CARPATHIAN J. MATH. Online version at http://carpathian.ubm.ro
33 (2017), No. 1, 43 - 48 Print Edition: ISSN 1584 - 2851 Online Edition: ISSN 1843 - 4401

On an isomorphism lying behind the class number formula

VLAD CRIŞAN

ABSTRACT. Let p be an odd prime such that the Greenberg conjecture holds for the maximal real cyclotomic subfield $\mathbb{K}_1$ of $\mathbb{Q}[\zeta_p]$. Let $A_n = (\mathcal{C}(\mathbb{K}_n))_p$ be the p-part of the class group of $\mathbb{K}_n$, the n-th field in the cyclotomic tower, and let $\underline{E}_n, \underline{C}_n$ be the global and cyclotomic units of $\mathbb{K}_n$, respectively. We prove that under this premise, there is some n_0 such that for all $m \geq n_0$, the class number formula $\left|(\underline{E}_m/\underline{C}_m)_p\right| = |A_m|$ hides in fact an isomorphism of $\Lambda[\mathrm{Gal}(\mathbb{K}_1/\mathbb{Q})]$-modules.

1. NOTATIONS AND AUXILIARY RESULTS

We fix an odd prime $p > 3$ and introduce the following notations: for $n \geq 1$, we set $\mathbb{K}_n = \mathbb{Q}[\zeta_{p^n} + \overline{\zeta}_{p^n}]$, with ζ_{p^n} a primitive p^n-th root of unity. The norm maps are denoted by $N_{n,m} = \mathbf{N}_{\mathbb{K}_n/\mathbb{K}_m}$; for a number field $\mathbf{K}$, we denote by $\mathbf{K}_\infty$ its cyclotomic $\mathbb{Z}_p$-extension. In our case, $\mathbb{K}_\infty = \bigcup_{n\geq 1} \mathbb{K}_n$ is a totally real field. We let $\mathbb{B}_\infty/\mathbb{Q}$ be the $\mathbb{Z}_p$-extension of $\mathbb{Q}$, so $\mathbb{K}_\infty = \mathbb{K}_1 \cdot \mathbb{B}_\infty$, G_n is the Galois group of $\mathbb{K}_n/\mathbb{Q}$ and Γ is the Galois group of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}_1)$, with $\tau \in \Gamma$ a topological generator. We also let $\Gamma_n = \mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_1)$. We write as usual $T = \tau - 1$, $\Lambda = \mathbb{Z}_p[[T]]$ and

$$\omega_n = \tau^{p^{n-1}} - 1 = (T+1)^{p^{n-1}} - 1, \qquad \nu_{n,m} = \omega_n/\omega_m, \quad \text{for } n > m \geq 1.$$

We lift G_1 to G_n in the standard way. Notice that $\tau^{p^{n-1}}$ is the largest power of τ which fixes $\mathbb{K}_n$, so we have that $\alpha^{\omega_n} = 1$, for all $\alpha \in \mathbb{K}_n$. Let A_n be the p-Sylow subgroup of the ideal class group $\mathcal{C}(\mathbb{K}_n)$ of $\mathbb{K}_n$ and let $A_\infty = \varprojlim_n A_n$ be the projective limit of the groups $(A_n)_{n\geq 1}$; Greenberg's Conjecture specializes in our contexts to the following statement:

Greenberg's Conjecture: $|A_\infty| < \infty$.

Let $\underline{E}_n$ and $\underline{C}_n$ denote the global and the cyclotomic units of $\mathbb{K}_n$, respectively. Then the class number formula ([4] Theorem 8.2) reads $|\mathcal{C}(\mathbb{K}_n)| = |\underline{E}_n/\underline{C}_n|$, so the corresponding p-parts satisfy $|A_n| = \left|(\underline{E}_n/\underline{C}_n)_p\right|$. In this paper we prove that assuming Greenberg's conjecture, the last equality underlines an isomorphism of $\Lambda[G_1]$-modules, for all n sufficiently large.

