_5$ | $\mathfrak{A}_5, \delta$ |

$\alpha = (12345), \beta = (13)(45), \gamma = (1534), \omega = (154), \delta = (14)$

先に述べたように、複比の体 $K := K_5 = \boldsymbol{Q}(x_1, \ldots, x_5)^{\mathrm{PGL}(2,\boldsymbol{Q})}$ の生成元の取り方は色々あるが、ここでは、前節の例3.2で挙げた取り方を採用して（更に簡単のため $y_1 = x, y_2 = y$ とおいて）、$P = [x_1, \ldots, x_5] = [0, xy, x, 1, \infty] = [0, y, 1, x^{-1}, \infty] \in \mathcal{M}_{0,5}$ によって定まる

$$x = \frac{x_3 - x_1}{x_3 - x_5}\Big/\frac{x_4 - x_1}{x_4 - x_5}\ , \qquad y = \frac{x_2 - x_1}{x_2 - x_5}\Big/\frac{x_3 - x_1}{x_3 - x_5}$$

を選ぶことにする。（後で消去する変数になるので、他の取り方でも、得られる多項式に変わりはない。）

### 4.1. 5 次二面体群 $D_5$・5 次巡回群 $C_5$・Frobenius 群 $F_{20}$.

$\alpha = (12345), \beta = (13)(45) \in \mathfrak{S}_5$ で生成される 5 次二面体群 $D_5 = \langle \alpha, \beta \rangle$ による固定体を考えよう[1]。

生成元 $\alpha = (12345), \beta = (13)(45)$ の $x, y$ への作用は次で与えられる：

$$\alpha : \begin{cases} x \longmapsto 1 - xy \\ y \longmapsto \dfrac{1-y}{1-xy} \end{cases}\ , \qquad \beta : \begin{cases} x \longmapsto x \\ y \longmapsto \dfrac{1-y}{1-xy} \end{cases}\ .$$

[1]群を表わす $D_5$ などの記号は、抽象群としての同型類や置換群としての共役類を表わすこともあるが、ここでは以下、上記の元で生成される置換群そのものを表わすものとする。

$\alpha$ の作用による $x$ の軌道 $S_1 = \mathrm{Orb}_{C_5}(x)$ は、$w_0 := x, w_i := \alpha^i(w_0)$（添字は $i \in \boldsymbol{Z}/5\boldsymbol{Z}$ とみる）とおくと、

$$S_1 = \{w_i | i \in \boldsymbol{Z}/5\boldsymbol{Z}\} = \left\{x, 1-xy, y, \frac{1-y}{1-xy}, \frac{1-x}{1-xy}\right\}$$

である。

$S_1$ の元を根とする多項式

$$f(X) := \prod_{u \in S_1}(X-u) =: X^5 + c_4X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$$

を作ると、$f \in K^{C_5}[X]$ となるので、各係数 $c_i$ は $C_5$ 不変であり、$\boldsymbol{Q}(\boldsymbol{c}) := \boldsymbol{Q}(c_0, \ldots, c_4)$ とおくと、$\boldsymbol{Q}(\boldsymbol{c}) \subset K^{C_5}$ となることまではすぐわかる。そこで、

(1) $\boldsymbol{Q}(\boldsymbol{c}) = K^{C_5}$ であるか。
(2) もしそうなら、$\boldsymbol{Q}(\boldsymbol{c})$ が $\boldsymbol{Q}$ 上有理的であるか。即ち、$\boldsymbol{Q}(\boldsymbol{c}) = \boldsymbol{Q}(a,b)$ となる $a, b \in K^{C_5}$ が存在するか。
(3) もしそうなら、$f$ の各係数 $c_i$ を $a, b$ で書き表すことにより得られる $f(X) \in K^{C_5}[X] = \boldsymbol{Q}(a,b)[X]$ は、2 助変数の $\boldsymbol{Q}$ 上の生成的 $C_5$ 多項式である。

の手順で考察を進めて、うまくいくと生成的 $C_5$ 多項式が得られるであろう。

しかしながら、今の場合にはそうならない。実は、$S_1$ は $\alpha$ だけでなく $\beta$ の作用でも安定であり、$x$ の $D_5$ 軌道になっている：$S_1 = \mathrm{Orb}_{D_5}(x)$。（実際、$\alpha(w_i) = w_{i+1}, \beta(w_i) = w_{-i}$ となっていて、まさに $D_5$ の置換作用を実現している。）従って、$f \in K^{D_5}[X]$ であり、$c_i \in K^{D_5} \subsetneq K^{C_5}$ となっている。そこで、目標を $C_5$ から $D_5$ に切り替えて、

(1) $\boldsymbol{Q}(\boldsymbol{c}) = K^{D_5}$ であるか。
(2) もしそうなら、$\boldsymbol{Q}(\boldsymbol{c})$ が $\boldsymbol{Q}$ 上有理的であるか。即ち、$\boldsymbol{Q}(\boldsymbol{c}) = \boldsymbol{Q}(a,b)$ となる $a, b \in K^{D_5}$ が存在するか。
(3) もしそうなら、$f$ の各係数 $c_i$ を $a, b$ で書き表すことにより得られる $f(X) \in K^{D_5}[X] = \boldsymbol{Q}(a,b)[X]$ は、2 助変数の $\boldsymbol{Q}$ 上の生成的 $D_5$ 多項式である。

の手順で考察を進めることにする。うまくいくと生成的 $D_5$ 多項式が得られる。

まず、$\boldsymbol{Q}(\boldsymbol{c}) \subset K^{D_5}$ は構成から既に言えていた。逆向きの包含も $\mathrm{Stab}_{\mathrm{Aut}(\boldsymbol{Q}(x,y)/\boldsymbol{Q})}(S_1) = \{\sigma \in \mathrm{Aut}(\boldsymbol{Q}(x,y)/\boldsymbol{Q}) | \sigma(S_1) = S_1\} = D_5$ から従うので $\boldsymbol{Q}(\boldsymbol{c}) = K^{D_5}$ がわかるが、実質的には、これは次のような考察で $[F : \boldsymbol{Q}(\boldsymbol{c})] \leq \#D_5 = 10$ を示すのと同等である。まず、$x$ は $\boldsymbol{Q}(\boldsymbol{c})$ 上の 5 次多項式 $f$ の根なので、$[\boldsymbol{Q}(\boldsymbol{c}, x) : \boldsymbol{Q}(\boldsymbol{c})] \leq 5$ である。次に、

$$\prod_{u \in S} u = \frac{xy(1-x)(1-y)}{1-xy} = -c_0$$

より、$y$ が $\boldsymbol{Q}(\boldsymbol{c}, x)$ 上 2 次の関係式を満たすため、$[\boldsymbol{Q}(\boldsymbol{c}, x, y) : \boldsymbol{Q}(\boldsymbol{c}, x)] \leq 2$ となり、併せて、

$$[F : \boldsymbol{Q}(\boldsymbol{c})] = [\boldsymbol{Q}(\boldsymbol{c}, x, y) : \boldsymbol{Q}(\boldsymbol{c})] = [\boldsymbol{Q}(\boldsymbol{c}, x, y) : \boldsymbol{Q}(\boldsymbol{c}, x)][\boldsymbol{Q}(\boldsymbol{c}, x) : \boldsymbol{Q}(\boldsymbol{c})] \leq 2 \cdot 5 = 10$$

が言えて、$\boldsymbol{Q}(\boldsymbol{c}) = K^{D_5}$ が判明した。同時に、$f$ が $K^{D_5}$ 上既約であることもわかる。

$K^{D_5}$ の有理性を見るためには、$c_0, \ldots, c_4$ の間の関係式を調べる必要がある。各 $c_i$ は $x, y$ で書けているので、それらから $x, y$ を消去すれば良い。ここはなにがしかの計算代数ソフトウェアの力を借りよう。すると、

$$c_2 = c_0^2 - c_0 - 1 - 2c_1, \qquad c_3 = c_1 - c_0 + 3, \qquad c_4 = c_0 - 3$$

が得られる。そこで $c_0 = a, c_1 = b$ とおけば[2]、$K^{D_5} = \boldsymbol{Q}(a,b)$ であると同時に、$\boldsymbol{Q}$ 上の 2 助変数生成的 $D_5$ 多項式

$$f^{D_5}(a, b; X) = X^5 + (a-3)X^4 + (b-a+3)X^3 + (a^2 - a - 1 - 2b)X^2 + bX + a$$

[2]とするのは自然に見えるが、$c_0 = -a$ として、根のノルムが $a$ になる方が良かったような気もする。

が得られた。これは Brumer[B], 橋本 [H] が得た多項式の再構成である。尚、判別式は $D(f^{D_5}) = a^2 D_1(a,b)^2$、ここに

$$D_1(a,b) = \\ -4b^3 + (a^2 - 30a + 1)b^2 + 2a(12a^2 - 17a - 7)b - a(4a^4 - 4a^3 - 40a^2 + 91a - 4)$$

である。

**注 2.** $S_1$ の元 $w_i$ たちの間には、$w_{i-1}w_{i+1} = 1 - w_i$ という注目すべき関係式があり、これが $S_1$ を特徴づけている。実際、$\boldsymbol{Z}$ を添字とする（両側に延びた）数列 $\boldsymbol{w} = (x_i)_{i\in\boldsymbol{Z}}$ が関係式 $w_{i-1}w_{i+1} = 1 - w_i$ を満たすとき、$\boldsymbol{w}$ は周期 5 の数列となり、添字を $\boldsymbol{Z}/5\boldsymbol{Z}$ と考えたとき、上記の関係式を保つ 5 元の置換全体は 5 次二面体群 $D_5$ をなすことがわかる (Kihel[Ki])。この関係式をうまく用いると、$c_i$ たちの間の上記の関係式は、手計算程度でも得られる。

さて、$C_5$ 固定体 $K^{C_5}$ や $C_5$ 多項式が得たいならば、ある元 $v \in \boldsymbol{Q}(x,y)$ の $C_5$ 軌道で、$\beta$ で不変でないものを考える必要がある。例えば上で使った $w_i$ たちを用いて $v := w_1 - w_0 = 1 - x - xy$ とすれば、その $C_5$ 軌道 $S_2 = \mathrm{Orb}_{C_5}(v)$ については、$\beta(S_2) = \{-u | u \in S_2\}$ となるので、同様に $S_2$ の元を根とする多項式

$$f(X) := \prod_{u\in S_2}(X - u) =: X^5 + c_4X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$$

（但し、$c_4 = 0$）を作って、$\boldsymbol{Q}(\boldsymbol{c}) := \boldsymbol{Q}(c_0, \ldots, c_3)$ とおくと、$\boldsymbol{Q}(\boldsymbol{c}) = K^{C_5}$ となって $C_5$ 多項式が得られないだろうか。

まず、$f \in K^{C_5}[X]$ であり、$\boldsymbol{Q}(\boldsymbol{c}) = K^{C_5}$ もわかるが、$c_0, \ldots, c_3$ の間の関係式が容易には見つからない。実際、

$$c := -c_0 = \prod_{i\in\boldsymbol{Z}/5\boldsymbol{Z}} \alpha^i(v) = \prod_{i\in\boldsymbol{Z}/5\boldsymbol{Z}} (w_{i+1} - w_i)$$

について、$\alpha(c) = c, \beta(c) = -c$ なので、$c \in K^{C_5} \smallsetminus K^{D_5}$ かつ $c^2 \in K^{D_5}$、従って、$K^{D_5}(c) = \boldsymbol{Q}(a,b,c) = K^{C_5}$ となる。$c^2 \in K^{D_5} = \boldsymbol{Q}(a,b)$ を実際に $a, b$ で表わすと、

$$c^2 = D_1(a,b)$$

である。これが表わす曲面は有理楕円曲面で、特異点解消により実際に $K^{C_5}$ の有理生成系が得られ、これより $\boldsymbol{Q}$ 上 2 助変数の生成的 $C_5$ 多項式も得られる。それは [HT1] にあるように非常に複雑な形であり、代数的整数論への応用は困難なようだが、Kummer 理論との関連付けなどが試みられてはいる（[KRY]）。

次に $D_5$ から更に 2 次進めて $F_{20}$ の固定体に進むには、$\gamma = (1534)$ の作用を考えることになる。$F_{20} \rhd D_5$ なので、$\gamma$ の作用で $K^{D_5} = \boldsymbol{Q}(a,b)$ は安定であり、$\gamma$ の $x, y$ への作用が $x, y$ で書けるだけでなく、$a, b$ への作用も $a, b$ で書ける：

$$\gamma : \begin{cases} x \longmapsto \dfrac{x}{x-1} \\ y \longmapsto \dfrac{x-1}{x(1-y)} \end{cases}, \qquad \begin{cases} a \longmapsto -\dfrac{1}{a} \\ b \longmapsto \dfrac{5a+b}{a^2} \end{cases}.$$

そこで、$A := a + \gamma(a) = a - \dfrac{1}{a}, B := b + \gamma(b) = \dfrac{b + 5a + a^2b}{a^2}$ とおくと、$A, B \in K^{F_{20}}$ で、$K^{D_5} = \boldsymbol{Q}(a,b) = \boldsymbol{Q}(a,B)$ と $[\boldsymbol{Q}(a,B) : \boldsymbol{Q}(A,B)] = 2$ から、$K^{F_{20}} = \boldsymbol{Q}(A,B)$ が従う。また、$x$ は $\gamma^2 = \beta$ で不変であるから、$u_0 := x + \gamma(x) = \dfrac{x^2}{x-1}$ が $\gamma$ 不変となり、その $F_{20}$ 軌道

$$S_3 := \mathrm{Orb}_{F_{20}}(u_0) = \mathrm{Orb}_{\langle\alpha\rangle}(u_0) \\ = \left\{ \frac{x^2}{x-1}, -\frac{(1-xy)^2}{xy}, \frac{y^2}{y-1}, -\frac{(1-y)^2}{y(1-x)(1-xy)}, -\frac{(1-x)^2}{x(1-y)(1-xy)} \right\}$$

を根とする多項式

$$f(X) := \prod_{u \in S_3} (X - u) =: X^5 + c_4 X^4 + c_3 X^3 + c_2 X^2 + c_1 X + c_0$$

の各係数 $c_i \in K^{F_{20}}$ を $A, B$ で表わすことによって、$\boldsymbol{Q}$ 上 2 助変数の生成的 $F_{20}$ 多項式

$$f^{F_{20}}(A, B; X) = X^5 - (A-6)X^4 - (3A - B - 8)X^3 - (A^2 - A - 3B + 5)X^2 - \left(2A - 2 - \frac{B^2 - 5AB - 25}{A^2 + 4}\right) X - 1$$

が得られる。これは（若干の変数変換の下に）Lecacheux[Lec] が楕円曲線の 5 等分点を用いて構成した $F_{20}$ 多項式

$$f^{\mathrm{Lec}}(s, t; X) = X^5 + \left(t^2(s^2+4) - 2s - \frac{17}{4}\right) X^4 + \left((3t+1)(s^2+4) + \frac{13s}{2} + 1\right) X^3 - \left(t(s^2+4) + \frac{11s}{2} - 8\right) X^2 + (s-6)X + 1$$

の再構成となっている。

4.2. **5 次交代群 $\mathfrak{A}_5$ • 5 次対称群 $\mathfrak{S}_5$.** 5 次交代群 $\mathfrak{A}_5$ は、ガロア群の理論にとって歴史的にも重要な対象である。位数最小の非可換単純群であり、是非とも挑戦してみたい。

$\omega = (154)$ とすると、$\mathfrak{A}_5 = \langle D_5, \omega \rangle$ となる。また、$\omega$ の $F$ への作用は次のようになる：

$$\omega : \begin{cases} x \longmapsto \dfrac{1}{1-x} \\ y \longmapsto \dfrac{1-x}{1-xy} \end{cases} .$$

$\mathfrak{A}_5$ 内での $x$ の固定群は Klein の四元群 $V_4 = \langle (1\ 3)(4\ 5), (1\ 4)(3\ 5) \rangle$ であり、$\mathrm{Orb}_{\mathfrak{A}_5}(x)$ は 15 個の元からなる。$\omega$ は $V_4$ を正規化し、$\langle \omega \rangle \ltimes V_4 = \mathrm{Stab}_{\mathfrak{A}_5}(2) \simeq \mathfrak{A}_4$ である。そこで、$v_0 := x + \omega(x) + \omega^2(x) = \dfrac{1 - 3x + x^3}{x(x-1)}$ とすると、$\mathrm{Stab}_{\mathfrak{A}_5}(v_0) = \langle \omega \rangle \ltimes V_4$ で、$v_0$ の $\mathfrak{A}_5$ 軌道 $S_4 := \mathrm{Orb}_{\mathfrak{A}_5}(v_0)$ への $\mathfrak{A}_5$ の作用が自然な置換作用を実現する。実際、

$$\begin{aligned} S_4 &= \mathrm{Orb}_{\langle \alpha \rangle}(v_0) \\ &= \left\{ \frac{1-3x+x^3}{x(x-1)}, \frac{1-3x^2y^2+x^3y^3}{xy(1-xy)}, \frac{1-3y+y^3}{y(y-1)}, \right. \\ &\qquad \frac{1-3xy-3y^2+6xy^2+y^3-3x^2y^3+x^3y^3}{y(1-x)(1-y)(1-xy)}, \\ &\qquad \left. \frac{1-3xy-3x^2+6x^2y+x^3-3x^3y^2+x^3y^3}{x(1-x)(1-y)(1-xy)} \right\} \end{aligned}$$

であり、$S_4$ の元を根とする 5 次多項式

$$f(X) := \prod_{u \in S_4} (X - u) =: X^5 + c_4 X^4 + c_3 X^3 + c_2 X^2 + c_1 X + c_0$$

を作ると、前節のような目論見がうまくいく。

$$\begin{cases} \bar{u} := c_4 = \dfrac{a^2 - 10a + 1 - b}{a} \\ \bar{v} := c_2 = \dfrac{(2a^5 + 18a^4 - 140a^3 + 13a^2 - 2a) - (4a^3 + 20a^2 + 6a)b - (a^2+1)b^2}{a^3} \end{cases}$$

とおく[3] と、$K^{\mathfrak{A}_5} = \boldsymbol{Q}(\bar{u}, \bar{v})$ であることがわかり、$\boldsymbol{Q}$ 上の 2 助変数生成的 $\mathfrak{A}_5$ 多項式

$$f^{\mathfrak{A}_5}(\bar{u}, \bar{v}; X) = X^5 + \bar{u}X^4 + (-6\bar{u} - 10)X^3 + \bar{v}X^2 + (-\bar{u}^2 + 12\bar{u} + 25 - 3\bar{v})X + (\bar{u}^3 + 24\bar{u}^2 + 27\bar{u} - 24 + 9\bar{v})$$

を得る。判別式は $D(f^{\mathfrak{A}_5}) = \bar{D}_2(\bar{u}, \bar{v})^2$、ここに

$$\begin{aligned}\bar{D}_2(\bar{u}, \bar{v}) := {} & (24000 - 109600\bar{u} - 54720\bar{u}^2 + 91032\bar{u}^3 + 68280\bar{u}^4 + 13624\bar{u}^5 + 840\bar{u}^6 + 16\bar{u}^7) \\ & + (-28400 + 36240\bar{u} + 44284\bar{u}^2 + 9240\bar{u}^3 + 332\bar{u}^4)\bar{v} \\ & + (6480 + 1386\bar{u} - 90\bar{u}^2 - 4\bar{u}^3)\bar{v}^2 - 27\bar{v}^3\end{aligned}$$

である。但し、これは係数が若干大きい。次の段階である 5 次対称群 $\mathfrak{S}_5$ の作用も考慮すると、以下の変数変換を施した表示にも想到する。

5 次対称群 $\mathfrak{S}_5$ の作用を考えるには、任意の互換、例えば $\delta = (14)$ の作用を考えれば良い。$\mathfrak{S}_5 \rhd \mathfrak{A}_5$ なので、$\delta$ の $\bar{u}, \bar{v}$ への作用も $\bar{u}, \bar{v}$ で書ける：

$$\delta : \begin{cases} x \longmapsto 1 - x \\ y \longmapsto \dfrac{1 - xy}{1 - x} \end{cases}, \qquad \begin{cases} \bar{u} \longmapsto -\bar{u} - 15 \\ \bar{v} \longmapsto -\bar{v} - 180 \end{cases}.$$

そこで、$u := \bar{u} + 8,\ v := -(\bar{v} + 90) - 12(1 - 2u) = -\bar{v} + 24\bar{u} - 102$ とすれば、

$$\begin{cases} u \longmapsto 1 - u \\ v \longmapsto -v \end{cases}$$

であり、この方が $\mathfrak{S}_5$ の作用が簡明なのは明白である。$f^{\mathfrak{A}_5}$ を $u, v$ で表したものを次小節で用いるために改めて $f_5^{\mathfrak{A}_5}$ と書くと、

$$f_5^{\mathfrak{A}_5}(u, v; X) = X^5 - (8 - u)X^4 + (38 - 6u)X^3 - (v - 24u + 102)X^2 + (3v - u^2 - 44u + 171)X - (9v - u^3 - 51u + 134)$$

と係数は余り簡明にならないが、判別式は $D(f_5^{\mathfrak{A}_5}) = D_2(u, v)^2$、ここに

$$\begin{aligned}D_2(u, v) = {} & (16u^7 - 56u^6 + 472u^5 - 1040u^4 + 216u^3 + 688u^2 + 5000u - 2648) \\ & + (-140u^4 + 280u^3 - 916u^2 + 776u + 596)v \\ & + (-4u^3 + 6u^2 + 114u - 58)v^2 + 27v^3\end{aligned}$$

とやや係数が小さくなっている。

$U := u\delta(u) = u(1 - u), V := \dfrac{v}{u - \delta(u)} = \dfrac{v}{2u - 1}$ とすれば、$\mathfrak{S}_5$ 固定体は、$K^{\mathfrak{S}_5} = \boldsymbol{Q}(u, v)^{\langle\delta\rangle} = \boldsymbol{Q}(U, V)$ となり有理的である。$\mathfrak{S}_5$ 多項式も得られるが、特筆すべきでもあるまい。

### 4.3. 5 次交代群 $\mathfrak{A}_5$ 再び.

前小節で得た 5 次の $\mathfrak{A}_5$ 多項式

$$f_5^{\mathfrak{A}_5}(u, v; X) = X^5 - (8 - u)X^4 + (38 - 6u)X^3 - (v - 24u + 102)X^2 + (-u^2 - 44u + 171 + 3v)X + (u^3 + 51u - 134 - 9v)$$

は、その構成から $\mathfrak{A}_5$ が 5 根の置換として自然に作用するので、$\mathfrak{A}_5$ 拡大 $K = \boldsymbol{Q}(x, y)/K^{\mathfrak{A}_5} = \boldsymbol{Q}(u, v)$ において、1 根の固定体たる根体は $\mathfrak{A}_5$ の部分群 $\mathfrak{A}_4$ の固定体 $K^{\mathfrak{A}_4}$ である。この $\mathfrak{A}_4$ が $\mathfrak{A}_5$ の極大部分群であることに注目して、$\mathfrak{A}_5$ の他の極大部分群の固定体やそれを根体とする多項式を得ることを考えよう。$K^{\mathfrak{A}_5} = \boldsymbol{Q}(u, v)$ 上の分解体 $K = \boldsymbol{Q}(x, y)$ を共有するので、こうして得られた多項式も生成的 $\mathfrak{A}_5$ 多項式になるはずである。以下、[T2] での結果を紹介する。

$\mathfrak{A}_5$ の極大部分群の共役類は、$\mathfrak{A}_4, D_5, (\mathfrak{S}_3 \times \mathfrak{S}_2) \cap \mathfrak{A}_5 \simeq \mathfrak{S}_3$ の 3 種である。

[3] [HT1] では $u, v$ としているが、本稿では後で別の助変数に取替えてそちらを $u, v$ としたい。

| 極大部分群 | 群指数 | 固定するもの |
|---:|---|---|
| $\mathfrak{A}_4$ | 5 | 1 点 |
| $D_5$ | 6 | 数珠順列 |
| $(\mathfrak{S}_3 \times \mathfrak{S}_2) \cap \mathfrak{A}_5 \simeq \mathfrak{S}_3$ | 10 | 2 点の非順序対 |

$\mathfrak{A}_5$ の極大部分群の共役類

複比の体 $K = \boldsymbol{Q}(x, y)$ の $D_5$ 固定体 $\boldsymbol{Q}(x, y)^{D_5} = \boldsymbol{Q}(a, b)$ の生成元 $a, b$ と、$\mathfrak{A}_5$ 固定体 $\boldsymbol{Q}(x, y)^{\mathfrak{A}_5} = \boldsymbol{Q}(u, v)$ の生成元 $u, v$ との間の関係は、前小節で得られた結果より次のようになる：

$$u = \frac{a^2 - 2a + 1 - b}{a},$$
$$v = \frac{(-2a^5 + 6a^4 - 10a^3 + 11a^2 + 2a) + (4a^3 - 4a^2 + 6a)b - (a^2 + 1)b^2}{a^3}.$$

$D_5$ は $\mathfrak{A}_5$ の極大部分群なので、$\boldsymbol{Q}(u, v)$ と $\boldsymbol{Q}(a, b)$ との間に中間体はなく、また、$a$ は $\mathfrak{A}_5$ 不変でないので、$\boldsymbol{Q}(a, b) = \boldsymbol{Q}(u, v)(a)$ となる。上式から $b$ を消去して $a$ の $\boldsymbol{Q}(u, v)$ 上の最小多項式を求めれば、$\boldsymbol{Q}(x, y)^{D_5}$ を根体とする 6 次の生成的 $\mathfrak{A}_5$ 多項式

$$f_6^{\mathfrak{A}_5}(u, v; X) = X^6 - 2(u + 1)X^5 + (u^2 + 1)X^4 - vX^3 + (u^2 - 2u + 2)X^2 - 2(u - 2)X + 1$$

を得る。

この多項式には顕著な性質が幾つかある：

まず、$f_6^{\mathfrak{A}_5}(X) \in \boldsymbol{Z}[u, v][X]$ である上、係数が小さく、特に $v$ が中間次数 3 次の係数に単独で現れるのみなので、他の係数と無関係に 3 次の係数が自由に動かせる。これは珍しい。

次に、判別式は $D(f_6^{\mathfrak{A}_5}) = D(f_5^{\mathfrak{A}_5}) = D_2(u, v)^2$ で余計な因子が現れない。一般に、5 次多項式に対して、その 6 次分解式を作ると分解体を共有するが、判別式に余計な因子が現れ、係数も大きくなってしまうのが普通である。

さらに、$f_6^{\mathfrak{A}_5}$ は $\boldsymbol{Q}$ 上生成的 $\mathfrak{A}_5$-多項式で、係数・判別式が小さいのみならず、$f_6^{\mathfrak{A}_5}(X) \in \boldsymbol{Z}[u, v][X]$ で、かつ定数項が 1 である。このことから $u, v \in \boldsymbol{Z}$ に特殊化することにより、すべての根が単数である $\boldsymbol{Q}$ 上の $\mathfrak{A}_5$-多項式が得られる。明示的な単数を持った代数体は、代数的整数論の顕著な例を提供する（[T*] 参照）。

**注 3.** Brumer の $D_5$ 多項式と呼ばれている

$$f^{D_5}(a, b; X) = X^5 + (a - 3)X^4 + (b - a + 3)X^3 + (a^2 - a - 1 - 2b)X^2 + bX + a$$

は、実はもっと大きな 6 次の $\mathfrak{A}_5$ 多項式族

$$\begin{aligned} H(a, b, c; X) = X^6 &- (4 + 2b + 3c)X^5 + (2 + 2b + b^2 - ac)X^4 \\ &- (6 + 4a + 6b - 2b^2 + 5c + 2ac)X^3 \\ &+ (1 + b^2 - ac)X^2 + (2 - 2b)X + (1 + c) \end{aligned}$$

が $D_5$ に退化した場合である [B, AK, H]。$\mathfrak{A}_5$ は $H(a, b, c; X)$ の 6 根に 6 次可移置換群 ${}_6T_{12}$（次節参照）として作用し、この作用の 1 点固定群が $D_5$ である。$c = -1$ とすると、

$$\begin{aligned} H(a, b, -1; X) = X(X^5 &- (1 + 2b)X^4 + (2 + 2b + b^2 + a)X^3 \\ &- (1 + 2a + 6b - 2b^2)X^2 + (1 + b^2 + a)X + (2 - 2b)) \end{aligned}$$

で、$X = 0$ が根となり、Galois 群で固定されるので、残りの 5 次の因子が $D_5$ 多項式を与える。係数を変換すれば、

$$f^{D_5}(a, b; X) = \frac{1}{X} H\left(-2 + a - \frac{a^2}{4} + b, 1 - \frac{a}{2}, -1; X\right)$$

であることが確かめられる。一方、

$$f_6^{\mathfrak{A}_5}(u,v;X) = H\left(\frac{v+2u^2-10u+2}{4}, u-1, 0; X\right)$$

であることも直接確かめられるので、$H(a,b,c;X)$ が生成的であることがわかる。

もう一つの極大部分群 $(\mathfrak{S}_3\times\mathfrak{S}_2)\cap\mathfrak{A}_5 \simeq \mathfrak{S}_3$ についても、固定体 $K^{\mathfrak{S}_3}$ が $\boldsymbol{Q}$ 上有理的であることがわかり、その一つの生成元の $K^{\mathfrak{A}_5} = \boldsymbol{Q}(u,v)$ 上の最小多項式として、次の 10 次の $\boldsymbol{Q}$ 上生成的 $\mathfrak{A}_5$ 多項式が得られるが、流石に大きく、判別式にも余計な因子が現れる：

$$\begin{aligned} f_{10}^{\mathfrak{A}_5}(X) = {} & X^{10} + (4u-2)X^9 + (6u^2-6u+19)X^8 + (4u^3-6u^2+38u+2v-18)X^7 \\ & + (u^4-2u^3+21u^2+4uv-20u-2v+29)X^6 \\ & + (8u^3+2u^2v-12u^2-2uv-4u-9v+4)X^5 \\ & + (2u^4-4u^3-40u^2+42u+v^2-10)X^4 \\ & + (-12u^3+2u^2v+18u^2-2uv+30u+2v-18)X^3 \\ & + (u^4-2u^3+9u^2-4uv-8u+2v-4)X^2 + (-4u+v+2)X + 1 \quad . \end{aligned}$$

応用も困難かと思われるので詳細は略。

## 5. 複比の体の有理性問題：6 次の場合

6 次対称群 $\mathfrak{S}_5$ の可移部分群の共役類は次の表に挙げる 16 個である。

| [B-MK] | 位数 | 偶奇 | 非原始性 | 構造 | 生成元 | 解決 |
|---|---|---|---|---|---|---|
| ${}_6T_1$ | 6 | | ☆ | $C_6$ | $\alpha$ | ○ |
| ${}_6T_2$ | 6 | | ☆ | $\mathfrak{S}_3(6)$ | $\alpha^2, \beta$ | ○ |
| ${}_6T_3$ | 12 | | ☆ | $D_6$ | $\alpha, \beta$ | ○ |
| ${}_6T_4$ | 12 | + | ○ | $\mathfrak{A}_4$ | $\alpha^2, \tau_1, \tau_2$ | ○ |
| ${}_6T_5$ | 18 | | △ | $\mathfrak{S}_3\times C_3$ | ${}_6T_2, \gamma_1$ | ○ |
| ${}_6T_6$ | 24 | | ○ | $\mathfrak{A}_4\times C_2$ | ${}_6T_4, \theta$ | ○ |
| ${}_6T_7$ | 24 | + | ○ | ${\mathfrak{S}_4}^{(+)}$ | ${}_6T_4, \beta\theta$ | ○ |
| ${}_6T_8$ | 24 | | ○ | ${\mathfrak{S}_4}^{(-)}$ | ${}_6T_4, \beta$ | ○ |
| ${}_6T_9$ | 36 | | △ | $V_4 \ltimes (C_3\times C_3)$ | ${}_6T_3, \gamma_1$ | ○ |
| ${}_6T_{10}$ | 36 | + | △ | $C_4 \ltimes (C_3\times C_3)$ | $\alpha^2, \alpha\beta, \gamma_1, \delta$ | ○ |
| ${}_6T_{11}$ | 48 | | ○ | $\mathfrak{S}_4\times C_2$ | ${}_6T_4, \beta, \theta$ | ○ |
| ${}_6T_{12}$ | 60 | + | | $\mathfrak{A}_5(6)$ | ${}_6T_4, \varphi$ | ? |
| ${}_6T_{13}$ | 72 | | △ | $D_4 \ltimes (C_3\times C_3)$ | ${}_6T_9, \delta$ | ○ |
| ${}_6T_{14}$ | 120 | | | $\mathfrak{S}_5(6)$ | ${}_6T_8, \varphi$ | ○ |
| ${}_6T_{15}$ | 360 | + | | $\mathfrak{A}_6$ | ${}_6T_7, \varphi$ | ? |
| ${}_6T_{16}$ | 720 | | | $\mathfrak{S}_6$ | ${}_6T_{15}, \beta$ | ○ |

非原始性の欄は、○：$(2,2,2)$ 非原始的、△：$(3,3)$ 非原始的、☆：その両方

$$\alpha = (123456), \beta = (14)(23)(56), \theta = \alpha^3 = (14)(25)(36),$$
$$\gamma_1 = (135), \gamma_2 = (246), \delta = (14)(2563),$$
$$\tau_1 = (14)(25), \tau_2 = (14)(36), \varphi = (15243).$$

橋本-角皆 [HT2] では、${}_6T_{12} = \mathfrak{A}_5, {}_6T_{15} = \mathfrak{A}_6$ の 2 種を除いて、複比の体の固定体が有理的であることを示した。

$n = 5$ のときと異なり、$n = 6$ だと $6 = 2 \times 3$ であることから、可移部分群に $(3,3)$ および $(2,2,2)$ の非原始性を持つものがある。実際、$n = 6$ の場合には、可移部分群が原始的であることと非可解であることが同値になっている。ここでは、それぞれの非原始性を持つ中で極大な可移部分群について、複比の体の固定体を決定し、その有理性を示す。これより 6 次の生成的多項式が得られるが、Galois 閉包が所望の Galois 群である 6 次体は、2 次拡大と 3 次拡大との積み重ねで得られるので、本節では生成的多項式の明示的な構成には拘らないことにする。

5.1. 6 **次二面体群** $D_6$**.** $(3,3)$ と $(2,2,2)$ との両方の非原始性を持つ極大な部分群は、6 次二面体群 $D_6 = \langle \alpha, \beta \rangle = {}_6T_3$ （ここに、$\alpha = (123456), \beta = (14)(23)(56)$）であり、分割 $\{1,3,5\} \sqcup \{2,4,6\}$ および $\{1,4\} \sqcup \{2,5\} \sqcup \{3,6\}$ を保つ。簡明な計算のためには、複比の体の生成元を選ぶときに、この対称性を反映した取り方にしておくと都合が良い。そこで、

$$\begin{aligned}&[x_1, x_2, x_3, x_4, x_5, x_6] \\ &= \left[0, a, 1, \frac{1}{1-b}, \infty, \frac{c-1}{c}\right] = \left[\infty, \frac{a-1}{a}, 0, b, 1, \frac{1}{1-c}\right] = \left[1, \frac{1}{1-a}, \infty, \frac{b-1}{b}, 0, c\right].\end{aligned}$$

によって、$a, b, c \in K := K_6$ を定めることにする。$K = \boldsymbol{Q}\left(a, \dfrac{1}{1-b}, \dfrac{c-1}{c}\right) = \boldsymbol{Q}(a,b,c)$ である。$a, b, c$ を $x_1, \ldots, x_6$ で表わすと、

$$a = \frac{x_2 - x_1}{x_2 - x_5} \Big/ \frac{x_3 - x_1}{x_3 - x_5} \quad , \quad b = \frac{x_4 - x_3}{x_4 - x_1} \Big/ \frac{x_5 - x_3}{x_5 - x_1} \quad , \quad c = \frac{x_6 - x_5}{x_6 - x_3} \Big/ \frac{x_1 - x_5}{x_1 - x_3}$$

となる。6 次巡換 $\alpha = (123456)$ の作用は、

$$\begin{aligned}\alpha^{-1}(P) = [x_2, x_3, x_4, x_5, x_6, x_1] &= \left[a, 1, \frac{1}{1-b}, \infty, \frac{c-1}{c}, 0\right] \\ &= \left[0, \frac{(1-a)(1-b+bc)}{1-a+ab}, 1, \frac{1-b+bc}{c(1-a+ab)}, \infty, \frac{-a(1-b+bc)}{(1-c)(1-a+ab)}\right]\end{aligned}$$

（ここで、再正規化は

$$\xi \mapsto \frac{\xi - a}{\xi - \frac{c-1}{c}} \Big/ \frac{\frac{1}{1-b} - a}{\frac{1}{1-b} - \frac{c-1}{c}} = \frac{(1-b+bc)(\xi - a)}{(1-a+ab)(1-c+c\xi)}$$

で行なう）であることから、

$$\alpha : \begin{cases} a \mapsto \dfrac{(1-a)(1-b+bc)}{1-a+ab} \\ b \mapsto \dfrac{(1-b)(1-c+ca)}{1-b+bc} \\ c \mapsto \dfrac{(1-c)(1-a+ab)}{1-c+ca} \end{cases}$$

となる。また、$\beta = (14)(23)(56)$ についても同様に、

$$\beta : \begin{cases} a \mapsto \dfrac{b(1-c+ca)}{1-a+ab} \\ b \mapsto \dfrac{a(1-b+bc)}{1-c+ca} \\ c \mapsto \dfrac{c(1-a+ab)}{1-b+bc} \end{cases}$$

である。$\alpha^2=(135)(246)$ および $\alpha\beta=(15)(24)$ の作用は特に簡潔になる：

$$\alpha^2:\begin{cases}a\mapsto b\\ b\mapsto c\\ c\mapsto a\end{cases},\qquad \alpha\beta:\begin{cases}a\mapsto 1-b\\ b\mapsto 1-a\\ c\mapsto 1-c\end{cases}.$$

ここで、

$$x:=a(1-b),\quad y:=b(1-c),\quad z:=c(1-a),\quad p:=abc$$

とおこう。$x,y,z$ はそれぞれ正規化

$$[0,x,*,1,\infty,*],\qquad [\infty,*,0,y,*,1],\qquad [*,1,\infty,*,0,z]$$

により定まり、$p$ は $p^2+(x+y+z-1)p+xyz=0$ を満たす。$\boldsymbol{Q}(x,y,z)$ は $D_6$ の中心 $Z(D_6)=\langle\alpha^3\rangle$ の固定体で、$K=\boldsymbol{Q}(x,y,z)(p)$ となる。$\boldsymbol{Q}(x,y,z)$ への $D_6/Z(D_6)\simeq\mathfrak{S}_3$ の作用は、ちょうど $x,y,z$ への置換

$$\alpha:\begin{cases}x\mapsto z\\ y\mapsto x\\ z\mapsto y\\ p\mapsto (1-a)(1-b)(1-c)=1-(x+y+z)-p\end{cases},\qquad \beta:\begin{cases}x\mapsto y\\ y\mapsto x\\ z\mapsto z\\ p\mapsto p\end{cases}$$

になるので、$x,y,z$ の基本対称式を $s:=x+y+z, t:=xy+yz+zx, u:=xyz$ とおけば、$K^{D_6}=\boldsymbol{Q}(s,t,u)$ となる。

${}_6T_2=\langle\alpha^2,\beta\rangle\simeq\mathfrak{S}_3$ は、6 元集合 $\{x_1,\dots,x_6\}$ への $\mathfrak{S}_3$ の正則置換表現である。$p^2-(1-s)p+u=0$ および $\alpha(p)\neq p,\alpha^2(p)=p$ より、$K^{{}_6T_2}=K^{{}_6T_3}(p)=\boldsymbol{Q}(s,t,u,p)=\boldsymbol{Q}(t,u,p)$ となり、${}_6T_2$ の固定体 $K^{{}_6T_2}$ も有理的である。

5.2. $(3,3)$ **非原始可移群.** 分割 $\{1,3,5\}\sqcup\{2,4,6\}$ を保つ $(3,3)$ 非原始性を持つ極大な部分群は、${}_6T_{13}=\langle{}_6T_3,\gamma_1,\delta\rangle\simeq D_4\ltimes(C_3\times C_3)$ （ここに、$\gamma_1=(135),\delta=(14)(2563)$）である。

${}_6T_{13}$ の指数 2 の部分群 ${}_6T_9=\langle{}_6T_3,\gamma_1\rangle\simeq V_4\ltimes(C_3\times C_3)$ は ${}_6T_2$ を正規部分群として含み、${}_6T_9/{}_6T_2\simeq\langle\overline{\gamma_2},\overline{\alpha^3}\rangle\simeq\mathfrak{S}_3$ である。$K^{{}_6T_2}=\boldsymbol{Q}(s,t,u,p)=\boldsymbol{Q}(t,u,p)$ への $\overline{\gamma_2},\overline{\alpha^3}$ の作用は、

$$\overline{\gamma_2}:\begin{cases}s\mapsto -\dfrac{s}{p}\\ t\mapsto \dfrac{t}{p^2}\\ u\mapsto -\dfrac{u}{p^3}\\ p\mapsto -\dfrac{u}{p^2}\end{cases},\qquad \overline{\theta}:\begin{cases}s\mapsto s\\ t\mapsto t\\ u\mapsto u\\ p\mapsto 1-s-p=\dfrac{u}{p}\end{cases}$$

であり、さらに $\overline{\gamma_2}(1-s+t-u)=\dfrac{1-s+t-u}{p^2}$ であることから、

$$r_1:=\frac{p}{1-s+t-u},\qquad r_2:=-\frac{u}{1-s+t-u},\qquad r_3:=\frac{1-s-p}{1-s+t-u}$$

とおくと、$K^{{}_6T_2}=\boldsymbol{Q}(r_1,r_2,r_3)$ であり、$r_1,r_2,r_3$ への作用が

$$\overline{\gamma_2}:\begin{cases}r_1\mapsto r_2\\ r_2\mapsto r_3\\ r_3\mapsto r_1\end{cases},\qquad \overline{\theta}:\begin{cases}r_1\mapsto r_3\\ r_2\mapsto r_2\\ r_3\mapsto r_1\end{cases}$$

と置換になっている。従って、${}_6T_9$ による固定体 $K^{{}_6T_9}$ は、$r_1,r_2,r_3$ の基本対称式

$$s_9:=r_1+r_2+r_3,\qquad t_9:=r_1r_2+r_3r_1+r_2r_3,\qquad u_9:=r_1r_2r_3$$

で生成され有理的である：$K^{{}_6T_9}=\boldsymbol{Q}(s_9,t_9,u_9)$。

${}_6T_{13} = \langle {}_6T_9, \delta \rangle$ については、${}_6T_{13}/{}_6T_9 = \langle \overline{\delta} \rangle \simeq C_2$ の $K^{{}_6T_9} = \boldsymbol{Q}(s_9, t_9, u_9)$ への作用が、

$$\overline{\delta} : \begin{cases} s_9 \mapsto 1 - s_9 \\ t_9 \mapsto t_9 \\ u_9 \mapsto -u_9 \end{cases}$$

となるので、$s_{13} := \dfrac{2s_9 - 1}{u_9}$, $t_{13} := t_9$, $u_{13} := u_9^2$ とおくと、$K^{{}_6T_{13}} = \boldsymbol{Q}(s_{13}, t_{13}, u_{13})$ となり、有理的であることがわかる。

5.3. $(2,2,2)$ **非原始可移群.** 分割 $\{1,4\} \sqcup \{2,5\} \sqcup \{3,6\}$ を保つ $(2,2,2)$ 非原始性を持つ極大な部分群は、${}_6T_{11} = \langle {}_6T_3, \tau_1, \tau_2 \rangle \simeq \mathfrak{S}_3 \wr C_2 = \mathfrak{S}_3 \ltimes (C_2)^3 \simeq \mathfrak{S}_4 \times C_2$ （ここに、$\tau_1 = (14)(25), \tau_2 = (14)(36)$）である。${}_6T_{11}$ の中心は $Z({}_6T_{11}) = \langle \alpha^3 \rangle \simeq C_2$, であり、その固定体は前小節の $\boldsymbol{Q}(x,y,z)$ であった。${}_6T_{11}/Z({}_6T_{11}) = \langle \alpha^2, \alpha\beta, \tau_1, \tau_2 \rangle \simeq \mathfrak{S}_4$ の $K^{Z({}_6T_{11})} = \boldsymbol{Q}(x,y,z)$ への作用を考えよう。

$$\alpha^2 = (1\ 3\ 5)(2\ 4\ 6) : \begin{cases} x \mapsto y \\ y \mapsto z \\ z \mapsto x \end{cases}, \qquad \alpha\beta = (1\ 5)(2\ 4) : \begin{cases} x \mapsto x \\ y \mapsto z \\ z \mapsto y \end{cases},$$

$$\tau_1 = (1\ 4)(2\ 5) : \begin{cases} x \mapsto x \\ y \mapsto 1 - y \\ z \mapsto 1 - z \end{cases}, \qquad \tau_2 = (1\ 4)(3\ 6) : \begin{cases} x \mapsto 1 - x \\ y \mapsto y \\ z \mapsto 1 - z \end{cases}.$$

このままでも簡明だが、さらに見易くするために、$x' := 2x - 1, y' := 2y - 1, z' := 2z - 1$ とおこう。$\boldsymbol{Q}(x,y,z) = \boldsymbol{Q}(x',y',z')$ である。この変数変換は次の正規化から来る：

$$[0, x, *, 1, \infty, *] = [-1, x', *, 1, \infty, *],$$
$$[\infty, *, 0, y, *, 1] = [\infty, *, -1, y', *, 1],$$
$$[*, 1, \infty, *, 0, z] = [*, 1, \infty, *, -1, z'].$$

（標数 2 だと不可能なことに注意しよう。）すると、$x', y', z'$ への作用は次のようになる：

$$\alpha^2 : \begin{cases} x' \mapsto y' \\ y' \mapsto z' \\ z' \mapsto x' \end{cases}, \quad \alpha\beta : \begin{cases} x' \mapsto x' \\ y' \mapsto z' \\ z' \mapsto y' \end{cases}, \quad \tau_1 : \begin{cases} x' \mapsto x' \\ y' \mapsto -y' \\ z' \mapsto -z' \end{cases}, \quad \tau_2 : \begin{cases} x' \mapsto -x' \\ y' \mapsto y' \\ z' \mapsto -z' \end{cases}.$$

特筆すべきことに、この作用が ${}_6T_{11}/Z({}_6T_{11}) \simeq \mathfrak{S}_4$ の正八面体群としての 3 次元空間への標準的な作用に他ならない。これより、${}_6T_{11}$ による固定体は有理的で、

$$s_{11} = x'^2 + y'^2 + z'^2, \quad t_{11} = x'^2y'^2 + y'^2z'^2 + z'^2x'^2, \quad u_{11} = x'y'z'$$

とおけば、$K^{{}_6T_{11}} = \boldsymbol{Q}(x',y',z')^{\mathfrak{S}_4} = \boldsymbol{Q}(s_{11}, t_{11}, u_{11})$ となることは古典的な結果である。

5.4. 6 **次対称群** $\mathfrak{S}_6$**.** 現在のところ、ここまでのような直接的な計算では、6 次対称群 $\mathfrak{S}_6$ まで掘り進められてはいない。$\mathfrak{S}_6$ 固定体の有理性は、Siegel モジュラ関数体の有理性に関する結果（例えば井草 [Ig] など）を援用して得られている。手法が異なるので詳述はしないが簡単に触れておく。

$P = [t_1, \ldots, t_6] \in \mathcal{M}_{0,6}$ に対し、$X = t_i$ で分岐する 2 次被覆 $C : Y^2 = \prod_{i=1}^6 (X - t_i)$ を対応させ、その Jacobi 多様体 $J_C$ を考えることにより、レベル 2 構造付きの主偏極アーベル曲面のモジュライ空間 $\mathcal{A}_2[2]$ への射 $\mathcal{M}_{0,6} \longrightarrow \mathcal{A}_2[2]$ が定まるここで $\mathcal{M}_{0,6}$ の点の順番付けと $\mathcal{A}_2[2]$ のレベル 2 構造とが対応するので、それを忘れることにより、可換図式

$$\begin{array}{ccc} \mathcal{M}_{0,6} & \longrightarrow & \mathcal{A}_2[2] \\ \downarrow & & \downarrow \\ \mathcal{M}_{0,6}/\mathfrak{S}_6 & \longrightarrow & \mathcal{A}_2[2]/\mathrm{Sp}(4, \boldsymbol{F}_2) = \mathcal{A}_2 \end{array}$$

が得られる。ここに群同型 $\mathfrak{S}_6 \simeq \mathrm{Sp}(4, \boldsymbol{F}_2)$ が現れていることにも注意しよう。こうして、$\mathcal{M}_{0,6}/\mathfrak{S}_6$ の関数体 $K^{\mathfrak{S}_6}$ の有理性が、Siegel モジュラ関数体の有理性に帰着されて示される。

## 6. 複比の体の有理性問題と Noether 問題との関係

置換群 $G \subset \mathfrak{S}_n$ の作用に関する、Noether 問題（$n$ 変数有理関数体 $L = L_n$ の固定体 $L^G$ の有理性）と複比の体 $K = K_n$ の固定体 $K^G$ の有理性との間には、両方向とも自明な含意はないが、ある条件の下で $K^G$ の有理性から $L^G$ の有理性が従うことが知られている。

角皆 [T3] による部分的な結果の後、Reichstein により次の結果が得られている：

**定理 2** (Reichstein[R]). $n > 5$ とする。$G$ を $n$ 次対称群 $\mathfrak{S}_n$ の部分群とするとき、次は同値：

(1) $L^G$ が $K^G$ 上純超越的
(2) $L^G$ が $K^G$ 上 unirational
(3) $G$ の $\{1, \ldots, n\}$ への作用が、奇数位数の軌道を持つ

特に、$n$ が 5 以上の奇数のとき、$n$ 次置換群 $G \subset \mathfrak{S}_n$ に関する複比の体の固定体 $K^G$ が有理的ならば、$L^G$ も有理的、即ち、$G$ に関する Noether 問題が肯定的に解決される。

**例 6.1.** $n = 5$ のとき、5 次可移置換群 $G$ に関する複比の体の固定体 $K^G$ は有理的であり、従って、5 次可移置換群 $G$ に関する Noether 問題は肯定的である。特に、$G = \mathfrak{A}_5$ のときも含まれ、これは前田 [M] の結果の別証明となる。

## 参考文献


[AK] 穴井宏和、近藤武、$A_5$ を Galois 群に持つ 6 次式の族 —分解体と Galois 群の計算— 、「数式処理における理論とその応用の研究」、京大数理研講究録 **941** (1996), 57–72.

[B] Brumer, A., Curves with real multiplications, in preparation.

[B-MK] Butler, G., McKay, J., The transitive groups of degree up to eleven, *Comm. Algebra* **11** (1983), no. 8, 863–911.

[H] Hashimoto, K., On Brumer's family of RM-curves of genus two, *Tohoku Math. J.* (2) **52** (2000), no. 4, 475–488.

[HT1] Hashimoto, K., Tsunogai, H., Generic polynomials over $\boldsymbol{Q}$ with two parameters for the transitive groups of degree five, *Proc. Japan Acad.* **79A** (2003), 148–151.

[HT2] Hashimoto, K., Tsunogai, H., Noether's problem for transitive permutation groups of degree 6, Adv. Stud. Pure Math. **63** (*Galois-Teichmüller Theory and Arithmetic Geometry*) (2012), 189–220.

[HHR] Hashimoto, K., Hoshi, A., Rikuna, Y., Noether's problem and $\mathbb{Q}$-generic polynomials for the normalizer of the 8-cycle in $S_8$ and its subgroups, *Math. Comp.* **77** (2008), no. 262, 1153–1183.

[Ih] Ihara, Y., On the embedding of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ into $\widehat{GT}$, in "*The Grothendieck theory of Dessins d'Enfants*", London Math. Soc. Lecture Note Ser. 200, Cambridge University Press, 1994, 173–200.

[Ig] Igusa, J., Modular Forms and Projective Invariants, *Amer J. Math.* **89** (1967), 817–855.

[KM] Kemper, G., Mattig, E., Generic polynomials with few parameters, *J. Symbolic Computation* **30** (2000), 843–857.

[KRY] Kida, M., Renault, G., Yokoyama, K., Quintic polynomials of Hashimoto-Tsunogai, Brumer and Kummer, *Int. J. Number Theory* **5** (2009), no. 4, 555–571.

[Ki] Kihel, O., Groupe des unités pour des extensions diédrales complexes de degré 10 sur $\boldsymbol{Q}$, *J. Théor. Nombres Bordeaux* **13** (2001), no. 2, 469–482.

[Lec] Lecacheux, O., Construction de polynômes génériques à groupe de Galois résoluble, *Acta Arith.* **86** (1998), 207–216.

[Len] Lenstra, H. W., Rational functions invariant under a finite abelian group, *Invent. Math.* **25** (1974), 299–325.

[M] Maeda, T., Noether's Problem for $A_5$, *J. Algebra* **125** (1989), 418–430.

[T1] Tsunogai, H., Some new-type equations in the Grothendieck-Teichmüller group arising from geometry of $\mathcal{M}_{0,5}$, AMS Contemp. Math. 416 (JAMI Proceedings "*Primes and Knots*", T. Kohno, M.Morishita eds.) (2006), 263–284.

[T2] 角皆宏、単数を根とする $\mathfrak{A}_5$ 多項式族、「福岡数論研究集会」報告集 （小松亨編）(2006), 47–56.

[T3] Tsunogai, H., Toward Noether's Problem for the fields of cross-ratios, *Tokyo J. Math.* **39** (2017), no. 3, 901–922.
[T*] 角皆宏、ガロア群の構成問題の明示解の活用〜明示的な多項式があると出来ること〜、本報告集所収.
[R] Reichstein, Z., On a rationality problem for fields of cross-ratios, *Tokyo J. Math*, advance publication, 24 August 2019. https://projecteuclid.org/euclid.tjm/1566612102
[S] Shanks, D., The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152.
[W] Wang, S., A counterexample to Grunwald's theorem, *Ann. of Math.* **49(4)** (1948), 1008–1009.

上智大学理工学部情報理工学科 102-8554 東京都千代田区紀尾井町 7-1
*E-mail address*: tsuno-h@sophia.ac.jp

# 有限単純群の分類問題

田中康彦（大分大学）

## 1　素数 2 の役割

単純群とは、正規部分群が自明な部分群に限られる群をいう。Jordan-Hölder の定理によれば、すべての有限群は単純群を積み重ねたような構造をしている。有限単純群を分類するという問題は、有限群論において基本的・中心的な位置を占めてきた。有限群が数学の対象として認識されたのは、 Abel、 Galois による方程式の可解性問題にかかわる置換群論が最初と思われる。そのころにはすでに小さい単純群として、交代群、有限素体上の線型群などがすでに知られていた。

歴史的な歩みを正確にたどることは到底できないが、現在へと連なる有限群論のマイルストーンとして二点だけ述べておきたい。第一は Burnside 予想およびその肯定的解決である Feit-Thompson の定理であり、第二は有限単純群の構造が位数 2 の中心化群の構造によってほぼ決まってしまうと主張する Brauer-Fowler の原理である。

**Theorem** (Burnside 予想 [14]・Feit-Thompson の定理 [16])**.** 奇数位数の群は可解である。（注意：　現在では、Bender-Glauberman による証明の簡易化 [11] も知られている。）

このように端的に述べられる予想・定理は、たいていは奥深い理論を内包しているものである。Burnside 予想は 20 世紀初頭にまでさかのぼる。有名な「有限群論」もそのころに出版された。置換群論の全盛期から指標理論による表現論の発展を見ながら抽象代数学としての群論へと、時代の流れを感じさせる（もしくは主張する）一冊であった。当時 Burnside は位数 40,000 未満の群において予想が正しいと確認していたらしい。したがって、漠然としながらもおおよそ正しいと信じられていたのであろう。しかしながら予想が解決されるまでに 50 年の年月が過ぎ去った。放っておいたわけではないし、日本人の多大な貢献もあったのだが、結局の

ところ天才の出現を待たざるを得なかったということであろう。Feit と Thompson による論文は「Odd Order Paper」と呼ばれ、250 ページにも及ぶ、長大かつ難解な論文である。その意義を以下のようにまとめてみた。

**まとめ.** Burnside 予想の解決には以下の意義が認められる。

**現象論** Sylow の定理とあわせて、有限単純群は位数 2 の元を含むことがわかった。

**方法論** 局所解析、すなわち、局所部分群（中心化群もその一種）の構造を調べるためのさまざまな技術的指針を示した。

**将来展望** のちの位数 2 の元による特徴づけと併せ、単純群の分類問題の解決に対して一つの方向性を示した。

有限単純群が位数 2 の元を必ず含むとわかったとはいえ、そのままでは次の一歩が踏み出せなかったであろう。時間的には多少前後するが、そこに登場したのが、次の Brauer-Fowler の定理であった。

**Theorem** (Brauer-Fowler の定理 [10])**.** 有限単純群の位数は、位数 2 の元の中心化群の位数のある関数で押さえられる。

これにより有限単純群の位数は、位数 2 の元の中心化群の位数を指定すれば、高々有限の可能性に限られる。もちろん位数が限定されれば（乗積表が有限とおりなので）同型類は有限個に限られてしまう。Brauer の優れたところは、単に位数の問題では済ませず、位数 2 の元の中心化群の構造を指定したときに、有限単純群の構造までほとんど決めてしまえるという可能性を、簡単な実例をもって示したことである。

次の命題は、簡単な行列の計算によって示される。

**Proposition.** 有限単純群 $G^* = PSL_3(q)$ （$q \equiv 3 \pmod 4$） と位数 2 の元 $t = \mathrm{diag}(-1, -1, 1)$ に対しては、 $C_{G^*}(t) \cong GL_2(q)$ が成り立つ。

Brauer はこの命題の逆を考え、位数 2 の元による特徴づけの例を与えた。

**Theorem** (Brauer [12])**.** 有限単純群 $G$ とその位数 2 の元 $t$ に対して、$C_G(t) \cong GL_2(q)$ （$q \equiv 3 \pmod 4$）であると仮定する。このとき、以下のいずれかが成り立つ。

(1) $q > 3$ のときは、 $G \cong PSL_3(q)$ である。

(2) $q = 3$ のときは、 $G \cong PSL_3(3)$ または $G \cong M_{11}$ である。

最初の $q > 3$ のときは元の命題の逆が成立している。ここでは $q = 3$ の場合が真の例外となる。実際線型群とは関係のなさそうな群が現れる。これは古くから知られている Mathieu 群（のうち最も小さい群）である。これらの結果について、その意義を以下のようにまとめてみた。

**まとめ.** Brauer-Fowler による位数 2 の元の中心化群への着目には以下の意義が認められる。

**方法論** 位数 2 の元の中心化群の位数を指定すれば、単純群の構造は有限個に限られ、その同型類を決定する方法がありうること、その際に想定していない単純群（もしかすると未知の単純群）が現れる可能性もありうることを示した。

**将来展望** 問題を、「有限単純群の位数 2 の元の中心化群はどのような構造をもつか調べること」、「位数 2 の元の中心化群の構造を指定したときに単純群を分類すること」の二点に集約し定式化した。

以上により、単純群の分類に向けての方針が定まった。これまでしばしば登場してきたのが「位数 2 の元」である。これを奇素数 $p$ にして「位数 $p$ の元」と置き換えることはできない。さてそれではなぜ位数 2 なのか。有限単純群においては、素数 2 は奇素数に比して特別や役割を期待されているように見える。それで、次に素数 2 の特殊性について考えてみたい。

ここで取り上げるのは、素数 2 がみたす三つの性質

「$2 = 1 + 1$」、「2 は偶数」、「2 は最小の素数」

である。それぞれ簡単に見てみよう。

## 1.1 $2 = 1 + 1$

群 $G$ の元に対して、位数が 2 であることと、逆元が自分自身に一致することとは同値である。さて素数 $p$ に対して、単位元以外の元がすべて位数 $p$ である $p$ 群を考えよう。このとき以下の定理が成り立つ。

**Proposition.** $p$ を素数とする。$p$ 群 $P$ は単位元以外の元はすべて位数 $p$ であるとする。もし $p = 2$ ならば、 $P$ は可換群（基本可換 $p$ 群）である。

***Proof.*** 任意の元 $x, y \in P$ を取る。このとき、 $x^{-1}y^{-1}xy = xyxy = (xy)^2 = 1$ である。よって、 $xy = yx$ となる。

奇素数 $p$ に対しては反例がある。実際、 $p$ 元体上の 3 次元一般線型群 $GL_3(p)$ において、対角成分がすべて 1 の上三角行列全体のつくる部分群を考えよう。この群は位数 $p^3$ の非可換群であり、単位元以外のすべての元の位数が $p$ である。

次に素数位数の自己同型をもつ群を考えよう。群 $G$ の自己同型 $a$ が $x^a = x$ （$x \in G$）をみたすとき、固定点 $x$ をもつという。単位元はつねに固定点である。もし単位元以外に固定点をもたないならば、 $a$ は固定点なしに作用するという。このとき以下の定理が成り立つ。

**Proposition.** $p$ を素数とする。群 $G$ は固定点なしに作用する位数 $p$ の自己同型をもつとする。もし $p = 2$ ならば、 $G$ は奇数位数の可換群である。

***Proof.*** 群 $G$ の固定点なしの位数 2 の自己同型を $a$ とする。もし $G$ が偶数位数とすると、 $G$ は $a$ 不変なシロー 2 －部分群 $T$ をもつが、 $a$ は $T$ の中に単位元と異なる固定点をもってしまい矛盾が生じる。よって $G$ は奇数位数である。$G$ の部分集合 $S$ を $S = \{\ x^{-1}x^a \mid x \in G\ \}$ とおく。もし $x^{-1}x^a = y^{-1}y^a$ ならば、 $(xy^{-1})^a = xy^{-1}$ である。$a$ は固定点なしなので、 $x \neq y$ ならば $x^{-1}x^a \neq y^{-1}y^a$ である。よって元の個数を比べて $G = S$ となる。したがって、 $a$ は $G$ の各元をインバートする（逆元にうつす）。よって、任意の $x, y \in G$ に対して、 $xy = (x^{-1})^a(y^{-1})^a = (x^{-1}y^{-1})^a = ((yx)^{-1})^a = yx$ が成り立つ。

奇素数 $p$ に対しては反例がある。例えば、 4 元体上の 3 次元一般線型群 $GL_3(4)$ において、対角成分がすべて 1 の上三角行列全体のつくる部分群 $G$ を考えよう。この群は位数 $4^3$ の非可換群である。4 元体の乗法群の生成元 $\alpha$ により、 $a = \mathrm{diag}(\alpha, \alpha^{-1}, 1)$ とおき、$x \in G$ に対して $x$ の $a$ による共役を、 $x^a = a^{-1}xa$ と定義する。これにより、 $a$ は $G$ 上に位数 3 の自己同型を引き起こす。行列の計算により $a$ の $G$ 上の固定点は単位元に限ることがわかる。

ところが奇素数の場合には Thompson の大定理があり、実際、固定点なしの素数位数の自己同型をもつ群はべき零群であることが証明された（[23]）。この定理により、 Frobenius の問題（Frobenius 群における Frobenius 核のべき零性）が解決された（[24]）。ついでに（といっては大変失礼だが）言及すると、Thompson は 1970 年にフィールズ賞に輝いているが、その主たる業績として、「奇数位数の群の可解性（[16]）」「固定点なしの素数位数の自己同型をもつ群のべき零性（[23]）」「すべての局所部分群が可解群である単純群の分類（[25]）」が挙げられる。

## 1.2　2 は偶数

置換に関して次の命題は易しい。

**Proposition.** $p$ を素数とする。長さ $p$ の巡回置換は、 $p > 2$ ならば偶置換、 $p = 2$ ならば奇置換である。

***Proof.*** $(1, 2, \ldots, p) = (1, 2)(1, 3) \cdots (1, p)$ のように、長さ $p$ のサイクルは $p - 1$ 個の互換の積で表される。

さて偶数 $2k$ は 2 で割り切れてその商は $k$ になる。小学校でやるようにこれには、「大きさが $k$ のもの 2 個に分ける」、「大きさが 2 のもの $k$ 個に分ける」の二通りの意味がある。それぞれの意味に応じて、素数 2 に特有の命題が知られている。

**Proposition.** 指数 2 の部分群は正規部分群である。

***Proof.*** 【証明】群 $G$ の指数 2 の部分群を $H$ とする。このとき、 $G = H \cup (G - H)$ が $H$ に関する左かつ右剰余類分解になる。よって、 $H$ に関する左剰余類と右剰余類は一致する。（注意：有限群でなくても成り立つ。）

**Proposition.** 有限群 $G$ は指数 $2k$ （$k$ は奇数）の部分群 $M$ をもつとする。もし $G$ が位数 2 の元で $M$ のどの元とも共役でないものをもてば、$G$ は指数 2 の正規部分群をもつ。（よって $G$ は単純群ではない。）

***Proof.*** 【証明】群 $G$ は $M$ に関する右剰余類の集合 $\Omega$ 上に作用する。位数 2 の元 $t$ を取る。任意の $x \in G$ に対して、 $t^x = x^{-1}tx \notin M$ なので、$Mxt \neq Mx$ となる。ゆえに、 $t$ は $\Omega$ 上に固定点をもたないが、これは $t$ が $k$ 個の互換の積に対応する置換を引き起こすことを示している。したがって、 $H = \{\ \Omega$ 上に偶置換を引き起こす $G$ の元 $\}$ とすると、$H$ は $G$ の指数 2 の部分群となる。

最後の命題は、単純群においては位数 2 の元が共役という操作によってあちらこちらに動き回ることを示している。

## 1.3 2 は最小の素数

ここでは、 Burnside の定理に触れる。先に言及した「有限群論」にもすでに出ている。

**Definition.** 有限群 $G$ とその位数を割り切る素数 $p$ に対して、 $p'$ 部分群 $N$ で指数 $|G:N|$ が $p$ の累乗であるものを $p$ 補部分群（$p$ 補群）と呼ぶ。特に正規部分群であるとき、正規 $p$ 補部分群（正規 $p$ 補群）という。

**Proposition** (Burnside [14])**.** 有限群 $G$ に対して、その位数を割り切る最小の素数を $p$ とする。もし $G$ の Sylow $p$ 部分群が巡回群ならば、 $G$ は正規 $p$ 補部分群をもつ。（よって $G$ は単純群ではない。）

***Proof*.** ここでは、 Higman [19] による移送の理論を使った証明を概略だけ示す。$G$ の Sylow $p$ 部分群を $P$ とする。$P$ の焦点部分群を $P^* = \langle x^{-1}y \mid x, y \in P \text{ は } G \text{ において共役} \rangle$ と定義すると、 $P^* = P \cap G'$ となることが知られている。ここで、 $G'$ は $G$ の交換子群を表す。以上を認めると、

(1) $N_G(P) = C_G(P)$ となる。（$p$ の最小性より）

(2) 異なる $x, y \in P$ は $N_G(P)$ において共役でない。

(3) 異なる $x, y \in P$ は $G$ において共役でない。

(4) $P^* = 1$.

(5) $G' \neq G$.

Burnside の定理により、有限単純群の Sylow 2 部分群は巡回群ではない。もちろん奇素数に対しては反例がある。例えば五次交代群は、位数 $60 = 2^2 \times 3 \times 5$ なので、Sylow 3 部分群と Sylow 5 部分群は巡回群である。また、有限素体上の二次元射影特殊線型群 $PSL_2(p)$ （$p \geq 5$）は、位数 $p(p-1)(p+1)/2$ なので、 Sylow $p$ 部分群は巡回群である。

有限単純群 $G$ の Sylow $p$ 部分群を $P$ とすると、その焦点部分群 $P^*$ は上述のように $P^* = P \cap G'$ をみたす。ここで、 $G'$ は $G$ の交換子群を

表す。よって単純群の Sylow 部分群においては、共役という操作によって元が十分にあちらこちらに（焦点部分群が小さくならないように）動き回らないといけない。単純群でいるためには、周囲の監視の目が厳しくて結構ハードルが高いのである。

以上述べてきたように、有限単純群を具体的に解析するためには、素数 2 に対する特別な取り扱いが常に必要となる。

## 2　有限単純群の分類定理

まずは分類定理を述べておく。

**Theorem.** 有限単純群は次の知られている単純群のリスト $\mathcal{K}$ に載っている群のいずれかと同型である。

(1) 素数位数の群

(2) 五次以上の交代群

(3) 有限体上で定義された Lie 型の群（Chevalley 群、Steinberg 群など）

(4) 散在型の群（26 個）

以下では研究者たちが、この定理をどのような方針で証明しようと考え、それが実行されたかについて簡単に紹介する。群の演算と有限性だけから出発するので、証明が位数に関する帰納法によるのはおおよそ予想されることであろう。有限単純群が自己同型として作用する数学的な（例えば幾何学的な）対象を構築しそちらの方を分類するという考え方もあるが、現在のところ新しい分類が成功したという話は聞かない。

これ以後は、単純群といえばすべて非可換単純群を指す。リスト $\mathcal{K}$ を見るとわかるように、ターゲットとなる単純群の大部分が「奇数標数の有限体上で定義された Lie 型の群」である。それで、乱暴ではあるが定理の結論を大雑把に二つに分けて、「奇数標数の有限体上で定義された Lie 型の群」または「それ以外の群」のいずれかに同型であることを示そうと考える。当初は「それ以外の群」として未知の単純群が現れる可能性もあった。その場合は新しい群を付け加えてリスト $\mathcal{K}$ を更新し、もう一度やり直すという考えであった。

すでに見たように、 Feit-Thompson の定理、および、 Brauer-Fowler の原理を出発点にするならば、問題は以下の二つに分けられる。

(1) 有限単純群の位数 2 の元の中心化群にはどのような構造が可能かを調べる。

(2) 位数 2 の元の中心化群の構造を指定したときに、そのような位数 2 の元を含む有限単純群を分類する。

はじめの問題は、位数 2 の元の中心化群になりうる群を確定することである。例えば、明らかに中心の位数は偶数でないといけない。これを「選別の問題」と呼ぶことにする。あとの問題は、部分の性質によって全体を統制することである。Brauer の実例がその一例である。これを「特徴づけの問題」と呼ぶことにする。

有限単純群における素数 2 の役割に関しては、 Sylow 2 部分群に着目する流儀もあるので、少し言及しておく。巡回群である 2 群が有限単純群の Sylow 2 部分群になれないことはすでに見たとおりである。一般に有限単純群の Sylow 2 部分群は、構造が著しく制限されてしまう。したがって、位数 2 の元の中心化群の場合と同様に、 Sylow 2 部分群の選別と決定の問題が生じてくるのは自然なことである。

交代群や有限体上で定義された線型群を観察してみると、例えば、「基本可換 2 群」、「二面体群」、「準二面体群」、「環積型の 2 群」は、有限単純群の Sylow 2 部分群になれることがわかる。逆にこれらの 2 群による有限単純群の特徴づけも知られている（[26], [8], [18], [9], [5]）。それ以外にも多数の結果が知られているが、この方向ですべての有限単純群を網羅するには至らなかった。（すべては使わずに済んだ。）

## 2.1 特徴づけの問題

位数 2 の元の中心化群による特徴づけに関しては、Brauer の実例を出発点として、さまざまな結果が得られている。リスト $\mathcal{K}$ に載っている群に対しては、位数 2 の元による特徴づけが少なくとも一つはある。

有名な例をもう一つ紹介してみよう。言葉と記号を整理しておく。例外型と呼ばれる Lie 型の単純群 $G_2(q)$ は、定義体の標数が 3 で Frobenius 自己同型が平方根をもつときに、 Coxeter グラフの対称性に起因する自己同型をもつ。この自己同型で不変な元の全体がなす部分群を ${}^2G_2(q)$ と表す。このとき、 $q$ は 3 の奇数乗であり、 ${}^2G_2(q)$ は $q = 3$ の場合を除いて単純群になる。

**Proposition.** 有限単純群 $G^* = {}^2G_2(q)$ （$q = 3^{2m+1}$ （$m \geq 1$））は位数 2 の元 $t$ で、$C_{G^*}(t) = \langle t \rangle \times L$、$L \cong PSL_2(q)$ をみたすものを含む。

Brauer にならってこの命題の逆を考えると、以下の命題が得られる。

**Theorem** (Janko [20])**.** 有限単純群 $G$ とその位数 2 の元 $t$ に対して、$C_G(t) = \langle t \rangle \times L$, $L \cong PSL_2(q)$ （$q$ は 5 以上の奇素数べき）であると仮定する。このとき、以下のいずれかが成り立つ。

(1) $q > 5$ のときは、$q = 3^{2m+1}$ （$m \geq 1$）、$L \cong PSL_2(q)$、$G \cong {}^2G_2(q)$ である。

(2) $q = 5$ のときは、$L \cong PSL_2(5) \cong A_5$、$G \cong J_1$ である。

最初の $q > 5$ のときは元の命題の逆が成立していて、真の例外となるのが $q = 5$ の場合である。その際に現れる群 $J_1$ は、Mathieu 群以来初めて発見された線型群や交代群の系列に属さない単純群である。これが端緒となって、散在型と呼ばれる単純群（Mathieu 群以外に 21 個）が次々と現れるようになった。

**Definition.** 有限単純群 $G$ がリスト $\mathcal{K}$ に含まれているある群 $G^*$ に**似ている**とは、知られている特徴づけを利用すれば $G \cong G^*$ であることを示すに足るだけの情報が得られていることをいう。

分類定理は、次の定理に帰着される。

**Theorem.** 有限単純群は知られている単純群のリスト $\mathcal{K}$ に載っている群のいずれかに似ている。

## 2.2 選別の問題

「奇数標数の有限体上で定義された Lie 型の群」に分類される単純群と、「それ以外の群」に分類される単純群はどこが違うであろうか。実例を調べるために、言葉を用意する。

**Definition.** 有限群 $L$ が**準単純群**であるとは、$L' = L$ であり、かつ、$L/Z(L)$ が単純群であることをいう。有限群 $N$ が**半単純群**であるとは、$N' = N$ であり、かつ、$N/Z(N)$ が単純群の直積であることをいう。有限群 $G$ の部分群 $S$ が**連正規部分群**であるとは、部分群の列 $G_0, G_1, \ldots, G_n$

で、 $G_0 = G$、 $G_n = S$、 $G_i \trianglelefteq G_{i-1}$ （$1 \leq i \leq n$）となるものがあることをいう。有限群の**成分**とは、連正規準単純部分群をいう。有限群 $G$ の 2-*rank* とは、基本可換 2 部分群の rank の最大値をいい、 $m_2(G)$ と表す。

例えば線型群 $G^* = PSL_n(q)$ （$n \geq 4$、 $q$ は奇素数の累乗で $q > 3$）とする。位数 2 の元 $t = \mathrm{diag}(-1, -1, 1, \ldots, 1)$ に対して、 $C_{G^*}(t)$ はおおよそ $SL_2(q) \times SL_{n-2}(q)$ と同型である。よってこの同型により、 $SL_2(q)$ および $SL_{n-2}(q)$ に対応する部分群が $C_{G^*}(t)$ の成分である。あるいは交代群 $G^* = A_n$ （$n \geq 9$）と位数 2 の元 $t = (1,2)(3,4)$ に対して、 $C_{G^*}(t)$ は $D_8 \times S_{n-4}$ の指数 2 の部分群と同型である。よって $C_{G^*}(t)$ は $A_{n-4}$ 同型な成分をもつ。このように、一般に、奇数標数の有限体上で定義された高次元の線型群や大きい次数の交代群においては、位数 2 のある元の中心化群が成分をもつ。

有限単純群は、位数 2 のある元の中心化群が成分をもつとき成分型であると定義したい。しかしながら、技術的な理由により 2-rank が十分大きいこと（少なくとも 3 以上、できれば 4 以上）が望まれる。それで 2-rank に関する条件を付け加えて、以下のように定義する。

**Definition.** 有限単純群 $G$ が**成分型**であるとは、 $m_2(G) \geq 3$ であり、かつ、位数 2 のある元の中心化群が成分をもつことである。

以上により、奇数型の群の概念に到達する。

**Definition.** 有限単純群 $G$ が**奇数型**であるとは、 $m_2(G) \leq 2$ である（Odd Small）か、もしくは、成分型の群である（Odd Large）かのいずれかであることとする。

これによりわれわれの目標は次の定理の形に定式化される。

**Theorem.** 有限単純群が奇数型であれば、リスト $\mathcal{K}$ に含まれる単純群（奇数標数の有限体上で定義された線型群、もしくは、少数の例外の群）に似ている。

われわれの方針では、 2-rank が小さい単純群は別に扱わなければならない。幸いなことに、すでに知られている Sylow 2 部分群となりうる 2 群の選別、および、 Sylow 2 部分群による特徴付けの結果を利用することができる。

**Theorem** (Burnside [14], Brauer-Suzuki [13], Alperin-Brauer-Gorenstein [6], Gorenstein-Walter [18], Alperin-Brauer-Gorenstein [5], Lyons [21])**.** 有限単純群 $G$ が $m_2(G) \leq 2$ であるとする。このとき以下が成り立つ。

(1) $m_2(G) = 2$ である。

(2) $G$ の Sylow 2 部分群は、「二面体群」、「準二面体群」、「環積型の 2 群」、「4 元体上の 3 次元射影特殊ユニタリ群 $PSU_3(4)$ の Sylow 2 部分群と同型な 2 群」のいずれかである。

(3) $G$ はリスト $\mathcal{K}$ に含まれる群に似ている。

(注意： 位数 4 の基本可換群は位数 4 の二面体群と考えている。また二面体群の場合の特徴づけに関しては、 Bender による証明の簡易化 [9] が知られている。)

## 2.3 標準成分問題

有限単純群 $G$ が成分型の群であるとする。すると位数 2 のある元 $t$ に対して、 $C_G(t)$ は成分をもつので、それを $L$ としよう。このとき、$|L/Z(L)| < |G|$ である。われわれは帰納法によって分類定理を証明しようとしているので、 $L/Z(L)$ はリスト $\mathcal{K}$ に含まれている群に同型であると考えてよい。それで、ある位数 2 の中心化群が指定された構造の成分をもつときに、有限単純群の構造を決定するという問題が生じてくる。

しかしながらこれだけでは単純群の構造を決定することはできなかった。位数 2 の中心化群の成分についての情報が大ざっぱすぎたのである。その後、 Aschbacher が成分の概念を精密化した標準成分の概念を提案し, 成分型の単純群は少数の例外（例外の定義は省略）を除いて標準成分をもつことを示した。

**Theorem** (Aschbacher [1])**.** 有限単純群 $G$ は成分型であり、例外の場合には該当しないとする。このとき、位数 2 のある元 $t$ の中心化群 $C_G(t)$ の成分 $L$ と部分群 $Q = C_G(L)$ が、おおよそ次の条件をみたす。

(1) 任意の $x \in G$ に対して、 $[L, L^x] \neq 1$ である。

(2) $Q = C_G(L)$ とおくと、任意の $x \in G - N_G(Q)$ に対して、 $Q \cap Q^x$ は奇数位数である。

この定理の条件をみたす成分 $L$ を**標準成分**と呼ぶ。また、部分群 $Q$ は**ぴったりと埋め込まれている**という。イメージとしては、 $L$ は $G$ の中でも大きな部分を占め、$Q$ は $C_G(t)$ において $L$ のカバーできなかった

部分をしっかり補う感じである。多くの場合は、位数 2 の元 $u, v \in G$ とそれぞれの中心化群に含まれる成分 $K, L$ が、$G = \langle K, L \rangle$ であり、かつ、$K \cap L$ が大きい部分群であるように取れることを使う。その場合は、$K$ と $L$ に対する生成元と関係式から、$G$ に対する生成元と関係式が得られるのである。

Aschbacher は標準成分問題の応用として、奇数標数の有限体上で定義された Lie 型の単純群の特徴づけを与えた。

**Theorem** (Aschbacher [2])**.** 有限単純群 $G$ は成分型であるとする。もし $G$ がぴったりと埋め込まれた部分群 $Q$ を含み、$Q$ が適切な付加条件をみたせば、奇数標数の有限体上で定義された Lie 型の単純群、もしくは、Mathieu 群 $M_{11}$、$M_{12}$ のいずれかに似ている。

例えば、$G^* = PSL_n(q)$ （$n \geq 6$、$q$ は奇素数の累乗）としよう。位数 2 の元として、$t = \mathrm{diag}(-1, -1, 1, \ldots, 1)$ をとる。このとき中心化群 $C_{G^*}(t)$ は、$SL_{n-2}(q)$ とおおよそ同型な標準成分、および、$SL_2(q)$ とおおよそ同型なぴったりと埋め込まれた部分群をもつ。上の定理は、Brauer が最初に方向性を示した定理（$n = 3$、$q \equiv 3 \pmod 4$ の場合にあたる）の拡張になっている。

## 2.4 非成分型の単純群

この段階で残っている有限単純群は、位数 2 のどの元の中心化群も成分をもたないものである。

**Definition.** 有限単純群が**非成分型**であるとは、位数 2 のどの元の中心化群も成分をもたないこととする。有限群の 2 *local* 部分群とは、単位群でない 2 部分群の正規化群をいう。有限群 $G$ と素数 $p$ に対して、最大の正規 $p$ 部分群を $O_p(G)$ と表す。有限単純群 $G$ が**標数 2 型**であるとは、任意の 2 local 部分群 $L$ に対して、$C_L(O_2(L)) \subseteq O_2(L)$ が成り立つこととする。

標数 2 の有限体上で定義された線型群を考えよう。例えば $G^* = PSL_n(q)$（$n \geq 3$、$q$ は 2 の累乗）とする。位数 2 の元 $t$ の Jordan 標準形はサイズ 2 の Jordan セルを $k$ 個もつとしよう。このとき、$C = C_{G^*}(t)$ は以下の構造をもつ。

(1) $C$ は成分をもたない

(2) $O_2(C)$ は単位群でない

(3) $C/O_2(C)$ は $SL_k(q) \times SL_{n-2k}(q)$ とほとんど同型である。

(4) $C_L(O_2(L)) \subseteq O_2(L)$ が成り立つ

**Definition.** 有限単純群 $G$ は標数 2 型であるとする。奇素数 $p$ に対して、 $G$ の 2 *local p-rank* とは、すべての 2 local 部分群に対する $p$-rank の最大値をいう。有限単純群 $G$ の *rank*（Thompson rank）とは、$p$ が奇素数全体を動くときの 2 local $p$-rank の最大値をいい、 $e(G)$ で表す。

標数 2 の有限体上で定義された Lie 型の単純群においては、いくつかの小さい群を除けば Thompson rank は Lie rank と一致する。

さて成分型の単純群の分類の主要部分は、位数 2 の元の中心化群の構造を解析することであった。非成分型の単純群の分類においては、概念的に似た手法を取り入れる。位数 2 の元の中心化群の代わりに、適当な奇素数 $p$ に対する位数 $p$ の元の中心化群を考えるのである。その際には標準成分の類似物として、奇数型の標準成分なども現れる。そうすると奇数型の群の解析をした場合と同様に、 rank が小さいときに障害が生じる。そのためには rank が十分大きいこと（少なくとも 3 以上、できれば 4 以上）が望ましい。それで標数 2 型の定義に rank に関する条件を付け加えて、以下のように改めて定義しなおす。

**Definition.** 有限単純群 $G$ においては、任意の 2 local 部分群 $L$ に対して、 $C_L(O_2(L)) \subseteq O_2(L)$ が成り立っているとする。この群 $G$ が**標数 2 型**であるとは、 $e(G) \geq 3$ であることをいい、**ほぼ薄い**群であるとは、$e(G) \leq 2$ であることをいう。

以上により、偶数型の群の概念に到達する。

**Definition.** 有限群 $G$ が**偶数型**であるとは、ほぼ薄い群である（Even Small）か、もしくは、標数 2 型の群である（Even Large）かのいずれかであることとする。

これによりわれわれの目標は次の定理の形に定式化される。

**Theorem** (Gorenstein-Lyons [17], Aschbacher [4], ...)**.** 有限単純群が標数 2 型であれば、リスト $\mathcal{K}$ に含まれる単純群（標数 2 の有限体上で定義された線型群、もしくは、少数の例外の群）に似ている。

**Theorem** (Aschbacher-Smith [7], Aschbacher [3] (Mason [22]))**.** 有限単純群 $G$ がほぼ薄い群であれば、リスト $\mathcal{K}$ に含まれる単純群（標数 2 の有限体上で定義された線型群、もしくは、少数の例外の群）に似ている。

以上により、単純群分類の過程における主たる場合分けと、それぞれの場合に最も重要な問題を紹介することができた。それぞれの場合を一つもしくはごく少数の定理の形にして紹介したが、実際には非常に多く場合分けが必要であり、多くの研究者による成果の集大成であることに注意しておく。

Classification Grid

| | Odd | Even |
|---|---|---|
| Small | Small 2 rank Problems | Quasithin Problems |
| Large | Standard Component Problems | Odd Standard Component Problems |

## 3　実例：交代群と線型群

以下の表は、交代群 $A_n$ （$n \geq 5$）と射影特殊線型群 $L_n(q) = PSL_n(q)$（$n \geq 2$、 $q$ は素数の累乗）が、これまでに延べてきた 4 つのカテゴリー（Odd Small)、(Odd Large)、(Even Small)、(Even Large）のうちのどの部分に現れるかを示したものである。

Alternating Groups

| | Odd | Even |
|---|---|---|
| Small | $A_5, A_6, A_7$ | $A_5, A_6, A_8$ |
| Large | $A_n$ $(n \geq 9)$ | none |

Linear Groups

| | Odd | Even |
|---|---|---|
| Small | $L_2(4), L_3(2)$;<br>$L_2(q), L_3(q)$ ($q$ is odd);<br>$L_4(q)$ ($q \equiv 1(\mathrm{mod}8)$) | $L_2(5), L_2(7), L_2(9)$;<br>$L_2(2^n), L_3(2^n), L_4(2^n)$;<br>$L_5(2), L_6(2), L_7(2)$ |
| Large | Other than above groups of odd characteristic | Other than above groups of even characteristic |

しかしながら、この場合分けの境界はいろいろな意味でかなりあいまいである。

まず以下の例が示すように、いくつかの小さい群は複数のブロックに現れる。

- $A_5 \cong PSL_2(5) \cong PSL_2(4)$
- $PSL_2(7) \cong PSL_3(2)$
- $A_6 \cong PSL_2(9)$

他の Lie 型の群を加えてよければもっと例がある。（ユニタリ―群や斜交群については、例えば [15] を参照せよ。）

- $A_6 \cong PSL_2(9) \cong PSp_4(2)'$
- ${}^2G_2(3)' \cong PSL_2(8)$
- $PSU_3(3) \cong G_2(2)'$
- $PSp_4(3) \cong PSU_4(2)'$

このことは、奇数型の群と偶数型の群の境界が必ずしも絶対的ではないことを示唆している。実はこの現象は小さい群以外においても生じうる。上では偶数型の群として標数 2 型という定義を採用したが、これを別の定義に取り換えると、偶奇のカテゴリー間を移動する群が現れる。あくまでも分類定理の証明における技術的な理由による分け方であり、最善の定義になっているかは明らかではない。

さらに、$PSL_2(2^n)$（標数 2 で rank 1 の Lie 型の単純群のうちの一系列）は、上のリストでは小さい群に含めているが、実際の分類では「強く

埋め込まれた部分群をもつ群」としてあらかじめ別に分類される。よく知られているように、 Lie 型の群は再帰的な構造をもつ。その意味で基盤としての rank 1 の群を、どのように取り扱うかはとても重要である。標数 $p$ の Lie 型の群では、 Sylow $p$ 部分群の正規化群が Borel 部分群になる。よって特に rank 1 の群では、「Sylow $p$ 部分群はただ一つの極大部分群（それが Borel 部分群）に含まれる」という性質が成り立つ。例えばこの性質を、抽象的な rank 1 の群の定義として採用してみよう。分類定理の証明では、 Sylow 2 部分群がただ一つの極大部分群に含まれる単純群は別に取り扱われる。さて単純群が標数 $p$ の Lie 型の群に似ているならば、放物型部分群（放物型部分群は $p$ local 部分群である）からなる束の構造を持つはずである。よってある Sylow $p$ 部分群に着目したとき、それを含むいくつかの local 部分群で全体が生成されていることが望まれる。その意味で、 Sylow 部分群がただ一つの極大部分群に含まれる場合は別に考える必要がある。他の多くの場合とあわせてのちに Uniqueness Case と呼ばれる場合の一部になっている。これらは、すでに述べてきた意味での小さい単純群とは違った、例外的な意味での小さい群である。これを念頭に置いて Classification Grid を再点検したうえで、もう少し詳しく表現すると以下のようになっている。

Classification Grid (revisited)

| | Odd | Even |
|---|---|---|
| | Uniqueness Case | |
| Small | Small 2 rank Problems | Quasithin Problems |
| Large | Standard Component Problems | Odd Standard Component Problems |

このように、小さい群というと、位数から受ける印象により一見何となくくみしやすそうにみえるものの、実はいろいろと厄介な現象を引き起こすのである。これが有限単純群の分類を複雑怪奇なものと感じさせている主要な原因の一つである。

# References


[1] Aschbacher, M.: On finite groups of component type, Illinois J. Math. **19** 87–115 (1975).

