ON RAMIFICATION POLYGONS AND GALOIS GROUPS OF EISENSTEIN POLYNOMIALS

CHRISTIAN GREVE AND SEBASTIAN PAULI

ABSTRACT. Let $\varphi(x)$ be an Eisenstein polynomial of degree n over a local field and α be a root of $\varphi(x)$. Our main tool is the ramification polygon of $\varphi(x)$, that is the Newton polygon of $\rho(x) = \varphi(\alpha x + \alpha)/(\alpha^n x)$. We present a method for determining the Galois group of $\varphi(x)$ in the case where the ramification polygon consists of one segment.

1. INTRODUCTION

Algorithms for computing Galois groups are an important tool in constructive number theory. The commonly used algorithms for computing Galois groups of polynomials over $\mathbb{Q}$ (and $\mathbb{Q}(t)$) are based on the method of Stauduhar [20]. Considerable progress has been made in this area over the last ten years. For local fields however, that is for fields K complete with respect to a non-archimedian exponential valuation ν with residue class field $\underline{\mathsf{K}}$ of characteristic $p \neq \infty$, there is no general algorithm.

As the Galois groups of unramified extensions are explicitly known, we concentrate the Galois groups of totally ramified extensions. These can be generated by an Eisenstein polynomial, that is a polynomial $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_{\mathsf{K}}[x]$ with $\nu(\varphi_0) = 1$ and $\nu(\varphi_i) \geq 1$ for $1 \leq i \leq n-1$. We denote by α a root of $\varphi(x)$ in an algebraic closure $\overline{\mathsf{K}}$ of K.

If p does not divide the degree of $\varphi(x)$ the extension $\mathsf{K}(\alpha)$ is tamely ramified and can be generated by a pure polynomial. We show how this pure polynomial can be obtained and recall the (well known) explicit description of its Galois group (see section 2).

If p divides the degree of $\varphi(x)$ the situation becomes more difficult. John Jones and David Roberts have developed algorithms for determining the Galois group for the special cases of polynomials of degree 2^2, 2^3, and 3^2 over $\mathbb{Q}_2$ and $\mathbb{Q}_3$ respectively based on the resolvent method [7, 8, 9].

A useful tool for obtaining information about the splitting field and the Galois group is the ramification polygon $\operatorname{rp}(\varphi)$ of $\varphi(x)$, which is the Newton polygon $\operatorname{np}(\rho)$ of the ramification polynomial $\rho(x) = \varphi(\alpha x + \alpha)/(\alpha^n x) \in \mathsf{K}(\alpha)[x]$.

David Romano has treated the case of Eisenstein polynomials $\varphi(x)$ of degree $n = p^m$ with $\nu(\varphi_1) = 1$, so that the ramification polygon consists of one segment of slope $-h/(p^m - 1)$ where $\gcd(h, p^m - 1) = 1$ [16]. In this case the Galois group of $\varphi(x)$ is isomorphic to the group

$$\Gamma = \left\{ x \mapsto ax^\sigma + b \;\middle|\; a \in \mathbb{F}_{p^m}^\times, b \in \mathbb{F}_{p^m}, \sigma \in \operatorname{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^m} \cap \underline{\mathsf{K}}) \right\}$$

of permutations of $\mathbb{F}_{p^m}$. In [17] he generalizes his result to ramification polygons that are a line, on which only the end points have integral coordinates.

We develop the theory of ramification polygons further by attaching an additional invariant, the *associated inertia* to each segment of the ramification polygon (section 3). In section 4 we describe the shape of ramification polygons and show that the polygons, as well as the

associated inertias, which are the degrees of the splitting fields of associated polynomials, are invariants of $\mathsf{K}(\alpha)$. We find that the segments of the ramification polygon corresponds to the subfields of the field generated by $\varphi(x)$ (section 5). In section 6 we investigate how ramification polygons and their associated inertias behave in towers of subfields. This is followed by a description of the splitting field in the case of ramification polygons with one segment and a description of the maximal tamely ramified subfield of the splitting field in the general case (section 7). In section 8 we use these results to find Galois groups of Eisenstein polynomials with one sided ramification polygon with arbitrary slopes. Our methods can be generalized algorithmically to the case of ramification polygons with two segments [2] and beyond. In section 9 we give some examples for Galois groups determined in this way.

Notation. In the following K is a local field, complete with respect to a non-archimedian exponential valuation ν, where $\nu = \nu_{\mathsf{K}}$ is normalized such that $\nu(\pi) = \nu_{\mathsf{K}}(\pi) = 1$ for a uniformizing element π in the valuation ring $\mathcal{O}_{\mathsf{K}}$ of K. The continuation of ν to an algebraic closure $\overline{\mathsf{K}}$ of K is also denoted by ν. For $\gamma \in \overline{\mathsf{K}}$ and $\gamma' \in \overline{\mathsf{K}}$ we write $\gamma \sim \gamma'$, if $\nu(\gamma - \gamma') > \nu(\gamma)$.

We write ζ_n for a primitive n-th root of unity. We denote by $\underline{\mathsf{K}} = \mathcal{O}_{\mathsf{K}}/(\pi) \cong \mathbb{F}_q$ the residue class field of $\mathcal{O}_{\mathsf{K}}$ and by $\underline{\beta} = \beta + (\pi)$ the class of $\beta \in \mathcal{O}_{\mathsf{K}}$ in $\underline{\mathsf{K}}$. For $\underline{\gamma} \in \underline{\mathsf{K}}$ we denote by γ a lift of $\underline{\gamma}$ to $\mathcal{O}_{\mathsf{K}}$. If $\varphi(x) = \sum_{i=1}^{n} \varphi_i x^i \in \mathcal{O}_{\mathsf{K}}[x]$ we set $\underline{\varphi}(x) := \sum_{i=1}^{n} \underline{\varphi_i} x^i \in \underline{\mathsf{K}}[x]$.

2. Tamely Ramified Extensions

We present some results about tamely ramified subfields of totally ramified extensions and the splitting fields and Galois groups of totally and tamely ramified extensions.

Proposition 2.1. *Let $n = e_0 p^m$ with $p \nmid e_0$ and let*

$$\varphi(x) = x^n + \sum_{i=1}^{n-1} \varphi_i x^i + \varphi_0 \in \mathcal{O}_{\mathsf{K}}[x]$$

be a polynomial whose Newton polygon is a line of slope $-h/n$, where $\gcd(h, n) = 1$. Let α be a root of $\varphi(x)$. The maximum tamely ramified subextension M of $\mathsf{L} = \mathsf{K}(\alpha)$ of degree e_0 can be generated by the Eisenstein polynomial $x^{e_0} + \psi_0^b \pi^{e_0 a}$ with $\psi_0 \equiv \varphi_0 \bmod (\pi^{h+1})$ and where a and b are integers such that $ae_0 + bh = 1$.

Proof. As the Newton polygon of $\varphi(x)$ is a line all roots α of $\varphi(x)$ have the same valuation, namely $\nu(\alpha) = h/n$. Because $\gcd(h, n) = 1$, for each root α of $\varphi(x)$, the extension $\mathsf{K}(\alpha)/\mathsf{K}$ is totally ramified of degree n, which implies that $\varphi(x)$ is irreducible.

Since $n = e_0 p^m$ with $\gcd(e_0, p) = 1$ its maximum tamely ramified subextension M over K has degree $[\mathsf{M} : \mathsf{K}] = e_0$. We first show that M and the extensions generated by $x^{e_0} + \psi_0$ are isomorphic. Because $\nu(\varphi_0) = h$ and $\psi_0 \equiv \varphi_0 \bmod (\pi^{h+1})$, there is a principal unit $1 + \pi\varepsilon \in \mathcal{O}_{\mathsf{K}}$ such that $\psi_0 = (1 + \pi\varepsilon)\varphi_0$. Furthermore $\alpha^n = -\varphi_0 - \sum_{i=1}^{n-1} \varphi_i \alpha^i = -(1 + \pi_{\mathsf{L}}\delta)\varphi_0$ for some principal unit $1 + \pi_{\mathsf{L}}\delta \in \mathcal{O}_{\mathsf{L}}$ where π_{L} is a uniformizer of the valuation ring $\mathcal{O}_{\mathsf{L}}$ of L. The polynomial $x^{e_0} + \psi_0$ has a root over L if and only if $(\alpha^{p^m} x)^{e_0} + \psi_0$ has a root over L. Division by α^n yields

$$x^{e_0} + \frac{\psi_0}{\alpha^n} = x^{e_0} - \frac{(1 + \pi\varepsilon)\varphi_0}{(1 + \pi_{\mathsf{L}}\delta)\varphi_0} \equiv x^{e_0} - 1 \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x].$$

Obviously $\rho(x) = x^e - 1 \in \underline{\mathsf{L}}[x]$ is square free and $\rho(1) = 0$. With Newton lifting (and by reversing the transformations above) we obtain a root of $x^{e_0} + \psi_0$ in L. Let β be this root of

$x^{e_0}+\psi_0$. Then $\nu(\beta^b\pi^a)=bh/e+a=1/e$ and $\mathsf{M}=\mathsf{K}(\beta)=\mathsf{K}(\beta^b\pi^a)$. As $\beta^{e_0 b}\pi^{e_0 a}=-\psi_0^b\pi^{e_0 a}$ we have $\beta^b\pi^a$ is a root of $x^{e_0}+\psi_0^b\pi^{e_0 a}\in\mathcal{O}_\mathsf{K}[x]$. □

Corollary 2.2. *Let $\varphi(x)=\sum_{i=0}^e\varphi_i x^i\in\mathcal{O}_\mathsf{K}[x]$ be an Eisenstein polynomial and assume $p\nmid e$. If $\psi(x)=x^e+\psi_0$ with $\psi_0\equiv\varphi_0 \bmod(\pi^2)$, then the extensions generated by $\varphi(x)$ and $\psi(x)$ are isomorphic.*

It follows from Corollary 2.2 that the splitting field of an Eisenstein polynomial $\varphi(x)=\sum_{i=0}^e\varphi_i x^i\in\mathcal{O}_\mathsf{K}[x]$ with $p\nmid e$ is $\mathsf{N}=\mathsf{K}(\zeta_e,\sqrt[e]{-\varphi_0})$, where ζ_e is a primitive e-th root of unity. The Galois group of N/K is well known, we obtain it from the general description of Galois groups of normal, tamely ramified extensions (see, for instance, [5, chapter 16]):

Theorem 2.3. *Let K be a local field and q the number of elements of its residue class field. Let N/K be a normal, tamely ramified extension with ramification index e and inertia degree f. There exists an integer r with $r(q-1)\equiv 0 \bmod e$ such that $\mathsf{N}=\mathsf{K}(\zeta,\sqrt[e]{\zeta^r\pi})$, where ζ is a (q^f-1)-st root of unity and $q^f-1\equiv 0 \bmod e$. Let $k=\frac{r(q-1)}{e}$. The generators of the Galois group are the automorphisms*

$$s:\zeta\mapsto\zeta,\sqrt[e]{\zeta^r\pi}\mapsto\zeta^{(q^f-1)/e}\sqrt[e]{\zeta^r\pi}\quad\text{and}\quad t:\zeta\mapsto\zeta^q,\sqrt[e]{\zeta^r\pi}\mapsto\zeta^k\sqrt[e]{\zeta^r\pi}.$$

The Galois group of N/K as a finitely presented group is

$$\langle s,t\mid s^e=1,t^f=s^r,s^t=s^q\rangle\cong C_e\rtimes C_f,$$

3. Associated Polynomials

Associated (or residual) polynomials, first introduced by Ore [14], are a useful tool in the computation of ideal decompositions and integral bases [11, 12, 3] and the closely related problem of polynomial factorization over local fields [4, 15]. The associated polynomials yield information about the unramified part of the extension generated by a polynomial. We will use it in the construction of splitting fields of Eisenstein polynomials.

