ACTA ARITHMETICA
116.3 (2005)

Remarks on the λ_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_∞/k denote the cyclotomic $\mathbb{Z}_p$-extension and X_{k_∞} denote the Galois group of the maximal unramified abelian pro-p extension of k_∞ over k_∞. Greenberg's conjecture predicts that X_{k_∞} 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 ℓ. First of all, we will see that for such a field k, X_{k_∞} has a simple form (Theorem 1.3), and we will see what the finiteness of X_{k_∞} 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_∞} (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 ℓ'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 ℓ is a rational prime such that $\ell \equiv 1 \pmod{p}$, and k denotes the cyclic field of degree p with conductor ℓ. For an integer $n \geq 0$, we denote by k_n (resp. $\mathbb{Q}_n$) the nth layer of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k (resp. $\mathbb{Q}_\infty/\mathbb{Q}$), namely k_n (resp. $\mathbb{Q}_n$) is the intermediate field such that $[k_n : k] = p^n$ (resp. $[\mathbb{Q}_n : \mathbb{Q}] = p^n$).

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

$$X_{k_\infty} = \varprojlim A_{k_n}$$

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

By genus theory and a theorem of Iwasawa (cf. [8]), we know $X_{k_\infty} = 0$ if either $p \pmod{\ell} \notin (\mathbb{F}_\ell^\times)^p$ or $\ell \not\equiv 1 \pmod{p^2}$ holds (Theorem A in [16]). So in the following, we assume that $p \pmod{\ell} \in (\mathbb{F}_\ell^\times)^p$ and $\ell \equiv 1 \pmod{p^2}$. Namely, we assume that p splits in $k/\mathbb{Q}$, and that ℓ splits in $\mathbb{Q}_1/\mathbb{Q}$.

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

Lemma 1.1. *Suppose that Φ'_n is not the zero map. Then, for any $m \geq n$, the dimension of the cokernel of Φ'_m (as an $\mathbb{F}_p$-vector space) is equal to the dimension of the cokernel of Φ'_n (as an $\mathbb{F}_p$-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 Φ'_n is not zero. We define

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

where v ranges over all primes of $\mathbb{Q}_n$ lying over ℓ. If the image of Φ'_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 ℓ. Then $\kappa < \infty$ implies $\kappa < q$

by definition. In general, numerical calculation of κ is easy (cf. the proof of Lemma 1.1 in §2, and the examples in §4). We will define a similar map Φ_n in §2, and give a relation between κ and Φ_n. We believe this number κ and the maps Φ_n, Φ'_n play an important role in Iwasawa theory of k.

If $\kappa = 0$, the Φ'_n's are surjective for all $n \geq 0$, so from the surjectivity of Φ'_0 and the fact that $E'_{\mathbb{Q}}/(E'_{\mathbb{Q}})^p$ is generated by the image of p, we have $p \pmod{\ell} \notin (\mathbb{F}_\ell^\times)^p$. So by our assumption, we always have $\kappa \geq 1$.

Let ζ_p be a primitive pth root of unity, and put

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

We also define G and Γ by

$$G = \mathrm{Gal}(k_\infty/\mathbb{Q}_\infty) = \mathrm{Gal}(k/\mathbb{Q}), \qquad \Gamma = \mathrm{Gal}(k_\infty/k) = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}).$$

We take a generator σ 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 $X_{\mathbb{Q}_\infty} = \varprojlim A_{\mathbb{Q}_n} = 0$ (where $A_{\mathbb{Q}_n}$ is the p-Sylow subgroup of the ideal class group of $\mathbb{Q}_n$), so it is the zero map. Hence, by defining $\zeta_p x = \sigma x$, X_{k_∞} becomes an $R = \mathbb{Z}_p[\zeta_p]$-module. Since Γ acts on X_{k_∞}, X_{k_∞} is also a Λ-module where we put

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

Throughout this paper, we identify Λ with the formal power series ring $R[[T]]$ by identifying a generator γ of Γ with $1 + T$.

Let χ be a faithful character of $\mathrm{Gal}(k/\mathbb{Q})$, namely χ is an injective homomorphism from $\mathrm{Gal}(k/\mathbb{Q})$ to $\overline{\mathbb{Q}}_p^\times$. 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 $G_\chi(\kappa(\gamma)^{1-s} - 1) = L_p(s,\chi)$, 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 $\mathbb{Q}_\infty$ lying over ℓ).