[2] Aschbacher, M.: A characterization of Chevalley groups over fields of odd order I, II, Ann. of Math. (2) **106** 353–468 (1977), **111** 411–414 (1980).

[3] Aschbacher, M.: Thin finite simple groups, J. Algebra **54** 50–152 (1978).

[4] Aschbacher, M.: Finite groups of rank 3 I, II, Invent. Math. **63** 357–402 (1981), **71** 51–163 (1983).

[5] Alperin, J. L., Brauer, R., and Gorenstein, D.: Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, Trans. Amer. Math. Soc. **151** 1–261 (1970).

[6] Alperin, J. L., Brauer, R., and Gorenstein, D.: Finite simple groups of 2-rank two, Scripta Math. **29** 191–214 (1973).

[7] Aschbacher, M. and Smith, S. D.: *The classification of quasithin groups I, II*, Mathematical Surveys and Monographs 111, 112, Amer. Math. Soc., 2004.

[8] Bender, H.: On groups with abelian Sylow 2-subgroups, Math. Zeit. **117** 164–176 (1970).

[9] Bender, H.: Finite groups with dihedral Sylow 2-subgroups, J. Algebra **70** 216–228 (1981).

[10] Brauer, R. and Fowler, K. A.: On groups of even order, Ann. Math. (2) **62** 565–583 (1955).

[11] Bender, H. and Glauberman, G.: *Local analysis for the Odd Order Theorem*, Lecture Note Series 188, London Math. Soc., 1994.

[12] Brauer, R.: On finite Desarguesian planes, I, II, Math. Zeit. **90** 117–123 (1965), **91** 124–151 (1966).

[13] Brauer, R. and Suzuki, M.: On finite groups of even order whose 2-Sylow subgroup is a quaternion group, Proc. Nat. Acad. Sci. U.S.A. **45** 1757–1759 (1959).

[14] Burnside, W.: *Theory of groups of finite order*, Cambridge University Press 1897; second edition, 1911.

[15] Carter, R. W.: *Simple groups of Lie type*, Wiley-Interscience, New York, 1972.

[16] Feit, W. and Thompson, J. G.: Solvability of groups of odd order, Pacific J. Math. 13 775–1029 (1963).

[17] Gorenstein, D. and Lyons, R.: *The local structure of finite groups of characteristic* 2 *type*, Mem. Amer. Math. Soc. vol. 42 no. 276, 1983.

[18] Gorenstein, D. and Walter, J. H.: The characterization of finite groups with dihedral Sylow 2-subgroups, J. Algebra **2** 85–151, 218–270, 354–393 (1965).

[19] Higman, D. G.: Focal series in finite groups, Canad. J. Math. **5** 477–497 (1953).

[20] Janko, Z.: A new finite simple group with abelian Sylow 2-subgroups and its characterization, J. Algebra **3** 147–186 (1966).

[21] Lyons, R.: A characterization of $U_3(4)$, Trans. Amer. Math. Soc. **164** 371–387 (1972).

[22] Mason, G.: On the classification of quasithin groups, preprint.

[23] Thompson, J. G.: Finite groups with fixed-point-free automorphisms of prime order, Nat. Acad. Sci. U.S.A. **45** 578–581 (1959).

[24] Thompson, J. G.: Normal $p$-complements for finite groups, Math. Zeit. **72** 332–354 (1960).

[25] Thompson, J. G.: Nonsolvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. **74** 383–437 (1968); Pacific J. Math. **33** 451–536 (1970), **39** 483–534 (1971), **48** 511–592 (1973), **50** 215–297 (1974), **51** 573–630 (1974).

[26] Walter, J. H.: The characterization of finite groups with abelian Sylow 2-subgroups, Ann. of Math. (2) **89** 405–514 (1969).

# ガロワの逆問題と剛性の方法について

京都大学数理解析研究所　佐久川憲児

## 1　導入

本原稿は第２７回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」における同名講演[*1]の報告です.

## 2　研究の出発点とこのお話の目標

$k$ を体とし, その分離閉包 $\bar{k}$ を一つ固定する. また $k$ の絶対ガロワ群 $\mathrm{Gal}(\bar{k}/k)$ を $G_k$ で表すことにする. 本サマースクールで我々が考えている問題は次のものであった:

**問題 2.1** ($k$ に対するガロワの逆問題 (IGP($k$)))**.** 任意の有限群 $G$ は位相群 $G_k$ の商として現れるか? 言い換えれば, 任意の有限群 $G$ に対し, $\mathrm{Gal}(k'/k) \cong G$ を満たす $k$ の有限次ガロワ拡大 $k'$ は存在するか?

任意の有限群が $G_k$ の商として現れるときに, IGP($k$) は肯定的に解決できる, ということにしよう. この問題は任意の体に対し考察できるが, 勿論一般的には肯定的に解決できるとは限らない.

**例 2.2.** IGP($k$) が肯定的に解決できない例を見よう.

(1) $\bar{k} = k$ の時 $G_k = \{1\}$ なので, 自明群以外の有限群は $G_k$ の商として現れない.

(2) $k$ を有限体とすると, $G_k \cong \widehat{\mathbf{Z}}$ である, 従って, 仮に有限群 $G$ に対して連続全射 $G_k \twoheadrightarrow G$ が存在すれば, 自動的に $G$ は巡回群となる. 従って IGP($k$) は肯定的に解決されない. $G$ がアーベル群であったとしても, 巡回的でない場合にはこのような全射は決して存在しないことに注意しておこう.

(3) $p$ を素数とし, $k$ が $p$ 進体の場合を考える. このときよく知られているように任意の $k$ の有限次ガロワ拡大は可解拡大となる ([3]). 従って IGP($k$) は肯定的には解決できない. それでは問題に現れる群 $G$ を可解群に制限してはどうだろう? 実はこれでも問題は肯定的に解決できない. 実際局所類体論によれば

$$G_k^{\mathrm{ab}} \cong \widehat{\mathbf{Z}} \times \mathcal{O}_k^{\times}$$

となっており, 従って $G_k^{\mathrm{ab}}$ は位相的に有限生成である. 従って $G$ がアーベル群であったとしても, その生成元の数が $G_k^{\mathrm{ab}}$ の位相的生成元の数より多い時には決して全射 $G_k \twoheadrightarrow G$ は存在しない.

このような例を色々考えてみると, IGP($k$) が肯定的に解けるような体 $k$ というのは中々特別な体であるように思える. 少なくとも $G_k$ が有限生成であってはいけない (例 2.2 (2), (3)). 根拠があるか筆者は知らないが[*2], 次が予想されている:

---

[*1] ここだけワ=アと定義します.

[*2] 興味深いことに $k$ が有限体上の関数体の最大アーベル拡大のときに IGP は肯定的に解決されている.

**予想 2.3.** $k$ が $\mathbf{Q}$ 又は $\mathbf{Q}^{\mathrm{ab}}$ の有限次拡大であるならば, IGP($k$) は肯定的に解決できるだろう.

我々（私）が最も興味を持っている問題は $k = \mathbf{Q}$ の場合であるので, 以下この場合を中心に考えるという意味で IGP($\mathbf{Q}$) を単に IGP と書くことにしよう.

少しだけ確認できる分を見てみる. $k = \mathbf{Q}$ の時, Kronecker-Weber の定理により,

$$G_{\mathbf{Q}}^{\mathrm{ab}} \cong \widehat{\mathbf{Z}}^{\times} \cong \prod_{p:\text{素数}} \mathbf{Z}_p^{\times}$$

が成立する. 従って, 有限生成アーベル群の基本定理と算術級数定理により, 任意のアーベル群は $G_{\mathbf{Q}}$ の商として現れることが分かる.

上の証明は, $G_{\mathbf{Q}}^{\mathrm{ab}}$ の構造と有限生成アーベル群の構造**双方がよくわかっている**という事情に依っている. このような証明は明解で素晴らしいが, 現状 $G_{\mathbf{Q}}$ の構造も有限群の構造もどちらもよくわからないので, そのまま一般化することはどうも難しそうである.

ではどうするか? 一つのアイデアは, $G_k$ が良く分かっているような $k$ から話を始めるというものである. 我々は次の二つの定理を研究の出発点としよう:

**定理 2.4** (Hilbert の既約性定理の帰結)**.** $\mathbf{Q}(t)$ を $\mathbf{Q}$ 上の一変数代数関数体とする. もし IGP($\mathbf{Q}(t)$) が肯定的に解決できるならば, IGP もまた肯定的に解決できる.

**定理 2.5.** $G_{\overline{\mathbf{Q}}(t)}$ は可算濃度の元で位相的に生成される自由副有限群である. 特に, IGP($\overline{\mathbf{Q}}(t)$) は肯定的に解決される.

ヒルベルトの既約性定理は既に幾度か現れているので, ここでは認めることにする. 二つ目の定理は次の章に於いて証明の概略をあたえることとし, この章では先に我々の基本的な戦略とこの講演のゴールを設定することを急ぐことにしよう.

$\overline{\mathbf{Q}}(t)$ は $\mathbf{Q}(t)$ のガロワ拡大で, そのガロワ群は自明に $G_{\mathbf{Q}}$ と同型であるから, 次の完全列が存在することに注意しておこう:

$$1 \to G_{\overline{\mathbf{Q}}(t)} \to G_{\mathbf{Q}(t)} \to G_{\mathbf{Q}} \to 1. \tag{1}$$

我々のこの講演でみる IGP へのアプローチは, 次の問題を考えることである:

**問題 2.6.** $G$ を有限群とし, 連続全射準同型 $f\colon G_{\overline{\mathbf{Q}}(t)} \twoheadrightarrow G$ を一つとる (存在は定理 2.5 による). この $f$ がいつ $G_{\mathbf{Q}(t)}$ に伸びるかを問題とせよ. 即ち, $G_{\overline{\mathbf{Q}}(t)}$ に制限したとき $f$ と一致するような群準同型 $\tilde{f}\colon G_{\mathbf{Q}(t)} \twoheadrightarrow G$ がいつ存在するかを調べよ.

この講演の目標は**雑に言えば**以下の通りである:

**目標 2.7.** 有限群 $G$ を一つ固定する.

(1) 適当な連続全射準同型 $f\colon G_{\overline{\mathbf{Q}}(t)} \twoheadrightarrow G$ を一つとる. このとき, $f$ が $G_{\mathbf{Q}(t)}$ に「伸びる」[*3]ための, **純群論的な充分条件**を与える.

(2) (1) で与えた純群論的な判定法を用いて, $G_{\mathbf{Q}}$ の商として現れる有限群のかなり非自明な例を幾つかみる.

[*3] 実際には $G$ をその中心で割ったところで考えることが多い.

(1) を遂行するためにはそもそも $f$ を群論的に表しておく必要があるが, それは次の章で実行される. また, 純群論的の意味であるが, より具体的には「$G$ に対し・・・を満たす共役類が存在すれば $G$ は $G_{\mathbf{Q}}$ の商として現れる」というタイプの定理を証明することをさすことにする.

# 3 $G_{\overline{\mathbf{Q}}(t)}$ の構造定理

この章では定理 2.5 の証明を行う. 証明は幾何の助けを必要とする.

## 3.1 $\mathbf{C}(t)$ の場合

まずは代数的な分岐・不分岐の定義を確認しておこう.

**定義 3.1.** $K$ を $\mathbf{C}(t)$ の有限次拡大体とする. このとき, $K$ が $x \in \mathbf{C}$ **で不分岐**であるとは, 同型

$$K \otimes_{\mathbf{C}(t)} \mathbf{C}((t-x)) \cong \mathbf{C}((t-x))^{[K:\mathbf{C}(t)]}$$

が成立するときに言う. また, $\infty$ **で不分岐**であるとは,

$$K \otimes_{\mathbf{C}(t)} \mathbf{C}((1/t)) \cong \mathbf{C}((1/t))^{[K:\mathbf{C}(t)]}$$

が成立するときに言う. そうでないときに, $K/\mathbf{C}(t)$ は $x$ で**分岐**する, という. $\Sigma := \{a_1, \ldots, a_n\} \subset \mathbf{C} \cup \{\infty\}$ に対し, $\mathbf{C}(t)_\Sigma$ で $\mathbf{C}(t)$ の $\Sigma$ 外最大不分岐拡大を表すことにする. 即ち, 任意の $\mathbf{C}(t)_\Sigma/\mathbf{C}(t)$ の有限次部分拡大 $K/\mathbf{C}(t)$ は $\Sigma$ 以外の点では不分岐であり, $\mathbf{C}(t)_\Sigma$ はこのような性質を持つ拡大の中で最大のものとする.

$\mathbf{C}(t)_\Sigma$ が $\mathbf{C}(t)$ のガロワ拡大となることは容易に示せる.

**補題 3.2.** 任意の有限次拡大 $K/\mathbf{C}(t)$ は $\mathbf{C} \cup \{\infty\}$ の有限集合を除いて不分岐である. 特に

$$\bigcup_{\Sigma \subset \mathbf{C} \cup \{\infty\}:\text{有限集合}} \mathbf{C}(t)_\Sigma$$

は $\mathbf{C}(t)$ の代数閉包である.

*Proof.* $K$ はある $\mathbf{C}(t)$ 係数多項式 $F(u) = u^n + A_{n-1}u^{n-1} + \cdots + A_0$ の最小分解体としてよい. この方程式の根 $\alpha_1, \ldots, \alpha_n$ 達の判別式

$$\Delta := \prod_{i \neq j} (\alpha_i - \alpha_j)$$

を考えると, 明らかに $\Delta \in \mathbf{C}(t)^\times$ であり, 各 $A_i$ に代入可能な点 $x \in \mathbf{P}^1(\mathbf{C})$ を $\Delta$ に代入して得られる値 $\Delta(x) \in \mathbf{C}$ が 0 でない時に方程式

$$0 = F|_{t=x}(u) := u^n + A_{n-1}(t)u^{n-1} + \cdots + A_0(x)$$

は相異なる $n$ 個の根をもつ. Hensel の補題により, $F$ は $\mathbf{C}[\![t-x]\!][u]$ で互いに素な一次式の積に分解されるので, そのようなことにならない $x$ の有限性と合わせて主張は示された. □

この小節の目標は次の定理の証明の概略を与えることである:

**定理 3.3.** $\Sigma = \{x_1, \ldots, x_r\}$ を $\mathbf{C} \cup \{\infty\}$ の有限集合とし, その任意の元 $x$ に対し $t_x$ を $t - x$ または $1/t$ と取ることにしよう. $\mathbf{C}(t)$ 上の埋め込み

$$\mathbf{C}(t)_\Sigma \hookrightarrow \overline{\mathbf{C}(\!(t_x)\!)} = \mathbf{C}\{\{t_x\}\} := \cup_{n \geq 1} \mathbf{C}(\!(t_x^{1/n})\!) \tag{2}$$

を一つ固定し, 対応するガロワ群の埋め込み

$$\widehat{\mathbf{Z}} \cong \mathrm{Gal}(\mathbf{C}\{\{t_{x_i}\}\}/\mathbf{C}(\!(t_{x_i})\!)) \hookrightarrow \mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t))$$

による 1 の像を $\sigma_i$ と書くことにする[*4]. このとき, $\mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t))$ は $\{\sigma_x\}_{x \in \Sigma}$ で生成され, さらに埋め込みと $\Sigma$ の順序ををうまくとればその関係式は

$$\sigma_1 \cdots \sigma_r = 1$$

のみであるようにとれる. 特に $\mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t))$ は自由副有限群であってその階数は $|\Sigma| - 1$ となる.

**系 3.4.** $G_{\mathbf{C}(t)}$ は非可算階数の副自由群である. 特に, $\mathrm{IGP}(\mathbf{C}(t))$ は肯定的に解決される.

*Proof.* 最初の主張から二つ目が導かれるのは自明であろう. 最初の主張は, 同型

$$G_{\mathbf{C}(t)} \xrightarrow{\sim} \varprojlim_{\Sigma} \mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t))$$

から従う. □

証明に於いて重要であるのは, 次の事実である:

**事実 3.5** (リーマンの存在定理)**.** 任意のコンパクトリーマン面上には定数でない有理型関数が存在する. 別の言い方をすれば, 任意のコンパクトリーマン面 $X$ に対し, リーマン面の全射

$$X \to \mathbf{P}^1(\mathbf{C})$$

が存在する.

一般に, 一変数関数体 $\mathbf{C}(t)$ 上の有限次拡大体のことを $\mathbf{C}$ 上の**一変数代数関数体**とよぶ. 誤解を招く恐れは恐らくないので, しばらくは単に一変数代数関数体と呼ぶことにしよう. 上の事実から次が直ちに従う:

**定理 3.6.** 連結コンパクトリーマン面 $X$ に対し, $\mathbf{C}(X)$ で $X$ 上の有理型関数のなす体を表すことにする. このとき, $\mathbf{C}(X)$ は一変数代数関数体である. 更に対応 $X \mapsto \mathbf{C}(X)$ は連結コンパクトリーマン面の圏と一変数代数関数体の圏の間の同値を引き起こす. 但し, 連結コンパクトリーマン面の射は定数でない正則写像のみを考えることとする.

*Proof.* ここでは, この函手が実際定義されていることの証明と擬逆函手の構成のアイデアについてのみ述べる[*5]. $X$ を連結コンパクトリーマン面とし, $t\colon X \to \mathbf{P}^1(\mathbf{C})$ を定数でない有理型関数とする. $t$ は $\mathbf{C}(X)$ の元とみなせることに注意しよう. 逆関数定理から, 有理型関数 $t$ が局所同相

[*4] 実際には $\pm 1$ の曖昧さがあるが, あまり細かいことは気にしないでおこう.

[*5] 残りの部分は演習とする.

でない点は離散的であり, 更に $X$ がコンパクトであることから有限個であることがわかる. 従って $t$ はほとんどすべての点で局所同相であるわけであるが, $t$ での逆像の位数は $\mathbf{P}^1(\mathbf{C})$ 上殆ど定数であり, 再び $X$ のコンパクト性より有限であることがわかる. それを $n \in \mathbf{Z}_{\geq 1}$ とかくことにしよう. さて $X$ 上の定数でない有理型関数 $f$ をとる. $P \in \mathbf{P}^1(\mathbf{C})$ の $t$ での逆像を $Q_1, \ldots, Q_n$ と書き (重複度も込めて数える), $S_i$ を $T_1, \ldots, T_n$ の $i$ 次基本対象式としたとき, 対応

$$A_i \colon \mathbf{P}^1(\mathbf{C}) \ni P \mapsto S_i(f(Q_1), \ldots, f(Q_r)) \in \mathbf{P}^1(\mathbf{C})$$

は well-defined であり $\mathbf{P}^1(\mathbf{C})$ 上の有理型関数を定めることがわかる. 明らかに

$$\sum_{i=0}^{n} A_i(t) f^{n-i} = 0$$

が成立するので, $\mathbf{C}(t)(f)/\mathbf{C}(t)$ は拡大次数が $n$ 以下である. $f \in \mathbf{C}(X)$ は任意だったので, $\mathbf{C}(X)/\mathbf{C}(t)$ の拡大次数も $n$ 以下であることがわかる. 従って $\mathbf{C}(X)$ は代数関数体で函手が well-defined であることが示された.

代数関数体 $K/\mathbf{C}(t)$ が与えられているとしよう. $F \in \mathbf{C}[t, u]$ をこの体のモニックとは限らない定義方程式とするとき, $F$ の定める $\mathbf{P}^2(\mathbf{C})$ の解析空間を $X'$ とおくことにする. 定義から $X' \to \mathbf{P}^1(\mathbf{C})$ が存在し, $X'$ は一次元である. $X$ は $X'$ の特異点を解消して得られるリーマン面 $X \to X'$ とすると, $K \mapsto X$ が擬逆函手の対象の間の対応を定義する. 射の対応まで自然に伸びることは読者の演習としたい. □

**注意 3.7.** 証明から, 任意の連結コンパクトリーマン面は $\mathbf{C}$ 上の非特異射影的代数曲線の $\mathbf{C}$ 値点とみなせることがわかる. より詳しく言えば, 連結コンパクトリーマン面の圏と $\mathbf{C}$ 上の非特異射影的代数曲線の圏は同値であることがわかる.

さて, $t \colon X \to \mathbf{P}^1(\mathbf{C})$ を全射な連結コンパクトリーマン面の射とし, $f^\sharp \colon \mathbf{C}(t) \to \mathbf{C}(X)$ を対応する代数関数体の射としよう. $t$ が $x \in \mathbf{P}^1(\mathbf{C})$ で**不分岐点**であるとは, 集合 $f^{-1}(x)$ の位数が体の拡大次数 $[\mathbf{C}(X); \mathbf{C}(t)]$ と等しくなるときに言う. 不分岐でない点のことを, **分岐点という**. $x$ が不分岐な点であるならば, 任意の $t^{-1}(x)$ の点 $y$ に対し, $t$ は $y$ の十分小さな近傍で局所同相であることに注意しよう. これについては「逆」も成立し, 即ち $x$ に対し任意の $y \in t^{-1}(x)$ の近傍で $t$ が局所同相であれば, $x$ は不分岐点である. この概念が圏同値を通して既に定めた代数関数体における分岐・不分岐という概念と定理 3.6 における圏同値を介することにより同一視できることを見よう.

**補題 3.8.** コンパクトリーマン面の射 $t$ が $x \in \mathbf{P}^1(\mathbf{C})$ で不分岐であることと, 体の拡大 $\mathbf{C}(X)/\mathbf{C}(t)$ が $x$ で不分岐であることは同値である.

*Proof.* 以前と同じ記号を使おう. $x$ がコンパクトリーマン面サイドにおける不分岐点であるならば, Hensel の補題により $\mathbf{C}(X)/\mathbf{C}(t)$ の定義方程式は $\mathbf{C}[\![t_x]\!][u]$ に於いて一次式の積に分解し, 従って代数関数体側における不分岐点であることがわかる. 逆に $x$ がコンパクトリーマン面サイドにおける分岐点であるとき, 局所的には $t$ は $z \mapsto z^n$, $n \geq 2$ と同型となる. 従って $\mathbf{C}(X) \otimes_{\mathbf{C}(t)} \mathbf{C}(\!(t_x)\!)$ には $t_x^{1/n}$, $n \geq 2$ が含まれており, 従って代数側でもこれは分岐していることがわかる. 以上で証明が終了した. □

$\mathbf{P}^1(\mathbf{C})$ の有限集合 $\Sigma$ に対し, $\mathrm{FinCov}_S^{\mathrm{RS}}(\mathbf{P}^1(\mathbf{C}))$ で $\mathbf{P}^1(\mathbf{C})$ 上のコンパクトリーマン面 $X \to \mathbf{P}^1(\mathbf{C})$ であり $\Sigma$ の外不分岐であるもののなす圏を表し[*6], $\mathrm{FinExt}_\Sigma(\mathbf{C}(t))$ の有限次拡大であって $\Sigma$ の外不分岐であるものなす圏[*7]を表すことにすると, 上の補題から以下が直ちに導かれる:

**系 3.9.** 対応 $[X \mapsto \mathbf{C}(X)]$ は圏同値

$$\mathrm{FinCov}_\Sigma^{\mathrm{RS}}(\mathbf{P}^1(\mathbf{C})) \xrightarrow{\sim} \mathrm{FinExt}_\Sigma(\mathbf{C}(t))$$

を誘導する

さて, 一般の連結位相空間 $T$ に対し $T$ の被覆とは局所同相な連結位相空間の射 $f\colon S \to T$ のこととし, $\mathrm{Cov}(T)$ で $T$ の被覆のなす圏のことをあらわすことにする. 被覆 $f$ に対し $f^{-1}(x)$ の位数のことを $f$ **の次数**と呼ぶことにする. $\mathrm{FinCov}(T)$ で $\mathrm{Cov}(T)$ の次数有限な被覆のなす忠実充満部分圏をあらわすことにしよう.

**補題 3.10.** 次の自然な圏同値が存在する:

$$\mathrm{FinCov}_\Sigma^{\mathrm{RS}}(\mathbf{P}^1(\mathbf{C})) \xrightarrow{\sim} \mathrm{FinCov}(\mathbf{P}^1(\mathbf{C}) \setminus \Sigma)$$
$$[f\colon X \to \mathbf{P}^1(\mathbf{C})] \mapsto [f^{-1}(\mathbf{P}^1(\mathbf{C}) \setminus \Sigma) \to \mathbf{P}^1(\mathbf{C}) \setminus \Sigma].$$

*Proof.* 忠実充満函手であることはほぼ明らかであろうから, 本質的に全射であることを示す. $t\colon T \to \mathbf{P}^1(\mathbf{C}) \setminus \Sigma$ を位相的な有限次被覆とし, $T$ にはこの被覆を用いてリーマン面の構造を導入しておく. $D^\times$ で穴あき開円盤 $\{z \in \mathbf{C}^\times \mid |z| < 1\}$ を表すことにしよう. すると, $x \in \Sigma$ の十分小さな開近傍 $U$ をとると, $T|_U \to U$ は

$$D^\times \to D^\times; \quad z \mapsto z^i$$

と同相な被覆の有限直和となっている[*8]. そこで, $T|_U$ のコンパクト化を $D^\times$ の穴を埋めて, そこに自然に複素構造を入れることによって定義する. この操作を全ての $\Sigma$ の元に対して行えば, 自然にこれらは張り合いコンパクトリーマン面 $T^*$ が $T$ に有限個の点を付け加えることにより構成された. この対応 $T \mapsto T^*$ が擬逆函手を定める. □

一般の位相空間 $T$ に対し,

$$\widetilde{T} \to T$$

で $T$ の普遍被覆を表すことにし, $\pi_1(T, \widetilde{T})$ で $\widetilde{T}$ の $T$ 上の同型のなす群を表すことにする[*9]. 定義から $\pi_1(T, \widetilde{T})$ は $\widetilde{T}$ に $T$ 上作用している. そこで $T$ の有限次被覆の pro-system $\widehat{T} \to T$ を

$$\widehat{T} := \{\widetilde{T}/N \mid N : \pi_1(T, \widetilde{T}) \text{ 有限位数正規部分群 }\} \to T$$

[*6] 射は $\mathbf{P}^1(\mathbf{C})$ 上の射を採用する. また, RS は Rieman surface の略.
[*7] 射は $\mathbf{C}(t)$ 上の環準同型を採用する.
[*8] このことは $\pi_1(D^\times) \cong \mathbf{Z}$ からわかる.
[*9] $\widetilde{T} \to T$ を基点とした基本群である. 本当は普遍被覆からの射も情報として持たなければならないが, ここでは省略する.

で定めることにし, $\widehat{\pi}_1(T,\widetilde{T})$ で $\widehat{T}$ の $T$ 上の同型のなす群を表すことにする. ここで $\widetilde{T}/N$ は $\widetilde{T}$ を $N$ の作用で割った集合に $\widetilde{T}\to\widetilde{T}/N$ が局所同相となるような位相を入れた位相空間のこととしよう. 定義から

$$\widehat{\pi}_1(T,\widetilde{T}) := \mathrm{Aut}_T(\widehat{T}) := \varprojlim_N \mathrm{Aut}_T(\widetilde{T}/N) \cong \varprojlim_N \pi_1(T,\widetilde{T})/N$$

であるので, $\widehat{\pi}_1(T,\widetilde{T})$ は $\pi_1(T,\widetilde{T})$ の副有限完備化に自然に同型である.

**補題 3.11.** $T := \mathbf{P}^1(\mathbf{C})\setminus\Sigma$ としたとき, 次の自然な同型が存在する:

$$\mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t)) \cong \widehat{\pi}_1\left(T,\widetilde{T}\right).$$

*Proof.* まず, 自然な同型

$$\mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t)) \xrightarrow{\sim} \varprojlim_{K:\Sigma\text{の外不分岐な }\mathbf{C}(t)\text{ の有限次ガロワ拡大}} \mathrm{Gal}(K/\mathbf{C}(t)) \tag{3}$$

があることに注意しておこう. また, 系 3.9 から自然な同型

$$\varprojlim_{X\in\mathrm{FinCov}_\Sigma^{\mathrm{RS}}(\mathbf{P}^1(\mathbf{C}))} \mathrm{Aut}(X/\mathbf{P}^1(\mathbf{C})) \xrightarrow{\sim} \varprojlim_{K:\Sigma\text{の外不分岐な }\mathbf{C}(t)\text{ の有限次ガロワ拡大}} \mathrm{Gal}(K/\mathbf{C}(t)) \tag{4}$$

が存在することが容易にわかる. ここで左辺の Aut はコンパクトリーマン面としての自己同型全体をさす. さらに補題 3.10 から同型

$$\varprojlim_{X\in\mathrm{FinCov}_\Sigma^{\mathrm{RS}}(\mathbf{P}^1(\mathbf{C}))} \mathrm{Aut}(X/\mathbf{P}^1(\mathbf{C})) \xrightarrow{\sim} \varprojlim_{Y\in\mathrm{FinCov}(\mathbf{P}^1(\mathbf{C})\setminus\Sigma)} \mathrm{Aut}\left(Y/(\mathbf{P}^1(\mathbf{C})\setminus\Sigma)\right) \tag{5}$$

が従う. ここで右辺の Aut は位相空間としての自己同型全体をさす. 式 (5) の右辺は定義から $\widehat{\pi}_1\left(\mathbf{P}^1(\mathbf{C})\setminus\Sigma, \widetilde{(\mathbf{P}^1(\mathbf{C})\setminus\Sigma)}\right)$ と同型であるので, (3), (4) と合わせて主張が示せた. □

定理 3.3 の証明. 補題 3.10 から, $\pi_1\left(\mathbf{P}^1(\mathbf{C})\setminus\Sigma, \widetilde{(\mathbf{P}^1(\mathbf{C})\setminus\Sigma)}\right)$ が表示

$$\pi_1\left(\mathbf{P}^1(\mathbf{C})\setminus\Sigma, \widetilde{(\mathbf{P}^1(\mathbf{C})\setminus\Sigma)}\right) = \left\langle \sigma_x,\ x\in\Sigma \,\middle|\, \prod_{x\in\Sigma}\sigma_x = 1 \right\rangle$$

を持つことを示せばよい. ここで, $b\in\mathbf{P}^1(\mathbf{C})\setminus\Sigma$ と $b$ の普遍被覆への持ち上げ $\tilde{b}$ を取ると, 群の同型

$$\pi_1\left(\mathbf{P}^1(\mathbf{C})\setminus\Sigma, \widetilde{(\mathbf{P}^1(\mathbf{C})\setminus\Sigma)}\right) \xleftarrow{\sim} \pi_1\left(\mathbf{P}^1(\mathbf{C})\setminus\Sigma, b\right)$$

が $b$ でのファイバーを取る操作から誘導される. ここで右辺の群は通常の $b$ に基点を持つ基本群である. そこで, $b$ を始点に持つ道 $\sigma_x$ を $b$ から $x$ のごく近傍までの直線と $x$ の周りを半時計周りに一周する道との合成から定まる元としよう. すると, $\sigma_x$ たちは基本群を生成し, さらに適切に $x$ 達の順序を取れば $\sigma_x$ の積は 1 となり, それしか関係式は無いことが知られている (読者への演習問題とする. Van Kampen の定理を用いるとよい). 以上で証明は完了した. □

最後に一つ問題を挙げておこう. 筆者の知る限り, これは未解決問題なはずである[*10].

**問題 3.12.** 定理 3.3 の, ある種の幾何を用いないような純代数的証明は存在するか[*11]?

[*10] 興味深さは保証しない.

[*11] pro-$p$ 版ならば証明は易しい. $\mathbf{C}(t)$ の Brauer 群の計算に帰着される.

## 3.2 $\mathbf{C}$ から $\overline{\mathbf{Q}}$ へ

以下 $\overline{\mathbf{Q}}$ の $\mathbf{C}$ への埋め込みを一つ固定しておく:

$$\sigma_0 \colon \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}.$$

$K$ を $\overline{\mathbf{Q}}(t)$ の有限次拡大としたとき, この拡大が $x \in \mathbf{P}^1(\overline{\mathbf{Q}})$ で分岐/不分岐であるとは, 体の拡大 $K \otimes_{\overline{\mathbf{Q}}} \mathbf{C}/\mathbf{C}(t)$ が $x$ で分岐/不分岐であるときに言うことにしよう. これは埋め込み $\sigma_0$ の取り方によらない概念である (証明は読者の演習問題とする). この小節では次の定理の証明の概略を与え, 定理 2.5 の証明を完結させる:

**定理 3.13.** $\Sigma$ を $\mathbf{P}^1(\overline{\mathbf{Q}})$ の有限部分集合とする. このとき, 固定した埋め込みによる制限は同型

$$\mathrm{Gal}(\mathbf{C}(t)_\Sigma/\mathbf{C}(t)) \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t))$$

を誘導する.

証明の概略. 明らかに $\overline{\mathbf{Q}}(t)_\Sigma \otimes_{\overline{\mathbf{Q}}} \mathbf{C} \subset \mathbf{C}(t)_\Sigma$ が成立しており, また $\overline{\mathbf{Q}}(t)$ は $\mathbf{C}(t)$ の中で代数的に閉じているので, 全射は直ちにわかる. 単射性を示すには, 次の主張を示せばよい:

**主張 3.14.** $K/\mathbf{C}(t)$ を有限次拡大体で $\Sigma$ の外不分岐であるとする. このとき, ある $\Sigma$ の外不分岐な有限次拡大 $L/\overline{\mathbf{Q}}(t)$ と $\mathbf{C}(t)$ 上の単射準同型

$$K \hookrightarrow L \otimes_{\overline{\mathbf{Q}}} \mathbf{C}$$

が存在する.

主張から単射性が導かれるのはほぼ明らかであると思われるので, 以下この主張の証明の概略を与えることにしよう.

$K/\mathbf{C}(t)$ を主張と同様とし, $f \colon X \to \mathbf{P}^1_{\mathbf{C}}$ を対応する非特異射影的代数曲線の射とする. ここで, $X$ や $f$ を定義する方程式は代数的で係数は有限個しか現れないことから, $\mathbf{C}$ の部分代数 $R$ で $\overline{\mathbf{Q}}$ 上有限生成であるものと $f$ のモデルである $\overline{\mathbf{Q}}$ 上のスキームの射

$$\tilde{f} \colon \mathcal{X} \to \mathbf{P}^1_{\overline{\mathbf{Q}}} \times_{\mathrm{Spec}(\overline{\mathbf{Q}})} \mathrm{Spec}(R)$$

が存在する. $\mathrm{Spec}(R)$ をその開部分集合に取り換えることにより, $\tilde{f}$ は有限で $\Sigma$ の外でエタール[*12]であるようにとれることに注意しておこう. そこで, 次の事実を用いる:

**事実 3.15** (cf. [9, Corollaire 1.7])**.** $(\mathbf{P}^1_{\overline{\mathbf{Q}}} \setminus \Sigma) \times_{\mathrm{Spec}(\overline{\mathbf{Q}})} \mathrm{Spec}(R)$ 上のエタール被覆は,

$$\mathcal{Y} \times \mathcal{Z} \to (\mathbf{P}^1_{\overline{\mathbf{Q}}} \setminus \Sigma) \times_{\mathrm{Spec}(\overline{\mathbf{Q}})} \mathrm{Spec}(R)$$

の形の被覆の商である. ここで $\mathcal{Y} \to (\mathbf{P}^1_{\overline{\mathbf{Q}}} \setminus \Sigma)$ と $\mathcal{Z} \to \mathrm{Spec}(R)$ はともにエタール被覆. [*13]

[*12] 局所同相のスキーム論的類似物. 定義は「局所有限表示で平坦且つ不分岐な射」.

[*13] 証明は若干複雑である. 方針としては Abyanker の補題を用いて片方を固有スキームのケースに帰着させる.

この事実から, あるエタール被覆

$$\mathcal{Y} \times_{\mathrm{Spec}(\overline{\mathbf{Q}})} \mathcal{Z} \to \mathcal{X}$$

が存在することが直ちに従う. $\mathcal{O}(\mathcal{Z})$ の商体は $R$ の商体の有限次拡大体であり従って $\mathbf{C}$ の部分体と取れるので, $L$ として $\mathcal{Y}$ の関数体 $\overline{\mathbf{Q}}(\mathcal{Y})$ を取ればよい. これで主張は示された. □

定理 2.5 の証明. まず明らかに

$$G_{\overline{\mathbf{Q}}(t)} \xrightarrow{\sim} \varprojlim_{\Sigma \subset \mathbf{P}^1(\overline{\mathbf{Q}})} \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma / \overline{\mathbf{Q}}(t))$$

が成立している. 従って定理 2.5 は定理 3.13 と定理 3.3 の直接の帰結である. □

# 4 剛性の方法

以下しばらく有限群 $G$ を一つ固定しよう. この章では本講演の主定理について述べる.

## 4.1 集合 $\mathcal{E}_r^{\mathrm{in}}(G)$, $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$

まず大事な集合 $\mathcal{E}_r^{\mathrm{in}}(G)$ を定義しよう. $\mathrm{Int}(G)$ で $G$ の内部自己同型群 (inner automorphism group) を表すことにする. また, $\mathrm{int}\colon G \to \mathrm{Int}(G)$ は自然な群準同型とする.

**定義 4.1.** $r$ を正の整数とする. このとき集合 $\mathcal{E}_r(G)$ を

$$\mathcal{E}_r(G) := \{(g_1, \ldots, g_r) \in G^r \mid g_1 \cdots g_r = 1,\ \langle g_1, \ldots, g_r \rangle = G\}$$

で定義する. $\mathrm{Int}(G)$ の $\mathcal{E}_r(G)$ への作用を

$$\mathrm{int}(g)(g_1, \ldots, g_r) := (\mathrm{int}(g)(g_1), \ldots, \mathrm{int}(g)(g_r))$$

で定義する. このとき, 集合 $\mathcal{E}_r^{\mathrm{in}}(G)$ を

$$\mathcal{E}_r^{\mathrm{in}}(G) := \mathrm{Int}(G) \backslash \mathcal{E}_r(G)$$

で定義する. $\mathcal{E}_r^{\mathrm{in}}(G)$ の, $(g_1, \ldots, g_r)$ で代表される元を $[g_1, \ldots, g_r]$ で表すことにする.

さて, $\Sigma = \{x_1, \ldots, x_r\}$ を $\mathbf{P}^1(\overline{\mathbf{Q}})$ の位数 $r$ の有限部分集合とする. また $\sigma_i \in \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma / \overline{\mathbf{Q}}(t))$ を $x_i$ を反時計回りに回る道に対応する元とする. このとき, 適当に $x_i$ 達の順序を入れ替えておくことにより, 定理 2.5 の証明で見たように等式

$$\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma / \overline{\mathbf{Q}}(t)) = \langle \sigma_1, \ldots, \sigma_r | \sigma_1 \cdots \sigma_r = 1 \rangle\widehat{\ }$$

が成立する. 位相群 $\pi$ と有限群 $G$ に対し, $\mathrm{Surj}(\pi, G)$ で $\pi$ から $G$ への連続全射準同型のなす集合を表すことし, $G$ の内部自己準同型群 $\mathrm{Int}(G)$ は写像の合成で $\mathrm{Surj}(\pi, G)$ に左から作用していると見做すことにする.

**補題 4.2.** 記号は上と同じものを使うことにする. このとき, 全単射

$$\alpha_\Sigma\colon \mathrm{Int}(G)\backslash\mathrm{Surj}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)), G) \xrightarrow{\sim} \mathcal{E}_r^{\mathrm{in}}(G); \quad [f] \mapsto [f(\sigma_1), \ldots, f(\sigma_r)]$$

が存在する.

*Proof.* これは左辺に現れるガロワ群の具体的表示から明らか. □

さて, ここで次の仮定を考えることにしよう:
**(St)**: $\Sigma$ は $G_{\mathbf{Q}}$ の作用で安定である.
仮に条件 (St) が成り立っているならば, $\overline{\mathbf{Q}}(t)_\Sigma$ は $\mathbf{Q}(t)$ 上のガロワ拡大となる. 従って, 導入で見たように次の短完全列が存在する:

$$1 \to \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)) \to \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\mathbf{Q}(t)) \to G_{\mathbf{Q}} \to 1. \tag{6}$$

これからよく知られた外部作用

$$\rho_\Sigma\colon G_{\mathbf{Q}} \to \mathrm{Out}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t))) \tag{7}$$

が次で定義される[*14]:

$$\rho_\Sigma(\sigma) := \mathrm{int}(\tilde{\sigma}) \mod \mathrm{Int}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t))).$$

但し $\tilde{\sigma}$ は $\sigma$ の任意の持ち上げとする. $\mathrm{Out}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)))$ は自然な方法で有限集合 $\mathrm{Int}(G)\backslash\mathrm{Surj}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)), G)$ に作用することに注意しておこう. よって, $\rho_\Sigma$ を通して $G_{\mathbf{Q}}$ が自然に $\mathrm{Int}(G)\backslash\mathrm{Surj}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)), G)$ に作用していることがわかる. 具体的にはこの作用は

$$\sigma[f] := [\tau \mapsto f(\tilde{\sigma}\tau\tilde{\sigma}^{-1})],\ \sigma \in G_{\mathbf{Q}} \tag{8}$$

と書けている. 補題 4.2 から, $\alpha_\Sigma$ を用いることにより $\mathcal{E}_r^{\mathrm{in}}(G)$ に $G_{\mathbf{Q}}$ の作用が定まることが分かる. この作用を $a_\Sigma$ と書くことにしよう:

$$a_\Sigma\colon G_{\mathbf{Q}} \to \mathrm{Aut}(\mathcal{E}_r^{\mathrm{in}}(G)); \quad \sigma \mapsto [\boldsymbol{g} \mapsto \alpha_\Sigma\sigma\alpha_\Sigma^{-1}(\boldsymbol{g})].$$

**補題 4.3.** $a_\Sigma$ で固定点が存在すれば, 全射

$$\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\mathbf{Q}(t)) \twoheadrightarrow G/Z(G) \cong \mathrm{Int}(G)$$

が存在する. ただし $Z(G)$ は $G$ の中心とする.

*Proof.* まず, 短完全列 (6) は分裂することに注意しておく. 例えば以下のようにする[*15]:
$\overline{\mathbf{Q}}(t)_\Sigma$ をピュイズー級数体

$$\overline{\mathbf{Q}}\{\{t\}\} := \bigcup_{n\geq 1} \overline{\mathbf{Q}}(\!(t^{1/n})\!)$$

の部分体ととる[*16]. $G_{\mathbf{Q}}$ は $\overline{\mathbf{Q}}\{\{t\}\}$ の係数に作用すると思えば, この作用で $\overline{\mathbf{Q}}(t)_\Sigma$ は保たれる. 即ち

$$G_{\mathbf{Q}} \to \mathrm{Aut}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t))$$

[*14] 一般に群 $H$ に対し, $\mathrm{Out}(H) := \mathrm{Aut}(H)/\mathrm{Int}(H)$.
[*15] 局所座標 $t$ の定める接ベクトル基点に対応する分裂である.
[*16] 既に使っている事実であるが, $\overline{\mathbf{Q}}\{\{t\}\}$ は代数閉体となる. 従って自然に $\overline{\mathbf{Q}}(\!(t)\!)$ の代数閉包とみなせる.

が得られる.
そこで分裂

$$\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\mathbf{Q}(t)) \cong \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)) \rtimes G_{\mathbf{Q}}$$

を一つとって固定しよう.

さて, $[\boldsymbol{g}] \in \mathcal{E}_r^{\mathrm{in}}(G)$ を作用 $a_\Sigma$ での固定点とし, $f\colon \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)) \twoheadrightarrow G$ を $[\boldsymbol{g}]$ に対応する全射準同型とする. 仮定より, 任意の $\sigma \in G_{\mathbf{Q}}$ に対し,

$$a_\Sigma(\sigma)(f) = \mathrm{int}(g_\sigma) \circ f$$

を満たす $g_\sigma$ がモジュロ $Z(G)$ で一意的に存在する. この一意性から, $\sigma, \sigma' \in G_{\mathbf{Q}}$ に対し等式

$$\mathrm{int}(g_{\sigma\sigma'}) = \mathrm{int}(g_\sigma)\mathrm{int}(g_{\sigma'}) = \mathrm{int}(g_\sigma g_{\sigma'})$$

が従う. そこで写像 $\tilde{f}\colon \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t)) \rtimes G_{\mathbf{Q}} \to G/Z(G)$ を

$$\tilde{f}(\tau, \sigma) := f(\tau) g_\sigma \mathrm{mod}\ Z(G)$$

で定めると, これは well-defined であり, 更に群準同型であることが上の等式からわかる. 明らかに $\tilde{f}$ は全射であるので, 主張は示された. □

さて, 補題 4.3 はある意味では $G$ に対する IGP の成否に関する判定法を与えているわけではあるが, これは単に難しい問題を難しい問題に言い換えただけである. なぜならば, 問題は短完全列 (6) の構造があまりにも複雑で[*17], 結局作用 $a_G$ を直接解析することは殆どの場合不可能だからである. 一方で, (6) を理解することは大変難しいが, その「部分アーベル化」

$$1 \to \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma^{\mathrm{ab}}/\overline{\mathbf{Q}}(t)) := \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma/\overline{\mathbf{Q}}(t))^{\mathrm{ab}} \to \mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma^{\mathrm{ab}}/\mathbf{Q}(t)) \to G_{\mathbf{Q}} \to 1 \qquad (9)$$

は比較的容易に理解できる. 二つ目の群をアーベル化しているので, $G_{\mathbf{Q}}$ が

$$\rho_\Sigma^{\mathrm{ab}}\colon G_{\mathbf{Q}} \to \mathrm{Out}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma^{\mathrm{ab}}/\overline{\mathbf{Q}}(t))) = \mathrm{Aut}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma^{\mathrm{ab}}/\overline{\mathbf{Q}}(t)))$$

で作用していることに注意し, これを位相 $G_{\mathbf{Q}}$ 加群とみなす. $\widehat{\mathbf{Z}}(1)$ で $\overline{\mathbf{Q}}$ の 1 のべき根の逆極限が定める $G_{\mathbf{Q}}$ 加群を表すことにする:

$$\widehat{\mathbf{Z}}(1) := \varprojlim_n \boldsymbol{\mu}_n(\overline{\mathbf{Q}}).$$

$\widehat{\mathbf{Z}}(1)$ の位相群としての自己同型群は自然に $\widehat{\mathbf{Z}}^\times$ と同型となるので, $G_{\mathbf{Q}}$ の作用はこの群から $\widehat{\mathbf{Z}}^\times$ への連続全射群準同型を定めるが, これを**円分指標**とよび $\chi$ で表すことにする:

$$\chi\colon G_{\mathbf{Q}} \twoheadrightarrow \mathrm{Aut}(\widehat{\mathbf{Z}}(1)) \cong \widehat{\mathbf{Z}}^\times.$$

**補題 4.4.** 次の位相 $G_{\mathbf{Q}}$ 加群としての同型が存在する:

$$\mathrm{Gal}(\overline{\mathbf{Q}}(t)_\Sigma^{\mathrm{ab}}/\overline{\mathbf{Q}}(t)) \cong \widehat{\mathbf{Z}}[\Sigma]/\widehat{\mathbf{Z}} \otimes_{\widehat{\mathbf{Z}}} \widehat{\mathbf{Z}}(1).$$

ここで $\widehat{\mathbf{Z}}[\Sigma]$ は集合 $\Sigma$ を基底に持つ自由 $\widehat{\mathbf{Z}}$ 加群であり, $\widehat{\mathbf{Z}}$ は $\widehat{\mathbf{Z}}[\Sigma]$ の対角部分加群と見做している.

[*17] そこがとても面白い所でもある.

*Proof.* 複素数 $z$ に対し, $\boldsymbol{e}(z) := \exp(2\pi\sqrt{-1}z)$ と置く. この関数 $\boldsymbol{e}$ を以下の方法により, $\mathbf{A}_{\mathrm{f}} := \widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q}$ の指標とみなそう:

$$\mathbf{A}_{\mathrm{f}} \twoheadrightarrow \mathbf{A}_{\mathrm{f}}/\widehat{\mathbf{Z}} \xleftarrow{\sim} \mathbf{Q}/\mathbf{Z} \xrightarrow{\boldsymbol{e}} \mathbf{C}^{\times}.$$

$x \in \Sigma$ が $\mathbf{Q}$ 有理点であるとき, $\widehat{\mathbf{Z}}\sigma_x \subset \mathrm{Gal}(\overline{\mathbf{Q}}(t)^{\mathrm{ab}}_{\Sigma}/\overline{\mathbf{Q}}(t))$ は

$$\sigma_x \colon \overline{\mathbf{Q}}\{\{t_x\}\} \xrightarrow{\sim} \overline{\mathbf{Q}}\{\{t_x\}\}; \quad t_x^{\alpha} \mapsto \boldsymbol{e}(\alpha)t_x^{\alpha}$$

で定まっていた. 一方 $G_{\mathbf{Q}}$ の作用は係数への作用として定まっているので,

$$\sigma\sigma_x\sigma^{-1}(t_x^{\alpha}) = \sigma\sigma_x(t_x^{\alpha}) = \sigma(\boldsymbol{e}(\alpha)t_x^{\alpha}) = \boldsymbol{e}(\alpha\chi(\sigma))t_x^{\alpha}$$

が成立し, これは

$$\sigma\sigma_x\sigma^{-1} = \sigma_x^{\chi(\sigma)}$$

を意味する. $\mathbf{Q}$ 有理点でないときにはこの作用と $\Sigma$ の置換が混ざったものとなることは明らかであるので, 主張は示された. □

さて, $\sigma_x \in \mathrm{Gal}(\overline{\mathbf{Q}}(t)_{\Sigma}/\overline{\mathbf{Q}}(t))$ は一般的には体の埋め込み (2) に依存しており, 共役を除いてしか定義されていないことに注意する. $C_x := C(\sigma_x) \subset \mathrm{Gal}(\overline{\mathbf{Q}}(t)_{\Sigma}/\overline{\mathbf{Q}}(t))$ で $\sigma_x$ を含む共役類をあらわすことにすると, これは埋め込み (2) の取り方に依存していないことに注意しておこう. 一般に群 $H$ に対して, $\mathrm{Conj}(H)$ で $H$ の共役類のなす集合を表すことにする. $H$ の自己同型群は自然に $\mathrm{Conj}(H)$ に作用し, 且つその作用は外部自己同型群を経由することに注意しておこう. 従って, $\rho_{\Sigma}$ は群準同型

$$\rho_{\Sigma}^{\mathrm{conj}} \colon G_{\mathbf{Q}} \to \mathrm{Aut}\left(\mathrm{Conj}(\mathrm{Gal}(\overline{\mathbf{Q}}(t)_{\Sigma}/\overline{\mathbf{Q}}(t)))\right)$$

を誘導する. 次の系は補題 4.4 から直ちに従う:

**系 4.5.** $\chi \colon G_{\mathbf{Q}} \to \widehat{\mathbf{Z}}^{\times}$ を円分指標としたとき, 次の等式が成立する:

$$\rho_{\Sigma}^{\mathrm{conj}}(\sigma(C_x)) = C_{\sigma(x)}^{\chi(\sigma)}.$$

**定義 4.6.** $\mathcal{C} = (C_1, \ldots, C_r)$ を $G$ の共役類の組とする. このとき, $\mathcal{E}_r^{\mathrm{in}}(G)$ の部分集合 $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ を

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) := \{[g_1, \ldots, g_r] \in \mathcal{E}_r^{\mathrm{in}}(G) \mid g_i \in C_i\}$$

で定める[*18].

$s_{\Sigma} \colon G_{\mathbf{Q}} \to \mathrm{Aut}(\Sigma) = \mathfrak{S}_r$ を $G_{\mathbf{Q}}$ の $\Sigma$ への自然な作用とする. $\sigma$ を $G_{\mathbf{Q}}$ の元とし $\mathcal{C} = (C_1, \ldots, C_r)$ を $G$ の共役類の組としとき, 新たな共役類の組 $a_{\Sigma}(\sigma)\mathcal{C}$ を

$$a_{\Sigma}(\sigma)\mathcal{C} := (C^{\chi(\sigma)}_{s_{\Sigma(\sigma)}(1)}, \ldots, C^{\chi(\sigma)}_{s_{\Sigma(\sigma)}(r)})$$

で定める.

[*18] この集合は空となることも当然ある.

**補題 4.7.** $G_{\mathbf{Q}}$ の $\mathcal{E}_r^{\mathrm{in}}(G)$ への作用 $a_\Sigma(\sigma)$ は全単射

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) \xrightarrow{\sim} \mathcal{E}^{\mathrm{in}}(a_\Sigma(\sigma)\mathcal{C})$$

を誘導する.

*Proof.* これは系 4.5 から明らか. □

## 4.2 剛性の方法

いよいよ幾何的部分から離れて, 純粋に群論的な IGP の成否に関する判定法を与えることにしよう. 記号を用意する. $\mathcal{C} = (C_1, \ldots, C_r)$ を $G$ の共役類の組としたときに, $\langle \mathcal{C} \rangle$ で $\mathcal{C}$ の順序を忘れて定まる集合のこととする:

$$\langle \mathcal{C} \rangle := \{C_1, \ldots, C_r\}.$$

また, 整数 $n$ に対し $\mathcal{C}^n$ で各成分を $n$ 乗して定まる共役類の組をさすことにする:

$$\mathcal{C}^n := (C_1^n, \ldots, C_r^n).$$

ここで二つ重要な群論的概念を導入しよう.

**定義 4.8.** $\mathcal{C} = (C_1, \ldots, C_r)$ を $G$ の共役類の組とする. $\mathcal{C}$ が**有理的**であるとは, 任意の $|G|$ と互いに素な整数 $n$ に対し,

$$\langle \mathcal{C} \rangle = \langle \mathcal{C}^n \rangle$$

が成立するときに言う.

**定義 4.9.** 共役類の組 $\mathcal{C}$ が**準剛性を持つ**とは, $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ が一点集合となるときに言う. **剛性を持つ**, とは更に $G$ の中心が自明であるときに言う.

次が本稿の主結果である:

**定理 4.10** (剛性の方法)**.** 有限群 $G$ に対し, 有理的かつ準剛性を持つ共役類の組 $\mathcal{C}$ が存在すれば, 全射準同型

$$G_{\mathbf{Q}(t)} \twoheadrightarrow G/Z(G)$$

が存在する. 特に $\mathcal{C}$ が剛性を持てば, $G$ と同型なガロワ群を持つ $\mathbf{Q}$ のガロワ拡大が存在する.

実のところ証明は殆ど終わっているのであるが, より明確にするために二つ補題を準備しよう.

**補題 4.11.** $\mathcal{C} = (C_1, \ldots, C_r)$ を有理的な $G$ の共役類の組とし,

$$\alpha \colon \widehat{\mathbf{Z}}^\times \to \mathrm{Aut}(\langle \mathcal{C} \rangle)$$

を $\alpha(n)(C_i) := C_i^n$ で定める. このとき, ある有限集合 $\Sigma \subset \mathbf{P}^1(\mathbf{Q}^{\mathrm{ab}})$ が存在して, $\widehat{\mathbf{Z}}^\times$ 集合の同型

$$\Sigma \cong \langle \mathcal{C} \rangle$$

が存在する. 但しここで左辺の $\widehat{\mathbf{Z}}^\times$ 集合としての構造は円分指標の *(-1)* 乗 $\chi^{-1} \colon \mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q}) \xrightarrow{\sim} \widehat{\mathbf{Z}}^\times$ の逆写像で定まるものとする.

*Proof.* $\{S_i\}_{i=1}^m$ を $\langle \mathcal{C} \rangle$ の $\widehat{\mathbf{Z}}^\times$ 軌道とし, 全射

$$\mathrm{pr}_i \colon \widehat{\mathbf{Z}}^\times \twoheadrightarrow H_i$$

を軌道 $S_i$ に対応するものとしよう. 即ち $\widehat{\mathbf{Z}}^\times$ 作用付きの有限集合としての同型

$$H_i \xrightarrow{\sim} S_i$$

が存在する (ここで $H_i$ には自然に左からの掛け算で作用させる). ここで $K_i$ を $\mathbf{Q}$ のアーベル拡大でガロワ群が $H_i$ と自然に同型であるものとする. 藤井さんの講演 ([1]) であったように, $K_i$ は $\mathbf{Q}[H_i]$ 加群として自由かつ階数 1 であることに注意しておこう:

$$K_i \cong \mathbf{Q}[H_i].$$

そこで, $\mathbf{Q}[H_i]$ 加群としての生成元 $e_i \in K_i$ と任意の $a \in \mathbf{Q}^\times$ に対し, $a_i e_i$ の $H_i$ 軌道は自然と $H_i$ と $H_i$ 集合として同型であるので, 従って $S_i$ と $\widehat{\mathbf{Z}}^\times$ 集合として同型である. $\mathbf{Q}$ は無限体なので, $a_i$ を各軌道 $S_i$ 毎にうまくとれば, それらの定める各々の軌道は全て $\mathbf{Q}^{\mathrm{ab}}$ の相異なる元であるようにとれる. これらのなす集合を $\Sigma$ と置けば補題の条件を満たすことは容易に確かめられる. 以上で証明が完了した. □

**補題 4.12.** $\mathcal{C}$, $\Sigma$ を補題 4.11 でとったものとする. このとき, $\Sigma$ の順序をうまくとれば, $\mathcal{E}_r^{\mathrm{in}}(G)$ の部分集合 $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ は $G_{\mathbf{Q}}$ の $a_\Sigma$ による作用で安定である.

*Proof.* 補題 4.7 から,

$$a_\Sigma(\mathcal{C}) = \mathcal{C}$$

を示せば十分である. この式の左辺は

$$a_\Sigma(\mathcal{C}) := (C^{\chi(\sigma)}_{s_{\Sigma(\sigma)}(1)}, \ldots, C^{\chi(\sigma)}_{s_{\Sigma(\sigma)}(r)})$$

で定義されていたことを思い出す. また, 補題 4.11 から, $\Sigma = \{x_1, \ldots, x_r\}$ は任意の $\sigma \in G_{\mathbf{Q}}$ に対し等式

$$C^{\chi^{-1}(\sigma)}_{x_i} = C_{\sigma(x_i)}$$

を満たしており, これから, $x_i$ 達の順序をうまくとれば $C^{\chi(\sigma)}_{s_{\Sigma(\sigma)}(i)} = C_i$ が満たされることがわかる. 以上で補題の証明が完了した. □

定理 4.10 の証明. $\mathcal{C}$ を有理的かつ剛性をもつ $G$ の共役類の組とし, $\Sigma \subset \mathbf{P}^1(\mathbf{Q}^{\mathrm{ab}})$ を補題 4.11 でとったものとする. このとき, 補題 4.12 により $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ は $G_{\mathbf{Q}}$ の作用で安定である. しかも, 剛性の定義によりこれは一点集合であるので, その元 $\boldsymbol{g}$ は $G_{\mathbf{Q}}$ の作用で固定される. 従って補題 4.3 により主張は示された. □

次の章に於いてこのような共役類の組が存在するような群の例を見てみよう.

# 5 興味深い例

## 5.1 $\mathrm{SL}_2(\mathbf{F}_p)$, $\mathrm{PSL}_2(\mathbf{F}_p)$

ここではまず $\mathrm{SL}_2(\mathbf{F}_p)$ を見てみよう. 本小節は [8, Section 3.3.6] を参考にした. まず, 任意の零でない $\alpha, \beta \in \mathbf{F}_p$ に対し定まる二つの行列

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$$

は $\mathrm{SL}_2(\mathbf{F}_p)$ を生成することは直ちにわかる. 生成系の候補はここからとった方が紛れが無く良さそうであるが, その前に共役類の分類をしてみよう. $g \in \mathrm{SL}_2(\mathbf{F}_p)$ に対し, $C(g)$ で $g$ を含む共役類を表すことにする. また, $\alpha \in \mathbf{F}_p$ に対し, $C_\alpha$ で $\mathrm{SL}_2(\mathbf{F}_p) \setminus \{E_2\}$ のトレースが $\alpha$ となる元からなる部分集合をあらわすことにする:

$$C_\alpha := \{g \in \mathrm{SL}_2(\mathbf{F}_p) \setminus \{E_2\} \mid \mathrm{tr}(g) = \alpha\}.$$

明らかに $C_\alpha$ は共役作用で安定なので, これはいくつかの共役類の和集合として書けている.

**補題 5.1.** 以下の主張が成立する.

(1) $\alpha \neq \pm 2$ ならば, $C_\alpha$ はただ一つの共役類からなる.

(2) $\alpha = \pm 2$ ならば, $C_\alpha$ は二つの異なる共役類の和集合として書ける. 具体的には, $-c$ が $\mathbf{F}_p$ に於ける平方数でないような $c \in \mathbf{F}_p^\times$ に対し,

$$C_{\pm 2} = C\left(\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) \coprod C\left(\pm \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\right)$$

となる. より精密に, 上半三角冪単行列でなく更に最初の共役類に含まれない行列式 $\pm 2$ の元 $g \in \mathrm{SL}_2(\mathbf{F}_p)$ が与えられたとすると, ある平方数でない $-c$ に対して等式

$$ugu^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

を満たすような上半三角冪単行列 $u$ が存在する.

*Proof.* まず最初の主張を示そう. $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ を $C_\alpha$ の元とする. $\alpha$ は $\pm 2$ でないので, この行列は $SL_2(\mathbf{F}_p)$ の中で対角化可能であることに注意しておこう. 従って $g'$ をまた $C_\alpha$ の元とすると, ある $h \in SL_2(\overline{\mathbf{F}_p})$ であって

$$hgh^{-1} = g'$$

を満たすものが存在する. 従って任意の $\sigma \in G_{\mathbf{F}_p}$ に対して, $\sigma(h)h^{-1}$ は $g$ の $SL_2(\overline{\mathbf{F}_p})$ における中心加群に入る. 再び $g$ が対角化可能であることから, ある $k \in SL_2(\overline{\mathbf{F}_p})$ が存在して

$$Z_{SL_2(\overline{\mathbf{F}_p})}(g) = kTk^{-1}$$

が成立することに注意しよう. 但し $T$ は対角行列がなす $SL_2(\overline{\mathbf{F}_p})$ の部分群とする. 明らかに $Z_{SL_2(\overline{\mathbf{F}_p})}(g)$ は $G_{\mathbf{F}_p}$ の作用で安定であり, しかも $G_{\mathbf{F}_p}$ の作用付きで $\overline{\mathbf{F}_p}^\times$ と同型な群となっ

ていることが分かる. したがって Hilbert の定理 90 から, ある $\xi \in Z_{SL_2(\overline{\mathbf{F}_p})}(g)$ が存在して $\sigma(\xi)\xi^{-1} = \sigma(h)h^{-1}$ が任意の $\sigma \in G_{\mathbf{F}_p}$ に対して成立する. 作り方から $h' := h\xi^{-1}$ は $\mathbf{F}_p$ 係数行列であり, $h'gh'^{-1} = g'$ を満たす. 従って主張は示された.

次に二つ目の主張を示そう. $g$ は上と同じ記号とし, 今度はトレースが 2 で且つ上半冪単行列でないものとしよう. 仮定から $c$ はゼロではない. ここで次の等式が成立することに注意する

$$\begin{pmatrix} 1 & c^{-1}(1-a) \\ 0 & 1 \end{pmatrix} g \begin{pmatrix} 1 & c^{-1}(a-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}.$$

$g$ と $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ は共役でないという仮定を付けていたので, 自動的に $-c$ は平方数でないこともわかり, 主張は示される. □

以下 $\alpha \in \mathbf{F}_p$ を一つ固定しよう. さてここで $g_1, g_2, g_3$ を

$$g_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad g_2 := \begin{pmatrix} 1 & 0 \\ \alpha - 2 & 1 \end{pmatrix}, \quad g_3 := (g_1 g_2)^{-1} = \begin{pmatrix} 1 & -1 \\ 2-\alpha & \alpha - 1 \end{pmatrix}$$

で定める. また, 共役類の組 $\mathcal{C}$ を

$$\mathcal{C} := (C(g_1), C(g_2), C(g_3))$$

で定める. $\alpha$ が 2 でないならば $g_1, g_2$ は $\mathrm{SL}_2(\mathbf{F}_p)$ を生成するので, $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ は空集合でないことを注意しておこう.

**命題 5.2.** 次が成立する

(1) $2 - \alpha$ が平方数でないのであれば, $\mathcal{C}$ は剛性を持つ.
(2) 上の仮定が成立し, 更に $g_3$ の位数が 3 または 4 であれば $\mathcal{C}$ は有理的である.

*Proof.* まずはじめの主張を示す. $[g_1', g_2', g_3'] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C})$ を一つとろう. $g_1 = g_1'$ と仮定してかまわない. また, $g_1, g_2$ は $\mathrm{SL}_2(\mathbf{F}_p)$ を生成するので $g_2$ は上半三角冪単行列でない. 従って, 前の補題からある $g_1$ の中心化群の元 $u$ が存在して

$$ug_2'u^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

を満たす. $u$ が $g_1'$ と可換であることから

$$\mathrm{Tr}(g_3') = \mathrm{Tr}(ug_3'u^{-1}) = \mathrm{Tr}((g_1'ug_2'u^{-1})^{-1}) = c + 2$$

がわかり, 即ち $c = \alpha - 2$, 又は $ug_2'u^{-1} = g_2$ となる. 従って $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ はただ一つの元からなる.

二つ目の主張を示す. 最初の仮定から $C(g_1)$ と $C(g_2)$ は相異なる共役類で,

$$C_2 = C(g_1) \coprod C(g_2)$$

が成立する. 任意の $\mathrm{SL}_2(\mathbf{F}_p)$ の位数と互いに素な整数 $n$ に対し $C_2^n = C_2$ なので, $\{C(g_1)^n, C(g_2)^n\} = \{C(g_1), C(g_2)\}$ が成立する. もう一つの仮定から $C(g_3)^n = C(g_3)$ が成立するのは明らかであろう. 従って主張は示せた. □

**定理 5.3.** $p$ が 24 を法として $\pm 1$ と合同でないならば, 連続全射準同型

$$G_{\mathbf{Q}} \twoheadrightarrow \mathrm{PSL}_2(\mathbf{F}_p)$$

が存在する.

*Proof.* 上の命題の主張の二つ目に現れた条件を満たす $\alpha$ が存在することを示せばよい. まず 2 が $\mathbf{F}_p$ で平方数でないときには $\alpha = 0$ と置けばよく, 次に 3 が $\mathbf{F}_p$ で平方数でないときには $\alpha = -1$ と置けば良い. これらが満たされる条件は明らかに $p \not\equiv \pm 1 \pmod{p}$ であるので主張は示された. □

この方法だと, どうしても素数 $p$ について**合同条件**がついてしまう. $\mathrm{PSL}_2(\mathbf{F}_p)$ に対するガロワの逆問題の完全な解決については, 後の講演でお話しする予定である. 方法は**全く**異なる.

## 5.2 散在型単純群

ここでは単に結果を述べるにとどめる. 証明やそのレファレンスに関しては, [2] を参照されたい.

本サマースクールの田中氏の講演 [5] に於いても述べられたように, 有限単純群は以下の四つに大別されていた:

1. 素数位数の群
2. 五次以上の交代群
3. 有限体上定義された Lie 型の群
4. 散在型の群.

前小節で見た $\mathrm{PSL}_2(\mathbf{F}_p)$ はリストの三つ目, つまり Lie 型単純群である ($p \geq 5$ は仮定する). この小節ではリストの四つ目の単純群, 即ち散在型単純群について知られていることをまとめる.

**注意 5.4.** リストの最初の二つについてはガロワの逆問題は容易である. 一つ目は結局アーベルであるので, 既に導入部分で示してある. 二つ目もネーター問題が肯定的に解けることから既に示されている. 従って有限単純群に対する IGP で問題となるのは後の二つのクラスである.

散在型有限単純群は具体的には以下のように完全に分類されている:

- Mathieu 群, $\mathrm{M}_{11},\ \mathrm{M}_{12},\ \mathrm{M}_{22},\ \mathrm{M}_{23},\ \mathrm{M}_{24}$
- Janko 群, $\mathrm{J}_1,\ \mathrm{J}_2, \mathrm{J}_3, \mathrm{J}_4$
- Conway 群, $\mathrm{Co}_1,\ \mathrm{Co}_2,\ \mathrm{Co}_3$
- Fischer 群, $\mathrm{Fi}_{22},\ \mathrm{Fi}_{23},\ \mathrm{Fi}'_{24}$
- Higman-Sims 群 HS
- McLaughim 群 McL
- Held 群 He
- Rudvalis 群 Ru
- 鈴木群 Suz
- O'Nan 群 O′N

- 原田・Norton 群 HN
- Lyons 群 Ly
- Thompson 群 Th
- ベビーモンスター群 B
- モンスター群 M.

この分類の方法や歴史については [5], [6] やそこに含まれる引用文献を参照して頂きたい.

**定理 5.5** ([2, Theorem 10.3, (o)])**.** $M_{23}$ 以外の散在型有限単純群に対し, IGP は肯定的に解ける.

*Proof.* マシュー群 $\mathrm{M}_{23}, \mathrm{M}_{24}$ 以外の散在型単純群 $G$ に対しては, 有理的かつ剛性を持つ共役類の組が存在することを示すことが出来る. $\mathrm{M}_{24}$ については「組みひも剛性」を用いるのであるが, 本稿の範囲を超えるものであるので, ここでは詳細は述べない. 証明を知りたい方は [2, Theorem III. 7.12] を参照されたい. □

この結果により, 単純群に対する IGP はほぼリー型単純群の場合に帰着されることがわかる. 驚くべきことに, 近年まで古典リー型単純群の**基礎体を動かして得られる系列**にたいして, 一様に IGP が解決された例は知られていなかった. 例えば前節の結果にしても, 素数 $p$ に合同条件が必要だった. 次の講演に於いて, その初めての例である Zywina の結果を紹介したいと思う ([7]).

**謝辞**

本稿の初稿に目を通してくださり, 多数の有益なコメントをくださった大下達也さんに多大な感謝を申し上げます. また, 原稿の提出期限を延ばしてくださいました本サマースクールの世話人の方々に深くお礼申し上げます.

## 参考文献

[1] 藤井俊, ガロワ理論続論, 本サマースクール報告集.

[2] G. Malle, B. H. Matzat, Inverse Galois theory, Springer Monographs in Mathematics,Springer-Verlag, Berlin, 1999.

[3] J. P. Serre, Local fields, *Graduate Texts in Mathematics*, vol.**67**, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[4] J. P. Serre, Topics in Galois theory, Jones and Bartlett, Boston.

[5] 田中康彦, 有限単純群の分類問題について, 本サマースクール報告集.

[6] 鈴木 通夫, 有限単純群の分類, 数学, **34**, no. 3 (1982).

[7] 佐久川憲児, $\mathrm{PSL}_2(\mathbf{F}_p)$ に対するガロワの逆問題について, 本サマースクール報告集.

[8] Volklein, Goups as Galois groups, Cambridge Studies in AdvancedMathematics, **53**, Cambridge University Press, Cambridge, 1996.

[9] Rêvetements étales et groupe fondamental, S éminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA1), dirigé par A. Grothendieck, augmenté de deux exposés deM. Raynaud, *Springer Lecture Notes in Math.*, **224**, Springer-Verlag, Berlin-New York,1971.

# Résumé: Exposition of "The simplest cubic fields are non-isomorphic to each other"

岡崎龍太郎

September 5, 2019

## 1 総実3次体

$$K : \text{総実3次体}, \quad D(K) = K \text{の判別式} > 0.$$
$$\bullet^{(0)}, \bullet^{(1)}, \bullet^{(2)} : K \hookrightarrow \boldsymbol{R}$$

Minkowski 埋込

$$\alpha \in K \longmapsto \vec{\alpha} = \begin{pmatrix} \alpha^{(0)} \\ \alpha^{(1)} \\ \alpha^{(2)} \end{pmatrix} \in \boldsymbol{R}^3$$

対角的埋込

$$a \in \boldsymbol{Q} \longmapsto \begin{pmatrix} a \\ a \\ a \end{pmatrix} = a\vec{1} \in \boldsymbol{R}^3.$$

## 2　類体論による総実3次体の枚挙

$$K : \text{総実3次体}, \quad D(K) = K \text{の判別式} > 0.$$

**巡回3次体:**
Hasse [19], M.-N.Gras [15, 16], Ennola-Turunen [13] など.

$$K/\boldsymbol{Q} : \text{巡回3次拡大}$$

導手を指定:

$$f = p_1^* p_2 \cdots p_r,$$

$$p_2 \underset{3}{\equiv} p_3 \underset{3}{\equiv} \cdots p_r \underset{3}{\equiv} 1,$$

$$p_1^* = \begin{cases} 9 & \text{if } p_1 = 3 \\ p_1 & \text{if } p_1 \underset{3}{\equiv} 1 \end{cases}$$

位数3の Dirichlet 指標を指定:

$$\chi : \boldsymbol{Z}/f\boldsymbol{Z} \longrightarrow \boldsymbol{C}$$

Gaussian period

$$\sum_{\substack{j \in \boldsymbol{Z}/f\boldsymbol{Z} \\ \chi(j)=1}} e^{2\pi\sqrt{-1}j/f}$$

で $K$ を生成する.

$$f = \frac{a^2 + 3b^2}{4}, \quad a, b \in \boldsymbol{Z}$$

方程式 (上: $3 \nmid f$, 下: $3 \mid f$)

$$X^3 + X^2 + \frac{1-f}{3}X + \frac{(a-3)f+1}{27}$$

$$X^3 - \frac{f}{3} - \frac{af}{27}$$

**非正規3次体:**
Hasse [18], Reichardt [36], Scholz [37] など.

$$K/\boldsymbol{Q}(\sqrt{D}) : \text{巡回3次拡大}$$

Kummer 拡大を使用:

$$\alpha \in O(\boldsymbol{Q}(\sqrt{-3D})),$$

$$\alpha O(\boldsymbol{Q}(\sqrt{D})) = \mathfrak{a}^3 \prod_i \mathfrak{p}_i \bar{\mathfrak{p}}_i^2$$

$$a = \underset{\boldsymbol{Q}(\sqrt{-3D})/\boldsymbol{Q}}{N} \mathfrak{a}, \quad p_i = \underset{\boldsymbol{Q}(\sqrt{-3D})/\boldsymbol{Q}}{N} \mathfrak{p}_i,$$

$$p_i^2 | D, \quad p_i \underset{3}{\not\equiv} -1, \quad \left(\frac{-3D}{p_j}\right) \neq -1.$$

として,

$$\boldsymbol{Q}\left(\sqrt{-3}, \sqrt{-3D}\right)\left(\sqrt[3]{\alpha}\right)$$

の部分体

$$\boldsymbol{Q}\left(\sqrt[3]{\alpha} + \frac{a\prod_i p_i}{\sqrt[3]{\alpha}}\right)$$

を試す.

(3の分岐の条件のため, うまくいかない $\alpha$ もある. 従って, $\alpha$ をスクリーニングすることになる.)

