On units generated by Euler systems

Anupam Saikia

Department of Mathematics, IIT Guwahati,

Guwahati 781039.

Email: a.saikia@iitg.ernet.in

Abstract: In the context of cyclotomic fields, it is still unknown whether there exist Euler systems other than the ones derived from cyclotomic units. Nevertheless, we first give an exposition on how norm-compatible units are generated by any Euler system, following work of Coates. Then we prove that the units obtained from Euler systems and the cyclotomic units generate the same $\mathbb{Z}_p$-module for any odd prime p. The techniques adopted for the Iwasawa theoreitc proof in latter part of this article originated in Rubin's work on main conjectures of Iwasawa theory.

1 Introduction

Euler systems were introduced by Thaine and Kolyvagin. Later, Rubin used Euler system of cyclotomic units and elliptic units to prove the main conjecture of Iwasawa theory in various set-ups. In [Co], Coates gave a definition of Euler systems in the context of elliptic curves. His definition is somewhat stronger and different from that of Rubin and Kolyvagin, but it fits more closely with earlier work of Coates and Wiles ([CW 1], [CW 2]). In the context of cyclotomic fields, the definition analogous to [Co] is as follows. Let S be any finite set of rational primes, always containing 2. Let

$$W_S = \{\zeta \in \bar{Q} : \zeta^n = 1 \text{ with } (n, S) = 1\}.$$

DEFINITION : An Euler system is a map $\phi : W_S \longrightarrow \bar{Q}^\times$ which satisfies the following axioms:

- (E 1) $\phi(\eta^\sigma) = \phi(\eta)^\sigma \ \forall \ \sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, and $\phi(\eta^{-1}) = \phi(\eta)$.

- (E 2) If p is any rational prime not in S, we have

$$\prod_{\zeta \in \mu_p} \phi(\zeta\eta) = \phi(\eta^p) \ \forall \eta \in W_S.$$

- (E 3) Let p be any rational prime not in S. Then, for all $\eta \in W_S$ of order prime to p, and all $\zeta \in \mu_p$, we have

$$\phi(\zeta\eta) \equiv \phi(\eta) \bmod \mathfrak{p} \ \forall \mathfrak{p}|p. \tag{1}$$

[Here, $\mathfrak{p}$ is a prime ideal over p in any field that contains $\phi(\zeta\eta)$].

The basic example of an Euler system is essentially the classical system of cyclotomic units. We briefly describe them. Let Ω denote the non-zero integers $a_1, \ldots a_r$ and integers $n_1, \ldots, n_r$ such that $\sum_{j=1}^r n_j = 0$. Let $\lambda_\Omega(T)$ be given by

$$\lambda_\Omega(T) = \prod_{j=1}^r (T^{-a_j} - T^{a_j})^{n_j}.$$

Let S be the set consisting of 2 and all primes q such that q divides at least one of the a_i. Let $\phi_\Omega : W_S \longrightarrow \bar{Q}^\times$ be defined as

(i) $\phi_\Omega(\eta) = \lambda_\Omega(\eta)$ for $\eta \in W_S$ and $\eta \neq 1$.

(ii) $\phi_\Omega(1) = \lim_{T \to 1} \lambda_\Omega(T) = \prod_{j=1}^r a_j^{n_j}$.

It is easy to check that ϕ_Ω forms an Euler system. Given an Euler system $\phi : W_S \longrightarrow \bar{\mathbb{Q}}^\times$, there are two ways of constructing new ones:

- If n is any non-zero integer, $\phi \circ n$ is again an Euler system provided we enlarge S to include primes dividing n.

- If ξ is a primitive h-th root of 1, define $\phi_\xi(\eta) = \prod_\tau \phi(\eta\xi^\tau)$ where τ runs over the elements of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. Here, we enlarge S by including all the primes that divide h.

It is still unknown whether there exist Euler systems attached to cyclotomic fields other than those mentioned above.

2 Euler systems generate global units

In this section, we will explain how Euler systems attached to cyclotomic fields generate norm-compatible global units in the cyclotomic tower. The next three propositions are consequences of the axioms (E 1), (E 2) and (E 3), and are cyclotomic analogues of results in [Co]. For each $m \geq 1$, let μ_m denote the group of m-th roots of unity. If $\eta \in \mu_m$, with $(m, S) = 1$, then (E 1) shows that $\phi(\eta) \in \mathbb{Q}(\mu_m)^+ \subset \mathbb{Q}(\mu_m)$, where L^+ denotes the maximal real subfield of L. Let $\mathbb{Q}_m$ denote the cyclotomic field $\mathbb{Q}(\mu_m)$ and H_m denote the maximal real subfield of $\mathbb{Q}_m$, i.e., $H_m = \mathbb{Q}(\mu_m)^+$.

Proposition 2.1 *Let η be an element of μ_m with $(m, S) = 1$. Let p be any prime with $(p, m) = 1$, and $p \notin S$, Then, we have*

$$N_{H_{mp}/H_m}\phi(\zeta\eta) = \phi(\eta)^{Frob_p - 1} \quad \forall \zeta \in \mu_p, \ \eta \neq 1. \tag{2}$$

Here, $Frob_p$ denotes the Frobenius element of p in the Galois group of H_m over $\mathbb{Q}$, which is unramified at p.

Proof: By axiom E1 and E2,

$$N_{H_{mp}/H_m}\phi(\zeta\eta) = \prod_{\sigma \in Gal(H_{mp}/H_m)} \phi(\zeta\eta)^{\sigma} = \prod_{\sigma \in Gal(\mathbb{Q}_{mp}/\mathbb{Q}_m)} \phi(\zeta^\sigma \eta^\sigma)$$

$$= \frac{\prod_{\xi \in \mu_p} \phi(\xi\eta)}{\phi(1.\eta)} = \frac{\phi(\eta^p)}{\phi(\eta)} = \phi(\eta)^{Frob_p - 1}. \quad \square$$

Proposition 2.2 *Let η be any element of μ_m with $(m, S) = 1$. Let p be any prime with $(p, m) = (p, S) = 1$. For each $n \geq 0$, let ζ_n be a primitive p^{n+1}-root of 1 such that $\zeta_{n+1}^p = \zeta_n$. Then the sequence $\phi(\zeta_n\eta^{Frob_p^{-n}})(n = 0, 1, \ldots)$, is norm compatible in the tower H_{mp^∞} over H_{mp}.*

Proof: By axioms E1 and E2,

$$N_{H_{mp^{n+1}}/H_{mp^n}}\phi(\zeta_n\eta^{Frob_p^{-n}}) = \prod_{\sigma \in Gal(H_{mp^{n+1}}/H_{mp^n})} \phi(\zeta_n\eta^{Frob_p^{-n}})^{\sigma} = \prod_{\sigma \in Gal(\mathbb{Q}_{mp^{n+1}}/\mathbb{Q}_{mp^n})} \phi(\zeta_n^\sigma\eta^{Frob_p^{-n}})$$

$$= \prod_{\xi \in \mu_p} \phi(\xi\zeta_n\eta^{Frob_p^{-n}}) = \phi(\zeta_n^p\eta^{pFrob_p^{-n}}) = \phi(\zeta_{n-1}\eta^{Frob_p^{-(n-1)}}). \quad \square$$

