Remarks on the $\lambda_p$-invariants of cyclic fields of degree $p$

by

MASATO KURIHARA (Tokyo)

0. Introduction. We fix an odd prime number $p$ throughout this paper. For a totally real field $k$, let $k_\infty/k$ denote the cyclotomic $\mathbb{Z}_p$-extension and $X_{k_\infty}$ denote the Galois group of the maximal unramified abelian pro-$p$ extension of $k_\infty$ over $k_\infty$. Greenberg’s conjecture predicts that $X_{k_\infty}$ is finite. In a series of papers [4], [12], [16], [2], [3], T. Fukuda, K. Komatsu, M. Ozaki, H. Taya, and G. Yamamoto intensively studied the case that $p = 3$ and $k$ is a cyclic cubic field with prime conductor.

In this paper, we consider a cyclic field $k$ of degree $p$ with prime conductor $\ell$. First of all, we will see that for such a field $k$, $X_{k_\infty}$ has a simple form (Theorem 1.3), and we will see what the finiteness of $X_{k_\infty}$ means (Remark 1.5). Next, we will develop the idea of Ozaki and Yamamoto [16], and obtain more general conditions which imply the finiteness of $X_{k_\infty}$ (see Propositions 1.7–1.10 in §1, cf. also Corollaries 1.4, 1.6). They are conditions on fields of degree $p$ over $\mathbb{Q}$, so it is not difficult to check them for numerical examples. In fact, these conditions are satisfied by many examples. (For $p = 3$, these conditions are satisfied for all $\ell < 10000$ except $\ell = 8677$ (cf. §4.1). For $p = 5$, these conditions are satisfied for all $\ell < 100000$ except three $\ell$’s (cf. §4.4.). (We do not use $p$-adic $L$-functions. For the relation with Tsuji’s criterion, see Remark 1.11.)

I would like to express my hearty thanks to Manabu Ozaki for valuable discussion with him on the topic of this paper. I also thank Toru Komatsu and Ryohei Takeuchi heartily for helping me to compute the numerical examples.

1. Results. Let $p$ be an odd prime number. Assume that $\ell$ is a rational prime such that $\ell \equiv 1 \pmod{p}$, and $k$ denotes the cyclic field of degree $p$ with conductor $\ell$. For an integer $n \geq 0$, we denote by $k_n$ (resp. $Q_n$) the $n$th layer of the cyclotomic $\mathbb{Z}_p$-extension $k_\infty/k$ (resp. $Q_\infty/Q$), namely $k_n$ (resp. $Q_n$) is the intermediate field such that $[k_n : k] = p^n$ (resp. $[Q_n : Q] = p^n$).

2000 Mathematics Subject Classification: Primary 11R23; Secondary 11R18.
Let $A_{k_n}$ be the $p$-Sylow subgroup of the ideal class group of $k_n$, and

$$X_{k_\infty} = \lim_{\leftarrow} A_{k_n}$$

the projective limit of $A_{k_n}$ with respect to the norm maps. So $X_{k_\infty}$ is isomorphic to the Galois group of the maximal unramified abelian pro-$p$ extension of $k_\infty$ over $k_\infty$. Since only one prime $\ell$ is ramified in $k/\mathbb{Q}$, by genus theory we have $A_\ell = 0$. But $X_{k_\infty}$ is nonzero, in general. By Ferrero–Washington’s theorem [1], $X_{k_\infty}$ is a finitely generated $\mathbb{Z}_p$-module whose rank is denoted by $\lambda$ (the Iwasawa $\lambda$-invariant). A famous conjecture by Greenberg asserts that $X_{k_\infty}$ is finite, namely $\lambda = 0$ ([6]).

By genus theory and a theorem of Iwasawa (cf. [8]), we know $X_{k_\infty} = 0$ if either $p \equiv 1 \pmod{\ell}$ holds (Theorem A in [16]). So in the following, we assume that $p \equiv 0 \pmod{\ell}$ and $\ell \equiv 1 \pmod{p^2}$. Namely, we assume that $p$ splits in $k/\mathbb{Q}$, and that $\ell$ splits in $\mathbb{Q}_1/\mathbb{Q}$.

Let $\mathcal{O}_{\mathbb{Q}_n}$ be the integer ring of $\mathbb{Q}_n$ and $E'_{\mathbb{Q}_n} = (\mathcal{O}_{\mathbb{Q}_n}[1/p])^\times$ be the group of $p$-units. For a prime $v$ of $\mathbb{Q}_n$ lying over $\ell$, we denote by $\kappa(v) = \mathcal{O}_{\mathbb{Q}_n}/v$ the residue field of $v$. Let $\mathcal{O}_{\mathbb{Q}_n}(v)$ be the localization of $\mathcal{O}_{\mathbb{Q}_n}$ at $v$, and $\partial_v : \mathcal{O}_{\mathbb{Q}_n}(v) \to \mathcal{O}_{\mathbb{Q}_n}(v)/v = \kappa(v)$ be the reduction map. Since $v$ is prime to $p$, $\partial_v$ induces a homomorphism

$$\partial_v : E'_{\mathbb{Q}_n} \to \kappa(v)^\times$$

where $\kappa(v)^\times$ is the multiplicative group of nonzero elements in $\kappa(v)$. Since $p$ divides the order of $\kappa(v)^\times$, $\kappa(v)^\times/(\kappa(v)^\times)^p$ is cyclic of order $p$. We consider the map

$$\Phi_n' : E'_{\mathbb{Q}_n} \to \bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p$$

which is induced by $x \mapsto (\partial_v x)$ where $v$ ranges over all primes of $\mathbb{Q}_n$ lying over $\ell$.

**Lemma 1.1.** Suppose that $\Phi_n'$ is not the zero map. Then, for any $m \geq n$, the dimension of the cokernel of $\Phi_n'$ (as an $p$-vector space) is equal to the dimension of the cokernel of $\Phi_n'_{\mathbb{Q}_n}$ (as an $p$-vector space).

We will give a proof of this lemma in §2.

**Definition 1.2.** Assume that there is $n \geq 0$ such that the image of $\Phi_n'$ is not zero. We define

$$\kappa = \dim \text{Cokernel} \left( \Phi_n' : E'_{\mathbb{Q}_n} \to \bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p \right)$$

where $v$ ranges over all primes of $\mathbb{Q}_n$ lying over $\ell$. If the image of $\Phi_n'$ is zero for all $n \geq 0$, we define $\kappa = \infty$.

By Lemma 1.1, this definition does not depend on the choice of $n$. Let $q$ be the number of the primes of $\mathbb{Q}_\infty$ lying over $\ell$. Then $\kappa < \infty$ implies $\kappa < q$
by definition. In general, numerical calculation of $\kappa$ is easy (cf. the proof of Lemma 1.1 in §2, and the examples in §4). We will define a similar map $\Phi_n$ in §2, and give a relation between $\kappa$ and $\Phi_n$. We believe this number $\kappa$ and the maps $\Phi_n, \Phi'_n$ play an important role in Iwasawa theory of $k$.

If $\kappa = 0$, the $\Phi'_n$’s are surjective for all $n \geq 0$, so from the surjectivity of $\Phi'_0$ and the fact that $E'_Q/(E'_Q)^p$ is generated by the image of $p$, we have $p \pmod{\ell} \not\in (\mathbb{F}_\ell^\times)^p$. So by our assumption, we always have $\kappa \geq 1$.

Let $\zeta_p$ be a primitive $p$th root of unity, and put

$$R = \mathbb{Z}_p[\zeta_p].$$

We also define $G$ and $\Gamma$ by

$$G = \text{Gal}(k_\infty/Q_\infty) = \text{Gal}(k/Q), \quad \Gamma = \text{Gal}(k_\infty/k) = \text{Gal}(Q_\infty/Q).$$

We take a generator $\sigma$ of $G$ and consider $N_G = 1 + \sigma + \cdots + \sigma^{p-1}$. Then, for $x \in X_{k_\infty}$, the map $N_G : X_{k_\infty} \to X_{k_\infty} (x \mapsto N_G(x))$ factors through $X_{Q_\infty} = \lim A_{Q_n} = 0$ (where $A_{Q_n}$ is the $p$-Sylow subgroup of the ideal class group of $Q_n$), so it is the zero map. Hence, by defining $\zeta_p x = \sigma x$, $X_{k_\infty}$ becomes an $R = \mathbb{Z}_p[\zeta_p]$-module. Since $\Gamma$ acts on $X_{k_\infty}$, $X_{k_\infty}$ is also a $\Lambda$-module where we put

$$\Lambda = R[[\Gamma]] = \mathbb{Z}_p[\zeta_p][[\Gamma]].$$

Throughout this paper, we identify $\Lambda$ with the formal power series ring $R[[T]]$ by identifying a generator $\gamma$ of $\Gamma$ with $1 + T$.

