CYCLOTOMIC UNITS IN $\mathbf{Z}_p$-EXTENSIONS

Radan Kučera, Jan Nekovář

1. Introduction

Let p be a prime number, k an abelian field (i.e. a finite abelian extension of $\mathbf{Q}$), and K the cyclotomic $\mathbf{Z}_p$-extension of k. For each $n \geq 0$, let K_n denote the unique extension of k in K of degree p^n over k. Let E_{K_n} be the group of units of K_n, C_{K_n} the Sinnott group of circular units of K_n, and $h^+_{K_n}$ the class number of the maximal real subfield of K_n. Sinnott (see [**S**2, p.182]) proved the following

Theorem (Sinnott)**.** *There is a rational number c, depending only on K, such that, for all sufficiently large n, we have*

$$[E_{K_n} : C_{K_n}] = \begin{cases} c \cdot h^+_{K_n} & \text{if } k \text{ is imaginary,} \\ c \cdot 2^{[K_n:\mathbf{Q}]} \cdot h^+_{K_n} & \text{if } k \text{ is real.} \end{cases}$$

Let k be real, and for each $n \geq 0$ let $C_{1,K_n} = \{\varepsilon \in E_{K_n};\, \varepsilon^2 \in C_{K_n}\}$. Then there is a rational number c_1, depending only on K, such that

$$[E_{K_n} : C_{1,K_n}] = c_1 \cdot h^+_{K_n}$$

for all sufficiently large n.

Let $\overline{C}_{K_n} \supseteq C_{K_n}$ be the Washington group of cyclotomic units of K_n (the definitions of both groups are given below). The motivation of this paper (based on a question of M. Kolster) was to compare projective limits (with respect to norms) $C = \varprojlim(C_{K_n} \otimes \mathbf{Z}_p)$ and $\overline{C} = \varprojlim(\overline{C}_{K_n} \otimes \mathbf{Z}_p)$. Unfortunately, we were not able to decide whether $C = \overline{C}$ in general, but we shall prove the following analogy of Sinnott's theorem, which implies that C is of finite index in $\overline{C}$:

Theorem. *There are a rational number c' and an integer d, depending only on K, such that, for all sufficiently large n, we have*

$$[E_{K_n} : \overline{C}_{K_n}] = c' \cdot p^{t_n} \cdot h^+_{K_n},$$

where $t_n \geq 0$ are integers smaller than d.

It seems to be reasonable to expect that one can always take $d = 1$ in the previous theorem, but we were unable to prove it.

During the work on this paper, the first named author was supported by a postdoctoral grant from Université Laval in Québec and Centre interuniversitaire en calcul mathématique algébrique; the second named author was supported by a fellowship from the Miller Institute for Basic Research at the University of California at Berkeley. The authors wish to express their gratitude to these institutions for their hospitality.

2. Notations and preliminaries

Let p be a prime number, fixed through the whole paper. Let $q = p$, if p is odd, and let $q = 4$ if $p = 2$. For any positive integer m let $\zeta_m = e^{2\pi i/m}$. For any integer $n \geq 0$ we define B_n to be the real subfield of $\mathbf{Q}(\zeta_{qp^n})$ of absolute degree p^n. Let $B = \bigcup_{n=0}^{\infty} B_n$.

We choose an abelian field k, which may be real or imaginary, and for convinience we suppose k to be contained in the complex field $\mathbf{C}$. Let X be the group of characters of $\mathrm{Gal}(k/\mathbf{Q})$, considered as a group of Dirichlet characters modulo the conductor of k. For any $\chi \in X$ there is Iwasawa's decomposition $\chi = \theta\psi$, where θ is a character of the first kind (i.e. the conductor of θ is not divisible by qp) and ψ is a character of the second kind (i.e. an even character whose conductor and order are powers of p). Let

$$X' = \{\theta;\ \chi = \theta\psi \in X,\ \theta \text{ of } 1^{\text{st}} \text{ kind},\ \psi \text{ of } 2^{\text{nd}} \text{ kind}\}$$

and let k' be the field corresponding to X'. It is easy to see that $kB_n = k'B_n$ for all sufficiently large n, so it is enough to prove Theorem for k'. Therefore in the whole paper we shall suppose that the conductor of k is either f or qf, where $p \not| f$. For any integer $n \geq 0$, let $K_n = kB_n$ and $L_n = B_n(\zeta_{qf}) = \mathbf{Q}(\zeta_{qp^n f})$. Similarly, let $K = kB$ and $L = B(\zeta_{qf})$. Let $H = \mathrm{Gal}(L/K)$. It is clear that, for any $n \geq 0$, the Galois group $\mathrm{Gal}(L_n/K_n)$ is isomorphic to H via restriction. We shall identify these groups.

For any abelian field M, let E_M and W_M be the group of units of M and the group of roots of unity in M, respectively. The Sinnott group of circular units of M is defined as the intersection $C_M = D_M \cap E_M$, where D_M is the subgroup of the multiplicative group $M^\times$ generated by -1 and

$$\{\mathrm{N}_{\mathbf{Q}(\zeta_m)/M\cap\mathbf{Q}(\zeta_m)}(1-\zeta_m^a);\ a, m \in \mathbf{Z},\ 1 < m \not| a\}$$

(see [**S**2, p. 201]). Let $\overline{C}_M$ be the Washington group of cyclotomic units of M, namely $\overline{C}_M = C_{\mathbf{Q}(\zeta_m)} \cap E_M$, where m is the conductor of M (see [**W**2, p. 143]).

Let $\ell_M : M^\times \to \mathbf{R}[\mathrm{Gal}(M/\mathbf{Q})]$ be the logarithmic mapping defined for any $\alpha \in M^\times$ by

$$\ell_M(\alpha) = -\tfrac{1}{2} \sum_{\sigma \in \mathrm{Gal}(M/\mathbf{Q})} \log|\alpha^\sigma|\sigma^{-1}.$$

Let $T_M = \ell_M(D_M)$ and $T_{0,M} = T_M \cap (1 - e_{1,M})T_M$, where $e_{1,M} = \frac{1}{[M:\mathbf{Q}]}\sum_{\sigma\in\mathrm{Gal}(M/\mathbf{Q})} \sigma$ is the idempotent corresponding to the trivial character on $\mathrm{Gal}(M/\mathbf{Q})$.

