On Noether's problem for cyclic groups of prime order

Dedicated to Professor Shizuo Endo on the Occasion of his 80th Birthday

By Akinari Hoshi

Department of Mathematics, Niigata University, 8050 Ikarashi 2-no-cho, Nishi-ku, Niigata 950-2181, Japan

(Communicated by Shigefumi Mori, M.J.A., Feb. 12, 2015)

Abstract: Let k be a field and G be a finite group acting on the rational function field $k(x_g \mid g \in G)$ by k-automorphisms $h(x_g) = x_{hg}$ for any $g, h \in G$. Noether's problem asks whether the invariant field $k(G) = k(x_g \mid g \in G)^G$ is rational (i.e. purely transcendental) over k. In 1974, Lenstra gave a necessary and sufficient condition to this problem for abelian groups G. However, even for the cyclic group C_p of prime order p, it is unknown whether there exist infinitely many primes p such that $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$. Only known 17 primes p for which $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$ are $p \leq 43$ and $p = 61, 67, 71$. We show that for primes $p < 20000$, $\mathbf{Q}(C_p)$ is not (stably) rational over $\mathbf{Q}$ except for affirmative 17 primes and undetermined 46 primes. Under the GRH, the generalized Riemann hypothesis, we also confirm that $\mathbf{Q}(C_p)$ is not (stably) rational over $\mathbf{Q}$ for undetermined 28 primes p out of 46.

Key words: Noether's problem; rationality problem; algebraic tori; class number; cyclotomic field.

1. Introduction. Let k be a field and K be an extension field of k. A field K is said to be *rational* over k if K is purely transcendental over k. A field K is said to be *stably rational* over k if the field $K(t_1, \ldots, t_n)$ is rational over k for some algebraically independent elements $t_1, \ldots, t_n$ over K. Let G be a finite group acting on the rational function field $k(x_g \mid g \in G)$ by k-automorphisms $h(x_g) = x_{hg}$ for any $g, h \in G$. We denote the fixed field $k(x_g \mid g \in G)^G$ by $k(G)$. Emmy Noether [27,28] asked whether $k(G)$ is rational (= purely transcendental) over k. This is called Noether's problem for G over k, and is related to the inverse Galois problem (see a survey paper of Swan [32] for details). Let C_n be the cyclic group of order n.

We define the following sets of primes:

$R = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}$ (rational cases),

$U = \{251, 347, 587, 2459, 2819, 3299, 4547, 4787, 6659, 10667, 12227, 14281, 15299, 17027, 17681, 18059, 18481, 18947\}$ (undetermined cases),

$X = \{59, 83, 107, 163, 487, 677, 727, 1187, 1459, 2663, 3779, 4259, 7523, 8837, 10883, 11699, 12659, 12899, 13043, 13183, 13523, 14243, 14387, 14723, 14867, 16547, 17939, 19379\}$ (not rational cases under the GRH)

with $\#R = 17$, $\#U = 18$, $\#X = 28$.

The aim of this paper is to show the following theorem.

Theorem 1.1. *Let $p < 20000$ be a prime. If* (i) *$p \notin R \cup U \cup X$ or* (ii) *under the GRH, the generalized Riemann hypothesis, $p \notin R \cup U$, then $\mathbf{Q}(C_p)$ is not stably rational over $\mathbf{Q}$.*

2. Noether's problem for abelian groups. We give a brief survey of Noether's problem for abelian groups. The reader is referred to Swan's survey papers [31] and [32].

