JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Kevin KEATING

Perturbing Eisenstein polynomials over local fields

Tome 30, nº 2 (2018), p. 681-694.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_681_0>

Journal de Théorie des Nombres de Bordeaux **30** (2018), 681–694

Perturbing Eisenstein polynomials over local fields

par Kevin KEATING

Résumé. Soit K un corps local de caractéristique résiduelle p et soit L/K une extension séparable finie totalement ramifiée. Soit π_L une uniformisante de L, de polynôme minimal $f(X)$ sur K. Supposons que $\tilde{\pi}_L$ est une autre uniformisante de L telle que $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\pi_L^{\ell+2}}$ pour certains $\ell \geq 1$ et $r \in \mathcal{O}_K$. Soit $\tilde{f}(X)$ le polynôme minimal de $\tilde{\pi}_L$ sur K. Dans cet article nous donnons des congruences pour les coefficients de $\tilde{f}(X)$ en termes de ℓ, r, et les coefficients de $f(X)$. Ces congruences améliorent le travail de Krasner [8].

Abstract. Let K be a local field whose residue field has characteristic p and let L/K be a finite separable totally ramified extension. Let π_L be a uniformizer for L and let $f(X)$ be the minimum polynomial for π_L over K. Suppose $\tilde{\pi}_L$ is another uniformizer for L such that $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\pi_L^{\ell+2}}$ for some $\ell \geq 1$ and $r \in \mathcal{O}_K$. Let $\tilde{f}(X)$ be the minimum polynomial for $\tilde{\pi}_L$ over K. In this paper we give congruences for the coefficients of $\tilde{f}(X)$ in terms of ℓ, r, and the coefficients of $f(X)$. These congruences improve work of Krasner [8].

1. Introduction

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. 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. 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

$$\tilde{f}(X) = X^n - \tilde{c}_1X^{n-1} + \cdots + (-1)^{n-1}\tilde{c}_{n-1}X + (-1)^n \tilde{c}_n$$

be the minimum polynomial of $\tilde{\pi}_L$ over K. In this paper we use the techniques developed in [7] to obtain congruences for the coefficients of $\tilde{f}(X)$ in terms of ℓ, r, and the coefficients of $f(X)$.

Manuscrit reçu le 8 janvier 2017, révisé le 6 mars 2017, accepté le 16 juin 2017.

2010 *Mathematics Subject Classification.* 11S15, 11S05.

Mots-clefs. local fields, Eisenstein polynomials, symmetric polynomials, indices of inseparability, digraphs.

The Hasse–Herbrand function $\varphi_{L/K} : [-1, \infty) \to [-1, \infty)$ of L/K is defined in Chapter IV of [10] for finite Galois extensions, and in the appendix to [1] for finite separable extensions. Krasner [8, p. 157] showed that for $1 \le h \le n$ we have $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\kappa_h(\ell)}}$, where $\kappa_h(\ell) = \lceil \varphi_{L/K}(\ell) + \frac{h}{n} \rceil$. In Theorem 4.3 we prove that $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$ for certain integers $\rho_h(\ell)$ such that $\rho_h(\ell) \ge \kappa_h(\ell)$. Let h be the unique integer such that $1 \le h \le n$ and n divides $n\varphi_{L/K}(\ell) + h$. Krasner [8, p. 157] gave a formula for the congruence class modulo $\mathcal{P}_K^{\kappa_h(\ell)+1}$ of $\tilde{c}_h - c_h$. In Theorem 4.5 we give similar formulas for up to $v_p(n) + 1$ values of h.

Heiermann [4] gave formulas which are analogous to the results presented here. Let $S \subset \mathcal{O}_K$ be the set of Teichmüller representatives for $\overline{K}$. Let π_K be a uniformizer for K and let $\mathcal{F}(X)$ be the unique power series with coefficients in S such that $\pi_K = \pi_L^n \mathcal{F}(\pi_L)$. Suppose $\tilde{\pi}_L$ is another uniformizer for L such that $\tilde{\pi}_L \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{P}_L^{\ell+2}}$ for some $\ell \ge 1$ and $r \in S$. Let $\tilde{\mathcal{F}}$ be the series with coefficients in S such that $\pi_K = \tilde{\pi}_L^n \tilde{\mathcal{F}}(\tilde{\pi}_L)$. Using Theorem 4.6 of [4] one can compute some coefficients of $\tilde{\mathcal{F}}$ in terms of r and the coefficients of $\mathcal{F}$.

In Section 2 we recall some facts about symmetric polynomials from [7]. The main focus is on expressing monomial symmetric polynomials in terms of elementary symmetric polynomials. In Section 3 we define the indices of inseparability of L/K and some generalizations of the Hasse–Herbrand function $\varphi_{L/K}$. In Section 4 we prove our main results. In Section 5 we give some examples which illustrate how the theorems from Section 4 are applied.

