Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Computing Galois groups of Eisenstein polynomials over p-adic fields

Chad Awtrey, Jonathan Milstead, and Sebastian Pauli

Abstract

We present a degree independent algorithm for computing Galois groups of Eisenstein polynomials over p-adic fields that combines the ramification polygon approach and resolvent methods.

1. *Introduction*

The most efficient algorithms for computing Galois groups of polynomials over global fields are based on Stauduhar's relative resolvent method [25][9][7]. These methods are not directly generalizable to the local field case, since they require a field that contains the global fields in which all roots of the polynomial can be approximated.

Let $\mathbb{Q}_p$ be the field of p-adic numbers, K a finite extension of $\mathbb{Q}_p$, $\varphi \in K[x]$ Eisenstein, and α a root of φ. We present an algorithm that determines the Galois group $\mathrm{Gal}(K(\alpha)/K) = \mathrm{Gal}(\varphi)$ that is the automorphism group $\mathrm{Aut}(N/K)$ of the normal closure N of $K(\alpha)/K$.

Previous algorithms for computing Galois groups of local fields were restricted either to extensions of low degree (up to 14) or to polynomials of special form. Algorithms for degrees up to 11 were given by Jones and Roberts [16][17][15] and were followed by methods for polynomials of degree 12 and 14 by Awtrey and others [1][2][3][5]. All these use a variety of criteria for narrowing down the possible Galois groups, including information about the ramification filtration and absolute resolvents. The algorithms for computing Galois groups of Eisenstein polynomial make use of the the information contained in the ramification polygon, that is the Newton polygon to obtain information about the splitting field of φ. Romano [23] describes $\mathrm{Gal}(\phi)$ for Eisenstein polynomials φ where $\mathcal{R}(\varphi)$ has one segment and the only points on the segments are the endpoints. The algorithm by Greve and Pauli [11] very efficiently returns the Galois group of polynomials where $\mathcal{R}(\varphi)$ consists of one segment. In his thesis [10] Greve builds on this approach to give and algorithm for Eisenstein polynomials whose ramification polygon consists of two segments.

Our Algorithm

We combine ideas from all the above approaches in an algorithm that determines the Galois group $\mathrm{Gal}(\varphi) = \mathrm{Gal}(K(\alpha)/K)$ of an Eisenstein polynomial φ. An essential additional ingredient is the tower of subfields that corresponds to the ramification polygon of φ [11]. In the remainder of this paper we will fill in the details of the following algorithm:

Algorithm 1.1 `GaloisGroup`.

Input: $\varphi \in \mathcal{O}_K[x]$ Eisenstein

2000 *Mathematics Subject Classification* 00000.

Output: $\mathrm{Gal}(\varphi)$

(1) $G = \{id\}$.
(2) Find the tower of subfields $K = L_{\ell+1} \subseteq L_\ell \subset L_{\ell-1} \subset \dots L_1 \subset L_0 = K(\alpha)$ corresponding to the ramification polygon of φ such that the ramification polygon of L_i/L_{i+1} $(0 \le i \le \ell)$ consists of one segment.
(3) For i from ℓ to 0 by -1:
   (a) Determine $\mathrm{Gal}(L_i/L_{i+1})$.
   (b) Find a small set $\mathcal{G}$ of subgroups of $\mathrm{Gal}(L_i/L_{i+1}) \wr G$ that contains the Galois group of L_i/K.
   (c) If $\#\mathcal{G} \neq 1$ use relative resolvents to determine the $G \in \mathcal{G}$ that is the Galois group of L_i/K.
(4) Return G.

In section 2 we recall the results about the existence of such a tower of subfields of K and describe a method for computing generating polynomials for the relative extensions in the tower. The ramification polygon of these polynomials consists of one segment and their Galois groups can be efficiently computed with the methods from [11] (section 3). In Algorithm 1.1 we iteratively compute Galois groups of towers of extensions consisting of an extension whose generating polynomial has a ramification polygon consisting of one segment over an extension with a known Galois group. The Galois group of the tower is contained in the wreath product of the two Galois groups. In section 4 we give criteria that a subgroup of the wreath product must meet in order to possibly be the Galois group of the tower and find that these narrow the number of possible groups considerably. If more than one candidate group is left we use relative resolvents (section 5) to determine the Galois group. Our algorithm is illustrated with some examples in section 6.

Notation

We denote by $\mathbb{Q}_p$ the field of p-adic numbers and by v_p the (exponential) valuation normalized such that $v_p(p) = 1$. By K we denote a finite extension of $\mathbb{Q}_p$, by $\mathcal{O}_K$ the valuation ring of K, and by π a uniformizer of $\mathcal{O}_K$. We write v_K for the valuation of K that is normalized such that $v_K(\pi) = 1$ and also denote the unique extension of v_K to an algebraic closure $\overline{K}$ of K (or to any intermediate field) by v_K. Fractions are always assumed to be in lowest terms. For $\gamma \in \mathcal{O}_K$ we denote by $\underline{\gamma}$ the class $\gamma + (\pi)$ in $\underline{K} = \mathcal{O}_K/(\pi)$.

2. *Ramification Polygons and Subfields*

Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree $e_0 p^m$ where $\gcd(p, m) = 1$, α a root of φ and $L = K(\alpha)$. The *ramification polygon* $\mathcal{R}(\varphi)$ of φ is the Newton polygon of the *ramification polynomial* $\rho(x) = \varphi(\alpha x + \alpha)/(\alpha^n) \in K(\alpha)[x]$ of φ, where α is a root of φ. The ramification polygon $\mathcal{R}(\varphi)$ of φ is an invariant of L/K called the ramification polygon of L/K denoted by $\mathcal{R}(L/K)$. The general shape of a ramification polygon of an Eisenstein polynomial is given in Figure 1, see for example [11].

The ramification data obtained from slopes of the segments of the ramification polygon is complemented by the data obtained from the residual (or associated) polynomials that were introduced by Ore [20].

Definition 2.1. Let L be a finite extension of $\mathbb{Q}_p$ with uniformizer α. Let $\rho(x) = \sum_i \rho_i x^i \in \mathcal{O}_L[x]$. Let $\mathcal{S}$ be a segment of the Newton polygon of ρ of length l with endpoints $(k, v_\alpha(\rho))$