Let $\chi$ be a faithful character of $\text{Gal}(k/Q)$, namely $\chi$ is an injective homomorphism from $\text{Gal}(k/Q)$ to $\mathbb{Q}_p^\times$. We consider the $p$-adic $L$-function $L_p(s, \chi)$ of Kubota–Leopoldt, and the associated power series $G_\chi(T) \in R[[T]]$ such that $G_\chi(\kappa(1 - s) - 1) = L_p(s, \chi)$, where $\kappa : \Gamma \to \mathbb{Z}_p^\times$ is the cyclotomic character. By Ferrero–Washington’s theorem [1], $\zeta_p - 1$ does not divide $G_\chi(T)$. Let $f_\chi(T) \in R[T]$ be the distinguished polynomial of $G_\chi(T)$, so $G_\chi(T) = u(T)f_\chi(T)$ for some unit power series $u(T) \in R[[T]]^\times$ (cf. [19, §7.1]). By Kida’s formula ([11], [10]), the degree of $f_\chi(T)$ is $q - 1$ (recall that $q$ is the number of the primes of $Q_\infty$ lying over $\ell$).

**Theorem 1.3.** Let $p$ be a prime of $k$ lying over $p$, and $p_n$ be the prime of $k_n$ lying over $p$. We denote by $c_p$ the class of $(p_n)$ in $X_{k_\infty}$. Then there exist a polynomial $k(T) \in R[T]$ and an isomorphism

$$\Lambda/(f_\chi(T), Tk(T)) \cong X_{k_\infty}$$

of $\Lambda = R[[\Gamma]] = R[[T]]$-modules such that $k(T)$ modulo $(f_\chi(T), Tk(T))$ corresponds to $c_p$. If $\kappa < \infty$, we can take $k(T)$ to be a distinguished polynomial of degree $\kappa - 1$. If $\kappa = \infty$, we can take $k(T)$ such that $\zeta_p - 1$ divides $k(T)$. 
We will prove this theorem in §3. Suppose $\kappa < \infty$. Since $T$ is prime to $f_\chi(T)$, the greatest common divisor of $f_\chi(T)$ and $Tk(T)$ divides $k(T)$, so its degree is smaller than or equal to $\kappa - 1$. This implies that the $R$-rank of $X_{k_{\infty}}$ is $\leq \kappa - 1$. Since $\lambda$ is the $\Z_p$-rank of $X_{k_{\infty}}$, we have

**Corollary 1.4.** $\lambda \leq (p - 1)(\kappa - 1)$.

Ozaki and Yamamoto ([16, Theorem 1]) showed that if $\kappa = 1$, then $\lambda = 0$ in the case $p = 3$. The above corollary is a generalization of their result. (They also quoted the case $\kappa = 2$ of the above corollary as a theorem of the author in [16, Theorem 4].)

**Remark 1.5.** Theorem 1.3 tells us that $X_{k_{\infty}}$ is finite if and only if $f_\chi(T)$ is prime to $k(T)$. (Note that $k(T)$ is defined modulo $f_\chi(T)$.) By our experience of numerical computation (cf. §4), it seems to us that there is no relation between $k(T)$ and $f_\chi(T)$. If this is true, the probability that a root of $f_\chi(T) = 0$ happens to be a root of $k(T) = 0$ in an algebraic closure of $\Q_p$ which is a set of cardinality of the continuum would be very small, and almost zero.

Next, we will give some conditions which imply the finiteness of $X_{k_{\infty}}$, namely $\lambda = 0$. Ozaki and Yamamoto ([16, Theorem 2]) proved (in the case $p = 3$) that if $\kappa = 2$ and $f_\chi(T)$ is irreducible, we have $\lambda = 0$. When $\kappa < \infty$, the degree of $k(T)$ is $\kappa - 1$. Hence, Theorem 1.3 implies

**Corollary 1.6.** Suppose that $\kappa < \infty$. If $f_\chi(T)$ does not have a factor of degree $\leq \kappa - 1$, then $\lambda = 0$.

As we mentioned before Theorem 1.3, the degree of $f_\chi(T)$ is $q - 1$ where $q$ is the number of the primes of $\Q_\infty$ lying over $\ell$. On the other hand, by the definition of $\kappa$, we have $\kappa < q$, so $\kappa - 1$ is smaller than the degree of $f_\chi(T)$. Hence, if $f_\chi(T)$ is irreducible, $f_\chi(T)$ satisfies the condition in this corollary.

In this paper, we mainly study the case $\kappa = 2$. The following propositions will be proved in §3.

**Proposition 1.7.** Assume that $\kappa = 2$. If there is a subfield $F$ of $k_1$ such that $F \neq \Q_1$, $F \neq k$, $[F : \Q] = p$, and such that the prime ideal of $F$ lying over $p$ is principal, then $\lambda = 0$.

A similar result with the additional assumption $\ell \equiv 1 \pmod{p^3}$ (in the case $p = 3$) was proved in Ozaki and Yamamoto [16].

Let $R = \Z_p[\zeta_p]$ be as above, and $v_R$ be the normalized additive valuation of $R$, namely $v_R(\zeta_p - 1) = 1$. Ozaki and Yamamoto gave a condition which implies $\lambda = 0$, using a generalized Bernoulli number ([16, Corollary 3]). For the generalized Bernoulli number $B_{1,\chi\omega}^{-1}$, if $v_R(B_{1,\chi\omega}^{-1}) = 0$, then we have $X_{k_{\infty}} = 0$, and if $v_R(B_{1,\chi\omega}^{-1}) = 1$, then $f_\chi(T)$ is irreducible, and we also have $\lambda = 0$ ([16, Corollary 3]). We proceed to the case $v_R(B_{1,\chi\omega}^{-1}) = 2$. 

Proposition 1.8. Assume that $\kappa = 2$ and $v_R(B_{1,0^{-1}}) = 2$. If moreover $p^4$ does not divide the class numbers of all subfields of $k_1$ with degree $p$ over $\mathbb{Q}$, then we have $\lambda = 0$.

In order to deal with the case $\kappa > 2$, we also need the following propositions.

Proposition 1.9. Suppose that $\kappa \leq p$ and $\ell \equiv 1 \pmod{p^3}$. We also assume there are subfields $F$ and $F'$ of $k_1$ such that

(i) $F \neq \mathbb{Q}_1$, $F \neq k$, $F' \neq \mathbb{Q}_1$, $F' \neq k$, and $[F : \mathbb{Q}] = [F' : \mathbb{Q}] = p$,
(ii) the prime of $F$ over $\ell$ is principal, and the prime of $F'$ over $\ell$ is not principal, and
(iii) $p^4$ does not divide the class number of $F$.

Then $\lambda = 0$.

Proposition 1.10. Suppose that $\kappa = \infty$. Furthermore, we assume that there is a subfield $F \subset k_1$ with $F \neq k$ and $[F : \mathbb{Q}] = p$ such that $p^4$ does not divide the class number of $F$ and the prime over $p$ is not principal. Then $\lambda = 0$.

Remark 1.11 (Remark on Tsuji’s criterion). Kraft and Schoof [13] and independently Ichimura and Sumida [7] gave efficient criteria for Greenberg’s conjecture when the degree $[k : \mathbb{Q}]$ of the ground field $k$ is prime to $p$. After the work of Fukuda and Komatsu [3], recently T. Tsuji gave a good criterion [18] where she removed the assumption on $[k : \mathbb{Q}]$ in the criterion of Ichimura and Sumida. In the above notation, for each irreducible factor $P_i(T)$ of $f_\chi(T)$, her criterion presents a necessary and sufficient condition that $P_i(T)$ does not divide the characteristic power series $F_k(T)$ of $X_{k,\infty}$. Theorem 1.3 says that if $\kappa < \infty$ and $\deg P_i(T) > \kappa - 1$, then $P_i(T)$ does not divide $F_k(T)$. So we only have to check the factors $P_i(T)$ with degree $\leq \kappa - 1$. For example, if $\kappa = 2$, we only have to check the factors of degree 1. Further, it happens that some factors need not be checked (cf. Proposition 3.4). Numerical examples will be given in §4.

2. A homomorphism $\Phi_n$ and the invariant $\kappa$

Proof of Lemma 1.1. We define $M_n$ by

$M_n = \bigoplus \nu \ell, v \in P_0, \kappa(v)\chi^\nu / (\kappa(v)^\chi)^p$

where $\nu$ ranges over all primes of $\mathbb{Q}_n$ over $\ell$, and define $M_m$ similarly. Put $\Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Then both $M_n$ and $M_m$ are $\mathbb{F}_p[[\Gamma]]$-modules. We take a generator $\gamma$ of $\Gamma$ and identify $\mathbb{F}_p[[\Gamma]]$ with the formal power series ring $\mathbb{F}_p[[T]]$ by the correspondence $\gamma \leftrightarrow 1 + T$. Since $M_m$ is isomorphic to $\mathbb{F}_p[\text{Gal}(\mathbb{Q}_m/\mathbb{Q})/D]$ where $D$ is the decomposition group of $\ell$, it is generated by one element as an $\mathbb{F}_p[[T]]$-module. Taking a generator $x_m$, we write

$M_m = \mathbb{F}_p[[T]], x_m \simeq \mathbb{F}_p[[T]]/(T^{\#m})$
where \( q_m \) is the number of the primes of \( \mathbb{Q}_m \) lying over \( \ell \). Note that for any \( i \geq 0 \), we have a canonical isomorphism \( O_{\mathbb{Q}_i}/\ell O_{\mathbb{Q}_i} \simeq \bigoplus_{v|\ell, v \in P_{\mathbb{Q}_i}} \kappa(v) \).