Theorem 2.1 (Fischer [5], see also Swan [32, Theorem 6.1]). *Let G be a finite abelian group with exponent e. Assume that* (i) *either* char $k = 0$ *or* char $k > 0$ *with* char $k \nmid e$, *and* (ii) *k contains a primitive e-th root of unity. Then $k(G)$ is rational over k.*

Theorem 2.2 (Kuniyoshi [16,17,18]). *Let G be a p-group and k be a field with* char $k = p > 0$. *Then $k(G)$ is rational over k.*

Masuda [22,23] gave an idea to use a technique of Galois descent to Noether's problem for cyclic groups C_p of order p. Let ζ_p be a primitive p-th root of unity, $L = \mathbf{Q}(\zeta_p)$ and $\pi = \mathrm{Gal}(L/\mathbf{Q})$. Then, by

2010 Mathematics Subject Classification. Primary 11R18, 11R29, 12F12, 13A50, 14E08, 14F22.

doi: 10.3792/pjaa.91.39

Theorem 2.1, we have $\mathbf{Q}(C_p)=\mathbf{Q}(x_1,\dots,x_p)^{C_p}=(L(x_1,\dots,x_p)^{C_p})^{\pi}=L(y_0,\dots,y_{p-1})^{\pi}=L(M)^{\pi}(y_0)$ where $y_0=\sum_{i=1}^{p}x_i$ is π-invariant, M is free $\mathbf{Z}[\pi]$-module and π acts on $y_1,\dots,y_{p-1}$ by $\sigma(y_i)=\prod_{j=1}^{p-1}y_j^{a_{ij}}$, $[a_{ij}]\in GL_n(\mathbf{Z})$ for any $\sigma\in\pi$. Thus the field $L(M)^{\pi}$ may be regarded as the function field of some algebraic torus of dimension $p-1$ (see e.g. [37, Chapter 3]).

Theorem 2.3 (Masuda [22,23], see also [32, Lemma 7.1])**.**
(i) *M is projective $\mathbf{Z}[\pi]$-module of rank one*;
(ii) *If M is a permutation $\mathbf{Z}[\pi]$-module, i.e. M has a $\mathbf{Z}$-basis which is permuted by π, then $L(M)^{\pi}$ is rational over $\mathbf{Q}$. In particular, $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$ for $p\le 11$.*[*1)]

Swan [30] gave the first negative solution to Noether's problem by investigating a partial converse to Masuda's result.

Theorem 2.4 (Swan [30, Theorem 1], Voskresenskiĭ [34, Theorem 2])**.**
(i) *If $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$, then there exists $\alpha\in\mathbf{Z}[\zeta_{p-1}]$ such that $N_{\mathbf{Q}(\zeta_{p-1})/\mathbf{Q}}(\alpha)=\pm p$*;
(ii) (Swan) *$\mathbf{Q}(C_{47})$, $\mathbf{Q}(C_{113})$ and $\mathbf{Q}(C_{233})$ are not rational over $\mathbf{Q}$*;
(iii) (Voskresenskiĭ) *$\mathbf{Q}(C_{47})$, $\mathbf{Q}(C_{167})$, $\mathbf{Q}(C_{359})$, $\mathbf{Q}(C_{383})$, $\mathbf{Q}(C_{479})$, $\mathbf{Q}(C_{503})$ and $\mathbf{Q}(C_{719})$ are not rational over $\mathbf{Q}$.*

Theorem 2.5 (Voskresenskiĭ [35, Theorem 1])**.** *$\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$ if and only if there exists $\alpha\in\mathbf{Z}[\zeta_{p-1}]$ such that $N_{\mathbf{Q}(\zeta_{p-1})/\mathbf{Q}}(\alpha)=\pm p$.*

Hence if the cyclotomic field $\mathbf{Q}(\zeta_{p-1})$ has class number one, then $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$. However, it is known that such primes are exactly $p\le 43$ and $p=61,67,71$ (see Masley and Montgomery [21, Main theorem] or Washington's book [38, Chapter 11]).

Endo and Miyata [4] refined Masuda-Swan's method and gave some further consequences on Noether's problem when G is abelian (see also [36]).

Theorem 2.6 (Endo and Miyata [4, Theorem 2.3])**.** *Let G_1 and G_2 be finite groups and k be a field with* char $k=0$. *If $k(G_1)$ and $k(G_2)$ are rational* (*resp. stably rational*) *over k, then $k(G_1\times G_2)$ is rational* (*resp. stably rational*) *over k.*[*2)]

The converse of Theorem 2.6 does not hold for general k, see e.g. Theorem 2.10 below.

[*1)] The author [9, Chapter 5] generalized Theorem 2.3 (ii) to Frobenius groups F_{pl} of order pl with $l\mid p-1$ ($p\le 11$).

[*2)] Kang and Plans [15, Theorem 1.3] showed that Theorem 2.6 is also valid for any field k.

Theorem 2.7 (Endo and Miyata [4, Theorem 3.1])**.** *Let p be an odd prime and l be a positive integer. Let k be a field with* char $k=0$ *and $[k(\zeta_{p^l}):k]=p^{m_0}d_0$ with $0\le m_0\le l-1$ and $d_0\mid p-1$. Then the following conditions are equivalent*:
(i) *For any faithful $k[C_{p^l}]$-module V, $k(V)^{C_{p^l}}$ is rational over k*;
(ii) *$k(C_{p^l})$ is rational over k*;
(iii) *There exists $\alpha\in\mathbf{Z}[\zeta_{p^{m_0}d_0}]$ such that*

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

Further suppose that $m_0>0$. Then the above conditions are equivalent to each of the following conditions:
(i′) *For any $k[C_{p^l}]$-module V, $k(V)^{C_{p^l}}$ is rational over k*;
(ii′) *For any $1\le l'\le l$, $k(C_{p^{l'}})$ is rational over k.*

Theorem 2.8 (Endo and Miyata [4, Proposition 3.2])**.** *Let p be an odd prime and k be a field with* char $k=0$. *If k contains $\zeta_p+\zeta_p^{-1}$, then $k(C_{p^l})$ is rational over k for any l. In particular, $\mathbf{Q}(C_{3^l})$ is rational over $\mathbf{Q}$ for any l.*

Theorem 2.9 (Endo and Miyata [4, Proposition 3.4, Corollary 3.10])**.**
(i) *For primes $p\le 43$ and $p=61,67,71$, $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$*;
(ii) *For $p=5,7$, $\mathbf{Q}(C_{p^2})$ is rational over $\mathbf{Q}$*;
(iii) *For $l\ge 3$, $\mathbf{Q}(C_{2^l})$ is not stably rational over $\mathbf{Q}$.*

Theorem 2.10 (Endo and Miyata [4, Theorem 4.4])**.** *Let G be a finite abelian group of odd order and k be a field with* char $k=0$. *Then there exists an integer $m>0$ such that $k(G^m)$ is rational over k.*

Theorem 2.11 (Endo and Miyata [4, Theorem 4.6])**.** *Let G be a finite abelian group. Then $\mathbf{Q}(G)$ is rational over $\mathbf{Q}$ if and only if $\mathbf{Q}(G)$ is stably rational over $\mathbf{Q}$.*

Ultimately, Lenstra [19] gave a necessary and sufficient condition of Noether's problem for abelian groups.

Theorem 2.12 (Lenstra [19, Main Theorem, Remark 5.7])**.** *Let k be a field and G be a finite abelian group. Let $k_{\rm cyc}$ be the maximal cyclotomic extension of k in an algebraic closure. For $k\subset K\subset k_{\rm cyc}$, we assume that $\rho_K={\rm Gal}(K/k)=\langle\tau_k\rangle$ is finite cyclic. Let p be an odd prime with $p\ne$* char k *and $s\ge 1$ be an integer. Let $\mathfrak{a}_K(p^s)$ be a $\mathbf{Z}[\rho_K]$-ideal defined by*

$$\mathfrak{a}_K(p^s) = \begin{cases} \mathbf{Z}[\rho_K] & \text{if } K \neq k(\zeta_{p^s}) \\ (\tau_K - t, p) & \text{if } K = k(\zeta_{p^s}) \text{ where } t \in \mathbf{Z} \\ & \quad \text{satisfies } \tau_K(\zeta_p) = \zeta_p^t \end{cases}$$

and put $\mathfrak{a}_K(G) = \prod_{p,s} \mathfrak{a}_K(p^s)^{m(G,p,s)}$ *where* $m(G,p,s) = \dim_{\mathbf{Z}/p\mathbf{Z}}(p^{s-1}G/p^sG)$*. Then the following conditions are equivalent*:
(i) $k(G)$ *is rational over* k;
(ii) $k(G)$ *is stably rational over* k;
(iii) *for* $k \subset K \subset k_{\mathrm{cyc}}$*, the* $\mathbf{Z}[\rho_K]$*-ideal* $\mathfrak{a}_K(G)$ *is principal and if* char $k \neq 2$*, then* $k(\zeta_{r(G)})/k$ *is cyclic extension where* $r(G)$ *is the highest power of* 2 *dividing the exponent of* G.

Theorem 2.13 (Lenstra [19, Corollary 7.2], see also [20, Proposition 2, Corollary 3])**.** *Let* n *be a positive integer. Then the following conditions are equivalent*:
(i) $\mathbf{Q}(C_n)$ *is rational over* $\mathbf{Q}$;
(ii) $k(C_n)$ *is rational over* k *for any field* k;
(iii) $\mathbf{Q}(C_{p^s})$ *is rational over* $\mathbf{Q}$ *for any* $p^s \parallel n$;
(iv) $8 \nmid n$ *and for any* $p^s \parallel n$*, there exists* $\alpha \in \mathbf{Z}[\zeta_{\varphi(p^s)}]$ *such that* $N_{\mathbf{Q}(\zeta_{\varphi(p^s)})/\mathbf{Q}}(\alpha) = \pm p$.

Theorem 2.14 (Lenstra [19, Corollary 7.6], see also [20, Proposition 6])**.** *Let* k *be a field which is finitely generated over its prime field. Let* P_k *be the set of primes* p *for which* $k(C_p)$ *is rational over* k*. Then* P_k *has Dirichlet density* 0 *inside the set of all primes* p*. In particular,*

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

where $\pi(x)$ *is the number of primes* $p \leq x$*, and* $\pi^*(x)$ *is the number of primes* $p \leq x$ *for which* $\mathbf{Q}(C_p)$ *is rational over* $\mathbf{Q}$.

Theorem 2.15 (Lenstra [20, Proposition 4])**.** *Let* p *be a prime and* $s \geq 2$ *be an integer. Then* $\mathbf{Q}(C_{p^s})$ *is rational over* $\mathbf{Q}$ *if and only if* $p^s \in \{2^2, 3^m, 5^2, 7^2 \mid m \geq 2\}$.

However, even in the case $k = \mathbf{Q}$ and $p < 1000$, there exist primes p (e.g. 59, 83, 107, 251, etc.) such that the rationality of $\mathbf{Q}(C_p)$ over $\mathbf{Q}$ is undetermined (see Theorem 1.1). Moreover, we do not know whether there exist infinitely many primes p such that $\mathbf{Q}(C_p)$ is rational over $\mathbf{Q}$. This derives a motivation of this paper.

We finally remark that although $\mathbf{C}(G)$ is rational over $\mathbf{C}$ for any abelian group G by Theorem 2.1, Saltman [33] gave a p-group G of order p^9 for which Noether's problem has a negative answer over $\mathbf{C}$ using the unramified Brauer group $B_0(G)$. Indeed, one can see that $B_0(G) \neq 0$ implies that $\mathbf{C}(G)$ is not retract rational over $\mathbf{C}$, and hence not (stably) rational over $\mathbf{C}$.

Theorem 2.16. *Let* p *be any prime.*
(i) (Saltman [33]) *There exists a meta-abelian* p*-group* G *of order* p^9 *such that* $B_0(G) \neq 0$;
(ii) (Bogomolov [1]) *There exists a group* G *of order* p^6 *such that* $B_0(G) \neq 0$;
(iii) (Moravec [26]) *There exist exactly* 3 *groups* G *of order* 3^5 *such that* $B_0(G) \neq 0$;
(iv) (Hoshi, Kang and Kunyavskii [11]) *For groups* G *of order* p^5 $(p \geq 5)$*,* $B_0(G) \neq 0$ *if and only if* G *belongs to the isoclinism family* Φ_{10}*. There exist exactly* $1 + \gcd\{4, p-1\} + \gcd\{3, p-1\}$ *groups* G *of order* p^5 $(p \geq 5)$ *such that* $B_0(G) \neq 0$.

In particular, for the cases where $B_0(G) \neq 0$*,* $\mathbf{C}(G)$ *is not retract rational over* $\mathbf{C}$*. Thus* $\mathbf{C}(G)$ *is not* (*stably*) *rational over* $\mathbf{C}$.

The reader is referred to [3,12,11,2,13,14] and the references therein for more recent progress about unramified Brauer groups and retract rationality of fields.

3. Proof of Theorem 1.1. By Swan's theorem (Theorem 2.4), Noether's problem for C_p over $\mathbf{Q}$ has a negative answer if the norm equation $N_{F/\mathbf{Q}}(\alpha) = \pm p$ has no integral solution for some intermediate field $\mathbf{Q} \subset F \subset \mathbf{Q}(\zeta_{p-1})$ with $[F : \mathbf{Q}] = d$. When $d = 2$, Endo and Miyata gave the following result:

Proposition 3.1 (Endo and Miyata [4, Proposition 3.6])**.** *Let* p *be an odd prime satisfying one of the following conditions*:
(i) $p = 2q + 1$ *where* $q \equiv -1 \pmod 4$*,* q *is square-free, and any of* $4p - q$ *and* $q + 1$ *is not square*;
(ii) $p = 8q + 1$ *where* $q \not\equiv -1 \pmod 4$*,* q *is square-free, and any of* $p - q$ *and* $p - 4q$ *is not square. Then* $\mathbf{Q}(C_p)$ *is not rational over* $\mathbf{Q}$.

By Proposition 3.1 and case-by-case analysis for $d = 2$ and $d = 4$, Endo and Miyata confirmed that Noether's problem for C_p over $\mathbf{Q}$ has a negative answer for some primes $p < 2000$ ([4, Appendix]). The computational results of Proposition 3.1 for $p < 20000$ are also given in an extended version of the paper [10, Section 5].

In general, we may have to check all intermediate fields $\mathbf{Q} \subset F \subset \mathbf{Q}(\zeta_{p-1})$ with degree $2 \leq d \leq \varphi(p-1)$. However, fortunately, it turns out that for many cases, we can determine the rationality of $\mathbf{Q}(C_p)$ by some intermediate field F of low degree $d \leq 8$.

We make an algorithm using the computer software PARI/GP [29] for general $d \mid p-1$. We can prove Theorem 1.1 by function `NP(j,{GRH},{L})` of PARI/GP which may determine whether Noether's problem for C_{p_j} over $\mathbf{Q}$ has a positive answer for the j-th prime p_j unconditionally, i.e. without the GRH, if $\mathtt{GRH}=0$ (resp. under the GRH if $\mathtt{GRH}=1$). The code of the function `NP(j,{GRH},{L})` can be obtained in an extended version of the paper [10, Section 3].

`NP(j,{GRH},{L})` returns the list $[d_+, d_-, \mathtt{GRH}]$ for the j-th prime p_j and $L=\{l_+, l_-\}$ without the GRH if $\mathtt{GRH}=0$ (resp. under the GRH if $\mathtt{GRH}=1$) where $d_\pm=[K_{\pm,i}:\mathbf{Q}]$ if the norm equation $N_{K_{\pm,i}/\mathbf{Q}}(\alpha)=\pm p_j$ has no integral solution for some i-th subfield $\mathbf{Q}\subset K_{\pm,i}\subset \mathbf{Q}(\zeta_{p_j-1})$ with $i\geq l_\pm$, $d_\pm=$ `Rational` if the norm equation $N_{\mathbf{Q}(\zeta_{p_j-1})/\mathbf{Q}}(\alpha)=\pm p_j$ has an integral solution. The second and third inputs {`GRH`}, {`L`} may be omitted. If they are omitted, the function `NP` runs as $\mathtt{GRH}=0$ and $\mathtt{L}=[1,1]$, namely it works without the GRH and for all subfields $\mathbf{Q}\subset K_{\pm,i}\subset\mathbf{Q}(\zeta_{p_j-1})$ respectively.

We further define the set of primes:

$$\begin{aligned}
S_0 = \{&5987, 7577, 9497, 9533, 10457, 10937,\\
&11443, 11897, 11923, 12197, 12269, 13037,\\
&13219, 13337, 13997, 14083, 15077, 15683,\\
&15773, 16217, 16229, 16889, 17123, 17573,\\
&17657, 17669, 17789, 17827, 18077, 18413,\\
&18713, 18979, 19139, 19219, 19447, 19507,\\
&19577, 19843, 19973, 19997\},\\
S_1 = \{&11699, 12659, 12899, 13043, 14243, 14723,\\
&17939, 19379\}\subset X,\\
T_0 = \{&197, 227, 491, 1373, 1523, 1619, 1783, 2099,\\
&2579, 2963, 5507, 5939, 6563, 6899, 7187,\\
&7877, 14561, 18041, 18097, 19603\},\\
T_1 = \{&8837\}\subset X
\end{aligned}$$

with $\#S_0=40$, $\#S_1=8$, $\#T_0=20$, $\#T_1=1$.

We split the proof of Theorem 1.1 ($p<20000$) into three parts:

(i) $p\in S_0\cup S_1$;
(ii) $p\in T_0\cup T_1$;
(iii) $p\notin U\cup S_0\cup S_1\cup T_0\cup T_1$.

We will treat the cases (i), (ii), (iii) in Subsections 3.1, 3.2, 3.3 respectively.

3.1. Case $p\in S_0\cup S_1$. When $p_j\in S_0\cup S_1$, we should take a suitable list `L` for the function `NP(j,GRH,L)`. For $p_j\in S_0$ (resp. $p_j\in S_1$), we may take the following `L` in L_0 (resp. L_1) respectively:

```
L0=[[20,19],[1,3],[1,3],[9,1],[1,3],[1,3],
    [1,3],[1,3],[1,3],[3,1],[1,3],[9,3],
    [1,3],[1,3],[1,3],[1,3],[10,1],[4,1],
    [8,3],[1,3],[3,1],[1,3],[1,3],[1,3],
    [1,3],[1,3],[9,3],[1,3],[9,3],[9,3],
    [1,3],[1,3],[1,3],[1,3],[1,3],[1,3],
    [1,3],[1,3],[3,1],[9,3]];
L1=[[3,1],[3,1],[1,3],[1,3],[1,3],[41,1],
    [4,1],[3,1]];
```

Let $S_{0,j}$ (resp. $S_{1,j}$) be the index set $\{j\}$ of the set $S_0=\{p_j\}$ (resp. S_1).

```
S0j=[783,962,1177,1180,1279,1328,
     1380,1425,1428,1458,1467,1553,
     1572,1584,1651,1661,1761,1831,
     1840,1884,1886,1948,1974,2020,
     2028,2030,2041,2044,2072,2109,
     2136,2158,2171,2180,2205,2214,
     2221,2245,2258,2262];
S1j=[1404,1513,1535,1554,1673,1723,
     2057,2193];
```

For example, we take $p_j=5987\in S_0$ with $j=783$. Then `NP(783,0)` does not work well in a reasonable time. However, `NP(783,0,[20,19])` returns an answer in a few seconds:

```
gp > NP(783,0,[20,19])
[8, 8, 0]
```

Namely, the norm equation $N_{K_{+,i}/\mathbf{Q}}(\alpha)=p_j$ has no integral solution for some i-th subfield $\mathbf{Q}\subset K_{+,i}\subset\mathbf{Q}(\zeta_{p_j-1})$ with $i\geq 20$ and $[K_{+,i}:\mathbf{Q}]=8$, and $N_{K_{-,i}/\mathbf{Q}}(\alpha)=-p_j$ has no integral solution for some i-th subfield $\mathbf{Q}\subset K_{-,i}\subset\mathbf{Q}(\zeta_{p_j-1})$ with $i\geq 19$ and $[K_{-,i}:\mathbf{Q}]=8$.

We can confirm Theorem 1.1 for $p_j\in S_0$ (resp. $p_j\in S_1$) unconditionally, i.e. without the GRH, (resp. under the GRH) using `NP(j,GRH,L)` with $\mathtt{GRH}=0$ (resp. $\mathtt{GRH}=1$). For the actual computation, see an extended version of the paper [10, Subsection 3.1].

3.2. Case $p\in T_0\cup T_1$. When $p_j\in T_0\cup T_1$, because the computation of `NP(j,GRH)` may take more time and memory resources, we will do that by case-by-case analysis. We can confirm Theorem 1.1 for $p_j\in T_0$ (resp. $p_j\in T_1$) unconditionally (resp. under the GRH) using `NP(j,GRH)` with $\mathtt{GRH}=0$

(resp. GRH $=1$) as follows. In particular, for two primes $p_j = 5507$ with $j = 728$ and $p_j = 7187$ with $j = 918$, it takes about 55 days and 45 days respectively in our computation. See an extended version of the paper [10, Subsection 3.2] for the actual computation.

3.3. Case $p \notin U \cup S_0 \cup S_1 \cup T_0 \cup T_1$. When $p_j \notin U \cup S_0 \cup S_1 \cup T_0 \cup T_1$, we just apply the function `NP(j,GRH)`.

Let U_j (resp. X_j, $T_{0,j}$, $T_{1,j}$) be the index set $\{j\}$ of $U = \{p_j\}$ (resp. X, T_0, T_1).

```
Uj=[54,69,107,364,410,463,616,643,
    858,1302,1461,1676,1787,1963,2031,
    2070,2117,2155];
Xj=[17,23,28,38,93,123,129,195,232,386,
    526,584,953,1101,1323,1404,1513,
    1535,1554,1569,1602,1673,1685,
    1723,1741,1915,2057,2193];
T0j=[45,49,94,220,241,256,276,317,
    376,427,728,780,848,887,918,
    995,1707,2066,2074,2224];
T1j=[1101];
```

Then we can confirm Theorem 1.1 for $p_j \notin U \cup S_0 \cup S_1 \cup T_0 \cup T_1$ unconditionally (resp. under the GRH) when $p_j \notin X$ (resp. $p_j \in X$) using `NP(j,GRH)` with GRH $= 0$ (resp. GRH $= 1$). The actual results of `NP(j,GRH)` for primes $p_j < 20000$ ($j \le 2262$) in PARI/GP are described in an extended version of the paper [10, Section 4].

Proof of Theorem 1.1. Let $p < 20000$ be a prime. Theorem 1.1 follows from the result in Subsection 3.1 (resp. Subsection 3.2, Subsection 3.3) for $p \in S_0 \cup S_1$ (resp. $p \in T_0 \cup T_1$, $p \notin U \cup S_0 \cup S_1 \cup T_0 \cup T_1$). □

Added remark 3.2. From the view point of Theorems 2.4 and 2.5, Noether's problem for C_p over $\mathbf{Q}$ is closely related to Weber's class number problem (see e.g. Fukuda and Komatsu [6], [7], [8]). Actually, after this paper was posted on the arXiv, Fukuda announced to the author that he proved the non-rationality of $\mathbf{Q}(C_{59})$ over $\mathbf{Q}$ without the GRH. Independently, Lawrence C. Washington pointed out to John C. Miller that his methods for finding principal ideals of real cyclotomic fields in [24], [25] may be valid for $\mathbf{Q}(\zeta_{p-1})$ at least some small primes p. Indeed, Miller announced to the author that he proved that $\mathbf{Q}(C_p)$ is not rational over $\mathbf{Q}$ for $p = 59$ (resp. 251) without the GRH (resp. under the GRH) by using a similar technique as in [24], [25]. It should be interesting how to improve the methods of Fukuda and Miller for higher primes p.

Acknowledgments. The author thanks Profs. Shizuo Endo and Ming-chang Kang for valuable discussions. He also thanks Profs. Keiichi Komatsu, Takashi Fukuda and John C. Miller for helpful comments. This work was supported by JSPS KAKENHI Grant Number 25400027.

References

[1] F. A. Bogomolov, The Brauer group of quotient spaces of linear representations, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 3, 485–516, 688; translation in Math. USSR-Izv. **30** (1988), no. 3, 455–485.

[2] F. A. Bogomolov and C. Böhning, Isoclinism and stable cohomology of wreath products, in *Birational geometry, rational curves, and arithmetic*, Springer, New York, 2013, pp. 57–76.

[3] H. Chu, S.-J. Hu, M. Kang and B. E. Kunyavskii, Noether's problem and the unramified Brauer group for groups of order 64, Int. Math. Res. Not. IMRN **2010**, no. 12, 2329–2366.

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

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

[6] T. Fukuda and K. Komatsu, Weber's class number problem in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$, Experiment. Math. **18** (2009), no. 2, 213–222.

[7] T. Fukuda and K. Komatsu, Weber's class number problem in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$, II, J. Théor. Nombres Bordeaux **22** (2010), no. 2, 359–368.

[8] T. Fukuda and K. Komatsu, Weber's class number problem in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$, III, Int. J. Number Theory **7** (2011), no. 6, 1627–1635.

[9] 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

[10] A. Hoshi, On Noether's problem for cyclic groups of prime order, arXiv:1402.3678v2.

[11] A. Hoshi, M. Kang and B. E. Kunyavskii, Noether's problem and unramified Brauer groups, Asian J. Math. **17** (2013), no. 4, 689–713.

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

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

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

[15] M. Kang and B. Plans, Reduction theorems for Noether's problem, Proc. Amer. Math. Soc. **137**

(2009), no. 6, 1867–1874.

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

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

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

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

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

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

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

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

[24] J. C. Miller, Class numbers of totally real fields and applications to the Weber class number problem, Acta Arith. **164** (2014), no. 4, 381–398.

[25] J. C. Miller, Real cyclotomic fields of prime conductor and their class numbers, arXiv:1407.2373. (to appear in Math. Comp.).

[26] P. Moravec, Unramified Brauer groups of finite and infinite groups, Amer. J. Math. **134** (2012), no. 6, 1679–1704.

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

[28] E. Noether, Gleichungen mit vorgeschriebener Gruppe, Math. Ann. **78** (1917), no. 1, 221–229.

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

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

[31] 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, Dekker, New York, 1981.

[32] R. G. Swan, Noether's problem in Galois theory, in *Emmy Noether in Bryn Mawr* (*Bryn Mawr, Pa., 1982*), edited by B. Srinivasan and J. Sally, 21–40, Springer, New York, 1983.

[33] D. J. Saltman, Noether's problem over an algebraically closed field, Invent. Math. **77** (1984), no. 1, 71–84.

[34] V. E. Voskresenskiĭ, On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $Q(x_1, \cdots, x_n)$, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 366–375. English translation: Math. USSR-Izv. **4** (1970), no. 2, 371–380.

[35] V. E. Voskresenskiĭ, Rationality of certain algebraic tori, Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), 1037–1046. English translation: Math. USSR-Izv. **5** (1971), no. 5, 1049–1056.

[36] V. E. Voskresenskiĭ, Fields of invariants of abelian groups, Uspekhi Mat. Nauk **28** (1973), no. 4 (172), 77–102. English translation: Russian Math. Surveys **28** (1973), no. 4, 79–105.

[37] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ], Translations of Mathematical Monographs, 179, Amer. Math. Soc., Providence, RI, 1998.

[38] L. C. Washington, *Introduction to cyclotomic fields*, second edition, Graduate Texts in Mathematics, 83, Springer, New York, 1997.