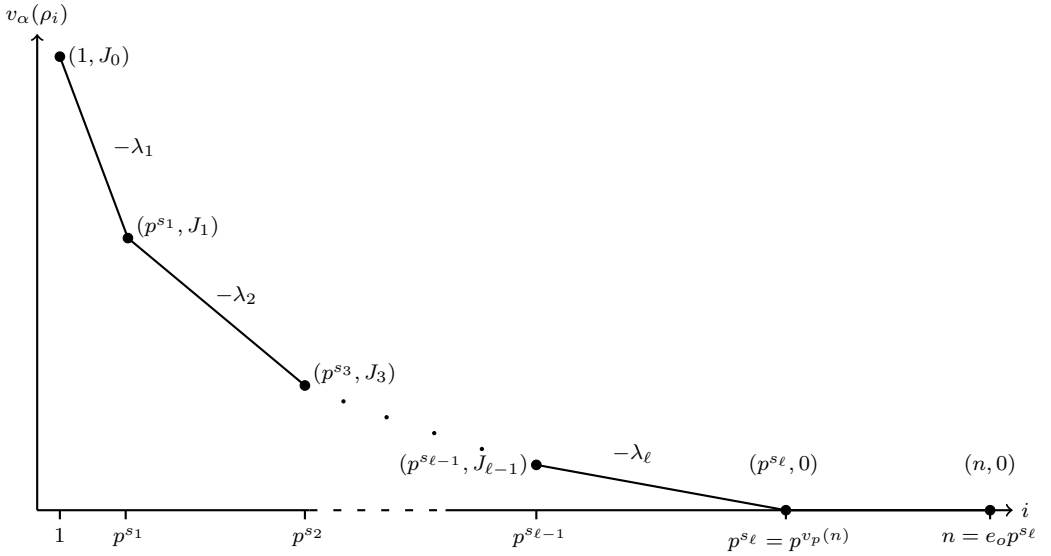

FIGURE 1. *Ramification polygon of an Eisenstein polynomial φ of degree n and discriminant $(\pi)^{n+J_0-1}$ with $\ell+1$ segments and $u-1$ points on the polygon with ordinate above 0.*

and $(k+l, v_\alpha(\rho_{k+l}))$, and slope $-h/e = (v_\alpha(\rho_{k+l}) - v_\alpha(\rho_k))/l$ then

$$\underline{A}(x) = \sum_{j=0}^{l/e} \underline{\rho_{je+k}\alpha^{jh-v_\alpha(\rho_k)}} x^j \in \underline{K}[x]$$

is called the *residual polynomial* of $\mathcal{S}$.

While the residual polynomials of the segments of the ramification polygon are not invariants of the extension generated by an Eisenstein polynomial they are representatives of the *residual polynomial classes* which are invariants of the extension [22].

Now let $\mathcal{S}_1, \ldots, \mathcal{S}_\ell, \mathcal{S}_{\ell+1}$ be the segments of the ramification polygon $\mathcal{R}$ of φ where $\mathcal{S}_{\ell+1}$ may have length 0. Denote by by $-\lambda_1 < \cdots < -\lambda_{\ell+1} = 0$ the slopes of the segments, and by $\underline{A}_1, \ldots, \underline{A}_\ell$ their residual polynomials (see Figure 1). The Galois group of φ has the blocks [11, Lemma 5.2]

$$\Delta_i = \{\alpha' \in \overline{K} : \varphi(\alpha') = 0 \text{ and } \nu_L(\alpha' - \alpha_1) \geq \lambda_i + 1\} \quad (1 \leq i \leq \ell).$$

We can order the roots $\alpha_1, \ldots, \alpha_n$ such that

$$\Delta_i^{(r)} = \left\{\alpha_{(r-1)p^{s_i}+1}, \ldots, \alpha_{rp^{s_i}}\right\} \tag{2.1}$$

for $1 \leq r \leq k$ and $k = n/p^{s_i}$. Similarly to the normal case these blocks correspond to a tower of subfields as illustrated in Figure 2 [11, Theorem 5.4]. Each relative extension in the tower has a ramification polygon consisting of one segment:

THEOREM 2.2 [11, Theorem 6.2]. *For $1 \leq i \leq \ell+1$ the ramification polygon $\mathcal{R}(L_{i-1}/L_i)$ consists of exactly one segment, which corresponds to the segment S_i of $\mathcal{R}(L/K)$ as follows:*

(a) *The slope of $\mathcal{R}(L_{i-1}/L_i)$ is equal to the slope of S_i.*
(b) *For each root $\underline{\delta}$ of the residual polynomial $\underline{A}_i(y)$ of S_i the element $\underline{\delta}^{p^{s_{i-1}}}$ is a root of the residual polynomial of $\mathcal{R}(L_{i-1}/L_i)$.*

$$\begin{array}{rll}
 & L_0 = K(\alpha_1) & \Delta_0 = \{\alpha_1\} \\
p^{s_1} & \cup & \cap \\
 & L_1 = K(\alpha_1 \cdots \alpha_{p^{s_1}}) & \Delta_1 = \{\alpha_1, \ldots, \alpha_{p^{s_1}}\} \\
p^{s_2 - s_1} & \cup & \cap \\
 & \vdots & \vdots \\
p^{s_{\ell-1} - s_{\ell-2}} & \cup & \cap \\
 & L_{\ell-1} = K(\alpha_1 \cdots \alpha_{p^{s_{\ell-1}}}) & \Delta_{\ell-1} = \{\alpha_1, \ldots, \alpha_{p^{s_{\ell-1}}}\} \\
p^{s_\ell - s_{\ell-1}} & \cup & \cap \\
 & L_\ell = K(\alpha_1 \cdots \alpha_{p^{s_\ell}}) & \Delta_\ell = \{\alpha_1, \ldots, \alpha_{p^{s_\ell}}\} \\
e_0 & | & | \\
 & K = L_{\ell+1} & \Delta_{\ell+1} = \{\alpha_1, \ldots, \alpha_n\}
\end{array}$$

FIGURE 2. *Subfields of $L = K(\alpha_1)$ and the corresponding blocks, where the roots of $\alpha_1, \ldots, \alpha_n$ of $\varphi \in \mathcal{O}_K[x]$ are ordered as in Equation (2.1) and $n = e_0 p^\ell$ with $p \nmid e_0$.*

Next we describe how to compute the tower of extensions $L_0 \supset L_1 \supset \cdots \supset L_m = K$ where $m = \ell$ or $m = \ell + 1$ (compare [10, Algorithmus 4.3 and Algorithmus 4.5]). Since the ramification polygon $\mathcal{R}(\varphi)$ of φ is the Newton polygon of the ramification polynomial $\rho(x) = \varphi(\alpha x + \alpha)/\alpha^n \in K(\alpha)[x]$ it yields a factorization $\rho = \rho_1 \cdot \cdot \rho_m$ of ρ over $K(\alpha)$ where for $1 \le i \le m$ the factor ρ_i corresponds to the i-th segment of $\mathcal{R}(\varphi)$. Over $K(\alpha)$ we obtain the factorization $\varphi = \varphi_1 \cdot \cdots \cdot \varphi_m$ where

$$\varphi_i(x) = \alpha^{\deg \rho_i} \rho_i \left(\frac{x - \alpha}{\alpha} \right).$$

Now let $\psi = \prod_{i=1}^{m-1} \varphi_i$. The minimal polynomial $\mu \in \mathcal{O}_K[x]$ of the constant coefficient $\alpha_1 \cdot \cdots \cdot \alpha_{p^s_{m-1}}$. of ψ generates $L_\ell = K(\alpha_1 \cdot \cdots \cdot \alpha_{p^s_{m-1}})$ over K. We continue this process with $\psi \in L_{m-1}[x]$ whose ramification polynomial has $m - 1$ segments until we have reached $L_0 = K(\alpha_1)$.

The ramification polygon and its residual polynomials also yield further information about the structure of the splitting field of φ.

