

Perturbing Eisenstein polynomials over local fields

Kevin Keating
Department of Mathematics
University of Florida

May 25, 2017

Local Fields

Let K be a field which is complete with respect to a discrete valuation $v_K : K^\times \rightarrow \mathbb{Z}$, whose residue field \overline{K} is a perfect field of characteristic p . Also let

$$\begin{aligned}\mathcal{O}_K &= \{\alpha \in K : v_K(\alpha) \geq 0\} \\ &= \text{ring of integers of } K\end{aligned}$$

$$\pi_K = \text{uniformizer for } \mathcal{O}_K \text{ (i. e., } v_K(\pi_K) = 1)$$

$$\begin{aligned}\mathcal{P}_K &= \pi_K \cdot \mathcal{O}_K \\ &= \text{unique maximal ideal of } \mathcal{O}_K\end{aligned}$$

Let K^{sep} be a separable closure of K , and let L/K be a finite totally ramified subextension of K^{sep}/K . Write

$[L : K] = n = up^\nu$ with $p \nmid u$. Define $\bar{v}_p : \mathbb{Z} \rightarrow \mathbb{Z}$ by $\bar{v}_p(h) = \min\{v_p(h), \nu\}$.

Extensions and Power Series

Let $T \subset \mathcal{O}_K$ be the set of Teichmüller representatives for \overline{K} .
Let π_K, π_L be uniformizers for K, L , and let

$$\mathcal{G}(X) = a_0X^n + a_1X^{n+1} + a_2X^{n+2} + \dots$$

be the unique power series with coefficients in T such that $\pi_K = \mathcal{G}(\pi_L)$.

Suppose $\tilde{\pi}_L$ is another uniformizer for L . Let

$$\tilde{\mathcal{G}}(X) = \tilde{a}_0X^n + \tilde{a}_1X^{n+1} + \tilde{a}_2X^{n+2} + \dots$$

be the series with coefficients in T such that $\pi_K = \tilde{\mathcal{G}}(\tilde{\pi}_L)$.

Extensions and Powers Series, continued

Now assume that

$$\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{P}_L^{\ell+2}}$$

for some $\ell \geq 1$, $r \in T$.

Question: For which $i \geq 0$ do we know that $\tilde{a}_i = a_i$?

Write $\pi_L = \psi(\tilde{\pi}_L)$ with $\psi \in T[[X]]$. Then

$$\begin{aligned}\psi(X) &\equiv X - rX^{\ell+1} \pmod{X^{\ell+2}} \\ \pi_K &= \mathcal{G}(\pi_L) = \mathcal{G}(\psi(\tilde{\pi}_L)).\end{aligned}$$

Suppose $\text{char}(K) = p$. Then $T = \overline{K}$, so $\mathcal{G}(\psi(X)) \in T[[X]]$. It follows that $\tilde{\mathcal{G}}(X) = \mathcal{G}(\psi(X))$.

Extensions and Powers Series ($\text{char}(K) = p$)

Suppose $\bar{v}_p(h) = j$. Then $n + h = wp^j$ for some integer w .
Hence $\psi(X)^{n+h} \in \overline{K}[[X^{p^j}]]$ and

$$\begin{aligned}\psi(X)^{n+h} &\equiv (X - rX^{\ell+1})^{n+h} \pmod{X^{n+h+(\ell+1)p^j}} \\ &\equiv X^{n+h}((1 - rX^\ell)^{p^j})^w \pmod{X^{n+h+(\ell+1)p^j}} \\ &\equiv X^{n+h} - wr^{p^j} X^{n+h+\ell p^j} \pmod{X^{n+h+(\ell+1)p^j}}.\end{aligned}$$

It follows from the above that if $i < h + \ell p^{\bar{v}_p(h)}$ for all $h \geq 0$ such that $a_h \neq 0$ then $\tilde{a}_i = a_i$.

Furthermore, if $i \leq h + \ell p^{\bar{v}_p(h)}$ for all $h \geq 0$ such that $a_h \neq 0$ then we can express \tilde{a}_i as a polynomial in r with coefficients expressed in terms of $\{a_g : g \leq i\}$.