If M_1/M_2 is an extension of abelian fields, then the restriction map

$$\mathrm{res}_{M_1/M_2} : \mathbf{R}[\mathrm{Gal}(M_1/\mathbf{Q})] \to \mathbf{R}[\mathrm{Gal}(M_2/\mathbf{Q})]$$

is the ring homomorphism induced by the restriction of automorphisms and the corestriction map

$$\mathrm{cor}_{M_1/M_2} : \mathbf{R}[\mathrm{Gal}(M_2/\mathbf{Q})] \to \mathbf{R}[\mathrm{Gal}(M_1/\mathbf{Q})]$$

is the homomorphism of additive groups determined by

$$\mathrm{cor}_{M_1/M_2}\,\sigma = \sum_{\tau|_{M_2}=\sigma} \tau,$$

for any $\sigma \in \mathrm{Gal}(M_2/\mathbf{Q})$. The sum is taken over all $\tau \in \mathrm{Gal}(M_1/\mathbf{Q})$ whose restriction to M_2 is σ.

3. The relative index of Washington's and Sinnott's units

Our aim is to compute the index $\left[\overline{C}_{K_n} : C_{K_n}\right]$ up to a bounded factor.

For any integral sequences a_n, b_n, we shall write $a_n \approx b_n$ if there exist integers x, $y \geq 1$ satisfying $a_n \mid xb_n$ and $b_n \mid ya_n$ for all n.

Lemma 1.

$$\left[\overline{C}_{K_n} : C_{K_n}\right] \approx [T^H_{0,L_n} : \mathrm{cor}_{L_n/K_n} T_{0,K_n}].$$

Proof. Sinnott proved that

$$0 \longrightarrow W_M \longrightarrow C_M \xrightarrow{\ell_M} T_{0,M} \longrightarrow 0$$

is an exact sequence for any abelian field M (see Lemma 4.2 of [**S**2]). Taking H-invariants for $M = L_n$ gives the exact sequence

$$0 \longrightarrow W_{L_n}^H \longrightarrow C_{L_n}^H \xrightarrow{\ell_{L_n}} T_{0,L_n}^H \longrightarrow H^1(H, W_{L_n}).$$

Of course, $H = \mathrm{Gal}(L_n/K_n)$, so $W_{L_n}^H = W_{K_n}$ and directly from the definition we have $C_{L_n}^H = \overline{C}_{K_n}$. It is easy to see that $\ell_{L_n}(\alpha) = \mathrm{cor}_{L_n/K_n} \ell_{K_n}(\alpha)$ for any $\alpha \in K_n^\times$, so the following diagram with exact rows commutes

$$\begin{tikzcd} 0 \arrow[r] & C_{K_n}/W_{K_n} \arrow[r, "\ell_{K_n}"] \arrow[d, "\subseteq"'] & T_{0,K_n} \arrow[r] \arrow[d, "\mathrm{cor}_{L_n/K_n}"] & 0 \\ 0 \arrow[r] & \overline{C}_{K_n}/W_{K_n} \arrow[r, "\ell_{L_n}"] & T_{0,L_n}^H \arrow[r] & H^1(H, W_{L_n}) \end{tikzcd}$$

and the lemma follows from the following lemma, because $W_{K_n} \subseteq C_{K_n} \subseteq \overline{C}_{K_n} \subseteq E_{K_n}$, so $\overline{C}_{K_n}/C_{K_n}$ is finite (by [**S**2]) and isomorphic to $\big(\overline{C}_{K_n}/W_{K_n}\big)/\big(C_{K_n}/W_{K_n}\big)$.

Lemma 2. *$\#H^1(H, W_{L_n})$ is bounded by a constant.*

Proof. Let $\mu_m = \langle \zeta_m \rangle$ be the group of m-th roots of unity. We have $W_{L_n} = \mu_f \times \mu_{qp^n}$, so

$$H^1(H, W_{L_n}) = H^1(H, \mu_f) \times H^1(H, \mu_{qp^n}),$$

so it is enough to show that $H^1(H, \mu_{qp^n})$ is bounded. If the action of H on μ_{qp^n} is trivial, then

$$\#H^1(H, \mu_{qp^n}) = \#\,\mathrm{Hom}(H, \mu_{qp^n}) \le \#H_{p^\infty},$$

where H_{p^∞} is the p-Sylow subgroup of H and we are done. Let us suppose that the action of H on μ_{qp^n} is not trivial. Then H can be written as a product of cyclic groups generated, say, by $\sigma_1, \dots, \sigma_s$, and σ_1 has a non-trivial action on μ_{qp^n}.

We need to distinguish two cases. At first, let us suppose $p \ne 2$. Since $H \subseteq \mathrm{Gal}(L_n/B_n)$, the action of σ_i^{p-1} on $\mu_{p^{1+n}}$ is trivial for each $i \in \{1, \dots, s\}$. For any $i \in \{1, \dots, s\}$ let us choose $c_i \in \mathbf{Z}$ satisfying $\zeta_{p^{1+n}}^{\sigma_i} = \zeta_{p^{1+n}}^{c_i}$. We have $c_i^{p-1} \equiv 1 \pmod{p^{1+n}}$ for each $i \in \{1, \dots, s\}$ and $c_1 \not\equiv 1 \pmod{p^{1+n}}$, therefore $c_1 \not\equiv 1 \pmod{p}$. For any $\rho \in \mu_{p^{1+n}}$ there is unique $\xi \in \mu_{p^{1+n}}$ satisfying $\xi^{c_1 - 1} = \rho$; let us define the coboundary $f_\rho : H \to \mu_{p^{1+n}}$ by $f_\rho(\tau) = \xi^{\tau - 1}$ for each $\tau \in H$. It is clear that $f_\rho(\sigma_1) = \rho$. Let $f : H \to \mu_{p^{1+n}}$ be a crossed homomorphism. For any $i \in \{2, \dots, s\}$ we have

$$\big(f(\sigma_1)\big)^{\sigma_i} f(\sigma_i) = f(\sigma_1\sigma_i) = \big(f(\sigma_i)\big)^{\sigma_1} f(\sigma_1),$$

so

$$\big(f(\sigma_i)\big)^{c_1 - 1} = \big(f(\sigma_1)\big)^{c_i - 1}.$$

Therefore f is uniquely determined by the value $\rho = f(\sigma_1)$, hence $f = f_\rho$. We have proved $H^1(H, \mu_{qp^n}) = 0$ in this case.

