Proc. London Math. Soc. Page 1 of 42
doi:10.1112/plms/pdr044

Refined Iwasawa theory and Kolyvagin systems of Gauss sum type

Masato Kurihara

Abstract

In this paper, we establish a refinement of the usual Iwasawa main conjecture for the ideal class groups of CM-fields over a totally real field, using higher Fitting ideals.

1. *Introduction*

In this paper, we generalize the results in our previous paper [10], and prove a more refined relationship between algebraic objects and analytic objects than the usual Iwasawa main conjecture.

Suppose that p is an odd prime number, and consider at first a finite abelian extension $K/\mathbf{Q}$ such that p does not divide $[K:\mathbf{Q}]$. Let χ be an odd Dirichlet character of $\mathrm{Gal}(K/\mathbf{Q})$ such that the conductor of χ coincides with that of K. When the group of pth roots of unity μ_p is in K, we assume $\chi \neq \omega$ where ω is the Teichmüller character that gives the action of $\mathrm{Gal}(K/\mathbf{Q})$ on μ_p. Suppose $A_K = \mathrm{Cl}_K \otimes \mathbf{Z}_p$ is the p-component of the ideal class group of K and A_K^χ is the χ-component of A_K (for the precise definition, see § 3.2). Then Mazur and Wiles [13] proved the celebrated Iwasawa main conjecture and also proved

$$\#A_K^\chi = \#O_\chi / B_{1,\chi^{-1}} O_\chi \tag{1.1}$$

as a corollary of the main conjecture where $O_\chi = \mathbf{Z}_p[\mathrm{Image}\,\chi]$ and $B_{1,\chi^{-1}}$ is the generalized Bernoulli number.

This is an equality on the orders, but we can get more information on A_K^χ as an O_χ-module from the values of zeta functions. Using the Euler system of Gauss sums, Kolyvagin and Rubin proved an isomorphism

$$A_K^\chi \simeq \bigoplus_{i \geqslant 1} \Theta_{i,K}^{(\delta),\chi} / \Theta_{i-1,K}^{(\delta),\chi} \tag{1.2}$$

as O_χ-modules where $(\Theta_{i,K}^{(\delta),\chi})_{i \geqslant 0}$ is an increasing sequence of ideals of O_χ, $\Theta_{0,K}^{(\delta),\chi} = B_{1,\chi^{-1}} O_\chi$, and the ideals $\Theta_{i,K}^{(\delta),\chi}$ are determined by some arguments of Euler systems from some Stickelberger elements (Kolyvagin [8, Theorem 7] and Rubin [16, Theorem 4.4]; in [16] only the case $K = \mathbf{Q}(\mu_p)$ was studied but the same argument works for K with $p \nmid [K:\mathbf{Q}]$). For the precise definition of these ideals $\Theta_{i,K}^{(\delta),\chi}$, see § 8.

In our previous paper [10], we generalized the above result to a finite and abelian extension K/k such that p does not divide $[K:k]$ where k is a totally real base field and K is a CM-field. We also assume $\chi \neq \omega$ when μ_p is in K. We obtained an isomorphism [10, Theorem 0.1]

$$A_K^\chi \simeq \bigoplus_{i \geqslant 1} \Theta_{i,K/k}^\chi / \Theta_{i-1,K/k}^\chi \tag{1.3}$$

as O_χ-modules (under certain mild assumption on χ), using an increasing sequence $(\Theta_{i,K/k}^\chi)_{i \geqslant 0}$ of ideals of O_χ. The ideals $\Theta_{i,K/k}^\chi$ are determined by some Stickelberger elements of fields

Received 29 December 2009; revised 6 April 2011.

2010 *Mathematics Subject Classification* 11R23, 11R29, 11R42.

over k, so determined by some analytic information coming from zeta values. (We can also define $\Theta^{(\delta),\chi}_{i,K/k}$ by the argument of Euler systems over k, and in our case $\Theta^{(\delta),\chi}_{i,K/k} = \Theta^{\chi}_{i,K/k}$ holds. The ideal $\Theta^{\chi}_{i,K/k}$ is better than $\Theta^{(\delta),\chi}_{i,K/k}$ for numerical computations. For the definition of these ideals, see § 8.) More precisely, an idea in [**10**] was to use the higher Fitting ideals (for the definition, see § 9), and we proved in [**10**] that

$$\mathrm{Fitt}_{i,O_\chi}(A^{\chi}_K) = \Theta^{\chi}_{i,K/k}, \tag{1.4}$$

for all $i \geqslant 0$ where the left-hand side is the ith Fitting ideal. The equality (1.4) immediately implies the isomorphism (1.3). In the following, we fix a totally real base field k, and omit k from the notation and write $\Theta^{\chi}_{i,K}$ for $\Theta^{\chi}_{i,K/k}$.

In this paper, we generalize the above result (1.4), and study the Iwasawa theoretic version. Let K/k and χ be as above. We consider the Iwasawa module $X_{K_\infty} = \varprojlim A_{K_m}$ for the cyclotomic $\mathbf{Z}_p$-extension K_∞ of a CM-field K (K_m is the mth layer of K_∞/K), and the χ-component $X^{\chi}_{K_\infty}$. The Iwasawa main conjecture proved by Mazur and Wiles [**13**] in the case $k = \mathbf{Q}$ and by Wiles [**23**] in general is the Iwasawa theoretic version of (1.1), and can be stated as

$$\mathrm{Fitt}_{0,\Lambda}(X^{\chi}_{K_\infty}) = (\theta^{\chi}_{K_\infty}), \tag{1.5}$$

since $\mathrm{Fitt}_{0,\Lambda}(X^{\chi}_{K_\infty})$ is equal to the characteristic ideal of $X^{\chi}_{K_\infty}$ in this case (cf. Theorem 9.6 and Lemma 9.1). Here, $\Lambda = \mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]^{\chi}$ is the χ-component of $\mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]$, and $\theta^{\chi}_{K_\infty}$ is the projective limit of the χ-component $\theta^{\chi}_{K_m}$ of the Stickelberger element of K_m (see § § 3.4 and9.3) and is essentially the p-adic L-function of Deligne and Ribet [**2**]. In this paper, we study the higher Fitting ideal $\mathrm{Fitt}_{i,\mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]}(X^{\chi}_{K_\infty})$ for any $i \geqslant 0$, and will prove that it is equal to some higher Stickelberger ideal $\Theta^{\chi}_{i,K_\infty}$ (see § 8 for the definition) which is generated by some elements coming from the p-adic L-function. Our main theorem is Theorem 2.1 in § 2, which is stated as

(Theorem 2.1) $$\mathrm{Fitt}_{i,\Lambda}(X^{\chi}_{K_\infty}) = \Theta^{\chi}_{i,K_\infty},$$

for any $i \geqslant 0$. The case $i = 0$ of Theorem 2.1 is nothing but (1.5), and so our Theorem 2.1 is a refinement of the usual main conjecture. We mention here that we do not give a new proof of the main conjecture because we use the main conjecture as an important ingredient of the proof.

Our Theorem 2.1 is regarded as the Iwasawa theoretic version of the structure theorem (1.3), and so is also a generalization of (1.2) by Kolyvagin [**8**] Theorem 7 and Rubin [**16**] for abelian fields over $\mathbf{Q}$. We will also obtain another structure theorem; see Corollary 2.4.

An essential difference in our case from [**10**] is that, here, we have to work over group rings while one worked over discrete valuation rings in [**10**]. A key new ingredient is Kolyvagin systems of Gauss sum type, especially those which do not come from Euler systems.

More precisely, the key of the proof of our main theorem is the construction of some element $x_{\mathfrak{n},\mathfrak{l}}$ (cf. § 8) in the multiplicative group having good properties (for the key property of $x_{\mathfrak{n},\mathfrak{l}}$, see Lemma 10.2). The essential ingredient of $x_{\mathfrak{n},\mathfrak{l}}$ is the Kolyvagin system $\kappa_{\mathfrak{n},\mathfrak{l}}$ of Gauss sum type.

The notion of Kolyvagin systems was introduced by Mazur and Rubin [**12**]. The first important property is '$\kappa_n \in H^1_{\mathcal{F}(n)}$' in the terminology of Mazur and Rubin (cf. [**12**, Definition 3.1.3]), which had not been recognized before [**12**]. A more important and beautiful property of our Kolyvagin system $\kappa_{\mathfrak{n},\mathfrak{l}}$ is that *they are related to the values of L-functions* (see the properties (ii) and (iv) below). Without explaining the notation, we gather here the properties of $\kappa_{\mathfrak{n},\mathfrak{l}}$. We prove (under the assumption that $\kappa_{\mathfrak{n},\mathfrak{l}}$ is defined and $\mathfrak{n}\mathfrak{l}$ is well-ordered; see Propositions 5.2, 6.4, 6.5 and also Corollary 6.2 for the details)

(i) for each prime $\mathfrak{r}$ dividing $\mathfrak{n}$, $\mathrm{div}_{\mathfrak{r}}(\kappa_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{r}}(\kappa_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$;

(ii) $\mathrm{div}_{\mathfrak{l}}(\kappa_{\mathfrak{n},\mathfrak{l}}) = \delta_{\mathfrak{n}}$;

(iii) for each prime $\mathfrak{r}$ dividing $\mathfrak{n}$, $\overline{\phi}_{\mathfrak{r}}(\kappa_{\mathfrak{n},\mathfrak{l}}) = 0$;
(iv) $\overline{\phi}_{\mathfrak{l}}(\kappa_{\mathfrak{n},\mathfrak{l}}) = -\delta_{\mathfrak{n}\mathfrak{l}}$.

Here, $\overline{\phi}_{\mathfrak{l}}$ is defined from the reciprocity map (see § 3.3 for the definition), and $\delta_{\mathfrak{n}}$, $\delta_{\mathfrak{n}\mathfrak{l}}$ are defined from the values of L-functions. The property (i) is a usual property of Kolyvagin systems (Euler systems), and the property (iii) corresponds to '$\kappa_n \in H^1_{\mathcal{F}(n)}$' in the terminology of Mazur and Rubin. The properties (ii) and (iv) are new, and are beautiful relations between the L-values and the Kolyvagin system of Gauss sum type.

The idea in this paper can be applied to a more general case, namely, to the Iwasawa theory for more general p-adic representations, for example, for elliptic curves (see [11]). In this paper, we study only the minus class groups because this case is the most typical and simplest case in this theory.

In § 2, we state our main theorem. In § 3, we fix notation in this paper and prove basic lemmas. We review in § 4 the Euler system of Gauss sum type in [10]. Suppose that k is a totally real number field, and K is a CM-field such that K/k is finite and abelian. For a prime $\mathfrak{l}$ which splits completely in K, we consider the Euler system $g_{\mathfrak{l}}^K$ of Gauss sum type constructed in [10]. This element $g_{\mathfrak{l}}^K$ is related to the values of L-functions, namely, the image of $g_{\mathfrak{l}}^K$ under the 'divisor' map is related to L-values by definition (see § 4.2), and we prove that the image of $g_{\mathfrak{l}}^K$ under the reciprocity map of local class field theory is also related to L-values (see Proposition 6.1). In § 4, we also prove the congruence relation (Proposition 4.2) which is not trivial since our Euler system is a 'finite' Euler system (see § 4.2). Using some abelian extension $K(\mathfrak{n})/k$, we can define the Kolyvagin derivative $\kappa_{\mathfrak{n},\mathfrak{l}} (\in K^\times/(K^\times)^{p^N})$ from $g_{\mathfrak{l}}^{K(\mathfrak{n})}$ by the usual argument of Euler systems if the prime $\mathfrak{l}$ *splits completely* in $K(\mathfrak{n})$. But we need $\kappa_{\mathfrak{n},\mathfrak{l}}$ for more general $\mathfrak{l}$ which does not split in $K(\mathfrak{n})$. In § 5, we construct $\kappa_{\mathfrak{n},\mathfrak{l}}$ for *more general primes* $\mathfrak{l}$, and prove the above properties (i)–(iv) in § 6. We introduce in § 7 the element $x_{\mathfrak{n},\mathfrak{l}}$, which plays an important role in the proof of Theorem 2.1. In § 8, we define two higher Stickelberger ideals $\Theta_{i,K}^{(\delta),\chi}$ and $\Theta_{i,K}^{\chi}$. The former is related to the theory of Euler systems, but the latter is better in general (cf. Remark 8.2). In § 9, after we gather known facts on Fitting ideals, we prove that $\Theta_{i,K_\infty}^{\chi}$ is in the higher Fitting ideal of the Iwasawa module (Corollary 9.12). In § 10, we prove Theorem 2.1. We also give some numerical examples in Remark 10.5.

NOTATION. For an abelian group A and an integer n, $A[n]$ and A/n denote the kernel and cokernel, respectively, of the multiplication by n. The notation A/n will be used even for multiplicative groups. For example, for the multiplicative group $K^\times$ of a field K, $K^\times/n$ means $K^\times/(K^\times)^n$. For a group G and a G-module M, M^G denotes the G-invariant part of M (the maximal subgroup of M on which G acts trivially), and M_G denotes the G-coinvariant of M (the maximal quotient of M on which G acts trivially). For a prime number p, we denote by ord_p the additive discrete valuation of $\mathbf{Q}$ associated to p, which is normalized such that $\mathrm{ord}_p(p) = 1$. For a positive integer n, μ_n denotes the group of all nth roots of unity in an algebraic closure of the field we are considering. For a number field or a local field F, O_F denotes the ring of integers.

2. *Main result*

Throughout this paper, k is the base field which is a totally real number field of finite degree over $\mathbf{Q}$. We assume that p is an odd prime number, and suppose that K_0 is a CM-field such that K_0/k is finite and abelian, and $[K_0 : k]$ is prime to p. In this § 2, we denote by K_∞ the cyclotomic $\mathbf{Z}_p$-extension of K_0. (In §§ 3–7, we consider more general K, and K_∞ denotes the cyclotomic $\mathbf{Z}_p$-extension of K.) We put $X_{K_\infty} = \varprojlim A_{K_{0,m}}$ where $A_{K_{0,m}}$ is the p-component of the ideal class group of $K_{0,m}$ for the intermediate field $K_{0,m}$ of K_∞/K_0 such that $[K_{0,m} : K_0] = p^m$.

This $\mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]$-module X_{K_∞}, which is isomorphic to the Galois group of the maximal unramified abelian pro-p extension of K_∞, is often called the Iwasawa module.

Since $[K_0 : k]$ is prime to p, X_{K_∞} is decomposed into the character components for characters of $\mathrm{Gal}(K_0/k)$ (see § 3, Subsection 3.2). Let χ be an odd character of $\mathrm{Gal}(K_0/k)$. When $k(\mu_p) \subset K_0$, we assume $\chi \neq \omega$ where ω is the Teichmüller character which gives the action of $\mathrm{Gal}(K_0/k)$ on the group of pth roots of unity. We also assume that the conductor of χ is equal to the conductor of K_0/k, and consider the χ-component $X_{K_\infty}^{\chi}$ (see § 3.2) which is a $\mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]^{\chi}$-module. (When we are interested in the χ-component, we may assume that the conductor of K_0/k equals that of χ; cf. Subsection 3.2.) We put $\Lambda = \mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]^{\chi} = O_\chi[\![\mathrm{Gal}(K_\infty/K_0)]\!]$ where $O_\chi = \mathbf{Z}_p[\mathrm{Image}\,\chi]$.

Let $\theta_{K_\infty}^{\chi}$ be the projective limit of the χ-component $\theta_{K_{0,m}}^{\chi}$ of the Stickelberger element of $K_{0,m}$ (see §§ 3.4 and 9.3). As we explained in § 1, the main conjecture states that the characteristic ideal of $X_{K_\infty}^{\chi}$ is generated by $\theta_{K_\infty}^{\chi}$. In this paper, we prove that more information on the structure of $X_{K_\infty}^{\chi}$ can be derived from the p-adic zeta functions, more precisely from the Stickelberger elements of abelian extensions that contain K_∞. In § 8, we define the higher Stickelberger ideals $\Theta_{i,K_{0,m}}^{\chi}$ for any $i \geqslant 0$ and $m \geqslant 0$, using the Stickelberger elements of several fields L which contain $K_{0,m}$ such that L/k is finite and abelian. We define the Stickelberger ideal $\Theta_{i,K_\infty}^{\chi} \subset \Lambda$ of K_∞ to be the projective limit of $\Theta_{i,K_{0,m}}^{\chi}$ (see § 9.5). In particular, $\Theta_{0,K_\infty}^{\chi}$ is a principal ideal generated by $\theta_{K_\infty}^{\chi}$ (the ideals $\Theta_{i,K_\infty}^{\chi}$ for $i \geqslant 1$ are not principal ideals, in general).

To state our main theorem, we use higher Fitting ideals (see § 9 for the definition and the basic properties of higher Fitting ideals). The following is our main theorem.

THEOREM 2.1. *We assume that the μ-invariant of $X_{K_\infty}^{\chi}$ is zero (namely, $X_{K_\infty}^{\chi}$ is finitely generated over $\mathbf{Z}_p$), and that $\chi(\mathfrak{p}) \neq 1$ for any prime $\mathfrak{p}$ of k above p. Then we have*

$$\mathrm{Fitt}_{i,\Lambda}(X_{K_\infty}^{\chi}) = \Theta_{i,K_\infty}^{\chi}, \tag{2.1}$$

for all $i \geqslant 0$.

REMARK 2.2. (1) The left-hand side of the above equation is an algebraic object and the right-hand side is a p-adic analytic object. The above theorem gives a more refined relationship between them than the usual main conjecture.

(2) If we know all Fitting ideals $\mathrm{Fitt}_{i,\Lambda}(X_{K_\infty}^{\chi})$, then we can determine the pseudo-isomorphism class of $X_{K_\infty}^{\chi}$ (Lemma 9.2). So the above theorem says that the information on the p-adic L-functions determines *the pseudo-isomorphism class of* $X_{K_\infty}^{\chi}$. For example, it determines whether $X_{K_\infty}^{\chi}$ contains $\Lambda/(f^2)$ or $\Lambda/(f) \oplus \Lambda/(f)$ when $f^2 \mid \theta_{K_\infty}^{\chi}$ for some irreducible $f \in \Lambda$, although a generator of $\mathrm{char}(X_{K_\infty}^{\chi})$ is conjectured to have only simple roots.

(3) In the case $\mathrm{rank}_{O_\chi} X_{K_\infty}^{\chi} \leqslant 2$, if we know all $\mathrm{Fitt}_{i,\Lambda}(X_{K_\infty}^{\chi})$, then we can determine the isomorphism class of $X_{K_\infty}^{\chi}$ (Lemma 9.3). If $\mathrm{rank}_{O_\chi} X_{K_\infty}^{\chi} \geqslant 3$, then the isomorphism class is not determined (Remark 9.4).

(4) We can remove the assumption $\chi(\mathfrak{p}) \neq 1$ in Theorem 2.1, which will be treated in [**11**].

Put $R_{K_{0,m}} = \mathbf{Z}_p[\mathrm{Gal}(K_{0,m}/K_0)]^{\chi} = O_\chi[\mathrm{Gal}(K_{0,m}/K_0)]$. As a corollary of Theorem 2.1, we prove in § 10.3 the following theorem.

THEOREM 2.3. *Under the same assumption as Theorem* 2.1, *for any $m \geqslant 0$, we have*

$$\mathrm{Fitt}_{i,R_{K_{0,m}}}(A_{K_{0,m}}^{\chi}) = \Theta_{i,K_{0,m}}^{\chi},$$

for all $i \geqslant 0$.

Let ψ be a character of $\mathrm{Gal}(K_{0,m}/K_0)$ of order p^m where $m \geqslant 0$. We define $O_{\chi\psi} = O_\chi[\mu_{p^m}]$. The ring homomorphism $R_{K_{0,m}} \longrightarrow O_{\chi\psi}$ induced by $\sigma \mapsto \psi(\sigma)$ ($\sigma \in \mathrm{Gal}(K_{0,m}/K_0)$) is denoted by the same letter ψ. We regard $O_{\chi\psi}$ as an $R_{K_{0,m}}$-module by the ring homomorphism $\psi : R_{K_{0,m}} \longrightarrow O_{\chi\psi}$. We define $A^{\chi\psi}_{K_{0,m}} = A^{\chi}_{K_{0,m}} \otimes_{R_{K_{0,m}}} O_{\chi\psi}$ which is an $O_{\chi\psi}$-module. Put $\Theta_i^{\chi\psi} = \psi(\Theta^{\chi}_{i,K_{0,m}})$. From Theorem 2.3 we immediately have the following corollary (see § 10.3).

Corollary 2.4. *There is an isomorphism*

$$A^{\chi\psi}_{K_{0,m}} \simeq \bigoplus_{i\geqslant 1} \Theta_i^{\chi\psi}/\Theta_{i-1}^{\chi\psi}$$

of $O_{\chi\psi}$-modules.

Taking $m = 0$ and $\psi = 1$ in Corollary 2.4, we obtain [**10**, Theorem 0.1], which is (1.3) in § 1. Hence, Corollary 2.4 is a generalization of (1.2) and (1.3) in § 1.

Theorem 2.1 also says that [**9**, Conjecture 8.2] is true. In Theorem 2.1, the case $i = 0$ is nothing but the main conjecture proved by Wiles, and the case $i = 1$ can be proved by the same method as [**9**, Theorem 8.4] if we use the Euler system constructed in [**10**]. Hence, what is essentially new is the case $i \geqslant 2$.

In the paper [**9**], we studied the initial Fitting ideal $\mathrm{Fitt}_{0,\mathbf{Z}_p[\![\mathrm{Gal}(K_\infty/k)]\!]}(X_{K_\infty})$ for a general CM-field K. In this paper, concerning the higher Fitting ideals, we only consider the case $K = K_{0,m}$ for some m.

3. *Notation and preliminary lemmas*

3.1.

For a finite prime $\mathfrak{l}$ of k, we denote by $\kappa(\mathfrak{l})$ the residue field of $\mathfrak{l}$, and by $N(\mathfrak{l})$ the absolute norm of $\mathfrak{l}$ (so $N(\mathfrak{l}) = \#\kappa(\mathfrak{l})$). We define $n_\mathfrak{l}$ by $n_\mathfrak{l} = \mathrm{ord}_p(N(\mathfrak{l}) - 1)$. We fix a positive integer $N > 0$ in §§ 3–7.

Lemma 3.1. *There are infinitely many primes $\mathfrak{l}$ of degree 1 such that $n_\mathfrak{l} \geqslant N$ and that there is a cyclic extension $k(\mathfrak{l})/k$ of degree $p^{n_\mathfrak{l}}$ which is unramified outside $\mathfrak{l}$ and which is totally ramified at $\mathfrak{l}$.*

We denote by $\mathcal{S}$ the set of all finite primes $\mathfrak{l}$ of k that satisfy the conditions of Lemma 3.1. If p divides the class number of k, then $k(\mathfrak{l})$ is not unique. But we take a $k(\mathfrak{l})$ satisfying the above conditions for each prime $\mathfrak{l} \in \mathcal{S}$, and fix it throughout this paper.

Correction: In [**10**, Lemma 4.3], it is stated that there exists a unique such extension, but clearly we do not have the uniqueness if k has an unramified abelian extension of degree p. The word 'unique' in the statement in [**10**, Lemma 4.3] should be deleted.

Proof of Lemma 3.1. Suppose that the p-primary component A_k of the ideal class group of k is generated as an abelian group by the classes of prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. Suppose that the order of the class $[\mathfrak{q}_j]$ in A_k is p^{a_j}. We take $\xi_j \in k^\times$ such that $\mathfrak{q}_j^{p^{a_j}} = (\xi_j)$ for each j. We denote by $\mathcal{U}$ the subgroup of $k^\times$ generated by the unit group $E_k = O_k^\times$ and $\xi_1, \ldots, \xi_s$.

We take n sufficiently large such that $n \geqslant N$ and $k(\mu_{p^n}) \neq k(\mu_{p^{n+1}})$. The Galois group $\mathrm{Gal}(k(\mu_p)/k)$ acts on $\mathrm{Gal}(k(\mu_{p^{n+1}})/k(\mu_{p^n}))$ trivially, and on $\mathrm{Gal}(k(\mu_{p^n}, \mathcal{U}^{1/p^n})/k(\mu_{p^n}))$ via ω where $\omega : \mathrm{Gal}(k(\mu_p)/k) \longrightarrow \mathbf{Z}_p^\times$ is the Teichmüller character which gives the action on μ_p. Hence, $k(\mu_{p^{n+1}})/k(\mu_{p^n})$ and $k(\mu_{p^n}, \mathcal{U}^{1/p^n})/k(\mu_{p^n})$ are linearly disjoint, and $k(\mu_{p^n}, \mathcal{U}^{1/p^n}) \neq$

$k(\mu_{p^{n+1}}, \mathcal{U}^{1/p^n})$. We take a prime $\mathfrak{l}$ of k of degree 1, which is prime to $p\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$, which splits completely in $k(\mu_{p^n}, \mathcal{U}^{1/p^n})$, and which does not split completely in $k(\mu_{p^{n+1}}, \mathcal{U}^{1/p^n})$. By the Chebotarev density theorem, there are infinitely many such $\mathfrak{l}$. We will show that $\mathfrak{l}$ satisfies the conditions of Lemma 3.1.

First of all, since $\mathfrak{l}$ splits in $k(\mu_{p^n})$ and does not split in $k(\mu_{p^{n+1}})$, it is clear that $n_{\mathfrak{l}} = n$.

Let H_k be the p-Hilbert class field of k (hence $A_k \simeq \mathrm{Gal}(H_k/k)$), and $k\{\mathfrak{l}\}$ be the maximal p-extension of k in the ray class field mod $\mathfrak{l}$. We know by class field theory $\mathrm{Gal}(k\{\mathfrak{l}\}/H_k) \simeq (\kappa(\mathfrak{l})^\times/(E_k \bmod \mathfrak{l})) \otimes \mathbf{Z}_p$ where $(E_k \bmod \mathfrak{l})$ is the image of E_k in $\kappa(\mathfrak{l})^\times$. Since $\mathfrak{l}$ splits completely in $k(E_k^{1/p^n})$ and $n = n_{\mathfrak{l}}$, we have $(E_k \bmod \mathfrak{l}) = \{1\}$, and $\mathrm{Gal}(k\{\mathfrak{l}\}/H_k) \simeq \mathbf{Z}/p^{n_{\mathfrak{l}}}$.

Furthermore, since $\mathfrak{l}$ splits completely in $k(\mathcal{U}^{1/p^n})$, by class field theory we can show that the sequence

$$0 \longrightarrow \mathrm{Gal}(k\{\mathfrak{l}\}/H_k) \longrightarrow \mathrm{Gal}(k\{\mathfrak{l}\}/k) \longrightarrow \mathrm{Gal}(H_k/k) \longrightarrow 0$$

splits as an exact sequence of abelian groups (see the proof of Kurihara [**10**, Lemma 4.3]). This shows that k has a cyclic extension of degree $p^{n_{\mathfrak{l}}}$, which is unramified outside $\mathfrak{l}$ and which is totally ramified at $\mathfrak{l}$. □

3.2.

Suppose that K/k is a finite and abelian extension, and K is a CM-field (hence K is totally imaginary and there is an intermediate field K^+ of K/k such that K^+ is totally real, and $[K : K^+] = 2$). We write $\mathrm{Gal}(K/k) = \Delta(K/k) \times \Gamma(K/k)$ where the order of $\Delta(K/k)$ is prime to p, and $\Gamma(K/k)$ is a p-group.

Suppose that $\chi : \Delta(K/k) \longrightarrow \overline{\mathbf{Q}}_p^\times$ is a character of $\Delta(K/k)$ whose values are in an algebraic closure of $\mathbf{Q}_p$. For a $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$-module M we define M^χ by

$$M^\chi = M \otimes_{\mathbf{Z}_p[\Delta(K/k)]} O_\chi,$$

where $O_\chi = \mathbf{Z}_p[\mathrm{Image}\,\chi]$ is the $\mathbf{Z}_p[\Delta(K/k)]$-module on which $\Delta(K/k)$ acts via χ. Since we can also write $M^\chi = M \otimes_{\mathbf{Z}_p[\mathrm{Gal}(K/k)]} O_\chi[\Gamma(K/k)]$, it is an $O_\chi[\Gamma(K/k)]$-module. For any element $x \in M$ we denote by x^χ the image of x in M^χ (namely, $x^\chi = x \otimes 1$).

Since $\#\Delta(K/k)$ is prime to p, the group algebra $\mathbf{Z}_p[\Delta(K/k)]$ is a direct sum of discrete valuation rings, more precisely, $\mathbf{Z}_p[\Delta(K/k)] = \bigoplus_\chi O_\chi$ where χ runs through all $\mathbf{Q}_p$-conjugate classes of characters of $\Delta(K/k)$ (we say that two $\overline{\mathbf{Q}}_p^\times$-valued characters χ_1 and χ_2 of $\Delta(K/k)$ are $\mathbf{Q}_p$-conjugate if $\sigma \circ \chi_1 = \chi_2$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$). Hence, $\mathbf{Z}_p[\mathrm{Gal}(K/k)] = \bigoplus_\chi O_\chi[\Gamma(K/k)]$ and

$$M = \bigoplus_\chi M^\chi$$

hold for any $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$-module M. Therefore, to study M, it suffices to study each M^χ. Throughout this paper, we assume that χ is *odd*. Also, when K contains μ_p, we assume $\chi \neq \omega$ where ω is the Teichmüller character.

For any number field F we denote by Cl_F the ideal class group of F, and by A_F the p-component $\mathrm{Cl}_F \otimes \mathbf{Z}_p$. For a field K as above, we are interested in the $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$-module $A_K = \mathrm{Cl}_K \otimes \mathbf{Z}_p$. We denote by K_0 the subfield of K corresponding to $\Gamma(K/k)$ by Galois theory, hence $\mathrm{Gal}(K/K_0) = \Gamma(K/k)$ and $\mathrm{Gal}(K_0/k) = \Delta(K/k)$. Without loss of generality, we may assume that the conductor of χ is equal to the conductor of K_0/k. In fact, let $\Delta_\chi \subset \Delta(K/k)$ be the kernel of $\chi : \Delta(K/k) = \mathrm{Gal}(K_0/k) \longrightarrow \overline{\mathbf{Q}}_p^\times$, and $K_{0,\chi}$ be the subfield of K_0 corresponding to Δ_χ. We also regard Δ_χ as a subgroup of $\mathrm{Gal}(K/k) = \Delta(K/k) \times \Gamma(K/k)$, and denote by K_χ the subfield of K corresponding to $\Delta_\chi \subset \mathrm{Gal}(K/k)$. Since $[K : K_\chi] = \#\Delta_\chi$ is prime to p, A_{K_χ} is isomorphic to the Δ_χ-coinvariant $(A_K)_{\Delta_\chi}$ by the usual norm argument. So $A_{K_\chi}^\chi$ is isomorphic to $A_K^\chi = ((A_K)_{\Delta_\chi})^\chi$. Hence, when we study A_K^χ, we may regard χ as a character of

$\mathrm{Gal}(K_{0,\chi}/k)$, and may assume $K_0 = K_{0,\chi}$. So in the following, we assume that the conductor of χ is equal to the conductor of K_0/k.