Indices of Inseparability (Fried, Heiermann)

Assume $\text{char}(K) = p$. For $0 \leq j \leq \nu$ define

$$i_j = \min\{h : h \geq 0, a_h \neq 0, \bar{v}_p(h) \leq j\}.$$

Then i_j does not depend on the choice of π_K or π_L . We say that i_j is the j th index of inseparability of L/K . We have $0 = i_\nu < i_{\nu-1} \leq \dots \leq i_1 \leq i_0$.

It follows from the above that if $i < i_j + \ell p^j$ for $0 \leq j \leq \bar{v}_p(i)$ then $\tilde{a}_i = a_i$.

For $0 \leq j \leq \nu$ define

$$\begin{aligned}\tilde{\phi}_j(x) &= i_j + p^j x \\ \phi_j(x) &= \min\{\tilde{\phi}_{j'}(x) : 0 \leq j' \leq j\}.\end{aligned}$$

Let $i \geq 0$ and set $\bar{v}_p(i) = j$. If $i < \phi_j(\ell)$ then $\tilde{a}_i = a_i$.

What if $\text{char}(K) = 0$?

Suppose $\text{char}(K) = 0$. For $0 \leq j \leq \nu$ define

$$i_j^{\pi_L} = \min\{h : h \geq 0, a_h \neq 0, \bar{v}_p(h) \leq j\}$$
$$i_j = \min\{i_{j'}^{\pi_L} + (j' - j)v_L(p) : j \leq j' \leq \nu\}.$$

Then $i_j^{\pi_L}$ may depend on the choice of π_L (but not on π_K), but i_j depends only on the extension L/K .

The functions $\tilde{\phi}_j$ and ϕ_j are defined as in the characteristic- p case. Once again, if $\bar{v}_p(i) = j$ and $i < \phi_j(\ell)$ then $\tilde{a}_i = a_i$.

Theorem (Fried, Heiermann): For $x \geq 0$ we have

$$\phi_{L/K}(x) = \frac{1}{n} \cdot \phi_\nu(x).$$

An Example

Let $K = \mathbb{F}_3((t))$ and let L/K be a totally ramified extension of degree 9. Suppose π_L is a uniformizer for L such that $t = \mathcal{G}(\pi_L)$ with

$$\mathcal{G}(X) = X^9 + X^{27} - X^{42} - X^{48} + X^{49} + \dots$$

Then

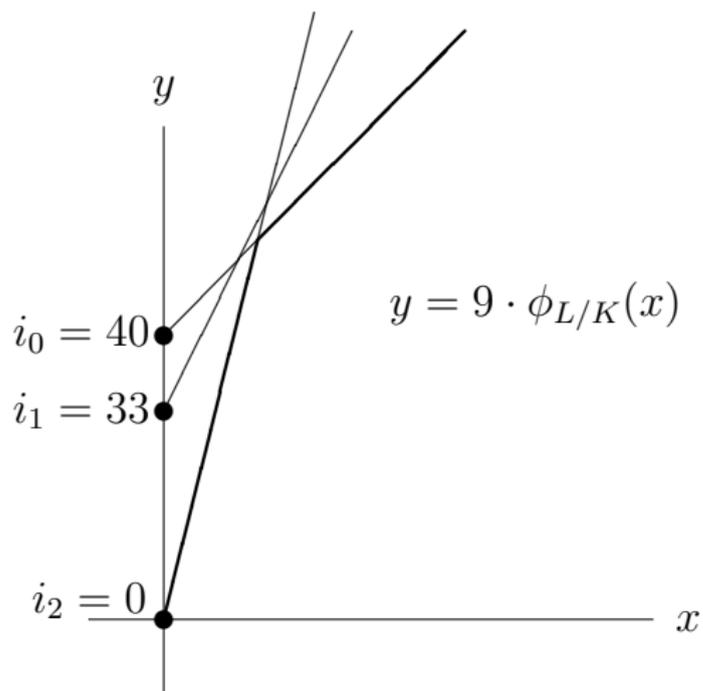
$$i_0 = 49 - 9 = 40$$

$$i_1 = 42 - 9 = 33$$

$$i_2 = 9 - 9 = 0.$$

The Hasse-Herbrand function for the example can be deduced from the indices of inseparability:

$\phi_{L/K}$ for the Example



Powers Series and Eisenstein Polynomials

Let π_L be a uniformizer for L and let

$$f(X) = X^n - c_1 X^{n-1} + \cdots + (-1)^{n-1} c_{n-1} X + (-1)^n c_n$$

be the minimum polynomial of π_L over K . Then $f(X)$ is the Weierstrass polynomial of the series $\mathcal{G}(X) - \pi_K$.

