TOKYO J. MATH.
VOL. 22, NO. 2, 1999

The Iwasawa λ-invariants of Real Abelian Fields and the Cyclotomic Elements

Masato KURIHARA

Tokyo Metropolitan University

0. Introduction.

Our aim in this paper is to introduce an element

$$c_{l,r}\in\mathbf{F}_l \quad (l\text{: a prime number, } r\text{: an integer} > 1)$$

in a finite field $\mathbf{F}_l$, and also an element $c^{\chi}_{l,r,p^n}\in\mathbf{F}_l$ (p: some prime number, n: a positive integer) for a Dirichlet character χ. We also introduce a function $r\mapsto n(r)$ ($r>1$, $n(r)\in\mathbf{Z}_{>0}$) where $n(r)$ is the number defined as an "index" of $c_{l,r}$'s for all l, and also introduce a function $r\mapsto n^{\chi}(r)_p$ where $n^{\chi}(r)_p$ is an "index" of c^{χ}_{l,r,p^n}. These functions $n(r)$, $n^{\chi}(r)_p$, and elements $c_{l,r}$, c^{χ}_{l,r,p^n} are defined only in terms of elementary number theory (§1, §2).

Theoretically $n(r)$ is the order of the Tate Shafarevich group of the motive $\mathbf{Z}(r)$ in the sense of [1] (and $n^{\chi}(r)$ corresponds to the χ-part of the Tate Shafarevich group of $\mathbf{Z}(r)$). In §3 we describe the relation between the elements in §1, §2 and the cyclotomic elements of Deligne and Soulé [2] [15] [16]. These cyclotomic elements (and their indexes) are useful for the arithmetic of cyclotomic fields. In this paper, we show that they can be used for a numerical verification of Greenberg's conjecture. For a totally real number field K and a prime number p, Greenberg's conjecture asserts that the Galois group of the maximal unramified abelian pro-p extension of the cyclotomic $\mathbf{Z}_p$-extension K^{cycl}_{∞} is finite [6]. When we check this conjecture numerically, one of the problems lay in studying the group of units. For example, it is difficult to find fundamental units in general. Kraft and Schoof [11] and Ichimura and Sumida [7] [8] found good criterions to verify this conjecture for real abelian number fields, in which they do not use fundamental units, but use only cyclotomic units. This paper is in the same stream and we do not use fundamental units either.

In §5, we give some simple criterions (Theorems 5.4, 5.8, cf. also Theorems 1.6, 2.5) on Greenberg's conjecture in some simple cases, and give some examples (Example 5.5 treats some quadratic fields with $p=3$ and Example 5.10 treats $K=\mathbf{Q}(\sqrt{m}, \cos(2\pi/7))$

Received October 4, 1995
Revised August 31, 1998

with $m < 1{,}000$ and $p = 7$).

The first version of this paper was written in 1995, but it took a long time for the publishing procedure, and I am responsible for this delay. I would like to thank H. Taya very much for his persuading me to complete this paper, and for a lot of discussions on Greenberg's conjecture with him. This paper was written just after Ichimura and Sumida [7] and was influenced by [7]. I would like to thank H. Ichimura for guiding me to the theory of cyclotomic fields more than ten years ago, and for some useful discussion. I would like to thank K. Komatsu for discussion about several related topics, and to thank H. Sumida for discussion.

Notation. We denote by μ_n the group of n-th roots of unity in an algebraic closure of $\mathbf{Q}$. For a number field F, O_F denotes its integer ring. For a prime number p, an integer r, and a $\mathbf{Z}_p$-module M with Galois action, $M(r)$ means the Tate twist, namely $M \otimes \mathbf{Z}_p(1)^{\otimes r}$ where $\mathbf{Z}_p(1) = \varprojlim \mu_{p^n}$. For a group G and a G-module M, we denote by M^G (resp. M_G) the invariant part (resp. the coinvariant) of M, namely $M^G = \{x \in M : \sigma(x) = x \text{ for all } \sigma \in G\}$ and $M_G = M/\langle(\sigma - 1)x : \sigma \in G, x \in M\rangle$. For an abelian group A and an integer $n > 0$, the cokernel of the multiplication by n is denoted by A/n. Even in the case A is multiplicative, we use A/n instead of A/A^n.

1. The elements $c_{l,r}$ in a finite field and a positive integer $n(r)$.

In this section, we treat "the trivial character" case at first. Let l be an odd prime number and g be a primitive root mod l. Namely, g is an element of $\mathbf{F}_l$ which generates the multiplicative group $\mathbf{F}_l^\times$. For a positive integer r greater than 1, we define

$$c_{l,r} = \prod_{i=1}^{l-2} (1 - g^i)^{i^{r-1}} \tag{1}$$

which is an element of $\mathbf{F}_l^\times$. For any element x in $\mathbf{F}_l^\times$, we define $\mathrm{order}_{\mathbf{F}_l^\times}(x)$ to be the order of x in the group $\mathbf{F}_l^\times$. We also define $\mathrm{index}_l(x)$ to be the index of the subgroup generated by x in $\mathbf{F}_l^\times$. So we have $\mathrm{index}_l(x) = (l-1)/\mathrm{order}_{\mathbf{F}_l^\times}(x)$. We are interested in the value $\mathrm{index}_l(c_{l,r})$. We can easily show that $\mathrm{index}_l(c_{l,r})$ does not depend on the choice of a primitive root g. Here is a table of this value.

l	$r=2$	$r=3$	$r=4$	$r=5$
3	1	1	1	1
5	1	1	1	1
7	2	2	2	2
11	5	1	1	1
13	1	1	1	1
17	4	2	4	2
19	3	1	3	1
23	22	2	22	2
29	7	1	7	1
31	10	2	2	10

Apparently these values have a different nature according as r is even or odd. In fact, if r is even, $\mathrm{order}_{\mathbf{F}_l^\times}(c_{l,r})$ is small, so $\mathrm{index}_l(c_{l,r})$ becomes big.

LEMMA 1.1. *If $r \geq 2$ is even,* $\mathrm{order}_{\mathbf{F}_l^\times}(c_{l,r})$ *is bounded by the denominator of $\zeta(1-r)$ where $\zeta(s)$ is the Riemann zeta function.*

On the other hand, if r is odd, $\mathrm{index}_l(c_{l,r})$ is usually small, but we have

LEMMA 1.2. *If $r \geq 3$ is odd, for a prime number p and $n > 0$, there exists l such that p^n divides* $\mathrm{index}_l(c_{l,r})$.

The lemmas in this section will be proved in §3. By Lemma 1.2, the least common multiple of all $\mathrm{index}_l(c_{l,r})$'s (where l ranges over all odd prime numbers) is infinity. We would also like to consider the greatest common divisor of them. But $\mathrm{index}_l(c_{l,r})$ always divides $l-1$, so we have to modify the definition of $\mathrm{index}_l(x)$.

For a prime number p, we denote by v_p the normalized additive valuation (namely, $v_p(p)=1$). For x in $\mathbf{F}_l^\times$ and a prime number p, we define $\mathrm{index}_l(x)_p^*$ to be $p^{v_p(\mathrm{index}_l(x))}$ if $v_p(\mathrm{index}_l(x)) < v_p(l-1)$, and to be p^∞ otherwise. Hence if p is prime to $l-1$, by definition, $\mathrm{index}_l(x)_p^* = p^\infty$. We define

$$\mathrm{index}_l(x)^* := \prod_p \mathrm{index}_l(x)_p^* \tag{2}$$

where p ranges over all prime numbers.

DEFINITION 1.3. We define $n(r)$ to be the greatest common divisor of all $\mathrm{index}_l(c_{l,r})^*$ where l ranges over all odd prime numbers. (The greatest common divisor is calculated formally for p^∞.) We denote by $n(r)_p$ the p-part of $n(r)$ (so $n(r) = \prod_p n(r)_p$).

LEMMA 1.4. $n(r)_p \neq p^\infty$.

The proof will be given in §3. Further, the coincidence of Deligne-Soulé's cyclotomic element with Beilinson's cyclotomic element implies $n(r) \neq \infty$, namely $n(r)$ is a positive integer.

This number $n(r)$ is closely related to the arithmetic of the cyclotomic fields. For example, we can reformulate [17] Proposition 8.18 as follows.

PROPOSITION 1.5 ([17] Proposition 8.18). *For an odd prime number p, let μ_p be the group of p-th roots of unity, and $A_{(p)}$ be the p-Sylow subgroup of the ideal class group of $\mathbf{Q}(\mu_p)$. Let ω be the Teichmüller character for $\Delta_{(p)} = \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$. We denote by $A_{(p)}^{\omega^i}$ the subgroup of $A_{(p)}$ on which $\Delta_{(p)}$ acts via ω^i. Then, for an odd positive integer $r \geq 3$, $n(r) = 1$ if and only if $A_{(p)}^{\omega^{1-r}} = 0$ for every odd prime number p.*

By this proposition we know that Vandiver's conjecture predicts $n(r)=1$ for any odd positive integer $r \geq 3$. By [12] Corollary 3.8, we have $n(3)=1$. On the other hand, as we will see below, Greenberg's conjecture predicts a weaker form that $n(r)_p$'s are bounded when r ranges over all odd positive integers ≥ 3.

We fix an odd prime number $p$. Let $\mathbf{Q}_\infty = \mathbf{Q}(\mu_{p^\infty})$ be the field generated by all p^n-th roots of unity, and L_∞ be the maximal unramified abelian pro-$p$ extension of $\mathbf{Q}_\infty$, and $X_{\mathbf{Q}_\infty} = \mathrm{Gal}(L_\infty/\mathbf{Q}_\infty)$. We also denote by X^{ω^i} the subgroup of $X_{\mathbf{Q}_\infty}$ on which $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ $(=\Delta_{(p)})$ acts via ω^i. Put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]^{\omega^i} \simeq \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}(\mu_p))]]$, which is isomorphic to a power series ring over $\mathbf{Z}_p$. We regard X^{ω^i} as a $\Lambda$-module, and consider its characteristic power series $\in \Lambda$.

THEOREM 1.6. *Let r_0 be an odd positive integer $\geq 3$, and $p$ be a prime number. If $X^{\omega^{1-r_0}}$ is finite, the $p$-part $n(r)_p$ is bounded when $r \geq 3$ ranges over all $r \equiv r_0$* (mod$p-1$). *More precisely, the following conditions are equivalent.*

(i) *There exists a positive integer $n$ such that for any $r$ satisfying $r \equiv r_0$* (mod$p-1$) *and $r \geq 3$, p^n does not divide $n(r)$. (Namely, $n(r)_p$ is bounded for $r$ satisfying the condition above.)*

(ii) *The characteristic power series of $X^{\omega^{1-r_0}}$ does not have a root in $\mathbf{Z}_p$.*

The proof will be given in §4.

