Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Kevin KEATING

Extensions of local fields and elementary symmetric polynomials

Tome 30, n^{o} 2 (2018), p. 431-448.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_431_0>

Journal de Théorie des Nombres
de Bordeaux **30** (2018), 431–448

Extensions of local fields and elementary symmetric polynomials

par Kevin KEATING

Résumé. Soit K un corps local de caractéristique résiduelle p et soit L/K une extension séparable finie totalement ramifiée de degré n. Soient $\sigma_1, \ldots, \sigma_n$ les K-plongements de L dans une clôture séparable de K. Pour tout $1 \leq h \leq n$, soit $e_h(X_1, \ldots, X_n)$ le polynôme symétrique élémentaire en n variables de degré h, et pour tout $\alpha \in L$, soit $E_h(\alpha) = E_h(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$. Soit $\mathcal{P}_K$ l'idéal maximal de l'anneau des entiers de K et soit $j = \min\{v_p(h), v_p(n)\}$. Nous montrons que $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{\lceil (i_j+hr)/n \rceil}$ pour tout $r \in \mathbb{Z}$, où i_j est l'indice d'inséparabilité d'ordre j de l'extension L/K. Dans certains cas, nous montrons également que $E_h(\mathcal{P}_L^r)$ n'est contenu dans aucune puissance supérieure de $\mathcal{P}_K$.

Abstract. Let K be a local field whose residue field has characteristic p and let L/K be a finite separable totally ramified extension of degree n. Let $\sigma_1, \ldots, \sigma_n$ denote the K-embeddings of L into a separable closure of K. For $1 \leq h \leq n$ let $e_h(X_1, \ldots, X_n)$ denote the hth elementary symmetric polynomial in n variables, and for $\alpha \in L$ set $E_h(\alpha) = e_h(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$. Let $\mathcal{P}_K$ be the maximal ideal of the ring of integers of K and let $j = \min\{v_p(h), v_p(n)\}$. We show that for $r \in \mathbb{Z}$ we have $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{\lceil (i_j+hr)/n \rceil}$, where i_j is the jth index of inseparability of L/K. In certain cases we also show that $E_h(\mathcal{P}_L^r)$ is not contained in any higher power of $\mathcal{P}_K$.

1. The problem

Let K be a field which is complete with respect to a discrete valuation v_K. Let $\mathcal{O}_K$ be the ring of integers of K and let $\mathcal{P}_K$ be the maximal ideal of $\mathcal{O}_K$. Assume that the residue field $\overline{K} = \mathcal{O}_K/\mathcal{P}_K$ of K is a perfect field of characteristic p. Let K^{sep} be a separable closure of K, and let L/K be a finite totally ramified subextension of K^{sep}/K of degree $n = up^\nu$, with $p \nmid u$. Let $\sigma_1, \ldots, \sigma_n$ denote the K-embeddings of L into K^{sep}. For $1 \leq h \leq n$ let $e_h(X_1, \ldots, X_n)$ denote the hth elementary symmetric polynomial in n variables, and define $E_h : L \to K$ by setting $E_h(\alpha) = e_h(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$

Manuscrit reçu le 26 août 2016, révisé le 9 juin 2017, accepté le 16 juin 2017.
2010 *Mathematics Subject Classification.* 11S15, 11S05.
Mots-clefs. local fields, symmetric polynomials, norm, trace, indices of inseparability, digraphs.

for $\alpha \in L$. We are interested in the relation between $v_L(\alpha)$ and $v_K(E_h(\alpha))$. In particular, for $r \in \mathbb{Z}$ we would like to compute the value of

$$g_h(r) = \min\{v_K(E_h(\alpha)) : \alpha \in \mathcal{P}_L^r\}.$$

The following proposition shows that $g_h(r)$ is a well-defined integer:

Proposition 1.1. *Let L/K be a totally ramified extension of degree n. Let $r \in \mathbb{Z}$ and let h satisfy $1 \le h \le n$. Then $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{\lceil hr/n \rceil}$ and $E_h(\mathcal{P}_L^r) \neq \{0\}$.*

Proof. For the first claim we observe that if $\alpha \in \mathcal{P}_L^r$ then $v_L(E_h(\alpha)) \ge hr$, and hence $v_K(E_h(\alpha)) \ge hr/n$. To prove the second claim 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. By Krasner's lemma [6] there is $D > 1$ with the following property: For every Eisenstein polynomial

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

in $\mathcal{O}_K[X]$ such that $\tilde{c}_i \equiv c_i \pmod{\mathcal{P}_K^D}$ for $1 \le i \le n$, there is a root $\tilde{\pi}_L$ of $\tilde{f}(X)$ in K^{sep} such that $K(\tilde{\pi}_L) = K(\pi_L) = L$. By choosing $\tilde{c}_h$ to be nonzero we get a uniformizer $\tilde{\pi}_L$ for L such that $E_h(\tilde{\pi}_L) = \tilde{c}_h \neq 0$. Let π_K be a uniformizer for K. Then for t sufficiently large we have $\pi_K^t \tilde{\pi}_L \in \mathcal{P}_L^r$ and

$$E_h(\pi_K^t \tilde{\pi}_L) = \pi_K^{ht} E_h(\tilde{\pi}_L) = \pi_K^{ht} \tilde{c}_h \neq 0.$$

Therefore $E_h(\mathcal{P}_L^r) \neq \{0\}$. ☐

Since L/K is totally ramified, for $\alpha \in L$ we have

$$v_K(E_n(\alpha)) = v_K(\mathrm{N}_{L/K}(\alpha)) = v_L(\alpha).$$

Therefore $g_n(r) = r$ for $r \in \mathbb{Z}$. The map $E_1 = \mathrm{Tr}_{L/K}$ is also well-understood, at least when L/K is a Galois extension of degree p (see [8, V §3, Lem. 4] or [1, III, Prop. 1.4]).

Proposition 1.2. *Let L/K be a totally ramified extension of degree n and let $\mathcal{P}_L^d$ be the different of L/K. Then for every $r \in \mathbb{Z}$ we have $E_1(\mathcal{P}_L^r) = \mathcal{P}_K^{\lfloor (d+r)/n \rfloor}$. Therefore $g_1(r) = \lfloor (d+r)/n \rfloor$.*

Proof. Since $E_1(\mathcal{P}_L^r)$ is a nonzero fractional ideal of K we have $E_1(\mathcal{P}_L^r) = \mathcal{P}_K^s$ for some $s \in \mathbb{Z}$. By Proposition 7 in [8, III §3] we have

$$\mathcal{P}_L^{d+r} \subset \mathcal{O}_L \cdot \mathcal{P}_K^s = \mathcal{P}_L^{ns}$$
$$\mathcal{P}_L^{d+r} \not\subset \mathcal{O}_L \cdot \mathcal{P}_K^{s+1} = \mathcal{P}_L^{n(s+1)}.$$

It follows that $ns \le d + r < n(s+1)$, and hence that $s = \lfloor (d+r)/n \rfloor$. ☐

In this paper we determine a lower bound for $g_h(r)$ which depends on the indices of inseparability of L/K. When $h = p^j$ with $0 \leq j \leq \nu$ and $\overline{K}$ is large enough we show that $g_h(r)$ is equal to this lower bound. This leads to a formula for $g_{p^j}(r)$ which can be expressed in terms of a generalization of the different of L/K (see Remark 5.4).

In Sections 2 and 3 we prove some preliminary results involving symmetric polynomials. The main focus is on expressing monomial symmetric polynomials in terms of elementary symmetric polynomials. In Section 4 we prove our lower bound for $g_h(r)$. In Section 5 we show that $g_h(r)$ is equal to this lower bound in some special cases.

The author thanks the referee for suggesting improvements to the proofs of Propositions 1.1 and 3.3.

2. Symmetric polynomials and cycle digraphs

Let $n \geq 1$, let $w \geq 1$, and let $\boldsymbol{\lambda}$ be a partition of w. We view $\boldsymbol{\lambda}$ as a multiset of positive integers such that the sum $\Sigma(\boldsymbol{\lambda})$ of the elements of $\boldsymbol{\lambda}$ is equal to w. The number of parts of $\boldsymbol{\lambda}$ is called the length of $\boldsymbol{\lambda}$, and is denoted by $|\boldsymbol{\lambda}|$. For $k \geq 1$ we let $k * \boldsymbol{\lambda}$ be the partition of kw which is the multiset sum of k copies of $\boldsymbol{\lambda}$, and we let $k \cdot \boldsymbol{\lambda}$ be the partition of kw obtained by multiplying the parts of $\boldsymbol{\lambda}$ by k. If $|\boldsymbol{\lambda}| \leq n$ let $m_{\boldsymbol{\lambda}}(X_1, \ldots, X_n)$ be the monomial symmetric polynomial in n variables associated to $\boldsymbol{\lambda}$, as defined for instance in Section 7.3 of [9]. For $1 \leq h \leq n$ let $e_h(X_1, \ldots, X_n)$ denote the hth elementary symmetric polynomial in n variables.

