Canad. Math. Bull. Vol. **46** (1), 2003 pp. 149–156

The Ramification Polygon for Curves over a Finite Field

John Scherk

Abstract. A Newton polygon is introduced for a ramified point of a Galois covering of curves over a finite field. It is shown to be determined by the sequence of higher ramification groups of the point. It gives a blowing up of the wildly ramified part which separates the branches of the curve. There is also a connection with local reciprocity.

1 Introduction

Let k be a finite field of characteristic p with q elements and let L/K be a totally ramified Galois extension of local fields over k with Galois group G. Denote by ν_L (respectively ν_K) their valuations. Let z (respectively y) be a local parameter for L (respectively K). Then z satisfies an Eisenstein equation

$$f(z) = z^e + \cdots + a_1 z + a_0 = 0 \tag{1}$$

where $a_i \in \mathcal{O}_K = k[[y]]$, $\nu_K(a_i) \geq 1$ for all i, $\nu_K(a_0) = 1$, $a_e = 1$, and $e = e_0 p^r$ with $(e_0, p) = 1$. G has a filtration

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset \cdots$$

given as follows: for $i \geq -1$,

$$\gamma \in G_i \iff \gamma z - z \equiv 0 \pmod{z^{i+1}}.$$

This note studies "Puiseux expansions" for γz, where $\gamma \in G_1$, *i.e.*, for the wildly ramified part of the extension. A neat way to do this is to use a Newton polygon, the ramification polygon. While writing this paper, the author discovered that a similar Newton polygon was introduced by Krasner in [2] for local extensions of number fields. He obtained results analogous to those in Section 2 in this case.

In Section 2 the ramification polygon is introduced and its basic properties derived. The polygon determines a blowing-up of $\mathbb{A}^2$. This is discussed in Section 3. In Section 4 a connection with local reciprocity is explained. This result holds in the number field case as well and seems to be unknown there.

Received by the editors March 21, 2001.
AMS subject classification: 11G20.

https://doi.org/10.4153/CMB-2003-015-9 Published online by Cambridge University Press

2 The Ramification Polygon

For $i \geq 1$, let
$$U_L^i = 1 + (z^i) \subset \mathcal{O}_L^*, \quad U_K^i = 1 + (y^i) \subset \mathcal{O}_K^*.$$
For $\gamma \in G_i$, $i \geq 1$, write
$$\gamma z = z + s_\gamma z, \quad s_\gamma \in (z^i).$$
Then we can define a homomorphism
$$t_i \colon G_i/G_{i+1} \longrightarrow U_L^i/U_L^{i+1} \cong (z^i)/(z^{i+1}) \cong k$$
by
$$t_i(\bar{\gamma}) = \overline{1 + s_\gamma},$$
which is injective. Under the identification with k, $\overline{1 + s_\gamma}$ corresponds to $\bar{s}_\gamma$, the leading coefficient of s_γ as a power series in z.

Now the local parameter y can be written as a power series in z. Regarding f then as a polynomial with coefficients in $\mathcal{O}_L$, set
$$g(x) = g(x, z) := f(zx + z) \in \mathcal{O}_L[x].$$
Notice that
$$g(0) = f(z) = 0.$$
If $\gamma \in G_1$, then s_γ is a root of g, and if $s \in L$ is a root of g, then $sz + z$ is a root of f.

The *ramification polygon* Δ of L/K is defined to be the Newton polygon of g: write
$$g(x) = \sum_{i=1}^{e} b_i x^i, \quad b_i \in \mathcal{O}_L,$$
and let
$$P_i = \big(i, \nu_L(b_i)\big), \quad i = 1, \ldots, e.$$
Then Δ is the boundary of the convex hull of
$$\bigcup_{i=1}^{e} (P_i + \mathbf{R}_+^2).$$
Corollary 1 shows that Δ does not in fact depend on the choice of f.