2. The case of nontrivial Dirichlet character.

In this section, for simplicity, we fix an odd prime number $p$ and study only $p$-part.

Let $N>0$ be an integer and $\chi\colon (\mathbf{Z}/N)^\times \to \mathbf{C}^\times$ be a nontrivial, primitive Dirichlet character. We assume that $\chi$ is *even* and that the order of $\chi$ divides $p-1$, and regard $\chi$ as a character

$$\chi : (\mathbf{Z}/N)^\times \to \mathbf{Z}_p^\times .$$

(We can treat more general $\chi$ by the same method, but it is not suitable very much for numerical calculation. So here, we restrict ourselves to the above case.)

Let $n$ be a positive integer. We consider a prime number $l$ such that $l \equiv 1$ (modp^nN). We put $M = (l-1)/p^nN$. Let $g$ be a primitive root mod$l$. For an odd positive integer $r$ and an integer $i$, we define

$$c_{l,N,r,p^n}(i) = \prod_{j=0}^{p^n-1} (1-g^{Mi+NMj})^{NM(i+Nj)^{r-1}} \in \mathbf{F}_l^\times . \tag{3}$$

Note that by definition $c_{l,N,r,p^n}(i)^{p^n} = 1$. Since the subgroup of p^n-th roots of unity in $\mathbf{F}_l^\times$ is a $\mathbf{Z}_p$-module and the image of $\chi$ is in $\mathbf{Z}_p$, $c_{l,N,r,p^n}(i)^{\chi(j)}$ can be naturally defined. We define

$$c_{l,r,p^n}^\chi = \prod_{\substack{i=1 \\ (i,N)=1}}^{N} c_{l,N,r,p^n}(i)^{\chi(i)^{-1}} \in \mathbf{F}_l^\times . \tag{4}$$

LEMMA 2.1. *Suppose $l$ is a prime number such that $l \equiv 1$* (modp^nN), *and $m \geq 0$ is an integer with $m<n$. Then we have*

$$(c_{l,r,p^n}^\chi)^{p^m} = c_{l,r,p^{n-m}}^\chi .$$

PROOF. It is enough to show $c_{l,N,r,p^n}(i)^p = c_{l,N,r,p^{n-1}}(i)$ for $n \geq 2$. We put $M = (l-1)/p^n N$. Then we have

$$c_{l,N,r,p^n}(i)^p = \prod_{j=0}^{p^n-1} (1 - g^{Mi+NMj})^{NMp(i+Nj)^{r-1}}$$

$$= \prod_{j=0}^{p^{n-1}-1} (1 - g^{(Mi+NMj)p})^{NMp(i+Nj)^{r-1}} = c_{l,N,r,p^{n-1}}(i)\,.$$

Here, in order to get the second equality, we used $\prod_{k=0}^{p-1} (1 - xg^{NMp^{n-1}k}) = 1 - x^p$. □

Let $\mathrm{order}_{\mathbf{F}_l^\times}(x)$ be as in §1. For $x \in \mathbf{F}_l^\times$ such that $x^{p^n} = 1$, we define $\mathrm{index}_{l,p^n}(x)^*$ to be $p^n/\mathrm{order}_{\mathbf{F}_l^\times}(x)$ if $p^n/\mathrm{order}_{\mathbf{F}_l^\times}(x) < p^n$, and to be p^∞ otherwise. Then, we can show that $\mathrm{index}_{l,p^n}(c_{l,r,p^n}^\chi)^*$ does not depend on the choice of the primitive root g. As in §1, we define

DEFINITION 2.2. We define $n^\chi(r)_p$ to be the greatest common divisor of all $\mathrm{index}_{l,p^n}(c_{l,r,p^n}^\chi)^*$ where l (resp. n) ranges over all prime numbers (resp. all positive integers) such that $l \equiv 1 \pmod{p^n N}$.

Again we have

LEMMA 2.3. $n^\chi(r)_p \neq p^\infty$

which will be seen in §3. So $n^\chi(r)_p$ is an integer (some power of p).

LEMMA 2.4. *Assume* $r \equiv r' \pmod{(p-1)p^{n-1}}$. *Then,* p^n *divides* $n^\chi(r)_p$ *if and only if* p^n *divides* $n^\chi(r')_p$.

The proof is straightforward from the definition of $c_{l,r,N,p^n}(i)$, so we omit it. This lemma can be regarded as an analogy of a weak version of Kummer congruence.

Let $\mathbf{Q}(\mu_N)$ be the field of the N-th roots of unity, and K be the subfield of $\mathbf{Q}(\mu_N)$ which corresponds by Galois theory to the kernel of χ. Put $K_\infty = K(\mu_{p^\infty})$ the field generated by all p^n-th roots of unity over K. Let L_∞ be the maximal unramified abelian pro-p extension of K_∞, and $X_{K_\infty} = \mathrm{Gal}(L_\infty/K_\infty)$.

We regard $\chi : \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{Z}_p^\times$ as a character of $\mathrm{Gal}(K(\mu_p)/\mathbf{Q})$ by composing it with a natural map $\mathrm{Gal}(K(\mu_p)/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$. In general, for a character ψ of $\mathrm{Gal}(K(\mu_p)/\mathbf{Q})$ and $\mathbf{Z}_p[\mathrm{Gal}(K(\mu_p)/\mathbf{Q})]$-module M, we define the ψ-component by $M^\psi = M \otimes_{\mathbf{Z}_p[\mathrm{Gal}(K(\mu_p)/\mathbf{Q})]} \mathbf{Z}_p[\psi]$ where $\mathbf{Z}_p[\psi]$ is a ring generated by the image of ψ over $\mathbf{Z}_p$, and we regard it as a $\mathbf{Z}_p[\mathrm{Gal}(K(\mu_p)/\mathbf{Q})]$-module by $\sigma \cdot x = \psi(\sigma)x$ for $\sigma \in \mathrm{Gal}(K(\mu_p)/\mathbf{Q})$ and $x \in \mathbf{Z}_p[\psi]$. We consider $X_{K_\infty}^\chi$ which is a $\mathbf{Z}_p[\chi][[\mathrm{Gal}(K_\infty/K(\mu_p))]]$-module. Put $\Lambda = \mathbf{Z}_p[\chi][[\mathrm{Gal}(K_\infty/K(\mu_p))]]$. By our assumption $\mathrm{Image}(\chi) \subset \mathbf{Z}_p$, Λ is isomorphic to the formal power series ring $\mathbf{Z}_p[[T]]$. We denote $X_{K_\infty}^\chi$ simply by X^χ.

Our basic criterion is described as follows.

THEOREM 2.5. *We fix an odd positive integer* $r_0 \geq 3$.

(1) *Let* ω *be the Teichmüller character. Assume that* $\chi\omega^{1-r_0}(p) \neq 1$. *We put* $\psi = \chi\omega^{1-r_0}$. *Then, the following conditions are equivalent.*

(i) *There exists some positive integer n such that for any r satisfying* $r\equiv r_0 \pmod{p-1}$ *and* $r\geq 3$, p^n *does not divide* $n^{\chi}(r)_p$. (*Namely,* $n^{\chi}(r)_p$ *is bounded for r satisfying the condition above.*)

(ii) *The characteristic power series of* X^{ψ} $(=X^{\chi\omega^{1-r_0}})$ *does not have a root in* $\mathbf{Z}_p$.

(2) *Assume that* $\chi\neq 1$ *and* $\chi(p)=1$. *For* $r\equiv 1 (\mathrm{mod}\, p-1)$, *put* $a_r=v_p(r-1)+1$ (v_p *is the normalized additive valuation of p such that* $v_p(p)=1$). *Then, the following conditions are equivalent.*

(i) *There exists some positive integer n such that for any r satisfying* $r\geq 3$ *and* $r\equiv 1(\mathrm{mod}\, p-1)$, p^{n+a_r} *does not divide* $n^{\chi}(r)_p$. (*Namely,* $n^{\chi}(r)_p/p^{a_r}$ *is bounded for r satisfying the condition above.*)

(ii) *The characteristic power series of* X^{χ} *does not have a root in* $\mathbf{Z}_p$.

Note that by Lemma 2.4, in order to show that p^n does not divide $n^{\chi}(r)_p$ for all r, it suffices to check finitely many r's.

In many cases the characteristic power series of X^{ψ} has its every root in $\mathbf{Z}_p$. For example, if every root of the characteristic power series of $X^{\psi^{-1}\omega}$ is in $\mathbf{Z}_p$ (this condition is automatically satisfied if its λ-invariant is 1), then every root of the characteristic power series of X^{ψ} is in $\mathbf{Z}_p$. So in this case if we check the condition (i), then we know the λ-invariant of X^{ψ} vanishes. Note that in [7] they assume the λ-invariant of $X^{\psi^{-1}\omega}$ is 1, although they do not need this assumption in their succeeding work [8].

We will give some criterions in §5 which are more suitable for numerical calculation.

3. Cyclotomic elements.

Let ζ be a primitive N-th root of unity, and $r\geq 2$ be an integer. We consider a Galois cohomology group $H^1(\mathbf{Q}(\zeta), \hat{\mathbf{Z}}(r))=\prod_p H^1(\mathbf{Q}(\zeta), \mathbf{Z}_p(r))$ (where $\mathbf{Z}_p(r)$ is the Tate twist and p ranges over all prime numbers), in which there is a cyclotomic element $c_r^D(\zeta)$ by Deligne and Soulé ([16], [2]).

LEMMA 3.1 (cf. [1] page 384). *There exists an element*

$$c_r^D(\zeta)\in H^1(\mathbf{Q}(\zeta), \hat{\mathbf{Z}}(r))$$

which satisfies the following property. For any integer $m\geq 1$, *the image of* $N^{r-1}c_r^D(\zeta)$ *in*

$$H^1(\mathbf{Q}(\mu_{mN}), \mathbf{Z}/m(r))\simeq(\mathbf{Q}(\mu_{mN})^{\times}/m)\otimes\mu_m^{\otimes(r-1)}$$

(*note that* $\mathbf{Q}(\mu_{mN})^{\times}/m$ *means* $\mathbf{Q}(\mu_{mN})^{\times}/(\mathbf{Q}(\mu_{mN})^{\times})^m$ (*cf. notation*)) *coincides with*

$$\sum_{w^m=\zeta}(1-w)\otimes(w^N)^{\otimes(r-1)}$$

where w ranges over all m-th roots of ζ (*resp. all m-th roots of unity except* 1) *if* $\zeta\neq 1$ (*resp.* $\zeta=1$).