Proposition 2.3 *For all $\eta \in W_S$ with $\eta \neq 1$, $\phi(\eta)$ is a unit.*

In order to prove the above proposition, we need the following lemma:

Lemma 2.4 *Let p be any prime and $K/\mathbb{Q}$ be a finite extension. Let $\alpha \in K$ be a universal norm in the tower $K(\mu_{p^\infty})$. Then every prime ideal in the factorization of α divides p.*

Proof: Let $\mathfrak{q}$ be a prime not dividing p that occurs in the factorization of α. Now, the Galois group $Gal(K(\mu_{p^\infty})/K)$ is a subgroup of $\mathbb{Z}_p^\times$. After finitely extending K, we can assume that the Galois group is $\mathbb{Z}_p$. Since $\mathfrak{q}$ is unramified in the tower, it is enough to show that its decomposition group in non-trivial. Then, $\mathfrak{q}$ will be an inert prime, and infinite power of $\mathfrak{q}$ will divide the universal norm α, which is absurd. If the decomposition group is trivial, it will imply that the residue fields in the tower $K(\mu_{p^\infty})/F$ are finite. But, if ζ and ξ are p-power roots of unity, then $\zeta \not\equiv \xi$ modulo $\mathfrak{q}$ unless $\mathfrak{q}$ lies above p.

Proof of proposition 2.3: Let η be a primitive root of order $m = p^{n+1}b$, where $(p, b) = 1$. Let us denote the number field $\mathbb{Q}(\eta)^+$ by K. We know that $\phi(\eta) \in K$. Let $\mathfrak{q}$ be a prime ideal in K that divides $\phi(\eta)$. By proposition 2.2, $\phi(\eta)$ is a universal norm in the tower $\mathbb{Q}(\mu_{p^\infty}\eta)^+$ over $K = \mathbb{Q}(\eta)^+$. Clearly, $\phi(\eta)^2 \in K$ is a universal norm in the tower $K(\mu_{p^\infty})$ over K. Hence, $\mathfrak{q}$ must divide p by the above lemma. If b is not 1 we are through, as $\mathfrak{q}$ must also divide any prime factor of b.

Now consider the case $b = 1$. Then $\eta = \zeta_n$, and by proposition 2.2, $N_{H_{p^{n+1}}/H_p}\phi(\zeta_n) = \phi(\zeta_0)$. Now,

$$
\begin{aligned}
N_{H_p/\mathbb{Q}}\phi(\zeta_0) &= \left(N_{\mathbb{Q}(\mu_p)/\mathbb{Q}}\phi(\zeta_0)\right)^{\frac{1}{2}} \\
&= \left(\prod_{\sigma \in Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})} \phi(\zeta_0)^\sigma\right)^{\frac{1}{2}} \\
&= \left(\prod_{\sigma \in Gal(\mathbb{Q}(\mu_p)/\mathbb{Q})} \phi(\zeta_0^\sigma)\right)^{\frac{1}{2}} \\
&= \left(\frac{\prod_{\xi \in \mu_p} \phi(\xi)}{\phi(1)}\right)^{\frac{1}{2}} \\
&= \left(\frac{\phi(1)}{\phi(1)}\right)^{\frac{1}{2}} = \pm 1.
\end{aligned}
$$

Noting that $K = \phi(\zeta_n)^+$ is totally ramified over $\mathbb{Q}$ at p, we have only one prime $\mathfrak{q}$ of K above p. But now $(\phi(\eta)) = \mathfrak{q}^r$ for some integer r, and r has to be zero as the norm of $\phi(\eta)$ is ± 1. Thus, $\phi(\eta)$ is a global unit in the ring of integers of K. $\qquad\square$

Thus, we can conclude that Euler systems attached to cyclotomic fields generate norm-compatible global units.

3 Statement of main result

Let p be an odd prime, and ζ_n be a fixed p^{n+1}-th root of unity such that $\zeta_{n+1}^p = \zeta_n \forall n \geq 0$. Let F_n denote the number field $\mathbb{Q}(\zeta_n)^+$. Let

$$\mathcal{H}(p) = \text{ the set of Euler systems } \phi : W_S \longrightarrow \bar{\mathbb{Q}}^\times \text{ such that } p \notin S.$$

By proposition 2.3, above, $\phi(\zeta_n)$ is a global unit in F_n for any $\phi \in \mathcal{H}(p)$. By proposition 2.2,

$$N_{F_{n+1}/F_n}\phi(\zeta_{n+1}) = \phi(\zeta_n). \tag{3}$$

4

Let us define

$$\mathcal{E}_n = \{\phi(\zeta_n) \mid \phi \in \mathcal{H}(p)\}.$$

Let E_n and C_n denote respectively the global units and the cyclotomic units in F_n. Let $\mathfrak{p}_n$ be the unique maximal ideal of F_n above p. We denote the completion of F_n at $\mathfrak{p}_n$ by Φ_n. Let U_n be the principal local units of Φ_n, i.e., the local units in Φ_n congruent to $1 \mod \mathfrak{p}_n$. Let $E_{n,1}$, $C_{n,1}$ and $\mathcal{E}_{n,1}$ denote respectively the subgroup of principal units in E_n, C_n and $\mathcal{E}_n$. These subgroups can be canonically embedded in U_n. Let $\tilde{E}_{n,1}$, $\tilde{C}_{n,1}$ and $\tilde{\mathcal{E}}_{n,1}$ be respectively the closure of $E_{n,1}$, $C_{n,1}$ and $\mathcal{E}_{n,1}$ in U_n. Let $\bar{E}_n = \mathbb{Z}_p \otimes E_n$, $\bar{C}_n = \mathbb{Z}_p \otimes C_n$ and $\bar{\mathcal{E}}_n = \mathbb{Z}_p \otimes \mathcal{E}_n$. By Leopoldt's conjecture, which is proved to be true for the abelian extensions F_n of $\mathbb{Q}$, we have $\bar{E}_n = \tilde{E}_{n,1}$, $\bar{C}_n = \tilde{C}_{n,1}$ and $\bar{\mathcal{E}}_n = \tilde{\mathcal{E}}_{n,1}$. Hence we have a natural inclusion

$$\bar{C}_n \subset \bar{\mathcal{E}}_n \subset \bar{E}_n.$$

The main result of this paper is the theorem below:

Theorem 3.1 *The $\mathbb{Z}_p$-module generated by the global units derived from Euler systems attached to p-power cyclotomic fields is the same as the $\mathbb{Z}_p$-module generated by the cyclotomic units. In other words, $\bar{\mathcal{E}}_n = \bar{C}_n$.*

Note that the index of $\bar{C}_n$ in $\bar{E}_n$ equals $h_{p,n}$, where $h_{p,n}$ denotes the p-part of the class number of $F_n = \mathbb{Q}(\zeta_n)^+$. Vandiver has conjectured that $h_{p,0} = 1$ (which is equivalent to saying that $h_{p,n} = 1$ for all $n = 0, 1, 2, \ldots$). If one can show that $[\bar{E}_0 : \bar{\mathcal{E}}_0] = 1$, then it will imply Vandiver's conjecture by virtue of theorem 3.1. Of course, even to attempt this approach to Vandiver's conjecture, one would certainly require an Euler system which is not derived from cyclotomic units.