THEOREM 2.3 [11, Theorem 7.4]. *Let $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_K[x]$ be Eisenstein of degree $n = e_0 p^m$ with $p \nmid e_0$ and $m > 0$. Assume the ramification polygon $\mathcal{R}(\varphi)$ of φ consists of $\ell + 1$ segments $\mathcal{S}_1, \ldots, \mathcal{S}_{\ell+1}$. For $1 \le i \le \ell$ let*

- *$m_i = -h_i/e_i$ be the slope of $\mathcal{S}_i$ with $\gcd(h_i, e_i) = 1 = d_i e_i + b_i h_i$ for $d_i, b_i \in \mathbb{Z}$,*
- *$\underline{A}_i(y) \in \mathcal{O}_L[y]$ be the residual polynomial and f_i the degree of the splitting field of $\underline{A}_i$ over $\underline{K}$,*
- *$\gamma_i \in \overline{K}$ such that $\underline{A}_i(\gamma_i) = 0$, and*
- *$v_i = e_0 \cdot p^{m - s_{i-1}} + n + 1$.*

Moreover we denote by I the unramified extension of K of degree

$$f = \operatorname{lcm}(f_1, \ldots, f_\ell, [K(\zeta_{e_1 e_0}) : K], \ldots, [K(\zeta_{e_\ell e_0}) : K]) \tag{2.2}$$

and by N the splitting field of φ. Let α be a root of φ and $K(\alpha) = L_0 \supset L_1 \supset \cdots \supset L_\ell \supset K$ as in Figure 2 be the tower of subfields corresponding to $\mathcal{R}(\varphi)$. Then:

(a) *The field*

$$T = I\left(\sqrt[e_1 e_0]{(-1)^{v_1} \gamma_1^{b_1 n} \varphi_0}, \ldots, \sqrt[e_\ell e_0]{(-1)^{v_\ell} \gamma_\ell^{b_\ell n} \varphi_0} \right)$$

is a subfield of N/K, such that N/T is a p-extension.

(b) *For $1 \le i \le \ell - 1$ the extensions TL_{i-1}/TL_i are elementary abelian.*

(c) *The extension T/K is Galois and tamely ramified with ramification index $e_0 \cdot \operatorname{lcm}(e_1, \ldots, e_\ell)$. Furthermore $[T : K] < n^2$.*

When working with the global representation in section 5 we can compute with a lower precision if the coefficients of the generating polynomials are smaller, using ideas from Monge's reduction [19].

LEMMA 2.4 [22, Lemmata 5.4 and 5.7]. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree n with root α let $\rho \in \mathcal{O}_K(\alpha)[x]$ be its ramification polynomial, and let*

$$\mathcal{R} = \{(1, J_0), (p^{s_1}, J_1), \ldots, (p^{s_{u-1}}, J_{u-1}), (p^{s_u}, 0), \ldots, (n, 0)\}$$

its ramification polygon. Denote by $\phi_{\mathcal{R}} : \mathbb{R}^{>0} \to \mathbb{R}^{>0}$, $\lambda \mapsto \min_{0 \le i \le u}\{\frac{1}{n}(J_i + \lambda p^{s_i})\}$ the Hasse-Herbrand function *of $\mathcal{R}$ and for $m \in \mathbb{Z}^{>0}$ let*

$$\underline{S}_m(x) = \underline{\rho(\alpha^m x)/\operatorname{cont}_\alpha(\rho(\alpha^m x))} \in \underline{K}[x]$$

where $\operatorname{cont}_\alpha(\rho(\alpha^m x))$ is the largest power pf α that divide all coefficients of $\rho(\alpha^m x)$.

(i) *If $\mathcal{R}$ has a segment $\mathcal{S}$ of integral slope $-m \in \mathbb{Z}$, with left endpoint (k, w) and residual polynomial $\underline{A}$ then $\underline{S}_m(x) = x^k \underline{A}(x)$.*

(ii) *If $\mathcal{R}$ has no segment of slope $-m \in \mathbb{Z}$ then $\underline{S}_m(x) = x^{p^s}$ where $0 \le s \le v_p(n)$ such that $v(\rho_{p^s}) + p^s \cdot m = \min_{0 \le r \le v_p(n)} v(\rho_{p^r}) + p^r \cdot m$.*

(iii) *If there is $m \in \mathbb{Z}^{>0}$ such that $k \equiv n\phi_{\mathcal{R}}(m) \bmod n$, $j = \frac{n + n\phi_{\mathcal{R}}(m) - k}{n}$, and $\underline{S}_m : \underline{K} \to \underline{K}$ is surjective then there is an Eisenstein polynomial*

$$\psi(x) = \sum_{i=0}^{n} x^i \sum_{l=0}^{\infty} \psi_{i,l} \pi^l \in \mathcal{O}_K[x]$$

with $\psi_{k,j} = 0$ such that $K[x]/(\psi) \cong K(\alpha)$.

3. *Ramification Polygons with one Segment*

If the ramification polygon of an Eisenstein polynomial consists of one segment, then we can explicitly give its Galois group. In particular if the segment is horizontal we have a tamely ramified extension and its Galois group is well known.

THEOREM 3.1 (see for example [10, Satz 3.2 and Satz 3.6]). *Let ζ denote a primitive $(q^f - 1)$-st root of unity, where $q = |\underline{K}|$, and let $L = K(\zeta, \sqrt[e]{\zeta^r \pi})$ be tamely ramified. Let $g = \gcd(q^f - 1, r(q - 1))$ and $u \in \mathbb{Z}^{>0}$ minimal such that $q^{fu} - 1 \equiv 0 \bmod (e(q^f - 1)/g)$. Let ξ be a primitive $(q^{fu} - 1)$-st root of unity and $s = r(q^{fu} - 1)/(q^f - 1)$. Then*

$$N = K(\xi, \sqrt[e]{\xi^s \pi})$$

is the normal closure of L/K, with Galois group $\langle x, y : x^e = 1, y^{fu} = x^s, xy = yx^q \rangle$.

If the degree of φ is a power of p and the ramification polygon consists of one segment the slope of the segment and its residual polynomial determine the splitting field of φ.

THEOREM 3.2 [11, Theorems 7.3 and 8.2]. *Let $\varphi \in \mathcal{O}_K[x]$ be an Eisenstein polynomial of degree $n = p^m$ and assume that its ramification polygon $\mathcal{R}(\varphi)$ consists of one segment of slope $-h/e$ where $\gcd(h, e) = 1 = ae + bh$ for $a, b \in \mathbb{Z}$. Let α be a root of φ, $L = K(\alpha)$ and let*

$\underline{A}(y) \in \underline{L}[y]$ be the residual polynomial of $\mathcal{R}(\varphi)$ and let f be the degree of the splitting field of $\underline{A}_r \in \underline{K}[y]$ over $\underline{K}$. Let I/L be the unramified extension of degree $\operatorname{lcm}(f, [L(\zeta_e) : L])$ where ζ_e is a primitive e-the root of unity. Choose an $\varepsilon \in \overline{K}$ with $\underline{A}(\underline{\varepsilon}) = 0$.