Let $r \geq 1$ and let $\phi(X) = a_r X^r + a_{r+1} X^{r+1} + \cdots$ be a power series with generic coefficients a_i. Let $1 \leq h \leq n$ and let $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_h\}$ be a partition with h parts, all of which are $\geq r$. Then for every sequence $t_1, \ldots, t_h$ consisting of h distinct elements of $\{1, \ldots, n\}$, the coefficient of $X_{t_1}^{\mu_1} X_{t_2}^{\mu_2} \ldots X_{t_h}^{\mu_h}$ in $e_h(\phi(X_1), \ldots, \phi(X_n))$ is equal to $a_{\boldsymbol{\mu}} := a_{\mu_1} a_{\mu_2} \ldots a_{\mu_h}$. It follows that

$$e_h(\phi(X_1), \ldots, \phi(X_n)) = \sum_{\boldsymbol{\mu}} a_{\boldsymbol{\mu}} m_{\boldsymbol{\mu}}(X_1, \ldots, X_n), \tag{2.1}$$

where the sum ranges over all partitions $\boldsymbol{\mu}$ with h parts, all of which are $\geq r$. By the fundamental theorem of symmetric polynomials there is $\psi_{\boldsymbol{\mu}} \in \mathbb{Z}[X_1, \ldots, X_n]$ such that $m_{\boldsymbol{\mu}} = \psi_{\boldsymbol{\mu}}(e_1, \ldots, e_n)$. In this section we use a theorem of Kulikauskas and Remmel [7] to compute some of the coefficients of $\psi_{\boldsymbol{\mu}}$.

The formula of Kulikauskas and Remmel can be expressed in terms of tilings of a certain type of digraph. We say that a directed graph Γ is a cycle digraph if it is a disjoint union of finitely many directed cycles of length ≥ 1. We denote the vertex set of Γ by $V(\Gamma)$, and we define the sign of Γ to be $\mathrm{sgn}(\Gamma) = (-1)^{w-c}$, where $w = |V(\Gamma)|$ and c is the number of cycles that make up Γ.

Let Γ be a cycle digraph with $w \geq 1$ vertices and let $\boldsymbol{\lambda}$ be a partition of w. A $\boldsymbol{\lambda}$-tiling of Γ is a set S of subgraphs of Γ such that:

(1) Each $\gamma \in S$ is a directed path of length ≥ 0.
(2) The collection $\{V(\gamma) : \gamma \in S\}$ forms a partition of the set $V(\Gamma)$.
(3) The multiset $\{|V(\gamma)| : \gamma \in S\}$ is equal to $\boldsymbol{\lambda}$.

Let $\boldsymbol{\mu}$ be another partition of w. A $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling of Γ is an ordered pair (S, T), where S is a $\boldsymbol{\lambda}$-tiling of Γ and T is a $\boldsymbol{\mu}$-tiling of Γ. Let Γ' be another cycle digraph with w vertices and let (S', T') be a $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling of Γ'. An isomorphism from (Γ, S, T) to (Γ', S', T') is an isomorphism of digraphs $\theta : \Gamma \to \Gamma'$ which carries S onto S' and T onto T'. Say that the $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tilings (S, T) and (S', T') of Γ are isomorphic if there exists an isomorphism from (Γ, S, T) to (Γ, S', T'). Say that (S, T) is an admissible $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling of Γ if (Γ, S, T) has no nontrivial automorphisms. Let $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma)$ denote the number of isomorphism classes of admissible $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tilings of Γ.

Let $w \geq 1$ and let $\boldsymbol{\lambda}, \boldsymbol{\mu}$ be partitions of w. Set

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{|\boldsymbol{\lambda}|+|\boldsymbol{\mu}|} \cdot \sum_{\Gamma} \mathrm{sgn}(\Gamma)\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma), \tag{2.2}$$

where the sum is over all isomorphism classes of cycle digraphs Γ with w vertices. Since $\eta_{\boldsymbol{\mu}\boldsymbol{\lambda}} = \eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ we have $d_{\boldsymbol{\mu}\boldsymbol{\lambda}} = d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$. Kulikauskas and Remmel [7, Thm. 1 (ii)] proved the following:

Theorem 2.1. *Let $n \geq 1$, let $w \geq 1$, and let $\boldsymbol{\mu}$ be a partition of w with at most n parts. Let $\psi_{\boldsymbol{\mu}}$ be the unique element of $\mathbb{Z}[X_1, \ldots, X_n]$ such that $m_{\boldsymbol{\mu}} = \psi_{\boldsymbol{\mu}}(e_1, \ldots, e_n)$. Then*

$$\psi_{\boldsymbol{\mu}}(X_1, \ldots, X_n) = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda}\boldsymbol{\mu}} \cdot X_{\lambda_1} X_{\lambda_2} \ldots X_{\lambda_k},$$

where the sum is over all partitions $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ of w such that $\lambda_i \leq n$ for $1 \leq i \leq k$.

The remainder of this section is devoted to computing the values of $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma)$ and $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ in some special cases.

Proposition 2.2. *Let $w \geq 1$, let $\boldsymbol{\lambda}, \boldsymbol{\mu}$ be partitions of w, and let Γ be a directed cycle of length w. Assume that Γ has a $\boldsymbol{\lambda}$-tiling S which is unique up to isomorphism, and that $\mathrm{Aut}(\Gamma, S)$ is trivial. Similarly, assume that Γ has a $\boldsymbol{\mu}$-tiling T which is unique up to isomorphism, and that $\mathrm{Aut}(\Gamma, T)$ is trivial. Then $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = w$.*

Proof. For $0 \leq i < w$ let S_i be the rotation of S by i steps. Then the isomorphism classes of $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tilings of Γ are represented by (S_i, T) for $0 \leq i < w$. Since $\mathrm{Aut}(\Gamma, T)$ is trivial, all these tilings are admissible. $\square$

Proposition 2.3. *Let a, b, c, ℓ, m, w be positive integers such that $\ell a = mb + c = w$ and $b \neq c$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of ℓ copies of a, let $\boldsymbol{\mu}$ be the partition of w consisting of m copies of b and 1 copy of c, and let Γ be a directed cycle of length w. Then $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = a$.*

Proof. The cycle digraph Γ has a $\boldsymbol{\lambda}$-tiling S which is unique up to isomorphism, and a $\boldsymbol{\mu}$-tiling T which is unique up to isomorphism. For $0 \leq i < a$ let S_i be the rotation of S by i steps. Then the isomorphism classes of $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tilings of Γ are represented by (S_i, T) for $0 \leq i < a$. Since $\operatorname{Aut}(\Gamma, T)$ is trivial, all these tilings are admissible. □

Proposition 2.4. *Let b, c, m, w be positive integers such that $mb + c = w$ and $b \neq c$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of 1 copy of w and let $\boldsymbol{\mu}$ be the partition of w consisting of m copies of b and 1 copy of c. Then $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{w+m+1}w$.*

Proof. If the cycle digraph Γ has a $\boldsymbol{\lambda}$-tiling then Γ consists of a single cycle of length w. Hence by (2.2) we get $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{w+m+1}\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma)$. It follows from Proposition 2.3 that $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = w$. Therefore $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{w+m+1}w$. □

Proposition 2.5. *Let a, b, ℓ, m, w be positive integers such that $\ell a = mb = w$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of ℓ copies of a, let $\boldsymbol{\mu}$ be the partition of w consisting of m copies of b, and let Γ be a directed cycle of length w.*

(1) *The number of isomorphism classes of $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tilings of Γ is* $\gcd(a, b)$.
(2) *Let (S, T) be a $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling of Γ. Then the order of* $\operatorname{Aut}(\Gamma, S, T)$ *is* $\gcd(\ell, m)$.

Proof. (1) Identify $V(\Gamma)$ with $\mathbb{Z}/w\mathbb{Z}$ and consider the translation action of $b\mathbb{Z}/w\mathbb{Z}$ on $(\mathbb{Z}/w\mathbb{Z})/(a\mathbb{Z}/w\mathbb{Z})$. The isomorphism classes of $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tilings of Γ correspond to the orbits of this action, and these orbits correspond to cosets of $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b) \cdot \mathbb{Z}$ in $\mathbb{Z}$.

(2) The automorphisms of (Γ, S, T) are rotations of Γ by k steps, where k is a multiple of both a and b. Hence the number of automorphisms is $w/\operatorname{lcm}(a, b)$, which is easily seen to be equal to $\gcd(\ell, m)$. □

The following proposition generalizes the second part of [7, Thm. 6].

Proposition 2.6. *Let a, b, ℓ, m, w be positive integers such that $\ell a = mb = w$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of ℓ copies of a and let $\boldsymbol{\mu}$ be the partition of w consisting of m copies of b. Set $u = \gcd(a, b)$ and $v = \gcd(\ell, m)$. Then $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{w-v+\ell+m}\binom{u}{v}$. In particular, if $u < v$ then $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = 0$.*

Proof. Set $i = a/u$ and $j = b/u$. Then $m = vi$ and $\ell = vj$. Let Γ be a cycle digraph which has an admissible $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling, and let Γ_0 be one of the cycles which make up Γ. Then the length of Γ_0 is divisible by $\operatorname{lcm}(a, b) = uij$.