Further, this property characterizes the element $c_r^D(\zeta)$ *modulo torsion elements.*

We will sketch the proof. Let p be a prime number. We denote by (ζ_{p^n}) a generator of $\mathbf{Z}_p(1)$ (namely, ζ_{p^n} is a primitive p^n-th root of unity such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$).

We first assume N is prime to p. We put $F = \mathbf{Q}(\mu_N)$ and $F_n = \mathbf{Q}(\mu_{Np^n})$. We define $\alpha_n^{(p)} \in (F_n^\times/p^n) \otimes \mu_{p^n}^{\otimes(r-1)} \simeq H^1(F_n, \mathbf{Z}/p^n(r))$ by

$$\alpha_n^{(p)} = (1 - \zeta^{1/p^n}\zeta_{p^n}) \otimes \zeta_{p^n}^{\otimes(r-1)} + (1 - \zeta^{1/p^{n+1}}\zeta_{p^n}) \otimes \zeta_{p^{n-1}}^{\otimes(r-1)} + \cdots + (1 - \zeta^{1/p^{2n-1}}\zeta_{p^n}) \otimes \zeta_p^{\otimes(r-1)}$$

where ζ^{1/p^m} is the unique element of μ_N such that $(\zeta^{1/p^m})^{p^m} = \zeta$. We denote by

$$N_{F_n/F} : H^1(F_n, \mathbf{Z}/p^n(r)) \simeq (F_n^\times/p^n) \otimes \mu_{p^n}^{\otimes(r-1)} \to H^1(F, \mathbf{Z}/p^n(r))$$

the corestriction map. Then the elements $N_{F_n/F}(\alpha_n^{(p)}) \in H^1(F, \mathbf{Z}/p^n(r))$ form a projective system ([15] Lemma 1). We define $c_r^D(\zeta)^{(p)} = (N_{F_n/F}(\alpha_n^{(p)})) \in H^1(F, \mathbf{Z}_p(r))$.

Next we assume p divides N, so $N = p^m N'$ for some $m > 0$ and N' which is prime to p. We put $F = \mathbf{Q}(\mu_N)$ and $F_n = \mathbf{Q}(\mu_{N'p^n})$ with $n \geq m$. We write $\zeta = (\zeta')^{1/p^m}\zeta_{p^m}^i$ with $\zeta' \in \mu_{N'}$. This time, we define $\alpha_n^{(p)}$ by

$$\alpha_n^{(p)} = (1 - (\zeta')^{1/p^n}\zeta_{p^n}^i) \otimes (\zeta_{p^n}^i)^{\otimes(r-1)},$$

and consider $N_{F_n/F}(\alpha_n^{(p)}) \in H^1(F, \mathbf{Z}/p^n(r))$. We put $c_r^D(\zeta)^{(p)} = (N_{F_n/F}(\alpha_n^{(p)})) \in H^1(F, \mathbf{Z}_p(r))$.

We define $c_r^D(\zeta) = (c_r^D(\zeta)^{(p)}) \in H^1(F, \hat{\mathbf{Z}}(r))$. Then we can check $c_r^D(\zeta)$ satisfies the property in Lemma 3.1. Uniqueness comes from the fact that the intersection of the kernels of $H^1(\mathbf{Q}(\mu_N), \hat{\mathbf{Z}}(r)) \to H^1(\mathbf{Q}(\mu_{mN}), \mathbf{Z}/m(r))$ for all m consists of torsion elements. □

For any number field F and a prime number p, we consider etale cohomology groups $H_{et}^*(\mathit{Spec}\, O_F[1/p], \mathbf{Z}_p(r))$, which we simply denote by $H^*(O_F[1/p], \mathbf{Z}_p(r))$.

By the construction of $c_r^D(\zeta)^{(p)}$ in the proof above, it is in the subgroup $H^1(\mathbf{Z}[\zeta, 1/p], \mathbf{Z}_p(r))$ of $H^1(\mathbf{Q}(\zeta), \mathbf{Z}_p(r))$. For a number field F and a prime number l which is different from p, we consider a natural map

$$\phi_{l,F,n} : H^1(O_F[1/p], \mathbf{Z}/p^n(r)) \to \bigoplus_{\lambda | l} H^1(\kappa(\lambda), \mathbf{Z}/p^n(r))$$

where λ ranges over all primes of F over l, and $\kappa(\lambda) = O_F/\lambda$ is the residue field of λ.

LEMMA 3.2. (i) *For any element* $x \in H^1(\mathbf{Z}[\zeta, 1/p], \mathbf{Z}/p^n(r))$ *there is a prime number* l *such that* $l \equiv 1 \pmod{Np^n}$ *and that* $\phi_{l,\mathbf{Q}(\zeta),n}(x) = 0$.

(ii) *Assume* K *is real abelian, and* r *and* p *are odd. If* $x \in H^1(O_K[1/p], \mathbf{Z}/p^n(r))$ *satisfies* $x \notin p^i H^1(O_K[1/p], \mathbf{Z}/p^n(r))$, *there is a prime number* l *such that* $l \equiv 1 \pmod{Np^n}$ *and that* $\phi_{l,K,n}(x) \notin p^i \bigoplus_{\lambda | l} H^1(\kappa(\lambda), \mathbf{Z}/p^n(r))$.

PROOF. (i) Let ζ_{p^n} be a primitive p^n-th root of unity. Put $L = \mathbf{Q}(\zeta, \zeta_{p^n})$. We denote the image of x in $H^1(L, \mathbf{Z}/p^n(r)) \simeq (L^\times/p^n) \otimes \mu_{p^n}^{\otimes(r-1)}$ by $x' \otimes \zeta_{p^n}^{\otimes(r-1)}$. By Chebotarev density, we can take a prime number l which splits completely at $L(\sqrt[p^n]{x'})/\mathbf{Q}$. Then, $\phi_{l,L,n}(x' \otimes \zeta_{p^n}^{\otimes(r-1)}) = 0$, so $\phi_{l,\mathbf{Q}(\zeta),n}(x) = 0$.

(ii) As in (i) we put $L = K(\zeta_{p^n})$ and take x'. By our assumption, we have

$H^0(L/K, \mathbf{Z}/p^n(r))=0$, so $H^1(O_K[1/p], \mathbf{Z}/p^n(r)) \rightarrow H^1(O_L[1/p], \mathbf{Z}/p^n(r))$ is injective. By Chebotarev density, we can take a prime number l which splits completely at $L/\mathbf{Q}$ such that the Frobenius of a prime λ of L over l generates the Galois group of $L(\sqrt[p^n]{x'})/L$. Then, $\phi_{l,L,n}(x' \otimes \zeta_{p^n}^{\otimes(r-1)})$ is not divisible by p^i, so we get the assertion. □

We proceed to the proof of Lemmas in §1 and §2.

First of all, we consider $c_r^D(1) \in H^1(\mathbf{Q}, \hat{\mathbf{Z}}(r))$. For a prime number $l \geq 3$, put $L=\mathbf{Q}(\mu_{l-1})$. We take a primitive $(l-1)$-th root ξ of unity. The image of $c_r^D(1)$ in $H^1(L, (\mathbf{Z}/(l-1))(r)) \simeq L^\times/(l-1) \otimes \mu_{l-1}^{\otimes(r-1)}$ is by Lemma 3.1,

$$\sum_{i=1}^{l-2} (1-\xi^i) \otimes (\xi^i)^{\otimes(r-1)} = \left(\prod_{i=1}^{l-2} (1-\xi^i)^{i^{r-1}} \right) \otimes \xi^{\otimes(r-1)}.$$

We suppose that p is a prime number such that p^n divides $l-1$. Then, the image of $c_r^D(1)$ in $H^1(L, \mathbf{Z}/p^n(r)) \simeq L^\times/p^n \otimes \mu_{p^n}^{\otimes(r-1)}$ is

$$\prod_{i=1}^{l-2} (1-\xi^i)^{i^{r-1}} \otimes (\xi')^{\otimes(r-1)}$$

where $\xi' = \xi^{(l-1)/p^n} \in \mu_{p^n} \subset L^\times$. Note that $c_r^D(1) = (c_r^D(1)^{(p)}) \in \prod_p H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$, and that the image of $c_r^{(D)}(1)$ in $H^1(L, \mathbf{Z}/p^n(r))$ is that of $c_r^D(1)^{(p)}$.

Hence, the index of the subgroup generated by the image of $c_r^D(1)^{(p)}$ in $H^1(\mathbf{F}_l, \mathbf{Z}/p^n(r)) = \mathbf{F}_l^\times/p^n \otimes \mu_{p^n}^{\otimes(r-1)}$ is equal to the index of the subgroup generated by $c_{l,r} = \prod_{i=1}^{l-2} (1-g^i)^{i^{r-1}} \operatorname{mod} (\mathbf{F}_l^\times)^{p^n}$ in $\mathbf{F}_l^\times/p^n$.

Proof of Lemma 1.4. Suppose $r \geq 3$ is odd and p is an odd prime number. Let $n(r)_p$ be the p-part of $n(r)$ defined in §1. Since $H^0(\mathbf{Q}, \mathbf{Z}/p(r))=0$, $H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))$ is a free $\mathbf{Z}_p$-module of rank 1 (cf. [15] Theorem 1). By Lemma 3.2 (ii), considering the index of the image of $c_r^D(1)^{(p)}$ in $H^1(\mathbf{F}_l, \mathbf{Z}/p^n(r))$ above, we have

$$n(r)_p = \sharp(H^1(\mathbf{Z}[1/p], \mathbf{Z}_p(r))/\langle c_r^D(1)^{(p)} \rangle) \tag{5}$$

where $\langle c_r^D(1)^{(p)} \rangle$ is the $\mathbf{Z}_p$-submodule generated by $c_r^D(1)^{(p)}$. By [16] §6 (cf. [16] Th. 3 and the proof of [15] Th. 1), the right hand side is finite, so we get Lemma 1.4 in §1 for odd p.

For $p=2$, we have $c_{3,r} = 1-2 = -1$ for all r, so $\operatorname{index}_3(c_{3,r})=1$ and $n(r)_2=1$. □

If Beilinson's cyclotomic element coincides with Deligne-Soulé's element, we have $n(r) < \infty$. In fact, if $c_r^D(1)$ coincides with Beilinson's cyclotomic element (this was announced by Beilinson), $c_r^D(1)$ comes from the K-group $K_{2r-1}(\mathbf{Z})$, namely there is an element $c_r(1) \in K_{2r-1}(\mathbf{Z})$ whose image in $H^1(\mathbf{Q}, \hat{\mathbf{Z}}(r))$ is $c_r^D(1)$ (because Beilinson's element lives in $K_{2r-1}(\mathbf{Z}) \otimes \mathbf{Q}$). So the coincidence of Beilinson's element and Deligne-Soulé's element implies $n(r) \leq \sharp(K_{2r-1}(\mathbf{Z})/\langle c_r(1) \rangle) < \infty$.