THEOREM 1.3. *Let $\mathfrak{p}$ be a prime of k lying over p, and $\mathfrak{p}_n$ be the prime of k_n lying over $\mathfrak{p}$. We denote by $\mathbf{c}_{\mathfrak{p}}$ the class of $(\mathfrak{p}_n)$ in X_{k_∞}. Then there exist a polynomial $k(T) \in R[T]$ and an isomorphism*

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

of $\Lambda\,(= R[[\Gamma]] = R[[T]])$-modules such that $k(T)$ modulo $(f_\chi(T), Tk(T))$ corresponds to $\mathbf{c}_{\mathfrak{p}}$. 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_∞} is $\leq \kappa - 1$. Since λ is the $\mathbb{Z}_p$-rank of X_{k_∞}, 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_∞} 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 $\mathbb{Q}_p$ 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_∞}, 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 $\mathbb{Q}_\infty$ lying over ℓ. On the other hand, by the definition of κ, 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 $F \neq \mathbb{Q}_1$, $F \neq k$, $[F : \mathbb{Q}] = p$, 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 $R = \mathbb{Z}_p[\zeta_p]$ 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* $v_R(B_{1,\chi\omega^{-1}}) = 2$. *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* $\kappa \le p$ *and* $\ell \equiv 1 \pmod{p^3}$. *We also assume there are subfields* F *and* F' *of* k_1 *such that*

(i) $F \ne \mathbb{Q}_1$, $F \ne k$, $F' \ne \mathbb{Q}_1$, $F' \ne k$, *and* $[F:\mathbb{Q}] = [F':\mathbb{Q}] = p$,
(ii) *the prime of* F *over* ℓ *is principal*, *and the prime of* F' *over* ℓ *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* $F \ne k$ *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_∞}. 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 $\le \kappa - 1$. 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 Φ_n and the invariant κ

Proof of Lemma 1.1. We define M_n by $M_n = \bigoplus_{v\mid\ell,\, v\in P_{\mathbb{Q}_n}} \kappa(v)^\times/(\kappa(v)^\times)^p$ where v ranges over all primes of $\mathbb{Q}_n$ over ℓ, and define M_m similarly. Put $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Then both M_n and M_m are $\mathbb{F}_p[[\Gamma]]$-modules. We take a generator γ of Γ 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 $\mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})/D]$ where D is the decomposition group of ℓ, it is generated by one element as an $\mathbb{F}_p[[T]]$-module. Taking a generator x_m, we write

$$M_m = \mathbb{F}_p[[T]]x_m \simeq \mathbb{F}_p[[T]]/(T^{q_m})$$

where q_m is the number of the primes of $\mathbb{Q}_m$ lying over ℓ. 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 $\mathbb{Q}_n$ 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 ℓ.

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

$$\dim \operatorname{Cokernel}(\Phi'_n : E'_{\mathbb{Q}_n} \to M_n) = \dim \operatorname{Cokernel}(\Phi'_m : E'_{\mathbb{Q}_m} \to M_m) = i.$$

This completes the proof of the lemma.

Next, we will define a homomorphism Φ_n. Let $E_{\mathbb{Q}_n}$ be the unit group of $O_{\mathbb{Q}_n}$. Then Φ'_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

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

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

$$\Phi_n : E_{\mathbb{Q}_n} \to \Big(\bigoplus_{v|\ell} \kappa(v)^\times/(\kappa(v)^\times)^p\Big)^0.$$

LEMMA 2.1. *Suppose that Φ'_n is not the zero map. Then the dimension of the cokernel of Φ_n as an $\mathbb{F}_p$-vector space is equal to κ.*

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 $\Phi'_n(E'_{\mathbb{Q}_n}) = T^i\mathbb{F}_p[[T]]x_n$. Since $E_{\mathbb{Q}_n}/E^p_{\mathbb{Q}_n}$ is generated by cyclotomic units, $T(E'_{\mathbb{Q}_n}/(E'_{\mathbb{Q}_n})^p) = E_{\mathbb{Q}_n}/E^p_{\mathbb{Q}_n}$, and we have $\Phi_n(E_{\mathbb{Q}_n}) = T^{i+1}\mathbb{F}_p[[T]]x_n$. Note that $i+1 \le q_n$ by our assumption. Hence,

$$\dim \mathrm{Cokernel}(\Phi_n) = (i+1) - 1 = i = \dim \mathrm{Cokernel}(\Phi'_n) = \kappa.$$

