

GENUS GROWTH IN \mathbb{Z}_p -TOWERS OF FUNCTION FIELDS

MICHIEL KOSTERS AND DAQING WAN

(Communicated by Mathew A. Papanikolas)

ABSTRACT. Let K be a function field over a finite field k of characteristic p and let K_∞/K be a geometric extension with Galois group \mathbb{Z}_p . Let K_n be the corresponding subextension with Galois group $\mathbb{Z}/p^n\mathbb{Z}$ and genus g_n . In this paper, we give a simple explicit formula for g_n in terms of an explicit Witt vector construction of the \mathbb{Z}_p -tower. This formula leads to a tight lower bound on g_n which is quadratic in p^n . Furthermore, we determine all \mathbb{Z}_p -towers for which the genus sequence is stable, in the sense that there are $a, b, c \in \mathbb{Q}$ such that $g_n = ap^{2n} + bp^n + c$ for n large enough. Such genus stable towers are expected to have strong stable arithmetic properties for their zeta functions. A key technical contribution of this work is a new simplified formula for the Schmid-Witt symbol coming from local class field theory.

1. INTRODUCTION

1.1. Global function fields. Let K be a function field over a finite field k of characteristic p . Let

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$$

be a geometric \mathbb{Z}_p -tower of function fields such that $\text{Gal}(K_n/K) = \mathbb{Z}_p/p^n\mathbb{Z}_p$. Let g_n denote the genus of K_n . We assume that the tower is only ramified at a finite number of places of K . In the spirit of Iwasawa theory, an emerging new research area is to study the possible stable arithmetic properties for the sequence of zeta functions of K_n as n varies; see [2] and [5] for recent progress and the relevant references there. A necessary condition for the sequence of zeta functions to be arithmetically stable is that the genus sequence g_n must be stable in the sense that g_n is a quadratic polynomial in p^n for large n . The aim of this paper is to classify all genus stable \mathbb{Z}_p -towers of K .

First, we give an explicit construction of all geometric \mathbb{Z}_p -towers of K using Witt vectors of K , via an improved presentation of the classical Artin-Schreier-Witt theory. This explicit construction leads to a simple explicit genus formula for the genus sequence; see Theorem 4.1. As an application, we derive an explicit quadratic lower bound in p^n for g_n , which is tight in many cases. This explicit formula also allows us to derive a simple criterion for when the genus g_n is a quadratic polynomial in p^n for large n .

By the Riemann-Hurwitz formula, the genus can be calculated from local ramification information and we can reduce to the local case where there is only one

Received by the editors March 15, 2017, and, in revised form, June 7, 2017.

2010 *Mathematics Subject Classification*. Primary 11G20, 11R37, 12F05.

Key words and phrases. \mathbb{Z}_p -extension, Artin-Schreier-Witt, Schmid-Witt, local field, global field, genus, conductor.

ramified prime. To illustrate our result in this introduction, here we consider an essential case, that is, $K = k(X)$ is the rational function field and the geometric \mathbb{Z}_p -tower K_∞ is only ramified at infinity. Then any such \mathbb{Z}_p -tower K_∞ over $K = k(X)$ can be uniquely constructed from a constant $c \in \mathbb{Z}_p$ and a primitive convergent power series

$$f(X) = \sum_{(i,p)=1} c_i X^i \in \mathbb{Z}_q[[X]], \quad c_i \in \mathbb{Z}_q, \quad \lim_i c_i = 0,$$

where $\mathbb{Z}_q = W(\mathbb{F}_q)$ denotes the Witt vectors of \mathbb{F}_q , and $f(X)$ is called primitive if not all c_i are divisible by p . The construction is explicitly given by the following Witt vector equation:

$$K_\infty : (Y_0^p, Y_1^p, \dots) - (Y_0, Y_1, \dots) = c\beta + \sum_{(i,p)=1} c_i(X^i, 0, \dots),$$

where both sides are Witt vectors and β is any fixed element of \mathbb{Z}_q with trace 1.

Theorem 1.1. *Let K_∞ be a geometric \mathbb{Z}_p -tower ramified only at infinity as constructed above by a primitive convergent power series $f(X)$. Then, we have*

(1). *For each integer $n \geq 1$, the genus g_n is given by the following formula:*

$$2g_n = \sum_{k=1}^n (p-1)p^{k-1} \left(-1 + \max_{i: v_p(c_i) < k} \left\{ ip^{k-1-v_p(c_i)} \right\} \right),$$

where v_p denotes the standard p -adic valuation with $v_p(p) = 1$.

(2). *For any $\epsilon > 0$, there is a constant $c(\epsilon)$ such that for all $n > c(\epsilon)$, we have*

$$g_n \geq \frac{p^{2n}}{2(p+1) + \epsilon}.$$

(3). *The tower K_∞ is genus stable in the sense that for all large enough n one has*

$$g_n = ap^{2n} + bp^n + c, \quad a, b, c \in \mathbb{Q}$$

if and only if

$$d := \max_{(i,p)=1} \left\{ \frac{i}{p^{v_p(c_i)}} \right\}$$

exists (and is thus a finite rational number).

Remarks. Part (2) shows that the genus sequence g_n grows at least quadratically in p^n . The lower bound in (2) cannot be improved in general. In particular, it implies that the lower bound for the genus in the literature is incorrect: the ϵ cannot be dropped (Remark 4.3). The proof of the above theorem follows from Corollary 4.2, Proposition 4.4 and Proposition 4.9.

