

GALOIS GROUPS OF EISENSTEIN POLYNOMIALS WHOSE RAMIFICATION POLYGON HAS ONE SIDE

CHRISTIAN GREVE AND SEBASTIAN PAULI

ABSTRACT. Let $\varphi(x)$ be an Eisenstein polynomial over a local field and α be a root of $\varphi(x)$. We describe the Galois group of $\varphi(x)$ in the case where the Newton polygon of $\varphi(\alpha x + \alpha)/x$ has only one side.

1. INTRODUCTION

Let K be a field complete with respect to a non-archimedean exponential valuation ν with residue class field \underline{K} of characteristic $p \neq \infty$; we call K a local field. Assume that ν is normalized such that $\nu(\pi) = 1$ where π is a uniformizing element in the valuation ring \mathcal{O}_K of K .

The Newton polygon of a polynomial $\varphi(x) = \sum_{i=0}^n \varphi_i x^i \in \mathcal{O}_K[x]$ is the lower convex hull of the set of points $\{(i, \nu(\varphi_i)) \mid 0 \leq i \leq n\}$. The negative of the slopes of the segments of the Newton polygon of $\varphi(x)$ are the exponential valuations of the roots of $\varphi(x)$.

Now let $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_K[x]$ be an Eisenstein polynomial, which means $\nu(\varphi_0) = 1$ and $\nu(\varphi_i) \geq 1$ for $1 \leq i \leq n-1$, and denote by α a root of $\varphi(x)$ in an algebraic closure \overline{K} of K .

If p does not divide the degree of $\varphi(x)$ the extension $K(\alpha)$ is tamely ramified and can be generated by a pure polynomial. In Section 2 we show how this pure polynomial can be obtained and recall the explicit description of its Galois group. Furthermore we describe the splitting field of polynomials, whose degree is coprime to p and whose associated polynomial, obtained by “flattening” its Newton polygon, is square free over \underline{K} .

If p divides the degree of $\varphi(x)$ the situation becomes more difficult. John Jones and David Roberts have developed algorithms based on the resolvent method for the special cases of extensions of degree 2^2 , 2^3 , and 3^2 over \mathbb{Q}_2 and \mathbb{Q}_3 respectively [JR04, JR06, JR08]. David Romano has treated the case of Eisenstein polynomials $\varphi(x)$ of degree p^m whose ramification polygon, that is the Newton polygon of the ramification polynomial $\varphi(\alpha x + \alpha)/(\alpha^n x)$, consists of one segment with slope $-h/(p^m - 1)$, where h is a natural number with $\gcd(h, p^m - 1) = 1$ [Rom00, Rom07]. In this case the Galois group is isomorphic to the group

$$\Gamma = \{x \mapsto ax^\sigma + b \mid a \in \mathbb{F}_{p^m}^\times, b \in \mathbb{F}_{p^m}, \sigma \in \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_{p^m} \cap \underline{K})\}$$

of permutations of \mathbb{F}_{p^m} , therefore the Galois group is uniquely determined by the exponent m .

In Section 3, we consider a wider class of Eisenstein polynomials. We assume a one-sided ramification polygon as well, but allow arbitrary slopes. This class of Eisenstein polynomials leads to various new Galois groups. We show that the associated polynomial of the ramification polynomial of these polynomials is squarefree and find their splitting field using the results from Section 2. This enables us to compute an explicit description of the Galois group as a subgroup of the affine group $\text{AGL}(m, p)$.

In Section 4 we give several concrete examples of Eisenstein polynomials with one-sided ramification polygon and compute their Galois groups using our results from Section 3.

2. EISENSTEIN POLYNOMIALS OF TAME DEGREE

Proposition 2.1. *Let $\varphi(x) = x^e + \sum_{i=1}^{e-1} \varphi_i x^i + \varphi_0 \in \mathcal{O}_K[x]$ of degree $e = e_0 p^m$ with $\gcd(e_0, p) = 1$ be a polynomial whose Newton polygon is a line of slope $-h/e$, where $\gcd(e, h) = 1$. Let α be a root of $\varphi(x)$. The maximum tamely ramified subextension M of $L = K(\alpha)$ of degree e_0 can be generated by the Eisenstein polynomial $x^{e_0} + \psi_0^b \pi^{e_0 a}$ where $\psi_0 \equiv \varphi_0 \pmod{(\pi^{h+1})}$ and 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 $\nu(\alpha) = h/e$. Because $\gcd(e, h) = 1$, for each root α of $\varphi(x)$ the extension $K(\alpha)/K$ is totally ramified of degree e , which implies that $\varphi(x)$ is irreducible. So the extensions $K(\alpha)$ are isomorphic. We fix a root α of $\varphi(x)$ and set $L = K(\alpha)$.