Suppose Γ_0 has length $k\cdot uij$. Let $\boldsymbol{\lambda}_0$ be the partition of $kuij$ consisting of kj copies of $a=ui$, and let $\boldsymbol{\mu}_0$ be the partition of $kuij$ consisting of ki copies of $b=uj$. Then by Proposition 2.5 (2) every $(\boldsymbol{\lambda}_0,\boldsymbol{\mu}_0)$-tiling of Γ_0 has automorphism group of order $\gcd(ki,kj)=k$. Since Γ has an admissible $(\boldsymbol{\lambda},\boldsymbol{\mu})$-tiling we must have $k=1$. Therefore Γ consists of v cycles, each of length uij. By Proposition 2.5 (1) the number of isomorphism classes of $(\boldsymbol{\lambda}_0,\boldsymbol{\mu}_0)$-tilings of a uij-cycle Γ_0 is $\gcd(a,b)=u$. An admissible $(\boldsymbol{\lambda},\boldsymbol{\mu})$-tiling of Γ consists of v nonisomorphic $(\boldsymbol{\lambda}_0,\boldsymbol{\mu}_0)$-tilings of uij-cycles. Hence the number of isomorphism classes of admissible $(\boldsymbol{\lambda},\boldsymbol{\mu})$-tilings of Γ is $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma)=\binom{u}{v}$. Hence by (2.2) we get $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}=(-1)^{w-v+\ell+m}\binom{u}{v}$. $\square$

3. Some subrings of $\mathbb{Z}[X_1,\dots,X_n]$

Let $n\geq 1$. In some cases we can get information about the coefficients $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ which appear in the formula for $\psi_{\boldsymbol{\mu}}$ given in Theorem 2.1 by working directly with the ring $\mathbb{Z}[X_1,\dots,X_n]$. In this section we define a family of subrings of $\mathbb{Z}[X_1,\dots,X_n]$. We then study the p-adic properties of the coefficients $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ by showing that for certain partitions $\boldsymbol{\mu}$ the polynomial $\psi_{\boldsymbol{\mu}}$ is an element of one of these subrings.

For $k\geq 0$ define a subring R_k of $\mathbb{Z}[X_1,\dots,X_n]$ by

$$R_k=\mathbb{Z}[X_1^{p^k},\dots,X_n^{p^k}]+p\mathbb{Z}[X_1^{p^{k-1}},\dots,X_n^{p^{k-1}}]+\dots+p^k\mathbb{Z}[X_1,\dots,X_n].$$

We can characterize R_k as the set of $F\in\mathbb{Z}[X_1,\dots,X_n]$ such that for $1\leq i\leq k$ there exists $F_i\in\mathbb{Z}[X_1,\dots,X_n]$ such that

$$F(X_1,\dots,X_n)\equiv F_i(X_1^{p^i},\dots,X_n^{p^i}) \pmod{p^{k+1-i}}. \tag{3.1}$$

Lemma 3.1. *Let $k,\ell\geq 0$ and let $F\in R_k$. Then $p^\ell F\in R_{k+\ell}$ and $F^{p^\ell}\in R_{k+\ell}$.*

Proof. The first claim is clear. To prove the second claim with $\ell=1$ we note that for $1\leq i\leq k$ it follows from (3.1) that

$$F(X_1,\dots,X_n)^p\equiv F_i(X_1^{p^i},\dots,X_n^{p^i})^p \pmod{p^{k+2-i}}.$$

In particular, the case $i=k$ gives

$$\begin{aligned}F(X_1,\dots,X_n)^p&\equiv F_k(X_1^{p^k},\dots,X_n^{p^k})^p &&\pmod{p^2}\\ &\equiv F_k(X_1^{p^{k+1}},\dots,X_n^{p^{k+1}}) &&\pmod{p}.\end{aligned}$$

It follows that $F^p\in R_{k+1}$. By induction we get $F^{p^\ell}\in R_{k+\ell}$ for $\ell\geq 0$. $\square$

Lemma 3.2. *Let $k,\ell\geq 0$ and let $F\in R_k$. Then for any $\psi_1,\dots,\psi_n\in R_\ell$ we have $F(\psi_1,\dots,\psi_n)\in R_{k+\ell}$.*

Proof. Since $F \in R_k$ we have

$$F(X_1, \dots, X_n) = \sum_{i=0}^{k} p^{k-i} \phi_i(X_1^{p^i}, \dots, X_n^{p^i})$$

for some $\phi_i \in \mathbb{Z}[X_1, \dots, X_n]$. Since $\psi_j \in R_\ell$, by Lemma 3.1 we get $\psi_j^{p^i} \in R_{i+\ell}$. Since $R_{i+\ell}$ is a subring of $\mathbb{Z}[X_1, \dots, X_n]$ it follows that $\phi_i(\psi_1^{p^i}, \dots, \psi_n^{p^i}) \in R_{i+\ell}$. By Lemma 3.1 we get $p^{k-i}\phi_i(\psi_1^{p^i}, \dots, \psi_n^{p^i}) \in R_{k+\ell}$. We conclude that $F(\psi_1, \dots, \psi_n) \in R_{k+\ell}$. □

Proposition 3.3. *Let $w \geq 1$ and let $\boldsymbol{\lambda}$ be a partition of w with at most n parts. For $j \geq 0$ let $\boldsymbol{\lambda}^j = p^j \cdot \boldsymbol{\lambda}$. Then $\psi_{\boldsymbol{\lambda}^j} \in R_j$.*

Proof. We use induction on j. The case $j = 0$ is trivial. Let $j \geq 0$ and assume that $\psi_{\boldsymbol{\lambda}^j} \in R_j$. Since $\boldsymbol{\lambda}^{j+1} = p \cdot \boldsymbol{\lambda}^j$ we get

$$\begin{aligned} m_{\boldsymbol{\lambda}^{j+1}}(X_1, \dots, X_n) &= m_{\boldsymbol{\lambda}^j}(X_1^p, \dots, X_n^p) \\ &= \psi_{\boldsymbol{\lambda}^j}(e_1(X_1^p, \dots, X_n^p), \dots, e_n(X_1^p, \dots, X_n^p)). \end{aligned}$$

For $1 \leq i \leq n$ let $\theta_i \in \mathbb{Z}[X_1, \dots, X_n]$ be such that

$$e_i(X_1^p, \dots, X_n^p) = \theta_i(e_1, \dots, e_n).$$

It follows from the above that

$$\psi_{\boldsymbol{\lambda}^{j+1}}(X_1, \dots, X_n) = \psi_{\boldsymbol{\lambda}^j}(\theta_1(X_1, \dots, X_n), \dots, \theta_n(X_1, \dots, X_n)).$$

Since

$$\begin{aligned} e_i(X_1, \dots, X_n)^p &\equiv e_i(X_1^p, \dots, X_n^p) \pmod p \\ &\equiv \theta_i(e_1, \dots, e_n) \pmod p \end{aligned}$$

we have $\theta_i(X_1, \dots, X_n) \equiv X_i^p \pmod p$, and hence $\theta_i \in R_1$. Therefore by Lemma 3.2 we get $\psi_{\boldsymbol{\lambda}^{j+1}} \in R_{j+1}$. □

Corollary 3.4. *Let $t \geq j \geq 0$, let $w' \geq 1$, and set $w = w'p^t$. Let $\boldsymbol{\lambda}'$ be a partition of w' and set $\boldsymbol{\lambda} = p^t \cdot \boldsymbol{\lambda}'$. Let $\boldsymbol{\mu}$ be a partition of w such that there does not exist a partition $\boldsymbol{\mu}'$ with $\boldsymbol{\mu} = p^{j+1} * \boldsymbol{\mu}'$. Then p^{t-j} divides $d_{\boldsymbol{\lambda\mu}}$. This holds in particular if $p^{j+1} \nmid |\boldsymbol{\mu}|$.*

Proof. Since $d_{\boldsymbol{\lambda\mu}}$ does not depend on n we may assume without loss of generality that $n \geq w$. It follows from this assumption that $|\boldsymbol{\lambda}| \leq n$, so by Proposition 3.3 we have $\psi_{\boldsymbol{\lambda}} \in R_t$. Since $w \leq n$ the parts of $\boldsymbol{\mu} = \{\mu_1, \dots, \mu_h\}$ satisfy $\mu_i \leq n$ for $1 \leq i \leq h$. Therefore the formula for $\psi_{\boldsymbol{\lambda}}$ given by Theorem 2.1 includes the term $d_{\boldsymbol{\mu\lambda}} X_{\mu_1} X_{\mu_2} \dots X_{\mu_h}$. The assumption on $\boldsymbol{\mu}$ implies that $X_{\mu_1} X_{\mu_2} \dots X_{\mu_h}$ is not a p^{j+1} power. Since $\psi_{\boldsymbol{\lambda}} \in R_t$ this implies that p^{t-j} divides $d_{\boldsymbol{\mu\lambda}}$. Since $d_{\boldsymbol{\lambda\mu}} = d_{\boldsymbol{\mu\lambda}}$ we get $p^{t-j} \mid d_{\boldsymbol{\lambda\mu}}$. □

Proposition 3.5. *Let $w' \geq 1$, $j \geq 1$, and $t \geq 0$. Let $\boldsymbol{\lambda}'$, $\boldsymbol{\mu}'$ be partitions of w' such that the parts of $\boldsymbol{\lambda}'$ are all divisible by p^t. Set $w = w'p^j$, so that $\boldsymbol{\lambda} = p^j \cdot \boldsymbol{\lambda}'$ and $\boldsymbol{\mu} = p^j * \boldsymbol{\mu}'$ are partitions of w. Then $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} \equiv d_{\boldsymbol{\lambda}'\boldsymbol{\mu}'} \pmod{p^{t+1}}$.*

Proof. As in the proof of Corollary 3.4 we may assume without loss of generality that $n \geq w'$. Then $|\boldsymbol{\lambda}'| = |\boldsymbol{\lambda}| \leq n$. It follows from Proposition 3.3 that $m_{\boldsymbol{\lambda}'} = \psi_{\boldsymbol{\lambda}'}(e_1, \ldots, e_n)$ for some $\psi_{\boldsymbol{\lambda}'} \in R_t$. Using induction on k we see that for $1 \leq i \leq n$ and $k \geq 0$ we have

$$e_i(X_1^{p^j}, \ldots, X_n^{p^j})^{p^k} \equiv e_i(X_1, \ldots, X_n)^{p^{j+k}} \pmod{p^{k+1}}.$$