Now, let us suppose $p = 2$. Since $H \subseteq \mathrm{Gal}(L_n/B_n)$, any σ_i acts on $\mu_{2^{2+n}}$ like the identity or the complex conjugation. Let $c_i \in \{1, -1\}$ satisfy $\zeta_{2^{2+n}}^{\sigma_i} = \zeta_{2^{2+n}}^{c_i}$ for each $i \in \{1, \dots, s\}$. Then $c_1 = -1$. For any $\rho \in \mu_{2^{2+n}}$ there is the coboundary $f_\rho : H \to \mu_{p^{2+n}}$ defined by $f_\rho(\tau) = \rho^{\tau - 1}$ for each $\tau \in H$. Then $f_\rho(\sigma_1) = \rho^{-2}$, so we have 2^{1+n} different coboundaries. Let $f : H \to \mu_{p^{2+n}}$ be a crossed homomorphism. For any $i \in \{2, \dots, s\}$ we have

$$\big(f(\sigma_i)\big)^{-2} = \big(f(\sigma_1)\big)^{c_i - 1},$$

hence $f(\sigma_i) = \pm 1$ if $c_i = 1$ and $f(\sigma_i) = \pm f(\sigma_1)$ if $c_i = -1$. Therefore there exist at most 2^{s-1} crossed homomorphisms with the same value $f(\sigma_1)$ and

$$\#H^1(H, \mu_{qp^n}) \le \frac{2^{2+n}\, 2^{s-1}}{2^{1+n}} = 2^s.$$

The lemma is proved.

Remark. In fact, we have reproved a version of Sah's lemma.

Lemma 3.

$$[T_{0,L_n}^H : \operatorname{cor}_{L_n/K_n} T_{0,K_n}] \approx [((1-e_{1,L_n})T_{L_n})^H : \operatorname{cor}_{L_n/K_n}(1-e_{1,K_n})T_{K_n}].$$

Proof. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & T_{0,K_n} & \xrightarrow{\subseteq} & (1-e_{1,K_n})T_{K_n} & \longrightarrow & ((1-e_{1,K_n})T_{K_n})/T_{0,K_n} & \longrightarrow & 0 \\
 & & {\scriptstyle \operatorname{cor}_{L_n/K_n}}\downarrow & & \downarrow{\scriptstyle \operatorname{cor}_{L_n/K_n}} & & \downarrow{\scriptstyle f_n} & & \\
0 & \longrightarrow & T_{0,L_n}^H & \xrightarrow{\subseteq} & ((1-e_{1,L_n})T_{L_n})^H & \longrightarrow & X_n & \longrightarrow & 0
\end{array}$$

where

$$X_n = \big(((1-e_{1,L_n})T_{L_n})^H + T_{0,L_n}\big)/T_{0,L_n} \subseteq \big(((1-e_{1,L_n})T_{L_n})/T_{0,L_n}\big)^H$$

and f_n is determined by the corestriction. Since $\operatorname{cor}_{L_n/K_n}$ is injective, the Snake lemma gives the following exact sequence:

$$\begin{aligned}
0 \longrightarrow \operatorname{Ker} f_n \longrightarrow T_{0,L_n}^H/\operatorname{cor}_{L_n/K_n} T_{0,K_n} \longrightarrow & \\
\longrightarrow ((1-e_{1,L_n})T_{L_n})^H/\operatorname{cor}_{L_n/K_n}(1-e_{1,K_n})T_{K_n} \longrightarrow \operatorname{Coker} f_n \longrightarrow 0.&
\end{aligned}$$

Proposition 4.1 of [**S**2] gives that

$$\begin{aligned}
\#((1-e_{1,K_n})T_{K_n})/T_{0,K_n} &\approx p^n, \\
\#((1-e_{1,L_n})T_{L_n})/T_{0,L_n} &\approx p^n.
\end{aligned}$$

Because $T_{0,L_n}^H/\operatorname{cor}_{L_n/K_n} T_{0,K_n}$ is finite by Lemma 1, all groups in the previous exact sequence are finite and the lemma will be proved if we show

$$\#\operatorname{Ker} f_n \approx \#\operatorname{Coker} f_n.$$

Of course,

$$\frac{\#\operatorname{Ker} f_n}{\#\operatorname{Coker} f_n} = \frac{\#((1-e_{1,K_n})T_{K_n})/T_{0,K_n}}{\#X_n}.$$

Since $X_n \subseteq ((1-e_{1,L_n})T_{L_n})/T_{0,L_n}$, it is enough to show that there is a positive integer c satisfying $p^n \mid c(\#X_n)$. Let

$$\alpha_n = \mathrm{N}_{\mathbf{Q}(\zeta_{qp^n})/B_n}(1-\zeta_{qp^n}).$$

It is easy to see that $\alpha_n \in D_{L_n}^H$, so $\ell_{L_n}(\alpha_n) \in T_{L_n}^H$ and $(1-e_{1,L_n})\ell_{L_n}(\alpha_n) + T_{0,L_n} \in X_n$. We shall use the isomorphism

$$((1-e_{1,L_n})T_{L_n})/T_{0,L_n} \cong (e_{1,L_n}T_{L_n})/T_{L_n}^{\mathrm{Gal}(L_n/\mathbf{Q})}$$

(see the proof of Proposition 4.1 of [**S**2]). This isomorphism sends $\beta_n = (1-e_{1,L_n})\ell_{L_n}(\alpha_n) + T_{0,L_n}$ to $\gamma_n = e_{1,L_n}\ell_{L_n}(\alpha_n) + T_{L_n}^{\mathrm{Gal}(L_n/\mathbf{Q})}$. We have

$$e_{1,L_n}\ell_{L_n}(\alpha_n) = -\tfrac{1}{2}e_{1,L_n}\sum_{\sigma\in\mathrm{Gal}(L_n/\mathbf{Q})}\log|\alpha_n^\sigma| = -\tfrac{1}{2}e_{1,L_n}\log|\mathrm{N}_{L_n/\mathbf{Q}}(\alpha_n)|$$

and

$$\mathrm{N}_{L_n/\mathbf{Q}}(\alpha_n) = \mathrm{N}_{B_n/\mathbf{Q}}(\mathrm{N}_{L_n/B_n}(\alpha_n)) = \mathrm{N}_{\mathbf{Q}(\zeta_{qp^n})/\mathbf{Q}}(1-\zeta_{qp^n})^{[L_n:B_n]} = p^{\varphi(qf)},$$

so $\gamma_n = -\frac{\varphi(qf)}{2} e_{1,L_n} \log p + T_{L_n}^{\mathrm{Gal}(L_n/\mathbf{Q})}$. Sinnott proved (see [**S**2, the last paragraph of p. 204]) that

$$2T_{L_n}^{\mathrm{Gal}(L_n/\mathbf{Q})} \subseteq \ell_{L_n}(\mathbf{Q}^\times) = -\frac{[L_n:\mathbf{Q}]}{2} e_{1,L_n} \log |\mathbf{Q}^\times|.$$

Let b be the order of β_n in X_n. Then b is also the order of γ_n, so $\frac{1}{2}\varphi(qf)b$ is a multiple of $\frac{1}{4}[L_n : \mathbf{Q}] = \frac{1}{4}\varphi(qp^n f)$. We have proved that p^n divides $2b$, so $p^n \mid 2(\#X_n)$. The lemma is proved.