1.2. Local function fields. Set $K = k((T))$, where k is a finite field of characteristic p and cardinality q . Local class field theory studies the abelian Galois extensions of K . Combining local class field theory and the theory of Artin-Schreier-Witt extensions gives us the so-called Schmid-Witt symbol

$$[\ , \]_n : W_n(K) \times K^* \rightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p,$$

where $W_n(K)$ is the ring of Witt-vectors of K of length n , and $1 \leq n \leq \infty$. The strongest case is when $n = \infty$, in which case the symbol $[\ , \]_\infty$ will be simply

denoted by $[,)$. In the simplest classical case $n = 1$, the symbol $[,)_1$, coming from Artin-Schreier theory, has the following beautiful simple formula:

$$[,)_1 : K \times K^* \rightarrow \mathbb{Z}/p\mathbb{Z}$$

$$(x, y) \mapsto \text{Tr}_{k/\mathbb{F}_p} (\text{Res}(x \cdot dy/y))$$

where dy is the derivative of y (see [9]).

As n grows, the situation becomes more complicated. Various formulas for $[,)_n$ for finite n were essentially known, but none of them completely seem to capture the simplicity of the formula for $n = 1$. Furthermore, these formulas have not been generalized to $[,)$. See [10, Proposition 3.4, Proposition 3.5, Proposition 4.3] for some of these formulas. We have found a new, simple and practical formula for $[,)$ (and thus for $[,)_n$ for all n). In the formula below, \tilde{x} and \tilde{y} are very explicit (see Theorem 3.2).

Theorem 1.2.

$$[x, y) = \text{Tr}_{\mathbb{Z}_q/\mathbb{Z}_p} (\text{Res}(\tilde{x} \cdot d\tilde{y}/\tilde{y})).$$

The simple nature of the above formula allows for easy computation of conductors and higher ramification groups of all \mathbb{Z}_p -towers, as in Proposition 3.3. These are the key technical results for our genus calculations, which might be of independent interest.

Remark 1.3. Many proofs in this paper, mostly regarding Artin-Schreier-Witt theory and Schmid-Witt symbols, have been removed since these results are mostly known or can be derived easily from known results. For an extended version of this paper with complete proofs, see [4].

2. ARTIN-SCHREIER-WITT EXTENSIONS

2.1. **Witt vectors.** For a detailed description, see [8], or follow the exercises from [6, Chapter VI, Exercises 46-48]. We will give a brief summary which we will use as a black box.

Let p be a prime number. Let R be a commutative ring with identity. We define the ring of p -typical Witt vectors $W(R) = W_\infty(R)$ as follows.

Definition 2.1. Let \mathcal{C} be the category of commutative rings with identity. Then there is a unique functor $W : \mathcal{C} \rightarrow \mathcal{C}$ such that the following hold:

- For a commutative ring R , one has $W(R) = R^{\mathbb{Z}_{\geq 0}}$ as sets.
- If $f : R \rightarrow S$ is a ring morphism, then the induced ring morphism satisfies $W(f)((r_i)_i) = (f(r_i))_i$.
- The map $g = (g^{(i)})_i : W(R) \rightarrow R^{\mathbb{Z}_{\geq 0}}$ defined by

$$(r_i)_i \rightarrow \left(\sum_{j=0}^i p^j r_j^{p^{i-j}} \right)_i$$

is a ring morphism (where $R^{\mathbb{Z}_{\geq 0}}$ has the product ring structure).

In $W(R)$ one has

$$(r_0, \dots) + (r'_0, \dots) = (r_0 + r'_0, \dots),$$

$$(r_0, \dots) \cdot (r'_0, \dots) = (r_0 \cdot r'_0, \dots),$$

where the formulas for the latter coordinates are quite complicated. The zero element of $W(R)$ is $(0, 0, \dots)$ and the identity element is $(1, 0, 0, \dots)$. One has $W(\mathbb{F}_p) = \mathbb{Z}_p$. If k is a finite field of q elements, then $W(k)$ is isomorphic to the ring \mathbb{Z}_q of integers of the unramified field extension of \mathbb{Q}_p with residue field k .

The above map g is called the ghost map, and this map is an injection if p is not a zero divisor in R . This ghost map, together with functoriality, determines the ring structure. Furthermore, we have the Teichmüller map

$$\begin{aligned} [\] : R &\rightarrow W(R) \\ r &\mapsto (r, 0, 0, \dots). \end{aligned}$$

This map is multiplicative: for $r, s \in R$ one has $[rs] = [r][s]$. We have the so-called Verschiebung group morphism

$$\begin{aligned} V : W(R) &\rightarrow W(R) \\ (r_0, r_1, r_2, \dots) &\mapsto (0, r_0, r_1, r_2, \dots). \end{aligned}$$

We make $W(R)$ into a topological ring as follows. The open sets around 0 are the sets of the form $V^i W(R)$. We call this the V -adic topology. With this topology, $W(R)$ is complete and Hausdorff. Furthermore, a ring morphism $R \rightarrow S$ induces a continuous map $W(R) \rightarrow W(S)$. Any $r = (r_0, r_1, \dots) \in W(R)$ can be written as $r = \sum_{i=0}^{\infty} V^i [r_i]$.