(i) *$N = I\left(\sqrt[e]{\varepsilon^b \alpha}\right)$ is the splitting field of φ.*

(ii) *$\operatorname{Gal}(\varphi) = G_1 \rtimes H$, where G_1 is the first ramification group and H corresponds to the maximal tamely ramified subfield of the splitting field of φ*

(iii) *$\operatorname{Gal}(\varphi)$ is isomorphic to the group*

$$\widetilde{G} = \{t_{a,v} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto xa + v \mid a \in H' \leq \mathrm{GL}(m,p),\ v \in (\mathbb{F}_p)^m\}$$

of permutations of the vector space $(\mathbb{F}_p)^m$, where H' describes the action of H on $\Theta_h(G_h/G_{h+1}) \leq \wp^h/\wp^{h+1}$ (see definition above).

For an algorithm for computing the Galois group of Eisenstein polynomials whose ramification polygon consists of one segment see [10, Algorithmus 6.1].

4. *Candidates for Galois Groups*

In this section we describe several criteria that have to be met for a group to be a Galois group over a p-adic field. As it is a Galois group it has to be transitive. From the ramification filtration we know that it has to be solvable and obtain a few more criteria. Further criteria can be obtained from a concrete polynomial by computing its automorphism group, considering certain absolute resolvents, and the subfield structure of the polynomials in our algorithms.

Automorphism Groups of Subfields

As the degree of $K(\alpha)$ is relatively small and root finding in local fields is efficient [21] we can efficiently compute the automorphism group of $K(\alpha)/K$ which yields some information about $\operatorname{Gal}(\varphi)$. A similar result also holds for other subfield of the splitting field.

THEOREM 4.1 [4, Theorem 3.6]. *Let $\varphi \in \mathcal{O}_K[x]$ be irreducible of degree n and α a root of φ in some algebraic closure of K. Let $L = K(\alpha)$ and $G = \operatorname{Gal}(\varphi)$. Then $\operatorname{Aut}(L/K) \cong \operatorname{Cen}_{S_n}(G)$, where $\operatorname{Cen}_{S_n}(G)$ is the centralizer of G in S_n.*

PROPOSITION 4.2 [4, Proposition 2.6]. *Let $G = \operatorname{Gal}(L/K)$ and let J be a subgroup of G that fixes some subfield M of the normal closure of L/K, then $\operatorname{Aut}(M/K) \cong \operatorname{Nor}_G(J)/J$ where $\operatorname{Nor}_G(J)$ is the normalizer of J in G.*

Resolvents

Resolvents are the method of choice for determining Galois groups over global fields. In this section we use two specific absolute resolvents to reduce the number of candidate groups. In the next section we use relative resolvents to find the Galois group among the candidate groups.

DEFINITION 4.3. Let $\varphi \in \mathcal{O}_K[x]$ be a polynomial with roots $\alpha_1, \ldots, \alpha_n$ in some algebraic closure. Let $H < G$ be subgroups of S_n acting on $\{x_1, \ldots, x_n\}$ with $\operatorname{Gal}(\varphi) \leq G$. Let $G//H$ denote a set of representatives of right cosets of G/H. If $F \in \mathcal{O}_K[x_1, \ldots, x_n]$ satisfies $H =$

$\mathrm{Stab}_G F$ then

$$R_F(t) = \prod_{\sigma \in G//H} (t - F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})) \in \mathbb{Z}[t]$$

is called the relative resolvent polynomial corresponding to $H < G$. If $G = S_n$, we call the resolvent polynomial an absolute resolvent.

With the following theorem, given for polynomials over the integers in [24], we obtain information about the Galois group from the resolvent.

THEOREM 4.4. *Using the notation of the preceding definition, set $m = [G : H] = \deg R_F$. Then, if R_F is squarefree, its Galois group (as a subgroup of S_m) is equal to $\tau(\mathrm{Gal}(\varphi))$, where τ is the natural group homomorphism from G to S_m given by the natural right action of G on G/H. In particular, the list of the degrees of the irreducible factors of R_F in $\mathcal{O}_K[x]$ is the same as the list of the orbit lengths of the action of $\tau(\mathrm{Gal}(\varphi))$ on $\{1, \ldots, m\}$. In particular, R_F has a root in $\mathcal{O}_K$ if and only if $\mathrm{Gal}(\varphi)$ is contained in a conjugate of H.*

When R_F is not squarefree there is a Tschirnhausen transformation on φ resulting in a polynomial ψ such that R_F with respect to ψ is squarefree. The degrees of the irreducible factors of $R_F \in \mathcal{O}_K[x]$ are efficiently obtained with an OM-algorithm, see for example [13]. Note that one does not need to derive a complete factorization, so that the lifting step described in [14] can be omitted.

For checking whether a group can be the Galois group of $\varphi \in \mathcal{O}_K[x]$ we use the following two absolute resolvents. In the last step of each iteration we use relative resolvents we find the $\mathrm{Gal}(\varphi)$ among the candidate groups.

Let $\mathrm{disc}\,(\varphi)$ denote the discriminant of φ. Then

$$R(t) = t^2 - \mathrm{disc}\,(\varphi) \tag{4.1}$$

is a resolvent for $H = A_n$, $G = S_n$. Thus $\mathrm{Gal}(\varphi) \leq A_n$ if and only if $v_K(\mathrm{disc}\,(\varphi))$ is even.

The following polynomial is a resolvent for the group pair $H \cong S_2 \times S_{n-2}$ and $G = S_n$:

$$\mathrm{R_2(t)} = \prod_{1 \leq \mathrm{i} < \mathrm{j} \leq \mathrm{n}} (\mathrm{t} - \alpha_\mathrm{i} - \alpha_\mathrm{j}). \tag{4.2}$$

To avoid errors from approximating the roots of φ, we obtain R_2 from the resultant $\mathrm{res}_x(\varphi(t), \varphi(x+t))/t^n$ by halving all the exponents.

Tower of Two Extensions

Let $L_1 \subset L_0 = K(\alpha)$. Denote by N the normal closure of L/K and by N_1 the normal closure of L_1/K. Let T_1 be the maximal tamely ramified subextension of N_1/K and let T_0 be the maximal tamely ramified subextension of the normal closure of L_0/L_1. We assume that T_1 and the Galois group $\mathrm{Gal}(L_1/K) = \mathrm{Aut}(N_1/K)$ are known. Theorem 2.3 yields T_0 and section 3 yields $\mathrm{Gal}(L_0/L_1)$. A lattice of subfields of N/K is given in Figure 4.

In the following we view the (complete) wreath product as a permutation group. In particular, the wreath product $H \wr G$ has imprimitive action on the Cartesian product of the G-sets of the constituent groups.

THEOREM 4.5 [18]. *Let $K \subset L \subset M$ be finite separable field extensions. Then $\mathrm{Gal}(M/K)$ can be embedded into $\mathrm{Gal}(M/L) \wr \mathrm{Gal}(L/K)$,*

In our case we have that $\mathrm{Gal}(L_0/K)$ is isomorphic to a subgroup of $\mathrm{Gal}(L_0/L_1) \wr \mathrm{Gal}(L_1/K)$. Since $\mathrm{Gal}(L_0/L_1)$ and $\mathrm{Gal}(L_1/K)$ are solvable all subgroups of $\mathrm{Gal}(L_0/L_1) \wr \mathrm{Gal}(L_1/K)$ are solvable.