4. Sinnott's modules

For the following lemma we shall need Sinnott's module U. Let m be the product of all primes dividing f. Let M be either K_n or L_n, $n \geq 0$, and $G = \mathrm{Gal}(M/\mathbf{Q})$. We put $s(X) = \sum_{\tau \in X} \tau \in \mathbf{Z}[G]$ for any subgroup X of G and $e_M^+ = \frac{1+j}{2}$, where j is the restriction of the complex conjugation in G. For any prime $l \mid pm$ let $I_{l,M} \subseteq G$ be the inertia group of l and λ_l be a Frobenius automorphism for l in G; λ_l is well-defined modulo $I_{l,M}$. We define

$$e_{l,M} = \frac{1}{\# I_{l,M}} s(I_{l,M}) \qquad \text{and} \qquad (l, M)^* = \lambda_l^{-1} e_{l,M}.$$

For each positive divisor $r \mid pm$ let $I_{r,M}$ be the subgroup of G generated by all $I_{l,M}$ with $l \mid r$. Then U_M can be defined as the $\mathbf{Z}[G]$-module generated in $\mathbf{Q}[G]$ by the elements

$$s(I_{r,M}) \prod_{l \mid \frac{pm}{r}} (1 - (l, M)^*),$$

where r varies over the positive divisors of pm (see Proposition 2.3 of [**S**2]). Similarly, we define V_M as the $\mathbf{Z}[G]$-module generated in $\mathbf{Q}[G]$ by the elements

$$s(I_{r,M}) \prod_{l \mid \frac{m}{r}} (1 - (l, M)^*),$$

where r runs through the set of the positive divisors of m (the module V_M is denoted by U_m in [**S**2]).

Lemma 4. *For any $n \geq 0$*

$$[((1 - e_{1,L_n})T_{L_n})^H : \mathrm{cor}_{L_n/K_n}(1 - e_{1,K_n})T_{K_n}] = [(e_{L_n}^+ U_{L_n})^H : \mathrm{cor}_{L_n/K_n}\, e_{K_n}^+ U_{K_n}].$$

Proof. Corollary on page 207 of [**S**2] and the last but three line of the same page give

$$(1 - e_{1,M})T_M = \omega'_M U_M = \omega'_M e_M^+ U_{0,M}$$

for any abelian field M. Here

$$U_{0,M} = U_M \cap (1 - e_{1,M})U_M$$

and

$$\omega'_M = \sum_\chi L'(0, \overline{\chi}) e_{\chi,M},$$

where the sum is taken over all even non-trivial characters χ of $G = \mathrm{Gal}(M/\mathbf{Q})$, $e_{\chi,M} = \frac{1}{[M:\mathbf{Q}]} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}$ is the idempotent and $L(s, \chi)$ the L-series corresponding to χ. Since $L'(0, \overline{\chi}) \neq 0$ for all such characters, multiplying by ω'_M is a bijection on

$$(e_M^+ U_{0,M}) \otimes \mathbf{R} = e_M^+(1 - e_{1,M})\mathbf{R}[G].$$

Moreover

$$\mathrm{res}_{L_n/K_n}\, \omega'_{L_n} = \sum_\chi L'(0, \overline{\chi})\, \mathrm{res}_{L_n/K_n}\, e_{\chi,L_n} = \omega'_{K_n},$$

because $\mathrm{res}_{L_n/K_n} e_{\chi,L_n}$ is e_{χ,K_n} if χ is also a character of $\mathrm{Gal}(K_n/\mathbf{Q})$ and 0 otherwise. Hence

$$\omega'_{L_n} \mathrm{cor}_{L_n/K_n} \alpha = \mathrm{cor}_{L_n/K_n}(\alpha \, \mathrm{res}_{L_n/K_n} \omega'_{L_n}) = \mathrm{cor}_{L_n/K_n}(\omega'_{K_n}\alpha)$$

for any $\alpha \in \mathbf{Q}[\mathrm{Gal}(K_n/\mathbf{Q})]$ and the following diagram commutes

$$\begin{array}{ccc} e^+_{K_n} U_{0,K_n} & \xrightarrow{\omega'_{K_n}} & (1-e_{1,K_n})T_{K_n} \\ {\scriptstyle \mathrm{cor}_{L_n/K_n}} \downarrow & & \downarrow {\scriptstyle \mathrm{cor}_{L_n/K_n}} \\ e^+_{L_n} U_{0,L_n} & \xrightarrow{\omega'_{L_n}} & (1-e_{1,L_n})T_{L_n} \end{array}$$

The rows of this diagram are isomorphisms, so we have obtained that

$$[((1-e_{1,L_n})T_{L_n})^H : \mathrm{cor}_{L_n/K_n}(1-e_{1,K_n})T_{K_n}] = [(e^+_{L_n} U_{0,L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{0,K_n}].$$

We have a direct sum $U_M = U_{0,M} \oplus s(\mathrm{Gal}(M/\mathbf{Q}))\mathbf{Z}$ (see [**S**2, p. 193]) for any abelian field M, so

$$\begin{aligned} \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n} &= (\mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{0,K_n}) \oplus s(\mathrm{Gal}(L_n/\mathbf{Q}))\mathbf{Z}, \\ (e^+_{L_n} U_{L_n})^H &= (e^+_{L_n} U_{0,L_n})^H \oplus s(\mathrm{Gal}(L_n/\mathbf{Q}))\mathbf{Z}. \end{aligned}$$

Hence

$$[(e^+_{L_n} U_{0,L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{0,K_n}] = [(e^+_{L_n} U_{L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n}]$$

and the lemma follows.