Now let us restrict to the case where $R = K$ is a field of characteristic p . The ring $W(K)$ has the subring $W(\mathbb{F}_p) = \mathbb{Z}_p$. Witt vectors $(x_0, x_1, \dots) \in W(K)$ with $x_0 \neq 0$, have a multiplicative inverse (note that $W(K)$ is not a field, since p is not invertible). The Frobenius map $x \mapsto x^p$ on K induces a ring morphism

$$\begin{aligned} F : W(K) &\rightarrow W(K) \\ (r_0, r_1, \dots) &\mapsto (r_0^p, r_1^p, \dots). \end{aligned}$$

In fact, one has $VF = FV = \cdot p$. One also sees that $W(K)$ is a torsion-free \mathbb{Z}_p -module. Let K'/K be a Galois extension and let $g \in G = \text{Gal}(K'/K)$. Then we have a map $W(g) : W(K') \rightarrow W(K')$. If K'/K is finite Galois, we define the following $W(K)$ -linear trace map:

$$\begin{aligned} \text{Tr}_{W(K')/W(K)} : W(K') &\rightarrow W(K) \\ x &\mapsto \sum_{g \in G} W(g)x. \end{aligned}$$

2.2. Artin-Schreier-Witt theory. For a full treatment of Artin-Schreier-Witt theory, see [4].

Fix a prime p and let K be a field of characteristic p . Let K^{sep} be a separable closure of K . We define a group morphism

$$\begin{aligned} \wp = F - \text{id} : W(K^{\text{sep}}) &\rightarrow W(K^{\text{sep}}) \\ x &\mapsto Fx - x, \end{aligned}$$

with kernel \mathbb{Z}_p . One can easily show that this map is surjective. For $a \in W(K)$ and $x = (x_0, x_1, \dots) \in \wp^{-1}a \subset W(K^{\text{sep}})$, we set $K(\wp^{-1}a) = K(x_0, x_1, \dots)$. This extension does not depend on the choice of x . In fact, $K(\wp^{-1}a) = K(\wp^{-1}b)$ if $a \equiv b \pmod{\wp W(K)}$.

We endow $W(K)/\wp W(K)$ with the induced topology, which is the same as the p -adic topology (where a basis of open sets around 0 is given by $\{p^i(W(K)/\wp W(K)) : i \in \mathbb{Z}_{\geq 0}\}$). We endow Galois groups with the Krull topology. The main theorem we need from Artin-Schreier-Witt theory is the following.

Theorem 2.2. *Let K be a field of characteristic p with absolute abelian Galois group $G = \text{Gal}(K^{\text{ab}}/K)$ and with p -part G_p . Then as topological groups one has*

$$W(K)/\wp W(K) \cong \text{Hom}_{\text{cont}}(G_p, \mathbb{Z}_p)$$

$$\bar{a} = \overline{\wp x} \mapsto (g \mapsto gx - x).$$

Furthermore, the field extension of K corresponding to $\bar{a} = \overline{\wp x} \in W(K)/\wp W(K)$ under this bijection and Galois theory is equal to $K(\wp^{-1}a)$ and the map

$$\text{Gal}(K(\wp^{-1}a)/K) \rightarrow \text{Hom}(\mathbb{Z}_p \bar{a}, \mathbb{Z}_p)$$

$$g \mapsto (r\bar{a} \mapsto r(gx - x))$$

is an isomorphism of topological groups.

Proof. See [4, Theorem 3.4, Theorem 3.6]. □

Let H be an abelian group. We define its p -adic completion, a \mathbb{Z}_p -module, to be

$$\widehat{H} = \varprojlim_i H/p^i H.$$

We make \widehat{H} into a topological group by giving a basis $\{p^i \widehat{H} : i \in \mathbb{Z}_{\geq 0}\}$ around 0. We call this the p -adic topology.

For $x \in K$, we set $\wp x = x^p - x$. One easy lemma is the following.

Lemma 2.3. *Let K be a field of characteristic p . Let \mathfrak{B} be a basis of $K/\wp K$ over \mathbb{F}_p . Then the map*

$$\bigoplus_{\mathfrak{B}} \widehat{\mathbb{Z}_p} \rightarrow W(K)/\wp W(K)$$

$$(a_b)_{b \in \mathfrak{B}} \rightarrow \sum_i a_b [b] \pmod{\wp W(K)}$$

is an isomorphism of topological groups.

Proof. See [4, Proposition 3.10]. □

Example 2.4. In certain cases, one can easily find a basis of $K/\wp K$ over \mathbb{F}_p . Below we will construct a subset \mathcal{D} of K which injects into $K/\wp K$ and such that its image forms an \mathbb{F}_p -basis of $K/\wp K$. For this purpose, it is enough to show that $\text{Span}_{\mathbb{F}_p}(\mathcal{D}) \cap \wp K = 0$ and $\text{Span}_{\mathbb{F}_p}(\mathcal{D}) + \wp K = K$.

- Assume K is a finite field. Take any vector b with $b \notin \wp K$, that is, take any $b \in K$ with $\text{Tr}_{K/\mathbb{F}_p}(b) \neq 0$. One can take $\mathcal{D} = \{b\}$.
- Assume $K = k((T))$ for a perfect field k . Let \mathcal{B} be a subset of k giving a basis of $k/\wp k$ over \mathbb{F}_p and let \mathcal{C} be a basis of k over \mathbb{F}_p . Then one can take

$$\mathcal{D} = \mathcal{B} \sqcup \{cT^{-i} : c \in \mathcal{C}, (i, p) = 1, i \geq 1\}.$$

Let us prove this result. If $f \in Tk[[T]]$, then set $g = -\sum_{i=0}^{\infty} f^{p^i} \in Tk[[T]]$.