2. Symmetric polynomials and cycle digraphs

Let $n \ge 1$, let $w \ge 1$, and let $\boldsymbol{\mu}$ be a partition of w. We view $\boldsymbol{\mu}$ as a multiset of positive integers such that the sum of the elements of $\boldsymbol{\mu}$ is equal to w. The number of parts of $\boldsymbol{\mu}$ is called the length of $\boldsymbol{\mu}$, and is denoted by $|\boldsymbol{\mu}|$. For $\boldsymbol{\mu}$ such that $|\boldsymbol{\mu}| \le n$ we let $m_{\boldsymbol{\mu}}(X_1, \dots, X_n)$ be the monomial symmetric polynomial in n variables associated to $\boldsymbol{\mu}$; see [11, Section 7.3] for the definition and general facts about monomial symmetric polynomials. For $1 \le h \le n$ let $e_h(X_1, \dots, X_n)$ denote the elementary symmetric polynomial of degree h in n variables. By the fundamental theorem of symmetric polynomials there is a unique polynomial $\psi_{\boldsymbol{\mu}} \in \mathbb{Z}[X_1, \dots, X_n]$ such that $m_{\boldsymbol{\mu}} = \psi_{\boldsymbol{\mu}}(e_1, \dots, e_n)$. In this section we use a theorem of Kulikauskas and Remmel [9] to compute certain 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 $\operatorname{sgn}(\Gamma) = (-1)^{w-c}$, 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

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{|\boldsymbol{\lambda}|+|\boldsymbol{\mu}|} \cdot \sum_{\Gamma} \operatorname{sgn}(\Gamma) \eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma), \tag{2.1}$$

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 $d_{\boldsymbol{\mu}\boldsymbol{\lambda}} = d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$. In Theorem 1 (ii) of [9], Kulikauskas and Remmel proved the following:

Theorem 2.1. *Let $n \geq 1$, let $w \geq 1$, and let $\boldsymbol{\mu}$ be a partition of w whose length is $\leq n$. 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 $1 \leq \lambda_i \leq n$ for $1 \leq i \leq k$.

We now recall some formulas from [7] for computing values of $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma)$.

Proposition 2.2. *Let a, b, c, d, w be positive integers such that $a \neq c$, $b \neq d$, and let r, s be nonnegative integers. Let Γ be a directed cycle of length w.*

(1) *Suppose $w = ra = sb + d$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of r copies of a, and let $\boldsymbol{\mu}$ be the partition of w consisting of s copies of b and one copy of d. Then $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = a$.*
(2) *Suppose $w = ra + c = sb + d$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of r copies of a and one copy of c, and let $\boldsymbol{\mu}$ be the partition of w consisting of s copies of b and one copy of d. Then $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = w$.*

Proof. Statement (1) follows from Proposition 2.5 of [7] if $s = 0$, and from Proposition 2.3 of [7] if $s \geq 1$. Statement (2) follows from Proposition 2.2 of [7]. □

Using these formulas we can compute $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ in some cases.

Proposition 2.3. *Let a, b, c, d, w be positive integers such that $a \neq c$ and $b \neq d$. Let r, s be nonnegative integers such that $w = ra + c = sb + d$ and $a > sb$. Let $\boldsymbol{\lambda}$ be the partition of w consisting of r copies of a and 1 copy of c, and let $\boldsymbol{\mu}$ be the partition of w consisting of s copies of b and 1 copy of d. Then*

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = \begin{cases} (-1)^{r+s+w+1} w & \text{if } b \nmid c \text{ or } sb < c, \\ (-1)^{r+s+w+1}(w - ab) & \text{if } b \mid c \text{ and } sb \geq c. \end{cases}$$

Proof. Let Γ be a cycle digraph which has an admissible $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling. Suppose Γ consists of a single cycle of length w. Then by Proposition 2.2(2) we have $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = w$. Suppose Γ has more than one cycle. Since Γ has a $\boldsymbol{\mu}$-tiling, Γ has a cycle Γ_1 such that $|V(\Gamma_1)| \leq sb$. Since $a > sb$ and Γ has a $\boldsymbol{\lambda}$-tiling, it follows that $|V(\Gamma_1)| = c = mb$ for some m such that $1 \leq m \leq s$. Hence if Γ has more than one cycle we must have $b \mid c$ and $c \leq sb$. Let $\boldsymbol{\lambda}_1$ be the partition of c consisting of one copy of c and let $\boldsymbol{\mu}_1$ be the partition of c consisting of m copies of b. Then every $\boldsymbol{\lambda}$-tiling of Γ restricts to a $\boldsymbol{\lambda}_1$-tiling of Γ_1, and every $\boldsymbol{\mu}$-tiling of Γ restricts to a $\boldsymbol{\mu}_1$-tiling of Γ_1. It follows from Proposition 2.2(1) that $\eta_{\boldsymbol{\lambda}_1\boldsymbol{\mu}_1}(\Gamma_1) = b$.

Let Γ_2 be another cycle of Γ. Since Γ has a $\boldsymbol{\lambda}$-tiling, $|V(\Gamma_2)| \geq a > sb$. Hence every $\boldsymbol{\mu}$-tiling of Γ restricts to a tiling of Γ_2 which includes a path δ with $|V(\delta)| = d$. Since $\boldsymbol{\mu}$ has only one part equal to d, it follows that $\Gamma = \Gamma_1 \cup \Gamma_2$. Therefore we have $|V(\Gamma_2)| = ra = (s - m)b + d$. Let $\boldsymbol{\lambda}_2$ be the partition of ra consisting of r copies of a and let $\boldsymbol{\mu}_2$ be the partition of $(s-m)b+d = ra$ consisting of $s-m$ copies of b and 1 copy of d. Then every $\boldsymbol{\lambda}$-tiling of Γ restricts to a $\boldsymbol{\lambda}_2$-tiling of Γ_2, and every $\boldsymbol{\mu}$-tiling of Γ restricts to a $\boldsymbol{\mu}_2$-tiling of Γ_2. It follows from Proposition 2.2(1) that $\eta_{\boldsymbol{\lambda}_2\boldsymbol{\mu}_2}(\Gamma_2) = a$. Hence

$$\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma) = \eta_{\boldsymbol{\lambda}_1\boldsymbol{\mu}_1}(\Gamma_1) \cdot \eta_{\boldsymbol{\lambda}_2\boldsymbol{\mu}_2}(\Gamma_2) = ba.$$