Lemma 5.

$$[(e^+_{L_n} U_{L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n}] \approx [(e^+_{L_n} V_{L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}].$$

Proof. By Lemma 1.1 of [**S**2] we have

$$\begin{aligned} [(e^+_{L_n} U_{L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n}] = {} & ((e^+_{L_n} U_{L_n})^H : (e^+_{L_n} V_{L_n})^H)[(e^+_{L_n} V_{L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}] \\ & \cdot (\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n} : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n}), \end{aligned}$$

where (:) means the generalized index (see [**S**2], p. 187). The lemma will be proved if we show that

$$((e^+_{L_n} U_{L_n})^H : (e^+_{L_n} V_{L_n})^H) \approx 1 \qquad \text{and} \qquad (\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n} : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n}) \approx 1.$$

Since cor_{L_n/K_n} is an injective homomorphism,

$$(\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n} : \mathrm{cor}_{L_n/K_n} e^+_{K_n} U_{K_n}) = (e^+_{K_n} V_{K_n} : e^+_{K_n} U_{K_n}),$$

which is independent of n for n sufficiently large (the p-part of the index is described in Proposition 6.2 of [S2], while for the non-p-part we can use the "$p \neq l$" case of Sinnott's proof of Theorem 6.1 of [S2]). Lemma 1.2(a) of [**S**2] gives

$$\begin{aligned} ((e^+_{L_n} U_{L_n})^H : (e^+_{L_n} V_{L_n})^H) = {} & ((1-e_{p,L_n})(e^+_{L_n} U_{L_n})^H : (1-e_{p,L_n})(e^+_{L_n} V_{L_n})^H) \\ & \cdot ((e^+_{L_n} U_{L_n})^{HI_{p,L_n}} : (e^+_{L_n} V_{L_n})^{HI_{p,L_n}}). \end{aligned}$$

We have

$$((1-e_{p,L_n})e^+_{L_n} U_{L_n})^H = ((1-e_{p,L_n})e^+_{L_n} V_{L_n})^H$$

(see [**S**2, last line of p. 210]), so

$$((1-e_{p,L_n})(e^+_{L_n}U_{L_n})^H:(1-e_{p,L_n})(e^+_{L_n}V_{L_n})^H)=\frac{[((1-e_{p,L_n})e^+_{L_n}V_{L_n})^H:(1-e_{p,L_n})(e^+_{L_n}V_{L_n})^H]}{[((1-e_{p,L_n})e^+_{L_n}U_{L_n})^H:(1-e_{p,L_n})(e^+_{L_n}U_{L_n})^H]}.$$

To prove that the numerator and the denominator of the last expression are bounded, we define mappings

$$\begin{aligned}F_1&:((1-e_{p,L_n})e^+_{L_n}V_{L_n})^H/(1-e_{p,L_n})(e^+_{L_n}V_{L_n})^H\to H^1(H,(e^+_{L_n}V_{L_n})^{I_{p,L_n}})\\ F_2&:((1-e_{p,L_n})e^+_{L_n}U_{L_n})^H/(1-e_{p,L_n})(e^+_{L_n}U_{L_n})^H\to H^1(H,(e^+_{L_n}U_{L_n})^{I_{p,L_n}})\end{aligned}$$

as follows. For any $u\in V_{L_n}$ (resp. $u\in U_{L_n}$) let F_1 (resp. F_2) maps the class containing $(1-e_{p,L_n})e^+_{L_n}u$ to the cohomology class of the crossed homomorphism sending $h\in H$ to $(h-1)e^+_{L_n}u$. It is easy to check that F_1 and F_2 are well-defined injective homomorphisms. Proposition 6.2 (and Lemma 5.4 for the non-p-part) of [**S**2] gives that there is n_0 such that for all $n\geq n_0$ we have

$$\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}}=(e^+_{L_n}V_{L_n})^{I_{p,L_n}}.$$

Directly from the definition we have $\operatorname{res}_{L_n/L_{n_0}}(e^+_{L_n}V_{L_n})=e^+_{L_{n_0}}V_{L_{n_0}}$, so $\operatorname{cor}_{L_n/L_{n_0}}s(I_{p,L_{n_0}})=s(I_{p,L_n})$ implies

$$\operatorname{cor}_{L_n/L_{n_0}}(s(I_{p,L_{n_0}})e^+_{L_{n_0}}V_{L_{n_0}})=s(I_{p,L_n})e^+_{L_n}V_{L_n}.$$

Since L_n is a cyclotomic field, we have by Proposition 5.1 of [**S**1] that $U_{L_n}=V_{L_n}\cdot U_{p,L_n}$, where U_{p,L_n} is the $\mathbf{Z}[\mathrm{Gal}(L_n/\mathbf{Q})]$-module generated in $\mathbf{Q}[\mathrm{Gal}(L_n/\mathbf{Q})]$ by $s(I_{p,L_n})$ and $1-(p,L_n)^*$. Lemma 5.2 of [**S**1] gives

$$(e^+_{L_n}U_{L_n})^{I_{p,L_n}}=((e^+_{L_n}V_{L_n})U_{p,L_n})^{I_{p,L_n}}=s(I_{p,L_n})e^+_{L_n}V_{L_n}+(1-\lambda^{-1}_{p,L_n})(e^+_{L_n}V_{L_n})^{I_{p,L_n}}$$

and for any $n\geq n_0$ we have

$$\begin{aligned}(e^+_{L_n}U_{L_n})^{I_{p,L_n}}&=\operatorname{cor}_{L_n/L_{n_0}}(s(I_{p,L_{n_0}})e^+_{L_{n_0}}V_{L_{n_0}})+(1-\lambda^{-1}_{p,L_n})\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}}\\&=\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}U_{L_{n_0}})^{I_{p,L_{n_0}}}.\end{aligned}$$

Since $\operatorname{cor}_{L_n/L_{n_0}}$ is an injective homomorphism, we have obtained for each $n\geq n_0$

$$\begin{aligned}H^1(H,(e^+_{L_n}V_{L_n})^{I_{p,L_n}})&\cong H^1(H,(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}})\\ H^1(H,(e^+_{L_n}U_{L_n})^{I_{p,L_n}})&\cong H^1(H,(e^+_{L_{n_0}}U_{L_{n_0}})^{I_{p,L_{n_0}}})\end{aligned}$$

and

$$((1-e_{p,L_n})(e^+_{L_n}U_{L_n})^H:(1-e_{p,L_n})(e^+_{L_n}V_{L_n})^H)\approx 1.$$