One has $\wp g = f$. Note that $a_i T^{-ip} \equiv a_i^{1/p} T^{-i} \pmod{\wp K}$ (where we use that k is perfect). Hence we find $\text{Span}_{\mathbb{F}_p}(\mathcal{D}) + \wp K = K$. Let $f = \sum_i a_i T^i$. One has $\wp f = \sum_i a_i^p T^{ip} - \sum_i a_i T^i$. We find $\text{Span}_{\mathbb{F}_p}(\mathcal{D}) \cap \wp K = 0$.

- Assume $K = k(X)$ for some perfect field k . Let \mathcal{B} be a subset of k giving a basis of $k/\wp k$ over \mathbb{F}_p and let \mathcal{C} be a basis of k over \mathbb{F}_p . Then one can take

$$\mathcal{D} = \mathcal{B} \sqcup \bigsqcup_f \left\{ \frac{bX^i}{f^j} : (j, p) = 1, j \geq 1, 0 \leq i < \deg(f), b \in \mathcal{C} \right\} \\ \sqcup \{bX^j, (j, p) = 1, j \geq 1, b \in \mathcal{C}\},$$

where $f \in k[X]$ runs over monic irreducible polynomials. One can easily show this by using partial fractions.

3. LOCAL FUNCTION FIELDS

Let k be a finite field of cardinality q and characteristic p . We set $\mathbb{Z}_q = W(k)$. Let $K = k((T))$. The field K has a natural valuation. If $f = \sum_{i \geq v} a_i T^i$ with $a_v \neq 0$, then the valuation is v . We set $\mathfrak{p} = Tk[[T]]$, the unique maximal ideal of $k[[T]]$.

Let K^{ab} be the maximal abelian extension of K . Let $G = \text{Gal}(K^{\text{ab}}/K)$ with p -part G_p , all endowed with the Krull topology. Set $\widehat{K}^* = \varprojlim_n K^*/(K^*)^{p^n}$, the p -adic completion of K^* with its natural p -adic topology. Note that $\widehat{K}^* \cong T^{\mathbb{Z}_p} \times U_1$ where $U_1 = 1 + \mathfrak{p}$ are the one units of K . We usually identify \widehat{K}^* with $T^{\mathbb{Z}_p} \times U_1$. We have a natural map $K^* \rightarrow \widehat{K}^*$, with kernel k^* .

The Artin map (or Artin reciprocity law) from class field theory is a certain group morphism $K^* \rightarrow G$ (see [9]). This map is usually the best way to understand the group G and to understand ramification in abelian extensions of K . This Artin map induces a homeomorphism

$$\psi : \widehat{K}^* \rightarrow G_p.$$

Theorem 2.2 gives an isomorphism $W(K)/\wp W(K) \rightarrow \text{Hom}_{\text{cont}}(G_p, \mathbb{Z}_p)$. If we combine both maps, we obtain a \mathbb{Z}_p -bilinear, hence continuous, symbol

$$[\ , \] : W(K)/\wp W(K) \times \widehat{K}^* \rightarrow \mathbb{Z}_p \\ (\overline{\wp x}, y) \mapsto \psi(y)x - x.$$

This symbol is often called the Schmid-Witt symbol. For $1 \leq n \leq \infty$, reducing module p^n gives the level n Schmid-Witt symbol

$$[\ , \]_n : W_n(K)/\wp W_n(K) \times \widehat{K}^* \rightarrow \mathbb{Z}_p/p^n \mathbb{Z}_p$$

mentioned in the introduction, where $W_n(K)$ denotes the length n Witt vectors.

Note that the group $W(K)/\wp W(K)$ can be described as follows.

Proposition 3.1. *Let $\alpha \in k$ with $\text{Tr}_{k/\mathbb{F}_p}(\alpha) \neq 0$ and set $\beta = [\alpha] \in \mathbb{Z}_q \subset W(K)$. Then any $x \in W(K)$ has a unique representative in $W(K)/\wp W(K)$ of the form*

$$c\beta + \sum_{i \geq 1, (i, p) = 1} c_i [T^{-i}].$$

with $c \in \mathbb{Z}_p$ and $c_i \in \mathbb{Z}_q$ with $c_i \rightarrow 0$ as $i \rightarrow \infty$.

Proof. This follows from Lemma 2.3 and Example 2.4. □

Combining known formulas for $[\ , \]$ as in [10] together with our insight of Proposition 3.1 allows one to prove a simple formula for $[\ , \]$, which we now describe.

Consider the ring

$$R = \left\{ \sum_{i \in \mathbb{Z}} a_i T^i : a_i \in \mathbb{Z}_q, \lim_{i \rightarrow -\infty} a_i = 0 \right\} = \lim_{\leftarrow i} \mathbb{Z}_q/p^i \mathbb{Z}_q((T))$$

of two-sided power series with some convergence property. We have a residue map

$$\begin{aligned} \text{Res} : R &\rightarrow \mathbb{Z}_q \\ \sum_i a_i T^i &\rightarrow a_{-1}. \end{aligned}$$

Let $x \in W(K)$. Let $c\beta + \sum_{(i,p)=1} c_i [T]^{-i}$ be its unique representative modulo $\wp W(K)$ as in Proposition 3.1. We define a map

$$\begin{aligned} \tilde{\cdot} : W(K)/\wp W(K) &\rightarrow R \\ c\beta + \sum_{(i,p)=1} c_i [T]^{-i} \pmod{\wp W(K)} &\mapsto c\beta + \sum_{(i,p)=1} c_i T^{-i}. \end{aligned}$$