Suppose $b \nmid c$ or $c > sb$. Then it follows from the above that the only cycle digraph which has a $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling consists of a single cycle of length w. Hence by (2.1) we get

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{(r+1)+(s+1)} \cdot (-1)^{w-1} w.$$

Suppose $b \mid c$ and $sb \geq c$. Then $c = mb$ with $1 \leq m \leq s$. Hence there are two cycle digraphs which have a $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-tiling: a single cycle of length w, and the union of two cycles with lengths $c = mb$ and $ra = (s - m)b + d$.

Therefore by (2.1) we get

$$d_{\boldsymbol{\lambda\mu}} = (-1)^{(r+1)+(s+1)}((-1)^{w-1}w + (-1)^{w-2}ab).$$

Hence the formula for $d_{\boldsymbol{\lambda\mu}}$ given in the theorem holds in both cases. □

We recall some results from [7] regarding the p-adic properties of the coefficients $d_{\boldsymbol{\lambda\mu}}$. Let $w \geq 1$ and let $\boldsymbol{\lambda}$ be a partition of w. For $k \geq 1$ let $k * \boldsymbol{\lambda}$ be the partition of kw which is the multiset sum of k copies of $\boldsymbol{\lambda}$, and let $k \cdot \boldsymbol{\lambda}$ be the partition of kw obtained by multiplying the parts of $\boldsymbol{\lambda}$ by k.

Proposition 2.4. *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 $d_{\boldsymbol{\lambda\mu}}$.*

Proof. This is proved in Corollary 3.4 of [7]. □

Proposition 2.5. *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 $d_{\boldsymbol{\lambda\mu}} \equiv d_{\boldsymbol{\lambda}'\boldsymbol{\mu}'} \pmod{p^{t+1}}$.*

Proof. This is proved in Proposition 3.5 of [7]. □

3. Indices of inseparability

Let L/K be a totally ramified extension of degree $n = up^\nu$, with $p \nmid u$. Let π_L be a uniformizer for L whose minimum polynomial over K is

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

For $k \in \mathbb{Z}$ define $\overline{v}_p(k) = \min\{v_p(k), \nu\}$. For $0 \leq j \leq \nu$ set

$$\begin{aligned} i_j^{\pi_L} &= \min\{nv_K(c_h) - h : 1 \leq h \leq n,\ \overline{v}_p(h) \leq j\} \\ &= \min\{v_L(c_h\pi_L^{n-h}) : 1 \leq h \leq n,\ \overline{v}_p(h) \leq j\} - n. \end{aligned} \tag{3.1}$$

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. 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

$$i_j = \min\{i_{j'}^{\pi_L} + (j' - j)e_L : j \leq j' \leq \nu\}. \tag{3.2}$$

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]; for the characteristic-p case see also [2, p. 232–233] and [3, Section 2]. Write $i_j = A_jn - b_j$ with $1 \leq b_j \leq n$.

Remark 3.1. If $i_j^{\pi_L}$ is finite we can write $i_j^{\pi_L} = a_jn - b_j$ with $a_j \geq 1$ (see [7, Section 4]). Thus if $i_j = i_{j'}^{\pi_L} + (j' - j)e_L$ then $A_j = a_{j'} + (j' - j)e_K$.

The following facts are easy consequences of the definitions:

(1) $0 = i_\nu < i_{\nu-1} \leq \ldots \leq i_1 \leq i_0 < \infty$.

(2) If $\mathrm{char}(K) = p$ then $i_j = i_j^{\pi_L}$.

(3) Let $m = \overline{v}_p(i_j)$. If $m \leq j$ then $i_j = i_m = i_j^{\pi_L} = i_m^{\pi_L}$. If $m > j$ then $\mathrm{char}(K) = 0$ and $i_j = i_m^{\pi_L} + (m-j)e_L$.

Following [4, (4.4)], for $0 \leq j \leq \nu$ we define functions $\tilde{\varphi}_j : [0,\infty) \to [0,\infty)$ by $\tilde{\varphi}_j(x) = i_j + p^j x$. The generalized Hasse–Herbrand functions $\varphi_j : [0,\infty) \to [0,\infty)$ are then defined by

$$\varphi_j(x) = \min\{\tilde{\varphi}_{j_0}(x) : 0 \leq j_0 \leq j\}. \tag{3.3}$$

It follows that $\varphi_j(x) \leq \varphi_{j'}(x)$ for $0 \leq j' \leq j$. By Corollary 6.11 of [4] we have $\varphi_\nu(x) = n\varphi_{L/K}(x)$ for all $x \geq 0$.

For a partition $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ whose parts satisfy $1 \leq \lambda_i \leq n$ define $c_{\boldsymbol{\lambda}} = c_{\lambda_1} c_{\lambda_2} \ldots c_{\lambda_k}$. The following is proved in Proposition 4.2 of [7].