2. A CORE LEMMA

For every $n \geq 1$, let $\underline{e}_1, \ldots, \underline{e}_{r_n}$ (with the dependence on n being understood) be a corresponding fundamental system of units of $\underline{E}_n$, where $r_n = [\mathbb{K}_n : \mathbb{Q}] - 1$, as $\mathbb{K}_n$ is totally real. Then every element in $\underline{E}_n$ is of the form $\pm\underline{e}_1^{a_1} \cdot \ldots \cdot \underline{e}_{r_n}^{a_{r_n}}$, where $a_1, \ldots, a_{r_n} \in \mathbb{Z}$. Let $g \in \mathbb{Z}$ be a generator for $(\mathbb{Z}/p^2\mathbb{Z})^\times$ and hence also for $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for any $n \geq 2$. Let $\eta_n = \frac{\zeta_{p^n}^g - \overline{\zeta}_{p^n}^g}{\zeta - \overline{\zeta}}$ and let $C_n = \eta_n^{\mathbb{Z}_p[G_n]}$ be the subgroup of $\underline{C}_n$ generated by η_n as a $\mathbb{Z}[G_n]$-module. Then $C_n = \underline{C}_n/\{\pm 1\}$ ([4] Lemma 8.11). As p is odd, we have

Received: 02.03.2016. In revised form: 04.07.2016. Accepted: 25.09.2016
2010 *Mathematics Subject Classification*. 11R23.
Key words and phrases. *Number Theory, Iwasawa Theory.*

$$(\underline{E}_n/\underline{C}_n)_p = (\underline{E}_n/C_n)_p\,.$$

For each $j = 1, \ldots, r_n$, write

$$q_j \cdot p^{\alpha_j} = \left|\underline{e}_j^{\mathbb{Z}} / \left(\underline{e}_j^{\mathbb{Z}} \cap C_n\right)\right|.$$

Now let $e_j = \underline{e}_j^{q_j}$ and let E_n be the subgroup of $\underline{E}_n$ generated by the elements $e_1, \ldots, e_{r_n}$ as a $\mathbb{Z}$-module. Notice that for each j we have $e_j \in (\underline{E}_n/C_n)_p$ and E_n/C_n is a subgroup of $\underline{E}_n/C_n$ with $|E_n/C_n| = \left|(\underline{E}_n/C_n)_p\right|$. As everything in sight is abelian, the p-Sylow subgroup is unique and thus

$$E_n/C_n \cong (\underline{E}_n/C_n)_p\,.$$

Notice also that the elements $(\eta_n)_{n\geq 1}$ form a norm-coherent sequence in the extension $\mathbb{K}_\infty/\mathbb{K}$.

Recall that the norms $N_{n,m} : A_n \to A_m$ are surjective for all $n > m \geq 1$, since $\mathbb{K}_2 \cap \mathbb{H}(\mathbb{K}_1) = \mathbb{K}_1$ (here $\mathbb{H}$ stands for the Hilbert class field). Consequently, the numbers $|A_n|$ build an increasing sequence of positive integers bounded above by $|A_\infty|$, which was assumed to be finite. There must be thus an integer n_0 such that for any $n \geq m \geq n_0$, we have $|A_n| = |A_m| = |A_\infty|$ and the norm $N_{n,m}$ is in fact an isomorphism, so we have

$$A_n = A_m \cong A_\infty, \quad \forall n > m \geq n_0. \tag{2.1}$$

We now look at the ideal lift map $\iota_{m,n} : A_m \to A_n$ and its kernel (of capitulation). Let $k' > 0$ be such that $(A_\infty)^{p^{k'}} = 0$, and $n > n_0$. Since $N_{n,m} \circ \iota_{m,n} : A_m \to A_m$ is the p^{n-m} power map for $n > m \geq n_0$, by letting $n = m + k'$ we have

$$N_{n,m} \circ \iota_{m,n}(A_m) = (A_m)^{p^{k'}} = 0.$$

We have seen that $N_{n,m}$ is an isomorphism, so

$$\iota_{m,n}(A_m) \subset \text{ Ker } (N_{n,m} : A_n \to A_m) = 0.$$

This argument also works for $1 \leq m < n_0$: let $k = k' + n_0$. Then $\iota_{m,n} = \iota_{n_0,n} \circ \iota_{m,n_0}$ and since $\iota_{m,n_0}(A_m) \subset A_{n_0}$, $\iota_{n_0,n}(A_{n_0}) = \{1\}$, it follows that $\iota_{m,n}(A_m) = \{1\}$. We have proved:

Lemma 2.1. *Assuming Greenberg's conjecture, there exists a constant k such that for all $m \geq 1$ and $n \geq m + k$ we have*

$$A_n \cong A_\infty \quad \textit{and} \quad \iota_{m,n}(A_m) = 0.$$

We now turn our attention to the units and start by proving that the cyclotomic units are stable in the cyclotomic tower, in the following sense:

Lemma 2.2. *For any $n \geq m \geq 1$, we have $C_n \cap \mathbb{K}_m = C_m$.*

Proof. We know that C_n is a cyclic $\mathbb{Z}[G_n]$ module and $N_{\mathbb{K}_n/\mathbb{Q}}(C_n) = \{1\}$. So there is a surjective homomorphism

$$\mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]) \to C_n \quad \text{given by} \quad \overline{\theta} \to \eta_n^\theta,$$

where $\overline{\theta}$ denotes the image of $\theta \in \mathbb{Z}[G_n]$ in $\mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n])$.

We know C_n has finite index in E_n, so it has the same $\mathbb{Z}$-rank as E_n, namely $[\mathbb{K}_n : \mathbb{Q}]-1$ by Dirichlet's Unit Theorem. This is the same as the $\mathbb{Z}$-rank of $\mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n])$, so by Vasconcelos' Theorem ([3] Theorem 2.4), we know that the kernel of the above described map must be trivial. We have thus a short exact sequence

$$1 \longrightarrow \mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]) \xrightarrow{\overline{\theta}\to\eta_n^{\theta}} C_n \longrightarrow 1. \tag{2.2}$$

The inclusion $C_m \subseteq C_n \cap \mathbb{K}_m$ is clear. Conversely, consider $e \in C_n \cap \mathbb{K}_m$. Then $e = \eta_{n+1}^{\theta}$, for some $\theta \in \mathbb{Z}[G_n]$. We have that $G_n = \Gamma_n \times \langle\sigma\rangle$, where $\langle\sigma\rangle$ is the cyclic group $G_1 = \mathrm{Gal}(\mathbb{K}_1/\mathbb{Q})$. Hence one has an isomorphism of $\mathbb{Z}$-algebras $\phi : \mathbb{Z}[G_n] \xrightarrow{\sim} \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$ given by

$$\phi\left(\sum_i a_i \cdot g_i\right) = \sum_i a_i h_i \otimes n_i,$$

where $a_i \in \mathbb{Z}$, $g_i \in G_n$, $h_i \in \Gamma_n$, $n_i \in G_1$ and $g_i = h_i \cdot n_i$.

By a slight abuse of notation, we shall write ω_m for the image of $\omega_m = \tau^{p^{m-1}} - 1 = (T+1)^{p^{m-1}} - 1$ in $\mathbb{Z}[\Gamma_n]$ and similarly for $\nu_{m,1}, T$, etc. For the rest of the proof ω_m, $\nu_{m,1}$, T, etc will always refer to elements in $\mathbb{Z}[\Gamma_n]$. Let $\widehat{\omega_m} = \phi^{-1}(\omega_m \otimes 1)$. Since $e \in \mathbb{K}_m$, we have $e^{\widehat{\omega_m}} = 1$, thus

$$\eta_n^{\widehat{\omega_m}\cdot\theta} = 1. \tag{2.3}$$

By (2.2), this implies that $\widehat{\omega_m} \cdot \theta \in N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]$. Let $z \in \mathbb{Z}[G_n]$ be such that $\widehat{\omega_m} \cdot \theta = N_{\mathbb{K}_n/\mathbb{Q}} \cdot z$ and let us write $N_{\mathbb{K}_n/\mathbb{Q}} = \nu_{n,1} \cdot N_\sigma$, where N_σ is the norm map $N_{\mathbb{K}_1/\mathbb{Q}}$. Under the isomorphism $\mathbb{Z}[G_n] \cong \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$, the element $\widehat{\omega_m} \in \mathbb{Z}[G_n]$ is mapped to $\omega_m \otimes 1$ and $N_{\mathbb{K}_n/\mathbb{Q}}$ is mapped to $\nu_{n,1} \otimes N_\sigma$. Now let $\{e_i\}_{i=1}^{\frac{p-1}{2}}$ be a $\mathbb{Z}$-basis for $\mathbb{Z}[G_1]$. Then for all $i = 1, 2, \ldots, \frac{p-1}{2}$, there exist integers a_i, c_i and elements $\theta_i, \tilde{z}_i \in \mathbb{Z}[\Gamma_n]$ such that

$$\phi(\theta) = \sum_{i=1}^{(p-1)/2} a_i\theta_i \otimes e_i \quad \text{and} \quad \phi(z) = \sum_{i=1}^{(p-1)/2} c_i\tilde{z}_i \otimes e_i.$$