PROPOSITION 4.6. *Let T as in Figure 4 and $W = \mathrm{Gal}(L_0/L_1) \wr \mathrm{Gal}(L_1/K)$. If $H \leq W$ is the Galois group of L_0/K then*

(i) *H is transitive,*
(ii) *$\#H = [TN_1 : K] \cdot p^w$ for some $v_p([TN_1L_0 : TN_1]) \leq w \leq e_0 \cdot [N_1 : T_1] \cdot v_p([TN_1L_0 : TN_1])$,*
(iii) *if $v_K(\mathrm{disc}\,(L_0/K))$ is even then $H < A_n$,*
(iv) *$\mathrm{Aut}(L_0/K) \cong \mathrm{Cen}_{S_n}(H)$,*
(v) *the list of the degrees of the irreducible factors of R_2 from Equation 4.2 over $\mathcal{O}_K[x]$ is the same as the list of the orbit lengths of the action of $\tau(H)$ on $\{1, \ldots, n(n-1)/2\}$ where τ is the permutation representation of H acting on the cosets $S_n/(S_2 \times S_{n-2})$.*

Proof. (i) follows from Galois theory. (iii) and (v) follow with the resolvents from Equations 4.1 and 4.2 from Theorem 4.4. For (iv) see Theorem 4.1.

(ii) Let $\varphi_0 \in L_1[x]$ be the generating polynomial of L_0/L_1. TN_1/K is normal. We obtain the normal closure of TN_1L_0/K as the composite of the conjugates of TL_0N_1 over TN_1. The polynomial $\varphi_0 \in L_1[x]$ it is fixed by the automorphisms of T/K, except for e_0 conjugates if $[L_1 : K]$ is not a power of p. Thus we only need to consider the conjugation of φ_0 over N_1/T_1L_1 and L_1/K and possible e_0 conjugates over T and the number of conjugates is at least 1 and at most $e_0[N_1 : T_1]$. □

As $[TN_1L_0 : TN_1] \leq p^{s_1}$ an initial upper bound for $[N : K]$ is $[N_1 : K][T : T_1]p^{s_1 w}$ by Proposition 4.6(ii). The test Proposition 4.6(v) is cheap as long as no Tschirnhausen transformation has to be used. We suggest using it early on in the filtering of groups if this is the case and later if a Tschirnhausen transformation is needed.

Since the fields in the subfield lattice of the splitting field of φ (Figure 4) correspond to subgroups of $\mathrm{Gal}(\varphi) = \mathrm{Gal}(L_0/K)$, this helps us elimanate further candidate groups.

PROPOSITION 4.7. *Let T as in Figure 4 and $G = \mathrm{Gal}(L_0/L_1) \wr \mathrm{Gal}(L_1/K)$. If $H \leq G$ is the Galois group of L_0/K then then there are subgroups B_1, B, C, D_1, D_0 of H such that*

(vi) *$B_1 \trianglelefteq H$ with $H/B_1 \cong \mathrm{Gal}(T_0/K)$,*
(vii) *$B \trianglelefteq H$ with $B \leq B_1$ and $H/B \cong \mathrm{Gal}(T/K)$,*
(viii) *$C \trianglelefteq H$ with $C < B_1$ and $H/C \cong \mathrm{Gal}(L_1/K)$,*
(ix) *$C/(B \cap C) \cong \mathrm{Gal}(T/T_1)$,*
(x) *$D_1 < H$ with $[H : D_1] = [L_1 : K]$,*
(xi) *$D_1/(B_1 \cap D_1) \cong \mathrm{Gal}(T_1/K)$ and $(B_1 \cap D_1)/(B \cap D_1) \cong \mathrm{Gal}(T/K)$,*
(xii) *$D_0 \trianglelefteq D_1$ with $D_1/D_0 \cong \mathrm{Gal}(L_1/L_0) = \mathrm{Aut}(T_0L_1/L_0)$,*
(xiii) *$(B \cap D_0)/(B \cap D_1) \cong (\mathbb{Z}/p\mathbb{Z})^{s_1}$,*
(xiv) *$(B \cap C)/(B \cap C \cap D_0)$ is an elementary abelian p-group of order at most p^{s_1},*
(xv) *$\mathrm{Aut}(TL_0/K) \cong \mathrm{Nor}_H(B \cap D_0)/(B \cap D_0)$.*

Proof. (vi) to (xii) follow from Figure 4 and Galois theory. (xiii) is a consequence of Theorem 2.3(b). (xiv) holds, since by Theorem 2.3 $\mathrm{Gal}(TL_0/TL_1)$ is elementary abelian of order p^{s_1} and $TN_1L_0 = TL_0 \cdot TN_1$ and thus the extension TN_1L_0/TN_1 is elementary abelian and its order divides p^{s_1}. (xv) follows from Proposition 4.2. □