The injectivity of $\operatorname{cor}_{L_n/L_{n_0}}$ also implies

$$\begin{aligned}(e^+_{L_n}U_{L_n})^{I_{p,L_n}H}&=(\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}U_{L_{n_0}})^{I_{p,L_{n_0}}})^H=\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}U_{L_{n_0}})^{I_{p,L_{n_0}}H}\\ (e^+_{L_n}V_{L_n})^{I_{p,L_n}H}&=(\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}})^H=\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}H}.\end{aligned}$$

Therefore

$$\begin{aligned}((e^+_{L_n}U_{L_n})^{HI_{p,L_n}}:(e^+_{L_n}V_{L_n})^{HI_{p,L_n}})&=(\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}U_{L_{n_0}})^{I_{p,L_{n_0}}H}:\operatorname{cor}_{L_n/L_{n_0}}(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}H})\\&=((e^+_{L_{n_0}}U_{L_{n_0}})^{I_{p,L_{n_0}}H}:(e^+_{L_{n_0}}V_{L_{n_0}})^{I_{p,L_{n_0}}H})\end{aligned}$$

and the lemma is proved.

5. Λ-modules

Lemma 6. *There are $\mu, \nu_1, \nu_2 \in \mathbf{Z}$ such that $\mu \geq 0$ and*

$$p^{\mu p^n + \nu_1} \mid [(e^+_{L_n} V_{L_n})^H \otimes \mathbf{Z}_p : (\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}) \otimes \mathbf{Z}_p] \mid p^{\mu p^n + \nu_2}$$

for each $n \geq 0$.

Proof. Up to now we have worked in the Galois group rings of L_n and K_n, but for the computation of the p-part of $[(e^+_{L_n} V_{L_n})^H : \mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}]$ (which is precisely $[(e^+_{L_n} V_{L_n})^H \otimes \mathbf{Z}_p : (\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}) \otimes \mathbf{Z}_p]$) we have to work in the inverse limits of these group rings (with respect to the restrictions). Let

$$R_L = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(L_n/\mathbf{Q})], \qquad R_K = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})], \qquad \Lambda = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(L_n/\mathbf{Q}(\zeta_{qf})] \cong \mathbf{Z}_p[[T]].$$

The previous isomorphism can be described as follows: $1+T$ is the image of $\gamma = (\dots, \gamma_n, \dots)$, where $\gamma_n \in \mathrm{Gal}(L_n/\mathbf{Q}(\zeta_{qf}))$ is determined by $\gamma_n(\zeta_{qp^n}) = \zeta_{qp^n}^{1+q}$. We have

$$\mathrm{res}_{L_n/L_{n-1}} \circ \mathrm{cor}_{L_n/K_n} = \mathrm{cor}_{L_{n-1}/K_{n-1}} \circ \mathrm{res}_{K_n/K_{n-1}}$$

for each $n \geq 1$, so there is a well-defined injective homomorphism $\mathrm{cor}_{L/K} : R_K \to R_L$. Similarly, we have a homomorphism $\mathrm{res}_{L/K} : R_L \to R_K$. It is easy to see that R_L and R_K are finitely generated Λ-modules without Λ-torsion (Λ acts on R_K via $\mathrm{res}_{L/K}$). Let $\omega_n = \gamma^{p^n} - 1$.

For each integer $n \geq 0$ we have natural projections

$$\pi_L^{(n)} : R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \to \mathbf{Q}_p[\mathrm{Gal}(L_n/\mathbf{Q})] \qquad \text{and} \qquad \pi_K^{(n)} : R_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \to \mathbf{Q}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$$

with kernels $\omega_n(R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$ and $\omega_n(R_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$, respectively.

Let A be a finitely generated Λ-module in $R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ (resp. $R_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$). We say, after Sinnott, that A satisfies $(*)$ if, for any integer $n \geq 0$, Λ-module $\omega_n A$ has finite index in $A \cap \mathrm{Ker}\, \pi_L^{(n)}$ (resp. $A \cap \mathrm{Ker}\, \pi_K^{(n)}$).

Let A, B be finitely generated Λ-modules in $R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. We say that A and B are comparable if there are positive integers a, b such that $p^a A \subseteq B$ and $p^b B \subseteq A$.

For any positive divisor r of m we can consider

$$\alpha_r = (\dots, s(I_{r,L_n}) \prod_{l \mid \frac{m}{r}} (1 - (l, L_n)^*), \dots) \in R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p.$$

We define V_L to be the R_L-module generated in $R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ by the elements α_r, where r runs through the set of the positive divisors of m. Similarly we define R_K-module $V_K \subseteq R_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Let $e^+_L = (\dots, e^+_{L_n}, \dots)$ and $e^+_K = (\dots, e^+_{K_n}, \dots)$. It is easy to see that

$$(e^+_{L_n} V_{L_n}) \otimes \mathbf{Z}_p = \pi_L^{(n)}(e^+_L V_L) \qquad \text{and} \qquad (\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}) \otimes \mathbf{Z}_p = \pi_L^{(n)}(\mathrm{cor}_{L/K} e^+_K V_K).$$

Proposition 6.1 of [**S**2] gives that $e^+_L V_L$ and $e^+_K V_K$ satisfy $(*)$, hence $\mathrm{cor}_{L/K} e^+_K V_K$ also satisfies $(*)$. Lemma 5.4 of [**S**2] implies that

$$(\#H)(e^+_L V_L)^H \subseteq e^+_L s(H) V_L \subseteq \mathrm{cor}_{L/K} e^+_K V_K \subseteq (e^+_L V_L)^H,$$

so $(e^+_L V_L)^H$ and $\mathrm{cor}_{L/K} e^+_K V_K$ are comparable. By Lemma 6.2 of [**S**2], $(e^+_L V_L)^H$ satisfies $(*)$ and there are $\mu, \nu \in \mathbf{Z}$ such that $\mu \geq 0$ and, for all sufficiently large n,

$$(\pi_L^{(n)}(e^+_L V_L)^H : (\mathrm{cor}_{L_n/K_n} e^+_{K_n} V_{K_n}) \otimes \mathbf{Z}_p) = p^{\mu p^n + \nu}.$$

There is a Λ-module $A' \subseteq R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ such that $e_L^+ V_L \subseteq A'$ and, for all sufficiently large n, the kernel of $\pi_L^{(n)}$ in $e_L^+ V_L$ is equal to $\omega_n A'$ (see the proof of Lemma 6.2 of [**S**2] for $A = e_L^+ V_L$). Therefore we have an exact sequence

$$0 \longrightarrow \omega_n A' \xrightarrow{\subseteq} e_L^+ V_L \xrightarrow{\pi_L^{(n)}} (e_{L_n}^+ V_{L_n}) \otimes \mathbf{Z}_p \longrightarrow 0.$$