Another interesting point to note here is the connection of theorem 3.1 to Greenberg's conjecture. Greenberg's conjecture is equivalent to the statement that the only universal norms in $\bar{E}_0$ is the group $\bar{C}_0$. Since the values of Euler systems are universal norms, theorem 3.1 gives evidence for Greenberg's conjecture. One can raise the question whether the only universal norms in each $\bar{E}_n$ are those coming from Euler systems.

We will prove the above theorem by establishing a relation involving Iwasawa modules, and then by descent.

4 Iwasawa theoretic set-up

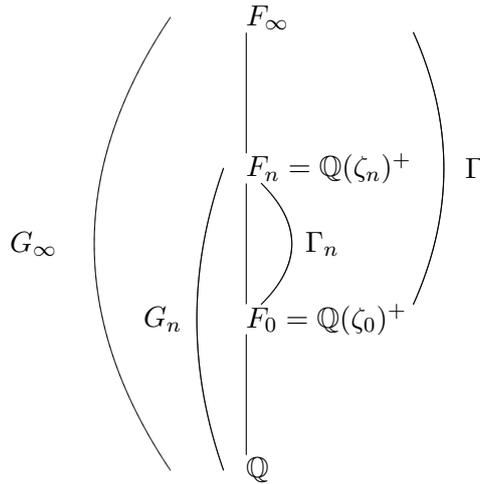Let us consider the infinite extension

$$F_\infty = \cup_{n \geq 0} F_n,$$

where $F_n = \mathbb{Q}(\zeta_n)^+$ and ζ_n is a primitive p^{n+1}-th root of unity such that $\zeta_{n+1}^p = \zeta_n$. Let us define the Galois groups

$$G_n = G(F_n/\mathbb{Q}), \qquad \Gamma_n = G(F_n/F_0).$$

Let G_∞ be the Galois group of F_∞ over $\mathbb{Q}$ and Γ be the Galois group $\mathrm{Gal}(F_\infty/F_0)$. Clearly,

$$G_\infty = G(F_\infty/\mathbb{Q}) = \Delta \times \Gamma, \quad \text{where } \Delta \simeq G(F_1/\mathbb{Q}).$$

We have the following field diagram:

Let R_n be the group ring of G_n with coefficients in $\mathbb{Z}_p$. These group rings form an inverse system under the canonical maps from R_m to R_n. We define

$$R_\infty = \varprojlim_n \mathbb{Z}_p[G_n].$$

A R_∞-module N is called a torsion R_∞-module if it is annihilated by a non-zero-divisor in R_∞. If N is a finitely generated torsion R_∞-module, then there is an injective R_∞-module homomorphism

$$\bigoplus_{i=1}^{r} R_\infty/g_i R_\infty \hookrightarrow N \tag{4}$$

with finite cokernel. The elements g_i are not uniquely determined, but the ideal $\prod_i g_i R_\infty$ is. We call the ideal $\prod_i g_i R_\infty$ the *characteristic ideal* of N and denote it by $\mathrm{char}(N)$. The characteristic ideal is multiplicative in exact sequence: if $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ is an exact sequence of torsion R_∞-modules then

$$\mathrm{char}(N) = \mathrm{char}(N')\mathrm{char}(N'').$$

From now on, M will always denote a fixed power of p. We denote the group ring of G_n with coefficients in $\mathbb{Z}_p$ modulo M by $R_{n,M}$, i.e.,

$$R_{n,M} = (\mathbb{Z}/M\mathbb{Z})\,[G_n] = R_n/MR_n.$$

We denote the p-part of the ideal class group of F_n by A_n. These groups form an inverse system under the norm maps and we denote the inverse limit by A_∞.

Now, the $\mathbb{Z}_p$-modules U_n, $\bar{C}_n$, $\bar{\mathcal{E}}_n$ and $\bar{E}_n$ defined in the previous section are equipped with an R_n-module structure. They form an inverse system of R_n-modules with respect to the norm maps. Thus, we define the inverse limits

$$U_\infty = \varprojlim_n U_n, \ \ E_\infty = \varprojlim_n \bar{E}_n, \ \ \mathcal{E}_\infty = \varprojlim_n \bar{\mathcal{E}}_n, \ \ C_\infty = \varprojlim_n \bar{C}_n.$$

These inverse limits have the natural structure of a R_∞-module. We will first determine a relation between the Iwasawa modules $\mathcal{E}_\infty$ and C_∞. Then, we will descend to the n-th layer.

Proposition 4.1 *The characteristic ideal of A_∞ contains the characteristic ideal of $E_\infty/\mathcal{E}_\infty$.*

Proof of theorem 3.1 assuming proposition 4.1 : Our main result follows easily from proposition 4.1. We have the following exact sequence of R_∞-modules

$$0 \longrightarrow \mathcal{E}_\infty/C_\infty \longrightarrow E_\infty/C_\infty \longrightarrow E_\infty/\mathcal{E}_\infty \longrightarrow 0.$$
$$\Rightarrow \ \mathrm{char}(E_\infty/C_\infty) = \mathrm{char}(E_\infty/\mathcal{E}_\infty)\mathrm{char}(\mathcal{E}_\infty/C_\infty). \tag{5}$$

By "main conjecture" of Iwasawa theory for cyclotomic fields, we have

$$\mathrm{char}(A_\infty) = \mathrm{char}(E_\infty/C_\infty) \tag{6}$$

Then proposition 4.1 combined with (5) and (6) imply that $\mathrm{char}(\mathcal{E}_\infty/C_\infty) = R_\infty$. That tells us that $\mathcal{E}_\infty/C_\infty$ is a finite R_∞ submodule of U_∞/C_∞. However, it is well-known

that $U_\infty/C_\infty \simeq R_\infty/(g)$. For instance, the results in [Sa] gives an explicit proof of this fact. Hence, U_∞/C_∞ has no non-trivial finite R_∞-submodule. Thus, $\mathcal{E}_\infty/C_\infty = 0$, and $(C_\infty)_{\Gamma_n} = (\mathcal{E}_\infty)_{\Gamma_n}$. However, by the R_∞-module structure of C_∞, we know that $(C_\infty)_{\Gamma_n} = \bar{C}_n$. Moreover, $(\mathcal{E}_\infty)_{\Gamma_n} \twoheadrightarrow \bar{\mathcal{E}}_n$. Thus, the canonical injection $\bar{C}_n \longrightarrow \bar{\mathcal{E}}_n$ is also surjective, and we have our main result.

Our approach to proposition 4.1 will be as follows. We will use the units generated by Euler systems to construct new elements (called Koyvagin class), which factorize non-trivially. We will then determine the factorization of these new elements (proposition 6.2). This gives us a systematic way of obtaining relations in the ideal class group. These relations will be recast in Iwasawa theoretic set-up, and we will obtain a suitable ideal which annihilates the Iwasawa module of class groups. This approach originated in Rubin's work. In the remaining sections, we will closely follow Rubin's proof of the main conjectures of Iwasawa theory.