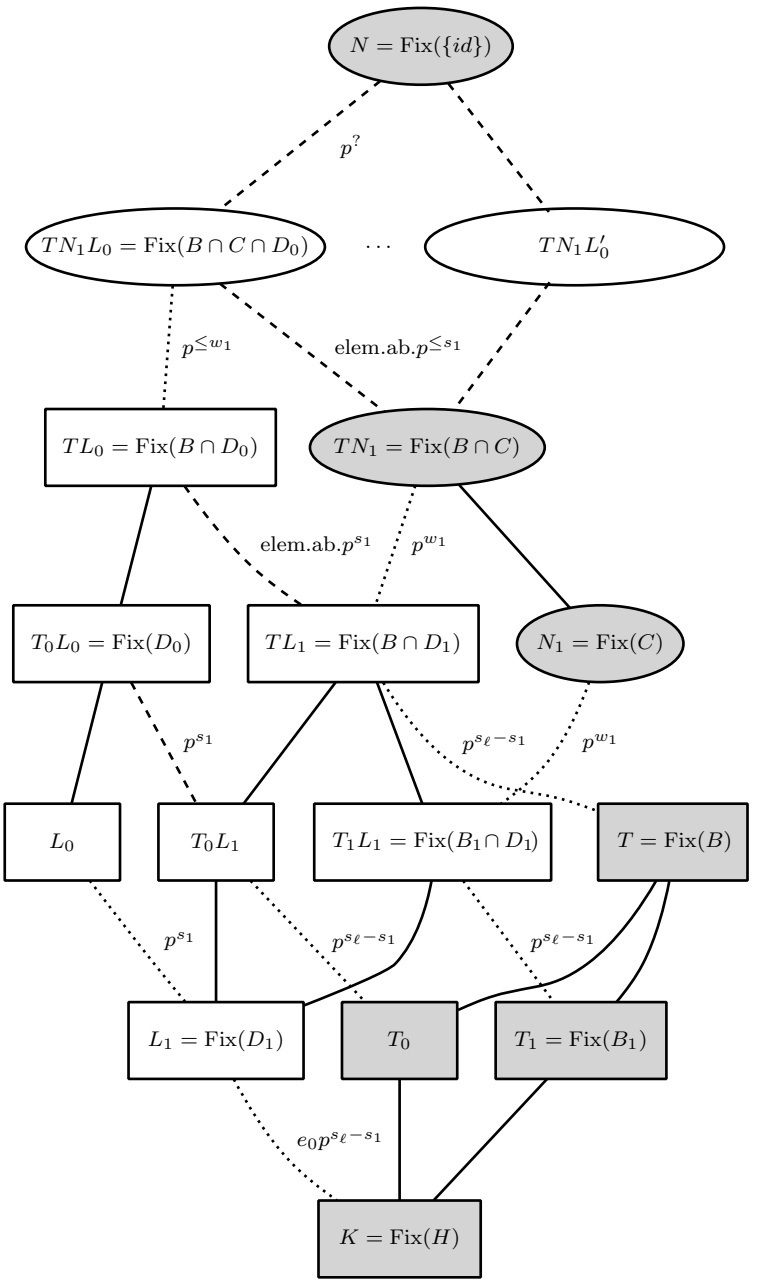

FIGURE 3. *(Incomplete) subfield lattice of the normal closure N of L_0/K. The fields L_0 and L_1 are as in Figure 2, N_1 is the normal closure of L_1/K and T_1 is the maximal tamely ramified normal subextensions of N_1. T_0L_0/L_1 is the normal closure of L_0/L_1 with maximal tamely ramified subextension T_0L_1/L_1 (see Theorem 3.2). The maximal tamely ramified subextension of N/K is T from Theorem 2.3. The fields $TN_1L_0^{(1)} = TN_1L_0$ to $TN_1L_0^{(m)}$ are the conjugates of $TN_1L_0^{(1)} = TN_1L_0$ over TN_1. The groups B, B_1, C, D_0, and D_1 are as in Proposition 4.7. Fields in rectangles are explicitly known, shaded fields are normal over K. Solid lines denote normal tamely ramified extensions and dashed lines normal p-extensions.*

5. *Relative resolvents*

In this section, we assume the circumstances and notation from section 4. Specifically, we assume that we have used the methods of the previous section to eliminate possible Galois groups for L_0/K and have failed to uniquely identify the group. At this stage of the algorithm, we will rule out the other candidate groups by using relative resolvents.

Because relative resolvents rely on the ordering of the polynomial's roots we must explore block matching. We also need a field over which the polynomial ϕ is square free and splits into linear factors. We find a tower $L_0^* \supset L_1^* \supset K^*$ of global fields that corresponds to our tower of fields $L_0 \supset L_1 \supset K$, such that the generating polynomials of the global extensions generate the local extensions. We find a completion $K_{\mathfrak{q}}^*$ of the global field K^* in which the generating polynomial ψ of L_0^*/K^* is square free and splits into linear factors. Over $K_{\mathfrak{q}}^*$ we compute the resolvent, which has coefficients in K^*.

Block Matching

At this point in our algorithm, we have an upper bound group W that contains $\mathrm{Gal}(L_0/K)$. In order to accurately reflect this containment, the roots of our polynomial must be ordered to match the blocks from the wreath product W.

To facilitate finding the blocks corresponding to the subfield structure $K \subset L_1 \subset L_0 = K(\alpha)$, we construct a global representation following the approach described in [15]. Let $\Phi \in \mathbb{Z}[x]$ be a polynomial that generates $K/\mathbb{Q}_p$ and set $K^* = \mathbb{Q}[x]/(\Phi)$. We let $\varphi_1(y)$ be a polynomial so that $L_1 = K[y]/\varphi_1(y)$ and write the defining polynomial of L_0/L_1 as $\varphi_0(x, y) \in K[y][x]$. Then we have $\psi(x) = \mathrm{res}_y(\varphi_0(x, y), \varphi_1(y))$. By construction, $\mathrm{Gal}(\psi)$ over K, will be isomorphic to $\mathrm{Gal}(L_0/K)$. Thus we can restrict ourselves entirely to finding $\mathrm{Gal}(\psi)$. In other words, ψ replaces our polynomial and the blocks will be of the roots β_i of ψ.

We find a prime ideal $\mathfrak{q}$ so that the factorization of $\psi \in K^*[x]$ is squarefree modulo $\mathfrak{q}$. Then we find the lcm of the degrees of the irreducible factors and form the unramified extension of $K_{\mathfrak{q}}^*$ of that degree. This approach is given in more detail and a proof is provided in [9]. Considering ψ over this extension we can approximate all the roots and give them some arbitrary ordering. F inally, by forming the global field $K^*[x]/(\psi)$, we can use the following theorem to find the blocks for our subfield structure:

THEOREM 5.1 [8, Satz 5.2]. *Let R be an integral domain with 1 and F its field of fractions. Let $E_1 = F(\beta)$ and $E_0 = F(\alpha)$ with $\mathbb{Q} \subseteq E_1 \subseteq E_0$ and $\phi_1, \phi \in R[x]$ be the minimal polynomials of β and α, respectively. Let $\omega \in R[x]$ be the embedding polynomial with $\omega(\alpha) = \beta$. Denote the conjugates of α and β in some algebraic closure of F by $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$, respectively. Defining $\Delta_i = \{\alpha_j : \omega(\alpha_j) = \beta_i\}$ it follows:*

(i) *$\Delta_1, \ldots, \Delta_m$ form a block system of $\mathrm{Gal}(\phi)$. Furthermore, $n = m\#\Delta_i$.*

(ii) *$\mathrm{Gal}(\phi_1) = \mathrm{Gal}(E_1/F)$ is isomorphic to the permutation representation of $\mathrm{Gal}(\phi) = \mathrm{Gal}(E_0/F)$ with respect to $\Delta_1, \ldots, \Delta_m$ under the mapping $\theta : \beta_i \mapsto \Delta_i$.*

Next, we determine the permutation σ that maps the block system Δ_i to the block system of the wreath product. Our root approximations are then re-ordered using σ so that they may be used in forming relative resolvents.

Stauduhar's Method

To implement Stauduhar's method [25], we enumerate conjugacy classes of maximal subgroups of W that match all criteria in Propositions 4.6 and 4.7, and we pick one representative from each conjugacy class; let $\mathfrak{J}$ denote this collection of representatives, ordered

by size so that $\#J_1 \geq \#J_2, \ldots$, for each $J_i \in \mathfrak{J}$. For a given $J \in \mathfrak{J}$, we compute a multivariable polynomial F whose stabilizer in W is J.