Proof of Lemma 1.1. If $r \geq 2$ is even, $H^1(\mathbf{Q}, \hat{\mathbf{Z}}(r))$ is isomorphic to $H^0(\mathbf{Q}, \mathbf{Q}/\mathbf{Z}(r))$ whose order is equal to the denominator of $\zeta(1-r)$. Let l be an odd prime number. As we have seen, for a prime number p such that p^n divides $l-1$, the p-part of $\operatorname{order}_{\mathbf{F}_l^\times}(c_{l,r})$ is the order of the image of $c_r^D(1)^{(p)}$ in $H^1(\mathbf{F}_l, \mathbf{Z}/p^n(r))$. This implies that $\operatorname{order}_{\mathbf{F}_l^\times}(c_{l,r})$ is bounded by the denominator of $\zeta(1-r)$.

PROOF OF LEMMA 1.2. Let $r\geq 3$ be odd. For a prime number p and $n>0$, by Lemma 3.2 (i), there is a prime number l such that $l\equiv 1 \pmod{p^n}$ and that the image of $c_r^D(1)^{(p)}$ in $H^1(\mathbf{F}_l, \mathbf{Z}/p^n(r))$ is zero. So $c_{l,r}\in(\mathbf{F}_l^\times)^{p^n}$, hence p^n divides $\operatorname{index}_l(c_{l,r})$.

In the rest of this section, as in §2 we assume p is an odd prime number, and χ is an even nontrivial Dirichlet character of conductor N with order dividing $p-1$. We denote by K the real abelian field corresponding to the kernel of χ. Let ζ_N be a primitive N-th root of unity. For an odd integer $r\geq 3$, we define

$$(c_r^{(p)})^\chi = \sum_{\substack{i=1\\(i,N)=1}}^{N} \chi(i)^{-1} c_r^D(\zeta_N^i)^{(p)} \in H^1(\mathbf{Z}[\zeta_N, 1/p], \mathbf{Z}_p(r)) .$$

Since $(c_r^{(p)})^\chi$ is in the $\operatorname{Gal}(\mathbf{Q}(\zeta_N)/K)$-invariant part, we regard $(c_r^{(p)})^\chi$ as an element of $H^1(O_K[1/p], \mathbf{Z}_p(r))\simeq H^1(\mathbf{Z}[\zeta_N, 1/p], \mathbf{Z}_p(r))^{\operatorname{Gal}(\mathbf{Q}(\zeta_N)/K)}$.

For a $\mathbf{Z}_p[\operatorname{Gal}(K/\mathbf{Q})]$-module M, we define M^χ to be the χ-component of M (as in §2), namely $M^\chi = M\otimes_{\mathbf{Z}_p[\operatorname{Gal}(K(\mu_p)/\mathbf{Q})]}\mathbf{Z}_p[\chi]$ where $\mathbf{Z}_p[\chi]$ is a ring $\mathbf{Z}_p$ on which $\operatorname{Gal}(K/\mathbf{Q})$ acts via χ (note that we are assuming $\operatorname{Image}(\chi)\subset\mathbf{Z}_p$). We may regard

$$(c_r^{(p)})^\chi \in H^1(O_K[1/p], \mathbf{Z}_p(r))^\chi .$$

LEMMA 3.3. *Let ζ_N be a primitive N-th root of unity with $N>1$ as above, and (ζ_{p^n}) be a generator of $\mathbf{Z}_p(1)$ (so $\zeta_{p^{n+1}}^p=\zeta_{p^n}$).*

(i) *We assume N is prime to p. We put $\xi=\zeta_N^{1/p^n}\zeta_{p^n}^{1/N}$ which is a primitive Np^n-th root of unity. (Here, ζ_N^{1/p^n} (resp. $\zeta_{p^n}^{1/N}$) is a unique element of μ_N (resp. μ_{p^n}) such that $(\zeta_N^{1/p^n})^{p^n}=\zeta_N$ (resp. $(\zeta_{p^n}^{1/N})^N=\zeta_{p^n}$).) For any i, the image of $c_r^D(\zeta_N^i)^{(p)}$ in*

$$H^1(\mathbf{Q}(\mu_{Np^n}), \mathbf{Z}/p^n(r))\simeq(\mathbf{Q}(\mu_{Np^n})^\times/p^n)\otimes\mu_{p^n}^{\otimes(r-1)}$$

is

$$N^{1-r}\prod_{j=0}^{p^n-1}(1-\xi^{i+Nj})^{(i+Nj)^{r-1}}\otimes\zeta_{p^n}^{\otimes(r-1)} .$$

(ii) *We assume $N=pN'$ and N' is prime to p. Write $\zeta_N=\zeta_{N'}\zeta_p^{1/N'}$ where $\zeta_{N'}$ is a primitive N'-th root of unity. We put $\xi=\zeta_{N'}^{1/p^n}\zeta_{p^{n+1}}^{1/N'}$. For i which is prime to p, the image of $c_r^D(\zeta_N^i)^{(p)}$ in*

$$H^1(\mathbf{Q}(\mu_{Np^n}), \mathbf{Z}/p^n(r))\simeq(\mathbf{Q}(\mu_{Np^n})^\times/p^n)\otimes\mu_{p^n}^{\otimes(r-1)}$$

is

$$(N')^{1-r}\prod_{j=0}^{p^n-1}(1-\xi^{i+Nj})^{(i+Nj)^{r-1}}\otimes\zeta_{p^n}^{\otimes(r-1)} .$$

PROOF. (i) By Lemma 3.1, the image of $c_r^D(\zeta_N^i)$ is

$$N^{1-r}\sum_{j=0}^{p^n-1}(1-\zeta_N^{i/p^n}\zeta_{p^n}^j)\otimes(\zeta_{p^n}^{Nj})^{\otimes(r-1)}=\sum_{j=0}^{p^n-1}(1-\zeta_N^{i/p^n}\zeta_{p^n}^{i/N}\zeta_{p^n}^j)\otimes(\zeta_{p^n}^{i/N}\zeta_{p^n}^j)^{\otimes(r-1)}$$

$$=N^{1-r}\prod_{j=0}^{p^n-1}(1-\xi^{i+Nj})^{(i+Nj)^{r-1}}\otimes\zeta_{p^n}^{\otimes(r-1)}.$$

(ii) By the construction in Lemma 3.1, the image of $c_r^D(\zeta_N^i)$ in $H^1(\mathbf{Q}(\mu_{Np^n}), \mathbf{Z}/p^{n+1}(r))$ is

$$\sum_{\sigma\in\mathrm{Gal}(\mathbf{Q}(\mu_{Np^n})/\mathbf{Q}(\mu_N))}\sigma((1-\zeta_{N'}^{i/p^n}\zeta_{p^{n+1}}^{i/N'})\otimes(\zeta_{p^{n+1}}^{i/N'})^{\otimes(r-1)})$$

$$=\sum_{q=0}^{p^n-1}(1-\zeta_{N'}^{i/p^n}\zeta_{p^{n+1}}^{(1+pq)i/N'})\otimes(\zeta_{p^{n+1}}^{(1+pq)i/N'})^{\otimes(r-1)}$$

$$=\sum_{q=0}^{p^n-1}(1-\xi^i\xi^{N'pq(i/N')})\otimes(\zeta_{p^{n+1}}^{(1+pq)i/N'})^{\otimes(r-1)}$$

$$=\sum_{j=0}^{p^n-1}(1-\xi^i\xi^{Nj})\otimes(\zeta_{p^{n+1}}^{(i/N')+(Nj/N')})^{\otimes(r-1)}\quad(\text{where } j=qi/N'\in\mathbf{Z}/p^n)$$

$$=(N')^{1-r}\prod_{j=0}^{p^n-1}(1-\xi^{i+Nj})^{(i+Nj)^{r-1}}\otimes\zeta_{p^{n+1}}^{\otimes(r-1)}.\quad\square$$

PROOF OF LEMMA 2.3. Let n be a positive integer, and l be a prime number such that $l\equiv 1\ (\mathrm{mod}\,p^nN)$. Let g be a primitive root of $\mathbf{F}_l^\times$. We put $M=(l-1)/p^nN$, and define

$$c'_{l,N,r,p^n}(i)=\prod_{j=0}^{p^n-1}(1-g^{Mi+NMj})^{(i+Nj)^{r-1}}\,\mathrm{mod}(\mathbf{F}_l^\times)^{p^n}\in\mathbf{F}_l^\times/p^n$$

and $(c'_{l,r,p^n})^\chi=\prod_{i=1}^N(c'_{l,N,r,p^n}(i))^{\chi(i)^{-1}}$. So the order of $(c'_{l,r,p^n})^\chi$ in $\mathbf{F}_l^\times/p^n$ is the same as that of c_{l,r,p^n}^χ in $\mathbf{F}_l^\times$ where c_{l,r,p^n}^χ is the element defined in §2 (4). We consider $(\bigoplus_{\lambda|l}H^1(\kappa(\lambda), \mathbf{Z}/p^n(r)))^\chi$ where λ ranges over all primes of K over l. By Lemma 3.3, the order of the image of $(c_r^{(p)})^\chi$ in $(\bigoplus_{\lambda|l}H^1(\kappa(\lambda), Z/p^n(r)))^\chi$ is equal to the order of $(c'_{l,r,p^n})^\chi$ in $\mathbf{F}_l^\times/p^n$, so equal to $\mathrm{order}_{\mathbf{F}_l^\times}(c_{l,r,p^n}^\chi)$.

For a totally real number field F and an odd integer $r\geq 3$, $H^1(O_F[1/p], \mathbf{Z}_p(r))$ is a $\mathbf{Z}_p$-module of rank $[F:\mathbf{Q}]$ ([15] Theorem 1). From $H^0(O_K[1/p], \mathbf{Z}/p(r))=0$, $H^1(O_K[1/p], \mathbf{Z}_p(r))^\chi$ is a free $\mathbf{Z}_p$-module of rank 1 (note that we are assuming $\mathrm{Image}(\chi)\subset\mathbf{Z}_p$). So by Lemma 3.2 (ii), we have

$$n^\chi(r)_p=\#(H^1(O_K[1/p], \mathbf{Z}_p(r))^\chi/\langle(c_r^{(p)})^\chi\rangle)\qquad(6)$$

where $\langle(c_r^{(p)})^\chi\rangle$ is the subgroup generated by $(c_r^{(p)})^\chi$. Hence by [16] §6 (cf. [16] Th. 3 and the proof of [15] Th. 1), we have $n^\chi(r)_p<\infty$.

