ACTA ARITHMETICA
171.1 (2015)

A comparison of elliptic units in certain prime power conductor cases

by

ULRICH SCHMITT (München)

1. Introduction. In the theory of abelian extensions of imaginary quadratic number fields K, elliptic units play a role analogous to that of cyclotomic units in the theory of abelian extensions of $\mathbb{Q}$. Elliptic units are central objects in the Iwasawa theory of CM elliptic curves. In fact, they appear in Rubin's two-variable main conjecture [Ru91, Theorem 41(i)] and they are used in the construction of p-adic L-functions (see [Y82], [dS87] and [BV10]). Moreover, Coates and Wiles [CW77] studied elliptic units in connection with the Birch and Swinnerton-Dyer conjecture.

Now, let K be an imaginary quadratic number field and E/K an elliptic curve with complex multiplication by $\mathcal{O}_K$, the ring of integers of K, with good ordinary reduction above a split prime p, $p \neq 2, 3$. Denote by $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ the two distinct primes of $\mathcal{O}_K$ above p and write $K_{k,n} := K(E[\bar{\mathfrak{p}}^k \mathfrak{p}^n])$, $k, n \geq 0$, for the field obtained by adjoining to K the coordinates of $\bar{\mathfrak{p}}^k \mathfrak{p}^n$-division points of E. We write $K_\infty = \bigcup_{k,n} K_{k,n}$, G for the Galois group $G(K_\infty/K)$ and $\Lambda(G)$ for the Iwasawa algebra of G with coefficients in $\mathbb{Z}_p$. By $S \subset \Lambda(G)$ we denote the canonical Ore set as defined at the beginning of Section 3 and write S-tor for the category of finitely generated $\Lambda(G)$-modules that are S-torsion. Furthermore, we write $\mathcal{E}_\infty = \varprojlim_{k,n} (\mathcal{O}_{K_{k,n}}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ for the projective limit (with respect to norm maps) of the global units $\mathcal{O}_{K_{k,n}}^\times$ tensored with $\mathbb{Z}_p$. We will define two $\Lambda(G)$-submodules $\mathcal{C}_Y$ and $\mathcal{C}_R$ of $\mathcal{E}_\infty$, consisting of those elliptic units considered by Yager in [Y82] and Rubin in [Ru91], respectively. Under the assumption that the conductor $\mathfrak{f}$ of E/K is a prime power, we prove the following result.

THEOREM 3.19. *Let $\mathfrak{f} = \mathfrak{l}^r$ for some prime ideal $\mathfrak{l}$ of $\mathcal{O}_K$ and some $r \geq 1$. Then in $K_0(S\text{-tor})$ we have*

2010 *Mathematics Subject Classification*: Primary 11G16; Secondary 11R23, 14K22.
Key words and phrases: elliptic units, Iwasawa theory, complex multiplication.

DOI: 10.4064/aa171-1-4

$$[\mathcal{C}_R/\mathcal{C}_Y] = [\Lambda(G/D_{\mathfrak{l}})],$$

where we write $D_{\mathfrak{l}}$ *for the decomposition group of* $\mathfrak{l}$ *in* $G = G(K_\infty/K)$.

Before we outline the structure of this paper, let us make some remarks concerning the generality and the applications of the theorem. First, we note that if E is already defined over $\mathbb{Q}$ and E is a representative with minimal discriminant and conductor in its $\bar{\mathbb{Q}}$-isomorphism class as in [Si99, Appendix A, §3], then $\mathfrak{f} = \mathfrak{l}^r, r \geq 1$, is a prime power (see [S14, Theorem A.6.8 and Proposition A.6.9]), so that the theorem applies in these cases.

Next, we briefly mention some applications of Theorem 3.19. In a talk held in Cambridge on the occasion of J. Coates' 60th birthday, K. Kato stated a conjecture for, in general, non-abelian p-adic Lie extensions $F_\infty/\mathbb{Q}$ containing the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{\mathrm{cyc}}$. Kato's conjecture concerns the existence of an element $L_{p,u} \in K_1(\mathbb{Z}_p[[G(F_\infty/\mathbb{Q})]]_{S^*})$, where S^* is a certain Ore set, depending on a global unit u. This $L_{p,u}$ is required to satisfy a prescribed interpolation property and to map to a specified element under the connecting homomorphism $\partial : K_1(\mathbb{Z}_p[[G(F_\infty/\mathbb{Q})]]_{S^*}) \to K_0(S^*\text{-tor})$ from K-theory, where S^*-tor denotes the category of finitely generated $\mathbb{Z}_p[[G(F_\infty/\mathbb{Q})]]$-modules which are S^*-torsion. Theorem 3.19 can be used to prove (under a torsion assumption) an analogous statement in the commutative setting K_∞/K described above (see [S14, Theorem 2.4.41]).

Moreover, Theorem 3.19 can be used to bridge the work of Yager and Rubin on the two-variable main conjecture when proving the non-commutative Iwasawa main conjecture as stated in [CFKSV] for CM elliptic curves $E/\mathbb{Q}$ (with prime power conductor over K). Compare the work [BV10] of Bouganis and Venjakob, in particular Remark 2.8 there.

In the present paper we proceed as follows.

1° In Section 2 we define groups of elliptic units studied by Rubin, de Shalit and Yager.

2° In Subsection 3.1 we show that Yager's elliptic units coincide with a group of elliptic units considered by de Shalit (Proposition 3.1).

3° In Subsection 3.2 we determine a (relatively small) set of generators of $\mathcal{C}_R = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ (Corollary 3.7), and afterwards show that the quotient of $\mathcal{C}_R$ and de Shalit's elliptic units (i.e., $\mathcal{C}_R/\mathcal{C}_Y$ by step 2°) is S-torsion by giving a concrete element of S that annihilates the quotient (Theorem 3.10).

4° In Subsection 3.3 we determine the image of $\mathcal{C}_Y$ under the (two-variable) semilocal version $\mathbb{L}$ of the Coleman map for the formal group $\hat{E}$ associated to a Weierstraß equation of E (Corollary 3.14).

5° In Subsection 3.4 we determine the image of $\mathcal{C}_R$ under $\mathbb{L}$ subject to the condition that the conductor of E/K is a prime power (Theorem 3.18).

6° In Subsection 3.5 we combine the descriptions of $\mathcal{C}_Y$ and $\mathcal{C}_R$ via $\mathbb{L}$ and prove Theorem 3.19.

For basic facts about elliptic units our main references are the works [Ru91] by Rubin and [dS87] by de Shalit. For Robert's treatment of elliptic units see [R73], [R90] and [R92]. There are other useful accounts due to Rubin [Ru87, Appendix] and to Coates and Wiles [CW77, Section 5], [CW78, Section 3]. The different notation used in some of the above is compared in Bley [B04].

We note that large portions of the present paper are slightly modified versions of parts of the author's doctoral dissertation [S14]. For related results about elliptic units, we refer to the paper [V12] by Viguié, who proves a similar statement to Lemma 3.2 (compare [V12, Lemma 2.4, Corollary 2.5]). He also determines a set of generators for projective limits of elliptic units for certain $\mathbb{Z}_p$-extensions [V12, Lemma 2.7]. Our situation is different in that we deal with $\mathbb{Z}_p^2$-extensions, which requires different ideas.

We also want to refer to the paper [K12], where Y. Kang establishes, for a p-adic L-function interpolating values of primitive Hecke L-functions, an analogue of Yager's main result from [Y82]. Kang uses a modification of the elliptic units used by Yager.

2. Definition of elliptic units. In this section we recall some different, yet (as we will see) closely related definitions of elliptic units. Throughout, K will denote a quadratic imaginary number field. We will eventually be interested in the fields $F = K_{k,n} := K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$ for an elliptic curve E/K with complex multiplication by $\mathcal{O}_K$, where $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are distinct primes of K above a rational prime p, $p \neq 2, 3$, at which E/K has good reduction.

2.1. Rubin's elliptic units. Let us recall the definition of elliptic units for a number field F which is an abelian Galois extension of a quadratic imaginary field K containing the Hilbert class field H of K that is used by Rubin in [Ru91]. For an integral ideal $\mathfrak{m}$ of K we denote by $K(\mathfrak{m})$ the ray class field of K modulo $\mathfrak{m}$. We fix an embedding $\bar{K} \subset \mathbb{C}$ and a period lattice $L \subset \mathbb{C}$ of some elliptic curve defined over H with complex multiplication by $\mathcal{O}_K$; for the existence of such a curve Rubin refers to [Sh71, Theorem 5.7]. For any integral ideal $\mathfrak{a} \subset \mathcal{O}_K$, $(\mathfrak{a}, 6) = 1$, he then considers the meromorphic function

$$\Theta_0(z;\mathfrak{a}) = \Theta_0(z;L,\mathfrak{a}) = \left(\frac{\Delta(L)^{N\mathfrak{a}}}{\Delta(\mathfrak{a}^{-1}L)}\right)^{1/12} \prod_{u\in(\mathfrak{a}^{-1}L/L)/\pm 1} (\wp(z;L)-\wp(u;L))^{-1},$$

where Δ is the Ramanujan Δ-function, a twelfth root of $\Delta(L)^{N\mathfrak{a}}/\Delta(\mathfrak{a}^{-1}L)$ is fixed and $\wp(z;L)$ is the Weierstraß $\wp$-function for the lattice L.

Now, let $\mathfrak{m}$ be an integral ideal of K such that $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{m}$ is injective (recall that $\mathcal{O}_K^\times$ is a finite group) and let $\tau \in \mathbb{C}/L$ be an element of order exactly $\mathfrak{m}$. It is shown in [B04, Proposition 2.2] that $\Theta_0(\tau;\mathfrak{a})$ belongs to $K(\mathfrak{m})$.

Definition 2.1. Let K be a quadratic imaginary number field and F a finite abelian Galois extension of K, containing the Hilbert class field of K. Rubin makes the following definitions:

(i) C_F is the group generated by all elements

$$(N_{FK(\mathfrak{m})/F}\Theta_0(\tau;\mathfrak{a}))^{\sigma-1}, \tag{1}$$

where σ ranges over $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ over the integral ideals of K such that $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{m}$ is injective, $\mathfrak{a}$ over the integral ideals such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$, and τ over the primitive $\mathfrak{m}$-division points. $N_{FK(\mathfrak{m})/F}$ denotes the norm map from the composite field $FK(\mathfrak{m})$ of F and $K(\mathfrak{m})$ to F and we note that the elements $\sigma - 1$ generate the augmentation ideal $I(F/K)$, i.e., the kernel of the augmentation map $\mathrm{aug} : \mathbb{Z}[G(F/K)] \to \mathbb{Z}$.

(ii) $\mathcal{C}(F)$, the group of elliptic units of F, is

$$\mathcal{C}(F) = \mu_\infty(F)C_F,$$

where $\mu_\infty(F)$ is the group of all roots of unity in F.

(iii) For $K_{k,n} := K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$ as above we also define the projective limit of Rubin's elliptic units

$$\mathcal{C}_R := \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p),$$

where the limit is taken with respect to norm maps.

2.2. De Shalit's elliptic units. De Shalit considers the function

$$\Theta(z;L,\mathfrak{a}) = \Theta_0(z;\mathfrak{a})^{12},$$

which is an elliptic function with respect to L and can be expressed in terms of the fundamental theta function, which is noted in [dS87, II, 2.3]. Moreover, $\Theta(z;L,\mathfrak{a})$ satisfies the monogeneity relation

$$\Theta(cz;cL,\mathfrak{a}) = \Theta(z;L,\mathfrak{a}), \qquad c \in \mathbb{C}^\times.$$

Assumption 2.2. From now on we assume that K has class number one. Note that this is automatically satisfied whenever we consider an elliptic curve E/K with complex multiplication by $\mathcal{O}_K$.

So we can find $\Omega \in L$ and $x_\mathfrak{n} \in \mathcal{O}_K$ such that $L = \mathcal{O}_K\Omega$ and $\mathfrak{n} = (x_\mathfrak{n})$ for any integral ideal $\mathfrak{n}$ of K. With this notation, $\Omega/x_\mathfrak{n}$ is a primitive $\mathfrak{n}$-division point in $\mathbb{C}/L$.

Definition 2.3. De Shalit makes the following definitions:

(i) $\Theta_{\mathfrak{n}}$ is the subgroup of $K(\mathfrak{n})^{\times}$ generated by

$$\Theta(1;\mathfrak{n},\mathfrak{a}) = \Theta(\tau; L, \mathfrak{a}), \tag{2}$$

where $\mathfrak{a}$ ranges over the integral ideals of K such that $(\mathfrak{a}, 6\mathfrak{n}) = 1$, and τ is a primitive $\mathfrak{n}$-division point in $\mathbb{C}/L$.