## 3　Reduction Theory による総実3次体の枚挙 (体→方程式)

Davenport [7, 8], Davenport-Heilbronn [9, 10], Ennola-Turunen [12] Belabas [2] ( 新谷 [39], 大野 [34], 中川 [33] に繋がる流れ.)

$$K : \text{総実3次体}, \quad D(K) = K \text{の判別式} > 0.$$

$K$ の整数底 $(1, \alpha, \beta)$

$$O(K) = \boldsymbol{Z} + \alpha\boldsymbol{Z} + \beta\boldsymbol{Z}.$$

に線型形式

$$L(Z, X, Y) = Z + X\alpha + Y\beta, \quad L(X, Y) = X\alpha + Y\beta$$

を結びつけて, 3次形式を定義する.

$$\Delta(\alpha, \beta; X, Y) \ = \ \prod_{i=0}^{2} \left( L_K^{(i)} - L_K^{(i+1)} \right) \cdots \sqrt{\text{Discriminant Form}}$$

$$I(\alpha, \beta; X, Y) \ = \ \frac{1}{\left| \left( \ 1, \vec{\alpha}, \vec{\beta} \ \right) \right|} \prod_{i=0}^{2} \left( L^{(i)} - L^{(i+1)} \right) \cdots \text{Index Form}$$

整数底の間の関係式

$$I(\alpha)\beta = \alpha^2 + c_1\alpha + c_0, \quad (c_0, c_1 \in \boldsymbol{Z}), \quad I(\alpha) \left| \left( \ 1, \vec{\alpha}, \vec{\beta} \ \right) \right| = \left| \left( \ 1, \vec{\alpha}, \vec{\alpha}^2 \ \right) \right|$$

より,

$$I(\alpha, \beta; X, Y) = I(\alpha) \prod_{i=0}^{2} \left( X + \frac{\alpha^{(i)} + \alpha^{(i+1)} + c_1}{I(\alpha)} Y \right)$$

は $K$ を生成する代数的数の方程式である. また,

$$D(I(\alpha, \beta; X, Y)) = D(K).$$

Davenport-Heilbronn [9] は仮因子の理論を使って, $I(\alpha, \beta; X, Y)$ が primitive だと結論している.

この方法はこのままだと3次体のオーダーを枚挙する. 3次体の枚挙に必要な篩は Davenport-Heilbronn [10] を参照.

## 4　Reduction Theory による総実3次体の枚挙 (方程式→体)

$$K : \text{総実3次体}, \quad D(K) = K \text{の判別式} > 0.$$

$$O(K) = \boldsymbol{Z} + \alpha\boldsymbol{Z} + \beta\boldsymbol{Z}.$$

$$I(\alpha,\beta;X,Y) = \frac{\displaystyle\prod_{i=0}^{2}\left(\left(\alpha^{(i)} - \alpha^{(i+1)}\right)X + \left(\beta^{(i)} - \beta^{(i+1)}\right)Y\right)}{\left|\left(\begin{array}{c} 1, \vec{\alpha}, \vec{\beta} \end{array}\right)\right|}$$

$\alpha,\ \beta$ の取り方から来る $I(\alpha,\beta;X,Y)$ の変化は2元3次形式の Reduction Theory で吸収する. Cremona [4] の Reduction Theory が仕組を掘り下げている. Ennola-Turunen [12] は3次体の枚挙用に $GL_2(\boldsymbol{Z})$ による Reduction Theory を Tuning している.

2元3次形式

$$F(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3$$

の共変2次形式は Hessian のみである.

$$\begin{aligned} H(F;X,Y) &= -\frac{1}{4}\begin{vmatrix} \dfrac{\partial^2 F(X,Y)}{\partial X^2} & \dfrac{\partial^2 F(X,Y)}{\partial X\partial Y} \\ \dfrac{\partial^2 F(X,Y)}{\partial X\partial Y} & \dfrac{\partial^2 F(X,Y)}{\partial X^2} \end{vmatrix} \\ &= (b^2 - 3ac)X^2 + (bc - 9ad)XY + (c^2 - 3bd)Y^2 \\ &=: AX^2 + BXY + CY^2 \end{aligned}$$

$$\begin{aligned} F : \text{reduced} &\iff H(F;X,Y) : \text{reduced} \\ &\iff -A \le B < A < C \ \vee\ 0 \le -B < A = C \end{aligned}$$

$$|a| \le \frac{2D(F)^{1/4}}{3\sqrt{3}}, \quad |b| \le \frac{2D(F)^{1/4}}{\sqrt{3}}, \quad |bc| < D^{1/2}, \quad |ad| < \frac{4D^{1/2}}{27}$$

**注)**　Llorente-Oneto [26] と Llorente-Quer [29] は3次体の方程式に別の正規化 $X^3 + aX + b$ を用いている.

## 5　2元3次形式 $F(X,Y)=aX^3+bX^2Y+cXY^2+dY^3$ の不変式論

判別式:

$$D=D(F)=b^2c^2-4ac^3-4b^3d+18abcd-27a^2d^2$$

共変 2次形式:

$$\begin{aligned}H(F;X,Y) &= -\frac{1}{4}\begin{vmatrix}\dfrac{\partial^2F(X,Y)}{\partial X^2} & \dfrac{\partial^2F(X,Y)}{\partial X\partial Y}\\ \dfrac{\partial^2F(X,Y)}{\partial X\partial Y} & \dfrac{\partial^2F(X,Y)}{\partial X^2}\end{vmatrix}\\ &= (b^2-3ac)X^2+(bc-9ad)XY+(c^2-3bd)Y^2\\ &=: AX^2+BXY+CY^2\end{aligned}$$

$$D(H)=B^2-4AC=-3D(F).$$

$F$ と $H(F)$ の Jacobian = 共変3次形式:

$$\begin{aligned}J(F;X,Y) &= -\begin{vmatrix}\dfrac{\partial F(X,Y)}{\partial X} & \dfrac{\partial F(X,Y)}{\partial Y}\\ \dfrac{\partial H(F;X,Y)}{\partial X} & \dfrac{\partial H(F;X,Y)}{\partial Y}\end{vmatrix}\\ &= (2b^3-9abc+27a^2d)X^3+3(b^2c-6ac^2+9abd)X^2Y\\ &\quad -3(bc^2-6b^2d+9acd)XY^2-(2c^3-9bcd+27ad^2)Y^3.\end{aligned}$$

$$D(J)=729D(F)^3.$$

また

$$J(J(F))=-729D(F)^2F$$

Syzygy

$$4H^3=J^2+27DF^2.$$

## 6　2元3次形式の因数分解の正規化

O. [35]

総実2元3次形式

$$F(X,Y)=aX^3+bX^2Y+cXY^2+dY^3\in \boldsymbol{R}[X,Y],\quad D(F)>0.$$

因数分解

$$F(X,Y)=\prod_{i=0}^{2}\left(\alpha_iX+\beta_iY\right),\quad \boldsymbol{\alpha}=\begin{pmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\end{pmatrix},\boldsymbol{\beta}=\begin{pmatrix}\beta_0\\ \beta_1\\ \beta_2\end{pmatrix}\in \boldsymbol{R}^3.$$

基底の外積

$$\boldsymbol{\delta}=\boldsymbol{\alpha}\times\boldsymbol{\beta}=\begin{pmatrix}\delta_0\\ \delta_1\\ \delta_2\end{pmatrix},\ \delta_i=\begin{vmatrix}\alpha_{i+1} & \beta_{i+1}\\ \alpha_{i+2} & \beta_{i+2}\end{vmatrix},(\text{添字は }\mathrm{mod}3\text{ で読む}).$$

平面格子の正規化 (記号が無い積は成分毎の積)

$$\boldsymbol{\alpha}X+\boldsymbol{\beta}Y\rightsquigarrow\boldsymbol{\delta}\boldsymbol{\alpha}X+\boldsymbol{\delta}\boldsymbol{\beta}Y$$

外積の性質より,

$$\boldsymbol{\delta}\boldsymbol{\alpha},\boldsymbol{\delta}\boldsymbol{\beta}\perp\vec{1}.$$

また, $\boldsymbol{\delta}\boldsymbol{\alpha}$ と $\boldsymbol{\delta}\boldsymbol{\beta}$ はCanonicalに決まる. 即ち,

$$\boldsymbol{\xi}=(\xi_i)_{i=0}^2,\quad \xi_0\xi_1\xi_2=1\Longrightarrow(\boldsymbol{\xi}\boldsymbol{\alpha}\times\boldsymbol{\xi}\boldsymbol{\beta})\,\boldsymbol{\xi}\boldsymbol{\alpha},(\boldsymbol{\xi}\boldsymbol{\alpha}\times\boldsymbol{\xi}\boldsymbol{\beta})\,\boldsymbol{\xi}\boldsymbol{\beta}$$

は$\xi$に依存しない.

平面格子の正規化の計量

$$Q(X,Y)=\frac{1}{2}\|\boldsymbol{\delta}\boldsymbol{\alpha}X+\boldsymbol{\delta}\boldsymbol{\beta}Y\|^2=H(F;X,Y).$$

2元3次形式の因数分解の正規化

$$F(X,Y)=\frac{1}{\delta_0\delta_1\delta_2}\prod_{i=0}^{2}\left(\delta_i\alpha_iX+\delta_i\beta_iY\right).$$

## 7　2元3次形式の自己同型

Ayad [1], [39]

判別式が正 $(D(F) > 0)$ の総実2元3次形式 $F$:

$$F(X,Y) = F\begin{pmatrix} X \\ Y \end{pmatrix} = aX^3 + bX^2Y + cXY^2 + dY^3 \in \boldsymbol{R}[X,Y],$$

左の式を中央の式の略記と見る.

変数変換

$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \in GL_2(\boldsymbol{Z})$$

を定義:

$$(F \circ T)\begin{pmatrix} X \\ Y \end{pmatrix} = F\left(T\begin{pmatrix} X \\ Y \end{pmatrix}\right) = F\begin{pmatrix} t_{11}X + t_{12}Y \\ t_{21}X + t_{22}Y \end{pmatrix}$$

解釈を変える:

$$F(X,Y) = N\left((\boldsymbol{\alpha},\boldsymbol{\beta})\,;X,Y\right) = \prod_{i=0}^{2}(\alpha_i X + \beta_i Y)\cdots \text{Norm Form}$$

見方:

$$F \overset{\text{ほぼ}}{\longleftrightarrow} \boldsymbol{Z\alpha} + \boldsymbol{Z\beta}.$$

$$(F \circ T)(X,Y) = N((\boldsymbol{\alpha},\boldsymbol{\beta})\,T;X,Y)$$

見方:

$$\text{変数変換} \longleftrightarrow \text{格子の基底の取り換え}$$

$$\begin{aligned} \text{Aut}(H(F)) &= \{T \in GL_2(\boldsymbol{Z}) : H(F)\circ T = H(F)\}; \\ \text{Aut}(\boldsymbol{Z\alpha},\boldsymbol{Z\beta},\|\bullet\|) &= \text{Aut}(H(F)); \quad (\text{見方}) \\ \text{Aut}(F) &= \{T \in GL_2(\boldsymbol{Z}) : F\circ T = F\} \subset \text{Aut}(H(F)); \end{aligned}$$

但し, $(\boldsymbol{\alpha},\boldsymbol{\beta})$ による $F$ の因数分解が正規化済だとする.

## 8　2元3次形式の非自明な自己同型

判別式が正 $(D(F)>0)$ の総実2元3次形式 $F$:

$$F(X,Y)=F\begin{pmatrix}X\\Y\end{pmatrix}=aX^3+bX^2Y+cXY^2+dY^3\in\boldsymbol{R}[X,Y]$$

$F$ の自明な自己同型：

$$T=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad F\circ T=F.$$

$F$ の自己同型でないものの例:

$$F\circ\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=-F.$$

自己同型

$$T\in\mathrm{Aut}(F)\cap SL_2(\boldsymbol{Z})\subset\mathrm{Aut}(H(F))\cap SL_2(\boldsymbol{Z})$$

の一般論. (簡単のため正規化済の $(\boldsymbol{\alpha},\boldsymbol{\beta})$ について.)

$$(\boldsymbol{\alpha},\boldsymbol{\beta}),(\boldsymbol{\alpha},\boldsymbol{\beta})T,(\boldsymbol{\alpha},\boldsymbol{\beta})T^2,(\boldsymbol{\alpha},\boldsymbol{\beta})T^3,\ldots:\text{有界}\therefore\text{周期的}.$$

$$T^\ell=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \ell:\text{最小周期}.$$

$T$ の固有値は1の巾根で, $T$ のサイズ $2\times2$ より, それら固有値は2次まで. よって, $T$ の固有値は次の複素数に限られる.

$$\pm1,\pm\sqrt{-1},\pm\frac{-1+\sqrt{-3}}{2},\pm\frac{1+\sqrt{-3}}{2}.$$

$$T^j\neq\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad (j=1,2,3,\ldots).$$

より, $F$ の非自明な自己同型の固有値の集合は次のものに限られる.

$$\left\{\frac{-1+\sqrt{-3}}{2},\frac{-1-\sqrt{-3}}{2}\right\},\quad (\text{周期}3)$$

## 9　非自明な自己同型を持つ2元3次形式

判別式が正 $(D(F)>0)$ の総実2元3次形式 $F$:

$$F(X,Y)=F\begin{pmatrix}X\\Y\end{pmatrix}=aX^3+bX^2Y+cXY^2+dY^3\in\boldsymbol{R}[X,Y]$$

$F$ が非自明な自己同型を持つとする.

$$T\in\mathrm{Aut}(F)\cap SL_2(\boldsymbol{Z}),\quad 1+T+T^2=0\quad\therefore T^3=1.$$

すると, $\boldsymbol{Z}\boldsymbol{\alpha}+\boldsymbol{Z}\boldsymbol{\beta}$ の逐次最小の集合 $(M)$ の濃度は3の倍数となる.

また, 簡単のため, $(\boldsymbol{\alpha},\boldsymbol{\beta})$ が正規化済とする.

さらに, $F$ が reduced だとする.

$$\#\mathcal{M}=\begin{cases}2 & \text{if } \|\boldsymbol{\alpha}\|<\|\boldsymbol{\beta}\| \ \wedge\ \boldsymbol{\alpha}\cdot\boldsymbol{\beta}\neq 0\\ 4 & \text{if } \|\boldsymbol{\alpha}\|<\|\boldsymbol{\beta}\| \ \wedge\ \boldsymbol{\alpha}\cdot\boldsymbol{\beta}=0\\ 4 & \text{if } \|\boldsymbol{\alpha}\|=\|\boldsymbol{\beta}\| \ \wedge\ \boldsymbol{\alpha}\cdot\boldsymbol{\beta}\notin\left\{0,-\frac{1}{2}\|\alpha\|^2\right\}\\ 8 & \text{if } \|\boldsymbol{\alpha}\|=\|\boldsymbol{\beta}\| \ \wedge\ \boldsymbol{\alpha}\cdot\boldsymbol{\beta}=0\\ 12 & \text{if } \|\boldsymbol{\alpha}\|=\|\boldsymbol{\beta}\| \ \wedge\ \boldsymbol{\alpha}\cdot\boldsymbol{\beta}=-\frac{1}{2}\|\alpha\|^2\end{cases}$$

より,

$$H(F)=\frac{\|\alpha\|^2}{2}(X^2-XY+Y^2)$$

$$T=\begin{pmatrix}0&-1\\1&-1\end{pmatrix},\quad\begin{pmatrix}-1&1\\-1&0\end{pmatrix}$$

となる. ($F$: reduced という設定の効果で相似変形が見えない.)
この下で $F=F\circ T$ を係数の1次方程式として解くと

$$F=\ G_{a,b}(X,Y)=aX^3+bX^2Y+(-b-3a)XY^2+aY^3$$

$D(F)=(b^2+3ab+9a^2)^2$,　分解体は巡回3次体

となる.

**注)**　$GL_2(\boldsymbol{Z})$ の場合は $X^3-2XY^2$ が $(X,Y)\longmapsto(X,-Y)$ で不変となる事情で煩雑になる.

## 10　巡回3次体から2元3次形式の自己同型へ (目標設定)

$$K : \text{巡回3次体}, \quad D(K) = f^2 > 0, \quad 0 < f \in \boldsymbol{Z}.$$

$$\langle \sigma \rangle = \mathrm{Gal}(F/\boldsymbol{Q}).$$

$$\bullet^{(0)} : K \hookrightarrow \boldsymbol{R}$$

$$\bullet^{(i)} : \alpha \in K \longmapsto \left(\alpha^{\sigma^i}\right)^{(0)} \in \boldsymbol{R}$$

$$O(K) = \boldsymbol{Z} + \boldsymbol{Z}\alpha + \boldsymbol{Z}\beta$$

「3次体 $\rightsquigarrow$ Index Form」の理論と「2元3次形式 $\rightsquigarrow$ 格子の正規化」の理論を組み合せたい.

$$\begin{pmatrix} \alpha^{(0)} \\ \alpha^{(1)} \\ \alpha^{(2)} \end{pmatrix} \longmapsto \begin{pmatrix} \alpha^{(1)} - \alpha^{(2)} \\ \alpha^{(2)} - \alpha^{(0)} \\ \alpha^{(0)} - \alpha^{(1)} \end{pmatrix}$$

は $\vec{1}\boldsymbol{R}$ を消して, $\vec{1}^{\perp}$ 上では回転を含む相似拡大になっている.

$$\boldsymbol{Z}\frac{1}{\sqrt[6]{D(K)}}\left(\vec{\alpha}^{\sigma} - \vec{\alpha}^{\sigma^2}\right) + \boldsymbol{Z}\frac{1}{\sqrt[6]{D(K)}}\left(\vec{\beta}^{\sigma} - \vec{\beta}^{\sigma^2}\right)$$

は共変な2次形式 (格子の計量) と3次形式 (Norm Form) を与える. 後者が $K$ の Index Form になっている.

共変な2次形式と3次形式を巡回3次体の幾何的な構造から直接につくることはできないだろうか？

巡回3次体の場合, $\boldsymbol{R}^3$ 内の $K$, そして $O(K)$ は座標3個の巡回置換で不変である. そこで, $O(K) \smallsetminus \boldsymbol{Z}$ の元で $\boldsymbol{R}\vec{1}$ からの距離が最小のものを $\alpha$ として, $\beta = \alpha^{\sigma}$ と置こう.

$$\mathrm{dist}\left(\vec{\alpha}, \boldsymbol{R}\vec{1}\right) = \mathrm{dist}\left(O(K) \smallsetminus \boldsymbol{Z}, \boldsymbol{R}\vec{1}\right), \quad \beta = \alpha^{\sigma}$$

すると, $(1, \alpha, \beta)$ が $K$ の整数底となる.

$$O(K) = \boldsymbol{Z} + \boldsymbol{Z}\alpha + \boldsymbol{Z}\beta$$

## 11　巡回3次体から2元3次形式の自己同型へ (格子発見)

$$K : \text{巡回3次体}, \quad D(K) = f^2 > 0, \quad 0 < f \in \boldsymbol{Z}.$$
$$\langle \sigma \rangle = \mathrm{Gal}(F/\boldsymbol{Q}).$$
$$\mathrm{dist}\left(\vec{\alpha}, \boldsymbol{R}\vec{1}\right) = \mathrm{dist}\left(O(K) \smallsetminus \boldsymbol{Z}, \boldsymbol{R}\vec{1}\right), \quad \beta = \alpha^{\sigma}$$
$$O(K) = \boldsymbol{Z} + \boldsymbol{Z}\alpha + \boldsymbol{Z}\beta$$

このデータに格子を結びつける.

$$\boldsymbol{Z}\left(\vec{\alpha}^{\sigma} - \vec{\alpha}^{\sigma^2}\right) + \boldsymbol{Z}\left(\vec{\beta}^{\sigma} - \vec{\beta}^{\sigma^2}\right)$$

計量は数論的に正規化するなら

$$\begin{aligned} Q(\alpha, \beta; X, Y) &= \frac{1}{2}\| X\left(\vec{\alpha}^{\sigma} - \vec{\alpha}^{\sigma^2}\right) + Y\left(\vec{\beta}^{\sigma} - \vec{\beta}^{\sigma^2}\right) \|^2 \\ &= \operatorname*{tr}_{K/\boldsymbol{Q}}\left(\alpha^2 - \alpha^{\sigma+\sigma^2}\right) \cdot \left(X^2 - XY + Y^2\right) \end{aligned}$$

となる. 但し, $\boldsymbol{R}^3$から誘導される計量は補正因子を取る. また,

$$\bullet^{\perp} : \boldsymbol{R}^3 \longmapsto (\boldsymbol{R}\vec{1})^{\perp} \cdots \text{直交射影}$$

を使うと,

$$\left[\boldsymbol{Z}\left(\vec{\alpha}^{\perp}\right) + \boldsymbol{Z}\left(\vec{\beta}^{\perp}\right) : \boldsymbol{Z}\left(\vec{\alpha}^{\sigma} - \vec{\alpha}^{\sigma^2}\right) + \boldsymbol{Z}\left(\vec{\beta}^{\sigma} - \vec{\beta}^{\sigma^2}\right)\right] = 3.$$

となるから,

$$f = \mathrm{covol}(O(K)) = \operatorname*{tr}_{K/\boldsymbol{Q}}\left(\alpha^2 - \alpha^{\sigma+\sigma^2}\right)$$

となる. 他方,

$$f \mid \prod_{i=0}^{2}(\alpha_{(i+1)} - \alpha_{(i+2)})$$

より,

$$\alpha_{(i+1)} - \alpha_{(i+2)} \in \prod_{\mathfrak{p}|f} \mathfrak{p}^{1+\mathrm{ch}(3\in\mathfrak{p})}$$

## 12　巡回3次体から2元3次形式の自己同型へ (到着)

$$K : \text{巡回3次体}, \quad D(K) = f^2 > 0, \quad 0 < f \in \boldsymbol{Z}.$$
$$\langle \sigma \rangle = \mathrm{Gal}(F/\boldsymbol{Q}).$$
$$\mathrm{dist}\left(\vec{\alpha}, \boldsymbol{R}\vec{1}\right) = \mathrm{dist}\left(O(K) \smallsetminus \boldsymbol{Z}, \boldsymbol{R}\vec{1}\right), \quad \beta = \alpha^{\sigma}$$
$$O(K) = \boldsymbol{Z} + \boldsymbol{Z}\alpha + \boldsymbol{Z}\beta$$
$$\boldsymbol{Z}\left(\vec{\alpha}^{\sigma} - \vec{\alpha}^{\sigma^2}\right) + \boldsymbol{Z}\left(\vec{\beta}^{\sigma} - \vec{\beta}^{\sigma^2}\right)$$

このデータから2元3次形式を作ってある.

$$I(\alpha, \beta; X, Y) = \pm\frac{1}{f}\prod_{i=0}^{2}\left(\left(\alpha^{(i)} - \alpha^{(i+1)}\right)X + \left(\beta^{(i)} - \beta^{(i+1)}\right)Y\right)$$

$$\alpha \longleftrightarrow \begin{pmatrix} \alpha \\ \alpha^{\sigma} \\ \alpha^{\sigma^2} \end{pmatrix}, \quad \alpha^{\sigma} \longleftrightarrow \begin{pmatrix} \alpha^{\sigma} \\ \alpha^{\sigma^2} \\ \alpha \end{pmatrix}$$

を横目に見て

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}^{\sigma} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

と$\sigma$を拡張する. すると,

$$\vec{\alpha} \overset{\sigma}{\longmapsto} \vec{\beta} \overset{\sigma}{\longmapsto} -\vec{\alpha} - \vec{\beta}$$
$$\left(\vec{\alpha}^{\sigma}, \vec{\beta}^{\sigma}\right) = \left(\vec{\alpha}, \vec{\beta}\right)T, \quad T = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

となる. 従って,

$$I(\alpha, \beta; X, Y) = I(\alpha^{\sigma}, \beta^{\sigma}; X, Y) = I((\alpha, \beta)T; X, Y)$$

$$I(\alpha, \beta; X, Y) = aX^3 + bX^2Y + (-b - 3a)XY^2 + aY^3$$
$$D(I(\alpha, \beta; X, Y)) = (b^2 + 3ab + 9a^2)^2, \quad a, b \in \boldsymbol{Z}.$$

## 13　巡回3次体の族 (要約)

巡回3次体 $K$ は

$$\begin{aligned} F(X,Y) = I(\alpha,\alpha^\sigma;X,Y) &= G_{a,b}(X,Y) \\ &= aX^3+bX^2Y+(-b-3a)XY^2+aY^3 \\ D(I(\alpha,\alpha^\sigma;X,Y)) &= (b^2+3ab+9a^2)^2, \quad a,b\in\boldsymbol{Z} \end{aligned}$$

によってパラメトライズされる.

**注)**　先に方程式を与えた場合は, $F$ の分解体の退化が起こりえる. 実際

$$a=tuv(v-u), \quad b=tu^3-3tuv^2+tv^3, \quad t,u,z\in\boldsymbol{Z}$$

のとき

$$F(u,v)=0$$

となる. また, $a=0$ の場合は, $b$ を自由にしても

$$F(X,Y)=bXY(X-Y)$$

となり, $F$ の分解体は退化する.

　見つけ方:　$0\neq a,b,u,v\in\boldsymbol{Z}$, $\gcd(u,v)=1$ の下で

$$au^3+bu^2v-(b+3a)uv^2+av^3=0$$

となったとする. $u$, $v$, $v-u$ を法とする合同式の考察から,

$$a=tuv(v-u), \quad \exists t\in\boldsymbol{Z}$$

が分かる. 次に方程式を $a=uv(v-u)$ で除すると

$$tu^3-b-3tuv^2+tv^3=0.$$

となる.　(若林 [41] は既約性の少し弱い十分条件を証明している.)

**注)**　この族は $\boldsymbol{Q}$ 上では1変数 $b/a$ でパラメトライズされている.

## 14 巡回3次体とThue方程式

M.Bennett [3], O. [35]

$$\begin{aligned} G_{a,b}(X,Y) &= aX^3+bX^2Y+(-b-3a)XY^2+aY^3 \\ D(I(\alpha,\alpha^\sigma;X,Y)) &= (b^2+3ab+9a^2)^2, \quad a,b\in \boldsymbol{Z} \end{aligned}$$

M.Bennett の衝撃的な結果 [3] にはThue 方程式

$$G_{a,b}(X,Y)=1$$

の解の個数$R(a,b)$が 0, 3, 6 か 9 に限られるいう系がある. 同じ論文でパラメーター$k\in \boldsymbol{Z}$入りで

$$G_{2k+1,-3k-1}(2,1)=G_{2k+1,-3k-1}(-1,-2)=G_{2k+1,-3k-1}(-1,1)=0.$$

という現象が指摘されている.

$$G_{2k+1,-3k-1}(2,1)=X^3-X^2Y-2XY^2+Y^3+k(X-2Y)(2X-Y)(X+Y)$$

また,

$$G_{2k,b}(X,Y)=2kX^3+bX^2Y+(-b-6k)XY^2+2kY^3 \underset{2}{\equiv} bXY(X-Y)$$

について, $R(2k,b)=0$という現象も指摘されている. $G_{2k,b}$の分解体で2が完全分解することから, 素イデアルの分解とThue方程式の関連に興味が湧く.

講演者の定理 [35, Theorem 1.3] は$D(G_{a,b})\geq 2.56\cdot 10^8$の下で, $R(a,b)$が0か3に限られることを示した.

若林 [41] は$D(G_{a,b})$に関する条件を外して, $R(a,b)$が0か3に限られることを示した. また 若林[42] はThue不等式

$$|G_{a,b}(X,Y)|\leq 2b+3a$$

を解いた.

Thue 方程式

$$G_{1,n-1}(X,Y)=1$$

は更に有名である.

## 15 Simplest cubic field とThue 方程式

D.Shanks [38], E.Thomas [40], Mignotte [31], 若林 [41, 42], 星 [22]

D.Shanks [38] の simplest cubic field $K_n$ の定義方程式は

$$P_n = G_{1,n-1}(X,1) = X^3 + (n-1)X^2 - (n+2)X + 1, \quad n \in \boldsymbol{Z}$$

であり, $P_n$ の判別式

$$(n^2+n+7)^2$$

が平方数であることから数体 $K_n$ は巡回3次体である.

パラメーターの交換 $n \longleftrightarrow -n-1$ が中間の項の係数の交換を起こすから,

$$K_{-n-1} = K_n$$

という体の重復がある. この重復を $n$ の範囲の制限 $n \geq 0$ によって除こう.

$n \geq 0$ の範囲では $n^2+n+7$ が増加函数になるから, $G_{1,n-1}$ は互いに同値ではない.

E.Thomas [40] は $n \geq 1.365 \times 10^7$ の下でThue 方程式

$$G_{1,n-1}(X,Y) = 1$$

の解が $(1,0)$, $(0,1)$, $(-1,-1)$ に限られることを示した. $n$ に関する条件を落とすことができるという E.Thomas の予想を Mignotte [31] が証明した. これは Baker 理論を使う証明だったが, 超幾何函数を使う研究もあり右辺を $n$ の言葉で小さい数に置き換えた Thue 方程式や Thue 不等式まで発展している. この方向の研究は若林 [41, 42] の研究が究極の結果となっている.

他方, 講演者は CIRM の講演で $K_n$ の重複を研究した. 星 [22] はこの研究を発展させて, 右辺が $n^2+n+7$ の約数の場合を完全に解いた.

## 16 Simplest cubic field の重複問題

$K_n : P_n = G_{1,n-1}(X,1) = X^3+(n-1)X^2-(n+2)X+1, \quad n \in \boldsymbol{Z}$

しかし, simplest cubic field の重複が他にもあることが知られている:

$$K_0 = K_6 = K_{13} = K_{1260}; \quad K_1 = K_4 = K_{55}; \quad K_2 = K_{67}; \quad K_3 = K_{2390}.$$

ここで, 自然に次の疑問が湧いてくる:

**Problem:** *simplest cubic field*の重複は以上で全てなのではないだろうか*?*

Diophantine Analysis から解答が出てきた: Thue 方程式

$$X^3 + (n-1)X^2Y - (n+2)XY^2 + Y^3 = 1.$$

から自明な解$(1,0), (0,1), (-1,-1)$ 以外の解を排除する研究の分析から我々の疑問の検証が出てきた.

## References

[1] M.Ayad, "Automorphismes d'une forme binaire cubique et représentation d'entiers", C. R. Acad. Sci. Paris Sér. I Math. 299, no. 19 (1984) 959–962.

[2] K.Belabas, "A fast algorithm to compute cubic fields", Math. Comp. 66, no. 219 (1997) 1213–1237.

[3] M.A.Bennett, "On the representation of unity by binary cubic forms", Trans. Amer. Math. Soc. 353, no. 4 (2001) 1507–1534.

[4] J.E.Cremona, "Reduction of binary cubic and quartic forms", LMS J. Comput. Math. 2 (1999) 64–94.

[5] J.E.Cremona, "Corrigendum: "Reduction of binary cubic and quartic forms" [LMS J. Comput. Math. 2 (1999) 64–94", LMS J. Comput. Math. 4 (2001) 73.

[6] J.E.Cremona and M.Stoll, "On the reduction theory of binary forms" J. Reine Angew. Math. 565 (2003) 79–99.

[7] H.Davenport, "On the class-number of binary cubic forms. I", J. London Math. Soc. 26 (1951) 183–192.

[8] H.Davenport, "On the class-number of binary cubic forms. II", J. London Math. Soc. 26 (1951) 192–198.

[9] H.Davenport and H.Heilbronn, "On the density of discriminants of cubic fields", Bull. London Math. Soc. 1 (1969) 345–348.

[10] H.Davenport and H.Heilbronn, "On the density of discriminants of cubic fields. II" Proc. Roy. Soc. London Ser. A 322, no. 1551 (1971) 405–420.

[11] B.N.Delone and D.K.Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10 American Mathematical Society, Providence, R.I. (1964).

[12] V.Ennola and R.Turunen, "On totally real cubic fields", Math. Comp. 44 (1985), no. 170, 495–518.

[13] V.Ennola and R.Turunen, "On cyclic cubic fields", Math. Comp. 45 (1985), no. 172, 585–589.

[14] I.Gaál, *Diophantine equations and power integral bases. New computational methods*, Birkhäuser Boston, Inc., Boston, MA, (2002), ISBN: 0-8176-4271-4

[15] M.-N.Gras, "Nombre de classes, unités et bases d'entiers des extensions cubiques cycliques de $\mathbf{Q}$", Journées Arithmétiques

(Grenoble, 1973) pp. 101–106. Bull. Soc. Math. France Mém., No. 37, Soc. Math. France, Paris, 1974.

[16] M.-N.Gras, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbf{Q}$", J. Reine Angew. Math. 277 (1975), 89–116.

[17] M.-N.Gras, "Familles d'unités dans les extensions cycliques réelles de degré 6 de $\mathbf{Q}$", Théorie des nombres, Années 1984/85–1985/86, Fasc. 2, Exp. No. 2, 27 pp., Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1986.

[18] H.Hasse, "Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage", Math. Z. 31 (1930), no. 1, 565–582.

[19] H.Hasse, "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern", Abh. Deutsch. Akad. Wiss. Berlin. Math.-Nat. Kl. 1948, (1948) no. 2, 95 pp. (1950).

[20] D.Hilbert, "Theory of algebraic invariants", Translated from the German and with a preface by Reinhard C. Laubenbacher. Edited and with an introduction by Bernd Sturmfels. Cambridge University Press, Cambridge, 1993. ISBN: 0-521-44457-8; 0-521-44903-0

[21] Akinari Hoshi "On the simplest quartic fields and related Thue equations", *The Joint Conference of ASCM 2009 and MACIS 2009*, 320–329, COE Lect. Note, 22, Math-for-Ind. (MI) Lect. Note Ser., Kyushu Univ. Fac. Math., Fukuoka, (2009)

[22] Akinari Hoshi, "On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the sim-

plest cubic fields", J. Number Theory 131, no. 11 (2011) 2135–2150.

[23] Akinari HOSHI, "On the simplest sextic fields and related Thue equations", Funct. Approx. Comment. Math. 47, part 1 (2012) 35–49. ISBN: 978-83-232-2442-6

[24] B.Hutz and M.Stoll, "Smallest representatives of $\mathrm{SL}(2,\mathbb{Z})$-orbits of binary forms and endomorphisms of $\mathbb{P}^1$", Acta Arith. 189, no. 3 (2019), 283–308.

[25] Llorente, Pascual. Cubic fields and class fields of real quadratic fields. (Spanish) Publ. Sec. Mat. Univ. Autònoma Barcelona 26 (1982), no. 2, 93–109.

[26] P.Llorente and A.V.Oneto, "On the real cubic fields", Math. Comp. 39, no. 160 (1982), 689–692.

[27] P.Llorente and E.Nart, "Effective determination of the decomposition of the rational primes in a cubic field", Proc. Amer. Math. Soc. 87 (1983), no. 4, 579–585.

[28] F.Diaz y Diaz and P. Llorente and J.Quer, "Cubic fields, a congruential criterion for Scholz's theorem and new real quadratic fields with 3-rank equal to 4", Arch. Math. (Basel) 50 (1988), no. 4, 356–359.

[29] P.Llorente and J.Quer, "On totally real cubic fields with discriminant $D < 10^7$", Math. Comp. 50 (1988), no. 182, 581–594.

[30] M.Laurent, M.Mignotte and Y.Nesterenko, "Formes linéaires en deux logarithmes et déterminants d'interpolation", J. Number Theory 55, no. 2 (1995) 285–321.

[31] M.Mignotte, "Verification of a conjecture of E. Thomas", J. Number Theory 44, no. 2 (1993) 172–177.

[32] P.Morton, "Characterizing cyclic cubic extensions by automorphism polynomials", J. Number Theory 49, no. 2 (1994), 183–208.

[33] J.Nakagawa, "On the relations among the class numbers of binary cubic forms" Invent. Math. 134, no. 1 (1998), 101–138.

[34] Y.Ohno, "A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms", Amer. J. Math. 119, no. 5 (1997), 1083–1094.

[35] R.Okazaki, "Geometry of a cubic Thue equation", Publ. Math. Debrecen 61, no. 3-4 (2002), 267–314.

[36] H.Reichardt, "Arithmetische Theorie der kubischen Körper als Radikalkörper", Monatsh. Math. Phys. 40 (1933), no. 1, 323–350.

[37] A. Scholz "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander" "Idealklassen und Einheiten in kubischen Körpern" J. die Reine Angew. Math. 166, (1932) 201–203.

[38] D.Shanks, "The simplest cubic fields", Math. Comp. 28 (1974) 1137–1152.

[39] T.Shintani, "On Dirichlet series whose coefficients are class numbers of integral binary cubic forms", J. Math. Soc. Japan 24 (1972) 132–188.

[40] E.Thomas, "Complete solutions to a family of cubic Diophantine equations", J. Number Theory 34 no. 2 (1990),, 235–250.

[41] I.Wakabayashi, "Number of solutions for cubic Thue equations with automorphisms", Ramanujan J. 14, no. 1 (2007), 131–154.

[42] I.Wakabayashi, "Simple families of Thue inequalities. Ann. Sci. Math. Québec 31, no. 2 (2007) 211–232 (2008).

[43] L.C.Washington, "Class numbers of the simplest cubic fields", Math. Comp. 48, no. 177 (1987) 371–384.

# ガロア群の構成問題の明示解の活用 ～明示的な多項式があると出来ること～

角皆 宏

Galois 群の構成問題では所望の Galois 群を持つ多項式を明示的に得ることを目標の一つとするが、既に存在が証明されている群に対する多項式の明示的構成や、既に多項式が明示的に構成されている群に対するより簡明な多項式の構成については、既存の結果の後追いのように見られて、低い評価をされがちである。そこで本稿では、明示的構成の意義、明示的で簡明な多項式を利用して出来ることの一部を紹介したい。具体的には、

- 整数環の決定（特に、単生 (monogenic) な代数体の構成）
- 単数群の決定（まで行かなくても明示的な単数を持つ代数体の構成）
- 2 次不分岐拡大の明示的構成（による類数の可除性）

などを扱う。

## 1. Shanks の巡回 3 次式

先立つ稿 [T*, 注 1] でも現れたように、

$$f(t;X) = X^3 - tX^2 + (t-3)X + 1 \in \boldsymbol{Q}(t)[X]$$

は、$\boldsymbol{Q}$ 上の 1 助変数の生成的 $C_3$ 多項式である。$X \to -X, t \to -t$ と変数変換した多項式

$$f^{\mathrm{Sh}}(t;X) = X^3 - tX^2 - (t+3)X - 1 \in \boldsymbol{Q}(t)[X]$$

を用いることも多く[1]、Shanks の巡回 3 次式と呼ばれる。特に、$t \in \boldsymbol{Z}$ に特殊化した場合には常に $\boldsymbol{Q}$ 上既約で、その根体（＝分解体）である巡回 3 次体 $K = K_t$ は、基本単数などの数論的な重要な情報が明示的に求まりやすい特徴があり、最簡 3 次体 (simplest cubic fields) と呼ばれる (Shanks[Sh])。

有理関数体 $\boldsymbol{Q}(t)$ 上の多項式として成り立っていることをまとめておく。$f^{\mathrm{Sh}}$ の判別式は $D(f^{\mathrm{Sh}}) = \Delta^2$ （$\Delta = \Delta(t) := t^2 + 3t + 9$）であり、$\mathrm{Gal}(f^{\mathrm{Sh}}/\boldsymbol{Q}(t)) = \langle\sigma\rangle \simeq C_3$ の根への作用は $\sigma(\theta) = -\dfrac{1}{1+\theta}$ で、$\theta_{i+1} = \sigma(\theta_i)$ となるように、3 根 $\theta_i$ $(i \in \boldsymbol{Z}/3\boldsymbol{Z})$ の番号付けを決めておく。尚、$f^{\mathrm{Sh}}(t;X) = -X^3 f^{\mathrm{Sh}}(-t-3;X^{-1})$ であるので、$t$ を $-t-3$ に変えても根体は変わらない。

1.1. **冪基底.** $n$ 次代数体 $K$ の整数環 $\mathcal{O}_K$ が $\Theta = (1, \theta, \ldots, \theta^{n-1})$ の形の整数基を持つとき、即ち、$\mathcal{O}_K = \boldsymbol{Z}[\theta]$ となる $\theta \in \mathcal{O}_K$ が存在するとき、$K$ は単生 (monogenic) といい、このときの $\Theta$ を冪基底、$\theta \in \mathcal{O}$ をその生成元と呼ぶ。一般に、$\theta \in \mathcal{O}_K$ に対し、そのモニックな最小多項式を $f(X) \in \boldsymbol{Z}[X]$ とすると、$D(f) = D_K \cdot (\mathcal{O}_K : \boldsymbol{Z}[\theta])^2$ が成り立つ。$\theta$ が $K$ の冪基底の生成元である必要十分条件は、$D_K = D(f)$ である。特に、$D(f)$ が平方無縁 (square-free) であれば、$D(f) = D_K$ かつ $\mathcal{O}_K = \boldsymbol{Z}[\theta]$ となり、$\theta$ は冪基底の生成元となる。しかし、冪基底は常に存在するとは限らない。

さて、$t \in \boldsymbol{Z}$ に対し、$f^{\mathrm{Sh}}(t;X)$ の根体（分解体）$K = K_t$ の判別式を $D_K = D_{K_t}$、整数環を $\mathcal{O} = \mathcal{O}_t$、$f^{\mathrm{Sh}}$ の根の 1 つを $\theta = \theta_t$ とするとき、$\theta$ が $\mathcal{O}$ の冪基底を生成するか、即ち、$\mathcal{O} = \boldsymbol{Z}[\theta] \simeq \boldsymbol{Z}[X]/(f^{\mathrm{Sh}}(t;X))$ であるかどうかを考えよう。上で見たように、

$$D(f^{\mathrm{Sh}}) = \Delta^2 = D_K \cdot (\mathcal{O} : \boldsymbol{Z}[\theta])^2$$

---

第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」報告集原稿.

[1] こうすると、根のノルムが $+1$ になる。

であり、$\Delta$ の素因数分解によっては、$\mathcal{O} \neq \boldsymbol{Z}[\theta]$ となる場合もあるが、PARI/GP などで実験してみると、$\mathcal{O} = \boldsymbol{Z}[\theta]$ となる場合も多いことがわかる。

実際、次が示せる：

**命題 1.1** (Cusick[Cu, Lemma 1])**.** $t \in \boldsymbol{Z}$ で、$\Delta = t^2 + 3t + 9$ が平方無縁のとき、$p|\Delta$ なる素数は $K/\boldsymbol{Q}$ で分岐する。特に、$p|D_K$ となることから、$\mathcal{O} = \boldsymbol{Z}[\theta]$、即ち、$\mathcal{O}$ は冪基底 $(1, \theta, \theta^2)$ を持つ。

**証明** . $p|\Delta$ とする。$\Delta$ が平方無縁なので、$p||\Delta$ である。$3|\Delta \Longleftrightarrow 3|t \Longleftrightarrow 3^2|\Delta$ より、$p \neq 3$ が言える。$Y = X - \dfrac{t}{3}$ と変数変換（立方完成）して、

$$f^{\mathrm{Sh}}(t; Y + \frac{t}{3}) = Y^3 - \frac{1}{3}\Delta Y - \frac{1}{27}(2t+3)\Delta \in \boldsymbol{Z}_p[X]$$

が Eisenstein 型になるので（或いは $p$ 進 Newton 多角形（Appendix A 参照）を考えれば）、$f^{\mathrm{Sh}}(t; Y + \dfrac{t}{3})$ のすべての根の付値が $\dfrac{1}{3}$ であり、$p$ が根体 $K$ で完全分岐することが分かる。従って、$p^2|D_K$ で $p \nmid (\mathcal{O}_K : \boldsymbol{Z}[\theta])$ となる。これが $p|\Delta$ なるすべての $p$ で成り立つので、$(\mathcal{O}_K : \boldsymbol{Z}[\theta]) = 1$ となる。 □

最も簡単な場合は $\Delta = t^2+3t+9 =: p$ が素数のときである[2]。この場合は、$p^2 = D_K \cdot (\mathcal{O} : \boldsymbol{Z}[\theta])^2$ なので、$D_K = 1$ または $D_K = p^2$ であり、数の幾何を用いた Minkowski の定理：$D_K = 1 \Longleftrightarrow K = \boldsymbol{Q}$ を援用して、$D_K > 1$ から $D_K = p^2$ および $\mathcal{O} = \boldsymbol{Z}[\theta]$ が従う、といっても良い。

さて、このとき、$D_K = D(f^{\mathrm{Sh}}) = p^2$ であるから、$K/\boldsymbol{Q}$ では $p$ のみが分岐するので、$K$ は $p$ 分体 $\boldsymbol{Q}(\zeta_p)$ の唯一の 3 次巡回部分体である[3]。円分体論からは、むしろ Gauss の 3 項周期と結びつけるのが自然であろう (Lehmer[L])。

$p$ を $p \equiv 1 \pmod 3$ なる素数とし、$g$ を $\bmod p$ の原始根とするとき、Gauss の 3 項周期 $\eta_i$ は次で与えられる：

$$\eta_i := \sum_{k=0}^{\frac{p-1}{3}-1} \zeta_p^{g^{i+3k}} \qquad (i = 0, 1, 2).$$

これを根とする多項式は

$$F(X) = X^3 + X^2 - \frac{p-1}{3}X - \frac{(L+3)p-1}{27} \in \boldsymbol{Z}[X]$$

（ここに、$L$ は $4p = L^2 + 27M^2, L \equiv 1 \pmod 3$ で定まる。）であり[4]、その判別式は、$D(F) = p^2M^2$ である。$F$ の根体 $K$ は $\boldsymbol{Q}(\zeta_p)$ の唯一の 3 次巡回部分体で、$D_K = p^2$ であるから、$(\mathcal{O} : \boldsymbol{Z}[\eta_0]) = M$ となり、$\eta_i$ が冪基底を与えるのは $M = 1$ の場合に限る。これが最簡 3 次体の場合である。実際、$4p = 4(t^2+3t+9) = (2t+3)^2 + 27$ なので、必要なら $t$ を $-t-3$ に置き換えて $t \equiv 2 \pmod 3$ に取れば、$L = 2t + 3 \equiv 1 \pmod 3$ となり、

$$f^{\mathrm{Sh}}(t; X) = X^3 - tX^2 - (t+3)X - 1 = X^3 - \frac{L-3}{2}X^2 - \frac{L+3}{2}X - 1$$

で、$X = Y + \dfrac{L-1}{6}$ と変換すると、

$$F(Y) = f^{\mathrm{Sh}}(\frac{L-3}{2}; Y + \frac{L-1}{6})$$

であることがわかる。従って、$f^{\mathrm{Sh}}$ の根 $\theta_0 = \theta, \theta_1, \theta_2$ と Gauss の 3 項周期 $\eta_i$ との関係は、

$$\theta_i = \eta_i + \frac{L-1}{6}$$

---

[2] このような $p, t$ が無限個あるかどうかは勿論知られていないが、実験的には結構ある。

[3] 従って $p \equiv 1 \pmod 3$ である筈だが、それは $p = t^2 + 3t + 9$ であることからもわかる。

[4] 2 次の係数は容易にわかる。1 次の係数も工夫して計算すると何とかなる。定数項を直接計算しようとすると Jacobi 和になるのでその決定は難しいが、$F$ が 3 次巡回多項式であることから、判別式が平方数になることを用いて決定することも出来る。

である。

1.2. **単数群.** Shanks の巡回 3 次式

$$f^{\mathrm{Sh}}(t;X) = X^3 - tX^2 - (t+3)X - 1 \in \boldsymbol{Q}(t)[X]$$

の 3 根 $\theta_0, \theta_1, \theta_2$ の間には、その構成から、

$$\theta_{i+1} = -\frac{1}{1+\theta_i}, \qquad \theta_0\theta_1\theta_2 = 1$$

という関係があるのであった。$t \in \boldsymbol{Z}$ の場合には根体 $K = K_t$ の単数であり、$\theta_i$ のうちの任意の 2 つは独立な単数となる。総実 3 次体 $K$ の単数群の階数は 2 なので、まずはこれで階数の分だけの独立な単数を得たことになる。では、これが基本単数系を成すだろうか。

一般に、数の幾何や二次形式の簡約理論（Appendix B 参照）により、判別式を用いて単数規準の下からの評価が得られる（Appendix C 参照）。一方、実二次体の場合を考えても分かるように、一般論による単数規準の上からの評価は非常に困難である。そこで単数が明示的に得られることが非常に重要になる。

さて、今の総実 3 次体の場合には、判別式を用いた単数規準の下からの評価として、次が得られる（Appendix C 参照）：

**定理 1.2** (Cusick[Cu, Theorem 1])**.** 総実 3 次体 $K$ の判別式を $D_K$、単数規準を $R_K$ とするとき、

$$R_K \geq \frac{1}{16}(\log \frac{D_K}{4})^2$$

である。

では、$f^{\mathrm{Sh}}(t;X)$ の 3 根 $\theta_0, \theta_1, \theta_2$ のうちの任意の 2 つを取ると、基本単数系をなすだろうか。少なくとも、$\Delta = t^2 + 3t + 9$ が平方無縁かつ充分大きい $t \in \boldsymbol{Z}$ については、これが成り立つことが示せる。

$f^{\mathrm{Sh}}(t;X)$ の 3 根のうち、唯一の正の根を $\theta = \theta_0$ とすると、$\theta_2 < -1 < \theta_1 < 0 < \theta_0$ となっており、さらに $\theta > t+1$ である。$t$ が小さいときにも結果を得ようとすると、誤差項まで含めた精密な評価や細かい議論、さらに小さいところの有限個を潰すための個別計算などが必要であるが、簡単のため、本稿では $t \in \boldsymbol{Z}$ が充分大きいとき（特に $t > 0$）のみ考え、$t \longrightarrow +\infty$ での漸近挙動だけを見よう。このとき、$\theta = t(1 + o(1))$ である。$\theta_{i+1} = \sigma(\theta_i) = -\dfrac{1}{1+\theta}$ であることに注意すると、$\theta_1 = -t^{-1}(1+o(1)),\ \theta_2 = -1 + o(1)$ であることがわかる。

$\Theta = (\theta_0, \theta_1)$ とし、

$$R(\Theta) = R(\theta_0, \theta_1) := \left|\det \begin{pmatrix} \log|\theta_0| & \log|\sigma(\theta_0)| \\ \log|\theta_1| & \log|\sigma(\theta_1)| \end{pmatrix}\right| = \left|\det \begin{pmatrix} \log|\theta_0| & \log|\theta_1| \\ \log|\theta_1| & \log|\theta_2| \end{pmatrix}\right|$$

とする。単数系 $\Theta$ が $\pm 1$ とともに生成する部分群 $U = U(\Theta) := \langle -1, \theta_0, \theta_1 \rangle \in \mathcal{O}_K^\times$ について、群指数を $i(\Theta) := (\mathcal{O}_K^\times : U(\Theta))$ と書くと、$R(\Theta) = i(\Theta)R_K$ である。$R_K$ の下からの評価は得られている。$R(\Theta)$ を計算して $R(\Theta) < 2R_K$ なら、$R(\Theta) = R_K$ で $\Theta$ が基本単数系を成すことが言える。

$R(\Theta)$ の $t \longrightarrow +\infty$ での漸近挙動を見ると、

$$\begin{aligned} R(\Theta) &= \left|\det \begin{pmatrix} \log|t(1+o(1))| & \log|-t^{-1}(1+o(1))| \\ \log|-t^{-1}(1+o(1))| & \log|-1+o(1)| \end{pmatrix}\right| \\ &= \left|\det \begin{pmatrix} \log t + o(1) & -\log t + o(1) \\ -\log t + o(1) & o(1) \end{pmatrix}\right| \\ &= (\log t)^2 + o(\log t) \end{aligned}$$

となる。一方、$D_K = \Delta^2 = (t^2+3t+9)^2 = t^2(1+o(1))$ より、

$$\begin{aligned}(\log\frac{D_K}{4})^2 &= (2\log(t^2(1+o(1))) - \log 4)^2\\ &= (4\log t - \log 4 + o(1))^2\\ &= 16(\log t)^2 + o((\log t)^2)\end{aligned}$$

となるので、

$$\frac{R(\Theta)}{(\log\frac{D_K}{4})^2} = \frac{(\log t)^2 + o(\log t)}{16(\log t)^2 + o((\log t)^2)} \longrightarrow \frac{1}{16}$$

が従う。特に、十分大きい $t$ に対し、

$$R(\Theta) < \left(\frac{1}{16}+\varepsilon\right)(\log\frac{D_K}{4})^2 < 2R_K$$

となり、$\Theta$ が基本単数系をなすことが言える。また併せて、定理の不等式の定数 1/16 が（下限としても下極限としても）best possible であることもわかる。

## 2. Lehmer の巡回 5 次式

前節の Shanks の巡回 3 次式の 5 次の類似として、$p \equiv 1 \pmod 5$ なる素数 $p$ に関する Gauss の 5 項周期をずらして巡回 5 次体の単数を得ようという狙いから、$p = t^4+5t^3+15t^2+25t+25$ の形の素数に対して、E. Lehmer は次の巡回 5 次多項式を得た：

$$\begin{aligned}f^{\mathrm{Leh}}(t,X) = X^5 + t^2X^4 - 2(t^3+3t^2+5t+5)X^3\\ + (t^4+5t^3+11t^2+15t+5)X^2 + (t^3+4t^2+10t+10)X + 1.\end{aligned}$$

これは実際、$p = t^4+5t^3+15t^2+25t+25$ が素数かどうかに関わりなく、$\boldsymbol{Q}(t)$ 上の $C_5$ 多項式となっている（生成的ではない）。

有理関数体 $\boldsymbol{Q}(t)$ 上の多項式として成り立っていることをまとめておく。$f^{\mathrm{Leh}}$ の判別式は

$$D(f^{\mathrm{Leh}}) = \Delta_0(t)^2\Delta_1(t)^4$$

（ここに、$\Delta_0 = \Delta_0(t) := t^3+5t^2+10t+7, \Delta_1 = \Delta_1(t) := t^4+5t^3+15t^2+25t+25$）であり、残念ながら $\Delta_1$ の冪だけではないが、

$$(t^3+5t^2+10t+18)\Delta_0(t) - (t^2+5t+5)\Delta_1(t) = 1$$

となることから、この 2 つの因子が（$t \in \boldsymbol{Z}$ に特殊化した後でも）互いに素であることに注意しておこう。$\mathrm{Gal}(f^{\mathrm{Leh}}/\boldsymbol{Q}(t)) = \langle\sigma\rangle \simeq C_5$ の根への作用は

$$\sigma(\theta_i) = \frac{(t+2)+t\theta-\theta^2}{1+(t+2)\theta}$$

である（[ScWa] [5]）。$\theta_{i+1} = \sigma(\theta_i)$ となるように、5 根 $\theta_i$ $(i \in \boldsymbol{Z}/5\boldsymbol{Z})$ の番号付けを取ることにする。

以下、本節では、最終節を除いて、$t \in \boldsymbol{Z}$ に特殊化したときの根体（＝分解体）$K = K_t$ を考える。$t \in \boldsymbol{Z}$ のときは、mod2 で既約なことから、$f^{\mathrm{Leh}}(t,X) \in \boldsymbol{Z}[X]$ は常に既約である。また、根 $\theta = \theta_t$ は $K$ の単数になる。

[5] 小さい $n$ について数値計算して係数を求めて帰納した、と書いてある。わかってしまえば確かめるのは（計算代数ソフトウェアを使えば）簡単。

2.1. **判別式・整数環.** $t \in \boldsymbol{Z}$ に特殊化し、その根 $\theta = \theta_t$ および根体（分解体）である巡回5次体 $K = K_t = \boldsymbol{Q}(\theta_t)$ を考える。判別式 $D_K$ を決定するため、$p|D(f) = \Delta_0(t)^2\Delta_1(t)^4$ なる素数 $p$ での分岐状況を見よう。$K$ で素数 $p$ が分岐するとき、完全分岐（分岐指数 5）であるから、$p^4|D_K$ （$p \neq 5$ なら $p^4||D_K$）である。

まず、$p|\Delta_0(t)$ の場合には、$v_p(\Delta_0(t)) = a$ 即ち $p^a||\Delta_0(t)$ とおいて、

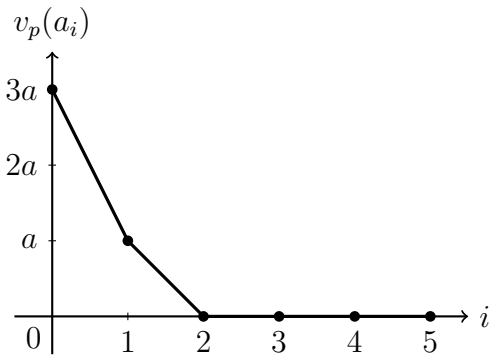
$$\begin{aligned} f^{\mathrm{Leh}}&(t; Y - (t^2+3t+4)) \\ &= Y^5 - (4t^2+15t+20)Y^4 - 2(t^2+4t+5)(3t^2+11t+15)Y^3 \\ &\quad - (4t^6+48t^5+251t^4+733t^3+1261t^2+1215t+515)Y^2 \\ &\quad + (t^5+13t^4+63t^3+156t^2+200t+110)\Delta_0(t)Y - \Delta_0(t)^3 \in \boldsymbol{Z}[X] \end{aligned}$$

の $p$ 進 Newton 多角形を考えると、根の付値が $0, 0, 0, a, 2a$ であることがわかり、付値がすべて整数なので、$p$ は $K/\boldsymbol{Q}$ で不分岐である。特に、$p \nmid D_K$ であり、$p|(\mathcal{O}_K : \boldsymbol{Z}[\theta])$ となる。従って、$f^{\mathrm{Leh}}$ を用いて冪基底に関する結果を得るのは難しい。これだけでも、前節の Shanks の巡回3次式が非常に簡明で有難かったことがわかるだろう。

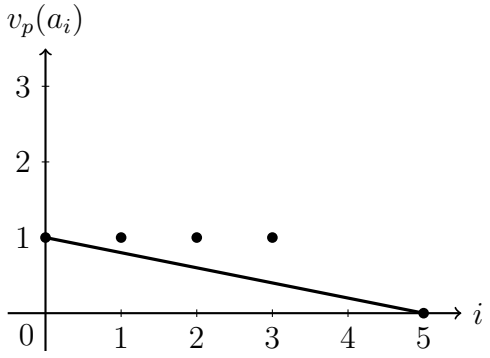
一方、$p||\Delta_1(t)$ の場合には、$5|\Delta_1(t) \Longrightarrow 5|t \Longrightarrow 5^2||\Delta_1(t)$ より $p \neq 5$ であり、$Y = X + \dfrac{t^2}{5}$ と変数変換（5乗完成）して、

$$\begin{aligned} f^{\mathrm{Leh}}(t; Y - \frac{t^2}{5}) &= Y^5 - \frac{2}{5}\Delta_1(t)Y^3 + \frac{1}{25}(4t^2+10t+5)\Delta_1(t)Y^2 \\ &\quad - \frac{1}{125}(3t^4+15t^3+20t^2-50)\Delta_1(t)Y \\ &\quad - \frac{1}{3125}(4t^6+30t^5+65t^4-200t^2-125t+125)\Delta_1(t) \in \boldsymbol{Z}_p[X] \end{aligned}$$

が Eisenstein 型になるので（或いは $p$ 進 Newton 多角形を考えれば）、根の付値が $1/5$ であり、$p$ が $K$ で完全分岐する。従って、$\Delta_1(t)$ が平方無縁であれば、$D_K = \Delta_1(t)^4$ かつ $(\mathcal{O}_K^{\times} : \boldsymbol{Z}[\theta]) = \Delta_0(t)$ とわかる。




$f^{\mathrm{Leh}}(t; Y - (t^2+3t+4)),\ p^a||\Delta_0(t)$
の $p$ 進 Newton 多角形




$f^{\mathrm{Leh}}(t; Y - \dfrac{t^2}{5}),\ p||\Delta_1(t)$
の $p$ 進 Newton 多角形

元々の $p = \Delta_1(t) = t^4+5t^3+15t^2+25t+25$ が素数の場合には、$p \equiv 1 \pmod 5$ であって、$K$ は円分体 $\boldsymbol{Q}(\zeta_p)$ の唯一の 5 次巡回部分体である。その構成から、根 $\theta_i$ と Gauss の5項周期

$$\eta_i := \sum_{k=0}^{\frac{p-1}{5}-1} \zeta_p^{g^{i+5k}} \qquad (i = 0, \ldots, 4)$$

（$g$ は $\bmod p$ の原始根）との間には、（適切な番号付の下に）次の関係がある (Lehmer[L])：

$$\theta_i = \left(\frac{t}{5}\right)\eta_i - \frac{1}{5}\left(t^2 - \left(\frac{t}{5}\right)\right) \quad .$$

尚、正規整数基に関しては、次の結果がある (Spearman-Williams[SpWi])：

**定理 2.1** (Spearman-Williams)**.** $n \in \boldsymbol{Z}$ とする。$5 \nmid n$ かつ $\Delta_1(n)$ が平方無縁のとき、$K$ は $\theta + \frac{1}{5}\left(t^2 - \left(\frac{t}{5}\right)\right)$ の共役系からなる正規整数基をもつ。

2.2. **単数群.** $t \in \boldsymbol{Z}$ に特殊化したとき、$f^{\mathrm{Leh}}(t, X)$ の根 $\theta = \theta_0, \theta_1, \ldots, \theta_4$ は $K$ の単数であり、そのうち任意の 4 つは独立な単数となる。従って、単数群 $\mathcal{O}_K^\times$ の階数一杯（階数 4）の部分群を生成する。では、これが基本単数系を成すだろうか。Schoof-Washington[ScWa] の結果を紹介する。

**定理 2.2** (Schoof-Washington)**.** $p = \Delta_1(t) = t^4 + 5t^3 + 15t^2 + 25t + 25$ が素数のとき、$f^{\mathrm{Leh}}(t, X)$ の根は単数群 $\mathcal{O}_K^\times$ を生成する。特に、単数規準 $R_K$ は、

$$R_K = |\det(\log|\theta_{i+j}|)_{1\le i,j\le 4}| \quad .$$

**注 2.3.** この結果を用いて、[ScWa] では、類数公式

$$h_K R_K = \frac{1}{16}\prod_{\chi\neq 1}\sqrt{p}L(1,\chi)$$

（ここに $\chi$ は非自明な指標 $\mathrm{Gal}(K/\boldsymbol{Q}) \longrightarrow \boldsymbol{C}^\times$ を亘る）、および $R_K = R(\theta)$ と $L(1,\chi)$ の数値計算から、$K$ の類数 $h_K$ を計算している。$L(1,\chi)$ の計算には Gauss 和（Gauss 周期の線型結合）が現れるが、そこでも Gauss 周期を計算する代わりに $f^{\mathrm{Leh}}(t, X)$ の根を用いている。特に、この場合には $R_K$ が小さいので、大きい $h_K$ が現れる。例えば、$p = 641491$ $(t = 27)$ のとき、$h_K = 1566401$（素数）であり、$p$ 分体 $\boldsymbol{Q}(\zeta_p)$ の最大実部分体 $\boldsymbol{Q}(\zeta_p)^+$ の類数 $h_p^+ = h_{\boldsymbol{Q}(\zeta_p)^+}$ が $p$ より大きい素数で割れる例を提供している ([ScWa, Theorem 4.1])。これより、$h_p^+$ の素因子の大きさを上から評価するだけでは、Vandiver 予想 $p \nmid h_p^+$ が証明できないことがわかる。

さて、上の定理を示すために、まず、巡回 5 次体の単数規準に関する次の下からの評価を示す：

**命題 2.4** ([ScWa, Corollary 2.7])**.** 巡回 5 次体 $K$ の導手を $f_K$、単数規準を $R_K$ とするとき、

$$R_K \ge \frac{1}{5^2}(\log\frac{f_K}{2})^4 \quad .$$

（尚、判別式 $D_K$ で書くと、$D_K = f_K^4$ なので、$R_K \ge \frac{1}{2^8 5^2}(\log\frac{D_K}{2^4})^4$ である。）

そのために、格子の最短ベクトルの大きさを評価する（Appendix B 参照）：

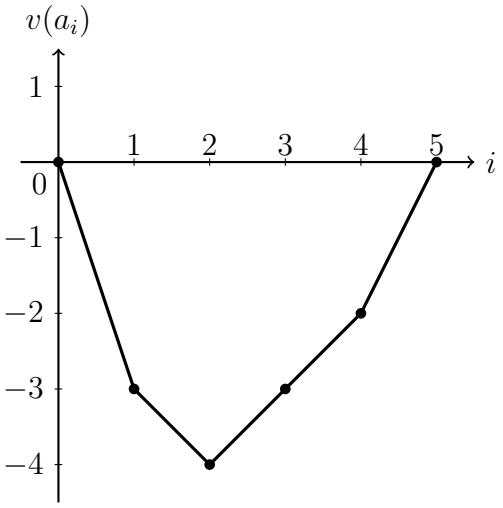
**定理 2.5** ([ScWa, Theorem 2.2])**.** $V = \boldsymbol{R}^4$ を 4 次元実 Euclid 空間 $(|\cdot|)$、$L \subset V$ を $V$ の格子とし、5 次巡回群 $G = \langle\sigma\rangle$ が $V$ に等距離的に作用して、$L$ が $G$ 作用で安定とし、ノルム $N = \sum_{\tau\in G}\tau$ が $V$ を消す（$N(V) = \{\boldsymbol{0}\}$）とする。このとき、

$$|\boldsymbol{x}| \le 2^{\frac{1}{2}}5^{-\frac{1}{8}}\det(L)^{\frac{1}{4}}$$

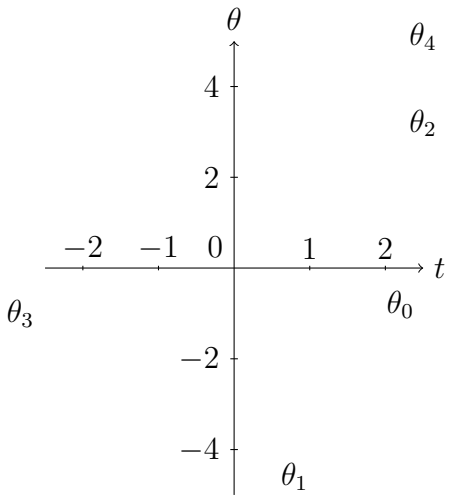
となる $\boldsymbol{x} \in L \smallsetminus \{\boldsymbol{0}\}$ が存在する。

**注 2.6.** $K$ が単なる総実 5 次体でなく、巡回 5 次体であることから、Galois 群 $G = \mathrm{Gal}(K/\boldsymbol{Q})$ が等距離的に作用することを念頭に置いた設定にして、一般の格子に対する Hermite 定数による評価 $|\boldsymbol{x}| \le \gamma_4^{\frac{1}{2}}\det(L)^{\frac{1}{4}}$ よりも良い評価を得ている。実際、$2^{\frac{1}{2}}5^{-\frac{1}{8}} = 1.156\cdots < \gamma_4^{\frac{1}{2}} = 2^{\frac{1}{4}} = 1.189\cdots$ である。

さて一方、$f^{\mathrm{Leh}}(t, X)$ の根 $\theta = \theta_0, \theta_1, \ldots, \theta_4$ のうち任意の 4 つを取ると $K$ の基本単数系を成すだろうか。ここでも前節と同様に、本稿では充分大きい $t$ のみ考えることにして、$t \longrightarrow +\infty$ のときの漸近挙動だけを見るに留める。根の増大度を調べるため、$\boldsymbol{Q}(t) \hookrightarrow \boldsymbol{Q}((t^{-1}))$ と埋込んで、$t^{-1}$ 進 Newton 多角形を見ると、根の $t^{-1}$ 進付値が $3, 1, -1, -1, -2$ であることがわかる。




$f^{\mathrm{Leh}}(t,X)$ の $t^{-1}$ 進 Newton 多角形




$f^{\mathrm{Leh}}(t,\theta)=0$ のグラフ

ここで

$$\theta_{i+1}=\sigma(\theta_i)=\frac{(t+2)+t\theta_i-\theta_i^2}{1+(t+2)\theta_i}$$

であるので、これらの根が $C_5=\langle\sigma\rangle$ の作用に関して移る順番は、根の付値が $1\to-2\to-1\to3\to-1\to1$ の順であることがわかり、付値が $1$ のものを $\theta=\theta_0$ に選べば、

$$\theta_0=t^{-1}(-1+o(1)),\qquad \theta_1=t^2(-1+o(1)),\qquad \theta_2=t(1+o(1)),$$
$$\theta_3=t^{-3}(-1+o(1)),\qquad \theta_4=t(1+o(1))$$

となることがわかる。これより、$\log|\theta_0|=-\log t+o(1)$, $\log|\theta_1|=2\log t+o(1)$, $\log|\theta_2|=\log t+o(1)$, $\log|\theta_3|=-3\log t+o(1)$, $\log|\theta_4|=\log t+o(1)$ であるので、$\Theta=(\theta_0,\theta_1,\theta_2,\theta_3)$ に対する $R(\Theta)$ の漸近挙動は、

$$\begin{aligned}
R(\Theta)&=|\det(\log|\theta_{i+j}|)_{0\le i,j\le3}|\\
&=\left|\det\begin{pmatrix}-\log t+o(1) & 2\log t+o(1) & \log t+o(1) & -3\log t+o(1)\\ 2\log t+o(1) & \log t+o(1) & -3\log t+o(1) & \log t+o(1)\\ \log t+o(1) & -3\log t+o(1) & \log t+o(1) & -\log t+o(1)\\ -3\log t+o(1) & \log t+o(1) & -\log t+o(1) & 2\log t+o(1)\end{pmatrix}\right|\\
&=\left|\det\begin{pmatrix}-1 & 2 & 1 & -3\\ 2 & 1 & -3 & 1\\ 1 & -3 & 1 & -1\\ -3 & 1 & -1 & 2\end{pmatrix}\right|\cdot(\log t)^4+o((\log t)^4)\\
&=71(\log t)^4+o((\log t)^4)
\end{aligned}$$

となる。

また、$p=\Delta_1(t)=t^4+5t^3+15t^2+25t+25$ が素数のとき、導手は $f_K=p=t^4(1+o(1))$ であるから、

$$\begin{aligned}
(\log\frac{f_K}{2})^4&=(\log(t^4(1+o(1))-\log2)^4\\
&=(4\log t-\log2+o(1))^4\\
&=2^8(\log t)^4+o((\log t)^4)
\end{aligned}$$

となるので、

$$\frac{R(\Theta)}{(\log \frac{f_K}{2})^4} = \frac{71(\log t)^4 + o((\log t)^4)}{2^8(\log t)^4 + o((\log t)^4)} \longrightarrow \frac{71}{2^8}$$

が従う。

一方、

$$\frac{R_K}{(\log \frac{f_K}{2})^4} \geq \frac{1}{5^2}$$

であったので、充分大きい $t$ に対し、

$$\frac{R(\Theta)}{R_K} \leq 5^2 \cdot \left(\frac{71}{2^8} + \varepsilon\right) < 7$$

が言える[6]。Hermite 定数の改良など頑張ったが、言えたのは $i(\Theta) = (\mathcal{O}_K^\times : U(\Theta)) = \dfrac{R(\Theta)}{R_K} < 7$ までで、$i(\Theta) < 2$ までは絞れていない。そこで、$\mathcal{O}_K^\times/U(\Theta)$ への Galois 作用から $\boldsymbol{Z}[C_5]/N \simeq \boldsymbol{Z}[\zeta_5]$ 加群の構造が入るので、その位数 $i(\Theta)$ に制約がかかることを利用して、$i(\Theta) = 1$ まで絞り込んでいる。

2.3. **不分岐 2 次拡大.** $t \in \boldsymbol{Z}$ のとき $f^{\mathrm{Leh}}(t, X)$ の根 $\theta = \theta_t$ は単数なので、$K(\sqrt{\theta})/K$ は奇素数 $p$ の上で不分岐である。従って、あとは 2 と無限素点の上で不分岐、かつ $K(\sqrt{\theta}) \neq K$ であれば、$K$ の不分岐 2 次拡大が得られ、特に、$K$ の類数 $h_K$ について 2 による可除性 $2|h_K$ が得られる。しかしながら、PARI/GP を用いて実験的に相対判別式 $D(K(\sqrt{\theta})/K) = D_{K(\sqrt{\theta})}D_K^{-2}$ を計算してみると、($|t| < 100$ くらいまで計算した範囲では[7]) $D(K(\sqrt{\theta})/K) = -2^{10}$ となって、$K(\sqrt{\theta})/K$ で 2 が分岐してしまうようである。ここで、$D(K(\sqrt{\theta})/K) < 0$ となって気付くのは、無限素点については、そもそも $\mathrm{tr}_{K/\boldsymbol{Q}}(\theta) = -t^2 \leq 0, N_{K/\boldsymbol{Q}}(\theta) = -1 < 0$ なので、総正ではあり得なかった。しかしそこで $K(\sqrt{-\theta})/K$ を考えて計算してみても、同じ $t$ の範囲で $D(K(\sqrt{-\theta})/K) = 2^{10}$ となってしまい、不分岐 2 次拡大が得られない。

そんな状況の中で、特殊化する $t$ の値の範囲を $t \in \boldsymbol{Q}$ まで拡げることで、中野 [N] は次を示した：

**定理 2.7.** 無限に多くの $t \in \boldsymbol{Q}$ に対し、$K(\sqrt{\theta(\theta - t - 1)})$ は $K$ 上の不分岐 2 次拡大であり、これにより、不分岐 2 次拡大を持つ巡回 5 次体の無限族を得る（即ち、相異なるものが無限個現れる）。

実際には、$t \in \boldsymbol{Q}$ は次のように取れる：楕円曲線 $E : U^2 = T^3 + 5T^2 + 10T + 7$（Cremona リストの `368e1`）の Mordell-Weil rank は 1 で、$E(\boldsymbol{Q}) = \langle P \rangle \simeq \boldsymbol{Z}$（ここに $P = (-1, 1)$）であり、$P$ の奇数倍点 $(t, u) \in E(\boldsymbol{Q}) \smallsetminus [2]E(\boldsymbol{Q})$ の $t$ 座標 $t \in \boldsymbol{Q}$ を取ればよい。ここに $\Delta_0(T) = f^{\mathrm{Leh}}(T, T + 1) = T^3 + 5T^2 + 10T + 7$ であることに注意する（というかそのようにして現れる）。

まず、$K(\sqrt{\theta})/K,\ K(\sqrt{\theta - t - 1})/K$ ともに奇素数の上のすべての有限素点で不分岐であることを示す。$t$ の分母を割らない奇素数 $p$ については、根 $\theta$ は $p$ 進単数なので、$K(\sqrt{\theta})/K$ で不分岐。また、$\theta - t - 1$ は

$$\begin{aligned} f^{\mathrm{Leh}}(t, X + t + 1) = {} & \\ & X^5 + (t^2 + 5t + 5)X^4 + 2t(t^2 + 4t + 5)X^3 + (t^4 + 3t^3 - t^2 - 15t - 15)X^2 \\ & - (t^4 + 7t^3 + 18t^2 + 20t + 5)X + (t^3 + 5t^2 + 10t + 7) \end{aligned}$$

の根なので、$(t, u) \in E(\boldsymbol{Q})$ であることから付値が偶数であり、$K(\sqrt{\theta - t - 1})/K$ でも不分岐。$t$ の分母を割る奇素数 $p$ については、$t$ の分母が平方数であることと、Newton 多角形（Appendix A 参照）を見て根の付値が偶数であることを見る。無限素点の不分岐性

[6] [ScWa] では、小さい $t$ にも通用するように誤差項も含めた評価を考えているため、ここの評価が 11 未満に留まっている。

[7] 一般的にも決定できそうなので、良い演習問題であろう。

のために組み合わせて、総正な元 $\theta(\theta-t-1)$ を考える。2 の上での不分岐性には $P$ の奇数倍点であることが効いている。以上により、$K(\sqrt{\theta(\theta-t-1)})/K$ は不分岐で、これが真に 2 次拡大 $(K(\sqrt{\theta(\theta-t-1)}) \neq K)$ となるためには、ここで惰性する素数を見つければ良い。無限性には Chebotarev の密度定理を用いる。以上を併せて所望の結果を得る。

## 3. Brumer の二面体型 5 次式

前節までは、巡回拡大体（特に Galois であり abel）であったので、円分体から外に出ない話であった[8]。もっと野趣溢れる非 Galois・非 abel 拡大の場合にも、明示的な多項式の力を借りて、“密林・迷宮の探検”([H2]) に出掛けよう、というのである。

まずはじめに、[T*, §4.1] を振り返って、Brumer の $D_5$ 多項式

$$f^{D_5}(a,b;X) = X^5 + (a-3)X^4 + (b-a+3)X^3 + (a^2-a-1-2b)X^2 + bX + a$$

について、$a, b$ を不定元とした有理関数体 $k := \boldsymbol{Q}(a,b)$ 上の多項式として成り立つ基本的な性質をまとめておこう。判別式は $D(f^{D_5}) = a^2 D_1(a,b)^2$ で、ここに

$$D_1(a,b) = \\ -4b^3 + (a^2-30a+1)b^2 + 2a(12a^2-17a-7)b - a(4a^4-4a^3-40a^2+91a-4)$$

であった。また、有理関数体 $k = \boldsymbol{Q}(a,b)$ 上の分解体（根体 $K = k(\theta)$ の Galois 閉包）$\widetilde{K}$ は $k$ の $D_5$ 拡大であり、$G = \mathrm{Gal}(\widetilde{K}/k) = D_5$ の唯一の 5 次巡回部分群 $C_5$ の固定体（$\widetilde{K}$ に含まれる唯一の $k$ の 2 次拡大）が $k(\sqrt{D_1(a,b)})$ であることが、$C_5$ 不変体の考察からわかる[9]。

さて、$a = \pm 1$ に特殊化した多項式

$$f_{1,b}(X) := f^{D_5}(1,b;X) = X^5 - 2X^4 + (b+2)X^3 - (2b+1)X^2 + bX + 1$$
$$f_{-1,b}(X) := f^{D_5}(-1,b;X) = X^5 - 4X^4 + (b+4)X^3 - (2b-1)X^2 + bX - 1$$

は、判別式が簡明かつ $b \in \boldsymbol{Z}$ のとき根が単数になるので、興味深い上に計算がしやすい場合である。以下、本節では専らこの場合に得られている結果を紹介する。最終節を除いて、$b \in \boldsymbol{Z}$ に特殊化したときの根体 $K = K_b$ を考える。

### 3.1. 判別式・整数環.

$a = 1$ に特殊化した多項式 $f_{1,b}$ の根を $\theta = \theta_b$、根体を $K = K_b$、分解体を $\widetilde{K} = \widetilde{K}_b$ としよう。$f_{1,b}$ の判別式は、

$$D(f_{1,b}) = D_1(1,b)^2, \qquad D_1(1,b) = -4b^3 - 28b^2 - 24b - 47$$

であり、$D_1(1,b)$ が平方数なら $\widetilde{K} = K$ で 5 次巡回拡大に退化するが、そうでなければ、$\widetilde{K}$ は $D_5$ 拡大で、その唯一の 2 次中間体 $F$ は $F = \boldsymbol{Q}(\sqrt{D_1(1,b)})$ である。$D_1(1,b) \equiv 1 \pmod 4$ なので、2 は $F/\boldsymbol{Q}$ で不分岐。

**命題 3.1.** *$p$ が $K/\boldsymbol{Q}$ で不分岐ならば、$F/\boldsymbol{Q}$ でも不分岐。$D_1 = D_1(1,b)$ が平方無縁であれば、逆も成り立つ。*

**証明 .** $D_1 = d^2\Delta$（$\Delta$ は平方無縁）とすると、$p : K/\boldsymbol{Q}$ で不分岐 $\Longrightarrow p : \widetilde{K}/\boldsymbol{Q}$ で不分岐 $\Longrightarrow p : F/\boldsymbol{Q}$ で不分岐 $\Longrightarrow p \nmid \Delta$ で、$D_1$ が平方無縁であれば、$d = 1$ なので $p \nmid D_1 \Longrightarrow p \nmid D_K \Longrightarrow p : K/\boldsymbol{Q}$ で不分岐、まで戻れる。

**注 3.2.** $D_1(1,b)$ が平方因子 $p^2$ で割れるときは、$p$ が $K/\boldsymbol{Q}$ で完全分岐して、$F/\boldsymbol{Q}$ では不分岐、ということがある。例：$b = 4$ のとき $f_{-1,4}(X) = X^5 - 2X^4 + 6X^3 - 9X^2 + 4X + 1$ で、$D_1(f_{-1,4}) = -7 \cdot 11^2$ である。$F = \boldsymbol{Q}(\sqrt{-7 \cdot 11^2}) = \boldsymbol{Q}(\sqrt{-7})$ で 11 は不分岐。一方、$f_{-1,4}(Y-4) = Y^5 - 11(2Y^4 - 18Y^3 + 83Y^2 - 196Y + 189)$ が 11 に関して Eisenstein 型なので、$K/\boldsymbol{Q}$ で 11 は完全分岐。7 は $K/\boldsymbol{Q}, F/\boldsymbol{Q}$ の両方で分岐し、$\widetilde{K}/\boldsymbol{Q}$ での分岐指数は 2 。

[8] だからこそ Gauss 周期とも関連して面白かった、とも言えるが。

[9] この意味で $D_1(a,b)$ の符号の選択は標準的なものが定まっていると言える。

**定理 3.3** (Lavallee-Spearman-Williams-Yang [LSWY])**.** 無限に多くの $b \in \boldsymbol{Z}$ に対し、$f_{1,b}$ の根体 $K = \boldsymbol{Q}(\theta)$ は相異なる単生な二面体型 5 次体である。

**証明 .** $D_1(1,b)$ が平方無縁であれば、$p|D_1(1,b)$ なる素数は $F = \boldsymbol{Q}(\sqrt{D_1(1,b)})$ で分岐し、従って $K$ でも分岐するので、$p|D_K$ となる。$p^2||D_1(1,b)^2 = D(f_{1,b}) = D_K \cdot (\mathcal{O}_K : \boldsymbol{Z}[\theta])^2$ より、$p \nmid (\mathcal{O}_K : \boldsymbol{Z}[\theta])$ が言えて、これがすべての $p|D(f_{1,b})$ で言えるので、$(\mathcal{O}_K : \boldsymbol{Z}[\theta]) = 1$ となり、$\theta$ が $K$ の冪基底の生成元になる。$D_1(1,b)$ が平方無縁になる $b \in \boldsymbol{Z}$ は、Erdös[E] により無限にある（Appendix D 参照)。 □

