Ideal class groups of CM-fields with non-cyclic Galois action

Masato Kurihara and Takashi Miura

Abstract. Suppose that L/k is a finite and abelian extension such that k is a totally real base field and L is a CM-field. We regard the ideal class group Cl_L of L as a $\mathrm{Gal}(L/k)$-module. As a sequel of the paper [8] by the first author, we study a problem whether the Stickelberger element for L/k times the annihilator ideal of the roots of unity in L is in the Fitting ideal of Cl_L, and also a problem whether it is in the Fitting ideal of the Pontrjagin dual $(\mathrm{Cl}_L)^\vee$. We systematically construct extensions L/k for which these properties do not hold, and also give numerical examples.

0 Introduction

Our aim in this paper is to study the Galois action on the ideal class group of a CM-field over a totally real base field. Let k be a totally real number field and L be a CM-field such that L/k is finite and abelian. In this paper, we fix an odd prime number p, and study the p-component A_L of the ideal class group Cl_L, namely $A_L = \mathrm{Cl}_L \otimes \mathbb{Z}_p$. We put $R_L = \mathbb{Z}_p[\mathrm{Gal}(L/k)]$ and regard A_L as an R_L-module.

Let $\theta_{L/k}$ be the Stickelberger element defined by

$$\theta_{L/k} = \sum_{\sigma \in \mathrm{Gal}(L/k)} \zeta(0, \sigma)\sigma^{-1} \in \mathbb{Q}[\mathrm{Gal}(L/k)]$$

where $\zeta(s, \sigma) = \sum_{(\frac{L/k}{\mathfrak{a}})=\sigma} N(\mathfrak{a})^{-s}$ is the partial zeta function. We define $\mu_{p^\infty}(L)$ to be the group of roots of unity in L with order a power of p, and $I_L = \mathrm{Ann}_{R_L}(\mu_{p^\infty}(L))$ to be the annihilator ideal of $\mu_{p^\infty}(L)$ in R_L. The results in Deligne and Ribet [2] imply that $I_L\theta_{L/k} \subset R_L$. In this setting, Brumer's conjecture claims that

$$\text{(B)} \qquad I_L\theta_{L/k} \subset \mathrm{Ann}_{R_L}(A_L).$$

For a commutative ring R and a finitely presented R-module M, we denote by $\mathrm{Fitt}_R(M)$ the (initial) Fitting ideal of R (cf. Northcott [12] §3.1). In general, we have $\mathrm{Fitt}_R(M) \subset \mathrm{Ann}_R(M)$. As a sequel of the paper [8], we study in this paper the following two stronger properties (SB) and (DSB) than (B);

$$\text{(SB)} \qquad I_L\theta_{L/k} \subset \mathrm{Fitt}_{R_L}(A_L),$$

and

$$\text{(DSB)} \qquad I_L\theta_{L/k} \subset \mathrm{Fitt}_{R_L}((A_L)^\vee).$$

Here, $(A_L)^\vee$ is the Pontrjagin dual of A_L with cogredient Galois action, namely $\sigma \in \mathrm{Gal}(L/k)$ acts as $(\sigma f)(x) = f(\sigma x)$ for $f \in (A_L)^\vee$ and $x \in A_L$. In many cases, these two properties hold true. For example, if $k = \mathbb{Q}$, (SB) always holds true, which was proved in our previous paper [9]; if the μ-invariant of L vanishes and any prime above p does not split in L/L^+, (SB) holds by Nickel [11] Theorem 4; if $\mu_{p^\infty}(L)$ is cohomologically trivial, (DSB) holds by Greither [4]. (Nickel [11] Theorem 4 implies more, for example, it implies that (SB) holds true if all primes above p are tamely ramified in L/k and $L^{\mathrm{cl}} \not\subset (L^{\mathrm{cl}})^+(\mu_p)$ where L^{cl} denotes the normal closure of L over $\mathbb{Q}$.) But these two properties do not hold in general (see [5], [8]). In [5], some explicit numerical examples for which (SB) does not hold were given. In [8], (DSB) was studied but explicit numerical examples for which (DSB) does not hold were not given. In this paper, we give explicit numerical examples for which (DSB) does not hold, and also give explicit conditions under which (DSB) does not hold. Also, we give explicit examples for which neither (SB) nor (DSB) holds. While the first author studied (SB) and (DSB) in [8] using Iwasawa theoretic arguments, we study these problems in this paper by investigating finite and abelian extensions directly. Concerning the background and known results on these two problems, see [8] and [3]. For the function field case, see Popescu [13].

We are interested in the Teichmüller character component of A_L. So we assume that a primitive p-th root of unity is in L, and put $K = k(\mu_p)$, which is a subfield of L. Let K_∞/K (resp. L_∞/L) be the cyclotomic $\mathbb{Z}_p$-extension of K (resp. L). We assume that L/k is a finite and abelian extension, L/K is a p-extension and $L \cap K_\infty = K$. We denote by K^+ the maximal real subfield of K, and by L_n the n-th layer of L_∞/L (so $[L_n : L] = p^n$) for any integer $n \geq 0$. If $\mathrm{Gal}(L/K)$ is cyclic, (SB) and (DSB) are equivalent. In this paper, we consider the case that $\mathrm{Gal}(L/K)$ is *not cyclic*. In §1 we will prove the following theorem (we will prove in §1 a slightly more general Theorem 1.2).

Theorem 0.1 *We assume that no prime above p splits in K/K^+ (namely* (NTZ) *is satisfied, see the beginning of §1), and also that if a prime v splits in K/K^+, v is unramified in L/K (we call this property* (R)*, see the beginning of §1). Suppose also that $G = \mathrm{Gal}(L/K)$ is not cyclic. Then* (DSB) *does not hold for L_n/k for all $n \geq 0$. Namely, we have*

$$I_{L_n}\theta_{L_n/k} \not\subset \mathrm{Fitt}_{R_{L_n}}((A_{L_n})^\vee)$$

for all $n \geq 0$.

In §2 we will give an explicit numerical example L/k of Theorem 0.1 where $k = \mathbb{Q}(\sqrt{1901})$, $p = 3$, $K = k(\mu_3)$ and $L = K(\alpha, \beta)$ with $\alpha^3 - 84\alpha - 191 = 0$ and $\beta^3 - 57\beta - 68 = 0$. Then we know that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. For this L/k, we explicitly compute A_L, the Galois action on it, $\theta_{L/k}$ and also $\mathrm{Fitt}_{R_L}((A_L^-)^\vee)$ (for the minus part A_L^-, see the beginning of §1). We will see directly

$$\#\mu_{p^\infty}(L)\theta_{L/k} \notin \mathrm{Fitt}_{R_L}((A_L)^\vee)$$

from these computations for this example.

In §3 and §4 we study the case that L/k does not satisfy (NTZ). In §3 we prove Proposition 3.2 which says that if L/k satisfies some conditions, L/k satisfies neither (SB) nor (DSB). Using this Proposition 3.2, we will see in §3.2 that there is an explicit example L/k for which neither (SB) nor (DSB) holds. The example we give in §3.2 is $p = 3$, $k = \mathbb{Q}(\sqrt{69}, \sqrt{713})$, $K = k(\mu_3)$, and $L = K(\alpha, \beta)$ where $\alpha^3 - 6\alpha - 3 = 0$ and $\beta^3 - 6\beta - 1 = 0$. Then we know that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. For this L/k, neither (SB) nor (DSB) holds.

The condition of Proposition 3.2 is not easy to check. In §4 we will prove another theorem by which we can easily construct examples for which neither (SB) nor (DSB) holds.

Theorem 0.2 *Suppose that L/k satisfies the conditions of §4.1. Then neither* (SB) *nor* (DSB) *holds for L_n/k for any integer $n \geq 1$. Namely, we have both*

$$I_{L_n}\theta_{L_n/k} \not\subset \mathrm{Fitt}_{R_{L_n}}(A_{L_n}) \quad \textit{and} \quad I_{L_n}\theta_{L_n/k} \not\subset \mathrm{Fitt}_{R_{L_n}}((A_{L_n})^\vee)$$

for all $n \geq 1$.

We give in §4.3 a numerical example for which Theorem 0.2 can be applied.

We would like to thank heartily X.-F. Roblot who kindly helped us to compute the numerical examples in this paper. Especially, we learned much from him on the computation of the L-values and of the Galois action on the class group of a number field. The first author would like to thank C. Greither for several significant discussions with him.

Erratum for the paper [8]: The first named author would like to make a correction concerning his previous paper [8]. In page 426 line 21, the correct formula is $\hat{H}^{-1}(G, \mathcal{X}^\omega_{L_\infty}) = \hat{H}^0(G, A^\omega_{L_\infty})^\vee = (\bigwedge^2 G)(1)$.

Notation
For any positive integer n, μ_{p^n} denotes the group of p^n-th roots of unity. For a group G and a G-module M, we denote by M^G the G-invariant part of M (the maximal subgroup of M on which G acts trivially), and by M_G the G-coinvariant of M (the maximal quotient of M on which G acts trivially).

1 The case that there is no trivial zero

In this section, we assume the conditions before Theorem 0.1. Namely, $K = k(\mu_p)$, L/k is a finite and abelian extension, $K \subset L$, L/K is a p-extension, and $L \cap K_\infty = K$. Suppose that K^+ is the maximal real subfield of K. We take $n \in \mathbb{Z}_{\geq 0}$ and consider the n-th layer L_n of the cyclotomic $\mathbb{Z}_p$-extension L_∞/L. We put $R_{L_n} = \mathbb{Z}_p[\mathrm{Gal}(L_n/k)]$. Any R_{L_n}-module M is decomposed into $M = M^+ \oplus M^-$ where $M^\pm = \{x \in M \mid \rho(x) = \pm x\}$ for the complex conjugation $\rho \in \mathrm{Gal}(L_n/k)$. Let ω be the Teichmüller character which gives the action of $\mathrm{Gal}(K/k)$ on μ_p. For any $\mathbb{Z}_p[\mathrm{Gal}(K/k)]$-module M, we define M^ω to be

$$\begin{aligned} M^\omega &= M \otimes_{R_K} R_K/\langle\{\sigma - \omega(\sigma) \mid \sigma \in \mathrm{Gal}(K/k)\}\rangle \\ &\simeq \{x \in M \mid \sigma(x) = \omega(\sigma)x \text{ for all } \sigma \in \mathrm{Gal}(K/k)\}. \end{aligned}$$

Note that $M \mapsto M^\omega$ is an exact functor.

For any $n \in \mathbb{Z}_{\geq 0}$, we call the following condition $(\mathrm{R})_n$;

$(\mathrm{R})_n$ Any prime which splits in K/K^+ is unramified in L_n/K.

We simply write (R) for the condition $(\mathrm{R})_0$.

We also consider the following condition (no trivial zero);

(NTZ) No prime above p splits in K/K^+.

Of course, if n is sufficiently large, the condition $(\mathrm{R})_n$ implies (NTZ). Also, if we assume (NTZ) and (R), then we get $(\mathrm{R})_n$ for all $n \geq 0$.

The following is a key Proposition of this section.

Proposition 1.1 *We assume that L_n/k satisfies $(\mathrm{R})_n$ and $G = \mathrm{Gal}(L/K)$ is not cyclic. Then we have*

$$\#(A_{L_n}^-)^{\mathrm{Gal}(L_n/K)} > \#A_K^-$$

and

$$\#(A_{L_n}^\omega)^{\mathrm{Gal}(L_n/K)} > \#A_K^\omega.$$

Proof. We put $\Gamma_n = \mathrm{Gal}(K_n/K)$ and $G_n = \mathrm{Gal}(L_n/K)$. Then $G_n = G \times \Gamma_n$ by our assumption.