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

$$x^{e_0} + \frac{\psi_0}{\alpha^e} = x^{e_0} - \frac{(1 + \pi\varepsilon)\varphi_0}{(1 + \pi_L \delta)\varphi_0} \equiv x^{e_0} - 1 \pmod{\pi_L \mathcal{O}_L[x]}.$$

Obviously $\rho(x) = x^{e_0} - 1 \in \mathbb{L}[x]$ is squarefree 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 $x^{e_0} + \psi_0$. Set $\gamma = \beta^b \pi^a$, then $\nu(\gamma) = \nu(\beta^b \pi^a) = bh/e_0 + a = 1/e$ and $M = K(\beta) = K(\gamma)$. As $\gamma^{e_0} = \beta^{e_0 b} \pi^{e_0 a} = -\psi_0^b \pi^{e_0 a}$, γ is a root of $x^{e_0} + \psi_0^b \pi^{e_0 a} \in \mathcal{O}_K[x]$. \square

Corollary 2.2. *Let $\varphi(x) = \sum_{i=0}^n \varphi_i x^i \in \mathcal{O}_K[x]$ be an Eisenstein polynomial with $p \nmid n$. If $\psi(x) = x^n + \psi_0$ with $\psi_0 \equiv \varphi_0 \pmod{(\pi^2)}$, 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 $\varphi(x) = \sum_{i=0}^n \varphi_i x^i \in \mathcal{O}_K[x]$ with $p \nmid n$ is $N = K(\zeta_n, \sqrt[n]{-\varphi_0})$, where ζ_n is a primitive n -th root of unity. The extension generated by $\varphi(x)$ is normal if and only if K contains the n -th roots 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, [Has80, 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 N/K with ramification index e and inertia degree f . There exists an integer r with $r(q-1) \equiv 0 \pmod{e}$ such that $N = K(\zeta, \sqrt[e]{\zeta^r \pi})$, where ζ is a $(q^f - 1)$ -st root of unity and $q^f - 1 \equiv 0 \pmod{e}$. 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

$$\langle s, t \mid s^e = 1, t^f = s^r, s^t = s^q \rangle.$$

So the splitting field of $x^n + \varphi_0 \in \mathcal{O}_K[x]$ with $p \nmid n$ and $\nu(\varphi_0) = 1$ is $\mathbf{N} = \mathbf{K}(\zeta, \sqrt[n]{-\varphi_0})$, where ζ is a primitive $(q^f - 1)$ -st root of unity for $f = [\mathbf{K}(\zeta_n) : \mathbf{K}]$. Its Galois group is

$$\langle s, t \mid s^n = 1, t^f = 1, s^t = s^a \rangle \cong C_n \rtimes C_f,$$

where we denote by C_n the cyclic group of order n .

The Associated Polynomial. Let $\varphi(x) = \sum_{i=0}^n \varphi_i x^i \in \mathcal{O}_K[x]$ be a not necessarily irreducible monic polynomial whose Newton polygon consists of one segment with slope $-h/e$ where $\gcd(e, h) = 1$. In the following we use the associated polynomial of $\varphi(x)$ to find the splitting field of $\varphi(x)$.

Let α be a root of $\varphi(x)$, set $\mathbf{L} = \mathbf{K}(\alpha)$, let $\pi_{\mathbf{L}}$ be a uniformizing element of \mathbf{L} , and let $\mathcal{O}_{\mathbf{L}}$ be the valuation ring of \mathbf{L} . We have $\nu(\alpha) = h/e$ and thus $\nu(\alpha^e/\pi^h) = 0$. We consider the polynomial

$$\frac{\varphi(\alpha x)}{\pi^{hn/e}} = \sum_{i=0}^n \frac{\varphi_i \alpha^i}{\pi^{hn/e}} x^i \equiv \sum_{j=0}^{n/e} \frac{\varphi_{je} \alpha^{je} x^{je}}{\pi^{hn/e}} \pmod{\pi_{\mathbf{L}} \mathcal{O}_{\mathbf{L}}[x]}.$$

The congruence holds, because the x -coordinate of points with integer coordinates on the Newton polygon of $\varphi(x)$ is a multiple of e . For $\gamma = \alpha^e/\pi^h$ we have $\nu(\gamma) = \nu(\alpha^e/\pi^h) = 0$. Substituting $\gamma \pi^h$ for α^e yields

$$\frac{\varphi(\alpha x)}{\pi^{hn/e}} \equiv \sum_{j=0}^{n/e} \frac{\varphi_{je} \pi^{jh} (\gamma x^e)^j}{\pi^{hn/e}} \pmod{\pi_{\mathbf{L}} \mathcal{O}_{\mathbf{L}}[x]}.$$

If we replace γx^e by y we obtain the *associated polynomial* of $\varphi(x)$:

$$A(y) = \sum_{j=0}^{n/e} \varphi_{je} \pi^{h(j-n/e)} y^j \in \mathcal{O}_K[y],$$

which was introduced by Ore [Ore28, MN92]. As $x = 1$ is a root of $\varphi(\alpha x)/\pi^{hn/e}$, one of the roots of $A(y)$ in \mathbf{L} is γ .

Assume that $\gcd(e, p) = 1$ and that $A(y)$ is square free over \mathbf{K} . Let \mathbf{M}/\mathbf{K} be the minimal unramified extension over which $A(y)$ splits into linear factors, say $A(y) = (y - \gamma_1) \cdots (y - \gamma_{n/e})$ over \mathbf{M} . Let $\mathbf{N} = \mathbf{M}(\alpha, \zeta_e)$ where α is a root of $\varphi(x)$ and ζ_e an e -th root of unity. The field \mathbf{N} is the splitting field of $\varphi(x)$, if $\varphi(x)$ or equivalently $\frac{\varphi(\alpha x)}{\pi^{hn/e}}$, splits into linear factors over \mathbf{N} . We obtain

$$\frac{\varphi(\alpha x)}{(\gamma \pi^h)^{n/e}} \equiv \left(x^e - \frac{\gamma_1}{\gamma}\right) \cdots \left(x^e - \frac{\gamma_{n/e}}{\gamma}\right) \pmod{\pi_{\mathbf{N}} \mathcal{O}_{\mathbf{N}}[x]},$$

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

Over \mathbf{M} the polynomial $\varphi(x)$ splits into irreducible factors $\theta_i(x) = \sum_{j=0}^e \theta_{i,j} x^j$ ($1 \leq i \leq n/e$) where $\theta_{i,0} \equiv \gamma_i \pi^h \pmod{(\pi^{h+1})}$. By Proposition 2.1 the extensions generated by the $\theta_i(x)$ are isomorphic to the extensions generated by the polynomials $x^e + (\gamma_i \pi^h)^b \pi^{ae} = x^e + \gamma_i \pi$ with $ae + bh = 1$. We have proved:

Lemma 2.4. *Assume the Newton polygon of $\varphi(x) = \sum_{i=0}^n \varphi_i x^i \in \mathcal{O}_K[x]$ consists of one segment of slope $-h/e$ with $\gcd(h, e) = 1$ and $\gcd(e, p) = 1$ and the associated polynomial $A(y) = \sum_{j=0}^{n/e} \varphi_{je} \pi^{h(j-n/e)} y^j$ of $\varphi(x)$ is square free over \mathbf{K} . Then the splitting field of $\varphi(x)$ is a tamely ramified extension of degree e over the unramified extension of degree $f = \text{lcm}(f_0, f_1)$ with $f_0 = [\mathbf{K}(\zeta_e) : \mathbf{K}]$ and*

$f_1 = \text{lcm}(\deg a_1, \dots, \deg a_t)$, where $a_1(y), \dots, a_t(y)$ are the irreducible factors of $A(y)$ over \mathbb{K} . The ramified part of the extension can be generated by $x^e + \gamma\pi$, where γ is a root of $A(y)$.

3. EISENSTEIN POLYNOMIALS OF WILD DEGREE

In order to determine the Galois group of an Eisenstein polynomial $\varphi(x)$ of wild degree we look at its splitting field. We obtain the inertia degree and ramification index of the splitting field from the ramification polynomial of $\varphi(x)$ and the associated polynomial of the ramification polynomial.

Splitting Fields. Let $\varphi(x) = \sum_{i=0}^n \varphi_i x^i \in \mathcal{O}_{\mathbb{K}}[x]$ be an Eisenstein polynomial and let $\alpha \in \overline{\mathbb{K}}$ be a root of $\varphi(x)$. The valuation of all roots of $\varphi(x)$ is $1/n = \nu(\alpha)$. We consider

$$\psi(x) := \varphi(\alpha x + \alpha) = \sum_{i=0}^n \varphi_i (\alpha x + \alpha)^i = \sum_{i=0}^n \varphi_i \sum_{j=0}^i \binom{i}{j} \alpha^{i-j} (\alpha x)^j = \sum_{j=0}^n \sum_{i=j}^n \binom{i}{j} \varphi_i \alpha^i x^j.$$

As 0 is a root of $\psi(x) = \varphi(\alpha x + \alpha)$ the polynomial $\psi(x)$ is divisible by x . We set

$$\rho(x) := \frac{\psi(x)}{\alpha^n x} = \prod_{i=2}^n \left(x - \frac{\alpha^{(i)} - \alpha}{\alpha} \right),$$

where $\alpha = \alpha^{(1)}, \dots, \alpha^{(n)}$ are the roots of $\varphi(x)$. This reduces finding the splitting field of $\varphi(x)$ of degree n over \mathbb{K} to finding the splitting field of $\rho(x)$ of degree $n-1$ over $\mathbb{K}(\alpha)$. Let $\rho(x) = \sum_{j=0}^{n-1} \rho_j x^j$ then $\rho_{n-1} = 1$ and $\rho_{j-1} = \sum_{i=j}^n \binom{i}{j} \varphi_i \alpha^{i-n}$ for $1 \leq j \leq n-1$. The polynomial $\rho(x)$ is called the *ramification polynomial* of $\varphi(x)$ and its Newton polygon the *ramification polygon* of $\varphi(x)$ (also see [Sch03]).

Lemma 3.1. *Let $\varphi(x)$ be an Eisenstein polynomial and α a root of $\varphi(x)$. If $\psi(x) = \sum_{i=0}^n \psi_i x^i = \varphi(\alpha x + \alpha)$, then $\nu(\psi_i) \geq \nu(\psi_{p^s})$ for $p^s \leq i < p^{s+1}$.*

Proof. For $p^s \leq j < p^{s+1}$ and $i \geq j$ we have $\nu \binom{i}{j} \geq \nu \binom{i}{p^s}$. The result follows with $\psi_j = \sum_{i=j}^n \binom{i}{j} \varphi_i \alpha^i$. \square

If we want to draw the ramification polygon it suffices by Lemma 3.1 to consider the coefficients ρ_{p^s-1} for $0 \leq s \leq \nu_p(n)$ and the coefficient ρ_{n-1} . Hence the ramification polygon is the lower convex hull of the set

$$\left\{ (p^s - 1, \min_{p^s \leq i \leq n} \{ \nu_\alpha \binom{i}{p^s} + \nu_\alpha(\varphi_i) + i - n \}) \mid 0 \leq s \leq \nu_p(n) \right\} \cup \{ (n-1, 0) \}.$$

Assume that the Newton polygon of $\rho(x)$ is a straight line. It follows from Lemma 3.1 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 $n = p^m$. We use Lemma 2.4 to find the splitting field of $\rho(x)$. If $-h/e$ with $\gcd(h, e) = 1$ is the slope of the Newton polygon of $\rho(x)$, the associated polynomial of $\rho(x)$ is

$$A(y) = \sum_{j=0}^{(n-1)/e} A_j y^j = \sum_{j=0}^{(n-1)/e} \rho_{je} \alpha^{h(j-(n-1)/e)} y^j.$$

By construction $A_0 \neq 0$. We consider the polynomial $B(x) = \sum_{i=0}^n B_i x^i = xA(x^e)$. It follows from Lemma 3.1 that if $B_i \neq 0$ then $i = p^s$ for some $s \in \{0, \dots, m\}$. Therefore $B'(x) = B_1 = A_0$ and $\gcd(B(x), B'(x)) = 1$. Thus $B(x)$ is square free, which implies that $A(x)$ is square free. Lemma 2.4 yields the splitting field of $\rho(x)$ over $\mathbb{K}(\alpha)$, this field is the splitting field of $\varphi(x)$ over \mathbb{K} .

We summarize the result in the following Proposition:

Proposition 3.2. *Let $\varphi(x) \in \mathcal{O}_K[x]$ be an Eisenstein polynomial of degree p^m . If the Newton polygon of the ramification polynomial $\rho(x)$ consists of one segment with slope $-h/e$ where $\gcd(h, e) = 1$ then the splitting field of $\varphi(x)$ is a totally ramified extension of degree p^m over a tamely ramified extension whose inertia degree and ramification index can be obtained from $\rho(x)$ with Lemma 2.4.*

Remark 3.3. If α is a root of an Eisenstein polynomial $\varphi(x)$ whose ramification polygon is a line, then the discriminant $d_{L/K}$ of $L = K(\alpha)$ and the slope of the ramification polygon of $\varphi(x)$ are directly related. Let $-\frac{h}{e}$ be the slope of the ramification polygon of $\varphi(x)$ and $\alpha = \alpha^{(1)}, \dots, \alpha^{(p^m)}$ the roots of $\varphi(x)$. We have

$$\begin{aligned} \nu(d_{L/K}) &= \nu(d_\varphi) = \nu(N_{L/K}(\varphi'(\alpha))) = \nu_\alpha(\varphi'(\alpha)) = \nu_\alpha\left(\prod_{i=2}^{p^m}(\alpha^{(i)} - \alpha)\right) \\ &= \sum_{i=2}^{p^m} \left(\nu_\alpha\left(\frac{\alpha^{(i)} - \alpha}{\alpha}\right) + 1 \right) = (p^m - 1) \left(\frac{h}{e} + 1 \right). \end{aligned}$$

Galois groups. We determine the structure of the Galois group of an Eisenstein polynomial $\varphi(x)$ of degree p^m whose ramification polygon consists of one segment of arbitrary slope.

Denote by N the splitting field of $\varphi(x)$, by L the subfield generated by a root of $\varphi(x)$, and by K_1 the maximal tamely ramified subfield of N/K with $[K_1 : K] = ef$ (see Lemma 2.4). Set $G = \text{Gal}(\varphi) = \text{Gal}(N/K)$, $H = \text{Gal}(N/L)$, and let $G_1 \trianglelefteq G$ be the first ramification subgroup of N/K . Then $G = G_1 \rtimes H$ holds, as L and K_1 satisfy the conditions $L \cap K_1 = K$ and $LK_1 = N$. 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 $G \geq G_0 \geq G_1 \geq \dots$ of G .

Lemma 3.4. *Let $\varphi(x)$ be an Eisenstein polynomial over K of degree p^m whose ramification polygon consists of one segment of slope $-h/e$, where $\gcd(h, e) = 1$. The ramification filtration of $G = \text{Gal}(\varphi)$ is*

$$G \geq G_0 \geq G_1 = G_2 = \dots = G_h > G_{h+1} = 1.$$

The group G_1 is isomorphic to the additive group of \mathbb{F}_{p^m} .

Proof. The Newton polygon of the polynomial $\varphi(x)$ over K consists of one segment with slope $-1/p^m$. Therefore the Newton polygon over K_1 consists of one segment with slope $-e/p^m$ and we get, that $\varphi(x)$ is irreducible over K_1 because of $\gcd(e, p^m) = 1$. This yields $N = K_1(\alpha)$, where α is a root of $\varphi(x)$. Hence we have to show the equality $\nu_N(\alpha^g - \alpha) = h + 1$ for all $g \in G_1$. Recall, that $\nu_N\left(\frac{\alpha^g - \alpha}{\alpha}\right) = e \cdot \frac{h}{e} = h$ holds, as $\frac{\alpha^g - \alpha}{\alpha}$ is a root of the ramification polynomial $\rho(x)$ of $\varphi(x)$. We obtain

$$\nu_N(\alpha^g - \alpha) = \nu_N\left(\frac{\alpha^g - \alpha}{\alpha}\right) + \nu_N(\alpha) = h + 1$$

as desired.

As the quotients G_i/G_{i+1} for $i \geq 1$ embed into the additive Group of the residue class field of N (see [Ser63, chapter IV]), the second statement follows from $G_1 = G_h = G_h/G_{h+1}$. \square

Remark 3.5. Lemma 3.4 together with the formula for the different of a normal extension (see [Ser63, chapter IV]) yields the discriminant $d_{N/K}$ of the splitting field N of $\varphi(x)$:

$$\nu(d_{N/K}) = f \cdot (ep^m - 1 + h \cdot (p^m - 1)),$$

where f is the inertia degree of \mathbb{N}/\mathbb{K} .

The next theorem specifies the action of H on G_1 and describes the Galois group G as a subgroup of the affine group $\text{AGL}(m, p)$. We denote by $\wp = (\pi_{\mathbb{N}})$ the maximal ideal of the valuation ring $\mathcal{O}_{\mathbb{N}}$. 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 \mathbb{N} . Furthermore,

$$\Theta_i : G_i/G_{i+1} \rightarrow \wp^i/\wp^{i+1} : g \mapsto \left(\frac{\pi_{\mathbb{N}}^g}{\pi_{\mathbb{N}}} - 1 \right) \pmod{\wp^{i+1}}$$

embeds each quotient G_i/G_{i+1} into \wp^i/\wp^{i+1} (see again [Ser63, chapter IV]).

Theorem 3.6. *Let $\varphi(x) \in \mathcal{O}_{\mathbb{K}}[x]$ be an Eisenstein polynomial of degree p^m , whose ramification polygon consists of one single segment of slope $-\frac{h}{e}$ where $\gcd(h, e) = 1$. Then $\text{Gal}(\varphi) = G_1 \rtimes H$, 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 3.2). Moreover, $\text{Gal}(\varphi)$ is isomorphic to the group*

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

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 shown, that $\text{Gal}(\varphi) = G_1 \rtimes H$. If $\tilde{G}_1 = \{s_v : x \mapsto x+v \mid v \in (\mathbb{F}_p)^m\}$ and $\tilde{H} = \{u_a : x \mapsto xa \mid a \in H'\}$ then $\tilde{G} = \tilde{G}_1 \rtimes \tilde{H}$, where the action of \tilde{H} on \tilde{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 $\tilde{G}_1 \cong G_1 = G_h/G_{h+1}$ by Lemma 3.4.

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

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

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 $\pi_{\mathbb{N}}^g = \pi_{\mathbb{N}}(1 + \delta)$ with $\delta \in \wp^h$. Then $\Theta_h(g)^b = \delta^b \pmod{\wp^{h+1}}$. For computing $\Theta_h(g^b) = \left(\frac{\pi_{\mathbb{N}}^{g^b}}{\pi_{\mathbb{N}}} - 1 \right) \pmod{\wp^{h+1}}$, set $\pi_{\mathbb{N}}^{b^{-1}} = \pi_{\mathbb{N}}\varepsilon$ with $\varepsilon \in \mathcal{O}_{\mathbb{N}}^\times$ and

consider $\pi_{\mathbb{N}}^{g^b} = \pi_{\mathbb{N}}^{b^{-1}gb} = (\pi_{\mathbb{N}}\varepsilon)^{gb} = (\pi_{\mathbb{N}}^g\varepsilon^g)^b$. This is modulo \wp^{h+1} congruent to $(\pi_{\mathbb{N}}^g\varepsilon)^b = (\pi_{\mathbb{N}}(1 + \delta)\varepsilon)^b = (\pi_{\mathbb{N}}\varepsilon)^b(1 + \delta)^b = \pi_{\mathbb{N}}(1 + \delta^b)$ 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 $\text{GL}(m, p)$, which describes the action of H on $\Theta_h(G_1)$. Then $H \cong H' \cong \tilde{H}$ and thus $\text{Gal}(\varphi) \cong \tilde{G}$. \square

In order to obtain an explicit description of the group \tilde{G} for a given polynomial, it remains to determine the matrix group H' . We can read-off the action of H on \wp^h/\wp^{h+1} from the generating automorphisms of the tame Galois group H (Theorem 2.3). Hence we have a representation of H of dimension \tilde{f} over \mathbb{F}_p , where \tilde{f} denotes the inertia degree of the ground field \mathbb{K} . Now, we have to find the submodule $\Theta_h(G_1)$ of dimension m of the corresponding H -module to get the group H' . This can be realized with the ‘‘Meataxe’’-algorithm, which is implemented in the computer algebra systems Magma [BC95] and GAP [Gap05].

4. 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 $L = K(\alpha)$ the field generated by a root α of the respective polynomial. In the first two examples ζ is a primitive 8-th root of unity.

Example 4.1. 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. The associated polynomial of the ramification polynomial $\rho(x) \in L[x]$ is congruent to $x^2 + 1$ in $\underline{L}[x]$. Because ζ^2 is a root of $x^2 + 1$, Lemma 2.4 gives us $N = L(\zeta, \sqrt[4]{\zeta^2\alpha})$ as the splitting field of $\rho(x)$ over L , which is also the splitting field of $\varphi(x)$ over \mathbb{Q}_3 (see Proposition 3.2). Set $\pi_N = \sqrt[4]{\zeta^2\alpha}$. By Theorem 2.3 (with $e = 4, f = 2$ and $r = 2$) the group $H = \text{Gal}(N/L)$ is generated by the automorphisms

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

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

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

Example 4.2. 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 $\underline{L}[x]$. As $x^2 + 2$ splits into linear factors over $\underline{L} \cong \mathbb{F}_3$, 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 $N = L(\zeta, \sqrt[4]{\alpha})$ (see Lemma 2.4 and Proposition 3.2). By Theorem 2.3 (with $e = 4, f = 2$ and $r = 0$) the group $H = \text{Gal}(N/L)$ 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 $\text{Gal}(\varphi)$ is isomorphic to

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

Example 4.3. Let $\varphi(x) = x^{81} + 3x^{80} + 3x^{70} + 3x^{60} + \dots + 3x^{10} + 3 \in \mathbb{Q}_3[x]$. 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 $\rho(x) \in \mathbb{L}[x]$ is congruent to $x^{10} + 2 = (x+1)(x+2)(x^4 + \dots)(x^4 + \dots)$ in $\mathbb{L}[x]$. Let ζ be a $(3^4 - 1)$ -th root of unity. Because $\zeta^0 = 1$ is a root of $x^{10} + 2$, Lemma 2.4 gives us $\mathbb{N} = \mathbb{L}(\zeta, \sqrt[8]{\alpha})$ as the splitting field of $\rho(x)$ over \mathbb{L} , which is also the splitting field of $\varphi(x)$ over \mathbb{Q}_3 (see Proposition 3.2). By Theorem 2.3 (with $e = 8, f = 4$ and $r = 0$) the group $H = \text{Gal}(\mathbb{N}/\mathbb{L})$ is generated by the automorphisms

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

With a basis corresponding to $1, \zeta, \zeta^2, \zeta^3$ of $\wp/\wp^2 \cong (\mathbb{F}_3^4, +)$, we obtain

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

which represent the action of s and t on G_1 . Hence the Galois group of $\varphi(x)$ is isomorphic to the group

$$\begin{aligned} G &= \{t_{a,v} : (\mathbb{F}_3)^4 \rightarrow (\mathbb{F}_3)^4 : x \mapsto xa + v \mid a \in \langle S, T \rangle, v \in (\mathbb{F}_3)^4\} \\ &\cong C_3^4 \rtimes (C_8 \rtimes C_4). \end{aligned}$$

REFERENCES

- [BC95] W. Bosma and J. J. Cannon, *Handbook of Magma functions*, School of Mathematics, University of Sydney, Sydney, 1995.
- [Gap05] The GAP Group. *GAP - Groups, Algorithms and Programming*, Version 4.4. (2005), <http://www.gap-system.org>.
- [Has80] H. Hasse, *Number Theory*, Springer Verlag, Berlin, 1980.
- [JR04] J. Jones and D. Roberts, *Nonic 3-adic Fields*, in ANTS VI, Springer Lecture Notes in Computer Science, 3076, 293-308 (2004).
- [JR06] J. Jones and D. Roberts, *A Database of Local Fields*, J. Symbolic Comput., **41**, 80-97 (2006), <http://math.asu.edu/~jj/localfields>.
- [JR08] J. Jones and D. Roberts, *Octic 2-adic Fields*, J. Number Theory., **128**, 1410-1429 (2008)
- [MN92] J. Montes and E. Nart, *On a Theorem of Ore*, J. Algebra, **146** (1992), 318-334.
- [Ore28] Ö. Ore, *Newtonsche Polynome in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84-117.
- [Rom00] D. S. Romano, *Galois groups of strongly Eisenstein polynomials*, Dissertation, UC Berkeley, 2000.
- [Rom07] D. S. Romano, *Ramification polygons and Galois groups of wildly ramified extensions*, Preprint, 2007.
- [Sch03] J. Scherk, *The Ramification Polygon for Curves over a Finite Field*, Canadian Mathematical Bulletin, **46** (2003), no. 1, 149-156.
- [Ser63] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1963.

E-mail address: greve@math.uni-duesseldorf.de

E-mail address: s_pauli@uncg.edu