4. Proof of the theorems in sections 1 and 2.

Let χ be an even Dirichlet character of conductor N with order dividing $p-1$, and K be the real abelian field corresponding to the kernel of χ.

We denote by μ_{p^n} the group of p^n-th roots of unity, and define $K_n = K(\mu_{p^n})$, $K_\infty = \bigcup K_n$, and $G_\infty = \mathrm{Gal}(K_\infty/K)$. Remind our notation that $M(r)$ is the Tate twist and M^G (resp. M_G) is the G-invariants (resp. G-coinvariant) (cf. Notation).

Let E'_{K_n} be the group of p-units (units outside p) of K_n. Then by Kummer sequence and the Tate twists, we have an injection

$$E'_{K_n} \otimes \mathbf{Z}/p^n(r-1) \hookrightarrow H^1(O_{K_n}[1/p], \mathbf{Z}/p^n(r)).$$

Taking the projective limits with respect to the norm maps, we have

$$\varprojlim E'_{K_n}(r-1) = \varprojlim E'_{K_n} \otimes \mathbf{Z}_p(r-1) \hookrightarrow \varprojlim H^1(O_{K_n}[1/p], \mathbf{Z}_p(r)).$$

Let $\mathscr{C}_{K_n}$ be the subgroup of cyclotomic p-units in E'_{K_n}, namely $\mathscr{C}_{K_n} = N_{L_n/K_n}(\mathscr{C}_{L_n})$ where $L_n = \mathbf{Q}(\mu_N, \mu_{p^n})$ and N_{L_n/K_n} is the norm, and $\mathscr{C}_{L_n}$ is the intersection of $O_{L_n}[1/p]^\times$ and the group generated by $\{1-\zeta, \pm\zeta \mid \zeta$ is a root of unity in $L_n\}$. We have a canonical homomorphism

$$\begin{aligned}(\varprojlim \mathscr{C}_{K_n}(r-1))_{G_\infty} &\longrightarrow (\varprojlim E'_{K_n}(r-1))_{G_\infty} \\ &\longrightarrow (\varprojlim H^1(O_{K_n}[1/p], \mathbf{Z}_p(r)))_{G_\infty} \longrightarrow H^1(O_K[1/p], \mathbf{Z}_p(r))\end{aligned}$$

whose image we denote by C_r. Then, C_r is the group of cyclotomic elements.

Concerning C_r, Kolster, Nguyen Quang Do, and Fleckinger [10], after the case $K = \mathbf{Q}$ by Bloch and Kato [1], showed an analogy of the class number formula.

LEMMA 4.1 ([10] Theorem 5.4). $\sharp(H^1(O_K[1/p], \mathbf{Z}_p(r))/C_r) = \sharp H^2(O_K[1/p], \mathbf{Z}_p(r))$.

We consider their χ-components. We know C_r^χ is generated by $(c_r^{(p)})^\chi$ for $\chi \neq 1$, and by $c_r^D(1)^{(p)}$ for $\chi = 1$ (cf. [16] §4). Hence by (5) and (6) (note that $n^\chi(r)_p = n(r)_p$ if $\chi = 1$), we obtain

COROLLARY 4.2. $n^\chi(r)_p = \sharp(H^1(O_K[1/p], \mathbf{Z}_p(r))/C_r)^\chi = \sharp H^2(O_K[1/p], \mathbf{Z}_p(r))^\chi$.

On the other hand, $H^2(O_K[1/p], \mathbf{Z}_p(r))$ can be described as follows. Let $A'_{K_n} = Pic(O_{K_n}[1/p])$ be the p-Sylow subgroup of the p-ideal class group of $O_{K_n}[1/p]$ ($=$the Galois group of the maximal unramified abelian p-extension of K_n, in which every prime of K_n over p is completely decomposed). We put $X'_{K_\infty} = \varprojlim A'_{K_n}$. We also define $X_{K_\infty} = \varprojlim A_{K_n}$ where $A_{K_n} = Pic(O_{K_n})$ is the p-Sylow subgroup of the ideal class group of O_{K_n}.

LEMMA 4.3. *We have an exact sequence*

$$0 \longrightarrow X'_{K_\infty}(r-1)_{G_\infty} \longrightarrow H^2(O_K[1/p], \mathbf{Z}_p(r)) \longrightarrow \left(\bigoplus_{v \mid p} \mathbf{Z}_p\right)^0 (r-1)_{G_\infty} \longrightarrow 0.$$

Here, v ranges over all primes of K_∞ over p and $(\bigoplus \mathbf{Z}_p)^0$ means the kernel of the map $\bigoplus \mathbf{Z}_p \to \mathbf{Z}_p$, which sends (a_i) to Σa_i.

Indeed, by Kummer sequence and $\mathrm{Br}(O_{K_n}[1/p])$ (the Brauer group)$=(\bigoplus_{v|p}\mathbf{Z}_p)^0$, we have an exact sequence

$$0 \longrightarrow A'_{K_n}/p^n \longrightarrow H^2(O_{K_n}[1/p], \mathbf{Z}/p^n(1)) \longrightarrow \Big(\bigoplus_{v|p} \mathbf{Z}/p^n\Big)^0 \longrightarrow 0\,.$$

Taking $\otimes\, \mathbf{Z}_p(r-1)$ and taking the limit, we get an exact sequence

$$0 \longrightarrow X'_{K_\infty}(r-1) \longrightarrow \varprojlim H^2(O_{K_n}[1/p], \mathbf{Z}_p(r)) \longrightarrow \Big(\bigoplus_{v|p} \mathbf{Z}_p\Big)^0(r-1) \longrightarrow 0\,.$$

Taking Galois coinvariants, we get the conclusion.

We consider χ-component $H^2(O_K[1/p], \mathbf{Z}_p(r))^\chi$, and get

COROLLARY 4.4. (i) *We put $\psi=\chi\omega^{1-r}$. If $\psi(p)\neq 1$ or $\chi=1$, we have an isomorphism*

$$X^\psi_{K_\infty}(r-1)_{G_\infty} \xrightarrow{\simeq} H^2(O_K[1/p], \mathbf{Z}_p(r))^\chi\,.$$

(ii) *If $\chi\neq 1$, $\chi(p)=1$ and $r\equiv 1 \pmod{p-1}$, we have an exact sequence*

$$0 \longrightarrow (X'_{K_\infty})^\chi(r-1)_{G_\infty} \longrightarrow H^2(O_K[1/p], \mathbf{Z}_p(r))^\chi \longrightarrow \mathbf{Z}/p^{a_r} \longrightarrow 0$$

where $a_r=v_p(r-1)+1$ as in Theorem 2.5.

PROOF. (i) If $\psi(p)\neq 1$, we have $(\bigoplus_{v|p}\mathbf{Z}_p)^\psi=0$. If $\chi=1$, then $K_n=\mathbf{Q}(\mu_{p^n})$ and $(\bigoplus_{v|p}\mathbf{Z}_p)^0=(\mathbf{Z}_p)^0=0$. In both cases, we have $((\bigoplus_{v|p}\mathbf{Z}_p(r-1))^0)^\chi=((\bigoplus_{v|p}\mathbf{Z}_p)^0)^\psi(r-1)=0$. So by Lemma 4.3, $(X')^\psi_{K_\infty}(r-1)_{G_\infty}\simeq H^2(O_K[1/p], \mathbf{Z}_p(r))^\chi$. On the other hand, we have an exact sequence

$$\bigoplus_{v|p} \mathbf{Z}_p \longrightarrow X_{K_\infty} \longrightarrow X'_{K_\infty} \longrightarrow 0\,.$$

If $\psi(p)\neq 1$, taking ψ-components, we have $X^\psi_{K_\infty}\simeq(X')^\psi_{K_\infty}$. If $\chi=1$, then $K_n=\mathbf{Q}(\mu_{p^n})$ and the prime of K_n over p is principal. So $X'_{K_\infty}=X_{K_\infty}$, and we get the conclusion.

(ii) Since $\chi(p)=1$ and $\mathrm{Image}(\chi)\subset\mathbf{Z}_p$, we have $(\bigoplus_{v|p}\mathbf{Z}_p)^\chi=\mathbf{Z}_p$. If we denote by κ the cyclotomic character $G_\infty\to\mathbf{Z}_p^\times$, by our assumption on χ, the image of $\kappa: G_\infty\to\mathbf{Z}_p^\times$ is $1+p\mathbf{Z}_p$. So we can calculate $\mathbf{Z}_p(r-1)_{G_\infty}\simeq\mathbf{Z}/p^{a_r}$. We get the conclusion by taking the χ-component of the exact sequence in Lemma 4.3. □

From Corollaries 4.2 and 4.4, we have

COROLLARY 4.5. (i) *We put $\psi=\chi\omega^{1-r}$. If $\psi(p)\neq 1$ or $\chi=1$, we have*

$$\# X^\psi_{K_\infty}(r-1)_{G_\infty}=n^\chi(r)_p\,.$$

(ii) *If $\chi\neq 1$, $\chi(p)=1$, and $r\equiv 1 \pmod{p-1}$, we have*

$$\sharp(X'_{K_\infty})^\chi(r-1)_{G_\infty} = n^\chi(r)_p/p^{a_r}$$

where $a_r = v_p(r-1)+1$ *as in Theorem* 2.5.

We proceed to the proof of the theorems in sections 1 and 2.

We will prove Theorem 1.6. We take $\chi = 1$. We put $X = X_{\mathbf{Q}_\infty}$. For an odd integer $r_0 \ge 3$, we consider its ω^{1-r_0}-part $X^{\omega^{1-r_0}} = X_{\mathbf{Q}_\infty}^{\omega^{1-r_0}}$. Since the set $\{r \in \mathbf{Z};\ r \equiv r_0 (\mathrm{mod}\, p-1),\ r \ge 3\}$ is dense in $\mathbf{Z}_p$, the characteristic power series of $X^{\omega^{1-r_0}}$ has a root in $\mathbf{Z}_p$ if and only if for any $n > 0$ there exists $r \ge 3$ such that $r \equiv r_0 (\mathrm{mod}\, p-1)$, and that the order of $X^{\omega^{1-r_0}}(r-1)_{G_\infty}$ is greater than p^n. By Corollary 4.5 (i), $\sharp X^{\omega^{1-r_0}}(r-1)_{G_\infty} \ge p^n$ is equivalent to $p^n \mid n(r)_p$, which completes the proof of Theorem 1.6.