Proposition 3.2. *Let $w \geq 1$ and let $\boldsymbol{\lambda} = \{\lambda_1, \ldots, \lambda_k\}$ be a partition of w whose parts satisfy $1 \leq \lambda_i \leq n$. Choose q to minimize $\overline{v}_p(\lambda_q)$ and set $t = \overline{v}_p(\lambda_q)$. Then $v_L(c_{\boldsymbol{\lambda}}) \geq i_t^{\pi_L} + w$. 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 $i \neq q$.*

4. Perturbing π_L

In this section we prove our main theorems. We begin by applying the results of Section 2 to the totally ramified extension L/K. Write $[L:K] = n = up^\nu$ with $p \nmid u$. Let π_L, $\tilde{\pi}_L$ be uniformizers for L, with minimum polynomials over K given by

$$f(X) = X^n - c_1 X^{n-1} + \cdots + (-1)^{n-1} c_{n-1} X + (-1)^n c_n$$
$$\tilde{f}(X) = X^n - \tilde{c}_1 X^{n-1} + \cdots + (-1)^{n-1} \tilde{c}_{n-1} X + (-1)^n \tilde{c}_n.$$

Let $1 \leq h \leq n$ and set $j = \overline{v}_p(h)$. Define a function $\rho_h : \mathbb{N} \to \mathbb{N}$ by

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

Let $\ell \geq 1$. We say $\tilde{f} \sim_\ell f$ if $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$ for $1 \leq h \leq n$. Thus $\sim_\ell$ is an equivalence relation on the set of minimum polynomials over K for uniformizers of L.

Let $\sigma_1, \ldots, \sigma_n$ be the K-embeddings of L into K^{sep}. For each partition $\boldsymbol{\mu}$ of length $\leq n$ define $M_{\boldsymbol{\mu}} : L \to K$ by

$$M_{\boldsymbol{\mu}}(\alpha) = m_{\boldsymbol{\mu}}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

For $1 \leq h \leq n$ define $E_h : L \to K$ by

$$E_h(\alpha) = e_h(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

Then $c_h = E_h(\pi_L)$ and $\tilde{c}_h = E_h(\tilde{\pi}_L)$.

Proposition 4.1. *Let $\varphi(X) = r_1X + r_2X^2 + \cdots$ be a power series with coefficients in $\mathcal{O}_K$ such that $\tilde{\pi}_L = \varphi(\pi_L)$. Then for $1 \le h \le n$ we have*

$$E_h(\tilde{\pi}_L) = \sum_{\boldsymbol{\mu}} r_{\mu_1} r_{\mu_2} \dots r_{\mu_h} M_{\boldsymbol{\mu}}(\pi_L),$$

where the sum ranges over all partitions $\boldsymbol{\mu} = \{\mu_1, \dots, \mu_h\}$ of length h.

Proof. This is a special case of Proposition 4.4 in [7]. □

Proposition 4.2. *Let $n \ge 1$, let $w \ge 1$, and let $\boldsymbol{\mu}$ be a partition of w whose length is $\le n$. Then*

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

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

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

Let $\ell \ge 1$. Our first main result gives congruences between the coefficients of $f(X)$ and the coefficients of $\tilde{f}(X)$ under the assumption $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^{\ell+1}}$.

Theorem 4.3. *Let π_L, $\tilde{\pi}_L$ be uniformizers for L and let $f(X)$, $\tilde{f}(X)$ be the minimum polynomials for π_L, $\tilde{\pi}_L$ over K. Suppose there are $\ell \ge 1$ and $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\tilde{\pi}_L) \equiv \pi_L \pmod{\mathcal{P}_L^{\ell+1}}$. Then $\tilde{f} \sim_\ell f$.*

Proof. We first show that the theorem holds in the case where $\tilde{\pi}_L = \pi_L + r\pi_L^{\ell+1}$, with $r \in \mathcal{O}_K$. Let $1 \le h \le n$ and set $j = \overline{v}_p(h)$. For $0 \le s \le h$ let $\boldsymbol{\mu}_s$ be the partition of $\ell s + h$ consisting of $h - s$ copies of 1 and s copies of $\ell + 1$. Then by Proposition 4.1 we have

$$\tilde{c}_h = E_h(\tilde{\pi}_L) = \sum_{s=0}^{h} M_{\boldsymbol{\mu}_s}(\pi_L) r^s = c_h + \sum_{s=1}^{h} M_{\boldsymbol{\mu}_s}(\pi_L) r^s. \tag{4.1}$$

To prove that $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$ it suffices to show that $v_K(M_{\boldsymbol{\mu}_s}(\pi_L)) \ge \rho_h(\ell)$ for $1 \le s \le h$. Therefore by Proposition 4.2 it suffices to show $v_L(d_{\boldsymbol{\lambda}\boldsymbol{\mu}_s} c_{\boldsymbol{\lambda}}) \ge \varphi_j(\ell) + h$ for all $1 \le s \le h$ and all partitions $\boldsymbol{\lambda}$ of $\ell s + h$ whose parts are at most n.

Let $1 \le s \le h$ and set $m = \min\{j, \overline{v}_p(s)\}$. Then $m \le j$ and $s \ge p^m$. Let $\boldsymbol{\lambda} = \{\lambda_1, \dots, \lambda_k\}$ be a partition of $\ell s + h$ such that $1 \le \lambda_i \le n$ for $1 \le i \le k$. Choose q to minimize $\overline{v}_p(\lambda_q)$ and set $t = \overline{v}_p(\lambda_q)$. By Proposition 3.2 we have $v_L(c_{\boldsymbol{\lambda}}) \ge i_t^{\pi_L} + \ell s + h$. Suppose $m < t$. Then $m < \nu$, so we have $p^{m+1} \nmid \gcd(h - s, s)$. Hence by Proposition 2.4 we get $v_p(d_{\boldsymbol{\lambda}\boldsymbol{\mu}_s}) \ge t - m$.

Thus

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

Suppose $m \geq t$. Then

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

In both cases we get

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

and hence $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$. Since this holds for $1 \leq h \leq n$ we get $\tilde{f} \sim_\ell f$.

We now prove the general case. Since $\tilde{f}$ is the minimum polynomial of $\sigma(\tilde{\pi}_L)$ over K we may assume without loss of generality that $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^{\ell+1}}$. By repeated application of the special case above we get a sequence $\pi_L^{(0)} = \pi_L, \pi_L^{(1)}, \pi_L^{(2)}, \dots$ of uniformizers for L with minimum polynomials $f^{(0)} = f, f^{(1)}, f^{(2)}, \dots$ such that for all $i \geq 0$ we have $\pi_L^{(i)} \equiv \tilde{\pi}_L \pmod{\mathcal{P}_L^{\ell+i+1}}$ and $f^{(i+1)} \sim_{\ell+i} f^{(i)}$. It follows that $f^{(i+1)} \sim_\ell f^{(i)}$, and hence that $f^{(i)} \sim_\ell f$ for all $i \geq 0$. Since the sequence $(f^{(i)})$ converges coefficientwise to $\tilde{f}$ it follows that $\tilde{f} \sim_\ell f$. □

Recall that the Hasse–Herbrand function $\varphi_{L/K} : [-1, \infty) \to [-1, \infty)$ is defined for arbitrary finite separable extensions L/K (see for instance the appendix to [1]). We say that $b \geq 0$ is a lower ramification break of L/K if $\varphi'_{L/K}(b)$ is undefined. This extends the usual definition of lower ramification breaks for Galois extensions.

Remark 4.4. It follows from Theorem 4.3 that if $\sigma(\tilde{\pi}_L) \equiv \pi_L \pmod{\mathcal{P}_L^{\ell+1}}$ for some $\sigma \in \mathrm{Aut}_K(L)$ then $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\rho_h(\ell)}}$ for $1 \leq h \leq n$. Define functions $\kappa_h : \mathbb{N} \to \mathbb{N}$ by

$$\kappa_h(\ell) = \left\lceil \frac{\varphi_\nu(\ell) + h}{n} \right\rceil.$$

Krasner [8, p. 157] showed that $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^{\kappa_h(\ell)}}$. Since $\kappa_h(\ell) \leq \rho_h(\ell)$ Krasner's congruences are in general weaker than the congruences that follow from Theorem 4.3. If ℓ is greater than or equal to the largest lower ramification break of L/K then for $0 \leq j \leq \nu$ we have $\varphi_j(\ell) = \varphi_\nu(\ell)$, and hence $\kappa_h(\ell) = \rho_h(\ell)$. Therefore Theorem 4.3 does not improve on Krasner's results in these cases.

For certain values of h we get a more refined version of the congruences given by Theorem 4.3.

Theorem 4.5. *Let L/K be a finite totally ramified extension of degree $n = up^\nu$. For $0 \le m \le \nu$ write the mth index of inseparability of L/K in the form $i_m = A_m n - b_m$ with $1 \le b_m \le n$. Let π_L, $\tilde{\pi}_L$ be uniformizers for L such that there are $\ell \ge 1$, $r \in \mathcal{O}_K$, and $\sigma \in \mathrm{Aut}_K(L)$ with $\sigma(\tilde{\pi}_L) \equiv \pi_L + r\pi_L^{\ell+1} \pmod{\mathcal{P}_L^{\ell+2}}$. Let $0 \le j \le \nu$ satisfy $\overline{v}_p(\varphi_j(\ell)) = j$, and let h be the unique integer such that $1 \le h \le n$ 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

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

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

Proof. We first prove that the theorem holds for $\hat{\pi}_L = \pi_L + r\pi_L^{\ell+1}$. Let

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

be the minimum polynomial for $\hat{\pi}_L$ over K. Let $1 \le s \le h$ and let $\boldsymbol{\lambda}$ be a partition of $\ell s + h$ whose parts are at most n. Choose q to minimize $\overline{v}_p(\lambda_q)$ and set $t = \overline{v}_p(\lambda_q)$. Recall that $\boldsymbol{\mu}_s$ is the partition of $\ell s + h$ consisting of $h - s$ copies of 1 and s copies of $\ell + 1$. Since $\overline{v}_p(h) = \overline{v}_p(\varphi_j(\ell)) = j$ it follows from the proof of Theorem 4.3 that $v_K(d_{\boldsymbol{\lambda}\boldsymbol{\mu}_s} c_{\boldsymbol{\lambda}}) \ge k$. Suppose $v_K(d_{\boldsymbol{\lambda}\boldsymbol{\mu}_s} c_{\boldsymbol{\lambda}}) = k$. Then the inequalities in the proof of Theorem 4.3 must be equalities. Hence there is $0 \le m \le j$ such that $s = p^m$, $v_L(c_{\boldsymbol{\lambda}}) = i_t^{\pi_L} + \ell p^m + h$, and $\varphi_j(\ell) = \tilde{\varphi}_m(\ell)$.

It follows that $m \in S_j$ and $\boldsymbol{\lambda}$ is a partition of w_m, where

$$w_m = \ell p^m + h = \tilde{\varphi}_m(\ell) - i_m + h = \varphi_j(\ell) + h - i_m = (k - A_m)n + b_m.$$

Let $\boldsymbol{\kappa}_m$ be the partition of w_m consisting of $k - A_m$ copies of n and 1 copy of b_m. By Proposition 3.2 we see that $\boldsymbol{\lambda}$ has at most one element not equal to n. Therefore $\boldsymbol{\lambda} = \boldsymbol{\kappa}_m$. Hence $c_{\boldsymbol{\lambda}} = c_{\boldsymbol{\kappa}_m} = c_n^{k-A_m} c_{b_m}$ and $\overline{v}_p(b_m) = \overline{v}_p(\lambda_q) = t$. Using equation (4.1) and Proposition 4.2 we get

$$\hat{c}_h \equiv c_h + \sum_{m \in S_j} d_{\boldsymbol{\kappa}_m \boldsymbol{\mu}_{p^m}} c_n^{k-A_m} c_{b_m} r^{p^m} \pmod{\mathcal{P}_K^{k+1}}. \tag{4.2}$$

Let $m \in S_j$. Since

$$j = \overline{v}_p(\varphi_j(\ell)) = \overline{v}_p(\tilde{\varphi}_m(\ell)) = \overline{v}_p(i_m + \ell p^m)$$

and $m \leq j$ we get $m \leq \overline{v}_p(i_m) = \overline{v}_p(b_m)$. Hence $b'_m = b_m/p^m$ is an integer. Let $\boldsymbol{\kappa}'_m$ be the partition of

$$w'_m = (k - A_m)up^{\nu-m} + b'_m = h_0 p^{j-m} + \ell$$

consisting of $k - A_m$ copies of $up^{\nu-m}$ and 1 copy of b'_m. Let $\boldsymbol{\mu}'_{p^m}$ be the partition of w'_m consisting of $h_0p^{j-m} - 1$ copies of 1 and 1 copy of $\ell + 1$. Since $h \leq n$ we have $up^{\nu-m} > h_0p^{j-m} - 1$. Hence if $b'_m \neq up^{\nu-m}$ then we can compute $d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}}$ using Proposition 2.3.

Suppose $b_m < h$. Then $h_0p^{j-m} - 1 \geq b'_m$, so by Proposition 2.3 we get

$$d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}} = (-1)^{k+\ell+A_m}(h_0p^{j-m} + \ell - up^{\nu-m}).$$

Suppose $h \leq b_m < n$. Then $h_0p^{j-m} - 1 < b'_m$, so by Proposition 2.3 we get

$$d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}} = (-1)^{k+\ell+A_m}(h_0p^{j-m} + \ell).$$

Suppose $b_m = n$, so that $b'_m = up^{\nu-m}$. Since $up^{\nu-m} > h_0p^{j-m} - 1$, the only cycle digraph which admits a $(\boldsymbol{\kappa}'_m, \boldsymbol{\mu}'_{p^m})$-tiling consists of a single cycle Γ of length w'_m. By Proposition 2.2(1) we get $\eta_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}}(\Gamma) = up^{\nu-m}$. It then follows from (2.1) that

$$d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}} = (-1)^{k+\ell+A_m} up^{\nu-m}.$$

Hence in all three cases we have $d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}} = g_m$.

Since $p^t \mid b_m$ we have $p^{t-m} \mid b'_m$. Therefore by Proposition 2.5 we get

$$d_{\boldsymbol{\kappa}_m \boldsymbol{\mu}_{p^m}} \equiv d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}} \pmod{p^{t-m+1}}. \tag{4.3}$$

Since $m \leq t \leq \nu$ it follows from (3.2) and (3.1) that

$$\begin{aligned} i_m &\leq i_t^{\pi_L} + (t-m)e_L \\ nA_m - b_m &\leq nv_K(c_{b_m}) - b_m + (t-m)e_L \\ A_m &\leq v_K(c_{b_m}) + (t-m)e_K \\ k+1 &\leq k - A_m + v_K(c_{b_m}) + (t-m+1)e_K. \end{aligned} \tag{4.4}$$

Using (4.3) and (4.4) we get

$$\begin{aligned} d_{\boldsymbol{\kappa}_m \boldsymbol{\mu}_{p^m}} c_n^{k-A_m} c_{b_m} &\equiv d_{\boldsymbol{\kappa}'_m \boldsymbol{\mu}'_{p^m}} c_n^{k-A_m} c_{b_m} && \pmod{\mathcal{P}_K^{k+1}} \\ &\equiv g_m c_n^{k-A_m} c_{b_m} && \pmod{\mathcal{P}_K^{k+1}}. \end{aligned}$$

Hence by (4.2) the theorem holds when $\tilde{\pi}_L = \hat{\pi}_L$.

We now prove the theorem in the general case. We may assume that

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

It follows that $\tilde{\pi}_L \equiv \hat{\pi}_L \pmod{\mathcal{P}_L^{\ell+2}}$, so by Theorem 4.3 we get $\tilde{c}_h \equiv \hat{c}_h \pmod{\mathcal{P}_K^{\rho_h(\ell+1)}}$. Since

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

and $\varphi_j(\ell+1) > \varphi_j(\ell)$ we get $\rho_h(\ell+1) > k$. Therefore $\tilde{c}_h \equiv \hat{c}_h \pmod{\mathcal{P}_K^{k+1}}$, so the theorem holds for $\tilde{\pi}_L$. □

Remark 4.6. Suppose $\overline{v}_p(\varphi_j(\ell)) = j' \leq j$. Then $\varphi_j(\ell) = \varphi_{j'}(\ell)$. In particular, $\varphi_\nu(\ell) = \varphi_{j'}(\ell)$ with $j' = \overline{v}_p(\varphi_\nu(\ell))$. Hence if $1 \leq h \leq n$ and n divides $\varphi_\nu(\ell)+h$ then Theorem 4.5 gives a congruence for $\tilde{c}_h$ modulo $\mathcal{P}_K^{k+1}$, where $k = (\varphi_\nu(\ell)+h)/n$. This is the congruence obtained by Krasner [8, p. 157]. If ℓ is greater than or equal to the largest lower ramification break of L/K then $\varphi_j(\ell) = \varphi_\nu(\ell)$ for $0 \leq j \leq \nu$. Therefore Theorem 4.5 does not extend [8] in these cases.

5. Some examples

In this section we give two examples related to the theorems proved in Section 4. We first apply these theorems to a 3-adic extension of degree 9.

Example 5.1. 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 $\varphi_j(\ell)$:

ℓ	$\tilde{\varphi}_0(\ell)$	$\tilde{\varphi}_1(\ell)$	$\tilde{\varphi}_2(\ell)$	$\varphi_0(\ell)$	$\varphi_1(\ell)$	$\varphi_2(\ell)$
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

$$\tilde{f}(X) = X^9 - \tilde{c}_1X^8 + \cdots + \tilde{c}_8X - \tilde{c}_9.$$

Suppose $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^2}$. Then by Theorem 4.3 we get $\tilde{f} \sim_1 f$. Using the table above we find that

$$\begin{aligned} \tilde{c}_h &\equiv c_h \pmod{\mathcal{P}_K^2} \quad \text{for } h \in \{1,3,9\}, \\ \tilde{c}_h &\equiv c_h \pmod{\mathcal{P}_K^3} \quad \text{for } h \in \{2,4,5,6,7,8\}. \end{aligned}$$

This is an improvement on [8], which gives $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^2}$ for $1 \le h \le 9$. If $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^3}$ we get $\tilde{f} \sim_2 f$, and hence $\tilde{c}_h \equiv c_h \pmod{\mathcal{P}_K^3}$ for $1 \le h \le 9$. If $\tilde{\pi}_L \equiv \pi_L \pmod{\mathcal{P}_L^4}$ we get $\tilde{f} \sim_3 f$, and hence

$$\begin{aligned} \tilde{c}_h &\equiv c_h \pmod{\mathcal{P}_K^3} \quad \text{for } 1 \le h \le 8, \\ \tilde{c}_9 &\equiv c_9 \pmod{\mathcal{P}_K^4}. \end{aligned}$$

Since the largest lower ramification break of L/K is 2, the congruences we get for $\ell \ge 2$ are the same as those in [8].

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 $\overline{v}_3(\varphi_0(1)) = 0$, $\overline{v}_3(\varphi_1(1)) = 1$, $\overline{v}_3(\varphi_2(1)) = 2$ and $S_0 = \{0\}$, $S_1 = \{1\}$, $S_2 = \{2\}$. The corresponding values of h are 1, 3, 9, and we have $h_0 = 1$, $k = 2$ in all three cases. By applying Theorem 4.5 with $\ell = 1$, $j = 0, 1, 2$ we get the following congruences:

$$\begin{aligned} \tilde{c}_1 &\equiv c_1 + (-1)^{2+1+2}(1+1)c_2 r && \pmod{\mathcal{P}_K^3} \\ &\equiv c_1 - 2c_2 r && \pmod{\mathcal{P}_K^3} \\ \tilde{c}_3 &\equiv c_3 + (-1)^{2+1+2}(1+1)c_6 r^3 && \pmod{\mathcal{P}_K^3} \\ &\equiv c_3 - 2c_6 r^3 && \pmod{\mathcal{P}_K^3} \\ \tilde{c}_9 &\equiv c_9 + (-1)^{2+1+1} c_9^2 r^9 && \pmod{\mathcal{P}_K^3} \\ &\equiv c_9 + c_9^2 r^9 && \pmod{\mathcal{P}_K^3}. \end{aligned}$$

Only the congruence for $\tilde{c}_9$ follows from [8].

Suppose $\tilde{\pi}_L \equiv \pi_L + r\pi_L^3 \pmod{\mathcal{P}_L^4}$. Then $\overline{v}_3(\varphi_2(2)) = 2$ and $S_2 = \{0,1,2\}$, which gives $h = 9$, $h_0 = 1$, and $k = 3$. By applying Theorem 4.5 with $\ell = 2$, $j = 2$ we get the following congruence:

$$\begin{aligned} \tilde{c}_9 \equiv c_9 &+ (-1)^{3+2+2}(9+2-9)c_9 c_2 r \\ &+ (-1)^{3+2+2}(3+2-3)c_9 c_6 r^3 + (-1)^{3+2+1} c_9^2 c_9 r^9 && \pmod{\mathcal{P}_K^4} \\ \equiv c_9 &- 2c_2 c_9 r - 2c_6 c_9 r^3 + c_9^3 r^9 && \pmod{\mathcal{P}_K^4}. \end{aligned}$$

Suppose $\tilde{\pi}_L \equiv \pi_L + r\pi_L^4 \pmod{\mathcal{P}_L^5}$. Then $\overline{v}_3(\varphi_0(3)) = 0$ and $S_0 = \{0\}$, so we get $h = 8$, $h_0 = 8$, and $k = 3$. By applying Theorem 4.5 with $\ell = 3$, $j = 0$ we get the following congruence:

$$\begin{aligned} \tilde{c}_8 &\equiv c_8 + (-1)^{3+3+2}(8+3-9)c_9 c_2 r && \pmod{\mathcal{P}_K^4} \\ &\equiv c_8 + 2c_2 c_9 r && \pmod{\mathcal{P}_K^4}. \end{aligned}$$

Again, since the largest lower ramification break of L/K is 2, the congruences we get for $\ell \geq 2$ are the same as those in [8].