Let $\rho(x)=\sum_{i=0}^n\rho_i x^i\in\mathcal{O}_\mathsf{K}[x]$ be a not necessarily irreducible monic polynomial whose Newton polygon $\mathrm{np}(\rho)$ consists of t segments:

$$(0,\nu(\rho_0))\leftrightarrow(a_1,\nu(\rho_{a_1})),\dots,(a_{t-1},\nu(\rho_{a_{t-1}}))\leftrightarrow(a_t,\nu(\rho_{a_t})$$

with slopes:

$$-h_1/e_1<-h_2/e_2<\cdots<-h_{t-1}/e_{t-1}<-h_t/e_t$$

with $\gcd(e_i,h_i)=1$ for $1\le i\le t$. Each of the segments corresponds to a factor $\rho_r(x)$ of $\rho(x)$. For each segment we obtain one associated polynomial as follows.

For $1\le r\le t$ let $b_r=\nu(\rho_{a_r})$. Consider the r-th segment $(a_{r-1},b_{r-1})\leftrightarrow(a_r,b_r)$ of $\mathrm{np}(\rho)$ and set $d_r=a_r-a_{r-1}$. We have $\frac{\nu(\rho_{a_r})-\nu(\rho_{a_{r-1}})}{d_r}=-\frac{h_r}{e_r}$. Let β be a root of $\rho(x)$ with $\nu(\beta)=h_r/e_r$, set $\mathsf{L}=\mathsf{K}(\beta)$, let π_L be an uniformizing element in the valuation ring $\mathcal{O}_\mathsf{L}$ of L. We have

$$\begin{aligned}\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}}=\sum_{i=0}^n\frac{\rho_i\beta^i x^i}{\pi^{b_{r-1}}\beta^{a_{r-1}}}&\equiv\sum_{i=a_{r-1}}^{a_r}\frac{\rho_i\beta^i x^i}{\pi^{b_{r-1}}\beta^{a_{r-1}}}\bmod\pi_\mathsf{L}\mathcal{O}_\mathsf{L}[x]\\&\equiv\sum_{j=0}^{d_r/e_r}\frac{\rho_{je+a_{r-1}}\beta^{je_r+a_{r-1}}x^{je_r+a_{r-1}}}{\pi^{b_{r-1}}\beta^{a_{r-1}}}\bmod\pi_\mathsf{L}\mathcal{O}_\mathsf{L}[x].\end{aligned}$$

The last congruence holds, because the x-coordinates of the points on the r-th segment of the Newton polygon are of the form $a_{r-1} + je_r$ $(0 \leq j \leq (a_{r-1} - a_r)/e_r)$. Division by $x^{a_{r-1}}$ yields

$$\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}x^{a_{r-1}}} \equiv \sum_{j=0}^{d_r/e_r} \frac{\rho_{je+a_{r-1}}\beta^{je_r}x^{je_r}}{\pi^{b_{r-1}}} \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x].$$

For $\gamma = \beta^{e_r}/\pi^{h_r}$ we have $\nu(\gamma) = \nu(\beta^{e_r}/\pi^{h_r}) = 0$. By substituting $\gamma\pi^{h_r}$ for β^{e_r} we get

$$\frac{\rho(\beta x)}{\pi^{b_{r-1}}\beta^{a_{r-1}}x^{a_{r-1}}} \equiv \sum_{j=0}^{d_r/e_r} \frac{\rho_{je_r+a_{r-1}}\pi^{jh_r}(\gamma x^{e_r})^j}{\pi^{b_{r-1}}} \bmod \pi_{\mathsf{L}}\mathcal{O}_{\mathsf{L}}[x].$$

If we replace γx^{e_r} by y we obtain the *associated polynomial* of $\rho(x)$ with respect to the r-th segment S_r of $\mathrm{np}(\rho)$:

$$\underline{A}_r(y) := \sum_{j=0}^{d_r/e_r} \underline{\rho_{je_r+a_{r-1}}\pi^{jh_r-b_{r-1}}}y^j \in \underline{\mathsf{K}}[y].$$

It follows immediately from the construction that:

Lemma 3.1. *Let $\beta_1, \ldots, \beta_n$ be the roots of $\rho(x)$. The roots of $\underline{A}(y) \in \underline{\mathsf{K}}[y]$ are of the form*

$$\underline{\left(\frac{\beta_i^{e_j}}{\pi^{h_j}}\right)}$$

for some $1 \leq i \leq n$ and some $1 \leq j \leq t$.

Definition 3.2. *Let $\underline{A}(y) \in \underline{\mathsf{K}}[y]$ be the associated polynomial of a segment S of $\mathrm{np}(\rho)$ and $\underline{\gamma}$ a root of $\underline{A}(y)$. We call the degree of the splitting field of $\underline{A}_r(y) \in \underline{\mathsf{K}}[y]$ over $\underline{\mathsf{K}}$ the associated inertia of S.*

Remark 3.3. The denominators of the slopes (in lowest terms) of the segments of the Newton polygon $\mathrm{np}(\rho)$ of a polynomial $\rho(x)$ are divisors of the ramification indices of the extensions generated by the irreducible factors of a polynomial. For each segment of $\mathrm{np}(\rho)$ the associated inertia is a divisor of the inertia degree of these extensions.

Remark 3.4. The factorization of $\underline{A}_r(y)$ yields a factorization of the factor of $\rho(x)$ that corresponds to S_r [14].

4. Ramification Polygons

Let $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in \mathcal{O}_{\mathsf{K}}[x]$ be an Eisenstein polynomial, $\alpha \in \overline{\mathsf{K}}$ a root of $\varphi(x)$ and $\mathsf{L} := \mathsf{K}(\alpha)$. The polynomial

$$\rho(x) = \sum_{i=0}^{n} \rho_i x^i := \frac{\varphi(\alpha x + \alpha)}{\alpha^n x} \in \mathcal{O}_{\mathsf{L}}[x].$$

is called the *ramification polynomial* of $\varphi(x)$ and its Newton polygon, which we denote by $\mathrm{rp}(\varphi)$, is called the *ramification polygon* of $\varphi(x)$ (also see [18]). Denoting the roots of $\varphi(x)$ in $\overline{\mathsf{K}}$ by $\alpha = \alpha_1, \ldots, \alpha_n$ we have

$$\rho(x) = \prod_{i=2}^{n}\left(x - \frac{\alpha_i - \alpha}{\alpha}\right) = \prod_{i=2}^{n}\left(x + 1 - \frac{\alpha_i}{\alpha}\right)$$

If the extension L/K generated by $\varphi(x)$ is Galois with Galois group G the segments of the ramification polygon $\mathrm{rp}(\varphi)$ correspond to the ramification subgroups of G:

$$G_j := \{\sigma \in G \mid \nu_{\mathsf{L}}(\sigma(\alpha) - \alpha) \geq j + 1\} \text{ for } j \geq 0.$$

Because $\nu_{\mathsf{L}}(\frac{\alpha_i - \alpha}{\alpha}) = \nu_{\mathsf{L}}(\alpha_i - \alpha) - 1$ the ramification polygon describes the filtration $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_k = 1$ of the Galois group, that is, a segment of slope $-m$ yields a jump at m in the filtration, which means $G_m \neq G_{m+1}$. If the extension L/K is not Galois, there is a similar interpretation for a filtration of the set of embeddings of L/K in $\overline{\mathsf{K}}$ in the context of non-Galois ramification theory (see [6]).

From the next lemma one can deduce the typical shape of the ramification polygon (see figure 1).

Lemma 4.1 ([18, Lemma 1])**.** *Let $\varphi(x) = \sum_{i=0}^{n} \varphi_i x^i \in \mathsf{K}[x]$ be an Eisenstein polynomial and $n = e_0 p^m$ with $p \nmid e_0$. Denote by α a root of $\varphi(x)$ and set $\mathsf{L} = \mathsf{K}(\alpha)$. Then the following hold for the coefficients of the polynomial $\psi(x) = \sum_{i=0}^{n} \psi_i x^i := \varphi(\alpha x + \alpha) \in L[x]$:*

(a) $\nu_{\mathsf{L}}(\psi_i) \geq n$ *for all* i.
(b) $\nu_{\mathsf{L}}(\psi_{p^m}) = \nu_{\mathsf{L}}(\psi_n) = n$.
(c) $\nu_{\mathsf{L}}(\psi_i) \geq \nu_{\mathsf{L}}(\psi_{p^s})$ *for* $p^s \leq i < p^{s+1}$ *and* $s < m$.

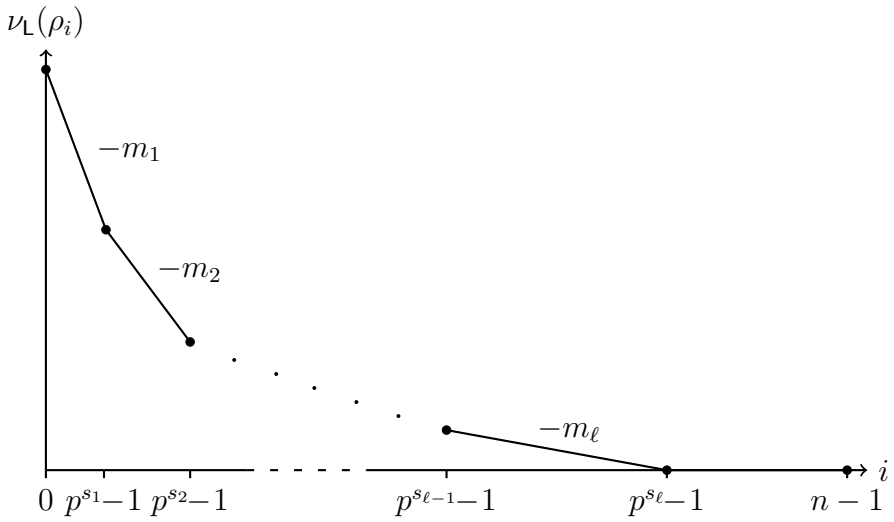

FIGURE 1. Shape of the ramification polygon

As a consequence we have:

Lemma 4.2. *If a ramification polygon consists of only one segment with slope, say $-m_1$ then $m_1 \leq \frac{p\nu(p)}{p-1}$.*

Proposition & Definition 4.3. *Let L/K be totally ramified and α a prime element of L and $\varphi(x)$ the minimal polynomial of α. Then $\mathrm{rp}(\varphi)$ and the associated inertia of the segments are invariants of L/K. We call $\mathrm{rp}(\mathsf{L}/\mathsf{K}) := \mathrm{rp}(\varphi)$ the ramification polygon of L/K.*

Proof. Let $\beta = \delta\alpha$ where $\delta \in \mathcal{O}_{\mathsf{L}} = \mathcal{O}_{\mathsf{K}}[\alpha]$ with $\nu_{\mathsf{L}}(\delta) = 0$. We can write δ in the form $\delta = \delta_0 + \delta_1\alpha + \delta_2\alpha^2 + \ldots$ with $\delta_i \in \mathcal{O}_{\mathsf{K}}$. Let $\beta = \beta_1, \ldots, \beta_n$ be the conjugates of β and let

$\widetilde{\varphi}(x)$ be the minimal polynomial of β. We compare the roots of the ramification polynomials of $\varphi(x)$ and $\widetilde{\varphi}(x)$

$$\rho(x) = \prod_{i=2}^{n} \left(x - \frac{\alpha_i - \alpha}{\alpha} \right) = \prod_{i=2}^{n} \left(x - \left(-1 + \frac{\alpha_i}{\alpha} \right) \right)$$

and

$$\widetilde{\rho}(x) = \prod_{i=2}^{n} \left(x - \frac{\beta_i - \beta}{\beta} \right) = \prod_{i=2}^{n} \left(x - \left(-1 + \frac{\beta_i}{\beta} \right) \right).$$

For $1 \leq i \leq n$ long division yields

$$\frac{\beta_i}{\beta} = \frac{\delta_0 \alpha_i + \delta_1 \alpha_i^2 + \ldots}{\delta_0 \alpha + \delta_1 \alpha^2 + \ldots} = \frac{\alpha_i}{\alpha} + \frac{\delta_1 (\alpha_i - \alpha)\alpha_i + \ldots}{\delta_0 \alpha + \delta_1 \alpha^2 + \ldots}.$$

We have $\nu_{\mathsf{L}}(-1+\alpha_i/\alpha) = m$ where m is one of the slopes of $\mathrm{rp}(\varphi)$. As $\nu_{\mathsf{L}}((\alpha_i - \alpha)\alpha_i) = m+2$ we have $1 - \beta_i/\beta \sim 1 - \alpha_i/\alpha$. Thus $\nu_{\mathsf{L}}(\beta_i - \beta) = m + 1$ and it follows that the slopes of the ramification polygon are independent of the choice of the uniformizing element of L and therefore invariants of L.