(ii) $C_{\mathfrak{n}}$ is the group of units in $K(\mathfrak{n})^{\times}$ whose 12th power belongs to $\mu_\infty(K(\mathfrak{n}))\Theta_{\mathfrak{n}}$ for any integral ideal $\mathfrak{n}$ of K such that $\mathcal{O}_K^{\times} \hookrightarrow \mathcal{O}_K/\mathfrak{n}$ is injective.

Remark 2.4. (i) $\Theta_{\mathfrak{n}}$ is independent of τ, which follows from 1 and Remark 2.6.

(ii) If $\mathfrak{n}$ is divisible by at least two distinct primes, then $\Theta_{\mathfrak{n}}$ is a subgroup of the group $\mathcal{O}_{K(\mathfrak{n})}^{\times}$ of units in $K(\mathfrak{n})^{\times}$.

(iii) The groups $\Theta_{\mathfrak{n}}$ and $C_{\mathfrak{n}}$ are $G(K(\mathfrak{n})/K)$-stable, which follows from [dS87, II, Proposition 2.4(ii)].

(iv) Note that Rubin's group $\mathcal{C}(F)$ for a ray class field $F = K(\mathfrak{n})$ is, in general, larger than $I(K(\mathfrak{n})/K)C_{\mathfrak{n}}$, since in the definition of generators as in (1) he allows $\mathfrak{m}$ to range over all integral ideals of K such that $\mathcal{O}_K^{\times} \to \mathcal{O}_K/\mathfrak{m}$ is injective.

The values of Θ at two different primitive $\mathfrak{n}$-division points are related through the action of the Galois group $G(K(\mathfrak{n})/K)$, which we want to illustrate in the next remark. Let us first introduce some notation for arithmetic Frobenius elements.

Definition 2.5. Let F/K be an abelian (finite or infinite) extension in which the prime ideal $\mathfrak{q}$ is unramified. We then write

$$(\mathfrak{q}, F/K) \in D_{\mathfrak{q}} \subset G(F/K)$$

for the arithmetic Frobenius at $\mathfrak{q}$ which (topologically) generates the decomposition group $D_{\mathfrak{q}}$. If $\mathfrak{c}$ is an ideal which has a prime decomposition $\prod_{i=1}^{r} \mathfrak{q}_i^{m_i}$ and each $\mathfrak{q}_i$ is unramified in F/K, then we define

$$(\mathfrak{c}, F/K) := \prod_{i=1}^{r} (\mathfrak{q}_i, F/K)^{m_i}.$$

Remark 2.6. If τ is any primitive $\mathfrak{n}$-division point we can find $c \in \mathcal{O}_K$, c prime to $\mathfrak{n}$, such that $\tau = c\Omega/x_{\mathfrak{n}}$. Let us write $\sigma_c = ((c), K(\mathfrak{n})/K)$ in $G(K(\mathfrak{n})/K)$. Then

$$\begin{aligned} \Theta(\Omega/x_{\mathfrak{n}}; L, \mathfrak{a})^{\sigma_c} &= \Theta(\Omega/x_{\mathfrak{n}}; (c)^{-1}L, \mathfrak{a}) \\ &= \Theta(c(\Omega/x_{\mathfrak{n}}); c(c)^{-1}L, \mathfrak{a}) = \Theta(\tau; L, \mathfrak{a}), \end{aligned} \tag{3}$$

where the first equality follows from [dS87, II, Proposition 2.4(ii)], using the main theorem of complex multiplication [Sh71, 5.3]. For the second equality we have used the monogeneity property. We conclude that the values of Θ

at two different primitive $\mathfrak{n}$-division points belong to the same orbit under the action of $G(K(\mathfrak{n})/K)$.

2.3. Yager's elliptic units. Let $I_{6p\mathfrak{f}}$ be the set of integral ideals of K which are prime to $6p\mathfrak{f}$ and let

$$\mathcal{S} = \Big\{\mu : I_{6p\mathfrak{f}} \to \mathbb{Z} \;\Big|\; \mu(\mathfrak{b}) = 0 \text{ for almost all } \mathfrak{b} \in I_{6p\mathfrak{f}} \text{ and } \sum_{\mathfrak{b}\in I_{6p\mathfrak{f}}} (N\mathfrak{b} - 1)\mu(\mathfrak{b}) = 0\Big\}.$$

For any $\mu \in \mathcal{S}$ we define

$$\Theta(z; L, \mu) = \prod_{\mathfrak{b}\in I_{6p\mathfrak{f}}} \Theta(z; L, \mathfrak{b})^{\mu(\mathfrak{b})}.$$

For certain $\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k$-division points τ Yager then considers $\Theta(\tau; L, \mu)$. Let us write $F_{k,n} = K(\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k)$ for the ray class field modulo $\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k$.

Definition 2.7. (i) Let $C_{Y,k,n}$ be the group generated by elements of the form

$$N_{F_{k,n}/K_{k,n}}\Theta(\tau; L, \mu)$$

for $k, n \geq 1$ and $\mu \in \mathcal{S}$, where we write $N_{F_{k,n}/K_{k,n}}$ for the norm map from $F_{k,n}$ to $K_{k,n}$.

(ii) We also define the projective limit of Yager's units

$$\mathcal{C}_Y := \varprojlim_{k,n}(C_{Y,k,n} \otimes_{\mathbb{Z}} \mathbb{Z}_p),$$

where the limit is taken with respect to norm maps.

Remark 2.8. (i) $C_{Y,k,n}$ is Galois stable by [dS87, II, Proposition 2.4].

(ii) Moreover, it does not matter which $\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k$-division point τ we start with since $\Theta(\tau; L, \mu)$ and $\Theta(\tau'; L, \mu)$ are in the same orbit under the action of $G(F_{k,n}/K)$ for any two such division points τ and τ'; compare Remark 2.6.

3. Results. As before, we write $F_{k,n} = K(\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k)$ and $K_{k,n} := K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$ for an elliptic curve E/K with complex multiplication by $\mathcal{O}_K$, where $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are distinct primes of K above a rational prime p, $p \neq 2, 3$, at which E/K has good reduction. For any Galois extension F/K we denote by $I(F/K)$ the augmentation ideal in $\mathbb{Z}[G(F/K)]$. We set $K_\infty = \bigcup_{k,n} K_{k,n}$, $G = \mathrm{Gal}(K_\infty/K)$ and write $\Lambda(G) = \Lambda(G, \mathbb{Z}_p)$ for the commutative Iwasawa algebra of G with coefficients in $\mathbb{Z}_p$. We also define the canonical Ore set

$$S = \{x \in \Lambda(G) \mid \Lambda(G)/\Lambda(G)x \text{ is finitely generated over } \Lambda(H)\},$$

where $H = G(K_\infty/K^{\mathrm{cyc}})$ and K^{cyc} is the cyclotomic $\mathbb{Z}_p$-extension of K so that $G/H \cong \mathbb{Z}_p$.

3.1. Comparison of Yager's and de Shalit's elliptic units

PROPOSITION 3.1. *We have*

$$C_{Y,k,n} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \big(I(K_{k,n}/K) N_{F_{k,n}/K_{k,n}}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k})\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

for all $k, n \geq 1$.

Proof. We start by showing that

$$I(K_{k,n}/K) N_{F_{k,n}/K_{k,n}}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \subseteq C_{Y,k,n}.$$

Let σ be an element of $G(K_{k,n}/K)$. Note that $I(K_{k,n}/K)$ is generated by the various $1-\sigma$ with σ running over $G(K_{k,n}/K)$. We have to show that elements of the form

$$(N_{F_{k,n}/K_{k,n}} \Theta(\tau; L, \mathfrak{a}))^{1-\sigma},$$

where τ is an $\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k$-division point and $\mathfrak{a}$ is an ideal of K prime to $6\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k$, belong to $C_{Y,k,n} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. To see this, choose a prime ideal $\mathfrak{c}$ of $\mathcal{O}_K$ prime to $6\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k$ such that $\sigma = (\mathfrak{c}, K_{k,n}/K)$. Let us define an element $\mu \in \mathcal{S}$ by

$$\mu(\mathfrak{a}) = 1, \quad \mu(\mathfrak{c}) = N\mathfrak{a}, \quad \mu(\mathfrak{a}\mathfrak{c}) = -1, \quad \text{and} \quad \mu(\mathfrak{b}) = 0 \quad \forall \mathfrak{b} \neq \mathfrak{a}, \mathfrak{a}\mathfrak{c}, \mathfrak{c}.$$

Using [dS87, II, Proposition 2.4(ii)], one can immediately verify that

$$(N_{F_{k,n}/K_{k,n}} \Theta(\tau; L, \mathfrak{a}))^{1-\sigma} = N_{F_{k,n}/K_{k,n}} \Theta(\tau; L, \mu).$$

We now turn to the other inclusion

$$C_{Y,k,n} \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq \big(I(K_{k,n}/K) N_{F_{k,n}/K_{k,n}}(\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k})\big) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Let $\mu \in \mathcal{S}$ and choose an integral ideal $\mathfrak{c}$ of K prime to $6p\mathfrak{f}$ such that $N\mathfrak{c} - 1 \in \mathbb{Z}_p^\times$ (recall that $p \neq 2, 3$). For any integral ideal $\mathfrak{a}$ of K we write $\sigma_\mathfrak{a} = (\mathfrak{a}, F_{k,n}/K)$. Using the identities $\Theta(\tau; L, \mathfrak{b})^{N\mathfrak{c}-\sigma_\mathfrak{c}} = \Theta(\tau; L, \mathfrak{c})^{N\mathfrak{b}-\sigma_\mathfrak{b}}$ from [dS87] and $\sum_\mathfrak{b}(N\mathfrak{b} - 1)\mu(\mathfrak{b}) = 0$ we get

$$\begin{aligned}\Theta(\tau; L, \mu)^{N\mathfrak{c}-1} \cdot \Theta(\tau; L, \mu)^{1-\sigma_\mathfrak{c}} &= \Theta(\tau; L, \mu)^{N\mathfrak{c}-\sigma_\mathfrak{c}} = \prod_\mathfrak{b} (\Theta(\tau; L, \mathfrak{b})^{N\mathfrak{c}-\sigma_\mathfrak{c}})^{\mu(\mathfrak{b})} \\ &= \prod_\mathfrak{b} (\Theta(\tau; L, \mathfrak{c})^{N\mathfrak{b}-\sigma_\mathfrak{b}})^{\mu(\mathfrak{b})} \\ &= \prod_\mathfrak{b} (\Theta(\tau; L, \mathfrak{c})^{1-\sigma_\mathfrak{b}})^{\mu(\mathfrak{b})},\end{aligned}$$

whence it follows that $\Theta(\tau; L, \mu)^{N\mathfrak{c}-1} \in I(F_{k,n}/K)\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$. Taking the norm from $F_{k,n}$ to $K_{k,n}$ and recalling that $N\mathfrak{c} - 1 \in \mathbb{Z}_p^\times$ finishes the proof. ∎

3.2. Comparison of Rubin's and de Shalit's elliptic units. In this subsection we compare Rubin's elliptic units $\mathcal{C}_R := \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ for the fields $K_{k,n}$ to de Shalit's units, and hence, through Proposition 3.1, to Yager's units $\mathcal{C}_Y := \varprojlim_{k,n}(C_{Y,k,n} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. We will show in Theorem 3.10 that the module $\mathcal{C}_R/\mathcal{C}_Y$ is S-torsion.

In order to prove Theorem 3.10, we will determine in three steps a relatively small set of generators of $\mathcal{C}_R$. First, for the fields $K_{k,n}$ we prove the following lemma, which says that in the definition of $C_{K_{k,n}}$ we can restrict ourselves to certain integral ideals $\mathfrak{m}$ dividing the conductor of $K_{k,n}$. The conductor of $K_{k,n}$, for $k, n \geq 0$, $(k,n) \neq (0,0)$, is given by $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$, where $\mathfrak{f}$ is the conductor of ψ_E, the Größencharacter of E/K (see [S14, Lemma 2.4.17]). As before, we assume that $p \neq 2, 3$. As a second step, we show that when passing to the projective limit $\varprojlim_{k,n}(C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ we can restrict to an even smaller set of integral ideals $\mathfrak{m}$ (compare Lemma 3.5). In a third step, we show that for the tower K_∞/K, $K_\infty = \bigcup_{n,k} K(E[\mathfrak{p}^n\bar{\mathfrak{p}}^k])$, the projective limit $\varprojlim_{K\subseteq_f L' \subset K_\infty} \mu_{p^\infty}(L')$ of p-power roots of unity, taken with respect to norm maps, vanishes.

The three steps combined give us the desired description of $\mathcal{C}_R$ in terms of a smaller set of generators (Corollary 3.7). For elements x of this smaller set of generators we can define an explicit element s belonging to S such that the product sx belongs to $\mathcal{C}_Y$, which proves Theorem 3.10.