5   Kolyvagin class

From now on, we fix n and refer to F_n simply as F, dropping the subscript. In this section, we will construct elements in $F^\times$ using the global units derived from any Euler system. The factorization of these elements can be easily determined, which will be shown in the following section. Let M be a fixed power of p. Let $\mathcal{S}_M$ be the set of square-free integers s such that each prime factor q of s splits in $F/\mathbb{Q}$ and $q \equiv 1 \bmod M$. For the rest of this paper, q will always denote a rational prime in $\mathcal{S}_M$, and $\mathfrak{q}$ will be a primes of F above q. Let η_q be a fixed primitive q-th root of 1. We write $F(q)$ for the field $F(\eta_q)$ and $G(q)$ for the Galois group $G(F(\eta_q)/F)$. Clearly, $\mathfrak{q}$ is totally ramified in $F(q)/F$ and the ramification index is $(q-1)$. Suppose σ_q in $G(q)$ sends η_q to η_q^t, where t is a primitive root mod q. Then $G(q)$ is cyclic and generated by σ_q.

As in [Ru 4], let us now define the following operators:

$$D_q = \sum_{i=1}^{q-2} i\sigma_q^i, \;\; D_s = \prod_{q|s} D_q, \;\; \text{and} \;\; N_q = \sum_{i=0}^{q-2} \sigma_q^i.$$

It is easily seen that

$$(\sigma_q - 1)D_q = (q - 1 - N_q). \tag{7}$$

From (2) of pp. 3, it follows that

$$
\begin{aligned}
N_q D_r \phi(\zeta_n \eta_{rq}) &= D_r N_{F(rq)/F(r)} \phi(\zeta_n \eta_{rq}) \\
&= (\mathrm{Frob}_q - 1) D_r \phi(\zeta_n \eta_r).
\end{aligned}
\tag{8}
$$

Proposition 5.1 $D_s \phi(\zeta_n \eta_s)$ *is an element of* $\left((F(s)^\times)/(F(s)^\times)^M \right)^{G(s)}$. *In other words,* $[(\sigma - 1) D_s \phi(\zeta_n \eta_s)]^{\frac{1}{M}}$ *is a well defined element of* $F(s)^\times$ *for all* σ *in* $G(s)$.

PROOF : We use induction on the number of primes dividing s. Suppose $q|s$ and $s = qr$. Then

$$
\begin{aligned}
(\sigma_q - 1) D_s \phi(\zeta_n \eta_s) &= (\sigma_q - 1) D_q D_r \phi(\zeta_n \eta_s) \\
&= (q - 1) D_r \phi(\zeta_n \eta_s)/(\mathrm{Frob}_q - 1) D_r \phi(\zeta_n \eta_r) \quad \text{(by (7) and (8)).}
\end{aligned}
$$

Since q is in $\mathcal{S}_M$, $M|(q-1)$. As $\mathrm{Frob}_q \in G(r)$, the induction hypothesis implies that the denominator in the last expression above is in $(F(r)^\times)^M$. Therefore,

$$
(\sigma_q - 1) D_s \phi(\zeta_n \eta_s) \in (F(s)^\times)^M.
$$

Since the σ_q generate $G(s)$, this completes the proof of the proposition. $\qquad \square$

As σ runs over the elements of $G(s)$, $\sigma \mapsto [(\sigma - 1) D_s \phi(\zeta_n \eta_s)]^{\frac{1}{M}}$ gives an element of $H^1\left(G(s), F(s)^\times\right)$. By Hilbert 90, this cohomology group is trivial. Therefore, there is an element $\beta_{s,\phi}$ in $F(s)^\times$ such that

$$
[(\sigma - 1) D_s \phi(\zeta_n \eta_s)]^{\frac{1}{M}} = (\sigma - 1) \beta_{s,\phi}.
\tag{9}
$$

Clearly, $\beta_{s,\phi}$ is unique up to multiplication by an element of $F^\times$. We can now make the following definition.

DEFINITION : *For* $s \in \mathcal{S}_M$, *Kolyvagin class is defined as*

$$
\kappa_{\phi,M}(s) = \frac{D_s \phi(\zeta_n \eta_s)}{\beta_{s,\phi}^M} \in F^\times/(F^\times)^M,
\tag{10}
$$

where ϕ is an Euler system in $\mathcal{H}(p)$ and $\beta_{s,\phi}$ is given by (9).

6 Factorization of Kolyvagin class

In the previous section we constructed certain elements, called Kolyvagin classes, in the $F^\times$ modulo Mth powers, where $F = \mathbb{Q}(\zeta_n)^+$. Here we will describe how one can determine the factorization of those elements. Such a factorization should be seen as a relation in the ideal class group of F. This process will lead to construction of an annihilator of the class group of F in the group ring $\frac{\mathbb{Z}}{M\mathbb{Z}}[Gal(F/\mathbb{Q}]$.

Let $\mathcal{O}_F$ be the ring of integers of F and

$$I_F = I = \bigoplus \mathbb{Z}\mathfrak{q}$$

be the group of fractional ideals of F written additively. Let

$$I_{F,q} = I_q = \bigoplus_{\mathfrak{q}|q} \mathbb{Z}\mathfrak{q}.$$

For any $x \in F^\times$, let $(x) \in I$ be the principal ideal generated by x, and $(x)_q$, $[x]_M$, and $[x]_{q,M}$ the projections of (x) to I_q, I/MI, and I_q/MI_q respectively. When there is no ambiguity, we drop the subscript M and simply write $[x]$ or $[x]_q$. Note that $[x]$ and $[x]_q$ are well defined for $x \in F^\times/(F^\times)^M$. The next two propositions are cyclotomic analogues of lemma 13 and theorem 14 in [Co]:

Proposition 6.1 *There is a Galois equivariant isomorphism*

$$\lambda_q : \left(\mathcal{O}_F/q\mathcal{O}_F\right)^\times / \left(\left(\mathcal{O}_F/q\mathcal{O}_F\right)^\times\right)^M \longrightarrow I_q/MI_q.$$

PROOF : Let $\tilde{\mathfrak{q}}$ be the unique prime of $F(q)$ above the prime $\mathfrak{q}$ of F and $\pi(\tilde{\mathfrak{q}})$ be a local parameter at $\tilde{\mathfrak{q}}$. The residue fields of q, $\mathfrak{q}$ and $\tilde{\mathfrak{q}}$ will be denoted by $k(q)$, $k(\mathfrak{q})$ and $k(\tilde{\mathfrak{q}})$ respectively. As q splits in F and $\mathfrak{q}$ is totally ramified in $F(q)/F$, the residue fields are all isomorphic. We have an isomorphism

$$G(q) \longrightarrow k(\tilde{\mathfrak{q}})^\times, \qquad \sigma \mapsto \pi(\tilde{\mathfrak{q}})^{1-\sigma} \bmod \tilde{\mathfrak{q}}.$$