As in Definition 4.3, we can form the relative resolvent polynomial $R_F(x)$ corresponding to J; that is,

$$R_F(x) = \prod_{\sigma \in W//J} (x - F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}))$$

where the α_i are roots of ψ and $W//J$ denotes a complete set of right coset representatives of W/J. We then factor $R(x)$ over K. If $A(x)$ is an irreducible factor of $R(x)$, say of degree m, then there exist elements $\sigma_1, \ldots, \sigma_m$ such that

$$A(x) = \prod_{i=1}^{m} (x - F(\alpha_{\sigma_i(1)}, \ldots, \alpha_{\sigma_i(n)})).$$

If B denotes the set of right cosets $\{J\sigma_i : 1 \leq i \leq m\}$, then $\mathrm{Gal}(\psi) \leq \tau^{-1}(\mathrm{Stab}_{\tau(W)}(B))$ (see [7, Thm. 3.2]). Consequently, we have the following two observations:

(1) Suppose R_F has a linear factor over K, of the form $x - F(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$. Then $\mathrm{Gal}(\psi) \leq \sigma^{-1} J \sigma$.
(2) More generally, if R_F factors as $A_1 \cdots A_k$ and let B_i denote the right cosets of W/J corresponding to A_i. Then

$$\mathrm{Gal}(\psi) \leq \bigcap_{i=1}^{k} \tau^{-1}(\mathrm{Stab}_{\tau(W)} B_i).$$

In the traditional Stauduhar approach, if R_F does have a linear factor (corresponding to some maximal subgroup J of W), we repeat the above process but with W replaced by the appropriate conjugate $\sigma^{-1} J \sigma$. Otherwise, if no resolvent has a linear factor, then $\mathrm{Gal}(\psi) = W$.

Ideally, one determines the appropriate conjugate of J by testing each root of the resolvent, checking if it defines a p-adic integer. This would be straightforward if we approximated the roots as p-adic numbers. Unfortunately, we are approximating the roots in a different field. Since it is very difficult to determine if a number in a p-adic field is close to a number in a q-adic field, we don't faithfully adhere to the traditional Stauduhar method. In other words, we don't determine the conjugate and continue descending to the Galois Group.

Instead, we use relative resolvents to eliminate the candidate groups. We form a relative resolvent for the starting group and one of the candidate groups J . If we find that our relative resolvent has a simple root in our p-adic integer ring, then we can safely eliminate all candidates that have greater order than J. We proceed with this approach until only one group remains.

In the case that the starting group W is a candidate left over from our filtering, we test it first and separately. We form relative resolvents, as needed, for W and its maximal subgroups. If we determine that one of the resolvents has a simple root in $\mathbb{Z}_p$ then we rule the starting group out and continue on to other candidate groups. If none of these resolvents have a simple root then none of the maximal subgroups or their conjugates contain the Galois Group, implying that W is the Galois Group.

Relative Resolvents and Orbit Length

While the traditional Stauduhar approach is guaranteed to work, there is a way to decrease the number descents taken. We propose the following modifications, which leverage the rich structure of Galois groups of local fields laid out in Propositions 4.6 and 4.7. Our modifications also aim to make use of other resolvent polynomials of low index, which can yield more information concerning $\mathrm{Gal}(\psi)$.

First, we compute representatives H_i for each transitive subgroup of S_n contained in W, not just the maximal ones. Note, we only include those that satisfy Propositions 4.6 and

4.7. Second, suppose the smallest maximal transitive subgroup of W has index k. We then compute a representative J_j for each conjugacy class of subgroups of index $\leq k$. For each H_i and each J_j, we compute the orbit lengths of the permutation representation of H_i acting on the cosets W/J_j; these orbit lengths are the same as the degrees of the irreducible factors of the relative resolvent polynomial corresponding to J_j. It is possible that one or more low-index subgroups give rise to orbit-length partitions that uniquely identify the Galois group. In this case, we compute and factor the corresponding relative resolvent(s). Otherwise, if the low-index subgroups do not yield enough information to completely identify G (i.e., they all have the same partitions), we proceed with the traditional Stauduhar approach.

6. *Examples*

We have implemented our algorithm in Magma [6]. The degrees of the irreducible factors of the resolvent polynomials over $\mathbb{Q}_p$ is computed with the OM algorithm from the Ideals+ package for Magma [12]. For the compuation of the invariant W relative H invariants we call the functions from the implementation of [7].

Example 6.1. We illustrate the effectiveness of the filtering criteria by giving the number of candidate groups after filtering the subgroups of $\mathrm{Gal}(L_0/L_1) \wr \mathrm{Gal}(L_1/K)$ using the criteria from Propositions 4.6 and 4.7. When the Galois group is determined unquely by the criteria, it is listed in the table.

K	φ	$n = e_0 p^{s_\ell}$	p^{s_1}	Gal L_0/L_1	Gal L_1/K	number of groups after criterion (i)	(ii)	(iii)	(iv)	(vi,vii)	(viii)	(ix)	(x-xii)	(xiii,xiv)	(v)	(xv)	Gal L_0/K
$\mathbb{Q}_2$	φ_{8a}	8	4	A_4	C_2	11	4	4	2	1	1	1	1	1	1	1	8T33
$\mathbb{Q}_2$	φ_{8b}	8	2	C_2	S_4	36	10	4	4	3	3	3	3	3	3	2	
$\mathbb{Q}_2$	φ_{8c}	8	2	C_2	D_4	26	26	14	2	2	1	1	1	1	1	1	8T17
$\mathbb{Q}_2$	φ_{8d}	8	2	C_2	D_4	26	26	14	11	11	11	11	11	11	8	7	
$\mathbb{Q}_2$	φ_{12a}	12	4	S_4	S_3	153	17	10	10	1	1	1	1	1	1	1	12T254
$\mathbb{Q}_2$	φ_{16}	16	4	A_4	A_4	1810	259	210	54	34	34	34	34	34	12	12	
$\mathbb{Q}_3$	φ_6	$2\cdot 3$	3	A_3	C_2	3	3	3	1	1	1	1	1	1	1	1	6T2
$\mathbb{Q}_3$	φ_{9a}	9	3	S_3	S_3	23	10	5	5	5	5	5	5	5	3	3	
$\mathbb{Q}_3$	φ_{9b}	9	3	S_3	S_3	23	7	5	5	3	3	3	3	3	2	2	9T24
$\mathbb{Q}_3$	φ_{12b}	12	3	C_3	D_4	21	7	7	3	3	3	3	3	3	3	3	
$\mathbb{Q}_3$	φ_{18a}	$2\cdot 9$	3	A_3	6T2	23	23	23	3	3	3	3	3	3	3	3	
$\mathbb{Q}_3$	φ_{18b}	18	9	9T19	C_2	119	29	24	24	1	1	1	1	1	1	1	18T476
$\mathbb{Q}_3$	φ_{27b}	27	3	S_3	M_9	279	40	29	28	12	12	12	12	12	11	11	
$\mathbb{Q}_5$	φ_{25}	25	5	C_5	C_5	9	9	9	7	7	7	7	7	7	7	7	
$\mathbb{Q}_7$	φ_{14a}	14	7	7T3	C_2	8	5	5	2	2	2	2	2	2	1	1	14T4
$\mathbb{Q}_7$	φ_{14b}	14	7	7T4	C_2	22	3	3	3	1	1	1	1	1	1	1	14T32
$\mathbb{Q}_7$	φ_{14c}	14	7	C_7	C_2	3	3	3	1	1	1	1	1	1	1	1	14T8