Now
$$b_i = \sum_{j=i}^{e} \binom{j}{i} a_j z^j.$$
Since $e | \nu_L(a_j)$, we have that
$$\nu_L(a_j z^j) \equiv j \pmod{e}, \quad j = i, \ldots, e$$
and thus they are all distinct. So
$$\nu_L(b_i) = \min_{i \leq j \leq e} \nu_L\left(\binom{j}{i} a_j z^j\right). \tag{2}$$

Lemma 1

(i) *For all i,* $\nu_L(b_i) \geq e$*;*
(ii) $\nu_L(b_e) = \nu_L(b_{p^r}) = e$*;*
(iii) $\nu_L(b_1) = \nu_L(\mathcal{D}) + 1$*, where* $\mathcal{D}$ *is the different of* L/K*;*
(iv) *for* $p^s < i < p^{s+1}$*,* $s < r$*,* $\nu_L(b_i) \geq \nu_L(b_{p^s})$*.*

Proof We have that

$$\nu_L\left(\binom{j}{i} a_j z^j\right) \geq e\nu_K(a_j) + j$$

for all j. Since $\nu_K(a_j) \geq 1$ for all $j < e$, (i) follows. Notice that

$$(zx + z)^e = z^e(x^{p^r} + 1)^{e_0} = z^e(x^e + \cdots + e_0 x^{p^r} + 1).$$

So (2) implies that

$$\nu_L(b_{p^r}) = e.$$

According to [3, III, §6, Cor. 2,],

$$\mathcal{D} = \left(f'(z)\right).$$

As

$$b_1 = zf'(z),$$

this proves (iii). Lastly, suppose that $s < r$, $p^s < i < p^{s+1}$. Let ν_p denote the p-adic valuation. Then, as is well known,

$$\nu_p\binom{j}{i} \geq \nu_p\binom{j}{p^s}$$

for all $j \geq i$. In particular, if $\binom{j}{p^s} \equiv 0 \pmod{p}$, then $\binom{j}{i} \equiv 0 \pmod{p}$. Therefore by (2)

$$\nu_L(b_i) \geq \nu_L(b_{p^s}).$$ ■

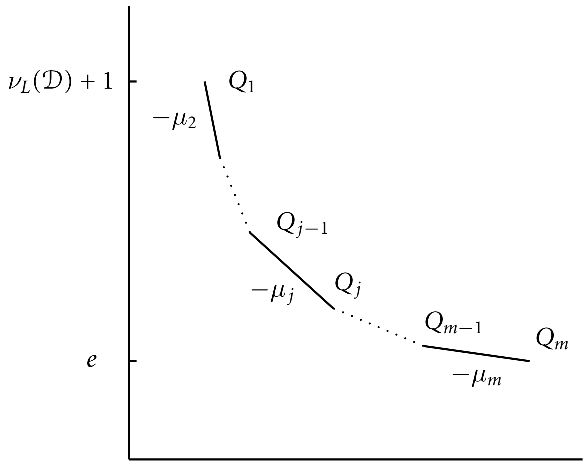
Thus P_i lies on Δ only if $i = p^s$ for some s. So let $Q_i = P_{p^{s_i}}$, $i = 1, \ldots, m$ be the vertices of Δ, where $0 = s_1 < \cdots < s_m = p^r$. Set $\nu_i = \nu_L(b_{p^{s_i}})$. Let $L_i = \overline{Q_{i-1}Q_i}$, $1 < i \leq m$ be the edges, and let $-\mu_i \in \mathbb{Q}$ be the slope of L_i.

Theorem 1 *The slopes* $-\mu_j$ *of the edges* $L_j = \overline{Q_{j-1}Q_j}$*,* $1 < j \leq m$*, are integral. The jumps in the sequence of higher ramification groups* $G_0 \supseteq G_1 \supseteq \cdots$ *are* $\mu_m < \cdots < \mu_2$*. The orders of the groups are* $|G_{\mu_j}| = p^{s_j}$*,* $1 < j \leq m$*.*

Proof We show that g has $p^{s_j} - p^{s_{j-1}}$ roots of order μ_j. Let $\bar{b}_i \in k$ be the coefficient of the lowest order term of $b_i \in \mathcal{O}_L = k[[z]]$. Now

$$\begin{aligned} g(z^{\mu_j}x) &= \sum_i b_i (z^{\mu_j}x)^i \\ &= \sum_i \bar{b}_i z^{\nu_L(b_i) + i\mu_j} x^i + \text{higher order terms.} \end{aligned}$$

https://doi.org/10.4153/CMB-2003-015-9 Published online by Cambridge University Press



The equation of L_j is

$$\eta + \mu_j \xi - (\nu_j + \mu_j p^{s_j}) = 0.$$

Since Δ is convex,

$$\nu_L(b_i) + \mu_j i - (\nu_j + \mu_j p^{s_j}) > 0$$

for all P_i not on L_j. Therefore

$$g(z^{\mu_j} x) \equiv z^{\nu_j + \mu_j p^{s_j}} \sum_{P_{p^s} \text{ on } L_j} \bar{b}_{p^s} x^{p^s} \pmod{z^{\nu_j + \mu_j p^{s_j} + 1}}. \tag{3}$$

So let

$$h_j(x) = \sum_{P_{p^s} \text{ on } L_j} \bar{b}_{p^s} x^{p^s} \in k[x].$$

This is an additive polynomial. Its degree is p^{s_j} and the lowest order term has degree $p^{s_{j-1}}$. Therefore the number of non-zero roots of h_j in $\bar{k}$ is $p^{s_j} - p^{s_{j-1}}$. A non-zero root $\bar{s}$ of h_j in k determines a root s of g in $\mathcal{O}_L$ of order μ_j and vice versa. Since g has e roots in $\mathcal{O}_L$, all the roots of h_j must lie in k and μ_j must be an integer. This also tells us that the sequence

$$0 \longrightarrow G_{\mu_j}/G_{\mu_j+1} \xrightarrow{t_{\mu_j}} U_L^{\mu_j}/U_L^{\mu_j+1} \cong k \xrightarrow{h_j} k \tag{4}$$

is exact. Therefore

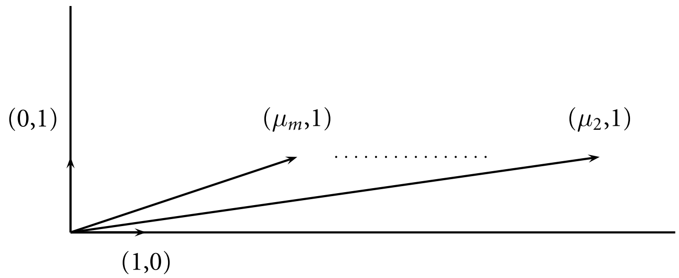
$$|G_{\mu_j}/G_{\mu_j+1}| = p^{s_j} - p^{s_{j-1}},$$

and

$$|G_{\mu_j}| = \sum_{i=2}^{j} (p^{s_i} - p^{s_{i-1}}) + 1 = p^{s_j}.$$

To see that $\mu_2, \dots, \mu_m$ are precisely the jumps in the sequence of ramification groups, let s be a root of g of order μ. Suppose μ is not one of $\mu_2, \dots, \mu_m$. Since Δ is

https://doi.org/10.4153/CMB-2003-015-9 Published online by Cambridge University Press



convex there will be a line with slope $-\mu$ which meets it at a single vertex, say Q_j, for some j, $1 \le j \le m$. And the rest of Δ will lie on one side of this line. Now expand $g(z^\mu x)$ as in (3):

$$g(z^\mu x) \equiv z^{\nu_j+\mu p^{s_j}} \bar{b}_{p^{s_j}} x^{p^{s_j}} \pmod{z^{\nu_j+\mu p^{s_j}+1}}.$$

But writing $s = z^\mu \tilde{s}$, with $\tilde{s} \in \mathcal{O}_L$, $\tilde{s}(0) \ne 0$, we have

$$0 = g(s) = g(z^\mu \tilde{s}) \equiv z^{\nu_j+\mu p^{s_j}} \bar{b}_{p^{s_j}} \tilde{s}^{p^{s_j}},$$

which is impossible since $\bar{b}_{p^{s_j}} \ne 0$. Therefore $\mu_2, \dots, \mu_m$ are the jumps. ■

Corollary 1 *The ramification polygon is independent of the choice of Eisenstein polynomial f.*

Proof The sequence of jumps and the orders of the ramification groups determine the numbers $\mu_2, \dots, \mu_m, p^{s_1}, \dots, p^{s_m}$ which in turn determine Δ. ■

3 Blowing Up

Equation (3) can be interpreted as a "blowing up" of the curve $g(x, z) = 0$, which separates the branches γz, $\gamma \in G_1$. The fan Σ associated with Δ [1, Section 8.2] consists of the cones generated by $\{(0, 1), (\mu_m, 1)\}$, $\{(\mu_{j+1}, 1), (\mu_j, 1)\}$ for $1 < j < m$ and $\{(\mu_2, 1), (1, 0)\}$.

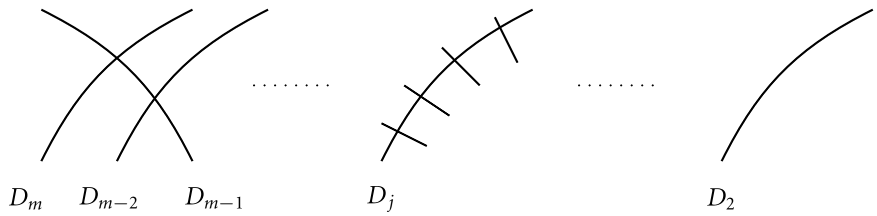
This fan defines a variety $X(\Sigma)$ over k and a proper map $\phi\colon X(\Sigma) \to \mathbb{A}^2$. Let Σ' be the fan consisting of the cones generated by $\{(\mu, 1), (\mu + 1, 1)\}$ for $0 \le \mu < \mu_2$ and $\{(\mu_2, 1), (1, 0)\}$. Then Σ' is a simple fan subordinate to Σ, and $X' := X(\Sigma')$ is smooth.

For each j, $1 < j \le m$, let Π_j be the cone spanned by $\{(\mu_j, 1), (1, 0)\}$. We have the canonical map

$$\phi_j\colon X(\Pi_j) \cong \mathbb{A}^2 \longrightarrow \mathbb{A}^2$$

defined by $\phi_j(x, y) = (xy^{\mu_j}, y)$. Then $\phi_j^* g$ is given by (3). Let D_j denote the exceptional curve $\{y = 0\}$ in $X(\Pi_j)$. Equation (3) can be interpreted geometrically as follows. Under the blow-up ϕ_j precisely the components of $g^{-1}(0)$ of order μ_j meet D_j. Their points of intersection are given by the roots of h_j.

https://doi.org/10.4153/CMB-2003-015-9 Published online by Cambridge University Press



Let Σ_j be the fan consisting of the cones generated by $\{(\mu_{i+1}, 1), (\mu_i, 1)\}$ for $1 < i < j$ and $\{(\mu_2, 1), (1, 0)\}$. Then $X(\Sigma_j)$ is an open subvariety of $X(\Sigma)$, and also a blow-up of $X(\Pi_j)$:

$$\begin{tikzcd} & X(\Sigma') \arrow[d] \\ X(\Sigma_j) \arrow[r] \arrow[d] & X(\Sigma) \\ X(\Pi_j) & \end{tikzcd}$$

In $X(\Sigma_j)$, the proper pre-image of D_j (also denoted by D_j) lies in the chart corresponding to the cone generated by $\{(\mu_j, 1), (\mu_{j-1}, 1)\}$. The components of the exceptional divisor of $\phi\colon X(\Sigma) \to \mathbb{A}^2$ are then the curves $D_2, \dots, D_m$. In the exceptional divisor of $X(\Sigma')$ there are $\mu_j - \mu_{j+1} - 1$ rational curves interpolated between D_{j+1} and D_j.

4 Local Reciprocity

In this section we point out how the polynomials h_j are connected with local reciprocity. Assume that G is abelian. The local reciprocity map

$$w\colon K^*/NL^* \longrightarrow G$$

respects the natural filtrations on both sides and induces maps w_i on the quotients. We first recall the description of these maps given in [3].