Hence, the norm map from \( \mathbb{Q}_m \) to \( \mathbb{Q} \) induces a map \( N : M_m \to M_n \). Put \( x_n = N(x_m) \). Since \( N : M_m \to M_n \) is surjective, \( M_n \) is generated by \( x_n \) and we can write \( M_n = \mathbb{F}_p[[T]]x_n \simeq \mathbb{F}_p[[T]]/(T^{q_n}) \) where \( q_n \) is the number of the primes of \( \mathbb{Q}_n \) lying over \( \ell \).

On the other hand, as an \( \mathbb{F}_p[[T]] \)-module, \( E_{\mathbb{Q}_n}^p/(E_{\mathbb{Q}_n}^p) \) is generated by the class of \( \mathbb{Q}(\zeta_{p^{n+1}}) \) where \( \zeta_{p^{n+1}} \) is a primitive \( p^{n+1} \)st root of unity, and \( N_{\mathbb{Q}(\zeta_{p^{n+1}})}/\mathbb{Q} \) is the norm map from \( \mathbb{Q}(\zeta_{p^{n+1}}) \) to \( \mathbb{Q} \). So the map \( E_{\mathbb{Q}_m}^p/(E_{\mathbb{Q}_m}^p) \to E_{\mathbb{Q}_n}^p/(E_{\mathbb{Q}_n}^p) \) which is induced by the norm map is surjective. Hence, if the image of \( \Phi'_m \) is \( T^i \mathbb{F}_p[[T]]x_m \), then the image of \( \Phi'_n \) is \( T^i \mathbb{F}_p[[T]]x_n \). Note that \( i < q_n \) by our assumption. We have

\[
\dim \text{Cokernel}(\Phi'_n : E_{\mathbb{Q}_n}^p \to M_n) = \dim \text{Cokernel}(\Phi'_m : E_{\mathbb{Q}_m}^p \to M_m) = i.
\]

This completes the proof of the lemma.

Next, we will define a homomorphism \( \Phi_n \). Let \( E_{\mathbb{Q}_n} \) be the unit group of \( O_{\mathbb{Q}_n} \). Then \( \Phi'_n \) induces a homomorphism

\[
E_{\mathbb{Q}_n} \to \bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p.
\]

The norm map from \( \mathbb{Q}_n \) to \( \mathbb{Q} \) induces a map \( O_{\mathbb{Q}_n}/\ell O_{\mathbb{Q}_n} = \bigoplus_{v|\ell} \kappa(v) \to \mathbb{F}_\ell \). So we have a natural homomorphism

\[
\bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^p
\]

whose kernel is denoted by \( (\bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p)^0 \). Since the diagram

\[
\begin{array}{ccc}
E_{\mathbb{Q}_n} & \xrightarrow{\Phi'_n | E_{\mathbb{Q}_n}} & \bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p \\
\downarrow & & \downarrow \\
E_{\mathbb{Q}}/(E_{\mathbb{Q}})^p & \to & \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^p
\end{array}
\]

is commutative (where \( E_{\mathbb{Q}} \) is the unit group of \( \mathbb{Z} \) and the vertical arrows are induced by the norm maps) and \( E_{\mathbb{Q}}/E_{\mathbb{Q}}^p = 0 \), the image of the upper horizontal map is contained in \( (\bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p)^0 \). We denote this map by

\[
\Phi_n : E_{\mathbb{Q}_n} \to \left( \bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p \right)^0.
\]

**Lemma 2.1.** Suppose that \( \Phi'_n \) is not the zero map. Then the dimension of the cokernel of \( \Phi_n \) as an \( \mathbb{F}_p \)-vector space is equal to \( \kappa \).
Proof. We use the same notation as in the proof of Lemma 1.1. The above map \( \bigoplus_{v|\ell} \kappa(v)^{\times}/(\kappa(v)^{\times})^p \to \mathbb{F}_{\ell}^{\times}/(\mathbb{F}_{\ell}^{\times})^p \) is induced by the norm map \( M_n \to M_0 \). Using \( M_n = \mathbb{F}_p[[T]]x_n \) \((\simeq (\mathbb{F}_p[[T]])/(T^{q_n}))\) and \( M_0 = \mathbb{F}_p x_0 \), where \( x_0 \) is the image of \( x_n \) under the norm map, we see the above map is induced by \( T \mapsto 0 \). Hence, \( (\bigoplus_{v|\ell} \kappa(v)^{\times}/(\kappa(v)^{\times})^p)^0 = T\mathbb{F}_p[[T]]x_n \). Suppose \( \Phi_n'(E_{Q_n}) = T^i\mathbb{F}_p[[T]]x_n \). Since \( E_{Q_n}/E_{Q_n}^p \) is generated by cyclotomic units, \( T(E_{Q_n}/(E_{Q_n})^p) = E_{Q_n}/E_{Q_n}^p \), and we have \( \Phi_n(E_{Q_n}) = T^{i+1}\mathbb{F}_p[[T]]x_n \). Note that \( i + 1 \leq q_n \) by our assumption. Hence,

\[
\dim \text{Cokernel}(\Phi_n) = (i + 1) - 1 = i = \dim \text{Cokernel}(\Phi_n') = \kappa.
\]

This completes the proof of the lemma.

3. Proof of Theorem 1.3 and propositions in Section 1. We use the following lemma (cf. Lemma 2.1 in [14]).

**Lemma 3.1.** Let \( L/K \) be a cyclic extension of degree \( p \) of totally real number fields which is not unramified. Then we have an exact sequence

\[
\to \hat{H}^0(L/K, A_L) \to \hat{H}^0(L/K, E_L) \to \left( \bigoplus_{v \in P_{\text{ram}}(K)} \hat{H}^0(L_w/K_v, E_{L_w}) \right)^0 \\
\to H^1(L/K, A_L) \to H^1(L/K, E_L) \to \bigoplus_{v \in P_{\text{ram}}(K)} H^1(L_w/K_v, E_{L_w}) \\
\to \ldots
\]

Here, the notation is as follows. \( P_{\text{ram}}(K) \) is the set of all ramified (finite) primes of \( K \) in \( L/K \). For \( v \in P_{\text{ram}}(K) \), we denote by \( w \) the unique prime of \( L \) lying over \( K \). For a prime \( w \) of \( L \) (resp. \( v \) of \( K \)), \( L_w \) (resp. \( K_v \)) is the completion of \( L \) at \( w \) (resp. \( K \) at \( v \)). We denote by \( E_L \) (resp. \( E_{L_w} \)) the unit group of the integer ring of \( L \) (resp. \( L_w \)). \( A_L \) is the \( p \)-Sylow subgroup of the ideal class group of \( L \), and \( \hat{H}^0(\ast, \ast) \) is the Tate cohomology. We define an isomorphism \( \hat{H}^0(L_w/K_v, E_{L_w}) \simeq \mathbb{Z}/p\mathbb{Z} \) by

\[
\hat{H}^0(L_w/K_v, E_{L_w}) \simeq \hat{H}^0(L_w/K_v, L_w^\times) \simeq H^2(L_w/K_v, L_w^\times) \simeq \mathbb{Z}/p\mathbb{Z}
\]

where the last map is the invariant map of local class field theory. (The first two groups are isomorphic because \( L_w/K_v \) is totally ramified.) The group \( (\bigoplus_{v \in P_{\text{ram}}(K)} \hat{H}^0(L_w/K_v, E_{L_w}))^0 \) denotes the kernel of

\[
\bigoplus_{v \in P_{\text{ram}}(K)} \hat{H}^0(L_w/K_v, E_{L_w}) \simeq \bigoplus_{v \in P_{\text{ram}}(K)} \mathbb{Z}/p \xrightarrow{\Sigma} \mathbb{Z}/p
\]

where \( \Sigma \) is the map defined by the sum.