The series $\mathcal{G}(X) \in T[[X]]$ such that $\mathcal{G}(\pi_L) = \pi_K$ can be computed iteratively from $f(X)$ (using Newton's method if $\text{char}(K) = p$).

For every $i \geq n$, knowing $\mathcal{G}(X)$ modulo X^i is equivalent to knowing $c_{n-h} \pi_L^h$ modulo π_L^i for $1 \leq h \leq n$. (In fact, each of these is equivalent to knowing the \mathcal{O}_K -algebra $\mathcal{O}_L/\mathcal{P}_L^i$.)

Indices of Inseparability via Eisenstein Polynomials

Let π_L be a uniformizer for L , and let

$$f(X) = X^n - c_1 X^{n-1} + \cdots + (-1)^{n-1} c_{n-1} X + (-1)^n c_n$$

be the minimum polynomial for π_L over K .

For $0 \leq j \leq \nu$ we have

$$i_j^{\pi_L} = \min\{v_L(c_h \pi_L^{n-h}) : 0 \leq h < n, v_p(n-h) \leq j\} - n$$

$$i_j = \min\{i_{j'}^{\pi_L} + (j' - j)v_L(p) : j \leq j' \leq \nu\}.$$

The Problem

Let L/K be a finite separable totally ramified subextension of K^{sep}/K of degree $[L : K] = n$. Let π_L be a uniformizer for L and let

$$f(X) = X^n - c_1 X^{n-1} + \cdots + (-1)^{n-1} c_{n-1} X + (-1)^n c_n$$

be the minimum polynomial of π_L over K . Let $\ell \geq 1$, let $r \in \mathcal{O}_K$, and let $\tilde{\pi}_L$ be another uniformizer for L such that $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{P}_L^{\ell+2}}$. Let

$$\tilde{f}(X) = X^n - \tilde{c}_1 X^{n-1} + \cdots + (-1)^{n-1} \tilde{c}_{n-1} X + (-1)^n \tilde{c}_n$$

be the minimum polynomial of $\tilde{\pi}_L$ over K . We wish to obtain congruences for the coefficients \tilde{c}_i of $\tilde{f}(X)$ in terms of ℓ , r , and the coefficients of $f(X)$.

Krasner's Work

Krasner (1937) showed that for $1 \leq h \leq n$ we have

$$\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\kappa_h(\ell)}},$$

where $\kappa_h(\ell) = \lceil \varphi_{L/K}(\ell) + \frac{h}{n} \rceil$.

We prove that

$$\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$$

for certain integers $\rho_h(\ell)$ such that $\rho_h(\ell) \geq \kappa_h(\ell)$.

Let h be the unique integer such that $1 \leq h \leq n$ and n divides $n\varphi_{L/K}(\ell) + h$. Krasner gave a formula for the congruence class modulo $\mathcal{P}_K^{\kappa_h(\ell)+1}$ of $\tilde{c}_h - c_h$. We give similar formulas for up to $\nu + 1$ values of h .

A Theorem

Let $1 \leq h \leq n$ and set $j = \bar{v}_p(h)$. Define

$$\rho_h(\ell) = \left\lceil \frac{\varphi_j(\ell) + h}{n} \right\rceil.$$

Let $\pi_L, \tilde{\pi}_L$ be uniformizers for L and let

$$f(X) = X^n - c_1 X^{n-1} + \cdots + (-1)^{n-1} c_{n-1} X + (-1)^n c_n$$

$$\tilde{f}(X) = X^n - \tilde{c}_1 X^{n-1} + \cdots + (-1)^{n-1} \tilde{c}_{n-1} X + (-1)^n \tilde{c}_n$$

be the minimum polynomials for $\pi_L, \tilde{\pi}_L$ over K .

Theorem 1: Suppose $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^{\ell+1}}$ for some $\ell \geq 1$.