Any element $y \in \widehat{K}^* \cong T^{\mathbb{Z}_p} \times (1 + Tk[[T]])$ can uniquely be written as (with some abuse of notation)

$$y = T^e \cdot \prod_{(i,p)=1} \prod_{j=0}^{\infty} (1 - a_{ij} T^i)^{p^j}$$

with $e \in \mathbb{Z}_p$ and $a_{ij} \in k$. We define another map

$$\begin{aligned} \tilde{\cdot} : \widehat{K}^* \cong T^{\mathbb{Z}_p} \times (1 + Tk[[T]]) &\rightarrow T^{\mathbb{Z}_p} \times (1 + T\mathbb{Z}_q[[T]]) \\ T^e \cdot \prod_{(i,p)=1} \prod_{j=0}^{\infty} (1 - a_{ij} T^i)^{p^j} &\mapsto T^e \cdot \prod_{(i,p)=1} \prod_{j=0}^{\infty} (1 - [a_{ij}] T^i)^{p^j}. \end{aligned}$$

Furthermore, we define the group morphism

$$\begin{aligned} \text{dlog} : T^{\mathbb{Z}_p} \times (1 + T\mathbb{Z}_q[[T]]) &\rightarrow \mathbb{Z}_q((T)) \\ T^e \cdot f &\mapsto \frac{e}{T} + \frac{df}{f} \end{aligned}$$

where df is the formal derivative of f . We have the following formula for $[\ , \]$, which resembles formulas for the simpler symbol $[\ , \]_1$ as in [9].

Theorem 3.2. *Let $x \in W(K)$ and $y \in \widehat{K}^*$. Then one has*

$$[x, y] = \text{Tr}_{\mathbb{Z}_q/\mathbb{Z}_p}(\text{Res}(\tilde{x} \cdot \text{dlog}\tilde{y})).$$

Equivalently, let $x \equiv c\beta + \sum_{(i,p)=1} c_i [T]^{-i} \pmod{\wp W(K)}$ as in Proposition 3.1, and $y = T^e \cdot \prod_{(i,p)=1} \prod_{j=0}^{\infty} (1 - a_{ij} T^i)^{p^j} \in \widehat{K}^$ with $a_{ij} \in k$ and $e \in \mathbb{Z}_p$. Then one has:*

$$[x, y] = ce \text{Tr}_{\mathbb{Z}_q/\mathbb{Z}_p}(\beta) - \sum_{j=0}^{\infty} p^j \text{Tr}_{\mathbb{Z}_q/\mathbb{Z}_p} \left(\sum_{(i,p)=1} c_i \sum_{l|i} l [a_{ij}]^{i/l} \right) \in \mathbb{Z}_p.$$

Proof. For a complete proof, see [4, Theorem 4.7]. Let us sketch the main idea of the proof. A formula for $[\ , \]_n$ is given in [10, Proposition 3.2]. In this formula, there is a choice of a lift of x and y to characteristic 0. With our choices of lifts \tilde{x} and \tilde{y} and a simple computation, the formula simplifies and allows for a uniform formula in n for $[\ , \]_n$. This gives us our new formula, which we initially found using more abstract class field theory. \square

For a finite abelian extension L/K , the Artin map induces a map $\psi_L : K^* \rightarrow \text{Gal}(L/K)$. The conductor of L/K is defined to be $\mathfrak{f}(L/K) = \mathfrak{p}^i$ where i is minimal such that $U_i \subseteq \ker(\psi_L)$, where $U_i = 1 + \mathfrak{p}^i$ for $i \geq 1$ and $U_0 = k[[T]]^*$. The explicit formula above allows one to easily compute conductors.

Proposition 3.3. *Let $x = \wp(y_0, y_1, \dots) \in W(K)$ with $x \equiv c\beta + \sum_{(i,p)=1} c_i [T]^{-i} \pmod{\wp W(K)}$ as in Proposition 3.1. Let $n \in \mathbb{Z}_{\geq 1}$. One has*

$$\mathfrak{f}_n := \mathfrak{f}(K(y_0, y_1, \dots, y_{n-1})/K) = \mathfrak{p}^{u_n}$$

with

$$u_n = \begin{cases} 1 + \max\{ip^{n-v(c_i)-1} : i \text{ such that } v(c_i) < n\} & \text{if } \exists i : v(c_i) < n, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The result follows from Theorem 3.2 after some combinatorial computations. See [4, Proposition 4.14] for the details. \square

Remark 3.4. Let us give an essentially equivalent version of Proposition 3.3 in terms of upper ramification groups. Let $x \in W(K)$ as in Proposition 3.3. For $r \in \mathbb{Z}_{\geq 0}$ consider the r -th upper ramification group

$$H^r = \psi_{K(\wp^{-1}x)}(U_r) \subseteq \text{Gal}(K(\wp^{-1}x)/K) \cong \text{Hom}(\mathbb{Z}_p\bar{x}, \mathbb{Z}_p).$$

One then has

$$H^r = \{\tau : \tau\bar{x} \in p^{b_r}\mathbb{Z}_p\} \subseteq \text{Hom}(\mathbb{Z}_p\bar{x}, \mathbb{Z}_p),$$

where

$$b_r = \begin{cases} \min\{v(c_i) + \lceil \log_p(\frac{r}{i}) \rceil : (i, p) = 1\} & \text{if } r \geq 1, \\ \min\{v(c_i) : (i, p) = 1\} & \text{if } r = 0. \end{cases}$$

See [4, Proposition 4.14] for the details.

Remark 3.5. Let us briefly discuss the similarities and improvements on the essentially two formulas for $[\ , \]_n$ given in [10]. Let $x \in W(K)$ and $y \in K^*$. The first formula, in Proposition 3.4 and Proposition 3.5 in [10], looks as follows:

$$[x, y]_n = \pi_n \left(\text{Tr}_{\mathbb{Z}_q/\mathbb{Z}_p} \left(\text{Res} \left(\frac{dY}{Y} X^{(n-1)} \right) \right) \right).$$

Here $Y \in \mathbb{Z}_q((T))^*$ is a lift of y , $X \in W(\mathbb{Z}_q((T)))$ is a lift of x , $X^{(n-1)} \in \mathbb{Z}_q((T))$ is the $(n-1)$ -st ghost component of X and π_n is the reduction modulo $p^n\mathbb{Z}_p$. This formula resembles the classical formula for $[\ , \]_1$, and it has flexibility for the choices of lifts, which is very convenient. Unfortunately, this formula does depend on n with the term $X^{(n-1)}$ and hence does not directly give a formula for $[\ , \]$. Furthermore, it is hard to directly use the formula to obtain information about ramification groups and conductors. For the latter reason, a second formula for $[\ , \]_n$ is derived ([10, Proposition 4.3]). This formula also only seems to work for a fixed n , but its upside is that it is very explicit and easy to understand. The formula

only works for x which are in ‘reduced form’. An element $x \in W(K)$ has many different reduced forms, which are all equivalent modulo $\wp W(K)$. Unfortunately, this formula is much less conceptual and does not resemble the formula for $[\cdot, \cdot]_1$.

In our exposition, we associate to each element of $W(K)$ a unique reduced form. We can do this because of our understanding of $W(K)/\wp W(K)$ as in Proposition 3.1. This allows us to combine strengths from both formulas: our formulas for $[\cdot, \cdot]_n$ in Theorem 3.2 look conceptual and are still very usable. As an extra bonus, our approach gives us one formula for $[\cdot, \cdot]$.

In [10], especially in Corollary 1.1 and Corollary 5.1, formulas for ramification groups and conductors can be found. Our results in Proposition 3.3 and Remark 3.4 are very similar, but we have formulated them in a convenient way for our applications later in this paper.

4. GLOBAL FUNCTION FIELDS

Let k be a finite field of characteristic p . Let $K = K_0$ be a function field over k (a finitely generated field extension of k of transcendence degree 1) with full constant field k . Let $x = (x_0, x_1, \dots) = \wp(y_0, y_1, \dots) \in W(K)$. This Witt vector defines a field extension K_∞/K . For simplicity, we assume that $x_0 \notin \wp K$. Set $K_i = K(y_0, y_1, \dots, y_{i-1})$. One then has a tower of fields $K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_\infty = K(y_0, y_1, \dots)$ with $\text{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ and $\text{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

4.1. Genus formula. Let \mathfrak{p} be a place of K with residue field $k_{\mathfrak{p}}$ and uniformizer $\pi_{\mathfrak{p}}$. Then, locally, this extension is given by $x = (x_0, x_1, \dots) \in W(K_{\mathfrak{p}})$ where $K_{\mathfrak{p}} \cong k_{\mathfrak{p}}((\pi_{\mathfrak{p}}))$ is the completion at \mathfrak{p} (by the Cohen structure theorem). Let $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}$ with $\text{Tr}_{k_{\mathfrak{p}}/\mathbb{F}_p}(\alpha_{\mathfrak{p}}) \neq 0$. Set $\beta_{\mathfrak{p}} = [\alpha_{\mathfrak{p}}] \in W(k_{\mathfrak{p}})$. One has

$$x \equiv c_{\mathfrak{p}}\beta_{\mathfrak{p}} + \sum_{(i,p)=1} c_{\mathfrak{p},i}[\pi_{\mathfrak{p}}]^{-i} \pmod{\wp W(K_{\mathfrak{p}})}$$

with $c_{\mathfrak{p}} \in \mathbb{Z}_p$ and $c_{\mathfrak{p},i} \in W(k_{\mathfrak{p}})$ and $c_{\mathfrak{p},i} \rightarrow 0$ as $i \rightarrow \infty$ (Proposition 3.1). Proposition 3.3 then shows that the conductor at \mathfrak{p} of K_n/K is equal to $\mathfrak{f}_{\mathfrak{p},n} = \mathfrak{p}^{u_{\mathfrak{p},n}}$ with

$$u_{\mathfrak{p},n} = \begin{cases} 1 + \max\{ip^{n-v(c_{\mathfrak{p},i})-1} : i \text{ such that } v(c_{\mathfrak{p},i}) < n\} & \text{if } \exists i : v(c_{\mathfrak{p},i}) < n, \\ 0 & \text{otherwise.} \end{cases}$$

The conductor of K_n/K is the formal expression

$$\mathfrak{f}_n = \mathfrak{f}(K_n/K) = \prod_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p},n},$$

which is a finite product.

Let g_n be the genus of K_n , where the genus is the genus of the corresponding smooth projective curve defined by K_n over the integral closure of k inside K_n . We let n_c be maximal such that K_{n_c}/K is a constant field extension.

Theorem 4.1. *For $n \in \mathbb{Z}_{\geq 1}$, we have*

$$p^{\min\{n_c, n\}}(2g_n - 2) = p^n(2g_0 - 2) + \sum_{\mathfrak{p}} [k_{\mathfrak{p}} : k] \sum_{i=1}^n \varphi(p^i) u_{\mathfrak{p},i}.$$

Proof. This is an application of the Riemann-Hurwitz formula, together with the Führerdiskriminantenproduktformel. See [4, Theorem 5.2]. □

4.2. Genus lower bound. We assume that the tower is not a constant extension, otherwise, the genus g_n will be a constant. This means that n_c is finite. Since K_∞/K is abelian and infinite, by class field theory, the extension K_∞/K must be ramified at some prime. Let n_u be maximal such that K_{n_u}/K is unramified. Then $n_c \leq n_u < \infty$.