3.2. **単数群.** $K$ の単数群について、総実代数体のときの [ScWa] の方法の類似を辿り、Kihel[Ki] は次を示した[10]：

**定理 3.4** (Kihel[Ki, Théorème 3.6, Corollaire 3.2])**.** $D_1(1,b)$ が平方無縁であるような充分大きい $b \in \boldsymbol{Z}$ （従って $K$ の符号数は $(r_1, r_2) = (1,2)$ で $\widetilde{K}$ は総虚）に対し、$f_{1,b}$ の根 $\theta = \theta_0, \theta_1, \ldots, \theta_4$ のうち任意の 4 つの成す系 $\Theta$ は $\widetilde{K}$ の基本単数系となる。また、このとき、$(\theta, 1-\theta)$ は $K$ の基本単数系となる。

前節の巡回 5 次体における基本単数系の決定と同様な方法で、総虚 $D_5$ 拡大体 $\widetilde{K}$ の単数規準の下からの評価と、$\mathcal{O}_{\widetilde{K}}^{\times}/U(\Theta)$ の $\boldsymbol{Z}[\zeta_5]$ 加群構造による $i(\Theta) = (\mathcal{O}_{\widetilde{K}}^{\times} : U(\Theta))$ の値の制約とを併せて、この結果を得る。

3.3. **不分岐 $(2,2)$ 拡大.** 前節で紹介した Lehmer の巡回 5 次式に関する中野 [N] の結果に触発され、$f^{D_5}$ の根 $\theta$ の平方根添加により、根体 $K = \boldsymbol{Q}(\theta)$ 上の不分岐 2 次拡大 $K(\sqrt{\theta})/K$ が得られないか、と考えたことから得た結果（加藤, 角皆 [Ka, T]）を紹介する。

ここでは、$a = -1$ に特殊化した多項式

$$f_{-1,b}(X) = f^{D_5}(-1, b; X) = X^5 - 4X^4 + (b+4)X^3 - (2b-1)X^2 + bX - 1$$

を考える。判別式は $D(f_{-1,b}) = D_1(-1,b)^2$（ここに、$D_1(-1,b) = -4b^3 + 32b^2 - 44b - 127$）であり、$D_1(-1,b)$ は唯一の実根 $\beta = -1.346\cdots$ を持つ。$b < \beta$ のとき、$f_b$ は 5 実根を持ち $K$ は総実だが、$b > \beta$ のとき、$f_b$ は 1 実根と 2 対の虚根を持ち符号数 $(r_1, r_2) = (1,2)$ で単数群の階数は $r_1 + r_2 - 1 = 2$ である。

$b \in \boldsymbol{Z}$ のとき $f(X) = f_{-1,b}(X)$ の根 $\theta = \theta_b$ は単数なので、$K(\sqrt{\theta})/K$ は奇素数 $p$ の上で不分岐である。$b > \beta$ であれば $f$ は実根がただ一つで正（実際 $0 < \theta < 1$）なので、$\theta$ は総正[11]。で、無限素点も $K(\sqrt{\theta})/K$ で不分岐。後は 2 の上の素点も不分岐かつ $K(\sqrt{\theta}) \neq K$ であれば、$K$ の不分岐 2 次拡大が得られ、特に、$K$ の類数 $h_K$ について 2 による可除性 $2|h_K$ が得られる。しかしながら、PARI/GP を用いて実験的に相対判別式 $D(K(\sqrt{\theta})/K) = D_{K(\sqrt{\theta})} D_K^{-2}$ を計算してみると、($|t| < 100$ くらいまで計算した範囲では[12]) $D(K(\sqrt{\theta})/K) = 2^{10}$ となって、$K(\sqrt{\theta})/K$ で 2 が分岐してしまうようであった。

ここまでは $b \in \boldsymbol{Z}$ で考えてきたが、ここからは探索範囲を $b \in \boldsymbol{Q}$ に拡げざるを得ない。但し奇素数と無限素点での状況を変えたくないので、$b > \beta$ かつ $b \in \boldsymbol{Z}[\frac{1}{2}]$ 即ち $b = \dfrac{m}{2^\nu}$ の形で試すことを考えた。加藤 [Ka] による精力的な実験観察により、$\nu = 4n+2$, $n \geq 1$, $m \equiv 1 \pmod 8$ のときに $D(K(\sqrt{\theta})/K) = 1$ 即ち $K(\sqrt{\theta})/K$ が不分岐になることが観察された[13]。さらに、$1-\theta = \alpha(\theta)\alpha^{-1}(\theta)$ も $K$ 内の単数であることから、最終的には次の結果に至った：

---

[10][Ki] にある多項式 $p(x) = x^5 - Sx^4 + (T+S+5)x^3 - (S^2+S-2T-5)x^2 + (T+2S+5)x - (S+3)$ と本稿の $f^{D_5}$ との関係は、$p(x) = -f^{D_5}(S+3, T+2S+5; -x)$ である。従って、[Ki] で扱っている $S = -2, -4$ の場合は、それぞれ $f^{D_5}$ では $a = 1, -1$ に相当し、$f^{D_5}$ の根 $\theta$ に対し、$-\theta$ が $p(x)$ の根になる。多項式の明示形を用いる場合、この手のことがしばしばあるので要注意。

[11]総実 ($b < \beta$) の場合に出来ると面白いのだが、このときは負の根が 2 個、$0 < \theta < 1$ なる根が 1 個、$\theta > 1$ なる根が 2 個なので、うまく組み合わせても総正な単数を得るのは難しい。

[12]一般的にも決定できそうなので、良い演習問題であろう。

[13]中野 [N] の結果を勉強した後だったので、合同条件で明快に規定されてしまうのは衝撃的な観察結果であった。その後、修論完成に向けての共同研究で、未整理ながら証明までは辿り着いたが、進学せずに数学の研究から離れてしまったため、証明の道筋の整理や結果の改良には加われず、[T] を共著論文に出来なかったのは残念であった。彼の貢献を特にここに記しておきたい。

**定理 3.5** (角皆 [T, Theorem A])**.** $n$ を正整数、$m \in \boldsymbol{Z}$ を $m \equiv 1 \pmod 8$ なる整数で、$\dfrac{m}{2^{4n+2}} > \beta$ を満たすものとする。$f(X) := f^{D_5}(-1, \dfrac{m}{2^{4n+2}}; X)$ とおくと既約で、その根を $\theta$ とし、根体を $K = K_{n,m} = \boldsymbol{Q}(\theta)$ とする。このとき、$L = K(\sqrt{\theta}, \sqrt{1-\theta})$ とすると、

(1) $K$ は二面体型 5 次体で、$L/K$ は不分岐。
(2) さらに $m \equiv 9 \pmod{16}$ ならば[14]、$L/K$ は $(2,2)$ 型。
(3) $n$ を固定する毎に、族

$$\{K_{n,m} \,|\, m \equiv 9\,(\mathrm{mod}16), m > 0\}$$

は不分岐 $(2,2)$ 拡大を持つ二面体型 5 次体の無限族を成す。

また、定理の状況下で $K$ の Galois 閉包 $\widetilde{K}$ を考えると、$L$ の Galois 閉包 $\widetilde{L}$ は $\widetilde{K}$ 上不分岐であり、さらに $\widetilde{L}^\sharp := \widetilde{L}(\sqrt{-1})$ とおくと、

**定理 3.6** (角皆 [T, Theorem B])**.** $n$ を正整数、$m \in \boldsymbol{Z}$ を $m \equiv 9 \pmod{16}$ なる整数で、$\dfrac{m}{2^{4n+2}} > \beta$ を満たすものとする。このとき、$\widetilde{L}^\sharp$ は $\widetilde{K}$ の不分岐 $(\boldsymbol{Z}/2\boldsymbol{Z})^5$ 拡大。従って、$\widetilde{K}$ のイデアル類群の 2-rank は 5 以上で、$\widetilde{K}$ の類数は 32 で割れる。

さらに、 $n$ を固定する毎に、族

$$\left\{\widetilde{K}_{n,m} \,\middle|\, m \equiv 9\,(\mathrm{mod}16), m > 0\right\}$$

は、不分岐 $(\boldsymbol{Z}/2\boldsymbol{Z})^5$ 拡大を持つ $D_5$ 拡大の無限族を成す。

## 4. Brumer の $\mathfrak{A}_5$ 型 6 次式

先立つ稿 [T*, 注 3] でも触れたように、Brumer は 3 助変数で 6 次の生成的 $\mathfrak{A}_5$ 多項式を得ているが、我々は複比の体での有理性問題に関する考察から、その部分族ながら生成的な 2 助変数の 6 次生成的 $\mathfrak{A}_5$ 多項式

$$f_6^{\mathfrak{A}_5}(u,v;X) = X^6 - 2(u+1)X^5 + (u^2+1)X^4 - vX^3 + (u^2-2u+2)X^2 - 2(u-2)X + 1$$

を得た。非可換単純群 $\mathfrak{A}_5$ を Galois 群に持つ多項式としては充分に簡明であって、しかも $f_6^{\mathfrak{A}_5}(u,v;X) \in \boldsymbol{Z}[u,v][X]$ かつモニックで定数項が 1 なので、$u, v \in \boldsymbol{Z}$ に特殊化すると、根 $\theta = \theta_{u,v}$ が単数になる。諸々の実験的考察や実例の提供に役立てたいところであるが、まだ計算例などは余り多くないようであり、今後の活用が待たれる[15]。

4.1. **判別式・整数環.** $f_6^{\mathfrak{A}_5}$ の判別式は $D(f_6^{\mathfrak{A}_5}) = D_2(u,v)^2$、ここに

$$\begin{aligned} D_2(u,v) = {} & (16u^7 - 56u^6 + 472u^5 - 1040u^4 + 216u^3 + 688u^2 + 5000u - 2648) \\ & + (-140u^4 + 280u^3 - 916u^2 + 776u + 596)v \\ & + (-4u^3 + 6u^2 + 114u - 58)v^2 + 27v^3 \end{aligned}$$

であった。

**定理 4.1** (Spearman-Watanabe-Williams [SpWaWi])**.** 無限に多くの $t \in \boldsymbol{Z}$ に対し、$F_t(X) := f_6^{\mathfrak{A}_5}(1, 3t; X) = X^6 - 4X^5 + 2X^4 - 3tX^3 + X^2 + 2X + 1$ の根体 $K = \boldsymbol{Q}(\theta)$ は相異なる単生な $\mathfrak{A}_5$ 型 5 次体である。

$t \in \boldsymbol{Z}$ に対し、$F_t$ は、$t = 1$ のときを除いては既約で、Galois 群は $\mathfrak{A}_5 \simeq \mathrm{PSL}(2,5)$ である。判別式 $D(F_t) = D_2(1,3t)^2 = (729t^3 + 522t^2 + 1788t + 2648)^2$ で、$D_2(1,3t)$ が平方無縁なら $F_t$ の根 $\theta$ が冪基底を生成する。

---

[14] $m \equiv 1 \pmod{16}$ のときも大体大丈夫だが、$L = K$ となる例（$b = -\dfrac{47}{64}, \dfrac{127}{64}$）がある。

[15] 特に単数群については、$\mathfrak{A}_5$ が $\mathfrak{S}_6$ の偶な部分群であることから、根体の符号数は $(r_1, r_2) = (6,0)$（総実）あるいは $(2,2)$ であって、単数群の階数 $r_1 + r_2 - 1 = 5$ または 3 であり、総実でない階数 3 の場合に独立な単数を明示的に 3 個与えるだけでも、容易ではなさそうである。

4.2. **不分岐 2 次拡大.** 前節のように、$u, v \in \boldsymbol{Z}$ に対し、根体 $K = \boldsymbol{Q}(\theta)$ の上に不分岐 2 次拡大 $K(\sqrt{\theta})/K$ が乗らないだろうか。PARI/GP を用いて実験してみると、$K(\sqrt{\theta})/K$ の相対判別式が自明（すべての有限素点が不分岐）になる場合も多く見つかり、$u, v$ に関する合同条件で規定されるようである。現状では観察に留まる。

## 5. 他の例

生成的ではないが、より次数の大きい例としては、LaMacchia[LaM] による PSL$(2,7)$ 型 7 次多項式

$$\begin{aligned} f(a,A;X) = X^7 &+ 2(1-3a)X^6 + (-3+4a+8a^2)X^5 + (-2+6a-14a^2)X^4 \\ &+ (2-4a+6a^2-8a^3)X^3 + 8(2+a)a^2X^2 + 4(-3+2a)a^2X - 8a^3 \\ &+ Ax^3(1-x) \end{aligned}$$

の部分族

$$\begin{aligned} f^{\mathrm{PSL}(2,7)}(b;X) &:= f(\frac{1}{2}, b-\frac{5}{2}; -X) \\ &= X^7 + X^6 + X^5 + bX^4 + (b-2)X^3 - 5X^2 - 2X + 1 \end{aligned}$$

（判別式は $D(f^{\mathrm{PSL}(2,7)}) = (b^2-5b-25)^2(27b^2-135b+769)^2$）に関しても、冪基底に関する結果が得られている：

**定理 5.1** (Lavallee-Spearman-Yang[LSY])**.** 無限に多くの $b \in \boldsymbol{Z}$ に対し、$f_b(X)$ は相異なる単生な PSL$(2,7)$ 型 7 次体を与える。

## Appendix A. Newton 多角形

多項式の係数の付値から根の付値の情報を得るために用いられるのがNewton 多角形 (Newton polygon)である。Rosen[R, pp. 210–215], 橋本 [H2, 第 7 章：多項式の樹林と Newton] などを参考に基本事項や例を紹介する。

$K$ を完備離散付値体、$v$ をその付値とする。多項式 $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ で $a_0a_n \neq 0$ なるものに対し、$a_i \neq 0$ なる $i$ に対して点 $P_i = (i, v(a_i))$ を座標平面上にプロットして、$P_0$ から $P_n$ までの点の凸包を作り、その境界のうち線分 $P_0P_n$ の下側の部分の折れ線 $\mathcal{L}$ を、$f$ の（$v$ に関する）Newton 多角形と呼ぶ。Newton 多角形を構成する各線分を辺、その両端の $x$ 座標の差を辺の幅と呼ぶ。$f$ の Newton 多角形を構成する辺を左側から $L_1, \ldots, L_t$ とし、$L_i$ の傾きを $s_i$ とすると、凸性から $(s_i)_{i=1}^t$ は単調増加な有理数列を成す。

$K$ の代数閉包 $\widetilde{K}$ を固定し、$v$ の $\widetilde{K}$ への延長も同じく $v$ で表わす。このとき、$\widetilde{K}$ での $f$ の根の付値について、次が成り立つ：

**定理 A.1.** $K$ を完備離散付値体、$v$ をその付値とする。$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ について、$a_0a_n \neq 0$ とする。$f$ の Newton 多角形 $\mathcal{L} = (L_i)_{i=1}^t$ の各辺 $L_i$ に対し、その幅を $w_i$ 、傾きを $s_i$ とする。

(1) $i = 1, \ldots, t$ に対し、$f$ は $\widetilde{K}$ 内に付値 $-s_i$ の根を（重複度を含めて）$w_i$ 個持つ。
(2) $f$ は $K$ 内で $f(X) = f_1(X) \cdots f_t(X)$ と分解される。ここに、$\deg f_i = w_i$ で $f_i$ の根の付値はどれも $-s_i$ である。（$f_i$ が $K$ 上既約とは限らない。）特に、$\mathcal{L}$ が 2 本以上の線分から成るとき、$f$ は $K$ 上可約。
(3) $L_i$ が両端以外に格子点を通らないとき、$f_i$ は $K$ 上既約。

(1) は、係数（＝根の対称式）の付値と根の付値とを注意深く比べれば（やや細かい議論だが初等的に）得られる。(2) は、$K$ 上共役な根 $x$ が付値 $v(x) = [K(x):K]^{-1}N_{K(x)/K}(x)$ を共有することから、(3) は、$f_i$ の幾つかの根の積の付値が整数になるのが全ての根の積の場合のみであることから、それぞれ従う。

次のような良く知られた結果も、上記の定理の系として直ちに得られる：

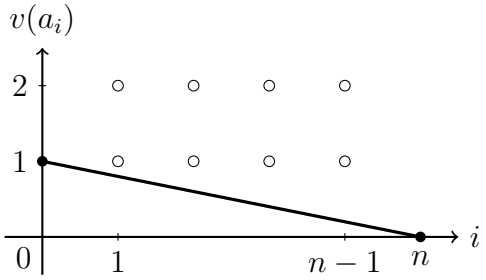
**命題 A.2.** $K, v, f$ を上記の定理の通りとする。

(1) (Eisenstein の判定法) $v(a_n) = 0,\ v(a_i) > 0\ (1 \le i \le n-1),\ v(a_0) = 1$ ならば、$f$ は $K$ 上既約。

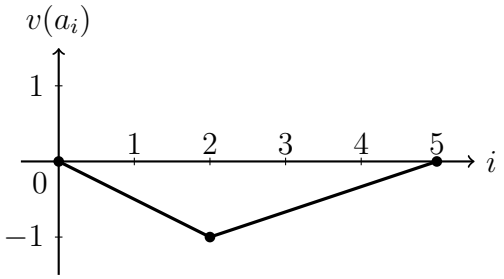
(2) $v(a_0) = v(a_n) = 0$ かつ或る $1 \le i \le n-1$ に対し $v(a_i) < 0$ ならば、$f$ は $K$ 上可約。

**例 A.3.** (1) $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ が Eisenstein 多項式（即ち、$v(a_i) > 0\ (1 \le i \le n-1),\ v(a_0) = 1$）のとき、点 $P_1, \ldots, P_{n-1}$ のあり得る場所は白丸の所で、凸包の内部に入り、Newton 多角形は下左図のようになる。$f$ は $K$ 上既約で、$n$ 個の根の付値はすべて $\dfrac{1}{n}$ であり、根体 $K(\theta)$ は $K$ 上完全分岐。

(2) $p$ を素数とし、$f(X) = X^5 + p^{-1}X^2 + 1 \in \boldsymbol{Q}[X]$ を考える。$\boldsymbol{Q} \subset \boldsymbol{Q}_p$ とみたときの $p$ 進 Newton 多角形は下左図のようになるので、$\boldsymbol{Q}_p$ 上での既約分解は $f(X) = f_1(X)f_2(X)$ の形になる。ここに、$\deg f_1 = 2$ で根の $p$ 進付値は $\dfrac{1}{2}$、$\deg f_2 = 3$ で根の $p$ 進付値は $-\dfrac{1}{3}$ である。実は、$f$ は $\boldsymbol{Q}$ 上既約であり、根体 $k = \boldsymbol{Q}(\theta)$ において、$p\mathcal{O}_k = \mathfrak{p}_1^2\mathfrak{p}_2^3$ （$\mathfrak{p}_1, \mathfrak{p}_2$ は 1 次の素イデアル）と分解・分岐する。




(1) $f$ : Eisenstein 多項式




(2) $f(X) = X^5 + \frac{1}{p}X^2 + 1$

## Appendix B. 数の幾何

Minkowski の凸体定理は、数の幾何 (geometry of numbers) の全ての源泉である、と Cassels[Ca]Chapter III の冒頭に書いてある。

B.1. **凸体定理.** $n$ 次元実 Euclid 空間 $\boldsymbol{R}^n$ 内の集合 $X$ が、原点を内点として含み、原点対称かつ凸であるとき、凸体 (convex body) と呼ぶことにする。（予めコンパクト性を課すこともある。）

**定理 B.1** (Minkowski の第 1 凸体定理)**.** 凸体 $X \subset \boldsymbol{R}^n$ について、$\mathrm{vol}(X) > 2^n$ ならば、$X$ は原点 $\mathbf{0}$ 以外の格子点 $\boldsymbol{x} \in X \cap (\boldsymbol{Z}^n \smallsetminus \{\mathbf{0}\})$ を含む。特に、$X$ がコンパクトであれば、$\mathrm{vol}(X) \ge 2^n$ でもよい。

$\boldsymbol{R}^n$ の部分 $\boldsymbol{Z}$ 加群 $L$ が離散かつ $\boldsymbol{R}$ 上では $\boldsymbol{R}^n$ を張るとき、格子 (lattice) であるという。このとき、$\boldsymbol{R}^n/L$ はコンパクトで体積有限なので、その体積を $\det(L) := \mathrm{vol}(\boldsymbol{R}^n/L)$ と書く。標準的な格子 $\boldsymbol{Z}^n$ を一般の格子 $L$ に変えると、次のようになる：

**定理 B.2** (Minkowski の第 1 凸体定理・格子版)**.** $\boldsymbol{R}^n$ の凸体 $X \subset \boldsymbol{R}^n$ について、格子 $L$ に対して $\mathrm{vol}(X) > 2^n \det(L)$ ならば、$X$ は原点 $\mathbf{0}$ 以外の $L$ の点 $\boldsymbol{x} \in X \cap (L \smallsetminus \{\mathbf{0}\})$ を含む。特に、$X$ がコンパクトであれば、$\mathrm{vol}(X) \ge 2^n \det(L)$ でもよい。

$\boldsymbol{R}^n$ の格子 $L$ に対して、$\mathbf{0}$ 以外の元の大きさ $|\boldsymbol{x}|$ の最小値を $\lambda_1 = \lambda_1(L)$ と書く：

$$\lambda_1 = \lambda_1(L) := \min_{\boldsymbol{x} \in L \smallsetminus \{\mathbf{0}\}} |\boldsymbol{x}| = \min\{r \mid \exists \boldsymbol{x} \in L \smallsetminus \{\mathbf{0}\} : |\boldsymbol{x}| \le r\} \quad .$$

凸体定理で $X$ として原点中心で半径 $\lambda$ の $n$ 次元球体を取ると、$\mathrm{vol}(X) = \lambda^n V_n$（ここに、$V_n$ は $n$ 次元単位球体の体積で、$V_n = \pi^{\frac{n}{2}}\Gamma\left(1 + \dfrac{n}{2}\right)^{-1}$）であるから、$\lambda^n V_n = 2^n \det(L)$ の

とき、$X$ 内に非零格子点 $\boldsymbol{x} \in L \setminus \{\boldsymbol{0}\}$ が存在する。これより

$$\lambda_1(L) \le 2\left(\frac{\det(L)}{V_n}\right)^{\frac{1}{n}} = 2\sqrt{\pi}\det(L)^{\frac{1}{n}}\Gamma\left(1+\frac{n}{2}\right)^{-\frac{1}{n}}$$

を得る。

B.2. **逐次最小.** $\lambda_1(L)$ の定義を拡張して、更に $1 \le j \le n$ なる各 $j$ に対し、$L$ に含まれる $j$ 個の線型独立系 $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j)$ で長さ $|\boldsymbol{x}_i|$ が高々 $r$ であるようなものが存在する $r$ の最小値を、$\lambda_j = \lambda_j(L)$ と書き、この $\lambda_1, \dots, \lambda_n$ を $L$ の（$|\cdot|$ に関する）逐次最小 (successive minima) と呼ぶ。定義により、$0 < \lambda_1 \le \cdots \le \lambda_n < \infty$ である。上で得た $\lambda_1(L)$ の評価の改良（精密化）として次が成り立つ：

**定理 B.3** (Minkowski の第 2 凸体定理・逐次最小定理)**.** $\boldsymbol{R}^n$ の格子 $L$ に対して

$$\frac{2^n}{n!}\frac{\det(L)}{V_n} \le \lambda_1 \cdots \lambda_n \le 2^n \frac{\det(L)}{V_n}.$$

B.3. **正定値 2 次形式の格子点での最小値.** $\boldsymbol{R}^n$ 上の正定値 2 次形式 $Q$ を考える。$Q$ は正定値 $n$ 次実対称行列 $A$ により $Q(\boldsymbol{x}) = Q_A(\boldsymbol{x}) := {}^t\boldsymbol{x}A\boldsymbol{x}$ と表せる。$Q$ に関する正規直交基底 $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_n)$ を取り、$B = (\boldsymbol{x}_1 \ \cdots \ \boldsymbol{x}_n)^{-1}$ とすれば、$B\boldsymbol{x}_i = \boldsymbol{e}_i$ であるから、$A = {}^tBB$ となり、特に $\det(Q) := \det(A) = \det(B)^2$ および $\mathrm{vol}\{\boldsymbol{x} \in \boldsymbol{R}^n | Q(\boldsymbol{x}) \le 1\} = \det(A)^{-\frac{1}{2}}V_n$ である。$\boldsymbol{Z}^n$ 上で 2 次形式 $Q$ を考えることは、行列 $B$ で移せば、格子 $L := B^{-1}\boldsymbol{Z}^n$ 上で標準的な 2 次形式 $|\boldsymbol{x}|^2 = x_1^2 + \cdots + x_n^2$ を考えることと同じである。

さて、正定値 2 次形式 $Q$ の非零格子点 $\boldsymbol{x} \in \boldsymbol{Z}^n \setminus \{\boldsymbol{0}\}$ での値 $Q(\boldsymbol{x})$ の最小値

$$m = m(Q) := \min_{\boldsymbol{x} \in \boldsymbol{Z}^n \setminus \{\boldsymbol{0}\}} Q(\boldsymbol{x})$$

を考えよう。$n$ 次元回転楕円体 $X = X(Q, \mu) := \{\boldsymbol{x} \in \boldsymbol{R}^n | Q(\boldsymbol{x}) \le \mu\}$ に対して凸体定理を適用することにより、$\mathrm{vol}(X) = \mu^{\frac{n}{2}}\det(Q)^{-\frac{1}{2}}V_n = 2^n$ のとき、$X \cap (\boldsymbol{Z}^n \setminus \{\boldsymbol{0}\}) \ne \emptyset$ となるので、

$$m(Q) \le 4\left(\frac{\det(Q)}{{V_n}^2}\right)^{\frac{1}{n}}$$

を得る。しかし、2 次形式の簡約により、より良い評価が得られる。

**定理 B.4** (see Cassels[Ca, Chapter II.3.2, Theorem I])**.** $n$ 変数の正定値 2 次形式 $Q$ に対し、

$$m(Q) \le \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \det(Q)^{\frac{1}{n}} \quad .$$

ここまでなら証明は初等的である。しかしながら、定数 $(4/3)^{\frac{n-1}{2}}$ が best possible なのは $n = 2$ のときのみである。

B.4. **Hermite 定数.** そこで、一般の $n$ に対し、best possible な値、即ち、

$$\gamma_n := \sup\left\{ m_Q \det(Q)^{-\frac{1}{n}} \,\middle|\, Q : \boldsymbol{R}^n \text{ 上の正定値 2 次形式} \right\}$$
$$= \sup\left\{ \lambda_1(L)^2 \det(L)^{-\frac{2}{n}} \,\middle|\, L : \boldsymbol{R}^n \text{ の格子} \right\}$$

を $n$ 次の Hermite 定数 (Hermite constant) と呼ぶ。上のことから、$\gamma_n$ の上からの評価 $\gamma_n \le \left(\frac{4}{3}\right)^{\frac{n-1}{2}}$ が得られる。一般の $n$ に対する $\gamma_n$ の値は決定されていないが、小さい $n$ に対する値は求められている（[Ca, Appendix]）：

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\gamma_n$ | 1 | $2 \cdot 3^{-\frac{1}{2}}$ | $2^{\frac{1}{3}}$ | $2^{\frac{1}{2}}$ | $2^{\frac{3}{5}}$ | $2 \cdot 3^{-\frac{1}{6}}$ | $2^{\frac{6}{7}}$ | 2 |

これを用いれば、定義により、$m(Q) \le \gamma_n \det(Q)^{\frac{1}{n}}$, $\lambda_1(L) \le \gamma_n^{\frac{1}{2}} \det(L)^{\frac{1}{n}}$ である。

## Appendix C. 判別式を用いた単数規準の下からの評価

C.1. **基本単数系・単数規準.** $K$ を $n$ 次代数体で、その符号数を $(r_1, r_2)$ とし、$\iota^{(i)}$ を $K$ の $\boldsymbol{C}$ への非同値な埋込み（無限素点）で、$1 \leq i \leq r_1$ が実、$r_1+1 \leq i \leq r_1+r_2$ が虚とする。Dirichlet の単数定理により、単数群の階数は $r = r_1+r_2-1$ である。$1 \leq i \leq r_1$（実）のとき $c_i = 1$、$r_1+1 \leq i \leq r_1+r_2$（虚）のとき $c_i = 2$ として、$\ell^i(\alpha) := c_i \log|\iota^{(i)}(\alpha)|$ とおく。また、$r_1+1 \leq i \leq r_1+r_2$ に対して、$\iota^{(i+r_2)}$ を $\iota^{(i)}$ の複素共役としておこう。すると、$\iota^{(i)}$ $(1 \leq i \leq r_1+2R_2 = n)$ が $K$ の $\boldsymbol{C}$ への相異なる埋込み全体となる。

$K$ の階数一杯 (full rank) の単数系 $\mathcal{E} := (\varepsilon_1, \ldots, \varepsilon_r)$（$r$ は単数群の階数）に対して、$R(\mathcal{E}) = R(\varepsilon_1, \ldots, \varepsilon_r) := |\det(\ell^{(i)}(\varepsilon_j))_{i,j}|$ と書こう。$\mathcal{E}$ が基本単数系、即ち、$\overline{\mathcal{O}^\times} := \mathcal{O}^\times/(\text{torsion})$ の $\boldsymbol{Z}$ 加群としての基底を成すとき、$R(\mathcal{E})$ は $\mathcal{E}$ に依らず一定で、$K$ の単数規準 (regulator) と呼び、$R_K$ と書く。$\mathcal{E}$ が階数一杯のとき、$\overline{\langle\mathcal{E}\rangle} = \overline{\langle\varepsilon_1, \ldots, \varepsilon_r\rangle} \subset \overline{\mathcal{O}^\times}$ は有限指数で、$R(\mathcal{E}) = R_K \cdot (\overline{\mathcal{O}^\times} : \overline{\langle\mathcal{E}\rangle})$ となる。従って、$R_K$ の何らかの下からの評価 $B$ に対し、明示的に得られた階数一杯の単数系 $\mathcal{E} := (\varepsilon_1, \ldots, \varepsilon_r)$ が $R(\mathcal{E}) < 2B$ を満たせば、$R_K = R(\mathcal{E})$ が言えて、$\mathcal{E}$ が基本単数系を成すことがわかる。$K$ が $\boldsymbol{Q}$ 上 Galois であるときには、$G = \mathrm{Gal}(K/\boldsymbol{Q})$ の作用を考えると、$\mathcal{E}$ が $G$ 不変（例えば或る単数 $\varepsilon$ の共役系）であれば、商加群 $\overline{\mathcal{O}^\times}/\overline{\langle\mathcal{E}\rangle}$ に $G$ 作用が入ることから、群指数 $(\overline{\mathcal{O}^\times} : \overline{\langle\mathcal{E}\rangle})$ に制約が付き、もう少し大きい $k$ に対して $R(\mathcal{E}) < kB$ で良いこともある。

C.2. **単数規準の下からの評価.** さて、判別式を用いた単数規準の下からの評価の常套手段を紹介しよう[16]。記述の簡単のために以下 $K$ は総実とし、$K/\boldsymbol{Q}$ には非自明な中間体がないものとする。

**命題 C.1.** $n$ 次総実代数体 $K$ について、$K/\boldsymbol{Q}$ には非自明な中間体がないものとする。このとき、

$$R_K \geq C\left(\log \frac{D_K}{M}\right)^{n-1}$$

（ここに $C, M$ は $n$ のみに依る定数）の形の下からの評価が存在する。

まず、次を示す：

**補題 C.2.** $K$ の $\pm1$ 以外の任意の単数 $\varepsilon \in \mathcal{O}_K^\times \setminus \{\pm1\}$ に対し、$\varepsilon$ の共役を $\varepsilon_j$ $(j = 1, \ldots, n)$ とするとき、

$$\log \frac{D_K}{M} \leq C\left(\sum_{j=1}^{n} (\log|\varepsilon_j|)^2\right)^{\frac{1}{2}}$$

となるような $n$ のみに依る定数 $C, M$ が存在する。

**証明.** $K$ の単数 $\varepsilon \in \mathcal{O}_K^\times \setminus \{\pm1\}$ を取ると、仮定から $K = \boldsymbol{Q}(\varepsilon)$ となる。

$$D(\varepsilon) := \prod_{1 \leq i < j \leq n} (\varepsilon^{(i)} - \varepsilon^{(j)})^2$$

を考えると、$D(\varepsilon) = D_K \cdot (\mathcal{O}_K : \boldsymbol{Z}[\varepsilon])^2$ であり、特に $D_K \leq D(\varepsilon)$ である。さらに、$\varepsilon$ の共役 $\varepsilon^{(i)}$ たちに、$|\varepsilon_1| \leq \cdots \leq |\varepsilon_n|$ となるように番号を付けると、

$$D(\varepsilon) = \prod_{1 \leq i < j \leq n} (\varepsilon_i - \varepsilon_j)^2 = \left(\prod_{1 \leq i < j \leq n} \left(1 - \frac{\varepsilon_i}{\varepsilon_j}\right)\right)^2 \cdot \prod_{j=1}^{n} |\varepsilon_j|^{2(j-1)}$$

である。

[16] $K$ の次数のみによる評価もあるが、それは所定の次数で単数規準の最小のものを決定するようなときに使うものである。ここでは個々の $K$ に対して議論するので、判別式や符号数などを用いた評価を考えるのである。

ここで、第 1 因子については、$z_i := \varepsilon_i/\varepsilon_{i+1}$ とおけば、

$$f(z_1,\dots,z_{n-1}) := \prod_{k=1}^{n-1}\prod_{i=1}^{n-k}\left(1-\prod_{j=0}^{k-1} z_{i+j}\right)^2$$

であり、$|z_i| \le 1$ なので、この（コンパクトな）範囲での $f$ の最大値 $M_n$ で上から押さえられる。自明な（細かい計算不要な）$M_n$ の上界としては、$M_n \le 2^{n(n-1)}$ が得られる。より詳しくは、例えば $n=3$ のとき、$f(z_1,z_2) = ((1-z_1)(1-z_2)(1-z_1z_2))^2$ の $|z_1| \le 1,\ |z_2| \le 1$ での最大値 $M_3$ は、$M_3 = f(0,-1) = f(-1,0) = 4$ である。一般に $M_n \ge 2^{2\left[\frac{n}{2}\right]}$ であるが、$n \le 11$ ならば実際 $M_n = 2^{2\left[\frac{n}{2}\right]}$ であることが知られている (Pohst[P])。例えば、$M_5 = 16$ である。初等的で具体的な最大値計算であるが、一般には煩わしいようである[17]。

一方、第 2 因子については、$\varepsilon \in \mathcal{O}_K^\times$ であるから、$\prod_{i=1}^{n} |\varepsilon_i| = 1$ なので、Cauchy-Schwarz の不等式を使って、

$$\begin{aligned}
\log\left(\prod_{j=1}^{n}|\varepsilon_j|^{2(j-1)}\right) &= \log\left(\prod_{j=1}^{n}|\varepsilon_j|^{2(j-1)-(n-1)}\right)\\
&= \sum_{j=1}^{n}(2j-n-1)\log|\varepsilon_j|\\
&\le \left(\sum_{j=1}^{n}(2j-n-1)^2\right)^{\frac12}\left(\sum_{j=1}^{n}(\log|\varepsilon_j|)^2\right)^{\frac12}\\
&\le C_n\left(\sum_{j=1}^{n}(\log|\varepsilon_j|)^2\right)^{\frac12}
\end{aligned}$$

となる。ここに $C_n = \sqrt{\dfrac{1}{3}n(n+1)(n-1)}$ である。

以上より、

$$\log\frac{D_K}{M_n} \le \log\frac{D(\varepsilon)}{M_n} \le C_n\left(\sum_{j=1}^{n}(\log|\varepsilon_j|)^2\right)^{\frac12}$$

となり、補題の形の不等式が得られた。 □

ところで、$\boldsymbol{\ell} = (\ell^i)_{i=1}^n : \mathcal{O}_K^\times \longrightarrow \boldsymbol{R}^n$ の像 $L := \boldsymbol{\ell}(\mathcal{O}_K^\times)$ は、$(n-1)$ 次元超平面 $W_0 := \{\boldsymbol{x} = (x_i)_{i=1}^n \in \boldsymbol{R}^n | x_1 + \cdots + x_n = 0\}$ 内の格子であって、（$W_0$ を $(n-1)$ 個の成分に射影せずに $\boldsymbol{R}^n$ の Euclid ノルムで測ったとき）$\det(L) = \mathrm{vol}(W_0/L) = \sqrt{n}R_K$ である。従って、Hermite 定数を用いた $\lambda_1(L)$ の上からの評価 $\lambda_1(L) \le \gamma_{n-1}^{\frac12}\det(L)^{\frac{1}{n-1}}$ により、

$$\left(\sum_{j=1}^{n}(\log|\varepsilon_j|)^2\right)^{\frac12} \le \gamma_{n-1}^{\frac12}\det(L)^{\frac{1}{n-1}}$$

を満たす単数 $\varepsilon \in \mathcal{O}_K^\times \smallsetminus \{\pm1\}$ が存在する。$K/\boldsymbol{Q}$ に非自明な中間体が存在しないという仮定から、$K = \boldsymbol{Q}(\varepsilon)$ である。以上より、

$$\log\frac{D_K}{M_n} \le C_n\left(\sum_{j=1}^{n}(\log|\varepsilon_j|)^2\right)^{\frac12} \le C_n\gamma_{n-1}^{\frac12}(\sqrt{n}R_K)^{\frac{1}{n-1}}$$

[17] Cusick[Cu] でも tedious と書かれている。

となり、これより $D_K$ を用いた $R_K$ の下からの評価

$$R_K \geq \frac{1}{\sqrt{n}C_n^{n-1}\gamma_{n-1}^{\frac{n-1}{2}}}\left(\log \frac{D_K}{M_n}\right)^{n-1}$$

が所望の形で得られた。

**注 C.3.** $n=3$ のときには、$C_3 = 2\sqrt{2},\ \gamma_2 = \dfrac{2}{\sqrt{3}},\ M_3 = 4$ より、定理 1.2 を得る。

**注 C.4.** $K/\boldsymbol{Q}$ が Galois 拡大であれば、$\mathcal{O}_K^\times$ の $G = \mathrm{Gal}(K/\boldsymbol{Q})$ 作用による格子 $L$ の対称性（$\boldsymbol{Z}[G]$ 加群構造）を利用して、さらに良い評価が得られる。$n=5$ のときに、定理 2.5 は、$G$ 作用の条件下で改良した上限を $\gamma_4$ の代わりに用いた上で、$C_5 = 2\sqrt{10},\ M_5 = 16$ により得られる。

## Appendix D. 多項式の値の平方無縁性

整数環や冪基底の考察においては、判別式やその因子が平方無縁 (square-free) の場合に良い結果が得られた。整数係数多項式 $f(X) \in \boldsymbol{Z}[X]$ の $X = n \in \boldsymbol{Z}$ での値が充分多くの場合に平方無縁たりうるか、という問題に対しては、次の Erdös の結果 [E] が良く用いられる：

**定理 D.1** (Erdös)**.** Let $f(x) \in \boldsymbol{Z}[x]$ be a polynomial of degree $l \geq 3$ whose coefficients are integers with highest common factor 1. Assume that $l \geq 3$ and that $f(x)$ is not divisible by the $(l-1)$-th power of a linear polynomial with integral coefficients. (When $l$ is a power of 2, we require an additional assumption that $f(n) \not\equiv 0 \pmod{2^{l-1}}$ for some integer $n$.) Then there are infinitely many positive integers $n$ for which $f(n)$ is $(l-1)$-th power free.

特に $l = 3$ の場合として、原始的（係数の最大公約数が 1）である整数係数 3 次式 $f(X) \in \boldsymbol{Z}[X]$ は、多項式として平方因子を持たなければ、無限に多くの正整数値 $X = n \in \boldsymbol{Z}_{>0}$ に対し、$f(n)$ が平方無縁な整数となる。$n \longrightarrow \infty$ のとき、筆頭係数の符号に応じて $f(n) \longrightarrow \pm\infty$ であるから、無限に多くの平方無縁な整数値を取ることもわかる。（同じ値は有限回しか取らないから、と言っても良い。）

## 参考文献


[AK] 穴井宏和、近藤武、$A_5$ を Galois 群に持つ 6 次式の族 —分解体と Galois 群の計算— 、「数式処理における理論とその応用の研究」、京大数理研講究録 **941** (1996), 57–72.

[B] Brumer, A., Curves with real multiplications, in preparation.

[Ca] Cassels, J. W. S., *An introduction to the geometry of numbers*, Corrected reprint of the 1971 edition, Classics in Mathematics, Springer-Verlag, Berlin, 1997.

[Cu] Cusick, T. W., Lower bounds for regulators, in "*Number Theory*", Noordwijkerhout 1983, Proceedings of Jornées Arithmétiques, Lec. Notes in Math. 1068, Springer-Verlag, 1984.

[E] Erdös, P., Arithmetical properties of polynomials, *J. London Math. Soc.* **28** (1953), 416–425.

[H1] Hashimoto, K., On Brumer's family of RM-curves of genus two, *Tohoku Math. J.* (2) **52** (2000), no. 4, 475–488.

[H2] 橋本喜一朗、探検！数の密林・数論の迷宮、日本評論社, 2017.

[HT] Hashimoto, K., Tsunogai, H., Generic polynomials over $\boldsymbol{Q}$ with two parameters for the transitive groups of degree five, *Proc. Japan Acad.* **79A** (2003), 148–151.

[JLY] Jensen, C. U., Ledet, A., Yui, N., *Generic Polynomials, constructive aspects of Galois theory*, MSRI Publ., Cambridge Univ. Press, 2002.

[Ka] 加藤優一、2 次不分岐拡大を持つ二面体型 5 次体の無限族の構成、修士論文（上智大学）, 2018.

[Ki] Kihel, O., Groupe des unités pour des extensions diédrales complexes de degré 10 sur $\boldsymbol{Q}$, *J. Théor. Nombres Bordeaux* **13** (2001), no. 2, 469–482.

[LaM] LaMacchia, S. E., Polynomials with Galois group PSL(2, 7), *Comm. Algebra* **8** (1980), no. 10, 983–992.

[LSWY] Lavallee, M. J., Spearman, B. K., Williams, K. S., Yang, Q., Dihedral quintic fields with a power basis, *Math. J. Okayama Univ.* **47** (2005), 75–79.

[LSY] Lavallee, M. J., Spearman, B. K., Yang, Q., $PSL(2,7)$ septimic fields with a power basis, *J. Thér. Nombres Bordeaux* **24** (2012), no. 2, 369–375.
[L] Lehmer, E., Connection between Gaussian periods and cyclic units, *Math. Comp.* **50** (1988), 535–541.
[LL] Lehmer, D. H., Lehmer, E., The Lehmer project, *Math. Comp.* **61** (1993), no. 203, 313–317.
[N] Nakano, S., A family of quintic cyclic fields with even class number parameterized by rational points on an elliptic curve, *J. Number Theory* **129** (2009), 2943–2951.
[P] Pohst, M., Regulatorabschätzungen für total reelle algebraische Zahlkörper, *J. Number Theory* **9** (1977), no. 4, 459–492.
[R] Rosen, M., *Number Theory in Function Fields*, Graduate Texts in Math., vol 210, Springer-Verlag, 2001.
[ScWa] Schoof, R., Washington, L. C. , Quintic polynomials and real cyclotomic fields with large class numbers, *Math. Comp.* **50** (1988), no. 182, 543–556.
[Sh] Shanks, D., The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152.
[SpWi] Spearman, B. K., Williams, K. S., Normal integral bases for Emma Lehmer's parametric family of cyclic quintics, *J. Théor. Nombres Bordeaux* **16** (2004), no. 1, 215–220.
[SpWaWi] Spearman, B. K., Watanabe, A., Williams, K. S., $PSL(2,5)$ sextic fields with a power basis, *Kodai Math. J.* **29** (2006), No. 1, 5–12.
[T] Tsunogai, H., A construction of an infinite family of dihedral quintic fields with unramified biquadratic extensions, to appear in "*Algebraic number theory and related topics 2017*", RIMS Kôkyûroku Bessatsu, Res. Inst. Math. Sci. (RIMS), Kyoto.
[T*] 角皆宏、複比の体での有理性問題、本報告集所収.

上智大学理工学部情報理工学科 102-8554 東京都千代田区紀尾井町 7-1
*E-mail address*: tsuno-h@sophia.ac.jp

# $\mathrm{PSL}_2(\mathbf{F}_p)$ に対するガロワの逆問題について

京都大学数理解析研究所　佐久川憲児

## 1　導入

本原稿は第２７回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」における同名講演の報告です.

## 2　目標と方法

この文章では素数を $p$ で表すことにする. 講演の目標は次の定理を証明した論文 [7] を紹介することである.

**定理 2.1.** ([7, Theorem 1.1]) 有限群 $\mathrm{PSL}_2(\mathbf{F}_p)$ に対するガロワの逆問題は肯定的な解を持つ. $p \geq 11$ ならば, より詳しく次のことがわかる:
ガロワ群が $\mathrm{PSL}_2(\mathbf{F}_p)$ と同型で, $2p$ の外不分岐な $\mathbf{Q}$ のガロワ拡大 $K$ が存在する.

幾つか定理について注意点を述べておこう.

**注意 2.2.**
(1) $p$ が 5 以上のとき, $\mathrm{PSL}_2(\mathbf{F}_p)$ は単純群である. このように代数群から来る有限単純群を *Lie* **型の有限単純群**というが, 定理 2.1 は [7] でも述べられているように, 一つの古典 Lie 型有限単純群の系列に対してガロワの逆問題を解決した**最初の場合**である.
(2) [4] では剛性の方法による部分的な解決を解説した. その方法では, 基本的には構成したガロワ拡大の**分岐をコントロールすることはできない**. 従って, 仮に剛性の方法で $\mathrm{PSL}_2(\mathbf{F}_p)$ のガロワの逆問題が解決できたとしても, その主張は定理 2.1 より分岐のコントロールという意味では弱くなる可能性が高い. 一方で定理 2.1 における $K$ は $\mathbf{Q}(t)$ の「幾何的に連結な」ガロワ拡大の特殊化として実現できるかはわからない (正則実現という). この点に関しては剛性の方法のほうがより優れている.
(3) $p$ が小さい場合のガロワの逆問題は肯定的に解けるので, 以下では $p$ は 11 以上の場合を考える.

定理 2.1 の証明におけるガロワ拡大の構成方法は [4] に於ける方法とはかなり異なる. [4] に於いて我々はエタール基本群上の商として拡大の存在を保証したが, ここではエタールコホモロジー由来の線型表現を利用してガロワ拡大を構成するのである.

この講演は [7] を解説することが目的であるが, 議論を短縮する為に次の仮定を設けて定理を証明することとする:
**(仮定)** 素数 $p$ は $11,\ 23,\ 29,\ 31$ ではない.
$11, 29, 31$ に関しては IGP は既に剛性の方法を用いてとかれている ([4] 参照). 23 だけが例外的にこのサマースクールで証明を与えることが出来ないのであるが, この場合も勿論 [7] ではカバーされている. 例外的な場合も含めた完全な証明については元論文を参照されたい.

本原稿では, エタールコホモロジーに関する予備知識は仮定します. この話題に関する日本語で

読める良い文献として, [3] がありますので, 必要ならば適宜参照しながら読まれると良いかと思います.

## 3 $\mathrm{PSL}_2(\mathbf{F}_p)$ の極大部分群について

まず $\mathrm{PSL}_2(\mathbf{F}_p)$ の極大部分群について思い出す. $\mathrm{PSL}_2(\mathbf{F}_p)$ の**ボレル部分群**とは, 上半三角行列のなす部分群と共役となるもののことをさす. $\mathrm{PSL}_2(\mathbf{F}_p)$ の**非分裂カルタン部分群** $C$ とは, $\mathrm{PSL}_2(\mathbf{F}_p)$ の巡回部分群で位数が $\frac{1+p}{2}$ となるもののことをさす. より具体的には, 以下のようにして構成される:

$\mathbf{F}_p$ 加群としての同型

$$\mathbf{F}_{p^2} \cong \mathbf{F}_p^2$$

を一つ固定し, これから得られる射

$$\iota\colon \mathbf{F}_{p^2}^{\times} \hookrightarrow \mathrm{GL}_2(\mathbf{F}_p)$$

を考える. すると, $C$ は $\tilde{C} := \mathrm{Im}(\iota) \cap \mathrm{SL}_2(\mathbf{F}_p)$ の $\mathrm{PSL}_2(\mathbf{F}_p)$ における像と共役である. 構成から, $\mathbf{F}_p^2$ は $\tilde{C}$ 加群として**絶対既約ではない**. $N$ を $C$ の正規化群としたとき, $C$ の $N$ における指数は 2 となっていることがわかる.

**定理 3.1** ([5, 2.4, 2.5, 2.6])**.** $\mathrm{PSL}_2(\mathbf{F}_p)$ の極大真部分群 $H$ は次の三つのうちの何れかである:

(1) $H$ は $\mathrm{PSL}_2(\mathbf{F}_p)$ のボレル部分群である.
(2) $H$ は $\mathrm{PSL}_2(\mathbf{F}_p)$ のカルタン部分群の正規化群である.
(3) $H$ は $A_4$, $\mathfrak{S}_4$, $A_5$ の何れかと同型である.

この定理から, $\mathrm{PSL}_2(\mathbf{F}_p)$ の部分群 $G$ が $\mathrm{PSL}_2(\mathbf{F}_p)$ と一致する事を示したければ, 次の三つの事柄を示せばよい:

(1) $G$ はボレル部分群に含まれない.
(2) $G$ は非分裂カルタン部分群の正規化群に含まれない.
(3) $G$ は $A_4$, $\mathfrak{S}_4$, $A_5$ に含まれない.

これらの命題及び仮定等を, 簡単の為にボレルケース, カルタンケース, 例外ケースと呼ぶことにしよう.

## 4 あるガロワ表現の構成とその性質

$U$ をアファインスキーム $\mathbf{A}^1_{\mathbf{Z}[1/2]} \setminus \{0, \pm 1\}$ とし, $E$ を以下の方程式で定義される $U$ 上の楕円曲線[*1]とする:

$$E\colon t(t^2-1)y^2 = x(x+1)(x+t^2).$$

[*1] $S$ をスキームとしたとき, $S$ 上の楕円曲線とは幾何的に連結な射影的かつ滑らかな種数 1 の曲線 $E \to S$ と切断 $S \to E$ の組のこととする. 通常の楕円曲線の場合と同様に $E$ は $S$ 上の可換群スキームとなる.

但し $E$ の $U$ スキームとしての構造は $t$ 成分への射影として定め, これを $f$ で表すこととしよう:

$$f\colon E \to U; \quad (x, y, t) \mapsto t.$$

さて, $E[p]$ でこの $U$ 上の楕円曲線の $p$ ねじれ点がなすエタール層を表すことにする. 具体的には任意の $U$ 上のエタールスキーム $T \to U$ に対し $E[p]$ の $T$ 値点は

$$E[p](T) := E(T)[p] := \mathrm{Mor}_S(T, E)[p]$$

で定める[*2]. 同様に $T_pE$ によって $E$ の $p$ 進テイト加群の定める $U$ 上の滑らかな $\mathbf{Z}_p$ 層をあらわすことにしよう.

**定義 4.1.** 連続 $G_{\mathbf{Q}}$ 表現 $V_{\mathbf{F}_p}, V_{\mathbf{Z}_p}$ を

$$V_{\mathbf{F}_p} := \mathrm{H}^1_{\mathrm{et,c}}(U_{\overline{\mathbf{Q}}}, E[p]), \quad V_{\mathbf{Z}_p} := \mathrm{H}^1_{\mathrm{et,c}}(U_{\overline{\mathbf{Q}}}, T_pE)$$

により定める. ここで各々の右辺はコンパクト・サポートエタールコホモロジーを表す.

$T_pE$ は重さが 1 の純な $\mathbf{Z}_p$ 層であるので, $V_{\mathbf{Z}_p}$ は重さ 0 のガロワ表現であることに注意しておこう. 即ち, 不分岐な素点に於ける幾何的フロベニウスの固有値は全て「絶対値 1」である. 定義よりガロワ表現の自然な射 $V_{\mathbf{Z}_p} \to V_{\mathbf{F}_p}$ が得られるが, 計算によりこれが同型

$$V_{\mathbf{Z}_p} \otimes_{\mathbf{Z}_p} \mathbf{F}_p \xrightarrow{\sim} V_{\mathbf{F}_p} \tag{1}$$

を誘導することが分かる. この $V_{\mathbf{F}_p}$ が欲しいガロワ表現である. これは次の性質を満たす:

**命題 4.2.** ([7, Lemma 2.1])

(1) $V_{\mathbf{Z}_p}, V_{\mathbf{F}_p}$ は階数 4 である.
(2) $G_{\mathbf{Q}}$ の作用と両立する非退化対称形式

$$\langle\ ,\ \rangle\colon V_{\mathbf{F}_p} \otimes_{\mathbf{F}_p} V_{\mathbf{F}_p} \to \mathbf{F}_p$$

が存在する. 但し $G_{\mathbf{Q}}$ は $\mathbf{F}_p$ に自明に作用しているとする.
(3) $G_{\mathbf{Q}}$ 表現 $V_{\mathbf{Z}_p}, V_{\mathbf{F}_p}$ は $2p$ の外不分岐である.

*Proof.* 簡単に証明のアイデアだけを述べるにとどめる. まず (1) は Ogg-Grothendieck-Shafarevich の公式と呼ばれる, エタール層のオイラー標数の計算から従う. (2) は $E$ に定まっている Weil ペアリングと $U$ の Poincare ペアリングを合わせて得られるペアリングである. これらは両方とも交代的なので, 二つ合わせて対称形式を与えることがわかる. 最後に (3) であるが, これは $E$ の $\mathbf{Z}[1/2]$ 上の滑らかなコンパクト化 $X$ があることと, $V_{\mathbf{Z}_p}$ が $X$ の 2 次のエタールコホモロジーの部分商となることから従う. □

[*2] $E$ が $S$ 上の楕円曲線のとき, 任意の $S$ スキーム $T$ に対しその $T$ 値点のなす集合 $\mathrm{Mor}_S(T, E)$ には自然にアーベル群の構造が入る ($E$ は $S$ 上の可換群スキームである). $\mathrm{Mor}_S(T, E)[p]$ はアーベル群 $\mathrm{Mor}_S(T, E)$ の $p$ ねじれ部分群のことである. 「局所的」にはこれは $S$ 上の定数層 $(\mathbf{Z}/p\mathbf{Z})^2$ と同型である.

**定義 4.3.** $\ell$ を $2p$ を割り切らない素数とし, $\mathrm{Frob}_\ell \in G_{\mathbf{Q}}$ で $\ell$ での幾何的フロベニウス元をあらわすことにする. 多項式 $\mathrm{ch}_\ell^{(n)}(X)$ を

$$\mathrm{ch}_\ell^{(n)}(X) := \det\left(1 - \mathrm{Frob}_\ell^n X \mid V_{\mathbf{Z}_p}\right)$$

で定める.

命題 4.2 (3) からこれは well-defined であることに注意しておこう. また, Deligne の定理 (Weil 予想) により, $\mathrm{ch}_\ell^{(n)}(X) \in \mathbf{Z}[1/\ell][X]$ である. さらに全射 (1) から, 等式

$$\mathrm{ch}_\ell^{(n)}(X) \bmod p = \det\left(1 - \mathrm{Frob}_\ell^n X \mid V_{\mathbf{F}_p}\right) \tag{2}$$

が成立していることにも注意しておこう. 小さな素数 $\ell$ に対してこの多項式を計算しておくことが後に重要となる:

**命題 4.4.** ([7, Lemma 2.4]) 次の等式が成立する:

$$\mathrm{ch}_3^{(1)}(X) = 1 - \frac{2}{9}X^2 + X^4, \quad \mathrm{ch}_5^{(1)}(X) = \left(1 - \frac{2}{5}X + X^2\right)^2.$$

*Proof.* Lefschetz の跡公式により, この固有多項式の計算は楕円曲線 $E$ の $\mathbf{F}_\ell, \mathbf{F}_{\ell^2}$ 有理点の個数の計算に帰着される. 例えば [7, Lemma 2.3] を参照されたい. $\ell$ が $3, 5$ の時は十分手で計算可能であるので, その部分は読者の演習問題としておく. □

さて, $O(V_{\mathbf{F}_p})$ により $V_{\mathbf{F}_p}$ とその上の対称形式から定まる直交群を表すことにしよう:

$$O(V_{\mathbf{F}_p}) := \{g \in \mathrm{Aut}_{\mathbf{F}_p}(V_{\mathbf{F}_p}) \mid \langle gv, gw\rangle = \langle v, w\rangle,\ \forall v, w \in V_{\mathbf{F}_p}\}.$$

良く知られているように, この直交群は $V_{\mathbf{F}_p}$ のある 3 次元超平面に対する鏡映変換で生成されている. そこでその元 $g$ に対し, $\mathrm{Sp}(g) \in \{\pm 1\}$ を

$$\mathrm{Sp}(g) := \begin{cases} 1 \quad , & g \text{ が偶数個の鏡映変換の積で書けるとき,} \\ -1 \quad , & g \text{ が奇数個の鏡映変換の積で書けるとき,} \end{cases}$$

と定めると, これは well-defined であり, **シュピノールノルム**と呼ばれる群準同型

$$\mathrm{Sp}\colon O(V_{\mathbf{F}_p}) \twoheadrightarrow \{\pm 1\}$$

を定める. この核と $\mathrm{SO}(V_{\mathbf{F}_p})$ との共通部分を $\Omega(V_{\mathbf{F}_p})$ と書くことにしよう:

$$\Omega(V_{\mathbf{F}_p}) := \mathrm{KerSp} \cap \mathrm{SO}(V_{\mathbf{F}_p}) = \{g \in SO(V_{\mathbf{F}_p}) \mid g \text{ は偶数個の鏡映変換の積で書ける }\}.$$

**事実 4.5.** $\Omega(V_{\mathbf{F}_p})$ は $\Omega_4^+(p)$ と同型である. 即ち, 直行形式 $\langle\ ,\rangle$ の極大アイソトロピック部分空間[*3]の次元は 2 である.

[*3] アイソトロピック部分空間とは, 任意の二つの元が直交するような部分空間のことである.

$\Omega_4^+(p)$ について一言述べておく. 良く知られているように, $V$ が標数が 2 でない有限体上の $2m$ 次元ベクトル空間とすると, $V$ 上の非退化直交形式は同値なものを除いて二種類ある. 一つは

$$\sum_{i=1}^{m} x_{2i-1}x_{2i}$$

に同値なもので, もう一つは $\epsilon$ が考えている有限体の非平方数としたとき

$$\sum_{i=1}^{m-1} x_{2i-1}x_{2i} + x_{2m-1}^2 - \epsilon x_{2m}^2$$

と同値となるものである. これらから定まる直交群をそれぞれ $O^+(V)$, $O^-(V)$ と書く. $V \cong \mathbf{F}_q^{2m}$ のときこれらは $O^+(q)$, $O^-(q)$ と書かれることもある. $\Omega$ についても同様である.

命題 4.2 から我々はガロワ表現

$$\rho_{\mathbf{F}_p} \colon G_{\mathbf{Q}} \to O(V_{\mathbf{F}_p})$$

を得た. より詳しく次の補題が成立している:

**補題 4.6.** ([7, Lemma 5.2]) $\rho_{\mathbf{F}_p}$ の像は $\Omega(V_{\mathbf{F}_p})$ に含まれる.

**補題 4.7.** 次の例外同型が存在する:

$$\mathrm{SL}_2(\mathbf{F}_p) \times \mathrm{SL}_2(\mathbf{F}_p)/\langle(-E_2, -E_2)\rangle \xrightarrow{\sim} \Omega(V_{\mathbf{F}_p}).$$

特に $\rho_{\mathbf{F}_p}$ と $i$ 番目の射影とを合成することにより, 連続群準同型

$$\rho_{\mathbf{F}_p}^{(i)} \colon G_{\mathbf{Q}} \xrightarrow{\rho_{\mathbf{F}_p}} \Omega(V_{\mathbf{F}_p}) \twoheadrightarrow \mathrm{PSL}_2(\mathbf{F}_p)$$

を得る.

*Proof.* 同型の構成についてだけ述べることにする. $(\mathcal{V}, (\ ,\ ))$ を $\mathbf{F}_p$ 上の二次元斜交空間とする. このとき, $\mathcal{W} := \mathcal{V}^{\otimes 2}$ 上の直交形式を

$$\langle v \otimes w, v' \otimes w' \rangle_{\mathcal{W}} := (v, v')(w, w')$$

で定めることにする. 明らかに $\mathcal{W}$ の極大アイソトロピック部分空間の次元は 2 であるので, 同型

$$(V_{\mathbf{F}_p}, \langle\ ,\ \rangle) \cong (\mathcal{W}, \langle\ ,\ \rangle_{\mathcal{W}})$$

が存在する. $\mathrm{SL}_2(\mathbf{F}_p)$ は斜交形式 $(\ ,\ )$ を保つので, 自然な作用により射

$$\mathrm{SL}_2(\mathbf{F}_p) \times \mathrm{SL}_2(\mathbf{F}_p) \to O(V_{\mathbf{F}_p})$$

が得られる. この射が補題における同型を与える. □

## 5 $G_{\mathbf{Q}(\sqrt{-1})}$ 上への制限

ここでは, $V_{\mathbf{F}_p}$ の $G_{\mathbf{Q}(\sqrt{-1})}$ 上への制限について調べる. $W$ をこの制限として得られる表現の部分既約表現とする. 次を示すことを目標とする:

**命題 5.1.** $W$ の次元は 2 であり, $G_{\mathbf{Q}(\sqrt{-1})}$ 加群としての同型

$$V_{\mathbf{F}_p} \cong W \oplus W$$

が存在する. 更に, もし $W$ が $G_{\mathbf{Q}(\sqrt{-1})}$ 加群として, 絶対既約でなければ, $\rho_{\mathbf{F}_p}(I_p)$ はアーベル群であり, その位数は $p^2-1$ を割り切る.

証明の為には幾ばくかの準備が必要である. $Q$ で四元数群を表すことにする:

$$Q = \{\pm 1, \pm i,\ \pm j,\ \pm k\} \subset \mathbb{H}^\times.$$

ここで $\mathbb{H}$ は四元数体としている.

**補題 5.2.** $G_{\mathbf{Q}(\sqrt{-1})}$ の作用と可換となる $Q$ の $V_{\mathbf{F}_p}$ 上への作用が存在する. また, $-1 \in Q$ の作用は $-1$ 倍写像と一致する.

*Proof.* $i, j \in Q$ の $E/\mathbf{Q}(\sqrt{-1})$ 上の作用を

$$i; (x, y, t) \mapsto (x, \sqrt{-1}y, -t), \quad j; (x, y, t) \mapsto (t^{-2}x, \sqrt{-1}t^{-1}y, t^{-1})$$

で定義することにすると, 簡単にこの作用は $Q$ の作用まで伸びることがわかる. 更に, 明らかにこの作用は $E[p]$ 上に $U$ 上同変な作用を引き起こすものであるので, 最初の主張は示された. 二つ目は易しい. □

**補題 5.3.** $W$ は $V_{\mathbf{F}_p}$ と等しくない. 即ち $V_{\mathbf{F}_p}$ の $G_{\mathbf{Q}(\sqrt{-1})}$ への制限は既約でない.

*Proof.* $Z := \mathrm{End}_{G_{\mathbf{Q}(\sqrt{-1})}}(W)$ と置くと, $W$ が既約なので $Z$ は有限可除環であり, 従って可換体である. 若し $V_{\mathbf{F}_p} = W$ ならば当然 $W$ に $Q$ が作用し, $Z$ が可換であるので $Q$ の $Z^\times$ での像もまた可換である. 一方で任意の $Q$ の $\{1\}$ と異なる正規部分群は必ず $-1$ を含むので, $Q \to Z^\times$ は単射である. これは $Z$ の可換性に反する. □

$QW$ は 3 次元でないことは $W$ の既約性と $QW \neq W$ (これは上の証明から明らか) からわかる. 従って $W$ の次元は 1 又は 2 である. 命題 5.1 を示したいのであるから, 以下 $W$ の次元が 1 であると仮定して矛盾を導こう. $G_{\mathbf{Q}(\sqrt{-1})}$ の指標 $\beta$ を一次元空間 $W$ により定義されるものであるとする:

$$\beta\colon G_{\mathbf{Q}(\sqrt{-1})} \to \mathrm{Aut}_{\mathbf{F}_p}(W) \cong {\mathbf{F}_p}^\times.$$

また, $\chi_p$ で mod $p$ 円分指標を表すことにする:

$$\chi_p\colon G_{\mathbf{Q}} \to \mathbf{F}_p^\times.$$

指標 $\beta$ は $2p$ の外不分岐であったが, その分岐をコントロールする次の二つの補題が鍵となる:

**補題 5.4.** ([7, Proposition 4.3 (1), Lemma 7.5]) ある $e \in \{0, \pm 1\}$ が存在して, 指標 $\beta\chi_p^e$ は任意の奇素数で不分岐となる.

**補題 5.5.** ([7, Proposition 6.1]) 任意の 2 での惰性群の元 $\sigma \in I_2$ に対し, $\sigma^{12}$ は $V_{\mathbf{F}_p}$ 上冪単である. 但しここで $I_2$ は $G_{\mathbf{Q}}$ の 2 に於ける惰性群を表すことにする.

この原稿ではこれらの証明の詳細には踏み込まないことにし, 最後の章に於いて証明方針についてのみ述べる. まずはこれらを認めて命題 5.1 を証明してみよう.

命題 5.1 の証明. $\mathfrak{p} \subset \mathbf{Z}[\sqrt{-1}]$ で 2 の上にある素イデアルを表すことにし, $I_{\mathfrak{p}}$ で $\mathfrak{p}$ での惰性群を表すことにする. 補題 5.4 で存在が保証された $e$ に対し, $\beta' := \beta\chi_p^e$ と置く. $\mathbf{Q}(\sqrt{-1})$ の類数が 1 であることより, $\beta'(G_{\mathbf{Q}(\sqrt{-1})}) = \beta'(I_{\mathfrak{p}})$ であることに注意しよう. 特に補題 5.5 より, $\beta'(G_{\mathbf{Q}(\sqrt{-1})})^{12} = 1$ であることに注意しておく.

$\mathbf{Q}_2(\sqrt{-1})$ のアーベル拡大であって, 分岐指数が 3 で割り切れるものは, 局所類体論から直ちにその非存在性が言える. つまり, $\beta'(I_{\mathfrak{p}})^4 = 1$ であり, 故に

$$\beta'(G_{\mathbf{Q}(\sqrt{-1})})^4 = 1 \tag{3}$$

が従う.

5 は $\mathbf{Q}(\sqrt{-1})$ で分裂するので, $\mathrm{Frob}_5 \in G_{\mathbf{Q}(\sqrt{-1})}$ であることに注意すれば, (3) より, $\mathrm{ch}_5^{(4)}(5^{4e})$ は $p$ で割り切れることが分かる. これが矛盾を導くことを見よう. 特性多項式の対称性により, $e = 0, 1$ の場合のみ計算すればよい. すると, 補題 4.4 と簡単な対称式の計算により, 等式

$$\mathrm{ch}_5^{(4)}(1) = 2^{14}3^2/5^8, \quad \mathrm{ch}_5^{(4)}(5^4) = 2^{14}3^25^27^229^2$$

を得る. これらは最初に置いた $p$ に対する仮定から $p$ で割り切れないので, 矛盾が導かれ, 最初の主張の証明が完了した.

$W$ の次元が 2 で且つ絶対既約でないならば, $G_{\mathbf{Q}(\sqrt{-1})}$ の表現はある指標

$$\psi\colon G_{\mathbf{Q}(\sqrt{-1})} \to \mathbf{F}_{p^2}^{\times}$$

から定まっていることがわかる. このことから二つ目の主張は直ちに従う. □

**系 5.6.** 任意の $\sigma \in G_{\mathbf{Q}(\sqrt{-1})}$ に対し, $\det(1 - \rho_{\mathbf{F}_p}(\sigma)T)$ は $1, T^2$ の係数が 1 であるような二次多項式の平方である.

*Proof.* 命題 5.1 から, $Q$ の作用を考えて $G_{\mathbf{Q}(\sqrt{-1})}$ 加群としての同型 $V \cong W \oplus W$ が存在することがわかる. この系はその明らかな帰結である. □

さて, もう少し詳しく $V_{\mathbf{F}_p}$ の $G_{\mathbf{Q}(\sqrt{-1})}$ 加群としての構造を見てみよう. 直交形式空間としての同型

$$(V_{\mathbf{F}_p}, \langle\ ,\ \rangle) \cong (\mathcal{W}, \langle\ ,\ \rangle_{\mathcal{W}})$$

があったことを思い出す. また例外同型により $\Omega(V_{\mathbf{F}_p})$ を $\mathrm{SL}_2(\mathbf{F}_p)^2$ の商と同一視する. 任意の $\sigma \in G_{\mathbf{Q}(\sqrt{-1})}$ に対し, この同一視を用いることにより,

$$\rho_{\mathbf{F}_p}(\sigma) = [(A_\sigma, B_\sigma)], \quad A_\sigma, B_\sigma \in \mathrm{SL}_2(\mathbf{F}_p)$$

と書くことにしよう. 定義から, 明らかに $A_\sigma$ の $\mathrm{PSL}_2(\mathbf{F}_p)$ での像は $\rho_{\mathbf{F}_p}^{(1)}(\sigma)$ と一致し, 同様に $B_\sigma$ の $\mathrm{PSL}_2(\mathbf{F}_p)$ での像は $\rho_{\mathbf{F}_p}^{(2)}(\sigma)$ と一致する.

**補題 5.7.** $A_\sigma$ または $B_\sigma$ のどちらかのトレースは $\pm 2$ である. 特に何方かは必ず位数が $2p$ を割り切る.

*Proof.* $a, a^{-1}$ を $A_\sigma$ の, $b, b^{-1}$ を $B_\sigma$ の固有値とする. このとき定義と $V_{\mathbf{F}_p}$ の自己双対性から $\det(1-\rho_{\mathbf{F}_p}(\sigma)T)$ の根は $\{ab, ab^{-1}, a^{-1}b, a^{-1}b^{-1}\}$ となる. 系 5.6 から, $ab$ はその他の三つのどれかと等しくなくてはならない. 仮に $ab = ab^{-1}$ ならば $b = \pm 1$ となり, $ab = a^{-1}b$ ならば $a = \pm 1$ なのでこれらの場合は補題の主張が示される. 一方 $ab = a^{-1}b^{-1}$ ならば 5.6 から $ab^{-1} = a^{-1}b$ が成立しなくてはならないので, ある $\epsilon \in \{\pm 1\}$ により $a = b\epsilon$ と書けている. 従って $a^2 = a^{-2}$ が成立し, これから $a^4 = 1$ を得る. $a^2 = 1$ ならば補題の主張は成立する. 一方 $a^2 = -1$ ならば, 簡単な計算により

$$\det(1-\rho_{\mathbf{F}_p}(\sigma)T) = (1-T^2)^2$$

を得るがこれは系 5.6 と矛盾する. 従って主張は示せた. □

**系 5.8.** $\rho^{(1)}_{\mathbf{F}_p}(G_{\mathbf{Q}(\sqrt{-1})})$ と $\rho^{(2)}_{\mathbf{F}_p}(G_{\mathbf{Q}(\sqrt{-1})})$ のいずれかは位数が $p$ である $\mathrm{PSL}_2(\mathbf{F}_p)$ の部分群に含まれる.

*Proof.* 系の主張が成立していないとすると, ある二つの元 $\sigma, \sigma' \in G_{\mathbf{Q}(\sqrt{-1})}$ が存在して, $A_\sigma, B_{\sigma'}$ は位数が $2p$ と互いに素であるが $A_{\sigma'}, B_\sigma$ は位数が $2p$ を割り切るものが存在する. $\sigma, \sigma'$ をそれぞれ $2p$ 乗に置き換えることにより, $B_\sigma$ と $A_{\sigma'}$ がそれぞれ 1 としてよい. しかしこのとき $A_{\sigma,\sigma'}$ と $B_{\sigma\sigma'}$ の位数は双方ともに $2p$ をわりきらないので, これは補題 5.7 に矛盾する. □

以下では $\rho^{(2)}_{\mathbf{F}_p}(G_{\mathbf{Q}(\sqrt{-1})})$ の位数が $p$ で割り切れると仮定しておこう. 特に $\mathcal{V}$ の一次元部分空間であり, 任意の $\sigma \in G_{\mathbf{Q}(\sqrt{-1})}$ に対し $B_\sigma$ で固定されるものがある. これを $\mathcal{V}_1$ とすると, $G_{\mathbf{Q}(\sqrt{-1})}$ 加群の単射

$$\mathcal{V} \otimes \mathcal{V}_1 \hookrightarrow \mathcal{W} \cong V_{\mathbf{F}_p} \tag{4}$$

を得る. 命題 5.1 よりこの像は $W$ と一致する.

# 6 証明

この章で次の定理を証明する:

**定理 6.1.** $\rho^{(1)}$ は全射である.

以前に注意したように, $\rho^{(1)}$ の像が極大部分群に含まれないことを示せばよい. それぞれ三つのケース毎に証明していこう.

## 6.1 ボレルケース

まずボレルケースから始める. このとき構成から, 任意の $\sigma \in G_{\mathbf{Q}(\sqrt{-1})}$ に対し $A_\sigma \in \mathrm{SL}_2(\mathbf{F}_p)$ は $\mathrm{SL}_2(\mathbf{F}_p)$ のあるボレル部分群に含まれる. 従ってこれらはある一次元部分空間を固定する. これは $W$ の $G_{\mathbf{Q}(\sqrt{-1})}$ 加群としての既約性に反する. つまり $\rho^{(1)}_{\mathbf{F}_p}(G_{\mathbf{Q}})$ はボレル部分群に含まれない.

## 6.2 カルタンケース

次にカルタンケースを考える. $C$ を $\mathrm{PSL}_2(\mathbf{F}_p)$ のカルタン部分群として, $N$ を $C$ の $\mathrm{PSL}_2(\mathbf{F}_p)$ における正規化部分群とする. 以下 $\rho^{(1)}_{\mathbf{F}_p}(G_{\mathbf{Q}}) \subset N$ を仮定しよう.

**補題 6.2.** $\rho^{(1)}_{\mathbf{F}_p}(I_p)$ は自明であるか $C$ と一致する.

*Proof.* これは命題 5.1 の直接の帰結である. □

$N/C$ は位数 2 であるので, 我々は二次指標

$$\varepsilon\colon G_{\mathbf{Q}} \to \{\pm 1\} \tag{5}$$

を得る. 対応する $\mathbf{Q}$ の高々二次の拡大体を $L$ と書くことにする.

**補題 6.3.** $L$ は 2 の外不分岐である. 従って, $\mathbf{Q}$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{-1})$ のいずれかである.

*Proof.* まず, $2p$ の外不分岐であることは命題 4.2 からわかる. また補題 6.2 から $p$ でも不分岐であることがわかる. □

**補題 6.4.** 任意の $g \in N \setminus C$ と任意のその持ち上げ $\tilde{g} \in \mathrm{SL}_2(\mathbf{F}_p)$ に対し,

$$\mathrm{Tr}(\tilde{g}) = 0$$

が成立する.

命題 4.4 から, $\rho^{(1)}_{\mathbf{F}_p}(\mathrm{Frob}_3)$ と $\rho^{(1)}_{\mathbf{F}_p}(\mathrm{Frob}_5)$ の (持ち上げの) トレースは 0 ではない[*4]. 従って, 補題 6.4 から

$$\varepsilon(\mathrm{Frob}_3) = 1, \quad \varepsilon(\mathrm{Frob}_5) = 1$$

を得る. 即ち 3,5 は $L$ に於いて分裂する. しかし, 補題 6.3 から, $L \neq \mathbf{Q}$ ならばいずれの場合もこのようなことは起こらないことがわかる. 実際, $L = \mathbf{Q}(\sqrt{2})$ の場合は 3, 5 双方とも惰性しており, $L = \mathbf{Q}(\sqrt{-1})$ ならば 3 が惰性, $L = \mathbf{Q}(\sqrt{-2})$ の場合には 5 が惰性する. 上の議論により $\varepsilon$ が自明指標であることがわかり, 結局 $\rho^{(1)}_{\mathbf{F}_p}(G_{\mathbf{Q}}) \subset C$ がわかる.

**補題 6.5.** $\rho^{(1)}_{\mathbf{F}_p}(I_p) = 1$ が成立する.

*Proof.* これは局所類体論と $C$ の位数が $\frac{1+p}{2}$ であることから従う. □

上の補題から, $\rho^{(1)}_{\mathbf{F}_p}$ は 2 の外不分岐な指標であり, $(\rho^{(1)}_{\mathbf{F}_p})^4 = 1$ をみたすことが前小節と同様の議論からわかる. 故に, 構成から $\rho_{\mathbf{F}_p}(\mathrm{Frob}_3^4)$ の固有値として $\pm 1$ が現れることがわかる. 一方命題 4.4 から, 次の等式を得る:

$$\mathrm{ch}_3^{(4)}(1) = \frac{2^{12} \times 5^2}{3^8}, \quad \mathrm{ch}_3^{(4)}(-1) = \frac{2^4}{3^8}.$$

これらは明らかに $p$ で割り切れないので, 以上でカルタンケースの証明が完了した.

[*4] $\mathrm{Frob}_3$ に関しては補題 5.7 と同様の議論を繰り返す必要がある. 詳しくは [7, Proposition 5.6] 参照.

### 6.3 例外ケース

最後に例外ケースの証明を行う. $M$ を $A_4, \mathfrak{S}_4.A_5$ のいずれかと同型である $\mathrm{PSL}_2(\mathbf{F}_p)$ の部分群とする. ここでは次の群論的補題が重要である.

**補題 6.6** ([5, Section 2.6])**.** $g \in M$ に対し, $g$ の持ち上げ $\tilde{g}$ を取り $u := \mathrm{Tr}(\tilde{g})^2$ と置く. このとき, $u$ は $0, 1, 2, 4$ の何れかであるか, 又は $u^2 - 3u + 1 = 0$ を満たす.

さて, $\rho^{(1)}_{\mathbf{F}_p}(\mathrm{Frob}_3)$ の持ち上げ $\tilde{g}$ を一つとり, $u_5 := \mathrm{Tr}(\tilde{g})^2$ と置こう. 命題 4.4 から, $u_5 = 4/25$ である. 従って, $u_5$ はまず $\mathbf{F}_p$ の中で零ではない. また, $u_5 = 1$ となる必要十分条件は $4 = 25$, 即ち $p = 23$ であるが, これは最初に設けた仮定から除外されている. 同様に最初の仮定から $u_5 = 2, 4$ もあり得ないことがわかる. 更に

$$u_5^2 - 3u_5 + 1 = \frac{11 \times 31}{5^4}$$

であるので, 再び仮定からこれは $\mathbf{F}_p$ の中で零ではない. 以上の計算と補題 6.6 から, $\rho^{(1)}_{\mathbf{F}_p}(G_{\mathbf{Q}})$ は決して $M$ の部分群とはならないことが示せた.

## 7 分岐のコントロール

以上で証明が完了したが, ポイントはガロワ表現 $\rho_{\mathbf{F}_p}$ の 2 と $p$ に於ける分岐を調べることであった (補題 5.4, 補題 5.5). この章ではこの二つの補題の証明の方針について述べる.

### 7.1 $p$ での分岐について

ここでは補題 5.4 の証明の方針を述べる.

まず, 従分岐重さ (tame inertia weights) と呼ばれる概念を思い出すことにする. $I_p \subset G_{\mathbf{Q}_p}$ を分岐群とし, $I_p^t$ でその従分岐商を表すことにする. つまり, $I_p^t$ は $I_p$ を野性分岐群 $P_p$ で割った群である. 良く知られているように, 自然な同型

$$I_p^t \xrightarrow{\sim} \prod_{\ell \neq p} \mathbf{Z}_\ell(1)$$

が存在する. ここで $p$ の冪 $q = p^m$ を一つとると, 自然な同一視 $\mathbf{Z}/(q-1)\mathbf{Z}(1) = \mathbf{F}_q^\times$ と上の自然な同型から群準同型

$$\epsilon \colon I_p^t \twoheadrightarrow \mathbf{F}_q^\times$$

が得られる. $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$ を上の $\epsilon$ と $\mathbf{F}_q$ の自己同型との合成により得られる準同型たちを表すことにすると, これら $m$ 個の準同型のことを $I_p^t$ **のレベル** $m$ **の基本指標**と呼ぶ. さて, $V$ を既約 $\mathbf{F}_p[I_p]$ 加群とする. このとき, $P_p$ は $V$ に自明に作用していることが比較的容易に証明できる ([5, Proposition 4] 参照). ここで $Z$ を $V$ の $\mathbf{F}_p[I_p]$ 加群としての自己準同型環を表すことにすると, $V$ の既約性より $Z$ は有限体となっている. そこで, 同型 $Z \cong \mathbf{F}_q$, $q = p^m$ を一つ固定すると, $V$ への $I_p^t$ の作用から指標

$$\alpha \colon I_p^t \to \mathbf{F}_q^\times$$

を得る. このとき, $\alpha = \epsilon_1^{e_1} \cdots \epsilon_m^{e_m}$ を満たす整数 $e_1, \ldots, e_m$ が $p$ を法として一意的に存在するが, この $e_1, \ldots, e_m \in \{0, 1, \ldots, p-1\}$ を $V$ **の従分岐重さ**と呼ぶ. 一般の $\mathbf{F}_p[I_p]$ 加群についてはその既約成分の従分岐重さとして現れる整数のことを, $V$ の従分岐重さと定めることにする. 補題 5.4 は次の Caruso による定理と我々の楕円曲面 $E$ が $\mathbf{Z}_p$ 上半安定モデルを持つことから直ちに得られる:

**定理 7.1** ([2, Théoreme 1.2])**.** $\mathcal{X}$ を $\mathbf{Z}_p$ 上の固有且つ安定還元を持つスキームとする[*5]. また, $i$ を $p-1$ より小さな非負整数とする. このとき, $\mathbf{F}_p[I_p]$ 加群 $\mathrm{H}^i_{\mathrm{et}}(\mathcal{X}_{\overline{\mathbf{Q}}_p}, \mathbf{F}_p)^\vee$ の従分岐重さは $\{0, 1, \ldots, i\}$ に属する.