To prove that the associated inertia is an invariant of L/K we consider the segment with slope $-m = -h/e$ of the Newton polygons of $\rho(x)$ and $\widetilde{\rho}(x)$.

The roots of the corresponding associated polynomials $\underline{A}(y) \in \underline{\mathsf{L}}[y]$ and $\underline{\widetilde{A}}(y) \in \underline{\mathsf{L}}[y]$ with respect to the segment with slope m are of the form (see Lemma 3.1):

$$\underline{\left(\frac{(-1 + \alpha_i/\alpha)^e}{\alpha^h} \right)} \text{ and } \underline{\left(\frac{(-1 + \beta_i/\beta)^e}{\beta^h} \right)}.$$

Because $-1 + \beta_i/\beta \widetilde{-} 1 + \alpha_i/\alpha$ we have

$$\frac{(-1 + \beta_i/\beta)^e}{\beta^h} \sim \frac{1}{\delta^h} \frac{(-1 + \alpha_i/\alpha)^e}{\alpha^h}.$$

Therefore the roots of $\underline{A}(y)$ and $\underline{\widetilde{A}}(y)$ differ only by the factor $\underline{\delta}^{-h} \in \underline{\mathsf{K}} = \underline{\mathsf{K}}$. So, if $\underline{A}(y) = \prod_{i=1}^{d}(y - \gamma_i)$ then $\underline{\widetilde{A}}(y) = \prod_{i=1}^{d}(y - \gamma_i$
$\mathit{underline}\delta^h)$. Clearly the polynomials $\underline{A}(y)$ and $\underline{\widetilde{A}}(y)$ have the same splitting fields which implies that the associated inertias are the same. □

Lemma 4.4. *Let* L/K *be totally ramified of degree* p^m *and let* $-m_1, \ldots, -m_\ell$ *be the slopes of* $\mathrm{rp}(\mathsf{L}/\mathsf{K})$. *Let* T/K *be tamely ramified with ramification index* e_0 *and* $\mathsf{N} = \mathsf{TK}$. *Then the slopes of* $\mathrm{rp}(\mathsf{N}/\mathsf{T})$ *are* $-e_0 \cdot m_1, \ldots, -e_0 \cdot m_\ell$.

Proof. Let α be a uniformizer of L/K, $\varphi(x)$ its minimal polynomial and $\alpha = \alpha_1, \ldots, \alpha_{p^m} \in \overline{\mathsf{K}}$ its conjugates. Let β be a uniformizing element of T. If $a, b \in \mathbb{Z}$ such that $ae_0 - bp^m = 1$ then $\nu_{\mathsf{T}}(\alpha^a/\beta^b) = 1/p^m$. The ramification polynomial $\rho(x) \in \mathcal{O}_{\mathsf{N}}[x]$ of the minimal polynomial of α^a/β^b is

$$\rho(x) = \prod_{i=2}^{p^m} \left(x + 1 - \frac{\alpha_i^a}{\beta^b} \frac{\beta^b}{\alpha^a} \right) = \prod_{i=2}^{p^m} \left(x + 1 - \frac{\alpha_i^a}{\alpha^a} \right).$$

Each quotient α_i/α is of the form $1 + \gamma_i \alpha^{m_q}$ with $\nu(\gamma_i) = 0$ for some $1 \leq q \leq \ell$. As $\gcd(a, p) = 1$ we get $(\alpha_i/\alpha)^a = (1 + \gamma\alpha^{m_q})^a \sim 1 + a\gamma\alpha^{m_q}$, which implies that the exponential

valuation of the roots of $\rho(x) \in \mathsf{T}[x]$ are $e \cdot m_q$ $(1 \le q \le \ell)$. Thus the slopes of $\mathrm{rp}(\mathsf{N}/\mathsf{T})$ are $-e_0 \cdot m_1, \ldots, -e_0 \cdot m_\ell$. □

5. Blocks and Subfields

In the following we use the connection between blocks of the Galois group and subfields of an extension to describe and calculate a specific chain of subfields of our extension L/K, which is not Galois in general. We denote by $G = \mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathsf{L}/\mathsf{K})$ the Galois group of L/K, which is the automorphism group of the normal closure of L over K. As $\varphi(x)$ is irreducible, G acts transitively on the set of roots $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ of $\varphi(x)$.

Definition 5.1. A non-empty subset Δ of Ω is called a *block*, if $\sigma(\Delta) \cap \Delta \in \{\emptyset, \Delta\}$ for all $\sigma \in G$. The group $G_\Delta := \{\sigma \in G \mid \sigma(\Delta) = \Delta\}$ is called the *stabilizer* of Δ. The set $\{\Delta = \Delta^{(1)}, \ldots, \Delta^{(k)}\} := \{\sigma(\Delta) \mid \sigma \in G\}$ is the *block system* with respect to Δ. It constitutes a partition of Ω, thus $n = k \cdot |\Delta|$.

For the remainder of this section we fix the following notation (compare figure 1). The Eisenstein polynomial $\varphi(x)$ has degree $n = e_0 p^m$, its ramification polynomial is denoted by $\rho(x) = \sum_{j=0}^{n-1} \rho_j x^j$, and its ramification polygon $\mathrm{rp}(\varphi)$ consists of $\ell + 1$ segments. By Lemma 4.1 there are natural numbers $0 = s_0 < s_1 < \ldots < s_\ell = r$, so that the i-th segment S_i is of the form

$$(p^{s_{i-1}} - 1, \nu_{\mathsf{L}}(\rho_{p^{s_{i-1}}-1})) \leftrightarrow (p^{s_i} - 1, \nu_{\mathsf{L}}(\rho_{p^{s_i}-1}))$$

for $1 \le i \le \ell$. The last segment $S_{\ell+1} = (p^\ell - 1, 0) \leftrightarrow (n-1, 0)$ is horizontal. We denote the slopes of the segment of $\mathrm{rp}(\varphi)$ by $-m_1 < -m_2 < \ldots < -m_{\ell+1} = 0$.

We choose the numbering of the roots $\alpha = \alpha_1, \ldots, \alpha_n$ of $\varphi(x)$ compatible to the ramification polygon, that is, such that, for $1 \le i \le \ell + 1$

$$\nu_{\mathsf{L}}\left(\frac{\alpha_{p^{s_{i-1}}+1} - \alpha_1}{\alpha_1}\right) = \ \ldots \ = \nu_{\mathsf{L}}\left(\frac{\alpha_{p^{s_i}} - \alpha_1}{\alpha_1}\right) = m_i.$$

The following lemma says, that we can refine this numbering according to certain block systems.

Lemma 5.2. *The Galois group of $\varphi(x)$ has the blocks*

$$\Delta_i = \{\alpha_1, \ldots, \alpha_{p^{s_i}}\} = \{\alpha' \in \overline{\mathsf{K}} \mid \varphi(\alpha') = 0 \text{ and } \nu_{\mathsf{L}}(\alpha' - \alpha_1) \ge m_i + 1\} \quad (1 \le i \le \ell).$$

We can order the roots $\alpha_1, \ldots, \alpha_n$ such that $\Delta_i^{(r)} = \left\{\alpha_{(r-1)p^{s_i}+1}, \ldots, \alpha_{rp^{s_i}}\right\}$ for $1 \le r \le k$ and $k = n/p^{s_i}$.

Proof. Let $\sigma \in \mathrm{Gal}(\varphi)$. We show, that $\sigma(\Delta_i) \cap \Delta_i$ is empty or equal to Δ_i. If $\sigma(\alpha_1) \in \Delta_i$ we have $\nu_{\mathsf{L}}(\sigma(\alpha_1) - \alpha_1) \ge m_i + 1$. Then we have for an arbitrary $\alpha_j \in \Delta_i$ that

$$\begin{aligned}\nu_{\mathsf{L}}(\sigma(\alpha_j) - \alpha_1) &= \nu_{\mathsf{L}}(\sigma(\alpha_j) - \sigma(\alpha_1) + \sigma(\alpha_1) - \alpha_1) \\ &= \nu_{\mathsf{L}}(\sigma(\alpha_j - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) \ge m_i + 1,\end{aligned}$$

since $\nu_{\mathsf{L}}(\sigma(\alpha_j - \alpha_1)) \ge m_i + 1$. Because of our choice of ordering of $\alpha_1, \ldots, \alpha_n$ only the differences $\alpha_k - \alpha_1$ for $k \le p^{s_i}$ have exponential valuation greater than or equal to $m_i + 1$, which implies $\sigma(\alpha_j) \in \Delta_i$.

$$
\begin{array}{rll}
 & \mathsf{L}_0 = \mathsf{L} = \mathsf{K}(\alpha_1) & \Delta_0 = \{\alpha_1\} \\
p^{s_1} & \cup & \cap \\
 & \mathsf{L}_1 = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_1}}) & \Delta_1 = \{\alpha_1, \ldots, \alpha_{p^{s_1}}\} \\
p^{s_2 - s_1} & \cup & \cap \\
 & \vdots & \vdots \\
p^{s_{\ell-1} - s_{\ell-2}} & \cup & \cap \\
 & \mathsf{L}_{\ell-1} = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_{\ell-1}}}) & \Delta_{\ell-1} = \{\alpha_1, \ldots, \alpha_{p^{s_{\ell-1}}}\} \\
p^{s_\ell - s_{\ell-1}} & \cup & \cap \\
 & \mathsf{L}_\ell = \mathsf{K}(\alpha_1 \cdots \alpha_{p^{s_\ell}}) & \Delta_\ell = \{\alpha_1, \ldots, \alpha_{p^{s_\ell}}\} \\
e_0 & \cup & \cap \\
 & \mathsf{L}_{\ell+1} = \mathsf{K} & \Delta_{\ell+1} = \{\alpha_1, \ldots, \alpha_n\}
\end{array}
$$

FIGURE 2. The subfields of $L = \mathsf{K}(\alpha_1)$ and the corresponding blocks, where the roots of $\alpha_1, \ldots, \alpha_n$ of $\varphi(x) \in \mathcal{O}_\mathsf{K}[x]$ are ordered as in Lemma 5.2 and $n = e_0 p^\ell$ with $p \nmid e_0$.

If $\sigma(\alpha_1) \notin \Delta_i$ we have $\nu_\mathsf{L}(\sigma(\alpha_1) - \alpha_1) < m_i + 1$. In this case we get for an arbitrary $\alpha_j \in \Delta_i$, that

$$\nu_\mathsf{L}(\sigma(\alpha_j) - \alpha_1) = \nu_\mathsf{L}(\sigma(\alpha_j - \alpha_1) + (\sigma(\alpha_1) - \alpha_1)) < m_i + 1$$

and $\sigma(\alpha_j) \notin \Delta_i$ follows.

The ordering of the roots α_i according to the ramification polygon and the subordering according to the block systems $\{\Delta_i^{(1)}, \ldots, \Delta_i^{(k)}\}$ are consistent, because $\Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_\ell$. □

There is a correspondence between the blocks and the subfields of L/K. For a subgroup H of the Galois group G of L/K we write $\mathrm{Fix}(H)$ for the fixed field under H. A proof of the theorem can be found in [10].