Then $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$ for $1 \leq h \leq n$.

Another Theorem

Theorem 2: For $0 \leq m \leq \nu$ write the m th index of inseparability of L/K in the form $i_m = A_m n - b_m$ with $1 \leq b_m \leq n$. Suppose there are $\ell \geq 1$ and $r \in \mathcal{O}_K$ with

$$\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{P}_L^{\ell+2}}.$$

Let $0 \leq j \leq \nu$ be such that $\bar{v}_p(\varphi_j(\ell)) = j$, and let h be the unique integer such that $1 \leq h \leq n$ and n divides $\varphi_j(\ell) + h$. Set $k = (\varphi_j(\ell) + h)/n$ and $h_0 = h/p^j$. Then

$$\tilde{c}_h \equiv c_h + \sum_{m \in S_j} g_m c_n^{k-A_m} c_{b_m} r^{p^m} \pmod{\mathcal{P}_K^{k+1}},$$

where ...

Theorem 2, continued

$$S_j = \{m : 0 \leq m \leq j, \varphi_j(\ell) = \tilde{\varphi}_m(\ell)\}$$

$$g_m = \begin{cases} (-1)^{k+\ell+A_m}(h_0 p^{j-m} + \ell - up^{\nu-m}) & \text{if } b_m < h \\ (-1)^{k+\ell+A_m}(h_0 p^{j-m} + \ell) & \text{if } h \leq b_m < n \\ (-1)^{k+\ell+A_m} up^{\nu-m} & \text{if } b_m = n. \end{cases}$$

An Example

Let K be a finite extension of the 3-adic field \mathbb{Q}_3 such that $v_K(3) \geq 2$. Let

$$f(X) = X^9 - c_1X^8 + \cdots + c_8X - c_9$$

be an Eisenstein polynomial over K such that $v_K(c_2) = v_K(c_6) = 2$, $v_K(c_h) \geq 2$ for $h \in \{1, 3\}$, and $v_K(c_h) \geq 3$ for $h \in \{4, 5, 7, 8\}$. Let π_L be a root of $f(X)$. Then $L = K(\pi_L)$ is a totally ramified extension of K of degree 9, so we have $u = 1$, $\nu = 2$. It follows from our assumptions about the valuations of the coefficients of $f(X)$ that the indices of inseparability of L/K are $i_0 = 16$, $i_1 = 12$, and $i_2 = 0$. Therefore $A_0 = 2$, $A_1 = 2$, $A_2 = 1$, and $b_0 = 2$, $b_1 = 6$, $b_2 = 9$. We get the following values for $\tilde{\varphi}_j(\ell)$ and $\varphi_j(\ell)$:

Example (Theorem 1)

l	$\tilde{\varphi}_0(l)$	$\tilde{\varphi}_1(l)$	$\tilde{\varphi}_2(l)$	$\varphi_0(l)$	$\varphi_1(l)$	$\varphi_2(l)$
0	16	12	0	16	12	0
1	17	15	9	17	15	9
2	18	18	18	18	18	18
3	19	21	27	19	19	19

Now let $\tilde{\pi}_L$ be another uniformizer for L , with minimum polynomial

$$\tilde{f}(X) = X^9 - \tilde{c}_1 X^8 + \cdots + \tilde{c}_8 X - \tilde{c}_9.$$

Suppose $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^2}$. Then by Theorem 1 and the table above we get

$$\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^2} \text{ for } h \in \{1, 3, 9\},$$

$$\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^3} \text{ for } h \in \{2, 4, 5, 6, 7, 8\}.$$

Example (Theorem 2)

Suppose $\tilde{\pi}_L \equiv \pi_L + r\pi_L^2 \pmod{\mathcal{P}_L^3}$, with $r \in \mathcal{O}_K$. By the table above we get $\bar{v}_3(\varphi_0(1)) = 0$, $\bar{v}_3(\varphi_1(1)) = 1$, $\bar{v}_3(\varphi_2(1)) = 2$ and $S_0 = \{0\}$, $S_1 = \{1\}$, $S_2 = \{2\}$. The corresponding values of h are 1, 3, 9, so we have $h_0 = 1$, $k = 2$ in all three cases.