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*

$$\to \widehat{H}^0(L/K, A_L) \to \widehat{H}^0(L/K, E_L) \to \Big(\bigoplus_{v\in P_{\mathrm{ram}}(K)} \widehat{H}^0(L_w/K_v, E_{L_w})\Big)^0$$
$$\to H^1(L/K, A_L) \to H^1(L/K, E_L) \to \bigoplus_{v\in P_{\mathrm{ram}}(K)} H^1(L_w/K_v, E_{L_w})$$
$$\to \dots$$

Here, the notation is as follows. $P_{\mathrm{ram}}(K)$ is the set of all ramified (finite) primes of K in L/K. For $v \in P_{\mathrm{ram}}(K)$, 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 $\widehat{H}^0(*,*)$ is the Tate cohomology. We define an isomorphism $\widehat{H}^0(L_w/K_v, E_{L_w}) \simeq \mathbb{Z}/p\mathbb{Z}$ by

$$\widehat{H}^0(L_w/K_v, E_{L_w}) \simeq \widehat{H}^0(L_w/K_v, L_w^\times) \simeq H^2(L_w/K_v, L_w^\times) \simeq \mathbb{Z}/p\mathbb{Z}$$

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 $(\bigoplus_{v\in P_{\mathrm{ram}}(K)} \widehat{H}^0(L_w/K_v, E_{L_w}))^0$ denotes the kernel of

$$\bigoplus_{v\in P_{\mathrm{ram}}(K)} \widehat{H}^0(L_w/K_v, E_{L_w}) \simeq \bigoplus_{v\in P_{\mathrm{ram}}(K)} \mathbb{Z}/p \xrightarrow{\Sigma} \mathbb{Z}/p$$

where Σ 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_∞ unramified outside p, and $\mathcal{X}_{k_\infty} = \mathrm{Gal}(\mathcal{M}_\infty/k_\infty)$ be its Galois group. We denote by $\mathcal{U}_{k_\infty}$ the group of semi-local units, namely

$$\mathcal{U}_{k_\infty} = \varprojlim \bigoplus_{\mathfrak{p}|p} U^1_{k_{n,\mathfrak{p}_n}}$$

where $\mathfrak{p}$ ranges over all primes of k over p, and $\mathfrak{p}_n$ is the prime of k_n over $\mathfrak{p}$, and $U^1_{k_{n,\mathfrak{p}_n}}$ is the principal units of $k_{n,\mathfrak{p}_n}$. By class field theory, we have an exact sequence

$$\mathcal{U}_{k_\infty} \to \mathcal{X}_{k_\infty} \to X_{k_\infty} \to 0.$$

Put $G = \mathrm{Gal}(k_\infty/\mathbb{Q}_\infty) = \langle\sigma\rangle$ and $N_G = 1 + \sigma + \cdots + \sigma^{p-1}$. If we denote by $\mathcal{X}_{\mathbb{Q}_\infty}$ the Galois group of the maximal abelian pro-p extension of $\mathbb{Q}_\infty$ unramified outside p over $\mathbb{Q}_\infty$, we have $\mathcal{X}_{\mathbb{Q}_\infty} = 0$. So multiplication by N_G is zero on $\mathcal{X}_{k_\infty}$, and we can regard $\mathcal{X}_{k_\infty}$ as a $\Lambda = \mathbb{Z}_p[\zeta_p][[\Gamma]]$-module. Hence, we have an exact sequence

$$\mathcal{U}_{k_\infty}/N_G\mathcal{U}_{k_\infty} \to \mathcal{X}_{k_\infty} \to X_{k_\infty} \to 0$$

of Λ-modules.