Theorem 5.3. *Let $\varphi(x) \in \mathsf{K}[x]$ be irreducible of degree n, $\varphi(\alpha) = 0$, $\mathsf{L} = \mathsf{K}(\alpha)$, and G the Galois group of L/K.*

(a) *The correspondence $\Delta \mapsto \mathrm{Fix}(G_\Delta)$ is a bijection between the set of blocks containing α and the set of subfields of L/K.*
(b) *For two blocks Δ_1, Δ_2 with corresponding subfields $\mathsf{L}_1, \mathsf{L}_2$ we have $\mathsf{L}_1 \subseteq \mathsf{L}_2$ if and only if $\Delta_2 \subseteq \Delta_1$.*

The next theorem describes the subfields corresponding to the blocks of Lemma 5.2, see Figure 2.

Theorem 5.4. *Let $\mathsf{L} = \mathsf{K}(\alpha)$ and for $0 \le i \le \ell$ let $\mathsf{L}_i = \mathsf{K}(\beta_i)$ with $\beta_i = \alpha_1 \cdot \ldots \cdot \alpha_{p^{s_i}}$. Then $\mathsf{L} = \mathsf{L}_0 \supset \mathsf{L}_1 \supset \ldots \supset \mathsf{L}_\ell \supset \mathsf{K}$ with $[\mathsf{L}_i : \mathsf{L}_{i+1}] = p^{s_{i+1} - s_i}$ for $i \le \ell - 1$ and $[\mathsf{L}_\ell : \mathsf{K}] = e$.*

Proof. For $1 \le i \le \ell$ denote by E_i the field $\mathrm{Fix}(G_{\Delta_i})$ that corresponds to the block $\Delta_i = \{\alpha_1, \ldots, \alpha_{p^{s_i}}\}$ (see Theorem 5.3). The field E_i has degree $m = \frac{n}{p^{s_i}}$ over K. We show, that

$\mathsf{E}_i = \mathsf{L}_i$. Let $h(x) = \prod_{\alpha_j \in \Delta_i}(x - \alpha_j)$. Because $h(x)$ stays invariant under the action of G_{Δ_i} and it divides $\varphi(x)$ and it has the correct degree p^{s_i}, it is the minimal polynomial of α_1 over E_i. The field generated by the coefficients of $h(x)$ is equal to E_i. If this field had degree $m' < m$ over K, we would get the contradiction $[\mathsf{L} : \mathsf{K}] = m'p^{s_i} < mp^{s_i} = n$. In fact, even the constant coefficient β_i of $h(x)$ is sufficient to generate E_i, since L/K is totally ramified and $\nu_{\mathsf{L}}(\beta_i) = p^{s_i} = [L : E_i]$ holds. Hence β_i is a primitive element for E_i/K and we get $\mathsf{E}_i = \mathsf{L}_i$ as proposed. The inclusion and degree statements follow directly from theorem 5.3. □

In the case of a Galois extension L/K the subfields L_i are exactly the ramification subfields of L/K, that is, the fixed fields under the ramification subgroups of the Galois group. For an extension, which is not Galois, they are fixed fields under the "ramification subsets" of the set of embeddings of L/K in $\overline{\mathsf{K}}$ (see again [6]).

Remark 5.5. An explicit computation of the subfields $\mathsf{L}_i = \mathsf{K}(\beta_i)$ on a computer means finding the elements β_i as elements of L/K. This yields an embedding of L_i/K in L/K. Then a generating polynomial for L_i/K can be obtained by a minimal polynomial calculation. We briefly describe how the elements β_i in L/K can be determined.

Polynomial factorization techniques [1, 15] yield a factorization $\rho(x) = r_1(x) \cdot \ldots \cdot r_{\ell+1}(x) \in \mathsf{L}[x]$ of the ramification polynomial, where $r_j(x)$ corresponds to the j-th segment of the ramification polygon. Reversing the transformation from $\varphi(x)$ to $\rho(x)$ this gives us a factorization $\varphi(x) = p_1(x) \cdot \ldots \cdot p_{\ell+1}(x) \in \mathsf{L}[x]$ of $\varphi(x)$ with

$$p_j(x) = \prod_{\nu_{\mathsf{L}}(\frac{\alpha_i - \alpha}{\alpha}) = m_j} (x - \alpha_i) \in \overline{\mathsf{K}}[x]$$

for $2 \leq j \leq \ell + 1$ and

$$p_1(x) = (x - \alpha) \prod_{\nu_{\mathsf{L}}(\frac{\alpha_i - \alpha}{\alpha}) = m_1} (x - \alpha_i) \in \overline{\mathsf{K}}[x].$$

Now $\gamma_i \in \mathsf{L}$ is equal to the constant coefficient of $p_1(x) \cdot \ldots \cdot p_i(x)$.

6. Ramification Polygons and Subfields

We investigate how ramification polygons and their associated inertias behave in towers of subfields. We continue to use the notation from section 5 (also see Figure 2). By construction of the subfields L_i we expect a strong connection between the ramification polygon of $\varphi(x)$ and the ramification polygons of generating polynomials for the extensions $\mathsf{L}_{i-1}/\mathsf{L}_i$. The following lemma and theorem describe the connection in detail.

Lemma 6.1. *Assume the ramification polygon of* $\mathrm{rp}(\varphi) = \mathrm{rp}(\mathsf{L}/\mathsf{K})$ *consists of the segments* $S_1, \ldots, S_{\ell+1}$ *of lengths* $p^{s_1} - 1, p^{s_2} - p^{s_1}, \ldots, p^{s_{\ell+1}} - p^{s_\ell}$ *with slopes* $-m_1 < \cdots < -m_{\ell+1} = 0$. *Then*

(a) *the ramification polygon* $\mathrm{rp}(\mathsf{L}_1/\mathsf{K})$ *has exactly* ℓ *segments* $T_1, \ldots, T_\ell$ *of lengths* $p^{s_2}/p^{s_1} - 1, (p^{s_3} - p^{s_2})/p^{s_1} \ldots, (p^{s_{\ell+1}} - p^{s_\ell})/p^{s_1}$ *with slopes* $-m_2, \ldots, -m_{\ell+1} = 0$,
(b) *the associated inertia of* T_i *is equal to the associated inertia of* S_{i+1}, *and*
(c) *for each root* $\underline{\delta}$ *of* $\underline{A}_i(y)$ *the element* $\underline{\delta}^{p^{s_1}}$ *is a root of the associated polynomial of* T_i.

Proof. We assume that the roots of $\varphi(x)$ are ordered as in Lemma 5.2. Let $\Delta_1 = \Delta_1^{(1)}, \ldots, \Delta_1^{(k)}$ be the block system for the smallest block Δ_1. If $\alpha \in \Delta_1^{(r)}$ with $2 \le r \le k$, then $\nu_{\mathsf{L}}(\alpha - \alpha_1) = m_\lambda + 1 < m_1 + 1$ for some $\lambda \in \{2, \ldots, \ell+1\}$. Thus we can write $\alpha = \alpha_1 + \delta\alpha_1^{m_\lambda+1}$ for some $\delta \in \overline{\mathsf{K}}$ with $\nu(\delta) = 0$. If $\alpha, \alpha' \in \Delta_1^{(r)}$ then $\nu_{\mathsf{L}}(\alpha - \alpha') = m_1 + 1$. Thus, if $\alpha' = \alpha_1 + \delta'\alpha_1^{m_\lambda+1}$ for some $\delta' \in \overline{\mathsf{K}}$ with $\nu(\delta') = 0$ then $\delta' \sim \delta$. Recall that by our ordering of the roots of $\varphi(x)$ we have $\alpha_i \in \Delta_1^{(1)}$ and $\alpha_{(r-1)p^{s_1}+i} \in \Delta_1^{(r)}$ for $1 \le i \le p^{s_1}$ and $2 \le r \le k$. By the considerations above there is a $\varepsilon \in \overline{\mathsf{K}}$ with $\nu(\varepsilon) = 0$ so that for some $\lambda \in \{2, \ldots, \ell+1\}$:

$$-1 + \frac{\alpha_{(r-1)p^{s_1}+i}}{\alpha_i} \sim \varepsilon\alpha_1^{m_\lambda}. \tag{1}$$

For $1 \le r \le k$ let $\beta_r = \prod_{\alpha \in \Delta_1^{(r)}} \alpha$, so that $\mathsf{L}_1 = \mathsf{K}(\beta_1)$. Then $\psi(x) = \prod_{r-1}^{k} x - \beta_r$ is the minimal polynomial of β_1 over K. The ramification polynomial of $\psi(x)$ is:

$$\frac{\psi(\beta_1 x + \beta_1)}{\beta_1^k x} = \prod_{r=2}^{k}\left(x - \left(-1 + \frac{\beta_r}{\beta_1}\right)\right) = \prod_{r=2}^{k}\left(x - \left(-1 + \frac{\alpha_{r-1p^{s_1}+1} \cdot \cdots \cdot \alpha_{rp^{s_1}}}{\alpha_1 \cdot \cdots \cdot \alpha_{p^{s_1}}}\right)\right).$$

By relation (1) there are $\varepsilon_r \in \overline{\mathsf{K}}$ with $\nu(\varepsilon_r) = 0$ and $\lambda \in \{2, \ldots, \ell+1\}$ so that

$$-1 + \frac{\beta_r}{\beta_1} \sim 1 + (1 + \varepsilon_r\alpha_1^{m_\lambda})^{p^{s_1}} = \varepsilon_r^{p^{s_1}}\alpha_1^{m_\lambda p^{s_1}} + \sum_{i=1}^{p^{s_1}-1}\binom{p^{s_1}}{i}\varepsilon_r^i\alpha_1^{m_\lambda \cdot i}.$$

If we show that

$$-1 + \frac{\beta_r}{\beta_1} \sim \varepsilon^{p^{s_1}}\alpha_1^{m_\lambda p^{s_1}}, \tag{2}$$

then clearly (a) holds. We now proof (b) and (c) for S_2 and T_1. The results for the other segments follow analogously.

The roots of the ramification polygon of φ with valuation m_2 are $-1 + \alpha_i/\alpha_1 \sim \varepsilon_i\alpha_1^{m_2}$ for some $\varepsilon_i \in \overline{\mathsf{K}}$ with $\nu(\varepsilon) = 0$ and $p^{s_1} + 1 \le i \le p^{s_2}$. By Lemma 3.1 this gives the roots

$$\underline{\left(\frac{(\varepsilon_i\alpha_1^{m_2})^{e_2}}{\alpha_1^{h_2}}\right)} = \underline{\varepsilon_i}^{e_2}$$

of the associated polynomial $\underline{A}_2(y)\underline{\mathsf{K}}[y]$ of S_2, where $m_2 = h2/e_2$ with $\gcd(h_2, e_2) = 1$. For each $\underline{\varepsilon_i}^{e_2}$ of $\underline{A}_2(y)$ there is root of the ramification polynomial of $\psi(x)$ with $-1 + \beta_r/\beta_1 \sim \varepsilon_i^{p^{s_1}}\alpha_1^{m_2^{p^{s_1}}}$. With this we obtain the corresponding roots of the associated polynomial $\underline{B}_1(y) \in \underline{\mathsf{K}}[y]$ of T_1:

$$\underline{\left(\frac{(\varepsilon_i^{p^{s_1}}\alpha_1^{m_2 p^{s_1}})^{e_2}}{\beta_1^{h_2}}\right)} = \underline{\left(\frac{(\varepsilon_i^{e_2 p^{s_1}}\alpha_1^{h_2 p^{s_1}})^{e_2}}{(\alpha_1 \cdot \cdots \cdot \alpha_{p^{s_1}})^{h_2}}\right)} = \left(\underline{\varepsilon_i}^{e_2}\right)^{p^{s_1}}.$$

This proofs (c). As $\varepsilon \mapsto \varepsilon^p$ is an automorphism of $\underline{\mathsf{K}}$ the splitting fields of $\underline{A}_2(y)$ and $\underline{B}_1(y)$ are isomorphic, which implies (b).