Since $\psi_{\boldsymbol{\lambda}'} \in R_t$ it follows that

$$\begin{aligned} m_{\boldsymbol{\lambda}}(X_1, \ldots, X_n) &= m_{\boldsymbol{\lambda}'}(X_1^{p^j}, \ldots, X_n^{p^j}) \\ &= \psi_{\boldsymbol{\lambda}'}(e_1(X_1^{p^j}, \ldots, X_n^{p^j}), \ldots, e_n(X_1^{p^j}, \ldots, X_n^{p^j})) \\ &\equiv \psi_{\boldsymbol{\lambda}'}(e_1(X_1, \ldots, X_n)^{p^j}, \ldots, e_n(X_1, \ldots, X_n)^{p^j}) \pmod{p^{t+1}}. \end{aligned}$$

We also have $m_{\boldsymbol{\lambda}} = \psi_{\boldsymbol{\lambda}}(e_1, \ldots, e_n)$. Therefore there is a symmetric polynomial $\tau \in \mathbb{Z}[X_1, \ldots, X_n]$ such that

$$\psi_{\boldsymbol{\lambda}}(e_1, \ldots, e_n) = \psi_{\boldsymbol{\lambda}'}(e_1^{p^j}, \ldots, e_n^{p^j}) + p^{t+1}\tau(X_1, \ldots, X_n).$$

It follows from the fundamental theorem of symmetric polynomials that $\tau \in \mathbb{Z}[e_1, \ldots, e_n]$. Hence we have

$$\psi_{\boldsymbol{\lambda}}(X_1, \ldots, X_n) \equiv \psi_{\boldsymbol{\lambda}'}(X_1^{p^j}, \ldots, X_n^{p^j}) \pmod{p^{t+1}}.$$

Since $w' \leq n$ the parts of $\boldsymbol{\mu}'$ and $\boldsymbol{\mu}$ are all $\leq n$. Therefore the formula for $\psi_{\boldsymbol{\lambda}'}$ given by Theorem 2.1 includes the term $d_{\boldsymbol{\mu}'\boldsymbol{\lambda}'}X_{\mu_1'}X_{\mu_2'}\ldots X_{\mu_h'}$, and the formula for $\psi_{\boldsymbol{\lambda}}$ includes the term

$$d_{\boldsymbol{\mu}\boldsymbol{\lambda}}X_{\mu_1}X_{\mu_2}\ldots X_{\mu_{p^jh}} = d_{\boldsymbol{\mu}\boldsymbol{\lambda}}X_{\mu_1'}^{p^j}X_{\mu_2'}^{p^j}\ldots X_{\mu_h'}^{p^j}.$$

It follows that $d_{\boldsymbol{\mu}\boldsymbol{\lambda}} \equiv d_{\boldsymbol{\mu}'\boldsymbol{\lambda}'} \pmod{p^{t+1}}$. Therefore we have $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} \equiv d_{\boldsymbol{\lambda}'\boldsymbol{\mu}'} \pmod{p^{t+1}}$. □

4. Containment

Let L/K be a totally ramified extension of degree $n = up^\nu$, with $p \nmid u$. Let $\sigma_1, \ldots, \sigma_n$ be the K-embeddings of L into K^{sep}. Let $1 \leq h \leq n$ and recall that $E_h : L \to K$ is defined by $E_h(\alpha) = e_h(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$ for $\alpha \in L$. In this section we define a function $\gamma_h : \mathbb{Z} \to \mathbb{Z}$ such that for $r \in \mathbb{Z}$ we have $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{\gamma_h(r)}$. The function γ_h will be defined in terms of the indices of inseparability of the extension L/K. In the next section we show that $\mathcal{O}_K \cdot E_h(\mathcal{P}_L^r) = \mathcal{P}_K^{\gamma_h(r)}$ holds in certain cases.

Let π_L be a uniformizer for L and let

$$f(X) = X^n - c_1X^{n-1} + \cdots + (-1)^{n-1}c_{n-1}X + (-1)^n c_n$$

be the minimum polynomial of π_L over K. Then $c_h = E_h(\pi_L)$. For $k \in \mathbb{Z}$ define $\overline{v}_p(k) = \min\{v_p(k), \nu\}$. For $0 \le j \le \nu$ set

$$\begin{aligned} i_j^{\pi_L} &= \min\{nv_K(c_h) - h : 1 \le h \le n,\ \overline{v}_p(h) \le j\} \\ &= \min\{v_L(c_h\pi_L^{n-h}) : 1 \le h \le n,\ \overline{v}_p(h) \le j\} - n. \end{aligned}$$

Then $i_j^{\pi_L}$ is either a nonnegative integer or ∞. If $\mathrm{char}(K) = p$ then $i_j^{\pi_L}$ must be finite, since L/K is separable. If $i_j^{\pi_L}$ is finite write $i_j^{\pi_L} = a_jn - b_j$ with $1 \le b_j \le n$. Then $v_K(c_{b_j}) = a_j$, $v_K(c_h) \ge a_j$ for all h with $1 \le h < b_j$ and $\overline{v}_p(h) \le j$, and $v_K(c_h) \ge a_j + 1$ for all h with $b_j < h \le n$ and $\overline{v}_p(h) \le j$. Let $e_L = v_L(p)$ denote the absolute ramification index of L. We define the jth index of inseparability of L/K to be

$$i_j = \min\{i_{j'}^{\pi_L} + (j' - j)e_L : j \le j' \le \nu\}.$$

By Proposition 3.12 and Theorem 7.1 of [4], i_j does not depend on the choice of π_L. Furthermore, our definition of i_j agrees with Definition 7.3 in [4] (see also [5, Rem. 2.5]; for the characteristic-p case see [2, p. 232–233] and [3, §2]).

The following facts are easy consequences of the definitions:

(1) $0 = i_\nu < i_{\nu-1} \le \cdots \le i_1 \le i_0 < \infty$.
(2) If $\mathrm{char}(K) = p$ then $e_L = \infty$, and hence $i_j = i_j^{\pi_L}$.
(3) Let $m = \overline{v}_p(i_j)$. If $m \le j$ then $i_j = i_m = i_j^{\pi_L} = i_m^{\pi_L}$. If $m > j$ then $\mathrm{char}(K) = 0$ and $i_j = i_m^{\pi_L} + (m - j)e_L$.

Lemma 4.1. *Let $1 \le h \le n$ and set $j = \overline{v}_p(h)$. Then $v_L(c_h) \ge i_j^{\pi_L} + h$, with equality if and only if either $i_j^{\pi_L} = \infty$ or $i_j^{\pi_L} < \infty$ and $h = b_j$.*

Proof. If $i_j^{\pi_L} = \infty$ then we certainly have $v_L(c_h) = \infty$. Suppose $i_j^{\pi_L} < \infty$. If $b_j < h \le n$ then $v_L(c_h) = nv_K(c_h) \ge n(a_j + 1)$, and hence

$$v_L(c_h) \ge na_j + n > na_j - b_j + h = i_j^{\pi_L} + h.$$

If $1 \le h < b_j$ then

$$v_L(c_h) \ge na_j > na_j - b_j + h = i_j^{\pi_L} + h.$$

Finally, we observe that $v_L(c_{b_j}) = na_j = i_j^{\pi_L} + b_j$. □

For a partition $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ whose parts satisfy $\lambda_i \le n$ for $1 \le i \le k$ define $c_{\boldsymbol{\lambda}} = c_{\lambda_1}c_{\lambda_2}\ldots c_{\lambda_k}$.

Proposition 4.2. *Let $w \ge 1$ and let $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ be a partition of w whose parts satisfy $\lambda_i \le n$. Choose q to minimize $\overline{v}_p(\lambda_q)$ and set $t = \overline{v}_p(\lambda_q)$. Then $v_L(c_{\boldsymbol{\lambda}}) \ge i_t^{\pi_L} + w$. If $v_L(c_{\boldsymbol{\lambda}}) = i_t^{\pi_L} + w$ and $i_t^{\pi_L} < \infty$ then $\lambda_q = b_t$ and $\lambda_i = b_\nu = n$ for all $i \ne q$.*

Proof. If $i_t^{\pi_L} = \infty$ then $v_L(c_{\lambda_q}) = \infty$, and hence $v_L(c_{\boldsymbol{\lambda}}) = \infty$. Suppose $i_t^{\pi_L} < \infty$. By Lemma 4.1 we have $v_L(c_{\lambda_q}) \geq i_t^{\pi_L} + \lambda_q$, and $v_L(c_{\lambda_i}) \geq \lambda_i$ for $i \neq q$. Hence $v_L(c_{\boldsymbol{\lambda}}) \geq i_t^{\pi_L} + w$, with equality if and only if $v_L(c_{\lambda_q}) = i_t^{\pi_L} + \lambda_q$ and $v_L(c_{\lambda_i}) = \lambda_i$ for $i \neq q$. It follows from Lemma 4.1 that these conditions hold if and only if $\lambda_q = b_t$ and $\lambda_i = b_\nu$ for all $i \neq q$. □

Proposition 4.3. *Let $w \geq 1$, let $\boldsymbol{\mu}$ be a partition of w with $h \leq n$ parts, and set $j = \overline{v}_p(h)$. Let $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ be a partition of w whose parts satisfy $\lambda_i \leq n$, choose q to minimize $\overline{v}_p(\lambda_q)$, and set $t = \overline{v}_p(\lambda_q)$. Then*