Corollary 4.2. *Let $n \geq n_u$. The following statements hold:*

i.

$$p^{n_c}(2g_n - 2) \geq p^n(2g_0 - 2) + p^n - p^{n_u} + p^{n_u} \frac{p^{2(n-n_u)} - 1}{p + 1}.$$

ii.

$$\liminf_{n \rightarrow \infty} \frac{g_n}{p^{2n}} \geq \frac{1}{2p^{n_u+n_c}(p + 1)}.$$

iii. *For any $\epsilon > 0$, there is an integer m such that for all $n \geq m$ one has*

$$g_n \geq \frac{p^{2n-n_u-n_c}}{2(p + 1) + \epsilon} \geq \frac{p^{2n-n_u-n_c-1}}{3 + \epsilon}.$$

Proof. We try to make the genus as small as possible in the genus formula. The smallest genus is obtained if only one prime \mathfrak{p} is ramified with $[k_{\mathfrak{p}} : k] = 1$, such that $u_{\mathfrak{p},n} = 1 + p^{n-n_u-1}$ for $n > n_u$, and $u_{\mathfrak{p},n} = 0$ for $n \leq n_u$ (see Proposition 3.3). One finds for $n \geq n_u$ by Theorem 4.1:

$$\begin{aligned} p^{n_c}(2g_n - 2) &\geq p^n(2g_0 - 2) + \sum_{i=n_u+1}^n \varphi(p^i) (1 + p^{i-n_u-1}) \\ &= p^n(2g_0 - 2) + p^n - p^{n_u} + p^{n_u} \frac{p^{2(n-n_u)} - 1}{p + 1}. \end{aligned}$$

The first part is proved. The second and third part follow by looking at the last term of the formula from the first part. □

Remark 4.3. The bounds in Corollary 4.2 are often sharp when the p -part of the class group of K is 0. In particular, the bounds are sharp when $K = k(X)$, the projective line. We will give explicit examples later.

Gold and Kisilevsky in [3, Theorem 1] state that for large n , if $n_c = 0$ one has:

$$g_n \geq \frac{p^{2(n-n_u)-1}}{3}.$$

This result contains a small error which makes the result incorrect for $p = 2, g_0 = 0$ (one really needs the ϵ in that case; see Proposition 4.9). Secondly, in their proof they reduce to the case $n_u = 0$, but they forget that if $n_u > 0$, then more primes must ramify and hence the genus will grow faster.

Assume from now on that $n_u = 0$. In fact Gold and Kisilevsky prove in an intermediate step

$$\liminf_{n \rightarrow \infty} \frac{g_n}{p^{2n}} \geq \frac{p - 1}{2p^2}.$$

Our result actually gives the tight bound

$$\liminf_{n \rightarrow \infty} \frac{g_n}{p^{2n}} \geq \frac{1}{2(p + 1)}.$$

Li and Zhao in [7] construct a \mathbb{Z}_p -tower with the property

$$\lim_{n \rightarrow \infty} \frac{g_n}{p^{2n}} = \frac{1}{2(p+1)}.$$

Li and Zhao furthermore write “It would be interesting to determine if the bound of Gold and Kisilevsky is the best and find some \mathbb{Z}_p -extension which realizes it.” Our results show that their tower actually attains our limit.

4.3. Genus stability. We will now introduce a special class of \mathbb{Z}_p -extensions of K . We are interested in classifying the cases when g_n for large enough n stabilizes. Note that g_n is bounded below by a quadratic polynomial in p^n by Corollary 4.2. We will now study the case where g_n at some point becomes a quadratic polynomial in p^n . A \mathbb{Z}_p -tower K_∞/K is called geometric if $n_c = 0$.

Proposition 4.4. *Let K_∞/K be a geometric \mathbb{Z}_p -extension. Then the following are equivalent:*

- i. *There are $a, b, c \in \mathbb{Q}$, $m \in \mathbb{Z}_{\geq 0}$ such that for $n \geq m$ one has*

$$g_n = ap^{2n} + bp^n + c.$$

- ii. *The extension K_∞/K is ramified at only finitely many places and for all \mathfrak{p} the set*

$$\{ip^{-v(c_{\mathfrak{p},i})} : (i, p) = 1\}$$

has a maximum.

- iii. *The extension K_∞/K is ramified at only finitely many places and for each \mathfrak{p} which ramifies there are $a_{\mathfrak{p}} \in \mathbb{Q}_{>0}$ and $n_{\mathfrak{p}} \in \mathbb{Z}_{\geq 0}$ such that for $n \geq n_{\mathfrak{p}}$ one has*

$$u_{\mathfrak{p},n} = 1 + a_{\mathfrak{p}}p^n.$$

Proof. i \iff iii: This follows easily from Theorem 4.1.

ii \iff iii: This follows directly from the definition of the $u_{\mathfrak{p},n}$. □

Definition 4.5. A geometric \mathbb{Z}_p -extension K_∞/K is called *genus-stable* if one of the equivalent conditions of Proposition 4.4 is satisfied.