Proof of Theorem 1.3. Let \( \mathcal{M}_\infty/k_\infty \) be the maximal abelian pro-\( p \) extension of \( k_\infty \) unramified outside \( p \), and \( \mathcal{X}_{k_\infty} = \text{Gal}(\mathcal{M}_\infty/k_\infty) \) be its Galois
group. We denote by $U_{k\infty}$ the group of semi-local units, namely
\[ U_{k\infty} = \lim_{\to} \bigoplus_{p\mid \mathfrak{p}} U_{k_{n,pn}}^1 \]
where $\mathfrak{p}$ ranges over all primes of $k$ over $p$, and $p_n$ is the prime of $k_n$ over $p$, and $U_{k_{n,pn}}^1$ is the principal units of $k_{n,pn}$. By class field theory, we have an exact sequence
\[ U_{k\infty} \to X_{k\infty} \to X_{k\infty} \to 0. \]
Put $G = \text{Gal}(k_{\infty}/Q_{\infty}) = \langle \sigma \rangle$ and $N_G = 1 + \sigma + \cdots + \sigma^{p-1}$. If we denote by $X_{Q_{\infty}}$ the Galois group of the maximal abelian pro-$p$ extension of $Q_{\infty}$ unramified outside $p$ over $Q_{\infty}$, we have $X_{Q_{\infty}} = 0$. So multiplication by $N_G$ is zero on $X_{k\infty}$, and we can regard $X_{k\infty}$ as a $\Lambda = Z_p[\zeta_p][[T]]$-module. Hence, we have an exact sequence
\[ U_{k\infty}/N_GU_{k\infty} \to X_{k\infty} \to X_{k\infty} \to 0 \]
of $\Lambda$-modules.

We will show that $X_{k\infty}$ is generated by one element as a $\Lambda$-module. To see this, it is enough to see that the $\Gamma$-coinvariant $(X_{k\infty})_{\Gamma}$ is generated by one element as an $R = Z_p[\zeta_p]$-module. Let $G_{k,p}$ (resp. $G_{k,\infty,p}$) be the Galois group of the maximal extension of $k$ (resp. $k_{\infty}$) unramified outside $p$ over $k$ (resp. $k_{\infty}$), and $X_k$ be the Galois group of the maximal abelian pro-$p$ extension of $k$ unramified outside $p$ over $k$. From the inflation-restriction exact sequence
\[ 0 \to H^1(\Gamma, Q_p/Z_p) \to H^1(G_{k,p}, Q_p/Z_p) \to H^1(G_{k,\infty,p}, Q_p/Z_p)^{\Gamma} \to 0, \]
taking the Pontryagin dual, we have $(X_{k\infty})_{\Gamma} = \text{Ker}(X_k \to \Gamma)$. By class field theory (and $A_k = 0$ as we mentioned in §1), $X_k$ is isomorphic to $(\bigoplus_{p\mid \mathfrak{p}} U_{k_{p}}^1)/(\text{the image of } E_k \otimes Z_p)$ and $X_Q$ is isomorphic to $G = U_{Q_p}^1 \simeq Z_p$. Hence, $\text{Ker}(X_k \to \Gamma)$ is isomorphic to $\text{Ker}(\text{Norm} : \bigoplus_{p\mid \mathfrak{p}} U_{k_{p}}^1 \to U_{Q_p}^1)/(\text{the image of } E_k \otimes Z_p)$. Recall that $p$ splits in $k/Q$ and $U_{k_p}^1 = U_{Q_p}^1 \simeq Z_p$. Since $\text{Ker}(\text{Norm} : \bigoplus_{\mathfrak{p}\mid \mathfrak{p}} U_{k_{\mathfrak{p}}}^1 \to U_{Q_p}^1)$ is a free $R$-module of rank 1, $(X_{k_{\infty}})_{\Gamma} = \text{Ker}(X_k \to \Gamma)$ is generated by one element as an $R$-module. By Nakayama’s lemma, $X_{k_{\infty}}$ is generated by one element as a $\Lambda$-module.

We write $X_{k_{\infty}} \simeq \Lambda/I$. Since $X_{k_{\infty}}$ does not have a nontrivial finite $\Lambda$-submodule ([9, Theorem 18]), $I$ is principal. By the Iwasawa Main Conjecture proved by Mazur and Wiles [15], the characteristic ideal of $X_{k_{\infty}}$ is generated by $f_{X}(T)$. Hence, we have an isomorphism
\[ X_{k_{\infty}} \simeq \Lambda/(f_{X}(T)). \]

Let $Q_{p,\infty}/Q_p$ be the cyclotomic $Z_p$-extension of the $p$-adic field $Q_p$ and $Q_{p,n}$ be the $n$th layer. For any $n \geq 1$, we denote by $\zeta_{p^n}$ a primitive $p^n$th root of unity such that $\zeta_{p^n}^p = \zeta_p$ for all $n$. Put $\pi_n = N_{Q_p(\zeta_{p,n+1})/Q_p,n}(1 - \zeta_{p^n+1})$
where $N_{\mathbb{Q}_p}(\mathbb{Q}_p^*/\mathbb{Q}_p)$ is the norm map from $\mathbb{Q}_p(\mathbb{Q}_p^*/\mathbb{Q}_p)$ to $\mathbb{Q}_p$. Let $\pi = (\pi_n)$ be the projective system with respect to the norm maps. It is well known that the group of the local units $\mathcal{U}_{\mathbb{Q}_p, \infty} = \lim U_{\mathbb{Q}_p, n}^1$ is a free $\mathbb{Z}_p[[T]]$-module of rank 1, and is generated by $T\pi$ (where $T = \gamma - 1$ and $\gamma$ is the fixed generator of $\Gamma$).

We take a prime $p$ of $k$ lying over $p$, and fix it. Since $p$ splits in $k/\mathbb{Q}$, we have $k_p = \mathbb{Q}_p$, hence by the above remark, $\mathcal{U}_{k, \infty}/N_G\mathcal{U}_{k, \infty}$ is a free $\Lambda$-module of rank 1, and is generated by the class of $(T\pi, 1, \ldots, 1)$ (where we suppose the first component corresponds to $p$). On the other hand, if we identify $\mathcal{X}_{k, \infty}$ with a quotient of the projective limit of the idele groups of $k_n$, by class field theory, the class of the idele $(\pi, 1, 1, \ldots)$ (where we again suppose the first component corresponds to $p$) clearly maps to $c_p$ by the natural map $\mathcal{X}_{k, \infty} \to X_{k, \infty}$. Hence, $X_{k, \infty}$ can be written as

$$X_{k, \infty} \cong \Lambda/(f_{\mathcal{X}}(T), Tk(T))$$

where $k(T) \in \Lambda$ corresponds to $c_p$.

Next, we will see that

$$(1) \quad \kappa < \infty \iff \text{the class of } p_n \text{ in } (A_{k_n})_G \text{ is nonzero for sufficiently large } n.$$ 

Let $M/\mathbb{Q}_n$ be the maximal abelian extension which is unramified outside $\ell$ and whose Galois group has exponent $p$. Then, by class field theory, $\text{Gal}(M/\mathbb{Q}_n)$ is isomorphic to $\bigoplus_{\nu|\ell} \mathcal{O}_\nu^\times/(\mathcal{O}_\nu^\times)_p/\Phi_n(E_{\mathbb{Q}_n})$, and the prime $p_n$ of $\mathbb{Q}_n$ above $p$ splits in $M$ if and only if $\Phi_n^\prime(\pi_n) = 0$ in the above group, namely $\Phi_n^\prime(\pi_n) \in \Phi_n^\prime(E_{\mathbb{Q}_n})$. As we showed in the proof of Lemma 2.1, we have $\Phi_n^\prime(E_{\mathbb{Q}_n}) = T\Phi_n^\prime(E_{\mathbb{Q}_n}^\prime) = (T\Phi_n^\prime(\pi_n))$, hence $\Phi_n^\prime(\pi_n) \in \Phi_n^\prime(E_{\mathbb{Q}_n})$ is equivalent to $\Phi_n^\prime(\pi_n) = 0$. So, $p_n$ splits in $M$ if and only if $\Phi_n^\prime(\pi_n) = 0$.

On the other hand, $M$ is the maximal subfield of the $p$-Hilbert class field of $k_n$ such that $M/\mathbb{Q}_n$ is abelian. (Note that the inertia group of a prime above $\ell$ in $\text{Gal}(M/k_n)$ is cyclic, so $M/k_n$ is unramified everywhere.) We have an isomorphism $(A_{k_n})_G \simeq \text{Gal}(M/k_n)$. Hence, $p_n$ splits in $M$ if and only if the class of $p_n$ in $(A_{k_n})_G$ is zero. We saw in the last paragraph that this is equivalent to $\Phi_n^\prime(\pi_n) = 0$, hence we obtain the equivalence (1) (recall that the image of $\pi_n$ in $E_{\mathbb{Q}_n}^\prime/(E_{\mathbb{Q}_n}^\prime)_p$ is a generator).

For a general number field $K$, let $A_K$ denote the $p$-Sylow subgroup of the ideal class group of $K$, and $A'_K$ denote the quotient of $A_K$ by the subgroup generated by the classes of the primes lying over $p$. Namely, $A'_K = \text{Pic}(O_K[1/p])$.