Note that since $G(q)$ is the inertia group in $F(q)/F$, the above isomorphism does not depend on the choice of the parameter $\pi(\tilde{\mathfrak{q}})$. If σ_q maps to $\gamma(\tilde{\mathfrak{q}})$ under the above isomorphism, then clearly $\gamma(\tilde{\mathfrak{q}})$ is a generator of $k(\tilde{\mathfrak{q}})^\times$. By our identification above, $\gamma(\tilde{\mathfrak{q}})$ can be regards as a generator of $k(\mathfrak{q})^\times$. For any $w \in \left(\mathcal{O}_F/q\mathcal{O}_F\right)^\times$, we have

$$w \equiv \gamma(\tilde{\mathfrak{q}})^{a(\mathfrak{q})} \bmod \mathfrak{q} \text{ for some integer } a(\mathfrak{q}) \bmod (q-1).$$

Let us define
$$\lambda_q(w) = \sum_{\mathfrak{q}|q} (a(\mathfrak{q}) \bmod M)\, \mathfrak{q}.$$

Galois equivariance and surjectivity follow easily. Since both sides have the same cardinality, we have a Galois equivariant isomorphism. □

Note : Since q splits in F, we have a Galois equivariant map

$$\bar{\lambda}_q : \left(\mathcal{O}_F/q\mathcal{O}_F\right)^\times / \left(\left(\mathcal{O}_F/q\mathcal{O}_F\right)^\times\right)^M \longrightarrow \mathbb{Z}/M\mathbb{Z}\,[G]$$

given by

$$\bar{\lambda}_q(w)\mathfrak{q} = \lambda_q(w), \tag{11}$$

where we fix a $\mathfrak{q}$ above q.

Proposition 6.2 *For $qs \in \mathcal{S}_M$, we have*

$$(i)\ \left[\kappa_{\phi,M}(s)\right]_q = 0.$$
$$(ii)\ \left[\kappa_{\phi,M}(sq)\right]_q = \lambda_q(\kappa_{\phi,M}(s)).$$

PROOF : Recall that
$$\kappa_{\phi,M}(s) = \frac{D_s\phi(\zeta_n\eta_s)}{\beta_{s,\phi}^M} \in F^\times/(F^\times)^M.$$

Since $\phi(\zeta_n\eta_s)$ is a unit in $F(s)$, so is $D_s\phi(\zeta_n\eta_s)$. Hence, the ideal generated by $\kappa_{\phi,M}(s)$ in $F(s)$ is determined by $\beta_{s,\phi}$. Note that q does not divide s, because qs is a square-free integer.

(i) q is unramified in $F(s)$, and $\beta_{s,\phi}^M$ is an M-th power in $F(s)$.

(ii) Let $\tilde{\mathcal{Q}}$ be a prime of $F(sq)$ above the prime $\mathfrak{q}$ of F. The ramification index of $\tilde{\mathcal{Q}}$ in $F(sq)/F$ is $(q-1)$. By definition of $\kappa_{\phi,M}(sq)$,

$$v_{\mathfrak{q}}(\kappa_{\phi,M}(sq)) = -\frac{M}{q-1}v_{\tilde{\mathcal{Q}}}(\beta_{sq,\phi}). \tag{12}$$

Since $F(sq)/F(q)$ is unramified at $\tilde{\mathcal{Q}}$, the local parameter $\pi(\tilde{\mathfrak{q}})$ at the prime ideal $\tilde{\mathfrak{q}}$ of $F(q)$ is also a local parameter at $\tilde{\mathcal{Q}}$. We have the following diagram of fields and prime ideals:
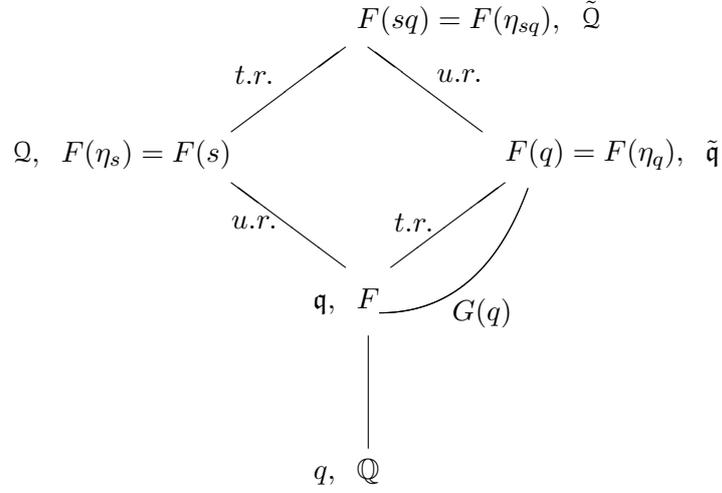
Let $v_{\tilde{\mathcal{Q}}}(\beta_{sq,\phi}) = b$. Then,

$$\beta_{sq,\phi} = \pi(\tilde{\mathfrak{q}})^b u, \quad \text{where } u \in F(sq) \text{ is prime to } \tilde{\mathcal{Q}}.$$

$$\Rightarrow \beta_{sq,\phi}^{1-\sigma_q} = \pi(\tilde{\mathfrak{q}})^{(1-\sigma_q)b} u^{1-\sigma_q}$$

$$\equiv \gamma(\tilde{\mathfrak{q}})^b \mod \tilde{\mathcal{Q}} \text{ (as } \sigma_q \text{ acts trivially on } u \text{ modulo } \tilde{\mathcal{Q}}).$$

From (9),

$$
\begin{aligned}
\beta_{sq,\phi}^{\sigma_q-1} &= \left[(\sigma_q - 1)D_{sq}\phi(\zeta_n\eta_{sq})\right]^{\frac{1}{M}} \\
&= \left[D_s\phi(\zeta_n\eta_{sq})^{(q-1)}/D_s\phi(\zeta_n\eta_s)^{\mathrm{Frob}_q-1}\right]^{\frac{1}{M}} \text{ [by (7) and (8)]} \\
&= \left[D_s\phi(\zeta_n\eta_{sq})^{(q-1)}/(\beta_{s,\phi}^M)^{\mathrm{Frob}_q-1}\right]^{\frac{1}{M}} \text{ [by (9)]} \\
&\equiv \left[D_s\phi(\zeta_n\eta_s)^{(q-1)}/(\beta_{s,\phi}^M)^{\mathrm{Frob}_q-1}\right]^{\frac{1}{M}} \mod \tilde{\mathcal{Q}} \text{ [by (1)]} \\
&\equiv \left[D_s\phi(\zeta_n\eta_s)/\beta_{s,\phi}^M\right]^{\frac{q-1}{M}} \mod \tilde{\mathcal{Q}} \text{ [since } \mathrm{Frob}_q(x) \equiv x^q \mod \tilde{\mathcal{Q}}] \\
\Rightarrow \gamma(\tilde{\mathfrak{q}})^{-b} &\equiv \kappa_{\phi,M}(s)^{\frac{q-1}{M}} \mod \tilde{\mathcal{Q}} \text{ [by definition of } \kappa_{\phi,M}(s)]. \quad (13)
\end{aligned}
$$

If $\lambda_q(\kappa_{\phi,M}(s)) = \sum_{\mathfrak{q}|q}(a(\mathfrak{q}) \mod M)\mathfrak{q}$,

$$\kappa_{\phi,M}(s) \equiv \gamma(\tilde{\mathfrak{q}})^{a(\mathfrak{q})} \mod \mathfrak{q} \text{ [by definition of } \lambda_q]$$

$$\Rightarrow \gamma(\tilde{\mathfrak{q}})^{-b} \equiv \gamma(\tilde{\mathfrak{q}})^{a(\mathfrak{q})\frac{q-1}{M}} \mod \mathfrak{q} \text{ [by (13)]}$$