We will show that $\mathcal{X}_{k_\infty}$ is generated by one element as a Λ-module. To see this, it is enough to see that the Γ-coinvariant $(\mathcal{X}_{k_\infty})_\Gamma$ is generated by one element as an $R = \mathbb{Z}_p[\zeta_p]$-module. Let $G_{k,p}$ (resp. $G_{k_\infty,p}$) be the Galois group of the maximal extension of k (resp. k_∞) unramified outside p over k (resp. k_∞), and $\mathcal{X}_k$ be the Galois group of the maximal abelian pro-p extension of k unramified outside p over k. From the inflation-restriction exact sequence

$$0 \to H^1(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(G_{k,p}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(G_{k_\infty,p}, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma \to 0,$$

taking the Pontryagin dual, we have $(\mathcal{X}_{k_\infty})_\Gamma = \mathrm{Ker}(\mathcal{X}_k \to \Gamma)$. By class field theory (and $A_k = 0$ as we mentioned in §1), $\mathcal{X}_k$ is isomorphic to $(\bigoplus_{\mathfrak{p}|p} U^1_{k_\mathfrak{p}})/(\text{the image of } E_k \otimes \mathbb{Z}_p)$ and $\mathcal{X}_\mathbb{Q}$ is isomorphic to $\Gamma = U^1_{\mathbb{Q}_p} \simeq \mathbb{Z}_p$. Hence, $\mathrm{Ker}(\mathcal{X}_k \to \Gamma)$ is isomorphic to $\mathrm{Ker}(\mathrm{Norm} : \bigoplus_{\mathfrak{p}|p} U^1_{k_\mathfrak{p}} \to U^1_{\mathbb{Q}_p})/(\text{the image of } E_k \otimes \mathbb{Z}_p)$. Recall that p splits in $k/\mathbb{Q}$ and $U^1_{k_\mathfrak{p}} = U^1_{\mathbb{Q}_p} \simeq \mathbb{Z}_p$. Since $\mathrm{Ker}(\mathrm{Norm} : \bigoplus_{\mathfrak{p}|p} U^1_{k_\mathfrak{p}} \to U^1_{\mathbb{Q}_p})$ is a free R-module of rank 1, $(\mathcal{X}_{k_\infty})_\Gamma = \mathrm{Ker}(\mathcal{X}_k \to \Gamma)$ is generated by one element as an R-module. By Nakayama's lemma, $\mathcal{X}_{k_\infty}$ is generated by one element as a Λ-module.

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

$$\mathcal{X}_{k_\infty} \simeq \Lambda/(f_\chi(T)).$$

Let $\mathbb{Q}_{p,\infty}/\mathbb{Q}_p$ be the cyclotomic $\mathbb{Z}_p$-extension of the p-adic field $\mathbb{Q}_p$ and $\mathbb{Q}_{p,n}$ be the nth layer. For any $n \geq 1$, we denote by ζ_{p^n} a primitive p^nth root of unity such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for all n. Put $\pi_n = N_{\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_{p,n}}(1 - \zeta_{p^{n+1}})$

where $N_{\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_{p,n}}$ is the norm map from $\mathbb{Q}_p(\zeta_{p^{n+1}})$ to $\mathbb{Q}_{p,n}$. 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 $\mathcal{U}_{\mathbb{Q}_{p,\infty}} = \varprojlim U^1_{\mathbb{Q}_{p,n}}$ is a free $\mathbb{Z}_p[[T]]$-module of rank 1, and is generated by $T\pi$ (where $T = \gamma - 1$ and γ is the fixed generator of Γ).

We take a prime $\mathfrak{p}$ of k lying over p, and fix it. Since p splits in $k/\mathbb{Q}$, we have $k_\mathfrak{p} = \mathbb{Q}_p$, hence by the above remark, $\mathcal{U}_{k_\infty}/N_G\mathcal{U}_{k_\infty}$ is a free Λ-module of rank 1, and is generated by the class of $(T\pi, 1, \ldots, 1)$ (where we suppose the first component corresponds to $\mathfrak{p}$). 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 $\mathfrak{p}$) clearly maps to $\mathbf{c}_\mathfrak{p}$ by the natural map $\mathcal{X}_{k_\infty} \to X_{k_\infty}$. Hence, X_{k_∞} can be written as

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

where $k(T) \in \Lambda$ corresponds to $\mathbf{c}_\mathfrak{p}$.

