数理解析研究所講究録
第2012巻 2016年 12-22

素数位数の巡回群に対するネーター問題について

新潟大学理学部数学科　星 明考
Akinari Hoshi, Department of Mathematics, Niigata University [1]

概要　有理数体 $\mathbb{Q}$ 上の素数位数の巡回群 C_p に対するネーター問題は，$\mathbb{Q}$ 上の有理関数体 $\mathbb{Q}(x_1,\dots,x_p)$ への巡回群 C_p の変数の置換による作用の不変体 $\mathbb{Q}(x_1,\dots,x_p)^{C_p}=\{a\in\mathbb{Q}(x_1,\dots,x_p)\mid \sigma(a)=a\ (\forall\sigma\in C_p)\}$ が $\mathbb{Q}$ 上有理的 (純超越的) か？を問うており，17個の素数 $p\leq 43$ と $p=61,67,71$ に対して肯定解をもつことが知られているが，解が肯定的となる素数 p が無限に存在するかどうかは分かっていない．本稿では，既知の結果の概説を行うとともに，論文 [Hos15] における，PARI/GP による $p<20000$ なる素数 p に対する計算結果を紹介する．

1　はじめに

本稿では，論文 [Hos15] における，素数位数の巡回群に対するネーター問題についての PARI/GP による計算結果を紹介する．また紙面の都合上，論文 [Hos15] に載せられなかった部分は arXiv から extended version [Hos-ex] として公開してあるので，そちらも参考にしていただきたい．

k を体，G を有限群とする．エミー・ネーター [Noe13, Noe17] によって提唱された，k 上の G に対するネーター問題とは，次のような問題である：

k 上の G に対するネーター問題 $\mathrm{Noe}(G/k)$:
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 $h(x_g)=x_{hg}$ $(\forall g,h\in G)$ によって作用するとき，不変体 $k(G):=k(x_g\mid g\in G)^G$ は k 上有理的 (純超越的) か？

すなわち，不変体 $k(G)$ が再び $n=|G|$ 変数有理関数体 $k(x_1,\dots,x_n)$ と同型であるかを問うている．ネーター問題は100年程前に提唱された問題であるが，まだ多くの場合にその答えが分かっていない．群 G がアーベル群の場合には，Lenstra [Len74] によって肯定解をもつための必要十分条件が与えられ，一応解決したとされているが，本稿で述べるとおり，有理数体 $\mathbb{Q}$ 上の素数位数の巡回群 C_p の場合でさえ，$p=83,107,163,\dots$ などに対するネーター問題 $\mathrm{Noe}(C_p/\mathbb{Q})$ の答えは依然よく分からない．

さらに，ネーター問題 $\mathrm{Noe}(G/k)$ が肯定的ならば k 上の G に対するガロア逆問題が肯定的に解ける，すなわち，k 上の G 拡大の存在がわかる，ことが知られている．このあたりのことについては，Jensen-Ledet-Yui [JLY02, Chapter 5], Garibaldi-Merkurjev-Serre [GMS03, Section 33], Hoshi [Hos14, Section 2] などを見ていただきたい．

以下で論文 [Hos15] の主定理を述べる．体の拡大 K/k に対して，K が k 上安定有理的であるとは，いくつかの K 上の代数的独立元 $t_1,\dots,t_n$ に対して，$K(t_1,\dots,t_n)$ が k 上有理的となることである．定義から，有理的 $\Rightarrow$ 安定有理的，となる．

[1] 本研究は科研費 25400027 の助成を受けています．

次の素数からなる集合 R, U, X を定義する：

$R = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}$ (有理的な場合),

$U = \{251, 347, 587, 2459, 2819, 3299, 4547, 4787, 6659, 10667,$
$12227, 14281, 15299, 17027, 17681, 18059, 18481, 18947\}$ (未解決の場合),

$X = \{59, 83, 107, 163, 487, 677, 727, 1187, 1459, 2663, 3779, 4259,$
$7523, 8837, 10883, 11699, 12659, 12899, 13043, 13183, 13523,$
$14243, 14387, 14723, 14867, 16547, 17939, 19379\}$ (GRH の下有理的でない場合).