(1) $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) \geq i_j + w$.
(2) *Suppose $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) = i_j + w$. Then $i_t^{\pi_L}$ is finite, $\lambda_q = b_t$, and $\lambda_i = n$ for all $i \neq q$.*

Proof. (1) Suppose $t \geq j$. Then by Corollary 3.4 we have $\overline{v}_p(d_{\boldsymbol{\lambda}\boldsymbol{\mu}}) \geq t - j$. Hence by Proposition 4.2 we get

$$v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) \geq (t-j)e_L + i_t^{\pi_L} + w \geq i_j + w.$$

Suppose $t < j$. Using Proposition 4.2 we get

$$v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) \geq v_L(c_{\boldsymbol{\lambda}}) \geq i_t^{\pi_L} + w \geq i_t + w \geq i_j + w.$$

(2) If $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) = i_j + w$ then all the inequalities above are equalities. In either case it follows that $i_t^{\pi_L}$ is finite and $v_L(c_{\boldsymbol{\lambda}}) = i_t^{\pi_L} + w$. Therefore by Proposition 4.2 we get $\lambda_q = b_t$ and $\lambda_i = n$ for all $i \neq q$. □

We now apply the results of Section 2 to our field extension L/K. For a partition $\boldsymbol{\mu}$ with at most n parts we define $M_{\boldsymbol{\mu}} : L \to K$ by setting $M_{\boldsymbol{\mu}}(\alpha) = m_{\boldsymbol{\mu}}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$ for $\alpha \in L$.

Proposition 4.4. *Let $r \geq 1$ and let $\alpha \in \mathcal{P}_L^r$. Choose a power series*

$$\phi(X) = a_r X^r + a_{r+1} X^{r+1} + \cdots$$

with coefficients in $\mathcal{O}_K$ such that $\alpha = \phi(\pi_L)$. Then for $1 \leq h \leq n$ we have

$$E_h(\alpha) = \sum_{\boldsymbol{\mu}} a_{\mu_1} a_{\mu_2} \ldots a_{\mu_h} M_{\boldsymbol{\mu}}(\pi_L),$$

where the sum ranges over all partitions $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_h\}$ with h parts such that $\mu_i \geq r$ for $1 \leq i \leq h$.

Proof. This follows from (2.1) by setting $X_i = \sigma_i(\pi_L)$ and taking $a_j \in \mathcal{O}_K$. □

Proposition 4.5. *Let $n \geq 1$, let $w \geq 1$, and let $\boldsymbol{\mu}$ be a partition of w with at most n parts. Then*

$$M_\mu(\pi_L) = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}},$$

where the sum is over all partitions $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ of w such that $\lambda_i \leq n$ for $1 \leq i \leq k$.

Proof. This follows from Theorem 2.1 by setting $X_i = E_i(\pi_L) = c_i$. $\square$

Let $1 \le h \le n$ and recall that we defined $g_h : \mathbb{Z} \to \mathbb{Z}$ by setting $g_h(r) = s$, where s is the largest integer such that $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^s$.

Theorem 4.6. *Let L/K be a totally ramified extension of degree $n = up^\nu$, with $p \nmid u$. Let $r \in \mathbb{Z}$, let $1 \le h \le n$, and set $j = \overline{v}_p(h)$. Then*

$$E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{\lceil (i_j+hr)/n \rceil}$$
$$g_h(r) \ge \left\lceil \frac{i_j + hr}{n} \right\rceil.$$

Proof. Let π_K be a uniformizer for K. Then for $t \in \mathbb{Z}$ we have

$$E_h(\mathcal{P}_L^{nt+r}) = E_h(\pi_K^t \cdot \mathcal{P}_L^r) = \pi_K^{ht} \cdot E_h(\mathcal{P}_L^r) \tag{4.1}$$

$$\left\lceil \frac{i_j + h(nt+r)}{n} \right\rceil = ht + \left\lceil \frac{i_j + hr}{n} \right\rceil. \tag{4.2}$$

Therefore it suffices to prove the theorem in the cases with $1 \le r \le n$. By Proposition 4.4 each element of $E_h(\mathcal{P}_L^r)$ is an $\mathcal{O}_K$-linear combination of terms of the form $M_{\boldsymbol{\mu}}(\pi_L)$, where $\boldsymbol{\mu}$ is a partition with h parts, all $\ge r$. Fix one such partition $\boldsymbol{\mu}$ and set $w = \Sigma(\boldsymbol{\mu})$; then $w \ge hr$. Using Proposition 4.5 we can express $M_{\boldsymbol{\mu}}(\pi_L)$ as a sum of terms $d_{\boldsymbol{\lambda\mu}} c_{\boldsymbol{\lambda}}$, where $\boldsymbol{\lambda} = \{\lambda_1, \lambda_2, \dots, \lambda_k\}$ is a partition of w into parts which are $\le n$. By Proposition 4.3 (1) we get $v_L(d_{\boldsymbol{\lambda\mu}} c_{\boldsymbol{\lambda}}) \ge i_j + w \ge i_j + hr$. Since $d_{\boldsymbol{\lambda\mu}} c_{\boldsymbol{\lambda}} \in K$ it follows that $v_K(d_{\boldsymbol{\lambda\mu}} c_{\boldsymbol{\lambda}}) \ge \lceil (i_j + hr)/n \rceil$. Therefore we have $v_K(M_{\boldsymbol{\mu}}(\pi_L)) \ge \lceil (i_j + hr)/n \rceil$, and hence $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{\lceil (i_j+hr)/n \rceil}$. $\square$

5. Equality

In this section we show that in some special cases we have $\mathcal{O}_K \cdot E_h(\mathcal{P}_L^r) = \mathcal{P}_K^{\lceil (i_j+hr)/n \rceil}$, where $j = \overline{v}_p(h)$. This is equivalent to showing that $g_h(r) = \lceil (i_j + hr)/n \rceil$ holds in these cases. In particular, we prove that if the residue field $\overline{K}$ of K is large enough then $g_{p^j}(r) = \lceil (i_j + rp^j)/n \rceil$ for $0 \le j \le \nu$. To prove that $g_h(r) = \lceil (i_j + hr)/n \rceil$ holds for all $r \in \mathbb{Z}$, by Theorem 4.6 it suffices to show the following: Let r satisfy

$$\left\lceil \frac{i_j + hr}{n} \right\rceil < \left\lceil \frac{i_j + h(r+1)}{n} \right\rceil. \tag{5.1}$$

Then there is $\alpha \in \mathcal{P}_L^r$ such that $v_K(E_h(\alpha)) = \lceil (i_j + hr)/n \rceil$. By (4.1) and (4.2) it's enough to prove this for r such that $1 \le r \le n$.

Once again we let π_L be a uniformizer for L whose minimum polynomial over K is

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

Theorem 5.1. *Let L/K be a totally ramified extension of degree $n = up^\nu$, with $p \nmid u$. Let j be an integer such that $0 \le j \le \nu$ and $\overline{v}_p(i_j) \ge j$. Then for all $r \in \mathbb{Z}$ we have*

$$\mathcal{O}_K \cdot E_{p^j}(\mathcal{P}_L^r) = \mathcal{P}_K^{\lceil (i_j + rp^j)/n \rceil}$$
$$g_{p^j}(r) = \left\lceil \frac{i_j + rp^j}{n} \right\rceil.$$

Proof. Set $m = \overline{v}_p(i_j)$. Then $i_j = (m-j)e_L + i_m^{\pi_L}$. In particular, if $\mathrm{char}(K) = p$ then $m = j$ and $i_j = i_m = i_m^{\pi_L}$. We can write $i_m^{\pi_L} = an - b$ with $1 \le b \le n$ and $\overline{v}_p(b) = m$. Since $j \le m$ there is $b' \in \mathbb{Z}$ such that $b = b'p^j$. Let $r_1 \in \mathbb{Z}$ and set $r = b' + r_1 up^{\nu - j}$. Then

$$i_j + rp^j = (m-j)e_L + an + r_1 n. \tag{5.2}$$

Therefore we have

$$\left\lceil \frac{i_j + rp^j}{n} \right\rceil = (m-j)e_K + a + r_1$$
$$\left\lceil \frac{i_j + (r+1)p^j}{n} \right\rceil = (m-j)e_K + a + r_1 + 1,$$

with $e_K = v_K(p) = e_L/n$. It follows that the only values of r in the range $1 \le r \le n$ satisfying (5.1) are of the form $r = b' + r_1 up^{\nu-j}$ with $0 \le r_1 < p^j$. Therefore it suffices to prove that $v_K(E_{p^j}(\pi_L^r)) = (m-j)e_K + a + r_1$ holds for these values of r.