To proof relation (2) we need to show that

$$\nu_{\mathsf{L}}\left(\sum_{i=1}^{p^{s_1}-1}\binom{p^{s_1}}{i}\varepsilon^i\alpha^{m_\lambda i}\right) > m_\lambda p^{s_1}.$$

By the ultrametric inequality it is sufficient to show that for $1 \leq i \leq p^{s_1-1}$

$$\nu_{\mathsf{L}}\left(\binom{p^{s_1}}{i}\gamma^i\alpha^{m_\lambda i}\right) > m_\lambda p^{s_1}.$$

As $\nu_p\left(\binom{p^{s_1}}{i}\right) = s_1 - \nu_p(i)$ this simplifies to $\nu_L(p)(s_1-\nu_p(i)) + m_\lambda i > m_\lambda p_1^s$ or

$$\frac{\nu_L(p)(s_1-\nu_p(i))}{p^{s_1}-i} > m_\lambda.$$

By Lemma 4.2 we have $\frac{\nu_L(p)}{p^{s_1-1}(p-1)} \geq m_1 > m_\lambda$. So it is sufficient to show that

$$\frac{\nu_L(p)(s_1-\nu_p(i))}{p^{s_1}-i} \geq \frac{\nu_L(p)}{p^{s_1-1}(p-1)},$$

which is equivalent to

$$\frac{p(p^{s_1}-i)}{p^{s_1}(p-1)(s_1-\nu_p(i))} \leq 1.$$

We write $i = ap^v$ with $p \nmid a$ and $v < s_1$ and obtain

$$\begin{aligned}\frac{p(p^{s_1}-i)}{p^{s_1}(p-1)(s_1-\nu_p(i))} &\leq \frac{p(p^{s_1}-p^v)}{p^{s_1}(p-1)(s_1-v)} = \frac{p}{p-1}\cdot\frac{p^{s_1-v}-1}{p^{s_1-v}(s_1-v)}\\ &= \frac{p}{p-1}\cdot\frac{1-(1/p)^{s_1-v}}{s_1-v} = \frac{1-(1/p)^{s_1-v}}{1-(1/p)}\cdot\frac{1}{s_1-v}\\ &= \left(1+\frac{1}{p}+\ldots\frac{1}{p^{s_1}-v-1}\right)\frac{1}{s_1-v} \leq 1.\end{aligned}$$

This completes the proof. □

Theorem 6.2. *The ramification polygon* $\mathrm{rp}(\mathsf{L}_{i-1}/\mathsf{L}_i)$ *consists of exactly one segment, which corresponds to the segment* S_i *of* $\mathrm{rp}(\mathsf{L}/\mathsf{K})$ *as follows:*

(a) *The slope of* $\mathrm{rp}(\mathsf{L}_{i-1}/\mathsf{L}_i)$ *is equal to the slope of* S_i.
(b) *The associated inertias of* $\mathrm{rp}(\mathsf{L}_{i-1}/\mathsf{L}_i)$ *and* S_i *are equal.*
(c) *For each root* $\underline{\delta}$ *of the associated polynomial* $\underline{A}_i(y)$ *of* S_i *the element* $\underline{\delta}^{p^{s_i-1}}$ *is a root of the associated polynomial of* $\mathrm{rp}(\mathsf{L}_{i-1}/\mathsf{L}_i)$.

Proof. The minimal polynomial of α_1 over L_1 is $\prod_{i=1}^{p^{s_1}}(x-\alpha_i)$. So the slope of $\mathrm{rp}(\mathsf{L}_0/\mathsf{L}_1)$ is equal to the slope of S_1. By the Theorem of the Product [14, 3] the associated polynomial of $\mathrm{rp}(\mathsf{L}_0/\mathsf{L}_1)$ is $\underline{A}_i(y)$. Thus (a), (b), and (c) hold for $i = 1$. The claims (a), (b), and (c) follow by induction on i by Lemma 6.1. □

7. Splitting Fields

In order to determine the Galois group of an Eisenstein polynomial $\varphi(x)$ we look at its splitting field. If the ramification polynomial of $\varphi(x)$ consists of one segment, we can explicitly construct the splitting field of $\varphi(x)$. In the general case we consider the splitting fields of the subfields corresponding to the segments of the ramification polygon and obtain the splitting field of $\varphi(x)$ as a p-extension over their compositum.

Ramification Polygons with One Segment. Assume that the Newton polygon of $\rho(x)$ is a straight line. It follows from Lemma 4.1 that this can only be the case if either $p \nmid n$ or $n = p^m$ for some positive integer m. Since we have treated the case $p \nmid n$ in section 2, we assume $n = p^m$.

The tamely ramified subfield of the splitting field of $\varphi(x)$ is the splitting field of the ramification polynomial $\rho(x)$ of $\varphi(x)$. We first consider the splitting field of such a polynomial $\rho(x)$ whose degree is not divisible by p.

Lemma 7.1. *Assume that the Newton polygon of $\rho(x) \in \mathcal{O}_{\mathsf{L}}[x]$ consists of one segment of slope $-h/e$ with $\gcd(h,e) = 1 = ae + bh$ for $a, b \in \mathbb{Z}$ and $\gcd(e,p) = 1$. Assume that its associated polynomial $\underline{A}(y) \in \underline{\mathsf{L}}[y]$ is square free and let f be its associated inertia. Let I/L be the unramified extension of degree $\operatorname{lcm}(f, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ and let $\varepsilon \in \mathcal{O}_{\mathsf{I}}$ with $\underline{A}(-\underline{\varepsilon}) = 0$. Then*

$$\mathsf{N} = \mathsf{I}\left(\sqrt[e]{-(-\varepsilon)^b \pi}\right)$$

is the splitting field of $\rho(x)$

Proof. Denote by $A(x) \in \mathcal{O}_{\mathsf{L}}[x]$ a lift of $\underline{A}(y)$. Let M/K be the minimal unramified extension over which $A(y)$ splits into linear factors, say $A(y) = (y - \gamma_1) \cdot \ldots \cdot (y - \gamma_{n/e})$ over M. Let $\mathsf{N} = \mathsf{M}(\beta, \zeta_e)$ where β is a root of $\rho(x)$ and ζ_e is an e-th root of unity. Let $\gamma = \beta^e/\pi^h$ then $\underline{A}(\underline{\gamma}) = 0$. The field N is the splitting field of $\rho(x)$, if $\rho(x)$ or equivalently $\frac{\rho(\beta x)}{\pi^{hn/e}}$, splits into linear factors over N. We obtain

$$\frac{\rho(\beta x)}{(\gamma\pi^h)^{n/e}} \equiv \left(x^e - \frac{\gamma_1}{\gamma}\right) \cdot \ldots \cdot \left(x^e - \frac{\gamma_{n/e}}{\gamma}\right) \bmod \pi_{\mathsf{N}}\mathcal{O}_{\mathsf{N}}[x],$$

where π_{N} denotes a uniformizer in the valuation ring $\mathcal{O}_{\mathsf{N}}$ of N. As $\gcd(e,p) = 1$ for $1 \le i \le n/e$ the polynomials $x^e - \frac{\gamma_i}{\gamma}$ are square free over $\underline{\mathsf{N}}$. Because $\zeta_e \in \mathsf{N}$, they split into linear factors over $\underline{\mathsf{N}}$. Hensel lifting yields a decomposition of $\frac{\rho(\beta x)}{(\gamma\pi^h)^{n/e}}$ into linear factors. It follows that $\rho(x)$ splits into linear factors over N, thus N is the splitting field of $\rho(x)$.

Over M the polynomial $\rho(x)$ splits into irreducible factors $\theta_i(x) = \sum_{j=0}^{e} \theta_{i,j} x^j$ $(1 \le i \le n/e)$ where $\theta_{i,0} \equiv -\gamma_i \pi^h \bmod (\pi^{h+1})$. By Proposition 2.1 the extensions generated by the $\theta_i(x)$ are isomorphic to the extensions generated by the polynomials $x^e + (-\gamma_i\pi^h)^b \pi^{ae} = x^e + (-\gamma_i)^b \pi$ with $ae + bh = 1$. □

Lemma 7.2. *Let u a power of p. Let $F(x) = \sum_{i=0}^{r} a_i x^{p^i} \in \mathbb{F}_u[x]$ be an additive polynomial and assume $e \in \mathbb{N}$ is a divisor of $u - 1$ and of all $p^i - 1$ for all $1 \le i \le r$ with $a_i \neq 0$. If $1 \in \mathbb{F}_u$ is a root of $G(x) = \sum_{i=0}^{r} a_i x^{(p^i-1)/e}$, then $F(x)$ splits into linear factors over $\mathbb{F}_u$ if and only if $G(x)$ splits into linear factors over $\mathbb{F}_u$.*

Proof (by Peter Müller). Clearly, if $F(x)$ splits into linear factors then $G(x)$ splits into linear factors, as the roots of $G(x)$ are powers of the roots of $F(x)$.

Let E be the splitting field of $x^e - 1$ over $\mathbb{F}_p$. Since $e \mid u - 1$ we have $E \subseteq \mathbb{F}_u$. Let M be the set if roots of $F(x)$ in the algebraic closure of $\mathbb{F}_p$. As $F(x)$ is additive M is additively closed. Furthermore, if $\lambda \in E$ and $v \in M$ then $\lambda v \in M$, because we had assumed that E is a subfield of $\mathbb{F}_{p^i}$ for all $1 \le i \le r$ with $a_i \neq 0$. Hence M is an E-vector space.

For each $0 \neq v \in M$ the element v^e is a root of $G(x)$ and therefore v^e is contained in $\mathbb{F}_u$. So $v^{e(u-1)} = 1$ and, as E contains the e-th roots of unity, $v^{u-1} \in E^\times$. Thus there exists $\lambda_v \in E^\times$ with $v^u = \lambda_v v$.

Now assume that $v \in M$ but $v \notin E$. As $G(1) = 0$ we have $1 \in M$. It follows from

$$\lambda_{(v+1)}(v+1) = (v+1)^u = v^u + 1^u = \lambda_v v + 1$$

and the linear independence of 1 and v, that $1 = \lambda_{(v+1)} = \lambda_v$. Hence $M \subseteq \mathbb{F}_u$, so $F(x)$ splits into linear factors over $\mathbb{F}_u$. □

Theorem 7.3. *Let $\varphi(x) \in \mathcal{O}_\mathsf{K}[x]$ be an Eisenstein polynomial of degree np^m and assume that its ramification polygon $\mathrm{rp}(\varphi)$ 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 $\varphi(x)$, $\mathsf{L} = \mathsf{K}(\alpha)$ and $\underline{A}(y) \in \underline{\mathsf{L}}[x]$ the associated polynomial of $\mathrm{rp}(\varphi)$ with associated inertia f. Then*

$$\mathsf{N} = \mathsf{I}\left(\sqrt[e]{-(\varepsilon^b)\alpha}\right)$$

is the splitting field of $\varphi(x)$ where I/L is the unramified extension of degree $\mathrm{lcm}(f, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ and $\varepsilon \in \overline{\mathsf{K}}$ is arbitrary with $\underline{A}(-\underline{\varepsilon}) = 0$.

Proof. By the construction of the ramification polynomial $\rho(x)$ the splitting field of $\rho(x)$ over L is the splitting field of $\varphi(x)$ over K. To be able to use Lemma 7.1 to find the splitting field of $\rho(x)$, we need to show that $\underline{A}(y)$ is square free.

Let $\rho(x) = \sum_{i=0}^{n} \rho_i x^i \in \mathcal{O}_\mathsf{K}[x]$ be the ramification polynomial of $\varphi(x)$. Then the associated polynomial to $\mathrm{rp}(\varphi)$ is

$$\underline{A}(y) = \sum_{j=0}^{(n-1)/e} \underline{A}_j y^j = \sum_{j=0}^{(n-1)/e} \rho_{je} \alpha^{h(j-(n-1)/e)} y^j \in \underline{\mathsf{L}}[y].$$

We consider the polynomial $\underline{B}(x) = \sum_{i=0}^{n} \underline{B}_i x^i = x\underline{A}(\underline{\gamma} x^e)$ for a root $\underline{\gamma}$ of $\underline{A}(y)$. It follows from the construction of $\underline{A}(y)$ that $A_j \neq 0$ if the corresponding coefficient ρ_{je} of $\rho(x)$ yields a vertex of $\mathrm{rp}(\varphi)$. By Lemma 4.1 if $\underline{B}_i \neq 0$ then $i = p^s$ for some $s \in \{0, \ldots, m\}$. Thus $\underline{B}(x)$ is an additive polynomial. Furthermore $\underline{B}'(x) = \underline{B}_1 = \underline{A}_0$, so $\gcd(\underline{B}(x), \underline{B}'(x)) = 1$ and therefore $\underline{B}(x)$ and $\underline{A}(x)$ are square free.