ここに，$|R| = 17$, $|U| = 18$, $|X| = 28$ である．以下が [Hos15] の主定理である：

定理 1 (Hoshi [Hos15, Theorem 1.1]).
p を素数，C_p を位数 p の巡回群とする．$p < 20000$ に対して，
(i) $p \notin R \cup U \cup X$ または (ii) GRH (一般リーマン予想) の下，$p \notin R \cup U$
ならば $\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上安定有理的でない．

ネーター問題はウェーバーの類数問題 (Fukuda, Komtsu [FK09], [FK10], [FK11] 参照) と関係が深い (定理 6 参照)．実際，論文 [Hos15] の preprint version [Hos-ex] を arXiv から公開した後，Fukuda [Fuk14] は $\mathbb{Q}(C_{59})$ が $\mathbb{Q}$ 上有理的でないことが分かることを教えてくれた．これとは独立に，L. C. Washington の示唆により，J. C. Miller [Mil14a] は [Mil14b], [Mil15] の手法を用いて，$\mathbb{Q}(C_{59})$ が $\mathbb{Q}$ 上有理的でないこと，$\mathbb{Q}(C_{251})$ が GRH の下 $\mathbb{Q}$ 上有理的でないことが分かることを教えてくれた．これらの結果をより大きな素数 p に対して拡張できるかどうかは，興味深い問題である．しかし，定理 1 で除外されている未解決の場合を同様の手法で解決することは，現状では難しいようである．

以下において，2 節で有理数体 $\mathbb{Q}$ 上のアーベル群に対するネーター問題についての既知の結果の概説し，3 節で主結果 (定理 1) の証明の方針を述べる (詳しくは，論文 [Hos15] とその extended version [Hos-ex] を見ていただきたい)．

謝辞. 本研究に対し，重要な示唆をいくつも与えて下さった遠藤静男氏，Ming-chang Kang 氏に深く感謝いたします．主定理の未解決の場合に関する情報を下さった，福田隆氏，小松啓一氏，John C. Miller 氏，講演の機会を与えて下さった，世話人の横山俊一氏，木田雅成氏，宗政昭弘氏，大浦学氏に深く感謝いたします．

2 アーベル群に対するネーター問題

本節では $\mathbb{Q}$ 上のアーベル群に対するネーター問題について既知の結果を述べる．Swan [Swa81], [Swa83] も参照していただきたい．以下，p を素数とし，C_n で位数 n の巡回群を表す．次の結果から，有限アーベル群 G に対して，$\mathbb{C}(G)$ は $\mathbb{C}$ 上有理的となる：

定理 2 (Fischer [Fis15], Swan [Swa83, Theorem 6.1] も参照).
G を指数 e の有限アーベル群とする．
(i) char $k = 0$ または char $k > 0$ であり char $k \nmid e$, かつ
(ii) k は 1 の原始 e 乗根を含む,
ならば $k(G)$ は k 上有理的である．

体 k が標数 $p>0$ であり，G が p 群の場合には，次の結果が知られている：

定理 3 (Kuniyoshi [Kun54, Kun55, Kun56]).
G を p 群，k を標数 $p>0$ の体とすれば，$k(G)$ は k 上有理的である．

Masuda [Mas55, Mas68] はガロア降下 (Galois descent) のアイデアをネーター問題に次のように用いた．ζ_p を 1 の原始 p 乗根とし，$L=\mathbb{Q}(\zeta_p)$, $\pi=\mathrm{Gal}(L/\mathbb{Q})$ とおけば，定理 2 より，

$$\mathbb{Q}(C_p)=\mathbb{Q}(x_1,\dots,x_p)^{C_p}=(L(x_1,\dots,x_p)^{C_p})^{\pi}=L(y_0,\dots,y_{p-1})^{\pi}=L(M)^{\pi}(y_0)$$

となる．ここで，$y_0=\sum_{i=1}^{p}x_i$ は π 不変，M は自由 $\mathbb{Z}[\pi]$ 加群，ガロア群 π は $y_1,\dots,y_{p-1}$ に

$$\sigma(y_i)=\prod_{j=1}^{p-1}y_j^{a_{ij}},\ [a_{ij}]\in GL_n(\mathbb{Z})\ (\sigma\in\pi)$$