この定理の証明は雑に言って

Step1 $\mathbf{F}_p$ 係数の「半安定」$G_{\mathbf{Q}_p}$ 表現の線形データによる言い換え ([1])
Step2 半安定還元を持つスキームに対する整 $p$ 進ホッジ比較定理 ([2])

という二つのステップからなっている. まず最初のステップで, Caruso は $\underline{\mathcal{M}}^r$ という $\mathbf{F}_p$ 上の「半安定」$G_{\mathbf{Q}_p}$ 表現を分類するような線型データの圏を導入し ([1, Chapter 2])[*6], 続いてその圏の単純対象の分類を行っている ([1, Theoreme 1.0.2]). [2] では, 半安定還元を持つ場合に $\mathbf{Z}/p^r\mathbf{Z}$ 係数のエタールコホモロジーと対数クリスタルコホモロジーに対し $p$ 進ホッジ比較定理を証明し[*7], それに Step 1 に於いて行った分類を適応することにより証明を完結させている・・・ようである. 大変申し訳ありませんが, 時間の都合上筆者はこの証明をフォローすることが出来ませんでした. 興味を持たれた読者はぜひこの二つの論文を参照ください. 多分面白いと思います.

## 7.2 2 での分岐について

最後に補題 5.5 の証明について簡単に方針を述べる[*8]. まず, $X \to \mathbf{P}^1_{\mathbf{Q}}$ を $E \to U$ の $\mathbf{Q}$ 上の射影的で滑らかなコンパクト化で相対的に極小であるものとする.

**事実 7.2** ([7, A.5])**.** ある 4 次元部分空間 $\mathcal{V}_p \subset \mathrm{H}^2_{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p(1))$ が存在して, $G_{\mathbf{Q}}$ 表現の同型

$$\mathrm{H}^2_{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_p(1)) = \mathcal{V}_p \oplus \mathbf{Q}_p^{30}$$

が存在する. また, $T := \mathrm{H}^2_{\mathrm{et}}(X_{\overline{\mathbf{Q}}}, \mathbf{Z}_p(1))$ は自由 $\mathbf{Z}_p$ 加群で, $\overline{\mathcal{V}}_p = (T \cap \mathcal{V}_p) \otimes_{\mathbf{Z}_p} \mathbf{F}_p$ は $V_{\mathbf{F}_p}$ と $\mathbf{F}_p[G_{\mathbf{Q}}]$ 加群として同型である.

さて, $p$ は 2 でないので, $I_2$ の $\mathcal{V}_p$ 上への表現は準冪単[*9]である. 任意の $\sigma \in I_2$ に対し, 正の整数 $m_\sigma$ を, $\sigma^{m_\sigma}$ の $\mathcal{V}_p$ 上への作用が冪単となるようなものの中で, 最小であるものとする.

**命題 7.3.** $m_\sigma$ は $p$ に依存しない.

---

[*5] 実際の定理は $\mathbf{Z}_p$ だけでなく, より一般の局所体の整数環上で述べられている. 但し, その局所体の絶対分岐指数は「素数 $p$ に比して比較的小さい」というタイプの仮定が設けられている.

[*6] 「$S$」上のフィルター付きフロベニウス加群のようなものである.

[*7] これによりガロワ表現を Step 1 で考えた線型データの話に帰着できる.

[*8] 筆者はこの証明は大変面白いと感じた. ある意味汎用性が高い証明であるようにも思われる.

[*9] つまり, ある開部分群へ制限すれば, 冪単表現である.

*Proof.* $\widetilde{V}_p := T \otimes \mathbf{Q}_p$ と置く. まず, $\sigma$ が $\mathcal{V}_p$ に冪単に作用する必要十分条件は $\mathrm{Tr}_{\mathcal{V}_p}(\sigma) = 4$ となることに注意しておく (ここでガロワ表現の重さが 0 であることを使う). 事実 7.2 から, これは $\mathrm{Tr}_{\widetilde{V}_p}(\sigma) = 34$ と同値であることに注意しておく. $X$ は曲面なので, $\mathrm{Tr}_{\widetilde{V}_p}(\sigma)$ が $p$ に依存しないことが落合により示されており ([6]), これで証明が完了する. □

**補題 7.4.** $T$ を $\mathbf{Z}_p$ 上の有限階数自由加群で, $g$ を $T$ の $\mathbf{Z}_p$ 線型変換とする. また, $g$ と $g \bmod p$ は両方とも準冪単であると仮定する. 正整数 $m, n$ を $g^m,\ g^n \bmod p$ が冪単となるような最小のものとしよう. 仮に $m$ が $p$ で割り切れなければ $m = n$ である.

*Proof.* まず, $\mathrm{Aut}_{\mathbf{Z}_p}(T) \to \mathrm{Aut}_{\mathbf{F}_p}(T \otimes_{\mathbf{Z}_p} \mathbf{F}_p)$ の核は副 $p$ 群であることに注意しておく. この注意から $g^n$ が生成する $\mathrm{Aut}_{\mathbf{Z}_p}(T)$ の位相的部分群は副 $p$ 群であることに注意しておく. 従ってある $p$ 冪 $p^r$ があって $g^{np^r}$ が冪単となるが, $m$ の最小性と $p$ と互いに素であることから $m|n$ がわかる. 逆の可除性はあきらかであろう. □

補題 7.4 と命題 7.3 から次が得られる:

**系 7.5.** $p$ が十分大きければ $m_\sigma$ は $\sigma^{m_\sigma}$ が $V_{\mathbf{F}_p}$ 上冪単となるような正整数のなかで最小のものである.

$\sigma \in I_2$ を一つとる. $\mathrm{PSL}_2(\mathbf{F}_p)$ の任意の元の位数は $p$ 又は $\frac{1+p}{2},\ \frac{p-1}{2}$ を割り切ることに注意しよう. 従って, 例外同型を思い出してみると, $\rho_{\mathbf{F}_p}(\sigma)$ の $\Omega(V_{\mathbf{F}_p})/\pm 1$ に於ける像の位数は $4p$, $\mathrm{lcm}(4, p-1)$, $\mathrm{lcm}(4, p+1)$ のいずれかを割り切ることがわかる. ここで系 7.5 から, $p$ が十分大きなときに $m_\sigma$ もまた $4p$, $\mathrm{lcm}(4, p-1)$, $\mathrm{lcm}(4, p+1)$ のいずれかを割り切る. 今 $p$ と $m_\sigma$ は互いに素としてよいので, 結局我々は

$$m_\sigma |\ \mathrm{lcm}(4, p-1), \quad \text{又は } m_\sigma |\ \mathrm{lcm}(4, p+1), \quad \forall p >> 0$$

を得た. 言い換えれば, 任意の十分大きな素数 $p$ は, ある整数 $a$ が存在して,

$$p = am_\sigma \pm 1,\ \frac{am_\sigma}{2} \pm 1$$

と書けている. これは等差数列となっている（!）ことに注意しよう. Dirichlet の算術級数定理により, この四つの等差数列で素数が全てカバーできるような公差はあまりないことがわかるが, 実際にそのためには $m_\sigma$ が 12 で割り切れることが必要となる. 以上で証明のスケッチが完了した.

**謝辞**

本稿の初稿に目を通してくださり, 多数の有益なコメントをくださった大下達也さんに多大な感謝を申し上げます. また, 原稿の提出期限を延ばしてくださいました本サマースクールの世話人の方々に深くお礼申し上げます.

## 参考文献

[1] C. Caruso, Représentations $p$-adiques semi-stables dans le cas $er < p - 1$,

[2] X. Caruso, Conjecture de l'inertue modereé de Serre, *Invent. Math.*, **171** 629–699 (2008).

[3] 三枝洋一, エタールコホモロジーと $\ell$ 進表現, 第 17 回整数論サマースクール「$\ell$ 進ガロア表現とガロア変形の整数論」報告集, 113–181 (2010).

[4] 佐久川憲児, ガロワの逆問題と剛性の方法について, 本サマースクール報告集.

[5] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, **15** 259–331 (1972).

[6] T. Ochiai, $l$-independence of the trace of monodromy, *Math. Ann.*, **315** 321–340 (1999).

[7] D. Zywina, The inverse Galois problem for $\mathrm{PSL}_2(\mathbf{F}_p)$, *Duke math. J.*, vol. **164**, no. 12 (2015).

# Rationality problem for algebraic tori

長谷川　寿人 (新潟大学)

本稿は第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」における講演「Rationality problem for algebraic tori」 の原稿です．本稿では，まず代数的トーラスの基本事項を確認し，代数的トーラス，とくにノルム 1 トーラスの有理性問題についての結果を紹介します．

## 1　代数的トーラスの有理性問題

**定義.** $X$ を $k$ 上の代数多様体とする．
・$X$ が $n$ 次射影空間 $\mathbb{P}^n$ に双有理同型であるとき，$X$ は $k$ 上**有理的**であるという．
・ある $r \geq 1$ に対して $X \times_k \mathbb{P}^r$ が $k$ 上有理的であるとき，$X$ は $k$ 上**安定有理的**であるという．
・有理射 $f : X \to \mathbb{P}^r$, $g : \mathbb{P}^r \to X$ があり $g \circ f = \mathrm{id}_X$ となるとき，$X$ は $k$ 上**レトラクト有理的**であるという．
・ある $m \geq 1$ に対して支配的射 $\mathbb{P}^m \dashrightarrow X$ があるとき，$X$ は $k$ 上**単有理的**であるという．

**注意.** 上の定義は，関数体の言葉で言えば $X$ の $k$ 上の関数体が有理的 (resp. 安定有理的，レトラクト有理的，単有理的) であるとき，$X$ は有理的 (resp. 安定有理的，レトラクト有理的，単有理的) であるということである．

まず，代数的トーラスの定義と基本事項について確認しておく．詳細については [Vos98], [Swa83, Section 12] を参照.

**定義.** $T$ を $k$ 上定義された代数群とする．このとき $T$ が $k$ 上の**代数的トーラス**であるとは，自然数 $n$ が存在して $T \otimes \bar{k} \simeq \bar{k}^{\times n}$ となるときをいう．

**命題 1.1.** $T$ を $k$ 上の代数的トーラスとする．このとき $k$ の有限次ガロア拡大 $K$ が存在して $T \otimes_k K \simeq K^{\times n}$ となる．このような $K$ の中で最小のものが存在する．

**定義.** $k$ 上の代数的トーラス $T$ に対し，$T \otimes_k K \simeq K^{\times n}$ が成り立つとき $T$ は $K$ で**分裂する**とい

う．$T$ が分裂する最小の $k$ の拡大体を**最小分裂体**という．

$K$ を $k$ 上の有限次ガロア拡大とし $G = \mathrm{Gal}(K/k)$ とする．$K$ で分裂する $k$ 上の代数的トーラス $T$ に対し，指標群 $X(T) = \mathrm{Hom}(T, K^\times)$ を考える．$T \otimes_k K \simeq K^{\times n}$ により $T \otimes_k K$ を $K^{\times n}$ と同一視することにより，$\mathrm{Hom}(T \otimes_k K, K^\times)$ は次の $v_i : K^{\times n} \to K^\times$ で生成される自由アーベル群とみなせる：

$$v_i : K^{\times n} \ni (x_1, x_2, \ldots, x_n) \mapsto x_i \in K^\times$$

これを加法的にかくと

$$\mathrm{Hom}(T \otimes_k K, K^\times) = \bigoplus_{i=1}^{n} \mathbb{Z} u_i \tag{$*$}$$

となる．ガロア群 $G$ は $\mathrm{Hom}(T \otimes_k K, K^\times)$ に次のように作用する：

$$(\sigma f)(x) = \sigma^{-1} f(\sigma x).$$

これにより $X(T)$ は $G$ 格子とみれる．

また，次の定理が成り立つ．

**定理 1.2** (小野 [Ono61, Proposition 1.2.4] 参照)**.** $K/k$ を有限次ガロア拡大，$G = \mathrm{Gal}(K/k)$ とする．このとき $G$ 格子 $M$ に対して，$K$ で分裂し $X(T) \simeq M$ となる $k$ 上の代数的トーラス $T$ が $k$ 同型を除きただ 1 つ存在する．

これにより，$K$ で分裂する代数的トーラスと $G$ 格子は一対一に対応する．

$T$ を $k$ 上の $n$ 次元代数的トーラスとする．指標群 $X(T) = \mathrm{Hom}(T \otimes_k \bar{k}, \bar{k}^\times)$ は加群として $\mathbb{Z}^{\oplus n}$ と同型であり，$k$ の絶対ガロア群 $\mathcal{G} = \mathrm{Gal}(\bar{k}/k)$ が作用することから，$T$ に対して連続準同型 $h : \mathcal{G} \to \mathrm{GL}_n(\mathbb{Z})$ が定まる．このとき $\mathcal{G}$ はコンパクトであり，$\mathrm{GL}_n(\mathbb{Z})$ は離散的であることから，$\mathcal{G}$ の像 $h(\mathcal{G})$ は $\mathrm{GL}_n(\mathbb{Z})$ の有限部分群になる．$k$ 上の $n$ 次元代数的トーラス $T$ は，連続準同型 $h : \mathcal{G} \to \mathrm{GL}_n(\mathbb{Z})$ の共役類によって決まる．ただし，$\mathcal{G}$ の像 $h(\mathcal{G})$ は $\mathrm{GL}_n(\mathbb{Z})$ の有限部分群．

$K/k$ をガロア拡大，$G = \mathrm{Gal}(K/k)$，$M = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \oplus \cdots \oplus \mathbb{Z}u_n$ を $G$ 格子とする．ただし，$\{u_1, u_2, \ldots, u_n\}$ は $M$ の $\mathbb{Z}$ 基底．このとき，有理関数体 $K(x_1, x_2, \ldots, x_n)$ に $G$ の作用を次のように定める：$\sigma \in G$ の $M$ への作用が $\sigma(u_i) = \sum_{j=1}^{n} \mathbb{Z}u_j$，$a_{ij} \in \mathbb{Z}$ であるとき，

$$\sigma(x_i) = \prod_{j=1}^{n} x_j^{a_{ij}}. \tag{1}$$

この作用をともなう体 $K(x_1, x_2, \ldots, x_n)$ を $K(M)$ とかく．

有限次ガロア拡大 $K/k$ で分裂する $k$ 上の代数的トーラス $T$，$M = X(T) = \sum_{i=1}^{n} \mathbb{Z}u_i$ とする．$T \otimes_k K \simeq K^{\times n}$ により $T \otimes_k K$ と $K^{\times n}$ を同一視すると $T \otimes_k K$ の関数体は，$(*)$ における $u_i$

を超越基底とする有理関数体 $K(u_1, u_2 \ldots, u_n)$ となる．このとき，代数的トーラス $T$ の関数体は $K(M)^G$ と同一視できる．

次に，代数的トーラスの有理性について知られている結果を述べる．

1 次元代数的トーラスは $k$ 上有理的である．2 次元，3 次元の代数的トーラスの有理性についてはそれぞれ Voskresenskii [Vos67], Kunyavskii [Kun90] によって与えられた：

**定理 1.3** (Voskresenskii [Vos67])**.** すべての 2 次元代数的 $k$ トーラスは $k$ 上有理的.

**定理 1.4** (Kunyavskii [Kun90])**.** すべての 3 次元代数的 $k$ トーラスは [Kun90, Theorem 1] の 15 の例外を除いて $k$ 上有理的．15 の例外は $k$ 上非レトラクト有理的.

4 次元，5 次元の安定 (レトラクト) 有理的な代数的トーラスの分類については，星-山崎 [HY17] により GAP を用いてあたえられた.

**定理 1.5** (星-山崎 [HY17, Theorem 1.8])**.** $L/k$ を体のガロア拡大，有限部分群 $G \simeq \mathrm{Gal}(L/k) \leq GL_4(\mathbb{Z})$ は $L(x_1, x_2, x_3, x_4)$ に式 (1) によって作用するとする.
(i) $L(x_1, x_2, x_3, x_4)^G$ は $k$ 上安定有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 2, 3, 4] に含まれない 487 個の群と共役.
(ii) $L(x_1, x_2, x_3, x_4)^G$ は $k$ 上非安定有理的かつレトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Table 2] の 7 個の群と共役.
(iii) $L(x_1, x_2, x_3, x_4)^G$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 3, 4] の 216 個の群と共役.

**定理 1.6** (星-山崎 [HY17, Theorem 1.11])**.** $L/k$ を体のガロア拡大，有限部分群 $G \simeq \mathrm{Gal}(L/k) \leq GL_4(\mathbb{Z})$ は $L(x_1, x_2, x_3, x_4, x_5)$ に式 (1) によって作用するとする.
(i) $L(x_1, x_2, x_3, x_4, x_5)^G$ は $k$ 上安定有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 11, 12, 13, 14, 15] に含まれない 3051 個の群と共役.
(ii) $L(x_1, x_2, x_3, x_4, x_5)^G$ は $k$ 上非安定有理的かつレトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Table 11] の 25 個の群と共役.
(iii) $L(x_1, x_2, x_3, x_4, x_5)^G$ は $k$ 上レトラクト有理的 $\Leftrightarrow$ $G$ は [HY17, Tables 12, 13, 14, 15] の 3003 個の群と共役.

## 2　ノルム 1 トーラスの有理性問題

$K/k$ を $n$ 次分離拡大，$L/k$ を $K/k$ のガロア閉包とする．$G = \mathrm{Gal}(L/k)$ を $n$ 次対称群 $S_n$ の部分群とみなし，$H = \mathrm{Gal}(L/K)$ とする．このとき，次の $\mathbb{Z}[G]$ 加群の完全系列がある：

$$0 \longrightarrow I_{G/H} \longrightarrow \mathbb{Z}[G/H] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

ここで $\epsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$, $\sum_{i=1}^{n} a_i e_i \mapsto \sum_{i=1}^{n} a_i$, $e_i = g_i H$ は $\mathbb{Z}[G/H]$ の $\mathbb{Z}$ 基底．この完全系列の双対をとると，次の完全系列をえる：

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G/H] \longrightarrow J_{G/H} \longrightarrow 0.$$

とくに，$J_{G/H} = \mathrm{Hom}_{\mathbb{Z}}(I_{G/H}, \mathbb{Z})$ は $\mathbb{Z}$ 階数 $n-1$ の $G$ 格子となる．この $J_{G/H}$ に対応する $k$ 上の代数的トーラスのことを，$K/k$ の**ノルム 1 トーラス**といい $R^{(1)}_{K/k}(\mathbb{G}_{m,K})$ とかく．

このとき，拡大 $K/k$ に対するノルム写像から誘導される $k$ 上の代数的トーラスの完全系列

$$1 \longrightarrow R^{(1)}_{K/k}(\mathbb{G}_{m,K}) \longrightarrow R_{K/k}(\mathbb{G}_{m,K}) \xrightarrow{N_{K/k}} \mathbb{G}_m \longrightarrow 1$$

をえる．ここで $R_{K/k}(\mathbb{G}_{m,K})$ は拡大 $K/k$ による乗法群 $\mathbb{G}_{m,K}$ のヴェイユ制限．

次にノルム 1 トーラス $R^{(1)}_{K/k}(\mathbb{G}_m)$ の有理性問題に関して知られている結果を述べる．

$K/k$ がガロア拡大のとき，以下の結果が知られている．

**定理 2.1.** $K/k$ をガロア拡大，$G = \mathrm{Gal}(K/k)$ とする．
(1) (遠藤-宮田 [EM75, Theorem 1.5], Saltman [Sal84, Theorem 3.14])
$R^{(1)}_{K/k}(\mathbb{G}_m)$ が $k$ 上レトラクト有理的 $\Leftrightarrow$ $G$ のすべてのシロー群は巡回群.
(2) (遠藤-宮田 [EM75, Theorem 2.3]) $R^{(1)}_{K/k}(\mathbb{G}_m)$ は $k$ 上安定有理的 $\Leftrightarrow$ $G = C_m$ または $G = C_n \times \langle \sigma, \tau : \sigma^k = \tau^{2^d} = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ $(d \geq 1, k \geq 3,\ n, k$ は奇数で $\gcd\{n, k\} = 1)$.

$K/k$ が非ガロア拡大の場合に関しても，$K/k$ のガロア閉包のガロア群が特定の群 (例えば，$S_n$, $A_n$, べき零群など) に対しての結果が知られているが，一般の場合についてはほとんどわかっていない (本サマースクールの星明考氏の「半単項式作用と有理性問題」の代数的トーラスの有理性問題の節を参照)．そこで，星-山崎 [HY] と長谷川-星-山崎 [HHY] において低い次元のノルム 1 トーラスの安定（レトラクト）有理性について，GAP を用いて分類を行った．

以下 $K/k$ を $n$ 次分離拡大，$L/k$ を $K/k$ のガロア閉包，$G = \mathrm{Gal}(L/k)$ を $n$ 次対称群 $S_n$ の可移部分群とみなし, $H = \mathrm{Gal}(L/K)$ とする．

星-山崎 [HY] では，$n = p$ (奇素数)， $n \leq 10$ に対して，安定 (レトラクト) 有理的な $n-1$ 次元のノルム 1 トーラス $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ の分類を，以下の安定有理性を除き，あたえた：

• $G = \mathrm{PSL}_2(\mathbb{F}_{2^e})$ $(n = 2^e + 1$ : フェルマー素数),

• $G \simeq 9T27 \simeq PSL_2(\mathbb{F}_8)$ $(n = 9)$,

• $10T11 \simeq A_5 \times C_2$ $(n = 10)$.

**定理 2.2** (星-山崎 [HY, Theorem 1.9]). $n = p$ (奇素数) に対して，$p-1$ 次のノルム 1 トーラス $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ はレトラクト有理的である．安定有理性は次のようになる：

(1) $G \simeq C_p \leq S_p$, $G \simeq D_p \leq S_p$ のとき，$T$ が $k$ 上安定有理的；

(2) $G \simeq C_p \rtimes C_m \leq S_p$ $(3 \leq m \mid p-1)$ のとき，$T$ は $k$ 非安定有理的；

(3) $G \simeq S_p$ $(p \geq 5)$ のとき，$T$ は $k$ 上非安定有理的；

(4) $G \simeq A_5 \leq S_5$ のとき，$T$ は $k$ 上安定有理的，

$G \simeq A_p \leq S_p$ $(p \geq 7)$ のとき，$T$ は $k$ 上非安定有理的;

(5) $G \simeq \mathrm{PSL}_2(\mathbb{F}_{11}) \leq S_{11}$ のとき，$T$ は $k$ 上非安定有理的；

(6) $G \simeq M_{11} \leq S_{11}$， $G \simeq M_{23} \leq S_{23}$ のとき，$T$ は $k$ 上非安定有理的;

(7) $\mathrm{PSL}_d(\mathbb{F}_q) \leq G \leq \mathrm{P\Gamma L}_d(\mathbb{F}_q) \simeq \mathrm{PGL}_d(\mathbb{F}_q) \rtimes C_e$ のとき，$T$ は $k$ 上非安定有理的．ここで $d \geq 3$, $p = \frac{q^d-1}{q-1}$, $q = l^e$；

(8) $\mathrm{PSL}_2(\mathbb{F}_{2^e}) < G \leq \mathrm{P\Gamma L}_2(\mathbb{F}_{2^e}) \simeq \mathrm{PSL}_2(\mathbb{F}_{2^e}) \rtimes C_e$ のとき，$T$ は $k$ 上非安定有理的．ここで $p = 2^e + 1$ はフェルマー素数.

**定理 2.3** (星-山崎 [HY, Theorem 1.11]). $n = 8, 9, 10$ に対して，$n-1$ 次のノルム 1 トーラス $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ の安定有理性，レトラクト有理性は次のようになる：

(1) $G = 8Tm$ のとき $(1 \leq m \leq 50)$.

(i) $G = 8T1 \simeq C_8$ のとき，$T$ は $k$ 上安定有理的；

(ii) $G = 8Tm$ $(2 \leq m \leq 50)$ のとき，$T$ は $k$ 上非レトラクト有理的.

(2) $G = 9Tm$ のとき $(1 \leq m \leq 34)$.

(i) $G = 9T1 \simeq C_9$，$9T3 \simeq D_9$ のとき，$T$ は $k$ 上安定有理的；

(ii) $G = 9T27 \simeq \mathrm{PSL}_2(\mathbb{F}_8)$ のとき，$T$ は $k$ 上レトラクト有理的;

(iii) $G = 9Tm$ $(2 \leq m \leq 34$ かつ $m \neq 3, 27)$ のとき，$T$ は $k$ 上非レトラクト有理的.

(3) $G = 10Tm$ のとき $(1 \leq m \leq 45)$.

(i) $G = 10T1 \simeq C_{10}$, $10T2 \simeq D_5$, $10T3 \simeq D_{10}$ のとき，$T$ は $k$ 上安定有理的；

(ii) $G = 10T11 \simeq A_5 \times C_2$ のとき，$T$ は $k$ 上レトラクト有理的;

(iii) $G = 10T4 \simeq F_{20}$, $10T5 \simeq F_{20} \times C_2$, $10T12 \simeq S_5$, $10T22 \simeq S_5 \times C_2$ のとき，$T$ は $k$ 上非安定有理的だがレトラクト有理的；

(iv) $G = 10Tm$ $(6 \leq m \leq 45$ で $m \neq 11, 12, 22)$ のとき，$T$ は $k$ 上非レトラクト有理的.

さらに長谷川-星-山崎 [HHY] では，従来用いていた flabby resolution を構成するためのプロ

グラムを改良し，上で例外となっていた $G = 10T11 \simeq A_5 \times C_2$ の安定有理性について解決し，さらに $12 \leq n \leq 15$ に対して，安定 (レトラクト) 有理的な $n-1$ 次元のノルム 1 トーラス $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ の分類について与えた．論文の中で用いている flabby resolution を構成するプログラム FlabbyResolutionFromBase.gap は山崎愛一氏のウェブページのアルゴリズムのページ (http://www.math.h.kyoto-u.ac.jp/ yamasaki/Algorithm/) からダウンロードできる．

**定理 2.4** (長谷川-星-山崎 [HHY, Theorem 1.2])**.** $n = 10, 12, 14, 15$ に対して，$n-1$ 次のノルム 1 トーラス $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ の安定有理性，レトラクト有理性は次のようになる：

(1) $G = 10T11 \simeq A_5 \times C_2$ のとき，$T$ は $k$ 上安定有理的.

(2) $G = 12Tm$ のとき $(1 \leq m \leq 301)$.

(i) $G = 12T1 \simeq C_{12}$, $12T5 \simeq C_3 \rtimes C_4$, $12T11 \simeq C_4 \times S_3$ のとき，$T$ は $k$ 上安定有理的；

(ii) $G = 12Tm$ $(1 \leq m \leq 301$ かつ $m \neq 1, 5, 11)$ のとき，$T$ は $k$ 上非レトラクト有理的.

(3) $n = 14Tm$ のとき $(1 \leq m \leq 63)$.

(i) $G = 14T1 \simeq C_{14}$, $14T2 \simeq D_7$, $14T3 \simeq D_{14}$ のとき，$T$ は $k$ 上安定有理的；

(ii) $G = 14T4 \simeq F_{42}$, $14T5 \simeq F_{21} \times C_2$, $14T7 \simeq F_{42} \times C_2$, $14T16 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \rtimes C_2$, $14T19 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \times C_2$, $14T46 \simeq S_7$, $14T47 \simeq A_7 \times C_2$, $14T49 \simeq S_7 \times C_2$ のとき，$T$ は $k$ 上非安定有理的だがレトラクト有理的；

(iii) $G = 14Tm$ $(6 \leq m \leq 63$ かつ $m \neq 7, 16, 19, 46, 47, 49)$ のとき，$T$ は $k$ 上非レトラクト有理的.

(4) $n = 15Tm$ のとき $(1 \leq m \leq 104)$.

(i) $G = 15T1 \simeq C_{15}$, $15T2 \simeq D_{15}$, $15T3 \simeq D_5 \times C_3$, $15T4 \simeq S_3 \times C_5$, $15T5 \simeq A_5$, $15T7 \simeq D_5 \times S_3$ $15T16 \simeq A_5 \times C_3 \simeq \mathrm{GL}_2(\mathbb{F}_4)$, $15T23 \simeq A_5 \times S_3$ のとき，$T$ は $k$ 上安定有理的；

(ii) $G = 15T6 \simeq C_{15} \rtimes C_4$, $15T8 \simeq F_{20} \times C_3$, $15T10 \simeq S_5$, $15T11 \simeq F_{20} \times S_3$, $15T22 \simeq (A_5 \times C_3) \rtimes C_2 \simeq \mathrm{GL}_2(\mathbb{F}_4) \rtimes C_2$, $15T24 \simeq S_5 \times C_3$, $15T29 \simeq S_5 \times S_3$ のとき，$T$ は $k$ 上非安定有理的だがレトラクト有理的；

(iii) $G = 15Tm$ $(9 \leq m \leq 104$ かつ $m \neq 10, 11, 16, 22, 23, 24, 29)$ のとき，$T$ は $k$ 上非レトラクト有理的.

**例** ($10T11 \leq S_{10}$ の場合の計算例)**.**

```
gap> Read("FlabbyResolutionFromBase.gap");

gap> J:=Norm1TorusJ(10,11);
<matrix group with 3 generators>
gap> StructureDescription(J); # 10T11=C_2 × A_5
"C2 x A5"
gap> IsInvertibleF(J); # 10T11 は retract k-rational
```

```
true
gap> T:=TransitiveGroup(10,11);
A(5)[x]2
gap> F:=FlabbyResolutionLowRankFromGroup(J,T).actionF;
<matrix group with 3 generators>
gap> Rank(F.1); # F の階数は 31
31
gap> F2:=FlabbyResolutionLowRankFromGroup(F,T).actionF;
<matrix group with 3 generators>
gap> Rank(F2.1); # [F]^fl の階数は 13
13
gap> F3:=FlabbyResolutionLowRankFromGroup(F2,T).actionF;
# 10T11 は stably k-rational
Group([ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ])
```

## 参考文献


[EM75] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85–104. Corrigenda: Nagoya Math. J. **79** (1980) 187–190.

[End11] S. Endo, *The rationality problem for norm one tori*, Nagoya Math. J. **202** (2011) 83–106.

[HHY] S. Hasegawa, A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori in small dimensions*, to appear in Math. Comp., arXiv:1811.02145.

[HY17] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. 248 (2017) no. 1176, v+215 pp.

[HY] A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori*, 12 pages. arXiv:1811.01676.

[Kun90] B. E. Kunyavskii, *Three-dimensional algebraic tori*, (Russian) Translated in Selecta Math. Soviet. **9** (1990) 1–21. Investigations in number theory (Russian), 90–111, Saratov. Gos. Univ., Saratov, 1987.

[Ono61] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. **74** (1961) 101–139.

[Sal84] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984) 165–215.

[Swa83] R. G. Swan, *Noether' s problem in Galois theory*, in "Emmy Noether in BrynMawr", edited by B. Srinivasan and J. Sally, Springer-Verlag, Berlin, 1983, pp. 2140.

[Vos67] V. E. Voskresenskii, *On two-dimensional algebraic tori II* Math. USSR Izv. **1** (1967)

691–696.

[Vos98] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, Translated from the Russian manuscript by Boris Kunyavski, Translations of Mathematical Monographs, 179, American Mathematical Society, Providence, RI, 1998.

# Norm one tori and Hasse norm principle

金井 和貴　(新潟大学)

**概要**

本稿は第 27 回整数論サマースクール「構成的ガロアの逆問題と不変体の有理性問題」における講演「Norm one tori and Hasse norm principle」のレジュメである．

Hasse norm principle(HNP) とは代数体の拡大に対して局所的な norm の束ね合わせと大域的な norm の “ずれ” が存在しないことを表す原理であり，Hasse により巡回拡大に対して成立することが示された．しかしながら一般には未解決である．本講演ではまずノルム 1 トーラスを用いた HNP の不変量のコホモロジカルな表示を与える．その後，HNP の近年の進展とトーラスの有理性問題の関係について述べる．

## 1　Hasse principle (HP) と Hasse norm principle (HNP)

代数体 $k$ 上で定義された方程式が $k$ に解を持つかという問題は古くから考えられてきた．一般に与えられた方程式が $k$ に解を持つかを判定する問題は難しく有力な方法は確立されていない．しかしながら，特定の方程式に対しては，$k$ に解を持つかという問題が，より易しい $k$ の任意の素点による完備化で解を持つかという問題に帰着されることがある．特に，二次形式に対しては Hasse-Minkowski の定理と呼ばれる次の定理が成立する．

定理 **1.1** (Hasse-Minkowski の定理 1921)**.** $k$ を代数体とし，$f$ を $k$ 上の二次形式とする．このとき以下は同値:

(i) $f = 0$ が $k$ に非自明解を持つ.
(ii) $f = 0$ が任意の $k$ の素点 $v$ による完備化 $k_v$ に非自明解を持つ.

このように，“方程式が $k$ に解を持つこと” と “方程式が $k$ の任意の素点による完備化で解を持つこと” が同値になるときに Hasse principle (HP) が成立すると呼ぶ[*1]．しかしながら，3 次以上の形式に対しては一般に HP が成立しないことが知られている:

定理 **1.2** (Selmer [Sel51])**.** $f = 3x^3 + 4y^3 + 5z^3$ とする．このとき，$f = 0$ は任意の $\mathbb{Q}$ の素点 $v$ による完備化 $\mathbb{Q}_v$(すなわち任意の $p$ 進数体 $\mathbb{Q}_p$ と実数体 $\mathbb{R}$) に非自明な解を持つが，$\mathbb{Q}$ に非自明解を持たない.

一般の $n$ 次形式に対して HP を考えることは二次形式に比べはるかに難しい．本稿では切り口

[*1] この原理は局所大域原理とも呼ばれる.

を変え，一般の $n$ 次形式へ向かうのではなく，代数体の拡大のノルムから定まる形式に対しての HP とも言える “Hasse norm principle (HNP)” を主題にする．

HNP の定義を与えよう．$F/k$ を代数体の有限次拡大とする．このとき，$N_{F/k} : F \to k$ をノルム写像とする．$J_k$ を $k$ のイデール群とする．$k$ のイデール $J_k$ と $F$ のイデール $J_F$ に対してもノルム写像が

$$\mathrm{N}_{F/k} : J_F \longrightarrow J_k; \quad (a_w)_w \longmapsto \left( \prod_{w|v} N_{F_w/k_v}(a_w) \right)_v$$

により定義される．また，$J_k$ は $\prod_v k_v^\times$ の部分群であり，$k$ の素点 $v$ に対して $k \hookrightarrow k_v$ であることから，$k^\times$ は $J_k$ に対角的に埋め込まれる．このとき

$$Ш(F/k) := (N_{F/k}(J_F) \cap k^\times)/N_{F/k}(F^\times)$$

と置く．これは局所的なノルムの像の束ね合わせと大域的なノルムの像の “ずれ” を表している．つまり

$$Ш(F/k) = \frac{\{a \in k^\times \mid \text{任意の局所的なノルム写像の像}\}}{\{a \in k^\times \mid \text{大域的なノルムの像}\}}$$

である．$Ш(F/k) = 0$ となるとき，$F/k$ に対して HNP が成立するという Hasse は巡回拡大に対して HNP が成立することを示した：

定理 **1.3** (Hasse のノルム定理 [Has31, Satz, page 64])．$L/k$ を代数体の巡回拡大とする．このとき

$$Ш(L/k) = 0.$$

証明は次節において，ガロア拡大 $L/k$ に対する $Ш(L/k)$ の考察を行うことによって与える．

注意 **1.4.** Hasse-Minkowskii の定理から二次拡大に対して HNP が成立することがわかる：

$L/k$ を二次拡大とする．このとき，$L = k(\sqrt{d})$ となる平方因子を持たない整数 $d$ が存在する．したがって，二次拡大 $L/k$ から Norm 形式 $f = X^2 + dY^2$ が定まる．$a \in k$ に対して，$f = a$ の斉次化 $F = X^2 + dY^2 - aZ^2 = 0$ を考えれば二次形式となるため，Hasse-Minkowskii の定理より，$k$ の任意の局所化において解を持つことと $k$ において解を持つことが同値となる (このとき $Z = 0$ となる解は，$d$ が平方因子を持たないことから自明解となってしまうことに注意する)．すなわち二次拡大 $L/k$ に対する HNP が成立する．

Hasse [Has31] では双二次拡大 $\mathbb{Q}(\sqrt{-39}, \sqrt{-3})/\mathbb{Q}$ に対して $Ш(L/k) \neq 0$ となることも述べている．しかしながら，双二次拡大であれば必ず $Ш(L/k) \neq 0$ となるというわけでもない．例えば $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$ とすれば $Ш(L/k) = 0$ となる．これらの例の差はなんであろうか．

本稿の前半においては，$Ш(F/k)$ を代数的 $k$ トーラスの視点から見直すことにより，コホモロジーを用いて記述し，この疑問への解答を与えることを目標とする．

また，後半においては，代数的トーラスの有理性問題と HNP の関係を明らかにすることを目標とする．

## 2　ノルム 1 トーラスと HNP

本節ではいくつかのコホモロジーについての事実を証明なしに用いることで，ガロア拡大 $L/k$ に対して $Ш(L/k)$ の $\mathbb{Z}$ の群コホモロジーを用いた記述を与える．Tate [Tat67] では類体論の文脈で $Ш(L/k)$ のコホモロジーを用いた記述を与えているが，本節では主に [PR94, Chapter 6.3] と [Vos98, Chapter 4.11] に基づき代数的トーラスの立場からこれを与える．また代数的トーラスの基本的な性質については本サマースクール長谷川氏の稿を参照されたい．

記号の準備を行う．$T$ を代数的 $k$ トーラスする．$T$ に対して $k$ の有限次ガロア拡大である分解体 $L$ が存在する．$G := \mathrm{Gal}(L/k)$ とする．$T(k)$ で $T$ の $k$ 有理点を表す．$k$ のアデールを $A_k$ で表し[*2]，$T$ のアデール環上の点を $T(A_k)$ とする[*3]．また，$C_k := J_k/k^\times$, $C_k(T) := T(A_k)/T(k)$ と置く．$T$ の指標加群を $X(T) := \mathrm{Hom}(T, \mathbb{G}_\mathrm{m})$ とし，$X_*(T) := \mathrm{Hom}(\mathbb{G}_\mathrm{m}, T)$ とする．

以降 $L/k$ のガロア群 $G$ と $G$ 加群 $M$ に対するガロアコホモロジー $H^i(G, M)$ を $H^i(L/k, M)$ でも表す．また，$k$ の絶対ガロア群 $G_k$ に対するコホモロジー $H^i(G_k, M)$ を $H^i(k, M)$ で表す．

代数群 $M$ の $k$ 点 $M(k)$ には絶対ガロア群が自然に作用する．したがって $H^i(k, M) := H^i(G_k, M(k))$ により，ガロアコホモロジーを考えることができる．

必要となる群コホモロジーに関する定理を述べよう．まず，次の定理が重要となる．

定理 **2.1** (Tate [Tat66])**.** $G$ を有限群，$M$ を $G$ 加群，$u \in H^2(G, M)$ とする．$G_p$ を $G$ の各シロー $p$ 部分群とする．このとき，$M$ が次の条件を満たすとする:

(i) 任意の素数 $p$ に対して，$H^1(G_p, M) = 0$,
(ii) $H^2(G_p, M)$ は $G_p$ と同じ位数の巡回群であり，$\mathrm{Res}^G_{G_p}(u)$ により生成される．ここで $\mathrm{Res}^G_{G_p}$ は $H^2(G, M)$ から $H^2(G_p, M)$ への制限写像.

このとき，任意の有限生成かつ tosion-free な $G$ 加群 $N$，$G$ の任意の部分群 $H$，任意の整数 $i$ に対して，$u$ とカップ積により定義される写像

$$\widehat{H}^i(H, N) \longrightarrow \widehat{H}^{i+2}(H, M \otimes N);\ a \longmapsto u \cup a$$

は同型写像となる．ここで $\widehat{H}$ は Tate コホモロジーを表す.

$k$ を局所体，$L/k$ を有限次ガロア拡大とすると，局所類体論から，$M = L^\times$ に対して $u_{L/k} \in H^2(L/k, L^\times)$ が一意的に定まり，定理 2.1 の仮定を満たすことが知られている．また，$k$ を代数体のときも，大域類体論から，$M = C_L$ のとき $u_{L/k} \in H^2(L/k, C_L)$ が一意的に定まり，定理 2.1 の仮定を満たす (詳細は [Tat67] 参照)．これらのことから，定理 2.1 より次が成り立つ.

---

[*2] $S$ をすべての無限素点を含む $k$ の素点の有限集合とする．$A_S := \prod_{v \in S} k_v \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}$ と置くと位相環となる．ここで，$A_k := \bigcup_S A_S$ は $S$ の包含関係による帰納極限で再び位相環となる．これを $k$ のアデールと呼んでいた.

[*3] $k$ 上の代数多様体のアデール環上の点 (アデール多様体)$V(A_k)$ は $k$ のアデールの定義と同様の手続きで得られる．すなわち，$S$ をすべての無限素点を含む $k$ の素点の有限集合とし，$V(A_S) := \prod_{v \in S} V(k_v) \times \prod_{\mathfrak{p} \notin S} V(\mathcal{O}_\mathfrak{p})$ と置き，$V(A_k) := \bigcup_S V(A_S)$ に対して，$S$ の包含関係に関しての帰納極限により位相を定義すればよい.

定理 **2.2** (Nakayama-Tate)**.** $T$ を代数的 $k$ トーラスとし，$L$ を $T$ の分解体とし，$G := \mathrm{Gal}(L/k)$ とする．$i$ を任意の整数とすると次が成立する．

(i) $k$ を局所体とする．このとき

$$\widehat{H}^i(G, T) \simeq \widehat{H}^{2-i}(G, X_*(T)).$$

(ii) $k$ を代数体とする．このとき

$$\widehat{H}^i(G, C_L(T)) \simeq \widehat{H}^{2-i}(G, X_*(T)).$$

ここで，$L/k$ を体 $k$ の有限次ガロア拡大

$$P^i(L/K, T) := \ker(\widehat{H}^i(L/k, T) \to \prod_v \widehat{H}^i(L_w/k_v, T))$$

と置き，特に $i = 1$ のとき $Ш(T) := P^1(L/K, T)$ と置く．

補題 **2.3** ([Vos98, Theorem, page 120], [PR94, Proposition 6.7, page 298])**.** $k$ を代数体，$T$ を代数的 $k$ トーラス，$L/k$ を有限次ガロア拡大とする．このとき，整数 $i \geq 1$ に対して

$$H^i(L/k, T(A_L)) \simeq \bigoplus_v H^i(L_w/k_v, T).$$

注意 **2.4.** 補題 2.3 は代数体 $k$ 上の可換代数群に対しても成立する．

この補題と定理 2.2 を用いれば $P^i(L/K, T)$ の $\mathbb{Z}$ のコホモロジーを用いた表示が得られる：

定理 **2.5.** $k$ を代数体，$T$ を代数的 $k$ トーラス，$L/k$ を有限次ガロア拡大である $T$ の分解体とし，$G := \mathrm{Gal}(L/k)$ とする．このとき

$$P^i(L/K, T) \simeq \ker(\widehat{H}^{3-i}(L/k, X(T)) \xrightarrow{\mathrm{Res}^G_{G_w}} \prod_v \widehat{H}^{3-i}(L_w/k_v, X(T))).$$

ここで $G_v$ は $v$ の分解群である．

証明**.** 完全系列

$$1 \to T(L) \to T(A_L) \to C_L(T) \to 1$$

に対して，コホモロジーの長完全系列を取れば

$$\cdots \to \widehat{H}^{i-1}(L/k, T(A_L)) \xrightarrow{g} \widehat{H}^{i-1}(L/k, C_L(T)) \to \widehat{H}^i(L/k, T) \xrightarrow{f} \widehat{H}^i(L/k, T(A_L)) \to \cdots$$

となる．このとき，補題 2.3 から

$$\widehat{H}^i(L/k, T(A_L)) \simeq \bigoplus_v \widehat{H}^i(L_w/k_v, T)$$

である．今，$G_v := \mathrm{Gal}(L_w/k_v)$ を $v$ の分解群とすると，$g = \bigoplus_v \mathrm{Cor}_{G_v}^G$ となる (詳細は [PR94, Proposition 6.8, page 304])．したがって，$P^i(L/K,T) = \ker f$ となる．また，完全性から $\ker f = \mathrm{coker}\, g$ であるから，補題 2.3 と定理 2.2 から

$$\begin{aligned} P^i(L/K,T) = \ker f &= \mathrm{coker}(\bigoplus_v \widehat{H}^{i-1}(L_w/k_v, T(A_L)) \xrightarrow{g} \widehat{H}^{i-1}(L/k, C_L(T))) \\ &= \mathrm{coker}(\bigoplus_v \widehat{H}^{i-3}(L_w/k_v, X_*(T)) \xrightarrow{g} \widehat{H}^{i-3}(L/k, X_*(T))). \end{aligned}$$

双対性から，

$$P^i(L/K,T) = \ker(\widehat{H}^{3-i}(L/k, X(T)) \xrightarrow{\prod_v \mathrm{Res}_{G_v}^G} \prod_v \widehat{H}^{3-i}(L_w/k_v, X(T)))$$

を得る． □

$Ш(T)$ と $Ш(F/k)$ には以下のような関係がある．

定理 **2.6.** $F/k$ を代数体の有限次拡大，$T$ をノルム 1 トーラス $T := R_{F/k}^{(1)}(\mathbb{G}_\mathrm{m})$ とする．このとき

$$Ш(F/k) \simeq Ш(T)$$

証明．$S := R_{F/k}(\mathbb{G}_\mathrm{m})$ とすれば、完全系列

$$1 \to T \to S \xrightarrow{N_{F/k}} \mathbb{G}_\mathrm{m} \to 0 \tag{1}$$

がある．コホモロジーの長完全系列をとれば，

$$P^\times \xrightarrow{N_{P/k}} k^\times \to H^1(k,T) \to H^1(k,S)$$

となり，Shapiro の補題と Hilbert の定理 90 より

$$H^1(k,S) \simeq H^1(F, \mathbb{G}_\mathrm{m}) = 1$$

であるから

$$H^1(k,T) \simeq k^\times / N_{F/k}(F^\times)$$

を得る．(1) より

$$1 \to T(A_{\bar{k}}) \to S(A_{\bar{k}}) \xrightarrow{N_{F/k}} A_{\bar{k}}^\times \to 1$$

が完全となるから，再びコホモロジーの長完全系列と Hilbert の定理 90 より

$$A_F^\times \xrightarrow{N_{F/k}} A_k^\times \to H^1(k, T(A_{\bar{k}})) \to H^1(K, S(A_{\bar{k}})) \subset \varinjlim \prod_v H^1(F_w/K_v, S) = 1$$

となる (最後の包含の詳細は [PR94, Proposition 6.6, page 297])． したがって

$$H^1(k, T_{A_{\bar{k}}}) \simeq J_k / N_{F/k}(J_F)$$

を得る．したがって，

$$\begin{aligned}
Ш(T) &= P^1(F/k, T) \\
&= \ker(H^1(F/k, T) \to \prod_v H^1(F_w/k_v, T)) \\
&= \ker(H^1(F/k, T) \to H^1(k, T(A_{\bar{k}}))) \\
&= \ker(k^\times/N_{F/k}(F^\times) \to J_k/N_{F/k}(J_F)) \\
&= (N_{F/k}(J_F) \cap k^\times)/N_{F/k}(F^\times) \\
&= Ш(F/k).
\end{aligned}$$

□

$L/k$ がガロア拡大ならばより具体的な公式が得られる．

定理 **2.7** (Tate [Tat67])．$L/k$ を代数体の有限次ガロア拡大とし，$G := \mathrm{Gal}(L/k)$ とする．このとき

$$Ш(L/k) \simeq \ker(H^3(G, \mathbb{Z}) \xrightarrow{\prod_v \mathrm{Res}^G_{G_v}} \prod_v H^3(G_v, \mathbb{Z})).$$

証明．定理 2.6 より，

$$Ш(T) = \ker(H^3(G, \mathbb{Z}) \xrightarrow{\prod_v \mathrm{Res}^G_{G_v}} \prod_v H^3(G_v, \mathbb{Z}))$$

を示せば良い．

ノルム 1 トーラス $T := R^{(1)}_{L/k}(\mathbb{G}_\mathrm{m})$ に対して，

$$X(R^{(1)}_{L/k}(\mathbb{G}_\mathrm{m})) \simeq J_G$$

より，完全系列

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to X(T) \to 0$$

が存在する．コホモロジーの長完全系列を取れば

$$H^2(G, \mathbb{Z}[G]) \to H^2(G, X(T)) \to H^3(G, \mathbb{Z}) \to H^3(G, \mathbb{Z}[G])$$

となる．$\mathbb{Z}[G]$ は $G$ 誘導加群だから $n \geq 1$ に対して $H^n(G, \mathbb{Z}[G]) = 0$．したがって

$$H^2(G, X(T)) \simeq H^3(G, \mathbb{Z})$$

となる．定理 2.5 において $i = 1$ とすれば

$$Ш(L/k) \simeq \ker(H^3(G, \mathbb{Z}) \xrightarrow{\prod_v \mathrm{Res}^G_{G_v}} \prod_v H^3(G_v, \mathbb{Z})).$$

□

したがって，巡回拡大 $L/k$，$G := \mathrm{Gal}(L/k)$ に対して，$H^3(G,\mathbb{Z}) = H^1(G,\mathbb{Z}) = 0$ であることから，Hasse のノルム定理 (定理 1.3) が成立することがただちにわかる．

系 **2.8.** $L/k$ を代数体の有限次ガロア拡大とする．このとき，$k$ の素点 $v$ の分解群がすべて巡回群ならば，

$$Ш(L/k) = H^3(G,\mathbb{Z}).$$

証明．定理 3 から，$k$ の素点 $v$ の分解群がすべて巡回群ならば，

$$\prod_v H^3(G_v,\mathbb{Z}) = \prod_v H^1(G_v,\mathbb{Z}) = 0$$

より

$$Ш(L/k) = H^3(G,\mathbb{Z})$$

となる． □

これらのことを踏まえると，前節の最後の疑問の答えが得られる．

例 **2.9** ($V_4$ 拡大の HNP)．$k = \mathbb{Q}$ とし，$L_1 = \mathbb{Q}(\sqrt{-39},\sqrt{-3}), L_2 = \mathbb{Q}(\sqrt{2},\sqrt{-1})$ とする．このとき，$\mathrm{Gal}(L_i/k) \simeq V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．それぞれの分解群について考えよう．Hilbert の分岐理論から，“素数 $p$ が不分岐”⇔“$p$ の分解群が巡回群” であることに注意しておく．また，いずれの場合も $\mathbb{Q}$ 上総虚な 4 次拡大であるから，無限素点は 2 個に分解しいずれも分岐指数 2 となる．すなわち，無限素点の分解群は位数 2 の巡回群となる．

・$L_1$ の場合：$L_1 = \mathbb{Q}(\sqrt{-39},\sqrt{-3}) = \mathbb{Q}(\sqrt{13},\sqrt{-3})$ であり 13 と $-3$ は mod4 で 1 だから，絶対判別式は $13^2 \cdot (-3)^2$ となる．したがって，分岐する素数は $13, 3$ のみである．

平方剰余記号を用いれば $\left(\frac{13}{3}\right) = \left(\frac{3}{13}\right) = 1$ となるから，3 は $\mathbb{Q}(\sqrt{13})$ において分解，13 は $\mathbb{Q}(\sqrt{-3})$ において分解することがわかる．分岐指数を $e$, 惰性次数を $f$, 分解の個数を $g$ とすると，$4 = [L:k] = efg$ であり，分解群の位数は $ef$ である．$g \geq 2$ であるから, $ef \leq 2$ となる．位数 2 の群は巡回群であるから，任意の分解群が巡回群となることがわかる．

したがって系 2.8 より，

$$Ш(L/k) = H^3(V_4,\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$$

・$L_2$ の場合：$L_1 = \mathbb{Q}(\sqrt{2},\sqrt{-1}) = \mathbb{Q}(\zeta_8)$ より，分岐する素数は 2 のみであり，2 は完全分岐している．したがって 2 の分解群 $D_2 \simeq V_4$ となる．したがって

$$\prod_v H^3(G_v,\mathbb{Z}) \simeq H^3(G,\mathbb{Z})$$

となる．制限写像の定義より $\mathrm{Res}^G_G$ は同型になる．すなわち

$$Ш(L/k) = 0.$$

## 3　非ガロア拡大の HNP

前節を踏まえて，非ガロア拡大の HNP に対する Drakokrust-Platonov [DP87] のアプローチを紹介する．

$F/k$ を代数体の有限次拡大とする．ノルム 1 トーラス $T := R^{(1)}_{F/k}(\mathbb{G}_{\mathrm{m}})$ に対して，$T$ が分裂するような $F$ を含むガロア拡大 $L/k$ で $T$ が存在する．$G := \mathrm{Gal}(L/k), H := \mathrm{Gal}(L/F)$ とする．このとき，$X(T) \simeq J_{G/H}$ より，完全系列

$$0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to X(T) \to 0$$

が存在する．このとき，前節の定理 2.7 の議論を踏襲し，上の系列のコホモロジーの長完全系列を取り，次の可換図式を考える：

$$\begin{array}{ccccc} H^2(G,\mathbb{Z}) & \xrightarrow{\phi_1} & H^2(G,\mathbb{Z}[G/H]) & \xrightarrow{\phi_2} & H^2(G,X(T)) \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} \\ \prod_v H^2(G_v,\mathbb{Z}) & \xrightarrow{\psi_1} & \prod_v H^2(G_v,\mathbb{Z}[G/H]) & \xrightarrow{\psi_2} & \prod_v H^2(G_v,X(T)) \end{array}$$

$$\begin{array}{ccccc} \xrightarrow{\phi_3} & H^3(G,\mathbb{Z}) & \xrightarrow{\phi_4} & H^3(G,\mathbb{Z}[G/H]) \\ & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ \xrightarrow{\psi_3} & \prod_v H^3(G_v,\mathbb{Z}) & \xrightarrow{\psi_4} & \prod_v H^3(G_v,\mathbb{Z}[G/H]) \end{array} \tag{2}$$

定理では $\mathbb{Z}[G]$ が $G$ 誘導加群であることから，$n \geq 1$ に対して $H^n(G,\mathbb{Z}[G]) = 0$ となっていたが，今回の系列では $\mathbb{Z}[G/H]$ となっており，$G$ 誘導加群ではないため，定理と同様の結果が得られない．

この図式において $Ш(T) = P^1(L/K,T) \simeq \ker \alpha_3$ である．ここで

$$\mathrm{Obs}_1(L/F/k) := \alpha_2^{-1}(\mathrm{Im}\,\psi_1)/\,\mathrm{Im}\,\phi_1$$

と置けば，$\mathrm{Obs}_1(F/k)$ は $Ш(T)$ に埋め込まれる．

実際には，$\mathrm{Obs}_1(L/F/k) \simeq Ш(F/k)/(k^\times \cap N_{L/k}(J_L))$ となることもわかる．証明には次の可換図式を用いる：

$$\begin{array}{ccc} \widehat{H}^0(H,C_F) & \xrightarrow{\mu_1} & \widehat{H}^0(G,C_F) \\ \uparrow{\scriptstyle \delta_1} & & \uparrow{\scriptstyle \delta_2} \\ \widehat{H}^0(H,J_F) & \xrightarrow{\mu_2} & \widehat{H}^0(G,J_F) \end{array}$$

ここで，$\mu_i = \mathrm{Cor}^H_G = N_{L/K}$，$\delta_i$ は $J_F \to C_F$ から誘導されるとする．この可換図式が後述する定理 3.1 における可換図式 (3) と等しいことから主張が従う．詳細は [DP87].

$\mathrm{Obs}_1(F/k)$ は群のアーベル化を用いて書くことができ，$Ш(T)$ に比べ遥かに計算しやすい．

定理 **3.1** (Drakokhrust-Platonov [PD85a, page 350], [PD85b, pages 789–790], [DP87, Theorem 1]). $F/k$ を代数体の有限次拡大とし，$L/k$ を $F$ を含むガロア拡大，$G := \mathrm{Gal}(L/k), H := \mathrm{Gal}(L/F)$ とする．このとき，

$$\mathrm{Obs}_1(L/F/k) \simeq \mathrm{Ker}\,\mu_1/\delta_1(\mathrm{Ker}\,\mu_2)$$

ここで

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\mu_1} & G/[G,G] \\ \uparrow{\scriptstyle \delta_1} & & \uparrow{\scriptstyle \delta_2} \\ \displaystyle\bigoplus_{v\in V_k}\left(\bigoplus_{w|v} H_w/[H_w,H_w]\right) & \xrightarrow{\mu_2} & \displaystyle\bigoplus_{v\in V_k} G_v/[G_v,G_v] \end{array} \tag{3}$$

であり，$\mu_1$, $\delta_1, \delta_2$ はそれぞれ包含 $H \subset G$, $H_w \subset H, G_v \subset G$ から定義され，$\mu_2$ は $h \in H_w = H \cap x^{-1}hx[G_v, G_v]$ $(x \in G)$ に対して

$$\mu_2(h[H_w, H_w]) = x^{-1}hx[G_v, G_v]$$

で定義される．

証明．可換図式 (2) を書き換えていく．$\mathbb{Z}[G/H] = \mathrm{Ind}_H^G(\mathbb{Z})$ である．ここで Ind は誘導加群を表す．Shapiro の補題より，

$$H^2(G, \mathbb{Z}[G/H]) \simeq H^2(H, \mathbb{Z})$$

となる．

また，$k$ の各素点 $v$ に対して，$v$ の $L$ への延長 $w$ をとり，$G_v := \mathrm{Gal}(L_w/k_v)$ を $v$ の $L$ に対する分解群，$v$ の $F$ への延長のなす集合 $W_v$ とすれば，

$$G_v \setminus G/H \to W_v\,;\, G_v\sigma H \mapsto w \circ \sigma\,|_F$$

により 1 対 1 対応が得られる．$G$ は両側剰余類分解により $G = \oplus_{i=1}^{r_v} G_v x_i^v H$ となる．よって，$\mathbb{Z}[G/H] \simeq \oplus_{i=1}^{r_v}\mathbb{Z}[M_i^v/H]$, $M_i^v = G_v x_i^v H\,(i = 1, \ldots, r_v)$ と $G_v$ 加群の直和に分解できる．$H_i^v := x_i^v H (x_i^v)^{-1} \cap G_v$ と置くと，$\mathbb{Z}[M_i^v/H] = \mathrm{Ind}_{H_i^v}^{G_v}(\mathbb{Z})$ となる．Shapiro の補題から

$$H^2(G_v, \mathbb{Z}[G/H]) \simeq \bigoplus_{i=1}^{r_v} H^2(H_i^v, \mathbb{Z})$$

となる．$H^2(G, \mathbb{Z}) \simeq H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ であるから，可換図式 (2) は

$$\begin{array}{ccc} H^1(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & H^1(H, \mathbb{Q}/\mathbb{Z}) \\ \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \beta_2} \\ \displaystyle\prod_v H^1(G_v, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\psi} & \displaystyle\prod_v \bigoplus_{i=1}^{r_v} H^1(H_i^v, \mathbb{Q}/\mathbb{Z}) \end{array} \tag{4}$$

と等しい．すなわち $\mathrm{Obs}_1(L/F/k) \simeq \mathrm{Ker}\,\beta_2^{-1}(\mathrm{Im}\,\psi)/\mathrm{Im}\,\varphi$ である．有限群 $\mathcal{F}$ に対して，$H^1(\mathcal{F}, \mathbb{Q}/\mathbb{Z})$ は $\mathcal{F}$ のアーベル化 $\mathcal{F}^{ab} = \mathcal{F}/[\mathcal{F}, \mathcal{F}]$ の双対であるから，可換図式 (4) の双対を取れば

$$\begin{array}{ccc} G/[G,G] & \xleftarrow{\mu_1} & H/[H,H] \\ \uparrow{\scriptstyle \delta_2} & & \uparrow{\scriptstyle \delta_1} \\ \displaystyle\bigoplus_{v\in V_k} G_v/[G_v,G_v] & \xleftarrow{\mu_2} & \displaystyle\bigoplus_{v\in V_k}\left(\bigoplus_{w|v} H_w/[H_w,H_w]\right) \end{array}$$

が得られる． □

[DP87] ではこの定理と，$F/k$ の拡大次数 $n$ が $pq(p, q$ は互いに素な素数) であるときに $F$ を含むガロア拡大 $L$ に対して $\mathrm{Obs}_1(L/F/k) = Ш(F/k)$ となることを用いて，$n = 6$ の場合に HNP が成立するための必要十分条件を与え，$n = 10$ の場合の実例も扱っている．

本稿では証明は述べられないが，$\mathrm{Obs}_1(L/F/k)$ と $Ш(F/k)$ の関係について述べた次の定理は非常に重要である．

定理 **3.2** (Drakokhrust[Dra89, Theorem 1, page 32], Opolka [Opo80, Satz 4])．$F/k$ を代数体の有限次拡大とし，$L/k$ を $F$ を含むガロア拡大，$G := \mathrm{Gal}(L/k), H := \mathrm{Gal}(L/F)$ とする．さらに，$\widetilde{L}/k$ を $L$ を含むガロア拡大で，$\widetilde{G} = \mathrm{Gal}(\widetilde{L}/k)$ が中心拡大

$$1 \to \widetilde{M} \to \widetilde{G} \to G \to 1$$

で $\widetilde{M} \cap [\widetilde{G}, \widetilde{G}] \simeq \widehat{H}^3(G, \mathbb{Z})$ を満たすとする (このような $\widetilde{G}$ を $G$ の Schur cover と呼ぶ)．また，$\widetilde{H} = \mathrm{Gal}(\widetilde{L}/F)$ と置く．このとき，

$$Ш(F/k) = \mathrm{Obs}_1(\widetilde{L}/F/k).$$

すなわち，任意の有限次拡大の $Ш(F/k)$ の計算は特別なガロア拡大 $\widetilde{L}$ の $\mathrm{Obs}_1(\widetilde{L}/F/k)$ を求めることに帰着される．しかしながら，実際に $\widetilde{G}$ を求めることは容易ではないことに注意しておく．

## 4 トーラスの有理性問題と HNP

$k$ を代数体，$T$ を代数的 $k$ トーラスとする．$\overline{T(k)}$ で $T(k)$ の $\prod_v T_{k_v}$ での閉包を表す．このとき

$$A(T) := (\prod_v T_{k_v})/\overline{T(k)}$$

と置く．$A(T) = 0$ のとき $T$ は弱近似性を持つと言う．

次の定理は HNP と弱近似性とトーラスの有理性問題の関係を示唆する．

定理 **4.1** (Voskresenskii [Vos69, Theorem 5, page 1213], [Vos70, Theorem 6, page 9], see also [Vos98, Section 11.6, Theorem, page 120])**.** $k$ を代数体，$T$ を代数的 $k$ トーラスとし，$X$ を $T$ の非特異な $k$ コンパクト化とし，$\overline{X} := X \times_k \overline{k}$ とする．このとき，次の完全系列が存在する：

$$0 \to A(T) \to H^1(k, \operatorname{Pic}\overline{X})^\vee \to Ш(T) \to 0$$

ここで $M^\vee = \operatorname{Hom}(M, \mathbb{Q}/\mathbb{Z})$ は $M$ のポントリャーギン双対である．

注意 **4.2.** 定理 4.1 は Sansuc [San81] により，線形代数群の場合まで一般化されている．

すなわち

$$\text{“}H^1(k, \operatorname{Pic}\overline{X}) = 0\text{”} \Leftrightarrow \text{“}A(T) = 0 \text{ かつ } Ш(T) = 0\text{”}$$

であることがわかる．さらに次が成立する．

定理 **4.3** (Voskresenskii [Vos69, Section 4, page 1213])**.** $k$ を代数体，$T$ を代数的 $k$ トーラスとし，$X$ を $T$ の非特異な $k$ コンパクト化とし，$\overline{X} := X \times_k \overline{k}$ とする．このとき，次の $G$ 格子の完全系列が存在する：

$$0 \to X(T) \to \widehat{Q} \to \operatorname{Pic}\overline{X} \to 0$$

ここで $\widehat{Q}$ は置換格子であり，Pic $\overline{X}$ は flabby である．

したがって，代数的 $k$ トーラス $T$ に対して

$$\text{“}T \text{ がレトラクト有理的”} \Leftrightarrow \text{“}[X(T)]^{fl} = [\operatorname{Pic}\overline{X}] \text{ が可逆”} \Rightarrow \text{“}H^1(k, \operatorname{Pic}\overline{X}) = 0\text{”}$$

が成立する．

前節の定理 3 を思い出せばトーラスの有理性問題と HNP の関係が明らかになる．

系 **4.4.** $F/k$ を代数体の有限次拡大，$T$ をノルム 1 トーラス $T := R^{(1)}_{F/k}(\mathbb{G}_{\mathrm{m}})$ とする．このとき，$T$ がレトラクト有理的ならば $Ш(F/k) = 0$.

すなわち，ノルム 1 トーラスがレトラクト有理的であるならば HNP が成立することを意味する．非レトラクト有理的であっても $H^1(k, \operatorname{Pic}\overline{X}) = 0$ となる，すなわち HNP が成立することがあることを注意しておく．ノルム 1 トーラスの有理性については多くの研究がなされており，非ガロア拡大に対してもレトラクト有理的となるものが得られている (ノルム 1 トーラスの有理性については本サマースクールの星明考氏の「半単項式作用と有理性問題」の代数的トーラスの有理性問題の節参照されたい)．

Kunyavskii [Kun90] によって，3 次元代数的 $k$ トーラスの有理性問題は解決されている．その分類において 3 次元の代数的 $k$ トーラスは $\mathrm{GL}_3(\mathbb{Z})$ の有限部分群の 73 個の $\mathbb{Z}$ 共役類に対応して 73 ケースに分類され，そのうち非レトラクト有理的である 15 個を除き有理的であることが示されている．さらに，Kunyavskii [Kun84] では以下の結果が得られている：

定理 **4.5** (Kunyavskii [Kun84, Proposition 1])**.** $k$ を代数体，$T$ を 3 次元代数的 $k$ トーラスとし，$X$ を $T$ の非特異な $k$ コンパクト化とする．また，$F_1/k$ (resp. $F_2/k$) を 4 次拡大でガロア閉包 $L_1/k$ (resp. $L_2/k$) が $\mathrm{Gal}(L_1/k) \simeq V_4$ (resp. $\mathrm{Gal}(L_2/k) \simeq A_4$) であるものとする．このとき 15 個の非レトラクト有理的なケースに対して,

$$H^1(k, \mathrm{Pic}\,\overline{X}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & (T = R^{(1)}_{F_1/k}(\mathbb{G}_{\mathrm{m}}) \text{ または } R^{(1)}_{F_2/k}(\mathbb{G}_{\mathrm{m}})), \\ 0 & (\text{otherwise}). \end{cases}$$

特に, $T = R^{(1)}_{F_1/k}(\mathbb{G}_{\mathrm{m}})$ と $R^{(1)}_{F_2/k}(\mathbb{G}_{\mathrm{m}})$ のケースを除き $A(T) = Ш(T) = 0$ である.

非レトラクト有理的な 15 ケースのうち 2 ケースのみが $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0$ となり，この 2 ケースには $V_4$ の場合も含まれていることを述べている．これは前節の例 2.8 において $V_4$ 拡大で HNP が成立しない場合があったことと符合する.

最後に非ガロア拡大の HNP について知られている結果を以下にまとめる.

$F/k$ を有限次拡大，$F$ のガロア閉包を $L/k$ とし，$G := \mathrm{Gal}(L/k)$ とする．すなわち，$G$ は $[F : k] = n$ とすれば，対称群 $S_n$ の可移部分群となる．以下の場合に対して成り立つ.

- $[F : k] = p$ : 素数 (Bartels [Bar81a])
- $[F : k] = n$ かつ $G \simeq D_n$ (Bartels [Bar81b])
- $[F : k] = n \geq 5$ かつ $G \simeq A_n$ (Macedo arXiv 2017 [Mac])
- $[F : k] = n$ かつ $G = C_m \times D_n (m, n \geq 3$ : 奇数で $\gcd(m, n) = 1)$ (遠藤 [End11])
- $[F : k] = n$ かつ $G \simeq S_n$ (Voskresenskii-Kunyavskii [VK84])

Bartels によるもの以外はすべて有理性問題から従っている．また HNP が成立するための必要十分条件としては以下が知られている：

- (Kunyavskii [Kun84]) $[F : k] = 4$ のとき，$G \simeq V_4, A_4$ の場合を除き HNP が成立する．$G \simeq V_4, A_4$ の場合は以下が成立する：
  (i) $Ш(F/k) = \mathbb{Z}/2\mathbb{Z}$ または $Ш(F/k) = 0$,
  (ii) $Ш(F/k) = 0 \Leftrightarrow k$ の (分岐する) 素点で分解群が $V_4$ を含むものが存在する.
- (Drakokhrust-Platonov [DP87]) $[F : k] = 6$ のとき，$G \simeq A_4, A_5$ の場合を除き HNP が成立する．$G \simeq A_4, A_5$ の場合は以下が成立する：
  (i) $Ш(F/k) = \mathbb{Z}/2\mathbb{Z}$ または $Ш(F/k) = 0$,
  (ii) $Ш(F/k) = 0 \Leftrightarrow k$ の (分岐する) 素点で分解群が $V_4$ を含むものが存在する.

最後の Drakokhrust-Platonov [DP87] における $A_5$ は $S_6$ に含まれる 6 点に作用する $A_5$ であるから，Macedo [Mac] の結果には反しないことを注意しておく.

また，星-金井-山崎 [HKY] では $[F : k] = n \leq 15$ かつ $n \neq 12$ の場合に対して HNP が成立するための必要十分条件を与えている．これらの中には上記の “分解群が $V_4$ を含むものが存在する” 以外のより複雑な条件を持つケースも現れている.

例 **4.6.** $S_{10}$ に含まれる $S_6$ と同型な可移部分群 $G$ に対して次の (i), (ii) が成立する：

(i) $Ш(F/k) = \mathbb{Z}/2\mathbb{Z}$ または $Ш(F/k) = 0$,
(ii) $Ш(F/k) = 0 \Leftrightarrow k$ の (分岐する) 素点で分解群 $G_v$ が (a) または (b) を満たすものが存在する :
(a) $D_4 \leq G_v \leq A_4$
(b) $V_4 \leq G_v$ かつ任意の $1 \leq i \leq 10$ に対して $|\ \mathrm{Orb}_{V4}(i)\ | = 2$.
$G$ の $V_4$ と同型な部分群 135 個のうち (b) の条件を満たすものは 45 個である.

## 参考文献


[Bar81a] H.-J. Bartels, *Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen*, J. Algebra **70** (1981) 179–199.

[Bar81b] H.-J. Bartels, *Zur Arithmetik von Diedergruppenerweiterungen*, Math. Ann. **256** (1981) 465–473.

*Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000) 771–793.

[CTS87] J.-L. Colliot-Thélène, J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: Applications*, J. Algebra **106** (1987) 148–205.

[Dra89] Yu. A. Drakokhrust, *On the complete obstruction to the Hasse principle*, (Russian) Dokl. Akad. Nauk BSSR **30** (1986) 5–8; translation in Amer. Math. Soc. Transl. (2) **143** (1989) 29–34.

[DP87] Yu. 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** (1986) 299–322.

[End11] S. Endo, *The rationality problem for norm one tori*, Nagoya Math. J. **202** (2011) 83–106.

[EM73] S. Endo, T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973) 7–26.

[EM75] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85–104. Corrigenda: Nagoya Math. J. **79** (1980) 187–190.

[FLN18] C. Frei, D. Loughran, R. Newton, *The Hasse norm principle for abelian extensions*, Amer. J. Math. **140** (2018) 1639–1685.

[Ger77] F. Gerth III, *The Hasse norm principle in metacyclic extensions of number fields*, J. London Math. Soc. (2) **16** (1977) 203–208.

[Ger78] F. Gerth III, *The Hasse norm principle in cyclotomic number fields*, J. Reine Angew. Math. **303/304** (1978) 249–252.

[Gur78a] S. Gurak, *On the Hasse norm principle*, J. Reine Angew. Math. **299/300** (1978) 16–27.

[Gur78b] S. Gurak, *The Hasse norm principle in non-abelian extensions*, J. Reine Angew.

Math. **303/304** (1978) 314–318.

[Gur80] S. Gurak, *The Hasse norm principle in a compositum of radical extensions*, J. London Math. Soc. (2) **22** (1980) 385–397.

[HHY] S. Hasegawa, A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori in small dimensions*, 20 pages, arXiv:1811.02145.

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

[HKY] A. Hoshi, K. Kanai, A. Yamasaki, *Norm one tori and Hasse norm princile*, arXiv:1910.01469.

[HY17] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. **248** (2017) no. 1176, v+215 pp.

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

[Kun90] B. E. Kunyavskii, *Three-dimensional algebraic tori*, Selecta Math. Soviet. **9** (1990) 1–21.

[Kun07] B. E. Kunyavskii, *Algebraic tori — thirty years after*, Vestnik Samara State Univ. (2007) 198–214.

[Len74] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974) 299–325.

[Lor05] M. Lorenz, *Multiplicative invariant theory*, Encyclopaedia Math. Sci., vol. 135, Springer-Verlag, Berlin, 2005.

[Mac] A. Macedo, *The Hasse norm principle for $A_n$-extensions*, arXiv:1806.11563.

[Man74] Yu. I. Manin, *Cubic forms: algebra, geometry, arithmetic*, North-Holland Mathematical Library 4, North-Holland, Amsterdam, 1974.

[Ono61] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961) 101–139.

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

[Ono65] T. Ono, *On the relative theory of Tamagawa numbers*, Ann. of Math. (2) **82** (1965) 88–111.

[Opo80] H. Opolka, *Zur Aufl"osung zahlentheoretischer Knoten* Math. Z. **173** (1980) 95–103.

[Pla82] V. P.Platonov, *Arithmetic theory of algebraic groups*, (Russian) Uspekhi Mat. Nauk **37** (1982) 3–54; translation in Russian Math. Surveys **37** (1982) 1–62.

[PD85a] V. P. Platonov, Yu. A. Drakokhrust, *On the Hasse principle for algebraic number fields*, (Russian) Dokl. Akad. Nauk SSSR **281** (1985) 793–797; translation in Soviet

Math. Dokl. **31** (1985) 349–353.

[PD85b] V. P. Platonov, Yu. A. Drakokhrust, *The Hasse norm principle for primary extensions of algebraic number fields*, (Russian) Dokl. Akad. Nauk SSSR **285** (1985) 812–815; translation in Soviet Math. Dokl. **32** (1985) 789–792.

[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.

[Sal84] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984) 165–215.

[San81] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. Reine Angew. Math. **327** (1981) 12–80.

[Sel51] E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951) 203–362.

[Tat66] J. Tate, *The cohomology groups of tori in finite Galois extensions of number fields*, Nagoya Math. J. **27** (1966) 709–719.

[Tat67] J. Tate, *Global class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 162–203, Thompson, Washington, D.C., 1967.

[Vos67] V. E. Voskresenskii, *On two-dimensional algebraic tori II*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967) 711–716; translation in Math. USSR-Izv. **1** (1967) 691–696.

[Vos69] V. E. Voskresenskii, *The birational equivalence of linear algebraic groups*, (Russian) Dokl. Akad. Nauk SSSR **188** (1969) 978–981; erratum, ibid. 191 1969 nos., 1, 2, 3, vii; translation in Soviet Math. Dokl. **10** (1969) 1212–1215.

[Vos70] V. E. Voskresenskii, *Birational properties of linear algebraic groups*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970) 3–19; translation in Math. USSR-Izv. **4** (1970) 1–17.

[Vos74] V. E. Voskresenskii, *Stable equivalence of algebraic tori*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974) 3–10; translation in Math. USSR-Izv. **8** (1974) 1–7.

[Vos88] V. E. Voskresenskii, *Maximal tori without affect in semisimple algebraic groups*, (Russian) Mat. Zametki 44 (1988) 309–318; translation in Math. Notes **44** (1988) 651–655.

[Vos98] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, Translated from the Russian manuscript by Boris Kunyavskii, Translations of Mathematical Monographs, 179. American Mathematical Society, Providence, RI, 1998.

[VK84] V. E. Voskresenskii, B. E. Kunyavskii, *Maximal tori in semisimple algebraic groups*, Kuibyshev State Inst., Kuibyshev (1984). Deposited in VINITI March 5, 1984, No. 1269-84 Dep. (Ref. Zh. Mat. (1984), 7A405 Dep.).

# 不分岐 BRAUER 群と不変体の有理性問題

谷本　祥

Abstract. このノートは 2019 年度第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」で筆者が担当した講演の講義ノートである。前半は不分岐 Brauer 群を定義して、不変体の有理性問題（Noether の問題）への応用に焦点を当てている。後半は有限群の不分岐コホモロジーについて、Bogomolov-Böhning の最近の結果を紹介している。

Contents



## 1. 導入

$k$ を標数 0 の代数閉体とする。$k$ 上定義された代数多様体 $X$ が有理的とは、ある空でない Zariski 開集合 $U \subset X$ が存在して、$U$ は射影空間 $\mathbb{P}^n$ の開集合に同型になることをいう。言い換えると、$X$ の函数体 $k(X)$ が $k$ の純超越拡大 $k(t_1, \cdots, t_n)$ に同型になることである。代数多様体 $X$ が安定有理的とは、ある 0 以上の整数 $n$ が存在して $X \times \mathbb{P}^n$ が有理的になることをいう。

与えられた多様体が有理的かという問題は古典的な問題である。特に有名なのが Lüroth の問題であろう:

**Lüroth の問題:** 代数多様体 $X$ が射影空間からの支配的な有理写像を認めるとき（つまり単有理的のとき）、$X$ は有理的かという問題。

1 次元及び 2 次元では肯定的に解かれたが、3 次元では反例が提出されている。([IM71], [CG72], [AM72]) 同様に古典的な問題として不変体の有理性問題が挙げられる:

**Noether の問題:** $G$ を簡約群とし、$k$ 上の線形空間 $V$ に $G$ が線形に作用するとする。さらに、一般点の固定群は自明と仮定する。このとき、$V//G$ は有理的か？言い換えると $k(V)$ の不変体 $k(V)^G$ は $k$ の純超越拡大に同型かという問題。

*Date*: September 16, 2019.