Let φ denote the Herbrand function, and ψ its inverse. Then if $N\colon L^* \to K^*$ is the norm, we have

$$N(U_L^{\psi(i)}) \subset U_K^i, \quad N(U_L^{\psi(i)+1}) \subset U_K^{i+1}$$

[3, V, Prop. 8]. Furthermore, the induced map

$$k \cong U_L^{\psi(i)}/U_L^{\psi(i)+1} \xrightarrow{N_i} U_K^i/U_K^{i+1} \cong k \tag{5}$$

is an additive polynomial of degree $|G_{\psi(i)}|$, and the sequence

$$0 \longrightarrow G_{\psi(i)}/G_{\psi(i)+1} \xrightarrow{t_{\psi(i)}} U_L^{\psi(i)}/U_L^{\psi(i)+1} \xrightarrow{N_i} U_K^i/U_K^{i+1}$$

https://doi.org/10.4153/CMB-2003-015-9 Published online by Cambridge University Press

is exact [3, V, Prop. 9].

Now there belongs to this sequence a "coboundary map"

$$\delta_i\colon\ \operatorname{coker} N_i \cong U_K^i/U_K^{i+1}NU_L^{\psi(i)} \longrightarrow G_{\psi(i)}/G_{\psi(i)+1}.$$

It is constructed as follows, keeping in mind the identifications in (5) (*cf.* [3, XV, Section 1]): take $a \in k \cong U_K^i/U_K^{i+1}$ and let $b \in \bar{k}$ be a solution of

$$N_i(b) = a.$$

Set

$$c = Fb - b,$$

where F is the Frobenius homomorphism. Then $c \in \ker N_i \subset k$ and c does not depend on the choice of b. This determines a well-defined homomorphism

$$U_K^i/U_K^{i+1}NU_L^{\psi(i)} \longrightarrow \ker N_i.$$

So define

$$\delta_i(a) := t_{\psi(i)}(c^{-1}) \in G_{\psi(i)}/G_{\psi(i)+1}.$$

On the other hand, the local reciprocity map w also respects the filtrations:

$$w(U_K^i/NU_L^{\psi(i)}) \subset G_{\psi(i)},$$

and induces isomorphisms

$$w_i\colon U_K^i/U_K^{i+1}NU_L^{\psi(i)} \longrightarrow G_{\psi(i)}/G_{\psi(i)+1}.$$

Serre [3, XV, Prop. 4] proves that

$$w_i(a) = \delta_i(a^{-1}), \quad a \in U_K^i/U_K^{i+1}NU_L^{\psi(i)}.$$

Since δ_i is determined by N_i, it is therefore of interest to know more about these additive polynomials. The quotients $G_{\psi(i)}/G_{\psi(i)+1}$ are trivial unless $\psi(i) = \mu_j$ for some j, or equivalently, $i = \varphi(\mu_j)$.

Theorem 2 *For $j \geq 2$, $N_{\varphi(\mu_j)}$ and h_j coincide up to a constant.*

Proof The polynomial h_j is an additive polynomial of degree $|G_{\mu_j}|$. Its kernel is $\operatorname{im} t_{\mu_j}$ (*cf.* (4)). Set $i = \varphi(\mu_j)$ so that $\mu_j = \psi(i)$. Then the degree of N_i is also $|G_{\mu_j}|$ and its kernel is $\operatorname{im} t_{\mu_j}$ too. Therefore N_i and h_j coincide up to a constant (*cf.* [3, V, Section 5]). ■

Remark 1 The isomorphisms

$$U_L^i/U_L^{i+1} \cong k, \quad U_K^i/U_K^{i+1} \cong k$$

depend on the choice of z, respectively y. Choosing an Eisenstein polynomial f is equivalent to fixing z. The norm map N_i regarded as an additive polynomial then still depends on the choice of y. Varying y multiplies N_i by a constant.

https://doi.org/10.4153/CMB-2003-015-9 Published online by Cambridge University Press

References

[1] V. I. Arnold, S. M. Gusein-Zade and A. N. Varchenko, *Singularities of Differentiable Maps.* Vol. II, Birkhäuser, 1988.
[2] M. Krasner, *Sur la primitivité des corps $\wp$-adiques.* Mathematica, Cluj, **13**(1937), 72–191.
[3] J. P. Serre, *Local fields.* Springer-Verlag, 1979.

Department of Mathematics
University of Toronto
100 St. George Street
Toronto, Ontario
M5S 3G3
email: scherk@math.toronto.edu