Let $\boldsymbol{\mu}$ be the partition of rp^j consisting of p^j copies of r. Then $E_{p^j}(\pi_L^r) = M_{\boldsymbol{\mu}}(\pi_L)$, so it follows from Proposition 4.5 that

$$E_{p^j}(\pi_L^r) = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}, \tag{5.3}$$

where the sum is over all partitions $\boldsymbol{\lambda} = \{\lambda_1, \dots, \lambda_k\}$ of rp^j such that $\lambda_i \le n$ for $1 \le i \le k$. It follows from Proposition 4.3 (1) that $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) \ge i_j + rp^j$. Suppose $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) = i_j + rp^j$. Then by Proposition 4.3 (2) we see that $\boldsymbol{\lambda}$ has at most one element which is not equal to n. Since $\Sigma(\boldsymbol{\lambda}) = rp^j = b + r_1 n$, and the elements of $\boldsymbol{\lambda}$ are $\le n$, it follows that $\boldsymbol{\lambda} = \boldsymbol{\kappa}$, where $\boldsymbol{\kappa}$ is the partition of rp^j which consists of 1 copy of b and r_1 copies of n. Since $E_{p^j}(\pi_L^r) \in K$ and $d_{\boldsymbol{\kappa}\boldsymbol{\mu}} c_{\boldsymbol{\kappa}} \in K$ it follows from (5.3) and (5.2) that

$$E_{p^j}(\pi_L^r) \equiv d_{\boldsymbol{\kappa}\boldsymbol{\mu}} c_{\boldsymbol{\kappa}} \pmod{\mathcal{P}_K^{(m-j)e_K + a + r_1 + 1}}. \tag{5.4}$$

Let $\boldsymbol{\kappa}'$ be the partition of r consisting of 1 copy of b' and r_1 copies of $up^{\nu-j}$, and let $\boldsymbol{\mu}'$ be the partition of r consisting of 1 copy of r. Then $\boldsymbol{\kappa} = p^j \cdot \boldsymbol{\kappa}'$ and $\boldsymbol{\mu} = p^j * \boldsymbol{\mu}'$. Since $v_p(b') = m - j$ it follows from Proposition 3.5 that $d_{\boldsymbol{\kappa}\boldsymbol{\mu}} \equiv d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'} \pmod{p^{m-j+1}}$. Suppose $m < \nu$. Then $b < n$, so $b' \ne up^{\nu-j}$. Hence by Proposition 2.4 we get $d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'} = (-1)^{r+r_1+1} r$. Since $r = b' + r_1 up^{\nu-j}$

and $v_p(b') = m - j$ this implies $v_p(d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'}) = v_p(r) = m - j$. Suppose $m = \nu$. Then $b = n$ and $b' = p^{-j}b = up^{\nu-j}$, so $\boldsymbol{\kappa}'$ consists of $r_1 + 1$ copies of $up^{\nu-j}$. Since $\gcd(up^{\nu-j}, r) = up^{\nu-j}$ and $\gcd(r_1 + 1, 1) = 1$, by Proposition 2.6 we get $d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'} = (-1)^{r+r_1+1}up^{\nu-j}$. Hence $v_p(d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'}) = \nu - j = m - j$ holds in this case as well. Since $d_{\boldsymbol{\kappa}\boldsymbol{\mu}} \equiv d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'} \pmod{p^{m-j+1}}$ it follows that $v_p(d_{\boldsymbol{\kappa}\boldsymbol{\mu}}) = m - j$. Therefore

$$v_K(d_{\boldsymbol{\kappa}\boldsymbol{\mu}}c_{\boldsymbol{\kappa}}) = v_K(d_{\boldsymbol{\kappa}\boldsymbol{\mu}}) + v_K(c_b c_n^{r_1}) = (m - j)e_K + a + r_1.$$

Using (5.4) we conclude that

$$v_K(E_{p^j}(\pi_L^r)) = (m - j)e_K + a + r_1. \qquad \square$$

Theorem 5.2. *Let L/K be a totally ramified extension of degree $n = up^\nu$, with $p \nmid u$. Let j be an integer such that $0 \le j \le \nu$ and $\overline{v}_p(i_j) < j$. Set $m = \overline{v}_p(i_j)$ and assume that $|\overline{K}| > p^m$. Then for all $r \in \mathbb{Z}$ we have*

$$\mathcal{O}_K \cdot E_{p^j}(\mathcal{P}_L^r) = \mathcal{P}_K^{\lceil (i_j + rp^j)/n \rceil}$$
$$g_{p^j}(r) = \left\lceil \frac{i_j + rp^j}{n} \right\rceil.$$

Proof. Since $m < j$ we have $i_m = i_j = i_j^{\pi_L}$. Therefore $i_j = an - b$ for some a, b such that $1 \le b < n$ and $\overline{v}_p(b) = m$. Hence $b = b'p^j + b''p^m$ for some b', b'' such that $0 < b'' < p^{j-m}$ and $p \nmid b''$. Let $r_1 \in \mathbb{Z}$ and set $r = b' + r_1 up^{\nu-j}$. Then

$$i_j + rp^j = an + r_1 n - b''p^m, \tag{5.5}$$

so we have

$$\left\lceil \frac{i_j + rp^j}{n} \right\rceil = a + r_1 + \left\lceil \frac{-b''p^m}{n} \right\rceil = a + r_1$$
$$\left\lceil \frac{i_j + (r+1)p^j}{n} \right\rceil = a + r_1 + \left\lceil \frac{p^j - b''p^m}{n} \right\rceil = a + r_1 + 1.$$

It follows that the only values of r in the range $1 \le r \le n$ satisfying (5.1) are of the form $r = b' + r_1 up^{\nu-j}$ with $0 \le r_1 < p^j$. It suffices to prove that for every such r there is $\beta \in \mathcal{O}_K$ such that $v_K(E_{p^j}(\pi_L^r + \beta\pi_L^{r+b''})) = a + r_1$.

Let $\eta(X) = E_{p^j}(\pi_L^r + X\pi_L^{r+b''})$. We need to show that there is $\beta \in \mathcal{O}_K$ such that $v_K(\eta(\beta)) = a + r_1$. It follows from Proposition 4.4 that $\eta(X)$ is a polynomial in X of degree at most p^j, with coefficients in $\mathcal{O}_K$. For $0 \le \ell \le p^j$ let $\boldsymbol{\mu}^\ell$ be the partition of $rp^j + \ell b''$ consisting of $p^j - \ell$ copies of r and ℓ copies of $r + b''$. By Proposition 4.4 the coefficient of X^ℓ in $\eta(X)$ is equal to $M_{\boldsymbol{\mu}^\ell}(\pi_L)$. By Proposition 4.5 we have

$$M_{\boldsymbol{\mu}^\ell}(\pi_L) = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda}\boldsymbol{\mu}^\ell} c_{\boldsymbol{\lambda}}, \tag{5.6}$$

where the sum is over all partitions $\boldsymbol{\lambda} = \{\lambda_1, \dots, \lambda_k\}$ of $rp^j + \ell b''$ such that $\lambda_i \le n$ for $1 \le i \le k$. Using Proposition 4.3 (1) and equation (5.5) we get

$$\begin{aligned} v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}^\ell} c_{\boldsymbol{\lambda}}) &\ge i_j + rp^j + \ell b'' \\ &= (a + r_1)n + (\ell - p^m)b'' \\ &> (a + r_1 - 1)n. \end{aligned} \tag{5.7}$$

Since $d_{\boldsymbol{\lambda}\boldsymbol{\mu}^\ell} c_{\boldsymbol{\lambda}} \in K$ it follows that $d_{\boldsymbol{\lambda}\boldsymbol{\mu}^\ell} c_{\boldsymbol{\lambda}} \in \mathcal{P}_K^{a+r_1}$. Therefore by (5.6) we have $M_{\boldsymbol{\mu}^\ell}(\pi_L) \in \mathcal{P}_K^{a+r_1}$.

Suppose $v_K(d_{\boldsymbol{\lambda}\boldsymbol{\mu}^\ell} c_{\boldsymbol{\lambda}}) = a + r_1$. Then $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}^\ell} c_{\boldsymbol{\lambda}}) = (a + r_1)n$, so by (5.7) we get $\ell \le p^m$. Hence for $p^m < \ell \le p^j$ we have $M_{\boldsymbol{\mu}^\ell}(\pi_L) \in \mathcal{P}_K^{a+r_1+1}$. Let $w = b + r_1 n = rp^j + b''p^m$ and let $\boldsymbol{\mu} = \boldsymbol{\mu}^{p^m}$ be the partition of w consisting of p^m copies of $r + b''$ and $p^j - p^m$ copies of r. Then the coefficient of X^{p^m} in $\eta(X)$ is $M_{\boldsymbol{\mu}}(\pi_L)$. Let $\boldsymbol{\kappa}$ be the partition of w consisting of 1 copy of b and r_1 copies of n. Suppose $\boldsymbol{\lambda}$ is a partition of w with parts $\le n$ such that $v_K(d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}) = a + r_1$. Since $(a + r_1)n = i_j + w$ it follows from Proposition 4.3 (2) that $\boldsymbol{\lambda}$ has at most one element which is not equal to n. Since $\Sigma(\boldsymbol{\lambda}) = b + r_1 n$, and the elements of $\boldsymbol{\lambda}$ are $\le n$, it follows that $\boldsymbol{\lambda} = \boldsymbol{\kappa}$. Hence by (5.6) we have

$$M_{\boldsymbol{\mu}}(\pi_L) \equiv d_{\boldsymbol{\kappa}\boldsymbol{\mu}} c_{\boldsymbol{\kappa}} \pmod{\mathcal{P}_K^{a+r_1+1}}. \tag{5.8}$$

Set $w' = b'p^{j-m} + b'' + r_1 u p^{\nu-m} = rp^{j-m} + b''$. Let $\boldsymbol{\kappa}'$ be the partition of w' consisting of 1 copy of $b'p^{j-m} + b''$ and r_1 copies of $up^{\nu-m}$, and let $\boldsymbol{\mu}'$ be the partition of w' consisting of 1 copy of $r + b''$ and $p^{j-m} - 1$ copies of r. Then $\boldsymbol{\kappa} = p^m \cdot \boldsymbol{\kappa}'$ and $\boldsymbol{\mu} = p^m * \boldsymbol{\mu}'$, so by Proposition 3.5 we have $d_{\boldsymbol{\kappa}\boldsymbol{\mu}} \equiv d_{\boldsymbol{\kappa}'\boldsymbol{\mu}'} \pmod{p}$.