It remains to be shown that $\mathrm{lcm}(f, [\mathsf{L}(\zeta_e) : \mathsf{L}])$ is the degree of the splitting field of $\underline{A}(y)$ over $\mathbb{F}_q \cong \underline{\mathsf{K}}$. Because the associate inertia f is the degree of the splitting field of $\underline{A}(y)$ over $\mathbb{F}_q$ and as $e \mid (q^f - 1)$ this follow from Lemma 7.2 with $u = q^f$, $F(x) = \underline{B}(x)$ and $G(x) := \underline{A}(\underline{\gamma} x)$. □

The General Case. In the general case, that is when $\mathrm{rp}(\varphi)$ consists of more than one segment, ramification polygon and associated polynomials do not provide enough information to describe the splitting field completely. But we can use the results for one segment and the correspondence of theorem 6.2 to give a subfield T, such that the splitting field of $\varphi(x)$ is a p-extension over T. In other words, the field T contains the maximal subfield of the splitting field, which has degree coprime to p over the ground field.

Theorem 7.4. *Let $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_\mathsf{K}[x]$ be Eisenstein of degree $n = ep^m$ with $p \nmid e$ and $m > 0$. Assume the ramification polygon $\mathrm{rp}(\varphi)$ of $\varphi(x)$ consists of $\ell + 1$ segments $S_1, \ldots, S_{\ell+1}$. For $1 \leq i \leq \ell$ let*

- *$m_i = -h_i/e_i$ be the slope of S_i with $\gcd(h_i, e_i) = 1 = d_i e_i + b_i h_i$ for $d_i, b_i \in \mathbb{Z}$,*
- *$A_i(y) \in \mathcal{O}_\mathsf{K}[y]$ be the associated polynomial and f_i associated inertia of S_i,*
- *$\gamma_i \in \overline{\mathsf{K}}$ such that $\underline{A}_i(\gamma_i) = 0$, and*
- *$v_i = b_i \cdot e \cdot p^{m - s_{i-1}} + n + 1$.*

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

$$f = \operatorname{lcm}(f_1, \dots, f_{\ell+1}, [\mathsf{K}(\zeta_{e_1}) : \mathsf{K}], \dots, [\mathsf{K}(\zeta_{e_\ell}) : \mathsf{K}])$$

and by N *the splitting field of* $\varphi(x)$*. Let* α *be a root of* $\varphi(x)$ *and* $\mathsf{K}(\alpha) = \mathsf{L}_0 \supset \mathsf{L}_1 \supset \cdots \supset \mathsf{L}_\ell \supset \mathsf{K}$ *as in Theorem 6.2 be the tower of subfields corresponding to* $\operatorname{rp}(\varphi)$*. Then:*

(a) *The field*

$$\mathsf{T} = \mathsf{I}\left(\sqrt[e_1]{\gamma_1^n \varphi_0}, \dots, \sqrt[e_\ell]{\gamma_\ell^n \varphi_0}, \sqrt[e]{\varphi_0}\right) \text{ for } 1 \le i \le \ell$$

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

(b) *For* $1 \le i \le \ell - 1$ *the extensions* $\mathsf{TL}_{i-1}/\mathsf{TL}_i$ *are elementary Abelian.*

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

Proof. Assume the that the roots $\alpha = \alpha_1, \dots, \alpha_n$ of $\varphi(x)$ are ordered as in Lemma 5.2 For $1 \le i \le \ell$ we have $\mathsf{L}_i = \mathsf{K}(\beta_i)$ with $\beta_i = \alpha_1 \cdots \alpha_{p^i})$. The conjugates of β_i are of the form $\beta_i^{(j)} = \alpha_{(j-1)p^{s_i}+1} \cdot \dots \cdot \alpha_{jp^{s_i}}$.

Theorem 7.3 yields the normal closure N_i of $\mathsf{L}_{i-1}/\mathsf{L}_i$. By Theorem 6.2 we can use e_i, b_i, and f_i of the segment S_i when determining N_i. If ε_i is a root of $\underline{A}_i(y)$ then, by Theorem 6.2 (c), we get

$$\mathsf{N}_i = \mathsf{I}_i\left(\sqrt[e_i]{-((-\varepsilon_i^{p^{s_{i-1}}})^{b_i})\beta_{i-1}}\right)$$

with $\mathsf{I}_i/\mathsf{L}_{i-1}$ unramified of degree $\operatorname{lcm}(f_i, [\mathsf{L}_{i-1}(\zeta_{e_i}), \mathsf{L}_{i-1}])$ and $-\delta_i \in \mathcal{O}_\mathsf{I}$ a lift of a root of the associated polynomial to $\operatorname{rp}(\mathsf{L}_{i-1}/\mathsf{L}_i)$. Furthermore $\mathsf{N}_i/\mathsf{L}_i$ is normal. By Lemma 8.1 the first ramification group and therefore the wildly ramified part of $\mathsf{N}_i/\mathsf{L}_i$ is elementary Abelian.

For the tamely ramified extension $\mathsf{L}_\ell/\mathsf{K}$ we set $\mathsf{N}_{\ell+1} = \mathsf{I}_{\ell+1} = \mathsf{L}_\ell(\zeta_{e_0})$.

We now collect all unramified extensions over K and consider the tower of extensions

$$\mathsf{IL} \supset \mathsf{IL}_1 \supset \cdots \supset \mathsf{IL}_\ell \supset \mathsf{I} \supset \mathsf{K}.$$

By the definition of I the extensions $\mathsf{IN}_i/\mathsf{IL}_i$ are Galois an totally ramified and their tamely ramified part $\mathsf{IN}_i/\mathsf{IL}_{i-1}$ is generated by $x^{e_i} + (-1)^{b_i}\varepsilon_i^{b_i p^{s_{i-1}}}\beta_{i-1}$.

Similarly to the unramified parts we now consider the tamely ramified parts over I. The minimal polynomial of $\sqrt[e_i]{-((-\varepsilon_i^{p^{s_{i-1}}})^{b_i})\beta_{i-1}}$ over I is the norm of its minimal polynomial of $\mathsf{N}_i/\mathsf{I}_i$:

$$\mathrm{N}_{\mathsf{IL}_{i-1}/\mathsf{I}}\left(x^e + ((-\varepsilon_i^{p^{s_{i-1}}})^{b_i}\beta_{i-1}\right)$$

and its constant term is $\left((-1)^{b_i}\varepsilon_i^{b_i p^{s_{i-1}}}\right)^{[\mathsf{IL}_{i-1}:\mathsf{I}]}(-1)^n\varphi_0$. The product of the conjugates of β_{i-1} is up to sign equal to $\prod_{i=1}^n \alpha_i = \pm\varphi_0$. So

$$\mathsf{T}_i = \mathsf{I}\left(\sqrt[e_i e_0]{(-1)^{v_i}\varepsilon_i^{b_i p^n}\varphi_0}\right)$$

is Galois and the tamely ramified part of IN_i/I $(1 \le i \le \ell)$. Each of these extensions contains $\mathsf{I}/\mathsf{L}_\ell/\mathsf{I}$. The compositum of the T_i is T. In the new tower of extensions

$$\mathsf{TL} = \mathsf{TL}_0 \supset \mathsf{TL}_1 \supset \cdots \supset \mathsf{TL}_{\ell-1} \supset \mathsf{T} \supset \mathsf{I} \supset \mathsf{K}$$

the extension T/K is Galois, because it is the compositum of Galois extensions. Also $\mathsf{TL}_{i-1}/\mathsf{TL}_i$ is an elementary Abelian p-Extension which proofs (b). It follows by induction that N/T is a p-extension.

The ramification index of T/K follows from Abhyankar's Lemma (see, for example, **??**chapter 5 §2]nark, as T is the compositum of the tamely ramified extensions T_i/K. A first, obvious, bound for $[\mathsf{T}:\mathsf{K}]$ is $e_0 \cdot [\mathsf{K}(\zeta_{e_0}):\mathsf{K}] \cdot \prod n_i$ with $n_i e_i f_i \cdot [\mathsf{K}(\zeta_{e_i}):\mathsf{K}]$. By Theorem 6.2 we can use the extension $\mathsf{L}_{i-1}/\mathsf{L}_i$ to estimate n_i for $1 \le i \le \ell$. We obtain

$$\prod_{i=1}^{\ell} n_i < (p^{s_1} p^{s_2-s_1} \cdot \ldots \cdot p^{s_\ell - s_{\ell-1}})^2 = (p^{s_\ell})^2 = (p^m)^2.$$

Furthermore $e_0 \cdot [\mathsf{K}(\zeta_{e_0}):\mathsf{K}] < e_0^2$ which implies (c). □

8. Galois Groups

In the case of an Eisenstein polynomial $\varphi(x)$ with one-sided ramification polygon we use the results of section 7 and the well known structure of Galois groups of tamely ramified extensions (theorem 2.3) to give an explicit description of $\mathrm{Gal}(\varphi)$.

Recall, that we denote the slope of the ramification polygon by $-h/e$ ($\gcd(h,e)=1$) and that the degree of $\varphi(x)$ is equal to p^m. Denote by N the splitting field of $\varphi(x)$, by L the subfield generated by a root of $\varphi(x)$, and by T the maximal tamely ramified subfield of N/K. By Lemma 7.1 T/K has ramification index e and its inertia degree f is determined by the degrees of the irreducible factors of the associated polynomial over $\underline{\mathsf{K}}$. Set $G = \mathrm{Gal}(\varphi) = \mathrm{Gal}(\mathsf{N}/\mathsf{K})$, $H = \mathrm{Gal}(\mathsf{N}/\mathsf{L})$, and let $G_1 \trianglelefteq G$ be the first ramification subgroup of N/K. Then $G = G_1 \rtimes H$ holds, as L and T satisfy the conditions $\mathsf{L} \cap \mathsf{T} = \mathsf{K}$ and $\mathsf{LT} = \mathsf{N}$. Because H is the Galois group of a tame extension, its structure is well known (Theorem 2.3). It remains to determine the group G_1 and the action of H on G_1.

We denote by G_i the i-th ramification subgroup of G. In the following, we examine the ramification filtration $G \ge G_0 \ge G_1 \ge \ldots$ of G.

Lemma 8.1. *The ramification filtration of $G = \mathrm{Gal}(\varphi)$ is*

$$G \ge G_0 \ge G_1 = G_2 = \ldots = G_h > G_{h+1} = \{\mathrm{id}\}$$

The group $G_1 = \mathrm{Gal}(\mathsf{N}/\mathsf{K}$ is isomorphic to the additive group of $\mathbb{F}_{p^m}$.