We denote by E_{L_n} the unit group and by $\mathcal{C}_{L_n}$ the idele class group of L_n. For any prime w of L_n, we denote by $L_{n,w}$ the completion of L_n at w, and by $E_{L_{n,w}}$ the unit group of $L_{n,w}$ if w is a finite prime, and $E_{L_{n,w}} = L_{n,w}^\times$ if w is an infinite prime. By Lemma 5.1 (2) in [7] (cf. also [8] §1), an exact sequence $0 \longrightarrow E_{L_n} \longrightarrow \prod_w E_{L_{n,w}} \longrightarrow \mathcal{C}_{L_n} \longrightarrow \mathrm{Cl}_{L_n} \longrightarrow 0$ yields an exact sequence

$$\begin{aligned} &\hat{H}^0(G_n, E_{L_n})^- \longrightarrow (\bigoplus_v \hat{H}^0(G_{n,v}, E_{L_{n,w}}))^- \longrightarrow \hat{H}^{-1}(G_n, A_{L_n})^- \\ &\longrightarrow H^1(G_n, E_{L_n})^- \longrightarrow (\bigoplus_v H^1(G_{n,v}, E_{L_{n,w}}))^- \longrightarrow \hat{H}^0(G_n, A_{L_n})^- \\ &\longrightarrow H^2(G_n, E_{L_n})^- \longrightarrow (\bigoplus_v H^2(G_{n,v}, E_{L_{n,w}}))^- \end{aligned}$$

where v runs over all finite primes of K, for each v we choose a prime w of L_n above v, and $G_{n,v} = \mathrm{Gal}(L_{n,w}/K_v)$ is the decomposition group of G_n at v. We know that $\hat{H}^0(G_{n,v}, E_{L_{n,w}})$ is isomorphic to the inertia group of $G_{n,v}$ by local class field theory. The exact sequence $0 \longrightarrow E_{L_{n,w}} \longrightarrow L_{n,w}^\times \longrightarrow \mathbb{Z} \longrightarrow 0$ implies that $H^1(G_{n,v}, E_{L_{n,w}}) = \mathbb{Z}/e_v\mathbb{Z}$ where e_v is the ramification index of v

in L_n/K, and that $H^2(G_{n,v}, E_{L_{n,w}})$ is a subgroup of the Brauer group of K_v. We denote by $\mathfrak{l}$ the prime of K^+ below v. If $\mathfrak{l}$ does not split in K/K^+, the complex conjugation ρ acts trivially on $\hat{H}^q(G_{n,v}, E_{L_{n,w}})$ ($q = 0, 1, 2$) by the above description, so ρ acts trivially on $\bigoplus_{v|\mathfrak{l}} \hat{H}^q(G_{n,v}, E_{L_{n,w}})$. Hence we have $(\bigoplus_{v|\mathfrak{l}} \hat{H}^q(G_{n,v}, E_{L_{n,w}}))^- = 0$. If $\mathfrak{l}$ splits in K/K^+, v is unramified in L_n/K by our assumption $(\mathrm{R})_n$. Therefore, we have $H^q(G_{n,v}, E_{L_{n,w}}) = 0$ ($q = 0, 1, 2$; see [14] Chap.XII §3 for the case $q = 2$). Thus, in any case we obtain

$$(1.1.1) \qquad (\bigoplus_v \hat{H}^q(G_{n,v}, E_{L_{n,w}}))^- = 0 \quad \text{for } q = 0,\ 1,\ 2.$$

Suppose that $\#\mu_{p^\infty}(L) = p^c$. Then we know $L_n = L(\mu_{p^{n+c}})$ and $K_n = K(\mu_{p^{n+c}})$. We will compute $H^q(G_n, E_{L_n})^- = H^q(G_n, E_{L_n}^-) = H^q(G_n, \mu_{p^{n+c}})$. As is well-known (for example, see Lemma 13.27 in [16]), we have $H^1(\Gamma_n, \mu_{p^{n+c}}) = 0$. Since Γ_n is cyclic, we have $H^q(\Gamma_n, \mu_{p^{n+c}}) = 0$ for any $q \geq 1$. This implies that

$$H^q(G_n, \mu_{p^{n+c}}) = H^q(G_n/\Gamma_n, H^0(\Gamma_n, \mu_{p^{n+c}})) = H^q(G, \mu_{p^c})$$

by the Serre-Hochschild spectral sequence. Therefore, we obtain

$$(1.1.2) \qquad H^q(G_n, E_{L_n})^- = H^q(G, \mu_{p^c}) \simeq H^q(G, \mathbb{Z}/p^c\mathbb{Z}).$$

Let $i_{L_n/K} : A_K^- \longrightarrow A_{L_n}^-$ be the natural map. Since the kernel of $i_{L_n/K}$ is isomorphic to the kernel of $H^1(G_n, E_{L_n})^- \longrightarrow (\bigoplus_v H^1(G_{n,v}, E_{L_{n,w}}))^-$ (cf. Remark 2.2 in [6]), considering (1.1.1), we have an isomorphism $\mathrm{Ker}(i_{L_n/K}) \simeq H^1(G_n, E_{L_n})^- \simeq H^1(G, \mathbb{Z}/p^c\mathbb{Z})$. Therefore, we have

$$(1.1.3) \qquad \#\,\mathrm{Ker}(i_{L_n/K} : A_K^- \longrightarrow (A_{L_n}^-)^{G_n}) = \#(G/G^{p^c}).$$

On the other hand, the norm map $A_{L_n}^- \longrightarrow A_K^-$ is surjective by Lemma 5.1 (1) in [7] (cf. Lemma 1.4 below). Therefore, the image of $i_{L_n/K}$ coincides with the image of the multiplication by $N_{G_n} = \Sigma_{\sigma \in G_n} \sigma$ on $A_{L_n}^-$. Thus, we have an exact sequence

$$0 \longrightarrow H^1(G_n, E_{L_n})^- \longrightarrow A_K^- \longrightarrow (A_{L_n}^-)^{G_n} \longrightarrow \hat{H}^0(G_n, A_{L_n}^-) \longrightarrow 0.$$

Using (1.1.1) and (1.1.2), we get

$$\begin{aligned} \mathrm{Coker}(i_{L_n/K} : A_K^- \longrightarrow (A_{L_n}^-)^{G_n}) &\simeq \hat{H}^0(G_n, A_{L_n})^- \simeq H^2(G_n, E_{L_n})^- \\ &\simeq H^2(G, \mathbb{Z}/p^c\mathbb{Z}). \end{aligned}$$

Considering an exact sequence

$$0 \longrightarrow \mathbb{Z}/p^c\mathbb{Z} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^c} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

and taking cohomology, we get an exact sequence

$$0 \longrightarrow H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)/p^c \longrightarrow H^2(G, \mathbb{Z}/p^c\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)[p^c] \longrightarrow 0$$

where $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)[p^c]$ is the kernel of the multiplication by p^c on $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)$. Since $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)$ is isomorphic to $\mathrm{Hom}(\bigwedge^2 G, \mathbb{Q}_p/\mathbb{Z}_p)$ by the universal coefficient sequence (see page 60 in Chap. III in [1] and Theorem 6.4 (iii) in Chap.

V in [1], cf. also Lemma 1.3 in [8]), we get $H^2(G,\mathbb{Q}_p/\mathbb{Z}_p)[p^c] \neq 0$ from our assumption that G is not cyclic. Since $H^1(G,\mathbb{Q}_p/\mathbb{Z}_p)$ is isomorphic to G as an abelian group, $H^1(G,\mathbb{Q}_p/\mathbb{Z}_p)/p^c$ is isomorphic to G/G^{p^c} as an abelian group. Therefore, we obtain

$$\# H^2(G,\mathbb{Z}/p^c\mathbb{Z}) > \# H^1(G,\mathbb{Q}_p/\mathbb{Z}_p)/p^c = \# G/G^{p^c}.$$

This implies that

$$\# \operatorname{Coker}(i_{L_n/K} : A_K^- \longrightarrow (A_{L_n}^-)^{G_n}) > \#(G/G^{p^c}). \tag{1.1.4}$$

It follows from (1.1.3) and (1.1.4) that $\# A_K^- < \#(A_{L_n}^-)^{G_n}$.

Since $H^1(G_n, E_{L_n})^\omega = H^1(G,\mu_{p^c}) \simeq H^1(G,\mathbb{Z}/p^c\mathbb{Z})$ and

$$\hat{H}^0(G_n, A_{L_n})^\omega \simeq H^2(G_n, E_{L_n})^\omega \simeq H^2(G,\mu_{p^c}) \simeq H^2(G,\mathbb{Z}/p^c\mathbb{Z}),$$

by the same method as above, we obtain an exact sequence

$$0 \longrightarrow H^1(G,\mathbb{Z}/p^c\mathbb{Z}) \longrightarrow A_K^\omega \longrightarrow (A_{L_n}^\omega)^{G_n} \longrightarrow H^2(G,\mathbb{Z}/p^c\mathbb{Z}) \longrightarrow 0. \tag{1.1.5}$$

Since

$$\# H^1(G,\mathbb{Z}/p^c\mathbb{Z}) = \# G/G^{p^c} < \# H^2(G,\mathbb{Z}/p^c\mathbb{Z}),$$

we obtain $\# A_K^\omega < \#(A_{L_n}^\omega)^{G_n}$. This completes the proof of Proposition 1.1.

As in the proof of Proposition 1.1, we suppose that $\#\mu_{p^\infty}(L) = \#\mu_{p^\infty}(K) = p^c$. Let $\kappa : \mathrm{Gal}(L_\infty/k) \longrightarrow \mathbb{Z}_p^\times$ be the cyclotomic character and γ be a generator of $\mathrm{Gal}(L_\infty/L) = \mathrm{Gal}(K_\infty/K)$. We fix this γ throughout this paper. Since $\#\mu_{p^\infty}(L) = p^c$, we know that $\mathrm{ord}_p(1-\kappa(\gamma)) = c$. We also regard γ as a generator of $\mathrm{Gal}(L_n/L) = \mathrm{Gal}(K_n/K)$. For $\theta_{K/k}$ and $\theta_{L_n/k}$, we have $p^c\theta_{K/k} \in R_K = \mathbb{Z}_p[\mathrm{Gal}(K/k)]$, $p^{n+c}\theta_{L_n/k} \in R_{L_n} = \mathbb{Z}_p[\mathrm{Gal}(L_n/k)]$, $(\gamma - \kappa(\gamma))\theta_{L_n/k} \in R_{L_n}$.

The Teichmüller character ω induces the ring homomorphism $R_K \longrightarrow R_K^\omega = \mathbb{Z}_p$ (resp. $R_{L_n} \longrightarrow R_{L_n}^\omega = \mathbb{Z}_p[\mathrm{Gal}(L_n/K)]$) such that $\sigma \mapsto \omega(\sigma)$ for all $\sigma \in \mathrm{Gal}(K/k)$ (note that $\mathrm{Gal}(L_n/k) = \mathrm{Gal}(L_n/K) \times \mathrm{Gal}(K/k)$). For an element $x \in R_K$ (resp. $x \in R_{L_n}$), we denote the image of x by x^ω.

Theorem 1.2 *We assume that L_n/k satisfies $(\mathrm{R})_n$, $G = \mathrm{Gal}(L/K)$ is not cyclic, and that $\mathrm{Fitt}_{\mathbb{Z}_p}(A_K^\omega) = (p^c\theta_{K/k}^\omega)$ where $p^c = \#\mu_{p^\infty}(K)$. We have*

$$(\gamma - \kappa(\gamma))\theta_{L_n/k} \notin \mathrm{Fitt}_{R_{L_n}}((A_{L_n})^\vee).$$

(If $n = 0$, we have $p^c\theta_{L/k} \notin \mathrm{Fitt}_{R_L}((A_L)^\vee)$.) In particular, we have

$$I_{L_n}\theta_{L_n/k} \not\subset \mathrm{Fitt}_{R_{L_n}}((A_{L_n})^\vee).$$

Remark 1.3 If $[K:k] = 2$ (for example, if $p = 3$), the class number formula implies $\mathrm{Fitt}_{\mathbb{Z}_p}(A_K^\omega) = (p^c\theta_{K/k}^\omega)$. In fact, by definition, we have $\theta_{K/k}^\omega = L(0,\omega^{-1})$. Since $[K:k] = 2$, we get $A_K^\omega = A_K^-$. So we obtain

$$\mathrm{Fitt}_{\mathbb{Z}_p}(A_K^\omega) = \mathrm{Fitt}_{\mathbb{Z}_p}(A_K^-) = (\# A_K^-) = (p^c L(0,\omega^{-1})) = (p^c\theta_{K/k}^\omega)$$

by the class number formula.

We often use the following lemmas in this paper.

Lemma 1.4 *Let L/K be an abelian p-extension of CM-fields. We put $G = \mathrm{Gal}(L/K)$. For a prime v of K, we denote by $I_v(L/K)$ the inertia group of v in G. Then we have an exact sequence*

$$\mu_{p^\infty}(K) \xrightarrow{a} (\bigoplus_v I_v(L/K))^- \longrightarrow (A_L^-)_G \xrightarrow{N} A_K^- \longrightarrow 0$$

where a is induced by the reciprocity map of local class field theory, v runs over all finite primes of K, and N is induced by the norm map.

Proof. This is Proposition 5.2 in [7].

In general, for an abelian extension L/k and a subfield K such that $k \subset K \subset L$, we define a ring homomorphism

$$c_{L/K} : \mathbb{Q}[\mathrm{Gal}(L/k)] \longrightarrow \mathbb{Q}[\mathrm{Gal}(K/k)]$$

by the restriction $\sigma \mapsto \sigma_{|K}$ for $\sigma \in \mathrm{Gal}(L/k)$. We will use the same notation $c_{L/K}$ for any group rings such as $R_L = \mathbb{Z}_p[\mathrm{Gal}(L/k)]$, $\mathbb{Z}_p[[\mathrm{Gal}(L/k)]]$ (in case L/k is infinite), etc.

Lemma 1.5 *Suppose that L/k is a finite and abelian extension and $k \subset K \subset L$. We denote by S_L (resp. S_K) the set of finite primes of k ramifying in L/k (resp. K/k). Then we have*

$$c_{L/K}(\theta_{L/k}) = (\prod_{v \in S_L \setminus S_K} (1 - \varphi_v^{-1}))\theta_{K/k}$$

where φ_v is the Frobenius of v in $\mathrm{Gal}(K/k)$.

Proof. This is well-known, and follows from the expression of $\theta_{L/k}(s)$ by the Euler product (see Tate [15] p.86 and Lemma 2.1 in [7]).

Proof of Theorem 1.2. Assume that $(\gamma - \kappa(\gamma))\theta_{L_n/k}$ is in $\mathrm{Fitt}_{R_{L_n}}((A_{L_n})^\vee)$. Let $c_{L_n/K} : R_{L_n} \longrightarrow R_K$ be the ring homomorphism defined by the restriction. Then we have

$$c_{L_n/K}((\gamma - \kappa(\gamma))\theta_{L_n/k}) \in \mathrm{Fitt}_{R_K}(((A_{L_n})^\vee)_{G_n})$$

where $G_n = \mathrm{Gal}(L_n/K)$. This implies that

$$c_{L_n/K}((\gamma - \kappa(\gamma))\theta_{L_n/k})^\omega \in \mathrm{Fitt}_{\mathbb{Z}_p}(((A_{L_n}^\omega)^\vee)_{G_n}).$$

If a prime $\mathfrak{l}$ of k is ramified in L_n/K, the primes of K^+ above $\mathfrak{l}$ do not split in K/K^+ by our assumption $(\mathrm{R})_n$, so $\omega(\varphi_{\mathfrak{l}}) \neq 1$. This implies that $c_{L_n/K}(\theta_{L_n/k}^\omega) = u\theta_{K/k}^\omega$ for some unit $u \in \mathbb{Z}_p^\times$ by Lemma 1.5. Since $\#\mu_{p^\infty}(L) = p^c$, we know that p^c divides $\kappa(\gamma) - 1$ but p^{c+1} does not. Therefore, we get

$$(c_{L_n/K}((\gamma - \kappa(\gamma))\theta_{L_n/k})^\omega) = (p^c\theta_{K/k}^\omega)$$

as ideals of $\mathbb{Z}_p$. Hence we obtain

$$p^c\theta^\omega_{K/k} \in \mathrm{Fitt}_{\mathbb{Z}_p}((((A^\omega_{L_n})^\vee)_{G_n}) = \mathrm{Fitt}_{\mathbb{Z}_p}((((A^\omega_{L_n})^{G_n})^\vee) = \mathrm{Fitt}_{\mathbb{Z}_p}((A^\omega_{L_n})^{G_n}).$$

Here, the last equality holds because $\mathrm{Fitt}_{\mathbb{Z}_p}(M) = (\#M)$ for any finite $\mathbb{Z}_p$-module M.

Since we are assuming $\mathrm{Fitt}_{\mathbb{Z}_p}(A^\omega_K) = (p^c\theta^\omega_{K/k})$, we get

$$\mathrm{Fitt}_{\mathbb{Z}_p}(A^\omega_K) \subset \mathrm{Fitt}_{\mathbb{Z}_p}((A^\omega_{L_n})^{G_n}),$$

which implies that $\#A^\omega_K \geq \#(A^\omega_{L_n})^{G_n}$. This contradicts Proposition 1.1. Thus, we get the conclusion of Theorem 1.2.

Proof of Theorem 0.1. Since (NTZ) and (R) imply $(\mathrm{R})_n$ for all $n \geq 0$, what we have to show is $\mathrm{Fitt}_{\mathbb{Z}_p}(A^\omega_K) = (p^c\theta^\omega_{K/k})$ by Theorem 1.2. We define the Iwasawa module X_{K_∞} by

$$X_{K_\infty} = \varprojlim A_{K_n}$$

where the limit is taken with respect to the norm maps. Then by our assumption (NTZ), we have an isomorphism $(X^-_{K_\infty})_{\mathrm{Gal}(K_\infty/K)} \simeq A^-_K$ by Lemma 1.4.

We put $\Lambda_{K_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/k)]] = \varprojlim R_{K_n}$. Similarly as in the finite level, we consider the ring homomorphism $\Lambda_{K_\infty} \longrightarrow \Lambda^\omega_{K_\infty} \simeq \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$ which is induced by ω, and we denote the image of $x \in \Lambda_{K_\infty}$ by $x^\omega \in \Lambda^\omega_{K_\infty}$. Let $((\gamma - \kappa(\gamma))\theta_{K_\infty/k})^\omega \in \Lambda^\omega_{K_\infty}$ be the projective limit of $((\gamma - \kappa(\gamma))\theta_{K_n/k})^\omega \in R^\omega_{K_n}$ (which is the numerator of the p-adic L-function of Deligne and Ribet). Then the main conjecture proved by Wiles [17] can be stated as

$$\mathrm{Fitt}_{\Lambda^\omega_{K_\infty}}(X^\omega_{K_\infty}) = (((\gamma - \kappa(\gamma))\theta_{K_\infty/k})^\omega)$$

because $X^\omega_{K_\infty}$ contains no nontrivial finite submodule and hence its Fitting ideal coincides with its characteristic ideal. Let $c_{K_\infty/K} : \Lambda_{K_\infty} \longrightarrow R_K$ be the restriction map. By the condition (NTZ), we get

$$c_{K_\infty/K}(((\gamma - \kappa(\gamma))\theta_{K_\infty/k})^\omega) = u((1 - \kappa(\gamma))\theta_{K/k})^\omega = u'p^c\theta^\omega_{K/k}$$

for some $u,\ u' \in \mathbb{Z}_p^\times$ by Lemma 1.5. From the isomorphism $(X^\omega_{K_\infty})_{\mathrm{Gal}(K_\infty/K)} \simeq A^\omega_K$, it follows that

$$\mathrm{Fitt}_{\mathbb{Z}_p}(A^\omega_K) = (p^c\theta^\omega_{K/k}).$$

2 A numerical example

In this section, we will give an example of a number field which does not satisfy (DSB). We will give an extension L/k explicitly, and compute the Stickelberger element of L/k and the Fitting ideals of A_L and $A^\vee_L$. We will see from these computations that (SB) holds for this L/k but (DSB) does not.

We take $p = 3$ and $k = \mathbb{Q}(\sqrt{1901})$. Then $p = 3$ is inert in k. Let F_α be the minimal splitting field of $X^3 - 84X - 191$ over $\mathbb{Q}$. We know that F_α contains k and F_α/k is a cubic cyclic extension which is unramified everywhere. We define F_β to be the minimal splitting field of $X^3 - 57X - 68$. Then we can check that F_β/k is a cubic cyclic extension of k which is unramified outside 3 and that the prime of k above 3 is totally ramified in F_β/k. Put $F = F_\alpha F_\beta$, $L = F(\mu_3)$ and $K = k(\mu_3)$. Then L/k satisfies all the conditions in Theorem 0.1. In fact, $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(F/k) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is not cyclic, and both conditions (NTZ) and (R) are satisfied because (3) is ramified in K/k and L/K is unramified outside (3). We also have $L \cap K_\infty = K$. (Theoretically the existence of F can be checked by class field theory. For a modulus $\mathfrak{m} = (3)^2$ of k, the ray class group of k modulo $\mathfrak{m}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$. So the class field theory tells us that there is an abelian extension F/k whose Galois group is $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and which is unramified outside 3, and $F \cap k_\infty = k$.)

Let σ (resp. τ) be a generator of $\mathrm{Gal}(F_\alpha/k)$ (resp. $\mathrm{Gal}(F_\beta/k)$). We can write the Stickelberger element for L/k as

$$\theta^-_{L/k} = \sum_{\substack{0\le i\le 2\\ 0\le j\le 2}} a_{ij}\sigma^i\tau^j \in \mathbb{Q}[G] \simeq \mathbb{Q}[\mathrm{Gal}(L/k)]^-.$$

Let χ be the unique quadratic character of $\mathrm{Gal}(K/k)$. We define characters φ_i of $\mathrm{Gal}(F_\alpha/k)$ and ψ_j of $\mathrm{Gal}(F_\beta/k)$ by

$$\varphi_i(\sigma) = \zeta_3^i \quad\text{and}\quad \psi_j(\tau) = \zeta_3^j \text{ for } 0 \le i,\ j \le 2$$

where ζ_3 is a primitive 3-rd root of unity. Then all the odd characters of $\mathrm{Gal}(L/k)$ can be written as $\Psi_{ij} = \chi\varphi_i\psi_j$. The element $\theta^-_{L/k}$ is characterized by the L-values;

$$\text{(2.1)} \qquad \Psi_{ij}(\theta^-_{L/k}) = L_{\{3\}}(0,\ \Psi_{ij}^{-1}) \ \text{ for all } \ i,j \ \text{ such that } \ 0 \le i,\ j \le 2$$

where $L_{\{3\}}(s,\ \Psi_{ij})$ is the L-function obtained by removing the Euler factors above 3, which is $(1 - \Psi_{ij}(3))$ in this example. In our case, $L_{\{3\}}(s,\ \Psi_{ij})$'s coincide with the usual L-functions $L(s,\ \Psi_{ij})$'s since (3) is ramified in any subfield of L corresponding to Ψ_{ij}. Using Pari/GP, we calculated the values of these L-functions at $s = 0$. The following table gives these values.

$(i,\ j)$	$(0,\ 0)$	$(1,\ 0)$	$(2,\ 0)$	$(0,\ 1)$	$(1,\ 1)$	$(2,\ 1)$	$(0,\ 2)$	$(1,\ 2)$	$(2,\ 2)$
$L(0,\ \Psi_{ij})$	18	24	24	60	96	24	60	24	96

This implies that

$$\theta^-_{L/k} = \frac{142}{3} - \frac{2}{3}\sigma - \frac{2}{3}\sigma^2 - \frac{38}{3}\tau - \frac{38}{3}\sigma\tau + \frac{34}{3}\sigma^2\tau - \frac{38}{3}\tau^2 + \frac{34}{3}\sigma\tau^2 - \frac{38}{3}\sigma^2\tau^2.$$

Now we identify $\mathbb{Z}_p[G]$ with $\mathbb{Z}_p[S,\ T]/((S+1)^3 - 1,\ (T+1)^3 - 1)$ by sending σ and τ to $S + 1$ and $T + 1$, respectively. In this ring, we have equalities $S^3 = -3S - 3S^2$, $T^3 = -3T - 3T^2$. Using S and T, we can rewrite $\theta^-_{L/k}$ as

$$\theta^-_{L/k} = 18 - 6S - 2S^2 - 42T - 18ST - 14S^2T - 14T^2 - 14ST^2 - \frac{38}{3}S^2T^2.$$

Since $I_L = (3,\ S,\ T)$, $I_L\theta^-_{L/k}$ is generated by the following three elements;

$$3\theta^-_{L/k} = 2(3^3 - 3^2S - 3S^2 - 7\cdot 3^2T - 3^3ST - 7\cdot 3S^2T - 7\cdot 3T^2 - 7\cdot 3ST^2 - 19S^2T^2),$$

$$S\theta^-_{L/k} = 8(3S + 3S^2T + 3ST^2 + 3S^2T^2),$$

and

$$T\theta^-_{L/k} = 4(5 \cdot 3T + 3^2S^2T + 2 \cdot 3ST^2 + 2 \cdot 3S^2T^2).$$

Next, we proceed to the ideal class groups. By the computation using Pari/GP, we have isomorphisms

$$A^-_K \simeq \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

and

$$A^-_L \simeq \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

as abelian groups. Therefore, we also have

$$(A^-_L)^\vee \simeq \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Moreover, using Pari/GP, we can compute the Galois action on A^-_L, namely how σ and τ act on this group. Pari/GP computes explicitly the basis of the ideal class group, which is represented by a basis of the ring of integers of L, though we do not write down here this representation. Let $\{g_1, \ldots, g_8\}$ be the basis of A^-_L corresponding to the above isomorphism, which was computed by Pari/GP. We denote by M_σ (resp. M_τ) the matrix corresponding to the action of σ (resp. τ) with respect to the above basis. The result of the computation is

$$M_\sigma = \begin{pmatrix} 1 & 0 & 0 & 0 & 9 & 9 & -9 & 9 \\ 3 & 4 & -3 & 3 & -3 & 3 & 3 & -3 \\ -1 & 1 & -1 & -1 & 0 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & -1 & 1 & 0 & -1 & 1 \\ -1 & 0 & 1 & 0 & 0 & -1 & -1 & -1 \\ 1 & -1 & 0 & 0 & 0 & -1 & 1 & 1 \\ -1 & 1 & 1 & 0 & 0 & 1 & -1 & 0 \end{pmatrix}$$

and

$$M_\tau = \begin{pmatrix} 1 & 0 & 9 & -9 & -9 & 0 & 0 & -9 \\ -3 & 1 & 3 & 0 & 0 & -3 & 0 & 3 \\ -1 & 1 & -1 & 0 & -1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & -1 & 1 & 1 & 0 & 0 \\ -1 & 1 & -1 & -1 & 1 & 1 & 0 & 0 \\ 1 & -1 & -1 & -1 & -1 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

This means that $\sigma(g_1) = g_1 + 3g_2 - g_3 + g_4 - g_6 + g_7 - g_8$, for example.

Thus, the transpose of a relation matrix of A_L^- is

$$\begin{pmatrix}
\sigma-1 & -3 & 1 & -1 & 0 & 1 & -1 & 1 \\
0 & \sigma-4 & -1 & 1 & 0 & 0 & 1 & -1 \\
0 & 3 & \sigma+1 & 1 & 1 & -1 & 0 & -1 \\
0 & -3 & 1 & \sigma & 1 & 0 & 0 & 0 \\
-9 & 3 & 0 & 0 & \sigma-1 & 0 & 0 & 0 \\
-9 & -3 & 1 & 0 & 0 & \sigma+1 & 1 & -1 \\
9 & -3 & 0 & 1 & 1 & 1 & \sigma-1 & 1 \\
-9 & 3 & 1 & -1 & -1 & 1 & -1 & \sigma \\
\tau-1 & 3 & 1 & 1 & -1 & 1 & -1 & 0 \\
0 & \tau-1 & -1 & 1 & 1 & -1 & 1 & 0 \\
-9 & -3 & \tau+1 & 0 & 0 & 1 & 1 & 1 \\
9 & 0 & 0 & \tau & 1 & 1 & 1 & 1 \\
9 & 0 & 1 & 0 & \tau-1 & -1 & 1 & -1 \\
0 & 3 & -1 & -1 & -1 & \tau-1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \tau-1 & 0 \\
9 & -3 & 0 & 0 & 0 & 0 & 1 & \tau-1 \\
27 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 9 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 3
\end{pmatrix}.$$

Here, each row vector represents a relation of A_L^-. Substituting $S+1$ and $T+1$ for σ and τ respectively, and applying the elementary row and column operations, we can reduce the above matrix to

$$\begin{pmatrix}
3S & 0 \\
9 & -S^2+ST-T^2 \\
S+T & S+S^2-T-ST-2S^2T+T^2 \\
ST & 3+S^2+2S^2T-T^2 \\
S^2 & 6-ST-2S^2T+T^2 \\
0 & 3S \\
0 & 3T \\
0 & 9 \\
0 & -S^2T+ST^2 \\
0 & S^2T^2
\end{pmatrix}.$$

Here, extra zero vectors and identity matrices which were appeared in the process of the reduction were removed. We know from this calculation that A_L^- is generated by two elements as an R_L^--module and that these two generators have 10 relations in A_L^-. Taking all the 2×2 minors in the above matrix and carrying out tedious computation, we obtain

$$\mathrm{Fitt}_{R_L^-}(A_L^-) = (81,\ 3S,\ 3T,\ 27-S^2T^2).$$

So we get

$$3\theta^-_{L/k} \equiv 2(27 - 19S^2T^2) \equiv -36S^2T^2 \equiv 0 \quad \left(\mathrm{mod}\ \mathrm{Fitt}_{R_L^-}(A_L^-)\right),$$

and also

$$S\theta^-_{L/k} \equiv T\theta^-_{L/k} \equiv 0 \quad \left(\mathrm{mod}\ \mathrm{Fitt}_{R_L^-}(A_L^-)\right).$$

Therefore, we conclude that

$$I_L\theta^-_{L/k} \subset \mathrm{Fitt}_{R_L^-}(A_L^-)$$

in this case. In particular, $\#\mu_{p^\infty}(L)\theta^-_{L/k} \in \mathrm{Fitt}_{R_L^-}(A_L^-)$ holds.

Note that we also have numerically checked

$$\mathrm{Fitt}_{\mathbb{Z}_p}((A_L^-)_G) = (27) = \mathrm{Fitt}_{\mathbb{Z}_p}(A_K^-).$$

This corresponds to the fact that the norm map induces an isomorphism

$$(A_L^-)_G \xrightarrow{\simeq} A_K^-.$$

Next we will calculate the Fitting ideal of the dual. Let $\{f_1, \ldots, f_8\}$ be the dual basis of $(A_L^-)^\vee$ determined by $\{g_1, \ldots, g_8\}$. Namely, $f_1, \ldots, f_8$ are homomorphisms from A_L^- to $\mathbb{Q}/\mathbb{Z}$ satisfying

$$f_1(g_1) = \frac{1}{27},\ f_1(g_j) = 0\ (j \neq 1),$$
$$f_2(g_2) = \frac{1}{9},\quad f_2(g_j) = 0\ (j \neq 2),$$

and for $3 \leq i \leq 8$,

$$f_i(g_i) = \frac{1}{3},\quad f_i(g_j) = 0\ (j \neq i).$$

Note that any element $f \in (A_L^-)^\vee$ can be written as

$$f = 27f(g_1)f_1 + 9f(g_2)f_2 + 3f(g_3)f_3 + \cdots + 3f(g_8)f_8.$$

Let $\widetilde{M_\sigma}$ (resp. $\widetilde{M_\tau}$) be the matrix representing the action of σ (resp. τ) on $(A_L^-)^\vee$ corresponding to the dual basis $\{f_1, \ldots, f_8\}$. Recall that $(A_L^-)^\vee$ have the cogredient Galois action. We have

$$\widetilde{M_\sigma} = \begin{pmatrix} 1 & 9 & -9 & 9 & 0 & -9 & 9 & -9 \\ 0 & 4 & 3 & -3 & 0 & 0 & -3 & 3 \\ 0 & -1 & -1 & -1 & -1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & -1 & -1 & 1 \\ -1 & 1 & 0 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 \end{pmatrix}$$

and

$$\widetilde{M}_\tau = \begin{pmatrix} 1 & -9 & -9 & -9 & 9 & -9 & 9 & 0 \\ 0 & 1 & 3 & -3 & -3 & 3 & -3 & 0 \\ 1 & 1 & -1 & 0 & 0 & -1 & -1 & -1 \\ -1 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ -1 & 0 & -1 & 0 & 1 & 1 & -1 & 1 \\ 0 & -1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 \end{pmatrix}.$$

Then the transpose of a relation matrix of $(A_L^-)^\vee$ is

$$\begin{pmatrix} \sigma-1 & 0 & 0 & 0 & -1 & -1 & 1 & -1 \\ -9 & \sigma-4 & 1 & -1 & 1 & -1 & -1 & 1 \\ 9 & -3 & \sigma+1 & 1 & 0 & 1 & 0 & 1 \\ -9 & 3 & 1 & \sigma & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 & \sigma-1 & 0 & 1 & -1 \\ 9 & 0 & -1 & 0 & 0 & \sigma+1 & 1 & 1 \\ -9 & 3 & 0 & 0 & 0 & 1 & \sigma-1 & -1 \\ 9 & -3 & -1 & 0 & 0 & -1 & 1 & \sigma \\ \tau-1 & 0 & -1 & 1 & 1 & 0 & 0 & 1 \\ 9 & \tau-1 & -1 & 0 & 0 & 1 & 0 & -1 \\ 9 & -3 & \tau+1 & 0 & 1 & -1 & 0 & 0 \\ 9 & 3 & 0 & \tau & 0 & -1 & 0 & 0 \\ -9 & 3 & 0 & 1 & \tau-1 & -1 & 0 & 0 \\ 9 & -3 & 1 & 1 & -1 & \tau-1 & 0 & 0 \\ -9 & 3 & 1 & 1 & 1 & 0 & \tau-1 & 1 \\ 0 & 0 & 1 & 1 & -1 & 0 & 0 & \tau-1 \\ 27 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

Calculating in the same way as before, we can reduce the above matrix to

$$\begin{pmatrix} 9 & 0 & -S^2T+ST^2 \\ S & 0 & -T^2 \\ T & 0 & -S^2 \\ 0 & 3 & S^2T \\ 0 & S & T^2 \\ 0 & T & -S^2 \\ 0 & 0 & 3 \\ 0 & 0 & S^2T^2 \end{pmatrix}.$$

From this, we know that $(A_L^-)^\vee$ is generated by three elements and that these elements have 8 relations in $(A_L^-)^\vee$. Furthermore, taking all the 3×3 minors in the above matrix, we obtain

$$\mathrm{Fitt}_{R_L^-}((A_L^-)^\vee) = (81,\ 9S,\ 9T,\ 3S^2,\ 3T^2,\ 3ST).$$

Thus, we have

$$\begin{aligned} \frac{3}{2}\theta_{L/k}^- &\equiv 27 - 19S^2T^2 \not\equiv 0 && \left(\mathrm{mod}\ \mathrm{Fitt}_{R_L^-}((A_L^-)^\vee)\right), \\ \frac{S}{8}\theta_{L/k}^- &\equiv 3S \not\equiv 0 && \left(\mathrm{mod}\ \mathrm{Fitt}_{R_L^-}((A_L^-)^\vee)\right), \\ \frac{T}{2}\theta_{L/k}^- &\equiv 3T \not\equiv 0 && \left(\mathrm{mod}\ \mathrm{Fitt}_{R_L^-}((A_L^-)^\vee)\right). \end{aligned}$$

In conclusion, we have

$$I_L\theta_{L/k}^- \not\subset \mathrm{Fitt}_{R_L^-}((A_L^-)^\vee)$$

unlike to the previous case. We also have

$$\#\mu_{p^\infty}(L)\theta_{L/k}^- = 3\theta_{L/k}^- \notin \mathrm{Fitt}_{R_L^-}((A_L^-)^\vee).$$

Note that we have checked numerically

$$\mathrm{Fitt}_{\mathbb{Z}_p}(((A_L^-)^\vee)_G) = \mathrm{Fitt}_{\mathbb{Z}_p}(((A_L^-)^G)) = (81) \subsetneq (27) = \mathrm{Fitt}_{\mathbb{Z}_p}(A_K^-),$$

namely $\#(A_L^-)^G = 81 > \#A_K^- = 27$. Note that this is the inequality which was obtained in Proposition 1.1.

3 Examples for which neither (SB) nor (DSB) holds

In this section, we will prove that there are extensions L/k for which neither (SB) nor (DSB) holds.

3.1. We begin with the following easy lemma.

Lemma 3.1 *Let k be a totally real number field and M/k be a finite abelian extension such that M is a CM-field. Suppose that M' is an intermediate CM-field of M/k such that M/M' is a p-extension. Then we have*

$$\#\,\mathrm{Ker}(A_{M'}^- \longrightarrow A_M^-) \leq [M : M'].$$

Proof. As is well-known, there is an injective map from $\mathrm{Ker}(A_{M'}^- \longrightarrow A_M^-)$ to $H^1(\mathrm{Gal}(M/M'), E_M)^- = H^1(\mathrm{Gal}(M/M'), \mu_{p^\infty}(M))$. We put $M'' = M \cap M'_\infty$ where M'_∞ is the cyclotomic $\mathbb{Z}_p$-extension of M', and $G = \mathrm{Gal}(M/M')$, $H = \mathrm{Gal}(M/M'')$. Consider an exact sequence

$$0 \longrightarrow H^1(G/H, \mu_{p^\infty}(M'')) \longrightarrow H^1(G, \mu_{p^\infty}(M)) \longrightarrow H^1(H, \mu_{p^\infty}(M)).$$

We know $H^1(G/H, \mu_{p^\infty}(M'')) = 0$ and $\mu_{p^\infty}(M) = \mu_{p^\infty}(M'')$. Therefore, we have

$$\#H^1(G, \mu_{p^\infty}(M)) \leq \#H^1(H, \mu_{p^\infty}(M)) \leq \#H \leq \#G = [M : M'],$$

which completes the proof of Lemma 3.1.

In this section we assume that k is a totally real number field and $K = k(\mu_p)$. For simplicity, we also assume $[K : k] = 2$ (namely we replace k by K^+ if it is needed). Suppose that L/k is an abelian extension such that $K \subset L$. We also assume that

$$\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus r},\ A_K^- \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus r} \text{ for some } r \geq 2,$$

and the natural map $A_K^- \longrightarrow A_L^-$ is the zero map.

Proposition 3.2 *Assume that L/k satisfies the above conditions. We also assume that there are intermediate fields K_α, K_β of L/K such that $[K_\alpha : K] = [K_\beta : K] = p$, each prime of k which splits in K and which is ramified in L is ramified in K_α, $A_{K_\alpha}^-$ is generated by exactly r elements as a $\mathbb{Z}_p[\mathrm{Gal}(K_\alpha/K)]$-module, $A_{K_\beta}^-$ is generated by exactly r' elements as a $\mathbb{Z}_p[\mathrm{Gal}(K_\beta/K)]$-module, and $r' > r$. Then neither* (SB) *nor* (DSB) *holds for L/k.*

We will give in §3.2 a numerical example which satisfies all the conditions of the above proposition. Before the proof, we remark that our assumption implies that (R) is not satisfied for L/k. In fact, if (R) is satisfied, by Lemma 1.4 we have isomorphisms $(A_L^-)_{\mathrm{Gal}(L/K_\alpha)} \simeq A_{K_\alpha}^-$ and $(A_L^-)_{\mathrm{Gal}(L/K_\beta)} \simeq A_{K_\beta}^-$. This shows that $r = r'$ by Nakayama's lemma. Therefore, (R) is not satisfied in our case. After the proof of Proposition 3.2, we will show that our assumption in Proposition 3.2 implies that (NTZ) is not satisfied for L/k.

Proof of Proposition 3.2. We have $L \cap K_\infty = K$. In fact, if we put $K' = L \cap K_\infty$, we know that $A_K^- \longrightarrow A_{K'}^-$ is injective. By Lemma 3.1, we have $\#\,\mathrm{Ker}(A_K^- \longrightarrow A_L^-) \leq \#\,\mathrm{Ker}(A_{K'}^- \longrightarrow A_L^-) \leq [L : K']$. Since the left hand side is p^r by our assumption, we must have $[L : K'] = p^r$ and $K' = K$. We put $p^c = \#\mu_{p^\infty}(L)$ as in §1. Then we have $\#\mu_{p^\infty}(K) = p^c$.

For an intermediate field M of L/K such that $[M : K] = p$, we consider $R_M = \mathbb{Z}_p[\mathrm{Gal}(M/k)]$ and the decomposition $R_M = R_M^+ \oplus R_M^-$. Here, $R_M^- = \mathbb{Z}_p[\mathrm{Gal}(M/k)]^-$ is isomorphic to $\mathbb{Z}_p[\mathrm{Gal}(M/K)]$. For any element $x \in R_M$, we denote by $x^- \in R_M^- \simeq \mathbb{Z}_p[\mathrm{Gal}(M/K)]$ the minus component of x. We take a faithful character $\psi_M : \mathrm{Gal}(M/K) \longrightarrow \mu_p \subset \overline{\mathbb{Q}}_p^\times$, and put $O_{\psi_M} = \mathbb{Z}_p[\mathrm{Image}\,\psi_M]$ which we regard as a $\mathbb{Z}_p[\mathrm{Gal}(M/K)]$-module on which $\mathrm{Gal}(M/K)$ acts via ψ_M. We also denote by ψ_M the ring homomorphism $\mathbb{Z}_p[\mathrm{Gal}(M/K)] \longrightarrow O_{\psi_M}$ which is defined by $\sigma \mapsto \psi_M(\sigma)$ for all $\sigma \in \mathrm{Gal}(M/K)$. We define $(A_M^-)_{\psi_M}$ by

$$(A_M^-)_{\psi_M} = A_M^- \otimes_{\mathbb{Z}_p[\mathrm{Gal}(M/K)]} O_{\psi_M}.$$

Suppose that σ_M is a generator of $\mathrm{Gal}(M/K)$. Then σ_M acts trivially on $\mu_{p^\infty}(M) = \mu_{p^\infty}(K) = \mu_{p^c}$. Thus, we have $(\sigma_M - 1)\theta_{M/k} \in \mathbb{Z}_p[\mathrm{Gal}(M/k)]$ where $\theta_{M/k}$ is the Stickelberger element of M/k. We consider $(\sigma_M - 1)\theta_{M/k}^- \in \mathbb{Z}_p[\mathrm{Gal}(M/K)]$ and $\psi_M((\sigma_M - 1)\theta_{M/k}^-) \in O_{\psi_M}$.

Lemma 3.3 *For an intermediate field M of L/K such that $[M : K] = p$, we have*

$$\mathrm{Fitt}_{O_{\psi_M}}((A_M^-)_{\psi_M}) = (\psi_M((\sigma_M - 1)\theta_{M/k}^-)).$$

Proof. This can be proved by the class number formula. Let $\mathrm{ord}_p : \mathbb{Q}_p^\times \longrightarrow \mathbb{Z}$ be the normalized additive valuation at p such that $\mathrm{ord}_p(p) = 1$. The class number formula says that $\mathrm{ord}_p(\# A_K^-) = \mathrm{ord}_p(p^c\theta_{K/k}^-)$ and

$$\mathrm{ord}_p(\# A_M^-) = \mathrm{ord}_p(p^c\theta_{K/k}^- N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}(\psi_M(\theta_{M/k}^-)))$$

where $N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}$ is the norm from $\mathbb{Q}_p(\mu_p)$ to $\mathbb{Q}_p$. Hence we have

$$\mathrm{ord}_p(\frac{\# A_M^-}{\# A_K^-}) = \mathrm{ord}_p(N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}(\psi_M(\theta_{M/k}^-))).$$

On the other hand, since the norm map $A_M^- \longrightarrow A_K^-$ is surjective by Lemma 1.4, we have

$$(A_M^-)_{\psi_M} = A_M^-/(1 + \sigma_M + ... + \sigma_M^{p-1})A_M^- = A_M^-/\operatorname{Image}(A_K^- \longrightarrow A_M^-).$$

Since the natural map $i_{L/K} : A_K^- \longrightarrow A_L^-$ is the zero map by our assumption, the image of $i_{M/K} : A_K^- \longrightarrow A_M^-$ is in the kernel of $i_{L/M} : A_M^- \longrightarrow A_L^-$. By Lemma 3.1 we have $\#\operatorname{Ker}(A_K^- \longrightarrow A_M^-) \leq p$ and $\#\operatorname{Ker}(A_M^- \longrightarrow A_L^-) \leq p^{r-1}$. Therefore, we must have $\#\operatorname{Ker}(A_K^- \longrightarrow A_M^-) = p$ and $\#\operatorname{Ker}(A_M^- \longrightarrow A_L^-) = p^{r-1}$. It follows that

$$\#(A_M^-)_{\psi_M} = \#\operatorname{Coker}(A_K^- \longrightarrow A_M^-) = p\frac{\# A_M^-}{\# A_K^-}.$$

This implies that

$$\mathrm{ord}_p(\#(A_M^-)_{\psi_M}) = \mathrm{ord}_p(N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}(\psi_M((\sigma_M - 1)\theta_{M/k}^-))).$$

Thus, we get $\mathrm{length}_{O_{\psi_M}}((A_M^-)_{\psi_M}) = \mathrm{length}_{O_{\psi_M}}(O_{\psi_M}/\psi_M((\sigma_M - 1)\theta_{M/k}^-))$, which implies the conclusion of Lemma 3.3 (note that O_{ψ_M} is a discrete valuation ring).

Now we prove Proposition 3.2. First, we will prove that (SB) does not hold. Since the map $(A_L^-)_{\mathrm{Gal}(L/K_\beta)} \longrightarrow A_{K_\beta}^-$ which is induced by the norm map is surjective, the number of generators of A_L^- as a $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-module is $\geq r'$ by Nakayama's lemma. We consider a surjective homomorphism $(A_L^-)_{\mathrm{Gal}(L/K_\alpha)} \longrightarrow A_{K_\alpha}^-$. Let $\psi_1 = \psi_{K_\alpha}$ be a faithful character of $\mathrm{Gal}(K_\alpha/K)$. For any $\mathbb{Z}_p[\mathrm{Gal}(K_\alpha/K)]$-module M, we define the ψ_1-quotient by $M_{\psi_1} = M \otimes_{\mathbb{Z}_p[\mathrm{Gal}(K_\alpha/K)]} O_{\psi_1}$. We consider a surjective homomorphism $((A_L^-)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1} \longrightarrow (A_{K_\alpha}^-)_{\psi_1}$ which is the ψ_1-quotient of the above homomorphism. The number of generators of $((A_L^-)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1}$ (resp. $(A_{K_\alpha}^-)_{\psi_1}$) as an O_{ψ_1}-module is $\geq r'$ (resp. r) by Nakayama's lemma. Therefore, we obtain

$$\operatorname{Ker}(((A_L^-)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1} \longrightarrow (A_{K_\alpha}^-)_{\psi_1}) \neq 0. \tag{3.1.1}$$

It follows from Lemma 3.3 that

$$\mathrm{Fitt}_{O_{\psi_1}}(((A_L^-)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1}) \subsetneq (\psi_1((\sigma_{K_\alpha} - 1)\theta_{K_\alpha/k}^-)).$$

Let $\sigma \in \mathrm{Gal}(L/K)$ be a K-isomorphism whose restriction to K_α is σ_{K_α}. The image of $(\sigma-1)\theta^-_{L/k}$ in $\mathbb{Z}_p[\mathrm{Gal}(K_\alpha/K)]$ is $u(\sigma_{K_\alpha}-1)\theta^-_{K_\alpha/k}$ for some unit u by Lemma 1.5 because all the primes of k which split in K and which are ramified in L are ramified in K_α. If $(\sigma-1)\theta^-_{L/k}$ was in $\mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(L/K)]}(A^-_L)$, $\psi_1((\sigma_{K_\alpha}-1)\theta^-_{K_\alpha/k})$ would be in $\mathrm{Fitt}_{O_{\psi_1}}(((A^-_L)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1})$, which is a contradiction. Therefore, we have $(\sigma-1)\theta^-_{L/k} \notin \mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(L/K)]}(A^-_L)$, and conclude that (SB) does not hold.

Next, we prove that (DSB) does not hold. In the proof of Lemma 3.3, we proved that $\#\,\mathrm{Ker}(A^-_K \longrightarrow A^-_{K_\beta}) = p$, $\#\,\mathrm{Ker}(i_{L/K_\beta}) = p^{r-1}$, and $\mathrm{Image}(i_{K_\beta/K}) = \mathrm{Ker}(i_{L/K_\beta})$. Let $\psi_2 = \psi_{K_\beta}$ be a faithful character of $\mathrm{Gal}(K_\beta/K)$. In the proof of Lemma 3.3 we also proved that $(A^-_{K_\beta})_{\psi_2}$ is isomorphic to $\mathrm{Coker}(i_{K_\beta/K})$, so we have an injective homomorphism

$$(A^-_{K_\beta})_{\psi_2} \hookrightarrow (A^-_L)^{\mathrm{Gal}(L/K_\beta)}. \tag{3.1.2}$$

Let π be a prime element of O_{ψ_2}. For any $m \in \mathbf{Z}_{>0}$ we know that $O_{\psi_2}/(\pi^m)$ is a Gorenstein ring, so the Pontrjagin dual $(O_{\psi_2}/(\pi^m))^\vee$ is isomorphic to $O_{\psi_2}/(\pi^m)$ (cf. [10] Proposition 4 on page 328). Since $(A^-_{K_\beta})_{\psi_2}$ is a finite O_{ψ_2}-module, we can apply the above argument to know that the Pontrjagin dual $((A^-_{K_\beta})_{\psi_2})^\vee$ is generated by exactly r' elements as a $\mathbb{Z}_p[\mathrm{Gal}(K_\beta/K)]$-module. Therefore, from the injectivity (3.1.2) we know that the number of generators of $(A^-_L)^\vee$ is $\geq r'$.

By the same method as (3.1.2), we obtain an injective homomorphism

$$(A^-_{K_\alpha})_{\psi_1} \hookrightarrow (A^-_L)^{\mathrm{Gal}(L/K_\alpha)}. \tag{3.1.3}$$

Taking the dual and the ψ_1-quotient, we have a surjective homomorphism

$$(((A^-_L)^\vee)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1} \longrightarrow ((A^-_{K_\alpha})_{\psi_1})^\vee$$

where the number of generators of $(((A^-_L)^\vee)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1}$ is $\geq r'$ and the number of generators of $((A^-_{K_\alpha})_{\psi_1})^\vee$ is r. Therefore, the above surjective homomorphism has nontrivial kernel. This implies that

$$\mathrm{Fitt}_{O_{\psi_1}}((((A^-_L)^\vee)_{\mathrm{Gal}(L/K_\alpha)})_{\psi_1}) \subsetneq (\psi_1((\sigma_{K_\alpha}-1)\theta^-_{K_\alpha/k}))$$

by Lemma 3.3. Therefore, by the same method as in the case of (SB), we know that $(\sigma-1)\theta^-_{L/k}$ is not in $\mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(L/K)]}((A^-_L)^\vee)$. Thus, (DSB) does not hold. This completes the proof of Proposition 3.2.

We finally remark that our assumption in Proposition 3.2 implies that (NTZ) is not satisfied for L/k. In fact, (3.1.1) and Lemma 1.4 imply that there is a prime $\mathfrak{p}$ of k which splits in K and is ramified in L/K_α. Then $\mathfrak{p}$ has to be ramified in K_α/K by our assumption. Therefore, the inertia group of $\mathfrak{p}$ in $\mathrm{Gal}(L/k)$ is not cyclic. This shows that $\mathfrak{p}$ is above p. Since $\mathfrak{p}$ splits in K, (NTZ) is not satisfied.

3.2. We give a numerical example which satisfies the conditions of Proposition 3.2.

Let $p = 3$, $k = \mathbb{Q}(\sqrt{69}, \sqrt{713})$ and $K = k(\mu_3) = k(\sqrt{-3})$. Suppose that α, β satisfy $\alpha^3 - 6\alpha - 3 = 0$ and $\beta^3 - 6\beta - 1 = 0$, and put $K_\alpha = K(\alpha)$, $K_\beta = K(\beta)$. The minimal splitting field of $x^3 - 6x - 3$ (resp. $x^3 - 6x - 1$) over $\mathbb{Q}$ is a $\mathfrak{S}_3$-extension and contains $\sqrt{69}$ (resp. $\sqrt{93}$). Therefore, both $k(\alpha)/k$ and $k(\beta)/k$ are cubic cyclic extensions. We put $L = K_\alpha K_\beta$. We have $\mathrm{Gal}(L/K) = \mathrm{Gal}(K_\alpha/K) \oplus \mathrm{Gal}(K_\beta/K) = \mathrm{Gal}(k(\alpha)/k) \oplus \mathrm{Gal}(k(\beta)/k) \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$.

There is only one prime $\mathfrak{p}$ in k above 3. We can check that both $k(\alpha)/k$ and $k(\beta)/k$ are unramified outside $\mathfrak{p}$, and that $\mathfrak{p}$ is totally ramified both in $k(\alpha)$ and in $k(\beta)$. Since $K = k(\sqrt{-3}) = k(\sqrt{-23})$, $\mathfrak{p}$ splits in K. Two primes of K above $\mathfrak{p}$ are totally ramified in L. So L/k satisfies neither (NTZ) nor (R).

We can easily check that $A_K^- \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ by the computations of the class numbers of imaginary quadratic fields which are contained in K. More precisely, we have

$$A_K^- = A_{\mathbb{Q}(\sqrt{-23})} \oplus A_{\mathbb{Q}(\sqrt{-31})}.$$

We can check that the natural map $A_{\mathbb{Q}(\sqrt{-23})} \longrightarrow A_{\mathbb{Q}(\sqrt{-23}, \sqrt{-3}, \alpha)}$ is the zero map both theoretically (using that the λ-invariant of $\mathbb{Q}(\sqrt{-23})$ is 1) and numerically (using Pari/GP). We will explain it numerically. By Pari/GP, we can check that $A^-_{\mathbb{Q}(\sqrt{-23}, \sqrt{-3}, \alpha)} \simeq \mathbb{Z}/3\mathbb{Z}$. Since the norm map $A^-_{\mathbb{Q}(\sqrt{-23}, \sqrt{-3}, \alpha)} \longrightarrow A_{\mathbb{Q}(\sqrt{-23})}$ is surjective by class field theory, it is bijective. This shows that the natural map $A_{\mathbb{Q}(\sqrt{-23})} \longrightarrow A_{\mathbb{Q}(\sqrt{-23}, \sqrt{-3}, \alpha)}$ is the zero map. Similarly, using $A^-_{\mathbb{Q}(\sqrt{-31}, \sqrt{-3}, \beta)} \simeq \mathbb{Z}/3\mathbb{Z}$, we know that $A_{\mathbb{Q}(\sqrt{-31})} \longrightarrow A_{\mathbb{Q}(\sqrt{-31}, \sqrt{-3}, \beta)}$ is also the zero map. Therefore, $A_K^- \longrightarrow A_L^-$ is the zero map.

Using Pari/GP, we can compute

$$A^-_{K_\alpha} \simeq \mathbb{Z}/81\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

The action of a generator σ_{K_α} of $\mathrm{Gal}(K_\alpha/K)$ is represented by the matrix

$$M_{\sigma_{K_\alpha}} = \begin{pmatrix} -32 & 21 & -27 \\ -10 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The meaning of the matrix is the same as §2. Putting $S = \sigma_{K_\alpha} - 1$, we obtain a relation matrix

$$\begin{pmatrix} S+33 & -21 & 27 & 81 & 0 & 0 \\ 10 & S-3 & 0 & 0 & 27 & 0 \\ 0 & 0 & S & 0 & 0 & 3 \end{pmatrix}$$

of $A^-_{K_\alpha}$ as a $\mathbb{Z}_p[\mathrm{Gal}(K_\alpha/K)]$-module. The above matrix is reduced to

$$\begin{pmatrix} 3 & S & 0 & 0 \\ 0 & 0 & 27S & 3+3S+S^2-9S^2 \end{pmatrix}.$$

This shows that $A^-_{K_\alpha}$ is generated by exactly two elements.

In the same way, we have

$$A^-_{K_\beta} \simeq \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

The action of a generator σ_{K_β} of $\mathrm{Gal}(K_\beta/K)$ is represented by the matrix

$$M_{\sigma_{K_\beta}} = \begin{pmatrix} -2 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We put $T = \sigma_{K_\beta} - 1$, then a relation matrix of $A_{K_\beta}^-$ is

$$\begin{pmatrix} T+3 & 0 & 3 & 9 & 0 & 0 \\ 0 & T & 0 & 0 & 3 & 0 \\ 0 & 0 & T & 0 & 0 & 3 \end{pmatrix}.$$

Therefore, $A_{K_\beta}^-$ is generated by exactly three elements. Thus, our L/k satisfies all the conditions of Proposition 3.2. Hence we know that neither (SB) nor (DSB) holds for our L/k.

We finally remark that we could not compute numerically the Fitting ideal of A_L^- for this example. We can compute

$$A_L^- \simeq \mathbb{Z}/81\mathbb{Z} \oplus \mathbb{Z}/81\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$$

as an abelian group. But since the degree of L is too large, we could not compute the action of $\mathrm{Gal}(L/K)$ on A_L^-, using Pari/GP.

4 Other examples

4.1. In this subsection, we describe the setting and the assumptions in this section. Let k' be a totally real number field and $K' = k'(\mu_p)$. We assume $(K')^+ = k'$, so $[K' : k'] = 2$. Let F'/k' be a finite and abelian p-extension such that $\mathrm{Gal}(F'/k')$ is *not cyclic*. We further assume that F'/k' is ramified at a prime above p. We put $L' = F'K'$. We assume (NTZ) and (R) for L'/k'. So every prime above p does not split in K'/k', and every prime which splits in K'/k' is unramified in L'/k'. Let k'_∞/k' (resp. F'_∞/F') be the cyclotomic $\mathbb{Z}_p$-extension. We further assume that $F' \cap k'_\infty = k'$, and all the primes of F' above p are totally ramified in F'_∞.

We also assume that there is a CM-field K'' which is a quadratic extension of k' such that $A_{K''}^- = 0$, and that there is a prime $\mathfrak{p}'$ of k' above p which is ramified in F' and which splits in K''. Put $L'' = F'K''$. Then (R) is not satisfied for L''/k' because $\mathfrak{p}'$ splits in K'' and is ramified in L''. Also, (NTZ) is not satisfied for L''/k' because $\mathfrak{p}'$ splits in K''. Since $\mathfrak{p}'$ splits in K'' and does not split in K', we have $K' \neq K''$. We assume that every prime of k' which is prime to p and which splits in K'' is unramified in L''/k'.

In this setting, we put $K = K'K''$. Then K is a CM-field and K/k' is an abelian extension such that $\mathrm{Gal}(K/k') \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The maximal real subfield K^+ of K is a quadratic extension of k'. We put $k = K^+$, $F = kF'$ and $L = kL' = kL''$. We have $K = kK' = k(\mu_p)$. Let $\mathfrak{p}'$ be a prime of k' above p which is ramified in F' and which splits in K''. Since $\mathfrak{p}'$ does not split in K', it does not split in k. We denote by $\mathfrak{p}$ the prime of k above $\mathfrak{p}'$. Then $\mathfrak{p}$ splits in K, and is ramified in L. In particular, neither (NTZ) nor (R) is satisfied for

L/k. Since every prime above p is totally ramified in F'_∞/F', every prime of L (resp. K) above p is also totally ramified in L_∞ (resp. K_∞).

4.2. In this subsection, we will prove Theorem 0.2. Put $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(L'/K') = \mathrm{Gal}(L''/K'') = \mathrm{Gal}(F/k) = \mathrm{Gal}(F'/k')$ and $\Gamma = \mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(K'_\infty/K') = \mathrm{Gal}(K''_\infty/K'')$. Let $\kappa : \Gamma \longrightarrow \mathbb{Z}_p^\times$ be the cyclotomic character and γ be a generator of Γ.

We put $\Gamma_1 = \mathrm{Gal}(K_1/K) = \mathrm{Gal}(K'_1/K') = \mathrm{Gal}(K''_1/K'')$ where K_1 (resp. K'_1, K''_1) is the first layer of K_∞/K (resp. K'_∞/K', K''_∞/K''). We regard γ as a generator of Γ_1.

As in §3, we consider $R_{K'_1} = \mathbb{Z}_p[\mathrm{Gal}(K'_1/k')]$ and the decomposition $R_{K'_1} = R^+_{K'_1} \oplus R^-_{K'_1}$. For any element $x \in R_{K'_1}$, we denote by $x^- \in R^-_{K'_1} \simeq \mathbb{Z}_p[\Gamma_1]$ the minus component of x. Let $\psi : \Gamma_1 \longrightarrow \mu_p \subset \overline{\mathbb{Q}}_p^\times$ be a faithful character, and $O_\psi = \mathbb{Z}_p[\mathrm{Image}\,\psi]$ be a $\mathbb{Z}_p[\Gamma_1]$-module on which Γ_1 acts via ψ. The ring homomorphism $\mathbb{Z}_p[\Gamma_1] \longrightarrow O_\psi$ defined by $\sigma \mapsto \psi(\sigma)$ for all $\sigma \in \Gamma_1$ is also denoted by ψ. So $\psi(x^-) \in O_\psi$ is defined for $x \in R_{K'_1}$.

For any $\mathbb{Z}_p[\Gamma_1]$-module M, we define M_ψ by $M_\psi = M \otimes_{\mathbb{Z}_p[\Gamma_1]} O_\psi$. We will prove

Lemma 4.1

$$\mathrm{Fitt}_{O_\psi}(((A^-_{L'_1})_G)_\psi) = (\psi(((\gamma - \kappa(\gamma))\theta_{K'_1/k'})^-)), \tag{4.2.1}$$

$$\mathrm{Fitt}_{O_\psi}((((A^-_{L'_1})^\vee)_G)_\psi) \subsetneq (\psi(((\gamma - \kappa(\gamma))\theta_{K'_1/k'})^-)). \tag{4.2.2}$$

Proof. We will first prove (4.2.1). Since $(\mathrm{R})_1$ is satisfied for L'_1/k', the norm map induces an isomorphism

$$(A^-_{L'_1})_G \xrightarrow{\simeq} A^-_{K'_1}$$

by Lemma 1.4. Therefore, we have $\mathrm{Fitt}_{R^-_{K'_1}}((A^-_{L'_1})_G) = \mathrm{Fitt}_{R^-_{K'_1}}(A^-_{K'_1})$.

Using the class number formula and the fact that $\#\mu_{p^\infty}(K'_1) = p\#\mu_{p^\infty}(K')$, we get

$$\mathrm{ord}_p\left(\frac{\#A^-_{K'_1}}{\#A^-_{K'}}\right) = \mathrm{ord}_p(N_{\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p}(\psi(\theta^-_{K'_1/k'}))) + 1$$

by the same method as Lemma 3.3. Since $A^-_{K'} \longrightarrow A^-_{K'_1}$ is injective in our case, we have an exact sequence

$$0 \longrightarrow A^-_{K'} \longrightarrow A^-_{K'_1} \longrightarrow (A^-_{K'_1})_\psi \longrightarrow 0.$$

It follows that

$$\mathrm{ord}_p(\#(A^-_{K'_1})_\psi) = \mathrm{length}_{O_\psi}((A^-_{K'_1})_\psi) = \mathrm{length}_{O_\psi}(O_\psi/\psi((\gamma - \kappa(\gamma))\theta^-_{K'_1/k'})),$$

which implies (4.2.1).

Next, we will prove (4.2.2). Suppose that n is an integer > 1. As in the proof of Proposition 1.1, we have $H^q(\mathrm{Gal}(L'_n/L'_1), E_{L'_n})^- = 0$ for any $q \geq 1$. Using the long exact sequence in §1 for L'_n/L'_1, we obtain $\hat{H}^0(\mathrm{Gal}(L'_n/L'_1), A^-_{L'_n}) = H^1(\mathrm{Gal}(L'_n/L'_1), A^-_{L'_n}) = 0$ by our assumption (NTZ). This implies that the natural map $A^-_{L'_1} \longrightarrow (A^-_{L'_n})^{\mathrm{Gal}(L'_n/L'_1)}$ is bijective (cf. the proof of Proposition 1.1). Put $A_{K'_\infty} = \varinjlim A_{K'_n}$ and $A_{L'_\infty} = \varinjlim A_{L'_n}$. Thus, we have an isomorphism

$$A^-_{L'_1} \xrightarrow{\simeq} (A^-_{L'_\infty})^{\mathrm{Gal}(L'_\infty/L'_1)}. \tag{4.2.2.1}$$

Put $\mathcal{X}_{K'_\infty} = A^\vee_{K'_\infty}$ and $\mathcal{X}_{L'_\infty} = A^\vee_{L'_\infty}$. In the proof of Theorem 0.3 in [8], we proved

$$\mathrm{Fitt}_{\Lambda^-_{K'_\infty}}((\mathcal{X}^-_{L'_\infty})_G) \subset (p, \gamma-1)(((\gamma-\kappa(\gamma))\theta_{K'_\infty/k'})^-). \tag{4.2.2.2}$$

The isomorphism (4.2.2.1) induces an isomorphism $(\mathcal{X}^-_{L'_\infty})_{G\times\mathrm{Gal}(L'_\infty/L'_1)} \simeq ((A^-_{L'_1})^\vee)_G$. We denote by $c_{K'_\infty/K'_1} : \Lambda_{K'_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(K'_\infty/k')]] \longrightarrow R_{K'_1}$ the natural restriction map. Since every prime of k' above p is ramified in K'_1, by Lemma 1.5 we have

$$c_{K'_\infty/K'_1}((\gamma-\kappa(\gamma))\theta_{K'_\infty/k'}) = (\gamma-\kappa(\gamma))\theta_{K'_1/k'}. \tag{4.2.2.3}$$

Hence by (4.2.2.2) and (4.2.2.3) we have

$$\mathrm{Fitt}_{R^-_{K'_1}}(((A^-_{L'_1})^\vee)_G) \subset (p, \gamma-1)(((\gamma-\kappa(\gamma))\theta_{K'_1/k'})^-),$$

which implies (4.2.2).

Next, we consider L''/K''. Since $K'' \neq K'$, K'' does not contain a primitive p-th root of unity, so neither does K''_1. Put $R_{K''_1} = \mathbb{Z}_p[\mathrm{Gal}(K''_1/k')]$. Since $I_{K''_1} = \mathrm{Ann}_{R_{K''_1}}(\mu_{p^\infty}(K''_1)) = R_{K''_1}$, we have $\theta_{K''_1/k'} \in R_{K''_1}$ by a theorem of Deligne and Ribet.

As we did for K'_1, we consider the decomposition $R_{K''_1} = R^+_{K''_1} \oplus R^-_{K''_1}$, and use the notation $x^- \in R^-_{K''_1}$ which is the minus component of x for any $x \in R_{K''_1}$. For a faithful character $\psi : \Gamma_1 \longrightarrow \mu_p$, we also consider the ring homomorphism $\psi : R^-_{K''_1} \simeq \mathbb{Z}_p[\Gamma_1] \longrightarrow O_\psi$.

We will prove

Lemma 4.2

$$\mathrm{Fitt}_{O_\psi}(((A^-_{L''_1})_G)_\psi) \subsetneq (\psi(\theta^-_{K''_1/k'})) \tag{4.2.3}$$

$$\mathrm{Fitt}_{O_\psi}((((A^-_{L''_1})^\vee)_G)_\psi) \subset (\psi(\theta^-_{K''_1/k'})). \tag{4.2.4}$$

Proof. We first note that

$$\mathrm{Fitt}_{O_\psi}((A^-_{K''_1})_\psi) = (\psi(\theta^-_{K''_1/k'})). \tag{4.2.3.1}$$

We can prove (4.2.3.1) by the class number formula, using the same method as Lemma 3.3 and (4.2.1) (now we use $\#\mu_{p^\infty}(K''_1) = \#\mu_{p^\infty}(K'') = 1$).

We first prove (4.2.3). By Lemma 1.4, we have a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\bigoplus_w I_w(L_1''/K_1''))^- & \xrightarrow{\alpha} & (A^-_{L_1''})_G & \longrightarrow & A^-_{K_1''} & \longrightarrow & 0 \\ & & \big\downarrow \beta & & \big\downarrow \gamma & & \big\downarrow & & \\ 0 & \longrightarrow & (\bigoplus_v I_v(L''/K''))^- & \xrightarrow{\delta} & (A^-_{L''})_G & \longrightarrow & A^-_{K''} & \longrightarrow & 0 \end{array}$$

where w (resp. v) runs over all finite primes of K_1'' (resp. K''). Let $v_{k'}$ be the prime of k' below a prime v of K''. If $v_{k'}$ is not above p and splits in K''/k', v is unramified in L'' by our assumption. Hence $(\bigoplus_v I_v(L''/K''))^- = (\bigoplus_{v|p} I_v(L''/K''))^-$. Similarly, we have $(\bigoplus_w I_w(L_1''/K_1''))^- = (\bigoplus_{w|p} I_w(L_1''/K_1''))^-$. If v is above p, v is totally ramified in K_1'' because every prime above p is totally ramified in F'_∞/F'. Let w be the prime of K_1'' above v. Then the restriction map $I_w(L_1''/K_1'') \longrightarrow I_v(L''/K'')$ is bijective because every prime of L'' above v is totally ramified in L_1''. Therefore, β is bijective. Since $A^-_{K''} = 0$, δ is also bijective. Thus, α has a left inverse $\beta^{-1} \circ \delta^{-1} \circ \gamma$. Hence we have isomorphisms

$$(4.2.3.2) \qquad (A^-_{L_1''})_G \simeq (\bigoplus_{w|p} I_w(L_1''/K_1''))^- \oplus A^-_{K_1''} \simeq (\bigoplus_{v|p} I_v(L''/K''))^- \oplus A^-_{K_1''}$$

as $R^-_{K_1''}$-modules. Since there is a prime $\mathfrak{p}'$ of k' above p which splits in K'' and which is ramified in L'', $(\bigoplus_{v|p} I_v(L''/K''))^- \neq 0$. Therefore, we have

$$\mathrm{Fitt}_{R^-_{K_1''}}((A^-_{L_1''})_G) \subset (p, \gamma - 1)\,\mathrm{Fitt}_{R^-_{K_1''}}(A^-_{K_1''}).$$

By (4.2.3.1), this implies that

$$\mathrm{Fitt}_{O_\psi}(((A^-_{L_1''})_G)_\psi) \subset \psi((\gamma-1)\theta^-_{K_1''/k'}).$$

This completes the proof of (4.2.3).

Finally, we will prove (4.2.4). Since $\#\mu_{p^\infty}(L_1'') = 1$, we have $H^1(G, E_{L_1''})^- = 0$. This implies that the natural map $A^-_{K_1''} \longrightarrow (A^-_{L_1''})^G$ is injective. Hence $((A^-_{L_1''})^\vee)_G \longrightarrow (A^-_{K_1''})^\vee$ is surjective, so $(((A^-_{L_1''})^\vee)_G)_\psi \longrightarrow ((A^-_{K_1''})^\vee)_\psi$ is also surjective, which gives an inclusion

$$\mathrm{Fitt}_{O_\psi}((((A^-_{L_1''})^\vee)_G)_\psi) \subset \mathrm{Fitt}_{O_\psi}(((A^-_{K_1''})^\vee)_\psi).$$

In general, for any $\mathbb{Z}_p[\Gamma_1]$-module M, we define M^ψ to be the kernel of $N_{\Gamma_1} = 1 + \gamma + ... + \gamma^{p-1}$ on M. We have an exact sequence

$$0 \longrightarrow M^\psi \longrightarrow M \xrightarrow{N_{\Gamma_1}} M \longrightarrow M_\psi \longrightarrow 0.$$

Suppose that M is finite. Then by the above exact sequence, we have

$$\#(M^\vee)_\psi = \#(M^\psi)^\vee = \#M^\psi = \#M_\psi.$$

Applying the above equality to $M = A^-_{K_1''}$, we get

$$\mathrm{Fitt}_{O_\psi}((((A^-_{L_1''})^\vee)_G)_\psi) \subset \mathrm{Fitt}_{O_\psi}(((A^-_{K_1''})^\vee)_\psi) = \mathrm{Fitt}_{O_\psi}((A^-_{K_1''})_\psi).$$

Using (4.2.3.1), we obtain (4.2.4).

Remark 4.3 Note that (4.2.3) shows that (SB) does not hold for L_1''/k'. In fact, we have $c_{L_1''/K_1''}(\theta_{L_1''/k'}) = u\theta_{K_1''/k'}$ for some $u \in R_{K_1''}^{\times}$ by Lemma 1.5 because all the primes of k' above p are ramified in K_1'', and a prime of k' which is not above p and which splits in K'' is unramified in L_1''/K_1''. So if $\theta_{L_1''/k'}$ was in $\mathrm{Fitt}_{R_{L_1''}}(A_{L_1''})$, $\theta^-_{K_1''/k'}$ would be in $\mathrm{Fitt}_{R^-_{K_1''}}((A^-_{L_1''})_G)$, and $\psi(\theta^-_{K_1''/k'})$ would be in $\mathrm{Fitt}_{O_\psi}(((A^-_{L_1''})_G)_\psi)$, which contradicts (4.2.3).

Now we proceed to the proof of Theorem 0.2. Let $\mathrm{Gal}(K/k')^\vee$ be the group of characters of $\mathrm{Gal}(K/k')$. For any $\chi \in \mathrm{Gal}(K/k')^\vee$ and a $\mathbb{Z}_p[\mathrm{Gal}(K/k')]$-module M, we define

$$M^\chi = \{x \in M \mid \sigma(x) = \chi(\sigma)x \ \text{ for all } \sigma \in \mathrm{Gal}(K/k')\}.$$

Let χ_1 be the trivial character, χ_k be the character corresponding to k/k', and χ' (resp. χ'') be the character corresponding to K'/k' (resp. K''/k'). Any $\mathbb{Z}_p[\mathrm{Gal}(K/k')]$-module M is decomposed into $M = M^{\chi_1} \oplus M^{\chi_k} \oplus M^{\chi'} \oplus M^{\chi''}$. Since χ', χ'' are odd characters (and χ_1, χ_k are even characters), we have $M^- = M^{\chi'} \oplus M^{\chi''}$. We identify $\mathcal{G}_n = \mathrm{Gal}(L_n/k)$ with $\mathrm{Gal}(L'_n/k')$ by the restriction map, and also identify $\mathcal{G}_n$ with $\mathrm{Gal}(L''_n/k')$. We have an isomorphism

$$A^-_{L_n} = A^{\chi'}_{L_n} \oplus A^{\chi''}_{L_n} \simeq A^-_{L'_n} \oplus A^-_{L''_n} \tag{4.2.5}$$

as $\mathbb{Z}_p[\mathcal{G}_n]$-modules for any $n \geq 0$.

Using the identifications of $\mathcal{G}_n$ with $\mathrm{Gal}(L'_n/k')$ and with $\mathrm{Gal}(L''_n/k')$, we regard $\theta_{L'_n/k'}$, $\theta_{L''_n/k'}$ as elements in $\mathbb{Q}[\mathcal{G}_n]$. Then we have

$$\theta_{L_n/k} = \theta_{L'_n/k'}\theta_{L''_n/k'}. \tag{4.2.6}$$

We will give a proof of (4.2.6). We use a technique of Tate [15] Proposition 1.8 on page 87. Let σ (resp. τ) be a generator of $\mathrm{Gal}(L_n/L'_n)$ (resp. $\mathrm{Gal}(L_n/L''_n)$), which is a cyclic group of order 2. Note that $\sigma\tau$ is in $\mathcal{G}_n$ and this equals to the complex conjugation ρ. We know that $\mathrm{Gal}(L_n/k') \simeq \mathcal{G}_n \times \langle\sigma\rangle \simeq \mathcal{G}_n \times \langle\tau\rangle$. We have an isomorphism

$$\mathbb{C}[\mathrm{Gal}(L_n/k')]^- \xrightarrow{\simeq} \mathbb{C}[\mathrm{Gal}(L'_n/k')]^- \oplus \mathbb{C}[\mathrm{Gal}(L''_n/k')]^- \simeq \mathbb{C}[\mathcal{G}_n]^- \oplus \mathbb{C}[\mathcal{G}_n]^-$$

where the first isomorphism is induced by $c_{L_n/L'_n} \oplus c_{L_n/L''_n}$ and the second isomorphism comes from our identifications of $\mathcal{G}_n$ with $\mathrm{Gal}(L'_n/k')$ and with $\mathrm{Gal}(L''_n/k')$. Since c_{L_n/L'_n} (resp. c_{L_n/L''_n}) is defined by $\sigma \mapsto 1$ (resp. $\tau \mapsto 1$), the above first isomorphism satisfies $a + b\sigma \mapsto (a+b, a-b)$ for any a, $b \in \mathbb{C}[\mathcal{G}_n]^-$.

Let x be an element of $\mathbb{C}[\mathrm{Gal}(L_n/k')]^-$. The multiplication by x defines an endomorphism of $\mathbb{C}[\mathrm{Gal}(L_n/k')]^-$ which is a free $\mathbb{C}[\mathcal{G}_n]^-$-module of rank 2. Hence, the determinant induces a homomorphism $\mathcal{N} : \mathbb{C}[\mathrm{Gal}(L_n/k')]^- \longrightarrow \mathbb{C}[\mathcal{G}_n]^-$. Namely, $\mathcal{N}(a + b\sigma) = a^2 - b^2$ for any a, $b \in \mathbb{C}[\mathcal{G}_n]^-$, and

$$\mathcal{N}(x) = c_{L_n/L'_n}(x)c_{L_n/L''_n}(x). \tag{4.2.7}$$

Let $\theta_{L_n/k'}(s)$ be a $\mathbb{C}[\mathrm{Gal}(L_n/k')]$-valued function defined in [15] satisfying $\theta_{L_n/k'}(0) = \theta_{L_n/k'}$. Using Tate [15] Proposition 1.8 on page 87, we have

$$\mathcal{N}(\theta_{L_n/k'}(s)) = \prod_{v \in S}(1 - \varphi_v^{-1}N(v)^{-s})\theta_{L_n/k}(s) \tag{4.2.8}$$

where S is the set of primes of k' which are ramified in k/k' and are unramified in L_n/k, and $N(v)$ is the norm of a prime v. If v is in S, it is unramified in L_n/K, so it is prime to p. Hence it is unramified in K', and is unramified in L'_n. Therefore, we have

$$S = \{v : \text{a prime of } k' \mid v \text{ is ramified in } L_n/k' \text{ and is unramified in } L'_n/k'\}.$$

By Tate [15] Corollary 1.7 on page 86, we have

$$c_{L_n/L'_n}(\theta_{L_n/k'}(s)) = \prod_{v\in S}(1-\varphi_v^{-1}N(v)^{-s})\theta_{L'_n/k'}(s). \tag{4.2.9}$$

If a prime v of k' is ramified in L_n and unramified in L''_n, it is ramified in K' so it is a prime above p. But this contradicts our assumption that all the primes above p are totally ramified in L''_n/L''. Hence there is no prime of k' which is ramified in L_n and unramified in L''_n. By Tate [15] Corollary 1.7 on page 86, we have

$$c_{L_n/L''_n}(\theta_{L_n/k'}(s)) = \theta_{L''_n/k'}(s). \tag{4.2.10}$$

By (4.2.7), (4.2.8), (4.2.9), and (4.2.10), we get

$$\mathcal{N}(\theta_{L_n/k'}(s)) = c_{L_n/L'_n}(\theta_{L_n/k'}(s))c_{L_n/L''_n}(\theta_{L_n/k'}(s)).$$

Substituting $s = 0$, we obtain (4.2.6). This completes the proof of (4.2.6).

Now, we will prove that (SB) does not hold for L_n/k for $n \geq 1$. Suppose that $(\gamma-\kappa(\gamma))\theta_{L_n/k}$ is in $\mathrm{Fitt}_{R_{L_n}}(A_{L_n})$. Since $(A^-_{L_n})_{\mathrm{Gal}(L_n/L_1)} \longrightarrow A^-_{L_1}$ is surjective by Lemma 1.4, we have $c_{L_n/L_1}((\gamma-\kappa(\gamma))\theta^-_{L_n/k}) \in \mathrm{Fitt}_{R^-_{L_1}}(A^-_{L_1})$, and

$$c_{L_n/K_1}((\gamma-\kappa(\gamma))\theta^-_{L_n/k}) \in \mathrm{Fitt}_{R^-_{K_1}}((A^-_{L_1})_G).$$

By Lemma 1.5, $c_{L_n/K_1}(\theta^-_{L_n/k}) = u\theta^-_{K_1/k}$ for some $u \in (R^-_{K_1})^\times$ because every prime of k above p is totally ramified in K_1, and every prime of k which is not above p and which splits in K is unramified. Therefore, we have

$$(\gamma-\kappa(\gamma))\theta^-_{K_1/k} \in \mathrm{Fitt}_{R^-_{K_1}}((A^-_{L_1})_G).$$

By (4.2.5) and (4.2.6), this implies that

$$(\gamma-\kappa(\gamma))\theta^-_{K'_1/k'}\theta^-_{K''_1/k'} \in \mathrm{Fitt}_{R^-_{K_1}}((A^-_{L'_1})_G)\,\mathrm{Fitt}_{R^-_{K_1}}((A^-_{L''_1})_G)$$

and

$$\psi((\gamma-\kappa(\gamma))\theta^-_{K'_1/k'}\theta^-_{K''_1/k'}) \in \mathrm{Fitt}_{O_\psi}(((A^-_{L'_1})_G)_\psi)\,\mathrm{Fitt}_{O_\psi}(((A^-_{L''_1})_G)_\psi).$$

On the other hand, by (4.2.1) and (4.2.3) we have

$$\mathrm{Fitt}_{O_\psi}(((A^-_{L'_1})_G)_\psi)\,\mathrm{Fitt}_{O_\psi}(((A^-_{L''_1})_G)_\psi) \subsetneq (\psi((\gamma-\kappa(\gamma))\theta^-_{K'_1/k'}\theta^-_{K''_1/k'})).$$

This is a contradiction.

By the same method, we can prove that (DSB) does not hold. Suppose that $(\gamma-\kappa(\gamma))\theta_{L_n/k}$ is in $\mathrm{Fitt}_{R_{L_n}}(A_{L_n}^{\vee})$. As we saw in §1, $H^1(\mathrm{Gal}(L_n/L_1), E_{L_n})^- = H^1(\mathrm{Gal}(L_n/L_1), \mu_{p^\infty}(L_n)) = 0$ ([16] Lemma 13.27), which implies that $A_{L_1}^- \longrightarrow A_{L_n}^-$ is injective. Therefore, we get

$$(\gamma-\kappa(\gamma))\theta_{K_1/k}^- \in \mathrm{Fitt}_{R_{K_1}^-}(((A_{L_1}^-)^{\vee})_G)$$

by the same method as above. By (4.2.5) and (4.2.6), we have

$$\begin{aligned}(\gamma-\kappa(\gamma))\theta_{K_1'/k'}^-\theta_{K_1''/k'}^- \in \quad & \mathrm{Fitt}_{R_{K_1}^-}(((A_{L_1'}^-)^{\vee})_G)\,\mathrm{Fitt}_{R_{K_1}^-}(((A_{L_1''}^-)^{\vee})_G) \\ & = \mathrm{Fitt}_{R_{K_1}^-}(((A_{L_1}^-)^{\vee})_G).\end{aligned}$$

But (4.2.2) and (4.2.4) imply that

$$\mathrm{Fitt}_{O_\psi}((((A_{L_1}^-)^{\vee})_G)_\psi) \subsetneq (\psi((\gamma-\kappa(\gamma))\theta_{K_1'/k'}^-\theta_{K_1''/k'}^-)),$$

which is a contradiction. This completes the proof of Theorem 0.2.

4.3. We give an example which satisfies the conditions of Theorem 0.2. We consider $p=3$, $k'=\mathbb{Q}(\sqrt{1901})$ and $K'=k'(\mu_3)$. Let F_α' (resp. F_β') be the minimal splitting field of $X^3-84X-191$ (resp. $X^3-57X-68$). Both F_α' and F_β' are $\mathfrak{S}_3$-extensions over $\mathbb{Q}$ containing k'. We put $F'=F_\alpha'F_\beta'$. The prime (3) of k' is ramified in F_β' , so in F'. The extension F'/k' is unramified outside 3. The Galois group $G=\mathrm{Gal}(F'/k')$ is not cyclic and isomorphic to $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$. Put $L'=F'K'$. Then L'/k' satisfies both (NTZ) and (R) as we explained in §2. From our construction (see §2), we know $F'\cap k_\infty'=k'$, and every prime above 3 is totally ramified in F_∞'/F'.

We put $K''=k'(\sqrt{-2})$. Then $A_{K''}^-=0$, and (3) splits in K''/k'. Put $L''=F'K''$. Then L''/K'' is unramified outside (3). We take $k=k'(\sqrt{6})=\mathbb{Q}(\sqrt{6},\sqrt{1901})$, $F=kF'$, $K=kK'=K'K''$, and $L=kL'$. Thus, the extension L/k satisfies all the conditions of Theorem 0.2, namely the conditions in the subsection 3.1. Applying Theorem 0.2, we know that neither (SB) nor (DSB) holds for L_n/k for all $n\geq 1$.

References

[1] Brown, K. S., *Cohomology of groups*, Graduate Texts in Math. **87**, Springer-Verlag 1982.

[2] Deligne, P. and Ribet, K., Values of abelian L-functions at negative integers over totally real fields, Invent. math. **59** (1980), 227-286.

[3] Greither, C., Arithmetic annihilators and Stark-type conjectures, *Stark's Conjectures: Recent Work and New Directions*, Contemporary Math. **358** (2004), 55-78.

[4] Greither, C., Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture, Compositio Math. **143** (2007), 1399-1426.

[5] Greither, C. and Kurihara, M., Stickelberger elements, Fitting ideals of class groups of CM fields, and dualisation, Math. Zeitschrift **260** (2008), 905-930.

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

[7] Kurihara, M., Iwasawa theory and Fitting ideals, J. reine angew. Math. **561** (2003), 39-86.

[8] Kurihara, M., On stronger versions of Brumer's conjecture, Tokyo Journal of Math. **34** (2011), 407-428.

[9] Kurihara, M. and Miura, T., Stickelberger ideals and Fitting ideals of class groups for abelian number fields, Math. Annalen **350** (2011), 549-575.

[10] Mazur, B. and Wiles, A., Class fields of abelian extensions of $\mathbf{Q}$, Invent. math. **76** (1984), 179-330.

[11] Nickel, A., On the equivariant Tamagawa number conjecture in tame CM-extensions, Math. Zeitschrift **268** (2011), 1-35.

[12] Northcott, D. G., *Finite free resolutions*, Cambridge Univ. Press, Cambridge New York 1976.

[13] Popescu, C., Stark's question and a refinement of Brumer's conjecture extrapolated to the function field case, Compos. Math. **140** (2004), 631-646.

[14] Serre, J.-P., *Corps Locaux*, Hermann, Paris 1968 (troisième édition).

[15] Tate, J., *Les conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, Progress in Math. **47**, Birkhäuser 1984.

[16] Washington, L., *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag 1982.

[17] Wiles, A., The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493-540.

Masato Kurihara and Takashi Miura
Department of Mathematics,
Keio University,
3-14-1 Hiyoshi, Kohoku-ku,
Yokohama, 223-8522, Japan
kurihara@math.keio.ac.jp
t-miura@math.keio.ac.jp