Let Γ be a cycle digraph which has an admissible $(\boldsymbol{\kappa}', \boldsymbol{\mu}')$-tiling. Suppose Γ has more than one component. Since Γ has a $\boldsymbol{\kappa}'$-tiling, Γ has at least one component Γ_0 such that $|V(\Gamma_0)| = k \cdot up^{\nu-m}$ for some k such that $1 \le k \le r_1$. Let $\boldsymbol{\kappa}'_0$ be the submultiset of $\boldsymbol{\kappa}'$ consisting of k copies of $up^{\nu-m}$. Then $\boldsymbol{\kappa}'_0$ is the unique submultiset of $\boldsymbol{\kappa}'$ such that Γ_0 has a $\boldsymbol{\kappa}'_0$-tiling. Furthermore there is a submultiset $\boldsymbol{\mu}'_0$ of $\boldsymbol{\mu}'$ such that Γ_0 has a $\boldsymbol{\mu}'_0$-tiling. We will see below that $\boldsymbol{\mu}'_0$ is uniquely determined.

Suppose r does not divide $kup^{\nu-m}$. Then there is $\ell \ge 0$ such that $\boldsymbol{\mu}'_0$ consists of 1 copy of $r + b''$ together with ℓ copies of r. By Proposition 2.3 we have $\eta_{\boldsymbol{\kappa}'_0\boldsymbol{\mu}'_0}(\Gamma_0) = up^{\nu-m}$. Let Γ_1 be the complement of Γ_0 in Γ, let $\boldsymbol{\kappa}'_1 = \boldsymbol{\kappa}' \smallsetminus \boldsymbol{\kappa}'_0$, and let $\boldsymbol{\mu}'_1 = \boldsymbol{\mu}' \smallsetminus \boldsymbol{\mu}'_0$. Since Γ_1 has no cycle of length $|V(\Gamma_0)| = b'' + (\ell + 1)r$ we have $\eta_{\boldsymbol{\kappa}'\boldsymbol{\mu}'}(\Gamma) = \eta_{\boldsymbol{\kappa}'_0\boldsymbol{\mu}'_0}(\Gamma_0)\eta_{\boldsymbol{\kappa}'_1\boldsymbol{\mu}'_1}(\Gamma_1)$. Hence $\eta_{\boldsymbol{\kappa}'\boldsymbol{\mu}'}(\Gamma)$ is divisible by p in this case.

On the other hand, suppose r divides $kup^{\nu-m}$. If r also divides $r+b''$ then $p \nmid r$, so $r \mid ku$. It follows that $r_1 up^{\nu-j} + b' = r \le ku \le r_1 u$, a contradiction. Hence there is $\ell \ge 1$ such that $\boldsymbol{\mu}'_0$ consists of ℓ copies of r. Let (S, T) be an admissible $(\boldsymbol{\kappa}', \boldsymbol{\mu}')$-tiling of Γ and let (S_0, T_0) be the restriction of (S, T) to Γ_0. Then (S_0, T_0) is a $(\boldsymbol{\kappa}_0', \boldsymbol{\mu}_0')$-tiling of Γ_0. By Proposition 2.5 (2) the automorphism group of (Γ_0, S_0, T_0) has order $\gcd(k, \ell)$. Since $\mathrm{Aut}(\Gamma_0, S_0, T_0)$ is isomorphic to a subgroup of $\mathrm{Aut}(\Gamma, S, T)$, it follows that $\gcd(k, \ell)$ divides $|\mathrm{Aut}(\Gamma, S, T)|$. Therefore the assumption that (S, T) is admissible implies that $\gcd(k, \ell) = 1$. Since $k \cdot up^{\nu-m} = \ell \cdot r$ we get $k \mid r$ and $\ell \mid up^{\nu-m}$. It follows that there is $q \in \mathbb{Z}$ with $r = kq$ and $up^{\nu-m} = \ell q$. By Proposition 2.5 (1) the number of isomorphism classes of $(\boldsymbol{\kappa}_0', \boldsymbol{\mu}_0')$-tilings of Γ_0 is

$$\eta_{\boldsymbol{\kappa}_0' \boldsymbol{\mu}_0'}(\Gamma_0) = \gcd(up^{\nu-m}, r) = \gcd(\ell q, kq) = q.$$

If $p \mid q$ then as above we deduce that $\eta_{\boldsymbol{\kappa}' \boldsymbol{\mu}'}(\Gamma)$ is divisible by p. On the other hand, if $p \nmid q$ then $q \mid u$; in particular, $q \le u$. Since $k \le r_1$ this gives the contradiction $r = kq \le r_1 u$. By combining the two cases we find that if Γ has more than one component then $\eta_{\boldsymbol{\kappa}' \boldsymbol{\mu}'}(\Gamma)$ is divisible by p.

Finally, suppose that Γ consists of a single cycle of length w'. Then by Proposition 2.2 we have $\eta_{\boldsymbol{\kappa}', \boldsymbol{\mu}'}(\Gamma) = w'$. Hence by (2.2) we get

$$d_{\boldsymbol{\kappa}\boldsymbol{\mu}} \equiv d_{\boldsymbol{\kappa}' \boldsymbol{\mu}'} \equiv \pm \eta_{\boldsymbol{\kappa}' \boldsymbol{\mu}'}(\Gamma) \equiv \pm w' \pmod{p}.$$

Since $w' \equiv b'' \pmod{p}$ it follows that $p \nmid d_{\boldsymbol{\kappa}\boldsymbol{\mu}}$. Hence by (5.8) we get

$$v_K(M_{\boldsymbol{\mu}}(\pi_L)) = v_K(c_{\boldsymbol{\kappa}}) = a + r_1.$$

Let π_K be a uniformizer for K and set $\phi(X) = \pi_K^{-a-r_1} \eta(X)$. Then $\phi(X) \in \mathcal{O}_K[X]$. Let $\overline{\phi}(X)$ be the image of $\phi(X)$ in $\overline{K}[X]$. We have shown that $\overline{\phi}(X)$ has degree p^m. Since $|\overline{K}| > p^m$ there is $\overline{\beta} \in \overline{K}$ such that $\overline{\phi}(\overline{\beta}) \ne 0$. Let $\beta \in \mathcal{O}_K$ be a lifting of $\overline{\beta}$. Then $\phi(\beta) \in \mathcal{O}_K^\times$. It follows that

$$v_K(E_{p^j}(\pi_L^r + \beta \pi_L^{r+b''})) = v_K(\eta(\beta)) = a + r_1.$$

Hence if $r = b' + r_1 up^{\nu-j}$ with $0 \le r_1 < p^j$ then

$$\mathcal{O}_K \cdot E_{p^j}(\mathcal{P}_L^r) = \mathcal{P}_K^{a+r_1} = \mathcal{P}_K^{\lceil (i_j + rp^j)/n \rceil}.$$

We conclude that this formula holds for all $r \in \mathbb{Z}$. □

Remark 5.3. Theorems 5.1 and 5.2 together imply that if $\overline{K}$ is sufficiently large then $g_{p^j}(r) = \lceil (i_j + rp^j)/n \rceil$ for $0 \le j \le \nu$. This holds for instance if $|\overline{K}| \ge p^\nu$.

Remark 5.4. Let L/K be a totally ramified separable extension of degree $n = up^\nu$. The different $\mathcal{P}_L^{d_0}$ of L/K is defined by letting d_0 be the largest integer such that $E_1(\mathcal{P}_L^{-d_0}) \subset \mathcal{O}_K$. For $1 \le j \le \nu$ one can define higher order analogs $\mathcal{P}_L^{d_j}$ of the different by letting d_j be the largest integer such that $E_{p^j}(\mathcal{P}_L^{-d_j}) \subset \mathcal{O}_K$. An argument similar to the proof of Proposition 1.2 shows that

$$\mathcal{O}_K \cdot E_{p^j}(\mathcal{P}_L^r) = \mathcal{P}_K^{\lfloor p^j (d_j + r)/n \rfloor}.$$

This generalizes Proposition 1.2, which is equivalent to the case $j = 0$ of this formula. By Proposition 3.18 of [4], the valuation of the different of L/K is $d_0 = i_0 + n - 1$. Using Theorems 5.1 and 5.2 we find that, if $\overline{K}$ is sufficiently large, d_j is the largest integer such that $\lceil (i_j - d_j p^j)/n \rceil \geq 0$. Hence $d_j = \lfloor (i_j + n - 1)/p^j \rfloor$ for $0 \leq j \leq \nu$.

Example 5.5. Let $K = \mathbb{F}_2((t))$ and let L be an extension of K generated by a root π_L of the Eisenstein polynomial $f(X) = X^8 + tX^3 + tX^2 + t$. Then the indices of inseparability of L/K are $i_0 = 3$, $i_1 = i_2 = 2$, and $i_3 = 0$. Since $\lceil (i_2 + 2^2 \cdot 1)/2^3 \rceil = 1$, the formula in Theorem 5.2 would imply $\mathcal{O}_K \cdot E_4(\mathcal{P}_L^1) = \mathcal{P}_K^1$. We claim that $E_4(\mathcal{P}_L) \subset \mathcal{P}_K^2$.