Lemma 3.2. *Let $k, n \geq 1$ be such that $\mathcal{O}_K^\times \to \mathcal{O}_K/\bar{\mathfrak{p}}^k$ and $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{p}^n$ are both injective. Let us write $F = K_{k,n} = K(E[\bar{\mathfrak{p}}^k\mathfrak{p}^n])$. Then, as a $\mathbb{Z}_p[G(F/K)]$-module, $C_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is already generated by elements of the form*

$$(N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}))^{\sigma-1},$$

where σ ranges over $\mathrm{Gal}(F/K)$*, $\mathfrak{m}$ over the integral ideals of K such that either*

$$\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n \quad \text{or} \quad \mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k \quad \text{or} \quad \mathfrak{m} = \mathfrak{f}'\mathfrak{p}^n \quad \text{for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f},$$

$\mathfrak{a}$ over integral ideals such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$, and τ over primitive $\mathfrak{m}$-division points.

Proof. First note that after extending scalars, since 12 is a unit in $\mathbb{Z}_p$, we have

$$(N_{FK(\mathfrak{m})/F}\Theta_0(\tau;\mathfrak{a}))^{\sigma-1} \otimes 1 = (N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}))^{\sigma-1} \otimes \frac{1}{12},$$

so clearly all elements of the form $(N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}))^{\sigma-1}$, for general $\mathfrak{m}$, τ, $\mathfrak{a}$ and σ as in (1), generate $C_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as a $\mathbb{Z}_p$-module. Hence, from now on it is sufficient to consider the function $\Theta(z;\mathfrak{a}) = \Theta(z; L, \mathfrak{a})$ (we omit the L from the notation).

Let us now fix an integral ideal $\mathfrak{m}$ of K such that $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{m}$ is injective. Write

$$x := N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}),$$

where $\mathfrak{a}$ is an integral ideal such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$ and τ is a primitive $\mathfrak{m}$-division point. We will show that $x^{\sigma-1}$, for any $\sigma \in G(F/K)$, is already contained in the module generated by the elements from the statement of the lemma. We will show step by step that we can impose more conditions on $\mathfrak{m}$ and still obtain a set of $\mathbb{Z}_p[G(K_{k,n}/K)]$-generators for $C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Let us first make some general definitions. We define $\mathfrak{f}' = \gcd(\mathfrak{f}, \mathfrak{m})$. We can then write

$$\mathfrak{m} = \mathfrak{f}' \bar{\mathfrak{p}}^{k'} \mathfrak{p}^{n'} \mathfrak{m}'$$

for some $\mathfrak{m}'$ such that $\gcd(\mathfrak{m}', p) = 1$, so that n', resp. k', is precisely the exponent of $\mathfrak{p}$, resp. $\bar{\mathfrak{p}}$, in $\mathfrak{m}$. We need not have $\gcd(\mathfrak{m}', \mathfrak{f}) = 1$. Let us define $\mathfrak{q} = \gcd(\mathfrak{m}, \mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n)$, so that

$$F \cap K(\mathfrak{m}) \subset K(\mathfrak{f}\bar{\mathfrak{p}}^k \mathfrak{p}^n) \cap K(\mathfrak{m}) = K(\mathfrak{q}),$$

where the last equality is a simple excercise in class field theory. Since $\mathfrak{f}$ and p are prime to each other, we have an equality

$$\mathfrak{q} = \mathfrak{f}' \bar{\mathfrak{p}}^{\min\{k,k'\}} \mathfrak{p}^{\min\{n,n'\}}.$$

For the norm map $N_{FK(\mathfrak{m})/F}$ restricted to $K(\mathfrak{m})$ we can write

$$N_{FK(\mathfrak{m})/F} = N_{K(\mathfrak{m})/(F\cap K(\mathfrak{m}))} = N_{K(\mathfrak{q})/(F\cap K(\mathfrak{m}))} \circ N_{K(\mathfrak{m})/K(\mathfrak{q})}, \tag{4}$$

where we note that $F \cap K(\mathfrak{m}) = F \cap K(\mathfrak{q})$. Let us now start with the computations. We will show that we may exclude the following classes of $\mathfrak{m}$ and still be left with a set of $\mathbb{Z}_p[G(K_{k,n}/K)]$-generators for $C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Case 1: $\gcd(\mathfrak{m}, p) = 1$. In this case, since E/K has good reduction at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, we also have $\gcd(\mathfrak{m}\mathfrak{f}, p) = 1$. By [dS87, II, Proposition 1.6, Corollary 1.7] we know that $K(\mathfrak{m}\mathfrak{f}) = K(E[\mathfrak{m}\mathfrak{f}])$ and that $K(E[\mathfrak{m}\mathfrak{f}])$ and $F = K(E[\bar{\mathfrak{p}}^k \mathfrak{p}^n])$ are linearly disjoint over K. Therefore,

$$F \cap K(\mathfrak{m}) \subset F \cap K(\mathfrak{m}\mathfrak{f}) = K,$$

which implies that $G(FK(\mathfrak{m})/F) \cong G(K(\mathfrak{m})/K)$. This shows that if we restrict the norm map $N_{FK(\mathfrak{m})/F}$ to $K(\mathfrak{m})$, then $N_{FK(\mathfrak{m})/F} = N_{K(\mathfrak{m})/K}$. We conclude that

$$x^{\sigma-1} = (N_{K(\mathfrak{m})/K} \Theta(\tau; \mathfrak{a}))^{\sigma-1} = 1,$$

since σ fixes K. From now on, we may and will assume that $\gcd(\mathfrak{m}, p) \neq 1$, i.e., that $\mathfrak{p} \mid \mathfrak{m}$ or $\bar{\mathfrak{p}} \mid \mathfrak{m}$.

Case 2: $n' > n$ or $k' > k$. If $n' > n$, then [dS87, II, Proposition 2.5] (see also [Ru99, Corollary 7.7, p. 197] for a more detailed proof) shows that

$$N_{K(\mathfrak{m})/K(\mathfrak{m}/\mathfrak{p})} \Theta(\tau; \mathfrak{a}) = \Theta(\pi\tau; \mathfrak{a}),$$

where $\pi\tau$ is now clearly a primitive $\frac{\mathfrak{m}}{\mathfrak{p}}$-division point. Here we use the fact that $\mathfrak{p}^n \mid \frac{\mathfrak{m}}{\mathfrak{p}}$ and $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{p}^n$ is injective, i.e., there is precisely one root of unity in K that is congruent to 1 modulo $\mathfrak{p}^n$. Since $\mathfrak{q} \mid \frac{\mathfrak{m}}{\mathfrak{p}}$, we also have

$$F \cap K(\mathfrak{m}) = F \cap K(\mathfrak{m}/\mathfrak{p}).$$

Using (4), this shows that $x = N_{FK(\mathfrak{m}/\mathfrak{p})/F}\Theta(\pi\tau;\mathfrak{a})$. Proceeding inductively, we may and will assume that $n' \leq n$. Analogously, we may assume $k' \leq k$.

CASE 3: $1 \leq n' < n$ or $1 \leq k' < k$. Without loss of generality, assume that $n' \geq 1$ (if $n' = 0$, then, by the first case, we may assume that $k' \geq 1$ and the following works precisely in the same way for k'). So $\mathfrak{p} \mid \mathfrak{m}$. While we have used [dS87, II, Proposition 2.5] above to see that we may make the exponent n' of $\mathfrak{p}$ in $\mathfrak{m}$ smaller if $n' > n$, we now use it to see that we may make it bigger whenever $n' < n$. In fact, by the above-cited proposition we have

$$\Theta(\tau;\mathfrak{a}) = N_{K(\mathfrak{m}\mathfrak{p})/K(\mathfrak{m})}\Theta\left(\frac{\tau}{\pi};\mathfrak{a}\right),$$

where, if we consider τ as an element of $E(\mathbb{C})$, we write $\frac{\tau}{\pi}$ for some primitive $\mathfrak{m}\mathfrak{p}$-division point in $E(\mathbb{C})$ such that $\pi\frac{\tau}{\pi} = \tau$ (while if we consider τ as an element of $\mathbb{C}/L$ then we can actually divide τ by π; this depends on whether we view Θ as a function on $E(\mathbb{C})$ or on $\mathbb{C}/L$). Using (4) again, we get

$$\begin{aligned} x &= N_{K(\mathfrak{m}\mathfrak{p})/(F\cap K(\mathfrak{m}))}\Theta\left(\frac{\tau}{\pi};\mathfrak{a}\right) \\ &= N_{(F\cap K(\mathfrak{m}\mathfrak{p}))/(F\cap K(\mathfrak{m}))} \circ N_{K(\mathfrak{m}\mathfrak{p})/(F\cap K(\mathfrak{m}\mathfrak{p}))}\Theta\left(\frac{\tau}{\pi};\mathfrak{a}\right), \end{aligned}$$

showing that x is just a product of $G(F/K)$-conjugates of the element $N_{K(\mathfrak{m}\mathfrak{p})/(F\cap K(\mathfrak{m}\mathfrak{p}))}\Theta\left(\frac{\tau}{\pi};\mathfrak{a}\right)$. Proceeding inductively, we may assume that $n' = n$.

We conclude that so far we may assume $k' \leq k$ and $n' \leq n$ and either $n = n'$ or $k = k'$. If both k' and n' are greater than zero, then the last argument shows that we may assume that $k' = k$ and $n' = n$.

In the last step we made $\mathfrak{m}$ larger so that $\mathfrak{p}^n \mid \mathfrak{m}$ (or $\bar{\mathfrak{p}}^k \mid \mathfrak{m}$). By our assumption on n and k, it follows that there is only one root of unity in K that is congruent to 1 modulo $\frac{\mathfrak{m}}{\mathfrak{m}'}$. This enables us to use [dS87, II, Proposition 2.5] in the next step to eliminate $\mathfrak{m}'$.

CASE 4: $\mathfrak{m}' \neq 1$. Let $\mathfrak{l} = (l)$ be a prime ideal of K dividing $\mathfrak{m}'$. In particular, $\mathfrak{l}$ is prime to p. First note that

$$\mathfrak{q} = \gcd\left(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\right).$$

In fact, if $\gcd\left(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\right)$ were equal to $\frac{\mathfrak{q}}{\mathfrak{l}}$ (it certainly could not be anything else), write $\mathfrak{l}^r$ for the exact power of $\mathfrak{l}$ in $\mathfrak{q}$. We then see that $\mathfrak{l}^r \mid \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$, and hence $\mathfrak{l}^r \mid \mathfrak{f}$. Moreover, $\mathfrak{l}^r \mid \mathfrak{m}$, so that $\mathfrak{l}^r \mid \mathfrak{f}'$. By the assumption $\gcd(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n) = \mathfrak{q}/\mathfrak{l}$, we have $\mathfrak{l}^r \nmid \frac{\mathfrak{m}}{\mathfrak{l}}$. On the other hand, $\mathfrak{l}^r \mid \mathfrak{f}'\frac{\mathfrak{m}'}{\mathfrak{l}}$ and $\mathfrak{f}'\frac{\mathfrak{m}'}{\mathfrak{l}} \mid \frac{\mathfrak{m}}{\mathfrak{l}}$. This is a contradiction, showing that $\mathfrak{q} = \gcd\left(\frac{\mathfrak{m}}{\mathfrak{l}}, \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n\right)$.

By [dS87] we have

$$N_{K(\mathfrak{m})/K(\mathfrak{m}/\mathfrak{l})}\Theta(\tau;\mathfrak{a}) = \begin{cases} \Theta(l\tau;\mathfrak{a}) & \text{if } \mathfrak{l} \mid \frac{\mathfrak{m}}{\mathfrak{l}}, \\ \Theta(l\tau;\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}} & \text{if } \mathfrak{l} \nmid \frac{\mathfrak{m}}{\mathfrak{l}}, \end{cases}$$

where $\sigma_{\mathfrak{l}} = \big(\mathfrak{l}, K(\frac{\mathfrak{m}}{\mathfrak{l}})/K\big)$ in the case $\mathfrak{l} \nmid \frac{\mathfrak{m}}{\mathfrak{l}}$. We conclude that

$$x = N_{K(\mathfrak{m})/(F\cap K(\mathfrak{q}))}\Theta(\tau;\mathfrak{a}) = \begin{cases} N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\Theta(l\tau;\mathfrak{a}) & \text{if } \mathfrak{l} \mid \frac{\mathfrak{m}}{\mathfrak{l}}, \\ N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}(\Theta(l\tau;\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}}) & \text{if } \mathfrak{l} \nmid \frac{\mathfrak{m}}{\mathfrak{l}}. \end{cases}$$

In the latter case, as all of the Galois groups involved are abelian, we see that

$$N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}(\Theta(l\tau;\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}}) = (N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\Theta(l\tau;\mathfrak{a}))^{1-\tilde{\sigma}_{\mathfrak{l}}^{-1}},$$

where we write $\tilde{\sigma}_{\mathfrak{l}}$ for any lift to F of the restriction of $\sigma_{\mathfrak{l}}$ to $F \cap K(\mathfrak{q})$. In any case, we find that x is a product of $G(F/K)$-conjugates of the element $N_{K(\mathfrak{m}/\mathfrak{l})/(F\cap K(\mathfrak{q}))}\Theta(l\tau;\mathfrak{a})$. Therefore we may assume that $\mathfrak{m}'$ is trivial.