によって作用する．この作用により，不変体 $L(M)^{\pi}$ はある $p-1$ 次元の代数的トーラスの関数体とみなせる ([Vos98, Chapter 3], [HY, Section 1] 参照)．このとき，以下が成り立つ：

定理 4 (Masuda [Mas55, Mas68], Swan [Swa83, Lemma 7.1] も参照).
(i) M は階数 1 の射影 $\mathbb{Z}[\pi]$ 加群．
(ii) M は置換 $\mathbb{Z}[\pi]$ 加群，すなわち，π の M への作用は M の $\mathbb{Z}$ 基底を置換する，ならば $L(M)^{\pi}$ は $\mathbb{Q}$ 上有理的である．特に，$p\leq 11$ に対して，$\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上有理的である．[2]

Swan [Swa69] は，定理 4 の逆を考える過程で，初めてネーター問題の否定解を与えた：

定理 5 (Swan [Swa69, Theorem 1], Voskresenskii [Vos70, Theorem 2]).
(i) $\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的ならばある $\alpha\in\mathbb{Z}[\zeta_{p-1}]$ が存在して $N_{\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}}(\alpha)=\pm p$ をみたす．
(ii) (Swan) $\mathbb{Q}(C_{47})$, $\mathbb{Q}(C_{113})$, $\mathbb{Q}(C_{233})$ は $\mathbb{Q}$ 上有理的でない．
(iii) (Voskresenskii) $\mathbb{Q}(C_{47})$, $\mathbb{Q}(C_{167})$, $\mathbb{Q}(C_{359})$, $\mathbb{Q}(C_{383})$, $\mathbb{Q}(C_{479})$, $\mathbb{Q}(C_{503})$, $\mathbb{Q}(C_{719})$ は $\mathbb{Q}$ 上有理的でない．

定理 6 (Voskresenskii [Vos71, Theorem 1]).
$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的となるための必要十分条件は，ある $\alpha\in\mathbb{Z}[\zeta_{p-1}]$ が存在して $N_{\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}}(\alpha)=\pm p$ をみたすことである．

定理 6 より，もし円分体 $\mathbb{Q}(\zeta_{p-1})$ の類数 $h(\mathbb{Q}(\zeta_{p-1}))$ が 1 であれば，$\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上有理的となる．しかし，$h(\mathbb{Q}(\zeta_{p-1}))=1$ となる素数 p は，$p\leq 43$, $p=61,67,71$ に限られる (Masley, Montgomery [MM76, Main theorem], Washington [Was97, Chapter 11] 参照)．

Endo, Miyata [EM73] は Masuda-Swan の方法を改良し，アーベル群 G に対するネーター問題の研究を行った ([Vos73] も参照)，特に，$\mathbb{Q}(C_{p^l})$ が $\mathbb{Q}$ 上有理的となるための必要十分条件を与えた (定理 8)．以下，論文 [EM73] の結果の一部を述べる．

定理 7 (Endo, Miyata [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 k 上有理的 (安定有理的) ならば $k(G_1\times G_2)$ も k 上有理的 (安定有理的) である．[3]

[2] 定理 4 (ii) は [Hos05, Chapter 5] で位数 pl $(l\mid p-1)$ のフロベニウス群 F_{pl} $(p\leq 11)$ に拡張されている．
[3] 定理 7 は一般の体 k 上で成り立つことが，Kang, Plans [KP09, Theorem 1.3] によって示されている．

定理7の逆は一般には成り立たない(定理12参照).