この問題は、$G$ が連結群のときは、未だ未解決の問題になっている。しかし、$G$ が有限群のときは、Saltman が最初にこの問題への反例を見つけた。([Sal84]) 商空間 $V/G$ は明らかに単有理的なので Saltman の反例は Lüroth の問題への反例にもなっている。Saltman の結果は双有理不変量である不分岐 Brauer 群を使っている。不分岐 Brauer 群は安定有理的な多様体に対しては自明になるので、不分岐 Brauer 群が自明でない多様体は自動的に非安定有理的ということになる。Saltman の反例提出後、Bogomolov や Saltman が不分岐 Brauer 群を計算するための一連の公式を用意し、1986 年から 88 年にかけて Colliot-Thélène や Sansuc などが Bogomolov と Saltman の結果に関するセミナーを開催し、88 年にチリで行われた the IX Escuela Latinoamericana de Mathemáticas で講演した。その講義に基づいて講義ノート [CTS07] が作成、流布された。このノートの前半はこの講義ノート [CTS07] の解説に終始している。

後半では、[Bog92] で Bogomolov によって導入された安定コホモロジーや不分岐コホモロジーを概観する。不分岐コホモロジーは安定有理性の障害となるコホモロジーなので、有理性問題にとって非常に重要であり、Lüroth の問題や Noether の問題への反例を構成するためのキーとなる不変量である。さらに、この不分岐コホモロジーの輪積を使った計算方法を紹介する。([BB13])

それでは、このノートの概要を説明する。このノートのセクション 2 から 4 は [CTS07] のセクション 5, 6, 7 に忠実に基づいている。なので、オリジナリティは全くと言っていいほどない。ただ、もしこのノートにミスがあれば、それは筆者の責任である。セクション 2 で不分岐 Brauer 群を定義し、安定有理多様体に対して不分岐 Brauer 群が自明になることを見る。セクション 3 では一連の不分岐 Brauer 群を計算するための Bogomolov の公式 ([Bog87]) を解説する。セクション 4 では上で挙げた有限群の不変体の有理性問題（Noether の問題）への Saltman や Bogomolov の反例を紹介する。これはクラス 2 の冪零群として構成される。セクション 5 では安定コホモロジー及び不分岐コホモロジーを導入し、それに関する結果を概観する。さらにセクション 6 では Bogomolov–Böhning の結果（[BB13]）を解説する。

**謝辞:** 整数論サマースクールでの講演の機会をくださった世話人の方々に心から御礼を申し上げます。また初稿に対してコメントを付けてくださった阿部健先生と星明考先生に感謝します。筆者は日本学術振興会科研費若手研究 19K14512、稲盛財団、文科省卓越研究員制度からの助成を受けています。

## 2. 不分岐 Brauer 群

このセクションでは函数体の不分岐 Brauer 群を定義し、さらに有理函数体に対して不分岐 Brauer 群が自明となることを見る。このセクションは [CTS07, Section 5] に基づいている。$K$ を標数 0 の体とする。$K$ の絶対 Galois 群を $\mathrm{Gal}(\overline{K}/K)$ と表記する。まずは体の Brauer 群を Galois コホモロジーを使って定義する。Brauer 群は代数幾何や数論幾何の多くの場面で使われる重要な不変量である。

**定義 2.1** (体の Brauer 群)**.** 標数 0 の体 $K$ に対してその Brauer 群を $\overline{K}^{\times}$ を係数とする 2 次 Galois コホモロジーとして定義する。つまり、

$$\mathrm{Br}(K) := H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^{\times}) = H^2_{\text{ét}}(\mathrm{Spec}K, \mathbb{G}_m)$$

で Brauer 群を定義する。体の拡大 $L/K$ が与えられたとき、自然な準同型 $\mathrm{Br}(K) \to \mathrm{Br}(L)$ が得られることに注意する。

**補足 2.2.** 一般に体 $K$ の Brauer 群は $K$ 上の中心的単純環の Brauer 同値による同値類のなす群とみなせるがこのノートではそれには触れない。

次に体 $K$ の離散付値環 $A$ を考える。このノートでは $A$ の剰余体 $\kappa$ が標数 0 の場合のみを考える。環 $A$ が完備と仮定すると $A$ 及び $K$ は $\kappa[[t]]$ 及び $\kappa((t))$ と同一視できる。このことを用いると、$K_{\mathrm{nr}}$ が $K$ の最大不分岐拡大体のとき、$\mathrm{Gal}(K_{\mathrm{nr}}/K) \cong \mathrm{Gal}(\overline{\kappa}/\kappa)$ がいえ、さらに $\mathrm{Gal}(\overline{K}/K_{\mathrm{nr}})$ と $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n$ との間に同型を構成できる。ところで $\widehat{\mathbb{Z}}$ のコホモロジカル次元は 1 なので $H^2(\mathrm{Gal}(\overline{K}/K_{\mathrm{nr}}), \overline{K^\times}) = 0$ がいえる。また Hilbert の定理 90 より、$H^1(\mathrm{Gal}(\overline{K}/K_{\mathrm{nr}}), \overline{K^\times}) = 0$ も従う。従って Galois コホモロジーの膨張写像と制限写像に関する Hochschild-Serre スペクトラル系列を用いて自然な同型

$$H^2(\mathrm{Gal}(K_{\mathrm{nr}}/K), K_{\mathrm{nr}}^\times) \cong H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = \mathrm{Br}(K)$$

が得られる。ところで離散付値環 $A$ は付値 $v : K^\times \to \mathbb{Z}$ を誘導するが、これは自然に $v : K_{\mathrm{un}}^\times \to \mathbb{Z}$ へと拡張される。従って、この写像は

$$H^2(\mathrm{Gal}(K_{\mathrm{nr}}/K), K_{\mathrm{nr}}^\times) \to H^2(\mathrm{Gal}(K_{\mathrm{nr}}/K), \mathbb{Z}) = H^2(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Z})$$

を誘導する。さらに、完全列 $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ より、上の写像の終域のコホモロジーは $H^1(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Q}/\mathbb{Z})$ と同一視できる。従って、今我々は準同型

$$\mathrm{Br}(K) \to \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Q}/\mathbb{Z})$$

を得た。この写像を $\partial_A$ と表す。

$A$ が完備でない場合、$A$ に付随する付値による $K$ の完備化を $\widehat{K}$ とおくと、$\partial_A$ を $\mathrm{Br}(K) \to \mathrm{Br}(\widehat{K})$ と $\partial_{\widehat{A}} : \mathrm{Br}(\widehat{K}) \to \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Q}/\mathbb{Z})$ の合成として定義する。

これで不分岐 Brauer 群を定義する準備は整った。この群を計算し、不変体の有理性問題に応用することがこのノートの主題の一つである。

**定義 2.3** (不分岐 Brauer 群)**.** $k$ を標数 0 の体とする。$K$ を $k$ 上の函数体とする。つまり、$K$ は $k$ 上体として有限生成と仮定する。今 $A$ が $K$ の離散付値環でその剰余体が $k$ を含むもの全体を走るとする。このとき不分岐 Brauer 群 $\mathrm{Br}_{\mathrm{nr}}(K/k)$ を

$$\mathrm{Br}_{\mathrm{nr}}(K/k) = \bigcap_A \ker \partial_A \subset \mathrm{Br}(K)$$

として定義する。

**補足 2.4.** $k$ が代数閉体の場合、$k^\times$ の元は何回でも割れるため $k \subset A$ が自動的にいえる。この場合、$\mathrm{Br}_{\mathrm{nr}}(K/k)$ を $\mathrm{Br}_{\mathrm{nr}}(K)$ と省略する。

有理函数体の不分岐 Brauer 群が自明となることを見る。まず、いくつかの補題を準備する。

**補題 2.5.** 自然な準同型 $\mathrm{Br}(k) \to \mathrm{Br}(K)$ の像は $\mathrm{Br}_{\mathrm{nr}}(K/k)$ に含まれる。

*Proof.* $\kappa$ は $k$ を含む体で $A = \kappa[[t]]$ かつ $K = \kappa((t))$ として良い。$v$ を $A$ の付値とすると、

$$\overline{k}^\times \subset K_{\mathrm{nr}}^\times \to^v \mathbb{Z}$$

は 0-写像である。従って、付値が誘導する

$$H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^\times) \to H^2(\mathrm{Gal}(K_{\mathrm{nr}}/K), K_{\mathrm{nr}}^\times) \to H^2(\mathrm{Gal}(\overline{\kappa}/\kappa), \mathbb{Z})$$

も 0-写像である。従って、題意が従う。 □

**補題 2.6.** $L/K$ を $k$ 上の函数体の拡大とする。このとき自然な準同型 $\mathrm{Br}(K) \to \mathrm{Br}(L)$ は $\mathrm{Br}_{\mathrm{nr}}(K/k)$ を $\mathrm{Br}_{\mathrm{nr}}(L/k)$ に写す。

*Proof.* $B$ を $L$ の離散付値環とする。$A = K \cap B$ とおく。$A = K$ のとき、題意は先ほどの補題と同様に従う。そこで $A$ も離散付値環とする。$\pi$ を $A$ の一意元とする。$e = v_B(\pi)$ とおくと、可換図式

$$\begin{array}{ccc} \mathrm{Br}(L) & \xrightarrow{\partial_B} & H^2(\mathrm{Gal}(\overline{\kappa_B}/\kappa_B), \mathbb{Z}) \\ {\scriptstyle \mathrm{Res}_{L/K}}\uparrow & & \uparrow{\scriptstyle e\cdot\mathrm{Res}_{\kappa_B/\kappa_A}} \\ \mathrm{Br}(K) & \xrightarrow{\partial_A} & H^2(\mathrm{Gal}(\overline{\kappa_A}/\kappa_A), \mathbb{Z}) \end{array} \tag{2.1}$$

が成り立つ。従って題意が従う。 □

まず体 $K$ が $k$ 上の一変数有理函数体のときの不分岐 Brauer 群の自明性を見る。

**補題 2.7.** $k$ を体とし $K = k(t)$ を $k$ 上の一変数有理函数体とする。このとき自然な準同型 $\mathrm{Br}(k) \to \mathrm{Br}_{\mathrm{nr}}(K/k)$ は同型となる。

*Proof.* $k$ が代数閉体のとき、Tsen の定理より $k(t)$ はいわゆる $C_1$-体だということがいえ、それより $\mathrm{Br}(k(t)) = 0$ が従う。一般の場合は [CTS07, Lemma 5.6] を参照されたい。 □

次の命題がこのセクションの主結果といえる。

**命題 2.8.** $K$ を体 $k$ 上の函数体とする。このとき、準同型 $\mathrm{Br}(K) \to \mathrm{Br}(K(t))$ は同型

$$\mathrm{Br}_{\mathrm{nr}}(K/k) \to \mathrm{Br}_{\mathrm{nr}}(K(t)/k)$$

を誘導する。特に $K$ が有理的なとき（またはより弱く安定有理的なとき）、自然な準同型

$$\mathrm{Br}(k) \to \mathrm{Br}_{\mathrm{nr}}(K/k)$$

は同型となる。

*Proof.* 最初の主張を示せば十分である。$L = K(t)$ とおく。補題 2.7 より $\mathrm{Br}(K) \to \mathrm{Br}(K(t))$ は単射であり、補題 2.6 より包含写像 $\mathrm{Br}_{\mathrm{nr}}(K/k) \subset \mathrm{Br}_{\mathrm{nr}}(L/k)$ が定まる。任意の $\alpha \in \mathrm{Br}_{\mathrm{nr}}(L/k)$ は明らかに $\mathrm{Br}_{\mathrm{nr}}(L/K) = \mathrm{Br}_{\mathrm{nr}}(K(t)/K)$ に含まれ、$\mathrm{Br}_{\mathrm{nr}}(K(t)/K)$ は $\mathrm{Br}(K)$ と一致する。従って $\alpha \in \mathrm{Br}(K)$ が $\mathrm{Br}(K(t))$ の中で $k$ 上不分岐のとき、$\alpha \in \mathrm{Br}_{\mathrm{nr}}(K/k)$ がいえることを示せば良い。

$A$ を $K$ の離散付値環とする。$\pi$ を $A$ の一意元とする。$B$ を $A[t]$ の $\pi A[t]$ による局所化とすると $\kappa_B = \kappa_A(t)$ がいえ、これより

$$\mathrm{Res}_{\kappa_B/\kappa_A} : \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa_A}/\kappa_A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa_B}/\kappa_B), \mathbb{Q}/\mathbb{Z})$$

は単射がいえる。従って主張は (2.1) より従う。

□

次に不分岐 Brauer 群とスキームの Brauer 群の関係を見る。一般にスキームの Brauer 群はエタールコホモロジーを使って定義できる。

**定義 2.9** (スキームの Brauer 群)**.** $X$ をある環上準射影スキームとする。このとき $X$ の Brauer 群を $X$ の 2 次エタールコホモロジー

$$\mathrm{Br}(X) := H^2_{\text{ét}}(X, \mathbb{G}_m)$$

として定義する。

**補足 2.10.** 上の定義はいわゆるコホモロジカル Brauer 群と呼ばれるものである。本来 Brauer 群は東屋代数を使って定義されるが二つの定義が一致することは準射影的の仮定の下 Gabber によって示された。

以下のように不分岐 Brauer 群と Brauer 群の関係は purity theorem で記述される。

**定理 2.11** (Purity theorem)**.** $k$ を標数 0 の体とする。$X$ を $k$ 上の非特異代数多様体とし、$k(X)$ を $X$ の函数体とする。このとき以下が成り立つ。

(1) 自然な準同型 $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$ は単射である。
(2) 包含関係 $\mathrm{Br}_{\mathrm{nr}}(k(X)/k) \subset \mathrm{Br}(X) \subset \mathrm{Br}(k(X))$ が成り立つ。
(3) $X$ が完備のとき $\mathrm{Br}_{\mathrm{nr}}(k(X)/k) = \mathrm{Br}(X)$ がいえる。

この定理が示すように、不分岐 Brauer 群とは函数体上のクラスで、完備非特異モデルに拡張するものたちがなす群と見なせる。またこの定理から完備非特異多様体に対して Brauer 群は双有理不変量であることがわかる。さらに、完備非特異多様体が有理的なとき、Brauer 群は自明となる。Artin-Mumford は [AM72] で単有理的だが Brauer 群が非自明な例をコニック束として構成して、Lüroth の問題への反例を提出した。

## 3. Bogomolov の公式

このセクションでは、不変体の不分岐 Brauer 群を計算するための Bogomolov の結果 [Bog87], [Bog89] を紹介する。このセクションは [CTS07, Section 6, Section 7.1] に基づいている。基礎体 $k$ は標数 0 の代数閉体と仮定する。このノートでは主に群が有限群の場合を扱う。

### 3.1. 一般公式.

まずは最も一般的な形の公式を議論する。

**定理 3.1** (一般公式)**.** $L$ を $k$ 上の函数体とする。$G$ を $L$ の $k$ 上の自己同型からなる有限群とする。このとき以下がいえる。

$$\mathrm{Br}_{\mathrm{nr}}(L^G) = \{\alpha \in \mathrm{Br}(L^G) |\ \text{全ての } H \in \mathcal{B}_G \text{ に対して} \alpha_H \in \mathrm{Br}_{\mathrm{nr}}(L^H)\}$$

ここで $\mathcal{B}_G$ は $G$ の 2 元で生成されるアーベル部分群全体の集合、$\alpha_H$ は $\alpha \in \mathrm{Br}(L^G)$ の $\mathrm{Br}(L^H)$ への制限である。

*Proof.* $K = L^G$ とおく。$\alpha \in \mathrm{Br}(K)$ とし、ある $K$ の離散付値環 $A$ に対して $\partial_A(\alpha) \neq 0$ と仮定する。このとき 2 元で生成されるアーベル部分群 $H \subset G$ が存在して $\alpha_H \notin \mathrm{Br}_{\mathrm{nr}}(L^H)$ を示したい。

いくつか Galois 理論のおさらいをする。$\tilde{A}$ を $A$ の $L$ の中での整閉包とし、$\mathfrak{p}$ を $\tilde{A}$ の素イデアルとする。$D \subset \mathrm{Gal}(L/K)$ を $\mathfrak{p}$ の分解群とし、$I \subset D$ を惰性群とする。このとき $I$ は $D$ の正規部分群である。局所化 $B = \tilde{A}_{\mathfrak{p}}$ は離散付値環である。今体の拡大

$$K = L^G \subset L^D \subset L^I \subset L$$

があるが、それに対応する環の拡大

$$A = B^G \subset B^D \subset B^I \subset B$$

がある。これに対応する剰余体の拡大を

$$F = F = F \subset E = E$$

とおく。このとき

$$D/I = \mathrm{Gal}(E/F) = \mathrm{Gal}(L^I/L^D)$$

がいえ、$B^I/A$ は不分岐がいえる。今 $F$ の標数が 0 なので、$I$ は $\overline{F}$ に含まれる 1 の根の群の部分群とみなせ、従って $I$ は巡回群であることがわかる。また $\overline{F}$ の 1 の根はすべて $k$ に含まれるため、$D$ の $I$ への共役作用は自明であることがわかる。従って、$D$ は $I$ の中心拡大であることがわかる。

では、証明に移る。仮に $\alpha_I \notin \mathrm{Br}_{\mathrm{nr}}(L^I)$ ならば主張は成り立つので、$\alpha_I \in \mathrm{Br}_{\mathrm{nr}}(L^I)$ とする。$B^D/A$ は不分岐拡大で剰余体が一致しているので $\partial_A(\alpha) \neq 0$ が $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\kappa_{B^D}}/\kappa_{B^D}), \mathbb{Q}/\mathbb{Z})$ の中で $\partial_{B^D}(\alpha) \neq 0$ を示す。ところで $\partial_{B^I}(\alpha) = 0$ である。$B^I/B^D$ は不分岐より

$$\begin{array}{ccc} \mathrm{Br}(L^I) & \xrightarrow{\partial_B} & \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{E}/E), \mathbb{Q}/\mathbb{Z}) \\ {\scriptstyle \mathrm{Res}_{L^I/L^D}}\uparrow & & \uparrow{\scriptstyle \mathrm{Res}_{E/F}} \\ \mathrm{Br}(L^D) & \xrightarrow{\partial_A} & \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \mathbb{Q}/\mathbb{Z}) \end{array}$$

は可換である。$g \in D$ でその剰余類 $\overline{g} \in D/I$ が $\partial_{B^D}(\alpha)(\overline{g}) \neq 0$ をみたすものとする。$H = \langle I, g \rangle$ とおけば $H$ はアーベル群で $\partial(\alpha^H) \neq 0$ は簡単に従う。したがって主張がいえた。 □

生成的に自由な作用を持つ簡約群についても似たような定理が成り立つ。

**定理 3.2.** [Bog89] $G$ を $k$ 上定義された簡約群とし、$X$ を $G$-作用があるアフィン多様体とする。今、すべての群作用が自由と仮定する。このとき

$$\mathrm{Br}_{\mathrm{nr}}(k(X)^G) = \{\alpha \in \mathrm{Br}(k(X)^G) | \text{ 全ての } H \in \mathcal{B}_G \text{ に対して} \alpha_H \in \mathrm{Br}_{\mathrm{nr}}(k(X)^H)\}$$

ここで $\mathcal{B}_G$ は $G$ の 2 元で生成される有限アーベル部分群全体の集合、$\alpha_H$ は $\alpha \in \mathrm{Br}(k(X)^G)$ の $\mathrm{Br}(k(X)^H)$ への制限である

*Proof.* [CTS07, Theorem 6.4] を参照されたい。 □

3.2. **Bogomolov の公式.** 有限群 $G$ がベクトル空間に線形に作用しているとき、その商空間の不分岐 Brauer 群を計算するための公式を紹介する。

**定理 3.3.** [Bog87] $G$ を有限群とし、$k$-ベクトル空間 $V$ に線形かつ忠実に作用するとする。このとき以下がいえる*:*

$$\begin{aligned} \mathrm{Br}_{\mathrm{nr}}(k(V)^G) &\cong \ker\left(H^2(G, k^\times) \to^{\mathrm{Res}} \prod_{A \in \mathcal{B}_G} H^2(A, k^\times)\right) \\ &\cong \ker\left(H^2(G, \mathbb{Q}/\mathbb{Z}) \to^{\mathrm{Res}} \prod_{A \in \mathcal{B}_G} H^2(A, \mathbb{Q}/\mathbb{Z})\right) \\ &\cong \ker\left(H^3(G, \mathbb{Z}) \to^{\mathrm{Res}} \prod_{A \in \mathcal{B}_G} H^2(A, \mathbb{Z})\right) \end{aligned}$$

さらに $\mathcal{B}_G$ をすべての $G$ のアーベル部分群からなる集合 $\mathcal{A}_G$ で置き換えても同様の公式が成り立つ。

*Proof.* まず $A \subset G$ をアーベル部分群とする。$A$ の $V$ への作用は同時対角化可能なので $k(V)^A$ は有理的であることがいえる。(Fischer の定理) したがって $\mathrm{Br}_{\mathrm{nr}}(k(V)^A) = 0$ がいえることに注意する。

次に任意の部分群 $H \subset G$ に対して

$$0 \to H^2(H, k(V)^\times) \to \mathrm{Br}(k(V)^H) \to \mathrm{Br}(k(V))$$

が完全となる。したがって定理 3.1 を使って

$$\mathrm{Br}_{\mathrm{nr}}(k(V)^G) \cong \ker\left(H^2(G, k(V)^\times) \to \prod_{A \in \mathcal{B}_G} H^2(A, k(V)^\times)\right)$$

がいえる。ところで、$k[V]$ は UFD で $k[V]^\times = k^\times$ なので

$$1 \to k^\times \to k(V)^\times \to \mathrm{Div}(V) \to 0$$

は完全列である。また $\mathrm{Div}(V)$ は様々な部分群 $H \subset G$ に対する $\mathbb{Z}[G/H]$ の置換加群の直和なので以下の置換加群の性質より、最初の公式が従う: 置換加群 $M$ に対して

$$H^1(G, M) = 0$$
$$\ker\left(H^2(G, M) \to \prod_{g \in G} H^2(\langle g \rangle, M)\right) = 0$$

が成り立つ。二つ目の公式は $k$ の 1 の根がなす群 $\mu$ と $\mathbb{Q}/\mathbb{Z}$ を同一視して $k/\mu$ がコホモロジカルに自明なことを使って証明できる。三つ目は $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ の完全列の長完全列を考えれば良い。

最後の主張はアーベル部分群 $A \subset G$ に対して $\mathrm{Br}_{\mathrm{nr}}(k(V)^A) = 0$ がいえることよりしたがう。 □

## 4. クラス 2 の冪零群について

このセクションでは Bogomolov の公式をクラス 2 の冪零群に適用し、$V/G$ が非有理的となる有限群 $G$ の例（Noether の問題への反例）を構成する。このセクションは [CTS07, Section 7.2] に基づいている。基礎体 $k$ は標数 0 の代数閉体とする。

$\Gamma$ を有限アーベル群とし、$C$ を別の有限アーベル群とする。$\Gamma$ の $C$ による中心拡大

$$0 \to C \to G \to \Gamma \to 0$$

を考える。そのような群は 2 次群コホモロジー $H^2(\Gamma, C)$ によって分類される。ここで $\Gamma$ の $C$ への作用は自明なものを考える。

今 $\Gamma$ はアーベル群なので $H_2(\Gamma, \mathbb{Z}) = \bigwedge^2 \Gamma$ がいえ、普遍係数定理より任意の $\Gamma$-加群 $M$ に対して、

$$0 \to \mathrm{Ext}^1(\Gamma, M) \to H^2(\Gamma, M) \to^{\omega_M} \mathrm{Hom}(\bigwedge^2 \Gamma, M) \to 0$$

は完全列になる。$M = C$ とおくと、準同型

$$\omega_C : H^2(\Gamma, C) \to \mathrm{Hom}(\bigwedge^2 \Gamma, C)$$

は $[G]$ を

$$\lambda_G : \bigwedge^2 \Gamma \to [G, G] \subset C, \gamma_1 \wedge \gamma_2 \mapsto [g_1, g_2]$$

に写す。ここで $g_i$ は $\gamma_i$ の $G$ への持ち上げである。

任意の部分群 $G' \subset G$ に対して $G'$ の $\Gamma$ への像を $\Gamma'$ とおき、$C' = G' \cap C$ とおくと $G'$ は $\Gamma'$ の $C'$ による中心拡大である。そこで $S_{G'}$ を $\lambda_{G'} : \bigwedge^2 \Gamma' \to C'$ の核とする。さらに、$S_{\mathrm{bic}}$ を $S_G$ の部分群で $S_G$ に含まれる $\gamma_1 \wedge \gamma_2$ の形の元で生成されるものとする。言い方を変えれば $S_{\mathrm{bic}}$ は 2 元で生成されるアーベル部分群 $A \subset G$ により定まる $S_A$ たちによって生成される部分群である。

**定理 4.1.** [Bog87] 今 $k$-ベクトル空間 $V$ に $G$ が線型かつ忠実に作用しているとする。このとき、以下がいえる。

$$\mathrm{Br}_{\mathrm{nr}}(k(V)^G) = \widehat{S_G/S_{\mathrm{bic}}}.$$

ここで、アーベル群 $M$ に対して $\widehat{M} = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ と定める。

したがって $V/G$ が安定有理的でないものを見つけるには $S_G \neq S_{\mathrm{bic}}$ となるクラス 2 の冪零群 $G$ を見つければ良い。

*Proof.* スペクトル列

$$H^p(\Gamma, H^q(C, \mathbb{Q}/\mathbb{Z})) \implies H^{p+q}(G, \mathbb{Q}/\mathbb{Z})$$

を用いると

$$0 \to \widehat{S_G} \to \ker(H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(C, \mathbb{Q}/\mathbb{Z})) \to \mathrm{Hom}(\Gamma, \widehat{C})$$

となる完全列が得られる。我々のゴールは

$$B_G = \mathrm{Br}_{\mathrm{nr}}(k(V)^G) \subset H^2(G, \mathbb{Q}/\mathbb{Z})$$

を計算することにある。任意のアーベル群に対して $B_A = 0$ なので、$B_G$ の関手性より

$$B_G \subset \ker(H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(C, \mathbb{Q}/\mathbb{Z}))$$

が従う。次に $B_G$ の $\mathrm{Hom}(\Gamma, \widehat{C})$ への像が 0 となることを見るが、それを示すのに任意の巡回群 $\Gamma' \subset \Gamma$ への制限が 0 になることを見れば良い。しかし、このとき $G'$ を $\Gamma'$ の逆像とすると $G'$ はアーベル群なので $B_{G'} = 0$ である。したがって主張が従う。

以上の議論により

$$B_G \subset \widehat{S_G}$$

を見た。今定理 3.3 より

$$B_G = \ker\left(H^2(G, \mathbb{Q}/\mathbb{Z}) \to \prod_{A \in \mathcal{B}_G} H^2(A, \mathbb{Q}/\mathbb{Z})\right)$$

だが、言い換えると

$$B_G = \ker\left(\widehat{S_G} \to \prod_{A \in \mathcal{B}_G} \widehat{S_A}\right)$$

だといえる。したがって

$$B_G = \ker(\widehat{S_G} \to \widehat{S_{\mathrm{bic}}})$$

がいえ、我々の主張が従う。 □

**例 4.2.** 今完全列

$$0 \to \mathrm{Ext}^1(\Gamma, C) \to H^2(\Gamma, C) \to \mathrm{Hom}(\bigwedge^2 \Gamma, C) \to 0$$

があるので、$\bigwedge^2 \Gamma$ の部分群 $S$ で $S_{\mathrm{bic}} \neq S$ となるものを見つければ有限群 $G$ で $V/G$ が安定有理的にならない例が見つかったことになる。$\Gamma = \mathbb{F}_p^4$ とおく。ここで $p$ は任意の素数とする。このとき、$\bigwedge^2 \Gamma \cong \mathbb{F}_p^6$ がいえる。ここで、基底は

$$e_1 \wedge e_2, e_3 \wedge e_4, e_1 \wedge e_3, e_2 \wedge e_4, e_1 \wedge e_4, e_2 \wedge e_3$$

をとる。純テンソルを考えたいので、射影空間 $\mathbb{P}(\bigwedge^2 \Gamma) = \mathbb{P}^5$ で考える。このとき純テンソルベクトルの集合は 2 次超曲面 $Q$ で与えられる。ここで、$Q$ は上の基底を使って

$$x_1x_2 - x_3x_4 + x_5x_6 = 0$$

で定義される。このとき、$S_{\mathrm{bic}} \neq S$ となる $S$ は $\mathbb{P}(S) \cap Q$ が $S$ を生成しない部分空間として与えられる。以下のような状況が考えられる。

(1) $S$ は 1 次元で $\mathbb{P}(S) \notin Q$ となっている場合。$\#G = p^9$ として取れる。これが Saltman が初めて見つけた $V/G$ が安定有理的とならない例である。([Sal84])
(2) $S$ は 2 次元で直線 $\mathbb{P}(S)$ は $Q$ に接している場合。$\#G = p^8$ として取れる。
(3) $S$ は 2 次元で直線 $\mathbb{P}(S)$ と $Q$ の交点は $\mathbb{F}_p$ 上定義されてない場合。$\#G = p^8$ として取れる。
(4) $S$ は 3 次元で平面 $\mathbb{P}(S)$ と $Q$ は直線に沿って交わる場合。$\#G = p^7$ として取れる。
(5) $S$ は 3 次元で平面 $\mathbb{P}(S)$ と $Q$ は一点で交わる場合。$\#G = p^7$ として取れる。

さらに Bogomolov は $\#G = p^6$ となる $G$ で $B_G \neq 0$ となる例を見つけた。([Bog87]) $\#G = p^n$, $n \leq 4$ のとき、$V^G$ は安定有理的であることが知られている。([CK01])

## 5. 安定コホモロジーと不分岐コホモロジー

このセクションでは Bogomolov によって [Bog92] で導入された安定コホモロジーや不分岐コホモロジーを概観する。$k$ を標数 0 の代数閉体と仮定する。$G$ を有限群とし、$M$ を有限加群で $G$ の作用は自明なものとする。$k$ 上の線形空間 $V$ が $G$ の忠実な表現として与えられたとし、$V^L$ を $V$ の開集合で $G$ が自由に作用するものとする。このとき、$M$ は $V^L/G$ 上の定数層 $F^M$ を誘導し、

$$H^*(G, M) = H^*_{\text{ét}}(V^L/G, F^M)$$

がいえる。[Bog92] で Bogomolov は Grothendieck のアイデアに習って、以下の安定コホモロジーを定義した。

**定義 5.1** (有限群の安定コホモロジー)**.** 今 $U \subset V^L$ が $V^L$ の空でない $G$-不変な開集合全体を走るとする。$G$ の安定コホモロジー $H^*_S(G, M)$ を以下の自然な写像の像として定義する:

$$H^*(G, M) \to \varinjlim H^*_{\text{ét}}(U/G, F^M)$$

この安定コホモロジー $H^*_S(G, M)$ は $V$ の取り方に依らないことがわかっている。([Bog92])

次に不分岐コホモロジーを定義する。$X = V^L/G$ とおく。次に $D$ を $k(X)$ の離散付値とする。すると、ある正規な双有理モデル $X_D$ が存在して $D$ は $X_D$ 上の因子として実現される。さらに $X_D$ のある開集合は $X$ の開集合 $U/G$ と同一視される。

$a \in H^*_S(G, M)$ が $D$ に関して不分岐であるとは、ある $X_D$ が存在して $a$ は $H^*_{\text{ét}}(X_D, F^M)$ の元の像と一致することをいう。$a \in H^*_S(G, M)$ が不分岐であるとは任意の離散付値に関して $a$ は不分岐であることをいう。

**定義 5.2** (有限群の不分岐コホモロジー)**.** $H^*_S(G, M)$ の不分岐な元全体がなす群を不分岐コホモロジーといい、

$$H^*_{\text{nr}}(G, M)$$

で表す。

この不変量は安定双有理不変量であることがいえる。さらに以下が言える。

**定理 5.3** (不分岐コホモロジーの消滅)**.** $V/G$ が安定有理的なとき、

$$H^i_{\text{nr}}(G, M) = 0$$

が任意の $i > 0$ に対して成り立つ。

Colliot-Thélène–Ojanguren は [CTO89] で不分岐 Brauer 群は自明だが、3 次不分岐コホモロジーが非自明な単有理多様体を構成し、Lüroth の問題に対する反例を与えた。さらに、Peyre は [Pey08] で有限群に関する Noether の問題への反例として不分岐 Brauer 群が自明だ

が、3 次不分岐コホモロジーが非自明となるものを与えた。Peyre の例は任意の奇素数 $p$ に対して $G$ の位数が $p^{12}$ となるものである。[HKY16] では Peyre の議論をさらに発展させて、$G$ の位数が $p^9$ となる例を構成した。

## 6. 同質族と輪積

最後のセクションでは、[BB13] の解説を簡潔に行い、安定コホモロジーの計算方法を紹介する。まず、二つの中心拡大が同質関係にある (isoclinic) ということの意味を解説する。

**定義 6.1.** 二つの群 $G_1, G_2$ とそれぞれの中心 $Z_1, Z_2$ について、$G_1, G_2$ が同質関係にあるとは二つの同型写像

$$\phi : G_1/Z_1 \cong G_2/Z_2, \quad \psi : [G_1, G_1] \cong [G_2, G_2]$$

が存在して、

$$\begin{array}{ccc} G_1/Z_1 \times G_1/Z_1 & \xrightarrow{\phi\times\phi} & G_2/Z_2 \times G_2/Z_2 \\ \downarrow{\scriptstyle [\cdot,\cdot]} & & \downarrow{\scriptstyle [\cdot,\cdot]} \\ [G_1, G_1] & \xrightarrow[\psi]{} & [G_2, G_2] \end{array} \tag{6.1}$$

が可換になることをいう。

この関係は Hall によって [Hal40] で初めて提唱されたようである。Hall の目的は $p$-群の分類問題のためであった。さらに、この関係はトロイダル関係と呼ばれる関係に同値になる。([BB13, Theorem 6]) そのことを使って、Bogomolov-Böhning は以下を示した:

**定理 6.2.** [BB13, Proposition 3, Theorem 6] 二つの群 $G_1, G_2$ が同質関係にあるとき、以下が言える*:* 標数 0 の代数閉体上の $G_i$ の忠実な表現を $V_i$ とおくと、$V_1/G_1$ と $V_2/G_2$ は安定双有理同値になる。

この定理は [HKK13] で提出された問題への解になっている。[HKK13] では位数が $p^5$ の群 $G$ がいつ $B_G \neq 0$ となるかを決定した。具体的には $B_G \neq 0$ となる位数 $p^5$ の群 $G$ 全体は $\Phi_{10}$ と呼ばれる同質族に一致することを示した。(ここで $p$ は奇素数。) しかし、位数が $p^5$ の群の Noether の問題は未だ未解決である。

さて、これらの概念や定理たちの応用を紹介しよう。$\mathcal{D}$ を有限群の集合で以下をみたすとする:

(1) 任意の $\mathcal{D}$ に含まれる群 $G$ について、その忠実な表現の商空間は安定有理的になる。
(2) 任意の $\mathcal{D}$ の群 $G$ 及び $G$ の元について、その中心化も $\mathcal{D}$ に含まれる。

さらにクラス $\mathcal{D}$ の群に対して、以下の操作を有限回行って得られる群のクラスを $\mathcal{C}_p(\mathcal{D})$ とおく:

- $\mathbb{Z}/p\mathbb{Z}$ との輪積 (wreath product) をとる: $H \mapsto H \wr \mathbb{Z}/p$
- 有限積を取る: $H_1, \cdots, H_r \mapsto H_1 \times \cdots \times H_r$
- 群を同質関係にある群と置き換える。

クラス $\mathcal{C}_p(\mathcal{D})$ の群は安定有理的な忠実表現の商空間を持つことがいえる。さらに、同質関係をうまく使って性質 (2) が $\mathcal{C}_p(\mathcal{D})$ でも成り立つことがいえる。([BB13, Proposition 10])

**例 6.3.** $p$ を素数とし、$q = p^k$ とく。$\ell$ を $p$ とは異なる奇素数とする。$G = \mathrm{GL}_n(\mathbb{F}_q)$ とおく。このとき $G$ の $\ell$-Sylow 部分群は

$$S = \mathbb{Z}/\ell^r \wr \mathbb{Z}/\ell \wr \cdots \wr \mathbb{Z}/\ell$$

の形でかける。従って $H^*_{\mathrm{nr}}(G, \mathbb{Z}/\ell) = H^*_{\mathrm{nr}}(S, \mathbb{Z}/\ell)$ は自明。

## References


[AM72] M. Artin and D. Mumford. Some elementary examples of unirational varieties which are not rational. *Proc. London Math. Soc. (3)*, 25:75–95, 1972.

[BB13] F. A. Bogomolov and C. Böhning. Isoclinism and stable cohomology of wreath products. In *Birational geometry, rational curves, and arithmetic*, Simons Symp., pages 57–76. Springer, Cham, 2013.

[BB14] F. Bogomolov and C. Böhning. Stable cohomology of alternating groups. *Cent. Eur. J. Math.*, 12(2):212–228, 2014.

[Bog87] F. A. Bogomolov. The Brauer group of quotient spaces of linear representations. *Izv. Akad. Nauk SSSR Ser. Mat.*, 51(3):485–516, 688, 1987.

[Bog89] F. A. Bogomolov. Brauer groups of the fields of invariants of algebraic groups. *Mat. Sb.*, 180(2):279–293, 1989.

[Bog92] F. A. Bogomolov. Stable cohomology of groups and algebraic varieties. *Mat. Sb.*, 183(5):3–28, 1992.

[Bog07] F. A. Bogomolov. Stable cohomology of finite and profinite groups. In *Algebraic groups*, pages 19–49. Universitätsverlag Göttingen, Göttingen, 2007.

[CG72] C. H. Clemens and P. A. Griffiths. The intermediate Jacobian of the cubic threefold. *Ann. of Math. (2)*, 95:281–356, 1972.

[CK01] H. Chu and M.-C. Kang. Rationality of $p$-group actions. *J. Algebra*, 237(2):673–690, 2001.

[CTO89] J.-L. Colliot-Thélène and M. Ojanguren. Variétés unirationnelles non rationnelles: au-delà de l'exemple d'Artin et Mumford. *Invent. Math.*, 97(1):141–158, 1989.

[CTS07] J.-L. Colliot-Thélène and J.-J. Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). In *Algebraic groups and homogeneous spaces*, volume 19 of *Tata Inst. Fund. Res. Stud. Math.*, pages 113–186. Tata Inst. Fund. Res., Mumbai, 2007.

[Hal40] P. Hall. The classification of prime-power groups. *J. Reine Angew. Math.*, 182:130–141, 1940.

[HKK13] A. Hoshi, M.-C. Kang, and B. E. Kunyavskii. Noether's problem and unramified Brauer groups. *Asian J. Math.*, 17(4):689–713, 2013.

[HKY16] A. Hoshi, M.-C. Kang, and A. Yamasaki. Degree three unramified cohomology groups. *J. Algebra*, 458:120–133, 2016.

[IM71] V. A. Iskovskih and Yu. I. Manin. Three-dimensional quartics and counterexamples to the Lüroth problem. *Mat. Sb. (N.S.)*, 86(128):140–166, 1971.

[Pey08] E. Peyre. Unramified cohomology of degree 3 and Noether's problem. *Invent. Math.*, 171(1):191–225, 2008.

[Sal84] D. J. Saltman. Noether's problem over an algebraically closed field. *Invent. Math.*, 77(1):71–84, 1984.



熊本大学大学院先導機構 熊本市中央区黒髪 2-39-1

熊本大学理学部数学教室
*E-mail address*: stanimoto@kumamoto-u.ac.jp

# 3次不分岐コホモロジー群とネーター問題

新潟大学理学部　星 明考
Akinari Hoshi, Department of Mathematics, Niigata University [1]

**概要**　この原稿は第27回整数論サマースクール (2019年9月) の講演のレジメです．この講演では，論文 星-Kang-山崎 [HKY20] “Degree three unramified cohomology groups and Noether’s problem for groups of order 243” の内容と証明法の一部を紹介します．

**謝辞.** 10回目の参加の今回は，世話人としての参加でした．世話人の一人として，参加して下さった皆様に心より感謝申し上げます．また，これまで重要な示唆と数多くのアドバイスを下さったMing-chang Kang 氏，遠藤静男氏，Jean-Louis Colliot-Thélène 氏にこの場を借りて御礼申し上げます．

## 目 次



## 1　主結果

$k$ を体，$k(x_1,\dots,x_n)$ を $k$ 上の $n$ 変数有理関数体とする．$L$ を $k$ 上有限生成な体 ($k$ 上の代数多様体 $X$ の関数体) とする．$L$ が $k$ **上有理的** ($k$-rational, rational over $k$) とは，$L$ が $k$ 上純超越的 ($k$ 上の有理関数体と同型) であることをいう．$L$ が $k$ **上安定有理的** (stably $k$-rational) とは，$L$ 上代数的独立な元 $y_1,\dots,y_m$ に対して，$L(y_1,\dots,y_m)$ が $k$ 上有理的であること．$k$ が無限体のとき，$L$ が $k$ **上レトラクト有理的** (retract $k$-rational) とは，$k$ 代数 (整域)$A \subset L$ が存在して，(i) $L$ は $A$ の商体; (ii) $f \in k[x_1,\dots,x_n]$ と $k$ 代数の準同型 $\varphi\colon A \to k[x_1,\dots,x_n][1/f]$, $\psi\colon k[x_1,\dots,x_n][1/f] \to A$ が存在し，$\psi\circ\varphi = 1_A$，をみたすこと (Saltman [Sal84b], Kang [Kan14] も参照). $L$ が $k$ **上単有理的** ($k$-unirational) とは，$L$ が $k$ 上有理的な体の部分体となることである．$k$ 上有限生成な体 $L_1$ と $L_2$ が**安定 $k$ 同型** (stably $k$-isomorphic) であるとは，$L_1$ 上代数的独立な元 $y_1,\dots,y_m$ と $L_2$ 上代数的独立な元 $z_1,\dots,z_n$ に対して，$L_1(y_1,\dots,y_m)$ と $L_2(z_1,\dots,z_n)$ が $k$ 同型となること．無限体 $k$ に対して，“$k$ 上有理的”⇒“$k$ 上安定有理的”⇒ “$k$ 上レトラクト有理的”⇒“$k$ 上単有理的” となる．

**定義 1.1.** 有限群 $G$ が有理関数体 $k(x_g : g \in G)$ に変数の置換 $h(x_g) = x_{hg}$ $(g,h \in G)$ によって，$k$ 自己同型として作用しているとする．この作用による不変体 $k(x_g : g \in G)^G = \{f \in k(x_g : g \in G) : \sigma(f) = f \ (\sigma \in G)\}$ を $k(G)$ とかく．($k(x_g : g \in G)/k(G)$ は $G$ ガロア拡大となる)

エミー・ネーター [Noe1913] は，$k(G)$ は $k$ 上有理的かという問いを提起し，現在では，この問題は ($G$ に対する $k$ 上の) **ネーター問題** (Noether’s prblem) と呼ばれている．代数幾何学における，いわゆるリューロー問題 (Lüroth’s problem) の特別な場合である．今回の前半の講義でも紹介があったように，この問題はガロア逆問題，生成的 $G$ 拡大の存在，生成的 $G$ トーサーの存在と深い関わりがある (Swan [Swa83], Manin-Tsfasman [MT86], Colliot-Thélène–Sansuc [CTS07], Serre [GMS03, pages 86–92] 参照).

以下，$G$ は有限群とする．ネーター問題に対して，次のような結果がある．

[1] 本研究は科研費 19K03418 の助成を受けています.

**定理 1.2** (Fischer [Fis1915], [Swa83, Theorem 6.1] も参照)**.** $G$ をアーベル群とし，その指数を $e$ とする．$k$ が 1 の $e$ 乗根を含むならば $k(G)$ は $k$ 上有理的．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的.

**定理 1.3** (Kuniyoshi [Kun56], Gaschütz [Gas59])**.** $k$ を標数 $p>0$ の体，$G$ を $p$ 群とする．このとき，$k(G)$ は $k$ 上有理的.

**定理 1.4** (Chu-Kang [CK01])**.** $G$ を位数 $\leq p^4$ の $p$ 群，その指数を $e$ とする．$k$ が 1 の $e$ 乗根を含むならば $k(G)$ は $k$ 上有理的．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的.

**定理 1.5** (Chu-Hu-Kang-Prokhorov [CHKP08])**.** $G$ を位数 32 の群，その指数を $e$ とする．$k$ が 1 の $e$ 乗根を含むならば $k(G)$ は $k$ 上有理的．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的.

Swan [Swa69] はネーター問題の最初の反例を構成した : $\mathbb{Q}(C_{47})$ は $\mathbb{Q}$ 上非有理的．ここで，$C_{47}$ は位数 47 の巡回群．アーベル群に対するネーター問題は 1970 年代に Voskresenskii, 遠藤-宮田, Lenstra などによって研究された (Swan [Swa83] 参照)．しかし，非アーベル群に対する研究は一般に難しい状況であった.

Saltman [Sal84a] は閉体 $\mathbb{C}$ 上でネーター問題の最初の反例を構成した : 位数 $p^9$ の $p$ 群 $G$ が存在して，$\mathbb{C}(G)$ は $\mathbb{C}$ 上非安定有理的．Saltman は $\mathbb{C}(G)$ の不分岐ブラウアー群の非消滅 $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(G))\neq 0$ を示すことで，これを証明した．実際，$\mathbb{C}(G)$ に対して，“有理的”⇒“安定有理的”⇒ “レトラクト有理的”⇒ $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(G))=0$ という関係がある.

不分岐ブラウアー群は Colliot-Thélène–Ojanguren [CTO89] によって，不分岐コホモロジー群に一般化された．実際，$H^2_{\mathrm{nr}}(K,\mathbb{Q}/\mathbb{Z})\simeq \mathrm{Br}_{\mathrm{nr}}(K)$．また，体 $K$ に対して，“有理的”⇒“安定有理的”⇒ “レトラクト有理的”⇒ $H^i_{\mathrm{nr}}(K,\mathbb{Q}/\mathbb{Z})=0$ $(i\geq 2)$ という関係となる.

**定理 1.6** (Colliot-Thélène–Ojanguren [CTO89, Section 3])**.** 関数体 $K/\mathbb{C}$, $\mathrm{trdeg}_{\mathbb{C}}K=6$ が存在して，$H^2_{\mathrm{nr}}(K,\mathbb{Q}/\mathbb{Z})=0$ かつ $H^3_{\mathrm{nr}}(K,\mathbb{Q}/\mathbb{Z})\neq 0$ をみたす．とくに，$K$ は $\mathbb{C}$ 上非レトラクト有理的.

不分岐コホモロジー群 $H^i_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ を使って，$\mathbb{C}(G)$ の有理性問題を考えたい．$i=2$ の場合には，Bogomolov の公式 (Bogomolov [Bog88], 定理 2.3 参照)，$i=3$ の場合には，Saltman-Peyre の方法 (Saltman [Sal95], Peyre [Pey93], 定理 2.15 参照) がある．しかしながら，後者の方法は大変複雑で，これまで特別な群 $G$ に対してしか，適応できていなかった :

**定理 1.7** (Peyre [Pey08, Theorem 2])**.** 位数 $p^{12}$ ($p$: 奇素数 ) の $p$ 群 $G$ が存在して，以下をみたす :
(i) 中心拡大 $0\to V\to G\to U\to 0$ で，$U$ と $V$ は $\dim_{\mathbb{F}_p}U=\dim_{\mathbb{F}_p}V=6$ なる基本アーベル $p$ 群;
(ii) $H^2_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})=0$ かつ $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})\neq 0$. とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上非レトラクト有理的.

星-Kang-山崎 [HKY16, Theorem 1.4] は，Peyre の方法で $G$ の位数がより小さいものを見つけた :

**定理 1.8** (星-Kang-山崎 [HKY16, Theorem 1.4])**.** 位数 $p^9$ ($p$: 奇素数 ) の $p$ 群 $G$ が存在して，
(i) 中心拡大 $0\to V\to G\to U\to 0$ で，$U$ と $V$ は $\dim_{\mathbb{F}_p}U=6$, $\dim_{\mathbb{F}_p}V=3$ なる基本アーベル $p$ 群;
(ii) $H^2_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})=0$ かつ $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})\neq 0$. とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上非レトラクト有理的.

主結果を述べる前に，次の Hall [Hal40, page 133] による同質族の概念を導入しておく :

**定義 1.9.** $G$ を有限群，$Z(G)$ を $G$ の中心，$[G,G]$ を $G$ の交換子群とする．群 $G_1$ と $G_2$ が**同質** (isoclinic) であるとは，群同型 $\theta\colon G_1/Z(G_1)\to G_2/Z(G_2)$, $\phi\colon [G_1,G_1]\to[G_2,G_2]$, $\phi([g,h])=[g',h']$ $(g'\in\theta(gZ(G_1)), h'\in\theta(hZ(G_1)), g,h\in G_1)$ が存在して，次の図式が可換となること:

$$\begin{array}{ccc} G_1/Z_1\times G_1/Z_1 & \xrightarrow{(\theta,\theta)} & G_2/Z_2\times G_2/Z_2 \\ {\scriptstyle [\cdot,\cdot]}\downarrow & \circlearrowleft & \downarrow{\scriptstyle [\cdot,\cdot]} \\ [G_1,G_1] & \xrightarrow{\phi} & [G_2,G_2]. \end{array}$$

同質による同値類を**同質族** (isoclinism family) という.

例えば，Hall-Senior [HS53] は位数 64 の群を 27 の同質族 $\Phi_1, \dots, \Phi_{27}$ に分類した (James-Newman-O'Brien [JNO90, Table I], [星, 12.3 節] 参照). Bogomolov-Böhning [BB13] は星-Kang-Kunyavskii [HKK13, Question 1.11] に答える形で以下を示した：

**定理 1.10** (Bogomolov-Böhning [BB13, Theorem 6])**.** 群 $G_1$ と $G_2$ が同質ならば $\mathbb{C}(G_1)$ と $\mathbb{C}(G_2)$ は安定 $\mathbb{C}$ 同型．とくに，$H^i_{\mathrm{nr}}(\mathbb{C}(G_1), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^i_{\mathrm{nr}}(\mathbb{C}(G_2), \mathbb{Q}/\mathbb{Z})$.

ネーター問題に話を戻したい．定理 1.4 と定理 1.5 より $p$ 群 $G$ に対する，$\mathbb{C}(G)$ の有理性問題は，$G$ が位数 $2^n$ $(n \geq 6)$ および位数 $p^m$ ($p$: 奇素数，$m \geq 5$) のときを考えればよい．

位数 $2^6 = 64$ の群 $G$ の場合．(原論文 [CHKK10] の結果を同質族 $\Phi_i$ をもちいて書き直しています)

**定理 1.11** (Chu-Hu-Kang-Kunyavskii [CHKK10])**.** $G$ を位数 64 の群とする．
(1) ([CHKK10, Theorem 1.8]) $H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \neq 0 \Leftrightarrow G \in \Phi_{16}$.
このとき，$H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ (Kang [Kan14, Remark, page 424] も参照 );
(2) ([CHKK10, Theorem 1.10]) $H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) = 0$ かつ $G \notin \Phi_{13}$ ならば $\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的.

しかし，$G \in \Phi_{13}$ のとき，$\mathbb{C}$ 上の有理性はよく分かっていない．

位数 $p^5 (p \geq 5)$ の群 (の同型類) は $2p + 61 + \gcd\{4, p-1\} + 2\gcd\{3, p-1\}$ 個，位数 $3^5$ の群は 67 個あり，同質族 $\Phi_1, \dots, \Phi_{10}$ に分類される (see [Jam80, Section 4]). Moravec [Mor12] は位数 $3^5 = 243$ の群 $G$ に対して，$H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \neq 0 \Leftrightarrow G \in \Phi_{10}$ (3 個) をコンピュータをもちいて確かめた．その一般化および理論的な証明は，星-Kang-Kunyavskii [HKK13] によってあたえられた：

**定理 1.12** (星-Kang-Kunyavskii [HKK13, Theorem 1.12], [Kan14, page 424] も参照)**.** $G$ を位数 $p^5$ ($p$: 奇素数 ) の $p$ 群とする．$H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \neq 0 \Leftrightarrow G \in \Phi_{10}$. このとき，$H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$.

位数 $p^5$ $(p \geq 5)$ の $G \in \Phi_{10}$ なる群は $1 + \gcd\{4, p-1\} + \gcd\{3, p-1\}$ 個ある ([Jam80, page 621]).

$H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) = 0$ のとき，$\mathbb{C}(G)$ が $\mathbb{C}$ 上有理的かどうか (ネーター問題) が当然問題になる．位数 $3^5 = 243$ の群 $G$ に対して，$\mathbb{C}$ 上のネーター問題は $G \in \Phi_7$ の場合を除いて，解決された：

**定理 1.13** (Chu-星-Hu-Kang [CHHK15, Theorem 1.13])**.** $G$ を位数 $3^5$ の群とする．
$H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) = 0$ かつ $G \notin \Phi_7$ ならば $\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的.

しかし，どうしても $G \in \Phi_7$ の場合には，$\mathbb{C}$ 上の有理性を示すことができなかった.

星-Kang-山崎 [HKY20] は Saltman-Peyre の方法を改良し，コンピュータ GAP [GAP] をもちいて計算できるようにした．その主定理は以下のように述べることができる：

**定理 1.14** (星-Kang-山崎 [HKY20, Theorem 1.14])**.** $G$ を位数 $3^5$ の群とする．
$H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \neq 0 \Leftrightarrow G \in \Phi_7$. このとき，$H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$.

| $\lvert G\rvert = 3^5$ | $\Phi_1$ | $\Phi_2$ | $\Phi_3$ | $\Phi_4$ | $\Phi_5$ | $\Phi_6$ | $\Phi_7$ | $\Phi_8$ | $\Phi_9$ | $\Phi_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z})$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\mathbb{Z}/3\mathbb{Z}$ |
| $H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z})$ | 0 | 0 | 0 | 0 | 0 | 0 | $\mathbb{Z}/3\mathbb{Z}$ | 0 | 0 | 0 |

**定理 1.15** (星-Kang-山崎 [HKY20, Theorem 1.15])**.** $G$ を位数 $p^5$ $(p = 5, 7)$ の群とする．
$H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \neq 0 \Leftrightarrow G \in \Phi_6, \Phi_7, \Phi_{10}$. このとき，$H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$.

| $\lvert G\rvert = p^5$ $(p = 5, 7)$ | $\Phi_1$ | $\Phi_2$ | $\Phi_3$ | $\Phi_4$ | $\Phi_5$ | $\Phi_6$ | $\Phi_7$ | $\Phi_8$ | $\Phi_9$ | $\Phi_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $H^2_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z})$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $\mathbb{Z}/p\mathbb{Z}$ |
| $H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z})$ | 0 | 0 | 0 | 0 | 0 | $\mathbb{Z}/p\mathbb{Z}$ | $\mathbb{Z}/p\mathbb{Z}$ | 0 | 0 | $\mathbb{Z}/p\mathbb{Z}$ |

定理 1.13 と定理 1.14 によって，位数 $3^5$ の群に対する $\mathbb{C}$ 上のネーター問題が解決される：

**定理 1.16.** $G$ を位数 $3^5$ の群とする．
$\mathbb{C}(G)$ は $\mathbb{C}$ 上 ( 安定, レトラクト ) 有理的 $\Leftrightarrow G \in \Phi_i$ $(1 \le i \le 6,\ 8 \le i \le 9)$.

$G$ の位数が $5^5$, $3^5$ のときも同様にして，$G \in \Phi_i$ $(1 \le i \le 4,\ 8 \le i \le 9)$ の場合には，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的であることを示せる．しかし，$G \in \Phi_5$ についての $\mathbb{C}$ 上の有理性はよく分かっていない．(このとき，$G$ は extra-special $p$ 群となる [HKY20, Section 1] 参照)

## 2　準備：不分岐コホモロジー群と安定コホモロジー群

**定義 2.1** (Saltman [Sal84a, Definition 3.1], [Sal85, page 56])．$k \subset K$ を体の拡大とする．$K$ の $k$ 上の**不分岐ブラウアー群** (unramified Brauer group) $\mathrm{Br}_{\mathrm{nr}}(K/k)$ とは，

$$\mathrm{Br}_{\mathrm{nr}}(K/k) = \bigcap_R \mathrm{Image}\{\mathrm{Br}(R) \to \mathrm{Br}(K)\}.$$

ただし，$\mathrm{Br}(R) \to \mathrm{Br}(K)$ は自然な埋め込み，$R$ は $k \subset R \subset K = Q(R)$ なる離散付置環をうごく．
基礎体 $k$ が文脈から明らかな場合には，$\mathrm{Br}_{\mathrm{nr}}(K/k)$ を単に $\mathrm{Br}_{\mathrm{nr}}(K)$ とかく．

**命題 2.2** (Saltman [Sal84a], [Sal85, Proposition 1.8])．$k$ を無限体，体 $K$ を $k$ 上レトラクト有理的とする．このとき，自然な射 $\mathrm{Br}(k) \to \mathrm{Br}(K)$ は同型 $\mathrm{Br}(k) \xrightarrow{\sim} \mathrm{Br}_{\mathrm{nr}}(K)$ を誘導する．とくに，$k = \overline{k}$ かつ $K$ は $k$ 上レトラクト有理的ならば $\mathrm{Br}_{\mathrm{nr}}(K) = 0$.

Saltman [Sal84a] は $\mathrm{Br}_{\mathrm{nr}}(K/k) \neq 0$ をもちいて，位数 $p^9$ の群 $G$ で $\mathbb{C}(G)$ が $\mathbb{C}$ 上非有理的な例をあたえた (1 章参照)．$\mathrm{Br}_{\mathrm{nr}}(K/k)$ は Grothendieck による (コホモロジカル) ブラウアー群 $\mathrm{Br}(X)$ と一致する．ただし，$X$ は関数体を $K$ とする $k$ 上の非特異射影多様体 ([Sal99, page 70, Proposition 10.5] 参照)．また，$\mathrm{Br}_{\mathrm{nr}}(K) \simeq H^3(X, \mathbb{Z})_{\mathrm{torsion}}$ でもある．ただし，$X$ は関数体を $K$ とする $\mathbb{C}$ 上の非特異射影単有理多様体 ([Voi14, page 134, Proposition 6.17] 参照)．Artin-Mumford [AM72] は $H^3(X, \mathbb{Z})_{\mathrm{torsion}}$ をもちいて，単有理的であるが有理的でない複素多様体 $X$ をあたえた ([Bog88, Theorem 1.1, Corollary] 参照).
Bogomolov [Bog88] は $\mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(G))$ に対する次の公式をあたえた：

**定理 2.3** (Bogomolov [Bog88, Theorem 3.1], Saltman [Sal90, Theorem 12])．$G$ を有限群，代数閉体 $k$ を $\mathrm{char}\ k = 0$ または $\mathrm{char}\ k = p \not| |G|$ とする．このとき，$\mathrm{Br}_{\mathrm{nr}}(k(G)/k)$ は次の $B_0(G)$ と同型：

$$B_0(G) = \bigcap_A \mathrm{Ker}\{\mathrm{res} : H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(A, \mathbb{Q}/\mathbb{Z})\}.$$

ただし，$A$ は巡回群または 2 つの巡回群の直積である $G$ の部分群をうごく．

$B_0(G) \le H^2(G, \mathbb{Q}/\mathbb{Z}) \simeq M(G)$, $M(G)$ は $G$ の Schur multiplier であることから，$B_0(G)$ は $G$ の **Bogomolov multiplier** ともよばれる (Kunyavskii [Kuny10] 参照)．とくに，$B_0(G) \simeq \mathrm{Br}_{\mathrm{nr}}(\mathbb{C}(G))$.

**定理 2.4.** (1) (Saltman [Sal84a, Theorem 3.6]) 位数 $p^9$ の $p$ 群 $G$ が存在して，$B_0(G) \neq 0$．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上非有理的.
(2) (Bogomolov [Bog88, Lemma 5.6]) 位数 $p^6$ の $p$ 群 $G$ が存在して，$B_0(G) \neq 0$．とくに，$\mathbb{C}(G)$ は $\mathbb{C}$ 上非有理的.

Colliot-Thélène–Ojanguren [CTO89] は不分岐コホモロジー群 $H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j})$ $(i \ge 1)$ を以下のように定義した．$K$ が非特異射影単有理多様体の関数体のとき，$H^1_{\mathrm{nr}}(K, \mathbb{Q}/\mathbb{Z}) = 0$ (Peyre [Pey08, page 192] 参照) となるため，$i \ge 2$ のときを考える．

$K$ を体，$K^{\mathrm{sep}}$ を $K$ の分離閉包，$\Gamma_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ を $K$ の絶対ガロア群，$\Gamma_K$ 加群 $M$ に対して，$H^i(K, M) := H^i(\Gamma_K, M)$ とおく．

ここで，$\Gamma_K$ 加群 $\mu_n^{\otimes j}$ の定義を思い出しておく．$\gcd\{\mathrm{char}\, k, n\} = 1$ とし，$\mu_n$ を $K^{\mathrm{sep}}$ の $n$ 乗根全体とする．$\mu_n$ は $\Gamma_K$ 加群とみなせる．$j \geq 1$ に対して，$\mu_n^{\otimes j}$ は $\Gamma_K$ の対角的作用によって $\Gamma_K$ 加群とみなし，$j = 0$ に対して，$\mu_n^{\otimes 0} := \mathbb{Z}/n\mathbb{Z}$ ($\Gamma_K$ の作用は自明とする)，$j < 0$ に対して，$\mu_n^{\otimes j} := \mathrm{Hom}(\mu_n^{\otimes -j}, \mathbb{Z}/n\mathbb{Z})$ と定義する．

**定義 2.5** (Colliot-Thélène–Ojanguren [CTO89], [CT95, Sections 2–4] も参照)．$K/k$ を体の有限生成拡大，$R$ を $k \subset R \subset K = Q(R)$ なる離散付置環，$\Bbbk_R$ を $R$ の剰余体とする．([GMS03, pages 15–19], [CT95, pages 21–22, page 26] によって) 自然な写像

$$r_R : H^i(K, \mu_n^{\otimes j}) \to H^{i-1}(\Bbbk_R, \mu_n^{\otimes (j-1)})$$

が定義でき，$R$ における $K$ の**剰余写像** (residue map) という．

**定義 2.6** (Colliot-Thélène–Ojanguren [CTO89], [CT95, Sections 2–4] も参照)．$n \geq 1$ に対して，体 $k$ を $\mathrm{char}\, k = 0$ または $\mathrm{char}\, k = p \nmid n$ とする．$K/k$ を体の有限生成拡大とする．$i \geq 2$, 整数 $j$ に対して，$K$ の $k$ 上の $i$ 次**不分岐コホモロジー群** (unramified cohomology group) $H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j})$ とは，

$$H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j}) := \bigcap_R \mathrm{Ker}\{r_R : H^i(K, \mu_n^{\otimes j}) \to H^{i-1}(\Bbbk_R, \mu_n^{\otimes (j-1)})\}.$$

ただし，$R$ は $k \subset R \subset K = Q(R)$ なる階数 1 の離散付置環をうごく．

[CT95, Theorem 4.1.1, page 30] によって，さらに, $K$ を $k$ 上の完備非特異多様体の関数体とすると，$H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j})$ は

$$H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j}) = \bigcap_R \mathrm{Image}\{H^i_{\text{ét}}(R, \mu_n^{\otimes j}) \to H^i_{\text{ét}}(K, \mu_n^{\otimes j})\}$$

とも定義される．ただし，$R$ は $k \subset R \subset K = Q(R)$ なる階数 1 の離散付置環をうごく．

体 $k$ が $\mathrm{char}\, k = 0$ のとき，$n$ に関する順極限

$$H^i(K/k, \mathbb{Q}/\mathbb{Z}(j)) = \varinjlim_n H^i(K/k, \mu_n^{\otimes j})$$

をとれば，$K$ の $k$ 上の $i$ 次**不分岐コホモロジー群** (unramified cohomology group)

$$H^i_{\mathrm{nr}}(K/k, \mathbb{Q}/\mathbb{Z}(j)) = \bigcap_R \mathrm{Ker}\{r_R : H^i(K/k, \mathbb{Q}/\mathbb{Z}(j)) \to H^{i-1}(\Bbbk_R, \mathbb{Q}/\mathbb{Z}(j-1))\}$$

が定義できる．

基礎体 $k$ が文脈から明らかな場合には，単に $H^i_{\mathrm{nr}}(K, \mu_n^{\otimes j})$ や $H^i_{\mathrm{nr}}(K, \mathbb{Q}/\mathbb{Z}(j))$ とかく．

$k$ が標数 0 の代数閉体のとき，$H^i_{\mathrm{nr}}(K/k, \mathbb{Q}/\mathbb{Z}(j))$ を $H^i_{\mathrm{nr}}(K/k, \mathbb{Q}/\mathbb{Z})$ とかく．有限群 $G$ に対して，$H^i_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \leq H^i(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z})$ である．

**定理 2.7.** $k$ を代数閉体とする．

(1) (Colliot-Thélène–Ojanguren [CTO89, Proposition 1.2]) 体 $k$ を $\mathrm{char}\, k = 0$ または $\mathrm{char}\, k = p \nmid n$ とする．体 $K$ と体 $L$ が安定 $k$ 同型ならば $H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j}) \xrightarrow{\sim} H^i_{\mathrm{nr}}(L/k, \mu_n^{\otimes j})$. とくに，$K$ が $k$ 上安定有理的ならば $H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j}) = 0$;

(2) (Merkurjev [Mer08, Proposition 2.15], [CTO89, Remarque 1.2.2], [CT95, Sections 2–4] も参照) $K$ が $k$ 上レトラクト有理的ならば $H^i_{\mathrm{nr}}(K/k, \mu_n^{\otimes j}) = 0$;

(3) (Colliot-Thélène [CT95, Proposition 4.2.3, page 34] 参照) $k$ を標数 0 の体とすると，$\mathrm{Br}_{\mathrm{nr}}(K/k) \simeq H^2_{\mathrm{nr}}(K/k, \mathbb{Q}/\mathbb{Z})$.

非特異有理連結な複素射影多様体 $X$ に対して，3 次不分岐コホモロジー群 $H^3_{\mathrm{nr}}(X,\mathbb{Q}/\mathbb{Z})$ は整数ホッジ予想の障害となる (Colliot-Thélène–Voisin [CTV12], Voisin [Voi14, Section 6.2] 参照)：

**定理 2.8** (Colliot-Thélène–Voisin [CTV12], Voisin [Voi14, Theorem 6.18] も参照)**.** 非特異複素射影多様体 $X$ に対して，完全列

$$0 \to H^3_{\mathrm{nr}}(X,\mathbb{Z}) \otimes \mathbb{Q}/\mathbb{Z} \to H^3_{\mathrm{nr}}(X,\mathbb{Q}/\mathbb{Z}) \to \mathrm{Tors}(Z^4(X)) \to 0$$

が存在する．ただし，

$$Z^4(X) = \mathrm{Hdg}^4(X,\mathbb{Z})/\mathrm{Hdg}^4(X,\mathbb{Z})_{\mathrm{alg}}$$

であり，“alg”は代数的なホッジ類をあらわす．とくに，$X$ が有理連結ならば

$$H^3_{\mathrm{nr}}(X,\mathbb{Q}/\mathbb{Z}) \simeq Z^4(X).$$

**定理 2.9** (Asok [Aso13], Asok-Morel [AM11, Theorem 3] も参照)**.**
(1) (Asok [Aso13, Theorem 1]) $n \geq 2$ に対して，非特異射影複素単有理多様体 $X$ が存在して，$H^i_{\mathrm{nr}}(\mathbb{C}(X),\mu_2^{\otimes i}) = 0$ $(1 < i < n)$, $H^n_{\mathrm{nr}}(\mathbb{C}(X),\mu_2^{\otimes n}) \neq 0$. とくに，$X$ は $\mathbb{A}^1$ 連結ではなく，$\mathbb{C}$ 上非レトラクト有理的;
(2) (Asok [Aso13, Theorem 3]) 素数 $l$ と $n \geq 2$ に対して，非特異射影複素有理連結多様体 $Y$ が存在して，$H^n_{\mathrm{nr}}(\mathbb{C}(Y),\mu_l^{\otimes n}) \neq 0$. とくに，$Y$ は $\mathbb{A}^1$ 連結ではなく，$\mathbb{C}$ 上非レトラクト有理的.

以下，不分岐コホモロジー $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ を計算する Saltman-Peyre の方法 ([Sal95], [Pey08]) を述べる．まず，体 $K = \mathbb{C}(G)$ に対して，$H^i(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z}) = H^i(\Gamma_K,\mathbb{Q}/\mathbb{Z})$ をとる．ただし，$\Gamma_K$ は $K$ の絶対ガロア群．$G$ は $\Gamma_K$ の商群であるから，膨張写像

$$\iota : H^i(G,\mathbb{Q}/\mathbb{Z}) \to H^i(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$$

を考えることができる．写像 $\iota$ の核と像は大変重要となる．$H^i_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z}) \leq H^i(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ に注意しておく．

ここから，部分群 $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \leq H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) \leq H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z}) \leq H^3(G,\mathbb{Q}/\mathbb{Z})$ を定義していく．そして，$\iota$ によって，同型 $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})/H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ および 2 部分を除いた同型 $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})/H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \to H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})/H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$，すなわち，$[H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) : H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})] = 2^d$ が成り立つことを見ていく．ここで $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})$ を導入したのは，$H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$ を直接計算するのは，一般に困難であるからである．

**定義 2.10.** Saltman [Sal95, page 230, Theorem 5.3] によって，$H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z}) \leq \iota(H^3(G,\mathbb{Q}/\mathbb{Z}))$ となる．そこで，Saltman [Sal95, page 220] にしたがって，

$$H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) := \mathrm{Ker}\{\iota : H^3(G,\mathbb{Q}/\mathbb{Z}) \to H^3(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})\}$$

と定義する．この $H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$ の元は **geometrically negligible class** とよばれる．

一方で，部分群 $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z}) \leq H^3(G,\mathbb{Q}/\mathbb{Z})$ は以下の定義 2.12 のように定義される．Peyre [Pey08, page 204, Proposition 3] によれば，$H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z}) = \iota^{-1}(H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z}))$ である．すなわち，膨張写像 $\iota$ は同型 $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})/H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ を誘導する．

定義 2.12 に必要な以下の定理を準備しておく：

**定理 2.11** (Neukirch-Schmidt-Wingberg [NSW08, page 118, Theorem 2.4.6], Jansen [Jan90] も参照)**.** $G$ と $H$ を有限群，$A$ を $\mathbb{Z}[G \times H]$ 加群とする．Lyndon-Hochschild-Serre スペクトラル系列

$$E_2^{p,q} = H^p(G, H^q(H,A)) \Rightarrow H^{p+q}(G \times H, A)$$

は $E_2$ 項で退化する．すなわち，$E_2^{p,q} = E_3^{p,q} = \cdots = E_\infty^{p,q}$．さらに，次の分解をえる：

$$H^n(G \times H, A) \simeq \bigoplus_{p+q=n} H^p(G, H^q(H, A)).$$

**定義 2.12.** $H \leq G$ を部分群，$Z_G(H)$ を $H$ の $G$ 内での中心化群とする．$g \in Z_G(H)$ に対して，写像

$$\partial_{H,g} : H^3(G, \mathbb{Q}/\mathbb{Z}) \to H^2(H, \mathbb{Q}/\mathbb{Z})$$

を次のように定義する：

$I = \langle g \rangle$ とする．写像 $m : H \times I \to G, (h, i) \mapsto hi$ から

$$m^* : H^3(G, \mathbb{Q}/\mathbb{Z}) \to H^3(H \times I, \mathbb{Q}/\mathbb{Z})$$

が誘導される．$\mathrm{pr}_2 : H \times I \to I$ を第 2 成分の射影，$i_2 : I \to H \times I, i \mapsto (e, i)$ によって，$I$ を $H \times I$ の部分群とみなす．ただし，$e$ は $H$ の単位元．写像 $i_2$ は制限写像

$$i_2^* : H^3(H \times I, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{res}} H^3(I, \mathbb{Q}/\mathbb{Z})$$

を誘導し，$\mathrm{pr}_2$ は $i_2^*$ の切断を誘導する．これにより，写像

$$S_{H,I} : H^3(H \times I, \mathbb{Q}/\mathbb{Z}) \to H^3(H \times I, \mathbb{Q}/\mathbb{Z})_1,\ \xi \mapsto \xi - \mathrm{pr}_2^* \circ i_2^*(\xi)$$

がえられる．ただし，

$$H^3(H \times I, \mathbb{Q}/\mathbb{Z})_1 = \mathrm{Ker}\{H^3(H \times I, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{res}} H^3(I, \mathbb{Q}/\mathbb{Z})\}.$$

Lyndon-Hochschild-Serre スペクトラル系列 [HS53]

$$E_2^{p,q} = H^p(H, H^q(I, \mathbb{Q}/\mathbb{Z})) \Rightarrow H^{p+q}(H \times I, \mathbb{Q}/\mathbb{Z})$$

を適用する．定理 2.11 から，スペクトル系列は $E_2$ 項で退化し，次の同型をえる：

$$\begin{aligned} &H^3(H \times I, \mathbb{Q}/\mathbb{Z}) \\ &\simeq H^3(H, H^0(I, \mathbb{Q}/\mathbb{Z})) \oplus H^2(H, H^1(I, \mathbb{Q}/\mathbb{Z})) \oplus H^1(H, H^2(I, \mathbb{Q}/\mathbb{Z})) \oplus H^0(H, H^3(I, \mathbb{Q}/\mathbb{Z})) \\ &\simeq H^3(H, \mathbb{Q}/\mathbb{Z}) \oplus H^2(H, H^1(I, \mathbb{Q}/\mathbb{Z})) \oplus 0 \oplus H^3(I, \mathbb{Q}/\mathbb{Z}). \end{aligned}$$

($I = \langle g \rangle$ は巡回群より，$H^2(I, \mathbb{Q}/\mathbb{Z}) = 0$) これより，写像

$$S_{H,I} : H^3(H \times I, \mathbb{Q}/\mathbb{Z}) \to H^3(H \times I, \mathbb{Q}/\mathbb{Z})_1,\ \xi = (\xi_0, \xi_1, 0, \xi_3) \mapsto \xi' = (\xi_0, \xi_1, 0, 0)$$

および写像

$$\varphi : H^3(H \times I, \mathbb{Q}/\mathbb{Z})_1 \to H^2(H, H^1(I, \mathbb{Q}/\mathbb{Z})),\ \xi' = (\xi_0, \xi_1, 0, 0) \mapsto \xi_1$$

がえられる．また単射

$$H^1(I, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathrm{Hom}(I, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/|I|\mathbb{Z} \simeq \frac{1}{|I|}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

から，目的の $\partial_{H,g} = \partial \circ m^* = \psi_g \circ \varphi \circ S_{H,I} \circ m^*$:

$$\begin{array}{ccccc} \partial_{H,g} : H^3(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{m^*} & H^3(H \times I, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\partial} & H^2(H, \mathbb{Q}/\mathbb{Z}) \\ & & \downarrow{\scriptstyle S_{H,I}} & \circlearrowleft & \uparrow{\scriptstyle \psi_g} \\ & & H^3(H \times I, \mathbb{Q}/\mathbb{Z})_1 & \xrightarrow{\varphi} & H^2(H, H^1(I, \mathbb{Q}/\mathbb{Z})) \end{array}$$

が定義できた．

そこで，Peyre [Pey08, page 197] にしたがって，

$$H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z}) = \bigcap_{\substack{H\le G\\ g\in Z_G(H)}} \mathrm{Ker}(\partial_{H,g})$$

と定義する．

部分群 $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \le H^3(G,\mathbb{Q}/\mathbb{Z})$ に戻ろう．$\mu$ を $\mathbb{C}$ 内の 1 のべき根全体のなす群とする．$G$ 加群としても $\Gamma_K$ 加群としても $\mu \simeq \mathbb{Q}/\mathbb{Z}$ である．

ここで，置換 $\mathbb{Z}[G]$ 格子の定義を思い出しておく．有限生成 $\mathbb{Z}[G]$ 加群 $P$ が**置換 $\mathbb{Z}[G]$ 格子** (permutation $\mathbb{Z}[G]$-lattice) であるとは，$P$ は階数有限の自由アーベル群であり $G$ の $P$ への作用が $P$ の $\mathbb{Z}$ 基底を置換する，すなわち $P = \oplus_{1\le i\le n}\mathbb{Z}\cdot x_i$ で $\sigma\cdot x_i = x_j$ $(\sigma\in G)$，となること．

**命題 2.13** (Saltman [Sal95, page 221, Lemma 4.6 (b)])．$\mathbb{Z}[G]$ 加群 $P^* \ge \mu$ が存在して，(i) 商群 $P := P^*/\mu$ は置換 $\mathbb{Z}[G]$ 格子; (ii) すべての部分群 $H \le G$ に対して，$H^1(H,P^*) = 0$; (iii) すべての $\varphi : \mu \to N$ が $P^*$ に拡張できる $\Leftrightarrow$ すべての $H \le G$ に対して，$H^1(H,\mu) \to H^1(H,N)$ は零写像，をみたす．

**定義 2.14** (Saltman [Sal95, Proposition 4.7])．$Q$ を置換 $\mathbb{Z}[G]$ 格子，$0 \to \mu \to Q^* \to Q \to 0$ を $\mathbb{Z}[G]$ 加群の完全系列で，すべての $H \le G$ に対して，$H^1(H,Q^*) = 0$ とする (例えば，$Q^*$ として，命題 2.13 から構成される $P^*$ をとればよい)

そこで，**置換 negligible class による群** (the group of permutation negligible classes) を

$$H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) := \mathrm{Ker}\{H^3(G,\mathbb{Q}/\mathbb{Z}) \to H^3(G,Q^*)\}$$

によって定義する．この名称は，実際

$$H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Image}\{H^2(G,Q) \xrightarrow{\delta} H^3(G,\mathbb{Q}/\mathbb{Z})\}$$

であることから来ている．ただし，$\delta : H^2(G,Q) \to H^3(G,\mathbb{Q}/\mathbb{Z})$ は $0 \to \mu \to Q^* \to Q \to 0$ から生じる連結準同型写像．定義 2.14 は $\mathbb{Z}[G]$ 加群 $Q^*$ の取り方に依存しているようにみえる．しかし，Saltman [Sal95, pages 221–222, Proposition 4.7] によって，(i) $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})$ は $Q^*$ のとり方によらない; (ii) $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Ker}\{H^3(G,\mathbb{Q}/\mathbb{Z}) \to H^3(G,L^\times)\}$ が成り立つ．ただし，$L := k(x_g : g\in G)$ は定義 1.1 の有理関数体．とくに，$H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \le H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$ となる．

Saltman [Sal95, page 191, Theorem 4.14] により，$G$ が巡回群を指数 2 として含む非可換 2 群のとき，$H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \lneq H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$ となる．しかし，Peyre [Pey08] は次の結果を示した：

**定理 2.15** (Peyre)．$\iota : H^3(G,\mathbb{Q}/\mathbb{Z}) \to H^3(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ を膨張写像とする．
(i) (Peyre [Pey08, Theorem 1]) 全射

$$\bar{\iota} : H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})/H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) \to H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$$

の核の位数は 2 べき，すなわち，$[H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) : H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})] = 2^d$. とくに，$G$ の位数が奇数ならば $H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z}) = H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})$.
(ii) (Peyre [Pey99, pages 196–197], [Pey08, Remark 2] も参照)

$$H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) = \sum_{H\le G} \mathrm{Cores}^G_H(\mathrm{Image}\{H^1(H,\mathbb{Q}/\mathbb{Z})^{\otimes 2} \xrightarrow{\cup} H^3(H,\mathbb{Q}/\mathbb{Z})\}).$$

ただし，カップ積は次の可換図式から得られる $(i\ge 1,\ j\ge 1)$：

$$\begin{array}{ccc} H^i(G,\mathbb{Q}/\mathbb{Z}) \times H^j(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & H^{i+1}(G,\mathbb{Z}) \times H^{j+1}(G,\mathbb{Z}) \\ \downarrow \cup & \circlearrowleft & \downarrow \cup \\ H^{i+j+1}(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & H^{i+j+2}(G,\mathbb{Z}). \end{array}$$

最後に Bogomolov による安定コホモロジーを定義する：

**定義 2.16** (Bogomolov [Bog07, Definition 6.4, Lemma 6.5, Theorem 6.8])**.** 商群

$$H^i_{\mathrm{s}}(G,\mathbb{Q}/\mathbb{Z}) = H^i(G,\mathbb{Q}/\mathbb{Z})/H^i_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$$

を $G$ の $i$ 次**安定コホモロジー群** (stable cohomology group) という ([Bog93, page 6], [BP11, page 938], [BB13, page 57], [BB14, page 212] も参照).

$i=3$ のとき，Saltman [Sal95, page 230, Theorem 5.3] から，$H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z}) \leq \iota(H^3(G,\mathbb{Q}/\mathbb{Z}))$ であるから，

$$H^3_{\mathrm{s}}(G,\mathbb{Q}/\mathbb{Z}) \simeq \iota(H^3(G,\mathbb{Q}/\mathbb{Z})) \geq H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$$

となる．

Bogomolov-Petrov-Tschinkel [BPT10, page 68] ([Bog07, Definition 8.5], [BP11, page 938], [BB14, page 214] も参照) では，$\iota(H^i(G,\mathbb{Q}/\mathbb{Z})) \cap H^i_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ を $H^i_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ と定義しているので注意が必要である．これは，我々の (Peyre による) 定義 2.12 とは異なる．

[HKY20] の主結果である定理 1.14 と定理 1.15 の証明の詳細については [HKY20, Section 3] をみていただきたい．とくに，そこで使われている我々が作成した GAP のアルゴリズムは

`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/UnramDeg3/`

から入手することができる．

ここに，GAP による計算結果を載せておく．Peyre による定理 2.15 (i) から，$|G|$ が奇数のときは，$H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z}) = H^3_{\mathrm{n}}(G,\mathbb{Q}/\mathbb{Z})$ であるから，ここから安定コホモロジー群 $H^3_{\mathrm{s}}(G,\mathbb{Q}/\mathbb{Z})$ もえられる．

| $\lvert G\rvert = 3^5$ | | $H^3(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ |
|---|---|---|---|---|---|
| $\Phi_7$ | $G(3^5,56)$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 7}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/3\mathbb{Z}$ |
| | $G(3^5,57)$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/3\mathbb{Z}$ |
| | $G(3^5,58)$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 9}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 7}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $\mathbb{Z}/3\mathbb{Z}$ |
| | $G(3^5,59)$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/3\mathbb{Z}$ |
| | $G(3^5,60)$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $\Phi_{10}$ | $G(3^5,28)$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}\oplus\mathbb{Z}/9\mathbb{Z}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 3}$ | $0$ |
| | $G(3^5,29)$ | $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/9\mathbb{Z}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $0$ |
| | $G(3^5,30)$ | $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/9\mathbb{Z}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ | $0$ |

| $\lvert G\rvert = 5^5$ | | $H^3(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ |
|---|---|---|---|---|---|
| $\Phi_5$ | $G(5^5,75)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 15}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 10}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 10}$ | $0$ |
| | $G(5^5,76)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 10}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 10}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 10}$ | $0$ |
| $\Phi_6$ | $G(5^5,3)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 7}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 7}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,4)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,5)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,6)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,7)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}\oplus\mathbb{Z}/25\mathbb{Z}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}\oplus\mathbb{Z}/25\mathbb{Z}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}\oplus\mathbb{Z}/25\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,8)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,9)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,10)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}\oplus\mathbb{Z}/25\mathbb{Z}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}\oplus\mathbb{Z}/25\mathbb{Z}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}\oplus\mathbb{Z}/25\mathbb{Z}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,11)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,12)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,13)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,14)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| $\Phi_7$ | $G(5^5,66)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 10}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 7}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,67)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,68)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,69)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,70)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| $\Phi_{10}$ | $G(5^5,33)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 5}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,34)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,35)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,36)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,37)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/5\mathbb{Z}$ |
| | $G(5^5,38)$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/5\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/5\mathbb{Z}$ |

| $\lvert G\rvert = 7^5$ | | $H^3(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{p}}(G,\mathbb{Q}/\mathbb{Z})$ | $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ |
|---|---|---|---|---|---|
| $\Phi_5$ | $G(7^5,82)$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 10}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 10}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 10}$ | $0$ |
| $\Phi_6$ | $G(7^5,7)$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 4}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 3}$ | $\mathbb{Z}/7\mathbb{Z}$ |
| $\Phi_7$ | $G(7^5,73)$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 6}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 5}$ | $\mathbb{Z}/7\mathbb{Z}$ |
| $\Phi_{10}$ | $G(7^5,38)$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 3}$ | $(\mathbb{Z}/7\mathbb{Z})^{\oplus 2}$ | $\mathbb{Z}/7\mathbb{Z}$ |

## 参考文献


[AM72] M. Artin, D. Mumford, *Some elementary examples of unirational varieties which are not rational*, Proc. London Math. Soc. **25** (1972) 75–95.

[Aso13] A. Asok, *Rationality problems and conjectures of Milnor and Bloch-Kato*, Compos. Math. **149** (2013) 1312–1326.

[AM11] A. Asok, F. Morel, *Smooth varieties up to $\mathbb{A}^1$-homotopy and algebraic h-cobordisms*, Adv. Math. **227** (2011) 1990–2058.

[Bog88] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Math. USSR Izv. **30** (1988) 455–485.

[Bog93] F. A. Bogomolov, *Stable cohomology of groups and algebraic varieties*, Russian Acad. Sci. Sb. Math. **76** (1993) 1–21.

[Bog07] F. A. Bogomolov, *Stable cohomology of finite and profinite groups*, Algebraic groups, 19–49, Universitätsverlag Göttingen, Göttingen, 2007.

[BB13] F. A. Bogomolov, C. Böhning, *Isoclinism and stable cohomology of wreath products*, Birational geometry, rational curves, and arithmetic, 57–76, Springer, New York, 2013.