Proof. Let π_{N} be a prime element of N. We have to show the equality $\nu_{\mathsf{N}}(\pi_{\mathsf{N}}^g - \pi_{\mathsf{N}}) = h+1$ for all $g \in G_1$. As $\mathsf{N} = \mathsf{LT}$ the ramification polygon $\mathrm{rp}(\mathsf{N}/\mathsf{T})$ is a line of slope $-e \cdot \frac{h}{e} = -h$. Thus $\nu_{\mathsf{N}}(\frac{\pi_{\mathsf{N}}^g - \pi_{\mathsf{N}}}{\pi_{\mathsf{N}}}) = h$ for all $g \in G$ and therefore we obtain

$$\nu_{\mathsf{N}}(\pi_{\mathsf{N}}^g - \pi_{\mathsf{N}}) = \nu_{\mathsf{N}}\left(\frac{\pi_{\mathsf{N}}^g - \pi_{\mathsf{N}}}{\pi_{\mathsf{N}}}\right) + \nu_{\mathsf{N}}(\pi_{\mathsf{N}}) = h+1 \text{ for all } g \in G_1$$

as desired. Since the quotients G_i/G_{i+1} for $i \ge 1$ embed into the additive Group of the residue class field of N (see [19, chapter IV]), the second statement follows from $G_1 = G_h = G_h/G_{h+1}$. □

The next theorem specifies the action of H on G_1 and describes the Galois group G as a subgroup of the affine group $\mathrm{AGL}(m,p)$. We denote by $\wp = (\pi_{\mathsf{N}})$ the maximal ideal of

the valuation ring $\mathcal{O}_{\mathsf{N}}$. The group G acts naturally on the quotients $\wp^i/\wp^{i+1}$ which are, as additive groups, isomorphic to the additive group of the residue class field of N. Furthermore,

$$\Theta_i : G_i/G_{i+1} \to (\wp^i/\wp^{i+1}, +) : gG_{i+1} \mapsto \left(\frac{\pi_{\mathsf{N}}^g}{\pi_{\mathsf{N}}} - 1\right) + \wp^{i+1}$$

embeds each quotient G_i/G_{i+1} into $\wp^i/\wp^{i+1}$ (see again [19, chapter IV]).

Theorem 8.2. *Let $\varphi(x) \in \mathcal{O}_{\mathsf{K}}[x]$ be an Eisenstein polynomial of degree p^m, whose ramification polygon consists of one single segment of slope $-\frac{h}{e}$ with $\gcd(h,e) = 1$. Then $\mathrm{Gal}(\varphi) = G_1 \rtimes H$, where G_1 is the first ramification group and H corresponds to the maximal tamely ramified subfield of the splitting field of $\varphi(x)$ (see Proposition 7.3). Moreover, $\mathrm{Gal}(\varphi)$ 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).

Proof. We have already seen, that $\mathrm{Gal}(\varphi) = G_1 \rtimes H$. If $\widetilde{G}_1 = \{s_v : x \mapsto x + v \mid v \in (\mathbb{F}_p)^m\}$ and $\widetilde{H} = \{u_a : x \mapsto xa \mid a \in H'\}$ then $\widetilde{G} = \widetilde{G}_1 \rtimes \widetilde{H}$, where the action of $\widetilde{H}$ on $\widetilde{G}_1$ is the multiplication of a vector by a matrix: $s_v^{u_a} : x \mapsto (xa^{-1} + v)a = x + va$. First of all, we have $\widetilde{G}_1 \cong G_1 = G_h/G_{h+1}$ by Lemma 8.1.

Now, we relate the actions of H on $\wp^h/\wp^{h+1}$ and on G_1. The injective homomorphism

$$\Theta_h : G_h/G_{h+1} = G_1 \to \wp^h/\wp^{h+1} : g \mapsto \left(\frac{\pi_{\mathsf{N}}^g}{\pi_{\mathsf{N}}} - 1\right) \bmod \wp^{h+1}$$

is a H-homomorphism, which means, that $\Theta_h(g)^b = \Theta_h(g^b)$ for $g \in G_1, b \in H$. To see that, let $\pi_{\mathsf{N}}^g = \pi_{\mathsf{N}}(1+\delta)$ with $\delta \in \wp^h$. Then $\Theta_h(g)^b = \delta^b \bmod \wp^{h+1}$. For computing $\Theta_h(g^b) = \left(\frac{\pi_{\mathsf{N}}^{g^b}}{\pi_{\mathsf{N}}} - 1\right) \bmod \wp^{h+1}$, set $\pi_{\mathsf{N}}^{b^{-1}} = \pi_{\mathsf{N}}\varepsilon$ with $\varepsilon \in \mathcal{O}_{\mathsf{N}}^\times$ and consider $\pi_{\mathsf{N}}^{g^b} = \pi_{\mathsf{N}}^{b^{-1}gb} = (\pi_{\mathsf{N}}\varepsilon)^{gb} = (\pi_{\mathsf{N}}^g\varepsilon^g)^b$. This is modulo $\wp^{h+1}$ congruent to $(\pi_{\mathsf{N}}^g\varepsilon)^b = (\pi_{\mathsf{N}}(1+\delta)\varepsilon)^b = (\pi_{\mathsf{N}}\varepsilon)^b(1+\delta)^b = \pi_{\mathsf{N}}(1+\delta^b)$ which proves the assertion.

It follows, that H acts on G_1 in the same way as it acts on $\Theta_h(G_1) \leq \wp^h/\wp^{h+1}$, where both groups are isomorphic to $(\mathbb{F}_{p^m}, +)$. Because the action on $\Theta_h(G_1)$ must be faithful, the action on G_1 is faithful, too. Let H' be the subgroup of $\mathrm{GL}(m,p)$, which describes the action of H on $\Theta_h(G_1)$. Then $H \cong H' \cong \widetilde{H}$ and thus $\mathrm{Gal}(\varphi) \cong \widetilde{G}$. □

Remark 8.3. Another way to describe the Galois group is as a finitely presented group:

$$\mathrm{Gal}(\varphi) \cong \left\langle s, t, a_1, \ldots, a_m \;\middle|\; \begin{array}{l} s^e = 1, t^f = s^r, s^t = s^q, [a_i, a_j] = 1, \\ a_i^p = 1, a_i^s = s_i, a_i^t = t_i \text{ for } 1 \leq i < j \leq m \end{array} \right\rangle.$$

Here s and t generate a subgroup isomorphic to H and $a_1, \ldots, a_m$ generate a normal subgroup isomorphic to G_1. The number e is the denominator of the slope of $\mathrm{rp}(\varphi)$ and f is equal to $\mathrm{lcm}(f_1, [\mathsf{K}(\zeta_e) : \mathsf{K}])$, where f_1 denotes the associated inertia. The integer r fulfills the condition $\underline{A}(\zeta^r) = 0$ for a primitive (q^f-1)-th root of unity ζ and the associated polynomial $A(y) \in \mathsf{L}[y]$ (compare lemma 7.1 and theorem 2.3). The elements s_i and t_i are words in $a_1, \ldots, a_m$. They are determined by the action of the generating automorphisms of H on $\Theta_h(G_1) = \Theta_h(G_h/G_{h+1}) \leq \wp^h/\wp^{h+1}$.

In both descriptions of $\mathrm{Gal}(\varphi)$ we need a little computation to get the action of H on $\Theta_h(G_1)$ and therefore the matrix group H' (or the elements s_i and t_i). As we have two generators of H explicitly as automorphisms of N/L (see 2.3), we can determine their action on $\wp^h/\wp^{h+1}$. We use the representation of H of dimension $\widetilde{f}\cdot f$ over $\mathbb{F}_p$, where $\widetilde{f}$ denotes the inertia degree of the ground field K.

Now, we have to find the submodule $\Theta_h(G_1) \cong \mathbb{F}_{p^m}^+$ of the H-module $(\wp^h/\wp^{h+1}, +) \cong \mathbb{F}_{q^f}^+$, as, in general, $q_f \geq p^m$. In the following lemma we show that $\Theta_h(G_1)$ can easily be computed form the zeros of the associated polynomial $\underline{A}(y) \in \underline{\mathsf{K}}[y]$. Recall that the splitting field N of $\varphi(x) \in \mathcal{O}_\mathsf{K}[x]$ can be represented in the form $\mathsf{N} = \mathsf{L}(\zeta, \pi_\mathsf{N}) = \mathsf{K}(\alpha)(\zeta, \pi_\mathsf{N})$ with $\pi_\mathsf{N} = \sqrt[e]{\zeta^r\alpha}$ and let $d = \frac{p^m-1}{e}$ be the degree of the associated polynomial $\underline{A}(y)$.

Lemma 8.4. *Let $\underline{\gamma}_1, \ldots, \underline{\gamma}_d$ be the zeros $\underline{A}(y)$ in $\underline{\mathsf{N}}$ and $a, b \in N$ with $ae - bp^m = 1$. Then:*

(a) *For $1 \leq i \leq d$ the residue class field $\underline{\mathsf{N}}$ contains the e-th roots of $\frac{\underline{\gamma}_i}{\underline{\zeta^{rh}}}$ which we denote by $\underline{\gamma}_{i,1}, \ldots, \underline{\gamma}_{i,e}$.*

(b) *The images of G_1 under Θ_h are*

$$\{0 + \wp^{h+1}, a\gamma_{i,j}\pi_\mathsf{N}^h + \wp^{h+1} | 1 \leq i \leq d, 1 \leq j \leq e\},$$

where $\gamma_{i,j}$ denotes a lift of $\underline{\gamma}_{i,j} \in \underline{\mathsf{N}}$ to $\mathcal{O}_\mathsf{N}$.

Proof. (a) The roots $-1 + \frac{\alpha_i}{\alpha}$ $(s \leq i \leq p^m)$ of the ramification polynomial $\rho(x)$ have N-valuation h and therefore the form $\xi\pi_\mathsf{N}^h$ for some $\xi \in \mathcal{O}_\mathsf{N}^\times$. By Lemma 3.1 the roots of $\underline{A}(y)$ are of the form

$$\underline{\left(\frac{(\xi\pi_\mathsf{N}^h)^e}{\alpha^h}\right)} = \underline{\left(\frac{\left(\xi\sqrt[e]{\zeta^r\alpha}\right)^e}{\alpha^h}\right)} = \underline{\xi^e\zeta^{rh}}.$$

(b) The homomorphism $\Theta_h : G_h/G_{h+1} \to (\wp^h/\wp^h + 1)$ is independent of the choice of the prime element. As in the proof of Lemma 4.4 we therefore can use the prime element $\pi'_\mathsf{N} = \alpha^a/\beta^b$, where β is an uniformizing element of T. Also as in the proof of Lemma 4.4, we use the representation $\alpha_i/\alpha = 1 + \delta\alpha^{h/e}$ with $\nu(\delta_i) = 0$ for the roots of $\rho(x)$. Note that δ and $\alpha^{h/e}$ in general are not elements of N.

Now we have for $\sigma \in G_1$, because $p \nmid a$, that

$$\frac{\sigma(\pi'_\mathsf{N})}{\pi'_\mathsf{N}} - 1 = \frac{\alpha_i^a}{\beta^b}\frac{\beta^b}{\alpha^a} - 1 = \left(\frac{\alpha_i}{\alpha}\right)^a - 1 = \alpha\delta\alpha^{h/e} + \ldots.$$

The image $\Theta_h(\sigma)$ is the coset of $a\delta\alpha^{h/e} + \ldots$ in $\wp^h/wp^{h+1}$. In order to find a representative by elements in N for this class we start with $\xi\sqrt[e]{\zeta^r\alpha}^h = \delta\alpha^{h/e}$ which is equivalent to $\delta = \gamma\sqrt[e]{\zeta^r}^h$. Thus, as $\xi \in \mathcal{O}_\mathsf{N}^\times$:

$$\frac{\sigma(\pi'_\mathsf{N})}{\pi'_\mathsf{N}} - 1 = a\xi\sqrt[e]{\zeta^r}^h\sqrt[e]{\alpha}^h + \cdots = a\xi\pi_\mathsf{N}^h + \cdots \equiv a\xi\pi_\mathsf{N}^h \bmod \wp^{h+1}.$$

Since each of the $d = (p^m - 1)/e$ roots of $\underline{A}(y)$ give e elements ξ, we have, together with $0 + \wp^{h+1}$, described all images of Θ_h. □

Remark 8.5. We use the notation from the proof of Lemma 8.4 above. The operation of the field automorphisms s and t (see Theorem 2.3) on $\Theta_h(G_1)$ are $s(\zeta^i\pi_\mathsf{N}^h + \wp^{h+1}) = \zeta^{\ell h+i}\pi_\mathsf{N}^h + \wp^{h+1}$ and $t(\zeta^i\pi_\mathsf{N}^h + \wp^{h+1}) = \zeta^{\ell hk+qi}\pi_\mathsf{N}^h + \wp^{h+1}$.