We have shown that we may restrict to $\mathfrak{m}$ of the form $\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n$ or $\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k$ or $\mathfrak{m} = \mathfrak{f}'\mathfrak{p}^n$ for some divisor $\mathfrak{f}'$ of $\mathfrak{f}$ and still get a generating set; in any case $\mathfrak{m} \mid \mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$. ∎

We now *split* the set of $\mathbb{Z}_p[G(F/K)]$-generators of $C_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ determined in Lemma 3.2 ($F = K_{k,n}$ as in the lemma) and define two new modules.

Definition 3.3. Let the setting be as in Lemma 3.2. Let $F = K_{k,n}$, $k, n \geq 1$.

(i) We define C'_F to be the subgroup of C_F generated by elements of the form

$$(N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}))^{\sigma-1},$$

where σ ranges over $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ over the integral ideals of K such that

$$\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n \quad \text{for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f},$$

$\mathfrak{a}$ over integral ideals such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$, and τ over primitive $\mathfrak{m}$-division points.

(ii) Moreover, we define D_F to be the subgroup of C_F generated by elements of the form

$$(N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}))^{\sigma-1},$$

where σ ranges over $\mathrm{Gal}(F/K)$, $\mathfrak{m}$ over the integral ideals of K such that

$$\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^k \text{ or } \mathfrak{m} = \mathfrak{f}'\mathfrak{p}^n \text{ for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f},$$

$\mathfrak{a}$ over integral ideals such that $(\mathfrak{a}, 6\mathfrak{m}) = 1$, and τ over primitive $\mathfrak{m}$-division points.

Remark 3.4. (i) First note that, by definition and Lemma 3.2, we have $(C'_F D_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p = C_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Also, C'_F and D_F are $G(F/K)$-stable (see [dS87, II, Proposition 2.4]). Moreover, it is not a difficult exercise to show that the norm maps $N_{K_{k,n}/K_{k',n'}}$, $k \geq k' \geq 1$, $n \geq n' \geq 1$, restrict to maps $C'_{K_{k,n}} \to C'_{K_{k',n'}}$ and $D_{K_{k,n}} \to D_{K_{k',n'}}$, respectively.

(ii) For any $\mathfrak{m}$ and any primitive $\mathfrak{m}$-division point τ the element $\Theta(\tau;\mathfrak{a})^{\sigma-1}$ belongs to $\mathcal{O}^{\times}_{K(\mathfrak{m})}$ for any $\sigma \in G(K(\mathfrak{m})/K)$ (see [S14, Remark 2.4.10]). It follows that $(N_{FK(\mathfrak{m})/F}\Theta(\tau;\mathfrak{a}))^{\sigma-1}$ belongs to $\mathcal{O}^{\times}_{F}$ for $F = K_{k,n}$ and any $\sigma \in G(F/K)$.

With the above definitions, Lemma 3.2 implies that for all $k, n \geq 1$ as in the lemma, we have surjections of $\mathbb{Z}_p[G(K_{k,n}/K)]$-modules

$$D_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p \twoheadrightarrow (C_{K_{k,n}}/C'_{K_{k,n}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

The next lemma shows that the natural inclusions $C'_{K_{k,n}} \hookrightarrow C_{K_{k,n}}$ induce isomorphisms of $\Lambda(G)$-modules

$$\varprojlim_{k,n}(C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cong \varprojlim_{k,n}(C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p). \tag{5}$$

Lemma 3.5. *We have*

$$\varprojlim_{k,n}(D_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = 0,$$

where the limit is taken with respect to the norm maps.

Proof. In Remark 3.4 we have explained that $D_{K_{k,n}} \subset \mathcal{O}^{\times}_{K_{k,n}}$. This inclusion induces

$$D_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \mathcal{O}^{\times}_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

and we note that by Dirichlet's unit theorem the group on the right is given by the direct sum of a finite number of copies of $\mathbb{Z}_p$ and the finite group of p-power roots of unity in $K_{k,n}$.

Let us make a few more observations. For any integral ideal $\mathfrak{a}$ of K we always have $K(\mathfrak{a}) \subset K(E[\mathfrak{a}])$ (see [Si99, II, Theorem 5.6]). It follows from [S14, Proposition A.6.3] that, for all $k, n \geq 1$,

$$K_{k,n} \cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k) \subset K_{k,n} \cap K(E[\mathfrak{f}'\bar{\mathfrak{p}}^k]) = K_{k,0}. \tag{6}$$

Likewise, for all $k, n \geq 1$ we have

$$K_{k,n} \cap K(\mathfrak{f}'\mathfrak{p}^n) \subset K_{k,n} \cap K(E[\mathfrak{f}'\mathfrak{p}^n]) = K_{0,n}. \tag{7}$$

For any $r \geq 1$, let us consider $d_{k+r,n+r} = (N_{K_{k+r,n+r}K(\mathfrak{m})/K_{k+r,n+r}}\Theta(\tau;\mathfrak{a}))^{\sigma-1}$, an arbitrary element of the set of generators of $D_{K_{k+r,n+r}}$ given in Definition 3.3, where

$$\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^{k+r} \quad \text{or} \quad \mathfrak{m} = \mathfrak{f}'\mathfrak{p}^{n+r} \qquad \text{for some divisor } \mathfrak{f}' \text{ of } \mathfrak{f}.$$

First assume that $\mathfrak{m} = \mathfrak{f}'\bar{\mathfrak{p}}^{k+r}$. Note that for $k, n \geq 1$ the Galois group $G(K_{k+r,n+r}/K_{k+r,n})$ is of order p^r, which follows from [dS87, II, Corollary

1.7], and any $g \in G(K_{k+r,n+r}/K_{k+r,n})$ fixes $K_{k+r,0}$. Then (6) shows that for $k, n \geq 1$ we have

$$\begin{aligned}
&N_{K_{k+r,n+r}/K_{k,n}}(d_{k+r,n+r}) \\
&= (N_{K_{k+r,n+r}/K_{k,n}} \circ N_{K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r})/(K_{k+r,0}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}))}\Theta(\tau;\mathfrak{a}))^{\sigma-1} \\
&= (N_{K_{k+r,n}/K_{k,n}} \circ N_{K_{k+r,n+r}/K_{k+r,n}} \circ N_{K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r})/(K_{k+r,0}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}))}\Theta(\tau;\mathfrak{a}))^{\sigma-1} \\
&= (N_{K_{k+r,n}/K_{k,n}} \circ N_{K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r})/(K_{k+r,0}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^{k+r}))}\Theta(\tau;\mathfrak{a}))^{p^r(\sigma-1)}.
\end{aligned}$$

By a similar argument for $\mathfrak{m} = \mathfrak{f}'\mathfrak{p}^{n+r}$, for $k, n \geq 1$ we have

$$\begin{aligned}
&N_{K_{k+r,n+r}/K_{k,n}}(d_{k+r,n+r}) \\
&\qquad = (N_{K_{k,n+r}/K_{k,n}} \circ N_{K(\mathfrak{f}'\mathfrak{p}^{n+r})/(K_{0,n+r}\cap K(\mathfrak{f}'\mathfrak{p}^{n+r})}\Theta(\tau;\mathfrak{a}))^{p^r(\sigma-1)},
\end{aligned}$$

which follows from (7). These two cases imply that for any element d of $D_{K_{k+r,n+r}}$ we have

$$N_{K_{k+r,n+r}/K_{k,n}}(d) = c^{p^r} \tag{8}$$

for some unit c in $\mathcal{O}_{K_{k,n}}^\times$.

Now, let $(a_{k,n})_{k,n}$ be an element of $\varprojlim_{k,n} D_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Let $k, n \geq 1$ be large enough so that they satisfy the conditions of Lemma 3.2, i.e., so that both $\mathcal{O}_K^\times \to \mathcal{O}_K/\bar{\mathfrak{p}}^k$ and $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{p}^n$ are injective. For any $r \geq 1$ the element $a_{k+r,n+r} \in D_{K_{k+r,n+r}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is of the form

$$a_{k+r,n+r} = \sum_{i=1}^m d_i \otimes b_i$$

for some $d_i \in D_{K_{k+r,n+r}}$ and $b_i \in \mathbb{Z}_p$, $i = 1, \ldots, m$. Using (8), we can find $c_1, \ldots, c_m$ in $\mathcal{O}_{K_{k,n}}^\times$ such that

$$a_{k,n} = (N_{K_{k+r,n+r}/K_{k,n}} \otimes \mathrm{id}_{\mathbb{Z}_p})(a_{k+r,n+r}) = \sum_{i=1}^m c_i^{p^r} \otimes b_i = \Big(\sum_{i=1}^m c_i \otimes b_i\Big)p^r,$$

and we see that as an element of $\mathcal{O}_{K_{k,n}}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $a_{k,n}$ is divisible by an arbitrarily large power of p since we can choose any $r \geq 1$. By the remark made at the beginning of the proof, only the trivial element satisfies this divisibility property. ∎

According to the definition we gave, elliptic units of an abelian extension F of K contain the roots of unity of F. Eventually, we will be interested in projective limits of elliptic units and need the following vanishing result for p-power roots of unity for $\mathbb{Z}_p^2$-extensions of K.

LEMMA 3.6. *Let L be a number field and M/L an extension containing a $\mathbb{Z}_p$-extension L_∞/L that is independent of the cyclotomic $\mathbb{Z}_p$-extension*

L_{cyc}/L of L. Then

$$\varprojlim_{L\subseteq_f L'\subset M} \mu_{p^\infty}(L') = 1,$$

where $\mu_{p^\infty}(L')$ denotes the group of p-power roots of unity in L', and the limit is taken over the finite extensions L' of L contained in M and with respect to norm maps.

Proof. Let $(\zeta_{L'})_{L'}$ be an element of $\varprojlim_{L\subseteq_f L'\subset M} \mu_{p^\infty}(L')$. Let us show that $\zeta_{L'} = 1$ for any finite extension L' of L. For any such extension the composite $L'L_\infty$ contains only finitely many p-power roots of unity since L_∞/L is independent of the cyclotomic $\mathbb{Z}_p$-extension L_{cyc}/L.

Let ζ_{p^n} be a primitive p^nth root of unity belonging to $L'L_\infty$ such that n is maximal with respect to this property. Write L'_m for the mth layer of the $\mathbb{Z}_p$-extension $L'L_\infty/L'$ (note that $G(L'L_\infty/L')$ embedds into $G(L_\infty/L) \cong \mathbb{Z}_p$ and the image is the continuous image of a compact set in a Hausdorff space and therefore closed in $G(L_\infty/L)$, hence of the form $p^n\mathbb{Z}_p \subset \mathbb{Z}_p$, and it follows that $G(L'L_\infty/L')$ is a $\mathbb{Z}_p$-extension). Then $G(L'_m/L')$ has order p^m. Let k be large enough so that ζ_{p^n} belongs to L'_k (such a k exists since $L'L_\infty = \bigcup_m L'_m$). Then

$$\zeta_{L'} = N_{L'_{k+n}/L'}(\zeta_{L'_{k+n}}) = N_{L'_k/L'}(N_{L'_{k+n}/L'_k}(\zeta_{L'_{k+n}})) = N_{L'_k/L'}(\zeta_{L'_{k+n}}^{p^n}) = 1,$$

since $\zeta_{L'_{k+n}} \in \mu_{p^\infty}(L'L_\infty) = \mu_{p^n} \subset L'_k$. ∎

Let us now recall that Rubin's elliptic units for an abelian finite extension F of K were defined by $\mathcal{C}(F) = \mu_\infty(F)C_F$, where $\mu_\infty(F)$ is the group of all roots of unity in F. Tensoring with $\mathbb{Z}_p$ kills the roots of unity of order prime to p, so that as subgroups of $\mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$,

$$\mathcal{C}(F) \otimes_{\mathbb{Z}} \mathbb{Z}_p = (\mu_{p^\infty}(F)C_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

where $\mu_{p^\infty}(F)$ is the group of p-power roots of unity in F. The extension K_∞/K, $K_\infty = \bigcup_{n,k} K(E[\mathfrak{p}^n\bar{\mathfrak{p}}^k])$, contains the cyclotomic and the anticyclotomic $\mathbb{Z}_p$-extension, so that Lemma 3.6 implies

$$\varprojlim_{k,n}(C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathcal{C}_R.$$

Together with (5) this proves the following result.