Taking H-invariants gives the exact sequence

$$0 \longrightarrow (\omega_n A')^H \xrightarrow{\subseteq} (e_L^+ V_L)^H \xrightarrow{\pi_L^{(n)}} (e_{L_n}^+ V_{L_n})^H \otimes \mathbf{Z}_p \longrightarrow Y_n \longrightarrow 0,$$

where Y_n is the kernel of the homomorphism $H^1(H, \omega_n A') \to H^1(H, e_L^+ V_L)$ induced by the inclusion $\omega_n A' \subseteq e_L^+ V_L$. Since $A' \subseteq R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, the action of ω_n is an injective mapping on A', so $H^1(H, A') \cong H^1(H, \omega_n A')$. For any Λ-module M, let M_{ω_n} be the submodule of M which is killed by the action of ω_n. As $e_L^+ V_L \subseteq A'$, we have $Y_n \subseteq \operatorname{Ker}\big(H^1(H, \omega_n A') \to H^1(H, A')\big)$ and the latter group is isomorphic to $H^1(H, A')_{\omega_n}$ (here we have used the fact that $A'_{\omega_n} = 0$, as $A' \subseteq R_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$). Because A' is a finitely generated Λ-module and H is finite, $H^1(H, A')$ is also a finitely generated Λ-module. Moreover, $H^1(H, A')$ is $(\#H)$-torsional, so, due to the well-known theorem on the structure of finitely generated Λ-modules, there are finite Λ-modules A, B and Λ-module $M \cong \bigoplus_{i=1}^s (\Lambda / p^{t_i} \Lambda)$, where $s, t_1, \dots, t_s$ are positive integers, such that

$$0 \longrightarrow A \longrightarrow H^1(H, A') \longrightarrow M \longrightarrow B \longrightarrow 0$$

is an exact sequence of Λ-modules. Taking the kernels of ω_n-action gives the following exact sequence

$$0 \longrightarrow A_{\omega_n} \longrightarrow H^1(H, A')_{\omega_n} \longrightarrow M_{\omega_n}$$

It follows easily from the structure of M that $M_{\omega_n} = 0$, so

$$H^1(H, A')_{\omega_n} \cong A_{\omega_n}.$$

Hence

$$[(e_{L_n}^+ V_{L_n})^H \otimes \mathbf{Z}_p : \pi_L^{(n)}((e_L^+ V_L)^H)] = \#Y_n \mid \#(H^1(H, A')_{\omega_n}) \mid \#A$$

is bounded. The lemma is proved.

6. Back to units

Proposition. *There are $\mu, \nu_1, \nu_2 \in \mathbf{Z}$ such that $\mu \geq 0$ and*

$$p^{\mu p^n + \nu_1} \mid \left[\overline{C}_{K_n} : C_{K_n}\right]_p \mid p^{\mu p^n + \nu_2}$$

for each $n \geq 0$, where $\left[\overline{C}_{K_n} : C_{K_n}\right]_p$ means the p-part of the index $\left[\overline{C}_{K_n} : C_{K_n}\right]$.

Proof. This follows from Lemmas 1, 3, 4, 5 and 6.

Lemma 7. *Let M be a real abelian field and $C_{1,M} = \{\varepsilon \in E_M; \varepsilon^2 \in C_M\}$. Then $[C_{1,M} : \overline{C}_M \cap C_{1,M}]$ is 1 or 2 and $[C_{1,M} : C_M]$ divides $2\left[\overline{C}_M : C_M\right]$.*

Proof. Let m be the conductor of M. Since M is real, we have $M \subseteq \mathbf{Q}(\zeta_m)^+$ and $C_M \subseteq C_{\mathbf{Q}(\zeta_m)^+}$. Any $\varepsilon \in C_{\mathbf{Q}(\zeta_m)^+}$ is (up to a sign) a combination of elements of the form $\mathrm{N}(1 - \zeta_n^a)$, such that $1 < n \mid m$ and $(a, n) = 1$, where N means the norm from $\mathbf{Q}(\zeta_n)$ to $\mathbf{Q}(\zeta_m)^+ \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_n)^+$ (see [**L**]). But

$$\mathrm{N}(1 - \zeta_n^a) = (1 - \zeta_n^a)(1 - \zeta_n^{-a}) = -\zeta_n^{-a}(1 - \zeta_n^a)^2.$$

Therefore $C_M \subseteq W_{\mathbf{Q}(\zeta_m)} C^2_{\mathbf{Q}(\zeta_m)}$.

Let $f : C_{1,M} \to W_{\mathbf{Q}(\zeta_m)}/W^2_{\mathbf{Q}(\zeta_m)}$ be defined as follows. For any $\varepsilon \in C_{1,M}$ there are $\rho \in W_{\mathbf{Q}(\zeta_m)}$ and $\eta \in C_{\mathbf{Q}(\zeta_m)}$ such that $\varepsilon^2 = \rho\eta^2$; let $f(\varepsilon) = \rho W^2_{\mathbf{Q}(\zeta_m)}$. It is easy to see that f is a well-defined homomorphism and that $[C_{1,M} : \operatorname{Ker} f]$ is 1 or 2. If $\varepsilon \in \operatorname{Ker} f$ then $\varepsilon^2 = \rho^2\eta^2$ for some $\rho \in W_{\mathbf{Q}(\zeta_m)}$ and $\eta \in C_{\mathbf{Q}(\zeta_m)}$, so $\varepsilon = \pm\rho\eta \in C_{\mathbf{Q}(\zeta_m)} \cap E_M = \overline{C}_M$. Therefore $[C_{1,M} : \overline{C}_M \cap C_{1,M}]$ is 1 or 2. It is easy to see that

$$[\overline{C}_M : C_M] = \frac{[\overline{C}_M : \overline{C}_M \cap C_{1,M}][C_{1,M} : C_M]}{[C_{1,M} : \overline{C}_M \cap C_{1,M}]}$$

and the lemma follows.