定理 8 (Endo, Miyata [EM73, Theorem 3.1]).
pを奇素数，$l>0$を整数，kを標数0の体で，$[k(\zeta_{p^l}):k]=p^{m_0}d_0$ $(0\le m_0\le l-1, d_0\mid p-1)$をみたすとする．このとき，次の3つの条件は同値である：
(i) 全ての忠実$k[C_{p^l}]$加群Vに対して，不変体$k(V)^{C_{p^l}}$はk上有理的；
(ii) $k(C_{p^l})$はk上有理的；
(iii) ある$\alpha\in\mathbb{Z}[\zeta_{p^{m_0}d_0}]$が存在して，以下をみたす：

$$N_{\mathbb{Q}(\zeta_{p^{m_0}d_0})/\mathbb{Q}}(\alpha)=\begin{cases}\pm p & m_0>0\\ \pm p^l & m_0=0.\end{cases}$$

さらに$m_0>0$のとき，条件(i),(ii),(iii)は次の2つの条件いずれとも同値となる：
(i′) すべての$k[C_{p^l}]$加群Vに対して，$k(V)^{C_{p^l}}$はk上有理的；
(ii′) すべての$1\le l'\le l$に対して，$k(C_{p^{l'}})$はk上有理的.

定理 9 (Endo, Miyata [EM73, Proposition 3.2]).
pを奇素数，kを標数0の体とする．$\zeta_p+\zeta_p^{-1}\in k$ならばすべての$l$に対して，$k(C_{p^l})$は$k$上有理的である．特に，すべての$l$に対して，$\mathbb{Q}(C_{3^l})$は$\mathbb{Q}$上有理的.

定理 10 (Endo, Miyata [EM73, Proposition 3.4, Corollary 3.10]).
(i) 素数$p\le 43$, $p=61,67,71$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) $l\ge 3$に対して，$\mathbb{Q}(C_{2^l})$は$\mathbb{Q}$上安定有理的でない.

定理5から，ノルム方程式$N_{F/\mathbb{Q}}(\alpha)=\pm p$がある$d$次中間体$\mathbb{Q}\subset F\subset\mathbb{Q}(\zeta_{p-1})$に対して整数解をもたなければ，$\mathbb{Q}(C_p)$は$\mathbb{Q}$上有理的でないことがわかる．Endo, Miyataは$d=2$のとき，次を与えている.

命題 11 (Endo, Miyata [EM73, Proposition 3.6]).
pを次の2つの条件のいずれかをみたす奇素数とする：
(i) $p=2q+1$, $q\equiv -1 \pmod 4$, qは平方因子を持たず，$4p-q$と$q+1$は平方数ではない;
(ii) $p=8q+1$, $q\not\equiv -1 \pmod 4$, qは平方因子を持たず，$p-q$と$p-4q$は平方数でなはい.
このとき，$\mathbb{Q}(C_p)$は$\mathbb{Q}$上有理的でない.

命題11 (i), (ii)によって，$\mathbb{Q}(C_p)$が$\mathbb{Q}$上有理的ではないことがわかる素数$p\le 20000$を表1, 表2にそれぞれ与える.

定理 12 (Endo, Miyata [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，ある整数$m>0$が存在して，$k(G^m)$はk上有理的となる.

定理 13 (Endo, Miyata [EM73, Theorem 4.6]).
有限アーベル群Gに対して，$\mathbb{Q}(G)$が$\mathbb{Q}$上有理的 $\Longleftrightarrow$ $\mathbb{Q}(G)$が$\mathbb{Q}$上安定有理的.