Corollary 3.7. *The natural inclusions induce the equalities*

$$\varprojlim_{k,n}(C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(C_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathcal{C}_R.$$

Let us record one more technical lemma stating that multiplication with the augmentation ideal commutes with passage to the projective limit. We will write $F_{k,n} = K(\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n)$ for the ray class field of K modulo $\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n$. Recall the definition of $\Theta_{\mathfrak{m}}$ from (2) and Remark 2.6.

LEMMA 3.8. *Let p be a prime number $(p,6)=1$ that splits in K into distinct primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. Then as subgroups of $\varprojlim_{n,k}(\mathcal{O}_{K_{k,n}}^{\times}\otimes_{\mathbb{Z}}\mathbb{Z}_p)$,*

$$I\varprojlim_{k,n}((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k})\otimes_{\mathbb{Z}}\mathbb{Z}_p) = \varprojlim_{n,k}((I(K_{k,n}/K)N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k})\otimes_{\mathbb{Z}}\mathbb{Z}_p), \tag{9}$$

where we write I for the augmentation ideal $I(K_\infty/K)$.

Proof. This follows from the fact that the norm maps on the groups $\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$ are surjective (see [dS87, II, 2.3 and proof of Proposition 2.4(iii)]). ∎

Before proving the next theorem, we need to make one more definition.

DEFINITION 3.9. For any prime ideal $\mathfrak{l}$ dividing $\mathfrak{f}$ we define a Galois automorphism $\sigma_{\mathfrak{l}}$ in $G(K_\infty/K)$ as follows. Write $n_{\mathfrak{l}}$ for the exact exponent of $\mathfrak{l}$ in $\mathfrak{f}$. Then we can consider the arithmetic Frobenius

$$\left(\mathfrak{l}, K\left(p^\infty\frac{\mathfrak{f}}{\mathfrak{l}^{n_{\mathfrak{l}}}}\right)/K\right) \quad \text{at } \mathfrak{l} \text{ in } G(K(p^\infty\tfrac{\mathfrak{f}}{\mathfrak{l}^{n_{\mathfrak{l}}}})/K),$$

take a lift of it to $G(K(p^\infty\mathfrak{f})/K)$ and write $\sigma_{\mathfrak{l}}$ for the restriction to $G(K_\infty/K)$.

THEOREM 3.10. *Fix any prime ideal $\mathfrak{c}$ of $\mathcal{O}_K$ such that $(\mathfrak{c},6p\mathfrak{f})=1$. The quotient $\mathcal{C}_R/\mathcal{C}_Y$, where*

$$\mathcal{C}_Y = I\varprojlim_{k,n}((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k})\otimes_{\mathbb{Z}}\mathbb{Z}_p),$$

is annihilated by the element

$$(\sigma_{\mathfrak{c}}-N\mathfrak{c})\cdot\prod_{\mathfrak{l}\mid\mathfrak{f}}(1-\sigma_{\mathfrak{l}}^{-1}),$$

where $\sigma_{\mathfrak{c}}=(\mathfrak{c},K_\infty/K)$ and the product is taken over the primes dividing the conductor $\mathfrak{f}$. In particular, the quotient is S-torsion.

Proof. For the last statement about S-torsion, we refer to [S14, Lemmata A.9.2 and A.9.5] for the fact that choosing $\mathfrak{c}$ to be equal to a prime $\mathfrak{q}$ such that $N(\mathfrak{q})$ is congruent to 1 modulo p makes the element $(\sigma_{\mathfrak{c}}-N\mathfrak{c})\cdot\prod_{\mathfrak{l}\mid\mathfrak{f}}(1-\sigma_{\mathfrak{l}}^{-1})$ belong to S. Let us now prove the first part of the theorem.

Let us write $C''_{K_{k,n}}$ for the subgroup $I(K_{k,n}/K)N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}$ of $C'_{K_{k,n}}$. By Corollary 3.7 and Lemma 3.8 the statement we are proving is equivalent to the assertion that the quotient of

$$\varprojlim_{n,k}(C''_{K_{k,n}}\otimes_{\mathbb{Z}}\mathbb{Z}_p)\subset\varprojlim_{k,n}(C'_{K_{k,n}}\otimes_{\mathbb{Z}}\mathbb{Z}_p)$$

is annihilated by $(\sigma_{\mathfrak{c}}-N\mathfrak{c})\cdot\prod_{\mathfrak{l}\mid\mathfrak{f}}(1-\sigma_{\mathfrak{l}}^{-1})$. It is clearly sufficient to show that, for all $k,n\geq 1$ as in Lemma 3.2 (i.e. such that both $\mathcal{O}_K^{\times}\to\mathcal{O}_K/\bar{\mathfrak{p}}^k$

and $\mathcal{O}_K^\times \to \mathcal{O}_K/\mathfrak{p}^n$ are injective),

$$(C'_{K_{k,n}}/C''_{K_{k,n}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

is annihilated by $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}|\mathfrak{f}}(1-\sigma_{\mathfrak{l}}^{-1})$. Take an arbitrary generator of $C'_{K_{k,n}}$, which is of the form

$$(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{a}))^{\sigma-1},$$

where σ belongs to $\mathrm{Gal}(K_{k,n}/K)$, $\mathfrak{f}'$ is some divisor of $\mathfrak{f}$, $\mathfrak{a}$ is an integral ideal such that $(\mathfrak{a}, 6\mathfrak{f}'p) = 1$, and τ is a primitive $\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n$-division point. We will show that this generator multiplied by $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}|\mathfrak{f}}(1-\sigma_{\mathfrak{l}}^{-1})$ belongs to $C''_{K_{k,n}}$.

Recall that we write

$$\mathfrak{f} = \prod_{\mathfrak{l}|\mathfrak{f}} \mathfrak{l}^{n_{\mathfrak{l}}},$$

where $n_{\mathfrak{l}} \geq 0$ is the exponent of the prime $\mathfrak{l}$ in the decomposition of $\mathfrak{f}$.

If $\mathfrak{l} \,|\, \mathfrak{f}'$, then we may assume that $\mathfrak{l}^{n_{\mathfrak{l}}} \,|\, \mathfrak{f}'$. This can be shown just as the third case in the proof of Lemma 3.2. In fact, if l is an $\mathcal{O}_K$-generator of $\mathfrak{l}$ and $m_{\mathfrak{l}}$, with $m_{\mathfrak{l}} < n_{\mathfrak{l}}$, is the exact exponent of $\mathfrak{l}$ in $\mathfrak{f}'$, then by [Ru99, Corollary 7.7], we have

$$N_{K(\mathfrak{l}^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)}\Theta\left(\frac{\tau}{l^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}};\mathfrak{a}\right) = \Theta(\tau;\mathfrak{a}),$$

which yields

$$\begin{aligned}&(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{a}))^{\sigma-1}\\ &\qquad = \left(N_{K(\mathfrak{l}^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)\cap K_{k,n})}\Theta\left(\frac{\tau}{l^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}};\mathfrak{a}\right)\right)^{\sigma-1},\end{aligned}$$

showing that our arbitrary generator is a product of Galois conjugates of

$$\left(N_{K(\mathfrak{l}^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K(\mathfrak{l}^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)\cap K_{k,n})}\Theta\left(\frac{\tau}{l^{n_{\mathfrak{l}}-m_{\mathfrak{l}}}};\mathfrak{a}\right)\right)^{\sigma-1}.$$

This shows that we may assume that the exponent of $\mathfrak{l}$ in $\mathfrak{f}'$ is equal to $n_{\mathfrak{l}}$ whenever $\mathfrak{l}$ already divides $\mathfrak{f}'$.

We now turn our attention to primes $\mathfrak{l}$ dividing $\mathfrak{f}$ but not dividing $\mathfrak{f}'$. It is now, that the element $(\sigma_{\mathfrak{c}} - N\mathfrak{c}) \cdot \prod_{\mathfrak{l}|\mathfrak{f}}(1-\sigma_{\mathfrak{l}}^{-1})$ comes into play. The next observation will explain why we need the factor $\sigma_{\mathfrak{c}} - N\mathfrak{c}$. For our arbitrary generator

$$(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{a}))^{\sigma-1}$$

of $C'_{K_{k,n}}$ we allow any $\mathfrak{a}$ prime to $6p\mathfrak{f}'$. In particular, $\mathfrak{l}$ might divide $\mathfrak{a}$. But we want to use [Ru99, Corollary 7.7] again, which we can only do for $\mathfrak{a}$ prime to $\mathfrak{l}$. Writing $\sigma_\mathfrak{c}$ also for the lift $(\mathfrak{c}, F_\infty/K)$ to $G(F_\infty/K)$, we see that [dS87, II, Proposition 2.4] shows

$$\Theta(\tau;\mathfrak{a})^{\sigma_\mathfrak{c}-N\mathfrak{c}} = \frac{\Theta(\tau;\mathfrak{ac})}{\Theta(\tau;\mathfrak{c})^{N\mathfrak{a}}\cdot\Theta(\tau;\mathfrak{a})^{N\mathfrak{c}}} = \Theta(\tau;\mathfrak{c})^{\sigma_\mathfrak{a}-N\mathfrak{a}},$$

so that

$$(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{a}))^{(\sigma_\mathfrak{c}-N\mathfrak{c})(\sigma-1)} = (N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{c}))^{(\sigma_\mathfrak{a}-N\mathfrak{a})(\sigma-1)}.$$

Therefore it is sufficient to show that

$$(N_{K_{k,n}K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{c}))^{(\sigma_\mathfrak{a}-N\mathfrak{a})(\sigma-1)\cdot\prod_{\mathfrak{l}|\mathfrak{f}}(1-\sigma_\mathfrak{l}^{-1})} \tag{10}$$

belongs to $C''_{K_{k,n}}$. Now, for a prime $\mathfrak{l}$ dividing $\mathfrak{f}$ but not dividing $\mathfrak{f}'$, we deduce from [Ru99, Corollary 7.7] that

$$N_{K(\mathfrak{l}\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)}\Theta\left(\frac{\tau}{l};\mathfrak{c}\right) = \Theta(\tau;\mathfrak{c})^{(1-\sigma_\mathfrak{l}^{-1})},$$

where we write $\sigma_\mathfrak{l}$ also for the lift of

$$\left(\mathfrak{l}, K\left(p^\infty\frac{\mathfrak{f}}{\mathfrak{l}^{n_\mathfrak{l}}}\right)/K\right)$$

to $G(K(p^\infty\mathfrak{f})/K)$ as in the definition of $\sigma_\mathfrak{l}$. Applying this to all the primes $\mathfrak{l}_1,\dots,\mathfrak{l}_r$ dividing $\mathfrak{f}$ but not dividing $\mathfrak{f}'$ we see that the element from (10) is equal to

$$\left(N_{K(\mathfrak{l}_1\dots\mathfrak{l}_r\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K_{k,n}\cap K(\mathfrak{f}'\bar{\mathfrak{p}}^k\mathfrak{p}^n))}\Theta\left(\frac{\tau}{l_1\dots l_r};\mathfrak{c}\right)\right)^{(\sigma_\mathfrak{a}-N\mathfrak{a})(\sigma-1)\cdot\prod_{\mathfrak{l}|\mathfrak{f}'}(1-\sigma_\mathfrak{l}^{-1})}, \tag{11}$$

where we write l_i for generators of $\mathfrak{l}_i$. Now we can proceed as in the first step, when we showed that if $\mathfrak{l}\,|\,\mathfrak{f}'$, then we may assume that $\mathfrak{l}^{n_\mathfrak{l}}\mid\mathfrak{f}'$, proving that the element from (11) belongs to $C''_{K_{k,n}}$. ∎

3.3. Description of Yager's units via the Coleman map. For any prime ideal $\mathfrak{P}$ of $K_{k,n}$ above the prime $\mathfrak{p}$ of K we write $K_{k,n,\mathfrak{P}}$ for the completion of $K_{k,n}$ at $\mathfrak{P}$, $\mathcal{O}^1_{K_{k,n,\mathfrak{P}}}$ for the subgroup of principal units in the group of units $\mathcal{O}^\times_{K_{k,n,\mathfrak{P}}}$, and $\hat{\mathcal{O}}^\times_{K_{k,n,\mathfrak{P}}}$ for the p-adic completion of $\mathcal{O}^\times_{K_{k,n,\mathfrak{P}}}$. We canonically have $\mathcal{O}^1_{K_{k,n,\mathfrak{P}}}\cong\hat{\mathcal{O}}^\times_{K_{k,n,\mathfrak{P}}}$. We will write

$$U_{k,n} = \prod_{\mathfrak{P}|\mathfrak{p}}\mathcal{O}^1_{K_{k,n,\mathfrak{P}}} \cong \prod_{\mathfrak{P}|\mathfrak{p}}\hat{\mathcal{O}}^\times_{K_{k,n,\mathfrak{P}}}$$

for the group of principal units, which is a subgroup of the semilocal units $\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}^{\times}_{K_{k,n,\mathfrak{P}}}$, and set

$$\mathcal{U}_\infty = \varprojlim_{k,n} U_{k,n},$$

where the projective limit is taken with respect to norm maps. We write $\mathcal{E}_\infty = \varprojlim_{k,n} (\mathcal{O}^{\times}_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ for the global units, where the projective limit is taken with respect to norm maps, and note that since Leopoldt's conjecture holds for finite abelian extensions of K, we have an embedding

$$\mathcal{E}_\infty \hookrightarrow \mathcal{U}_\infty.$$

In the following we will write $\Lambda(G, \widehat{\mathbb{Z}}_p^{ur})$ for the Iwasawa algebra of G with coefficients in $\widehat{\mathbb{Z}}_p^{ur}$, and $W(\bar{\mathbb{F}}_p)$ for the ring of Witt vectors of a fixed algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$. Next we remind the reader that there is a semilocal version

$$\mathbb{L} : \mathcal{U}_\infty \hookrightarrow \Lambda(G, \widehat{\mathbb{Z}}_p^{ur})$$

of the Coleman map for the formal group $\hat{E}$ associated to a fixed Weierstraß equation of E, which we briefly explain in the following remark and refer to [S14, Theorem 2.4.25 and Corollary 2.4.26] for more details regarding its construction and its injectivity.