Next, we will see that

$$\text{(1)} \qquad \kappa < \infty \Longleftrightarrow \text{the class of } \mathfrak{p}_n \text{ in } (A_{k_n})_G \text{ is nonzero for sufficiently large } n.$$

Let $M/\mathbb{Q}_n$ be the maximal abelian extension which is unramified outside ℓ and whose Galois group has exponent p. Then, by class field theory, $\mathrm{Gal}(M/\mathbb{Q}_n)$ is isomorphic to $(\bigoplus_{v\mid\ell} \kappa(v)^\times/(\kappa(v)^\times)^p)/\Phi'_n(E_{\mathbb{Q}_n})$, and the prime $\mathfrak{p}_n$ of $\mathbb{Q}_n$ above p splits in M if and only if $\Phi'_n(\pi_n) = 0$ in the above group, namely $\Phi'_n(\pi_n) \in \Phi'_n(E_{\mathbb{Q}_n})$. As we showed in the proof of Lemma 2.1, we have $\Phi'_n(E_{\mathbb{Q}_n}) = T\Phi'_n(E'_{\mathbb{Q}_n}) = \langle T\Phi'_n(\pi_n)\rangle$, hence $\Phi'_n(\pi_n) \in \Phi'_n(E_{\mathbb{Q}_n})$ is equivalent to $\Phi'_n(\pi_n) = 0$. So, $\mathfrak{p}_n$ splits in M if and only if $\Phi'_n(\pi_n) = 0$.

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 ℓ in $\mathrm{Gal}(M/k_n)$ is cyclic, so M/k_n is unramified everywhere.) We have an isomorphism $(A_{k_n})_G \simeq \mathrm{Gal}(M/k_n)$. Hence, $\mathfrak{p}_n$ splits in M if and only if the class of $\mathfrak{p}_n$ in $(A_{k_n})_G$ is zero. We saw in the last paragraph that this is equivalent to $\Phi'_n(\pi_n) = 0$, hence we obtain the equivalence (1) (recall that the image of π_n in $E'_{\mathbb{Q}_n}/(E'_{\mathbb{Q}_n})^p$ 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, $A'_K = \mathrm{Pic}(O_K[1/p])$.

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

We define

$$X'_{k_\infty} = \varprojlim A'_{k_n}$$

where the projective limit is taken with respect to the norm maps. Since $\mathbf{c}_{\mathfrak{p}}$ corresponds to $k(T)$, we have

$$X'_{k_\infty} \xrightarrow{\simeq} \Lambda/(f_\chi(T), k(T)).$$

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 $k(T) \equiv uT^{\kappa-1} \pmod{(\zeta_p - 1, T^{\kappa})}$ 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 $\mathfrak{p}_n$ in $(A_{k_n})_G$ are zero for all n. Hence, the image of $\mathbf{c}_{\mathfrak{p}}$ 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

$$H_K^2 = H^2(G_{K,p}, \mathbb{Z}_p(1))$$

where $\mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$ (μ_{p^n} is the group of p^nth roots of unity). Since H_K^2 is the same as the etale cohomology $H^2(\mathrm{Spec}\, O_K[1/p]_{\mathrm{et}}, \mathbb{Z}_p(1))$, by the Kummer sequence we obtain

Lemma 3.2. *We have an exact sequence*

$$0 \to A'_K \to H_K^2 \to B(O_K[1/p]) \to 0$$

where $B(O_K[1/p]) = \varprojlim \mathrm{Br}(O_K[1/p])[p^n] = (\bigoplus_{v|p} \mathbb{Z}_p)^0$ *is the Tate module of the Brauer group of* $O_K[1/p]$.

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

$$0 \to A'_{k_n} \to H_{k_n}^2 \to R \to 0$$

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

$$0 \to X'_{k_\infty} \to \mathbf{H}^2_{k_\infty} \to R \to 0$$

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

$$\mathbf{H}^2_{k_\infty} \simeq \Lambda/(Tf_\chi(T), Tk(T)).$$

We consider the subfield k_1 which is the first layer of k_∞/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

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

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

$$A'_{k_1} \simeq \Lambda/(f_\chi(T), k(T), \varphi(T)). \tag{2}$$

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 ℓ ramify in $F/\mathbb{Q}$. Put $\mathcal{G} = \mathrm{Gal}(k_\infty/F)$. Taking $\mathcal{G}$-coinvariants, we have an exact sequence

$$0 \to (X'_{k_\infty})_\mathcal{G} \to (\mathbf{H}^2_{k_\infty})_\mathcal{G} \to R_\mathcal{G} \to 0.$$