[BB14] F. A. Bogomolov, C. Böhning, *Stable cohomology of alternating groups*, Cent. Eur. J. Math. **12** (2014) 212–228.

[BP11] F. A. Bogomolov, T. Petrov, *Unramified cohomology of alternating groups*, Cent. Eur. J. Math. **9** (2011) 936–948.

[BPT10] F. A. Bogomolov, T. Petrov, Y. Tschinkel, *Unramified cohomology of finite groups of Lie type*, Cohomological and geometric approaches to rationality problems, 55–73, Progr. Math., 282, Birkhäuser Boston, Inc., Boston, MA, 2010.

[CHHK15] H. Chu, A. Hoshi, S.-J. Hu, M. Kang, *Noether's problem for groups of order* 243, J. Algebra **442** (2015) 233–259.

[CHKK10] H. Chu, S.-J. Hu, M. Kang, B. E. Kunyavskii, *Noether's problem and the unramified Brauer group for groups of order* 64, Int. Math. Res. Not. IMRN 2010 2329–2366.

[CHKP08] H. Chu, S.-J. Hu, M. Kang, Y. G. Prokhorov, *Noether's problem for groups of order* 32, J. Algebra **320** (2008) 3022–3035.

[CK01] H. Chu, M. Kang, *Rationality of p-group actions*, J. Algebra **237** (2001) 673–690.

[CT95] J.-L. Colliot-Thélène, *Birational invariants, purity and the Gersten conjecture*, K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), 1–64, Proc. Sympos. Pure Math., 58, Part 1, Amer. Math. Soc., Providence, RI, 1995.

[CTO89] J.-L. Colliot-Thélène, M. Ojanguren, *Variétés unirationnelles non rationnelles: au-delà de l'example d'Artin et Mumford*, Invent. Math. **97** (1989) 141–158.

[CTS07] J.-L. Colliot-Thélène, J.-J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups* (*with special regards to the Brauer group*), Algebraic groups and homogeneous spaces, 113–186, Tata Inst. Fund. Res. Stud. Math., Tata Inst. Fund. Res., Mumbai, 2007.

[CTV12] J.-L. Colliot-Thélène, C. Voisin, *Cohomologie non ramifiée et conjecture de Hodge entière*, Duke Math. J. **161** (2012) 735–801.

[Fis1915] E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen*, Nachr. Königl. Ges. Wiss. Göttingen (1915) 77–80.

[Gas59] W. Gaschütz, *Fixkörper von p-Automorphismengruppen rein-transzendenter Körpererweiterungen von p-Charakteristik*, Math. Z. **71** (1959) 466–468.

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.7, 2017 (http://www.gap-system.org).

[GMS03] S. Garibaldi, A. Merkurjev, J-P. Serre, *Cohomological invariants in Galois cohomology*, AMS Univ. Lecture Series, vol.28, Amer. Math. Soc., Providence, RI, 2003.

[Hal40] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940) 130–141.

[HS53] G. Hochschild, J-P. Serre, *Cohomology of group extensions*, Trans. Amer. Math. Soc. **74** (1953) 110–134.

[HKK13] A. Hoshi, M. Kang, B. E. Kunyavskii, *Noether's problem and unramified Brauer groups*, Asian J. Math. **17** (2013) 689–714.

[HKY16] A. Hoshi, M. Kang, A. Yamasaki, *Degree three unramified cohomology groups*, J. Algebra **458** (2016) 120–133.

[HKY20] A. Hoshi, M. Kang, A. Yamasaki, *Degree three unramified cohomology groups and Noether's problem for groups of order* 243, J. Algebra **544** (2020) 262–301.

[Jam80] R. James, *The groups of order $p^6$* (*$p$ an odd prime*), Math. Comp. **34** (1980) 613–637.

[JNO90] R. James, M. F. Newman, E. A. O'Brien, *The groups of order* 128, J. Algebra **129** (1990) 136–158.

[Jan90] U. Jannsen, *The splitting of the Hochschild-Serre spectral sequence for a product of groups*, Canad. Math. Bull. **33** (1990) 181–183.

[Kan14] M. Kang, *Bogomolov multipliers and retract rationality for semidirect products*, J. Algebra **397** (2014) 407–425.

[Kun56] H. Kuniyoshi, *Certain subfields of rational function fields*, Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, 241–243, Science Council of Japan, Tokyo, 1956.

[Kuny10] B. Kunyavskii, *The Bogomolov multiplier of finite simple groups*, in "Cohomological and geometric approaches to rationality problems", edited by F. Bogomolov and Y. Tschinkel, Birkhäuser, Boston, 2010.

[Mer08] A. Merkurjev, *Unramified elements in cycle modules*, J. Lond. Math. Soc. (2) **78** (2008) 51–64.

[Mor12] P. Moravec, *Unramified Brauer groups of finite and infinite groups*, Amer. J. Math. **134** (2012) 1679–170.

[MT86] Y. I. Manin, M. A. Tsfasman, *Rational varieties: algebra, geometry, arithmetic*, Russian Math. Surveys **41** (1986) 51–116.

[NSW08] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Second Edition. Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2008, xvi+825 pp.

[Noe1913] E. Noether, *Rationale Funktionenkörper*, Jber. Deutsch. Math.-Verein. **22** (1913) 316–319.

[Pey93] E. Peyre, *Unramified cohomology and rationality problems*, Math. Ann. **296** (1993) 247–268.

[Pey99] E. Peyre, *Application of motivic complexes to negligible classes*, Algebraic K-theory (Seattle, WA, 1997), 181–211, Proc. Sympos. Pure Math., 67, Amer. Math. Soc., Providence, RI, 1999.

[Pey08] E. Peyre, *Unramified cohomology of degree* 3 *and Noether's problem*, Invent. Math. **171** (2008) 191–225.

[Sal84a] D. J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984) 71–84.

[Sal84b] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984) 165–215.

[Sal85] D. J. Saltman, *The Brauer group and the center of generic matrices*, J. Algebra **97** (1985) 53–67.

[Sal90] D. J. Saltman, *Multiplicative field invariants and the Brauer group*, J. Algebra **133** (1990) 533–544.

[Sal95] D. J. Saltman, *Brauer groups of invariant fields, geometrically negligible classes, an equivariant Chow group, and unramified* $H^3$, K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), 189–246, Proc. Sympos. Pure Math., 58, Part 1, Amer. Math. Soc., Providence, RI, 1995.

[Sal99] D. J. Saltman, *Lectures on division algebras*, CBMS Regional Conference Series in Mathematics, 94, Amer. Math. Soc., Providence, RI, 1999.

[Swa69] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969) 148–158.

[Swa83] R. G. Swan, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (Bryn Mawr, Pa., 1982), 21–40, Springer, New York-Berlin, 1983.

[Voi14] C. Voisin, *Chow rings, decomposition of the diagonal, and the topology of families*, Annals of Mathematics Studies, 187, Princeton University Press, Princeton, NJ, 2014.

[星] 星明考，群論序説，日本評論社，2016 年，271 ページ.

Akinari Hoshi
Department of Mathematics
Niigata University
8050 Ikarashi 2-no-cho
Nishi-ku, Niigata, 950-2181
Japan
E-mail: hoshi@math.sc.niigata-u.ac.jp
Web: http://mathweb.sc.niigata-u.ac.jp/~hoshi/

# 3 次不分岐コホモロジー群の GAP による計算

山崎愛一

2019 年 9 月 10 日

## 目次



# 1 $H^3_p(G,\mathbb{Q}/\mathbb{Z})$ の計算

この章と次の章は, 星-Kang-山崎 [HKY] "Degree three unramified cohomology groups and Noether's problem for groups of order 243" の結果と計算機によるその具体的な計算例を主に扱う. $G$ は奇数位数の有限群とする.

## 1.1 Peyre の公式

置換 negligible class$H^3_p(G,\mathbb{Q}/\mathbb{Z})$ を最初に定義したのは Saltman[Sal95] である.
Peyre[Pey99][Pey08] は $H^3_p(G,\mathbb{Q}/\mathbb{Z})$ を具体的に次の式で表した.

$$H^3_p(G,\mathbb{Q}/\mathbb{Z}) = \sum_{H\leq G} \mathrm{Cores}^G_H\big(\mathrm{Image}\{H^1(H,\mathbb{Q}/\mathbb{Z})^{\otimes 2} \xrightarrow{\cup} H^3(H,\mathbb{Q}/\mathbb{Z})\}\big).$$

ただしカップ積は, $H^1(H,\mathbb{Q}/\mathbb{Z}), H^3(H,\mathbb{Q}/\mathbb{Z})$ をそれぞれ $H^2(H,\mathbb{Z}), H^4(H,\mathbb{Z})$ と同一視して行うものとする.

## 1.2 $H^4(G,\mathbb{Z}) \simeq H^3(G,\mathbb{Q}/\mathbb{Z})$ の計算

計算機上では $H^3(G,\mathbb{Q}/\mathbb{Z})$ 内で計算するよりも $H^4(G,\mathbb{Z})$ で計算するほうが楽なので

$$H^4_p(G,\mathbb{Z}) = \sum_{H\leq G} \mathrm{Cores}^G_H\big(\mathrm{Image}\{H^1(H,\mathbb{Q}/\mathbb{Z})^{\otimes 2} \xrightarrow{\cup} H^4(H,\mathbb{Z})\}\big)$$

を計算する.

まず $H^4(G,\mathbb{Z})$ を計算するために, 自明な $\mathbb{Z}[G]$-加群 $\mathbb{Z}$ の free resolution を計算する. これには GAP[GAP] 上でパッケージ HAP[HAP][EHS] を用いる. 具体的には,$G$ がべき零群のときは

`ResolutionNormalSeries(LowerCentralSeries(`$G$`,5))`

$G$ がべき零群ではないが可解群のときは

`ResolutionNormalSeries(DerivedSeries(`$G$`,5))`

で計算できる. ここでは $G$ は奇数位数と仮定しているので, 必ず可解群にはなる. 結果として free resolution

$$RG : \cdots \to P_5 \to P_4 \to P_3 \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

を得る. これは通常の bar resolution とは異なる. 例えば $G$ が位数 $p^5$($p$ は素数) の群のとき, $P_0 = \mathbb{Z}[G], P_1, P_2, P_3, P_4, P_5$ の $\mathbb{Z}[G]$-rank はそれぞれ 1,5,15,35,70,126 になる. 一般に bar resolution よりも $\mathbb{Z}[G]$-rank が小さくなるので計算機上で効率的にコホモロジーの計算ができる.

コチェイン複体 $\mathrm{Hom}_{\mathbb{Z}[G]}(P_*,\mathbb{Z})$ からコホモロジー群 $H^i(G,\mathbb{Z}) = Z^i(G,\mathbb{Z})/B^i(G,\mathbb{Z})$ が計算できる. free resolution の取り方によらずに $H^i(G,\mathbb{Z})$ が同型になることが知られている. しかし, $H^4(G,\mathbb{Z})$ の部分群として $H^4_p(G,\mathbb{Z})$,$H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ を計算する必要があるので, free resolution$RG$ を一つ固定して計算する必要がある. 具体的には HAP の関数 `CR_CocyclesAndCoboundaries(`$RG$`,4,true)` を用いて, $Z^4(G,\mathbb{Z})$,$B^4(G,\mathbb{Z})$ の $\mathbb{Z}$ 基底, $H^4(G,\mathbb{Z})$ のアーベル不変量と生成元を計算できる.

## 1.3 Peyre の公式の改良

星-Kang-山崎は $H^3_p(G,\mathbb{Q}/\mathbb{Z})$ を計算機で具体的に計算するために Peyre の公式を改良した. Peyre の公式では $H$ は $G$ の部分群すべてを動くが, 動かす $H$ をもっと減らすことを考える.

(i)$H$ の交換子群 $D(H)$ が $H$ 全体になるような $H$ は除外してよい. $D(H) = H$ のとき $H^2(H,\mathbb{Z}) \simeq H^1(H,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(H,\mathbb{Q}/\mathbb{Z}) \simeq H/D(H) = 1$ となるからである.

(ii) 共役な部分群の類から $H$ を一つずつ取ればよい. $H$ と共役な部分群 $H^\sigma = \sigma^{-1}H\sigma$ を考えると, $H^2(H^\sigma,\mathbb{Z})^{\otimes 2}$ のカップ積の $\mathrm{Cores}^G_{H^\sigma}$ による像と $H^2(H,\mathbb{Z})^{\otimes 2}$ のカップ積の $\mathrm{Cores}^G_H$ による像とは $H^4(G,\mathbb{Z})$ の同じ部分群になるからである.

(iii)$D(H') = D(H)$ かつ $H' < H$ のとき,$H'$ は除外してよい. $D(H') = D(H)$ かつ $H' < H$ のとき, 任意の $\chi' \in H^1(H',\mathbb{Q}/\mathbb{Z})$ に対して $\chi'$ を $H$ に延長できる. すなわち $\chi \in H^1(H,\mathbb{Q}/\mathbb{Z})$ が存在して $\chi' = \mathrm{Res}^H_{H'}\chi$ となる. このとき $\mathrm{Cores}^G_{H'}(\chi'_1 \cup \chi'_2) = \mathrm{Cores}^G_H\mathrm{Cores}^H_{H'}\big(\mathrm{Res}^H_{H'}\chi_1 \cup \mathrm{Res}^G_{H'}\chi_2\big) = \mathrm{Cores}^G_H\mathrm{Cores}^H_{H'}\big(\mathrm{Res}^H_{H'}(\chi_1 \cup \chi_2)\big) = [H:H']\mathrm{Cores}^G_H(\chi_1 \cup \chi_2)$ が成り立つ.

## 1.4 計算例

まず, 自明な $\mathbb{Z}[G]$-加群 $\mathbb{Z}$ の free resolution$RG$ をあらかじめ計算して固定する. `H4pFromResolution(`$RG$`)` で $H^4_p(G,\mathbb{Z})$ が計算できる.

以下に $G$ が位数 243 の群 $G(243,57)$ のときの計算例を示す. この群は isoclinism family $\Phi_7$ に属する.

```
gap> Read("H3nr.gap");
gap> G57:=SmallGroup(243,57);
<pc group of size 243 with 5 generators>
gap> RG57:=ResolutionNormalSeries(LowerCentralSeries(G57),5);
Resolution of length 5 in characteristic 0 for <pc group with 243 generators> .

gap> H4pFromResolution(RG57);
12[ [ 27, 2 ], [ 27, 2 ], [ 27, 5 ], [ 27, 2 ], [ 27, 2 ], [ 27, 5 ],
    [ 27, 2 ], [ 81, 13 ], [ 81, 13 ], [ 81, 13 ], [ 81, 12 ], [ 243, 57 ] ]
1/12
2/12
3/12
4/12
5/12
6/12
7/12
8/12
9/12
10/12
11/12
12/12
[ [ 3, 3, 3, 3, 3 ],
  [ [ 3, 3, 3, 3, 3, 3 ],
    [ [ 1, 0, 0, 0, 0, 0 ], [ 0, 1, 0, 0, 0, 0 ], [ 0, 0, 1, 0, 0, 0 ],
      [ 0, 0, 0, 1, 0, 0 ], [ 0, 0, 0, 0, 0, 1 ] ] ] ]
```

まず, 最初の 2 行の表示は, 条件 (i)-(iii) を満たす $G$ の部分群 $H$ は全部で 12 個あり, 同型類の番号がそれぞれ [27,2],[27,2],...,[243,57] であることを表している. $G$ の部分群は全部で 180 個あるので, かなり減らせているのが分かる. その次の表示 1/12 から 12/12 は $H^4_p(G,\mathbb{Z})$ の計算の進捗状況を表している. `H4pFromResolution(`$RG$`)` の戻り値は $[l_1,[l_2,l_3]]$ の形のリストで, $l_1$ は $H^4_p(G,\mathbb{Z})$ のアーベル不変量, $l_2$ は $H^4(G,\mathbb{Z})$ のアーベル不変量, $l_3$ は free resolution $RG$ に対する $H^4(G,\mathbb{Z})$ の中での $H^4_p(G,\mathbb{Z})$ の生成元を表している. 今の場合 $H^4_p(G,\mathbb{Z}) \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 5}$, $H^4(G,\mathbb{Z}) \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$ である. $H^4(G,\mathbb{Z})$ の生成元を $f_1,\ldots,f_6$ とおくとき, $H^4_p(G,\mathbb{Z})$ の生成元は $f_1,f_2,f_3,f_4,f_6$ である.

# 2 $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ の計算

## 2.1 Peyre の公式

Peyre は $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ を具体的な式の形

$$H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z}) = \bigcap_{\substack{H \leq G \\ g \in Z_G(H)}} \mathrm{Ker}(\partial_{H,g})$$

で表した.

## 2.2 Peyre の公式の改良

我々の最終目標は $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ を計算することである. $G$ は奇数位数と仮定しているので $H^3_p(G,\mathbb{Q}/\mathbb{Z}) = H^3_n(G,\mathbb{Q}/\mathbb{Z})$ が成り立つ. 従って $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})/H^3_p(G,\mathbb{Q}/\mathbb{Z})$ を計算すれば良い.. ところが,Peyre の公式を用いて直接 $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ を計算するのは困難である. $H^3_p(G,\mathbb{Q}/\mathbb{Z})$ がすでにかなり大きく, $H^3(G,\mathbb{Q}/\mathbb{Z})$ に近いことを利用する. $\gamma \in H^3(G,\mathbb{Q}/\mathbb{Z})$ が $H^3_p(G,\mathbb{Q}/\mathbb{Z})$ に属さないとき, $H^3_{\mathrm{nr}}(G,\mathbb{Q}/\mathbb{Z})$ に属するかどうか判定することを考える.

計算機上では $H^3(G,\mathbb{Q}/\mathbb{Z})$ の中で考えるよりも $H^4(G,\mathbb{Z})$ の中で計算するほうが楽なので,

$$H^4_{\mathrm{nr}}(G,\mathbb{Z}) = \bigcap_{\substack{H \leq G \\ g \in Z_G(H)}} \mathrm{Ker}(\widetilde{\partial}_{H,g})$$

を考える. ここで, $\widehat{\partial}_{H,g} : H^4(G,\mathbb{Z}) \to H^3(H,\mathbb{Z})$ は $\partial_{H,g} : H^3(G,\mathbb{Q}/\mathbb{Z}) \to H^2(H,\mathbb{Q}/\mathbb{Z})$ で $H^3(G,\mathbb{Q}/\mathbb{Z})$,$H^2(H,\mathbb{Q}/\mathbb{Z})$ をそれぞれ $H^4(G,\mathbb{Z})$,$H^3(H,\mathbb{Z})$ と同一視したものである.

Peyre の公式では $H$ は $G$ の部分群をすべて動き, $g$ は $Z_G(H)$ をすべて動く. これをもっと減らすことを考える.

(i) $I = \langle g \rangle$ ごとに考えればよい. $I = \langle g \rangle = \langle g' \rangle$ のとき, $\mathrm{Ker}(\widetilde{\partial}_{H,g}) = \mathrm{Ker}(\widetilde{\partial}_{H,g'})$ が成り立つからである.

(ii) $(H,I)$ の組は, 各共役類の中から一つずつ選べばよい. $\mathrm{Ker}(\widetilde{\partial}_{H,I}) = \mathrm{Ker}(\widetilde{\partial}_{H^\sigma,I^\sigma})$ が成り立つからである.

(iii) $(H,I)$ の組は, 包含関係 $(H',I') \leq (H,I)$ に関して極大なものだけを考えればよい. したがって $H = Z_G(I)$ のときのみを考えればよい. $H' \leq H, I' = \langle g' \rangle \leq I = \langle g \rangle$ のとき, $\mathrm{Ker}(\widetilde{\partial}_{H,g}) \leq \mathrm{Ker}(\widetilde{\partial}_{H',g'})$ が成り立つからである. さらに,$\langle g \rangle \leq Z_G(H)$ のとき $H \leq Z_G(\langle g \rangle)$ が成り立つので, $\big(H,\langle g \rangle\big) \leq \big(Z_G(\langle g \rangle),\langle g \rangle\big)$ が成り立つ. 極大性から, $\big(Z_G(\langle g \rangle),\langle g \rangle\big)$ だけを選べばよい. 明らかに $g$ は $Z_G(\langle g \rangle)$ に属する.

(iv) $H^3(H,\mathbb{Z}) \neq 0$ となる $H$ だけを考えればよい. $H^3(H,\mathbb{Z}) = 0$ のとき,$\widetilde{\partial}_{H,g} = 0$, $\mathrm{Ker}(\widetilde{\partial}_{H,g}) = H^4(G,\mathbb{Z})$ となるからである.

$l \in H^4(G,\mathbb{Z})$ に対して, `IsUnramifiedH3(RG,l)` は $l \in H^4_{\mathrm{nr}}(G,\mathbb{Z})$ かどうか判定する.

$G$ がそれほど大きくない奇数位数の群のときは, これで $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z}) \simeq H^4_{\mathrm{nr}}(G,\mathbb{Z})/H^4_p(G,\mathbb{Z})$ が計算できる. しかし $G$ が大きいとき (例えば $G$ の位数が $5^5$,$7^5$ のとき) は, これではまだ計算量が多すぎる. そこで, 条件 (v) を付け加えて $(H,I)$ をさらに絞る.

(v) $H^4_p(H,\mathbb{Z}) \neq H^4(H,\mathbb{Z})$ のときだけを考えればよい．条件 (iii) より,$g$ は $H$ の中心に属する．ここで, (a)$H$ を $G$ の部分群とみなしたときの $(H,\langle g\rangle)$ に対応する通常の $\partial_{H,g}$, (b)$H$ を $H$ の部分群とみなしたときの $(H,\langle g\rangle)$ に対応する $\partial'_{H,g}$, の二つを考える．このとき,$\partial'_{H,g}\circ \mathrm{Res}^G_H = \partial_{H,g}$ が成り立つ．$H^4_p(H,\mathbb{Z}) = H^4(H,\mathbb{Z})$ と仮定すると, $\partial'_{H,g} = 0$ なので, $\partial_{H,g} = 0$,$\mathrm{Ker}(\widetilde{\partial}_{H,g}) = H^4(G,\mathbb{Z})$ となる．

$l \in H^4(G,\mathbb{Z})$ に対して, `IsUnramifiedH3(`$RG$`,`$l$`:Subgroup)` は条件 (i)-(v) まで使って $(H,I)$ を絞ったうえで $l \in H^4_{\mathrm{nr}}(G,\mathbb{Z})$ かどうか判定する．多くの場合, 条件 (i)-(iv) のみを使う場合と比べて計算量が大幅に削減できる．これで $G$ の位数が $5^5$,$7^5$ の場合もすべての isoclinism family に対して $H^3_{\mathrm{nr}}(\mathbb{C}(G),\mathbb{Q}/\mathbb{Z})$ の計算が可能になった．

$H$ がどのようなときに $H^4_p(H,\mathbb{Z}) = H^4(H,\mathbb{Z})$ が成り立つかについては,`H4pFromResolution(`$RG$`)` を用いて計算することができる．$H$ の位数が $3^5$,$5^5$,$7^4$ の約数のときは次のとおりである．

$H = G(p,i)\,(p = 3,5,7,\ i = 1)$

$H = G(p^2,i)\,(p = 3,5,7,\ i = 1,2)$

$H = G(p^3,i)\,(p = 3,5,7,\ i = 1,2,3,4)$

$H = G(3^4,i)\,(i = 1,2,3,4,5,6,8,9,10,13,14)$

$H = G(p^4,i)\,(p = 5,7,\ i = 1,2,3,4,5,6,9,10,13,14)$

$H = G(3^5,i)\,(i = 1,3,4,5,6,7,8,9,10,11,12,19,20,21,22,23,24,25,26,27,33,35,43,44,45,46,47,49,50,66)$

$H = G(5^5,i)\,(i = 1,15,16,17,24,25,26,27,28,29,42,44,51,52,53,54,55,56,57,59,60,76)$

## 2.3 計算例

1.4 の計算の続きで,$H^4_{\mathrm{nr}}(G,\mathbb{Z})$ を決定する．$H^4(G,\mathbb{Z}) = \langle f_1,f_2,f_3,f_4,f_5,f_6\rangle \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 6}$, $H^4_p(G,\mathbb{Z}) = \langle f_1,f_2,f_3,f_4,f_6\rangle \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 5}$ なので, $f_5 \in H^4_{\mathrm{nr}}(G,\mathbb{Z})$ かどうか `IsUnramifiedH3(`$RG$`,`$l$`)` を使って調べればよい．

```
gap> IsUnramifiedH3(RG57,[0,0,0,0,1,0]);
1/17
[ [ 3, 3 ], [ 0, 0 ] ]
2/17
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
3/17
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
4/17
[ [ 3, 3, 3, 3 ], [ 0, 0, 0, 0 ] ]
5/17
[ [ 3, 3 ], [ 0, 0 ] ]
6/17
[ [ 3, 3 ], [ 0, 0 ] ]
7/17
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
```

```
8/17
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
9/17
[ [ 3 ], [ 0 ] ]
10/17
[ [ 3 ], [ 0 ] ]
11/17
[ [ 3 ], [ 0 ] ]
12/17
[ [ 3 ], [ 0 ] ]
13/17
[ [ 3 ], [ 0 ] ]
14/17
[ [ 3 ], [ 0 ] ]
15/17
[ [ 3 ], [ 0 ] ]
16/17
[ [ 3 ], [ 0 ] ]
17/17
[ [ 3 ], [ 0 ] ]
true
```

この例では条件 (i)-(iv) を満たす $(H, I)$ の組は全部で 17 個ある．それぞれについて $\widetilde{\partial}_{H,g}$ による $f_5$ の像が 0 になるかどうかを調べている．全部 0 になれば $H^4_{\mathrm{nr}}(G, \mathbb{Z})$ に属するので `true` を返し，一つでも 0 にならないものがあれば $H^4_{\mathrm{nr}}(G, \mathbb{Z})$ に属さないので `false` を返す．1 行目の表示 1/17 は進捗状況を表している．2 行目の表示は，$H^4(H, \mathbb{Z})$ のアーベル不変量 $[3, 3, 3]$ と $\widetilde{\partial}_{H,g}(f_5)$ の値 $[0, 0, 0]$ を表している．今の例では 17 個の $(H, I)$ についてすべて $\widetilde{\partial}_{H,g}$ の像が 0 になって `true` を返しているので，$f_5 \in H^4_{\mathrm{nr}}(G, \mathbb{Z})$ である．この結果が出るまでに一般的なパソコンで数分かかる．

次に，条件 (i)-(v) を満たす $(H, I)$ の組に絞った場合の計算を見ることにする．

```
gap> IsUnramifiedH3(RG57,[0,0,0,0,1,0]:Subgroup);
1/5
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
2/5
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
3/5
[ [ 3, 3, 3, 3 ], [ 0, 0, 0, 0 ] ]
4/5
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
5/5
[ [ 3, 3, 3 ], [ 0, 0, 0 ] ]
```

```
true
```

この場合,$(H, I)$ の組は 5 個ですみ, 計算時間も数秒で済む.
結局 $H^4_{\mathrm{nr}}(G, \mathbb{Z})$ が $H^4(G, \mathbb{Z})$ 全体となることが分かり, $H^3_{\mathrm{nr}}(\mathbb{C}(G), \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$ が結論される.

## 3 UnramDeg3 のインストール方法

まず,GAP 4.8.7 以降と HAP 1.11.15 以降があらかじめインストールされている必要がある. HAP のバージョンが古いとうまく動かない.

```
https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/UnramDeg3/H3nr.gap
```

をダウンロードする. 自分が GAP のプログラムをよく保存するフォルダ (例えば ~/data/gap など) に H3nr.gap をコピーする.
そのフォルダに移動して GAP を起動して,

```
GAP> Read("H3nr.gap")}
```

で H3nr.gap を読み込めば UnramDeg3 が使えるようになる.

## 参考文献


[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.7; 2017. (http://www.gap-system.org).

[EHS] G. Ellis, J. Harris, E. Sköldberg, *Polytopal resolution for finite groups*, J. reine angew. Math **598** (2006) 131–137.

[HAP] G. Ellis, The HAP package for group cohomology and related functors, Version 1.11.15; 2017. available from `http://hamilton.nuigalway.ie/Hap/`

[HKY] A. Hoshi, M.Kang, A. Yamasaki, *Degrree three unramified cohomology groups and Noether's problem for groups of order 243*, to appear in J.Algebra, arXiv: 1710.01958v2.

[Pey99] E. Peyre, *Application of motivic complexes to neglidgible classes*, Algebraic K-theory (Seattle, WA, 1997), 181–211, Proc. Sympos. Pure Math 67, Amer. Math. Soc., Providence, RI, 1999.

[Pey08] E. Peyre, *Unramified cohomology of degree 3 and Noether's problem*, Invent. Math. **171** (2008) 191–225.

[Sal95] D. J. Saltman, *The brauer group of invariant fields, geometrically neglidgible classes, an equivariant Chow group, and unramified $H^3$*, K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), 189–246, Proc. Sympos. Pure Math., 58, Part 1, Amer. Math. Soc., Provivdence, RI, 1995.

# 野性 McKay 対応概説

## – 数論的視点と最新成果 –

安田健彦（東北大学）

これは，2019 年度第 27 回整数論サマースクール「構成的ガロア逆問題と不変体の有理性問題」の報告集に載せる原稿で，講義レジュメを改訂したものである．

モチーフ積分を用いた野性 McKay 対応の研究については，既に論説 [12] や解説記事を他の機会に書いた（例えば，第 24 回代数若手研究会の報告集）．今回は整数論サマースクールでの講義なので，数論的視点からこのテーマへの導入を試み，その後 $p$ 進測度を用いた点数版野性 McKay 対応の証明を解説する．また，最近，野性スタック上のモチーフ積分の理論を構築し，応用として一般の群に対するモチーフ的野性 McKay 対応を証明することができたので [10]，その解説を最後に行う．

## 1　導入 – Galois 逆問題との関連 –

サマースクールのテーマである Galois 逆問題に対する Noether のアプローチをスキームを用いて幾何学的に説明すると以下のようになる．体 $K$ 上の代数多様体 $V$（主にアフィン空間 $\mathbb{A}^d_K$ を考える）に有限群 $G$ が忠実に作用しているとする．$X := V/G$ を付随する商多様体とし，

$$\pi\colon V \to X$$

を商射とする．$V^\circ \subset V$ と $X^\circ \subset X$ をそれぞれ $\pi$ のエタール軌跡とする．これらは稠密開部分多様体であり，射 $\pi|_{V^\circ}\colon V^\circ \to X^\circ$ は $G$ トーサー（$G$-torsor，主 $G$ 束とも）の構造を持つ．この開部分多様体 $X^\circ$ の $K$ 有理点

$$x\colon \operatorname{Spec} K \to X^\circ$$

に対し，その $\pi$ によるスキーム論的逆像

$$\pi^{-1}(x) := \operatorname{Spec} K \times_{x,X,\pi} V = \operatorname{Spec} L$$

は $\operatorname{Spec} K$ 上の $G$ トーサーとなり，射影 $\pi^{-1}(x) \to V$ は $G$ 同変射である．図式にすると以下のようになる．

$$\begin{array}{ccc} \pi^{-1}(x) = \operatorname{Spec} L & \xrightarrow{G\text{ 同変}} & V^\circ \\ {\scriptstyle G\text{ トーサー}}\downarrow & & \downarrow{\scriptstyle G\text{ トーサー}} \\ \operatorname{Spec} K & \xrightarrow[x]{} & X^\circ \end{array}$$

もし，Spec $L$ が連結であれば $L/K$ は Galois 群 $G$ を持つ Galois 拡大になり，Galois 逆問題が肯定的に解けることになる．もし $K$ が数体で $X$ が有理的（つまり $\mathbb{A}^d_K$ と双有理同値）であれば，十分多くの有理点が存在し，その中に $\pi^{-1}(x)$ が連結となるものが存在することも示される．このように，Galois 逆問題を商多様体 $X$ の有理性の問題に帰着するのが Noether のアプローチだった．

上では $X$ の有理点から Spec $K$ 上の $G$ トーサーが構成されたが，逆に $G$ トーサー Spec $L \to$ Spec $K$ と $K$ 上の $G$ 同変射 Spec $L \to V$ が与えられると $G$ 作用による商を取ることで $K$ 有理点

$$\operatorname{Spec} K = (\operatorname{Spec} L)/G \to V/G = X$$

が誘導される．このように商多様体 $X$ の $K$ 有理点と Spec $K$ 上の $G$ トーサーは密接に関連している．Galois 逆問題は存在問題だが，Galois 逆問題への Noether のアプローチの定量版として，以下のような（漠然とした）問題を考えることができる．

**問題 1.** $X$ の $K$ 有理点の「量」と Spec $K$ 上の $G$ トーサーのもしくは $K$ の $G$-Galois 拡大の）「量」を関連付けよ．

野性 McKay 対応では，この問題の局所体版に対する一つの答えを提供する．元来の McKay 対応[1]はこのような問題ではなかったが，McKay 対応に対するモチーフ積分を使ったアプローチを野性的な状況に一般化することを試みる中で，自然とこのような見方をするのが自然であることが分かってきた．また，局所体版の結果から，数体の場合に何が言えるかを（ヒューリスティックな議論で）考察することで有理点の分布に関する Manin 予想と数体の Galois 拡大の分布に関する Malle 予想が密接に関連することが明らかになった [9].

有理点やトーサーが無限にある場合は素朴に数えることが出来ないので，分岐や高さのようなもので重み付けをする必要があるが，そのために $\mathcal{O}$ 上のモデルや整数点を考える必要がある．

## 2 Serre-Bhargava の量公式と点の Hilbert スキーム

ここからは $K$ は非アルキメデス的局所体を表すことにする．$\mathcal{O}$ をその整数環，$\mathfrak{p}$ を $\mathcal{O}$ の極大イデアル，$k = \mathcal{O}/\mathfrak{p} = \mathbb{F}_q$ を剰余体とする．$K$ 上のトーサーの数え上げとして重要なものに，**Serre-Bhargava の量公式**（mass formula）がある．

$S_n$ を対称群とし，標準的な置換表現により $GL_n(\mathbb{C})$ に埋め込まれているとする．$S_n$ トーサー Spec $L \to$ Spec $K$ は，$K$ の絶対 Galois 群 $G_K$ から $S_n$ への連続準同形の $S_n$ 共役類に 1 対 1 に対応する．

$$\{\text{連続準同形 } G_K \to S_n\}/S_n \overset{1:1}{\longleftrightarrow} \{K \text{ 上の } S_n \text{ トーサー}\}/\cong$$

[1]McKay 対応は $SL_2(\mathbb{C})$ の有限部分群 $G$ に対し，同じ Dynkin 図形が二通りの全く異なる方法で構成されるという McKay の観察に由来する．二つの方法とは，一つは表現論を用いるもので，もう一つは商多様体 $\mathbb{C}^2/G$ の最小特異点解消の例外集合から構成するものである．

$S_n$ トーサー $\operatorname{Spec} L \to \operatorname{Spec} K$ に対して $a(L)$ を，付随する写像

$$G_K \to S_n \hookrightarrow GL_n(\mathbb{C})$$

の **Artin 導手**（Artin conductor）とする．

**定理 2** (Serre-Bhargava の量公式 [2]，cf. [6])．以下の等式が成り立つ：

$$\sum_L \frac{q^{-a(L)}}{\sharp \operatorname{Aut}(L)} = \sum_{i=0}^{n-1} P(n, n-i) q^{-i}$$

ここで，$L$ は $K$ 上の $S_n$ トーサーの同型類全体を走り，$\operatorname{Aut}(L)$ は $K$ 上の $S_n$ トーサーとしての同型群，$P(n,j)$ は整数 $n$ をちょうど $j$ 個の正整数に分ける分割の個数とする．

$S_n$ トーサー $\operatorname{Spec} L \to \operatorname{Spec} K$ に対し，$S_{n-1}$ 不変部分環 $L' = L^{S_{n-1}}$ を取ると，$K$ 上の $n$ 次エタール代数になる．$L$ と $L'$ は 1 対 1 に対応し Artin 導手 $a(L)$ は $L'/K$ の**判別式指数**（discriminant exponent）$d(L')$ に等しく，上の公式は

$$\sum_{L'} \frac{q^{-d(L')}}{\sharp \operatorname{Aut}(L')} = \sum_{i=0}^{n-1} P(n, n-i) q^{-i}$$

と書ける．$L'$ は $n$ 次エタール $L$ 代数の同型類全体を走る．元々Bhargava が証明したのはこの形の公式で，定理の式は Kedlaya による再定式化である．それ以前に Serre [8] は $L'/K$ が完全分岐体拡大に制限したときの公式

$$\sum_{L' : \text{完全分岐体拡大}} \frac{q^{-d(L')}}{\sharp \operatorname{Aut}(L')} = q^{1-n}$$

を得ていた．Bhargava の証明は組み合わせ論的議論で Serre の公式に帰着するものだった．

McKay 対応を用いると，Bhargava の公式を Serre の公式を介さずに証明することが出来るので，それを説明する．$\mathcal{O}$ 上の $2n$ 次元アフィン空間

$$\mathbb{A}^{2n}_{\mathcal{O}} = \operatorname{Spec} \mathcal{O}[x_1, \ldots, x_{2n}] = (\mathbb{A}^2_{\mathcal{O}})^n$$

に自然な $S_n$ の置換作用を入れる．商スキーム

$$X := \mathbb{A}^{2n}_{\mathcal{O}}/S_n = \operatorname{Spec} \mathcal{O}[x_1, \ldots, x_{2n}]^{S_n} = S^n \mathbb{A}^2_{\mathcal{O}}$$

はアフィン平面の $n$ **次対称積**（$n$-th symmetric product）と呼ばれるものになる．これは商特異点をもつが，特別な特異点解消を持つ．$n$ **点の Hilbert スキーム** $\operatorname{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O})$ は代数幾何でよく調べられている対象で，$\operatorname{Spec} \mathcal{O}$ 上の体のスペクトラム $\operatorname{Spec} K$ に対し，

$$\operatorname{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O})(K) = \{0 \text{ 次元閉部分スキーム } Z \subset \mathbb{A}^2_K \mid \dim_K \Gamma(\mathcal{O}_Z) = n\}$$

となるモジュライ空間である．$X$ に *Hilbert-Chow* 射という自然な射

$$\mathrm{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O}) \to X$$

が存在する．$\mathrm{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O})$ は $\mathcal{O}$ 上滑らかであり，上の射はクレパント特異点解消（次章，定義 4）と呼ばれるものになっている．McKay 対応により，上の定理の左辺は $X$ の弦点数（string point-count）

$$\sharp_{\mathrm{st}}(X)$$

（次章，定義 3）に $q^{-2n}$ を書けたものに等しいことが分かる．そして，弦点数の基本的な性質により $\sharp_{\mathrm{st}}(X)$ はクレパント特異点解消 $\mathrm{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O})$ の $k = \mathbb{F}_q$ 上の有理点の個数に等しいことが分かる．

$$\sharp_{\mathrm{st}}(X) = \sharp\mathrm{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O})(k)$$

最後に $\mathrm{Hilb}^n(\mathbb{A}^2_k/k) = \mathrm{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O}) \otimes_{\mathcal{O}} k$ は様々な次元のアフィン空間の非交和に分解することをもちいて，$k$ 有理点の個数は

$$\sum_{i=0}^{n-1} P(n, n-i) q^{2n-i}$$

であることが分かる．これらを合わせて，定理を得る．まとめると，証明は以下のように等式を繋げることで得られた．

$$\begin{aligned}
&\sum_L \frac{q^{2n-a(L)}}{\sharp\,\mathrm{Aut}(L)} \\
&= \sharp_{\mathrm{st}}(X) && \text{(McKay 対応)} \\
&= \sharp\mathrm{Hilb}^n(\mathbb{A}^2_{\mathcal{O}}/\mathcal{O})(k) && \text{(弦点数の性質)} \\
&= \sum_{i=0}^{n-1} P(n, n-i) q^{2n-i} && \text{(Hilbert スキームの分解)}
\end{aligned}$$

また，この証明により定理に現れる数を点の個数として幾何学的に解釈することができた．

## 3　p 進測度と弦点数

引き続き $K$ は非アルキメデス的局所体とし，前章の記法を用いる．整数環 $\mathcal{O}$ 上滑らかで相対次元 $d$ を持つスキーム $X$ を考えよう．整数点集合 $X(\mathcal{O})$ は $K$ 解析多様体[2]の構造を持つ．$d$ 次形式の層 $\Omega^d_{X/\mathcal{O}} = \bigwedge^d \Omega_{X/\mathcal{O}}$ の各 $k$ 点の近傍 $U$ での局所生成元は $U(\mathcal{O})$ の測度を定める．これらは貼り合い $X(\mathcal{O})$ の測度 $\mu_X$ を定め，

$$\mu_X(X(\mathcal{O})) = q^{-d} \cdot \sharp X(k)$$

[2] リジッド空間などではなく，通常の多様体と同じように「素朴」な方法で定義される $K$ 上の空間．参考文献として [5] を挙げておく．

となる（Weil の公式）.

同様の構成は，自然数 $r$ に対し，有理 $r$ 重 $d$ 形式の層

$$(\Omega^d_{X/\mathcal{O}})^{\otimes r} \otimes K(X)$$

の可逆 $\mathcal{O}_X$ 部分加群に対して行うことが出来る．$X$ が $\mathcal{O}$ 上滑らかな $V$ の有限群 $G$ による商 $X = V/G$ であるとき，このような可逆 $\mathcal{O}_X$ 部分加群が存在し（$r = \sharp G$ とする），$X(\mathcal{O})$ の測度 $\mu_X$ を定める．この可逆部分加群は標準因子 $K_{X/\mathcal{O}}$ に対応する．

**定義 3.** $X$ の**弦点数**（stringy point-count）$\sharp_{\mathrm{st}} X$ を

$$\sharp_{\mathrm{st}} X := q^d \cdot \mu_X(X(\mathcal{O})) \in \mathbb{R} \cup \{\infty\}$$

により定義する.

発散して無限大になることもあることに注意する．発散は，双有理幾何的な意味で特異点が「悪い[3]」ことを意味する．これを用いて，特異点の「悪さ」を調べることが出来る.

各 $\mathcal{O}$ 点は $k$ 点を誘導するので，$k$ 点 $x$ を誘導する $\mathcal{O}$ 点の集合を $X(\mathcal{O})_x$ と書くと

$$X(\mathcal{O}) = \bigsqcup_{x \in X(k)} X(\mathcal{O})_x$$

となり，

$$\sharp_{\mathrm{st}} X = \sum_{x \in X(k)} q^d \cdot \mu_X(X(\mathcal{O}))_x$$

が成り立つ．つまり，弦点数 $\sharp_{\mathrm{st}} X$ は $k$ 点を特異点から決まる重み $q^d \cdot \mu_X(X(\mathcal{O}))_x$ をつけて数え上げたものとなる．$X$ が点 $x$ で $\mathcal{O}$ 上滑らかなら，重みは 1 であり，特に $X$ 全体が $\mathcal{O}$ 上滑らかなら

$$\sharp_{\mathrm{st}} X = \sharp X(k)$$

となる.

**定義 4.** 正規 $\mathcal{O}$ スキーム $Y$ からの固有双有理射 $f\colon Y \to X$ が**クレパント**（crepant）であるとは，$f$ の相対標準因子が消える，つまり

$$K_{Y/X} := K_{Y/\mathcal{O}} - f^* K_{X/\mathcal{O}} = 0$$

となることを意味する．また $f$ が**クレパント特異点解消**（crepant resolution）であるとは，さらに $Y$ が $\mathcal{O}$ 上滑らかであることを意味する.

弦点数の一番大事な性質が，クレパント射による不変性である．$Y$，$X$ の両方に対して弦点数が定義され（例えば，商特異点のみを持つ場合），$f\colon Y \to X$ がクレパント射のとき，

$$\sharp_{\mathrm{st}} X = \sharp_{\mathrm{st}} Y$$

となる．特に，$f$ がクレパント特異点解消であれば，

$$\sharp_{\mathrm{st}} X = \sharp Y(k)$$

となる.

[3] ここで言う「悪い」とは，正確には「対数末端（log terminal）でない」という意味．対数末端特異点は極小モデル理論で基本的な特異点のクラス.

# 4　捻弧，点数版 McKay 対応，解捻

$X$ の $\mathcal{O}$ 点は代数幾何で考える弧の類似である．$k$ 代数多様体の**弧**（arc）とは射 $\operatorname{Spec} k[[t]] \to X$ のことである．そこで，我々は $\mathcal{O}$ スキーム $X$ の $\mathcal{O}$ 点（つまり，切断 $\operatorname{Spec}\mathcal{O} \to X$）のことも弧と呼ぶことにする．

導入で述べた対応により，ほとんどの（$X(\mathcal{O})$ の測度零部分を除き）弧に対し一意的に $G$ トーサー $\operatorname{Spec} L \to \operatorname{Spec} K$ が定まり，$G$ 同変射 $\operatorname{Spec}\mathcal{O}_L \to X$（$\mathcal{O}_L$ は $L$ の整数環，つまり，$\mathcal{O}$ の $L$ での整閉包）が誘導される．このような同変射を**捻弧**（twisted arc）と呼ぶ．各 $G$ トーサー $\operatorname{Spec} L \to \operatorname{Spec} K$ に対し，これを誘導する $\mathcal{O}$ 点の集合を $X(\mathcal{O})_L$ とし，測度零部分を無視すると

$$X(\mathcal{O}) = \bigsqcup_L X(\mathcal{O})_L$$

という分解を得る．

有限群 $G$ の $\mathcal{O}$ 線形作用 $G \curvearrowright \mathbb{A}^d_{\mathcal{O}}$ を考える．簡単のために商射 $\mathbb{A}^d_{\mathcal{O}} \to X$ は余次元 1 でエタール[4]であるとする．下で定義されるように，与えられた線形作用に付随する関数

$$v\colon \{G \text{ トーサー } \operatorname{Spec} L \to \operatorname{Spec} K\} \to \frac{1}{\sharp G}\mathbb{Z}$$

があり，弦点数 $\sharp_{\mathrm{st}} X = q^d \cdot \mu_X(X(\mathcal{O}))$ への $L$ の寄与 $q^d \cdot \mu_X(X(\mathcal{O})_L)$ は実は

$$\frac{q^{d-v(L)}}{\sharp \operatorname{Aut}(L)}$$

となる．これより野性 McKay 対応の点数版が従う．

**定理 5** (点数版野性 McKay 対応 [11])**.** 以下の等式が成り立つ．

$$\sharp_{\mathrm{st}} X = \sum_L \frac{q^{d-v(L)}}{\sharp \operatorname{Aut}(L)}$$

関数 $v$ を決定し，$L$ の寄与を計算するために必要となるのが**解捻**（untwisting）の手法である．$F$ を $\mathbb{A}^d_{\mathcal{O}}$ の座標環 $\mathcal{O}[x_1, \dots, x_d]$ の線形部分 $\bigoplus_i \mathcal{O} \cdot x_i$ とする．これは $G$ 作用を持つ階数 $d$ の自由 $\mathcal{O}$ 加群である．

**定義 6.** $G$ トーサー $\operatorname{Spec} L \to \operatorname{Spec} K$ に付随する**チューニング加群** $\Xi_L$（tuning module）を $G$ 同変 $\mathcal{O}$ 準同形のなす加群

$$\Xi_L := \operatorname{Hom}^G_{\mathcal{O}}(F, \mathcal{O}_L)$$

として定義する．

[4]つまり，ある余次元 2 以上の閉集合を取り除くとエタールになる．この条件は，射 $\mathbb{A}^d_{\mathcal{O}} \to X$ がクレパントであるという条件に言い換えても良い．この仮定を外すためには対数版弦点数を考える必要がある．対数版とは，双有理幾何，特に極小モデル理論でよくやるようにスキーム $X$ に $\mathbb{Q}$ 係数因子を付け加えることを意味する．

これは，$\mathrm{Hom}_{\mathcal{O}}(F,\mathcal{O}_L)\cong\mathcal{O}_L^{\oplus d}$ の階数 $d$ の自由 $\mathcal{O}$ 部分加群である．

**定義 7.** 関数 $v$ は

$$v(L):=\frac{f_L}{\sharp G}\,\mathrm{length}_{\mathcal{O}_L}\frac{\mathrm{Hom}_{\mathcal{O}}(F,\mathcal{O}_L)}{\mathcal{O}_L\cdot\Xi_L}$$

と定義される．ただし，$f_L$ は $\mathrm{Spec}\,L$ の連結成分の $K$ 上の剰余次数を表す.[5]

チューニング加群の双対加群 $\mathrm{Hom}_{\mathcal{O}}(\Xi_L,\mathcal{O})$ を考え，その $\mathcal{O}$ 上の対称代数

$$S^\bullet_{\mathcal{O}}\,\mathrm{Hom}_{\mathcal{O}}(\Xi_L,\mathcal{O})$$

を考える．これは再び $\mathcal{O}[x_1,\dots,x_d]$ と同型になる．元の $G$ 作用付きアフィン空間を $V$ と記し，$L$ に関する $V$ の**解捻空間**（untwisting space）を

$$V^{|L|}:=\mathrm{Spec}\,S^\bullet_{\mathcal{O}}\,\mathrm{Hom}_{\mathcal{O}}(\Xi_L,\mathcal{O})\cong\mathbb{A}^d_{\mathcal{O}}$$

と定義する．構成から次の 1 対 1 対応がある．

$$\{V^{|L|}\text{の }\mathcal{O}\text{ 点 }\}\overset{1:1}{\longleftrightarrow}\{G\text{ 同変射 }\mathrm{Spec}\,\mathcal{O}_L\to V\}$$

また自然な射 $V^{|L|}\to X$ が存在し，上の対応は $X(\mathcal{O})$ への写像と整合的となる．また，$X(\mathcal{O})$ への写像は $\mathrm{Aut}(L)$ 不変であり，測度零集合の外では $X(\mathcal{O})_L$ の上への $\sharp\,\mathrm{Aut}(L)$ 対 1 の対応となっている．これにより，

$$\mu_X(X(\mathcal{O})_L)=\frac{1}{\sharp\,\mathrm{Aut}(L)}\nu(V^{|L|}(\mathcal{O}))$$

が導かれる．ただし，$\nu$ は射 $V^{|L|}\to X$ の相対標準因子 $K_{V^{|L|}/X}$ から定まる $V^{|L|}(\mathcal{O})$ 上の測度である．そして，計算により $K_{V^{|L|}/X}$ は特殊ファイバー $V^{|L|}\otimes k$ に係数 $-v(L)$ を掛けたもの，

$$-v(L)\cdot(V^{|L|}\otimes k)$$

となることが分かる．これより，測度 $\nu$ は標準的な測度を $q^{-v(L)}$ がしたものであることが分かり，欲しかった等式

$$\mu_X(X(\mathcal{O})_L)=q^{d-v(L)}$$

を得る．

まとめると，定理 5の証明は以下のようになる．

$$\begin{aligned}\sharp_{\mathrm{st}}(X)&=\mu_X(X(\mathcal{O}))\\&=\sum_L\mu_X(X(\mathcal{O})_L)\\&=\sum_L\frac{\nu(V^{|L|}(\mathcal{O}))}{\sharp\,\mathrm{Aut}(L)}\\&=\sum_L\frac{q^{d-v(L)}}{\sharp\,\mathrm{Aut}(L)}.\end{aligned}$$

[5]論文 [11] の定義では $f_L$ が抜けていて間違っている．同論文の Errata で修正された．$f_L$ を付ける代わりに，$\mathrm{length}_{\mathcal{O}_L}$ を $\mathrm{length}_{\mathcal{O}}$ で取り替えても良い．

# 5　モチーフ的McKay対応

**定義 8.** 体 $k$ 上の**代数多様体の Grothendieck 環** $K_0(\mathbf{Var}_k)$ は，$k$ 代数多様体の同型類 $\{X\}$ で生成される自由アーベル群を以下の**鋏関係**（scissor relation）で割った商群として定義される：（鋏関係）$Y \subset X$ が閉部分多様体のとき，

$$\{X\} - \{Y\} - \{X \setminus Y\} = 0.$$

積は $\{X\}\{Y\} := \{X \times_k Y\}$ により与えられる．

$k$ が有限体のとき，**点数実現写像**

$$K_0(\mathbf{Var}_k) \to \mathbb{Z},\ \{X\} \mapsto \sharp X(k)$$

が存在する．したがって，$\{X\}$ は点の個数 $\sharp X(k)$ を精密化した不変量とみなすことができる．（基礎体 $k$ が複素数体の場合は位相的 Euler 標数の精密化とみることも出来る．）また $\{X\}$ は基礎体 $k$ が有限体でなくても意味を持つ．Grothendieck 環の元 $X$ は，$X$ のモチーフのトイ・モデルだと見なすことができる．

モチーフ積分の McKay 対応への応用を考えるために，環 $K_0(\mathbf{Var}_k)$ をさらに修正する必要がある．まず，

$$\mathbb{L} := \{\mathbb{A}^1_k\}$$

とする．自然数 $n$ と射 $f\colon Y \to X$ が，各幾何学的点 $x\colon \operatorname{Spec} K \to X$ に対し，ファイバー $f^{-1}(x)$ が $n$ 次元アフィン空間の有限群商 $\mathbb{A}^n_K/G$ に普遍同相（universally homeomorphic）であるとき，

$$\{Y\} = \{X\}\mathbb{L}^n$$

という関係式を追加することにより商環 $K_0(\mathbf{Var}_k)'$ を取る．また自然数 $r$ を固定し，$\mathbb{L}$ の $r$ 乗根 $\mathbb{L}^{1/r}$ を形式的に追加して得られる環を $K_0(\mathbf{Var}_k)'_r$．これを $\mathbb{L}$ で局所化したものを $\mathcal{M}'_r$ とおく．これは，$\{X\}\mathbb{L}^n,\ n \in \frac{1}{r}\mathbb{Z}$ という形の元で加法群として生成される． $F_m$ を $\dim X + n \le -m$ を満たす元 $\{X\}\mathbb{L}^n$ で生成される部分群とすると，$\mathcal{M}'_r$ の降下フィルトレーション $F_m,\ m \in \frac{1}{r}\mathbb{Z}$ が得られる．完備化

$$\widehat{\mathcal{M}'_r} := \varprojlim \mathcal{M}'_r/F_m$$

が定義される．完備化された環の中では，

$$\sum_{i\in\mathbb{N}} \{X_i\}\mathbb{L}^{n_i} \quad (\dim X_i + n_i \to -\infty)$$

という形の無限和が定義できる．$k$ が有限体のとき，この環においても等式 $\{X\} = \{Y\}$ は $\sharp X(k) = \sharp Y(k)$ を導く．ただし，上の点数実現写像を完備化まで拡張することはできないので，注意が必要．

これでモチーフ積分が値を取る環 $\widehat{\mathcal{M}'_r}$ が準備できたので，次に $\mathcal{O}$ スキーム上のモチーフ積分の理論を概説する．モチーフ積分は Kontsevich が $p$ 進積分の類似として Kontsevich が導入し，標数零の体上の理論は Denef-Loeser [3] により基礎づけられ

た．その後，Sebag [7] が完備離散付値環上の（形式）スキームに一般化した．しかし，後で説明するスタック上の理論が等標数でしか出来ていないので，**ここから等標数に限定する**ことにする．任意の体 $k$ に対し，$\mathcal{O} = k[[t]]$ とおく．$\mathcal{O}$ 上の平坦有限型スキーム $X$ で稠密開集合上では $\mathcal{O}$ 上滑らかになっているものを考える．$X$ の $\mathcal{O}$ 点をパラメタ付ける $k$ 上のスキーム（弧空間，Greenberg 関手）$J_\infty X$ が存在し，その上に $\widehat{\mathcal{M}'_r}$ に値をとる測度を定義できる．そして，可測関数

$$h\colon J_\infty X \to \frac{1}{r}\mathbb{Z} \cup \{\infty\}$$

（$h^{-1}(\infty)$ は測度零集合とする）に対し，積分

$$\int_{J_\infty X} \mathbb{L}^h \, d\mu_X \in \widehat{\mathcal{M}'_r} \cup \{\infty\}$$

が定義される．

前章で扱ったようなマイルドな特異点をもつ $X$ に対し，弦点数 $\sharp_{\mathrm{st}} X$ のモチーフ版である**弦モチーフ**（stringy motif）$M_{\mathrm{st}}(X)$ は，$\Omega^d_{X/\mathcal{O}}$ と $\omega_{X/\mathcal{O}}$ の差を測る関数 $h_X$ を用いて，

$$M_{\mathrm{st}}(X) := \int_{J_\infty X} \mathbb{L}^{h_X} \, d\mu_X \in \widehat{\mathcal{M}'_r} \cup \{\infty\}$$

と定義される．弦モチーフは弦点数と同様の性質を持つ．つまり，$X$ が $\mathcal{O}$ 上滑らかなら

$$M_{\mathrm{st}}(X) = \{X \otimes_{\mathcal{O}} k\}$$

となり，$Y \to X$ がクレパント特異点解消なら

$$M_{\mathrm{st}}(X) = \{Y \otimes_{\mathcal{O}} k\}$$

となる．

**注意 9.** 上の $X$ や $Y$ は $\mathcal{O}$ 上のスキームであるのに対し，測度，積分の値や弦モチーフは，剰余体 $k$ 上の Grothendieck 環 $K_0(\mathbf{Var}_k)$ から作られる環 $\widehat{\mathcal{M}'_r}$ に値を取ることに注意する．

野性 McKay 対応のモチーフ版は以下のように定式化できる．

**定理 10** (モチーフ的野性 McKay 対応 [10]). $k$ を任意の体とし，$\mathcal{O} = k[[t]]$ とする．有限群 $G$ の $\mathcal{O}$ 線形作用 $G \curvearrowright \mathbb{A}^d_{\mathcal{O}}$ を考え，$X = \mathbb{A}^d_{\mathcal{O}}/G$ とする．商射 $\mathbb{A}^d_{\mathcal{O}} \to X$ が余次元 1 でエタールであるとき，以下の等式が成り立つ．

$$M_{\mathrm{st}}(X) = \int_{\Delta_G} \mathbb{L}^{d-v}$$

ここで，$\Delta_G$ は $\operatorname{Spec} k((t))$ 上の $G$ トーサーをパラメタ付ける $k$ 上のモジュライ空間で，$v$ は前に定義されたもので $\Delta_G$ 上の関数を与える．右辺の積分は

$$\sum_{i \in \frac{1}{\sharp G}\mathbb{Z}} \{v^{-1}(i)\}\mathbb{L}^{d-i}$$

により定義される．

$\mathrm{Conj}(G)$ を $G$ の共役類の集合とする．$k=\mathbb{C}$ のとき（もしくは，より一般に $k$ が代数的閉体で標数が $\sharp G$ と素のとき），$\Delta_G$ は $\sharp\,\mathrm{Conj}(G)$ 個の点からなる 0 次元の空間であり，定理の右辺は

$$\sum_{[g]\in\mathrm{Conj}(G)} \mathbb{L}^{d-v(g)}$$

という $G$ の共役類を渡る和になる．この場合の定理は本質的に Batyrev [1]，Denef-Loeser [4] により証明された．クレパント特異点解消 $Y\to X$ が存在するとき，定理から

$$\{Y_{\mathbb{C}}\}=\sum_{[g]\in\mathrm{Conj}(G)} \mathbb{L}^{d-v(g)}$$

となる．これから位相的 Euler 標数実現をとることで，多様体 $Y(\mathbb{C})$ の位相的 Euler 標数と $G$ の共役類の個数が等しいという結果を得る．

$$\chi_{\mathrm{top}}(Y(\mathbb{C}))=\sharp\,\mathrm{Conj}(G)$$

最後の等式は，「物理学者の予想（phisicists' conjecture）」と呼ばれていたもので，Witten 達の弦理論の研究に由来する．

## 6　スタックによる再定式化

モチーフ的野性 McKay 対応の証明やさらなる一般化をするためにスタックを用いると見通しが良い．以下で考えるスタックは全て Deligne-Mumford スタックである．

再び $\mathcal{O}$ スキーム $V$ に有限群 $G$ が作用している状況を考えよう．$V$ と商スキーム $X=V/G$ の中間に，**商スタック**

$$\mathcal{X}:=[V/G]$$

が存在する．$\mathcal{X}$ は局所的には $V$ に近く，大域的には $X$ に近い．$V$ が $\mathcal{O}$ 上滑らかであれば，$\mathcal{X}$ も $\mathcal{O}$ 上滑らかである．また，$V$ が既約で $G$ 作用が忠実であれば，$\mathcal{X}\to X$ は固有双有理射となる．さらに，$V\to X$ が余次元 1 でエタールであるという条件は，$\mathcal{X}\to X$ が余次元 1 で同型射であると言い換えることが出来る．特に，$V$ が $\mathcal{O}$ 上滑らかで $V\to X$ が余次元 1 でエタールのとき，射

$$\mathcal{X}\to X$$

は **Deligne-Mumford スタックの圏におけるクレパント特異点解消**となる．前述の点数版 McKay 対応（定理 5），および，モチーフ的 McKay 対応（定理 10）は弦不変量はクレパント射により不変であるという主張の一種であるとみなすことができる．つまり，の性をスタックに $X$ の不変量と $\mathcal{X}$ の不変量（両定理の等式の右辺）が等しいという主張であると解釈することが出来る．

スタックの弦不変量は次章で説明するスタックに一般化されたモチーフ積分を用いてスキームの場合と同様に定義する．$V$ がアフィン空間で線形作用 $G$ の作用が線形であるとき，定義から比較的簡単に

$$\sharp_{\mathrm{st}}(\mathcal{X}) = \sum_{L} \frac{q^{d-v(L)}}{\sharp \operatorname{Aut}(L)}, \quad M_{\mathrm{st}}(\mathcal{X}) = \int_{\Delta_G} \mathbb{L}^{d-v}$$

が従い，定理 5と定理 10は

$$\sharp_{\mathrm{st}}(X) = \sharp_{\mathrm{st}}(\mathcal{X}), \quad M_{\mathrm{st}}(X) = M_{\mathrm{st}}(\mathcal{X})$$

という等式として定式化される．そして，最後の等式は次章で説明する**変数変換公式**から従う．

# 7　スタック上のモチーフ積分と変数変換公式

$\mathcal{O} = k[[t]]$ 上のスキーム $X$ の弧とは形式円盤 $\operatorname{Spec} k[[t]]$ からの射

$$\operatorname{Spec} k[[t]] \to X$$

のことだった．そして，モチーフ積分は弧の空間上の積分理論だった．McKay 対応に応用するには，スタック $\mathcal{X}$ に対し形式円盤からの射を考えただけでは十分ではなく，前述の捻弧に相当するものを考える必要がある．

**定義 11. 捻形式円盤**（twisted formal disk）を $\operatorname{Spec} k[[t]]$ のある有限群 $G$ に関する $G$ 被覆 $\operatorname{Spec} R \to \operatorname{Spec} k[[t]]$ に付随する商スタック $[\operatorname{Spec} R/G]$ のことであると定義する．ただし，$\operatorname{Spec} R$ は連結で正規であるとする．

つまり，$R$ はある $G$-Galois 拡大 $L/k((t))$ の整数環 $\mathcal{O}_L$ となる．

**定義 12.** $\mathcal{O}$ 上スタック $\mathcal{X}$ の**捻弧**（twisted arc）をある捻形式円盤 $\mathcal{E}$ からの表現可能射 $\mathcal{E} \to \mathcal{X}$ のことだと定義する．

Deligne-Mumford スタックの射が表現可能であるための必要十分条件は，付随する点の自己同型群の準同形が全て単射となることである．捻弧のなす空間（スタック）を $\mathcal{J}_\infty\mathcal{X}$ と記すことにする．$\mathcal{X}$ がスキームや代数空間であれば，捻弧は全て通常の弧であり，$\mathcal{J}_\infty\mathcal{X} = J_\infty\mathcal{X}$ となる．

$\mathcal{O}$ 上スタックの射 $f\colon \mathcal{Y} \to \mathcal{X}$ があると捻弧空間の間の写像

$$f_\infty\colon \mathcal{J}_\infty\mathcal{Y} \to \mathcal{J}_\infty\mathcal{X}$$

が誘導される．また $\mathcal{J}_\infty\mathcal{Y}$ 上の $f$ に関するヤコビ位数関数

$$\mathrm{j}_f\colon \mathcal{J}_\infty\mathcal{Y} \to \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

そして $\mathcal{J}_\infty\mathcal{Y}$, $\mathcal{J}_\infty\mathcal{X}$ のそれぞれの上にシフト関数

$$\mathfrak{s}_\mathcal{Y}\colon \mathcal{J}_\infty\mathcal{Y} \to \mathbb{Q},$$
$$\mathfrak{s}_\mathcal{X}\colon \mathcal{J}_\infty\mathcal{X} \to \mathbb{Q}$$

が定義される．シフト関数は上述の関数 $v$ に相当するものを非線形作用にまで一般化したものである．適当な条件の下で，$\mathcal{J}_\infty\mathcal{X}$ 上の可測関数 $h$ に対し，以下の等式が成り立つというのが**変数変換公式**（change of variables formula）である．

**定義 13** ([10])**.**

$$\int_{\mathcal{J}_\infty\mathcal{X}} \mathbb{L}^{h+\mathfrak{s}_\mathcal{X}}\, d\mu_\mathcal{X} = \int_{\mathcal{J}_\infty\mathcal{Y}} \mathbb{L}^{h\circ f_\infty - \mathrm{j}_f + \mathfrak{s}_\mathcal{Y}}\, d\mu_\mathcal{Y}$$

捻弧空間 $\mathcal{J}_\infty\mathcal{X}$ の構成，シフト関数 $\mathfrak{s}_\mathcal{X}$ の定義，変数変換公式の証明の全ては**解捻スタック**（untwisting stack）を用いてなされる．捻形式円盤 $\mathcal{E}$ に関する $\mathcal{X}$ の解捻スタックは $\mathcal{E}$ から $\mathcal{X}$ への表現可能射をパラメタ付ける Hom スタック

$$\mathrm{Utg}_\mathcal{E}(\mathcal{X}) := \underline{\mathrm{Hom}}^{\mathrm{rep}}_{\mathcal{O}}(\mathcal{E}, \mathcal{X})$$

として定義される．$\mathcal{X}$ が線型作用に付随する商スタック $[V/G]$ のとき，解捻スタックは前述の解捻空間 $V^{|L|}$ に相当する．捻形式円盤 $\mathcal{E}$ を固定すると，次の 1 対 1 対応を得る．

$$\{\text{捻弧 } \mathcal{E} \to \mathcal{X}\} \longleftrightarrow \{\text{弧 } \operatorname{Spec} k[[t]] \to \mathrm{Utg}_\mathcal{E}(\mathcal{X})\}$$

この対応を通し，捻弧の研究を通常の弧のそれに帰着する．実際には捻形式円盤はモジュライを持つので，捻形式円盤の普遍族に対して解捻スタックを構成する必要がある．また，そのために形式スキーム $\operatorname{Spf} k[[t]]$ 上の形式スタックを考える必要がでてくる．非捻弧を考える限り，弧のターゲットをスタックにしても，従来のスキームに対するモチーフ積分の理論は基本的にそのまま一般化できる．シフト関数 $\mathfrak{s}_\mathcal{X}$ は捻弧と対応する解捻スタックの非捻弧を考えたときにでてくるヤコビ位数関数の差として定義できる．従って，解捻スタックの非捻弧に対する変数変換公式を元のスタックの捻弧に対する公式に書き換えるときに，補正項であるシフト関数が現れる．

# 8　今後の研究課題

最後に，今後考えるべき問題・研究課題をいくつか挙げる．

**問題 14.** McKay 対応の等式の両辺のうち，どちらか片方でも計算できる例をもっと見つける．特に，非線形作用で何が起こっているか計算で解明できると面白い．

等式の片側が計算できれば，もう一方について非自明な結果を得る．例えば，右辺を計算することで左辺の特異多様体の不変量が分かり特異点の情報を得ることが出来る．逆に，例えば特異点解消を計算することで左辺を計算できれば，右辺の量（局所体の拡大の重み付き数え上げ，もしくは，そのモチーフ版）の公式を得る．

本稿では線形作用を中心に説明したが，非線形作用の場合でも McKay 対応は定式化される．しかし，より複雑になり計算できている例はほとんどない．

**問題 15.** 混標数における野性スタック上のモチーフ積分理論の構築とモチーフ的野性 McKay 対応の証明.

やはり，数論研究者が一番興味があるのは $\mathbb{Z}_p$ など，混標数の環上の理論だろう．この場合，$\Delta_G$ などのモジュライ空間の構成がまだ出来ていない．それ以外は，概ね等標数の場合と同じ議論が成立すると思われる.

**問題 16.** 数体，大域体上の McKay 対応の研究.

導入で述べたように，数体上の McKay 対応を考えることで Manin 予想と Malle 予想の関係が見えてくるが，まだヒューリスティックな議論のレベルに留まっている．これを，厳密な数学にしていくのは今後の課題だ.

**問題 17.** 他の野性分岐（wild ramification，暴分岐とも）との関連を調べる.

野性 McKay 対応では高次元の分岐を扱っているが，数論幾何では至る所で野性分岐が問題となる．野性分岐に関して，様々な研究がなされ理論も作られている．野性 McKay 対応や野性スタック上のモチーフ積分と他の野性分岐の理論を関連付けられたら面白い.

# 参考文献


[1] Victor V. Batyrev. Non-Archimedean integrals and stringy Euler numbers of log-terminal pairs. *J. Eur. Math. Soc. (JEMS)*, 1(1):5–33, 1999.

[2] Manjul Bhargava. Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm052, 20, 2007.

[3] Jan Denef and François Loeser. Germs of arcs on singular algebraic varieties and motivic integration. *Invent. Math.*, 135(1):201–232, 1999.

[4] Jan Denef and François Loeser. Motivic integration, quotient singularities and the McKay correspondence. *Compositio Math.*, 131(3):267–290, 2002.

[5] Jun-ichi Igusa. *An introduction to the theory of local zeta functions*, volume 14 of *AMS/IP Studies in Advanced Mathematics*. American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 2000.

[6] Kiran S. Kedlaya. Mass formulas for local Galois representations. *Int. Math. Res. Not. IMRN*, (17):Art. ID rnm021, 26, 2007. With an appendix by Daniel Gulotta.

[7] Julien Sebag. Intégration motivique sur les schémas formels. *Bull. Soc. Math. France*, 132(1):1–54, 2004.

[8] Jean-Pierre Serre. Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local. *C. R. Acad. Sci. Paris Sér. A-B*, 286(22):A1031–A1036, 1978.

[9] Takehiko Yasuda. Manin’s conjecture vs. Malle’s conjecture. arXiv:1505.04555.

[10] Takehiko Yasuda. Motivic integration over wild Deligne-Mumford stacks. arXiv:1908.02932.

[11] Takehiko Yasuda. The wild McKay correspondence and $p$-adic measures. *J. Eur. Math. Soc. (JEMS)*, 19(12):3709–3734, 2017.

[12] 安田 健彦. モチーフ積分による野性マッカイ対応. **数学**, 70(2):159–183, 2018.

# 宵の時間

# 虚二次体の射類体の相対べき整基底

関川隆太郎

東京理科大学 理工学研究科
博士後期課程一年

2019 年 9 月 6 日
整数論サマースクール 宵の時間



## 導入

代数体 $K$ に対して, その整数環を $\mathcal{O}_K$ で表す.

**定義 (べき整基底)**

代数拡大 $L/K, \alpha \in L$ に対し, $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ となるとき, $\alpha$ は $L/K$ のべき整基底を生成するとよぶ.

例. 1 の原始 $m$ 乗根 $\zeta_m = e^{\frac{2\pi i}{m}}$ は円分体 $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ のべき整基底を生成する. すなわち,

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m].$$

**問題**

与えられた代数拡大 $L/K$ の整基底, とくにべき整基底が存在するか.

例えば, 円分体のアナロジーである虚二次体の射類体は, 多くの場合にべき整基底をもつことが知られているが, 完全に解決していない.

# 虚二次体の射類体の相対べき整基底

$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ を除く虚二次体を $K$, $K$ のヒルベルト類体を $H$, $K$ の素イデアルを $\mathfrak{p}$, $K$ の整イデアル $\mathfrak{f}$ を法とする射類体を $K_\mathfrak{f}$ で表す.

**定理 (Schertz, 2010)**

$[K_\mathfrak{f} : H] \geq 3$ とする. 虚二次体 $K$ とその整イデアル $\mathfrak{f}$ が以下のどの場合でもないならば, $K_\mathfrak{f}/H$ はべき整基底をもつ.

1. $K$ 上 $2, 3$ が惰性し, $\mathfrak{f} = \mathfrak{p}^r \nmid 2$.
2. $K$ 上 $2$ が惰性し, $3$ が分岐する, かつ $\mathfrak{f} = \mathfrak{p}^r, \mathfrak{p} \mid 3$.
3. $K$ 上 $3$ が惰性し, $2$ が分岐する, かつ $\mathfrak{f} = \mathfrak{p}^r, \mathfrak{p} \mid 2$.

この中のうち $(1), (2)$ の場合はいくつか解決しているものもある. しかし $(3)$ の場合における結果は知られていなかった.



# 解決している例外型

素数 $p$ の上にある $K$ の素イデアルを $\mathfrak{p}_p$ で表す.

| 場合 | $\mathfrak{f}$ | $K$ の判別式 | $[K_\mathfrak{f} : H]$ | $K_\mathfrak{f}/H$ のべき整基底 |
|---|---|---|---|---|
| $(1)$ | $\mathfrak{p}_7$ | $-19$ | $3$ | 存在しない |
| | $\mathfrak{p}_3 = (3)$ | $-19$ | $4$ | 存在しない |
| | | $-43$ | $4$ | 存在しない |
| | | $-67$ | $4$ | 存在しない |
| | | $-163$ | $4$ | 存在しない |
| | $\mathfrak{p}_{11}$ | $-19$ | $5$ | 存在する |
| | | $-43$ | $5$ | 存在する |
| | $\mathfrak{p}_2^2 = (4)$ | $-67$ | $6$ | 存在しない |
| | | $-163$ | $6$ | 存在しない |
| $(2)$ | $\mathfrak{p}_3^2 = (3)$ | $-51$ | $3$ | 存在する |
| | | $-123$ | $3$ | 存在する |
| | | $-267$ | $3$ | 存在しない |
| $(3)$ | $\mathfrak{p}_2^4$ | $-40$ | $4$ | ? |

## 主結果

例外型にも適用できる, 計算機によるべき整基底の構成方法を考えた.

### 主結果 1

$K = \mathbb{Q}(\sqrt{-10})$, $\mathfrak{f} = \mathfrak{p}_2^4$ とする. これは (3) の場合である. $K_\mathfrak{f}/H$ のべき整基底は存在することがわかった. さらに, 生成元の最小多項式は

$$x^{16} + 4x^{15} + 12x^{14} + 8x^{13} - 24x^{12} - 76x^{11} - 52x^{10} + 116x^9 + 283x^8 + 172x^7 - 244x^6 - 516x^5 - 256x^4 + 264x^3 + 504x^2 + 324x + 81$$

である.

### 主結果 2

$K = \mathbb{Q}(\sqrt{-19})$, $\mathfrak{f} = \mathfrak{p}_7$ とする. これは (1) の場合である. $K_\mathfrak{f}/H$ のべき整基底は存在しないことが知られている (Cougnard-Fleckinger, 1989). 主結果 1 と同じ考え方で別証を与えた.



## べき整基底の存在, 非存在の証明について

証明には判別式を用いる.

### 定義 (元の判別式)

代数拡大 $L/K$, $\gamma \in L$ に対して

$$d_{L/K}(\gamma) = N_{L/K}\left(\prod_\sigma (\gamma - \gamma^\sigma)\right).$$

ここで $\sigma$ は $L$ からその代数閉包への非自明な $K$ 上の埋め込みをはしる.

### 命題

代数拡大 $L/K$ に対し, $\gamma \in \mathcal{O}_L$ がべき整基底をなす必要十分条件は,

$$\big(d_{L/K}(\gamma)\big) = d_{L/K}.$$

Schertz や Cougnard, Fleckinger は, この方程式の解に着目することでべき整基底の存在を証明している. この命題は次のように言い換えられる.

## 主結果 1 の証明の概要

$K=\mathbb{Q}(\sqrt{-10})$, $\mathfrak{f}=\mathfrak{p}_2^4$ とする. $\mathfrak{p}_2$ の上の $K_\mathfrak{f}$ のただ 1 つの素イデアルを $\mathfrak{P}$, ガロア群 $G(K_\mathfrak{f}/H)$ の生成元を $\sigma$ で表す.

**系**

$\gamma\in\mathcal{O}_{K_\mathfrak{f}}$ が $K_\mathfrak{f}/H$ のべき整基底をなす必要十分条件は

$$\begin{cases}(\gamma-\gamma^{\sigma})=\mathfrak{P}^2,\\(\gamma-\gamma^{\sigma^2})=\mathfrak{P}^6.\end{cases}$$

上記の系は次の補題を用いることで導ける.

**補題**

代数拡大 $L/M$, $M/K$ に関して

$$d_{L/K}=d_{M/K}^{[L:M]}\cdot N_{M/K}\left(d_{L/M}\right).$$



## 主結果 1 の証明の概要

**定理 (加法的ヒルベルトの定理 90)**

巡回拡大 $L/K$ に関して, $\langle\sigma\rangle=G(L/K)$ とおく. $\alpha\in L$ がある $\gamma\in L$ を用いて

$$\alpha=\gamma-\gamma^{\sigma}$$

と表せる必要十分条件は

$$\mathrm{Tr}_{L/K}(\alpha)=0.$$

($\Leftarrow$). $n=[L:K]$, $\theta\in L\setminus\mathrm{Ker}(\mathrm{Tr}_{L/K})$ とする. このとき, $\gamma$ を

$$\frac{1}{\mathrm{Tr}_{L/K}(\theta)}\left(\alpha\theta+(\alpha+\alpha^{\sigma})\theta^{\sigma}+\cdots+(\alpha+\cdots+\alpha^{\sigma^{n-3}})\theta^{\sigma^{n-3}}-\alpha^{\sigma^{n-1}}\theta^{\sigma^{n-2}}\right)$$

で定義すると, $\alpha=\gamma-\gamma^{\sigma}$ をみたす.

# 主結果 1 の証明の概要

## 構成方法

1. イデアル $\mathfrak{P}$ の単項イデアルとしての生成元 $\Pi \in K_{\mathfrak{f}}$ を計算する.
2. 次をみたす単数 $\epsilon \in \mathcal{O}_{K_{\mathfrak{f}}}^{\times}$ を計算する.

$$\begin{cases} \mathrm{Tr}_{K_{\mathfrak{f}}/H}(\Pi^2\epsilon) = 0, \\ (\Pi^2\epsilon + (\Pi^2\epsilon)^{\sigma}) = \mathfrak{P}^6. \end{cases}$$

3. 代数的整数 $\gamma \in \mathcal{O}_{K_{\mathfrak{f}}}$ で

$$\gamma - \gamma^{\sigma} = \Pi^2\epsilon$$

をみたすものを, 加法的ヒルベルトの定理を参考に構成する.

注. 以下の式より, $\gamma \in \mathcal{O}_{K_{\mathfrak{f}}}$ が $K_{\mathfrak{f}}/H$ のべき整基底をなすことがわかる.

$$(\gamma - \gamma^{\sigma^2}) = (\gamma - \gamma^{\sigma} - (\gamma - \gamma^{\sigma})^{\sigma}) = (\Pi^2\epsilon + (\Pi^2\epsilon)^{\sigma}) = \mathfrak{P}^6.$$



# 考察

結果,

$$x^{16} + 4x^{15} + 12x^{14} + 8x^{13} - 24x^{12} - 76x^{11} - 52x^{10} + 116x^9 + 283x^8 + 172x^7 - 244x^6 - 516x^5 - 256x^4 + 264x^3 + 504x^2 + 324x + 81$$

の根が $K_{\mathfrak{f}}/H$ のべき整基底の生成元の 1 つであることがわかった.

## 考察

1. 実験結果から, 以下が推測できる.
   - べき整基底の存在の判定に構成方法 (3) は必要ないのではないか.
   - 一般に, 構成方法 (2) の方程式

$$\begin{cases} \mathrm{Tr}_{K_{\mathfrak{f}}/H}(\Pi^2\epsilon) = 0, \\ (\Pi^2\epsilon + (\Pi^2\epsilon)^{\sigma}) = \mathfrak{P}^6. \end{cases}$$

   が解をもつかは分からないが, 解をもつ場合は基本単数の指数が十分小さい範囲にも解をもつのではないか.
2. 例外型にも適用できるため, データを集めることが可能.

## 計算結果

| 場合 | $\mathfrak{f}$ | $d_{K/\mathbb{Q}}$ | $[K_{\mathfrak{f}} : H]$ | $K_{\mathfrak{f}}/H$ のべき整基底 |
|---|---|---|---|---|
| (1) | $\mathfrak{p}_7$ | $-91$ | 3 | 存在する |
| | | $-115$ | 3 | 存在しない？ |
| | | $-187$ | 3 | 存在しない？ |
| | | $-427$ | 3 | 存在する？ |
| | | $-139$ | 3 | 存在する？ |
| | | $-283$ | 3 | 存在しない？ |
| | | $-307$ | 3 | 存在しない？ |
| | | $-643$ | 3 | ？ |
| | $\mathfrak{p}_{11}$ | $-187$ | 5 | 存在する (？) |
| | | $-403$ | 5 | ？ |
| (3) | $\mathfrak{p}_2^4$ | $-10$ | 4 | 存在する |
| | | $-52$ | 4 | ？ |
| | | $-88$ | 4 | 存在しない？ |
| | | $-148$ | 4 | ？ |
| | | $-232$ | 4 | 存在しない？ |



## 主結果 2 の証明の概要

$K = \mathbb{Q}(\sqrt{-19})$, $\mathfrak{f} = \mathfrak{p}_7$ とする. $K$ の類数は 1 より $H = K$. $K_{\mathfrak{f}}/K$ は 3 次巡回拡大である. $\mathfrak{p}_7$ の上の $K_{\mathfrak{f}}$ のただ 1 つの素イデアルを $\mathfrak{P}$, その生成元を $\Pi$ とおく.

**系**

$\gamma \in \mathcal{O}_{K_{\mathfrak{f}}}$ が $K_{\mathfrak{f}}/K$ のべき整基底をなす必要十分条件は

$$(\gamma - \gamma^{\sigma}) = \mathfrak{P}.$$

同様にべき整基底の構成を試みるが, 構成方法 (2) にあたる方程式をみたす単数が存在しないことが証明できる.

**定理 (S.)**

単数 $\epsilon \in \mathcal{O}_{K_{\mathfrak{f}}}$ で

$$\mathrm{Tr}_{K_{\mathfrak{f}}/K}(\Pi\epsilon) = 0$$

をみたすものは存在しない.

## 主結果 2 の証明の概要

単数 $\epsilon_0 \in \mathcal{O}_{K_\mathfrak{f}}$ で

$$\mathrm{Tr}_{K_\mathfrak{f}/K}(\Pi\epsilon_0) = 0$$

をみたすものが存在すると仮定する. $K_\mathfrak{f}$ の基本単数を $u_1$, $u_2$ とおく. 計算機を用いて, $K_\mathfrak{f}$ のイデアル $\mathfrak{p}_{11}\mathcal{O}_{K_\mathfrak{f}}$, $\mathfrak{p}_{61}\mathcal{O}_{K_\mathfrak{f}}$ を法として

$$u_1^{60} \equiv u_2^{60} \equiv 1$$

がわかる. さらに, $\epsilon = \pm u_1^{n_1} u_2^{n_2}$ を $n_1$, $n_2$ をそれぞれ 0 以上 59 以下の整数をはしらせることにより

$$\mathrm{Tr}_{K_\mathfrak{f}/K}(\Pi\epsilon) \equiv 0 \ (\mathrm{mod}\, \mathfrak{p}_{11}\mathfrak{p}_{61}\mathcal{O}_{K_\mathfrak{f}})$$

は解 $\epsilon \in \mathcal{O}_{K_\mathfrak{f}}^\times$ をもたないことがわかる. しかし, これは仮定と矛盾する. よって $K_\mathfrak{f}/K$ のべき整基底は存在しない.



## 今後の課題と参考文献

今回は例外型に対しても適用できる, べき整基底の構成方法を考えた. この手法を精密化し, 他の例外を調べ, 虚二次体の射類体に関して完全な分類を目指す.

[1] J. Cougnard, V. Fleckinger, Sur la monogénéité de l'anneau des entiers de certains corps de rayon, Manuscripta math. 63 (1989), no. 3, 365-376.

[2] I. Gaál, Diophantine equations and power integral bases, Birkhäuser, Boston (2002).

[3] R. Schertz, Complex multiplication, Cambridge University Press, Cambridge (2010).

[4] R. Sekigawa, Relative power integral bases in ray class fields of an imaginary quadratic number field (preprint).

# 明示的 Minkowski 単数と Weber の類数問題について

吉崎 彪雅

東京理科大学 理工学研究科 数学専攻 加塩研究室

2019 年 9 月 6 日



## Notation

まず，今回主に使用する概念と記法について．
$\zeta_n = \exp(\frac{2\pi}{2^{n+2}}\sqrt{-1})$ とする．
$n \geq 1$ に対して，$X_n = \zeta_n + \zeta_n^{-1}$ とする．
$X_1 = \sqrt{2}, X_n = \sqrt{2 + X_{n-1}}$ $(n \geq 2)$ が成立．
$\mathbb{B}_n = \mathbb{Q}(X_n)$ とすると，$\mathbb{Q} \subset \mathbb{B}_1 \subset \mathbb{B}_2 \subset \cdots \mathbb{B}_n \subset \cdots$ が成立し，それぞれ $\mathbb{Q}$ 上のガロア拡大である．
各ガロア群を $G_n = Gal(\mathbb{B}_n/\mathbb{Q})$ とすると，$G_n \cong \mathbb{Z}/2^n\mathbb{Z}$ が成立する．$\sigma_n$ を $G_n$ の生成元とする．
$\mathbb{B}_\infty = \cup_{n\geq 1}\mathbb{B}_n$ とすると，$\mathbb{B}_\infty$ は $\mathbb{Q}$ 上の無限次ガロア拡大となり，そのガロア群は加法群 $\mathbb{Z}_2$ に同型である．これを $\mathbb{Q}$ 上の円分 $\mathbb{Z}_2$ 拡大といい，各中間体 $\mathbb{B}_n$ を $n$th-layer と呼ぶ．
整数環は $\mathbb{Z}[X_n]$ となり，単数群を $E_n = \mathbb{Z}[X_n]^*$ とする．
$\mathbb{B}_n$ の類数を $h_n$ であらわすことにする．

# Weber の類数問題

**問題 (Weber の類数問題)**

$n \geq 1$ に対して，$h_n = 1$ であろう．

予想は $n = 1, \cdots, 6$ まで確かめられており，G.R.H.(一般化リーマン予想) を仮定すると $n = 7$ のときも成立することが知られている．



# 単数群との関係

**定義 (円単数群)**

$C_n = \langle \zeta_n^{\frac{1-a}{2}} \frac{1-\zeta_n^a}{1-\zeta_n} \mid 1 < a < 2^{n+1}, (2, a) = 1 \rangle_{\mathbb{Z}}$ を円単数群という．

単数群と円単数群の比について，以下が成立．

**事実**

全ての $n \geq 1$ に対して，$(E_n : C_n) = h_n$．

よって類数問題は，単数群の構造を調べることに帰着される．
代数体の単数群は一般に $\mathbb{Z}$ 加群としての構造を持つが，特にガロア拡大の場合，ガロア群は単数群にも作用する為，単数群はガロア加群となる．
たとえば $E_n$ において，
$\sum_{i=0}^{2^n-1} a_i \sigma_n^i \in \mathbb{Z}[G_n]$，$\epsilon \in E_n$ に対して，
$(\sum_{i=0}^{2^n-1} a_i \sigma_n^i)\epsilon = \epsilon^{a_0} \sigma_n(\epsilon)^{a_1} \cdots \sigma_n^{2^n-1}(\epsilon)^{a_{2^n-1}} \in E_n$ と作用する．

# Minkowski 単数

**定義 (Minkowski 単数)**

$K/\mathbb{Q}$ : ガロア拡大，$E$ を $K$ の単数群，$\mu_k$ をその捩れ部分，$G = Gal(K/\mathbb{Q})$ をガロア群とする．
$(E : \langle\beta\rangle_{\mathbb{Z}[G]}) < \infty$ を満たす $\beta \in E$ を，$K$ の *Minkowski* 単数とよぶ．特に，
$(E : \langle\mu_K, \beta\rangle_{\mathbb{Z}[G]}) = 1$ を満たすとき，$\beta$ を狭義 *Minkowski* 単数とよぶことにする．

Minkowski 単数はそう特別な概念ではない．というのも，次が成立．

**事実**

任意の有限次ガロア拡大に対して，*Minkowski* 単数は存在する．

しかし，狭義 Minkowski 単数は一般には存在するか分からない．



# 明示的 Minkowski 単数

狭義 Minkowski 単数は一般には存在するか分からないが，$\mathbb{B}_n$ については，それらしい明示的な単数がある．

**命題**

$V_n = \langle 1 + X_n\rangle_{\mathbb{Z}[G_n]}$ とすると，$V_n = C_n$

これより，$h_n = 1 \Leftrightarrow E_n = C_n = V_n \Leftrightarrow 1 + X_n$ : 狭義 Minkowski 単数となる．
よって現在 $n = 1, \cdots, 6$ に対して，$1 + X_n$ は狭義 Minkowski 単数である．

# 相対的手法

$N_{n+1/n} : E_{n+1} \longrightarrow E_n; \epsilon \mapsto \epsilon\sigma_{n+1}^{2^n}(\epsilon)$ を相対ノルムとする.
$n = 7$ のときを考えると，($h_6 = 1$ より) 以下の完全系列がある.

$$0 \longrightarrow \ker N_{7/6} \longrightarrow E_7 \longrightarrow E_6 \longrightarrow 0$$

これより

$$0 \longrightarrow \ker N_{7/6}/(V_7 \cap \ker N_{7/6}) \longrightarrow E_7/V_7 \longrightarrow E_6/V_6 = 0$$

となり，$\ker N_{7/6} \subset V_7$ を証明できれば，$E_7 = V_7$，すなわち $h_7 = 1$ が得られる.
よって問題は相対ノルムの核の考察に帰着された.



$\epsilon \in E_{n+1}$ に対して，$\epsilon = a + bX_{n+1}(a, b \in \mathbb{Z}[X_n])$ と一意にあらわせる.
よって $N_{n+1/n}(\epsilon) = N_{n+1/n}(a + bX_{n+1}) = a^2 - b^2X_{n+1}^2$ となり，特に
$\epsilon \in ker(N_{n+1/n})$ のとき，$a^2 - b^2X_{n+1}^2 = 1$ であるから，以下の問題を考えることが重要である.

**問題**

$x^2 - X_{n+1}^2y^2 = 1$ の，$\mathbb{Z}[X_n]$ 上の解はどのようなものか？

これはペル方程式の拡張であるから，次にペル方程式の解法を確認する.

# ペル方程式の解法

**(整数 $m > 0$ に対して，$x^2 - my^2 = 1$ の $\mathbb{Z}$ 上の解を求める)**

$\sqrt{m}$ の連分数展開を $\sqrt{m} = [a_0, \overline{a_1, \cdots, a_l}]$ とする．周期は $l$ であるから，

$$[a_0, \cdots, a_{l-1}] = \frac{p_{l-1}}{q_{l-1}} \qquad (l : \text{偶数})$$
$$[a_0, \cdots, a_{2l-1}] = \frac{p_{2l-1}}{q_{2l-1}} \qquad (l : \text{奇数})$$

とすると，$l$ が偶奇の時それぞれで，$(p_{l-1}, q_{l-1}), (p_{2l-1}, q_{2l-1})$ が $x^2 - my^2 = 1$ の解を生成する．

これの $\mathbb{Z}[X_n]$ における類似を考える．



# 新しい連分数展開

まず，$x^2 - X_{n+1}^2 y^2 = 1$ の $\mathbb{Z}[X_n]$ 上の解を求めたいので，$X_{n+1}$ の $\mathbb{Z}[X_n]$ 上の連分数展開が必要になると考え，次の展開を得た．

**定理**

$$X_{n+1} = 1 + \cfrac{1}{2(1+X_n)^{-1} + \cfrac{1}{2 + \cdots}} = [1, \overline{2(1+X_n)^{-1}, 2}]$$

この連分数展開の周期は 2 なので，$2 - 1 = 1$ での $\mathsf{convergent}(a_0 + \frac{1}{a_1})$ をみると，$1 + \frac{1}{2(1+X_n)^{-1}} = \frac{1+2(1+X_n)^{-1}}{2(1+X_n)^{-1}}$ より $p_1 = 1 + 2(1+X_n)^{-1}, q_1 = 2(1+X_n)^{-1}$ となり，$N_{n+1/n}(p_1 + X_{n+1}q_1) = 1$ を満たす．
さらに，$p_1 + X_{n+1}q_1 = -\frac{1+X_{n+1}}{1-X_{n+1}} \in V_{n+1}$ である．

**定理**

*Weber* 問題が正しい $\Leftrightarrow \ker N_{n+1/n} = \langle -1, \frac{X_{n+1}+1}{X_{n+1}-1} \rangle_{\mathbb{Z}[G_{n+1}]}$

が成立．

よって，$x^2 - X_{n+1}^2 y^2 = 1$ の解が，$p_1 + X_{n+1}q_1$(とその共役) によって生成されることが言えれば，Weber の類数問題は解決する．
最後に，$p_1 + X_{n+1}q_1$ が「ある意味で」$x^2 - X_{n+1}^2 y^2 = 1$ の最小解であるという事実を紹介する．

**定理**

全ての $n \geq 1$ と $q \in \mathbb{Q}, 0 < |q| < 1$ に対して，

$$(p_1 + X_{n+1}q_1)^q \notin ker(N_{n+1/n}).$$

**証明の方針.**

$q = \frac{1}{m}, m$ : 素数のときを示せばよい．
$m = 2$ のときは，$(p_1 + X_{n+1}q_1)^{\frac{1}{2}}$ の共役で実数に埋め込まれないものがあり，$\mathbb{B}_n$ が総実であることに反す．
$m \geq 3$ のとき，$Tr((p_1 + X_{n+1}q_1)^{\frac{2}{m}}) < 2^{n+1}17$ が証明でき，
$\epsilon(\neq \pm 1) \in ker(N_{n+1/n}) \Rightarrow Tr(\epsilon^2) \geq 2^{n+1}17$ という事実から，定理は従う． □

この事実から，$p_1 + X_{n+1}q_1$ が，別の元のべきによって得られるということはなくなり，ペル方程式の解法から考えて,「ある意味で」最小であることが分かる．



# 連分数展開アルゴリズム

連分数展開は普通，ガウス記号を使ったアルゴリズムによって得られる．

**(連分数展開アルゴリズム)**

$\alpha \in \mathbb{R}, \lfloor \alpha \rfloor$ を $\alpha$ を超えない最大の整数とする．

$$\alpha_0 := \alpha, a_0 := \lfloor \alpha_0 \rfloor$$
$$\alpha_m := (\alpha_{m-1} - a_{m-1})^{-1}, a_m := \lfloor \alpha_m \rfloor \quad (m \geq 1)$$

とすると，$\alpha = [a_0, a_1, \cdots] = a_0 + \dfrac{1}{a_1 + \cdots}$ となる．

これの類似を $\mathbb{Z}[X_n]$ 上の連分数展開にも与える．

**事実**

$\{1, 2\cos(\frac{2\pi i}{2^{n+2}})|i = 1, 2, \cdots 2^n - 1\}$ は $\mathbb{Z}[X_n]$ の整基底となる．
$\phi : \mathbb{Z}[X_n] \longrightarrow \mathbb{R}^{2^n}; a \mapsto (\sigma(a))_{\sigma \in G_n}$ と埋め込めば，その像は $\mathbb{R}^{2^n}$ の完全格子となり，基底 $\phi(\{1, 2\cos(\frac{2\pi i}{2^{n+2}})|i = 1, 2, \cdots 2^n - 1\})$ は，互いに直交する．

この事実をもとに，アルゴリズムを考える．
$\phi(X_{n+1}) := (\sqrt{2 + \sigma(X_n)})_{\sigma \in G_n} \in \mathbb{R}^{2^n}$ と埋め込む．$X_{n+1}$ は $\mathbb{Z}[X_{n+1}]$ のべき整基底をなすので，この埋め込みは $\mathbb{B}_{n+1}$ 全体に拡張できる．

**定理 (連分数展開アルゴリズム)**

$\alpha_0 := \alpha, \phi(a_0) : \phi(\alpha_0)$ に最も近い $\phi(\mathbb{Z}[X_n])$ の点
$\alpha_m := (\alpha_{m-1} - a_{m-1})^{-1}, \phi(a_m) : \phi(\alpha_m)$ に最も近い $\phi(\mathbb{Z}[X_n])$ の点　$(m \geq 1)$

とすると，$\alpha = X_{n+1}$ としたとき，$X_{n+1} = [1, \overline{2(1 + X_n)^{-1}, 2}]$ となる．



# その他の事実とアイディア

一般に整域では，ユークリッド整域 $\Rightarrow$ PID であるが，逆は成り立たない．しかし，ガロア拡大の整数環においては，この二つの概念は結構近い．

**事実**

$K/\mathbb{Q}$ : ガロア拡大，$\mathcal{O}_K$ : 整数環，$E$ : 単数群，$rk_{\mathbb{Z}}(E) \geq 4$ とする．このとき，

$$\mathcal{O}_K : \text{PID} \Leftrightarrow \mathcal{O}_K : \text{ユークリッド整域.}$$

よって，$\mathbb{Z}[X_n](n \geq 3)$ に対しては，PID $\Leftrightarrow$ ユークリッド整域である．
ゆえに，Weber 問題を信じれば $n \geq 3$ に対してはすべてユークリッド整域であるから，ユークリッドアルゴリズムが構成できるはずである．
ユークリッドアルゴリズムは $\mathbb{N}$ への写像でなくても，整列集合であれば良いので，たとえば相対ノルム $N_{7/6} : \mathbb{Z}[X_7] \longrightarrow \mathbb{Z}[X_6]$ に対して，$\mathbb{Z}[X_6]$ に適当な整列順序を定め，ユークリッドアルゴリズムを満たすように出来ないだろうか．

# 今後の課題

- 今は連分数展開から解を構成したにすぎず，$x^2 - X_{n+1}^2 y^2 = 1$ の全ての解がこの連分数展開から得られるかは難しい問題である．
- Weber 問題は $\mathbb{Q}$ 上円分 $\mathbb{Z}_p (p \neq 2)$ 拡大に対しても予想されているが，相対ノルムがペル方程式に似た形にならない為，ペル方程式の解法の応用は見込めそうにない．



# 参考文献 (1)

[1] J. Neukirch
Algebraic number theory
Splinger, 1999

[2] 福田 隆
重点解説岩澤理論
サイエンス社, SGC ライブラリ 145

[3] T. Morisawa, R. Okazaki
On Filtrations of Units of Viete Field
preprint

[4] S. H. Yang
Continued Fractions and Pell's Equation

[5] M. Harper, M. Murty
Euclidean Ring of Algebraic Integers
Canad. J. Math. Vol. 56(1), 2004 pp.71-76

[6] H. Yoshizaki
New Continued Fraction Expansion and Explicit Minkowski Units for Cyclotomic $\mathbb{Z}_2$-Extension of $\mathbb{Q}$
preprint

# $3x+1$ 問題のさまざまな一般化

2019.09.06

名古屋大学大学院 多元数理科学研究科
博士後期課程 2年 (D2) 前川大輔

# §1. 3x+1 問題 別名 Collatz 予想 とは？

$$T : \mathbb{Z} \to \mathbb{Z}$$

$$x \longmapsto \begin{cases} \frac{x}{2} & x: \text{偶数} \\ 3x+1 & x: \text{奇数} \end{cases}$$

と定めたとき、

$\forall x \in \mathbb{Z}_{>0}$, $\exists k \in \mathbb{Z}_{\geq 0}$ s.t. $T^k(x) = 1$ は なりたつか？

なりたちそう（予想）

- 2019年9月現在、未解決問題
- 正しそうか？
  - 反例は みつかっていない.
  - 計算機による検証によって [Roo] [Si]
    $1 \sim 2^{68 \sim 70}$ 程度までの正整数について
    予想は正しいことが確められている.

▶ Def 軌道 (orbit または trajectory)

集合 $S$ の要素 $x \in S$、$S$ 上の変換 $f: S \to S$ に対して、

無限列 $(x, f^1(x), f^2(x), \cdots)$ を $x$ の $f$ による軌道 という

例 $7 \in \mathbb{Z}$ の関数 $T$ による軌道は

$(7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, \textcircled{1}, 2, 1, 2, 1 \cdots)$

最後に注目

Collatz予想のいいかえ 1 ※27

正整数 $x$ の $T$ による軌道は、必ず 1 を含む.

▶ Def サイクル (cycle)

$x$ の $f$ による軌道において $f^{k+l}(x) = f^k(x)$ $(\exists k \in \mathbb{Z}_{\geq 0},\ \exists l \in \mathbb{Z}_{>0})$

であり、かつ $f^k(x), f^{k+1}(x), \cdots f^{k+l-1}(x)$ が相異なるとき、

軌道の部分有限列 $(T^k(x), \cdots, T^{k+l-1}(x))$ を サイクル とよぶ

また、このとき、$x$ の $f$ による軌道は このサイクルを含む という

例 7 の $T$ による軌道、

$(7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1, 2, 1, 2, 1 \cdots)$ は、サイクル $(2, 1)$ を含む。

※1 $l$ をサイクルの長さ という。

※2 サイクルは巡回置換 $(1, \cdots, l)$ で うつりあう同値関係で等しいものとする。 $(1, 2)$

例　1 ⇝ (1, 2, 12, 1, 2, 1, 2, ⋯)

3 ⇝ (3, 5, 8, 4, 2, 1, 2, 1, 2, 1, ⋯)

11 ⇝ (11, 20, 10, 5, 8, 4, 2, 1, 2, 1, ⋯)

Collatz予想のいいかえ2

正整数 $x$ の $T$ による軌道は必ず サイクル (1, 2) を含む

(= サイクル (2, 1))

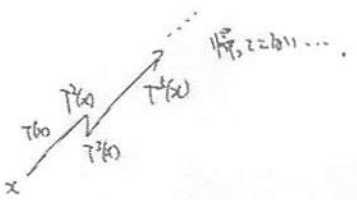
● Collatz予想が"否定"される2つの可能性

(1) ある正整数 $x$ の $T$ による軌道で、(1, 2) でないサイクルを含むものが存在する。


1 を含まないサイクルがあらわれる。

(2) ある正整数 $x$ の $T$ による軌道で、サイクルを含まないものが存在する。

↑「発散軌道」という。



# §2. Main Theorem

▷ Main Thm

Hasse Class の関数 $H$ について、

任意の整数 $x \in \mathbb{Z}$ に対し、

" $x$ の $H$ による軌動が周期的

$\Leftrightarrow$

$x$ の $H$ による剰余軌動が周期的 " がなりたつ

▷ Def. 剰余軌道 (residue orbit)

集合 $S$ から $S$ のある同値関係による剰余類 $R$ への
自然な全射 $\overline{\cdot} : S \twoheadrightarrow R$ があるとき、
$x \in S$ の、変換 $f : S \to S$ による軌道の各要素に
この全射をほどこして得る無限列
すなわち $(\overline{x}, \overline{f(x)}, \overline{f^2(x)}, \cdots)$ を
$x$ の $f$ による ($\overline{\cdot}$ についての) 剰余軌道 という

※ $R$ を剰余類の完全代表系としてもよい.

・例　$\overline{\cdot} : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ に対して

$x \in \mathbb{Z}$ の $T$ による（$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ についての）剰余軌道とは，

$\{1, 0\}$ の無限列 $(\overline{x}, \overline{T(x)}, \overline{T^2(x)}, \cdots)$ のことである．

・例の例　7 の $T$ による（$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ についての）剰余軌道とは，

$(\overline{7}, \overline{11}, \overline{17}, \overline{26}, \overline{13}, \overline{20}, \overline{10}, \overline{5}, \overline{8}, \overline{4}, \overline{2}, \overline{1}, \overline{2}, \overline{1}, \cdots)$

$= (\overline{1}, \overline{1}, \overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{1}, \overline{0}\ \overline{0}\ \overline{0}, \overline{1}\ \overline{0}\ \overline{1}, \cdots)$

のことである．

Thm (3)　Lagarias　1990　[Lag]

正整数 $x$ の $T$ による軌道が 周期的

⇕　(i.e サイクルを含む)

正整数 $x$ の $T$ による剰余軌道が周期的

- 軌道が周期的 ⟹ 剰余軌道が周期的　o.k
- 軌道が周期的 ⟸ 剰余軌道が周期的　非自明

※ 以下、3x+1 問題とその一般化では、
あつかう関数の (mod n) による剰余で
剰余軌道を考えるものとする。

? なぜ剰余を考えるか?

(一般化) 3x+1 関数は
入力の (mod n) の剰余がふるまいを決めるから。

この定理の"反例" Hasse Class には含まれないが、
C や T によく似た関数を考える。

$$S:\mathbb{Z}\to\mathbb{Z}$$

$$x \longmapsto \begin{cases} x/2 & (x\equiv 0 \mod 2) \\ 2x+1 & (x\equiv 1 \mod 2) \end{cases}$$

について

$1\in\mathbb{Z}$ の S による軌道は (1, 3, 7, 15, 31, 63, 127, 255, 511, ...) →

剰余軌道は (1, 1, 1, 1, 1, 1, 1, 1, 1, 1)

剰余軌道は周期的 だが 軌道は周期的でない!

▷ Def. Hasse Class の関数 (Hasse's generalization of $3x+1$ Function)

[Hep] [Mol] $d \in \mathbb{Z}_{\geq 2}$, $m \in \mathbb{Z}_{\geq 1}$ $\gcd(d, m) = 1$ なる2正整数をとり、

$r_1, \cdots, r_d \in \mathbb{Z}$ を $m_i \equiv r_i$ をみたすようにとって、

関数 $H_{d,m,r} : \mathbb{Z} \to \mathbb{Z}$

$$x \longmapsto \begin{cases} \dfrac{x}{d} & x \equiv 0 \pmod d \\ \dfrac{mx - r_i}{d} & x \equiv i \pmod d \end{cases}$$

と定めるとき、

これを Hasse Class の関数という

特に $d=2$, $m=3$, $r_1=-1$ の場合が 関数 $T$ である。

▷ Main Thm

Hasse Class の関数 $H$ について、

任意の整数 $x \in \mathbb{Z}$ に対し、

" $x$ の $H$ による軌動が 周期的

⇕

$x$ の $H$ による剰余軌動が 周期的 " がなりたつ

# §3 さまざまな一般化

・) 例 1　Hasse Class に属する関数

$$f(x) = \begin{cases} \dfrac{x}{3} & x \equiv 0 \\ \dfrac{4x+2}{3} & x \equiv 1 \\ \dfrac{4x+1}{3} & x \equiv 2 \end{cases} \pmod 3$$

・) 例 2　Hasse Class に属する関数

$$f(x) = \begin{cases} \dfrac{x - r_i}{p} & x \equiv r_i \\ \dfrac{x}{p} & x \equiv 0 \end{cases} \pmod p$$

$p$: prime

※ $x$ の $f$ による軌糸軌道 $(a_0, a_1, \cdots, a_n, \cdots)$ に対して

$a_0 + pa_1 + \cdots + p^n a_n + \cdots$ は $x$ の $p$ 進展開

・) 例3　　Hasse Class (を少し拡張したもの) に属する関数

$$f(x) \equiv \begin{cases} \dfrac{x}{4} & x \equiv 0 \\ \dfrac{3x+1}{4} & x \equiv 1 \\ \dfrac{3x+2}{4} & x \equiv 2 \\ \dfrac{9x+15}{4} & x \equiv 3 \end{cases} \pmod 4$$

$$f = T^2$$

Main Thm の拡張

代数体 $K$ の整数環 $\mathcal{O}_K$ について、

$d \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$, $m \in \mathcal{O}_K$ を　$\exists p$: $K$ の素付値 $\left|\dfrac{m}{d}\right|_p > 1$

$\bmod d\mathcal{O}$ の剰余類の完全代表系、$R \subset \mathcal{O}_K$ とし、

$\mathcal{O}_K \ni r_i$ $(i \in R)$ をそれぞれ $m_i \equiv r_i$ なるようにとる．

$$F(x) \equiv \begin{cases} \dfrac{x}{d} & x \equiv 0 \\ \dfrac{mx - r_i}{d} & x \equiv i \end{cases} \pmod{d\mathcal{O}}$$

と定める．

このとき、$\forall x \in \mathcal{O}_K$ について

"$F$による軌道が周期的 $\Leftrightarrow$ 剰余軌道が周期的"

・) 例 4　　拡張された Main Thm を適用できる関数

$K = \mathbb{Q}(\sqrt{2})$　　$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$

$$f(x) = \begin{cases} \dfrac{3x+1}{\sqrt{2}} & 1 \\ \dfrac{x}{\sqrt{2}} & 0 \end{cases} \pmod{\sqrt{2}\mathcal{O}_K}$$

$$f^2|_{\mathbb{Z}} = T$$

・) 例 5　　拡張された Main Thm を適用できる関数

$K = \mathbb{Q}(\sqrt{-1})$　　$\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$

$$f(x) = \begin{cases} \dfrac{x}{2} & x \equiv 0 \\ \dfrac{3x+1}{2} & x \equiv 1 \\ \dfrac{3x+\sqrt{-1}}{2} & x \equiv \sqrt{-1} \\ \dfrac{3x+1+\sqrt{-1}}{2} & x \equiv 1+\sqrt{-1} \end{cases} \pmod{2\mathcal{O}_K}$$

$$f|_{\mathbb{Z}} = T$$

# 参考文献


[Lag] J.C. Lagarias "The set of rational cycles for 3x+1 problem", Acta Arith. 56 (1990), 33-53

[Hep] E. Heppner "Eine Bemerkung zum Hasse-Syracuse Algorithmus", Archiv. Math 31 (1978). 317-329

[Mol] H. Moller "Uber Hasses Verllgemeinerung des Syracuse-Algorithmus (kakutani Problem)", Acta Arith 34 (1978). No.3 219-226

[Roo] E. Roosendaal "On the 3x+1 problem" http://www.ericr.nl/wondrous/

[Sil] T.O. Silvia "Computational verification of the 3x+1 conjecture" http://sweet.ua.pt/tos/3x+1.html

# Brocard-Ramanujan 問題について

武田　渉[1]

名古屋大学

整数論サマースクール宵の時間

[1]本研究の一部は JSPS 科研費 19J10705 の助成を受けたものです.





## Brocard-Ramanujan 問題

方程式

$$x^2 - 1 = l! \tag{1}$$

の整数解を考える.

**Problem 1.1 (Brocard-Ramanujan 問題 1885)**

方程式の整数解は $(x.l) = (5, 4), (11, 5), (71, 7)$ のみであるか?

**Theorem 1.2 (Overholt 1993)**

弱い *Szpiro conjecture* が真であるならば, $x^2 - 1 = l!$ の整数解 $(x.l)$ は有限個.

**弱い Szpiro conjecture**

ある正の定数 $\varepsilon$ が存在して, 任意の互いに素な非零整数の三つ組 $(a, b, c)$ で $a + b = c$ となるものに対して,

$$|abc| < \prod_{\substack{p|abc \\ p:\text{prime}}} p^{\varepsilon}$$

が成立.





## 一変数多項式への一般化

**Problem 1.3 (Brocard-Ramanujan 問題 (一般の多項式))**

$P(x)$ を整数係数な二次以上の多項式とする. このとき,

$$P(x) = l!, \tag{2}$$

の整数解 $(x, l)$ の数は有限個であるか?

**Theorem 1.4 (Berend-Harmse 2006)**

任意の二次以上 $\mathbf{Q}$ 上既約な多項式 $P(x)$ に対して, 方程式 *(2)* の解は有限個.

# 二変数斉次多項式への一般化

**Theorem 1.5**

$n$ を平方数でない正の整数とする. このとき, $x^2 - ny^2 = 1$ は整数解を無限個持つ.

**Theorem 1.6 (Erdős and Obláth 1937, Pollack and Shapiro 1973)**

$n \geq 2$ とする. このとき, $x^n + y^n = l!$ の整数解で $\gcd(x, y) = 1$ となるものは $(x, y, l) = (1, 1, 2)$ のみである. また, $n \geq 3$ に対して $x^n - y^n = l!$ は $\gcd(x, y) = 1$ となる整数解を持たない.





# Brocard-Ramanujan 問題の一般化

**Problem 1.7 (Brocard-Ramanujan 問題 (一般の二変数斉次多項式))**

$F(x, y)$ を整数係数な二次以上の二変数斉次多項式とする. このとき,

$$F(x, y) = l!, \tag{3}$$

の整数解 $(x, y, l)$ として現れる $l$ の数は有限個であるか?

# Brocard-Ramanujan 問題の一般化

**Corollary 1.8 (Theorem 1.5 の系)**

$n$ を平方数でない正の整数とする. このとき, $x^2 - ny^2 = l!$ は整数解 $(x, y, l)$ を無限個持つ.

**Theorem 1.9 (後に紹介する結果の系)**

$n$ を平方数でない正の整数とする. このとき, $x^2 - ny^2 = l!$ は整数解 $(x, y, l)$ として現れる $l$ は有限個.





# Main Theorem(既約な場合)

**Main Theorem 1 (T. 2019+)**

$F(x, y)$ を $\deg F \geq 2$ なる斉次多項式, $n \geq 1$ とする. このとき, $F(x, y)^n = l!$ の整数解 $(x, y, l)$ として現れる $l$ の数は有限個.

**Corollary 1.10 (Berend-Harmse 2006)**

任意の二次以上 $\mathbf{Q}$ 上既約な多項式 $P(x)$ に対して, 方程式 $P(x) = l!$ の解は有限個.

**Remark 1.11**

$l!$ を以下の関数に変えても有限性が示せる.

- $[1, \ldots, l]$ : 1 から $l$ の最大公約数,
- $p_1 \cdots p_l$ : 相異なる $l$ 個の素数の積 $(p_i < p_{i+1})$.

# Main Theorem(可約な場合)

## Main Theorem 2 (T. 2019+)

2 次以上の整数係数斉次多項式 $F(x,y)$ で以下のような既約分解を持つものを考える:

$$F(x,y)=\prod_{i=1}^{u} f_i(x,y)^{m_i}.$$

正の整数 $a\geq 1$, $b>1$ で $\bigcap_i \mathbf{P}(\mathcal{C}_{f_i})\supset\{p : \textit{prime} \mid p\equiv a \mod b\}$ となるものが存在するとき, $F(x,y)=l!$ の整数解 $(x,y,l)$ として現れる $l$ の数は有限個.

ただし, $\mathbf{P}(\mathcal{C}_{f_i})$ は $f_i(x,1)\equiv 0 \mod p$ が解を持たない様な素数 $p$ の集合.

## Remark 1.12

代数体に一般化した階乗関数 $\Pi_K$ や *Remark 1.11* の関数に対しても類似の結果を得ている.





# $F(x,y)$ で表示される整数

## Lemma 2.1

$F(x,y)=a_nx^n+a_{n-1}x^{n-1}y+\cdots+a_0y^n$ を既約多項式とし,
$g=\gcd(a_n,\ldots,a_0)$, $\Delta_F$ を多項式の判別式とする. 整数 $N$ の素因数分解を

$$N=gp_1\cdots p_sq_1^{l_1}\cdots q_t^{l_t}$$

とする. ここで, $q_i\in\mathbf{P}(\mathcal{C}_F)$ は $\gcd(q_i,a_na_0\Delta_F)=1$ となる素数で $p_i$ はその他の素数である.
このとき, ある $(x,y)$ で $N=F(x,y)$ となるならば, 任意の $i$ で $n|l_i$.

## Remark 2.2

説明の都合上 $q_i$ の条件が実際よりも強くなっている.

# $C$ に関する Bertrand 型の評価

**Lemma 2.3**

$L$ を $K/\mathbf{Q}$ の Galois 閉包として $n = [L : \mathbf{Q}]$, $\Delta$ を $L$ の判別式の絶対値とする. また, $C$ を $Gal(L/\mathbf{Q})$ の共役類とする.
このとき, ある $c > 0$ が存在して以下を満たす.
任意の $x > \exp(cn(\log \Delta)^2)$ に対して, $C$ に対応する $K$ の素イデアル $\mathfrak{p}$ でそのイデアルノルムが $\mathfrak{N}\mathfrak{p} \in (x, 2x)$ となるものが存在する.





# 主定理の証明

- Lemma 2.3 より, ある $c > 0$ が存在して, 任意の $x > \exp(cn(\log \Delta)^2)$ に対して, $Gal(K_F/\mathbf{Q})$ の共役類 $C$ に対応する素イデアル $\mathfrak{p}$ で $\mathfrak{N}\mathfrak{p} \in (x, 2x)$ となるものが存在する.

$\rightsquigarrow$ ここで $\mathfrak{N}\mathfrak{p} = p^f > \exp(cn(\log \Delta)^2)$ とすると共役類 $C$ に対応する素イデアル $\mathfrak{q}$ で $\mathfrak{N}\mathfrak{q} = q^f \in (p^f, 2p^f)$ となるものが存在.

$\Rightarrow$ つまり $p > \exp(\frac{c}{f} n(\log \Delta)^2)$ とすると共役類 $C$ に対応する素数 $q$ で $q \in (p, 2p)$ となる.

- $p \in \mathbf{P}(\mathcal{C}_F)$ なる素数に対して, $p!$ は Lemma 2.1 の形にはならない.

$\rightsquigarrow$ $p$ の倍数となる 2 番目に小さい整数は $2p$ で現れるため, $p \leq l < 2p$ に対して $l!$ は Lemma 2.1 の形にはならない.

$\rightsquigarrow$ 帰納法により, $p \leq l$ で $l!$ は Lemma 2.1 の形にはならない.

# $\mathbb{Z}$上の力学系について

大阪大学大学院理学研究科数学専攻
博士前期課程1年
後藤 倫

## 目次

- 動機・主定理の紹介
- 主張の解説
- 証明の概略
- 今後の課題

記法　定義　主張　未解説

# 動機

定理(G) $f^n := f \circ f \circ \cdots \circ f$ について、

$$\forall n, \exists x_n \quad f^{x_n}(a) \equiv_{b^n} x_n$$

:多くの$f \in \mathbb{Z}[x]$で、$b$が$f$に関する条件を満たせば成立(さらに$x_n$は$b$進収束する)

例: $f(x) = x^2 + x + 3$

$$f^3(0) \equiv_{10} 3,$$
$$f^{43}(0) \equiv_{10^2} 43,$$
$$f^{243}(0) \equiv_{10^3} 243, \ldots$$
$$f^{636048243}(0) \equiv_{10^9} 636048243, \ldots$$

# 直感的な考察

$$\exists x \in \mathbb{Z}_b := \prod_{p|b} \mathbb{Z}_p\,, \qquad f^x(a) = x$$

$$x = f^{f^{f^{\cdots^{\cdots}(a)}(a)}(a)}(a)$$

$f \uparrow_a (n) := f^n(a)$ とおくと

$$f \uparrow_a \uparrow_t (n) = \overbrace{f^{f^{\cdots f^{t}(a)\cdots}(a)}(a)}^{f\text{が}n\text{個}} \xrightarrow{n\to\infty} x$$

# 動機

$\uparrow_x : C(\mathbb{N},\mathbb{N}) \to C(\mathbb{N},\mathbb{N})$ について、何が言えるか?

ただし、$\mathbb{N} = \{0,1,2,\dots\}$、離散位相
$C(\mathbb{N},\mathbb{N})$: 合成, $\uparrow_x$ で閉じた半環
・環にしたい
・より狭いクラスはあるか?

# 主定理:

$\widehat{\mathbb{Z}} := \varprojlim_{n} \mathbb{Z}/n\mathbb{Z}$ 上に類似物がある.

定理. $C(\widehat{\mathbb{Z}},\widehat{\mathbb{Z}})$の部分環で、
- 多項式環を含み、
- 「合成」と「軌道の周期部分を取る」という操作について閉じた環が構成できる.

# 軌道

定義.　力学系$(X, f: X \to X)$の**軌道**
$\{x, f(x), f^2(x), \dots, f^n(x), \dots\}$

- 軌道のタワー記法

$$f \uparrow_x : \mathbb{N} \to X$$
$$n \mapsto f^n(x)$$

$\uparrow_x : C(X, X) \to C(\mathbb{N}, X)$

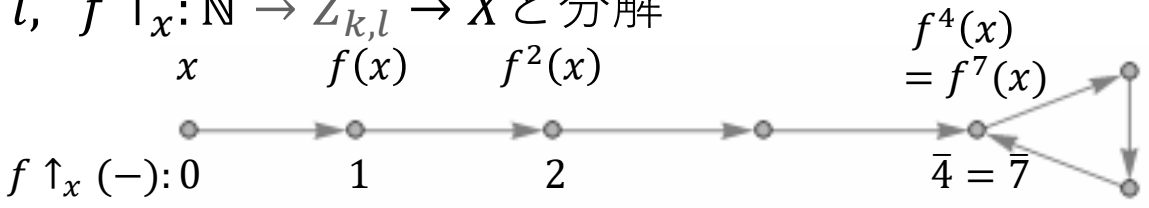
# 軌道の例: 前周期軌道

力学系$(X, f)$での $x \in X$の軌道が前周期的:
- $\exists k, l \in \mathbb{N}, f^k(x) = f^{k+l}(x)$

⇕

- $\exists k, l,\ \ f \uparrow_x : \mathbb{N} \to Z_{k,l} \to X$と分解

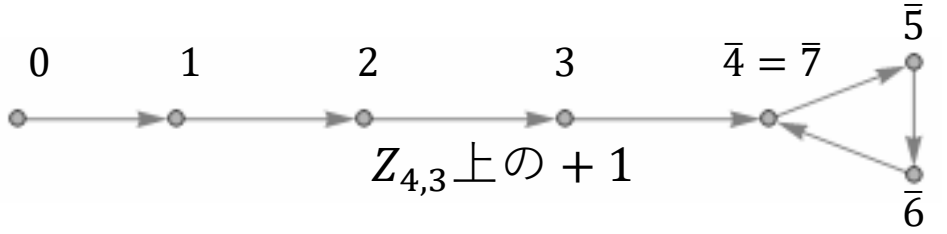
例:



# $\mathbb{N}$の副有限完備化

$$\widehat{\mathbb{N}} \coloneqq \varprojlim\{S\text{: 有限半群}|\mathbb{N} \twoheadrightarrow S\} = \varprojlim_{k,l} Z_{k,l}$$

$$Z_{k,l} \coloneqq {}^{\mathbb{N}}/_{\langle k \sim k+l \rangle} = (\{0,1,\dots,k-1\} \sqcup \mathbb{Z}_{k\leq}/l\mathbb{Z}, +)$$




# 副有限周期性

定義.　軌道$f\uparrow_x\colon \mathbb{N} \to X$が
連続に$\widehat{f\uparrow_x}\colon \widehat{\mathbb{N}} \to X$に伸びるとき
$x$を$f$の**副有限(前)周期点**といい、
制限$f\hat{\uparrow}_x\colon \widehat{\mathbb{Z}} \to X$を軌道の**周期部分**という.

# $\widehat{\mathbb{N}}$ の構造

・半群として、

$$\widehat{\mathbb{N}} \simeq \left(\mathbb{N} \sqcup \widehat{\mathbb{Z}}, \hat{+}\right),$$

$$a \hat{+} b := \begin{cases} a+b \in \mathbb{N} & (a,b \in \mathbb{N}) \\ a+b \in \widehat{\mathbb{Z}} & (otherwise) \end{cases}.$$

・制限位相はそれぞれ通常の位相.

・$\mathbb{N} \hookrightarrow \widehat{\mathbb{N}}$ は射影系の誘導する写像でもあり、特に稠密な埋め込み.

# $\widehat{\mathbb{N}}$ の構造

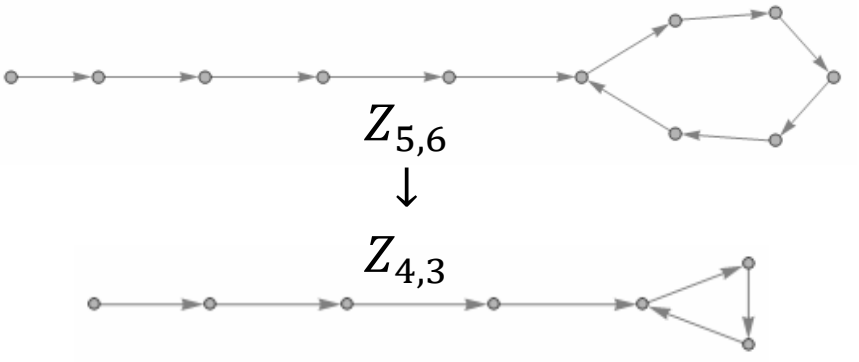
$$\widehat{\mathbb{N}} \simeq \mathbb{N} \sqcup \widehat{\mathbb{Z}}$$

$Z_{k,l}$

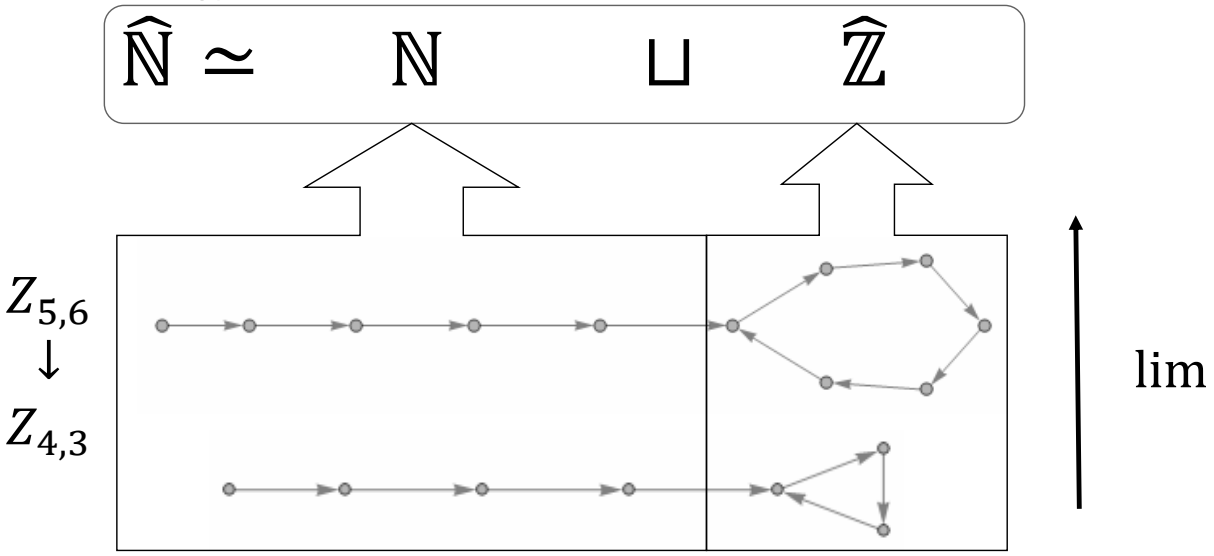
↓

$Z_{k',l'}$

$k' \leq k, l' | l$



# $\widehat{\mathbb{N}}$ の構造

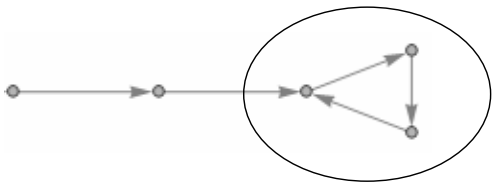



# 副有限周期性

軌道 $f\uparrow_x : \mathbb{N} \to X$ が連続に $\widehat{f\uparrow_x} : \widehat{\mathbb{N}} \to X$ に伸びるとき
$x$ を $f$ の副有限(前)周期点といい、
制限 $f\hat{\uparrow}_x : \widehat{\mathbb{Z}} \to X$ を軌道の周期部分という.

通常の前周期点のとき、周期部分になっている:

$$\begin{array}{ccccc} \widehat{\mathbb{Z}} & \hookrightarrow & \widehat{\mathbb{N}} & \hookleftarrow & \mathbb{N} \\ \downarrow & & \downarrow & & \downarrow \quad \searrow^{f\uparrow_x} \\ \mathbb{Z}/l\mathbb{Z} & \hookrightarrow & Z_{k,l} & \simeq & Z_{k,l} \quad \to X \end{array}$$



# 主定理:

$C(\hat{\mathbb{Z}}, \hat{\mathbb{Z}})$の部分環で、
- 多項式環を含み、
- 「合成」と「軌道をとる操作 $=\hat{\uparrow}_x$」について閉じた環が構成できる.

# 主定理:

$\mathrm{C}(\hat{\mathbb{Z}}, \hat{\mathbb{Z}})$の部分環で、
- 多項式環を含み、
- 「合成」と「軌道をとる操作 $=\hat{\uparrow}_x$」について閉じた環が構成できる.

# 構成の前提: 周期写像

定義. $P_f:\mathbb{N}\to\mathbb{N}$ が $f:\widehat{\mathbb{Z}}\to\widehat{\mathbb{Z}}$ の**周期写像**とは、

- $m=P_f(n)$ について、

$$\begin{array}{ccc}\widehat{\mathbb{Z}} & \xrightarrow{f} & \widehat{\mathbb{Z}} \\ \downarrow & \circlearrowleft & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\exists f_n} & \mathbb{Z}/n\mathbb{Z}.\end{array}$$

以降$P_f$ は$f$の周期写像とする.

# 周期写像

$$\begin{array}{ccc}\widehat{\mathbb{Z}} & \xrightarrow{f} & \widehat{\mathbb{Z}} \\ \downarrow & \circlearrowleft & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\exists f_n} & \mathbb{Z}/n\mathbb{Z}\end{array} \qquad (m=P_f(n))$$

例

- $f\in\widehat{\mathbb{Z}}[x], P_f=id_{\mathbb{N}}$
- $f(x)=\begin{cases}3x+1 & \left(x\in 2\widehat{\mathbb{Z}}+1\right)\\ \frac{x}{2} & \left(x\in 2\widehat{\mathbb{Z}}\right)\end{cases}$, $P_f(n)=2n$
- $f(x)=2x, g(y)=f\uparrow_x(y)=2^{\hat{y}}x, P_g=\varphi$

# 構成の前提: 順序

$\mathrm{Q} \coloneqq \{p^e\}$上の整列順序$\preccurlyeq$:

$$1 \prec 2 \prec 2^2 \prec \cdots \prec 2^n \prec \cdots \prec 3 \prec 3^2 \prec \cdots \prec 3^n \prec \cdots \prec 5 \prec 5^2 \prec \cdots$$

$$\alpha : \mathbb{N} \to \mathbb{N} : \alpha(n) = \max_{\preccurlyeq}\{p^e \mid p^e \text{ は} n \text{の約数}\}$$

# 主定理

$$A \coloneqq \{f \in C(\widehat{\mathbb{Z}}, \widehat{\mathbb{Z}}) \mid \exists P_f , \alpha\left(P_f(n)\right) \preccurlyeq \alpha(n)\}$$

は加法、乗法、合成、$\hat{\uparrow}_x$ について閉じている.

# 証明の概略

命題. $P_f$ ： $f$の周期写像、$P_g$ ：$g$の周期写像

$$\Downarrow$$

・$P_f \circ P_g$ ： $g \circ f$の周期写像

・$lcm \circ (P_f, P_g)$ : $f+g, fg$の周期写像

:定義と中国剰余定理から従う.

$\Rightarrow A$: $+,\times,\circ$ で閉じている.

# 証明の概略

補題1. $\#X = p$

$$\Downarrow$$

$\phi: X \to X$の軌道の周期部分の長さ$\leq p$

補題2.

$$\#\left(\mathbb{Z}/pn\mathbb{Z}\right)\Big/\left(\mathbb{Z}/n\mathbb{Z}\right) = \#\,\mathbb{Z}/p\mathbb{Z} = p$$

$g = f\,\hat{\uparrow}_x$と$p^e$について、

$$\exists n, \quad \alpha(n) = p^e$$

$$\begin{array}{ccc} \mathbb{Z}/pn\mathbb{Z} & \xrightarrow{f_{pn}} & \mathbb{Z}/pn\mathbb{Z} \\ \downarrow & \circlearrowleft & \downarrow \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{f_n} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

補題1. と補題2. より

$\alpha(P_g(pn)) \preccurlyeq \alpha(pP_g(n))$

$A$: $\hat{\uparrow}_x$ で閉じている.

# 課題

- $A$の環論的性質は？
- $A$の代数的/半群論的一般化は？
- $\mathbb{R}$上の類似、その他の類似物は？

# 参考文献

後藤, Arithmetic Convergence of double-iterated polynomials, arXiv: 1905.08589.

J. Almeida, Profinite semigroups and applications. Structural theory of automata, semigroups, and universal algebra, 1-45, Springer, Dordrecht, (2005)

N. Hindman and D.Strauss, Algebra in the Stone-Čech compactification. Theory and applications. De Gruyter Textbook. Walter de Gruyter & Co., Berlin, (2012)

D. B. Shapiro and S. D. Shapiro, Iterated exponents in number theory. Integers 7(2007)

A. Fan and L. Liao, On minimal decomposition of p-adic polynomial dynamical systems, Advances in Mathematics 228, Issue 4 (2011)

# 2 次有理写像による代数体の反復拡大について

山本 康太 (名古屋工業大学)
Kota Yamamoto (Nagoya Institute of Technology)

Joint work with Yasushi Mizusawa

1. Introduction
2. Main Results
3. Sketch of Proofs



## Introduction

$p$ : prime number, $k$ : number field, $[k : \mathbb{Q}] < \infty$,

$K_\infty/k$ : $\mathbb{Z}_p$-extension,

$L_\infty/K_\infty$ : maximal unramified abelian pro-$p$ extension.

$$X(K_\infty) := \mathrm{Gal}(L_\infty/K_\infty) \text{ : unramified Iwasawa module.}$$

### Known Facts

- $X(K_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/k)]]$-module.
- $X(K_\infty)$ : "pseudo-null" over $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/k)]] \Leftrightarrow X(K_\infty)$ : finite.

### GC (Greenberg's conjecture (1976))

$k$ : totally real, $K_\infty/k$ : cyclotomic $\mathbb{Z}_p$-extension

$\Rightarrow$ $X(K_\infty)$ : "pseudo-null", i.e. finite.

$K_\infty/k$ : $p$-adic Lie extension
$L_\infty/K_\infty$ : maximal unramified abelian pro-$p$ extension.

$$X(K_\infty) := \mathrm{Gal}(L_\infty/K_\infty) : \text{unramified Iwasawa module.}$$

The growth of the $p$-parts of class numbers has been studied along various $p$-adic Lie extensions $K_\infty/k$;

- $\mathbb{Z}_p^d \rtimes \mathbb{Z}_p$-extensions
  ([Cuoco-Monsky 1981], [Perbet 2011], [Lei 2017], $\cdots$),
- $\mathrm{GL}_2(\mathbb{Z}_p)$-extensions
  ([Sairaiji-Yamauchi 2015], [Hiranouchi 2017], [Ohshita 2018], $\cdots$).

## Motivation

We want to find basic $p$-adic Lie extensions $K_\infty/k$ over which the Iwasawa modules $X(K_\infty)$ are conjectually pseudo-null.



# Main Results (1/2)

Setting $\quad \phi(x) := \dfrac{1}{2}\left(x - \dfrac{1}{x}\right), \quad p = \deg\phi = 2,$

$\{b_n\}_{n\geq 0} : b_0 \in k, \ \phi(b_{n+1}) = b_n, \quad k_n := k(b_n), \quad K_n := k(\phi^{-n}(b_0)),$

$k^{\mathrm{cyc}}/k$ : cyclotomic $\mathbb{Z}_2$-extension, $\quad k_\infty := \bigcup_{n\geq 0} k_n, \quad K_\infty := \bigcup_{n\geq 0} K_n.$

## Theorem 1 ([Shen-Washington 1994]+[M.-Y.])

If $b_0^2 + 1 \notin k^2$, then the following hold true for $\forall n \in \mathbb{Z}_{\geq 0}$ :

- $\mathrm{Gal}(k_{n+2}/k_n) \cong \mathbb{Z}/4\mathbb{Z}$, and $k_{n+1} = k_n(\sqrt{b_n^2 + 1}\,)$,
- $b_0 \in \mathscr{O}_k \ \Rightarrow \ k_n/k$ is unramified outside $\{\mathfrak{p} \mid 2(b_0^2+1)\}$,
- $K_n = k_n\left(\cos\frac{2\pi}{2^{n+2}}\right)$, and so $K_\infty = k_\infty k^{\mathrm{cyc}}$,
- $k_\infty \not\subset k^{\mathrm{cyc}} \ \Rightarrow \ \mathrm{Gal}(K_\infty/k) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$

# Main Results (2/2)

**Cororally**

$k$ : totally real, $b_0^2 + 1 \notin k^2$. Assume that GC holds for each $k^{\mathrm{cyc}}k_n/k_n$.
Then $X(K_\infty)$ is a pseudo-null $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k)]]$-module.

**Pseudo-nullity (cf. [Venjakob 2003])**

If a $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k)]]$-module $M$ is f.g. over $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k^{\mathrm{cyc}})]]$, then
$M$ is "pseudo-null" over $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k)]] \Leftrightarrow$ it is $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k^{\mathrm{cyc}})]]$-torsion.

**Theorem 2**

$k = \mathbb{Q}$, $b_0^2 + 1 = q$ is prime s.t. $q \equiv 17 \pmod{32}$.
Then $X(K_\infty)$ is a finitely generated $\mathbb{Z}_2$-module of 2-rank at most 2,
in particular, a pseudo-null $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k)]]$-module.

e.g. $(b_0,\ q) = (4, 17), (20, 401), (36, 1297), (84, 7057)$.



# Remarks (1/2)

Suppose that $\zeta_\ell + \zeta_\ell^{-1} \in k$ for $\ell \geq 2$, where $\zeta_\ell := \exp(\frac{2\pi\sqrt{-1}}{\ell})$.
For $\ell' \geq 2$, put

$$\varphi(x) := \frac{\zeta_\ell^{-1}(x - \zeta_\ell)^{\ell'} - \zeta_\ell(x - \zeta_\ell^{-1})^{\ell'}}{(x - \zeta_\ell)^{\ell'} - (x - \zeta_\ell^{-1})^{\ell'}} \in k(x).$$

- [Chonoles, et al. 2014]; For $\ell = \ell' \geq 3$,
  calculating the Galois group of the numerator of $\varphi^n(x) - t \in k(t; x)$,
  which is called "generalized Rikuna polynomial" (cf. [Rikuna 2002]).
- $\ell = 2\ell' = 4$ (resp. $\ell = \ell' = 4$) $\Rightarrow$ $\phi(x) = \varphi(x)$ (resp. $\phi^2(x) = \varphi(x)$).
- [Shen-Washington (1994)] has constructed our $K_n$ when $k = \mathbb{Q}$.

## Remarks (2/2)

$\psi(x) \in k(x),\ \deg \psi \geq 2.$

**Definition**

$\psi$ : post-critically finite $:\Leftrightarrow \#\{\psi^n(c); n = 1, 2, \cdots\} < \infty$ ($\forall$ critical point $c$ of $\psi$).

$\phi$ is post-critically finite;

$$\phi(x) = \frac{1}{2}\left(x - \frac{1}{x}\right), \quad \pm\sqrt{-1} \mapsto \mp\sqrt{-1}.$$

$b_0 \in k,\ \psi^{-\infty}(b_0) := \bigcup_{n=0}^{\infty} \psi^{-n}(b_0)$

**Fact (Aitken-Hajir-Maire 2005, Cullinan-Hajir 2012)**

$\psi$ is post-critically finite $\Rightarrow$ # of all ramified primes in $k(\psi^{-\infty}(b_0))/k$ is finite.

$\mathrm{Gal}(k(\psi^{-\infty}(b_0))/k)$ becomes the image of "arboreal Galois representation" for $\psi$ and $b_0$. ([Boston-Jones], $\cdots$)



## Sketch of Proof (Thm.1 and Cor.)

- $N_{k_{n+1}/k_n}(b_{n+1}^2 + 1) = 4(b_n^2 + 1).$
- $x^4 - 4b_n x^3 - 6x^2 + 4b_n x + 1$ (= numerator of $\phi^2(x) - b_n$); $k_{n+2}/k_n$ is known as "simplest quartic extension".
- $\phi^n\left(A_n^i(b_n)\right) = b_0$ for all $0 \leq i \leq 2^n - 1$, where

$$A_n(x) = \frac{x\cos\frac{2\pi}{2^{n+1}} - \sin\frac{2\pi}{2^{n+1}}}{x\sin\frac{2\pi}{2^{n+1}} + \cos\frac{2\pi}{2^{n+1}}}.$$

- Put $n_0 := \max\{n \mid k_n \subset k^{\mathrm{cyc}}\}$. [Washington, §13.3]; $X(K_\infty)$ is f. g. over $\mathbb{Z}_2[[\mathrm{Gal}(K_\infty/k^{\mathrm{cyc}})]]$, and $\exists e \geq 0$ s.t.

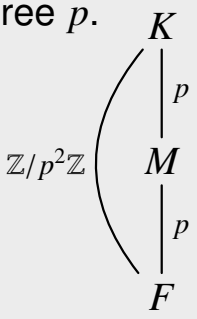
$$X(k_{n+n_0}k^{\mathrm{cyc}}) \cong X(K_\infty)/\text{"}\nu_{n,e}Y_e\text{"} \quad \text{for } \forall n \geq e.$$

# Key Theorem (Thm.2)

$T$ : finite set of primes of (a subfield of) a number field $K$,
$A^T(K)$ : $p$-Sylow subgroup of $T$-ideal class group of $K$
($Cl^T(K) = Cl(K)/\langle\{[\mathfrak{p}] \mid \mathfrak{p} \in T\}\rangle$ : $T$-ideal class group).

## Theorem 3 (Y. 2018)

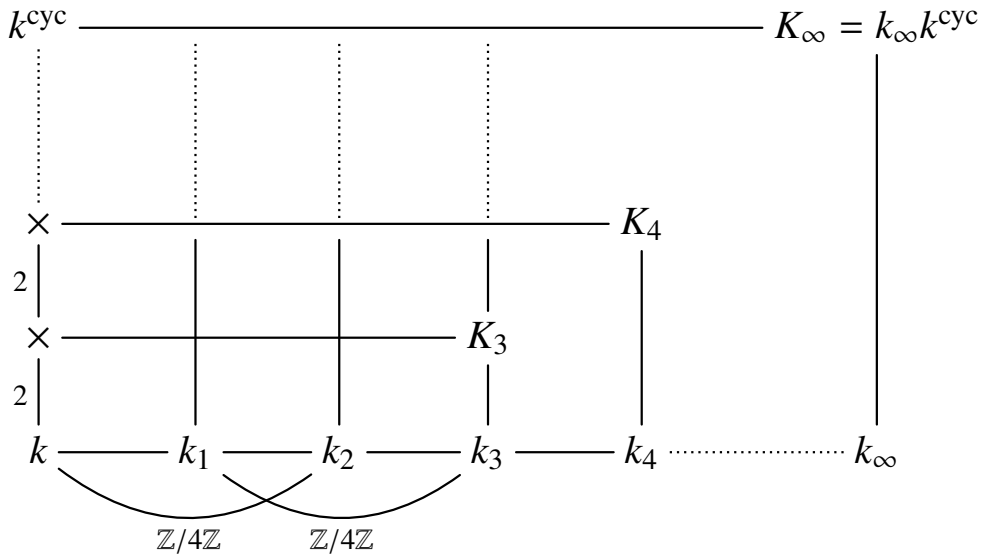
$K/F$ : $\mathbb{Z}/p^2\mathbb{Z}$-extension, $M/F$ : subextension of degree $p$.
$S$ : set of all ramified primes of $F$ in $K/F$,
$S_1 = \{\mathfrak{p} \in S \mid \mathfrak{p}$ is inert in $M/F\}$,
$S_2 = \{\mathfrak{p} \in S \mid \mathfrak{p}$ ramifies in $M/F\}$.
$S_1 \subset T \subset S = S_1 \cup S_2 \neq \emptyset$.
Then $A^T(M) = 0 \Rightarrow A^T(K) = 0$.




We use this theorem for $p = 2$ and $T = \{2\}$.
Note that $X(K_\infty) \cong \varprojlim A(K_n)$.



$k = \mathbb{Q}$, $b_0^2 + 1 = q \equiv 17 \pmod{32}$




- $A(k_2) \cong \mathbb{Z}/2\mathbb{Z}$, and $A^{\{2\}}(k_2) = 0$.
- By using Thm.4 recursively, $A^{\{2\}}(k_n(\cos\frac{2\pi}{2^m})) = 0$ for all $m \geq 2$ and $n \geq 0$.

# ガロア群の同質類とガロア拡大の構成

國府田 玄基 (東京理科大学理学研究科)
Joint work with 木田 雅成

2019 年 9 月 7 日
整数論サマースクール 宵の時間



## Isoclinism (同質性)

$G, H$：有限群

**Definition (Isoclinic, Isoclinism)**

$G, H$ に対して $\varphi : G/Z(G) \xrightarrow{\sim} H/Z(H)$, $\psi : G' \xrightarrow{\sim} H'$ が存在して, 次の図式が可換であるとき, $G, H$ は isoclinic (同質) であるという

($G \sim H$ とかく).

またこのとき, $(\varphi, \psi)$ の組を isoclinism (同質写像) という.

$$\begin{array}{ccc} G/Z(G) \times G/Z(G) & \xrightarrow{(aZ(G), bZ(G)) \mapsto [a,b]} & G' \\ \downarrow{\scriptstyle \varphi \times \varphi} & & \downarrow{\scriptstyle \psi} \\ H/Z(H) \times H/Z(H) & \xrightarrow{(cZ(H), dZ(H)) \mapsto [c,d]} & H' \end{array}$$

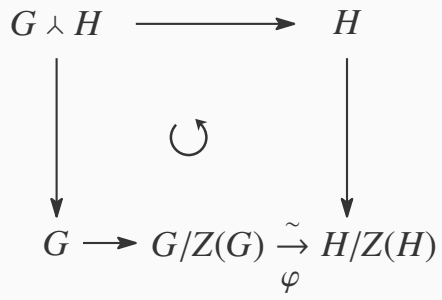
(ここで $G' = [G, G]$)

## Isoclinism の例

Isoclinic ($\sim$) は有限群上の同値関係である.

- 有限アーベル群全体は isoclinism class をなす.
- $D_4 \sim Q_8$
- $G$:有限群, $A$:有限アーベル群
  $\Longrightarrow G \sim G \times A$
- $G \sim H$, $(\varphi, \psi)$: isoclinism とする. $\Longrightarrow G \sim H \sim G \curlywedge H$
  ただし,

$$G \curlywedge H = \{(g,h) \in G \times H \mid \varphi(gZ(G)) = hZ(H)\}$$



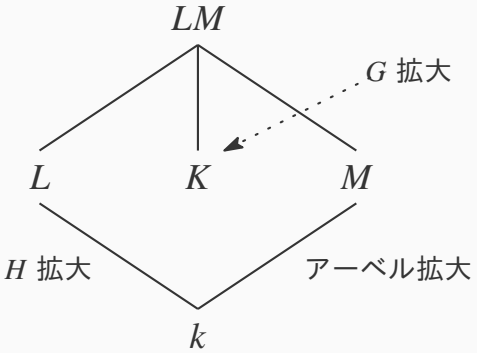

(fiber product, 詳しくは後述)



## Schmid の結果

**Theorem (P. Schmid, [Beitr. Algebra Geom., 2015])**

$Z(H) \subset H'$, $G \sim H$ とする.
$H$ 拡大 $L/k$ が存在
$\Longrightarrow$ $^{\exists}M/k$: アーベル拡大,
合成体 $LM$ の部分体に, $k$ 上 $G$ 拡大 $K/k$ が存在する.



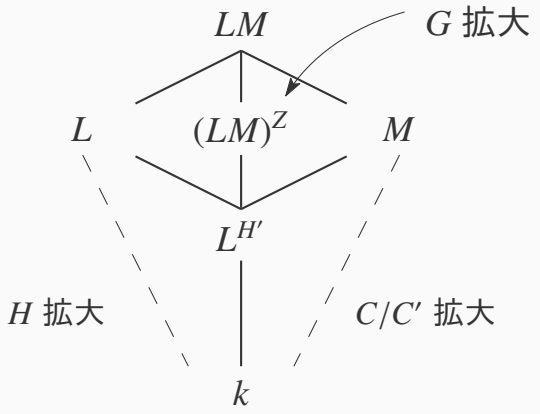

問: $M$ を特定できないか?

- $\mathrm{Gal}(M/k)$ はどのような
  アーベル群に同型か?
- 中間体 $L \cap M$ は何か?
- $G$ 拡大を固定する
  $\mathrm{Gal}(LM/k)$ の部分群は何か?

群論的に考察する.

**Theorem (Kida - K., to appear in Acta Arith.)**

$G \sim H$, $(\varphi, \psi)$: isoclinism,
$C = G \curlywedge H = \{(g,h) \in G \times H \mid \varphi(gZ(G)) = hZ(H)\}$
$Z_G = \{(g,1) \in C \mid g \in Z(G)\}$ とする.
$\Longrightarrow {}^{\exists}\gamma : C/Z_G C' \xrightarrow{\sim} H/H'$,
$C \cong H \curlywedge C/C' = \{(h, xC') \in H \times C/C' \mid hH' = \gamma(xZ_G C')\}$.
さらに, $Z = \{(h, (1,h)C') \mid h \in Z(H)\}$ とすれば,
$G \cong (H \curlywedge C/C')/Z$.

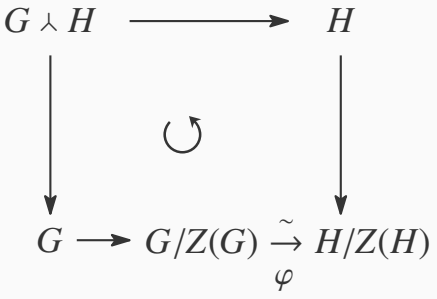


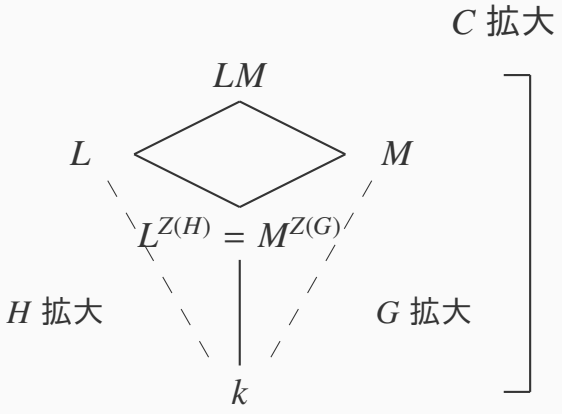

5

## Fiber product

$C = G \curlywedge H = \{(g,h) \in G \times H \mid \varphi(gZ(G)) = hZ(H)\}$

- 直積 $G \times H$ の部分群
- 合成体のガロア群




6

$\varphi : G/Z(G) \xrightarrow{\sim} H/Z(H)$ とする.

$$C = G \curlywedge H = \{(g,h) \in G \times H \mid \varphi(gZ(G)) = hZ(H)\}$$

$$Z_G = \{(g,1) \in C \mid g \in Z(G)\} \cong Z(G)$$
$$Z_H = \{(1,h) \in C \mid h \in Z(H)\} \cong Z(H)$$

このとき

$$C/Z_G \cong H, \quad C/Z_H \cong G,$$
$$|C| = |G||Z(H)| = |H||Z(G)|.$$

$C'$: 交換子部分群とすると,

$$C' \cap Z_G = C' \cap Z_H = 1.$$



## 主定理の証明

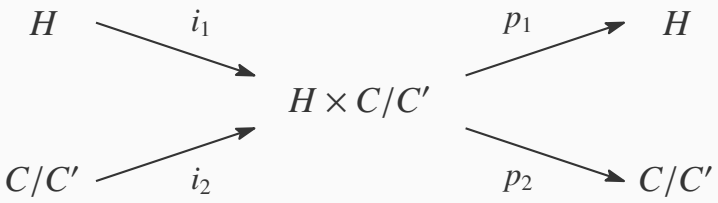
$$C = G \curlywedge H = \{(g,h) \in G \times H \mid \varphi(gZ(G)) = hZ(H)\}.$$

$C$ を別の直積で書く.

$$C \longrightarrow C/Z_G \times C/C'$$
$$x \longmapsto (xZ_G,\ xC')$$

この map は単射 ($\because \ker = Z_G \cap C' = 1$).
また, $C/Z_G \cong H$ であったから,

$$C \xrightarrow{\subset} H \times C/C'$$
$$(g,h) \longmapsto (h,\ (g,h)C')$$

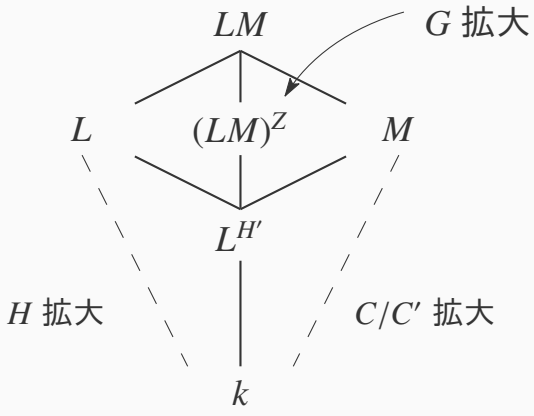



$$p_1(i_1(H) \cap C) = H', \qquad p_1(C) = H,$$
$$p_2(i_2(C/C') \cap C) = Z_G C'/C', \qquad p_2(C) = C/C'$$

Goursat's lemma により,

$$\gamma : (C/C')/(Z_G C'/C') \cong C/Z_G C' \xrightarrow{\sim} H/H',$$
$$C \cong H \curlywedge C/C' = \{(h, xC') \in H \times C/C' \mid hH' = \gamma(xZ_G C')\}.$$

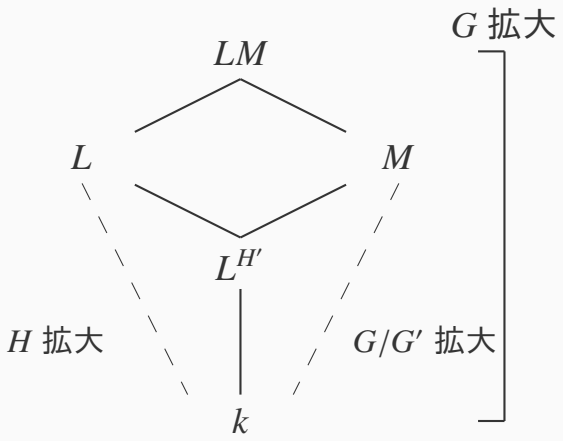





$C/Z_H \cong G$ であったから,
$Z_H$ の $H \times C/C'$ への埋め込みを
$Z = \{(h, (1,h)C') \mid (1,h) \in Z_H\}$
と書いて,
$(H \curlywedge C/C')/Z \cong G$ を得る.

**Corollary**

$G \sim H$, $(\varphi, \psi)$: isoclinism,
$G \twoheadrightarrow H$ 全射が存在する.
$\Longrightarrow {}^{\exists}\gamma : G/Z(G)G' \xrightarrow{\sim} H/H'$,
$G \cong H \curlywedge G/G' = \{(h, xG') \in H \times G/G' \mid hH' = \gamma(xZ_G G')\}$.




${}^{\exists}G \twoheadrightarrow H$ のときは
$C$ の代わりに $G$ がとれて,
$H \curlywedge G/G' \cong G$ を得る.



## Example

$G = C_4 \rtimes C_4$ (Transitive group ID : 16T8)

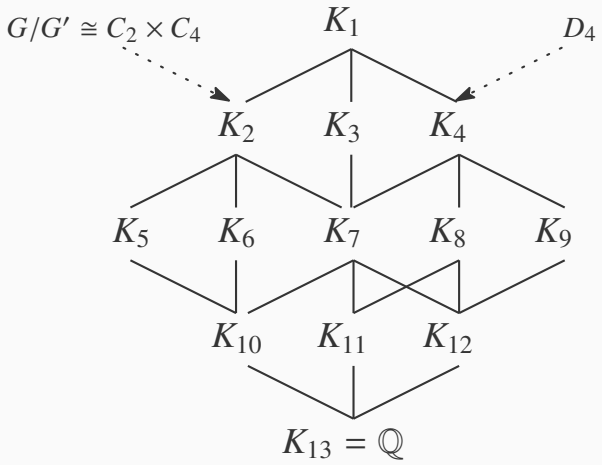
$$H = D_4 = \langle s, t \mid s^4 = t^2 = 1, tst^{-1} = s^{-1} \rangle$$
$$G = C_4 \rtimes C_4 = \langle u, v \mid u^4 = v^4 = 1, vuv^{-1} = u^{-1} \rangle$$

中心: $Z(H) = \langle s^2 \rangle, \quad Z(G) = \langle u^2, v^2 \rangle$
交換子群: $H' = \langle s^2 \rangle, \quad G' = \langle u^2 \rangle$

$$\varphi : G/\langle u^2, v^2 \rangle \xrightarrow{\sim} H/\langle s^2 \rangle;$$
$$u\langle u^2, v^2 \rangle \longmapsto s\langle s^2 \rangle,$$
$$v\langle u^2, v^2 \rangle \longmapsto t\langle s^2 \rangle$$

$$\therefore \quad G \sim H$$

$G \cong C_4 \rtimes C_4$ 拡大の図 (共役を除く)




左図で

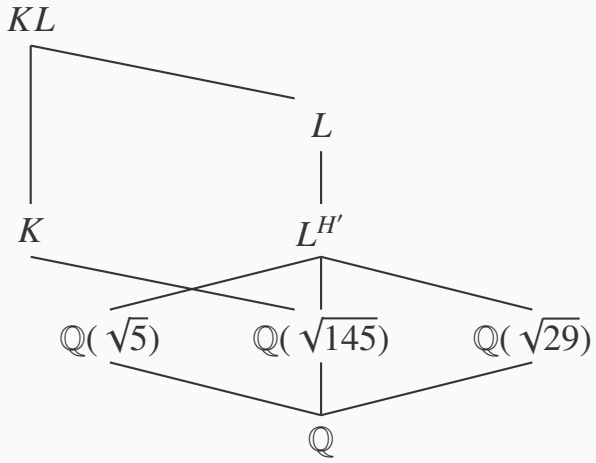
- $K_4$: $D_4$ 拡大,
  ただし $K_4/K_{10}$ : cyclic
- $K_2$: $C_2 \times C_4 (\cong G/G')$ 拡大

$D_4$ 拡大から $C_4 \rtimes C_4$ 拡大を作るには $K_7$ を $K_2$ に埋め込めば良い.
よりシンプルに, $K_{10}$ を $K_5$ ($C_4$ 拡大) に埋め込めばよい ※.
このとき合成体 $K_4K_5/\mathbb{Q}$ は $C_4 \rtimes C_4$ 拡大.

※ $K_{10}$ が $C_4$ 拡大に埋め込めるような $D_4$ 拡大を選ぶ必要がある.



$D_4$ 拡大:
$L = \mathbb{Q}\left(\sqrt{2(11+\sqrt{5})}, \sqrt{29}\right)$




$\mathbb{Q}(\sqrt{145})$ を, $K/\mathbb{Q}$ ($C_4$ 拡大) に埋め込む.
例えば $K = \mathbb{Q}\left(\sqrt{2(145+\sqrt{145})}\right)$ に埋め込む.
すると合成体 $KL$ は $C_4 \rtimes C_4$ 拡大となる.

# Infinitely many hyperelliptic curves with exactly two rational points

(Joint work with Yoshinosuke Hirakawa, arXiv: 1904.00215v2)

第 27 回整数論サマースクール　宵の時間

Keio University

Bannai Lab.

Hideki Matsumura

2019/09/07



## Contents

# §1 Main theorem

In number theory, it is one of classical problems to determine the sets of rational points of algebraic curves.
e.g. $C : y^2 = f(x)$. $C(\mathbb{Q}) = ?$

Key tool: The 2-descent.

The 2-descent $\rightsquigarrow$ ideal class group/unit group of $L_i$, where $L := \mathbb{Q}[T]/(f(T)) \simeq \prod_{i_1}^{m} L_i$, $L_i = \mathbb{Q}[T]/(f_i(T))$, $f = f_1 \cdots f_m \in \mathbb{Q}[T]$: irreducible decomposition.

**Problem**
Construct a family of hyperelliptic curves s.t. we can determine the set of rational points by the 2-descent.



# §1 Main theorem

$p \in \mathbb{Z}$: prime, $i, j \in \mathbb{Z}_{\geq 0}$.

$$C^{(p;i,j)} : y^2 = x(x^2 + 2^i p^j)(x^2 + 2^{i+1} p^j).$$

**Theorem**((1)-(3) Hirakawa-M, (4) M.)
Suppose one of the following conditions.
(1) $p \equiv 3 \pmod{16}$ and $(i, j) = (0, 1)$.
(2) $p \equiv 11 \pmod{16}$ and $(i, j) = (1, 1)$.
(3) $p \equiv \pm 3 \pmod{8}$ and $(i, j) = (0, 2)$.
(4) $p \equiv 7 \pmod{16}$ and $(i, j) = (0, 2)$.
Then, $C^{(p;i,j)}(\mathbb{Q}) = \{(0, 0), \infty\}$.

## §2 Algebraic curves with no nontrivial rational points

**Theorem**(cf. Tunnell, 1983) $p \in \mathbb{Z}$: prime.
$C^{(p)} : y^2 = x(x^2 - p^2)$: elliptic curve.
$p \equiv 3 \pmod 8$. $\Rightarrow C^{(p)}(\mathbb{Q}) = \{(0,0), (\pm p, 0), \infty\}$.

$\because$ 2-descent, Lutz-Nagell theorem.

We use their analogues in the proof of the main theorem.



## §3 Outline of the proof

$C := C^{(p;i,j)}$.

$$\begin{array}{ccccc} \phi: & C(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}) = \mathrm{Pic}^0_C(\mathbb{Q}) & \simeq \mathbb{Z}^{\oplus r} \oplus J(\mathbb{Q})_{\mathrm{tors}} \\ & \cup & & \cup & \\ & P & \longmapsto & [P - \infty] & \end{array}$$

Mordell-Weil rank

2-descent Lutz-Nagell

**Key tools**

1. 2-descent: prove $r = 0$ in cases $(1) - (3)$.
2. Richelot isogeny (+2-descent): prove $r = 0$ in case $(4)$.
3. Grant's Lutz-Nagell type theorem:
   Determine $C^{(p;i,j)}(\mathbb{Q})$.

# Conclusion

$p \in \mathbb{Z}$: prime, $i, j \in \mathbb{Z}_{\geq 0}$.

$$C^{(p;i,j)} : y^2 = x(x^2 + 2^i p^j)(x^2 + 2^{i+1} p^j).$$

**Theorem**((1)-(3) Hirakawa-M, (4) M.)
Suppose one of the following conditions.
(1) $p \equiv 3 \pmod{16}$ and $(i, j) = (0, 1)$.
(2) $p \equiv 11 \pmod{16}$ and $(i, j) = (1, 1)$.
(3) $p \equiv \pm 3 \pmod{8}$ and $(i, j) = (0, 2)$.
(4) $p \equiv 7 \pmod{16}$ and $(i, j) = (0, 2)$.
Then, $C^{(p;i,j)}(\mathbb{Q}) = \{(0, 0), \infty\}$.

Key tools
- 2-descent
- Richelot isogeny
- Lutz-Nagell



# References

[1] D. Grant, *On an analogue of the Lutz-Nagell theorem for hyperelliptic curves*, J. Number Theory **133** (2013), no. 3, 963–969.
[2] Y. Hirakawa and H. Matsumura, *Infinitely many hyperelliptic curves with exactly two rational points*, arXiv: 1904.00215v2.
[3] F. Richelot, *De transformatione integralium abelianorum primi ordinis commentatio*, J. Reine Angew. Math. **16** (1837), 221–341.
[4] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta. Arith. **98** (2001), no. 3, 245–277.
[5] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, Invent. Math. **72** (1983), no. 2, 323–334.