Remark 3.11. (i) We note that $\mathbb{L}$ is obtained as the limit $\varprojlim_k \mathbb{L}_k$ of maps $\mathbb{L}_k : \varprojlim_n U_{k,n} \to \Lambda(G_k, \widehat{\mathbb{Z}}_p^{ur})$ for $k \geq 1$, where $G_k = \mathrm{Gal}(K_{k,\infty}/K)$, $K_{k,\infty} = \bigcup_n K_{k,n}$.

(ii) The $\mathbb{L}_k$ are given in the following way. Write $\hat{D}$ for the completion of $\mathcal{O}_{K_{\infty,0}} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}}$. There is an isomorphism of formal groups $\theta : \hat{\mathbb{G}}_m \cong \hat{E}$, $\theta \in \hat{D}[[X]]$. We write $\phi = \sigma_\mathfrak{p}$ for the arithmetic Frobenius element at $\mathfrak{p}$ in $G(K_{\infty,0}/K)$ and note that $G(K_{\infty,0}/K)$ acts on $K_{\infty,0} \otimes_K K_\mathfrak{p}$ via the action on the first factor and that, by continuity, this action extends to the completion. Let us also fix a generator $(\zeta_n)_n$ of $\varprojlim_n \mu_{p^n}(\bar{K})$, i.e., a compatible system of primitive p-power roots of unity, and write

$$\omega_n = \theta^{\phi^{-n}}(\zeta_n - 1).$$

The semilocal version of Coleman's theorem (compare [dS87, II, Proposition 4.5]) says that for every

$$u = (u_n)_n \in U_{k,\infty} := \varprojlim_n U_{k,n}$$

there exists a unique power series $g_u(T) \in \mathcal{O}_{k,0,\mathfrak{p}}[[T]]^\times$ such that

$$u_n = (\phi^{-n} g_u)(\omega_n).$$

Moreover (compare [dS87, I, Section 3.4 and II, Proposition 4.6]), there is a unique G_k-homomorphism

$$i_k : U_{k,\infty} \to \Lambda(G_k, \hat{D}), \quad i_k(u) = \lambda_u \tag{12}$$

such that

$$\widetilde{\log g_u} \circ \theta(X) = \int_{G_{k,0}} (1+X)^{\kappa(\sigma)}\, d\lambda_u(\sigma), \tag{13}$$

where $G_{k,0} = \mathrm{Gal}(K_{k,\infty}/K_{k,0})$, κ denotes the $\mathbb{Z}_p^\times$-valued character defined by the action of $G_{k,0}$ on $E[\mathfrak{p}^\infty]$, and

$$\widetilde{\log g}(T) = \log g(T) - \frac{1}{p} \sum_{\omega \in \hat{E}[\mathfrak{p}]} \log g(T[+]\omega),$$

where, in turn, $\hat{E}[\mathfrak{p}]$ denotes the set of division points of level 1 in $\hat{E}$ and $[+]$ is addition induced by the formal group. The map $\mathbb{L}_k$ is now defined to be the composition of i_K with a map $\Lambda(G_k, \hat{D}) \to \Lambda(G_k, \hat{\mathbb{Z}}_p^{ur})$ induced by an embedding $\bar{\mathbb{Q}} \subset \mathbb{C}_p$.

Definition 3.12. Assume that p is prime to 6 and fix an $\mathcal{O}_K$-generator f of the conductor $\mathfrak{f}$ of E, i.e., $\mathfrak{f} = (f)$. For $k, n \geq 1$ and an integral ideal $\mathfrak{a}$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, we set

$$e_{k,n}(\mathfrak{a}) := N_{F_{k,n}/K_{k,n}}\left(\Theta\left(\frac{\Omega}{f\bar{\pi}^k\pi^n}, L, \mathfrak{a}\right)\right) \in \mathcal{O}_{K_{k,n}}^\times,$$

which defines a norm-compatible system $e(\mathfrak{a}) = (e_{k,n}(\mathfrak{a}))_{k,n} \in \varprojlim_{k,n} \mathcal{O}_{K_{k,n}}^\times$ of global units. We write $u(\mathfrak{a})$ for the image of $e(\mathfrak{a})$ in $\mathcal{E}_\infty$ and also denote by $u(\mathfrak{a})$ the image in $\mathcal{U}_\infty = \varprojlim_{k,n} U_{k,n}$ under $\mathcal{E}_\infty \hookrightarrow \mathcal{U}_\infty$. We define

$$\lambda_{\mathfrak{a}} := \lambda^0_{u(\mathfrak{a})} = \mathbb{L}(u(\mathfrak{a})),$$

as the p-adic integral measure on G corresponding to $u(\mathfrak{a})$ under $\mathbb{L}$. We moreover define

$$\lambda := \frac{1}{12} \cdot \frac{\lambda_{\mathfrak{a}}}{x_{\mathfrak{a}}} \in Q(\Lambda(G, \hat{\mathbb{Z}}_p^{ur})),$$

where $x_{\mathfrak{a}} := \sigma_{\mathfrak{a}} - N\mathfrak{a}$, $\sigma_{\mathfrak{a}} = (\mathfrak{a}, K_\infty/K) \in G$. It can be shown that λ is independent of $\mathfrak{a}$ and actually an integral measure, i.e., $\lambda \in \Lambda(G, \hat{\mathbb{Z}}_p^{ur})$ (compare [dS87, II proof of Theorem 4.12], where this is shown at the level of each $\Lambda(G_k, \widehat{\mathbb{Z}}_p^{ur})$).

Proposition 3.13. *The map $\mathbb{L}$ defines an isomorphism of $\Lambda(G)$-modules*

$$\varprojlim_{n,k}((N_{F_{n,k}/K_{n,k}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cong J\lambda,$$

where J is the annihilator in $\Lambda(G)$ of $\mu_{p^\infty}(K_\infty)$, the module of p-power roots of unity in K_∞.

Proof. The elements $u(\mathfrak{a})$, $(\mathfrak{a}, \mathfrak{f}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, from Definition 3.12, generate

$$\varprojlim_{n,k}((N_{F_{n,k}/K_{n,k}}\Theta_{\mathfrak{f}\mathfrak{p}^n\bar{\mathfrak{p}}^k}) \otimes_{\mathbb{Z}} \mathbb{Z}_p) \tag{14}$$

as a $\Lambda(G)$-module, which follows from a simple compactness argument. By definition, the image of $u(\mathfrak{a})$ under $\mathbb{L}$ is given by

$$\mathbb{L}(u(\mathfrak{a})) = 12x_{\mathfrak{a}}\lambda.$$

Note that 12 is a unit in $\mathbb{Z}_p$ since $p \neq 2,3$. The statement now follows from the fact that the elements $x_{\mathfrak{a}} = \sigma_{\mathfrak{a}} - N\mathfrak{a}$ for varying $\mathfrak{a}$, $(\mathfrak{a}, \mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$, generate J, which we prove in Lemma 3.15 below. ■

Using Proposition 3.1 and Lemma 3.8 we immediately get the following description of Yager's units $\mathcal{C}_Y := \varprojlim_{k,n}(C_{Y,k,n} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$.

Corollary 3.14. *The map* $\mathbb{L}$ *induces an isomorphism*

$$\mathcal{C}_Y \cong IJ\lambda,$$

where, we recall, I denotes the augmentation ideal $I(K_\infty/K)$ in $\Lambda(G)$.

Lemma 3.15. *The annihilator $J = \mathrm{Ann}_{\Lambda(G)}(\mu_{p^\infty}(K_\infty))$ of $\mu_{p^\infty}(K_\infty)$ in $\Lambda(G)$ is generated by $\sigma_{\mathfrak{a}} - N\mathfrak{a}$, $\mathfrak{a}$ and $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$, where $\sigma_{\mathfrak{a}} = (\mathfrak{a}, K_\infty/K)$.*

Proof. For each n we denote by l_n the greatest number such that $K_{n,n} = K(E[p^n])$ contains a primitive p^{l_n}th root of unity. Let us write $G_{n,n} = G(K_{n,n}/K)$. Then for each $n \geq 1$ we consider the $\mathbb{Z}_p/(p^{l_n})[G_{n,n}]$-module $\mu_{p^\infty}(K_{n,n})$. Let $\sum_g a_g g$ be an element of $\mathbb{Z}_p/(p^{l_n})[G_{n,n}]$ that annihilates $\mu_{p^\infty}(K_{n,n})$. By Chebotarev's density theorem, for all $g \in G_{n,n}$ we can find a prime ideal $\mathfrak{q}_g$ prime to $6\mathfrak{f}p$ such that $g = (\mathfrak{q}_g, K_{n,n}/K)$. We can then write

$$\sum_g a_g g = \sum_g a_g(g - \overline{N\mathfrak{q}_g}) + \sum_g a_g \overline{N\mathfrak{q}_g}.$$

Clearly, $\sum_g a_g(g - \overline{N\mathfrak{q}_g})$ belongs to the annihilator of $\mu_{p^\infty}(K_{n,n})$ (since $g = \overline{(\mathfrak{q}_g, K_{n,n}/K)}$ acts as multiplication by $N\mathfrak{q}_g$ on $\mu_{p^\infty}(K_{n,n})$) and we see that $\sum_g a_g\overline{N\mathfrak{q}_g}$, which is just the residue class of an integer, must be congruent to 0 modulo (p^{k_n}); this implies that $\sum_g a_g g = \sum_g a_g(g - \overline{N\mathfrak{q}_g})$ in $\mathbb{Z}_p/(p^{l_n})[G_{n,n}]$. We see that $\mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G_{n,n}]}(\mu_{p^\infty}(K_{n,n}))$ is generated by elements of the form $(\mathfrak{a}, K_{n,n}/K) - \overline{N\mathfrak{a}}$, $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$.

For each $n \geq 1$ we can now consider the exact sequence

$$0 \to \mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G_{n,n}]}(\mu_{p^\infty}(K_{n,n})) \to \mathbb{Z}_p/(p^{l_n})[G_{n,n}] \to \mathbb{Z}_p/(p^{l_n})(1) \to 0.$$

Passing to the projective limit, we get

$$J = \varprojlim_n \mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G_{n,n}]}(\mu_{p^\infty}(K_{n,n})).$$

Writing J_0 for the ideal of $\Lambda(G)$ generated by elements of the form $\sigma_{\mathfrak{a}} - N\mathfrak{a}$, $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}\bar{\mathfrak{p}}) = 1$, we have shown above that for each $n \geq 1$ the natural projection $\Lambda(G) \twoheadrightarrow \mathbb{Z}_p/(p^{l_n})[G_{n,n}]$ induces a surjection

$$J_0 \twoheadrightarrow \mathrm{Ann}_{\mathbb{Z}_p/(p^{l_n})[G_{n,n}]}(\mu_{p^\infty}(K_{n,n})).$$

Since $\Lambda(G)$ is compact and Noetherian, J_0 is also compact. Therefore, by passing to the limit we get the desired surjection $J_0 \twoheadrightarrow J$. ■

3.4. Description of Rubin's units via the Coleman map in the prime power conductor case. If E is already defined over $\mathbb{Q}$ and E is a representative with minimal discriminant and conductor in its $\bar{\mathbb{Q}}$-isomorphism class as in [Si99, Appendix A, §3], then

$$\mathfrak{f} = \mathfrak{l}^r, \qquad r \geq 1,$$

i.e., the conductor $\mathfrak{f}$ of the Größencharacter of E/K is a prime power for some prime ideal $\mathfrak{l}$ (see [S14, Theorem A.6.8 and Proposition A.6.9]). It is precisely this condition that we want to impose on a general elliptic curve E/K with CM by $\mathcal{O}_K$ in this subsection.