The polynomials in the table are $\varphi_{8a} = x^8 + 4x^5 + 2x^4 + 4x^2 + 2$, $\varphi_{16} = x^{16} + 4x^5 + 2x^4 + 4x^2 + 2$, $\varphi_6 = x^6 + 676 \cdot 3$, $\varphi_{18a} = x^{18} + 3$, $\varphi_{9a} = x^9 + 3$, $\varphi_{27b} = x^{27} + 3x^6 + 9x + 3$, $\varphi_{8b} = x^8 + 4x^7 + 4x^4 + 12x^2 + 2$, $\varphi_{8c} = x^8 + 2x^6 + 4x + 6$, $\varphi_{8d} = x^8 + 10x^6 + 12x^4 + 2$, $\varphi_{12a} = x^{12} + 6x^3 + 6x + 6$, $\varphi_{9b} = x^9 + 3x^3 + 9x^2 + 3$, $\varphi_{12b} = x^{12} + 6x^3 + 9x + 3$, $\varphi_{18b} = x^{18} + 12x + 6$, $\varphi_{25} = x^{25} + 130x^{20} + 475x^{16} + 125x^{12} + 525x^{11} + 175x^{10} + 125x^7 + 375x^6 + 525x^5 + 250x^2 + 375x + 120$, $\varphi_{14a} = x^{14} + 14x^2 + 7$, $\varphi_{14b} = x^{14} + 7x + 7$, $\varphi_{14c} = x^{14} - 21x^{12} - 147x^{10} + 70x^7 - 49x^5 - 77$.

In the case of extensions of degree 14 over $\mathbb{Q}_7$ the criteria always reduced the number of groups to one.

EXAMPLE 6.2. *Let $\varphi_{18a} = x^{18} + 3 \in \mathbb{Q}_3$. The ramification polygon $\mathcal{R}(\varphi_{18a})$ consists of three segments of slopes -9, -3, and 0. This yields a tower of extensions*

$$L_1 = L_2(\alpha) \supset L_2(\beta) \supset L_3(\gamma) \supset \mathbb{Q}_3$$

with $\gamma^2 + 3 = 0$, $\beta^3 + 26\gamma = 0$, and $\alpha^3 + 10\beta = 0$. With the methods from section 3 for computing Galois groups of polynomials whose ramification polygon consists of one segment we find that $\mathrm{Gal}(L_3/\mathbb{Q}_3) \cong C_2$, $\mathrm{Gal}(L_2/L_3) \cong A_3$, and $\mathrm{Gal}(L_1/L_2) \cong A_3$.

By Theorem 4.5 the Galois group of $L_2/\mathbb{Q}_3$ is isomorphic to a subgroup of the wreath product

$$\mathrm{Gal}(L_2/L_3) \wr \mathrm{Gal}(L_3/\mathbb{Q}_3) \cong A_3 \wr C_2.$$

With the criteria from Propositions 4.6 and 4.7 we determine that $\mathrm{Gal}(L_2/\mathbb{Q}_3) \cong$ 6T2 (see Example 6.1).

Again by Theorem 4.5 the Galois group of $L_1/\mathbb{Q}_3$ is isomorphic to a subgroup of the wreath product

$$\mathrm{Gal}(L_1/L_2) \wr \mathrm{Gal}(L_2/\mathbb{Q}_3) \cong A_3 \wr 6\mathrm{T}2.$$

As shown in Example 6.1 Propositions 4.6 and 4.7 reduce the number of groups to be considered to groups isomorphic to 18T18, 18T21, *and* 18T88 *with* 18T21 $<$ 18T88. *Using relative resolvents we check to which of these groups $\mathrm{Gal}(L_1/\mathbb{Q}_3)$ isomorphic. We get $\mathrm{Gal}(L_1/\mathbb{Q}_3) \cong$* 18T18.

References

1. C. Awtrey, *Dodecic 3-adic fields*, Int. J. Number Theory, **8**, no.4, 933–944, 2012.
2. C. Awtrey, B. Barkley, N. Miles, C. Shill, and E. Strosnider, *Degree 12 2-adic fields with automorphism group of order 4*, Rocky Mountain J. Math., (to appear).
3. C. Awtrey, N. Miles, J. Milstead, C. Shill, and E. Strosnider, *Degree 14 2-adic fields*, Involve, a journal of mathematics, **8**, no. 2, 329–336 (2015).
4. C. Awtrey, N. Mistry, and N. Soltz, *Centralizers of Transitive Permutation Groups and Applications to Galois Theory*, Missouri J. Math. Sci., **27** (2015), no. 1, 16–32.
5. J. Brown, R. Cass, R. Keaton, S. Parenti, and D. Shankman, *Degree 14 extensions of $\mathbb{Q}_7$*, Int. J. of Pure and Appl. Math., 100(2), 337-345 (2015).
6. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
7. C. Fieker, J. Klüners,
8. K. Geissler, *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, Dissertation, TU Berlin, 2003.
9. K. Geissler and J. Klüners, *Galois Group Computation for Rational Polynomials*, J. Symb. Comput. 30 (2000), 653-674.
10. C. Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, Dissertation, Universität Paderborn, 2010.
11. C. Greve and S. Pauli, *Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials*, International Journal of Number Theory **8** (2012), no. 6, 1401–1424.
12. J. Guardia, J, Montes, and E. Nart, *Arithmetic in big number fields: the '+ideals' package*, ArXiv e-prints (2010), arXiv:1005.4596 [math.NT].
13. J. Guardia, J, Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.
14. J. Guàrdia, E. Nart, and S. Pauli. *Single-factor lifting and factorization of polynomials over local fields*, J. Symbolic Comput., 47(11):1318–1346, 2012.
15. J. Jones and D. Roberts, *Nonic 3-adic Fields*, in ANTS VI, Springer Lecture Notes in Computer Science, 3076 (2004), 293–308.
16. J. Jones and D. Roberts, *A Database of Local Fields*, J. Symbolic Comput., **41** (2006), 80–97, http://math.asu.edu/~{}jj/localfields.
17. J. Jones and D. Roberts, *Octic 2-adic Fields*, J. Number Theory., **128** (2008), 1410–1429.

18. M. Krasner and L. Kaloujnine. *Produit complet des groupes de permutation et probleme d'extension de groupes II*. Acta Sci. Math. (Szeged), 14:39-66, 1951.
19. M. Monge, *A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields*, Int. J. Number Theory **10** (2014), no. 7, 1699–1727.
20. Ö. Ore, *Newtonsche Polynome in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84–117.
21. P. Panayi, *Computation of Leopoldt's p-adic regulator*, Dissertation, University of East Anglia, 1995.
22. S. Pauli and B. Sinclair, *Enumerating extensions of* (π)*-adic fields with given invariants*, preprint (2014), arXiv:1504.06671 [math.NT].
23. D. S. Romano, *Galois groups of strongly Eisenstein polynomials*, Dissertation, UC Berkeley, 2000.
24. L. Soicher, J. McKay, *Computing Galois groups over the rationals*, J. Number theory **20** (1985), 273?-281
25. R. Stauduhar, *The Determination of Galois Groups*, Math. Comp. **27** (1973), 981-?996.
26. J. Todd and H. Coxeter, *A practical method for enumerating cosets of a finite abstract group*, Proceedings of the Edinburgh Mathematical Society. Series II 5: 26?34, 1936.