Then

$$\phi(\widehat{\omega_m} \cdot \theta) = \sum_i a_i\omega_m\theta_i \otimes e_i \quad \text{and} \quad \phi(N_{\mathbb{K}_n/\mathbb{Q}} \cdot z) = \sum_i c_i\nu_{n,1}\tilde{z}_i \otimes N_\sigma e_i.$$

We now rewrite the expression $\sum_i c_i\nu_{n,1}\tilde{z}_i \otimes N_\sigma e_i$ along the basis $\{e_i\}_{i=1}^{\frac{p-1}{2}}$, so that one has

$$\phi(N_{\mathbb{K}_n/\mathbb{Q}} \cdot z) = \sum_i b_i\nu_{n,1}z_i \otimes e_i,$$

for some $b_i \in \mathbb{Z}$ and $z_i \in \mathbb{Z}[\Gamma_n]$ which can be computed in terms of the c_i's and $\tilde{z}_i$'s, respectively.

Due to the equality $\omega_m \cdot \theta = N_{\mathbb{K}_n/\mathbb{Q}} \cdot z$ in $\mathbb{Z}[G_n]$, we must have that for all $i = 1, 2, \ldots, \frac{p-1}{2}$, the identity $a_i\omega_m\theta_i = b_i\nu_{n,1}z_i$ holds in $\mathbb{Z}[\Gamma_n]$.

We also know that $\omega_m = \nu_{m,1} \cdot T$. Plugging this into the equality $a_i\omega_m\theta_i = b_i\nu_{n,1}z_i$, we obtain $a_i\nu_{m,1}T\theta_i = b_i\nu_{n,1}z_i$.

Let $\kappa : \mathbb{Z}[\Gamma_n] \to \frac{\mathbb{Z}[X]}{(X^{p^{n-1}}-1)}$ be an explicit isomorphism with $\kappa(T) = X - 1$. Then one has $\kappa(\omega_m) = X^{p^{m-1}} - 1$ and $\kappa(\nu_{n,1}) = \frac{X^{p^{n-1}}-1}{X-1}$. From $a_i\omega_m\theta_i = b_i\nu_{n,1}z_i$, we obtain

$$a_i(X^{p^{m-1}} - 1)\kappa(\theta_i) = b_i\frac{X^{p^{n-1}} - 1}{X - 1}\kappa(z_i) \quad \text{in} \quad \frac{\mathbb{Z}[X]}{(X^{p^{n-1}} - 1)}.$$

So there exists a polynomial $f_i(X) \in \mathbb{Z}[X]$ such that

$$a_i(X^{p^{m-1}} - 1)\kappa(\theta_i) + f_i(X)(X^{p^{n-1}} - 1) = b_i\frac{X^{p^{n-1}} - 1}{X - 1}\kappa(z_i) \quad \text{in} \quad \mathbb{Z}[X].$$

Dividing both sides by $\frac{X^{p^{m-1}}-1}{X-1}$ we get

$$a_i(X - 1)\kappa(\theta_i) + f_i(X)(X - 1)\frac{X^{p^{n-1}} - 1}{X^{p^{m-1}} - 1} = b_i\frac{X^{p^{n-1}} - 1}{X^{p^{m-1}} - 1}\kappa(z_i).$$

From this, one deduces that $\frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1} \mid a_i(X-1)\kappa(\theta_i)$ and since $\gcd((X-1), \frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1}) = 1$ with $\frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1}$ monic, we obtain $\frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1} \mid \kappa(\theta_i)$, as polynomials in $\mathbb{Z}[X]$. Hence there exists $g_i(X) \in \mathbb{Z}[X]$ such that $\kappa(\theta_i) = \kappa(\nu_{n,m}) \cdot g_i(X)$ as polynomials in $\frac{\mathbb{Z}[X]}{(X^{p^{n-1}}-1)}$. Thus $\theta_i = \nu_{n,m} \cdot s_i$, where $s_i = \kappa^{-1}(g_i(X)) \in \mathbb{Z}[\Gamma_n]$. Since this holds for all i, it implies via the isomorphism $\mathbb{Z}[G_n] \cong \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$ that one can write $\theta \in \mathbb{Z}[G_n]$ as $\widehat{\nu_{n,m}} \cdot s$, where $\widehat{\nu_{n,m}} = \phi^{-1}(\nu_{n,m} \otimes 1)$ and $s \in \mathbb{Z}[G_n]$. It is clear that $\eta_n^{\widehat{\nu_{n,m}}} = \eta_m$. Therefore, we obtain $e = \eta_n^{\widehat{\nu_{n,m}} \cdot s} = \eta_m^s$, which shows that $e \in C_m$, as required. □