One might hope to prove the following converse to Theorem 4.3: If π_L, $\tilde{\pi}_L$ are uniformizers for L whose minimum polynomials satisfy $\tilde{f} \sim_\ell f$, then there is $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\tilde{\pi}_L) \equiv \pi_L \pmod{\mathcal{P}_L^{\ell+1}}$. The example below shows that this is not necessarily the case:

Example 5.2. Let π_L be a root of the Eisenstein polynomial $f(X) = X^4 + 6X^2 + 4X + 2$ over the 2-adic field $\mathbb{Q}_2$. Then $L = \mathbb{Q}_2(\pi_L)$ is a totally ramified extension of $\mathbb{Q}_2$ of degree 4, with indices of inseparability $i_0 = 5$, $i_1 = 2$, and $i_2 = 0$. We get the following values for $\tilde{\varphi}_j(\ell)$ and $\varphi_j(\ell)$:

ℓ	$\tilde{\varphi}_0(\ell)$	$\tilde{\varphi}_1(\ell)$	$\tilde{\varphi}_2(\ell)$	$\varphi_0(\ell)$	$\varphi_1(\ell)$	$\varphi_2(\ell)$
0	5	2	0	5	2	0
1	6	4	4	6	4	4
2	7	6	8	7	6	6
3	8	8	12	8	8	8

Set $\tilde{\pi}_L = \pi_L + \pi_L^2$, and let the minimum polynomial for $\tilde{\pi}_L$ over $\mathbb{Q}_2$ be

$$\tilde{f}(X) = X^4 - \tilde{c}_1 X^3 + \tilde{c}_2 X^2 - \tilde{c}_3 X + \tilde{c}_4.$$

By Theorem 4.3 we have $\tilde{f} \sim_1 f$, and hence

$$\begin{aligned} \tilde{c}_1 &\equiv 0 \pmod{4} \\ \tilde{c}_2 &\equiv 6 \pmod{4} \\ \tilde{c}_3 &\equiv -4 \pmod{8} \\ \tilde{c}_4 &\equiv 2 \pmod{4}. \end{aligned}$$

Theorem 4.5 gives a refinement of the last congruence:

$$\begin{aligned} \tilde{c}_4 &\equiv 2 + (-1)^{2+1+1}(2+1-2) \cdot 2^{2-1} \cdot 6 + (-1)^{2+1+1} \cdot 2^{2-1} \cdot 2 \pmod{8} \\ &\equiv 2 \pmod{8}. \end{aligned}$$

Using this refinement we get $\tilde{f} \sim_2 f$.

Using [5] (see also [6, Table 4.2]) we obtain a list of the degree-4 extensions of $\mathbb{Q}_2$. Using the data in this list we find that $L/\mathbb{Q}_2$ is not Galois, and the only quadratic subextension of $L/\mathbb{Q}_2$ is $M/\mathbb{Q}_2$, where $M = \mathbb{Q}_2(\sqrt{-1})$. Hence $\mathrm{Aut}_{\mathbb{Q}_2}(L) = \mathrm{Gal}(L/M)$. Since the lower ramification breaks of $L/\mathbb{Q}_2$ are 1, 3, and the lower ramification break of $M/\mathbb{Q}_2$ is 1, the lower ramification break of L/M is 3. Hence if $\sigma \in \mathrm{Aut}_{\mathbb{Q}_2}(L)$ then $\sigma(\tilde{\pi}_L) \equiv \tilde{\pi}_L \pmod{\mathcal{P}_L^4}$. Since $\tilde{\pi}_L = \pi_L + \pi_L^2$ we get $\sigma(\tilde{\pi}_L) \not\equiv \pi_L \pmod{\mathcal{P}_L^3}$.

References

[1] P. DELIGNE, "Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0", in *Représentations des groups réductifs sur un corps local*, Travaux en Cours, Hermann, 1984, p. 119-157.

[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 (Berkeley, 1999)*, 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] J. W. JONES & D. P. ROBERTS, "Database of Local Fields", https://math.la.asu.edu/jj/localfields/, Retrieved 31 December 2016.

[6] ———, "A database of local fields", *J. Symb. Comput.* **41** (2006), no. 1, p. 80-97.

[7] K. KEATING, "Extensions of local fields and elementary symmetric polynomials", *J. Théor. Nombres Bordx* **30** (2018), no. 2, p. 431-448.

[8] M. KRASNER, "Sur la primitivité des corps $\mathfrak{P}$-adiques", *Mathematica* **13** (1937), p. 72-191.

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

[10] J.-P. SERRE, *Corps Locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, vol. 8, Hermann, 1962, 243 pages.

[11] 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/