We assume $\kappa < \infty$. Then $(A_{k_n})_G \simeq (\mathbb{F}_p)^{k-1}$. In fact, by the above equivalence (1), for sufficiently large $n$, the class of $p_n$ in $(A_{k_n})_G$ is nonzero. Since $\text{Gal}(k_n/k)$ acts trivially on $p_n$, the $\Lambda$-submodule $(c(p_n))$ of $(A_{k_n})_G$ generated by $c(p_n)$ has order $p$ (note again that $p((A_{k_n})_G) = 0$). Therefore,
it follows from \(\text{Gal}(M/\mathbb{Q}_n) \simeq (\mathbb{F}_p)^{\kappa+1}\) that \((A_{k_n})_G \simeq \text{Gal}(M/k_n) \simeq (\mathbb{F}_p)^{\kappa}\), and \((A'_{k_n})_G \simeq (\mathbb{F}_p)^{\kappa-1}\).

We define

\[X'_{k_\infty} = \lim_{\rightarrow \nu} A'_{k_n}\]

where the projective limit is taken with respect to the norm maps. Since \(c_p\) corresponds to \(k(T)\), we have

\[X'_{k_\infty} \xrightarrow{\cong} \Lambda/(f_\chi(T), k(T)).\]

On the other hand, \((A'_{k_n})_G \simeq (\mathbb{F}_p)^{\kappa-1}\) for all sufficiently large \(n\) implies \((X'_{k_\infty})_G = X'_{k_\infty}/(\zeta_p - 1)X'_{k_\infty} \simeq (\mathbb{F}_p)^{\kappa-1}\). Since \(\kappa - 1 = q - 1 = \deg(f_\chi(T))\), \(k(T)\) can be written as \(k(T) = uT^{\kappa-1} \mod (\zeta_p - 1, T^\kappa)\) for some unit \(u \in \mathbb{F}_p^\times\). So, by the Weierstrass preparation theorem, we can write \(k(T) = u(T)h(T)\) where \(u(T)\) is a unit power series and \(h(T)\) is a distinguished polynomial of degree \(\kappa - 1\). By changing the isomorphism \(\Lambda/(f_\chi(T), Tk(T)) \simeq X_{k_\infty}\) suitably, we may assume \(k(T)\) is a distinguished polynomial of degree \(\kappa - 1\).

Next, suppose that \(\kappa = \infty\). By the equivalence (1), the classes of \(p_n\) in \((A_{k_n})_G\) are zero for all \(n\). Hence, the image of \(c_p\) is zero in \((X_{k_\infty})_G = X_{k_\infty}/(\zeta_p - 1)X_{k_\infty}\). So, \(k(T)\) can be taken such that \(\zeta_p - 1\) divides \(k(T)\). This completes the proof of Theorem 1.3.

Before proceeding to the proofs of propositions, we will prepare some fundamental facts.

For a general number field \(K\), we denote by \(G_{K,p}\) the Galois group of the maximal extension of \(K\) which is unramified outside \(p\) over \(K\), and consider the Galois cohomology group

\[H^2_K = H^2(G_{K,p}, \mathbb{Z}_p(1))\]

where \(\mathbb{Z}_p(1) = \lim_{\rightarrow \nu} \mu_{p^n}\) (\(\mu_{p^n}\) is the group of \(p^n\)th roots of unity). Since \(H^2_K\) is the same as the etale cohomology \(H^2(\text{Spec} \mathcal{O}_K[1/p]_{\text{et}}, \mathbb{Z}_p(1))\), by the Kummer sequence we obtain

**Lemma 3.2.** We have an exact sequence

\[0 \to A'_{k} \to H^2_{k} \to B(\mathcal{O}_K[1/p]) \to 0\]

where \(B(\mathcal{O}_K[1/p]) = \lim_{\rightarrow \nu} \text{Br}(\mathcal{O}_K[1/p]/p^n) = (\bigoplus_{v|p} \mathbb{Z}_p)^0\) is the Tate module of the Brauer group of \(\mathcal{O}_K[1/p]\).

Since \(p\) is decomposed in \(k/\mathbb{Q}\), and every prime of \(k\) over \(p\) is totally ramified in \(k_n/k\), \(B(\mathcal{O}_{k_n}[1/p]) = (\bigoplus_{p|\nu} \mathbb{Z}_p)^0\) is a free \(R\)-module of rank 1 for all \(n \geq 0\). So by Lemma 3.2 we have an exact sequence

\[0 \to A'_{k_n} \to H^2_{k_n} \to R \to 0\]
for all \( n \geq 0 \) where \( \bigoplus_{p|p} \mathbb{Z}_p \) was denoted by \( R \). We define \( H^2_{k_\infty} \) to be the projective limit of \( H^2_{k_n} \) with respect to the corestriction maps. Put \( \Gamma_n = \text{Gal}(k_\infty/k_n) \). Since the \( p \)-cohomological dimension of \( G_{k_n} \) is 2, the corestriction map induces an isomorphism \( (H^2_{k_\infty})_{\Gamma_n} \cong H^2_{k_n} \) ([17, Chap. I, Prop. 18]). Taking the projective limit of the above exact sequence, we have an exact sequence

\[
0 \to X'_{k_\infty} \to H^2_{k_\infty} \to R \to 0
\]

(note that the norm map is surjective on each term). From \( (H^2_{k_\infty})_{\Gamma} \cong H^2_k \cong R \) (note that \( A'_k = 0 \)), we know that \( H^2_{k_\infty} \) is generated by one element as a \( \Lambda \)-module. We write \( H^2_{k_\infty} \cong \Lambda/I \). If we use this isomorphism, \( H^2_{k_\infty} \to R \) is induced by \( T \mapsto 0 \). Further, by Theorem 1.3 we have \( X'_{k_\infty} \cong \Lambda/(f_\chi(T), k(T)) \), hence the above exact sequence implies that \( I = (Tf_\chi(T), Tk(T)) \). Namely,

\[
H^2_{k_\infty} \cong \Lambda/(Tf_\chi(T), Tk(T)).
\]

We consider the subfield \( k_1 \) which is the first layer of \( k_\infty/k \). From the exact sequence

\[
0 \to A'_{k_1} \to H^2_{k_1} \to R \to 0,
\]

\( A'_{k_1} \) is isomorphic to the kernel of

\[
(H^2_{k_\infty})_{\Gamma_1} = \Lambda/(Tf_\chi(T), Tk(T), (1 + T)^p - 1) \to R.
\]

Hence, if we put \( \varphi(T) = ((1 + T)^p - 1)/T \), we have an isomorphism

\[
(2) \quad A'_{k_1} \cong \Lambda/(f_\chi(T), k(T), \varphi(T)).
\]

Suppose that \( F \) is a subfield of \( k_1 \) such that \( F \neq \mathbb{Q}_1, F \neq k \), and \([F : \mathbb{Q}] = p \). Then both \( p \) and \( \ell \) ramify in \( F/\mathbb{Q} \). Put \( G = \text{Gal}(k_\infty/F) \). Taking \( G \)-coinvariants, we have an exact sequence

\[
0 \to (X'_{k_\infty})_G \to (H^2_{k_\infty})_G \to R_G \to 0.
\]

(Recall that in the above exact sequence \( R = \bigoplus_{p|p} \mathbb{Z}_p \), on which \( G \) acts naturally. Since \( p \) is ramified in \( F \), the \( G \)-invariant part \( R_G \) is trivial.) Since \( G_{F,p} \) is also of \( p \)-cohomological dimension 2, the \( G \)-coinvariant of \( H^2_{k_\infty} \) is isomorphic to \( H^2_F \). Since \( B(O_F[1/p]) = 0 \), we have

\[
(H^2_{k_\infty})_G \cong H^2_F \cong A'_F.
\]

It is easy to see that \( R_G \cong R/(\zeta_p - 1) \cong \mathbb{Z}/p\mathbb{Z} \). Hence, the above exact sequence and the isomorphism \( (H^2_{k_\infty})_G \cong A'_F \) imply the exact sequence

\[
(3) \quad 0 \to (X'_{k_\infty})_G \to A'_F \to \mathbb{Z}/p\mathbb{Z} \to 0.
\]

For \( F \), we also need the following. Let \( p_F \) (resp. \( \mathcal{L}_F \)) be the prime of \( F \) lying over \( p \) (resp. \( \ell \)), and \([p_F] \) (resp. \( [\mathcal{L}_F] \)) the class of \( p_F \) (resp. \( \mathcal{L}_F \)) in \( A_F \).