The above result implies in particular that for any $n > m$, if $e \in \underline{E}_m \setminus C_m$ is a non-cyclotomic unit, then $e \notin C_n$ either. Notice also that $E_m \subseteq E_n$ for all $n \geq m \geq 1$. Therefore, the sizes of the groups E_m/C_m form an increasing sequence. The analytic class number formula implies that this sequence also must stabilize beyond n_0, so in view of (2.1), we have

$$|E_n/C_n| = |E_{n_0}/C_{n_0}| = |A_\infty|, \quad \forall n \geq n_0.$$

Since $E_mC_n \subseteq E_n = E_nC_n$ and E_m/C_m injects into $(E_mC_n)/C_n$ for $n > m$, we conclude that

$$E_n = E_mC_n, \quad \text{for all } n \geq m \geq n_0. \tag{2.4}$$

This identity implies in particular that $E_n^{\omega_m} \subset C_n$, for $n \geq m \geq n_0$.

3. Proof of the main Theorem

We now prove that the analytic class number formula also holds, for p-parts, as an isomorphism of $\Lambda[G_1]$-modules, for all sufficiently large m:

Proposition 3.1. *For any $m \geq n_0$, there is an isomorphism of $\Lambda[G_1]$-modules:*

$$(\underline{E}_m/\underline{C}_m)_p \cong A_m.$$

Proof. Recall that $(\underline{E}_m/\underline{C}_m)_p \cong E_m/C_m$ and this is an isomorphism of $\Lambda[G_1]$-modules, so it suffices to prove that $E_m/C_m \cong A_m$ as $\Lambda[G_1]$-modules. Let k be such that p^k annihilates E_{n_0}/C_{n_0} and let $n \geq n_0$ be such that $n - m \geq k$. Recall from above that under the given assumptions on m, n, k, we have $P_{m,n} :=$ Ker $(\iota_{m,n} : A_m \to A_n) \cong A_m$ as $\Lambda[G_1]$-modules, and also that $|E_m/C_m| = |A_m|$. Therefore, it suffices to prove that there is an injective homomorphism of $\Lambda[G_1]$-modules $\psi : E_m/C_m \hookrightarrow P_{m,n}$.

Let $\delta \in E_m \setminus C_m$; since the maps $E_m/C_m \hookrightarrow E_n/C_n$ are injective, as a consequence of Lemma 2.2, it follows that δ represents some class $d := [\delta] \in E_n/C_n$, for arbitrary $n \geq m$. Note that $p^{n-m} E_m/C_m = \{1\}$, since $n - m \geq k$. Thus, there exists some $x \in C_m$ such that $\delta^{p^{n-m}} = x$.

The norm $N_{n,m} : C_n \to C_m$ is surjective, so there exists $y \in C_n$ such that $x = N_{n,m}(y)$. Since δ is fixed by $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$, we have:

$$N_{n,m}(\delta) = \delta^{[\mathbb{K}_n:\mathbb{K}_m]} = \delta^{p^{n-m}} = x.$$

Viewing now δ as an element of $\mathbb{K}_n$ via the embedding $\mathbb{K}_m^\times \hookrightarrow \mathbb{K}_n^\times$, we see that $\gamma := \delta/y \in E_n$ has norm 1. Hilbert's Theorem 90 implies that there is some $\alpha \in \mathbb{K}_n^\times$ such that $\gamma = \alpha^{\omega_m}$.

We claim that $\alpha \notin \underline{E}_n$. Let $|\underline{E}_n/C_n| = p^s \cdot a$, with $(a,p) = 1$. Assuming $\alpha \in \underline{E}_n$, we would have $(\alpha^a)^{p^s} \in C_n$, so $\alpha^a \in E_n$. Since $m \geq n_0$, by (2.4) we have that $\gamma^a = (\alpha^a)^{\omega_m} \in C_n$. As $y \in C_n$, we obtain that $\delta^a \in C_n$ and since $(a,p) = 1$, this gives further that $\delta \in C_n$. But we chose $\delta \in E_m \setminus C_m$, so by Lemma 2.2, we get a contradiction. Thus α is not a unit.