Theorem 2.5 can be proved by the same method as Theorem 1.6. For Theorem 2.5 (2), we note that the characteristic power series of X^χ is the same as that of X'^χ (modulo units).

5. Calculation and Examples.

In this section, we give some criterions which are more suitable for numerical calculation. We use the same notation as in the previous section. Let l be a prime number such that $l-1 = p^n NM$, and consider the element $c^\chi_{l,r,p^n} \in \mathbf{F}_l$ (see (4)). In the following, whenever we consider the element c^χ_{l,r,p^n}, we assume $p^n N$ divides $l-1$ without mentioning it.

We assume that $\chi \ne 1$ and the order of the character χ divides $p-1$.

We denote by K the field corresponding to χ, and by K_∞ the cyclotomic $\mathbf{Z}_p$-extension of $K(\mu_p)$. As in the previous section, let X_{K_∞} be the Galois group of the maximal unramified abelian pro-p extension of K_∞, and X'_{K_∞} be the Galois group of the maximal unramified abelian pro-p-extension of K_∞, in which every prime over p is completely decomposed. We simply write X for X_{K_∞} and X' for X'_{K_∞}. We define $G_\infty = \mathrm{Gal}(K_\infty/K)$.

The following lemma will be used many times.

LEMMA 5.1. *Assume* p^n *divides* $l-1$, *and* $\zeta_{p^n,l}$ *be a primitive* p^n*-th root of unity in* $\mathbf{F}_l$. *We write* $c^\chi_{l,r,p^n} = \zeta^a_{p^n,l}$ *with* $a \in \mathbf{Z}$. *If* $v_p(a) = i$ (v_p *is a normalized additive valuation such that* $v_p(p) = 1$) *and* $i < n$, *we have*

(i) *If* $\chi\omega^{1-r}(p) \ne 1$, *we have* $\sharp(X^\psi(r-1))_{G_\infty} \le p^i$.

(ii) *If* $\chi(p) = 1$ *and* $r \equiv 1$ $(\mathrm{mod}\, p-1)$, *we have* $\sharp((X')^\chi(r-1))_{G_\infty} \le p^{i-a_r}$ *where* $a_r = v_p(r-1)+1$.

PROOF. Since $\mathrm{order}_{\mathbf{F}_l^\times}(c^\chi_{l,r,p^n}) = p^{n-i} > 1$, $p^i = \mathrm{index}_{l,p^n}(c^\chi_{l,r,p^n})^*$ where $\mathrm{index}_{l,p^n}(x)^*$ was defined in §2 before Definition 2.2. So by the definition of $n^\chi(r)_p$, we have $n^\chi(r)_p \le p^i$. By Corollary 4.5, we get the conclusion. □

Let r_0 be an odd positive integer ≥ 3.

We begin with the case

(I) $\psi(p) \ne 1$ where $\psi = \chi\omega^{1-r_0}$.

LEMMA 5.2. *If there exists l such that $c^{\chi}_{l,r_0,p} \neq 1$, then $X^{\psi} = 0$.*

In fact, by Lemma 5.1 (i), $X^{\psi}(r-1)_{G_\infty} = 0$, so we get $X^{\psi} = 0$ by Nakayama's lemma.

We call this case the *trivial case*. In the following, we consider the non-trivial case, hence $c^{\chi}_{l,r_0,p} = 1$ for all l (which satisfy the conditions).

LEMMA 5.3. *Suppose c^{χ}_{l,r_0,p^n} is defined with $n \geq 2$ (so $p^n N$ divides $l-1$).*

(i) *Let $\zeta_{p^n,l}$ be a primitive p^n-th root of unity in $\mathbf{F}_l$. For a fixed odd positive integer $r_0 \geq 3$, there exists a polynomial $f(T) \in \mathbf{Z}/p^n[T]$ such that*

$$\log_{\zeta_{p^n,l}}(c^{\chi}_{l,r,p^n}) \equiv f((1+p)^{r-r_0}-1) \pmod{p^n}. \tag{7}$$

(ii) *Assume that there are some integers r_1, r_2, and an integer $n \geq 2$ such that $r_1 \equiv r_2 \equiv r_0 \pmod{p-1}$, $r_1 \equiv r_2 \pmod{(p-1)p^{n-2}}$ and that $c^{\chi}_{l,r_1,p^n} = 1$, $c^{\chi}_{l,r_2,p^n} \neq 1$. Then, the coefficient of degree* 1 *of the polynomial $f(T)$ in* (i) *is a unit in $\mathbf{Z}/p^n$.*

(iii) *Under the assumption of* (ii), *X^{ψ} is cyclic as a $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K(\mu_p))]](\simeq \mathbf{Z}_p[[T]])$-module.*

(iv) *Under the assumption of* (ii), *X^{ψ} is finite or isomorphic to $\mathbf{Z}_p$.*

PROOF. (i) First of all, i^r is an Iwasawa function for any $i \in \mathbf{Z}$, namely there is a power series $\varphi(T) \in \mathbf{Z}_p[[T]]$ such that $i^r = \varphi((1+p)^r - 1)$. So for any $r' \in \mathbf{Z}$, there is a power series $\varphi_{r_0,r'}(T) \in \mathbf{Z}_p[[T]]$ such that $i^{r-r'} = \varphi_{r_0,r'}((1+p)^{r-r_0}-1)$ for any $r \in \mathbf{Z}$. By the definition of c^{χ}_{l,r,p^n}, we obtain a power series $f(T)$ as (7). Since this is a property modulo p^n, we may take $f(T)$ as a polynomial.

(ii) We write $f(T) = \alpha_0 + \alpha_1 T + \alpha_2 T^2 + \cdots$. If $f((1+p)^{r-r_0}-1) \not\equiv f((1+p)^{r'-r_0}-1) \pmod{p^n}$ with $r \equiv r' \pmod{p^{n-2}}$, we can check that α_1 is a unit by direct computation.

(iii) From (ii), there is r such that $r \equiv r_0 \pmod{p-1}$ and $\log_{\zeta_{p^n,l}}(c^{\chi}_{l,r,p^n}) \not\equiv 0 \pmod{p^2}$. This implies by Lemma 5.1 (i)

$$\# X^{\psi}(r-1)_{G_\infty} \leq p. \tag{8}$$

Hence X^{ψ} is a cyclic Λ-module by Nakayama's lemma.

(iv) We denote by E_{K_m} (resp. $\mathscr{C}_{K_m}$) the group of units (resp. cyclotomic units) of K_m, and put $\mathscr{E}_{K_\infty} = \varprojlim E_{K_m} \otimes \mathbf{Z}_p$ (resp. $\mathscr{C}_{K_\infty} = \varprojlim C_{K_m} \otimes \mathbf{Z}_p$). Consider the homomorphisms

$$\begin{aligned} \mathscr{E}^{\psi}_{K_\infty}(r_0-1) &\longrightarrow (E_{K_n} \otimes \mathbf{Z}_p(r_0-1))^{\chi} \longrightarrow H^1(O_{K_n}[1/p], \mathbf{Z}/p^n(r_0))^{\chi} \\ &\longrightarrow \Bigl(\bigoplus_{\lambda \mid l} H^1(O_{K_n}/\lambda, \mathbf{Z}/p^n(r_0)) \Bigr)^{\chi} \simeq (\mathbf{Z}/p^n[\mathrm{Gal}(K_n/\mathbf{Q})])^{\psi} \\ &\simeq \mathbf{Z}/p^n[\mathrm{Gal}(K_n/K_1)] \\ &\simeq \mathbf{Z}/p^n[T]/((1+T)^{p^{n-1}}-1). \end{aligned}$$

Now, an element in $\mathscr{C}^{\psi}_{K_\infty}(r_0-1)$ has the image in $\mathbf{Z}/p^n[T]/((1+T)^{p^{n-1}}-1)$, whose coefficient of degree 1 is a unit. Using this and $(\mathscr{E}_{K_\infty})^{\psi} \simeq \Lambda \simeq \mathbf{Z}_p[[T]]$, we know that the

λ-invariant of $(\mathscr{E}_{K_\infty}/\mathscr{C}_{K_\infty})^\psi$ is 1 or 0. By Iwasawa Main Conjecture proved by Mazur and Wiles, we have $char((\mathscr{E}_{K_\infty}/\mathscr{C}_{K_\infty})^\psi)=char(X^\psi)$ ($char$ is the characteristic ideal in Λ). Hence, if X^ψ is infinite, it is isomorphic to $\mathbf{Z}_p$ because it is cyclic and of λ-invariant 1. This completes the proof of the lemma.

THEOREM 5.4. *We put $\psi=\chi\omega^{1-r_0}$, and assume $\psi(p)=\chi\omega^{1-r_0}(p)\neq 1$.*

(i) *If there is a prime number l such that $c^\chi_{l,r_0,p}\neq 1$, then we have $X^\psi=0$. (Here, the definition of c^χ_{l,r,p^n} is in* (4). *We call this case the trivial case. In the following, we consider the nontrivial case.)*

(ii) *If there exist prime numbers l_1, l_2, and some integers $r_1, r_2\geq 3$, and an integer $n\geq 2$ such that $r_1\equiv r_2\equiv r_0$ $(\mathrm{mod}\, p-1)$, $r_1\equiv r_2$ $(\mathrm{mod}(p-1)p^{n-2})$ and that*

$$c^\chi_{l_1,r_1,p^n}=1\ , \quad c^\chi_{l_1,r_2,p^n}\neq 1\ , \quad \textit{and} \quad c^\chi_{l_2,r_1,p^n}\neq 1\ ,$$

then X^ψ is finite.

(iii) *Further, in the situation of* (ii), *if $n\geq 3$ and there is r' such that $r'\equiv r_0$ $(\mathrm{mod}\, p-1)$ and $c^\chi_{l,r',p^{n-1}}=1$ for any l, then X^ψ is isomorphic to $\mathbf{Z}/p^{n-1}$.*

PROOF OF THEOREM 5.4. (i) was proved in Lemma 5.2.

(ii) Let $f(T)$ be a polynomial satisfying the property of Lemma 5.3 (i) for l_1, and put $F(r)=f((1+p)^{r-r_0}-1)$. Since $c^\chi_{l_1,r_1,p^n}=1$, the constant term of $f(T)$ is not a unit. Further, by Lemma 5.3 (ii), the coefficient of degree 1 is a unit. Hence, $F(r)\equiv 0$ $(\mathrm{mod}\, p^n)$ if and only if $r\equiv r_1$ $(\mathrm{mod}\, p^{n-1})$. So p^n does not divide $n^\chi(r)_p$ for $r\equiv r_0$ $(\mathrm{mod}\, p-1)$ such that $r\not\equiv r_1$ $(\mathrm{mod}(p-1)p^{n-1})$. On the other hand, $c_{l_2,r_1,p^n}\neq 1$ implies that p^n does not divide $n^\chi(r)_p$ for $r\equiv r_1$ $(\mathrm{mod}(p-1)p^{n-1})$ (cf. Lemma 2.4). By Theorem 2.5 (1) and Lemma 5.3 (iv), we get the conclusion.

(iii) If $c^\chi_{l,r',p^{n-1}}=1$ for all l, by Lemma 2.1 $\mathrm{index}_{l,p^m}(c^\chi_{l,r',p^m})^*\geq p^{n-1}$ for all m and all l, so we have $n^\chi(r')_p\geq p^{n-1}$. On the other hand, the proof of (ii) above implies $n^\chi(r)_p<p^n$ for all r, so $n^\chi(r')_p=p^{n-1}$. By Corollary 4.5 (i), we have

$$\sharp X^\psi(r'-1)_{G_\infty}=p^{n-1}\ .$$

By Lemma 5.3 (iii), X^ψ is cyclic. We write $X^\psi(r-1)\simeq\Lambda/I_r$. Then by (8), for some r'' such that $r''\equiv r_0$ $(\mathrm{mod}\, p-1)$, we have $\sharp X^\psi(r''-1)_{G_\infty}\leq p$, so we can find $f(T)=\alpha_0+\alpha_1 T+\cdots$ in $I_{r''}$ with $\alpha_0\not\equiv 0$ $(\mathrm{mod}\, p^2)$. If p divides α_1, then for all r such that $r\equiv r''\equiv r_0$ $(\mathrm{mod}\, p-1)$ we have

$$\sharp X^\psi(r-1)_{G_\infty}\leq p\ ,$$

which contradicts the above equality because $n\geq 3$. Hence α_1 is a unit and X^ψ is a quotient of $\mathbf{Z}_p$. So X^ψ is isomorphic to $\mathbf{Z}/p^{n-1}$.

EXAMPLE 5.5. We consider the quadratic field $K=\mathbf{Q}(\sqrt{254})$ (resp. $K=\mathbf{Q}(\sqrt{473})$) for $p=3$. Greenberg's conjecture for these two examples had not been known before [7]. (The situation is explained in [9] §5.) Let χ be the character associated to the quadratic field $K=\mathbf{Q}(\sqrt{254})$ (resp. $K=\mathbf{Q}(\sqrt{473})$), and take $p=3$ and $r_0=3$. Then, $\chi\omega^{-2}(p)=\chi(p)=-1$, so we can apply the above argument. Since 3 divides the class number of K, we know this is a nontrivial case. For $l_1=5925313=254\cdot 4\cdot 3^6\cdot 8+1$ and $l_2=20738593=254\cdot 4\cdot 3^6\cdot 28+1$, we have $c^{\chi}_{5925313,77,3^6}=3662189\neq 1$, $c^{\chi}_{5925313,401,3^6}=1$, and $c^{\chi}_{20738593,401,3^6}=4919350\neq 1$. (Here, we took g to be the least primitive root for prime numbers l_1 and l_2.) So by Theorem 5.4 (ii), X^{χ} is finite (note that $\psi=\chi\omega^{-2}=\chi$). We can check $c_{l,77,3^5}=1$ for the first 15 primes satisfying $l\equiv 1 \pmod{p^5N}$, which suggests $X^{\chi}\simeq \mathbf{Z}/3^5$ by Theorem 5.4 (iii). For $\mathbf{Q}(\sqrt{473})$ by the same way, $c^{\chi}_{2758537,5,3^6}=713490\neq 1$, $c^{\chi}_{2758537,329,3^6}=1$, and $c^{\chi}_{13103047,329,3^6}=9409260\neq 1$. So X^{χ} is finite. We can also check $c_{l,5,3^5}=1$ for the first 15 primes satisfying $l\equiv 1 \pmod{p^5N}$, which again suggests $X^{\chi}\simeq \mathbf{Z}/3^5$. (T. Fukuda calculated $\sharp X^{\chi}\geq 3^5$ in both cases, so they are really isomorphic to $\mathbf{Z}/3^5$.)

We next consider the "split" case. We suppose

(II) $\chi(p)=1$ and $r_0=p$.

We can take r_0 generally, but for the simplicity of the argument we take $r_0=p$.

LEMMA 5.6. *If there exists l such that $c^{\chi}_{l,p,p^2}\neq 1$, then $(X')^{\chi}=0$.*

In fact, by Lemma 5.1 (ii), we have $(X')^{\chi}(r-1)_{G_\infty}=0$, so we get $(X')^{\chi}=0$ by Nakayama's lemma.

We call this case the *trivial case*. In the following, we consider the non-trivial case, namely we assume $c^{\chi}_{l,p,p^2}=1$ for all l.

LEMMA 5.7. *Suppose $c^{\chi}_{l,r,p^{n+1}}$ is defined with $n\geq 2$.*

(i) *Let $\zeta_{p^{n+1},l}$ be a primitive p^{n+1}-th root of unity in $\mathbf{F}_l$. There is a polynomial $f(T)=\alpha_1T+\alpha_2T^2+\cdots\in\mathbf{Z}/p^{n+1}[T]$ such that*

$$\log_{\zeta_{p^{n+1},l}} c^{\chi}_{l,r,p^{n+1}}\equiv f((1+p)^{r-1}-1) \pmod{p^{n+1}}.$$

(ii) *We assume $c^{\chi}_{l,p,p^2}=1$, $(c^{\chi}_{l,p,p^3})^2\neq c^{\chi}_{l,2p-1,p^3}$, and $(c^{\chi}_{l,p,p^3})^4\neq c^{\chi}_{l,2p-1,p^3}$. Then, for the coefficients of $f(T)$ in* (i), *we have $p\mid\alpha_1$, and $\alpha_1\not\equiv 0 \pmod{p^2}$, and α_2 is a unit in $\mathbf{Z}/p^{n+1}$.*

(iii) *Under the assumption of* (ii), *$(X')^{\chi}$ is cyclic as a $\Lambda=\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K(\mu_p))]](\simeq \mathbf{Z}_p[[T]])$ module.*

(iv) *Under the assumption of* (ii), *$(X')^{\chi}$ is finite or isomorphic to $\mathbf{Z}_p$.*

PROOF. (i) The existence of a polynomial $f(T)$ such that $\log_{\zeta_{p^{n+1},l}}(c^{\chi}_{l,r,p^{n+1}})\equiv f((1+p)^{r-1}-1) \pmod{p^{n+1}}$ follows from the definition of $c^{\chi}_{l,r,p^{n+1}}$ as in Lemma 5.3 (i). Let E_{K_m} (resp. E'_{K_m}) be the group of (resp. p-units) units in K_m. Put $\mathscr{E}'_{K_\infty}=\varprojlim E'_{K_m}\otimes\mathbf{Z}_p$ and $\mathscr{E}_{K_\infty}=\varprojlim E_{K_m}\otimes\mathbf{Z}_p$. Since $\chi(p)=1$, we have an exact sequence $0\to\mathscr{E}^{\chi}_{K_\infty}\to(\mathscr{E}'_{K_\infty})^{\chi}\to\mathbf{Z}_p\to 0$. This implies $f(0)=0$.

(ii) Note that by Lemma 2.1, we have $(c^{\chi}_{l,r,p^{n+1}})^{p^{n-1}}=c^{\chi}_{l,r,p^2}$ and $(c^{\chi}_{l,r,p^{n+1}})^{p^{n-2}}=c^{\chi}_{l,r,p^3}$. By direct computation of $f((1+p)^{r-1}-1)$, we see that the assumption $c^{\chi}_{l,p,p^2}=1$ implies $\alpha_1\equiv 0 \pmod{p}$, and the assumption $(c^{\chi}_{l,p,p^3})^2\neq c^{\chi}_{l,2p-1,p^3}$ implies that α_2 is a unit in $\mathbf{Z}/p^3$.

The assumption $(c^{\chi}_{l,p,p^3})^4 \neq c^{\chi}_{l,2p-1,p^3}$ implies $\alpha_1 \not\equiv 0$ (modp^2).

(iii) and (iv) can be proved by the same method as Lemma 5.3. We consider a map $(\mathscr{E}'_{K_\infty})^{\chi}(r_0-1) \to (\bigoplus_{\lambda | l} H^1(O_{K_n}/\lambda, \mathbf{Z}/p^n(r_0)))^{\chi}$, then we know that the $\lambda$-invariant of $char((\mathscr{E}'_{K_\infty}/\mathscr{C}_{K_\infty})^{\chi})$ is smaller than or equal to 2. Considering $char((\mathscr{E}'_{K_\infty}/\mathscr{C}_{K_\infty})^{\chi}) = char((\mathscr{E}_{K_\infty}/\mathscr{C}_{K_\infty})^{\chi})T = char(X^{\chi})T = char((X')^{\chi})T$ (where we identify $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K(\mu_p))]] \simeq \mathbf{Z}_p[[T]]$ in a usual way), we get the conclusion.

THEOREM 5.8. *We assume* $\chi(p)=1$.

(i) *If there is a prime number* $l$ *such that* $c^{\chi}_{l,p,p^2} \neq 1$, *then we have* $(X')^{\chi}=0$. (*We call this case the trivial case. In the following, we consider the nontrivial case.*)

(ii) *Assume that there exists a prime number* l_1 *such that* $(c^{\chi}_{l_1,p,p^3})^2 \neq c^{\chi}_{l_1,2p-1,p^3}$ *and* $(c^{\chi}_{l_1,p,p^3})^4 \neq c^{\chi}_{l_1,2p-1,p^3}$. *Assume also that there exist a prime number* l_2, *and some integers* r_1, $r_2 \geq 3$, *and an integer* $n \geq 2$ *such that* $r_1 \equiv r_2 \equiv 1$ (mod$p-1$), $r_1 \equiv r_2$ (mod$(p-1)p^{n-2}$) *and that*

$$c^{\chi}_{l_1,r_1,p^{n+1}} = 1\ , \quad c^{\chi}_{l_1,r_2,p^{n+1}} \neq 1\ , \quad \textit{and} \quad c^{\chi}_{l_2,r_1,p^{n+1}} \neq 1\ .$$

Then $X^{\chi}$ *is finite.*

(iii) *Further, in the situation of* (ii), *if* $n \geq 3$ *and there is* r' *such that* $r' \equiv 1$ (mod$p-1$), $r' \not\equiv 1$ (mod$(p-1)p^{n-1}$), *and* $c^{\chi}_{l,r',p^n} = 1$ *for any* $l$, *then* $(X')^{\chi}$ *is isomorphic to* $\mathbf{Z}/p^{n-1}$.

The proof is almost the same as Theorem 5.4.

(i) is Lemma 5.6.

(ii) By our assumption $c^{\chi}_{l_1,p,p^2} = c^{\chi}_{l_2,p,p^2} = 1$. Let $f(T)$ be a polynomial in Lemma 5.7 (i) for l_1. By Lemma 5.7 (ii), we can write $f(T) = T(T-\theta)u(T)$ where $\theta \in \mathbf{Z}/p^{n+1}$ and $u(T) \in \mathbf{Z}/p^{n+1}[[T]]^{\times}$, and $p$ divides $\theta$ but p^2 does not divide $\theta$.

Suppose that $r_1 \equiv 1$ (mod$p$). Since $f((1+p)^{r_1-1}-1) \equiv 0$ (modp^{n+1}) and p^2 does not divide $\theta$, p^n divides $(1+p)^{r_1-1}-1$. Let $g(T) = \beta_1 T + \beta_2 T^2 + \cdots$ be a polynomial in Lemma 5.7 (i) for l_2. Then $c^{\chi}_{l_2,r_1,p^{n+1}} \neq 1$ implies that β_1 is a unit, so $c^{\chi}_{l_2,p,p^2} \neq 1$. This is a contradiction. So $r_1 \not\equiv 1$ (mod$p$).

Hence, $(1+p)^{r_1-1} \equiv 1+\theta$ (modp^n). So if $r \not\equiv r_1$, 1 (modp^{n-1}), $f((1+p)^{r-1}-1) \not\equiv 0$ (modp^{n+1}). This implies $n^{\chi}(r)_p < p^{n+1}$ for all $r \equiv 1$ (mod$p-1$) such that $r \not\equiv r_1$, 1 (modp^{n-1}). So $n^{\chi}(r)_p < p^{n+a_r}$ for all $r \equiv 1$ (mod$p-1$) such that $r \not\equiv r_1$ (modp^{n-1}). On the other hand, the conditions $c^{\chi}_{l_2,r_1,p^{n+1}} \neq 1$ and $c^{\chi}_{l_2,p,p^2} = 1$ imply $n^{\chi}(r)_p < p^{n+1}$ for all $r \equiv 1$ (mod$p-1$) such that $r \equiv r_1$ (modp^{n-1}). So by Theorem 2.5 (2) and Lemma 5.7 (iv), $X^{\chi}$ is finite.

(iii) This can be proved by the same method as Theorem 5.4 by using Corollary 4.5 (ii), Lemma 5.7 (iii), and Theorem 5.8 (ii) above.

EXAMPLE 5.9. Let $K = \mathbf{Q}(\sqrt{695})$ and $\chi$ be the character associated to $K/\mathbf{Q}$. Take $p=7$. Then $\chi(p)=1$. We can take l_1 and l_2 which satisfy the conditions of Theorem 5.8 (ii). For example, for $l_1 = 160194721$ and $l_2 = 100121701$, we have $c^{\chi}_{l_1,p,p^3} = 102983153$ and $c^{\chi}_{l_1,2p-1,p^3} = 120231960$. (Here, we took $g$ to be the least primitive root for prime numbers l_1 and l_2.) So $c^{\chi}_{l_1,p,p^2}=1$, $(c^{\chi}_{l_1,p,p^3})^2 \neq c^{\chi}_{l_1,2p-1,p^3}$, and $(c^{\chi}_{l_1,p,p^3})^4 \neq c^{\chi}_{l_1,2p-1,p^3}$. Further, we have $c^{\chi}_{l_1,25,p^4}=1$ and $c^{\chi}_{l_1,67,p^4}=102983153 \neq 1$, and $c^{\chi}_{l_2,25,p^4}=39969650 \neq 1$. Hence by Theorem 5.8 (ii), $X^{\chi}$ is finite. We can check $c^{\chi}_{l,25,p^3}=1$ for the first 15 prime numbers $l$ with $l \equiv 1$ (modp^3N). So we probably have $(X')^{\chi} \simeq \mathbf{Z}/p^2$.

EXAMPLE 5.10. Next we consider a number field $K=\mathbf{Q}(\sqrt{m}, \cos(2\pi/7))$ of degree 6. We take $p=7$. Let K^{cycl}_{∞}/K be the cyclotomic $\mathbf{Z}_p$-extension, and $X_{K^{cycl}_{\infty}}$ be the Galois group of the maximal unramified abelian pro-p extension of K^{cycl}_{∞}. We can show that $X_{K^{cycl}_{\infty}}$ is finite for any $m<1000$.

Let $N$ be the conductor of the quadratic field $\mathbf{Q}(\sqrt{m})$ and $\chi$ be the corresponding quadratic character, $\omega$ the Teichmüller character. In order to show the finiteness of $X_{K^{cycl}_{\infty}}$, it suffices to check the finiteness of $X^{\psi}=X^{\psi}_{K_{\infty}}$ for $\psi=\chi\omega^4$, $\chi\omega^2$, and $\chi$. We take $r_0=3$, 5, 7, respectively.

(Probably) nontrivial cases of $(m, \psi)$ (in the above sense) are listed in the following table.

ψ	$\chi\omega^4$	$\chi\omega^2$	$\chi$ (split case)	$\chi$ (non-split case)
$m \equiv 1$ (mod 4)	173, 461	685, 745	417	577
$m \equiv 2$, 3 (mod 4)	202, 590	62, 498	123♯, 554(*)	
	678, 807	526, 598	695(*), 834	
	815, 878	935, 951(*)	995	

These $(m, \psi)$'s in the table satisfy the condition of Theorem 5.4 (ii) (resp. Theorem 5.8 (ii)) except $(123, \chi)$ marked with ♯. $(m, \psi)$'s marked with (*) satisfy the property of Theorem 5.4 (ii) (resp. Theorem 5.8 (ii)) for $n=3$ if $\psi(p) \neq 1$ (resp. if $\psi(p)=1$). $(m, \psi)$'s without any mark in the table satisfy Theorem 5.4 (ii) (or Theorem 5.8 (ii)) for $n=2$.

If $(m, \psi)$ with $m<1,000$ is not listed in this table, it is in the trivial case. We have $X^{\psi}=0$ (resp. $(X')^{\psi}=0$) if $\psi(p) \neq 1$ (resp. if $\psi(p)=1$).

If $\psi(p) \neq 1$ (resp. if $\psi(p)=1$), $(m, \psi)$'s in the table satisfy $c^{\chi}_{l,r_0,p}=1$ (resp. $c^{\chi}_{l,r_0,p^2}=1$) for the first 15 primes $l$ with $l \equiv 1$ (modpN) (resp. $l \equiv 1$ (modp^2N)). So they are probably in the nontrivial cases.

$m=951$ for $\psi=\chi\omega^2$ satisfies the property of Theorem 5.4 (ii) for $n=3$, and $c^{\chi}_{l,17,p^2}=1$ for the first 15 primes $l$ with $l \equiv 1$ (modp^2N). So we probably have $X^{\psi} \simeq \mathbf{Z}/p^2$ by Theorem 5.4 (iii). For $(m, \psi)=(554, \chi)$ and $(695, \chi)$, in the same way we probably have $(X')^{\psi} \simeq \mathbf{Z}/p^2$ by Theorem 5.8 (iii).

For $(m, \psi)=(123, \chi)$, we cannot apply Theorem 5.8 directly, but can verify the finiteness of $X^{\chi}$ in the following way. For a prime number $l$ with $l \equiv 1$ (modp^nN), let $f_l(T) \in \mathbf{Z}/p^n[[T]]$ be the power series constructed by the method in the proof of Lemma 5.3 (i), which satisfies $\log_{\zeta_{p^n},l} c^{\chi}_{l,r,p^n} \equiv f_l((1+p)^{r-1}-1)$ (modp^n). We consider an ideal $I$ of

$\mathbf{Z}/p^2[[T]]/(((1+T)^p-1)/T)$ generated by $f_l(T)/T$'s modp^2 where l ranges over the prime numbers with $l\equiv 1$ (modp^2N). Taking, for example, $l=506269$ and 843781, we know that I contains an irreducible element and is not principal. Using the argument in the proof of Lemma 5.3 (iv), we have $(\mathscr{E}_{K_\infty}/\mathscr{C}_{K_\infty})^\chi<\infty$, so X^χ is finite. We note that more general and systematic method than this method for $m=123$ was developed by Kraft and Schoof [11]. As a consequence, we obtain $\sharp X_{K_\infty^{cycl}}<\infty$ for any $m<1{,}000$.

References

[1] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives, in The Grothendieck Festschrift Vol I, Progr. Math. **86**, Birkhäuser, (1990), 333–400.

[2] P. Deligne, Le groupe fondamental de la droite projective moins trois points, *Galois groups over* $\mathbf{Q}$, MSRI Publ. **16**, Springer (1989), 79–298.

[3] T. Fukuda and K. Komatsu, On $\mathbf{Z}_p$-extensions of real quadratic fields, J. Math. Soc. Japan **38** (1986), 95–102.

[4] T. Fukuda, K. Komatsu and H. Wada, A remark on the λ-invariant of real quadratic fields, Proc. Japan Acad. Ser. A **62** (1986), 318–319.

[5] T. Fukuda and H. Taya, The Iwasawa λ-invariants of $\mathbf{Z}_p$-extensions of real quadratic fields, Acta Arith. **69** (1995), 277–292.

[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, Tohoku Math. J. **49** (1997), 203–215.

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

[9] H. Ichimura and H. Sumida, On the Iwasawa λ-invariant of the real p-cyclotomic field, J. Math. Sci. Univ. Tokyo **3** (1996), 457–470.

[10] M. Kolster, Thong Nguyen Quang Do and V. Fleckinger, Twisted S-units, p-adic class number formulas and the Lichtenbaum conjectures, Duke Math. J. **84** (1996), 679–717.

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

[12] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$, Compositio Math. **81** (1992), 223–236.

[13] J. S., Milne, *Arithmetic duality theorems*, Perspectives in Math. (1986), Academic Press.

[14] K. Rubin, The main conjecture: Appendix to *Cyclotomic Fields* (Combined Second Edition) by S. Lang, Grad. Texts in Math. **121**, Springer (1990).

[15] C. Soulé, On higher p-adic regulators, Lecture Notes in Math. **854**, Springer (1981), 372–401.

[16] C. Soulé, Élements cyclotomiques en K-théorie, Astérisque **147–148** (1987), 225–257.

[17] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. **83** (1980), Springer.

Present Address:
Department of Mathematics, Tokyo Metropolitan University,
Minami-Osawa, Hachioji-shi, Tokyo, 192–0397 Japan.