**Lemma 3.3.** At least either \([p_F] \neq 0 \) or \([\mathcal{L}_F] \neq 0 \).
Proof. We apply Lemma 3.1 to $F/\mathbb{Q}$. The primes ramified in $F/\mathbb{Q}$ are $p$ and $\ell$. By Lemma 3.1 we have an exact sequence

$$H^1(F_p/F, E_{F_p}) \oplus H^1(F_{\mathcal{L}/F}, E_{F_{\mathcal{L}/F}}) \to \widehat{H}^0(F/\mathbb{Q}, A_F) \to \widehat{H}^0(F/\mathbb{Q}, E_F).$$

The exact sequence $0 \to E_{F_p} \to F_{p_F} \to \mathbb{Z} \to 0$ yields a natural isomorphism $H^1(F_p/F, E_{F_p}) \cong \mathbb{Z}/p\mathbb{Z}$ by Hilbert Theorem 90. By the definition of the homomorphisms in Lemma 3.1, $H^1(F_p/F, E_{F_p}) \to \widehat{H}^0(F/\mathbb{Q}, A_F)$ is induced by the reciprocity map $F_p^\times \to D_{p_F} \subset A_F$ ($D_{p_F}$ is the decomposition group where we identified $A_F$ with the Galois group of the $p$-Hilbert class field of $F$), so the image of $1 \in \mathbb{Z}/p\mathbb{Z} \cong H^1(F_p/F, E_{F_p})$ in $\widehat{H}^0(F/\mathbb{Q}, A_F) = A_F^{\text{Gal}(F/\mathbb{Q})}$ is $[p_F]$. Similarly we deduce that the image of $1$ in $H^1(F_{\mathcal{L}/F}/\mathbb{Q}, E_{\mathcal{L}/F}) \cong \mathbb{Z}/p\mathbb{Z}$ is $[\mathcal{L}_F]$. Since $\widehat{H}^0(F/\mathbb{Q}, E_F) = E_F/\mathbb{N}_F/\mathbb{Q}E_F = 0$, the above exact sequence tells us that $A_F^{\text{Gal}(F/\mathbb{Q})}$ is generated by $[p_F]$ and $[\mathcal{L}_F]$. As in the proof of Theorem 1.3, we have $(A_F)^{\text{Gal}(F/\mathbb{Q})} = \mathbb{Z}/p\mathbb{Z}$, so $A_F^{\text{Gal}(F/\mathbb{Q})}$ is also of order $p$. Hence, at least one of $[p_F]$ and $[\mathcal{L}_F]$ is nonzero in $A_F$.

Proof of Proposition 1.7. Suppose that $\kappa = 2$. So we may assume $k(T) = T - \alpha$, and $v_R(\alpha) > 0$. Assume further that $X_{k_{\infty}}$ is infinite. Then we must have $f_X(\alpha) = 0$, and by the isomorphism (2) we have

$$A'_{k_1} \cong R/\varphi(\alpha).$$

Recall that $\text{Gal}(k_1/k)$ is generated by $\gamma$ and $\text{Gal}(k_1/\mathbb{Q}_1)$ is generated by $\sigma$. We suppose that $F$ corresponds to the subgroup $\langle \gamma\sigma^i \rangle$ of $\text{Gal}(k_1/\mathbb{Q}_1) = \text{Gal}(k_1/k) \times \text{Gal}(k_1/\mathbb{Q}_1)$ for some $i$ such that $0 < i < p$. We have

$$(X'_{k_{\infty}})_{\mathcal{S}} = A/(T - \alpha, (1 + T) - \zeta_p^{-i}) = R/(\zeta_p^{-i} - 1 - \alpha).$$

Hence, the exact sequence (3) yields an exact sequence

$$0 \to R/(\zeta_p^{-i} - 1 - \alpha) \to A'_{F} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Put $c_F = v_R(\zeta_p^{-i} - 1 - \alpha)$. Since the norm map $X'_{k_{\infty}} \to A'_{k_1}$ is surjective, the image of the norm map $A'_{k_1} \to A'_{F}$ coincides with the image of $(X'_{k_{\infty}})_{\mathcal{S}} = R/(\zeta_p^{-i} - 1 - \alpha) \to A'_{F}$, hence it is of order $p^{c_F}$.

We take a prime $\mathcal{L}$ of $k_1$ lying over $\ell$. Since $\mathcal{L}$ is totally ramified in $k_1/\mathbb{Q}_1$, $\sigma$ acts on $\mathcal{L}$ trivially. Writing $[\mathcal{L}]_{A'_{k_1}}$ for the class of $\mathcal{L}$ in $A'_{k_1}$, we have $(\zeta_p - 1)[\mathcal{L}]_{A'_{k_1}} = 0$. Hence, if we fix an isomorphism

$$A'_{k_1} \cong R/(\varphi(\alpha)) = R/(\langle (\zeta_p - 1)^c \rangle)$$

where $c = v_R(\varphi(\alpha))$, then $[\mathcal{L}]_{A'_{k_1}}$ corresponds to $a(\zeta_p - 1)^{c-1}$ for some $a \in R$. Since $c = v_R(\varphi(\alpha)) = v_R(\prod_{j=1}^{\infty}(1 + \alpha - \zeta_p^j))$, we have $c > c_F$. This shows
that the norm of $[\mathcal{L}]_{A'_{k_1}}$ in $A'_F$ is trivial. Since $\mathcal{L}_F$ is decomposed in $k_1/F$, $N_{k_1/F}(\mathcal{L}) = \mathcal{L}$ and the class of $\mathcal{L}_F$ in $A'_F$ is zero.

Note that by our assumption $[p_F] = 0$ in $A_F$, we have $A_F = A'_F$. So we get $[\mathcal{L}_F] = [p_F] = 0$ in $A_F$, which contradicts Lemma 3.3. Hence, $X'_{k_\infty}$ is finite, and we have $\lambda = 0$. This completes the proof of Proposition 1.7.

For the proof of Proposition 1.8, we need the following.

**Proposition 3.4.** We assume $\kappa = 2$. Suppose that $\alpha \in R$ is an element with $v_R(\alpha) = 1$. If $\ell^4$ does not divide the class numbers of all subfields of $k_1$ with degree $\ell$ over $\mathbb{Q}$, then $T - \alpha$ does not divide a generator of the characteristic ideal $\text{char}_A(X_{k_{\infty}})$.

**Proof.** Assume that $T - \alpha$ divides a generator of the characteristic ideal of $X_{k_{\infty}}$. Then $X_{k_{\infty}}$ is infinite, and $T - \alpha$ divides both $f_\chi(T)$ and $k(T)$. So $k(T)$, which we take to be distinguished, should be $k(T) = T - \alpha$ because $\kappa = 2$.

Since $v_R(\alpha) = 1$, there is an integer $i$ such that $0 < i < \ell$ and $\alpha/(\zeta_\ell - 1) \equiv -i \pmod{\zeta_\ell - 1}$. Hence, we have $v_R(\alpha - (\zeta_\ell^{-i} - 1)) > 1$. Let $F$ be the subfield of $k_1$ corresponding to the subgroup $\langle \gamma \sigma^i \rangle$ as in the proof of Proposition 1.7. Then, the exact sequence (3) yields an exact sequence

$$0 \to R/(\zeta_\ell^{-i} - 1 - \alpha) \to A'_F \to \mathbb{Z}/p\mathbb{Z} \to 0.$$ 

By our assumption on $i$, we have $#R/(\alpha - (\zeta_\ell^{-i} - 1)) \geq p^2$, hence $#A'_F \geq p^3$.

On the other hand, since $\ell^4$ does not divide $#A_F$, we must have $#A_F = #A'_F = p^3$. This shows that the prime $p_F$ of $F$ lying over $\ell$ is principal, and contradicts Proposition 1.7. The proof of Proposition 3.4 is complete.

**Proof of Proposition 1.8.** We may assume $k(T) = T - \alpha$. First, suppose $v_R(\alpha) \geq 2$, namely $v_R(k(0)) \geq 2$. Since $v_R(f_\chi(p)) = v_R(B_{1, \chi \omega^{-1}}) = 2$, it follows from $\deg f_\chi(T) = q - 1 \geq 2$ and $v_R(p) = p - 1 \geq 2$ that $v_R(f_\chi(0)) = v_R(f_\chi(p)) = 2$. Hence, $v_R(k(0)) \geq v_R(f_\chi(0)) = 2$. Since both $k(T)$ and $f_\chi(T)$ are distinguished polynomials and $\deg f_\chi(T) > \deg k(T)$, $k(T)$ does not divide $f_\chi(T)$. Thus, we obtain $\lambda = 0$.

If $v_R(\alpha) < 2$, we have $v_R(\alpha) = 1$. Then, by Proposition 3.4, $k(T)$ does not divide a characteristic power series of $X_{k_{\infty}}$. Hence, we have $\lambda = 0$. This completes the proof.

**Proof of Proposition 1.9.** Suppose that $F$ corresponds to the subgroup $\langle \gamma \sigma^i \rangle$ as in the proof of Proposition 1.7. Let $\mathcal{L}_F$ (resp. $p_F$) be the prime of $F$ lying over $\ell$ (resp. $p$). By our assumption (ii) and Lemma 3.3, $p_F$ is not principal. So by our assumption (iii), we have $#A'_F \leq p^2$. By the exact sequence (3), this implies that $\min(v_R(f_\chi(\zeta_\ell^{-i} - 1)), v_R(k(\zeta_\ell^{-i} - 1))) \leq 1$. We may assume this value is 1.
First, suppose \( v_R(f_\chi(\zeta_p^{-i} - 1)) = 1 \). Then \( f_\chi(T - (\zeta_p^{-i} - 1)) \) is an Eisenstein polynomial, so \( f_\chi(T) \) is irreducible. Since \( \deg k(T) = \kappa - 1 < \deg f_\chi(T) = q - 1 \), we get the finiteness of \( X_{k,\infty} \simeq \Lambda/(f_\chi(T), Tk(T)) \).