We consider the factorization of the non-trivial fractional ideal $(\alpha) \subset \mathbb{K}_n$ and will show that (α) is the lift of some non-principal ideal class $a_m \in A_m$. By construction, $\alpha^{\omega_m} = \gamma \in E_n$, so the ideal (α) is invariant under $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$.

We first prove that we can discard π from the factorization of (α) into prime ideals, where π denotes the generator for the unique prime ideal of $\mathbb{K}_n$ lying above the rational prime p. Indeed, $\pi^{\omega_m} \in C_n$, so modifying (α) by some power of (π) does not change the class $d \in E_n/C_n$ of δ. We may thus assume that π is not among the primes occurring with positive or negative exponents in the factorization of (α).

Let $\mathfrak{Q}$ be a prime dividing (α) and let $\mathfrak{q} = \mathfrak{Q} \cap \mathbb{K}_m$. We know that all the primes above $\mathfrak{q}$ in $\mathbb{K}_n$ are conjugate under the action of $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$, so we can write

$$(\alpha) = \prod_j \mathfrak{Q}_j^{f_j(\omega_m)},$$

where $\mathfrak{Q}_j$ are primes in $\mathbb{K}_n$ and $f_j(\omega_m)$ are elements of $\mathbb{Z}[\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)]$. Since (α) is invariant under $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$, we have $N_{n,m}(\alpha) = (\alpha)^{p^{n-m}}$ and thus for each j, also $p^{n-m} \cdot f_j(\omega_m) = \mathrm{Tr}(f_j) \cdot N_{n,m}$, with $\mathrm{Tr}(f_j)$ denoting the sum of the coefficients of f_j. This implies that all coefficients of f_j are equal, so f_j is a multiple of the norm $N_{n,m}$ for all j. This means precisely that $(\alpha) = \iota_{m,n}(\mathfrak{a})$ for an ideal $\mathfrak{a}$ whose class is in A_m.

We now prove that the ideal $\mathfrak{a}$ cannot be principal in $\mathbb{K}_m$, unless $[\delta] = 1$, so $\delta \in C_m$. Assume that $\mathfrak{a} = (\alpha_m)$, for some $\alpha_m \in \mathbb{K}_m$; then $\alpha_m \mathfrak{O}(\mathbb{K}_n) = (\alpha)$, hence $\alpha = \alpha_m \cdot u$, for some $u \in \underline{E}_n$. But then $\alpha^{\omega_m} = \alpha_m^{\omega_m} \cdot u^{\omega_m}$ and since $\alpha_m \in \mathbb{K}_m$, it follows that $\alpha_m^{\omega_m} = 1$, hence $\gamma \in C_m$, and $d = 1$, as claimed.

Now let $a = [\mathfrak{a}]$ denote the class of $\mathfrak{a}$ in A_m and let $\mathfrak{b} \in a$ be a further ideal, so $\mathfrak{b} = (\beta) \cdot \mathfrak{a}$ for some $\beta \in \mathbb{K}_m^\times$. Then $\mathcal{O}(\mathbb{K}_n)\mathfrak{b} = (\alpha \cdot \beta)$ is an ideal which contains $\alpha\beta$; but $(\alpha\beta)^{\omega_m} = \alpha^{\omega_m} = \gamma$. We obtained a map $\psi : E_m/C_m \to P_{n,m}$ given by $\psi([\delta]) = [\mathfrak{a}]$. The ideals in $\mathfrak{X} \in \psi[\delta]$ share the property that the principal ideal $\mathcal{O}(\mathbb{K}_n)\mathfrak{X}$ contains some $\xi \in \mathcal{O}(\mathbb{K}_n)\mathfrak{X}$ such that $\xi^{\omega_m} \in [\delta]$. The class is well defined. Indeed, assume that there is some further class $Y \in A_m$ and an ideal $\mathfrak{Y} \in Y$ which capitulates in $\mathcal{O}(\mathbb{K}_n)$, and there is some $y \in \mathcal{O}(\mathbb{K}_n) \cdot \mathfrak{Y}$ with $y^{\omega_m} \in [\delta]$. Then $(\alpha/y)^{\omega_m} \in C_n \cap \mathrm{Ker}\ (N_{n,m} : C_n \to C_m)$. Recall that $C_n \cong \mathbb{Z}[G_n]/\left(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]\right)$ and $\mathbb{Z}[G_n] \cong \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$. Thus, an element $\eta \in \mathrm{Ker}\ (N_{n,m} : C_n \to C_m)$ can be written as