7. The proof of the Theorem

At first, let us show that $[\overline{C}_{K_n} : C_{K_n}]$ can be divisible only by finitely many primes, namely by primes dividing $\#H$. Indeed,

$$\mathrm{N}_{L_n/K_n}(C_{L_n}) \subseteq C_{K_n} \subseteq C^H_{L_n} = \overline{C}_{K_n}$$

and

$$C^H_{L_n}/\,\mathrm{N}_{L_n/K_n}(C_{L_n}) = \hat{H}^0(H, C_{L_n})$$

is finite and $(\#H)$-torsional. Hence, due to Sinnott's theorem (see Introduction), it is enough to prove the Theorem locally. We shall do it by the following two lemmas.

For any prime l, the symbol $[\ :\ ]_l$ means the l-part of the index $[\ :\ ]$.

Lemma 8. *There are integers c_1 and c_2 such that*

$$p^{c_1}(h^+_{K_n})_p \mid [E_{K_n} : \overline{C}_{K_n}]_p \mid p^{c_2}(h^+_{K_n})_p,$$

where $(h^+_{K_n})_p$ means the p-part of $h^+_{K_n}$.

Proof. The theorems of Iwasawa and of Ferrero–Washington (e.g., see Theorem 13.13 and Theorem 7.15 of [**W**2]) give that there exist integers $\lambda \geq 0$ and ν such that

$$(h^+_{K_n})_p = p^{\lambda n+\nu}$$

for all sufficiently large n. We need to distinguish two cases.

At first, let us suppose that $p \neq 2$ or k is imaginary. Sinnott's theorem gives that there is an integer ν' such that

$$[E_{K_n} : C_{K_n}]_p = p^{\lambda n+\nu'}$$

for all sufficiently large n. Then the Proposition implies $\mu p^n + \nu_1 \leq \lambda n + \nu'$ for all sufficiently large n, hence $\mu = 0$. The lemma (in this case) follows from Sinnott's theorem and the Proposition.

Now, let us suppose that $p = 2$ and k is real. By Sinnott's theorem there are integers ν' and ν'' such that

$$[E_{K_n} : C_{K_n}]_2 = 2^{[K_n:\mathbf{Q}]+\lambda n+\nu'} \qquad \text{and} \qquad [E_{K_n} : C_{1,K_n}]_2 = 2^{\lambda n+\nu''}$$

for all sufficiently large n. Comparing with the Proposition gives

$$\mu 2^n + \nu_1 \leq [k : \mathbf{Q}] \cdot 2^n + \lambda n + \nu'$$

for all sufficiently large n, so $\mu \leq [k : \mathbf{Q}]$. On the other hand, Lemma 7 and the Proposition imply

$$[k : \mathbf{Q}] \cdot 2^n + \nu' - \nu'' \leq 1 + \mu 2^n + \nu_2,$$

for all sufficiently large n, hence $[k : \mathbf{Q}] \leq \mu$. Therefore $\mu = [k : \mathbf{Q}]$ and Sinnott's theorem and the Proposition give the lemma.

Lemma 9. *Let l be a prime different from p. Then $\left[E_{K_n} : \overline{C}_{K_n}\right]_l$ is independent of n, for n sufficiently large.*

Proof. By Washington's theorem, the l-part $(h^+_{K_n})_l$ of the class number $h^+_{K_n}$ is independent of n, for n sufficiently large (see [**W**1]).

At first, let us suppose that $p \neq 2$ or k is imaginary. Since $C_{K_n} \subseteq C_{K_{n+1}}$ and $\overline{C}_{K_n} \subseteq \overline{C}_{K_{n+1}}$, we can consider the homomorphism of finite groups $\overline{C}_{K_n}/C_{K_n} \to \overline{C}_{K_{n+1}}/C_{K_{n+1}}$ induced by the inclusion. The restriction of this homomorphism to the l-Sylow subgroups is injective, since $\varepsilon \in \overline{C}_{K_n} \cap C_{K_{n+1}}$ implies $\varepsilon^p = \mathrm{N}_{K_{n+1}/K_n}(\varepsilon) \in C_{K_n}$. Therefore

$$\left[\overline{C}_{K_n} : C_{K_n}\right]_l \mid \left[\overline{C}_{K_{n+1}} : C_{K_{n+1}}\right]_l.$$

Of course, $\left[\overline{C}_{K_n} : C_{K_n}\right]_l$ divides $[E_{K_n} : C_{K_n}]_l$, which is bounded by a constant by Sinnott's and Washington's theorems. Hence $\left[\overline{C}_{K_n} : C_{K_n}\right]_l$ is independent of n, for n sufficiently large, and the lemma follows in this case.

Now, let us suppose that $p = 2$ and k is real. Similarly as in the previous part we can prove that

$$\begin{aligned}\left[C_{1,K_n} : \overline{C}_{K_n} \cap C_{1,K_n}\right]_2 &\mid \left[C_{1,K_{n+1}} : \overline{C}_{K_{n+1}} \cap C_{K_{n+1}}\right]_2\\ \left[\overline{C}_{K_n} : \overline{C}_{K_n} \cap C_{1,K_n}\right]_2 &\mid \left[\overline{C}_{K_{n+1}} : \overline{C}_{K_{n+1}} \cap C_{K_{n+1}}\right]_2.\end{aligned}$$

Since $\left[C_{1,K_n} : \overline{C}_{K_n} \cap C_{1,K_n}\right]_2$ is 1 or 2 by Lemma 7, $\left[C_{1,K_n} : \overline{C}_{K_n} \cap C_{1,K_n}\right]_2$ is independent of n, for n sufficiently large. Hence, by Sinnott's theorem, we have the same for $\left[E_{K_n} : \overline{C}_{K_n} \cap C_{1,K_n}\right]_2$. Therefore $\left[\overline{C}_{K_n} : \overline{C}_{K_n} \cap C_{K_n}\right]_2$ is independent of n, for n sufficiently large. The lemma follows.

References

[**L**] G. Lettl, A note on Thaine's circular units, *J. Number Theory* **35** (1990), 224–226.

[**S**1] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math.* **108** (1978), 107–134.

[**S**2] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, *Inv. Math.* **62** (1980), 181–234.

[**W**1] L. C. Washington, The non-p-part of the class number in a cyclotomic $\mathbf{Z}_p$-extension, *Inv. Math.* **49** (1979), 87–97.

[**W**2] L. C. Washington, "Introduction to cyclotomic fields", Springer–Verlag, New York, 1982.

Radan Kučera
Department of Mathematics
Faculty of Science
Masaryk University
Janáčkovo nám. 2a
662 95 Brno
Czech Republic

Jan Nekovář[1]
Department of Mathematics
University of California
Berkeley
CA 94720
U.S.A.

[1] Address after August 1, 1993: Mathematical Institute, Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic