Higher Ramification Groups

Dean Bisogno

May 24, 2016

1 ABSTRACT

Studying higher ramification groups immediately depends on some key ideas from valuation theory. With that in mind, this paper will outline the essential results from valuation theory before proceeding to higher ramification groups. Higher ramification groups arise when studying extensions of fraction fields of Dedekind rings. Ramification groups are also useful when studying wildly ramified extensions of function fields. The goal while studying ramification in a wildly ramified extension of function fields is to calculate the exponent of the different. By Hilbert’s different theorem, the exponent of the different can be calculated by finding orders of higher ramification groups and ramification jumps. Higher ramification groups can also be used to study the subgroup structure of a Galois group, as the higher ramification group filtration can contain information about Sylow p-subgroups. The aim of this paper is to understand at a general level what higher ramification groups are, and investigate a couple examples of their applications.

2 PRELIMINARIES

2.1 VALUATIONS

Though valuations need not be discrete, many results discussed in this paper either require discrete valuations or are most easily understood with respect to a discrete valuation. Thus discrete valuations will be the focus of this section.

Definition 1 (Discrete Valuation Ring (DVR)).
A discrete valuation ring is a principal ideal domain $O$ with a unique maximal ideal $p \neq 0$.

Example 1.
Consider the ring $\mathbb{Z}$ and prime $p \in \mathbb{Z}$. The localization $\mathbb{Z}_{(p)}$ is a local PID with unique maximal ideal $p\mathbb{Z}_{(p)}$. Then $\mathbb{Z}_{(p)}$ satisfies the definition of a discrete valuation ring.

Example 2.
Consider $k[[x]]$, the formal power series of the field $k$. It was shown in Dummit and Foote,
Definition 2 (Uniformizing Parameter).

Let \( p \) be the unique maximal ideal of DVR \( O \). Since \( O \) is a PID, there exists a prime \( \pi \) in \( O \) such that \( p = (\pi) \). Such a \( \pi \) is called a uniformizing parameter.

Theorem 7, section 16.2 in Dummit and Foote, 2004 shows that taking the \( n \)th multiplication by a unit and generates the unique maximal ideal of \( p \) that is principal. Thus \( k[[x]] \) is a DVR.

Definition 3 (Discrete Valuation).

The exponent \( n \) used above is the valuation of \( a \), denoted \( v_p(a) \), it is a function \( v_p : K^* \to \mathbb{Z} \) where \( K \) is the field of fractions of \( O \). The valuation \( v_p \) can be extended to \( K \) by setting \( v_p(0) = \infty \). Further \( v_p \) satisfies the following

I. \( v_p(ab) = v_p(a) + v_p(b) \).

II. \( v_p(a + b) \geq \min\{v_p(a), v_p(b)\} \).

All valuations can be classified as either archimedean or nonarchimedean. A valuation \( v \) is nonarchimedean if \( v(n) \) is bounded for every \( n \in \mathbb{N} \). Proposition 3.6 in Neukirch, 1999, is often incorporated in the definition of discrete valuations, as every discrete valuation is nonarchimedean.

Proposition 1.

A valuation \( v(x) \) is nonarchimedean if and only if it satisfies \( v(x + y) \leq \max(v(x), v(y)) \).

Proof. (\( \Rightarrow \)) The reverse direction is straightforward. Just notice

\[
v(n) = v(1 + \ldots + 1) \leq 1 \forall n \in \mathbb{N}.
\]

(\( \Leftarrow \)) Now, \( v(n) \leq N \) for all \( n \in \mathbb{N} \) for some \( N \in \mathbb{N} \). Then for arbitrary \( x, y \in K \), without loss of generality, consider \( v(x) \geq v(y) \). Choose \( l \geq 0 \), then \( v(x)^l v(y)^{n-l} \leq v(x) \). Now applying binomial formula yields

\[
v(x + y)^n \leq \sum_{l=0}^{n} v(l) v(x)^l v(y)^{n-l} \leq N(n + 1)(v(x))^n
\]

taking the \( n^{th} \) root of both sides yields

\[
v(x + y) \leq N^{\frac{1}{n}} (1 + n)^{\frac{1}{n}} v(x) = N^{\frac{1}{n}} (1 + n)^{\frac{1}{n}} \max(v(x), v(y))
\]

The result then follows if letting \( n \to \infty \). The conclusion is then for any discrete valuation (which is nonarchimedean) \( v(x + y) \leq \max(v(x), v(y)) \). 

...
The following proposition is particularly useful because it provides a correspondence between prime ideals and valuations in Dedekind rings.

**Proposition 2** (Neukirch, 1999).

Let $O$ be a noetherian integral domain. $O$ is a Dedekind domain if and only if, for all prime ideals $p \neq 0$, the localizations $O_p$ are discrete valuation rings.

When the previous proposition is applied to $\mathbb{Z}$ and the fraction field $\mathbb{Q}$ is considered, the following proposition is gained.

**Proposition 3** (Neukirch, 1999).

Every valuation of $\mathbb{Q}$ is equivalent to one of $v_p(x)$ (the nonarchimedean valuations) or $v_\infty(x)$ (the archimedean valuations).

Finally, since ramification occurs via extensions or covers, it will be useful to know how valuations extend.

**Definition 4** (Prolongation of a valuation).

If $A \subset B$ are rings with $B$ integral over $A$, $p$ a prime in $A$, and $q$ prime in $B$ dividing $p$ with ramification index $e_q$, then $v_q(x) = e_q v_p(x)$ is a prolongation of $v_p$ with index $e_q$ (Serre, 1995).

### 2.2 Field Completion

With a valuation $\nu$ on a field $K$ then for any real number $a \in (0, 1)$ an absolute value on $K$ can be defined by

$$||x|| = \begin{cases} a^{\nu(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

which satisfies the usual conditions of a metric as outlined by Serre, 1995, II.1. A topology is then induced on $K$ via the absolute value metric, and the completion of $K$ with respect to the valuation $\nu$ is denoted by $\hat{K}$. Note also that the metrics induced by different choices of $a$ are topologically equivalent, so the completion is dependent only on $\nu$. Further, $\nu$ extends in the completion of $K$ to a valuation (which will continue to be called $\nu$) on $\hat{K}$ (Serre, 1995).

The Galois group of $\hat{L}/\hat{K}$ relates to the decomposition group of $L/K$ in the following way.

**Proposition 4.**

For $L/K$ Galois with group $G$, $v_p(x)$ a valuation on $K$ and $\omega_q(x)$ a prolongation of $v_p$, let $\hat{L}, \hat{K}$ be the completions of $L$ and $K$ with respect to $\omega_q$ and $v_p$ respectively. If $D_q(L/K)$ is the decomposition group of $q$ over $p$, then $\hat{L}/\hat{K}$ is Galois with Galois group $D(L/K)$ (Serre, 1995).

**Proof.** This is corollary 4 to theorem 1 in Serre, 1995, II.3, which shows that $[\hat{L} : \hat{K}] = ef$. As proven in class $|D(L/K)| = ef$.

### 3 Higher Ramification Groups

Consider now $K$, the fraction field of a Dedekind ring $O_K$, with valuation $\nu$ and uniformizing parameter $\pi_K$. For Galois extension $L/K$ with Galois group $G$; prolongation of $\nu$, $\omega$, on $L$;
uniformizing parameter \( \pi_L \) of \( \omega \); and discrete valuation ring \( O_L \). The definitions of the higher ramification groups generalize the definition of the inertia group.

**Definition 5** (Higher Ramification Groups, Serre, 1995).
For every real number \( i \geq -1 \) define the \( i \)th ramification group of \( L/K \) with respect to \( \omega \) by

\[
G_i = G_i(L/K) = \{ \sigma \in G | \omega(\sigma(a) - a) \geq i + 1 \ \forall \ a \in O_L \}.
\]

Note that because \( v \) corresponds to a prime \( p \) and \( \omega \) corresponds to a prime \( q | p \), the ramification groups are generalizations of the decomposition and inertia groups. The following is a proposition which helps characterize the higher ramification groups with respect to the presentation of valuations above.

**Proposition 5.**
For any \( a \in O_L \) and \( \sigma \in G \), \( \omega(\sigma(a) - a) \geq i + 1 \) if and only if \( \sigma(a) \equiv a \mod (\pi_L)^{i+1} \).

**Proof.**

\((\Rightarrow)\)

\[ \nu_L(\sigma(a) - a) \geq i + 1 \implies \sigma(a) - a = \pi_L^i \frac{x}{y} \]

where \( t \geq i + 1 \) and \( x, y, \pi_L \in O_L \) all relatively prime. This follows from the definition of the valuation in the first section. The equation above then implies \( \sigma(a) - a \equiv 0 \mod (\pi_L)^{i+1} \).

\((\Leftarrow)\)

\[ \sigma(a) - a \equiv 0 \mod (\pi_L)^{i+1} \implies \sigma(a) - a = \pi_L^i \frac{x}{y} \]

with the same restrictions as above. It follows then that \( \nu_L(\sigma(a) - a) \geq i + 1 \).

The condition that \( \nu(\sigma(a) - a) \geq i + 1 \) clearly induces the following filtration on \( G \)

\[ \{G_i(L/K)\}_{i \geq -1} = G_{-1} \supsetneq G_0 \supsetneq G_1 \supsetneq \ldots \]

This filtration can be investigated further due to the fact that \( \forall i, G_i \triangleleft G \).

**Proof.** Consider \( \tau \in G \). By membership of \( G \), \( \omega(\tau(a) - a) \geq 0 \ \forall \ a \in O_L \), i.e. \( \tau((\pi_L)^{i+1}) = (\pi_L)^{i+1} \) for all \( i \). Thus there is an induced automorphism \( \tilde{\tau} \) of \( O_L/(\pi_L^{i+1}) \). Now consider \( \phi_{i+1} : G \to \text{aut}(O_L/(\pi_L^{i+1})) \) such that \( \phi_{i+1}(\tau) = \tilde{\tau} \). This is a group homomorphism with \( \ker(\phi_{i+1}) = G_i \), so \( G_i \triangleleft G \) for all \( i \).

The first two ramification groups, \( G_{-1} \) and \( G_0 \), are already familiar. For \( i = -1 \) from the definition it follows \( G_{-1} = \{ \sigma \in G | \omega(\sigma(a) - a) \geq 0 \ \forall \ a \in O_L \} \) which is the definition of the decomposition group \( D_{\pi_K}(L/K) \). If \( \pi_K \) is fully ramified in the extension then \( G_{-1} = G \). For \( i = 0, G_0 \) equals the inertia group \( I(L/K) \) by noticing that \( \phi_1 \) is the homomorphism used to originally define the inertia group.

Occasionally it is useful to denote the first index of the ramification group in which an element \( \sigma \in G \) ceases to appear.

---

4
Definition 6.
Let \( x \in O_L \) such that \( O_L = O_K[x] \). Such an element is assured to exist by Neukirch, 1999, II.10.4. Then for \( \sigma \in G \) define
\[
i_{L/K}(\sigma) = \omega(\sigma(x) - x).
\]
Noting the argument above which showed \( G_i \triangleleft G \), it follows \( \forall \sigma, \tau \in G, i_{L/K}(\tau^{-1}\sigma\tau) = i_{L/K}(\sigma) \).

Another simple conclusion which follows from the definition of \( i_{L/K} \) is \( i_{L/K}(\sigma) \geq i + 1 \) if and only if \( \sigma \in G_i \).

Consider now \( H \subset G \) a subgroup, and let \( K' \) be the fixed field of \( H \) so that \( H = \text{Gal}(L/K') \). The following relations follow from the above propositions.

Proposition 6.
For every \( \sigma \in H \), \( i_{L/K'}(\sigma) = i_{L/K}(\sigma) \), and \( H_i = G_i \cap H \) (Serre, 1995).

Proof. Let \( \phi_{i+1} : G \to \text{Aut}(O_L/(\pi_L)^{i+1}) \) and \( \psi_{i+1} : H \to \text{Aut}(O_L/(\pi_L)^{i+1}) \) such that \( \phi_{i+1}(\sigma) = \bar{\sigma} \) and \( \psi_{i+1} \) defined similarly. As shown above, \( G_i = \ker(\phi_{i+1}) \) and \( H_i = \ker(\psi_{i+1}) \). Thus the conclusions hold.

4 The Upper Numbering and Ramification Jump

There is a renumbering of the ramification groups which lends itself to other computations. The ordering used above is called the lower numbering while the renumbering introduced below is called the upper numbering. The upper numbering is useful when working with quotient group computations, while the lower numbering works best for subgroup computations (Neukirch, 1999).

Definition 7 (Upper Numbering of the Higher Ramification groups).
Consider the function
\[
t = \varphi(s) = \int_0^s \frac{dx}{[G_0 : G_x]}
\]
called the Herbrand function which has inverse map \( \psi \). Then for any real \( s \geq -1 \) let \( G_s = G_{[s]} \) and renumber the ramification groups by \( G^t(L/K) = G_s(L/K) \) where \( s = \psi(t) \).

As this new numbering allows for noninteger indices, the index at which the ramification group changes is given a name.

Definition 8 (Ramification Jump).
If \( G^t(L/K) \neq G^{t+\epsilon}(L/K) \) for any \( \epsilon \geq 0 \) then \( t \) is called a ramification jump.

These two concepts are important for the final theorem of this paper. Which assures that in certain circumstances, ramification groups only change at integer indexes.

Theorem 1 (Hasse-Arf).
For a finite abelian extension \( L/K \), the jumps of the filtration \( \{G^i(L/K)\}_{i \geq -1} \) are rational integers.
Serre gives a useful interpretation of the Hasse-Arf theorem, namely that if \( G_i \neq G_{i+1} \) then \( \phi(i) \) is an integer. This interpretation is helpful in the following example (Serre, 1995).

**Example 3.**

Suppose \( G \) is a cyclic group of order \( p^n \) where \( p \) is the characteristic of \( \bar{K} \). Let \( G(i) \) be the subgroup of \( G \) with order \( p^{n-i} \). Then there exist integers \( i_0, \ldots, i_{n-1} \) such that all ramification groups are identified as follows:

\[
G_0 = G_{i_0} = G = G^{i_0} = G^1 = G_{i_0}
\]

\[
G_{i_0+1} = \ldots = G_{i_0+pl_1} = G(1) = G^{i_0+1} = \ldots = G^{i_0+pl_1} = G^{i_1} = G_{i_0+pl_1}
\]

\[
G_{i_0+pl_1} = \ldots = G_{i_0+pl_1+p^2l_2} = G(2) = G^{i_0+pl_1+p^2l_2} = G^{i_1+p^2l_2} = G_{i_0+pl_1+p^2l_2}
\]

\[\vdots\]

\[
G_{i_0+pl_1+p^2l_2+\ldots+p^{n-1}l_{n-1}+1} = 1 = G^{i_0+pl_1+p^2l_2+\ldots+p^{n-1}l_{n-1}+1}.
\]

**Proof.** Because \( G = Gal(\bar{L}/\bar{K}) \) is cyclic with order \( p^n \), it follows that \( \bar{L}/\bar{K} \) is an extension of finite fields, i.e. \( L \cong \mathbb{F}_{p^n} \) and \( K \cong \mathbb{F}_p \). Further recall that \( G \) is generated by fröbenius \( \sigma \) (shown in Math 567). By Euler's totient there are \( (p-1)p^n \) elements in \( G \) with order relatively prime to \( p^n \), consequently since \( p^n - (p-1)p^{n-1} = p^{n-1} \), there are \( n-1 \) distinct proper subgroups of \( G \). This places \( n \) as an upper bound on the number of distinct ramification groups. Consider Stichtenoth, 1993, III.8.6, which states that if \( char \bar{K} = p > 0 \), then \( G_{i+1} \triangleleft G_i \) for all \( i \). Then since each \( G_i \) is a subgroup of a cyclic group, for each ramification group there exists a \( \sigma^l \in G \) which generate \( G_i \). As argued above there are only \( n-1 \) such \( \sigma^l \) generating distinct proper subgroups of \( G \). This places \( n \) as the lower bound on the number of distinct ramification groups. Thus there are \( n-1 \) ramification jumps and \( G_i = (\sigma^l) \) where \( 0 \leq l < n \). Finally \( (\sigma^l) = Gal(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) \) which is isomorphic to the cyclic group of order \( p^n \).

### 5 Applications

#### 5.1 Cyclotomic Extensions of \( \mathbb{Q}_p \)

In this example consider the \( p \)-adic completion of \( \mathbb{Q} \) with respect to a valuation (and associated metric) \( v_p \). Let \( n = p^m \) and \( \zeta \) be a primitive \( n \)th root of unity and the extension \( \mathbb{Q}_p(\zeta)/\mathbb{Q}_p \) with Galois group \( G \). Recall that \( |\mathbb{Q}_p(\zeta):\mathbb{Q}_p| = \phi(n) = (p-1)p^{m-1} \) and \( G \cong \mathbb{Z}/n^* \).

Now, if \( 0 \leq v \leq m \) then let \( G^v \) be the subgroup of \( G \) isomorphic to the subgroup \( H \subset \mathbb{Z}/n^* \) such that \( a \equiv 1 \mod p^v \) for every \( a \in H \). Then \( Gal(\mathbb{Q}_p(\zeta^{p^v}))/\mathbb{Q}_p(\zeta^{p^v})) \cong G^v \) because \( Gal(\mathbb{Q}_p(\zeta^{p^v}))/\mathbb{Q}_p) \cong (\mathbb{Z}/p^v)^* \). Using this fact it is straight forward to find all ramification groups \( G_i \) of \( G \) (Serre, 1995).
Proposition 7.

The ramification groups $G_i$ of $G$ are

$$G_u = \begin{cases} 
G & u = 0 \\
G^1 & 1 \leq u \leq p - 1 \\
G^2 & p \leq u \leq p^2 - 1 \\
\vdots \\
\{1\} & p^{m-1} \leq u
\end{cases}$$

Proof. Consider an element $x \neq 1$ in $G(n) \cong \mathbb{Z}/n^*$ and $\sigma_x$ the corresponding element in $G$. Let $i \in \mathbb{Z}$ be maximal such that $x \equiv 1 \mod p^i$. By definition of $G(n)^i$ and maximality of $i$, $x \in G(n)^i$ but $x \notin G(n)^{i+1}$. Now consider

$$i_{Q_p(\zeta^{p^m})/Q_p}(\sigma_x) = \omega(\sigma_x(\zeta) - \zeta) = \omega(\zeta^q - \zeta) = \omega(\zeta^{q-1} - 1).$$

Because $\zeta^{q-1}$ is a primitive $p^{m-i}$ root of unity, $\zeta^{q-1} - 1$ is a uniformizer of the valuation on $Q_p(\zeta^{p^m-1})$ (this is Serre, 1995, prop. IV.17.iii). Then it follows

$$i_{Q_p(\zeta^{p^m})/Q_p}(\sigma_x) = [Q_p(\zeta^{p^m}) : Q_p(\zeta^{p^m-1})] = #(G(n)^{m-i}) = p^i.$$ 

If $p^{k-1} \leq u \leq p^k - 1$, then $\sigma_x \in G_u$ if and only if $i \geq k$. Consequently $G_u = G(n)^i$. //

5.2 Artin-Schreier Extensions in Positive Characteristic

What follows is the above theory of ramification groups, applied to extensions of function field. Rather than speaking of primes, the theory is rephrased in terms of places. For the purposes here a place $\pi_F$ in the extension $F/K$ is the maximal ideal of a valuation ring $O$ of $F/K$. Note that in number fields primes correspond to places (Stichtenoth, 1993). The set of all places of an extension is denoted $\mathbb{P}_F$. Another important tool is the generalized Hurwitz Genus formula defined in terms of Weil differentials (which are beyond the scope of this paper). Such a generalization yields the following (Stichtenoth, 1993).

Theorem 2 (Generalized Hurwitz Genus Formula).

Consider $F'/K$ an algebraic function field of genus $g'$ and $F'/F$ a finite separable extension, $K'$ denotes the constant field of $F'$, and $g'$ the genus of $F'/K'$.

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg(Diff(F'/F)).$$

Then the different exponent over a place $\deg(Diff(\pi_{F'/F}))$ can be computed using Hilbert’s different formula (Stichtenoth, 1993).

Definition 9 (Hilbert’s Different Formula).

Consider a Galois extension $F'/F$ of algebraic function fields. A place $\pi_F$ of $F$, and a place $\pi_{F'}$ of $F'$ such that $\pi_{F'}|\pi_F$. Then the different exponent can be calculated

$$\deg(Diff(\pi_{F'}|\pi_F)) = \sum_{i \geq 0} (|G_i| - 1).$$
The different exponent of the extension is then the sum over all places of the extension

\[ \text{deg}(\text{Diff}(F'/F)) = \sum_{\pi \in \mathcal{P}} \sum_{i=0}^\infty (|G_i|-1). \]

Putting the above together (along with Dedekind’s different formula (Stichtenoth, 1993)) results in the following Wild Riemann-Hurwitz formula.

**Definition 10** (Wild Riemann-Hurwitz, Pries, n.d.).

*For algebraically closed field $F$ which has characteristic $p$ and $p|e$ where $e$ is the ramification index of place, $\pi_F$, under a degree $d$ covering map $\phi : X \to Y$ of curves over $F$, and $g_X$, $g_Y$ are the genera of $X$ and $Y$ respectively.*

\[
2g_Y - 2 = d(2g_X - 2) + \sum_{\pi \in \mathcal{P}} \left( \sum_{i=0}^\infty |G_i(x)|-1 \right).
\]

Consider a smooth algebraic curve $X_{p,t} : x^p - x - y^t$, where $t = ap - 1$ and $a \in \mathbb{Z}^+$. Further consider a covering map $\psi : X_{p,t} \to \mathbb{A}_F^1$ such that $\psi(x, y) = y$. Since $\psi$ is unramified over $\mathbb{A}_F^1$, consider now $\psi : X_{p,t} \to \mathbb{P}_F^1$. Then $\psi$ is only ramified over $P_\infty$. From Hilbert’s different formula it follows that in order to compute the different exponent it is necessary to understand the Galois group of $\psi$ and the ramification groups of $P_\infty$. To do so consider $Aut(X)$. Let $\tau(x) = x + 1$ then if $x^p - x - y^t = 0$ it follows

\[
\tau(x)^p - \tau(x) - y^t = (x+1)^p - (x+1) - y^t = x^p + 1 - x - 1 - y^t = x^p - x - y^t = 0
\]

because $\text{char}(F) = p$. Consequently $\tau \in Aut(X_{p,t})$ and $<\tau> = Aut(X_{p,t}) \cong \mathbb{Z}/p$ which agrees with the conclusion of Stichtenoth, 1993, III.7.10. Then the Galois group of the cover is $G = Aut(\psi)$.

Applying the change of variables $\bar{y} = \frac{1}{y}$, $\bar{x} = x\bar{y}^a$ results in a compactification of $X_{p,t}$ where $P_\infty = (0,0)$. The change of variables yields:

\[
x^p - x - y^t = 0 \implies x^p - x - y^a p^{-1} = 0 \implies x^p - x - y^a p y^{-1} = 0
\]

\[
\implies x^p y^{-ap} - xy - ap - y^{-1} = 0 \implies (xy^{-a})^p - xy^{-a} y^{-a(p-1)} - y^{-1} = 0
\]

\[
\implies \bar{x}^p - \bar{x} \bar{y}^{a(p-1)} - \bar{y} = 0.
\]

Thus $X_{p,t} : \bar{x}^p - \bar{x} \bar{y}^{a(p-1)} - \bar{y}$ which is ramified over $P_\infty = (0,0)$. Notice now that $\nu_\infty(\bar{x}) = 1$ because $\bar{x}$ vanishes with order 1 at $P_\infty$ so $\pi_\infty = \bar{x}$ is a uniformizing parameter over $P_\infty$. Further applying $\tau$, the generator of $G$, to $\bar{x}$ results in the following:

\[
\tau(\bar{x}) = (x+1)\bar{y}^a = \bar{x} + \bar{y}^a
\]

\[
\implies \tau(\bar{x}) - \bar{x} = \bar{y}^a.
\]

Consequently it is possible to compute $i_c(\tau)$ (recall this is the index of the first ramification group in which $\tau$ no longer appears):

\[
\nu_\infty(\tau(\bar{x}) - \bar{x}) = \nu_\infty(\bar{y}^a) = a\nu_\infty(\bar{y})
\]
\[ a_{\infty}(\bar{y}) = a_{\infty}(\bar{x}^p - \bar{x}\bar{y}(p-1)) = a \cdot min\{\nu_{\infty}(\bar{x}^p), \nu_{\infty}(\bar{x}\bar{y}^a(p-1))\} \]

\[ \nu_{\infty}(\tau(\pi) - \pi) = \nu_{\infty}(\bar{y}^a) = a \cdot \nu_{\infty}(\bar{x}^p) = ap. \]

What has been calculated is the ramification jump \( t_{p_{\infty}} = ap - 1 \) meaning \( G = G_0 = \ldots = G_{ap-1} \triangleright G_{ap} = Gap + 1 = \ldots = 1 \). Because \( \mathbb{Z}/p \) is simple and \( G_{ap} \triangleleft G \) is a strict inclusion; this implies that \( G_{ap} = \{1\} \) and all previous ramification groups are isomorphic to \( \mathbb{Z}/p \). Consequently it is now possible to calculate the degree of the different with Hilbert’s different formula

\[ \sum_{P \in P_{\infty}} \sum_{i=0}^{\infty} |G_i| - 1 = \sum_{P \in P_{\infty}} (p - 1)(ap). \]

Where \( |\mathbb{Z}/p| = p \) and \( ap \) is the number of nontrivial ramification groups. Because \( P_{\infty} \) is the only ramified place, the above is simply \( (p - 1)(ap) \) as all other places have trivial ramification groups. Thus the genus of \( X_{p,t} \) can be accurately calculated (using \( ap = t + 1 \)):

\[ 2g_{X_{p,t}} - 2 = p(2g_{p_{\infty}}) - (p - 1)(ap) \implies g_{X_{p,t}} = \frac{-2p - (p - 1)(t + 1) + 2}{2} = \frac{(p - 1)(t + 1)}{2}. \]

This result can be confirmed using the standard Riemann-Hurwitz formula. For the covering map \( \phi : X_{p,t} \to \mathbb{A}^1 \), where \( \phi(x, y) = x \) which is ramified when \( x \in \mathbb{Z}/p \) and \( y = 0 \) with ramification index \( t = ap - 1 \) (not divisible by \( p \)):

\[ g_{X_{p,t}} = \frac{p(-2) + p(t - 1) + 2}{2} = \frac{(p - 1)(t + 1)}{2}. \]

Which agrees with the previous computation.
REFERENCES