Assumption 3.16. We assume that the conductor $\mathfrak{f}$ of the Größencharacter ψ over K is a prime power

$$\mathfrak{f} = \mathfrak{l}^r$$

for some prime ideal $\mathfrak{l}$ and some $r \geq 1$.

In the previous subsection we determined the image of Yager's elliptic units $\mathcal{C}_Y$ under the semilocal version $\mathbb{L}$ of the Coleman map. In this subsection we will determine the image under $\mathbb{L}$ of Rubin's elliptic units $\mathcal{C}_R := \varprojlim_{k,n}(\mathcal{C}(K_{k,n}) \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ under the above Assumption 3.16. Let us write $L_{k,n} = K(\bar{\mathfrak{p}}^k\mathfrak{p}^n)$ for the ray class field of K modulo $\bar{\mathfrak{p}}^k\mathfrak{p}^n$, so that we have $L_{k,n} \subset K_{k,n} \subset F_{k,n}$. We also set $L_\infty = \bigcup_{k,n} L_{k,n}$.

Definition 3.17. Assume that p is prime to 6 and prime to $\#(\mathcal{O}_K/\mathfrak{f})^\times$. For $k, n \geq 1$ and an integral ideal $\mathfrak{a}$, $(\mathfrak{a}, \bar{\mathfrak{p}}\mathfrak{p}) = 1$, we write

$$\tilde{e}_{k,n}(\mathfrak{a}) := \Theta\left(\frac{\Omega}{\bar{\pi}^k\pi^n}, L, \mathfrak{a}\right) \in \mathcal{O}_{L_{k,n}}^\times,$$

which defines a norm-compatible system $\tilde{e}(\mathfrak{a}) = (\tilde{e}_{k,n}(\mathfrak{a}))_{k,n} \in \varprojlim_{k,n} \mathcal{O}_{L_{k,n}}^\times$ of global units. Now take $k, n \geq 1$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^{k-1}\mathfrak{p}^{n-1})^\times$ is injective. Since the natural maps (induced by restriction) $G(K_{k,n}/K_{k-1,n-1}) \to G(L_{k,n}/L_{k-1,n-1})$ are bijections (see [S14, Corollary A.6.6]), $\tilde{e}(\mathfrak{a})$ is also a norm-compatible system in $\varprojlim_{k,n} \mathcal{O}_{K_{k,n}}^\times$.

We write $\tilde{u}(\mathfrak{a})$ for the image of $\tilde{e}(\mathfrak{a})$ in $\mathcal{E}_\infty$ and also denote by $\tilde{u}(\mathfrak{a})$ the image in $\mathcal{U}_\infty = \varprojlim_{k,n} U_{k,n}$ under $\mathcal{E}_\infty \hookrightarrow \mathcal{U}_\infty$. We define

$$\tilde{\lambda}_{\mathfrak{a}} := \tilde{\lambda}^0_{u(\mathfrak{a})} = \mathbb{L}(\tilde{u}(\mathfrak{a})),$$

as the p-adic integral measure on G corresponding to $\tilde{u}(\mathfrak{a})$ under $\mathbb{L}$. We also define

$$\tilde{\lambda} := \frac{1}{12} \cdot \frac{\tilde{\lambda}_{\mathfrak{a}}}{x_{\mathfrak{a}}} \in Q(\Lambda(G, \hat{\mathbb{Z}}_p^{ur})),$$

where $x_{\mathfrak{a}} := \sigma_{\mathfrak{a}} - N\mathfrak{a}$, $\sigma_{\mathfrak{a}} = (\mathfrak{a}, K_\infty/K) \in G$. As in the case of λ, the definition of $\tilde{\lambda}$ is independent of $\mathfrak{a}$ (see [dS87, II, Proposition 2.4(ii)]), and $\tilde{\lambda}$ is an integral measure, so that $\tilde{\lambda} \in \Lambda(G, \hat{\mathbb{Z}}_p^{ur})$.

THEOREM 3.18. *The map $\mathbb{L}$ gives an isomorphism of $\Lambda(G)$-modules*

$$\mathcal{C}_R \cong IJ\lambda + IJ\tilde{\lambda},$$

where, we recall, I denotes the augmentation ideal $I(K_\infty/K)$ in $\Lambda(G)$ and J is the annihilator of $\mu_{p^\infty}(K_\infty)$ in $\Lambda(G)$.

Proof. We know that $\varprojlim_{k,n}(C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathcal{C}_R$ by Corollary 3.7. We therefore look at $C'_{K_{k,n}}$ for $k, n \geq 1$ and note that, due to Assumption 3.16, it is generated by elements

$$(N_{K_{k,n}K(\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{a}))^{\sigma-1}, \tag{15}$$

where σ ranges over $\mathrm{Gal}(K_{k,n}/K)$, $0 \leq r' \leq r$, $\mathfrak{a}$ over integral ideals such that $(\mathfrak{a}, 6\mathfrak{l}^{r'}\bar{\mathfrak{p}}\mathfrak{p}) = 1$, and τ over primitive $\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n$-division points. If r' is greater than or equal to 1 (in which case $\mathfrak{a}$ is prime to $\mathfrak{l}$), then by [dS87, II, Proposition 2.5] we have

$$N_{K_{k,n}K(\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n)/K_{k,n}}\Theta(\tau;\mathfrak{a}) = N_{K(\mathfrak{l}^{r}\bar{\mathfrak{p}}^k\mathfrak{p}^n)/(K(\mathfrak{l}^{r'}\bar{\mathfrak{p}}^k\mathfrak{p}^n)\cap K_{k,n})}\Theta\left(\frac{\tau}{l^{r-r'}};\mathfrak{a}\right).$$

This shows that in (15) we may restrict to $r' = 0$ and $r' = r$ and still obtain a set of $\mathbb{Z}[\mathrm{Gal}(K_{k,n}/K)]$-generators of $C'_{K_{k,n}}$. We also may restrict to primitive division points of the form

$$\frac{\Omega}{\bar{\pi}^k\pi^n} \quad \text{and} \quad \frac{\Omega}{l^r\bar{\pi}^k\pi^n}$$

since the values of $\Theta(-;\mathfrak{a})$ at other primitive division points are Galois conjugates (see Remark 2.6 for the case $r' = r$). The case $r' = 0$ follows from [dS87, II, Proposition 2.4(ii)], whose proof uses, without mentioning it, [dS87, II, Lemma 1.4, p. 41]; see also [Ru99, Theorem 7.4]. So we have shown that

$$\begin{aligned} C'_{K_{k,n}} &= I(K_{k,n}/K)(N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}) + I(K_{k,n}/K)\Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}, \\ &= I(K_{k,n}/K)((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}) + \Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}) \end{aligned} \tag{16}$$

where, for two subgroups A, B of a group C, we write $A+B$ for the subgroup of C generated by A and B, even though we are dealing with subgroups of the multiplicative group $\mathcal{O}^\times_{K_{k,n}}$ above.

It is not difficult to prove that the norm maps

$$\begin{aligned} N_{K_{k',n'}/K_{k,n}} : ((N_{F_{k',n'}/K_{k',n'}}&\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}) \\ &\to ((N_{F_{k,n}/K_{k,n}}\Theta_{\mathfrak{f}\bar{\mathfrak{p}}^k\mathfrak{p}^n}) + \Theta_{\bar{\mathfrak{p}}^k\mathfrak{p}^n}) \end{aligned} \tag{17}$$

are surjective (compare [dS87, II, 2.3 and proof of Proposition 2.4(iii)]). Similarly to Lemma 3.8, one can show that this implies

$$I \varprojlim_{k',n'} ([(N_{F_{k',n'}/K_{k',n'}} \Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}] \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cong \varprojlim_{k,n} (C'_{K_{k,n}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

by compactness. Another compactness argument shows that

$$\varprojlim_{k',n'} ([(N_{F_{k',n'}/K_{k',n'}} \Theta_{\mathfrak{f}\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}) + \Theta_{\bar{\mathfrak{p}}^{k'}\mathfrak{p}^{n'}}] \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

is generated over $\Lambda(G)$ by $u(\mathfrak{a})$ and $\tilde{u}(\mathfrak{b})$, where $\mathfrak{a}, \mathfrak{b}$ range through the integral ideals of K such that $(\mathfrak{a}, \mathfrak{l}p) = 1$ and $(\mathfrak{b}, p) = 1$. We have

$$\mathbb{L}(u(\mathfrak{a})) = 12 x_{\mathfrak{a}} \lambda,$$

and likewise

$$\mathbb{L}(\tilde{u}(\mathfrak{b})) = 12 x_{\mathfrak{b}} \tilde{\lambda},$$

where, in the last line, $x_{\mathfrak{b}} = \sigma_{\mathfrak{b}} - N\mathfrak{b}$ with $\sigma_{\mathfrak{b}} = (\mathfrak{b}, K_\infty/K)$ as usual if $(\mathfrak{b}, 6p\mathfrak{l}) = 1$. In case $\mathfrak{l} \mid \mathfrak{b}$ we can consider $(\mathfrak{b}, L_\infty/K)$ and then define $\sigma_{\mathfrak{b}}$ to be a lift to $G(K_\infty/K)$. Note that $\mu_{p^\infty}(\bar{K}) \subset L_\infty$ (because for any primitive p^nth root of unity ζ_{p^n} the extension $K(\zeta_{p^n})/K$ is unramified outside the primes above p so the conductor of $K(\zeta_{p^n})/K$ divides a power of p, i.e., $K(\zeta_{p^n})$ is contained in a field $L_{m,m}$ for some $m \geq 1$). It follows that even if $\mathfrak{l} \mid \mathfrak{b}$ the element $x_{\mathfrak{b}} = \sigma_{\mathfrak{b}} - N\mathfrak{b}$ belongs to J. In combination with Lemma 3.15, this concludes the proof. ∎

3.5. Relations in $K_0(S\text{-tor})$. Let the setting be as in the previous subsection. In particular, we keep Assumption 3.16 that the conductor of ψ is a prime power $\mathfrak{f} = \mathfrak{l}^r$ for some prime $\mathfrak{l}$ and $r \geq 1$. We know from Theorem 3.10 that the quotient $\mathcal{C}_R/\mathcal{C}_Y$ is S-torsion. The aim of this subsection is to determine its class in $K_0(S\text{-tor})$, the K_0-group of the category S-tor of finitely generated $\Lambda(G)$-modules which are S-torsion. We will prove the following theorem.

THEOREM 3.19. *In $K_0(S\text{-tor})$ we have*

$$[\mathcal{C}_R/\mathcal{C}_Y] = [\Lambda(G/D_{\mathfrak{l}})],$$

where we write $D_{\mathfrak{l}}$ for the decomposition group of $\mathfrak{l}$ in $G = G(K_\infty/K)$.

Before giving the proof, we introduce some notation. Recall that we write $L_\infty = \bigcup_{k,n} L_{k,n}$, $L_{k,n} = K(\bar{\mathfrak{p}}^k \mathfrak{p}^n)$. The extension K_∞/L_∞ is a Galois extension of degree $\omega_K = \#\mu(K)$, the number of roots of unity of K (compare [S14, (A.6.3), (A.6.4) and Lemma A.6.4]). Note that ω_K is a unit in $\mathbb{Z}_p$ since $p \neq 2, 3$ and $2, 3$ are the only prime numbers that can possibly divide ω_K. We define the norm element

$$\mathcal{N} := \mathcal{N}_{K_\infty/L_\infty} := \sum_{g \in G(K_\infty/L_\infty)} g \in \Lambda(G).$$

Let us write $\Lambda = \Lambda(G)$ and $\tilde{\Lambda} = \Lambda(G, \widehat{\mathbb{Z}}_p^{ur})$ and recall $\sigma_{\mathfrak{l}}$ from Definition 3.9.

Proof of Theorem 3.19. We will prove the theorem in two steps. First, we will show that

$$[\mathcal{C}_R/\mathcal{C}_Y] = [\Lambda\mathcal{N}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N})].$$

Then, we will prove that $\Lambda\mathcal{N}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N})$ is isomorphic to $\Lambda(G/D_{\mathfrak{l}})$.