$$\eta = \eta_n^{\sum_{j=0}^{p-2} f_j(\tau)\otimes e_j} \qquad \text{and satisfies} \quad \eta^{\widehat{\nu_{n,m}}} = 1,$$

where $f_j \in \mathbb{Z}[\Gamma_n]$ and we keep the notations from Lemma 2.2.
From $C_n \cong \mathbb{Z}[G_n]/\left(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]\right)$, we obtain that $\eta^{\widehat{\nu_{n,m}}}$ must be in the ideal $N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]$. Therefore, there exists some $A = \sum_{j=0}^{p-2} \tilde{g}_j(\tau) \otimes e_j \in \mathbb{Z}[\Gamma_n] \otimes \mathbb{Z}[G_1]$ such that for each j, one has

$$\nu_{n,m} \cdot f_j(\tau) = g_j(\tau) \cdot \nu_{n,1},$$

with g_j explicitly computable in terms of $\tilde{g}_j$. Applying the same ideas as in the proof of Lemma 2.2, it follows that $\eta \in C_n^{\omega_m}$ and hence $\operatorname{Ker}(N_{n,m} : C_n \to C_m) = C_n^{\omega_m}$. Consequently, there is a unit $\varpi \in C_n$ such that $(\alpha/\varpi y)^{\omega_m} = 1$. Now $\operatorname{Ker}(\omega_m : \mathbb{K}_n^\times \to \mathbb{K}_n^\times) = \mathbb{K}_m^\times$, so we conclude that $\alpha = \varpi \cdot y \cdot z, z \in \mathbb{K}_m^\times$. This shows that $Y = a$, so the map is well defined. It is injective, since we have shown that its image $a = [\mathfrak{a}]$ is 1 if and only if $[\delta] = 1$.

We finally show that ψ is also compatible with the action of $\Lambda[G_1]$. It is linear, since for $c \in \mathbb{Z}_p$ we have the formal sequence of associations

$$\delta \mapsto \delta^c \Rightarrow \gamma \mapsto \gamma^c \Rightarrow (\alpha) \mapsto (\alpha)^c \Rightarrow [\mathfrak{a}] \mapsto [\mathfrak{a}]^c.$$

Likewise, for $g \in G_n$ we have the sequence:

$$\delta \mapsto g(\delta) \Rightarrow \gamma \mapsto g(\gamma) \Rightarrow (\alpha) \mapsto (g(\alpha)) \Rightarrow [\mathfrak{a}] \mapsto g([(\mathfrak{a}]),$$

so $\psi : E_m/C_m \to P_{m,n}$ is indeed an injective homomorphism of $\Lambda[G_1]$-modules, and since $|P_{m,n}| = |A_m| = |E_m/C_m|$, the map is also surjective, so it is an isomorphism. Moreover, $P_{m,n} \cong A_m$ as $\Lambda[G_1]$ - modules too, so we obtained an isomorphism $E_m/C_m \cong A_m$ as $\Lambda[G_1]$-modules, which completes the proof. □

Remark 3.1. One may note that the above result cannot be adapted to descend to levels which are lower than n_0. If we were able to do so, or if $n_0 = 1$, then we would obtain a weaker version of a famous conjecture due to Iwasawa and Leopoldt, which asserts that the p-part of the class group $\mathcal{C}(\mathbb{Q}[\zeta_p])^-$ is $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})]$-cyclic.

References

[1] Iwasawa, K., *On* $\mathbf{Z}_l$*-extensions of algebraic number fields*, Ann. of Math., **98** (1973), No. 2, 246–326
[2] Lang, S., *Cyclotomic fields I and II*, Springer-Verlag, 1990, GTM 121
[3] Matsumura, H., *Commutative Ring Theory*, Cambridge University Press, 1989
[4] Washington, Lawrence C., *Introduction to Cyclotomic fields, Second Edition*, Springer, 1997

Mathematisches Institut der Universität Göttingen
E-mail address: vlad.crisan@mathematik.uni-goettingen.de