Since $\gamma(\tilde{\mathfrak{q}})$ is a generator of $k(\mathfrak{q})^\times$, we have

$$\frac{q-1}{M}a(\mathfrak{q}) \equiv -b \bmod (q-1).$$
$$\Rightarrow \ v_{\mathfrak{q}}(\kappa_{\phi,M}(sq)) \equiv a(\mathfrak{q}) \mod M \ \text{ by } (12) \qquad \square$$

7 Kolyvagin sequence

By standard Iwasawa theory, $(A_\infty)_{\Gamma_n} = A_n$ (see [Wa] for a proof). Since A_n is finite, A_∞ is a finitely generated torsion R_∞-module by Nakayama's lemma. By structure theory of R_∞-modules, there is an exact sequence of R_∞-modules

$$0 \longrightarrow \bigoplus_{i=1}^{r} R_\infty/(f_i) \longrightarrow A_\infty \longrightarrow D \longrightarrow 0, \tag{14}$$

where D is finite. By definition, $\mathrm{char}(A_\infty) = \prod_i f_i R_\infty$. Let $y_i \in A_\infty$ be the image of $1 \in R_\infty/(f_i)$ and $A_\infty^0 = \sum_{i=1}^{r} R_\infty y_i$. Suppose J is the annihilator of $D = A_\infty/A_\infty^0$. Then J is of finite index in R_∞. Let M be a fixed power of p.

From (14), we obtain an exact sequence

$$D^{\Gamma_n} \longrightarrow \bigoplus_{i=0}^{r} R_n/(f_i) \longrightarrow A_n \longrightarrow D_{\Gamma_n} \longrightarrow 0. \tag{15}$$

It follow that $R_n/\mathrm{char}(A_\infty)R_n$ is finite. Let

$$N_n = \mid A_n \mid . \mid \frac{R_n}{\mathrm{char}(A_\infty)R_n} \mid, \qquad M' = MN_n.$$

DEFINITION : *Let $0 \le k \le r$. A Kolyvagin sequence of length k is a k-tuple $\mathfrak{Q} = (\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_k)$ of primes in F such that*

- *the $\mathfrak{q}_i$ lie above distinct rational primes in $\mathcal{S}_M$, and*

- *Frob$_{\mathfrak{q}_i} = \sigma_i|_{L_n}$, where $\sigma_i \in G(L_\infty/F_\infty)$ corresponds to $y_i \in A_\infty$ under Artin reciprocity [where y_i are as defined immediately after (14)].*

For a Kolyvagin sequence $\mathfrak{Q}$, we define the square-free integer $s(\mathfrak{Q})$ as

$$s(\mathfrak{Q}) = \prod_{i=1}^{k} q_i, \qquad \text{where } \ q_i = \mathfrak{q}_i|_{\mathbb{Q}}.$$

8 Key proposition

In this section, we work out the details of the proof of proposition 4.1. It is a simplified version of Rubin's arguments in (see [Ru 1], [Ru 2], [Ru 3], and [Ru 4]) together with ideas of Coates [Co].

Let $\Pi(k, n, M)$ be the set of all Kolyvagin sequence of length k. Let $\Psi(k, n, M)$ be the ideal in $R_{n,M} = R_n / M R_n$ generated by

$$\{\psi(\kappa_{\phi,M}(s(\mathfrak{Q}))) \mid \mathfrak{Q} \in \Pi(k, n, M), \psi \in \mathrm{Hom}_{R_n}(R_{n,M}\kappa_{\phi,M}(s(\mathfrak{Q})), R_{n,M})\}.$$

In order to prove 4.1, we need the following key proposition.

Proposition 8.1 $J\Psi(k, n, MN_n)R_{n,M} \subset f_{k+1}\Psi(k+1, n, M)$.

The following result is from Rubin [Ru 4]:

Lemma 8.2 *Let B be a p-torsion free finitely generated $\mathbb{Z}_p[G]$-module where G is a finite abelian group. If $f \in \mathbb{Z}_p[G]$ is not a zero divisor, $b \in B$, and*

$$\{\psi(b) : \psi \in Hom_{\mathbb{Z}_p[G]}(B, \mathbb{Z}_p[G])\} \subset f\mathbb{Z}_p[G],$$

then $b \in fB$.

Proposition 4.1 can be deduced from proposition 8.1 and lemma 8.2 as follows :

For $k = 0$, $\Pi(0, n, M)$ has just the empty sequence and

$$\{\psi(\kappa_{\phi,M}(1)) \bmod M \mid \psi \in \mathrm{Hom}_{R_n}(\bar{E}_n, R_n)\} \subset \Psi(0, n, M).$$

In other words,

$$\{\psi(\phi(\zeta_n)) \bmod M \mid \psi \in \mathrm{Hom}_{R_n}(\bar{E}_n, R_n)\} \subset \Psi(0, n, M).$$

If we use proposition 3.4 recursively, we obtain

$$J^r\Psi(0, n, MN_n^r)R_{n,M} \subset \mathrm{char}(A_\infty)\Psi(r, n, M) \subset \mathrm{char}(A_\infty)R_{n,M}$$
$$\Rightarrow J^r\psi(\phi(\zeta_n))R_{n,M} \subset \mathrm{char}(A_\infty)R_{n,M} \quad \forall \psi \in \mathrm{Hom}_{R_n}(\bar{E}_n, R_n) \quad \forall M$$
$$\Rightarrow J^r\psi(\phi(\zeta_n))R_n \subset \mathrm{char}(A_\infty)R_n.$$

Substituting $\bar{E}_n$ for B in the lemma above, we get

$$J^r(\phi(\zeta_n)) \subset \mathrm{char}(A_\infty)\bar{E}_n.$$

14

Taking inverse limit as n goes to infinity, we find that

$$J^r \mathcal{E}_\infty \subset \text{char}(A_\infty) E_\infty.$$

There is an obvious exact sequence

$$0 \longrightarrow \mathcal{E}_\infty / J^r \mathcal{E}_\infty \longrightarrow E_\infty / J^r \mathcal{E}_\infty \longrightarrow E_\infty / \mathcal{E}_\infty \longrightarrow 0.$$

Since J^r is an ideal of finite index in R_∞, $\mathcal{E}_\infty / J^r \mathcal{E}_\infty$ is finite and so its characteristic ideal is trivial. Thus,

$$\text{char}(E_\infty / \mathcal{E}_\infty) = \text{char}(E_\infty / J^r \mathcal{E}_\infty). \tag{16}$$

The exact sequence of R_∞-modules

$$0 \longrightarrow \text{char}(A_\infty) E_\infty / J^r \mathcal{E}_\infty \longrightarrow E_\infty / J^r \mathcal{E}_\infty \longrightarrow E_\infty / \text{char}(A_\infty) E_\infty \longrightarrow 0$$

implies that

$$\text{char}(E_\infty / \text{char}(A_\infty) E_\infty) | \text{char}(E_\infty / J^r \mathcal{E}_\infty). \tag{17}$$

It is clear from the structure theorem of R_∞-modules that $\text{char}(A_\infty) \mid \text{char}(E_\infty / \text{char}(A_\infty) E_\infty)$. Therefore, (16) and (17) imply that

$$\text{char}(A_\infty) | \text{char}(E_\infty / \mathcal{E}_\infty).$$

In order to facilitate the proof of proposition 8.1, we need the following lemma.

Lemma 8.3 *Let $0 \le k \le r$ and*

$$\mathfrak{Q} = (\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_{k+1}) \in \Pi(k+1, n, MN_n)$$

be a Kolyvagin sequence. Let q be the rational prime below $\mathfrak{q}_{k+1} = \mathfrak{q}$ and q_i be the rational prime below $\mathfrak{q}_i$ for $1 \le i \le k$. Let $s = \prod_{i=1}^{k} q_i$. Then there is a Galois equivariant map

$$\tilde{\psi} : R_{n,M} \kappa_{\phi,M}(sq) \longrightarrow R_{n,M},$$

such that for any $\rho \in J$, we have

$$\rho \bar{\lambda}_q(\kappa_{\phi,M'}(s)) \equiv f_{k+1} \tilde{\psi}(\kappa_{\phi,M}(sq)) \mod M.$$

15

PROOF : Let $\mathcal{C}_i$ be the class of $\mathfrak{q}_i$ in $A_n = A$. Let $\bar{A}_n$ be the quotient of A_n by the R_n-submodule generated by classes of $\mathcal{C}_1, \mathcal{C}_2, \ldots \mathcal{C}_k$. Let $A_\infty^k = \sum_{i=0}^k R_\infty y_i \subset A_\infty^0$. In the exact sequence (14) of pp. 13, the ideal J of R_∞ annihilates D. Let J_n be the image of J in R_n. From the exact sequence (15) of pp. 13, it is clear that J_n annihilates the kernel of the map

$$(A_\infty^0/A_\infty^k) \otimes R_n \longrightarrow \bar{A}_n.$$

Let $\mathcal{A}$ be the annihilator of the image $\bar{\mathcal{C}}_k$ of the ideal class of $\mathfrak{q}$ in $\bar{A}_n$. The annihilator of the class of $\mathfrak{q}$ in $(A_\infty^0/A_k^0) \otimes R_n$ is $f_{k+1}R_n$. So we have

$$J_n\mathcal{A} \subset f_{k+1}R_n. \tag{18}$$

By proposition 6.2 (i), we have

$$(\kappa_{\phi,M'}(sq)) = [\kappa_{\phi,M'}(sq)]_q \mod (M'I, \ R_n\mathcal{C}_1 + R_n\mathcal{C}_2 + \ldots + R_n\mathcal{C}_k). \tag{19}$$

Since $|A|$ divides $M' = MN_n$, $[\kappa_{\phi,M'}(sq)]_q \in \mathcal{A}R_{n,M'}\mathfrak{q}$, and by (18), $\rho[\kappa_{\phi,M'}(sq)]_q \in f_{k+1}R_{n,M'}$. Since f_{k+1} is not a zero divisor , we have a well defined map

$$f_{k+1}^{-1} : f_{k+1}R_{n,M'} \longrightarrow R_{n,M},$$

$$f_{k+1}g \mapsto h, \quad \text{where } h \text{ is given by}$$

$$f_{k+1}g = f_{k+1}h + MN_n\tilde{h}$$

$(\Rightarrow g = h + M.f_{k+1}^{-1}N_n\tilde{h}, \ \text{note that } f_{k+1} \text{ divides } N_n.)$

We define a map

$$\tilde{\psi} : R_{n,M}\kappa_{\phi,M}(sq) \longrightarrow R_{n,M}, \ \text{by}$$

$$\tilde{\psi}(\kappa_{\phi,M}(sq))\mathfrak{q} = f_{k+1}^{-1}\rho[\kappa_{\phi,M'}(sq)]_q \tag{20}$$

and extend by linearity to the whole of $R_{n,M}\kappa_{\phi,M}(sq)$. We have to verify that $\tilde{\psi}$ is well-defined. Let $\kappa_{\phi,M}(sq)^\tau = \alpha^M$ for some $\tau \in R_n$. We want to show that

$$\tau\tilde{\psi}(\kappa_{\phi,M}(sq)) \in MR_{n,M'}.$$

By (19),

$$(\alpha) = [\alpha]_q \mod (N_nI, \ R_n\mathcal{C}_1 + R_n\mathcal{C}_2 + \ldots + R_n\mathcal{C}_k).$$

Recall that $M' = MN_n$, where N_n is divisible by the order of A_n. Therefore, $[\alpha]_q \in \mathcal{A}R_{n,M'}\mathfrak{q}$ and by (18),

$$\rho[\alpha]_q \in f_{k+1}R_{n,M'}\mathfrak{q}$$

$$\tilde{\psi}(\kappa_{\phi,M}(sq)^\tau)\mathfrak{q} = \tau f_{k+1}^{-1}\rho[\kappa_{\phi,M}(sq)]_q$$

$$= f_{k+1}^{-1}\rho M[\alpha]_q \subset MR_{n,M'}.$$

16

Hence $\tilde{\psi}$ is well defined. Now, proposition 2.3 (ii), (20) and (11) imply that

$$f_{k+1}\tilde{\psi}(\kappa_{\phi,M}(sq)) \equiv \rho\bar{\lambda}_q(\kappa_{\phi,M'}(s)) \mod M. \qquad \square$$

PROOF OF PROPOSITION 8.1 : Let us consider any Kolyvagin sequence of length k in $\Pi(k,n,MN_n)$, say $\mathfrak{Q} = (\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_k)$ and let $s = s(\mathfrak{Q})$. Suppose ψ is an arbitrary element in $\mathrm{Hom}_{R_n}(R_{n,M'}\kappa_{\phi,M'}(s), R_{n,M'})$. We want to show that

$$\rho\psi(\kappa_{\phi,M'}(s))R_{n,M} \subset f_{k+1}\Psi(k+1,n,M) \quad \forall \rho \in J.$$

We will extend the above Kolyvagin sequence to one of length $k+1$. We apply Cebotarev density theorem in the following way:

Let
$$W = R_{n,M'}\kappa_{\phi,M'}(s) \subset F^\times/(F^\times)^{M'} \hookrightarrow F(\mu_{M'})^\times/(F(\mu_{M'})^\times)^{M'}.$$

See the proof of proposition 15.47 in [Wa] for the second injection above. Let $F' = F(\mu_{M'})$, $L = L_n$ (the maximal unramified abelian p-extension of F) and $H = F(\mu_{M'}, W^{\frac{1}{M'}})$. We have the following diagram of fields:

$$H = F(\mu_{M'}, W^{\frac{1}{M'}})$$

$$L \qquad F' = F(\mu_{M'})$$

$$F$$

We have a Kummer pairing

$$G(H/F') \times W \longrightarrow \mu_{M'},$$

and $G(F'/\mathbb{Q})$-isomorphism

$$G(H/F') \xrightarrow{\sim} \mathrm{Hom}(W, \mu_{M'}).$$

17

Complex conjugation acts trivially on the ideals of the real field F, therefore it acts trivially on $G(L/F)$ by global class field theory. It clearly implies that complex conjugation acts trivially on $G(LF'/F')$. However, complex conjugation acts non-trivially on $\mathrm{Hom}(W, \mu_{M'})$, and hence on $G(H/F')$. Thus, $LF' \cap H = F'$. Then ramification consideration tells us that $L \cap H = F$. If we ignore the Galois structure, then we have

$$G(H/F') \simeq \mathrm{Hom}(W, \mathbb{Z}/M'\mathbb{Z}). \tag{21}$$

Let

$$\tau : (\mathbb{Z}/M'\mathbb{Z})[G] \longrightarrow \mathbb{Z}/M'\mathbb{Z}, \quad \sum a_g g \longmapsto a_1.$$

We can define a map $\tau \circ \psi$ by composition:

$$\tau \circ \psi : W \xrightarrow{\psi} R_{n,M'} = (\mathbb{Z}/M'\mathbb{Z})[G] \xrightarrow{\tau} \mathbb{Z}/M'\mathbb{Z}.$$

Let γ in $G(H/F') \subset G(H/F)$ correspond to $\tau \circ \psi$ under (21). Let σ in $G(LH/F)$ be such that

$$\sigma \mid_L = \sigma_{k+1} \mid_L, \qquad \sigma \mid_H = \gamma.$$

It is possible to find such a σ because $L \cap H = F$. By Cebotarev Density Theorem, there are infinitely many degree 1 primes in F such that the corresponding Frobenius in $G(LH/F)$ is in the same conjugacy class as σ. We pick one such $\mathfrak{q}$ which is unramified in H/F. Since only finitely many primes are ramified in the finite extension H/F, such a choice is possible. Let q be the rational prime below $\mathfrak{q}$. As $\mathfrak{q}$ is an unramified prime of degree 1, q splits in F. Hence, $N_{F/\mathbb{Q}}\mathfrak{q} = q$. Since σ fixes $F(\mu_{M'})$, $\mathrm{Frob}_{\mathfrak{q}}$ fixes the residue field of $F(\mu_{M'})$ at $\mathfrak{q}$. Therefore,

$$N_{F/\mathbb{Q}}\mathfrak{q} = q \equiv 1 \bmod M'.$$

Thus, q is a prime in $\mathcal{S}_M$ (recall that $M' = MN_n$). We can now extend $\mathfrak{Q}$ to a Kolyvagin sequence $\mathfrak{Q}' = (\mathfrak{q}_1, \ldots \mathfrak{q}_k, \mathfrak{q})$ of length $k+1$. Clearly, $s(\mathfrak{Q}') = sq$. By lemma 3.6, there is a Galois equivariant map

$$\tilde{\psi} : R_{n,M}\kappa_{\phi,M}(sq) \longrightarrow R_{n,M},$$

such that

$$\rho\bar{\lambda}_q(\kappa_{\phi,M'}(s)) \equiv f_{k+1}\tilde{\psi}(\kappa_{\phi,M}(sq)) \bmod M. \tag{22}$$

Let $\bar{\mathfrak{q}}$ be a prime of H above $\mathfrak{q}$ such that $\mathrm{Frob}_{\bar{\mathfrak{q}}} = \sigma$. Let $w \in W$. Then $v_{\bar{\mathfrak{q}}}(w) \equiv 0 \bmod M'$. Now,

$$\begin{aligned}
\tau \circ \psi(w) = 0 \quad &\Leftrightarrow \quad \gamma(w^{\frac{1}{M'}}) = w^{\frac{1}{M'}} \\
&\Leftrightarrow \quad \mathrm{Frob}_{\bar{\mathfrak{q}}}(w^{\frac{1}{M'}}) = w^{\frac{1}{M'}} \\
&\Leftrightarrow \quad w \text{ is a } M' - \text{th power mod } \bar{\mathfrak{q}} \cap F = \mathfrak{q}.
\end{aligned}$$

18

Suppose $\bar{\lambda}_q(w) = \sum a_g g$. By definition of $\bar{\lambda}_q$, $\tau \circ \bar{\lambda}_q(w) = 0$ iff w is M'-th power mod $\mathfrak{q}$. Thus,

$$\tau \circ \bar{\lambda}_q(w) = 0 \Leftrightarrow w \text{ is a } M'\text{-th power mod } \mathfrak{q} \Leftrightarrow \tau \circ \psi(w) = 0.$$

Then,

$$\psi = u\bar{\lambda}_q, \qquad u \in (\mathbb{Z}/M'\mathbb{Z})^{\times}.$$

(The above statement can be easily proved, as shown in lemma 15.49 of [Wa]). From (22), it is now obvious that

$$\rho\psi(\kappa_{\phi,M'}(s)) \equiv u\rho\bar{\lambda}_q(\kappa_{\phi,M'}(s)) \equiv u f_{k+1} \tilde{\psi}(\kappa_{\phi,M}(sq)) \bmod M.$$

It is now clear that

$$J\Psi(k, n, MN_n) \subset f_{k+1}\Psi(k+1, n, M). \qquad \square$$

References

[Co]   Coates, J.; *'Elliptic Curves with Complex Multiplication and Iwasawa Theory'*, Bull. London Math. Soc., vol. 23 (1991), pp. 321–350.

[C-W 1] Coates, J. and Wiles, A.; *'On the conjecture of Birch and Swinnerton-Dyer'*, Invent. Math. vol. 39 (1977), pp. 223–251.

[C-W 2] Coates, J. and Wiles, A.; *'On p-adic L-functions and Elliptic Units'*; J. Austral. Math. Soc. (Series A) 26 (1978), pp. 1–25.

[Kol]   Kolyvagin, V.; *'Euler Systems'*, The Grothendieck Festchrift Vol. II, [Progress in Math. 87] (Birkhäuser, Boston, 1990) pp. 435–483.

[La]   Lang, S.; *Cyclotomic Fields*, [Springer- Verlag, 1978.]

[Ru 1]   Rubin, K.; *'The main conjecture'*, Appendix to : Cyclotomic fields I and II, S. Lang. *Graduate Texts in Math.*, vol. 121, New York: Springer-Verlag (1990), pp. 397–419.

[Ru 2]   Rubin, K.; *'The one variable main conjecture for elliptic curves with complex multiplication'*, *L*-function and arithmetic, [London Mathematical Society Lecture Notes 156 (Cambridge University Press, 1991).]

[Ru 3]   Rubin, K.; *'The "main conjectures" of Iwasawa theory for imaginary quadratic fields'*, Inventiones Math., vol. 103 (1991), pp. 25–68.

[Ru 4]   Rubin, K.; *'Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer'* Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., 1716, Springer, Berlin, (1999) pp 167–234.

[Sa]   Saikia, A.; *'A simple proof of a lemma of Coleman'*, Math Prc. Camb. Phil. Soc., vol 130 no. 2 (2001), pp. 209–220.

[Wa]   Washington, L.; *Introduction to Cyclotomic Fields*, [Springer- Verlag, 1997.]