表 1: [EM73, Proposition 3.6 (i)] をみたす素数 $p < 20000$

$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的ではないことがわかる素数 p
47,79,167,191,223,239,263,359,367,383,431,439,463,479,503,
599,607,719,823,839,863,887,911,983,1031,1039,1087,1103,1223,1231,
1303,1319,1327,1367,1399,1439,1447,1487,1511,1543,1559,1583,1663,1759,1823,
1831,1847,1871,1879,2039,2063,2087,2111,2207,2239,2383,2399,2423,2447,2543,
2671,2687,2711,2767,2879,2903,2927,2999,3023,3119,3167,3191,3319,3343,3359,
3391,3407,3463,3559,3607,3623,3671,3767,3847,3863,3919,3967,4007,4079,4111,
4127,4271,4327,4391,4423,4463,4567,4583,4639,4679,4703,4759,4783,4799,4831,
4871,4919,4943,4967,5039,5087,5119,5231,5279,5303,5399,5431,5471,5479,5503,
5519,5591,5623,5639,5647,5711,5791,5807,5839,5879,5903,5927,6047,6079,6143,
6199,6263,6287,6311,6367,6599,6703,6719,6791,6863,6871,6911,6983,6991,7079,
7103,7127,7159,7207,7247,7487,7559,7583,7607,7639,7703,7727,7823,7879,7919,
7927,8039,8087,8111,8167,8231,8287,8311,8423,8431,8447,8543,8599,8647,8663,
8719,8783,8807,8831,8863,8887,8999,9007,9103,9239,9319,9391,9431,9463,9479,
9511,9623,9679,9719,9743,9767,9791,9839,9871,9887,9967,10007,10039,10079,10103,
10111,10159,10223,10247,10271,10303,10343,10391,10399,10463,10559,10607,10631,10663,10687,
10799,10847,10903,11047,11087,11119,11159,11239,11279,11311,11383,11399,11423,11447,11471,
11519,11527,11743,11783,11807,11839,11887,11903,11927,11959,12071,12119,12143,12239,12263,
12391,12479,12487,12503,12527,12647,12671,12703,12743,12791,12823,12911,12919,12959,12967,
12983,13007,13063,13103,13127,13327,13367,13399,13463,13487,13567,13679,13687,13711,13759,
13799,13831,13903,13967,13999,14071,14087,14143,14159,14207,14303,14327,14423,14431,14447,
14479,14503,14519,14543,14591,14639,14759,14767,14783,14831,14879,15199,15263,15271,15287,
15359,15383,15439,15527,15559,15647,15671,15727,15767,15791,15919,15959,15991,16007,16063,
16087,16103,16127,16223,16231,16319,16447,16487,16519,16567,16631,16703,16823,16879,16943,
17159,17167,17207,17231,17327,17359,17383,17471,17519,17599,17783,17791,17807,17863,17903,
17959,18047,18119,18143,18191,18223,18287,18311,18367,18439,18583,18671,18679,18743,18839,
18911,18959,19031,19079,19087,19183,19231,19319,19391,19447,19471,19543,19559,19583,19687,
19727,19759,19919,19991

表 2: [EM73, Proposition 3.6 (ii)] をみたす素数 $p < 20000$

$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的ではないことがわかる素数 p
113,137,233,521,593,617,809,977,1033,1097,1129,1193,1289,1361,1489,
1553,1609,1777,1993,2129,2153,2281,2417,2441,2473,2609,2729,2833,2897,3049,
3089,3121,3209,3217,3433,3593,3761,3793,3881,4073,4241,4273,4297,4337,4457,
4561,4649,4657,4721,4817,4937,5009,5233,5297,5393,5417,5449,5521,5641,5737,
5897,6089,6217,6257,6353,6449,6473,6569,6577,6673,6737,6793,6833,6857,7121,
7177,7369,7433,7529,7537,7753,7793,7817,8009,8017,8081,8273,8297,8329,8369,
8521,8681,8689,8753,8849,8969,9041,9137,9161,9769,9833,9929,10289,10313,10321,
10889,10993,11057,11113,11177,11273,11497,11633,11657,11689,12041,12049,12073,12113,12329,
12433,12497,12553,12689,12713,12721,12809,13009,13297,13417,13513,13577,13649,13841,14033,
14057,14153,14249,14281,14321,14537,14633,14737,14929,15017,15217,15241,15313,15473,15497,
15569,15761,15817,15881,15889,16361,16369,16433,16529,16553,16649,16657,16937,17033,17041,
17257,17321,17393,17417,17449,17489,17609,17681,17737,18089,18097,18121,18257,18313,18353,
18481,19121,19249,19273,19433,19697,19753,19793,19889

最終的に，Lenstra [Len74] によって，有限アーベル群 G に対するネーター問題が肯定解を持つための必要十分条件が以下のように与えられた：

定理 14 (Lenstra [Len74, Main Theorem, Remark 5.7]).
k を体，G を有限アーベル群，k_{cyc} を k の代数閉包の中での最大円分拡大とする．$k \subset K \subset k_{\mathrm{cyc}}$ に対して，$\rho_K = \mathrm{Gal}(K/k) = \langle \tau_k \rangle$ は有限巡回群であるとする．体 k の標数とは異なる奇素数 p と $s \geq 1$ に対して，$\mathbb{Z}[\rho_K]$ のイデアル $\mathfrak{a}_K(p^s)$ を

$$\mathfrak{a}_K(p^s) = \begin{cases} \mathbb{Z}[\rho_K] & K \neq k(\zeta_{p^s}) \\ (\tau_K - t, p) & K = k(\zeta_{p^s}),\ \text{ただし } t \in \mathbb{Z} \text{ は } \tau_K(\zeta_p) = \zeta_p^t \text{ をみたす} \end{cases}$$