Next, suppose \( v_R(k(\zeta_p^{-i} - 1)) = 1 \). Then, by the same method, \( k(T) \) is irreducible. Assume that \( X_{k,\infty} \) is infinite. Then \( k(T) \) must divide \( f_\chi(T) \), and we have \( X_{k,\infty}' \simeq \Lambda/(k(T), \varphi_2(T)) \). Put \( \varphi(T) = ((1 + T)^p - 1)/T \) and \( \varphi_2(T) = ((1 + T)^p - 1)/T \). By the isomorphism (2), we have \( A'_{k_1} \simeq \Lambda/(k(T), \varphi(T)) \), and by the same method, we have \( A'_{k_2} \simeq \Lambda/(k(T), \varphi_2(T)) \). The natural map \( A'_{k_1} \to A'_{k_2} \) corresponds to the multiplication by \( \varphi_2(T)/\varphi(T) \). So it is injective because \( k(T) \) is irreducible and prime to \( \varphi_2(T) \).

Let \( \mathcal{L}_{k_1} \) (resp. \( p_{k_1} \)) be a prime of \( k_1 \) lying over \( \ell \) (resp. \( p \)). We denote by \( [\mathcal{L}_{k_1}]_{A_{k_1}} \) (resp. \( [p_{k_1}]_{A_{k_1}} \)) the class of \( \mathcal{L}_{k_1} \) (resp. \( p_{k_1} \)) in \( A_{k_1} \), and by \( [\mathcal{L}_{k_1}]_{A'_{k_1}} \) the class of \( \mathcal{L}_{k_1} \) in \( A'_{k_1} \). We will show that \( [\mathcal{L}_{k_1}]_{A'_{k_1}} \neq 0 \).

We denote by \( p_{F'} \) (resp. \( \mathcal{L}_{F'} \)) the prime of \( F' \) over \( p \) (resp. \( \ell \)). Suppose first that \( [p_{F'}]_{A_{F'}} = 0 \). Then, by Lemma 3.3, \( [\mathcal{L}_{F'}]_{A_{F'}} \neq 0 \) and \( [\mathcal{L}_{F'}]_{A'_{F'}} \neq 0 \) because \( A_{F'} = A'_{F'} \). Since \( \mathcal{L}_{F'} \) splits in \( k_1 \), \( N_{k_1/F'}([\mathcal{L}_{k_1}]_{A'_{k_1}}) = [\mathcal{L}_{F'}]_{A'_{F'}} \neq 0 \) implies \( [\mathcal{L}_{k_1}]_{A'_{k_1}} \neq 0 \). Next, suppose \( [p_{F'}]_{A_{F'}} \neq 0 \). As we saw before, \( A_{F'} \) is cyclic as an \( R \)-module. It follows from \( [p_{F'}]_{A_{F'}} \neq 0 \) and \( [\mathcal{L}_{F'}]_{A_{F'}} \neq 0 \), and \( (\zeta_p - 1)[p_{F'}]_{A_{F'}} = (\zeta_p - 1)[\mathcal{L}_{F'}]_{A_{F'}} = 0 \) that we can write \( [\mathcal{L}_{F'}]_{A_{F'}} = u[p_{F'}]_{A_{F'}} \), for some unit \( u \in R^\times \). Assume that we can write \( [\mathcal{L}_{k_1}]_{A_{k_1}} = a[p_{k_1}]_{A_{k_1}} \) for some \( a \in \Lambda \). Then the above implies that \( a \) is a unit (note that both \( p_{F'} \) and \( \mathcal{L}_{F'} \) split in \( k_1/F' \)). Hence, the \( \Lambda \)-submodule \( \langle [p_{k_1}]_{A_{k_1}} \rangle \) generated by \( [p_{k_1}]_{A_{k_1}} \) is equal to the \( \Lambda \)-submodule \( \langle [\mathcal{L}_{k_1}]_{A_{k_1}} \rangle \) generated by \( [\mathcal{L}_{k_1}]_{A_{k_1}} \). This implies \( \langle p_{F'} \rangle_{A_{F'}} = \langle [\mathcal{L}_{F'}]_{A_{F'}} \rangle \) in \( A_{F'} \). By our assumption (ii), this is zero, which contradicts Lemma 3.3. Hence, \( [\mathcal{L}_{k_1}]_{A_{k_1}} \) cannot be written as \( [\mathcal{L}_{k_1}]_{A_{k_1}} = a[p_{k_1}]_{A_{k_1}} \), namely \( [\mathcal{L}_{k_1}]_{A_{k_1}} \) is not in \( \langle [p_{k_1}]_{A_{k_1}} \rangle \) in \( A_{k_1} \). This implies \( [\mathcal{L}_{k_1}]_{A'_{k_1}} \neq 0 \) in \( A'_{k_1} \).

By Lemma 7 in Ozaki and Yamamoto [16] and \( \kappa \leq p \), we know that the image of \( [\mathcal{L}_{k_1}]_{A'_{k_1}} \) in \( A'_{k_2} \) is zero. This contradicts the injectivity of \( A'_{k_1} \to A'_{k_2} \), and completes the proof of Proposition 1.9.

**Proof of Proposition 1.10.** Let \( F \) correspond to the subgroup \( \langle \gamma \sigma^i \rangle \) as in the above proof. Since \( p^4 \) does not divide \# \( A_F \) and the prime of \( F \) lying over \( p \) is not principal, we have \( \# A_{F'} \leq p^2 \), and we may assume \( \min(v_R(f_\chi(\zeta_p^{-i} - 1)), v_R(k(\zeta_p^{-i} - 1))) = 1 \) as in the proof of Proposition 1.9.

First, suppose \( v_R(f_\chi(\zeta_p^{-i} - 1)) = 1 \). Then \( f_\chi(T) \) is irreducible. By our assumption \( [p_{F'}]_{A_{F'}} \neq 0 \), we have \( [p_{k_1}]_{A_{k_1}} \neq 0 \). This together with Theorem 1.3 implies that \( k(T) \) is nonzero in \( \Lambda/(f_\chi(T), Tk(T)) \). In particular, \( f_\chi(T) \) does not divide \( k(T) \). This shows that \( X_{k,\infty} \simeq \Lambda/(f_\chi(T), Tk(T)) \) is finite.
Next, suppose that \( v_R(k(\zeta_p^{-i} - 1)) = 1 \). Since \( \zeta_p - 1 \) divides \( k(T) \) by Theorem 1.3, \( k(T) \) can be written as \( k(T) = (\zeta_p - 1)u(T) \) for some \( u(T) \in \Lambda^X \). By Ferrero–Washington’s theorem [1], \( \zeta_p - 1 \) does not divide \( f_\chi(T) \), so again we obtain the finiteness of \( X_{k,\infty} \simeq \Lambda/(f_\chi(T), Tk(T)) = \Lambda/(f_\chi(T), (\zeta_p - 1)T) \).

4. Numerical examples

4.1. We first consider the case \( p = 3 \) for \( \ell < 10000 \). By a result of Fukuda and Komatsu [3] together with a result of Ozaki and Yamamoto [16], we already know \( \lambda = 0 \) in this case (Example 4.4 in [3]). In the method of Fukuda and Komatsu [3], the computation of the zeros of \( f_\chi(T) \) which is associated to the \( p \)-adic \( L \)-function \( L_p(s, \chi) \) plays an essential role. We will see that our conditions can be applied for \( \ell < 10000 \) except for \( \ell = 8677 \), namely we will see that we can verify \( \lambda = 0 \) without computing \( f_\chi(T) \) for these \( \ell \)'s.

There are 611 \( \ell \)'s which satisfy \( \ell \equiv 1 \pmod{3} \) and \( \ell < 10000 \). Among them 589 primes satisfy either \( \ell \not\equiv 1 \pmod{9} \), or \( 3 \not\in (\mathbb{F}_\ell^\times)^3 \), or \( \kappa = 1 \). For these \( \ell \)'s, we know \( \lambda = 0 \) by Theorem A and Theorem 1 in Ozaki and Yamamoto [16]. For the remaining 22 primes, 10 primes satisfy \( v_R(B_{1,\chi^{-1}}) = 1 \) (note: \( B_{2,\chi} \) is more easily computed because the conductor of \( \chi \) is smaller than that of \( \chi^{-1} \); it is easy to see that \( v_R(B_{1,\chi^{-1}}) = 1 \) is equivalent to \( v_R(f_\chi(0)) = 1 \), which in turn is equivalent to \( v_R(B_{2,\chi}) = 1 \), and for them Corollary 3 in [16] can be applied. The remaining primes are

2269, 3907, 4933, 5527, 6247, 6481, 7219, 7687, 8011, 8677, 9001, 9901.