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

$$(\mathbf{H}^2_{k_\infty})_\mathcal{G} \simeq H^2_F \simeq A'_F.$$

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

$$0 \to (X'_{k_\infty})_\mathcal{G} \to A'_F \to \mathbb{Z}/p\mathbb{Z} \to 0. \tag{3}$$

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

LEMMA 3.3. *At least either* $[\mathfrak{p}_F] \neq 0$ *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 ℓ. By Lemma 3.1 we have an exact sequence

$$H^1(F_{\mathfrak{p}_F}/\mathbb{Q}_p, E_{F_{\mathfrak{p}_F}}) \oplus H^1(F_{\mathcal{L}_F}/\mathbb{Q}_\ell, E_{F_{\mathcal{L}_F}}) \to \widehat{H}^0(F/\mathbb{Q}, A_F) \to \widehat{H}^0(F/\mathbb{Q}, E_F).$$

The exact sequence $0 \to E_{F_{\mathfrak{p}_F}} \to F_{\mathfrak{p}_F}^\times \to \mathbb{Z} \to 0$ yields a natural isomorphism $H^1(F_{\mathfrak{p}_F}/\mathbb{Q}_p, E_{F_{\mathfrak{p}_F}}) \simeq \mathbb{Z}/p\mathbb{Z}$ by Hilbert Theorem 90. By the definition of the homomorphisms in Lemma 3.1, $H^1(F_{\mathfrak{p}_F}/\mathbb{Q}_p, E_{F_{\mathfrak{p}_F}}) \to \widehat{H}^0(F/\mathbb{Q}, A_F)$ is induced by the reciprocity map $F_{\mathfrak{p}_F}^\times \to D_{\mathfrak{p}_F} \subset A_F$ ($D_{\mathfrak{p}_F}$ 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 $1 \in \mathbb{Z}/p\mathbb{Z} \simeq H^1(F_{\mathfrak{p}_F}/\mathbb{Q}_p, E_{F_{\mathfrak{p}_F}})$ in $\widehat{H}^0(F/\mathbb{Q}, A_F) = A_F^{\mathrm{Gal}(F/\mathbb{Q})}$ is $[\mathfrak{p}_F]$. Similarly we deduce that the image of 1 in $H^1(F_{\mathcal{L}_F}/\mathbb{Q}_\ell, E_{F_{\mathcal{L}_F}}) \simeq \mathbb{Z}/p\mathbb{Z}$ is $[\mathcal{L}_F]$. Since $\widehat{H}^0(F/\mathbb{Q}, E_F) = E_\mathbb{Q}/N_{F/\mathbb{Q}}E_F = 0$, the above exact sequence tells us that $A_F^{\mathrm{Gal}(F/\mathbb{Q})}$ is generated by $[\mathfrak{p}_F]$ and $[\mathcal{L}_F]$. As in the proof of Theorem 1.3, we have $(A_F)_{\mathrm{Gal}(F/\mathbb{Q})} = \mathbb{Z}/p\mathbb{Z}$, so $(A_F)^{\mathrm{Gal}(F/\mathbb{Q})}$ is also of order p. Hence, at least one of $[\mathfrak{p}_F]$ 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_∞} is infinite. Then we must have $f_\chi(\alpha) = 0$, and by the isomorphism (2) we have

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

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

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

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 $(X'_{k_\infty})_\mathcal{G} = R/(\zeta_p^{-i} - 1 - \alpha) \to A'_F$, hence it is of order p^{c_F}.

We take a prime $\mathcal{L}$ of k_1 lying over ℓ. Since $\mathcal{L}$ is totally ramified in $k_1/\mathbb{Q}_1$, σ 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

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

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 $c = v_R(\varphi(\alpha)) = v_R(\prod_{j=1}^{p-1}(1 + \alpha - \zeta_p^j))$, 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, $N_{k_1/F}(\mathcal{L}) = \mathcal{L}_F$ and the class of $\mathcal{L}_F$ in A'_F is zero.

Note that by our assumption $[\mathfrak{p}_F] = 0$ in A_F, we have $A_F = A'_F$. So we get $[\mathcal{L}_F] = [\mathfrak{p}_F] = 0$ in A_F, which contradicts Lemma 3.3. Hence, X'_{k_∞} 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 p^4 does not divide the class numbers of all subfields of k_1 with degree p over $\mathbb{Q}$, then $T - \alpha$ does not divide a generator of the characteristic ideal* $\mathrm{char}_\Lambda(X_{k_\infty})$.

Proof. Assume that $T-\alpha$ divides a generator of the characteristic ideal of X_{k_∞}. Then X_{k_∞} 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 $0 < i < p$ and $\alpha/(\zeta_p - 1) \equiv -i \pmod{\zeta_p - 1}$. Hence, we have $v_R(\alpha - (\zeta_p^{-i} - 1)) > 1$. 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

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

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

On the other hand, since p^4 does not divide $\#A_F$, we must have $\#A_F = \#A'_F = p^3$. This shows that the prime $\mathfrak{p}_F$ of F lying over p 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_∞}. 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. $\mathfrak{p}_F$) be the prime of F lying over ℓ (resp. p). By our assumption (ii) and Lemma 3.3, $\mathfrak{p}_F$ is not principal. So by our assumption (iii), we have $\#A'_F \leq p^2$. By the exact sequence (3), this implies that $\min(v_R(f_\chi(\zeta_p^{-i} - 1)), v_R(k(\zeta_p^{-i} - 1))) \leq 1$. 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_∞} is infinite. Then $k(T)$ must divide $f_\chi(T)$, and we have $X'_{k_\infty} \simeq \Lambda/(k(T))$. Put $\varphi(T) = ((1+T)^p - 1)/T$ and $\varphi_2(T) = ((1+T)^{p^2} - 1)/T$. By the isomorphism (2), we have $A'_{k_1} = \Lambda/(k(T), \varphi(T))$, and by the same method, we have $A'_{k_2} = \Lambda/(k(T), \varphi_2(T))$. 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. $\mathfrak{p}_{k_1}$) be a prime of k_1 lying over ℓ (resp. p). We denote by $[\mathcal{L}_{k_1}]_{A_{k_1}}$ (resp. $[\mathfrak{p}_{k_1}]_{A_{k_1}}$) the class of $\mathcal{L}_{k_1}$ (resp. $\mathfrak{p}_{k_1}$) 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 $\mathfrak{p}_{F'}$ (resp. $\mathcal{L}_{F'}$) the prime of F' over p (resp. ℓ). Suppose first that $[\mathfrak{p}_{F'}]_{A_{F'}} = 0$. 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 $[\mathfrak{p}_{F'}]_{A_{F'}} \neq 0$. As we saw before, $A_{F'}$ is cyclic as an R-module. It follows from $[\mathfrak{p}_{F'}]_{A_{F'}} \neq 0$, $[\mathcal{L}_{F'}]_{A_{F'}} \neq 0$, and $(\zeta_p - 1)[\mathfrak{p}_{F'}]_{A_{F'}} = (\zeta_p - 1)[\mathcal{L}_{F'}]_{A_{F'}} = 0$ that we can write $[\mathcal{L}_{F'}]_{A_{F'}} = u[\mathfrak{p}_{F'}]_{A_{F'}}$ for some unit $u \in R^\times$. Assume that we can write $[\mathcal{L}_{k_1}]_{A_{k_1}} = a[\mathfrak{p}_{k_1}]_{A_{k_1}}$ for some $a \in \Lambda$. Then the above implies that a is a unit (note that both $\mathfrak{p}_{F'}$ and $\mathcal{L}_{F'}$ split in k_1/F'). Hence, the Λ-submodule $\langle [\mathfrak{p}_{k_1}]_{A_{k_1}} \rangle$ generated by $[\mathfrak{p}_{k_1}]_{A_{k_1}}$ is equal to the Λ-submodule $\langle [\mathcal{L}_{k_1}]_{A_{k_1}} \rangle$ generated by $[\mathcal{L}_{k_1}]_{A_{k_1}}$. This implies $\langle [\mathfrak{p}_F]_{A_F} \rangle = \langle [\mathcal{L}_F]_{A_F} \rangle$ 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 $[\mathcal{L}_{k_1}]_{A_{k_1}} = a[\mathfrak{p}_{k_1}]_{A_{k_1}}$, namely $[\mathcal{L}_{k_1}]_{A_{k_1}}$ is not in $\langle [\mathfrak{p}_{k_1}]_{A_{k_1}} \rangle$ 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 $[\mathfrak{p}_F]_{A_F} \neq 0$, we have $[\mathfrak{p}_{k_1}]_{A_{k_1}} \neq 0$. 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 $u(T) \in \Lambda^\times$. 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 ℓ's.

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

$$\left(\frac{(z^2-1)(z^{-2}-1)}{(z-1)(z^{-1}-1)}\right)^{(\ell-1)/3} \equiv 1 \pmod{\ell}, \quad ((z-1)(z^{-1}-1))^{(\ell-1)/3} \not\equiv 1 \pmod{\ell}$$

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 $a^2 + 27b^2 = 36\ell$ such that $a, b \in \mathbb{Z}_{>0}$ 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 $v_R(B_{1,\chi\omega^{-1}}) = v_R(L_p(0,\chi))$, $v_R(B_{2,\chi}) = v_R(L_p(-1,\chi))$, $\deg f_\chi(T) = q - 1 \geq 2$ and $v_R(p) = 2$, we know that $v_R(B_{1,\chi\omega^{-1}}) = 2$ 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:

ℓ	2269	4933	5527	6481	7219	9001
a	246	375	435	246	24	462

For each ℓ 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 ℓ, we have $q = 3$, and $\kappa = \infty$ can be checked by the congruences

$$\left(\frac{(z^2-1)(z^{-2}-1)}{(z-1)(z^{-1}-1)}\right)^{(\ell-1)/3} \equiv 1 \pmod{\ell}, \quad ((z-1)(z^{-1}-1))^{(\ell-1)/3} \equiv 1 \pmod{\ell},$$

where z is the element in $\mathbb{F}_\ell$ as above. We obtain $\lambda = 0$ by applying Proposition 1.10. For each ℓ, 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 ℓ which satisfies $\ell < 100000$ and $\ell \equiv 1 \pmod{p^7}$. Then either $3 \notin (\mathbb{F}_\ell^\times)^3$ 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 ℓ satisfies both $\ell \equiv 1 \pmod 9$ and $3 \in (\mathbb{F}_\ell^\times)^3$, then we have $\kappa = 1$, or $\kappa = 2$, or $\kappa = \infty$. But theoretically, by Chebotarev's density theorem, κ can be any positive integer.

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

[1] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. 109 (1979), 377–395.

[2] T. Fukuda and K. Komatsu, *On Iwasawa λ_3-invariants of cyclic cubic fields of prime conductor*, Math. Comp. 70 (2001), 1707–1712.

[3] T. Fukuda and K. Komatsu, *Ichimura–Sumida criterion for Iwasawa λ-invariants*, Proc. Japan Acad. Ser. A Math. Sci. 76 (2000), no. 7, 111–115.

[4] T. Fukuda, K. Komatsu, M. Ozaki and H. Taya, *On Iwasawa λ_p-invariants of relative real cyclic extensions of degree p*, Tokyo J. Math. 20 (1997), 475–480.

[5] M. N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$*, J. Reine Angew. Math. 277 (1975), 89–116.

[6] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.

[7] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*, Internat. J. Math. 7 (1996), 721–744.

[8] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[9] —, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. 98 (1973), 246–326.

[10] —, *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tôhoku Math. J. 33 (1981), 263–288.

[11] Y. Kida, *ℓ-extensions of CM-fields and cyclotomic invariants*, J. Number Theory 12 (1980), 519–528.

[12] K. Komatsu, *On the $\mathbb{Z}_3$-extension of a certain cubic cyclic field*, Proc. Japan Acad. Ser. A Math. Sci. 74 (1998), no. 10, 165–166.

[13] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. 97 (1995), 135–155.

[14] M. Kurihara, *On the ideal class groups of the maximal real subfields of number fields with all roots of unity*, J. Eur. Math. Soc. 1 (1999), 35–49.

[15] B. Mazur and A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. 76 (1984), 179–330.

[16] M. Ozaki and G. Yamamoto, *Iwasawa λ_3-invariants of certain cubic fields*, Acta Arith. 97 (2001), 387–398.

[17] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. 5, Springer, 1964.

[18] T. Tsuji, *On the Iwasawa λ-invariants of real abelian fields*, Trans. Amer. Math. Soc. 355 (2003), 3699–3714.

[19] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, 1982.

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 (3986)