Let $\alpha \in \mathcal{P}_L$ and write $\alpha = a_1\pi_L + a_2\pi_L^2 + \cdots$, with $a_i \in \mathbb{F}_2$. It follows from Propositions 4.4 and 4.5 that $E_4(\alpha)$ is a sum of terms of the form $a_{\boldsymbol{\mu}} d_{\boldsymbol{\lambda}\boldsymbol{\mu}} c_{\boldsymbol{\lambda}}$, where $\boldsymbol{\lambda}$ is a partition whose parts are ≤ 8 and $\boldsymbol{\mu}$ is a partition with 4 parts such that $\Sigma(\boldsymbol{\lambda}) = \Sigma(\boldsymbol{\mu})$. We are interested only in those terms with K-valuation 1. We have $v_K(c_{\boldsymbol{\lambda}}) \geq 2$ unless $\boldsymbol{\lambda}$ is one of $\{5\}$, $\{6\}$, or $\{8\}$. If $\boldsymbol{\lambda} = \{8\}$ then $2 \mid d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ for any $\boldsymbol{\mu}$ by Corollary 3.4. If $\boldsymbol{\lambda} = \{6\}$ and $\boldsymbol{\mu} = \{1,1,1,3\}$ then $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = 6$ by Proposition 2.4. If $\boldsymbol{\lambda} = \{6\}$ and $\boldsymbol{\mu} = \{1,1,2,2\}$ then a computation based on (2.2) shows that $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = 9$. If $\boldsymbol{\lambda} = \{5\}$ and $\boldsymbol{\mu} = \{1,1,1,2\}$ then $d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = -5$ by Proposition 2.4. Combining these facts we get

$$E_4(\alpha) \equiv a_1^3 a_2 t + a_1^2 a_2^2 t \pmod{\mathcal{P}_K^2}.$$

Since $a_1, a_2 \in \mathbb{F}_2$ we have $a_1^3 a_2 + a_1^2 a_2^2 = 0$. Therefore $E_4(\alpha) \in \mathcal{P}_K^2$. Since this holds for every $\alpha \in \mathcal{P}_L$ we get $E_4(\mathcal{P}_L) \subset \mathcal{P}_K^2$. This shows that Theorem 5.2 does not hold without the assumption about the size of $\overline{K}$.

The following result shows that $g_h(r) = \lceil (i_j + hr)/n \rceil$ does not hold in general, even if we assume that the residue field of K is large. It also suggests that there may not be a simple criterion for determining when $g_h(r) = \lceil (i_j + hr)/n \rceil$ does hold.

Proposition 5.6. *Let L/K be a totally ramified extension of degree n, with $p \nmid n$. Let $r \in \mathbb{Z}$ and $1 \leq h \leq n$ be such that $n \mid hr$. Set $s = hr/n$, $u = \gcd(r, n)$, and $v = \gcd(h, s)$. Then $g_h(r) = \lceil (i_0 + hr)/n \rceil = s$ if and only if p does not divide the binomial coefficient $\binom{u}{v}$. In particular, if $u < v$ then $g_h(r) > s$.*

Proof. Since L/K is tamely ramified we have $\nu = 0$, $i_0 = 0$, and

$$\left\lceil \frac{i_0 + hr}{n} \right\rceil = \left\lceil \frac{hr}{n} \right\rceil = s.$$

It follows from Theorem 4.6 that $g_h(r) \geq s$. If $r' = nt + r$ then $s' = hr'/n = ht + s$, $u' = \gcd(r', n) = u$, and $v' = \gcd(h, s') = v$. Hence by (4.1) it suffices to prove the proposition in the cases with $1 \leq r \leq n$.

Suppose p does not divide $\binom{u}{v}$. To prove $g_h(r) = s$ it suffices to show that $v_K(E_h(\pi_L^r)) = s$. Let $\boldsymbol{\mu}$ be the partition of hr consisting of h copies of r. Then $E_h(\pi_L^r) = M_{\boldsymbol{\mu}}(\pi_L)$, so it follows from Proposition 4.5 that

$$E_h(\pi_L^r) = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda\mu}} c_{\boldsymbol{\lambda}}, \tag{5.9}$$

where the sum is over all partitions $\boldsymbol{\lambda} = \{\lambda_1, \dots, \lambda_k\}$ of hr such that $\lambda_i \leq n$ for $1 \leq i \leq k$. Let $\boldsymbol{\kappa}$ be the partition of $hr = sn$ consisting of s copies of n and let $\boldsymbol{\lambda}$ be a partition of hr whose parts are $\leq n$. Then by Proposition 4.3 (1) we have $v_L(d_{\boldsymbol{\kappa\mu}} c_{\boldsymbol{\lambda}}) \geq hr = sn$. Furthermore, if $v_L(d_{\boldsymbol{\kappa\mu}} c_{\boldsymbol{\lambda}}) = hr$ then by Proposition 4.3 (2) we have $\boldsymbol{\lambda} = \boldsymbol{\kappa}$. Hence by (5.9) we get

$$E_h(\pi_L^r) \equiv d_{\boldsymbol{\kappa\mu}} c_{\boldsymbol{\kappa}} \pmod{\mathcal{P}_K^{s+1}}.$$

By Proposition 2.6 we have $d_{\boldsymbol{\kappa\mu}} = \pm\binom{u}{v}$. Since $p \nmid \binom{u}{v}$ and $v_K(c_{\boldsymbol{\kappa}}) = s$ it follows that $v_K(E_h(\pi_L^r)) = s$. Therefore $g_h(r) = s$.

Suppose p divides $\binom{u}{v}$. By Proposition 4.4, each element of $E_h(\mathcal{P}_L^r)$ is an $\mathcal{O}_K$-linear combination of terms of the form $M_{\boldsymbol{\nu}}(\pi_L)$ where $\boldsymbol{\nu}$ is a partition with h parts, all $\geq r$. Fix one such partition $\boldsymbol{\nu}$ and set $w = \Sigma(\boldsymbol{\nu})$; then $w \geq hr = sn$. By Proposition 4.5 we can express $M_{\boldsymbol{\nu}}(\pi_L)$ as a sum of terms of the form $d_{\boldsymbol{\lambda\nu}} c_{\boldsymbol{\lambda}}$, where $\boldsymbol{\lambda} = \{\lambda_1, \lambda_2, \dots, \lambda_k\}$ is a partition of w into parts which are $\leq n$. By Proposition 4.3 (1) we have $v_L(d_{\boldsymbol{\lambda\nu}} c_{\boldsymbol{\lambda}}) \geq w \geq sn$. Suppose $v_L(d_{\boldsymbol{\lambda\nu}} c_{\boldsymbol{\lambda}}) = sn$. Then $w = sn$, and by Proposition 4.3 (2) we see that $\boldsymbol{\lambda}$ consists of k copies of n. It follows that $kn = w = sn$, and hence that $k = s$. Therefore $\boldsymbol{\lambda} = \boldsymbol{\kappa}$. Since $\Sigma(\boldsymbol{\nu}) = w = sn = hr$ we get $\boldsymbol{\nu} = \boldsymbol{\mu}$. Since $d_{\boldsymbol{\kappa\mu}} = \pm\binom{u}{v}$ and p divides $\binom{u}{v}$ we have $v_L(d_{\boldsymbol{\kappa\mu}} c_{\boldsymbol{\kappa}}) > v_L(c_{\boldsymbol{\kappa}}) = sn$, a contradiction. Hence $v_L(d_{\boldsymbol{\lambda\nu}} c_{\boldsymbol{\lambda}}) > sn$ holds in all cases. Since $d_{\boldsymbol{\lambda\nu}} c_{\boldsymbol{\lambda}} \in K$ we get $v_K(d_{\boldsymbol{\lambda\nu}} c_{\boldsymbol{\lambda}}) \geq s + 1$. It follows that $E_h(\mathcal{P}_L^r) \subset \mathcal{P}_K^{s+1}$, and hence that $g_h(r) \geq s + 1$. □

References

[1] I. B. Fesenko & S. V. Vostokov, *Local fields and their extensions*, 2nd ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, 2002, xi+345 pages.

[2] M. Fried, "Arithmetical properties of function fields II. The generalized Schur problem", *Acta Arith.* **25** (1974), p. 225-258.

[3] M. Fried & A. Mézard, "Configuration spaces for wildly ramified covers", in *Arithmetic fundamental groups and noncommutative algebra*, Proceedings of Symposia in Pure Mathematics, vol. 70, American Mathematical Society, 2002, p. 353-376.

[4] V. Heiermann, "De nouveaux invariants numériques pour les extensions totalement ramifiées de corps locaux", *J. Number Theory* **59** (1996), no. 1, p. 159-202.

[5] K. Keating, "Indices of inseparability in towers of field extensions", *J. Number Theory* **150** (2015), p. 81-97.

[6] M. Krasner, "Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique: suite de la démonstration", *C. R. Acad. Sci., Paris* **255** (1962), p. 224-226.

[7] A. Kulikauskas & J. Remmel, "Lyndon words and transition matrices between elementary, homogeneous and monomial symmetric functions", *Electron. J. Comb.* **13** (2006), no. 1, Article ID R18, 30 p.

[8] J.-P. SERRE, *Corps Locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, vol. 8, Hermann, 1962, 243 pages.
[9] R. P. STANLEY, *Enumerative combinatorics. Volume 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, 1999, xii+581 pages.

Kevin KEATING
Department of Mathematics
University of Florida
Gainesville, FL 32611, USA
E-mail: keating@ufl.edu
URL: https://people.clas.ufl.edu/keating/