By applying Theorem 2 with $\ell = 1$, $j = 0, 1, 2$ we get the following congruences:

$$\begin{aligned}\tilde{c}_1 &\equiv c_1 + (-1)^{2+1+2}(1+1)c_2r \pmod{\mathcal{P}_K^3} \\ &\equiv c_1 - 2c_2r \pmod{\mathcal{P}_K^3} \\ \tilde{c}_3 &\equiv c_3 + (-1)^{2+1+2}(1+1)c_6r^3 \pmod{\mathcal{P}_K^3} \\ &\equiv c_3 - 2c_6r^3 \pmod{\mathcal{P}_K^3} \\ \tilde{c}_9 &\equiv c_9 + (-1)^{2+1+1}c_9^2r^9 \pmod{\mathcal{P}_K^3} \\ &\equiv c_9 + c_9^2r^9 \pmod{\mathcal{P}_K^3}.\end{aligned}$$

Symmetric Polynomials and Extensions

For $1 \leq h \leq n$ let

$$e_h(X_1, \dots, X_n) = \sum_{1 \leq t_1 < \dots < t_h \leq n} X_{t_1} X_{t_2} \dots X_{t_h}$$

be the h th elementary symmetric polynomial in n variables.

Define $E_h : L \rightarrow K$ by $E_h(\alpha) = e_h(\sigma_1(\alpha), \dots, \sigma_n(\alpha))$, where $\sigma_1, \dots, \sigma_n$ are the K -embeddings of L into K^{sep} . Then

$$e_1(X_1, \dots, X_n) = X_1 + \dots + X_n \Rightarrow E_1(\alpha) = \text{Tr}_{L/K}(\alpha)$$

$$e_n(X_1, \dots, X_n) = X_1 X_2 \dots X_n \Rightarrow E_n(\alpha) = \text{N}_{L/K}(\alpha)$$

Suppose $L = K(\alpha)$ and $f_\alpha(X) = X^n + \sum_{h=1}^n (-1)^h b_h X^{n-h}$ is the minimum polynomial for α over K . Then $E_h(\alpha) = b_h$.

Monomial Symmetric Polynomials

Let $\mu = (\mu_1, \dots, \mu_h)$ be a partition of some positive integer w into $h \leq n$ parts.

View μ as a multiset, and let μ' be the sum of μ with the multiset consisting of $n - h$ copies of 0.

The monomial symmetric polynomial in n variables associated to μ is

$$m_{\mu}(X_1, \dots, X_n) = \sum_{\omega} X_1^{\omega_1} X_2^{\omega_2} \dots X_n^{\omega_n},$$

where the sum is taken over all distinct permutations $\omega = (\omega_1, \dots, \omega_n)$ of μ' .

For $\alpha \in L$ set $M_{\mu}(\alpha) = m_{\mu}(\sigma_1(\alpha), \dots, \sigma_n(\alpha)) \in K$.

Monomial and Elementary Symmetric Polynomials

An element $\alpha \in \mathcal{P}_L$ can be expressed in the form

$$\alpha = r_1 \pi_L + r_2 \pi_L^2 + \cdots \text{ with } r_i \in \mathcal{O}_K.$$

Therefore if $z \in E_h(\mathcal{P}_L)$ then z is a sum of terms of the form $r_{\mu_1} r_{\mu_2} \cdots r_{\mu_h} M_{\mu}(\pi_L)$, where $\mu = (\mu_1, \dots, \mu_h)$ is a partition with h parts.

$m_{\mu}(X_1, \dots, X_n)$ can be expressed as a polynomial in e_1, e_2, \dots, e_n :

$$m_{\mu} = \sum_{\lambda} d_{\lambda\mu} \cdot e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_k},$$

where $d_{\lambda\mu} \in \mathbb{Z}$ and the sum is taken over all partitions $\lambda = (\lambda_1, \dots, \lambda_k)$ of $w := \mu_1 + \cdots + \mu_h$ such that $\lambda_i \leq n$.

$$\text{Hence } M_{\mu}(\pi_L) = \sum_{\lambda} d_{\lambda\mu} \cdot c_{\lambda_1} c_{\lambda_2} \cdots c_{\lambda_k}.$$

Two Lemmas

For a partition $\lambda = \{\lambda_1, \dots, \lambda_k\}$ whose parts are $\leq n$ define $c_\lambda = c_{\lambda_1} c_{\lambda_2} \dots c_{\lambda_k}$.