9. Examples

We give some examples to demonstrate the calculation of Galois groups using our results. We consider two polynomials of degree 9 over $\mathbb{Q}_3$ leading to different Galois groups and one polynomial of degree 81 over $\mathbb{Q}_3$.

In each of the examples we denote by $\mathsf{L} = \mathsf{K}(\alpha)$ the field generated by a root α of the respective polynomial.

Example 9.1. romano example5.1

Example 9.2. We determine the Galois group of $\varphi(x) = x^9 + 9x + 3 \in \mathbb{Q}_3[x]$. The ramification polygon of $\varphi(x)$ is a straight line connecting the points $(0, 10)$ and $(8, 0)$ of slope $-\frac{h}{e} = -\frac{5}{4}$. Therefore the polynomial $\varphi(x)$ is not covered by Romano's results. Let α be a root of $\varphi(x)$ and $\mathsf{L} = \mathbb{Q}_3(\alpha)$. The associated polynomial $\underline{A}(y) = y^2 + 1 \in \underline{\mathsf{L}}[x] = \mathbb{F}_3[x]$. of the ramification polynomial $\rho(x) \in \mathsf{L}[x]$ is irreducible, so its associated inertia is $f = 2$. The inertia degree of the splitting field of $\rho(x)$ is $\operatorname{lcm}(2, 4) = 4$. Let ζ be a primitive eighth root of unity. Because $\underline{\zeta}^2$ is a root of $\underline{A}(y) = y^2 + 1$, Lemma 7.1 gives us $\mathsf{N} = \mathsf{L}(\zeta, \sqrt[4]{\zeta^2\alpha})$ as the splitting field of $\rho(x)$ over L, which is also the splitting field of $\varphi(x)$ over $\mathbb{Q}_3$ (see Proposition 7.3). Set $\pi_{\mathsf{N}} = \sqrt[4]{\zeta^2\alpha}$. By Theorem 2.3 (with $e = 4, f = 2$ and $r = 2$) the group $H = \operatorname{Gal}(\mathsf{N}/\mathsf{L})$ is generated by the automorphisms

$$s : \zeta \mapsto \zeta, \pi_{\mathsf{N}} \mapsto \zeta^2\pi_{\mathsf{N}} \text{ and } t : \zeta \mapsto \zeta^3, \pi_{\mathsf{N}} \mapsto \zeta\pi_{\mathsf{N}}.$$

With Remark 8.5 we get $S \in \mathrm{GL}(2, 3)$ as the representation matrix of the automorphism of $\mathbb{F}_{3^2}^+$ given by $\zeta^i \mapsto \zeta^{10+i}$ and $T \in \mathrm{GL}(2, 3)$ as the representation matrix of the automorphism $\zeta^i \mapsto \zeta^{3i}$. With a basis corresponding to $1, \zeta$ of $\wp^5/\wp^6 \cong (\mathbb{F}_{3^2}, +)$, we obtain

$$S = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \text{ and } T = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

which represent the action of s and t on the first ramification group G_1. The matrices S and T generate a representation of the quaternion group Q_8 of order 8 over $\mathbb{F}_3$. In this special case we are already in the right dimension 2 and it is not necessary to search for a submodule. Hence the Galois group of $\varphi(x)$ is isomorphic to the group

$$\begin{aligned} G &= \left\{ t_{a,v} : (\mathbb{F}_3)^2 \to (\mathbb{F}_3)^2 : x \mapsto xa + v \;\middle|\; a \in \langle S, T \rangle,\ v \in (\mathbb{F}_3)^2 \right\} \\ &\cong C_3^2 \rtimes Q_8. \end{aligned}$$

Example 9.3. Let $\varphi(x) = x^9 + 3x^2 + 6 \in \mathbb{Q}_3[x]$. Here, the ramification polygon connects the points $(0, 2)$ and $(8, 0)$, therefore has slope $-\frac{h}{e} = -\frac{1}{4}$. The associated polynomial of the ramification polynomial $\rho(x) \in L[x]$ is congruent to $x^2 + 2$ in $\underline{\mathsf{L}}[x]$. As $x^2 + 2$ splits into linear factors over $\underline{\mathsf{L}} \cong \mathbb{F}_3$, the polynomial $\rho(x)$ generates totally and tamely ramified extensions of degree 4 of L. Hence we must add the 4-th roots of unity to get the splitting field $\mathsf{N} = \mathsf{L}(\zeta, \sqrt[4]{\alpha})$ (see Lemma 7.1 and Proposition 7.3), where ζ is a primitive eighth root of unity. By Theorem 2.3 (with $e = 4, f = 2$ and $r = 0$) the group $H = \operatorname{Gal}(\mathsf{N}/\mathsf{L})$ is generated by the automorphisms

$$s : \zeta \mapsto \zeta, \sqrt[4]{\alpha} \mapsto \zeta^2\sqrt[4]{\alpha} \text{ and } t : \zeta \mapsto \zeta^3, \sqrt[4]{\alpha} \mapsto \sqrt[4]{\alpha}.$$

With a basis corresponding to $1, \zeta$ of $\wp/\wp^2 \cong (\mathbb{F}_{3^2}, +)$, we obtain

$$S = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$$

for the action of s and t on G_1. Again, we are already in the right dimension and do not have to search for a submodule. In this case S and T generate a representation of the dihedral group D_8 of order 8 over $\mathbb{F}_3$ and $\mathrm{Gal}(\varphi)$ is isomorphic to

$$\begin{aligned} G &= \left\{ t_{a,v} : (\mathbb{F}_3)^2 \to (\mathbb{F}_3)^2 : x \mapsto xa + v \;\middle|\; a \in \langle S, T \rangle,\ v \in (\mathbb{F}_3)^2 \right\} \\ &\cong C_3^2 \rtimes D_8. \end{aligned}$$

Example 9.4. We determine the Galois group of the polynomial

$$\varphi(x) = x^{81} + 3x^{80} + 3x^{70} + 3x^{60} + \ldots + 3x^{10} + 3 \in \mathbb{Q}_3[x].$$

Let α be a root of $\varphi(x)$ and $\mathsf{L} = \mathbb{Q}_3(\alpha)$. The ramification polygon of $\varphi(x)$ is a straight line connecting the points $(0, 10)$ and $(80, 0)$ of slope $-\frac{h}{e} = -\frac{1}{8}$. The associated polynomial of the ramification polynomial $\rho(x) \in \mathsf{L}[x]$ is

$$\underline{A}(y) = y^{10} + 2 = (y+1)(y+2)(y^4 + \ldots)(y^4 + \ldots) \in \underline{\mathsf{L}}[x].$$

Hence the associated inertia is 4. With $[\mathbb{Q}_3(\zeta_8) : \mathbb{Q}_3] = 2$ we obtain the inertia degree $f = \mathrm{lcm}(4, 2) = 4$ of the splitting field. So $\mathsf{T} \cong \mathbb{F}_{3^4}$. Let ζ be a $(3^4 - 1)$-th root of unity. Because $\zeta^0 = 1$ is a root of $\underline{A}(y) = y^{10} + 2$, Lemma 7.1 gives us $\mathsf{N} = \mathsf{L}(\zeta, \sqrt[8]{\alpha})$ as the splitting field of $\rho(x)$ over L, which is also the splitting field of $\varphi(x)$ over $\mathbb{Q}_3$ (see Proposition 7.3). By Theorem 2.3 (with $e = 8$, $f = 4$ and $r = 0$) the group $H = \mathrm{Gal}(\mathsf{N}/\mathsf{L})$ is generated by the automorphisms

$$s : \zeta \mapsto \zeta,\ \sqrt[8]{\alpha} \mapsto \zeta^{10} \sqrt[8]{\alpha} \text{ and } t : \zeta \mapsto \zeta^3,\ \sqrt[8]{\alpha} \mapsto \sqrt[8]{\alpha}.$$

By Remark 8.5 we obtain $S \in \mathrm{GL}(4, 3)$ as the representation matrix of the automorphism of $\mathbb{F}_{3^4}^+$ given by $\zeta^i \mapsto \zeta^{10+i}$ and $T \in \mathrm{GL}(4, 3)$ as the representation matrix of the automorphism $\zeta^i \mapsto \zeta^{3i}$. With a basis corresponding to $1, \zeta, \zeta^2, \zeta^3$ of $\wp/\wp^2 \cong (\mathbb{F}_{3^4}, +)$, these are

$$S = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 2 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix}.$$

Hence the Galois group of $\varphi(x)$ is isomorphic to the group

$$\begin{aligned} G &= \left\{ t_{a,v} : (\mathbb{F}_3)^4 \to (\mathbb{F}_3)^4 : x \mapsto xa + v \;\middle|\; a \in \langle S, T \rangle,\ v \in (\mathbb{F}_3)^4 \right\} \\ &\cong C_3^4 \rtimes \langle S, T \rangle. \end{aligned}$$

of order $3^4 \cdot 8 \cdot 4 = 2592$.

10. Acknowledgments

We thank Peter Müller from Universität Würzburg for the proof of Lemma 7.2. Support was provided in part by a new faculty grant from UNC Greensboro and by a grant from the Deutsche Forschungsgemeinschaft.

References

[1] D. Ford, S. Pauli, and X.-F. Roblot, *A Fast Algorithm for Polynomial Factorization over* $\mathbb{Q}_p$, Journal de Théorie des Nombres de Bordeaux **14** (2002) 151–169.

[2] C. Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, Dissertation, Universität Paderborn, 2010.

[3] J. Guardia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428 (2009).

[4] J. Guardia, E. Nart, S. Pauli, *Single Factor Lifting for Polynomials over Local Fields*, submitted (2011).

[5] H. Hasse, *Number Theory*, Springer Verlag, Berlin, 1980.

[6] C. Helou, *Non Galois Ramification Theory for Local Fields*, Fischer Verlag, Munich, 1990.

[7] J. Jones and D. Roberts, *Nonic 3-adic Fields*, in ANTS VI, Springer Lecture Notes in Computer Science, 3076 (2004), 293-308.

[8] J. Jones and D. Roberts, *A Database of Local Fields*, J. Symbolic Comput., **41** (2006), 80-97, `http://math.asu.edu/~jj/localfields`.

[9] J. Jones and D. Roberts, *Octic 2-adic Fields*, J. Number Theory., **128** (2008), 1410-1429.

[10] J. Klüners, *On Computing Subfields. A Detailed Description of the Algorithm*, Journal de Theorie des Nombres de Bordeaux, **10** (1998), 253-271.

[11] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, Dissertation, Universitat de Barcelona, 1999.

[12] J. Montes and E. Nart, *On a Theorem of Ore*, J. Algebra, **146** (1992), 318–334.

[13] W. Narkiewicz: *Elementary and Analytic Theory of Algebraic Numbers*, Springer Verlag, Berlin 2004.

[14] Ö. Ore, *Newtonsche Polynome in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84–117.

[15] S. Pauli, *Factoring polynomials over local fields II*, in G. Hanrot and F. Morain and E. Thomé, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010*, LNCS, Springer Verlag, 2010.

[16] D. S. Romano, *Galois groups of strongly Eisenstein polynomials*, Dissertation, UC Berkeley, 2000.

[17] D. S. Romano, *Ramification polygons and Galois groups of wildly ramified extensions*, Preprint, 2007.

[18] J. Scherk, *The Ramification Polygon for Curves over a Finite Field*, Canadian Mathematical Bulletin, **46**, no. 1 (2003), 149-156.

[19] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1963.

[20] R. P. Stauduhar, *The Determination of Galois Groups*, Math. Comp. **27** (1973), 981996.

Florastrasse 50, 40217 Düsseldorf, Germany
E-mail address: `grevec@web.de`

Department of Mathematics and Statistics, University of North Carolina at Greensboro, Greensboro, NC 27402, USA
E-mail address: `s_pauli@uncg.edu`