Step 1. From Corollary 3.14 and Theorem 3.18, we know that

$$[\mathcal{C}_R/\mathcal{C}_Y] = [(IJ\lambda + IJ\tilde{\lambda})/IJ\lambda] = [IJ\tilde{\lambda}/(IJ\tilde{\lambda}\cap IJ\lambda)], \tag{18}$$

where we consider $IJ\lambda$ and $IJ\tilde{\lambda}$ as Λ-submodules of $\tilde{\Lambda}$. Next, we have

$$\mathcal{N}\lambda = (1-\sigma_{\mathfrak{l}}^{-1})\tilde{\lambda} \quad \text{and} \quad \mathcal{N}\tilde{\lambda} = \omega_K\tilde{\lambda}, \tag{19}$$

which follows from the corresponding equations for the elliptic units $e_{k,n}(\mathfrak{a})$ and $\tilde{e}_{k,n}(\mathfrak{a})$, for all $k, n \geq 1$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\bar{\mathfrak{p}}^k\mathfrak{p}^n)^\times$ is injective (compare [dS87, II, Proposition 2.5] for the first equation). One easily derives

$$\mathcal{N}\cdot(IJ\tilde{\lambda}\cap IJ\lambda) = (1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}. \tag{20}$$

Since multiplication with $\mathcal{N}$ induces an isomorphism of $IJ\tilde{\lambda}$ and therefore also of $IJ\tilde{\lambda}\cap IJ\lambda$, equation (20) shows that the class on the right of (18) is

$$[IJ\tilde{\lambda}/(IJ\tilde{\lambda}\cap IJ\lambda)] = [IJ\tilde{\lambda}/((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda})]. \tag{21}$$

It follows from [S14, Lemmata A.9.2 and A.9.5] that all of the modules in the two exact sequences

$$IJ\tilde{\lambda}/((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}) \hookrightarrow \Lambda\tilde{\lambda}/((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}) \twoheadrightarrow \Lambda\tilde{\lambda}/IJ\tilde{\lambda} \tag{22}$$

and

$$((1-\sigma_{\mathfrak{l}}^{-1})\Lambda\tilde{\lambda})/((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}) \hookrightarrow \Lambda\tilde{\lambda}/((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda}) \twoheadrightarrow \Lambda\tilde{\lambda}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\tilde{\lambda}) \tag{23}$$

are S-torsion, where by $\hookrightarrow$ and $\twoheadrightarrow$ we denote injective and surjective maps, respectively. Since $1-\sigma_{\mathfrak{l}}^{-1}$ is not a zero-divisor in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$, i.e., for any $\Lambda(G)$-submodule M of $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$ multiplication with $1-\sigma_{\mathfrak{l}}^{-1}$ defines an isomorphism $M \cong (1-\sigma_{\mathfrak{l}}^{-1})M$, the two exact sequences show that

$$[IJ\tilde{\lambda}/((1-\sigma_{\mathfrak{l}}^{-1})IJ\tilde{\lambda})] = [\Lambda\tilde{\lambda}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\tilde{\lambda})]. \tag{24}$$

Moreover, the class on the right of (24) is equal to

$$[\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\tilde{\lambda}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})^2\tilde{\lambda})] = [\Lambda\mathcal{N}\lambda/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}\lambda)]. \tag{25}$$

Equations (18), (21), (24) and (25) show that

$$[\mathcal{C}_R/\mathcal{C}_Y] = [\Lambda\mathcal{N}\lambda/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}\lambda)]$$

and since λ is not a zero-divisor in $\Lambda(G, \hat{\mathbb{Z}}_p^{ur})$, by [S14, Proposition 2.4.28], we see that the class on the right is equal to

$$[\Lambda\mathcal{N}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N})],$$

as desired.

STEP 2. We remark that $\Lambda\mathcal{N}$ and $\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}$ are now already submodules of Λ and not only of $\tilde{\Lambda}$. Let us write H' for the closed subgroup $G(K_\infty/L_\infty)$ of G and $\mathrm{pr} : \Lambda(G) \twoheadrightarrow \Lambda(G/H')$ for the canonical projection. Then we have an exact sequence

$$0 \to \ker(\mathrm{pr}_{|\Lambda(G)\mathcal{N}}) \to \Lambda(G)\mathcal{N} \to \Lambda(G/H') \to 0, \tag{26}$$

which is exact because under pr the element $\mathcal{N}$ maps to $\omega_K \in \mathbb{Z}_p^\times$. Now, we claim that $\ker(\mathrm{pr}_{|\Lambda(G)\mathcal{N}}) = 0$. In fact, let $x\mathcal{N}$, $x \in \Lambda(G)$, belong to $\ker(\mathrm{pr})$. Then

$$0 = \mathrm{pr}(x\mathcal{N}) = \mathrm{pr}(x)\omega_K,$$

from which we conclude that $x \in \ker(\mathrm{pr})$, because $\omega_K \in \mathbb{Z}_p^\times$. But $\ker(\mathrm{pr})$ is generated over $\Lambda(G)$ by elements of the form $1-g$, $g \in H'$, and for such elements, $(1-g)\mathcal{N} = 0$ and therefore $x\mathcal{N} = 0$. It follows from (26) that

$$\Lambda(G)\mathcal{N} \cong \Lambda(G/H').$$

We get

$$\Lambda(G)\mathcal{N}/(\Lambda(G)(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}) \cong \Lambda(G/H')/(\Lambda(G/H')(1-\bar{\sigma}_{\mathfrak{l}}^{-1})), \tag{27}$$

where we write $\bar{\sigma}_{\mathfrak{l}}$ for the restriction of $\sigma_{\mathfrak{l}}$ to L_∞. Note that, by definition, $\bar{\sigma}_{\mathfrak{l}} = (\mathfrak{l}, L_\infty/K)$ is the arithmetic Frobenius element at $\mathfrak{l}$ for the extension L_∞/K, in which $\mathfrak{l}$ is unramified. In particular, $\bar{\sigma}_{\mathfrak{l}}$ topologically generates the decomposition group $D'_{\mathfrak{l}}$ of $\mathfrak{l}$ in $G/H' \cong G(L_\infty/K)$. It follows that

$$\Lambda(G/H')/(\Lambda(G/H')(1-\bar{\sigma}_{\mathfrak{l}}^{-1})) \cong \Lambda(G(L_\infty/K)/D'_{\mathfrak{l}}). \tag{28}$$

Next, we claim that no place $\mathfrak{L}$ of L_∞ above $\mathfrak{l}$ splits in K_∞/L_∞, i.e., for $\mathfrak{L}$ there is a unique extension $\mathfrak{L}'$ to K_∞. We also write $v_{\mathfrak{q}}$ for a non-archimedean place $\mathfrak{q}$ in order to stress that we think of it as a valuation. This means that we have to show that if $\mathfrak{L}'$ is a place of K_∞ above $\mathfrak{L}$, then

$$v_{\mathfrak{L}'} \circ g = v_{\mathfrak{L}'} \tag{29}$$

for all $g \in G(K_\infty/L_\infty)$. But for any $g \in G(K_\infty/L_\infty)$ and any $k, n \geq 1$, Lemma 3.21 below applied to $\mathfrak{m} = \bar{\mathfrak{p}}^k\mathfrak{p}^n$ shows that $(v_{\mathfrak{L}'})_{|K_{k,n}}$, the restriction of $v_{\mathfrak{L}'}$ to $K_{k,n}$, is the unique place of $K_{k,n}$ above $(v_{\mathfrak{L}'})_{|L_{k,n}}$, which implies that

$$(v_{\mathfrak{L}'})_{|K_{k,n}} \circ g_{|K_{k,n}} = (v_{\mathfrak{L}'})_{|K_{k,n}}.$$

This equation holds for all $k, n \geq 1$ and therefore implies (29).

Having shown that for any place $\mathfrak{L}$ of L_∞ above $\mathfrak{l}$ there is a unique extension $\mathfrak{L}'$ to K_∞, we can conclude that the canonical restriction map induces an isomorphism

$$G/D_{\mathfrak{l}} \xrightarrow{\sim} G(L_\infty/K)/D'_{\mathfrak{l}}, \tag{30}$$

where we write $D_{\mathfrak{l}}$ for the decomposition group of $\mathfrak{l}$ in $G = G(K_\infty/K)$.

All in all, equations (27), (28) and (30) show that we have an isomorphism of Λ-modules

$$\Lambda\mathcal{N}/(\Lambda(1-\sigma_{\mathfrak{l}}^{-1})\mathcal{N}) \cong \Lambda(G/D_{\mathfrak{l}}). \ \blacksquare \tag{31}$$

Before proving the lemma we have referred to above, let us record one immediate consequence of (31) and of the fact that $1-\sigma_{\mathfrak{l}}^{-1}$ belongs to S (see [S14, Lemma A.9.5]).

COROLLARY 3.20. *The $\Lambda(G)$-module $\Lambda(G/D_{\mathfrak{l}})$ is S-torsion.*

LEMMA 3.21. *Let $\mathfrak{m}$ be an integral ideal of K and let $\mathfrak{l}$ be a prime of K such that $(\mathfrak{l},\mathfrak{m}) = 1$. For any integer $r \geq 1$ and any prime $\mathfrak{L}$ of $K(\mathfrak{m})$ above $\mathfrak{l}$, $\mathfrak{L}$ cannot split in the extension $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$. In particular, $\mathfrak{L}$ cannot split in any subextension $L/K(\mathfrak{m})$ of $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$.*

Proof. Let $\mathfrak{L}$ be a prime of $K(\mathfrak{m})$ above $\mathfrak{l}$. Assume that $\mathfrak{L}$ splits in the extension $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$. Then the fixed field Z of the decomposition group of $\mathfrak{L}$ in $G(K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m}))$ is strictly greater than $K(\mathfrak{m})$, and $\mathfrak{L}$ is unramified in the extension $Z/K(\mathfrak{m})$ (see [N07, I, §9, Proposition 9.3(iii)] for the last fact). Since $\mathfrak{l}$ is unramified in $K(\mathfrak{m})/K$, this implies that there is one prime of Z above $\mathfrak{l}$ which has ramification index 1 in Z/K. But then, since Z/K is Galois, all primes of Z above $\mathfrak{l}$ have ramification index 1, which means that $\mathfrak{l}$ is unramified in the extension Z/K. In particular, $\mathfrak{l}$ does not divide the conductor of the extension Z/K. But the conductor of Z/K divides $\mathfrak{l}^r\mathfrak{m}$ and therefore must divide $\mathfrak{m}$, which contradicts the fact that Z is strictly greater than $K(\mathfrak{m})$. Therefore, $\mathfrak{L}$ cannot split in the extension $K(\mathfrak{l}^r\mathfrak{m})/K(\mathfrak{m})$. ∎

Acknowledgements. During this research the author was supported through Prof. O. Venjakob's *ERC Starting Grant IWASAWA* and the *Studienstiftung des deutschen Volkes.*

References

[B04] W. Bley, *Wild Euler systems of elliptic units and the Equivariant Tamagawa Number Conjecture*, J. Reine Angew. Math. 577 (2004), 117–146.

[BV10] T. Bouganis and O. Venjakob, *On the non-commutative main conjecture for elliptic curves with complex multiplication*, Asian J. Math. 14 (2010), 385–416.

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, *On the* GL_2 *main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. 101 (2005), 163–208.

[CW77] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.

[CW78] J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Austral. Math. Soc. Ser. A 26 (1978), 1–25.

[K12] Y. Kang, *On two-variable primitive p-adic L-functions*, Asian J. Math. 16 (2012), 171–188.

[N07] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 2007.

[R73] G. Robert, *Unités elliptiques*, Bull. Soc. Math. France 101 (1973), no. 36.

[R90] G. Robert, *Concernant la relation de distribution satisfaite par la fonction* φ *associée à un réseau complexe*, Invent. Math. 100 (1990), 231–257.

[R92] G. Robert, *La racine 12-ième canonique de* $\Delta(L)^{[\underline{L}:L]}/\Delta(\underline{L})$, in: Séminaire de Théorie des Nombres, Paris, 1989-90, Progr. Math. 102, Birkhäuser, Boston, 1992, 209–232.

[Ru87] K. Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), 527–560.

[Ru91] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.

[Ru99] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in: Arithmetic Theory of Elliptic Curves, Lecture Notes in Math. 1716, Springer, Berlin, 1999, 167–234.

[S14] U. Schmitt, *Towards a twist conjecture in non-commutative Iwasawa theory*, Doktorarbeit, Univ. Heidelberg, 2014, http://www.ub.uni-heidelberg.de/archiv/17176.

[dS87] E. de Shalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication. p-Adic L Functions*, Perspect. Math. 3, Academic Press, Boston, 1987.

[Sh71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, Princeton, NJ, 1971.

[Si99] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1999.

[V12] S. Viguié, *Global units modulo elliptic units and ideal class groups*, Int. J. Number Theory 8 (2012), 569–588.

[Y82] R. I. Yager, *On two variable p-adic L-functions*, Ann. of Math. 115 (1982), 411–449.

Ulrich Schmitt
München, Germany
E-mail: ulrich.schmitt@cantab.net

Received on 15.12.2014
and in revised form on 25.5.2015 (8030)