Lemma 1: Let $w \geq 1$ and let $\lambda = \{\lambda_1, \dots, \lambda_k\}$ be a partition of w whose parts satisfy $1 \leq \lambda_i \leq n$. Choose q to minimize $\bar{v}_p(\lambda_q)$ and set $t = \bar{v}_p(\lambda_q)$. Then $v_L(c_\lambda) \geq i_t^{\pi_L} + w$.

Let $w \geq 1$ and let λ be partition of w . For $k \geq 1$ let $k * \lambda$ be the partition of kw which is the multiset sum of k copies of λ , and let $k \cdot \lambda$ be the partition of kw obtained by multiplying the parts of λ by k .

Lemma 2: Let $t \geq j \geq 0$, let $w' \geq 1$, and set $w = w'p^t$. Let λ' be a partition of w' and set $\lambda = p^t \cdot \lambda'$. Let μ be a partition of w such that there does not exist a partition μ' with $\mu = p^{j+1} * \mu'$. Then p^{t-j} divides $d_{\lambda\mu}$.

Proving Theorem 1

Assume $\tilde{\pi}_L = \pi_L + r\pi_L^{\ell+1}$, with $r \in \mathcal{O}_K$. Let $1 \leq h \leq n$ and set $j = \bar{v}_p(h)$. For $0 \leq s \leq h$ let μ_s be the partition of $\ell s + h$ consisting of $h - s$ copies of 1 and s copies of $\ell + 1$. Then

$$\tilde{c}_h = E_h(\tilde{\pi}_L) = \sum_{s=0}^h M_{\mu_s}(\pi_L) r^s = c_h + \sum_{s=1}^h M_{\mu_s}(\pi_L) r^s.$$

To prove that $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$ it's enough to show that $v_K(M_{\mu_s}(\pi_L)) \geq \rho_h(\ell)$ for $1 \leq s \leq h$.

For this it suffices to show that $v_L(d_{\lambda\mu_s} c_\lambda) \geq \varphi_j(\ell) + h$ for all $1 \leq s \leq h$ and all partitions λ of $\ell s + h$ whose parts are $\leq n$.

Proving Theorem 1, continued

Let $1 \leq s \leq h$, set $j = \bar{v}_p(h)$, and set $m = \min\{j, \bar{v}_p(s)\}$. Then $m \leq j$ and $s \geq p^m$. Let $\lambda = \{\lambda_1, \dots, \lambda_k\}$ be a partition of $\ell s + h$ such that $1 \leq \lambda_i \leq n$ for $1 \leq i \leq k$. Choose q to minimize $\bar{v}_p(\lambda_q)$ and set $t = \bar{v}_p(\lambda_q)$. By Lemma 1 we get $v_L(c_\lambda) \geq i_t^{\pi_L} + \ell s + h$.

Suppose $m < t$. Then $m < \nu$, so we have $p^{m+1} \nmid \gcd(h-s, s)$. It follows from Lemma 2 that $v_p(d_{\lambda\mu_s}) \geq t - m$. Thus

$$\begin{aligned} v_L(d_{\lambda\mu_s} c_\lambda) &= v_L(d_{\lambda\mu_s}) + v_L(c_\lambda) \\ &\geq (t - m)v_L(p) + i_t^{\pi_L} + \ell s + h \\ &\geq i_m + \ell p^m + h. \end{aligned}$$

Proving Theorem 1, conclusion

Suppose $m \geq t$. Then

$$\begin{aligned}v_L(d_{\lambda\mu_s}c_\lambda) &\geq v_L(c_\lambda) \\ &\geq i_t^{\pi_L} + \ell s + h \\ &\geq i_t + \ell p^m + h \\ &\geq i_m + \ell p^m + h.\end{aligned}$$

In both cases we get

$$v_L(d_{\lambda\mu_s}c_\lambda) \geq \tilde{\varphi}_m(\ell) + h \geq \varphi_j(\ell) + h,$$

and hence $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$.