3.3.

In this subsection, we define two important homomorphisms $\mathrm{div}_{\mathfrak{l}}$ and $\phi_{\mathfrak{l}}$. Let K be a field as in § 3.2. We denote by Div_K the divisor group of K written additively. So, an element of Div_K is of the form $\Sigma n_i \rho_i$ where $n_i \in \mathbf{Z}$ and ρ_i is a finite prime of K. Suppose that

$$\mathrm{div} : K^\times \longrightarrow \mathrm{Div}_K$$

is the homomorphism that maps an element of $K^\times$ to its principal divisor, namely, for $x \in K^\times$, $\mathrm{div}(x) = \Sigma\, \mathrm{ord}_\rho(x)\rho \in \mathrm{Div}_K$ where ord_ρ is the normalized additive valuation associated to the prime ideal ρ.

Let $\mathcal{S}$ be the set of finite primes of k defined in § 3.1. For each $\mathfrak{l} \in \mathcal{S}$ we fix a prime $\mathfrak{l}_{\overline{k}}$ of an algebraic closure $\overline{k}$ above $\mathfrak{l}$ throughout this paper. For any subfield $F \subset \overline{k}$ the prime of F below $\mathfrak{l}_{\overline{k}}$ is denoted by $\mathfrak{l}_F$. So, when we consider finite extensions F_1/k, F_2/k such that $F_1 \subset F_2$, we are always taking (and fixing) primes such that $\mathfrak{l}_{F_2} \,|\, \mathfrak{l}_{F_1}$.

Suppose $K \subset \overline{k}$ is as above. We define $\mathcal{S}(K)$ by

$$\mathcal{S}(K) = \{\mathfrak{l} \in \mathcal{S} \mid \mathfrak{l} \text{ splits completely in } K\}.$$

Hence, $\mathfrak{l}_K$ is a prime of degree 1.

Assume that $\mathfrak{l}$ is a prime in $\mathcal{S}(K)$. We consider a map $K^\times \longrightarrow \bigoplus_{\rho|\mathfrak{l}} \mathbf{Z}$ defined by $x \mapsto \Sigma_{\rho|\mathfrak{l}}\, \mathrm{ord}_\rho(x)\rho$. Using the fixed prime $\mathfrak{l}_K$ of K above $\mathfrak{l}$, we regard $\bigoplus_{\rho|\mathfrak{l}} \mathbf{Z}$ as a free $\mathbf{Z}[\mathrm{Gal}(K/k)]$-module of rank 1 generated by $\mathfrak{l}_K$, and regard the above map as

$$\mathrm{div}_{\mathfrak{l}} : K^\times \longrightarrow \mathbf{Z}[\mathrm{Gal}(K/k)].$$

Taking $(- \otimes \mathbf{Z}/p^N)^\chi$, we obtain

$$\mathrm{div}_{\mathfrak{l}} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)],$$

which we also denote by the same notation $\mathrm{div}_{\mathfrak{l}}$.

We next define $\phi_{\mathfrak{l}}$. We assume $\mathfrak{l} \in \mathcal{S}$. Recall that in § 3.1 we took and fixed the field $k(\mathfrak{l})$ such that $k(\mathfrak{l})/k$ is a cyclic extension of degree $p^{n_{\mathfrak{l}}}$ which is unramified outside $\mathfrak{l}$ and is totally ramified at $\mathfrak{l}$. We define $G_{\mathfrak{l}}$ by

$$G_{\mathfrak{l}} = \mathrm{Gal}(k(\mathfrak{l})/k).$$

Let $\tilde{\mathfrak{l}} = \mathfrak{l}_{k(\mathfrak{l})}$ be the unique prime of $k(\mathfrak{l})$ above $\mathfrak{l}$. Suppose that $k_{\mathfrak{l}}$ and $k(\mathfrak{l})_{\tilde{\mathfrak{l}}}$ are the completions of k and $k(\mathfrak{l})$ at the primes $\mathfrak{l}$ and $\tilde{\mathfrak{l}}$, respectively. We consider the reciprocity map

$$\phi_{k_{\mathfrak{l}}} : k_{\mathfrak{l}}^\times \longrightarrow \mathrm{Gal}(k(\mathfrak{l})_{\tilde{\mathfrak{l}}}/k_{\mathfrak{l}}) = G_{\mathfrak{l}}$$

of local class field theory. Since the characteristic of the residue field $\kappa(\mathfrak{l})$ of $k_{\mathfrak{l}}$ is prime to p, $k_{\mathfrak{l}}$ contains a primitive $p^{n_{\mathfrak{l}}}$th root of unity. We can write $k(\mathfrak{l})_{\tilde{\mathfrak{l}}} = k_{\mathfrak{l}}(\sqrt[p^{n_{\mathfrak{l}}}]{\pi_{\mathfrak{l}}})$ for some prime element $\pi_{\mathfrak{l}}$ of $k_{\mathfrak{l}}$. We identify $G_{\mathfrak{l}}$ with the group $\mu_{p^{n_{\mathfrak{l}}}}$ of $p^{n_{\mathfrak{l}}}$th roots of unity by

$$\mathrm{Kum} : G_{\mathfrak{l}} \xrightarrow{\simeq} \mu_{p^{n_{\mathfrak{l}}}},\ \sigma \mapsto (\sigma - 1)(\sqrt[p^{n_{\mathfrak{l}}}]{\pi_{\mathfrak{l}}}).$$

Note that $(\sigma - 1)(\sqrt[p^{n_{\mathfrak{l}}}]{\pi_{\mathfrak{l}}})$ means, of course, $\sigma(\sqrt[p^{n_{\mathfrak{l}}}]{\pi_{\mathfrak{l}}})/\sqrt[p^{n_{\mathfrak{l}}}]{\pi_{\mathfrak{l}}}$, and that this map does not depend on the choice of $\pi_{\mathfrak{l}}$. We have

$$\mathrm{Kum} \circ \phi_{k_{\mathfrak{l}}}(u) = \overline{u}^{(1-N(\mathfrak{l}))/p^{n_{\mathfrak{l}}}} \in \mu_{p^{n_{\mathfrak{l}}}} \tag{3.1}$$

(Serre [**19**, Chapter XIV, Proposition 6 and Corollaire to Proposition 8]) for all units $u \in U_{k_{\mathfrak{l}}} = O_{k_{\mathfrak{l}}}^\times$ where $N(\mathfrak{l}) = \#\kappa(\mathfrak{l})$ is the absolute norm ($\kappa(\mathfrak{l})$ is the residue field of $\mathfrak{l}$), $\overline{u} = u \bmod \mathfrak{l} \in \kappa(\mathfrak{l})$ and we regard here $\mu_{p^{n_{\mathfrak{l}}}}$ as a subgroup of $\kappa(\mathfrak{l})^\times$. The extension $k(\mathfrak{l})_{\tilde{\mathfrak{l}}}/k_{\mathfrak{l}}$ is tamely ramified, and the above map is known as the tame symbol. (Note that some authors are using the inverse of our $\phi_{k_{\mathfrak{l}}}$ as the reciprocity map.)

LEMMA 3.2. *Let* $\phi_{k_\mathfrak{l},(N)} : k_\mathfrak{l}^\times \longrightarrow G_\mathfrak{l} \otimes \mathbf{Z}/p^N$ *be* $\phi_{k_\mathfrak{l}} \bmod p^N$. *Suppose that* $\beta \in k(\mathfrak{l})_{\tilde{\mathfrak{l}}}^\times$, $\sigma \in \mathrm{Gal}(k(\mathfrak{l})_{\tilde{\mathfrak{l}}}/k_\mathfrak{l}) = G_\mathfrak{l}$, *and that*

$$(\sigma - 1)\beta = \frac{\sigma(\beta)}{\beta} \equiv u^{(1-N(\mathfrak{l}))/p^N} \pmod{\tilde{\mathfrak{l}}}$$

holds for some $u \in U_{k_\mathfrak{l}} = O_{k_\mathfrak{l}}^\times$. *Then we have*

$$\phi_{k_\mathfrak{l},(N)}(u) = \sigma^{p^N \mathrm{ord}_\mathfrak{l}(\beta)},$$

where we extended to $k(\mathfrak{l})_{\tilde{\mathfrak{l}}}$ *the normalized additive valuation* $\mathrm{ord}_\mathfrak{l}$ *of* $k_\mathfrak{l}$.

Proof. Let

$$\mathrm{Kum}_{(N)} : G_\mathfrak{l} \otimes \mathbf{Z}/p^N \xrightarrow{\simeq} \mu_{p^N}$$

be the $\bmod p^N$ of the homomorphism Kum, namely $\sigma \mapsto (\sigma - 1)(\sqrt[p^N]{\pi_\mathfrak{l}})$. Then, by (3.1), we have

$$\mathrm{Kum}_{(N)} \circ \phi_{k_\mathfrak{l},(N)}(u) = \overline{u}^{(1-N(\mathfrak{l}))/p^N}.$$

Since

$$u^{(1-N(\mathfrak{l}))/p^N} \equiv \frac{\sigma(\beta)}{\beta} \equiv \left(\frac{\sigma(\sqrt[p^N]{\pi_\mathfrak{l}})}{\sqrt[p^N]{\pi_\mathfrak{l}}}\right)^{p^N \mathrm{ord}_\mathfrak{l}(\beta)} \equiv \frac{\sigma^{p^N \mathrm{ord}_\mathfrak{l}(\beta)}(\sqrt[p^N]{\pi_\mathfrak{l}})}{\sqrt[p^N]{\pi_\mathfrak{l}}},$$

we obtain $\phi_{k_\mathfrak{l},(N)}(u) = \sigma^{p^N \mathrm{ord}_\mathfrak{l}(\beta)}$. □

By the definition of $\mathcal{S}$ and local class field theory, we know that $k_\mathfrak{l}^\times/p^N = k_\mathfrak{l}^\times/(k_\mathfrak{l}^\times)^{p^N}$ is a direct sum of the kernels of $\mathrm{ord}_\mathfrak{l}$ and $\phi_{k_\mathfrak{l}}$. More precisely, we have the following lemma, immediately.

LEMMA 3.3. *For any* $\mathfrak{l} \in \mathcal{S}$, $k_\mathfrak{l}^\times/p^N$ *is a free* $\mathbf{Z}/p^N$*-module of rank* 2. *We define* V_1 *and* V_2 *to be the kernel of the map* $\mathrm{ord}_{\mathfrak{l},(N)} : k_\mathfrak{l}^\times/p^N \longrightarrow \mathbf{Z}/p^N$, *which is the normalized additive valuation* $\bmod p^N$ *and of the map* $\phi_{k_\mathfrak{l},(N)} : k_\mathfrak{l}^\times/p^N \longrightarrow G_\mathfrak{l} \otimes \mathbf{Z}/p^N$ *which is* $\phi_{k_\mathfrak{l}} \bmod p^N$, *respectively* . *Then both* V_1 *and* V_2 *are free of rank* 1 *over* $\mathbf{Z}/p^N$ *and*

$$k_\mathfrak{l}^\times/p^N = V_1 \oplus V_2.$$

Furthermore, V_2 *is the image of* $(k(\mathfrak{l})_{\tilde{\mathfrak{l}}}^{(N)})^\times \xrightarrow{N_\mathfrak{l}^{(N)}} k_\mathfrak{l}^\times \longrightarrow k_\mathfrak{l}^\times/p^N$ *where* $k(\mathfrak{l})_{\tilde{\mathfrak{l}}}^{(N)}$ *is the intermediate field of degree* p^N *of* $k(\mathfrak{l})_{\tilde{\mathfrak{l}}}/k_\mathfrak{l}$, *and* $N_\mathfrak{l}^{(N)}$ *is the norm map of* $k(\mathfrak{l})_{\tilde{\mathfrak{l}}}^{(N)}/k_\mathfrak{l}$.

Suppose that $\mathfrak{l}$ is in $\mathcal{S}(K)$. Since $\mathfrak{l}$ splits completely in K, the natural inclusion map $k \longrightarrow K$ induces an isomorphism $k_\mathfrak{l} \longrightarrow K_\rho$ for any prime ρ of K above $\mathfrak{l}$, where K_ρ is the completion of K at ρ. We consider the reciprocity map $K_\rho^\times \longrightarrow G_\mathfrak{l}$. We define $\phi_\mathfrak{l}$ by the composition

$$\phi_\mathfrak{l} : K^\times \longrightarrow \bigoplus_{\rho|\mathfrak{l}} K_\rho^\times \longrightarrow \bigoplus_{\rho|\mathfrak{l}} G_\mathfrak{l} = \left(\bigoplus_{\rho|\mathfrak{l}} \mathbf{Z}\right) \otimes G_\mathfrak{l} \simeq \mathbf{Z}[\mathrm{Gal}(K/k)] \otimes G_\mathfrak{l},$$

where the first map is the diagonal inclusion, the second map consists of the reciprocity maps and the third isomorphism is defined by the identification of $\bigoplus_{\rho|\mathfrak{l}} \mathbf{Z}$ with $\mathbf{Z}[\mathrm{Gal}(K/k)]$ using $\mathfrak{l}_K$. This map $\phi_\mathfrak{l}$ is a $\mathbf{Z}[\mathrm{Gal}(K/k)]$-linear homomorphism.

Again, taking $(- \otimes \mathbf{Z}/p^N)^\chi$, we obtain

$$\phi_\mathfrak{l} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)] \otimes G_\mathfrak{l},$$

which we also denote by the same letter $\phi_{\mathfrak{l}}$. When we fix a generator $\sigma_{\mathfrak{l}}$ of $G_{\mathfrak{l}}$, we have a non-canonical isomorphism $O_\chi/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{l}} \simeq O_\chi/p^N[\Gamma(K/k)]$, and we define $\overline{\phi}_{\mathfrak{l}}$ to be the composition of $\phi_{\mathfrak{l}}$ with this isomorphism

$$\overline{\phi}_{\mathfrak{l}} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)].$$

Namely, $\phi_{\mathfrak{l}}(x) = \overline{\phi}_{\mathfrak{l}}(x) \otimes \sigma_{\mathfrak{l}}$ for all x.

We put $K(\mathfrak{l}) = Kk(\mathfrak{l})$. We remark that if $x \in (K^\times/p^N)^\chi$ is a norm from $K(\mathfrak{l})$ (namely, x can be written as $x = N_{K(\mathfrak{l})/K}(y)$ for some $y \in (K(\mathfrak{l})^\times/p^N)^\chi$ where $N_{K(\mathfrak{l})/K}$ is the norm map), we have $\phi_{\mathfrak{l}}(x) = 0$ by local class field theory and the definition of $\phi_{\mathfrak{l}}$.

3.4.

In this subsection, we define the Stickelberger element for an abelian extension. Let K/k be a finite and abelian extension. For a non-zero ideal $\mathfrak{a}$ of O_K, we denote by $(\mathfrak{a}, K/k)$ the Artin symbol. We define the partial zeta function for $\sigma \in \mathrm{Gal}(K/k)$ by

$$\zeta(s,\sigma) = \sum_{(\mathfrak{a},K/k)=\sigma} N(\mathfrak{a})^{-s},$$

for $\mathrm{Re}(s) > 1$ where $N(\mathfrak{a})$ is the absolute norm and $\mathfrak{a}$ runs through all non-zero integral ideals that are prime to the ramified primes in K/k. The equivariant zeta function $\theta_{K/k}(s)$ is defined by

$$\theta_{K/k}(s) = \sum_{\sigma\in\mathrm{Gal}(K/k)} \zeta(s,\sigma)\sigma^{-1}.$$

Suppose that L/k is a finite and abelian extension such that $K \subset L$. The natural restriction map $\mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k)$ induces

$$c_{L/K} : \mathbf{C}[\mathrm{Gal}(L/k)] \longrightarrow \mathbf{C}[\mathrm{Gal}(K/k)].$$

Using the fact that $\theta_{K/k}(s)$ and $\theta_{L/k}(s)$ have the Euler products (Tate [21, Proposition 1.6]), we can show that

$$c_{L/K}(\theta_{L/k}(s)) = \left(\prod_{\mathfrak{l}\in R_{L/K}} (1 - N(\mathfrak{l})^{-s}\varphi_{\mathfrak{l}}^{-1})\right)\theta_{K/k}(s),$$

where $R_{L/K}$ is the set of finite primes of k which are ramified in L and which are unramified in K, and $\varphi_{\mathfrak{l}}$ is the Frobenius of $\mathfrak{l}$ in $\mathrm{Gal}(K/k)$ (cf. Tate [21, p. 86]).

The partial zeta functions have meromorphic continuation for the whole complex plane, and we know by Klingen and Siegel that $\theta_{K/k}(0)$ is in $\mathbf{Q}[\mathrm{Gal}(K/k)]$ (see [20]). We simply write θ_K for $\theta_{K/k}(0)$. By the above formula, we have

$$c_{L/K}(\theta_L) = \left(\prod_{\mathfrak{l}\in R_{L/K}} (1 - \varphi_{\mathfrak{l}}^{-1})\right)\theta_K.$$

Let K be as in § 3.2. We consider the χ-component $\mathbf{Z}_p[\mathrm{Gal}(K/k)]^\chi = O_\chi[\Gamma(K/k)]$ of the group ring. As in § 3.1, we assume $\chi \neq \omega$. Consider the natural map $\mathbf{Q}[\mathrm{Gal}(K/k)] = \mathbf{Q}[\Delta(K/k) \times \Gamma(K/k)] \longrightarrow \mathbf{Q}_p(\mathrm{Image}\,\chi)[\Gamma(K/k)]$ defined by $\Sigma a_{\sigma,\tau}(\sigma,\tau) \mapsto \Sigma a_{\sigma,\tau}\chi(\sigma)\tau$. We define $\theta_K^\chi \in \mathbf{Q}_p(\mathrm{Image}\,\chi)[\Gamma(K/k)]$ to be the image of θ_K by this map (see § 3.2 for the general definition of the element x^χ for general x). Since we are assuming $\chi \neq \omega$, we have

$$\theta_K^\chi \in O_\chi[\Gamma(K/k)]$$

by Deligne and Ribet [2]. We note that this element θ_K^χ is numerically computable in principle.

Suppose that L/k is finite and abelian such that $K \subset L$ and L/K is a p-extension. In the notation of § 3.2, we have $\Delta(K/k) = \Delta(L/k)$, and we can define $\theta_L^{\chi} \in O_{\chi}[\Gamma(L/k)]$. By the above equation, we have the following lemma, which will be used many times.

LEMMA 3.4. *Let $c_{L/K} : O_{\chi}[\Gamma(L/k)] \longrightarrow O_{\chi}[\Gamma(K/k)]$ be the restriction map. Then we have*

$$c_{L/K}(\theta_L^{\chi}) = \left(\prod_{\mathfrak{l} \in R_{L/K}} (1 - \varphi_{\mathfrak{l}}^{-1})^{\chi} \right) \theta_K^{\chi}.$$

4. *Euler systems of Gauss sum type*

In this section, we review the Euler system of Gauss sum type in [10], and prove some fundamental properties.

4.1.

From now on, we always assume the following. We consider a number field K as in § 3.2, namely, K is a CM-field such that K/k is finite and abelian. We use the same notation $\Delta(K/k)$, $\Gamma(K/k)$, K_0 (recall that K_0 is the field such that $\mathrm{Gal}(K/K_0) = \Gamma(K/k)$), and consider an odd character χ of $\Delta(K/k)$. As in § 3.2, we assume $\chi \neq \omega$, and the conductor of χ is equal to that of K_0. *We also assume that $\chi(\mathfrak{p}) \neq 1$ for all primes $\mathfrak{p}$ of k above p, and that the μ_{χ}-invariant of K is zero.* The second assumption means the following. For the cyclotomic $\mathbf{Z}_p$-extension K_{∞}/K, we define $X_{K_{\infty}}$ by $X_{K_{\infty}} = \varprojlim A_{K_n}$ where K_n is the intermediate field of degree p^n, and the limit is taken with respect to the norm maps. The assumption that the μ_{χ}-invariant of K vanishes means $\mu(X_{K_{\infty}}^{\chi}) = 0$; namely the χ-component $X_{K_{\infty}}^{\chi}$ is a finitely generated O_{χ}-module (this is always true by a famous theorem of Ferrero and Washington if $k = \mathbf{Q}$ (see [3])). We consider such general K in §§ 4–8 (we do not assume $K \subset K_{0,\infty}$). Furthermore, in §§ 4–7 we also assume that

(*) all primes of k above p are ramified in K, and all primes of K above p are totally ramified in K_{∞}.

4.2.

We next review the result in [10, § 4]. We consider abelian p-extensions L/K, more precisely, put

$$\mathcal{F} = \{L \mid K \subset L, L/k \text{ is finite and abelian, and } L/K \text{ is a } p\text{-extension}\},$$

and consider $L \in \mathcal{F}$. Note that $\mathrm{Gal}(L/k) = \Delta(L/k) \times \Gamma(L/k)$, $\Gamma(L/k) = \mathrm{Gal}(L/K_0)$ and $\Delta(L/k) = \Delta(K/k) = \mathrm{Gal}(K_0/k)$ (recall that K_0 is the field such that K/K_0 is a p-extension and $[K_0 : K]$ is prime to p). Note that L is a CM-field because K is a CM-field, L/K is a p-extension ($p \neq 2$) and L/k is an abelian extension.

We regard χ as a character of $\Delta(L/k)$, and consider the χ-components $(L^{\times} \otimes \mathbf{Z}_p)^{\chi}$, $(\mathrm{Div}_L \otimes \mathbf{Z}_p)^{\chi}$ and so on. Let A_L^{χ} be the χ-component of the p-component of the ideal class group of L. We denote by $O_L^{\times}$ and Div_L the unit group of L and the divisor group of L, respectively. As in § 3.3, we define $\mathrm{div} : L^{\times} \longrightarrow \mathrm{Div}_L$ to be the homomorphism that maps an element of $L^{\times}$ to its principal divisor. Then we have an exact sequence $0 \longrightarrow O_L^{\times} \otimes \mathbf{Z}_p \longrightarrow L^{\times} \otimes \mathbf{Z}_p \xrightarrow{\mathrm{div}} \mathrm{Div}_L \otimes \mathbf{Z}_p \longrightarrow A_L \longrightarrow 0$. Taking the χ-component, we obtain the following lemma.

LEMMA 4.1. *For $L \in \mathcal{F}$,*

$$0 \longrightarrow (L^{\times} \otimes \mathbf{Z}_p)^{\chi} \xrightarrow{\mathrm{div}} (\mathrm{Div}_L \otimes \mathbf{Z}_p)^{\chi} \longrightarrow A_L^{\chi} \longrightarrow 0$$

is exact.

Proof. This follows from $(O_L^\times \otimes \mathbf{Z}_p)^\chi = 0$, which can be easily checked by our assumption that χ is odd and $\chi \neq \omega$. □

We use the same notation as in § 3.3 for L. Recall that $\mathcal{S}(L)$ is the subset of finite primes of k defined by

$$\mathcal{S}(L) = \{\mathfrak{l} \in \mathcal{S} \mid \mathfrak{l} \text{ splits completely in } L\},$$

and we consistently fixed a prime $\mathfrak{l}_L$ of L above $\mathfrak{l}$ for each $\mathfrak{l} \in \mathcal{S}(L)$.

By Kurihara [10, Corollary 2.4] (note that the μ-invariant of L vanishes because of our assumption of the vanishing of the μ-invariant of K and the fact that L/K is a p-extension (Iwasawa [6, Theorem 2])), we have

$$\theta_L^\chi A_L^\chi = 0.$$

For $\mathfrak{l} \in \mathcal{S}(L)$ the class of $\mathfrak{l}_L$ in A_L^χ is denoted by $[\mathfrak{l}_L]^\chi$. Then $\theta_L^\chi[\mathfrak{l}_L]^\chi = 0$ holds. By the exact sequence in Lemma 4.1, there is a unique element $g_\mathfrak{l}^L$ in $(L^\times \otimes \mathbf{Z}_p)^\chi$ such that

$$\operatorname{div}(g_\mathfrak{l}^L) = \theta_L^\chi\, \mathfrak{l}_L^\chi \tag{4.1}$$

(note that $\mathfrak{l}_L^\chi$ is the image of $\mathfrak{l}_L$ in $(\operatorname{Div}_L \otimes \mathbf{Z}_p)^\chi$).

Suppose that M is a subfield such that $K_0 \subset M \subset L$ (where K_0 is the subfield such that $\operatorname{Gal}(K_0/k) = \Delta(K/k)$ as in § 3.2). Recall that we are taking $\mathfrak{l}_M$ such that $\mathfrak{l}_L \,|\, \mathfrak{l}_M$, so we can define $g_\mathfrak{l}^M$ similarly. Using Lemma 3.4, if $\mathfrak{l} \in \mathcal{S}(L)$, namely, if $\mathfrak{l} \in \mathcal{S}$ *splits completely* in L, then we have (see [10, Lemma 4.1])

$$N_{L/M}(g_\mathfrak{l}^L) = \left(\prod_{\rho \in R_{L/M}} (1 - \varphi_\rho^{-1})^\chi\right)(g_\mathfrak{l}^M), \tag{4.2}$$

where $N_{L/M}$ is the norm map and $R_{L/M}$ is defined similarly for L/M as in § 3.4. Note that if $\mathfrak{l}$ does not split completely in L, then (4.2) does not hold (the residue degree appears in the formula; cf. [10, Lemma 4.1]). Thus, for $\mathfrak{l} \in \mathcal{S}(L)$, for any intermediate field M of L/K_0, we obtain an Euler system $(g_\mathfrak{l}^M)$. But this is a 'finite' Euler system in the terminology of Mazur and Rubin [12] because it is defined only on the finite set $\{M \mid K_0 \subset M \subset L\}$. For more details on this Euler system, see [10, § 4].

4.3.

In this subsection, we recall the usual argument of Euler systems to construct the Kolyvagin derivative $\kappa_{\mathfrak{n},\mathfrak{l}}$. Recall at first that in § 3.1, for each $\mathfrak{r} \in \mathcal{S}$, we took and fixed a field $k(\mathfrak{r})$ such that $k(\mathfrak{r})/k$ is a cyclic extension of degree $p^{n_\mathfrak{r}}$, which is unramified outside $\mathfrak{r}$ and is totally ramified at $\mathfrak{r}$. We define $G_\mathfrak{r}$ by $G_\mathfrak{r} = \operatorname{Gal}(k(\mathfrak{r})/k)$. As in the usual argument of Euler systems, taking a generator $\sigma_\mathfrak{r}$ of $G_\mathfrak{r}$, we put

$$N_\mathfrak{r} = \sum_{i=0}^{p^{n_\mathfrak{r}}-1} \sigma_\mathfrak{r}^i \in \mathbf{Z}[G_\mathfrak{r}] \quad \text{and} \quad D_\mathfrak{r} = \sum_{i=0}^{p^{n_\mathfrak{r}}-1} i\sigma_\mathfrak{r}^i \in \mathbf{Z}[G_\mathfrak{r}].$$

A fundamental equation is $D_\mathfrak{r}(\sigma_\mathfrak{r} - 1) = p^{n_\mathfrak{r}} - N_\mathfrak{r}$.

We define $\mathcal{N}$ and $\mathcal{N}(K)$ to be the sets consisting of all square-free products of primes in $\mathcal{S}$ and $\mathcal{S}(K)$, respectively (we denote by 1 the ideal $(1) = O_k$ and suppose that 1 is both in $\mathcal{N}$ and $\mathcal{N}(K)$). For any $\mathfrak{n} \in \mathcal{N}$ with $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m$, define $k(\mathfrak{n})$ to be the compositum of the fields $k(\mathfrak{r}_1), \ldots, k(\mathfrak{r}_m)$, and $G_\mathfrak{n} = G_{\mathfrak{r}_1} \times \ldots \times G_{\mathfrak{r}_m}$ which is isomorphic to $\operatorname{Gal}(k(\mathfrak{n})/k)$.

For $\mathfrak{n} \in \mathcal{N}(K)$ we write $K(\mathfrak{n}) = Kk(\mathfrak{n})$. Clearly, we have $\operatorname{Gal}(K(\mathfrak{n})/K) = \operatorname{Gal}(k(\mathfrak{n})/k) = G_\mathfrak{n}$. Note that $K(\mathfrak{n}) \in \mathcal{F}$ where $\mathcal{F}$ is the set defined in § 4.2. We put $N_\mathfrak{n} = \Pi_{\mathfrak{r}|\mathfrak{n}} N_\mathfrak{r}$ and $D_\mathfrak{n} = \Pi_{\mathfrak{r}|\mathfrak{n}} D_\mathfrak{r}$, which are elements of $\mathbf{Z}[G_\mathfrak{n}]$.

We use the standard argument of Euler systems [15, § 2; 22, § 15.3]. For $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$, $D_\mathfrak{n} g_\mathfrak{l}^{K(\mathfrak{n})} \bmod p^N$ is in the $G_\mathfrak{n}$-invariant part of $(K(\mathfrak{n})^\times \otimes \mathbf{Z}/p^N)^\chi$. We define $\kappa_{\mathfrak{n},\mathfrak{l}} \in (K^\times \otimes$

$\mathbf{Z}/p^N)^\chi$ to be the unique element whose image in $(K(\mathfrak{n})^\times \otimes \mathbf{Z}/p^N)^\chi$ is $D_\mathfrak{n} g_\mathfrak{l}^{K(\mathfrak{n})}$. The uniqueness comes from the bijectivity of the natural map

$$(K^\times \otimes \mathbf{Z}/p^N)^\chi \longrightarrow ((K(\mathfrak{n})^\times \otimes \mathbf{Z}/p^N)^\chi)^{G_\mathfrak{n}},$$

which follows from our assumption $\chi \neq \omega$. Note that $\kappa_{1,\mathfrak{l}} = g_\mathfrak{l}^K$ for $\mathfrak{n} = 1$.

We next consider Stickelberger elements. Suppose that $\mathfrak{n} \in \mathcal{N}(K)$. In § 3.4, we defined $\theta_K^\chi \in O_\chi[\Gamma(K/k)]$. We define $\theta_{K(\mathfrak{n})}^\chi \in O_\chi[\Gamma(K(\mathfrak{n})/k)]$ by the same method. Since $\Gamma(K(\mathfrak{n})/k) = \Gamma(K/k) \times G_\mathfrak{n}$, we have $O_\chi[\Gamma(K(\mathfrak{n})/k)] = O_\chi[\Gamma(K/k)][G_\mathfrak{n}]$. The multiplication by $N_\mathfrak{n}$ gives an injective homomorphism

$$N_\mathfrak{n} : O_\chi/p^N[\Gamma(K/k)] \longrightarrow O_\chi/p^N[\Gamma(K/k)][G_\mathfrak{n}]$$

of $\mathrm{Gal}(K(\mathfrak{n})/k)$-modules, whose image is the $G_\mathfrak{n}$-invariant part. Since $D_\mathfrak{n}\theta_{K(\mathfrak{n})}^\chi \bmod p^N$ is in the $G_\mathfrak{n}$-invariant part of $O_\chi/p^N[\Gamma(K(\mathfrak{n})/k)]$ (which follows from the standard argument of the Euler system as above), it is in the image of $N_\mathfrak{n}$. Hence, there is a unique element $\delta_\mathfrak{n}$ in $O_\chi/p^N[\Gamma(K/k)]$ such that $N_\mathfrak{n}\delta_\mathfrak{n} = D_\mathfrak{n}\theta_{K(\mathfrak{n})}^\chi \bmod p^N$. Note that $\delta_1 = \theta_K^\chi$ for $\mathfrak{n} = 1$.

Suppose $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m$. We know

$$\theta_{K(\mathfrak{n})}^\chi \equiv (-1)^m \delta_\mathfrak{n}(\sigma_{\mathfrak{r}_1} - 1) \cdot \ldots \cdot (\sigma_{\mathfrak{r}_m} - 1) \pmod{p^N, (\sigma_{\mathfrak{r}_1} - 1)^2, \ldots, (\sigma_{\mathfrak{r}_m} - 1)^2} \tag{4.3}$$

by Kurihara [**10**, Lemma 4.4].

Suppose again that $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m \in \mathcal{N}(K)$ and $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$. We defined $\kappa_{\mathfrak{n},\mathfrak{l}} \in (K^\times/p^N)^\chi$ above, but this does depend on the choice of a generator $\sigma_\mathfrak{r}$ of $G_\mathfrak{r}$ for each $\mathfrak{r} \mid \mathfrak{n}$. Put

$$\mathcal{G}_\mathfrak{n} = G_{\mathfrak{r}_1} \otimes \ldots \otimes G_{\mathfrak{r}_m}.$$

Following Mazur and Rubin [**12**], we consider elements in $(K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n}$, and define

$$\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = \kappa_{\mathfrak{n},\mathfrak{l}} \otimes \sigma_{\mathfrak{r}_1} \otimes \ldots \otimes \sigma_{\mathfrak{r}_m} \in (K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n},$$

which does not depend on the choice of $\sigma_{\mathfrak{r}_i}$. In the same way, we define

$$\tilde{\delta_\mathfrak{n}} = \delta_\mathfrak{n} \otimes \sigma_{\mathfrak{r}_1} \otimes \ldots \otimes \sigma_{\mathfrak{r}_m} \in (O_\chi/p^N[\Gamma(K/k)]) \otimes \mathcal{G}_\mathfrak{n},$$

which is also independent of the choice of $\sigma_{\mathfrak{r}_i}$.

4.4.

We next prove a famous relation called congruence relation of Euler systems (cf. Rubin [**17**, Corollary 4.8.1]). We are dealing with a 'finite' Euler system, and cannot apply the usual argument directly, so we will give here a proof. A special case was proved and used in [**10**], but here we give a general version and its proof.

PROPOSITION 4.2 (Congruence relation). *Suppose $\mathfrak{r} \in \mathcal{S}$ is unramified in K and $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{r}))$ where $K(\mathfrak{r}) = Kk(\mathfrak{r})$. (Note that we do not assume $\mathfrak{r} \in \mathcal{S}(K)$.) Then, for any prime $\rho_\mathfrak{r}$ of $K(\mathfrak{r})$ above $\mathfrak{r}$, we have*

$$(g_\mathfrak{l}^K)^{(1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}} \equiv g_\mathfrak{l}^{K(\mathfrak{r})} \pmod{\rho_\mathfrak{r}},$$

where $N(\mathfrak{r})$ is the absolute norm $\#\kappa(\mathfrak{r})$ of $\mathfrak{r}$.

Proof. Let $\kappa(\rho_\mathfrak{r})$ be the residue field of $\rho_\mathfrak{r}$, and put $n' = \mathrm{ord}_p(\#\kappa(\rho_\mathfrak{r})^\times)$. Obviously, $n' \geqslant n_\mathfrak{r}$ and n' does not depend on the choice of $\rho_\mathfrak{r}$ and only on K because K/k is a Galois extension. Put $L = K(\mathfrak{r})$. By the Chebotarev density theorem, we can take a prime $\mathfrak{l}' \in \mathcal{S}(L(\mu_{p^{n'+n_\mathfrak{r}}}))$ such that the class $[\mathfrak{l}'_L]^\chi$ and the class $[\mathfrak{l}_L]^\chi$ coincide in A_L^χ. In fact, we take $n \geqslant n' + n_\mathfrak{r}$ sufficiently

large such that $L(\mu_{p^n}) \neq L(\mu_{p^{n+1}})$. Let H_L be the maximal subfield of the Hilbert p-class field of L such that $\Delta(L/k)$ acts on $\mathrm{Gal}(H_L/L)$ via χ (namely, H_L is the subfield such that $A_L^\chi \simeq \mathrm{Gal}(H_L/L)$ is bijective). We also consider $\mathcal{U}$ in the proof of Lemma 3.1. Using the action of $\Delta(L(\mu_p)/k)$, we know $L(\mu_{p^{n+1}}, \mathcal{U}^{1/p^n}) \cap H_L = L$ and $L(\mu_{p^n}, \mathcal{U}^{1/p^n}) \cap L(\mu_{p^{n+1}}) = L(\mu_{p^n})$. Hence, we can take $\mathfrak{l}' \in \mathcal{S}(L(\mu_{p^n}))$ satisfying the above property.

We put $L' = L(\mu_{p^{n'+n_\mathfrak{r}}})$ and $K' = K(\mu_{p^{n'+n_\mathfrak{r}}})$. We write $\mathcal{R}(L')$ for $(\bigoplus_{v|\mathfrak{r}} \kappa(v)^\times \otimes \mathbf{Z}_p)^\chi$ where $\kappa(v)$ is the residue field of a prime v of L' above $\mathfrak{r}$, and denote by

$$r_{L'} : (\{x \in L'^\times \mid (x) \text{ is prime to } \mathfrak{r}\} \otimes \mathbf{Z}_p)^\chi \longrightarrow \mathcal{R}(L'),$$

the natural homomorphism. We define $\mathcal{R}(K')$ and $r_{K'}$ similarly. Consider the images of $g_{\mathfrak{l}'}^{K'}$ and $g_{\mathfrak{l}'}^{L'}$ in $\mathcal{R}(L')$. Note that the natural map gives an isomorphism $\mathcal{R}(K') \xrightarrow{\simeq} \mathcal{R}(L')$ because all primes of K' above $\mathfrak{r}$ are totally ramified in L'. We identify $\mathcal{R}(L')$ with $\mathcal{R}(K')$ by this isomorphism. Then it follows from $[L' : K'] = p^{n_\mathfrak{r}}$ that the norm map induces the $p^{n_\mathfrak{r}}$th power map on $\mathcal{R}(L')$. On the other hand, by the norm property of the Euler system (see (4.2) in § 4.2) we have $N_{L'/K'}(g_{\mathfrak{l}'}^{L'}) = (g_{\mathfrak{l}'}^{K'})^{(1-\varphi_\mathfrak{r}^{-1})^\chi}$. Hence, on $\mathcal{R}(L')$ we get $r_{L'}(g_{\mathfrak{l}'}^{L'})^{p^{n_\mathfrak{r}}} = r_{K'}(g_{\mathfrak{l}'}^{K'})^{1-N(\mathfrak{r})^{-1}}$. For each prime v of L' above $\mathfrak{r}$, $\kappa(v)$ contains a primitive $p^{n'+n_\mathfrak{r}}$th root of unity, so we have $\mathrm{ord}_p(\#\kappa(v)^\times) \geqslant n' + n_\mathfrak{r}$. Therefore, the above equality implies

$$r_{L'}(g_{\mathfrak{l}'}^{L'}) \equiv r_{K'}(g_{\mathfrak{l}'}^{K'})^{(1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}} \pmod{p^{n'}}$$

(the congruence means the equality in $\mathcal{R}(L')/p^{n'}$). Since both L'/L and K'/K are unramified outside p and all primes above p of k are ramified in L and K by the assumption (*) in § 4.1, we have

$$N_{L'/L}(g_{\mathfrak{l}'}^{L'}) = g_{\mathfrak{l}'}^{L} \quad \text{and} \quad N_{K'/K}(g_{\mathfrak{l}'}^{K'}) = g_{\mathfrak{l}'}^{K}$$

by the norm property (4.2) in § 4.2. Taking the norm $N_{L'/L}$ of both sides of the above congruence, we get

$$r_L(g_{\mathfrak{l}'}^{L}) \equiv r_K(g_{\mathfrak{l}'}^{K})^{(1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}} \pmod{p^{n'}}. \tag{4.4}$$

Since $\mathcal{R}(L)$ is a free $O_\chi/p^{n'}$-module, the above congruence is the equality in $\mathcal{R}(L)$. This shows that Proposition 4.2 is true for $\mathfrak{l}'$.

By our assumption on $\mathfrak{l}'$, we can take an element $a \in (L^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(a) = (\mathfrak{l}'_L - \mathfrak{l}_L)^\chi$. Then we have $\mathrm{div}\, g_{\mathfrak{l}'}^L / a^{\theta_L^\chi} = \mathrm{div}\, g_{\mathfrak{l}}^L$, which implies, by Lemma 4.1, that $g_{\mathfrak{l}'}^L / a^{\theta_L^\chi} = g_{\mathfrak{l}}^L$ in $(L^\times \otimes \mathbf{Z}_p)^\chi$. In the same way, putting $b = N_{L/K}(a)$, we have $\mathrm{div}\, g_{\mathfrak{l}'}^K / b^{\theta_K^\chi} = \mathrm{div}\, g_{\mathfrak{l}}^K$, which implies $g_{\mathfrak{l}'}^K / b^{\theta_K^\chi} = g_{\mathfrak{l}}^K$ in $(K^\times \otimes \mathbf{Z}_p)^\chi$ by Lemma 4.1. Since $G_\mathfrak{r}$ acts on $\mathcal{R}(L)$ trivially, by Lemma 3.4 we have

$$\begin{aligned} r_L(a^{\theta_L^\chi}) &= r_L(a)^{(1-\varphi_\mathfrak{r}^{-1})^\chi \theta_K^\chi} = r_L(a)^{\theta_K^\chi (1-N(\mathfrak{r})^{-1})} = r_L(a^{p^{n_\mathfrak{r}}})^{\theta_K^\chi (1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}} \\ &= r_K(N_{L/K}(a))^{\theta_K^\chi (1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}} = r_K(b^{\theta_K^\chi})^{(1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}}. \end{aligned} \tag{4.5}$$

Combining (4.4) and (4.5), we get

$$r_L(g_{\mathfrak{l}}^L) = r_L\left(\frac{g_{\mathfrak{l}'}^L}{a^{\theta_L^\chi}}\right) = r_K\left(\frac{g_{\mathfrak{l}'}^K}{b^{\theta_K^\chi}}\right)^{(1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}} = r_K(g_{\mathfrak{l}}^K)^{(1-N(\mathfrak{r})^{-1})/p^{n_\mathfrak{r}}}.$$

This completes the proof of Proposition 4.2. □

We consider a homomorphism

$$\mathrm{div} : (K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n} \longrightarrow (\mathrm{Div}_K/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n}$$

induced by the homomorphism div, and denote it also by the same notation div. For $\mathfrak{r} \in \mathcal{S}(K)$ we also use

$$\mathrm{div}_\mathfrak{r} : (K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n} \longrightarrow (O_\chi/p^N[\Gamma(K/k)]) \otimes \mathcal{G}_\mathfrak{n},$$

which is obtained from $\mathrm{div}_{\mathfrak{r}} : (K^{\times}/p^N)^{\chi} \longrightarrow O_{\chi}[\Gamma(K/k)]/p^N$ defined in § 3.3. There, we also defined

$$\phi_{\mathfrak{r}} : (K^{\times}/p^N)^{\chi} \longrightarrow O_{\chi}/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{r}},$$

for $\mathfrak{r} \in \mathcal{S}(K)$ though we used $\mathfrak{l}$ instead of $\mathfrak{r}$ in § 3.3. If $\mathfrak{r}$ divides $\mathfrak{n}$, then the above homomorphism induces

$$\phi_{\mathfrak{r}} : (K^{\times}/p^N)^{\chi} \otimes \mathcal{G}_{\mathfrak{n}/\mathfrak{r}} \longrightarrow O_{\chi}/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{n}},$$

which we also denote by $\phi_{\mathfrak{r}}$.

PROPOSITION 4.3. *Suppose that* $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$.

(0) *If* ρ *is a prime of* K *that does not divide* $\mathfrak{n}\mathfrak{l}$, *then it is not in the support of* $\mathrm{div}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}})$.
(1) *For any prime* $\mathfrak{r}$ *dividing* $\mathfrak{n}$, *we have* $\mathrm{div}_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = \phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$.
(2) *We have* $\mathrm{div}_{\mathfrak{l}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = \tilde{\delta}_{\mathfrak{n}}$.

Proof. The property (0) follows from the fact that ρ is unramified in $K(\mathfrak{n})$, and $g_{\mathfrak{l}}^{K(\mathfrak{n})}$ is a unit outside $\mathfrak{l}$. The property (2) is immediate from the definitions of $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ and $\tilde{\delta}_{\mathfrak{n}}$. The property (1) is a standard property of Euler systems (cf. Rubin [**17**, Theorem 4.5.4]) and can be proved by the usual argument (see Rubin [**15**, Proposition 2.4]). We shall give here a proof to clarify where we use Proposition 4.2 and Lemma 3.2.

We take a lifting $\kappa^{\wedge}_{\mathfrak{n},\mathfrak{l}} \in (K^{\times} \otimes \mathbf{Z}_p)^{\chi}$ of $\kappa_{\mathfrak{n},\mathfrak{l}} \in (K^{\times}/p^N)^{\chi}$. By definition we can write $\kappa^{\wedge}_{\mathfrak{n},\mathfrak{l}} = D_{\mathfrak{n}} g_{\mathfrak{l}}^{K(\mathfrak{n})}/\beta^{p^N}$ for some $\beta \in (K(\mathfrak{n})^{\times} \otimes \mathbf{Z}_p)^{\chi}$. In the same way we write $\kappa^{\wedge}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}} = D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n}/\mathfrak{r})}/(\beta')^{p^N}$ for some $\beta' \in (K(\mathfrak{n}/\mathfrak{r})^{\times} \otimes \mathbf{Z}_p)^{\chi}$. Since $\kappa^{\wedge}_{\mathfrak{n},\mathfrak{l}}$, $\kappa^{\wedge}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}$ are elements of $(K^{\times} \otimes \mathbf{Z}_p)^{\chi}$, we compute

$$\begin{aligned}(\sigma_{\mathfrak{r}} - 1)\beta &= ((\sigma_{\mathfrak{r}} - 1) D_{\mathfrak{n}} g_{\mathfrak{l}}^{K(\mathfrak{n})})^{1/p^N} = ((p^{n_{\mathfrak{r}}} - N_{\mathfrak{r}}) D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n})})^{1/p^N} \\ &= (D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n})})^{p^{n_{\mathfrak{r}}-N}} / ((1 - \varphi_{\mathfrak{r}}^{-1}) D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n}/\mathfrak{r})})^{1/p^N} \\ &= (D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n})})^{p^{n_{\mathfrak{r}}-N}} / (1 - \varphi_{\mathfrak{r}}^{-1})\beta'.\end{aligned}$$

We apply Proposition 4.2 to $K(\mathfrak{n}/\mathfrak{r})$ to get $g_{\mathfrak{l}}^{K(\mathfrak{n})} \equiv (g_{\mathfrak{l}}^{K(\mathfrak{n}/\mathfrak{r})})^{(1-N(\mathfrak{r})^{-1})/p^{n_{\mathfrak{r}}}} \pmod{\rho_{\mathfrak{r}}}$ for any prime $\rho_{\mathfrak{r}}$ of $K(\mathfrak{n})$ above $\mathfrak{r}$. Therefore, we have

$$\begin{aligned}(\sigma_{\mathfrak{r}} - 1)\beta &\equiv (D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n}/\mathfrak{r})})^{(1-N(\mathfrak{r})^{-1})/p^N} / (\beta')^{1-N(\mathfrak{r})^{-1}} \pmod{\rho_{\mathfrak{r}}} \\ &= (D_{\mathfrak{n}/\mathfrak{r}} g_{\mathfrak{l}}^{K(\mathfrak{n}/\mathfrak{r})} / (\beta')^{p^N})^{(1-N(\mathfrak{r})^{-1})/p^N} = (\kappa^{\wedge}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})^{(1-N(\mathfrak{r})^{-1})/p^N} \\ &\equiv (\kappa^{\wedge}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})^{(N(\mathfrak{r})-1)/p^N} \pmod{\mathfrak{r}_K}.\end{aligned}$$

Here, we used the fact that $\varphi_{\mathfrak{r}}$ is the $N(\mathfrak{r})$th power map on the residue field of $\rho_{\mathfrak{r}}$ to get the first congruence, and that the $N(\mathfrak{r})$th power map is the identity map on the residue field of $\mathfrak{r}_K$ to get the last congruence.

By Lemma 3.2 we have $\phi_{\mathfrak{r}}(\kappa^{\wedge}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}) = \phi_{\mathfrak{r}}(\kappa_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}) = \sigma_{\mathfrak{r}}^{-p^N \mathrm{div}_{\mathfrak{r}}(\beta)}$. Therefore, we get

$$\phi_{\mathfrak{r}}(\kappa_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}) = \sigma_{\mathfrak{r}}^{-p^N \mathrm{div}_{\mathfrak{r}}(\beta)} = -\mathrm{div}_{\mathfrak{r}}(\beta^{p^N}) \otimes \sigma_{\mathfrak{r}} = \mathrm{div}_{\mathfrak{r}}(\kappa^{\wedge}_{\mathfrak{n},\mathfrak{l}}) \otimes \sigma_{\mathfrak{r}} = \mathrm{div}_{\mathfrak{r}}(\kappa_{\mathfrak{n},\mathfrak{l}}) \otimes \sigma_{\mathfrak{r}},$$

which implies $\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}) = \mathrm{div}_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}})$. □

REMARK 4.4. In § 5, we will give a more general definition of $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$, for which we will prove the same properties in Proposition 5.2.

5. *Kolyvagin systems of Gauss sum type* I

5.1.

In the argument to define $\kappa_{\mathfrak{n},\mathfrak{l}}$ in the previous section, *the assumption* $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$ *is needed* because we need the norm property (4.2) in § 4.2 for $L = K(\mathfrak{n})$, $M = K$ to define $g_{\mathfrak{l}}^{K(\mathfrak{n})}$, and (4.2) holds only when $\mathfrak{l}$ splits in $L = K(\mathfrak{n})$ as we explained after (4.2). But the theory of Kolyvagin systems by Mazur and Rubin [**12**] suggests that there would exist $\kappa_{\mathfrak{n},\mathfrak{l}}$ for more general $\mathfrak{l}$. They studied their theory mainly over principal ideal domains in [**12**], so we cannot apply it directly to our case. We shall construct in this section the elements $\kappa_{\mathfrak{n},\mathfrak{l}}$ explicitly under some (mild) assumptions on $\mathfrak{l}$.

We shall explain a little more what we need. When we define $\kappa_{\mathfrak{n},\mathfrak{l}}$, $\mathfrak{l}$ has to be chosen from $\mathcal{S}(K(\mathfrak{n}))$, and hence taken after we have taken $\mathfrak{n}$. But we need later elements $\kappa_{\mathfrak{n},\mathfrak{l}}$ where we take $\mathfrak{n}$ after we have taken $\mathfrak{l}$ (see § 10.2 where we define $x_{\mathfrak{n},\mathfrak{l}}$, taking $\mathfrak{n}$ after we have taken $\mathfrak{l}$). We sometimes need both $\kappa_{\mathfrak{l}_1,\mathfrak{l}_2}$ and $\kappa_{\mathfrak{l}_2,\mathfrak{l}_1}$ (see Remark 10.6); namely, we need $\kappa_{\mathfrak{n},\mathfrak{l}}$ for more general $(\mathfrak{n},\mathfrak{l})$. In the following, we define a certain subset $\mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$ of $\mathcal{N}(K)$, and define $\kappa_{\mathfrak{n},\mathfrak{l}} \in (K^\times/p^N)^\chi$ for all $(\mathfrak{n},\mathfrak{l})$ such that $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$, though it seems that $\kappa_{\mathfrak{n},\mathfrak{l}}$ could be defined for more general $(\mathfrak{n},\mathfrak{l})$ (cf. Remark 5.4 and § 6.3).

Suppose that c is the exponent of A_K^χ, namely, the smallest integer such that $p^c A_K^\chi = 0$. The following lemma is easy to prove, but is useful in § 5.2.

LEMMA 5.1. *Let g, g' be elements in $(K^\times/p^{N+c})^\chi$. Suppose* $\mathrm{div}(g) \equiv \mathrm{div}(g') \pmod{p^{N+c}}$. *Then we have* $g \bmod p^N = g' \bmod p^N$ *in* $(K^\times/p^N)^\chi$.

Proof. Consider the exact sequence

$$0 \longrightarrow A_K^\chi[p^{N+c}] \longrightarrow (K^\times/p^{N+c})^\chi \longrightarrow (\mathrm{Div}_K/p^{N+c})^\chi \longrightarrow A_K^\chi/p^{N+c} \longrightarrow 0.$$

Since $(K^\times \otimes \mathbf{Z}_p)^\chi$ is p-torsion free, $(K^\times/p^{N+c})^\chi$ is a free O_χ/p^{N+c}-module. Hence, the image of $A_K^\chi[p^{N+c}] = A_K^\chi$ in $(K^\times/p^{N+c})^\chi$ is in $p^N(K^\times/p^{N+c})^\chi$. This shows that $g \bmod p^N = g' \bmod p^N$. □

5.2.

For any integer $m \geqslant N$ we define $\mathcal{S}_m(K) = \{\mathfrak{l} \in \mathcal{S}(K) | n_{\mathfrak{l}} \geqslant m\}$. For any integer $n > 0$ we put

$$\mathcal{S}_{[n]}(K) = \mathcal{S}_{N+nc}(K),$$

and define $\mathcal{N}_{[n]}(K)$ to be the set consisting of all square-free products of primes in $\mathcal{S}_{[n]}(K)$.

For $\mathfrak{n} \in \mathcal{N}$ we define $\epsilon(\mathfrak{n})$ to be the number of primes which divide $\mathfrak{n}$ (namely, $\epsilon(\mathfrak{n}) = m$ for $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m$ in § 4.3), and consider $\mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$. For $\mathfrak{n} = 1$ we define $\epsilon(1) = 0$.

Suppose that $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$, and $\mathfrak{r}$ is a prime factor of $\mathfrak{n}$. Replacing N by $N + \epsilon(\mathfrak{n})c$, we can define $\phi_{\mathfrak{r}} : (K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \longrightarrow O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)] \otimes G_{\mathfrak{r}}$. By the same method as in the proof of Proposition 4.2, using the Chebotarev density theorem, we can take $\mathfrak{l}' \in \mathcal{S}_{[\epsilon(\mathfrak{n})]}(K(\mathfrak{n}))$ such that the classes $[\mathfrak{l}'_K]^\chi$ and $[\mathfrak{l}_K]^\chi$ in A_K^χ coincide. By the exact sequence in Lemma 4.1, there is a unique element $b \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$. Replacing N by $N + \epsilon(\mathfrak{n})c$, we define $\tilde{\delta}_{\mathfrak{n}}^{(N+\epsilon(\mathfrak{n})c)} \in O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)] \otimes G_{\mathfrak{n}}$, and $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'}^{(N+\epsilon(\mathfrak{n})c)} \in (K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_{\mathfrak{n}}$ by the usual Euler system argument in § 4.3. Using induction on $\epsilon(\mathfrak{n})$, we define

$$\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}} = \tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'}^{(N+\epsilon(\mathfrak{n})c)} - \tilde{\delta}_{\mathfrak{n}}^{(N+\epsilon(\mathfrak{n})c)} b - \sum_{\mathfrak{r} \mid \mathfrak{n}} (\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}} \otimes \phi_{\mathfrak{r}}(b)) \in (K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_{\mathfrak{n}}.$$

Here, we wrote the group law of $(K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_\mathfrak{n}$ additively though $K^\times$ is a multiplicative group. The element $\tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)}b$ means $\alpha b \otimes \tau \in (K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_\mathfrak{n}$ if $\tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)} = \alpha \otimes \tau \in O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)] \otimes \mathcal{G}_\mathfrak{n}$. The sum is taken over all primes dividing $\mathfrak{n}$. Note that $\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}}$ is defined by induction because of $\epsilon(\mathfrak{n}/\mathfrak{r}) < \epsilon(\mathfrak{n})$. We regard $\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}} \otimes \phi_\mathfrak{r}(b)$ as an element of $(K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_\mathfrak{n}$ by the identification

$$\begin{aligned}&((K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_{\mathfrak{n}/\mathfrak{r}}) \otimes_{O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)]} (O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)] \otimes \mathcal{G}_\mathfrak{r})\\ &\quad = (K^\times/p^{N+\epsilon(\mathfrak{n})c})^\chi \otimes \mathcal{G}_\mathfrak{n}.\end{aligned}$$

We put

$$\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = \tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}} \bmod p^N \in (K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n}.$$

Proposition 5.2. *The element $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ defined above is well-defined, namely independent of the choice of $\mathfrak{l}'$ (hence independent of the choice of b). This element satisfies the following properties.*

(0) *If ρ is a prime of K that does not divide $\mathfrak{n}\mathfrak{l}$, then it is not in the support of* $\mathrm{div}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}})$.
(1) *For any prime $\mathfrak{r}$ dividing $\mathfrak{n}$, we have* $\mathrm{div}_\mathfrak{r}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = \phi_\mathfrak{r}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$.
(2) *We have* $\mathrm{div}_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = \tilde{\delta}_\mathfrak{n}$.

Remark 5.3. In the above proposition, if we further assume that $\mathfrak{l}$ is in $\mathcal{S}(K(\mathfrak{n}))$, then we can take $\mathfrak{l}' = \mathfrak{l}$ and $b = 1$. Hence, we have $\phi_\mathfrak{r}(b) = 0$, and $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ defined above coincides with $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ defined in § 4.3. Therefore, our notation is consistent.

Proof. We prove this proposition by induction on $\epsilon(\mathfrak{n})$. We first show that the following conditions are satisfied.

$(0)'$ If ρ is a prime which does not divide $\mathfrak{n}\mathfrak{l}$, then it is not in the support of $\mathrm{div}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \bmod p^{N+c}$.

$(1)'$ For any prime $\mathfrak{r}$ dividing $\mathfrak{n}$, we have $\mathrm{div}_\mathfrak{r}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \equiv \phi_\mathfrak{r}(\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}) \pmod{p^{N+c}}$.

$(2)'$ We have $\mathrm{div}_\mathfrak{l}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \equiv \tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)} \pmod{p^{N+c}}$.

By induction on $\epsilon(\mathfrak{n})$, $N + \epsilon(\mathfrak{n})c = N + c + \epsilon(\mathfrak{n}/\mathfrak{r})c$ implies that $\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}} \bmod p^{N+c}$ is well-defined, that is, it does not depend on the choice of the auxiliary prime for $\mathfrak{r}$. Using $(0)'$, $(1)'$, $(2)'$ for $\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}}$, we have

$$\mathrm{div}(\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}}) \equiv \sum_{\mathfrak{r}' \mid \mathfrak{n}/\mathfrak{r}} \phi_{\mathfrak{r}'}(\tilde{\kappa}'^{(N+c)}_{\mathfrak{n}/\mathfrak{r}\,\mathfrak{r}',\mathfrak{r}})\, \mathfrak{r}'_K + \tilde{\delta}^{(N+\epsilon(\mathfrak{n})c)}_{\mathfrak{n}/\mathfrak{r}}\, \mathfrak{r}_K \pmod{p^{N+c}}.$$

Therefore, by Proposition 4.3(0), if a prime ρ is prime to $\mathfrak{n}\mathfrak{l}\mathfrak{l}'$, then ρ is not in the support of $\mathrm{div}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \bmod p^{N+c}$. Concerning $\mathfrak{l}'$, if $\mathfrak{l}' \neq \mathfrak{l}$, by Proposition 4.3(2) we have

$$\mathrm{div}_{\mathfrak{l}'}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \equiv \tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)} - \tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)} \equiv 0 \pmod{p^{N+c}}.$$

Hence, we obtain the property $(0)'$.

For $\mathfrak{r}$ such that $\mathfrak{r} \mid \mathfrak{n}$, we can compute

$$\begin{aligned}\mathrm{div}_\mathfrak{r}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) &\equiv \phi_\mathfrak{r}(\tilde{\kappa}^{(N+\epsilon(\mathfrak{n})c)}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}'}) - \tilde{\delta}^{(N+\epsilon(\mathfrak{n})c)}_{\mathfrak{n}/\mathfrak{r}} \otimes \phi_\mathfrak{r}(b) - \sum_{\mathfrak{r}' \mid \mathfrak{n}/\mathfrak{r}} \phi_\mathfrak{r}(\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r}\,\mathfrak{r}',\mathfrak{r}'}) \otimes \phi_{\mathfrak{r}'}(b)\\ &\equiv \phi_\mathfrak{r}(\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}) \pmod{p^{N+c}},\end{aligned}$$

by Proposition 4.3(1), (2) and the definition of $\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}$, $\tilde{\kappa}'_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}$. Thus, we get the property $(1)'$.

Concerning the property $(2)'$, we just note that $\mathfrak{l}$ is prime to $\mathfrak{n}$, and get

$$\mathrm{div}_\mathfrak{l}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \equiv -(-\tilde{\delta}^{(N+\epsilon(\mathfrak{n})c)}_\mathfrak{n}) \equiv \tilde{\delta}^{(N+\epsilon(\mathfrak{n})c)}_\mathfrak{n} \pmod{p^{N+c}}$$

if $\mathfrak{l}' \neq \mathfrak{l}$. If $\mathfrak{l}' = \mathfrak{l}$, then we get $\mathrm{div}_{\mathfrak{l}}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) = \tilde{\delta}_{\mathfrak{n}}^{(N+\epsilon(\mathfrak{n})c)}$ by Proposition 4.3(2).

The properties $(0)'$, $(1)'$, $(2)'$ imply that $\mathrm{div}(\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}) \bmod p^{N+c}$ is independent of the choice of $\mathfrak{l}'$. Hence, by Lemma 5.1, $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = \tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}} \bmod p^N$ is independent of the choice of $\mathfrak{l}'$. This completes the proof of Proposition 5.2. □

REMARK 5.4. We give another definition of $\mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$. Let K_∞/K be the cyclotomic $\mathbf{Z}_p$-extension, and K_m the mth layer. Since we assumed $\mu(X^\chi_{K_\infty}) = 0$, the map $A^\chi_{K_m}[p^N] \longrightarrow A^\chi_K[p^N]$ induced by the norm map becomes the zero map if m is sufficiently large. We take the minimal m satisfying the above property, and put $K_{[1]} = K_m$. We define inductively $K_{[n]}$ by $K_{[n]} = (K_{[n-1]})_{[1]}$ where we applied the above definition to $K_{[n-1]}$ instead of K. For $n > 0$ we put

$$\mathcal{S}_{[n]}(K) = \mathcal{S}(K_{[n]}),$$

and define $\mathcal{N}_{[n]}(K)$ to be the set consisting of all square-free products of primes in $\mathcal{S}_{[n]}(K)$. We consider $\mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$.

We assume $\mathfrak{n} \neq 1$ and $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$. By the Chebotarev density theorem, we can take $\mathfrak{l}' \in \mathcal{S}(K_{[\epsilon(\mathfrak{n})]}(\mathfrak{n}))$ such that $\mathfrak{l}'_{K_{[\epsilon(\mathfrak{n})]}}$ and $\mathfrak{l}_{K_{[\epsilon(\mathfrak{n})]}}$ yield the same class in $A^\chi_{K_{[\epsilon(\mathfrak{n})]}}$. By Lemma 4.1, for $K_{[\epsilon(\mathfrak{n})]}$ there is a unique element $b_{[\epsilon(\mathfrak{n})]} \in (K^\times_{[\epsilon(\mathfrak{n})]} \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b_{[\epsilon(\mathfrak{n})]}) = (\mathfrak{l}'_{K_{[\epsilon(\mathfrak{n})]}} - \mathfrak{l}_{K_{[\epsilon(\mathfrak{n})]}})^\chi$. Put $b = N_{K_{[\epsilon(\mathfrak{n})]}/K_{[1]}}(b_{[\epsilon(\mathfrak{n})]})$. Again, using induction on $\epsilon(\mathfrak{n})$, we define

$$(\tilde{\kappa}^{K_{[1]}}_{\mathfrak{n},\mathfrak{l}})' = \tilde{\kappa}^{K_{[1]}}_{\mathfrak{n},\mathfrak{l}'} - \tilde{\delta}^{K_{[1]}}_{\mathfrak{n}} b - \sum_{\mathfrak{r} \mid \mathfrak{n}} ((\tilde{\kappa}^{K_{[1]}}_{\mathfrak{n}/\mathfrak{r},\mathfrak{r}})' \otimes \phi^{K_{[1]}}_{\mathfrak{r}}(b)) \in (K^\times_{[1]}/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}},$$

and $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = N_{K_{[1]}/K}((\tilde{\kappa}^{K_{[1]}}_{\mathfrak{n},\mathfrak{l}})') \in (K^\times/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}}$. Then we can prove that this element $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ does not depend on the choice of $\mathfrak{l}'$ and satisfies the properties in Proposition 5.2. This definition looks similar to the first definition, but this method is useful when we study more general Galois representations (see [**11**]).

5.3.

The following lemma is useful when we choose $\mathfrak{l}'$ in the definition of $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ in the previous subsection.

LEMMA 5.5. *Assume $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m \in \mathcal{N}(K)$ and that $\mathfrak{l} \in \mathcal{S}(K)$ is prime to $\mathfrak{n}$. Suppose that for each $i = 1, \ldots, m$, $\sigma_i \in O_\chi/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{r}_i}$ is given. Then there are infinitely many $\mathfrak{l}' \in \mathcal{S}(K(\mathfrak{n}))$ which satisfy the following properties.*

(i) *The class $[\mathfrak{l}'_K]^\chi$ in A^χ_K coincides with the class $[\mathfrak{l}_K]^\chi$.*

(ii) *For the element $z \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(z) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$, $\phi_{\mathfrak{r}_i}(z) = \sigma_i$ holds for each $i = 1, \ldots, m$.*

Proof. Let $K\{\mathfrak{n}\}$ be the maximal abelian p-extension of K which is unramified outside $\mathfrak{n}$. For a prime v of K, we define $U_{K_v} = O^\times_{K_v}$ and $U^1_{K_v} = 1 + m_v O_{K_v}$ as usual where m_v is the maximal ideal of O_{K_v}. The residue field of v is denoted by $\kappa(v)$. By class field theory, we have an isomorphism

$$\frac{\prod_{v|\mathfrak{n}} K^\times_v/U^1_{K_v} \times \bigoplus_{v\nmid\mathfrak{n}} K^\times_v/U_{K_v}}{\text{the image of } K^\times} \otimes \mathbf{Z}_p \xrightarrow{\simeq} \mathrm{Gal}(K\{\mathfrak{n}\}/K),$$

which yields an exact sequence

$$0 \longrightarrow \left(\bigoplus_{v|\mathfrak{n}} \kappa(v)^\times \otimes \mathbf{Z}_p\right)^\chi \longrightarrow \mathrm{Gal}(K\{\mathfrak{n}\}/K)^\chi \longrightarrow A_K^\chi \longrightarrow 0,$$

where the injectivity of the second arrow follows from $(O_K^\times \otimes \mathbf{Z}_p)^\chi = 0$. We denote by $K\{\mathfrak{n}\}^\chi$ the intermediate field of $K\{\mathfrak{n}\}/K$ such that $\mathrm{Gal}(K\{\mathfrak{n}\}^\chi/K) = \mathrm{Gal}(K\{\mathfrak{n}\}/K)^\chi$.

By a method similar to what we did when we defined $\phi_\mathfrak{l}$ in § 3.3, we identify $(\bigoplus_{v|\mathfrak{n}} \kappa(v)^\times \otimes \mathbf{Z}_p)^\chi$ with $O_\chi[\Gamma(K/k)] \otimes G_{\mathfrak{r}_1} \oplus \ldots \oplus O_\chi[\Gamma(K/k)] \otimes G_{\mathfrak{r}_m}$. We take $\sigma_\chi \in (\bigoplus_{v|\mathfrak{n}} \kappa(v)^\times \otimes \mathbf{Z}_p)^\chi$ such that $\sigma_\chi \bmod p^N$ is $(\sigma_1, \ldots, \sigma_m)$, and regard σ_χ as an element of $\mathrm{Gal}(K\{\mathfrak{n}\}^\chi/K)$. Let $(\mathfrak{l}_K, K\{\mathfrak{n}\}^\chi/K) \in \mathrm{Gal}(K\{\mathfrak{n}\}^\chi/K)$ be the Artin symbol (the Frobenius of $\mathfrak{l}_K$). Note that $\Delta(K/k)$ acts trivially on $\mathrm{Gal}(K(\mathfrak{n})/K)$, so $K\{\mathfrak{n}\}^\chi \cap K(\mathfrak{n}) = K$. Put $L = K\{\mathfrak{n}\}^\chi K(\mathfrak{n})$, which is a subfield of $K\{\mathfrak{n}\}$. We take $\tau \in \mathrm{Gal}(L/K)$ whose image in $\mathrm{Gal}(K\{\mathfrak{n}\}^\chi/K)$ is $\sigma_\chi^{-1}(\mathfrak{l}_K, K\{\mathfrak{n}\}^\chi/K)$ and whose image in $\mathrm{Gal}(K(\mathfrak{n})/K)$ is the identity map.

Let $\mathcal{U}$ be as in the proof of Lemma 3.1. Considering the action of $\mathrm{Gal}(K_0(\mu_p)/k)$, we have $K(\mu_{p^{n+1}}, \mathcal{U}^{1/p^n}) \cap L = K$. Hence, by the Chebotarev density theorem there exist infinitely many $\mathfrak{l}' \in \mathcal{S}(K)$ such that $(\mathfrak{l}'_K, L/K) = \tau$ in $\mathrm{Gal}(L/K)$ where $(\mathfrak{l}'_K, L/K)$ is the Frobenius of $\mathfrak{l}'_K$ in $\mathrm{Gal}(L/K)$.

Since the image of $(\mathfrak{l}'_K, L/K)$ in $\mathrm{Gal}(K(\mathfrak{n})/K)$ is the identity, $\mathfrak{l}'$ is in $\mathcal{S}(K(\mathfrak{n}))$. Let $\Pi_{\mathfrak{l}'}$ be the idele whose $\mathfrak{l}'_K$-component is a prime element of $\mathfrak{l}'_K$ and whose other components are trivial. Let $\Pi_{\mathfrak{l},\sigma_\chi}$ denote the idele whose $(\Pi_{v|\mathfrak{n}} K_v^\times \otimes \mathbf{Z}_p)^\chi$-component is $\tilde{\sigma}_\chi^{-1} \in (\Pi_{v|\mathfrak{n}} K_v^\times \otimes \mathbf{Z}_p)^\chi$ which is a lifting of $\sigma_\chi^{-1} \in (\Pi_{v|\mathfrak{n}} U_{K_v}/U_{K_v}^1 \otimes \mathbf{Z}_p)^\chi$, and whose $\mathfrak{l}_K$-component is a prime element of $\mathfrak{l}_K$ and whose other components are trivial. By definition, $\Pi_{\mathfrak{l}'}$ and $\Pi_{\mathfrak{l},\sigma_\chi}$ have the same class in

$$\left(\frac{\prod_{v|\mathfrak{n}} K_v^\times/U_{K_v}^1 \times \bigoplus_{v\nmid\mathfrak{n}} K_v^\times/U_{K_v}}{\text{the image of } K^\times} \otimes \mathbf{Z}_p\right)^\chi = \mathrm{Gal}(K\{\mathfrak{n}\}^\chi/K).$$

Hence, there is an element $z \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\Pi_{\mathfrak{l}'} = z\Pi_{\mathfrak{l},\sigma_\chi}$ in $((\prod_{v|\mathfrak{n}} K_v^\times/U_{K_v}^1 \times \bigoplus_{v\nmid\mathfrak{n}} K_v^\times/U_{K_v}) \otimes \mathbf{Z}_p)^\chi$. Therefore, the class $[\mathfrak{l}'_K]^\chi$ in A_K^χ coincides with the class $[\mathfrak{l}_K]^\chi$, and $\mathrm{div}(z) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$. Furthermore, $\phi_{\mathfrak{r}_i}(z) = \sigma_i$ for all $i = 1, \ldots, m$. □

Remark 5.6. In the definition of $\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}$ in § 5.2, using Lemma 5.5, we can take $\mathfrak{l}' \in \mathcal{S}(K(\mathfrak{n}))$ and $b \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$ and $\phi_\mathfrak{r}^K(b) = 0$ in $O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)] \otimes G_\mathfrak{n}$ for all $\mathfrak{r}$ dividing $\mathfrak{n}$. Then we have $\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}} = \tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'}^{(N+\epsilon(\mathfrak{n})c)} - \tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)} b$, which implies that

$$\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = \tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'}^{(N+\epsilon(\mathfrak{n})c)} - \tilde{\delta}_\mathfrak{n}^{(N+\epsilon(\mathfrak{n})c)} b \bmod p^N.$$

This fact will be used later.

6. *Kolyvagin systems of Gauss sum type* II

In this section, we study $\phi_\mathfrak{r}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}})$ for $\mathfrak{r}$ dividing $\mathfrak{n}\mathfrak{l}$. We use the same notation K, χ, $g_\mathfrak{l}^\chi$, $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ and so on as in the previous section.

6.1.

Suppose that $\mathfrak{l} \in \mathcal{S}(K)$. We consider the homomorphism

$$\phi_\mathfrak{l} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)] \otimes G_\mathfrak{l}$$

defined in § 3.3.

PROPOSITION 6.1. *We have* $\phi_{\mathfrak{l}}(g_{\mathfrak{l}}^K) = -\delta_{\mathfrak{l}} \otimes \sigma_{\mathfrak{l}} = -\tilde{\delta}_{\mathfrak{l}}$.

When $k = \mathbf{Q}$, this proposition and the next corollary correspond to Rubin [**16**, Theorem 2.4] where it was proved by using the explicit form of Gauss sums. We do not know the explicit form of our $g_{\mathfrak{l}}^K$, so we prove this proposition by a completely different method which can be applied to general k. This proposition can be formulated in a simple form as above, because the homomorphism $\phi_{\mathfrak{l}}$ is defined not only on the $\mathfrak{l}$-units but defined on the whole $K^\times$ by using the reciprocity map.

Proof of Proposition 6.1. Put $L = K(\mathfrak{l})$. As in the proof of Proposition 4.2, using the Chebotarev density theorem, we can take $\mathfrak{l}' \in \mathcal{S}(L)$ such that the class $[\mathfrak{l}'_L]^\chi$ in A_L^χ coincides with the class $[\mathfrak{l}_L]^\chi$ in A_L^χ where $\mathfrak{l}_L$ is the unique prime of L above $\mathfrak{l}_K$. We take $a \in (L^\times \otimes \mathbf{Z}_p)^\chi$ such that $\operatorname{div}(a) = (\mathfrak{l}'_L - \mathfrak{l}_L)^\chi$.

Let $c_{L/K} : O_\chi[\Gamma(L/k)] \longrightarrow O_\chi[\Gamma(K/k)]$ be the natural restriction map. By Lemma 3.4 we have $c_{L/K}(\theta_L^\chi) = (1 - \varphi_{\mathfrak{l}}^{-1})\theta_K^\chi = 0$ because $\mathfrak{l} \in \mathcal{S}(K)$ implies $\varphi_{\mathfrak{l}} = 1$. Hence, $\sigma_{\mathfrak{l}} - 1$ divides θ_L^χ, and we can write

$$\theta_L^\chi = \alpha(\sigma_{\mathfrak{l}} - 1) + \beta(\sigma_{\mathfrak{l}} - 1)^2,$$

for some $\alpha \in O_\chi[\Gamma(K/k)]$ and $\beta \in O_\chi[\Gamma(L/k)]$. We have $\alpha \equiv -\delta_{\mathfrak{l}} \pmod{p^N}$ by (4.3) in § 4.3 (see [**10**, Lemma 4.4]). Since $\mathfrak{l}_L$ is totally ramified in L/K, we have $(\sigma_{\mathfrak{l}} - 1)\,\mathfrak{l}_L = 0$. It follows from $\sigma_{\mathfrak{l}} - 1 \mid \theta_L^\chi$ that $\theta_L^\chi(\mathfrak{l}_L)^\chi = 0$ in $(\mathrm{Div}_L \otimes \mathbf{Z}_p)^\chi$. Therefore, we have

$$\operatorname{div}(g_{\mathfrak{l}'}^L) = \theta_L^\chi(\mathfrak{l}'_L)^\chi = \theta_L^\chi(\mathfrak{l}'_L - \mathfrak{l}_L)^\chi = \operatorname{div}(a^{\theta_L^\chi}),$$

which implies $g_{\mathfrak{l}'}^L = a^{\theta_L^\chi}$ by Lemma 4.1.

Put $z = a^{\alpha + \beta(\sigma_{\mathfrak{l}} - 1)} \in (L^\times \otimes \mathbf{Z}_p)^\chi$. Using the congruence relation (Proposition 4.2), we compute

$$\begin{aligned}(\sigma_{\mathfrak{l}} - 1)z = a^{\theta_L^\chi} = g_{\mathfrak{l}'}^L &\equiv (g_{\mathfrak{l}'}^K)^{(1 - N(\mathfrak{l})^{-1})/p^{n_{\mathfrak{l}}}} \\ &\equiv (g_{\mathfrak{l}'}^K)^{(N(\mathfrak{l}) - 1)/p^{n_{\mathfrak{l}}}} \equiv (g_{\mathfrak{l}'}^K)^{-(1 - N(\mathfrak{l}))/p^{n_{\mathfrak{l}}}} \pmod{\rho_{\mathfrak{l}}},\end{aligned}$$

for any prime $\rho_{\mathfrak{l}}$ of L above $\mathfrak{l}$.

We denote by

$$\operatorname{div}_{\mathfrak{l}_L} : (L^\times \otimes \mathbf{Z}_p)^\chi \longrightarrow \left(\bigoplus_{\rho \mid \mathfrak{l}} \mathbf{Z}_p\right)^\chi \xrightarrow{\simeq} O_\chi[\Gamma(K/k)],$$

the homomorphism induced by $x \mapsto \Sigma_{\rho \mid \mathfrak{l}} \operatorname{ord}_\rho(x)\rho$ where ρ runs through all primes of L above $\mathfrak{l}$, and the second isomorphism is $\vartheta(\mathfrak{l}_L)^\chi \mapsto \vartheta$ for $\vartheta \in O_\chi[\Gamma(K/k)]$. It follows from Lemma 3.2 that

$$\begin{aligned}\phi_{\mathfrak{l}}(g_{\mathfrak{l}'}^K) &= -\operatorname{div}_{\mathfrak{l}_L}(z) \otimes \sigma_{\mathfrak{l}} \bmod p^N \\ &= -(\alpha + \beta(\sigma_{\mathfrak{l}} - 1)) \operatorname{div}_{\mathfrak{l}_L}(a) \otimes \sigma_{\mathfrak{l}} \bmod p^N \\ &= -\alpha \operatorname{div}_{\mathfrak{l}_L}(a) \otimes \sigma_{\mathfrak{l}} \bmod p^N = \alpha \otimes \sigma_{\mathfrak{l}} \bmod p^N \\ &= -\delta_{\mathfrak{l}} \otimes \sigma_{\mathfrak{l}}.\end{aligned}$$

Put $b = N_{L/K}(a) \in (K^\times \otimes \mathbf{Z}_p)^\chi$. By the definition of a, we have $\operatorname{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$. Since $\operatorname{div}(g_{\mathfrak{l}}^K) = \operatorname{div}(g_{\mathfrak{l}'}^K / b^{\theta_K^\chi})$, by Lemma 4.1 we obtain $g_{\mathfrak{l}}^K = g_{\mathfrak{l}'}^K / b^{\theta_K^\chi}$. Since b is a norm from L, by the remark in the end of § 3.3 (by local class field theory), we know $\phi_{\mathfrak{l}}(b) = 0$. Therefore, we finally have

$$\phi_{\mathfrak{l}}(g_{\mathfrak{l}}^K) = \phi_{\mathfrak{l}}(g_{\mathfrak{l}'}^K) = -\delta_{\mathfrak{l}} \otimes \sigma_{\mathfrak{l}} = -\tilde{\delta}_{\mathfrak{l}}. \qquad \square$$

Next, let us consider a map

$$(K^\times / p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}} \longrightarrow O_\chi / p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{n}\,\mathfrak{l}},$$

which is obtained from $\phi_{\mathfrak{l}} : (K^{\times}/p^N)^{\chi} \longrightarrow O_{\chi}/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{l}}$ by tensoring $\mathcal{G}_{\mathfrak{n}}$, and which we also denote by $\phi_{\mathfrak{l}}$.

COROLLARY 6.2. *We assume that* $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$. *Then we have* $\phi_{\mathfrak{l}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = -\tilde{\delta}_{\mathfrak{n}\,\mathfrak{l}}$.

Proof. We denote $\delta_{\mathfrak{l}}$, $\phi_{\mathfrak{l}}$ for $K(\mathfrak{n})$ by $\delta_{\mathfrak{l}}^{K(\mathfrak{n})}$, $\phi_{\mathfrak{l}}^{K(\mathfrak{n})}$. We apply Proposition 6.1 to $K(\mathfrak{n})$ to get

$$\phi_{\mathfrak{l}}^{K(\mathfrak{n})}(g_{\mathfrak{l}}^{K(\mathfrak{n})}) = -\delta_{\mathfrak{l}}^{K(\mathfrak{n})} \otimes \ \sigma_{\mathfrak{l}} \in O_{\chi}/p^N[\Gamma(K(\mathfrak{n})/k)] \otimes G_{\mathfrak{l}} = O_{\chi}/p^N[\Gamma(K/k) \times G_{\mathfrak{n}}] \otimes G_{\mathfrak{l}}.$$

Consider the commutative diagram

$$\begin{array}{ccc} (K(\mathfrak{n})^{\times}/p^N)^{\chi} & \xrightarrow{\phi_{\mathfrak{l}}^{K(\mathfrak{n})}} & O_{\chi}/p^N[\Gamma(K/k) \times G_{\mathfrak{n}}] \otimes G_{\mathfrak{l}} \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle N_{\mathfrak{n}}} \\ (K^{\times}/p^N)^{\chi} & \xrightarrow{\phi_{\mathfrak{l}}} & O_{\chi}/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{l}} \end{array}$$

where i is the natural inclusion map, and $N_{\mathfrak{n}}$ is the multiplication by $N_{\mathfrak{n}} = N_{G_{\mathfrak{n}}} = \Sigma_{\sigma \in G_{\mathfrak{n}}}\sigma$. Since $i(\kappa_{\mathfrak{n},\mathfrak{l}}) = D_{\mathfrak{n}} g_{\mathfrak{l}}^{K(\mathfrak{n})}$ and $D_{\mathfrak{n}}\delta_{\mathfrak{l}}^{K(\mathfrak{n})} \otimes \sigma_{\mathfrak{l}} = N_{\mathfrak{n}}\delta_{\mathfrak{n}\,\mathfrak{l}} \otimes \sigma_{\mathfrak{l}}$, we have $\phi_{\mathfrak{l}}(\kappa_{\mathfrak{n},\mathfrak{l}}) = -\delta_{\mathfrak{n}\,\mathfrak{l}} \otimes \sigma_{\mathfrak{l}}$ because $N_{\mathfrak{n}}$ is injective. Thus, we get $\phi_{\mathfrak{l}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = -\tilde{\delta}_{\mathfrak{n}\,\mathfrak{l}}$. □

6.2.

The homomorphism $\phi_{\mathfrak{r}} : (K^{\times}/p^N)^{\chi} \longrightarrow O_{\chi}/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{r}}$ induces

$$(K^{\times}/p^N)^{\chi} \otimes \mathcal{G}_{\mathfrak{n}} \longrightarrow O_{\chi}/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{n}} \otimes \mathcal{G}_{\mathfrak{r}},$$

which we also denote by $\phi_{\mathfrak{r}}$. In [12], for completely general $\mathfrak{n}$, Mazur and Rubin computed $\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}})$ for each $\mathfrak{r} \mid \mathfrak{n}$. In this paper, we consider the following special case.

Suppose that $\mathfrak{n} \in \mathcal{N}(K)$. We call $\mathfrak{n}$ *well-ordered* if $\mathfrak{n}$ has factorization $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m$ such that $\mathfrak{r}_{i+1} \in \mathcal{S}(K(\mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_i))$ for all $i = 1, \ldots, m-1$. The next lemma follows from Mazur and Rubin [12, Theorem A4].

LEMMA 6.3 (Mazur and Rubin). *Assume that* $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$ *and that* $\mathfrak{n}$ *is well-ordered. Then, for each* $\mathfrak{r} \mid \mathfrak{n}$, *we have* $\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = 0$.

Proof. Since we are in a special case, this lemma can be proved simply. Suppose that $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m$, that $\mathfrak{r}_{i+1} \in \mathcal{S}(K(\mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_i))$ for all $i = 1, \ldots, m-1$, and that $\mathfrak{r} = \mathfrak{r}_j$ for some j. Put $\mathfrak{m}_1 = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_{j-1}$, and $\mathfrak{m}_2 = \mathfrak{r}_j \cdot \ldots \cdot \mathfrak{r}_m$. We denote $\tilde{\kappa}_{\mathfrak{m}_2,\mathfrak{l}}$ for $K(\mathfrak{m}_1)$ by $\tilde{\kappa}_{\mathfrak{m}_2,\mathfrak{l}}^{K(\mathfrak{m}_1)}$. Since $\phi_{\mathfrak{r}}^{K(\mathfrak{m}_1)}(\tilde{\kappa}_{\mathfrak{m}_2,\mathfrak{l}}^{K(\mathfrak{m}_1)}) = 0$ implies $\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = 0$, to prove Lemma 6.3, we may assume $\mathfrak{r} = \mathfrak{r}_1$.

For a prime v of K above $\mathfrak{r}$, we will prove

$$\phi_{K_v}(\kappa_{\mathfrak{n},\mathfrak{l}}) = 0,$$

where $\phi_{K_v} : K_v^{\times}/p^N \longrightarrow G_{\mathfrak{r}} \otimes \mathbf{Z}/p^N$ is the reciprocity map of K_v. Let $K_v^{\times}/p^N = V_1 \oplus V_2$ be the decomposition in Lemma 3.3. Let v' be the prime of $K(\mathfrak{r})$ above v. Since v is totally ramified in $K(\mathfrak{r})/K$, the natural map $K_v^{\times}/p^N \longrightarrow K(\mathfrak{r})_{v'}^{\times}/p^N$ is injective on V_1. It follows from this fact and $V_2 = \operatorname{Ker}\phi_{K_v}$ that it is enough to show that the image of $\kappa_{\mathfrak{n},\mathfrak{l}}$ in $K(\mathfrak{r})_{v'}^{\times}/p^N$ vanishes, in order to get $\phi_{K_v}(\kappa_{\mathfrak{n},\mathfrak{l}}) = 0$.

We note that the image of $\kappa_{\mathfrak{n},\mathfrak{l}}$ in $K(\mathfrak{r})^{\times}/p^N$ is $D_{\mathfrak{r}}\kappa_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}^{K(\mathfrak{r})}$. Let $U_{K(\mathfrak{r})_{v'}}$ be the unit group of $K(\mathfrak{r})_{v'}$. The image of $D_{\mathfrak{r}}\kappa_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}^{K(\mathfrak{r})}$ in $K(\mathfrak{r})_{v'}^{\times}/p^N$ is in $U_{K(\mathfrak{r})_{v'}}/p^N$. Since $G_{\mathfrak{r}}$ acts on $U_{K(\mathfrak{r})_{v'}}/p^N$ trivially, $D_{\mathfrak{r}}$ acts on $U_{K(\mathfrak{r})_{v'}}/p^N$ as $p^{n_{\mathfrak{r}}}(p^{n_{\mathfrak{r}}}-1)/2 = 0$. Therefore, the image of $D_{\mathfrak{r}}\kappa_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}^{K(\mathfrak{r})}$ in $U_{K(\mathfrak{r})_{v'}}/p^N$ is zero. Thus, we get $\phi_{K_v}(\kappa_{\mathfrak{n},\mathfrak{l}}) = 0$, which implies $\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = 0$. □

Recall that we defined in § 5 $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} \in (K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n}$ for $\mathfrak{n}$ and $\mathfrak{l}$ such that $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$.

PROPOSITION 6.4. *Assume that $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$ and $\mathfrak{n}$ is well-ordered. Then, for each $\mathfrak{r} \mid \mathfrak{n}$, we have $\phi_\mathfrak{r}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = 0$.*

Proof. As we remarked in Remark 5.6, in the definition of $\tilde{\kappa}'_{\mathfrak{n},\mathfrak{l}}$ in § 5.2, using Lemma 5.5, we can take $b \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$ and $\phi_\mathfrak{r}(b) = 0$ in $O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)] \otimes G_\mathfrak{n}$ for all $\mathfrak{r}$ dividing $\mathfrak{n}$. Then

$$\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = \tilde{\kappa}^{(N+\epsilon(\mathfrak{n})c)}_{\mathfrak{n},\mathfrak{l}'} - \tilde{\delta}^{(N+\epsilon(\mathfrak{n})c)}_\mathfrak{n} b \pmod{p^N}.$$

Therefore, by Lemma 6.3 and $\phi_\mathfrak{r}(b) = 0$, we obtain

$$\phi_\mathfrak{r}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = \phi_\mathfrak{r}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'}) - \tilde{\delta}_\mathfrak{n}\phi_\mathfrak{r}(b) = 0. \qquad \square$$

We next consider

$$\phi_\mathfrak{l} : (K^\times/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n} \longrightarrow O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{n}\mathfrak{l}},$$

which is induced by $\phi_\mathfrak{l} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_\mathfrak{l}$.

PROPOSITION 6.5. *Assume that $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})+1]}(K)$ and that $\mathfrak{n}\mathfrak{l}$ is well-ordered. Then we have $\phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = -\tilde{\delta}_{\mathfrak{n}\mathfrak{l}}$.*

The assumption that $\mathfrak{n}\mathfrak{l}$ is well-ordered does not mean $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$, but means that $\mathfrak{n}\mathfrak{l}$ has factorization $\mathfrak{n}\mathfrak{l} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_{m+1}$ satisfying the property in the definition of the well-orderedness in the beginning of § 6.2 (namely, $\mathfrak{l} = \mathfrak{r}_i$ for some i).

Proof of Proposition 6.5. We take $\mathfrak{l}' \in \mathcal{S}_{[\epsilon(\mathfrak{n})+1]}(K(\mathfrak{n}\mathfrak{l})) = \mathcal{S}_{[\epsilon(\mathfrak{n}\mathfrak{l})]}(K(\mathfrak{n}\mathfrak{l}))$ and consider $\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}'}$. As in Remark 5.6, using Lemma 5.5, we can take an auxiliary prime $\mathfrak{l}'' \in \mathcal{S}_{[\epsilon(\mathfrak{n}\mathfrak{l})]}(K(\mathfrak{n}\mathfrak{l}))$ and $b \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b) = (\mathfrak{l}''_K - \mathfrak{l}'_K)^\chi$, $\phi_\mathfrak{r}(b) = 0$ for all $\mathfrak{r}$ dividing $\mathfrak{n}$, and $\phi_\mathfrak{l}(b) = 1 \otimes \sigma_\mathfrak{l}$ which is a generator of $O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_\mathfrak{l}$. We showed in Proposition 5.2 that $\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}'}$ does not depend on the choice of $\mathfrak{l}''$; that is, we have

$$\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}'} = \tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}''} - \tilde{\delta}_{\mathfrak{n}\mathfrak{l}} b - \tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} \otimes \phi_\mathfrak{l}(b).$$

Therefore, using $\phi_\mathfrak{l}(b) = 1 \otimes \sigma_\mathfrak{l}$, we have

$$\phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}'}) = \phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}''}) - \tilde{\delta}_{\mathfrak{n}\mathfrak{l}} \otimes \sigma_\mathfrak{l} - \phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) \otimes \sigma_\mathfrak{l}.$$

On the other hand, Proposition 6.4 tells us that $\phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}'}) = \phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n}\mathfrak{l},\mathfrak{l}''}) = 0$. Hence, we obtain $\phi_\mathfrak{l}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = -\tilde{\delta}_{\mathfrak{n}\mathfrak{l}}$ in $O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{n}\mathfrak{l}}$. $\square$

6.3.

It seems to the author that one can define $\kappa_{\mathfrak{n},\mathfrak{l}}$ and $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ in a more general setting. In this paper, we defined these elements under the assumption $\mathfrak{n}\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$ (cf. § 5.2 and Remark 5.4). This assumption is used to show that $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ is independent of the choice of $\mathfrak{l}'$ and b (cf. Proposition 5.2).

Suppose that $\mathfrak{n}\mathfrak{l} \in \mathcal{N}(K)$. Using Lemma 5.5, we can take $\mathfrak{l}' \in \mathcal{S}(K(\mathfrak{n}))$ and $b \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$ and $\phi_\mathfrak{r}(b) = 0$ for all $\mathfrak{r} \mid \mathfrak{n}$. We write the group law of $(K^\times \otimes \mathbf{Z}/p^N)^\chi \otimes \mathcal{G}_\mathfrak{n}$ additively as before. Can one show that $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'} - \tilde{\delta}_\mathfrak{n} b$ is independent of the choice of $\mathfrak{l}'$, and hence of b (by taking $\mathfrak{l}'$ sufficiently close to $\mathfrak{l}$)? If the answer is yes, then we can define $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ as $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}'} - \tilde{\delta}_\mathfrak{n} b$.

Concerning this question, currently the author can only show Proposition A.1 in Appendix, namely he knows the affirmative answer to this question only in case $\mathfrak{n}$ is a prime.

Another natural question is the following. Suppose that $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ is defined. Can one prove $\phi_{\mathfrak{l}}(\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}) = -\tilde{\delta}_{\mathfrak{n}\,\mathfrak{l}}$? In this paper, we proved this property only for $(\mathfrak{n},\mathfrak{l})$ such that $\mathfrak{l} \in \mathcal{S}(K(\mathfrak{n}))$ (Corollary 6.2), and for $(\mathfrak{n},\mathfrak{l})$ such that $\mathfrak{n}\,\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})+1]}(K)$ and $\mathfrak{n}\,\mathfrak{l}$ is well-ordered (Proposition 6.5).

7. *Elements* $x_{\mathfrak{n},\mathfrak{l}}$

In this section, we define elements $x_{\mathfrak{n},\mathfrak{l}} \in (K^\times \otimes \mathbf{Z}/p^N)^\chi$ and $\tilde{x}_{\mathfrak{n},\mathfrak{l}} \in (K^\times/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}}$ for $\mathfrak{n}\,\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$.

7.1.

We write the group law of $(K^\times/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}}$ additively. We assume that $\mathfrak{n}\,\mathfrak{l} \in \mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$ and $\mathfrak{n}\,\mathfrak{l}$ is well-ordered. Suppose that, for each prime $\mathfrak{r}$ that divides $\mathfrak{n}$, an element $a_{\mathfrak{r}} \in O_\chi/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{r}}$ is given (we shall give $a_{\mathfrak{r}}$ explicitly later in § 10, see the paragraph before Lemma 10.2). For a divisor $\mathfrak{d}$ of $\mathfrak{n}$ we define $a_{\mathfrak{d}}$ by

$$a_{\mathfrak{d}} = \bigotimes\nolimits_{\mathfrak{r}|\mathfrak{d}} a_{\mathfrak{r}} \in O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{d}},$$

where, for $\mathfrak{d} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_{m'}$, we identify $(O_\chi/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{r}_1}) \otimes_{O_\chi/p^N[\Gamma(K/k)]} \cdots \otimes_{O_\chi/p^N[\Gamma(K/k)]} (O_\chi/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{r}_{m'}})$ with $O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{d}}$. We put $a_1 = 1$. We define $\tilde{x}_{\mathfrak{n},\mathfrak{l}}$ by

$$\tilde{x}_{\mathfrak{n},\mathfrak{l}} = \sum_{\mathfrak{d}\,|\,\mathfrak{n}} a_{\mathfrak{d}} \otimes \tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}} \in (K^\times/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}},$$

where $a_{\mathfrak{d}} \otimes \tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}} \in (O_\chi/p^N[\Gamma(K/k)] \otimes \mathcal{G}_{\mathfrak{d}}) \otimes_{O_\chi/p^N[\Gamma(K/k)]} (K^\times/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}/\mathfrak{d}} = (K^\times/p^N)^\chi \otimes \mathcal{G}_{\mathfrak{n}}$, and the sum is taken over all divisors $\mathfrak{d}$ of $\mathfrak{n}$ including 1; namely, $\tilde{x}_{\mathfrak{n},\mathfrak{l}}$ is defined as a sum of $2^{\epsilon(\mathfrak{n})}$ terms.

Proposition 7.1. (0) *If ρ is a prime of K that does not divide $\mathfrak{n}\,\mathfrak{l}$, then it is not in the support of* $\mathrm{div}(\tilde{x}_{\mathfrak{n},\mathfrak{l}})$.

(1) *For each prime $\mathfrak{r}$ dividing $\mathfrak{n}$, we have* $\mathrm{div}_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n},\mathfrak{l}}) = \phi_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$.

(2) *For each prime $\mathfrak{r}$ dividing $\mathfrak{n}$, we have* $\phi_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n},\mathfrak{l}}) = a_{\mathfrak{r}} \otimes \phi_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$.

Proof. The property (0) is an immediate consequence of Proposition 5.2(0).

Concerning (1), using Proposition 5.2(0) and (1), we compute

$$\begin{aligned}
\mathrm{div}_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n},\mathfrak{l}}) &= \sum_{\substack{\mathfrak{d}\,|\,\mathfrak{n}\\ \mathfrak{r}\,|\,\mathfrak{d}}} a_{\mathfrak{d}} \otimes \mathrm{div}_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}}) + \sum_{\substack{\mathfrak{d}\,|\,\mathfrak{n}\\ \mathfrak{r}\nmid\mathfrak{d}}} a_{\mathfrak{d}} \otimes \mathrm{div}_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}}) \\
&= \sum_{\substack{\mathfrak{d}\,|\,\mathfrak{n}\\ \mathfrak{r}\nmid\mathfrak{d}}} a_{\mathfrak{d}} \otimes \phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d}\,\mathfrak{r},\mathfrak{l}}) \\
&= \sum_{\mathfrak{d}\,|\mathfrak{n}/\mathfrak{r}} a_{\mathfrak{d}} \otimes \phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d}\,\mathfrak{r},\mathfrak{l}}) \\
&= \phi_{\mathfrak{r}}\left(\sum_{\mathfrak{d}\,|\mathfrak{n}/\mathfrak{r}} a_{\mathfrak{d}} \otimes \tilde{\kappa}_{\mathfrak{n}/\mathfrak{d}\,\mathfrak{r},\mathfrak{l}}\right) = \phi_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}).
\end{aligned}$$

We next prove (2). Using Proposition 6.4, we have

$$\begin{aligned}\phi_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n},\mathfrak{l}}) &= \sum_{\substack{\mathfrak{d}\mid\mathfrak{n}\\ \mathfrak{r}\mid\mathfrak{d}}} a_{\mathfrak{d}}\otimes\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}}) + \sum_{\substack{\mathfrak{d}\mid\mathfrak{n}\\ \mathfrak{r}\nmid\mathfrak{d}}} a_{\mathfrak{d}}\otimes\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}})\\ &= \sum_{\substack{\mathfrak{d}\mid\mathfrak{n}\\ \mathfrak{r}\mid\mathfrak{d}}} a_{\mathfrak{d}}\otimes\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}})\\ &= a_{\mathfrak{r}}\otimes\left(\sum_{\mathfrak{d}\,|\mathfrak{n}/\mathfrak{r}} a_{\mathfrak{d}}\otimes\phi_{\mathfrak{r}}(\tilde{\kappa}_{\mathfrak{n}/\mathfrak{r}\,\mathfrak{d},\mathfrak{l}})\right)\\ &= a_{\mathfrak{r}}\otimes\phi_{\mathfrak{r}}(\tilde{x}_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}}).\end{aligned}$$

Thus, we get Proposition 7.1. □

Using Lemma 5.5 as in Remark 5.6, we take $\mathfrak{l}'\in\mathcal{S}_{[\epsilon(\mathfrak{n})]}(K(\mathfrak{n}))$ and $b\in(K^\times\otimes\mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b)=(\mathfrak{l}'_K-\mathfrak{l}_K)^\chi$ and $\phi_{\mathfrak{r}}(b)=0$ in $O_\chi/p^{N+\epsilon(\mathfrak{n})c}[\Gamma(K/k)]\otimes G_{\mathfrak{r}}$ for all $\mathfrak{r}$ dividing $\mathfrak{n}$.

Lemma 7.2.

$$\phi_{\mathfrak{l}'}(\tilde{x}_{\mathfrak{n},\mathfrak{l}}) = -\sum_{\mathfrak{d}|\mathfrak{n}} a_{\mathfrak{d}}\otimes(\tilde{\delta}_{(\mathfrak{n}/\mathfrak{d})\,\mathfrak{l}'}+\tilde{\delta}_{\mathfrak{n}/\mathfrak{d}}\otimes\phi_{\mathfrak{l}'}(b)).$$

Proof. As in Remark 5.6, we have $\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}}=\tilde{\kappa}_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}'}-\tilde{\delta}_{\mathfrak{n}/\mathfrak{d}}b$. Therefore, by the definition of $\tilde{x}_{\mathfrak{n},\mathfrak{l}}$ we get $\tilde{x}_{\mathfrak{n},\mathfrak{l}}=\tilde{x}_{\mathfrak{n},\mathfrak{l}'}-(\sum_{\mathfrak{d}|\mathfrak{n}}a_{\mathfrak{d}}\otimes\tilde{\delta}_{\mathfrak{n}/\mathfrak{d}})b$. By Corollary 6.2 we obtain

$$\phi_{\mathfrak{l}'}(\tilde{x}_{\mathfrak{n},\mathfrak{l}}) = -\sum_{\mathfrak{d}|\mathfrak{n}} a_{\mathfrak{d}}\otimes\tilde{\delta}_{(\mathfrak{n}/\mathfrak{d})\,\mathfrak{l}'}-\sum_{\mathfrak{d}|\mathfrak{n}} a_{\mathfrak{d}}\otimes\tilde{\delta}_{\mathfrak{n}/\mathfrak{d}}\otimes\phi_{\mathfrak{l}'}(b),$$

which completes the proof. □

7.2.

Recall that we took a generator $\sigma_{\mathfrak{r}}$ of $G_{\mathfrak{r}}$ for each $\mathfrak{r}\in\mathcal{S}$. We define $x_{\mathfrak{n},\mathfrak{l}}\in(K^\times\otimes\mathbf{Z}/p^N)^\chi$ by

$$\tilde{x}_{\mathfrak{n},\mathfrak{l}} = x_{\mathfrak{n},\mathfrak{l}}\otimes\bigotimes\nolimits_{\mathfrak{r}|\mathfrak{n}}\sigma_{\mathfrak{r}}.$$

For $\mathfrak{l}\in\mathcal{S}(K(\mathfrak{n}))$, $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}$ was defined by $\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}}=\kappa_{\mathfrak{n},\mathfrak{l}}\otimes\bigotimes_{\mathfrak{r}|\mathfrak{n}}\sigma_{\mathfrak{r}}$ in § 4. For any $(\mathfrak{n},\mathfrak{l})$ with $\mathfrak{n}\mathfrak{l}\in\mathcal{N}_{[\epsilon(\mathfrak{n})]}(K)$, we define $\kappa_{\mathfrak{n},\mathfrak{l}}\in(K^\times\otimes\mathbf{Z}/p^N)^\chi$ by

$$\tilde{\kappa}_{\mathfrak{n},\mathfrak{l}} = \kappa_{\mathfrak{n},\mathfrak{l}}\otimes\bigotimes\nolimits_{\mathfrak{r}|\mathfrak{n}}\sigma_{\mathfrak{r}},$$

which is consistent with the definition in the case $\mathfrak{l}\in\mathcal{S}(K(\mathfrak{n}))$. We also use an element $\overline{a}_{\mathfrak{d}}\in O_\chi/p^N[\Gamma(K/k)]$ which is defined by

$$a_{\mathfrak{d}} = \overline{a}_{\mathfrak{d}}\otimes\bigotimes\nolimits_{\mathfrak{r}|\mathfrak{d}}\sigma_{\mathfrak{r}}.$$

Recall that

$$\overline{\phi}_{\mathfrak{r}} : (K^\times/p^N)^\chi\longrightarrow O_\chi/p^N[\Gamma(K/k)]$$

is the homomorphism such that $\phi_{\mathfrak{r}}(x)=\overline{\phi}_{\mathfrak{r}}(x)\otimes\sigma_{\mathfrak{r}}$ for all x.

By Proposition 7.1 and Lemma 7.2, we have the following proposition.

Proposition 7.3. (0) *If ρ is a prime of K that does not divide $\mathfrak{n}\mathfrak{l}$, then it is not in the support of* $\mathrm{div}(x_{\mathfrak{n},\mathfrak{l}})$.

(1) *For each prime* $\mathfrak{r}$ *dividing* $\mathfrak{n}$, *we have* $\mathrm{div}_{\mathfrak{r}}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{r}}(x_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$.
(2) *For each prime* $\mathfrak{r}$ *dividing* $\mathfrak{n}$, *we have* $\overline{\phi}_{\mathfrak{r}}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{a}_{\mathfrak{r}}\overline{\phi}_{\mathfrak{r}}(x_{\mathfrak{n}/\mathfrak{r},\mathfrak{l}})$.
(3) *We take* $\mathfrak{l}'$ *and* b *as before Lemma* 7.2 *. Then we have*

$$\overline{\phi}_{\mathfrak{l}'}(x_{\mathfrak{n},\mathfrak{l}}) = -\sum_{\mathfrak{d}|\mathfrak{n}} \overline{a}_{\mathfrak{d}}(\delta_{(\mathfrak{n}/\mathfrak{d})\,\mathfrak{l}'} + \delta_{\mathfrak{n}/\mathfrak{d}}\overline{\phi}_{\mathfrak{l}'}(b)).$$

8. *Higher Stickelberger ideals*

Let $K, \chi, \ldots$ be as in the previous sections, namely as in § 4.1 (recall that we are fixing an odd character χ of $\Delta(K/k)$). In this section and the next section we do not assume (*) in § 4.1. In this section, we define the ith Stickelberger ideal $\Theta^{\chi}_{i,K} \subset O_{\chi}[\Gamma(K/k)]$ of K for all $i \in \mathbf{Z}_{\geqslant 0}$. More precisely, we define two ideals $\Theta^{(\delta),\chi}_{i,K}$, $\Theta^{\chi}_{i,K}$ such that $\Theta^{(\delta),\chi}_{i,K} \subset \Theta^{\chi}_{i,K}$. In the case where K is a subfield of the cyclotomic $\mathbf{Z}_p$-extensions of K_0 (namely, $K = K_{0,m}$ for some m in the notation of § 2), we will prove that they coincide in § 10. In Remark 8.2, we will see that they do not coincide in general.

8.1.

For $\mathfrak{n} \in \mathcal{N}(K)$ we consider $\delta_{\mathfrak{n}} \in O_{\chi}/p^N[\Gamma(K/k)]$, which is defined in § 4.3 (note that this is defined without the assumption (*) in § 4.1). We note that, by definition, all divisors $\mathfrak{l}$ of $\mathfrak{n} \in \mathcal{N}(K)$ satisfy $n_{\mathfrak{l}} \geqslant N$. To clarify this, we write $\mathcal{N}_N(K)$ for $\mathcal{N}(K)$. For $i \geqslant 0$ we define $\Theta^{(\delta,N),\chi}_{i,K}$ to be the ideal generated by

$$\{\delta_{\mathfrak{n}} \mid \mathfrak{n} \in \mathcal{N}_N(K),\ \epsilon(\mathfrak{n}) \leqslant i\}.$$

We define the small ith Stickelberger ideal $\Theta^{(\delta),\chi}_{i,K}$ by

$$\Theta^{(\delta),\chi}_{i,K} := \varprojlim_N \Theta^{(\delta,N),\chi}_{i,K} \subset \varprojlim_N O_{\chi}/p^N[\Gamma(K/k)] = O_{\chi}[\Gamma(K/k)].$$

In particular, $\Theta^{(\delta),\chi}_{0,K}$ is the principal ideal generated by θ^{χ}_K.

8.2.

We define $\Theta^{\chi}_{i,K}$ by the same method as in [**10**, § 3]. Let s and r be positive integers, and put $s' = \min\{x \in \mathbf{Z} : s < p^x\}$. We consider a ring

$$R = O_{\chi}[\Gamma(K/k)][\![S_1, \ldots, S_r]\!]/((1+S_1)^{p^{n_1}} - 1, \ldots, (1+S_r)^{p^{n_r}} - 1)$$

with $n_1, \ldots, n_r \geqslant N + s' - 1$. Let $f = \Sigma_{i_1,\ldots,i_r \geqslant 0} a_{i_1\ldots i_r} S_1^{i_1} \ldots S_r^{i_r} \bmod \mathcal{I}$ be an element of R where $a_{i_1\ldots i_r} \in O_{\chi}[\Gamma(K/k)]$ and $\mathcal{I} = ((1+S_1)^{p^{n_1}} - 1, \ldots, (1+S_r)^{p^{n_r}} - 1)$. Since $\mathrm{ord}_p(\binom{p^{n_l}}{j}) = \mathrm{ord}_p(p^{n_l}!/(j!(p^{n_l}-j)!)) \geqslant n_l - s' + 1$ for all j with $0 < j < p^{s'}$ $(1 \leqslant l \leqslant r)$, considering the coefficients of the expansion $(1+S_i)^{p^{n_l}} - 1$, we know $a_{i_1,\ldots,i_r} \bmod p^q$ with $q = \min\{n_1, \ldots, n_r\} - s' + 1$ and $i_1, \ldots, i_r \leqslant s$ is well-defined, namely $a_{i_1,\ldots,i_r} \bmod p^q$ is determined by f. Hence, $a_{i_1,\ldots,i_r} \bmod p^N$ is also well-defined. For $i \in \mathbf{Z}_{\geqslant 0}$ and $s \in \mathbf{Z}_{>0}$, we define $I_{i,s}(f)$ to be the ideal of $O_{\chi}/p^N[\Gamma(K/k)]$ generated by

$$\{a_{i_1,\ldots,i_r} \bmod p^N \mid 0 \leqslant i_1, \ldots, i_r \leqslant s \text{ and } i_1 + \ldots + i_r \leqslant i\}.$$

Recall that K_0 is a subfield of K such that $\Gamma(L/k) = \mathrm{Gal}(L/K_0)$ and $\Gamma(K/k) = \mathrm{Gal}(K/K_0)$. We define $\mathcal{F}'$ by

$$\mathcal{F}' = \{L_0 \mid K_0 \subset L_0, L_0/k \text{ is finite and abelian, } L_0/K_0 \text{ is a } p\text{-extension, } L_0 \cap K = K_0,$$
$$\text{and every prime above } p \text{ is unramified in } L_0/K_0\}.$$

For $L_0 \in \mathcal{F}'$ we put $L = L_0K$; then $L \in \mathcal{F}$ where $\mathcal{F}$ is the set we defined in § 4.2. We have a canonical isomorphism

$$\Gamma(L/k) = \mathrm{Gal}(L/K_0) = \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/L_0) \simeq \mathrm{Gal}(L/K) \times \Gamma(K/k).$$

We fix this isomorphism, and identify $O_\chi[\Gamma(L/k)]$ with $O_\chi[\Gamma(K/k)][\mathrm{Gal}(L/K)]$. For $s > 0$ we put

$$\mathcal{F}'_s = \{L_0 \in \mathcal{F}' \mid \mathrm{Gal}(L_0/K_0) \text{ is of the form } \mathrm{Gal}(L_0/K_0) = \mathbf{Z}/p^{n_1}\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/p^{n_r}\mathbf{Z} \text{ with } n_1, \ldots, n_r \geqslant N + s' - 1 \text{ for some } r > 0\} \cup \{K_0\}.$$

For $\mathfrak{n} \in \mathcal{N}(K)(= \mathcal{N}_N(K))$, we have $K_0(\mathfrak{n}) \cap K = K_0$, so $K_0(\mathfrak{n})$ is in $\mathcal{F}'$, and is in $\mathcal{F}'_1$. Suppose that L_0 is in $\mathcal{F}'_s$, $L = L_0K$ and $\mathrm{Gal}(L/K) = \mathrm{Gal}(L_0/K_0) = \mathbf{Z}/p^{n_1}\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/p^{n_r}\mathbf{Z}$. Fixing generators $\sigma_1, \ldots, \sigma_r$ of $\mathrm{Gal}(L/K)$, we have an isomorphism

$$\begin{aligned} O_\chi[\Gamma(L/k)] &= O_\chi[\Gamma(K/k)][\mathrm{Gal}(L/K)] \\ &\simeq O_\chi[\Gamma(K/k)][\![S_1, \ldots, S_r]\!]/((1+S_1)^{p^{n_1}} - 1, \ldots, (1+S_r)^{p^{n_r}} - 1), \end{aligned}$$

where σ_l corresponds to $1 + S_l$ $(1 \leqslant l \leqslant r)$. We regard $\theta^\chi_L \in O_\chi[\Gamma(L/k)]$ (see § 3.4) as an element of the lower right ring, and define $I_{i,s}(\theta^\chi_L) \subset O_\chi/p^N[\Gamma(K/k)]$ as above (we remark that Schoof studied the coefficients of θ^χ_L in the case that $\mathrm{Gal}(L/K)$ is cyclic in [18]). It is easy to check that $I_{i,s}(\theta^\chi_L)$ does not depend on the choice of generators $\sigma_1, \ldots, \sigma_r$ of $\mathrm{Gal}(L/K)$ (see [10, Lemma 3.1]; note that the ideal generated by the coefficients of degree i of θ^χ_L *depends* on the choice of $\sigma_1, \ldots, \sigma_r$, but the ideal $I_{i,s}(\theta^\chi_L)$ *does not*). We also note that this ideal $I_{i,s}(\theta^\chi_L)$ depends on the choice of L_0. We define $\Theta^{(N),\chi}_{i,s,K}$ to be the ideal of $O_\chi/p^N[\Gamma(K/k)]$ generated by

$$\{I_{i,s}(\theta^\chi_L) \text{ where } L = L_0K \mid L_0 \in \mathcal{F}'_s\},$$

and $\Theta^{(N),\chi}_{i,K}$ to be the ideal generated by $\bigcup_{s>0} \Theta^{(N),\chi}_{i,s,K}$. In Theorem 9.11, we prove a relation between $\Theta^{(N),\chi}_{i,K}$ and the Fitting ideals. Finally, we define

$$\Theta^\chi_{i,s,K} := \varprojlim_N \Theta^{(N),\chi}_{i,s,K} \quad \text{and} \quad \Theta^\chi_{i,K} := \varprojlim_N \Theta^{(N),\chi}_{i,K} \subset O_\chi[\Gamma(K/k)].$$

Suppose $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_i \in \mathcal{N}_N(K)$. We consider the isomorphism

$$O_\chi[\Gamma(K(\mathfrak{n})/k)] = O_\chi[\Gamma(K/k)][\![S_1, \ldots, S_i]\!]/((1+S_1)^{p^{n_{\mathfrak{r}_1}}} - 1, \ldots, (1+S_i)^{p^{n_{\mathfrak{r}_i}}} - 1)$$

defined by the correspondence $\sigma_{\mathfrak{r}_l} \leftrightarrow 1 + S_l$. Then, by (4.3)

$$\theta^\chi_{K(\mathfrak{n})} \equiv (-1)^i \delta_{\mathfrak{n}} S_1 \cdot \ldots \cdot S_i \pmod{p^N, S_1^2, \ldots, S_m^2}.$$

Hence, $\delta_{\mathfrak{n}}$ is in $\Theta^{(N),\chi}_{i,1,K}$, and we obtain $\Theta^{(\delta,N),\chi}_{i,K} \subset \Theta^{(N),\chi}_{i,1,K}$. Therefore, we have

$$\Theta^{(\delta),\chi}_{i,K} \subset \Theta^\chi_{i,1,K} \subset \Theta^\chi_{i,K}. \tag{8.1}$$

Remark 8.1. Suppose that L_0 is in $\mathcal{F}'$ and $L = L_0K$. We write I_L for the kernel of the restriction map $O_\chi[\Gamma(L/k)] \longrightarrow O_\chi[\Gamma(K/k)]$. Suppose that $i_{L/K} : O_\chi[\Gamma(K/k)] \longrightarrow O_\chi[\Gamma(L/k)]$ is the natural map induced by the homomorphism $\Gamma(K/k) \longrightarrow \Gamma(K/k) \times \mathrm{Gal}(L/K) = \Gamma(L/k)$. We define the ideal $\tilde{\Theta}^\chi_{i,K}$ to be the minimal ideal in

$$\{J : \text{ ideal of } O_\chi[\Gamma(K/k)] \mid \text{for any } L_0 \in \mathcal{F}', \theta^\chi_L \in i_{L/K}(J)O_\chi[\Gamma(L/k)] + I_L^{i+1} \text{ where } L = L_0K\}.$$

Then we can prove that $\Theta^\chi_{i,K_{0,m}} = \tilde{\Theta}^\chi_{i,K_{0,m}}$ for $K_{0,m}$ satisfying the assumptions of Theorem 2.4 (in fact, we can show that both are equal to the ith Fitting ideal of $A^\chi_{K_{0,m}}$). So we could adopt the above definition of $\tilde{\Theta}^\chi_{i,K}$ as the definition of $\Theta^\chi_{i,K}$. Our definition of $\Theta^\chi_{i,K}$ is more useful for numerical computation.

REMARK 8.2. In general, we have $\Theta_{i,K}^{(\delta),\chi} \neq \Theta_{i,K}^{\chi}$. We will give examples for which $\Theta_{i,K}^{(\delta),\chi} \subsetneq \Theta_{i,1,K}^{\chi} \subset \Theta_{i,K}^{\chi}$. For simplicity, we assume $A_k = 0$, $A_{K_0}^{\chi} = 0$ and $K_0 \cap k(\mu_p) = k$, and $\mathfrak{l}_0 \in \mathcal{S}(K_0)$ is a principal ideal. We consider $K = K_0(\mathfrak{l}_0)$, so K/K_0 is a p-extension such that $\mathrm{Gal}(K/K_0) = G_{\mathfrak{l}_0}$. Then, by genus theory, A_K^{χ} is generated by one element over $O_\chi[\Gamma(K/k)] = O_\chi[G_{\mathfrak{l}_0}]$ and $A_K^{\chi} \neq 0$ (cf. [9, Proposition 5.2]).

Concerning the Stickelberger ideals, we can first show that, for any $\mathfrak{l} \in \mathcal{S}(K)$, $\delta_{\mathfrak{l}}$ is not a unit in $O_\chi/p^N[\Gamma(K/k)] = O_\chi/p^N[G_{\mathfrak{l}_0}]$. In fact, we put $L = K(\mathfrak{l})$, $L_0 = K_0(\mathfrak{l})$ and $S = \sigma_{\mathfrak{l}} - 1 \in O_\chi/p^N[\Gamma(L/k)] = O_\chi/p^N[G_{\mathfrak{l}_0} \times G_{\mathfrak{l}}]$. We know $\theta_L^{\chi} \equiv -\delta_{\mathfrak{l}} S \pmod{p^N, S^2}$ by (4.3). On the other hand, by Lemma 3.4 we have $c_{L/L_0}(\theta_L^{\chi}) = (1 - \varphi_{\mathfrak{l}_0}^{-1})^{\chi} \theta_{L_0}^{\chi}$ where $c_{L/L_0} : O_\chi[\Gamma(L/k)] = O_\chi[G_{\mathfrak{l}_0} \times G_{\mathfrak{l}}] \longrightarrow O_\chi[G_{\mathfrak{l}}] = O_\chi[\Gamma(L_0/k)]$ is the restriction map. Since $\mathfrak{l}_0$ splits completely in K_0, it follows that $\varphi_{\mathfrak{l}_0} = (\mathfrak{l}_0, L_0/k)$ is in $\mathrm{Gal}(L_0/K_0) = G_{\mathfrak{l}}$. We write $\varphi_{\mathfrak{l}_0}^{-1} = \sigma_{\mathfrak{l}}^i$ for some $i \in \mathbf{Z}$ in $\mathrm{Gal}(L_0/K_0) = G_{\mathfrak{l}}$. Combining two equations, we obtain

$$-c_{L/L_0}(\delta_{\mathfrak{l}}) S \equiv (1 - (1+S)^i)\theta_{L_0}^{\chi} \equiv -i\theta_{L_0}^{\chi} S \pmod{p^N, S^2}.$$

Applying [9, Proposition 5.2] (or genus theory) also to L_0, we have $A_{L_0}^{\chi} \neq 0$. By Theorem 9.10 in the next section, $\theta_{L_0}^{\chi}$ is in $\mathrm{Fitt}_{0,O_\chi[G_{\mathfrak{l}}]}(A_{L_0}^{\chi})$. Hence, $\theta_{L_0}^{\chi}$ is not a unit. It follows from the above congruence that $c_{L/L_0}(\delta_{\mathfrak{l}})$ is not a unit, which shows that $\delta_{\mathfrak{l}}$ is not a unit.

Therefore, we have $\Theta_{1,K}^{(\delta),\chi} \subsetneq O_\chi[G_{\mathfrak{l}_0}]$ (namely $\Theta_{1,K}^{(\delta)}$ is too small).

Next, we consider $\Theta_{1,K}^{\chi}$. Suppose $\mathfrak{l}_0 = (x)$ for some $x \in k^\times$. By the Chebotarev density theorem, we can take $\mathfrak{r} \in \mathcal{S}$ such that $\mathfrak{r}$ is inert in $k(\sqrt[p]{x})$ and no prime above $\mathfrak{r}$ splits in K_0/K_0^+. We put $M = K(\mathfrak{r})$, $M_0 = K_0(\mathfrak{r})$, $S = \sigma_{\mathfrak{r}} - 1$, and write $\theta_M^{\chi} \equiv a_0 + a_1 S \pmod{p^N, S^2}$ with $a_0,\ a_1 \in O_\chi/p^N[G_{\mathfrak{l}_0}]$. Then we can check that a_1 is a unit. In fact, since $\mathfrak{r}$ is inert in $k(\sqrt[p]{x})$, $x \bmod \mathfrak{r}$ is not a pth power in the residue field of $\mathfrak{r}$. By the Artin reciprocity law, we know that $(\mathfrak{l}_0, M_0/k)$ is not a pth power in $\mathrm{Gal}(M_0/k)$. In the same way as above, we have $c_{M/M_0}(\theta_M^{\chi}) = (1 - \varphi_{\mathfrak{l}_0}^{-1})^{\chi} \theta_{M_0}^{\chi}$ where $\varphi_{\mathfrak{l}_0} = (\mathfrak{l}_0, M_0/k)$. We write $\varphi_{\mathfrak{l}_0}^{-1} = \sigma_{\mathfrak{r}}^j$ for some j which is prime to p. By the same method as above, we have

$$c_{M/M_0}(a_0 + a_1 S) \equiv -j\theta_{M_0}^{\chi} S \pmod{p^N, S^2}.$$

Since no prime above $\mathfrak{r}$ splits in K_0/K_0^+, we have $A_{M_0}^{\chi} = 0$ (cf. [9, Proposition 5.2]). Again by Theorem 9.10(1), $\theta_{M_0}^{\chi}$ has to be a unit in $O_\chi[G_{\mathfrak{r}}]$ (because $\nu_{1,\mathfrak{r}}(\theta_{K_0}^{\chi})$ is not a unit). Therefore, $c_{M/M_0}(a_0) \equiv 0$ and $c_{M/M_0}(a_1)$ is a unit because both j and $\theta_{M_0}^{\chi}$ are units. Hence, a_1 is a unit.

Since $M_0 \in \mathcal{F}'$, we obtain

$$\Theta_{1,K}^{(\delta),\chi} \subsetneq \Theta_{1,1,K}^{\chi} = \Theta_{1,K}^{\chi} = O_\chi[\Gamma(K/k)].$$

For example, if $k = \mathbf{Q}$, $K_0 = \mathbf{Q}(\sqrt{-6})$, $p = 3$, $N = 1$, $\mathfrak{l}_0 = 7$, $K = K_0(\mathfrak{l}_0) = K_0(\cos(2\pi/7))$, and χ is the non-trivial character of $\mathrm{Gal}(K_0/\mathbf{Q})$, then all the assumptions we made are satisfied. We can take $M_0 = K_0(\mathfrak{r})$ with $\mathfrak{r} = 13 \in \mathcal{S}$, for example. In this case, θ_M^{χ} can be computed as

$$\theta_M^{\chi} = -(4T + 4T^2) - (14 + 22T + 14T^2)S - (8 + 12 + 8T^2)S^2$$

$\bmod\,((1+T)^3 - 1, (1+S)^3 - 1)$ where we took $1 + S = \sigma_{\mathfrak{r}} \in G_{\mathfrak{r}} = (\mathbf{Z}/13\mathbf{Z})^\times \otimes \mathbf{Z}/3\mathbf{Z}$ which corresponds to $2 \otimes 1$, and $1 + T = \sigma_{\mathfrak{l}_0} \in G_{\mathfrak{l}_0} = (\mathbf{Z}/7\mathbf{Z})^\times \otimes \mathbf{Z}/3\mathbf{Z}$ which corresponds to $3 \otimes 1$. In this example, $a_1 = -(14 + 22T + 14T^2)$ is certainly a unit in $O_\chi/p^N[\Gamma(K/k)]$.

9. *Fitting ideals*

In this section, we describe known facts on Fitting ideals.

9.1.

Suppose that R is a commutative ring, and that M is a finitely presented R-module. By definition we have an exact sequence

$$R^m \xrightarrow{f} R^n \longrightarrow M \longrightarrow 0$$

of R-modules where m and n are positive integers. (If $m < n$, then using a projection $R^n \longrightarrow R^m$, we can replace the above sequence by the exact sequence $R^n \longrightarrow R^n \longrightarrow M \longrightarrow 0$, so we may assume $m \geqslant n$.) For an integer $i \geqslant 0$ the ith Fitting ideal of M is defined to be the ideal of R generated by all $(n-i) \times (n-i)$ minors of the matrix A corresponding to f. If $i \geqslant n$, then it is defined to be R. This definition depends only on M and does not depend on the choice of f (cf. Northcott [14, Chapter 3]). The ith Fitting ideal of M over R is denoted by $\mathrm{Fitt}_{i,R}(M)$. We have a sequence of ideals

$$\mathrm{Fitt}_{0,R}(M) \subset \mathrm{Fitt}_{1,R}(M) \subset \ldots \subset \mathrm{Fitt}_{n,R}(M) = \mathrm{Fitt}_{n+1,R}(M) = \ldots = R.$$

The 0th Fitting ideal is called the initial Fitting ideal, and the ideals $\mathrm{Fitt}_{i,R}(M)$ with $i \geqslant 1$ are called higher Fitting ideals.

These ideals give information on the structure of M as an R-module. For example, by definition, if $\mathrm{Fitt}_{r,R}(M) = R$, then M is generated by at most r elements.

9.2.

In this subsection, we suppose that O is a complete discrete valuation ring, and $\Lambda = O[\![T]\!]$. Note that this is a noetherian unique factorial domain (Bourbaki [1, § 4, Chapter 7, Proposition 8]). For finitely generated torsion Λ-modules M_1 and M_2, M_1 is said to be pseudo-isomorphic to M_2 if there is a Λ-homomorphism $M_1 \longrightarrow M_2$ whose kernel and cokernel are both of finite length as O-modules. This is an equivalence relation of finitely generated torsion Λ-modules [22, § 13.2]. We write $M_1 \sim M_2$ in this case. If $M \sim 0$, then M is said to be a pseudo-null module. For any finitely generated torsion Λ-module M, there is a pseudo-isomorphism $M \sim \Lambda/(a_1) \oplus \ldots \oplus \Lambda/(a_r)$ (Bourbaki [1, § 4, Chapter 7, Théorème 5]). In this situation, the characteristic ideal $\mathrm{char}(M)$ is defined by $\mathrm{char}(M) = (a_1 \cdot \ldots \cdot a_r)$.

The following lemma is well known.

LEMMA 9.1. *Suppose that M is a finitely generated torsion Λ-module, and it contains no non-trivial pseudo-null submodule.*

(1) *For any surjective Λ-homomorphism*

$$\varphi : \Lambda^n \longrightarrow M,$$

the kernel of φ is a free Λ-module of rank n.

(2) *The initial Fitting ideal $\mathrm{Fitt}_{0,\Lambda}(M)$ is a principal ideal.*

(3) *The initial Fitting ideal $\mathrm{Fitt}_{0,\Lambda}(M)$ is equal to the characteristic ideal $\mathrm{char}(M)$.*

Proof. (1) This follows from the fact that the projective dimension of M is at most 1 (see, for example, Wingberg [24, Proposition 2.1]).

(2) We have an exact sequence $0 \longrightarrow \Lambda^n \xrightarrow{f} \Lambda^n \longrightarrow M \longrightarrow 0$ by (1). Hence, $\mathrm{Fitt}_{0,\Lambda}(M)$ is a principal ideal generated by $\det A$ where A corresponds to f.

(3) Since $\mathrm{Fitt}_{0,\Lambda}(M)$ is generated by $\det A$, this follows from a well-known property $\mathrm{char}(M) = (\det A)$ (Bourbaki [1, § 4, Chapter 7, Corollaire to Proposition 14]). □

LEMMA 9.2. *Let M be a finitely generated torsion Λ-module such that*

$$M \sim \Lambda/(a_1) \oplus \ldots \oplus \Lambda/(a_r) \quad \text{with } (a_1) \supset (a_2) \supset \ldots \supset (a_r).$$

Then $\mathrm{Fitt}_{i,\Lambda}(M) = (a_1 \cdot \ldots \cdot a_{r-i})I_i$ *for all* i *with* $0 \leqslant i < r$ *where* I_i *is an ideal with* $\mathrm{length}_O \Lambda/I_i < \infty$. *In particular, if we know all* $\mathrm{Fitt}_{i,\Lambda}(M)$, *then we get to know all* a_j $(1 \leqslant j \leqslant r)$, *that is, we get to know the pseudo-isomorphism class of* M.

Proof. In general, if there is an exact sequence $M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ of R-modules, then we have $\mathrm{Fitt}_{i,R}(M_1)\,\mathrm{Fitt}_{0,R}(M_3) \subset \mathrm{Fitt}_{i,R}(M_2)$ by elementary consideration of the matrix corresponding to M_2 (see [14, p. 91]).

Applying this to an exact sequence $M \longrightarrow \Lambda/(a_1) \oplus \ldots \oplus \Lambda/(a_r) \longrightarrow F \longrightarrow 0$ where F is a pseudo-null Λ-module, we have

$$\mathrm{Fitt}_{i,\Lambda}(M)\,\mathrm{Fitt}_{0,\Lambda}(F) \subset \mathrm{Fitt}_{i,\Lambda}(\Lambda/(a_1) \oplus \ldots \oplus \Lambda/(a_r)) = (a_1 \cdot \ldots \cdot a_{r-i}).$$

Put $f_i = a_1 \cdot \ldots \cdot a_{r-i}$. We take an arbitrary $x \in \mathrm{Fitt}_{i,\Lambda}(M)$. Since $\Lambda/\mathrm{Fitt}_{0,\Lambda}(F)$ has finite length as an O-module, we can take y_1, $y_2 \in \mathrm{Fitt}_{0,\Lambda}(F)$ such that y_1 and y_2 are relatively prime. It follows from the above inclusion that f_i divides xy_1 and xy_2, and hence divides x. Therefore, $\mathrm{Fitt}_{i,\Lambda}(M) \subset (f_i)$, and we can write $\mathrm{Fitt}_{i,\Lambda}(M) = f_i I_i$ for some ideal I_i. We also have an exact sequence $\Lambda/(a_1) \oplus \ldots \oplus \Lambda/(a_r) \longrightarrow M \longrightarrow F' \longrightarrow 0$ with $\mathrm{length}_O F' < \infty$, by which we obtain

$$\mathrm{Fitt}_{i,\Lambda}(\Lambda/(a_1) \oplus \ldots \oplus \Lambda/(a_r))\,\mathrm{Fitt}_{0,\Lambda}(F') = f_i\,\mathrm{Fitt}_{0,\Lambda}(F') \subset \mathrm{Fitt}_{i,\Lambda}(M) = f_i I_i.$$

Hence, $\mathrm{Fitt}_{0,\Lambda}(F') \subset I_i$. This shows that Λ/I_i is of finite length as an O-module. □

Concerning the isomorphism class of M, we have the following lemma.

LEMMA 9.3. *Let M be a finitely generated torsion Λ-module such that M is free of rank 2 as an O-module. Then* $\mathrm{Fitt}_{0,\Lambda}(M)$ *and* $\mathrm{Fitt}_{1,\Lambda}(M)$ *determine the isomorphism class of* M.

Proof. This is [9, Lemma 9.1]. □

REMARK 9.4. If M is free of rank r with $r > 2$ as an O-module, then the Fitting ideals $\mathrm{Fitt}_{i,\Lambda}(M)$ do not determine the isomorphism class of M, in general.

For example, consider the Λ-modules M_1, M_2 corresponding to the matrices

$$A_1 = \begin{pmatrix} T^2 & \pi^2 \\ \pi^3 & T \end{pmatrix}, \quad A_2 = \begin{pmatrix} T & \pi^2 \\ \pi^3 & T^2 \end{pmatrix},$$

respectively, where π is a prime element of O. Then both M_1 and M_2 are free of rank 3 as O-modules. Clearly, we get $\mathrm{Fitt}_{0,\Lambda}(M_1) = \mathrm{Fitt}_{0,\Lambda}(M_2) = (T^3 - \pi^5)$, $\mathrm{Fitt}_{1,\Lambda}(M_1) = \mathrm{Fitt}_{1,\Lambda}(M_2) = (T, \pi^2)$, and $\mathrm{Fitt}_{i,\Lambda}(M_1) = \mathrm{Fitt}_{i,\Lambda}(M_2) = \Lambda$ for all $i \geqslant 2$. But M_1 is not isomorphic to M_2. In fact, put $I = (\pi^3, \pi T, T^2) \subset \Lambda$. Then we have $\mathrm{length}_O \Lambda/I = 4$, $\mathrm{length}_O M_1/IM_1 = 4 + 4 - 1 = 7$ and $\mathrm{length}_O M_2/IM_2 = 4 - 2 + 4 = 6$.

LEMMA 9.5. *We assume that $\psi : \Lambda \longrightarrow O_\psi$ is a surjective ring homomorphism such that O_ψ is a discrete valuation ring. For a finitely generated torsion Λ-module M we define $M^\psi = M \otimes_\Lambda O_\psi$ and $J_i^\psi = \psi(\mathrm{Fitt}_{i,\Lambda}(M))$. Then we have an isomorphism*

$$M^\psi \simeq \bigoplus_{i \geqslant 1} J_i^\psi / J_{i-1}^\psi$$

as O_ψ-modules; namely , if we know all $\mathrm{Fitt}_{i,\Lambda}(M)$ for $i \geqslant 0$, then we get to know the isomorphism class of M^ψ for all ψ.

Proof. In fact, by the definition of the Fitting ideals, we have $J_i^\psi = \mathrm{Fitt}_{i,O_\psi}(M^\psi)$. If M^ψ is isomorphic to $O_\psi/(a_1) \oplus \ldots \oplus O_\psi/(a_r)$ such that $(a_1) \supset (a_2) \supset \ldots \supset (a_r)$, then we have $\mathrm{Fitt}_{i,O_\psi}(M^\psi) = (a_1 \cdot \ldots \cdot a_{r-i})$. Therefore, we obtain the isomorphism stated in Lemma 9.5. □

9.3.

Let K, K_0, χ and so on be as before, namely, as in § 4.1 (but we do not assume (*) in § 4.1). *From now on, we also assume that K is in the cyclotomic $\mathbf{Z}_p$-extension $(K_0)_\infty$ of K_0.* We denote by $K_{0,m}$ the intermediate field of $(K_0)_\infty/K_0$ such that $[K_{0,m} : K_0] = p^m$. Our assumption means $K = K_{0,m}$ for some $m \geqslant 0$. By definition, $K_\infty = (K_0)_\infty$. We study $X_{K_\infty}^\chi = \varprojlim A_{K_n}^\chi$. Recall that we assumed $\mu(X_{K_\infty}^\chi) = 0$ in § 4.1. Put $\Lambda = O_\chi[\![\Gamma(K_\infty/k)]\!] = O_\chi[\![\mathrm{Gal}(K_\infty/K_0)]\!]$ which is isomorphic to the formal power series ring $O_\chi[\![T]\!]$, and we can apply the results in the previous subsection.

By Lemma 3.4, the elements $\theta_{K_n}^\chi$ ($\in O_\chi[\mathrm{Gal}(K_n/K_0)]$) for $n \gg 0$ become a projective system and we define $\theta_{K_\infty}^\chi \in O_\chi[\![\mathrm{Gal}(K_\infty/K_0)]\!] = \Lambda$ as their projective limit, which is the p-adic L-function of Deligne and Ribet. Since $X_{K_\infty}^\chi$ does not have a non-trivial finite Λ-submodule [**22**, Proposition 13.28], by the main conjecture proved by Wiles [**23**] and Lemma 9.1(3), we know the following theorem.

THEOREM 9.6 (Wiles [**23**]). *We have* $\mathrm{Fitt}_{0,\Lambda}(X_{K_\infty}^\chi) = (\theta_{K_\infty}^\chi)$.

For any $\mathfrak{n} \in \mathcal{N}$ we put $K(\mathfrak{n}) = Kk(\mathfrak{n})$ and consider the cyclotomic $\mathbf{Z}_p$-extension $K(\mathfrak{n})_\infty$ of $K(\mathfrak{n})$. The element $\theta_{K(\mathfrak{n})_\infty}^\chi \in O_\chi[\![\mathrm{Gal}(K(\mathfrak{n})_\infty/K_0)]\!] = \Lambda[G_\mathfrak{n}]$ is defined by the same method as above. For $\mathfrak{d} \in \mathcal{N}$ dividing $\mathfrak{n}$, we define the norm map

$$\nu_{\mathfrak{d},\mathfrak{n}} : \Lambda[G_\mathfrak{d}] \longrightarrow \Lambda[G_\mathfrak{n}]$$

by $\Sigma_{\sigma \in G_\mathfrak{d}} a_\sigma \sigma \mapsto \Sigma_{\sigma \in G_\mathfrak{d}} a_\sigma \tau'$ where $\tau' = \Sigma_{\tau_{|K(\mathfrak{d})_\infty} = \sigma} \tau$ (the sum is taken over all $\tau \in G_\mathfrak{n}$ whose restriction to $K(\mathfrak{d})_\infty$ is σ). Since $K_0(\mathfrak{n})$ satisfies the condition (A_p) in [**9**], we have the following.

THEOREM 9.7 [**9**, Theorem 0.9]. *We have*

$$\mathrm{Fitt}_{0,\Lambda[G_\mathfrak{n}]}(X_{K(\mathfrak{n})_\infty}^\chi) = (\{\nu_{\mathfrak{d},\mathfrak{n}}(\theta_{K(\mathfrak{d})_\infty}^\chi) \mid \mathfrak{d} \in \mathcal{N},\ \mathfrak{d} \text{ divides } \mathfrak{n}\}),$$

where the right-hand side is the ideal of $\Lambda[G_\mathfrak{n}]$ generated by all $\nu_{\mathfrak{d},\mathfrak{n}}(\theta_{K(\mathfrak{d})_\infty}^\chi)$.

We note that the Leopoldt conjecture is not needed in the proof of the above theorem because of $\chi \neq \omega$ (cf. [**9**, Remark 0.11(1)]). We also note that $\mathrm{Fitt}_{0,\Lambda}(X_{K_\infty}^\chi)$ is a principal ideal, but $\mathrm{Fitt}_{0,\Lambda[G_\mathfrak{n}]}(X_{K(\mathfrak{n})_\infty}^\chi)$ is not principal, in general.

In [**4**], Greither generalized the above theorem, and determined the initial Fitting ideal for more general cyclotomic $\mathbf{Z}_p$-extensions. By Greither [**4**, Theorem 7(i)], $\mathrm{Fitt}_{0,\Lambda}(X_{L_\infty}^\chi)$ is determined for $L = L_0K$ with $L_0 \in \mathcal{F}'$ (which was defined in § 8.2).

In particular, we have the following theorem.

THEOREM 9.8 (Greither [**4**, Theorem 7 (i)]). *For any $L = L_0K$ with $L_0 \in \mathcal{F}'$, we have*

$$\theta_{L_\infty}^\chi \in \mathrm{Fitt}_{0,\Lambda[\mathrm{Gal}(L/K)]}(X_{L_\infty}^\chi).$$

Recall that L in the above theorem satisfies the condition that *all primes of K_∞ above p are unramified in L_∞*. If we remove this assumption on the unramifiedness, then there exist counterexamples of the above property [**5**, Theorem 1.1].

9.4.

We next study A_K^χ and A_L^χ for $L \in \mathcal{F}$.

LEMMA 9.9. *The norm map induces an isomorphism*

$$(X_{L_\infty}^\chi)_{\mathrm{Gal}(L_\infty/L)} \xrightarrow{\simeq} A_L^\chi,$$

for any $L \in \mathcal{F}$.

Proof. In fact, by our assumption that $\chi(\mathfrak{p}) \neq 1$ for all primes $\mathfrak{p}$ of k above p, we have $(\bigoplus_{v|p} \mathbf{Z}_p)^\chi = 0$ where v ranges over primes of K_0 above p. Hence, we also have $(\bigoplus_{w|p} \mathbf{Z}_p)^\chi = 0$ where w ranges over primes of L above p, and $(\bigoplus_{w|p} I_w(L_\infty/L))^\chi = 0$ where $I_w(L_\infty/L)$ is the inertia group of w in $\mathrm{Gal}(L_\infty/L)$. Therefore, we obtain the above isomorphism (cf. [**9**, Proposition 5.2]). □

Suppose $L \in \mathcal{F}$. For a prime $\mathfrak{p}$ of k above p, by our assumption $\chi(\mathfrak{p}) \neq 1$, $1 - \chi(\mathfrak{p})^{-1}$ is a unit of O_χ. Hence, if $\mathfrak{p}$ is unramified in L, then $(1 - \varphi_\mathfrak{p}^{-1})^\chi$ is a unit of $O_\chi[\Gamma(L/k)]$ where $\varphi_\mathfrak{p}$ is the Frobenius of $\mathfrak{p}$ in $\mathrm{Gal}(L/k)$. Therefore, by Lemma 3.4, we have

$$c_{L_\infty/L}(\theta_{L_\infty}^\chi) = u\theta_L^\chi,$$

for some $u \in O_\chi[\Gamma(L/k)]^\times$.

Put $R_K = O_\chi[\Gamma(K/k)]$. For $\mathfrak{n}, \mathfrak{d} \in \mathcal{N}$ with $\mathfrak{d} \mid \mathfrak{n}$, we define the norm map $\nu_{\mathfrak{d},\mathfrak{n}} : R_K[G_\mathfrak{d}] \longrightarrow R_K[G_\mathfrak{n}]$ by the same method as above, and consider $\nu_{\mathfrak{d},\mathfrak{n}}(\theta_{K(\mathfrak{d})}^\chi) \in R_K[G_\mathfrak{n}] = O_\chi[\Gamma(K(\mathfrak{n})/k)]$.

In general, for any ideal I of R and an R-module M, by the definition of the Fitting ideals,

$$\mathrm{Fitt}_{i,R/I}(M/IM) = \mathrm{Fitt}_{i,R}(M) \bmod I \subset R/I$$

holds. Therefore, using Theorems 9.7, 9.8 and Lemma 9.9, we obtain the following theorem.

THEOREM 9.10. (1) *For any $\mathfrak{n} \in \mathcal{N}$, we have*

$$\mathrm{Fitt}_{0,R_K[G_\mathfrak{n}]}(A_{K(\mathfrak{n})}^\chi) = (\{\nu_{\mathfrak{d},\mathfrak{n}}(\theta_{K(\mathfrak{d})}^\chi) \mid \mathfrak{d} \in \mathcal{N},\ \mathfrak{d} \text{ divides } \mathfrak{n}\}),$$

where the right-hand side is the ideal of $R_K[G_\mathfrak{n}] = O_\chi[\Gamma(K(\mathfrak{n})/k)]$ generated by all $\nu_{\mathfrak{d},\mathfrak{n}}(\theta_{K(\mathfrak{d})}^\chi)$.

(2) *For any $L = L_0K$ with $L_0 \in \mathcal{F}'$, we have $\theta_L^\chi \in \mathrm{Fitt}_{0,R_K[\mathrm{Gal}(L/K)]}(A_L^\chi)$.*

9.5.

Let K be as above. We defined $\Theta_{i,K}^\chi$ in § 8.2. In this subsection, we prove the following theorem.

THEOREM 9.11 (cf. [**9**, Theorem 8.1]). *For any $i \geqslant 0$ we have*

$$\Theta_{i,K}^{(N),\chi} \subset \mathrm{Fitt}_{i,R_K/p^N}(A_K^\chi/p^N) \quad \textit{and} \quad \Theta_{i,K}^\chi \subset \mathrm{Fitt}_{i,R_K}(A_K^\chi).$$

Proof. This is essentially [**9**, Theorem 8.1]. Suppose that $L = L_0K$ with $L_0 \in \mathcal{F}_s'$ for some $s > 0$, and $\mathrm{Gal}(L/K) = \mathbf{Z}/p^{n_1}\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/p^{n_r}\mathbf{Z}$ for some $r > 0$. Put $G = \mathrm{Gal}(L/K)$. We take

generators $\sigma_1, \dots, \sigma_r$ of G, and identify $O_\chi[\Gamma(L/k)] = R_K[G]$ with

$$R_K[\![S_1, \dots, S_r]\!]/((1+S_1)^{p^{n_1}} - 1, \dots, (1+S_r)^{p^{n_r}} - 1)$$

by $\sigma_l \leftrightarrow 1 + S_l$ $(1 \leqslant l \leqslant r)$. By the definition of $\mathcal{F}'_s$ and the consideration in § 8.2, we have an isomorphism

$$R_K/p^N[G]/(S_1^{s+1}, \dots, S_r^{s+1}) \simeq R_K/p^N[\![S_1, \dots, S_r]\!]/(S_1^{s+1}, \dots, S_r^{s+1}).$$

We regard A_K^χ as an $R_K[G]$-module, on which G acts trivially. Let $R_K^m \xrightarrow{g} R_K^n \longrightarrow A_K^\chi \longrightarrow 0$ be an exact sequence of R_K-modules, and B be the matrix with m columns and n rows corresponding to g. We have an exact sequence $R_K[G]^{m+rn} \xrightarrow{g'} R_K[G]^n \longrightarrow A_K^\chi \longrightarrow 0$ of $R_K[G]$-modules where g' corresponds to the matrix

$$\begin{pmatrix} S_1 & \cdots & S_r & \cdots & \cdots & 0 & \cdots & 0 & \\ 0 & \cdots & 0 & \cdots & \cdots & 0 & \cdots & 0 & \\ \vdots & \cdots & \vdots & \cdots & \cdots & \vdots & \cdots & \vdots & B \\ \vdots & \cdots & \vdots & \cdots & \cdots & \vdots & \cdots & \vdots & \\ 0 & \cdots & 0 & \cdots & \cdots & S_1 & \cdots & S_r & \end{pmatrix}.$$

Then we know from the above matrix that

$$\mathrm{Fitt}_{0,R_K[G]}(A_K^\chi) = \sum_{i=0}^{n} \mathrm{Fitt}_{i,R_K}(A_K^\chi)(S_1, \dots, S_r)^i.$$

Since we have a surjective homomorphism $A_L^\chi \longrightarrow A_K^\chi$ of $R_K[G]$-modules [**9**, Lemma 5.1(1)], we have

$$\mathrm{Fitt}_{0,R_K[G]}(A_L^\chi) \subset \sum_{i=0}^{n} \mathrm{Fitt}_{i,R_K}(A_K^\chi)(S_1, \dots, S_r)^i.$$

This implies

$$\mathrm{Fitt}_{0,R_K[G]}(A_L^\chi) \bmod (p^N, S_1^{s+1}, \dots, S_r^{s+1}) \subset \sum_{i=0}^{n} \mathrm{Fitt}_{i,R_K/p^N}(A_K^\chi/p^N)(S_1, \dots, S_r)^i$$

in $R_K/p^N[\![S_1, \dots, S_r]\!]/(S_1^{s+1}, \dots, S_r^{s+1})$. By Theorem 9.10(2), we have $\theta_L^\chi \in \mathrm{Fitt}_{0,R_K[G]}(A_L^\chi)$, hence we obtain $I_{i,s}(\theta_L^\chi) \subset \mathrm{Fitt}_{i,R_K/p^N}(A_K^\chi/p^N)$. Thus, we have

$$\Theta_{i,K}^{(N),\chi} \subset \mathrm{Fitt}_{i,R_K/p^N}(A_K^\chi/p^N).$$

Since

$$\mathrm{Fitt}_{i,R_K}(A_K^\chi) = \varprojlim_N \mathrm{Fitt}_{i,R_K/p^N}(A_K^\chi/p^N),$$

from the definition of $\Theta_{i,K}^\chi$ we obtain the conclusion $\Theta_{i,K}^\chi \subset \mathrm{Fitt}_{i,R_K}(A_K^\chi)$. □

We define the Stickelberger ideals over K_∞ by

$$\Theta_{i,K_\infty}^{(\delta),\chi} = \varprojlim \Theta_{i,K_m}^{(\delta),\chi} \quad \text{and} \quad \Theta_{i,K_\infty}^{\chi} = \varprojlim \Theta_{i,K_m}^{\chi}.$$

From the inclusion $\Theta_{i,K_m}^{(\delta),\chi} \subset \Theta_{i,K_m}^\chi$, we know $\Theta_{i,K_\infty}^{(\delta),\chi} \subset \Theta_{i,K_\infty}^\chi \subset \Lambda$.

Corollary 9.12. *For any $i \geqslant 0$ we have*

$$\Theta_{i,K_\infty}^{(\delta),\chi} \subset \Theta_{i,K_\infty}^\chi \subset \mathrm{Fitt}_{i,\Lambda}(X_{K_\infty}^\chi).$$

Proof. Suppose that $0 \longrightarrow \Lambda^n \xrightarrow{f} \Lambda^n \longrightarrow X_{K_\infty}^{\chi} \longrightarrow 0$ is exact and that γ_m is a generator of $\mathrm{Gal}(K_\infty/K_m)$. Then, by Lemma 9.9, $f \bmod \gamma_m - 1$ yields an exact sequence $O_\chi[\Gamma(K_m/k)]^n \xrightarrow{f \bmod \gamma_m - 1} O_\chi[\Gamma(K_m/k)]^n \longrightarrow A_{K_m}^{\chi} \longrightarrow 0$. Hence, we have

$$\mathrm{Fitt}_{i,\Lambda}(X_{K_\infty}^{\chi}) = \varprojlim \mathrm{Fitt}_{i,O_\chi[\Gamma(K_n/k)]}(A_{K_n}^{\chi}).$$

Therefore, Theorem 9.11 implies Corollary 9.12. □

Concerning the commutativity of projective limits with Fitting ideals in a more general setting, see [**5**, Theorem 2.1].

10. *Proof of the main theorem*

In this section, we prove Theorem 2.1. In order to get the equality of two ideals, since we saw in the previous section that one inclusion holds (Corollary 9.12), we have to prove the other inclusion. Using $x_{\mathfrak{n},\mathfrak{l}}$ in § 7, we shall construct elements in the multiplicative group which give relations approximating submatrices of a relation matrix of $X_{K_\infty}^{\chi}$. The properties of Kolyvagin systems ((iii) and (iv) in § 1; more directly Proposition 7.3) play an important role (see Lemma 10.2 which is a key lemma).

10.1.

For each $\mathfrak{l} \in \mathcal{S}$, using the prime $\mathfrak{l}_{\overline{k}}$ we fixed, we regard $\mu_{p^n} \subset \overline{k}^\times$ as a subgroup of $\overline{k}_\mathfrak{l}^\times$ for all $n > 0$, where $\overline{k}_\mathfrak{l}$ is an algebraic closure of $k_\mathfrak{l}$. We fix a generator $\zeta_{p^n} \in \mu_{p^n}$ for all $n > 0$ such that $(\zeta_{p^{n+1}})^p = \zeta_{p^n}$. For each $\mathfrak{l} \in \mathcal{S}$ we take $\sigma_\mathfrak{l} \in G_\mathfrak{l}$ to be the element such that $\mathrm{Kum}(\sigma_\mathfrak{l}) = \zeta_{p^{n_\mathfrak{l}}}$ where Kum is the map defined in § 3.3.

We combine Rubin [**15**, Theorem 3.1] with Lemma 5.5 to get the following lemma.

LEMMA 10.1. *Assume $\mathfrak{n} = \mathfrak{r}_1 \cdot \ldots \cdot \mathfrak{r}_m \in \mathcal{N}(K)$ and that $\mathfrak{l} \in \mathcal{S}(K)$ is prime to $\mathfrak{n}$. Suppose that one is given $\sigma_i \in O_\chi/p^N[\Gamma(K/k)] \otimes G_{\mathfrak{r}_i}$ for each $i = 1, \ldots, m$, a finite $\mathrm{Gal}(K/k)$-submodule W of $(K^\times/p^N)^\chi$ and a $\mathrm{Gal}(K/k)$-equivariant homomorphism*

$$\lambda : W \longrightarrow O_\chi/p^N[\Gamma(K/k)].$$

Then there are infinitely many $\mathfrak{l}' \in \mathcal{S}(K(\mathfrak{n}))$ which satisfy the following properties.

(i) *The class $[\mathfrak{l}'_K]^\chi$ in A_K^χ coincides with the class $[\mathfrak{l}_K]^\chi$.*

(ii) *For the element $z \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(z) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$, $\phi_{\mathfrak{r}_i}(z) = \sigma_i$ holds for each $i = 1, \ldots, m$.*

(iii) *The submodule W is in the kernel of $\mathrm{div}_{\mathfrak{l}'} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)]$, and we have $\lambda(x) = \overline{\phi}_{\mathfrak{l}'}(x)$ for all $x \in W$.*

Proof. We follow the argument of the proof of Rubin [**15**, Theorem 3.1], and our proof is a modification of Rubin [**15**, Theorem 3.1]. So the reader who is not familiar with this kind of proof should consult the proof of Rubin [**15**, Theorem 3.1]. Put $G = \mathrm{Gal}(K/k)$. We define $\iota : \mathbf{Z}/p^N[G] \longrightarrow \mathbf{Z}/p^N$ by $a_1 1_G + \sum_{g \neq 1} a_g g \mapsto a_1$. Then $f \mapsto \iota \circ f$ defines an isomorphism

$$\mathcal{I} : \mathrm{Hom}_{\mathbf{Z}/p^N[G]}(M, \mathbf{Z}/p^N[G]) \xrightarrow{\simeq} \mathrm{Hom}(M, \mathbf{Z}/p^N),$$

for any $\mathbf{Z}/p^N[G]$-module M. In fact, $f \mapsto (x \mapsto \Sigma_{\sigma \in G} f(\sigma x)\sigma^{-1})$ gives the inverse of $\mathcal{I}$. Let ζ_{p^N} be the primitive p^Nth root of unity we fixed. We regard W as a $\mathbf{Z}/p^N[G]$-module, $O_\chi/p^N[\Gamma(K/k)]$ as a direct summand of $\mathbf{Z}/p^N[G]$ and λ as a map from W to $\mathbf{Z}/p^N[G]$. We define $\lambda' : W \longrightarrow \mu_{p^N}$ by $\lambda'(x) = \zeta_{p^N}^{-(\iota \circ \lambda)(x)}$.

Consider the Kummer pairing

$$\mathrm{Gal}(K(\mu_{p^N}, W^{1/p^N})/K(\mu_{p^N})) \times W \longrightarrow \mu_{p^N},$$

which is non-degenerate because of the injectivity of $(K^\times/p^N)^\chi \longrightarrow (K(\mu_{p^N})^\times/p^N)^\chi$. (Here, we regard χ as a character of $\Delta(K(\mu_{p^N})/k)$ using the natural restriction $\Delta(K(\mu_{p^N})/k) \longrightarrow \Delta(K/k)$.) Using this pairing, we regard λ' as an element of $\mathrm{Gal}(K(\mu_{p^N}, W^{1/p^N})/K(\mu_{p^N}))$.

Let $K\{\mathfrak{n}\}^\chi$ be as in the proof of Lemma 5.5, and let $\mathcal{U}$ and $k(\mu_{p^{n+1}}, \mathcal{U}^{1/p^n})$ be as in the proof of Lemma 3.1. We consider the compositum

$$L' = K\{\mathfrak{n}\}^\chi K(\mathfrak{n})(\mu_{p^{n+1}}, \mathcal{U}^{1/p^n}, W^{1/p^N}).$$

The Galois group $\mathrm{Gal}(K_0(\mu_p)/k)$ acts on $\mathrm{Gal}(K\{\mathfrak{n}\}^\chi/K)$ via χ, acts on $\mathrm{Gal}(K(\mathfrak{n})(\mu_{p^{n+1}})/K)$ via the trivial character, acts on $\mathrm{Gal}(K(\mu_{p^n}, \mathcal{U}^{1/p^n})/K(\mu_{p^n}))$ via ω and acts on $\mathrm{Gal}(K(\mu_{p^N}, W^{1/p^N})/K(\mu_{p^N}))$ via $\chi^{-1}\omega$. Hence $K\{\mathfrak{n}\}^\chi(\mu_{p^n})$, $K(\mathfrak{n})(\mu_{p^n})$, $K(\mu_{p^{n+1}})$, $K(\mu_{p^n}, \mathcal{U}^{1/p^n})$ and $K(\mu_{p^n}, W^{1/p^N})$ are all linearly disjoint over $K(\mu_{p^n})$. Hence, as in the proof of Lemma 5.5, we can apply the Chebotarev density theorem to L', and obtain infinitely many $\mathfrak{l}' \in \mathcal{S}(K(\mathfrak{n}))$ having the properties (i), (ii) and $(\mathfrak{l}'_{K(\mu_{p^n})}, K(\mu_{p^n}, W^{1/p^N})/K(\mu_{p^n})) = \lambda'$.

Since $\mathfrak{l}'$ is unramified in $K(\mu_{p^n}, W^{1/p^N})$, W is in the kernel of $\mathrm{div}_{\mathfrak{l}'} : (K^\times/p^N)^\chi \longrightarrow O_\chi/p^N[\Gamma(K/k)]$. We write $\varphi_{\mathfrak{l}'} = (\mathfrak{l}'_{K(\mu_{p^n})}, K(\mu_{p^n}, W^{1/p^N})/K(\mu_{p^n}))$. For any $x \in W$ we have

$$\zeta_{p^N}^{-(\iota\circ\lambda)(x)} = \lambda'(x) = \frac{\varphi_{\mathfrak{l}'}(\sqrt[p^N]{x})}{\sqrt[p^N]{x}} \equiv \frac{(\sqrt[p^N]{x})^{N(\mathfrak{l}')}}{\sqrt[p^N]{x}} = x^{(N(\mathfrak{l}')-1)/p^N},$$

where the congruence is mod $\mathfrak{l}'_{K(\mu_{p^n})}$. Let $\phi_{K_{\mathfrak{l}'_K}} : K^\times_{\mathfrak{l}'_K} \longrightarrow G_{\mathfrak{l}'} \otimes \mathbf{Z}/p^N$ be the reciprocity map, and $\mathrm{Kum}_{(N)}$ be the map defined in the proof of Lemma 3.2. Then, by (3.1), we have

$$(\mathrm{Kum}_{(N)} \circ \phi_{K_{\mathfrak{l}'_K}}(x)) \equiv x^{-(N(\mathfrak{l}')-1)/p^N} \equiv \zeta_{p^N}^{(\iota\circ\lambda)(x)} \pmod{\mathfrak{l}'_{K(\mu_{p^n})}}.$$

Since $\mathrm{Kum}_{(N)}(\sigma_{\mathfrak{l}'}) = \zeta_{p^N}$, we have

$$\phi_{K_{\mathfrak{l}'_K}}(x) = \sigma_{\mathfrak{l}'}^{(\iota\circ\lambda)(x)} = (\iota \circ \lambda)(x) \otimes \sigma_{\mathfrak{l}'}.$$

Since $(\iota \circ \overline{\phi}_{\mathfrak{l}'})(x) \otimes \sigma_{\mathfrak{l}'} = \phi_{K_{\mathfrak{l}'_K}}(x)$ and $\mathcal{I} : f \mapsto \iota \circ f$ is an isomorphism, it follows that

$$\overline{\phi}_{\mathfrak{l}'}(x) = \lambda(x).$$

This completes the proof of Lemma 10.1. □

10.2.

In this subsection, we prove Theorem 2.1.

Step 1. *Preliminary argument on a minor of a relation matrix of* $X^\chi_{K_\infty}$

By Lemma 9.1(1) there is an exact sequence

$$0 \longrightarrow \Lambda^n \xrightarrow{f} \Lambda^n \xrightarrow{g} X^\chi_{K_\infty} \longrightarrow 0. \tag{10.1}$$

Let A be the matrix corresponding to f. Consider the matrix A_i which is obtained from A by eliminating the n_1th row,..., the n_ith row and the m_1th column,..., the m_ith column (A_i is an $(n-i) \times (n-i)$ matrix). Our aim is to prove that $\det A_i$ is in $\Theta^{(\delta),\chi}_{i,K_\infty}$.

We put $A_0 = A$. By the main conjecture proved by Wiles (Theorem 9.6), we know $(\det A_0) = (\theta^\chi_{K_\infty})$. Thus, for $i = 0$, $\Theta^{(\delta),\chi}_{0,K_\infty} = (\det A_0)$ holds. In order to make our argument simple, we take the above exact sequence (10.1) such that $\det A_0 = \theta^\chi_{K_\infty}$. We also note that $\det A_0 \neq 0$. Suppose $i \geqslant 1$ in the following. We will prove $\det A_i \in \Theta^{(\delta),\chi}_{i,K_\infty}$ by induction on i. First of all, since $0 \in \Theta^\chi_{i,K_\infty}$ is clear, we may assume $\det A_i \neq 0$. Furthermore, by changing the order of

$m_1, \dots, m_i$ if it is needed, we may assume $\det A_r \neq 0$ for all r such that $0 \leqslant r \leqslant i$. In fact, let B be the $(n-i+1) \times n$ matrix obtained from A by eliminating the n_1th row,..., and the n_{i-1}th row. For l such that $1 \leqslant l \leqslant i$, we denote by B_l the matrix obtained from B by eliminating the m_jth columns for all j such that $1 \leqslant j \leqslant i$ and $j \neq l$. If $\det B_l = 0$ for all l $(1 \leqslant l \leqslant i)$, then the rank of B_l is equal to the rank of A_i which is $n-i$, so $\operatorname{rank} B = n-i$. This shows that $\operatorname{rank} A \leqslant n-i+i-1 = n-1$, which implies $\det A = 0$, and we get a contradiction. Therefore, one of $\det B_l$ is non-zero. Replacing m_i with m_l, we get $\det A_{i-1} = \det B_l \neq 0$. Proceeding in this way, we can take A_r such that $\det A_r \neq 0$ for all r such that $0 \leqslant r \leqslant i$.

Step 2. *Definition of a homomorphism* β_r

Taking m sufficiently large, we may assume that all primes of k above p are ramified in $K_{0,m}$, and all primes of $K_{0,m}$ above p are totally ramified in K_∞. We take positive integers N_m such that $N_m \to \infty$ as $m \to \infty$. To simplify the notation, we put $K = K_{0,m}$, $N = N_m$. Note that K satisfies the conditions of § 4.1 including (*), and we apply the results in §§ 2–9 for K and N.

Put $R_K = O_\chi[\Gamma(K/k)] = O_\chi[\mathrm{Gal}(K/K_0)]$, and denote by γ_m a generator of $\mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(K_\infty/K_{0,m})$. Since $(X^\chi_{K_\infty})_{\mathrm{Gal}(K_\infty/K)} \simeq A^\chi_K$ is bijective by Lemma 9.9, it is finite. Therefore, $\gamma_m - 1$ is prime to $\mathrm{char}(X^\chi_{K_\infty})$, and $\mathrm{Gal}(K_\infty/K)$-invariant $(X^\chi_{K_\infty})^{\mathrm{Gal}(K_\infty/K)}$ vanishes. Hence, taking $\mathrm{Gal}(K_\infty/K)$-coinvariants of the exact sequence (10.1), by Lemma 9.9 we obtain an exact sequence

$$0 \longrightarrow R_K^n \xrightarrow{\overline{f}} R_K^n \xrightarrow{\overline{g}} A_K^\chi \longrightarrow 0, \tag{10.2}$$

where $\overline{f}$ corresponds to the matrix $A \bmod \gamma_m - 1$.

Let $(\mathbf{e}_r)_{1 \leqslant r \leqslant n}$ be the standard basis of Λ^n in the exact sequence (10.1), and define $\mathbf{c}_1 = g(\mathbf{e}_1), \dots, \mathbf{c}_n = g(\mathbf{e}_n)$ which are generators of $X^\chi_{K_\infty}$ as a Λ-module. We denote by $\mathbf{c}_r^{(m)}$ the image of $\mathbf{c}_r$ in A^χ_K. The image of $\mathbf{e}_r$ in R^n_K will be denoted by the same notation $\mathbf{e}_r$. Hence, we have $\overline{g}(\mathbf{e}_r) = \mathbf{c}_r^{(m)} \in A^\chi_K$ for all r. Recall that we defined the set $\mathcal{S}_{[i-1]}(K)$ in § 5.2. We define

$$Q_r = \{\mathfrak{l} \in \mathcal{S}_{[i-1]}(K) \mid [\mathfrak{l}_K]^\chi = \mathbf{c}_r^{(m)}\},$$

for each r where $[\mathfrak{l}_K]^\chi$ is the class of $\mathfrak{l}_K$ in A^χ_K. By the Chebotarev density theorem, Q_r is an infinite set. We define $Q = \bigcup_{1 \leqslant r \leqslant n} Q_r$. Let Q_K be the set of primes of K above Q, and $\mathcal{D} = \bigoplus_{\rho \in Q_K} \mathbf{Z} \cdot \rho$ be the subgroup of Div_K consisting of all divisors whose supports are in Q_K. We have a natural surjective homomorphism

$$\alpha : (\mathcal{D} \otimes \mathbf{Z}_p)^\chi \longrightarrow R_K^n$$

defined by $[\mathfrak{l}_K]^\chi \mapsto \mathbf{e}_r$ for each $\mathfrak{l} \in Q_r$ and each r with $1 \leqslant r \leqslant n$.

Let $\mathcal{K}$ denote the preimage of $(\mathcal{D} \otimes \mathbf{Z}_p)^\chi$ under the map $(K^\times \otimes \mathbf{Z}_p)^\chi \xrightarrow{\mathrm{div}} (\mathrm{Div}_K \otimes \mathbf{Z}_p)^\chi$. The exact sequence in Lemma 4.1 yields an exact sequence

$$0 \longrightarrow \mathcal{K} \xrightarrow{\mathrm{div}} (\mathcal{D} \otimes \mathbf{Z}_p)^\chi \longrightarrow A^\chi_K \longrightarrow 0.$$

The homomorphism α induces a surjective homomorphism $\beta : \mathcal{K} \longrightarrow R^n_K$ such that the diagram of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{K} & \xrightarrow{\mathrm{div}} & (\mathcal{D} \otimes \mathbf{Z}_p)^\chi & \longrightarrow & A^\chi_K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle =} & & \\
0 & \longrightarrow & R^n_K & \xrightarrow{\overline{f}} & R^n_K & \xrightarrow{\overline{g}} & A^\chi_K & \longrightarrow & 0
\end{array}$$

commutes. We define

$$\beta_r = \mathrm{pr}_r \circ \beta : \mathcal{K} \xrightarrow{\beta} R^n_K \xrightarrow{\mathrm{pr}_r} R_K$$

to be the composition of β with the rth projection.

Taking $\bmod p^N$ of the natural homomorphism $\mathcal{K} \longrightarrow (K^\times \otimes \mathbf{Z}_p)^\chi$, we consider

$$\mathcal{K}/p^N \longrightarrow (K^\times/p^N)^\chi.$$

This is injective, and the image coincides with the preimage of $(\mathcal{D}/p^N)^\chi$ under the map $(K^\times/p^N)^\chi \xrightarrow{\mathrm{div}} (\mathrm{Div}_K/p^N)^\chi$. These properties can be checked by diagram chasing of the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_K^\chi[p^N] & \longrightarrow & \mathcal{K}/p^N & \xrightarrow{\mathrm{div}} & (\mathcal{D}/p^N)^\chi & \longrightarrow & A_K^\chi/p^N & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow & & \downarrow & & \downarrow{=} & & \\ 0 & \longrightarrow & A_K^\chi[p^N] & \longrightarrow & (K^\times/p^N)^\chi & \xrightarrow{\mathrm{div}} & (\mathrm{Div}_K/p^N)^\chi & \longrightarrow & A_K^\chi/p^N & \longrightarrow & 0 \end{array}$$

where the map $(\mathcal{D}/p^N)^\chi \longrightarrow (\mathrm{Div}_K/p^N)^\chi$ is injective. Using the above map $\mathcal{K}/p^N \longrightarrow (K^\times/p^N)^\chi$, we identify $\mathcal{K}/p^N$ with the preimage of $(\mathcal{D}/p^N)^\chi$ under the map div.

For each r with $1 \leqslant r \leqslant n$, we consider $\beta_r \bmod p^N \colon \mathcal{K}/p^N \longrightarrow R_K/p^N$ which we denote simply by β_r.

Step 3. *Definition of* $x_{\mathfrak{n},\mathfrak{r}}$ *and a key Lemma* 10.2

For any $\mathfrak{n} \in \mathcal{N}_{[i-1]}(K)$ whose prime divisors are all in Q, $Q_{\mathfrak{n},K}$ denotes the set of all prime divisors of K dividing $\mathfrak{n}$. We define $\mathcal{D}_\mathfrak{n} = \bigoplus_{\rho \in Q_{\mathfrak{n},K}} \mathbf{Z} \cdot \rho$ which is a subgroup of $\mathcal{D}$, and $\mathcal{K}_{\mathfrak{n},N}$ to be the preimage of $(\mathcal{D}_\mathfrak{n}/p^N)^\chi$ under the map $\mathrm{div} : \mathcal{K}/p^N \longrightarrow (\mathcal{D}/p^N)^\chi$. Note that $\mathcal{K}_{\mathfrak{n},N}$ is a finite submodule of $(K^\times/p^N)^\chi$.

Recall that we are studying A_i which is the matrix obtained from A by eliminating the n_1th row,..., the n_ith row and the m_1th column,..., the m_ith column. We choose $n_{i+1}, \ldots, n_n$ such that $\{n_1, \ldots, n_n\} = \{1, \ldots, n\}$. We take $\mathfrak{l}_r \in Q_{n_r}$ for each r with $1 \leqslant r \leqslant n$, and fix them. Put $\mathfrak{L} = \mathfrak{l}_1 \cdot \ldots \cdot \mathfrak{l}_n$. In the case $i = 1$, we put $\mathfrak{n} = \mathfrak{n}_1 = 1$ and $\mathfrak{l} = \mathfrak{l}_1$. Suppose $i \geqslant 2$. We consider $\mathcal{K}_{\mathfrak{L},N}$ and

$$\beta_{m_1} : \mathcal{K}_{\mathfrak{L},N} \longrightarrow R_K/p^N.$$

Applying Lemma 10.1, we can take $\mathfrak{r}_2 \in \mathcal{S}(K(\mathfrak{L}))$ such that $\mathfrak{r}_2 \in Q_{n_2}$, $\mathfrak{r}_2 \neq \mathfrak{l}_2$, and $\beta_{m_1}(x) = \overline{\phi}_{\mathfrak{r}_2}(x)$ for all $x \in \mathcal{K}_{\mathfrak{L},N}$. For any r such that $2 < r \leqslant i+1$, we take $\mathfrak{r}_r$ by induction on r. Put $\mathfrak{n}_{r-1} = \mathfrak{r}_2 \cdot \ldots \cdot \mathfrak{r}_{r-1}$. We consider

$$\beta_{m_{r-1}} : \mathcal{K}_{\mathfrak{L}\,\mathfrak{n}_{r-1},N} \longrightarrow R_K/p^N.$$

By induction on r, using Lemma 10.1, we take $\mathfrak{r}_r \in \mathcal{S}(K(\mathfrak{L}\,\mathfrak{n}_{r-1}))$ such that

(I) $\mathfrak{r}_r \in Q_{n_r}$ and $\mathfrak{r}_r \neq \mathfrak{l}_r$;

(II) for the $b_r \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b_r) = (\mathfrak{r}_{r,K} - \mathfrak{l}_{r,K})^\chi$, $\phi_{\mathfrak{r}_s}(b_r) = 0$ holds for any s such that $2 \leqslant s < r$ and

(III) $\beta_{m_{r-1}}(x) = \overline{\phi}_{\mathfrak{r}_r}(x)$ for all $x \in \mathcal{K}_{\mathfrak{L}\,\mathfrak{n}_{r-1},N}$.

Thus, we have taken $\mathfrak{r}_2, \ldots, \mathfrak{r}_{i+1}$. (Note that $\mathfrak{r}_1$ is not defined.)

In the case $i \geqslant 2$, put $\mathfrak{l} = \mathfrak{l}_1$, and $\mathfrak{n} = \mathfrak{n}_i = \mathfrak{r}_2 \cdot \ldots \cdot \mathfrak{r}_i$. In § 7, we defined the element $x_{\mathfrak{n},\mathfrak{l}}$ which is determined if $a_\mathfrak{r}$ is given for each $\mathfrak{r}$ dividing $\mathfrak{n}$. For each $\mathfrak{r}_r$ with $2 \leqslant r \leqslant i$, we take

$$a_{\mathfrak{r}_r} = \phi_{\mathfrak{r}_r}(b_r)$$

to define $x_{\mathfrak{n},\mathfrak{l}}$. In the case $i = 1$, $x_{\mathfrak{n},\mathfrak{l}} = x_{\mathfrak{n}_1,\mathfrak{l}} = x_{1,\mathfrak{l}} = \kappa_{1,\mathfrak{l}} = g_\mathfrak{l}^K$. Since the elements $\kappa_{\mathfrak{n}/\mathfrak{d},\mathfrak{l}}$ are all in $\mathcal{K}/p^N$, $x_{\mathfrak{n},\mathfrak{l}}$ is in $\mathcal{K}/p^N$.

Lemma 10.2. (i) *For* r *such that* $2 \leqslant r \leqslant i$, *let* $\beta_{m_{r-1}}$ *be the map defined in Step* 2. *Then we have*

$$\beta_{m_{r-1}}(x_{\mathfrak{n},\mathfrak{l}}) = 0,$$

for any r *such that* $2 \leqslant r \leqslant i$.

(ii) *Let* $\alpha_j = \mathrm{pr}_j \circ \alpha : (\mathcal{D}/p^N)^\chi \xrightarrow{\alpha} (R_K/p^N)^n \xrightarrow{\mathrm{pr}_j} R_K/p^N$ *be the composition of* α *with the* j*th projection. Then we have*

$$\alpha_j(\mathrm{div}(x_{\mathfrak{n},\mathfrak{l}})) = 0,$$

for any j *such that* $j \neq n_1, \ldots, n_i$.

Proof of Lemma 10.2. Since $x_{\mathfrak{n},\mathfrak{l}}$ is a unit outside $\mathfrak{n}\mathfrak{l}$ (Proposition 7.3(0)), (ii) is immediate from the definition of $x_{\mathfrak{n},\mathfrak{l}}$ (and the above property (I)). We will prove (i). For any r such that $2 \leqslant r \leqslant i$, let $b_r \in (K^\times \otimes \mathbf{Z}_p)^\chi$ be the element such that $\mathrm{div}(b_r) = (\mathfrak{r}_{r,K} - \mathfrak{l}_{r,K})^\chi$. By the definition of α, we have $\alpha(\mathrm{div}(b_r)) = 0$, hence we know from the definition of β that $\beta(b_r) = 0$ for any r such that $2 \leqslant r \leqslant i$. Put

$$x = x_{\mathfrak{n},\mathfrak{l}} b_r^{-\overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n}/\mathfrak{r}_r,\mathfrak{l}})} \ldots b_i^{-\overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}/\mathfrak{r}_i,\mathfrak{l}})}.$$

It follows from $\beta(b_r) = \ldots = \beta(b_i) = 0$ that

$$\beta_{m_{r-1}}(x_{\mathfrak{n},\mathfrak{l}}) = \beta_{m_{r-1}}(x).$$

By Proposition 7.3(1) we have $\mathrm{div}_{\mathfrak{r}_s}(x) = \overline{\phi}_{\mathfrak{r}_s}(x_{\mathfrak{n}/\mathfrak{r}_s,\mathfrak{l}}) - \overline{\phi}_{\mathfrak{r}_s}(x_{\mathfrak{n}/\mathfrak{r}_s,\mathfrak{l}}) = 0$ for any s such that $r \leqslant s \leqslant i$. This shows that $\mathrm{div}(x) \in (\mathcal{D}_{\mathfrak{L}\mathfrak{n}_{r-1}}/p^N)^\chi$, which implies $x \in \mathcal{K}_{\mathfrak{L}\mathfrak{n}_{r-1},N}$. Hence, applying the above property (III), we obtain

$$\beta_{m_{r-1}}(x) = \overline{\phi}_{\mathfrak{r}_r}(x).$$

By the above property (II), we have $\overline{\phi}_{\mathfrak{r}_r}(b_{r+1}) = \ldots = \overline{\phi}_{\mathfrak{r}_r}(b_i) = 0$. Therefore, we get

$$\overline{\phi}_{\mathfrak{r}_r}(x) = \overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n},\mathfrak{l}} b_r^{-\overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n}/\mathfrak{r}_r,\mathfrak{l}})}).$$

Now, using Proposition 7.3(2), we have

$$\overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n},\mathfrak{l}} b_r^{-\overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n}/\mathfrak{r}_r,\mathfrak{l}})}) = \overline{\phi}_{\mathfrak{r}_r}(b_r)\overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n}/\mathfrak{r}_r,\mathfrak{l}}) - \overline{\phi}_{\mathfrak{r}_r}(x_{\mathfrak{n}/\mathfrak{r}_r,\mathfrak{l}})\overline{\phi}_{\mathfrak{r}_r}(b_r) = 0.$$

Therefore, we have obtained $\beta_{m_{r-1}}(x_{\mathfrak{n},\mathfrak{l}}) = 0$, which completes the proof of Lemma 10.2. □

Step 4. *Approximation of the minor* $\det A_i$

We go back to the proof of Theorem 2.1. Since $x_{\mathfrak{n},\mathfrak{l}}$ is in $\mathcal{K}_{\mathfrak{L}\mathfrak{n}_i,N}$, we note that we also have

$$\beta_{m_i}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}})$$

by the property (III).

Put $\mathbf{x} = \beta(x_{\mathfrak{n},\mathfrak{l}}) \in (R_K/p^N)^n$ and $\mathbf{y} = \alpha(\mathrm{div}(x_{\mathfrak{n},\mathfrak{l}})) \in (R_K/p^N)^n$, which we regard as column vectors. Since $R_K/p^N = \Lambda/(\gamma_m - 1, p^N)$, we have

$$A\mathbf{x} \equiv \mathbf{y} \pmod{(\gamma_m - 1, p^N)}.$$

Let $\mathbf{x}' \in (R_K/p^N)^{n-i+1}$ be the vector obtained from $\mathbf{x}$ by eliminating the m_1th row,...,and the m_{i-1}th row, and $\mathbf{y}' \in (R_K/p^N)^{n-i+1}$ the vector obtained from $\mathbf{y}$ by eliminating the n_1th row,..., and the n_{i-1}th row. It follows from Lemma 10.2 (i) that the m_rth row of $\mathbf{x}$ is zero in R_K/p^N for all r such that $1 \leqslant r \leqslant i-1$. Therefore, we have

$$A_{i-1}\mathbf{x}' \equiv \mathbf{y}' \pmod{(\gamma_m - 1, p^N)}.$$

If $i \geqslant 2$, then the n_ith component of $\mathbf{y}$ is $\overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}/\mathfrak{r}_i,\mathfrak{l}}) = \overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}_{i-1},\mathfrak{l}})$ by Proposition 7.3(1). Hence, if the n_i'th component of $\mathbf{y}'$ is the n_ith component of $\mathbf{y}$, then by Lemma 10.2(ii) we have

$$\mathbf{y}' = \overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}_{i-1},\mathfrak{l}})\mathbf{e}_{n_i'},$$

where $\mathbf{e}_{n_i'}$ denotes the n_i'th standard basis vector of $(R_K/p^N)^{n-i+1}$. We saw $\beta_{m_i}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}})$ above. Therefore, the m_ith component of $\mathbf{x}$ is $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}})$. We suppose that the m_i'th

component of $\mathbf{x}'$ is the m_ith component of $\mathbf{x}$. Let $\mathrm{Adj}(A_{i-1})$ be the matrix of cofactors (namely, the (s,t) entry of $\mathrm{Adj}(A_{i-1})$ is $(-1)^{s+t}\det P_{ts}$ where P_{ts} is the matrix obtained by eliminating the tth row and the sth column of A_{i-1}). Multiplying both sides of $A_{i-1}\mathbf{x}' \equiv \overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}_{i-1},\mathfrak{l}})\mathbf{e}_{n_i'}$ by $\mathrm{Adj}(A_{i-1})$ on the left, we get

$$(\det A_{i-1})\mathbf{x}' \equiv \overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}_{i-1},\mathfrak{l}})\mathrm{Adj}(A_{i-1})\mathbf{e}_{n_i'}.$$

Hence, we obtain

$$(\det A_{i-1})\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}}) \equiv (-1)^{n_i'+m_i'}(\det A_i)\overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}_{i-1},\mathfrak{l}}) \pmod{(\gamma_m-1,p^N)}.$$

Recall that $\mathfrak{n}=\mathfrak{n}_i$. We are not concerned with the sign problem, and write the above equation as

$$(\det A_{i-1})\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}}) \equiv \pm(\det A_i)\overline{\phi}_{\mathfrak{r}_i}(x_{\mathfrak{n}_{i-1},\mathfrak{l}}) \pmod{(\gamma_m-1,p^N)}. \tag{10.3}$$

If $i=1$, then $x_{1,\mathfrak{l}} = g_{\mathfrak{l}}^K$, so the n_1-th component of $\mathbf{y}$ is θ_K^χ, and $\mathbf{y}=\theta_K^\chi\mathbf{e}_{n_1}$. Therefore, by the same method as above, we obtain

$$(\det A_0)\overline{\phi}_{\mathfrak{r}_2}(x_{\mathfrak{n}_1,\mathfrak{l}}) \equiv (-1)^{n_1+m_1}(\det A_1)\theta_K^\chi \pmod{(\gamma_m-1,p^N)}. \tag{10.4}$$

In order to clarify that we are working over $K=K_{0,m}$, we write $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m$ for $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})$.

LEMMA 10.3. *For $i\geqslant 1$ the limit of $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m$ exists in Λ as m goes to ∞. (Namely, if $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})'_m \in \Lambda$ is a lifting of $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m \in \Lambda/(p^{N_m},\gamma_m-1)$, $\lim_{m\to\infty}\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})'_m$ exists.) We denote the limit by $\lim_{m\to\infty}\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m$. We also have*

$$\lim_{m\to\infty}\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m = \pm\det A_i \in \Lambda.$$

Proof of Lemma 10.3. Recall that we took A_0 such that $\det A_0 = \theta_{K_\infty}^\chi$ in the beginning of this subsection. We have $\lim_{m\to\infty}\theta_{K_{0,m}}^\chi = \theta_{K_\infty}^\chi = \det A_0$. Hence, the above congruence (10.4) on $\overline{\phi}_{\mathfrak{r}_2}(x_{\mathfrak{n}_1,\mathfrak{l}})$ implies that the limit of $\overline{\phi}_{\mathfrak{r}_2}(x_{\mathfrak{n}_1,\mathfrak{l}})_m$ exists, and

$$\lim_{m\to\infty}\overline{\phi}_{\mathfrak{r}_2}(x_{\mathfrak{n}_1,\mathfrak{l}})_m = \pm\det A_1$$

because $\det A_0 \neq 0$. For general $i\geqslant 2$, by the same method as for $i=1$, using (10.3) for $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})$ and induction on i, we get

$$\det A_{i-1}\lim_{m\to\infty}\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m = \pm\det A_i\det A_{i-1}$$

(we note that the sign does not depend on m). Recall that we took A_r such that $\det A_r\neq 0$ for any r with $1\leqslant r\leqslant i$. Therefore, the limit of $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m$ exists, and we get

$$\lim_{m\to\infty}\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m = \pm\det A_i. \qquad \square$$

Step 5. *Final step of the proof of Theorem* 2.1

We now prove Theorem 2.1. Put $I_m=(p^{N_m},\gamma_m-1)$, and $\xi_m=\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m \in \Lambda/I_m$. Note that $(\xi_m)_m$ might not be a projective system (namely, $(\xi_m)_m \in \varprojlim\Lambda/I_m$ might not hold). Since ξ_m converges, the image $\xi_{n,m}$ of ξ_n for sufficiently large $n\gg m$ under the natural map $\pi_{n,m}:\Lambda/I_n\longrightarrow\Lambda/I_m$ does not depend on the choice of n. We denote it by ξ'_m. If the following Lemma 10.4 holds, then applying it to $\xi_n\in\Lambda/I_n$, we have $\xi_n\in\Theta_{i,K_{0,n}}^{(\delta,N),\chi}$. Since $\pi_{n,m}(\Theta_{i,K_{0,n}}^{(\delta,N_n),\chi})\subset\Theta_{i,K_{0,m}}^{(\delta,N_m),\chi}$, $\xi'_m=\xi_{n,m}$ is in $\Theta_{i,K_{0,m}}^{(\delta,N_m),\chi}$. By the construction of ξ'_m, $(\xi'_m)_m$ becomes a projective system. Hence, we obtain $(\xi'_m)_m\in\varprojlim\Theta_{i,K_{0,m}}^{(\delta,N_m),\chi}=\Theta_{i,K_\infty}^{(\delta),\chi}$. This shows that

$$\det A_i = \pm\lim_{m\to\infty}\xi_m = \pm\lim_{m\to\infty}\xi'_m \in \Theta_{i,K_\infty}^{(\delta),\chi}.$$

Therefore, we have

$$\mathrm{Fitt}_{i,\Lambda}(X^{\chi}_{K_\infty}) \subset \Theta^{(\delta),\chi}_{i,K_\infty}.$$

Combining the above inclusion with the inclusions $\Theta^{(\delta),\chi}_{i,K_\infty} \subset \Theta^{\chi}_{i,K_\infty} \subset \mathrm{Fitt}_{i,\Lambda}(X^{\chi}_{K_\infty})$ in Corollary 9.12, we get

$$\mathrm{Fitt}_{i,\Lambda}(X^{\chi}_{K_\infty}) = \Theta^{(\delta),\chi}_{i,K_\infty} = \Theta^{\chi}_{i,K_\infty}. \tag{10.5}$$

Therefore, our final task is to prove the following lemma.

LEMMA 10.4. *For any $i \geqslant 1$, $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m$ is in $\Theta^{(\delta,N_m),\chi}_{i,K_{0,m}}$.*

Proof of Lemma 10.4. To simplify the notation, we again write $K = K_{0,m}$, $N = N_m$, $\mathfrak{n} = \mathfrak{n}_i$ and $\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n}_i,\mathfrak{l}})_m$. Applying Lemma 10.1 to the map $\overline{\phi}_{\mathfrak{r}_{i+1}} : \mathcal{K}_{\mathfrak{n}\,\mathfrak{l},N} \longrightarrow R_K/p^N$, we can take $\mathfrak{l}' \in Q_{n_1}$ which satisfies the properties stated before Lemma 7.2, and

$$\overline{\phi}_{\mathfrak{r}_{i+1}}(x) = \overline{\phi}_{\mathfrak{l}'}(x),$$

for any $x \in \mathcal{K}_{\mathfrak{n}\,\mathfrak{l},N}$. In particular, we have

$$\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{l}'}(x_{\mathfrak{n},\mathfrak{l}}).$$

Let $b \in (K^\times \otimes \mathbf{Z}_p)^{\chi}$ be the element such that $\mathrm{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^{\chi}$. By Proposition 7.3(3) we have

$$\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}}) = \overline{\phi}_{\mathfrak{l}'}(x_{\mathfrak{n},\mathfrak{l}}) = -\sum_{\mathfrak{d}|\mathfrak{n}} \overline{a}_{\mathfrak{d}}(\delta_{\mathfrak{n}/\mathfrak{d}\,\mathfrak{l}'} + \delta_{\mathfrak{n}/\mathfrak{d}}\overline{\phi}_{\mathfrak{l}'}(b)).$$

Since $\epsilon(\mathfrak{n}/\mathfrak{d}) < \epsilon((\mathfrak{n}/\mathfrak{d})\,\mathfrak{l}') \leqslant \epsilon(\mathfrak{n}\,\mathfrak{l}') = i$ for any $\mathfrak{d}$ ($\epsilon(\mathfrak{n})$ is defined in the beginning of § 5.2), both $\delta_{\mathfrak{n}/\mathfrak{d}\,\mathfrak{l}'}$ and $\delta_{\mathfrak{n}/\mathfrak{d}}$ are in $\Theta^{(\delta,N),\chi}_{i,K}$. Hence, we get

$$\overline{\phi}_{\mathfrak{r}_{i+1}}(x_{\mathfrak{n},\mathfrak{l}}) \in \Theta^{(\delta,N),\chi}_{i,K}.$$

This completes the proof of Lemma 10.4 and Theorem 2.1. □

10.3.

In this subsection, we prove Theorem 2.3 and Corollary 2.4.

We first prove Theorem 2.3. Let $\pi_m : \Lambda \longrightarrow R_{K_{0,m}}$ be the natural map for any $m \geqslant 0$. By Lemma 9.9 we have $\pi_m(\mathrm{Fitt}_{i,\Lambda}(X^{\chi}_{K_\infty})) = \mathrm{Fitt}_{i,R_{K_{0,m}}}(A^{\chi}_{K_{0,m}})$. Since $\pi_m(\Theta^{(\delta),\chi}_{i,K_\infty}) \subset \Theta^{(\delta),\chi}_{i,K_{0,m}}$ by definition, using (10.5) in the proof of Theorem 2.1, we have

$$\mathrm{Fitt}_{i,R_{K_{0,m}}}(A^{\chi}_{K_{0,m}}) = \pi_m(\mathrm{Fitt}_{i,\Lambda}(X^{\chi}_{K_\infty})) = \pi_m(\Theta^{\chi}_{i,K_\infty}) = \pi_m(\Theta^{(\delta),\chi}_{i,K_\infty}) \subset \Theta^{(\delta),\chi}_{i,K_{0,m}} \subset \Theta^{\chi}_{i,K_{0,m}}.$$

The last inclusion is (8.1) in § 8. On the other hand, we have the other inclusion $\Theta^{\chi}_{i,K_{0,m}} \subset \mathrm{Fitt}_{i,R_{K_{0,m}}}(A^{\chi}_{K_{0,m}})$ by Theorem 9.11, so we get the equality $\mathrm{Fitt}_{i,R_{K_{0,m}}}(A^{\chi}_{K_{0,m}}) = \Theta^{(\delta),\chi}_{i,K_{0,m}} = \Theta^{\chi}_{i,K_{0,m}}$.

Next, we prove Corollary 2.4. Since we have shown $\pi_m(\Theta^{\chi}_{i,K_\infty}) = \Theta^{\chi}_{i,K_{0,m}}$ above, $\Theta^{\chi\psi}_i$ is the image of $\Theta^{\chi}_{i,K_\infty}$ under the map $\Lambda \xrightarrow{\pi_m} R_{K_{0,m}} \xrightarrow{\psi} O_{\chi\psi}$. Therefore, Corollary 2.4 is an immediate consequence of Theorem 2.1 and Lemma 9.5.

10.4.

Finally, we give two remarks in this subsection.

REMARK 10.5. We give some examples of numerical computation. Take $k=\mathbf{Q}$, $K_0=\mathbf{Q}(\sqrt{-2437})$, $p=3$ and χ to be the character associated to K_0. Then all the assumptions of Theorem 2.1 are satisfied. We identify Λ with $\mathbf{Z}_p[\![T]\!]$, using the correspondence between γ and $1+T$ where γ is the generator of $\mathrm{Gal}(K_\infty/K_0)$ such that $\kappa(\gamma)=1+p$, where κ is the cyclotomic character. It is easy to check that the λ-invariant of the p-adic L-function $\theta^\chi_{K_\infty}$ is 2, and $A_{K_0}=(\mathbf{Z}/3\mathbf{Z})^{\oplus 2}$. We have $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})\neq\Lambda$ because $\mathrm{Fitt}_{1,\mathbf{Z}_3}(A_{K_0})=(3)\neq\mathbf{Z}_3$. We regard $\theta^\chi_{K_\infty}=\theta^\chi_{K_\infty}(T)$ as an element of $\mathbf{Z}_3[\![T]\!]$; then we have $\mathrm{ord}_3(\theta^\chi_{K_\infty}(0))=2$. For a prime ℓ such that $\ell\equiv 1 \pmod{p^2}$, $K_0(\ell)$ denotes the maximal p-extension of K_0 in $K_0(\mu_\ell)$, and $G_\ell=\mathrm{Gal}(K_0(\ell)/K_0)$. We consider $\theta^\chi_{K_0(\ell)_\infty}\in\Lambda[G_\ell]$, and write

$$\theta^\chi_{K_0(\ell)_\infty}=\delta_0^{(\ell)}+\delta_1^{(\ell)}(\sigma_\ell-1)+\delta_2^{(\ell)}(\sigma_\ell-1)^2+\dots,$$

where $\delta_i^{(\ell)}\in\Lambda$ for $i\geqslant 0$. We compute the image $\overline{\delta_1^{(\ell)}}$ of $\delta_1^{(\ell)}$ in $\Lambda/(9,T^2)=\mathbf{Z}_3[T]/(9,T^2)$, and obtain

$$\overline{\delta_1^{(19)}}=2T+3 \quad\text{and}\quad \overline{\delta_1^{(37)}}=7T.$$

Hence, Theorem 2.1 implies that $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty}) \bmod (9,T^2)$ contains $2T+3$ and $7T$. This shows that the image of $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})$ in $\Lambda/(p^2,T^2)$ contains $(3,T)$, which implies that $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})\supset(3,T)$. Since $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})\neq\Lambda$, it follows that

$$\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})=(3,T).$$

By Lemma 9.3 the information that $\mathrm{Fitt}_{0,\Lambda}(X_{K_\infty})=(\theta^\chi_{K_\infty})$, $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})=(3,T)$ and $\mathrm{Fitt}_{2,\Lambda}(X_{K_\infty})=\Lambda$ determines the isomorphism class of $X^\chi_{K_\infty}$ (concerning relation matrices of $X^\chi_{K_\infty}$, see [9, Lemma 9.1]).

For both $K_0=\mathbf{Q}(\sqrt{-6226})$ and $\mathbf{Q}(\sqrt{-6910})$) with $p=3$, the λ-invariant of $\theta^\chi_{K_\infty}$ are also 2, and $A_{K_0}=(\mathbf{Z}/3\mathbf{Z})^{\oplus 2}$. We can also compute

$$\overline{\delta_1^{(19)}}=3 \quad\text{and}\quad \overline{\delta_1^{(37)}}=2T+3 \quad\text{for}\quad K_0=\mathbf{Q}(\sqrt{-6226})$$

and

$$\overline{\delta_1^{(19)}}=3T+3 \quad\text{and}\quad \overline{\delta_1^{(37)}}=7T \quad\text{for}\quad K_0=\mathbf{Q}(\sqrt{-6910}),$$

respectively.

Therefore, we get $\mathrm{Fitt}_{1,\Lambda}(X_{K_\infty})=(3,T)$ in these two cases, too. Hence, the isomorphism class is also determined by these data. In [7], Koike determined the isomorphism classes for many numerical examples, but in these two cases ($\mathbf{Q}(\sqrt{-6226})$ and $\mathbf{Q}(\sqrt{-6910})$) the isomorphism classes were not determined by his method.

REMARK 10.6. Using the theory in this paper, we can compute in several cases not only the Fitting ideals but also the matrix corresponding to $\overline{f}$ in (10.2) in § 10.2. We will give a simple example.

Suppose $K=K_{0,m}$, $\mathfrak{l}_1\mathfrak{l}_2\in\mathcal{N}_{[2]}(K)$ and $\mathfrak{l}_2\in\mathcal{S}(K(\mathfrak{l}_1))$. We assume that $\delta_{\mathfrak{l}_1\mathfrak{l}_2}$ is a unit in R_K/p^N. (The numerical computation of $\delta_{\mathfrak{n}}$ is easy in general.) Then $\mathrm{Fitt}_{2,R_K}(A^\chi_K)=R_K$ by Theorem 2.3, and A^χ_K is generated by two elements over R_K (cf. § 9.1). Assume further that A^χ_K is generated by $[\mathfrak{l}_1]^\chi$ and $[\mathfrak{l}_2]^\chi$. Then $\mathcal{K}_{\mathfrak{l}_1\mathfrak{l}_2,N}$ is a free R_K/p^N-module of rank 2, and $\kappa_{\mathfrak{l}_1,\mathfrak{l}_2}$, $\kappa_{\mathfrak{l}_2,\mathfrak{l}_1}$ is a basis of $\mathcal{K}_{\mathfrak{l}_1\mathfrak{l}_2,N}$. In fact, by Propositions 6.4 and 6.5, we have $\overline{\phi}_{\mathfrak{l}_1}(\kappa_{\mathfrak{l}_1,\mathfrak{l}_2})=0$, $\overline{\phi}_{\mathfrak{l}_2}(\kappa_{\mathfrak{l}_1,\mathfrak{l}_2})=\delta_{\mathfrak{l}_1\mathfrak{l}_2}$, $\overline{\phi}_{\mathfrak{l}_1}(\kappa_{\mathfrak{l}_2,\mathfrak{l}_1})=\delta_{\mathfrak{l}_1\mathfrak{l}_2}$, and $\overline{\phi}_{\mathfrak{l}_2}(\kappa_{\mathfrak{l}_2,\mathfrak{l}_1})=0$. This shows that $\overline{\phi}_{\mathfrak{l}_1}\oplus\overline{\phi}_{\mathfrak{l}_2}:\mathcal{K}_{\mathfrak{l}_1\mathfrak{l}_2,N}\longrightarrow(R_K/p^N)^{\oplus 2}$ is an isomorphism, and $\kappa_{\mathfrak{l}_1,\mathfrak{l}_2}$, $\kappa_{\mathfrak{l}_2,\mathfrak{l}_1}$ is a basis of $\mathcal{K}_{\mathfrak{l}_1\mathfrak{l}_2,N}$. Consider the exact sequence

$$\mathcal{K}_{\mathfrak{l}_1\mathfrak{l}_2}/p^N\xrightarrow{\mathrm{div}}(\mathcal{D}_{\mathfrak{l}_1\mathfrak{l}_2}/p^N)^\chi\longrightarrow A^\chi_K/p^N\longrightarrow 0.$$

Using the basis $\kappa_{\mathfrak{l}_1,\mathfrak{l}_2}$, $\kappa_{\mathfrak{l}_2,\mathfrak{l}_1}$, we can compute the relation matrix of A_K^χ/p^N to be

$$\begin{pmatrix} \overline{\phi}_{\mathfrak{l}_1}(g_{\mathfrak{l}_2}^K) & \delta_{\mathfrak{l}_2} \\ \delta_{\mathfrak{l}_1} & \overline{\phi}_{\mathfrak{l}_2}(g_{\mathfrak{l}_1}^K) \end{pmatrix}$$

by Proposition 5.2. Note that the entries of the matrix are numerically computable in principle if $k = \mathbf{Q}$. This is also an example in which both $\kappa_{\mathfrak{l}_1,\mathfrak{l}_2}$ and $\kappa_{\mathfrak{l}_2,\mathfrak{l}_1}$ play important roles.

Appendix A.

In this appendix, we prove the following proposition.

PROPOSITION A.1. *Suppose that $\mathfrak{r}$, $\mathfrak{l}$ are two distinct primes in $\mathcal{S}(K)$. We take $\mathfrak{l}' \in \mathcal{S}(K(\mathfrak{r}))$ and $b \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(b) = (\mathfrak{l}'_K - \mathfrak{l}_K)^\chi$ and $\phi_{\mathfrak{r}}^{(n_\mathfrak{r})}(b) = 0$ where $\phi_{\mathfrak{r}}^{(n_\mathfrak{r})} : (K^\times/p^{n_\mathfrak{r}})^\chi \longrightarrow O_\chi/p^{n_\mathfrak{r}}[\Gamma(K/k)] \otimes G_\mathfrak{r}$ is the map defined by taking $N = n_\mathfrak{r}$. Put $\tilde{\kappa}_{\mathfrak{r},\mathfrak{l}} = \tilde{\kappa}_{\mathfrak{r},\mathfrak{l}'} - \tilde{\delta}_\mathfrak{r} b$. Then $\tilde{\kappa}_{\mathfrak{r},\mathfrak{l}}$ does not depend on the choice of $\mathfrak{l}'$.*

Proof. Put $L = K(\mathfrak{r})$ and $G = \mathrm{Gal}(L/K)$. Suppose that we take two primes $\mathfrak{l}_1$, $\mathfrak{l}_2 \in \mathcal{S}(L)$ such that there exist b_1, $b_2 \in (K^\times \otimes \mathbf{Z}_p)^\chi$ with $\mathrm{div}(b_i) = ((\mathfrak{l}_i)_K - \mathfrak{l}_K)^\chi$ and $\phi_{\mathfrak{r}}^{(n_\mathfrak{r})}(b_i) = 0$ for $i = 1, 2$. Put $b = b_1/b_2$. We denote by $K\{\mathfrak{r}\}/K$ the maximal abelian p-extension which is unramified outside $\mathfrak{r}$. Consider the χ-component $\mathrm{Gal}(K\{\mathfrak{r}\}/K)^\chi$ of the Galois group, and define $K\{\mathfrak{r}\}^\chi$ to be the intermediate field such that $\mathrm{Gal}(K\{\mathfrak{r}\}^\chi/K) = \mathrm{Gal}(K\{\mathfrak{r}\}/K)^\chi$. We denote by L'/L the maximal unramified p-extension such that L'/K is abelian and $\Delta(K/k)$ acts on $\mathrm{Gal}(L'/L)$ via χ. Then we have a canonical isomorphism $\mathrm{Gal}(L'/L) \xrightarrow{\simeq} (A_L^\chi)_G$. Since the ramification index of a prime above $\mathfrak{r}$ in L/K is $p^{n_\mathfrak{r}}$ and the ramification index of a prime above $\mathfrak{r}$ in any abelian extension M/k is at most $p^{n_\mathfrak{r}}$, it follows that $LK\{\mathfrak{r}\}^\chi/L$ is unramified above $\mathfrak{r}$ and so unramified everywhere. Hence, the restriction map

$$\mathrm{Gal}(L'/L) = (A_L^\chi)_G \xrightarrow{\simeq} \mathrm{Gal}(K\{\mathfrak{r}\}^\chi/K)$$

is bijective.

Put $\Psi = ((\prod_{v|\mathfrak{r}} K_v^\times/U_{K_v}^1 \times \bigoplus_{v\nmid\mathfrak{r}} K_v^\times/U_{K_v}) \otimes \mathbf{Z}_p)^\chi$. We consider the commutative diagram

$$\begin{array}{ccccccccc} & & ((L^\times \otimes \mathbf{Z}_p)^\chi)_G & \xrightarrow{\mathrm{div}} & ((\mathrm{Div}_L \otimes \mathbf{Z}_p)^\chi)_G & \longrightarrow & (A_L^\chi)_G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \simeq} & & \\ 0 & \longrightarrow & (K^\times \otimes \mathbf{Z}_p)^\chi & \xrightarrow{i} & \Psi & \longrightarrow & \mathrm{Gal}(K\{\mathfrak{r}\}^\chi/K) & \longrightarrow & 0 \end{array}$$

where i is the natural map which is injective because of $(O_K^\times \otimes \mathbf{Z}_p)^\chi = 0$, and ψ is the map induced by the norm map. Since $\phi_{\mathfrak{r}}^{(n_\mathfrak{r})}(b) = 0$, the v-component of $i(b) \in ((\prod_{v|\mathfrak{r}} K_v^\times/U_{K_v}^1 \times \bigoplus_{v\nmid\mathfrak{r}} K_v^\times/U_{K_v}) \otimes \mathbf{Z}_p)^\chi$ is trivial for all $v \mid \mathfrak{r}$. Hence, $i(b)$ is in the image of ψ. Therefore, by the above commutative diagram, there is $a \in (L^\times \otimes \mathbf{Z}_p)^\chi$ such that $N_{L/K}(a) = b$ and $\mathrm{div}(a) = \mathfrak{l}_{1,L} - \mathfrak{l}_{2,L} + (\sigma_\mathfrak{r} - 1)x$ for some $x \in (\mathrm{Div}_L \otimes \mathbf{Z}_p)^\chi$.

We have $\mathrm{div}((g_{\mathfrak{l}_1}^L/g_{\mathfrak{l}_2}^L)(\theta_L^\chi a^{-1})) = -\theta_L^\chi(\sigma_\mathfrak{r} - 1)x$. Hence,

$$\mathrm{div}\left(D_\mathfrak{r}\left(\frac{g_{\mathfrak{l}_1}^L}{g_{\mathfrak{l}_2}^L}(\theta_L^\chi a^{-1})\right)\right) = -D_\mathfrak{r}\theta_L^\chi(\sigma_\mathfrak{r} - 1)x = (N_\mathfrak{r} - p^{n_\mathfrak{r}})\theta_L^\chi x.$$

By Lemma 3.4 we have $N_\mathfrak{r}\theta_L^\chi = (1 - \varphi_\mathfrak{r}^{-1})\theta_K^\chi N_\mathfrak{r} = 0$, hence $\mathrm{div}(D_\mathfrak{r}((g_{\mathfrak{l}_1}^L/g_{\mathfrak{l}_2}^L)(\theta_L^\chi a^{-1}))) = -p^{n_\mathfrak{r}}\theta_L^\chi x$ holds. We take $g_x \in (L^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(g_x) = \theta_L^\chi x$. This is possible because

$\theta_L^\chi A_L^\chi = 0$. Thus, we have $\mathrm{div}(D_\mathfrak{r}((g_{\mathfrak{l}_1}^L/g_{\mathfrak{l}_2}^L)(\theta_L^\chi a^{-1}))) = -\mathrm{div}(g_x^{p^{n_\mathfrak{r}}})$, which implies

$$D_\mathfrak{r}\left(\frac{g_{\mathfrak{l}_1}^L}{g_{\mathfrak{l}_2}^L}(\theta_L^\chi a^{-1})\right) = g_x^{-p^{n_\mathfrak{r}}}$$

in $(L^\times \otimes \mathbf{Z}_p)^\chi$ by Lemma 4.1. It follows that $D_\mathfrak{r}(g_{\mathfrak{l}_1}^L/g_{\mathfrak{l}_2}^L) = D_\mathfrak{r}\theta_L^\chi a$ in $(L^\times \otimes \mathbf{Z}/p^N)^\chi$. Hence, we have in $(L^\times \otimes \mathbf{Z}/p^N)^\chi$

$$\frac{\kappa_{\mathfrak{r},\mathfrak{l}_1}}{\kappa_{\mathfrak{r},\mathfrak{l}_2}} = D_\mathfrak{r}\theta_L^\chi a = \delta_\mathfrak{r} N_\mathfrak{r} a = \delta_\mathfrak{r} b = \delta_\mathfrak{r}\left(\frac{b_1}{b_2}\right).$$

Therefore, we obtain

$$\frac{\kappa_{\mathfrak{r},\mathfrak{l}_1}}{\delta_\mathfrak{r} b_1} = \frac{\kappa_{\mathfrak{r},\mathfrak{l}_2}}{\delta_\mathfrak{r} b_2}$$

in $(K^\times \otimes \mathbf{Z}/p^N)^\chi$. This implies $\tilde{\kappa}_{\mathfrak{r},\mathfrak{l}_1} - \tilde{\delta}_\mathfrak{r} b_1 = \tilde{\kappa}_{\mathfrak{r},\mathfrak{l}_2} - \tilde{\delta}_\mathfrak{r} b_2$, which completes the proof of Proposition A.1. □

Acknowledgements. I would like to express my sincere gratitude to late Professor Iwasawa for his interest in this work when I explained to him the first version of the theory in this paper. I would also like to thank K. Kato heartily for his interest in this work, and for giving me an opportunity of a series of lectures on this subject at Kyoto University in 2007. I would like to thank K. Rubin very much for his interesting lectures I attended in 2002 on Kolyvagin systems. I thank K. Kurano very much for citing to me an example in Remark 9.4, and M. Aoki for the discussions on the subject in this paper. I am very grateful to D. Burns, J. Coates, R. Greenberg and C. Greither for helpful discussions with them on the subjects related to this work. Finally, I thank very much the referee for his careful reading and suggestions.

References

1. N. Bourbaki, *Éléments de Mathématique, Algèbre Commutative*, Chapter 7 (Hermann, Paris, 1965).
2. P. Deligne and K. Ribet, 'Values of abelian L-functions at negative integers over totally real fields', *Invent. Math.* 59 (1980) 227–286.
3. B. Ferrero and L. Washington, 'The Iwasawa invariant μ_p vanishes for abelian number fields', *Ann. of Math.* 109 (1979) 377–395.
4. C. Greither, 'Computing Fitting ideals of Iwasawa modules', *Math. Z.* 246 (2004) 733–767.
5. C. Greither and M. Kurihara, 'Stickelberger elements, Fitting ideals of class groups of CM fields, and dualisation', *Math. Z.* 260 (2008) 905–930.
6. K. Iwasawa, 'On the μ-invariants of $\mathbf{Z}_\ell$-extensions', *Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki* (Kinokuniya, Tokyo, 1973) 1–11; Collected Papers 53, 709–719.
7. M. Koike, 'On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda = 2$', *J. Math. Sci. Univ. Tokyo* 6 (1999) 371–396.
8. V. A. Kolyvagin, 'Euler systems', *The Grothendieck Festschrift*, vol. II (Birkhäuser, Boston, 1990) 435–483.
9. M. Kurihara, 'Iwasawa theory and Fitting ideals', *J. reine angew. Math.* 561 (2003) 39–86.
10. M. Kurihara, 'On the structure of ideal class groups of CM-fields', *Doc. Math.*, Extra Volume Kato (2003) 539–563.
11. M. Kurihara, 'Refined Iwasawa theory for p-adic representations and the structure of Selmer groups', Preprint (2011) http://www.math.keio.ac.jp/ kurihara/index.htm.
12. B. Mazur and K. Rubin, *'Kolyvagin systems', Mem. Amer. Math. Soc.* 168 Number 799 (AMS, Providence, 2004).
13. B. Mazur and A. Wiles, 'Class fields of abelian extensions of $\mathbf{Q}$', *Invent. Math.* 76 (1984) 179–330.
14. D. G. Northcott, *Finite free resolutions* (Cambridge University Press, Cambridge, 1976).
15. K. Rubin, *The main conjecture, Appendix to cyclotomic fields I and II*, Graduate Texts in Mathematics 121 (ed. S. Lang; Springer, Berlin, 1990) 397–419.
16. K. Rubin, 'Kolyvagin's system of Gauss sums', *Arithmetic algebraic geometry* (eds G. van der Geer *et al.*), Progress in Mathematics 89 (Birkhäuser, Boston, 1991) 309–324.
17. K. Rubin, *Euler systems*, Annals of Mathematical Studies 147 (Princeton University Press, Princeton, NJ, 2000).

18. R. Schoof, 'The structure of the minus class groups of abelian number fields', *Sém. de Théorie des Nombres P aris 1988–89* (Birkhäuser, Boston, 1990) 185–204.
19. J.-P. Serre, *Corps locaux* (Hermann, Paris, 1968) (troisième édition).
20. C. R. Siegel, 'Über die Fourierschen Koeffizienten von Modulformen', *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* 1970 (1970) 15–56.
21. J. Tate, *Les conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, Progress in Mathematics 47 (Birkhäuser, Boston, 1984).
22. L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics 83 (Springer, Berlin, 1982).
23. A. Wiles, 'The Iwasawa conjecture for totally real fields', *Ann. of Math.* 131 (1990) 493–540.
24. K. Wingberg, 'Duality theorems for Γ-extensions of algebraic number fields', *Compos. Math.* 55 (1985) 333–381.

Masato Kurihara
Department of Mathematics
Keio University
3-14-1 Hiyoshi
Kohoku-ku
Yokohama 223-8522
Japan

kurihara@math.keio.ac.jp