Ozaki and Yamamoto calculated \( f_\chi(T) \) for these 12 primes, and found that \( f_\chi(T) \) is irreducible at least for 8 primes, more precisely unless \( \ell = 2269, 6481, 7219, 8677 \). They obtained \( \lambda = 0 \) for these 8 primes by [16, Theorem 2] and some extra argument. For \( \ell = 2269, 6481, \) Ozaki and Yamamoto proved \( \lambda = 0 \) by using an argument which is similar to Proposition 1.7, but with the additional condition \( \ell \equiv 1 \pmod{27} \). In conclusion, Ozaki and Yamamoto proved \( \lambda = 0 \) for all \( \ell < 10000 \) except \( \ell = 7219, 8677 \). For many \( \ell \)'s, Fukuda and Komatsu checked \( \lambda = 0 \) by using the generalized Ichimura–Sumida criterion [3], and their theorem can be applied for the above remaining 2 primes.

We will study the above 12 primes without computing \( f_\chi(T) \). First of all, we remark that \( \kappa = 1 \) is equivalent to the condition

\[
\left( \frac{(z^2 - 1)(z^{-2} - 1)}{(z - 1)(z^{-1} - 1)} \right)^{(\ell - 1)/3} \not\equiv 1 \pmod{\ell}
\]

in Theorem 1 of Ozaki and Yamamoto [16] when we take a primitive root \( g \).
of \( \ell \), and put \( z = g^{(\ell-1)/9} \). Similarly, \( \kappa = 2 \) is equivalent to the condition
\[
\left( \frac{(z^2-1)(z^{-2}-1)}{(z-1)(z^{-1}-1)} \right)^{(\ell-1)/3} \equiv 1 \pmod{\ell}, \quad \left( (z-1)(z^{-1}-1) \right)^{(\ell-1)/3} \not\equiv 1 \pmod{\ell}
\]
in Theorem 2 of Ozaki and Yamamoto [16]. Since \( p = 3 \), \( k_1 \) has two cubic subfields which are different from \( \mathbb{Q}_1 \) and \( k \). Their equations are obtained by the following method. Let \( (a, b) \) be a solution of \( a^2 + 27b^2 = 36 \) such that \( a, b \in \mathbb{Z}_{\geq 0} \) and \( b \not\equiv 0 \pmod{3} \). There are exactly 2 such solutions. For these 2 solutions \( (a, b) \), the equations
\[
X^3 - 27\ell X - 9a\ell = 0
\]
give two cubic subfields of \( k_1 \) which are different from \( \mathbb{Q}_1 \) and \( k \) (cf. [5]).

We checked the class numbers and the primes lying over 3, using PARI-GP. The conditions of Proposition 1.8 are satisfied for 6 primes,
\[
\ell = 2269, 4933, 6247, 7687, 9001, 9901,
\]
among the above 12 primes. (We note again that \( B_2, \chi \) is more easily computed. From \( v_R(B_{1,\chi^{-1}}) = v_R(L_p(0, \chi)) \), \( v_R(B_{2,\chi}) = v_R(L_p(-1, \chi)) \), \( \deg f_\chi(T) = q - 1 \geq 2 \) and \( v_R(p) = 2 \), we know that \( v_R(B_{1,\chi^{-1}}) = 2 \) is equivalent to \( v_R(f_\chi(0)) = 2 \), which in turn is equivalent to \( v_R(B_{2,\chi}) = 2 \).) So we conclude \( \lambda = 0 \) for them.

The conditions of Proposition 1.7 hold for the following 6 primes among the above 12 primes with the subfields \( F \) which correspond to the following values of \( a \):

<table>
<thead>
<tr>
<th>( \ell )</th>
<th>2269</th>
<th>4933</th>
<th>5527</th>
<th>6481</th>
<th>7219</th>
<th>9001</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a )</td>
<td>246</td>
<td>375</td>
<td>435</td>
<td>246</td>
<td>24</td>
<td>462</td>
</tr>
</tbody>
</table>

For each \( \ell \) above, we checked that the other subfield of degree \( p \) does not satisfy the conditions of Proposition 1.7. For example, for \( \ell = 7219 \), the subfield corresponding to \( a = 24 \) satisfies these conditions of Proposition 1.7, but the subfield corresponding to \( a = 429 \) does not.

For \( \ell = 3907, 8011 \), we have \( \kappa = \infty \). Since 27 does not divide \( \ell - 1 \) for these \( \ell \), we have \( q = 3 \), and \( \kappa = \infty \) can be checked by the congruences
\[
\left( \frac{(z^2-1)(z^{-2}-1)}{(z-1)(z^{-1}-1)} \right)^{(\ell-1)/3} \equiv 1 \pmod{\ell}, \quad \left( (z-1)(z^{-1}-1) \right)^{(\ell-1)/3} \equiv 1 \pmod{\ell},
\]
where \( z \) is the element in \( \mathbb{F}_\ell \) as above. We obtain \( \lambda = 0 \) by applying Proposition 1.10. For each \( \ell \), two cubic subfields which are different from \( \mathbb{Q}_1 \) and \( k \) both satisfy the conditions of Proposition 1.10. For example, for \( \ell = 3907 \), these are the two subfields corresponding to \( a = 192 \) and \( a = 375 \).

Consequently, our criteria could be applied for all primes \( \ell < 10000 \) except \( \ell = 8677 \). Namely, we could verify \( \lambda = 0 \) without using the computation of \( f_\chi(T) \) for all these \( \ell \neq 8677 \).
4.2. Suppose that $\ell \equiv 1 \pmod{p^c}$ and $c$ is very large. Then the degree of $f_{\chi}(T)$ is $\geq p^{c-1} - 1$ by Kida’s formula ([11], [10]), and it is very difficult to calculate the irreducible factors of $f_{\chi}(T)$.

Suppose $p = 3$ and take $\ell$ which satisfies $\ell < 100000$ and $\ell \equiv 1 \pmod{p^7}$. Then either $3 \not\in (\mathbb{F}_{\ell}^\times)^3$ or $\kappa = 1$ is satisfied except for $\ell = 17497$ and $52489$. We study these 2 remaining primes by using our propositions. The conditions of Proposition 1.8 are satisfied for $\ell = 52489$. Proposition 1.7 can be applied both for $\ell = 17497$ and $52489$. The conditions are satisfied for the subfield $F$ which corresponds to $a = 645$ (resp. $a = 1374$) for $\ell = 17497$ (resp. $\ell = 52489$). (For the value $a$, see 4.1.)

4.3. As we explained in 4.1, in the case $p = 3$ and $\ell < 10000$, if $\ell$ satisfies both $\ell \equiv 1 \pmod{9}$ and $3 \not\in (\mathbb{F}_{\ell}^\times)^3$, then we have $\kappa = 1$, or $\kappa = 2$, or $\kappa = \infty$. But theoretically, by Chebotarev’s density theorem, $\kappa$ can be any positive integer.

The smallest $\ell$ such that $\kappa = 3$ is $\ell = 11719$. (To see this, we have to calculate the map $\Phi'_2 : E_{Q_2}^\prime \rightarrow \bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p$. Since $E_{Q_2}^\prime/(E_{Q_2})^p$ is generated by the cyclotomic $p$-unit as we explained in the proof of Lemma 1.1, the computation of $\dim \text{Cokernel}(\Phi'_2)$ is easy.)

For $\ell = 11719$, if we take $F$ to be the subfield corresponding to $a = 3$ and $F'$ to be the subfield corresponding to $a = 564$, the conditions of Proposition 1.9 are satisfied. Thus, we get $\lambda = 0$ for $\ell = 11719$.

4.4. Next, we consider the case $p = 5$. The computation in this subsection was done by Masahiro Kato whom we thank very much. For $p = 5$, in the range $\ell < 100000$, there are 99 $\ell$’s which satisfy both $\ell \equiv 1 \pmod{25}$ and $5 \in (\mathbb{F}_{\ell}^\times)^5$. Among them, 76 primes satisfy $\kappa = 1$, 21 primes satisfy $\kappa = 2$, $\ell = 84551$ satisfies $\kappa = 3$, and $\ell = 59951$ satisfies $\kappa = 4$. For the primes with $\kappa = 1$, we have $\lambda = 0$ by Corollary 1.4. Among the 23 primes with $\kappa \geq 2$, 16 primes satisfy $v_R(B_{1,\chi\omega^{-1}}) = 1$. We have $\lambda = 0$ for these primes by Corollary 1.6. The remaining primes are

\[ 7151, 7901, 21001, 38851, 41201, 67651, 84551. \]

We checked that the conditions of Proposition 1.8 are satisfied for $\ell = 7151, 7901, 21001, 67651$. Consequently, for $p = 5$ we verified $\lambda = 0$ for all $\ell < 100000$ except $\ell = 38851, 41201, 84551$.

References


Department of Mathematics
Tokyo Metropolitan University
Hachioji, Tokyo, 192-0397, Japan
E-mail: m-kuri@comp.metro-u.ac.jp

Received on 26.2.2001
and in revised form on 25.3.2004