で定義し，$\mathfrak{a}_K(G) = \prod_{p,s} \mathfrak{a}_K(p^s)^{m(G,p,s)}$ とおく．ここで，$m(G,p,s) = \dim_{\mathbb{Z}/p\mathbb{Z}}(p^{s-1}G/p^sG)$ である．このとき，次の 3 つの条件は同値である：
(i) $k(G)$ は k 上有理的；
(ii) $k(G)$ は k 上安定有理的；
(iii) $k \subset K \subset k_{\mathrm{cyc}}$ に対して，$\mathfrak{a}_K(G)$ は $\mathbb{Z}[\rho_K]$ の単項イデアルで，k の標数が 2 でないときには，$k(\zeta_{r(G)})/k$ は巡回拡大となる．ここで，$r(G)$ は $r(G) \mid\mid \exp(G)$ なる 2 べきの整数．

特に，G が有限巡回群の場合には，次のように述べられる：

定理 15 (Lenstra [Len74, Corollary 7.2], [Len80, Proposition 2, Corollary 3] も参照).
$n \geq 1$ を整数とする．次の 4 つの条件は同値である：
(i) $\mathbb{Q}(C_n)$ は $\mathbb{Q}$ 上有理的；
(ii) すべての体 k に対して，$k(C_n)$ は k 上有理的；
(iii) すべての $p^s \mid\mid n$ に対して，$\mathbb{Q}(C_{p^s})$ は $\mathbb{Q}$ 上有理的；
(iv) $8 \nmid n$ かつすべての $p^s \mid\mid n$ に対して，ある $\alpha \in \mathbb{Z}[\zeta_{\varphi(p^s)}]$ が存在して，$N_{\mathbb{Q}(\zeta_{\varphi(p^s)})/\mathbb{Q}}(\alpha) = \pm p$.

ここから，$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的となるような素数 p の密度は 0 であることがわかる：

定理 16 (Lenstra [Len74, Corollary 7.6], [Len80, Proposition 6] も参照).
k を素体上有限生成な体とする．$k(C_p)$ が k 上有理的となる素数 p の集合 P_k のすべての素数の中でのディリクレ密度は 0 である．特に，$\pi(x)$ を $p \leq x$ なる素数の個数，$\pi^*(x)$ を $p \leq x$ かつ $\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的となる素数の個数とすれば，

$$\lim_{x \to \infty} \frac{\pi^*(x)}{\pi(x)} = 0.$$

$s \geq 2$ について，C_{p^s} に対する $\mathbb{Q}$ 上のネーター問題は完全に解決されている：

定理 17 (Lenstra [Len80, Proposition 4]).
p を素数，$s \geq 2$ を整数とする．$\mathbb{Q}(C_{p^s})$ が $\mathbb{Q}$ 上有理的 $\iff p^s \in \{2^2, 3^m, 5^2, 7^2 \mid m \geq 2\}$.

しかし，$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的かどうかは小さな素数 p に対しても一般にはよく分からない (定理 1). さらには，$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的となる素数 p が無限に存在するかどうかは未解決問題で，それを調べるのが論文 [Hos15] の一つのモチベーションとなっている．

また，$\mathbb{C}$ 上の非可換群 G に対するネーター問題 $\mathrm{Noe}(G/\mathbb{C})$ の研究は，近年，不分岐ブラウアー群，不分岐コホモロジーを用いて進展した．これについては，[CHKK10, Kan12, HKK13, BB13, Kan13, Kan14, Hos14, CHHK15, Hos16] などを見ていただきたい．

3 定理 1の証明

定理5 (定理6) から，ノルム方程式 $N_{F/\mathbb{Q}}(\alpha)=\pm p$ がある d 次中間体 $\mathbb{Q}\subset F\subset\mathbb{Q}(\zeta_{p-1})$ に対して整数解をもたなければ，$\mathbb{Q}(C_p)$ は $\mathbb{Q}$ 上有理的でないことがわかる．実際，Endo, Miyata [EM73, Appendix] は命題11と次数 $d=2,4$ の中間体 F を考察し，$\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的でない素数 $p<2000$ を調べている．我々の手法は，PARI/GP [PARI2] を用いて，$2\le d\le\varphi(p-1)$ なる d 次中間体 $\mathbb{Q}\subset F\subset\mathbb{Q}(\zeta_{p-1})$ のノルム方程式 $N_{F/\mathbb{Q}}(\alpha)=\pm p$ が整数解をもたないことを，以下のアルゴリズム NP(j,{GRH},{L}) によって確認できるようにし，それを $p\le 20000$ に対して適用することである．このアルゴリズムは，d が大きいとうまく動かないが，幸運なことに，多くの場合，$d\le 8$ なる d 次中間体 F を用いて $\mathbb{Q}(C_p)$ が $\mathbb{Q}$ 上有理的でないことが確認できた．詳しくは，論文 [Hos15] とその extended version [Hos-ex] (arXiv) を見ていただきたい．

```
NP(j,GRH=0,L=[1,1])=
{
 local(p,Z,G,C,d1,d2,B,S,k);
 p=prime(j);
 Z=znstar(p-1);
 G=matdiagonal(Z[2]);
 C=[];d1=[0,0];d2=[0,0];k=0;
 forsubgroup(H=G,p-1,C=concat(C,galoissubcyclo(Z,mathnf(concat(G,H)))));
 C=Set(C);
 if(GRH==0,
  for(i=L[1],#C,B=bnfinit(C[i]);S=bnfisintnorm(B,p);
   if(S==[],k=i;d1=[poldegree(C[i]),bnfcertify(B)];break)
  );
  for(i=L[2],#C,B=bnfinit(C[i]);S=bnfisintnorm(B,-p);
   if(S==[],if(i==k,d2=[poldegree(C[i]),1],
   d2=[poldegree(C[i]),bnfcertify(B)]);break)
  );
 );
 if(GRH==1,
  for(i=L[1],#C,B=bnfinit(C[i]);S=bnfisintnorm(B,p);
   if(S==[],d1=[poldegree(C[i]),1];break)
  );
  for(i=L[2],#C,B=bnfinit(C[i]);S=bnfisintnorm(B,-p);
   if(S==[],d2=[poldegree(C[i]),1];break)
  );
 );
if([d1[2],d2[2]]==[1,1],return([d1[1],d2[1],GRH]),return([Ratioal,GRH]))
}
```

NP(j,{GRH},{L}) は，j 番目の素数 p_j, GRH $=1,0$ とリスト $L=\{l_+,l_-\}$ に対して，GRH $=0$ $(=1)$ の場合には GRH (一般リーマン予想) を仮定せずに (仮定して)，i 番目の中間体 $\mathbb{Q}\subset K_{\pm,i}\subset\mathbb{Q}(\zeta_{p_j-1})$ $(i\ge l_\pm)$ に対してノルム方程式 $N_{K_{\pm,i}/\mathbb{Q}}(\alpha)=\pm p_j$ が整数解をもつかどうかを調べ，整数解がない i を見つければ，$[d_+,d_-,\mathrm{GRH}]$ $(d_\pm=[K_{\pm,i}:\mathbb{Q}])$ を返す．一方，最後の中間体，すなわち $\mathbb{Q}(\zeta_{p_j-1})$，までノルム方程式 $N_{\mathbb{Q}(\zeta_{p_j-1})/\mathbb{Q}}(\alpha)=\pm p_j$ が整数解を持てば，$d_\pm=$ Rational を返す．

2番目と3番目の入力 GRH, L は省略可能であり，省略された場合には，NP(j,{GRH},{L}) は GRH = 0, L = [1,1] として計算を行う．すなわち，GRH は仮定せず，すべての中間体 $\mathbb{Q} \subset K_{\pm,i} \subset \mathbb{Q}(\zeta_{p_j-1})$ $(i \geq 1)$ を調べる．

参考文献

[Bog88] F. A. Bogomolov, *The Brauer group of quotient spaces of linear representations*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987) 485–516, 688. English translation: Math. USSR-Izv. **30** (1988) 455–485.

[BB13] F. A. Bogomolov, C. Böhning, *Isoclinism and stable cohomology of wreath products*, Birational Geometry, Rational Curves, and Arithmetic, Springer New York, 2013, 57–76.

[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. 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.

[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 linearer Transformationen*, Nachr. Königl. Ges. Wiss. Göttingen (1915) 77–80.

[Fuk14] T. Fukuda, private communications, 2014.

[FK09] T. Fukuda, K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$*, Experiment. Math. **18** (2009) 213–222.

[FK10] T. Fukuda, K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II*, J. Théor. Nombres Bordeaux **22** (2010) 359–368.

[FK11] T. Fukuda, K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, III*, Int. J. Number Theory **7** (2011) 1627–1635.

[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.

[Hos05] A. Hoshi, *Multiplicative quadratic forms on algebraic varieties and Noether's problem for meta-abelian groups*, Ph. D. dissertation, Waseda University, 2005. http://dspace.wul.waseda.ac.jp/dspace/handle/2065/3004

[Hos-ex] A. Hoshi, *On Noether's problem for cyclic groups of prime order*, (extended version), arXiv:1402.3678.

[Hos14] A. Hoshi, *Rationality problem for quasi-monomial actions*, Algebraic number theory and related topics 2012, 203–227, RIMS Kôkyûroku Bessatsu **B51**, Res. Inst. Math. Sci. (RIMS), Kyoto, (2014).

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

[Hos16] A. Hoshi, *Birational classification of fields of invariants for groups of order* 128, J. Algebra **445** (2016) 394–432.

[HKK13] A. Hoshi, M. Kang, B. E. Kunyavskii, *Noether's problem and unramified Brauer groups*, Asian J. Math. **17** (2013) 689–714.

[HY] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*, arXiv:1210.4525, to appear in Mem. Amer. Math. Soc.

[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.

[Kan12] M. Kang, *Retract rational fields*, J. Algebra **349** (2012) 22–37.

[Kan13] M. Kang, *Frobenius groups and retract rationality*, Adv. Math. **245** (2013) 34–51.

[Kan14] M. Kang, *Bogomolov multipliers and retract rationality for semidirect products*, J. Algebra **397** (2014) 407–425.

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

[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.

[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.

[MM76] J. M. Masley, H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976) 248–256.

[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.

[Mil14a] J. C. Miller, private communications, 2014.

[Mil14b] J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arith. **164** (2014) 381–398.

[Mil15] J. C. Miller, *Real cyclotomic fields of prime conductor and their class numbers*, Math. Comp. **84** (2015) 2459–2469.

[Mor12] P. Moravec, *Unramified Brauer groups of finite and infinite groups*, Amer. J. Math. **134** (2012) 1679–1704.

[Noe13] E. Noether, *Rationale Funktionenkörper*, Jber. Deutsch. Math.-Verein. **22** (1913) 316–319.

[Noe17] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1917) 221–229.

[PARI2] PARI/GP, version `2.6.0` (alpha), Bordeaux, 2013. `http://pari.math.u-bordeaux.fr/`

[Swa69] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969) 148–158.

[Swa81] R. G. Swan, *Galois theory*, in Emmy Noether. A tribute to her life and work. Edited by James W. Brewer and Martha K. Smith, Monographs and Textbooks in Pure and Applied Mathematics, 69. Marcel Dekker, Inc., New York, 1981.

[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.

[Sal84] D. J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984) 71–84.

[Vos70] V. E. Voskresenskii, *On the question of the structure of the subfield of invariants of a cyclic group of 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*, Izv. Akad. Nauk SSSR Ser. Mat. (Russian) **35** (1971) 1037–1046. English translation: Math. USSR-Izv. **5** (1971) 1049–1056.

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

[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.

[Was97] L. C. Washington, *Introduction to cyclotomic fields*, Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

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/