Remark 4.6. Let L be a finite extension of \mathbb{Q}_p with prime \mathfrak{p} and ramification index $e = e(L/\mathbb{Q}_p)$. Let L_∞/L be a \mathbb{Z}_p -extension. In that case one has the following stability result for the discriminants (which can be seen as the analogue of the genus). There are $A, B \in \mathbb{Q}$ such that $\text{disc}(L_n/L) = \mathfrak{p}^{r_n}$ with $r_n = e(np^n) + Ap^n + B$ for n large enough. See [11, Section 3.1] for a proof. The reason that such a simple formula always holds is that U_1 is a finitely generated \mathbb{Z}_p -module in this case.

Remark 4.7. The definition of genus stability might look a bit arbitrary. However, it turns out that one can prove interesting results about genus stable towers. Here is an example. The L -functions of genus stable covers of the projective line behave nicely in a p -adic way. One can show that the p -adic valuations of the inverses of the zeros of such L -function are uniformly distributed and form a finite union of arithmetic progressions in many cases. The latter result can only hold for genus stable covers. See [2] and [5] for details.

For future reference, let us discuss the degree of such L -functions. Let K_∞/K be a geometric \mathbb{Z}_p -tower. Let $\chi : \text{Gal}(K_\infty/K) \rightarrow \mathbb{C}_p^*$ be a non-trivial finite character

of order $p^{m_\chi} > 1$. This character will factor through $\text{Gal}(K_{m_\chi}/K)$. Then one can associate to this character an L -function

$$L(\chi, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\text{Frob}(\mathfrak{p}))s^{\deg(\mathfrak{p})}} \in 1 + s\mathbb{C}_p[[s]],$$

where the product is taken over all primes of K which are unramified in the extension K_{m_χ}/K . Here $\text{Frob}(\mathfrak{p}) \in \text{Gal}(K_{m_\chi}/K)$ is the Frobenius element of \mathfrak{p} . By [1, Theorem A] $L(\chi, s)$ is a polynomial of degree

$$\deg(L(\chi, s)) = 2g(K) - 2 + \deg(\mathfrak{f}_{m_\chi}) = 2g(K) - 2 + \sum_{\mathfrak{p}} \deg(\mathfrak{p})u_{\mathfrak{p}, m_\chi},$$

where $u_{\mathfrak{p}, m_\chi}$ are as before. Assume now that K_∞/K is genus stable and only ramified at rational primes. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the ramifying primes in K_∞/K and set

$$d_j p^{-m_j} = \max\{ip^{-v(c_{\mathfrak{p}_j, i})} : (i, p) = 1\},$$

where $d_j, m_j \in \mathbb{Z}_{\geq 0}$ and with $p \nmid d_j$. Let $m = \max\{m_j : j = 1, \dots, r\}$. Then if $m_\chi > m$, one has

$$\deg(L(\chi, s)) = 2g(K) - 2 + r + \sum_{j=1}^r d_j p^{m_\chi - m_j - 1}.$$

Hence the degree of $L(\chi, s)$ is a linear polynomial in p^{m_χ} for large enough m_χ . Conversely, if the degree of $L(\chi, s)$ is a linear polynomial in p^{m_χ} for large enough m_χ , then the tower is genus stable.

4.4. Example: The projective line. Let $K = k(X)$ be the function field of the projective line where k is a finite field. We will study \mathbb{Z}_p -towers over K which ramify only at rational points. For $x \in k$, we set $\pi_x = X - x \in K$ and we set $\pi_\infty = 1/X \in K$. Let $\alpha \in k$ with $\text{Tr}_{k/\mathbb{F}_p}(\alpha) \neq 0$. Set $\beta = [\alpha]$. Analogous to Example 2.4, one can prove the following. Let $a = \wp y \in W(K)$ which gives rise to the extension $K(y)$ of K which ramifies only at rational points (see [4] for the slightly more general case).

Lemma 4.8. *The element a is equivalent modulo $\wp W(K)$ to a unique element of the form*

$$c\beta + \sum_{x \in k \cup \{\infty\}} \sum_{(i, p)=1} c_{x, i} [\pi_x]^{-i} \in W(K)$$

with $c \in \mathbb{Z}_p$, $c_{x, i} \in \mathbb{Z}_q$ such that $c_{x, i} \rightarrow 0$ as $i \rightarrow \infty$.

Proof. See [4, Lemma 5.8]. This follows from Example 2.4. □

Note that $a, a' \in W(K)$ give the same tower if and only if $a = a'c$ with $c \in \mathbb{Z}_p^*$. One can easily see when this happens in Lemma 4.8. We will now deduce data of the extension given by a .

Proposition 4.9. *Let $a = c\beta + \sum_{x \in k \cup \{\infty\}} \sum_{(i, p)=1} c_{x, i} [\pi_x]^{-i} = \wp(y_0, y_1, \dots) \in W(K)$ as in Lemma 4.8. Assume*

$$\min(\{v(c_{x, i}) : x \in k \cup \{\infty\}, (i, p) = 1\} \cup \{v(c)\}) = 0.$$

Consider the tower K_∞/K corresponding to a with subfield $K_n = K(y_0, y_1, \dots, y_{n-1})$ of genus g_n . For $x \in k \cup \{\infty\}$, set

$$u_{x,n} = \begin{cases} 1 + \max\{ip^{n-v(c_{x,i})-1} : (i,p) = 1 \text{ s.t. } v(c_{x,i}) < n\} & \text{if } \exists i : v(c_{x,i}) < n, \\ 0 & \text{otherwise.} \end{cases}$$

Then the extension K_n/K is Galois with group isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. One has

$$n_u = n_c = \min\{v(c_{x,i}) : x \in k \cup \{\infty\}, (i,p) = 1\}$$

and

$$f_n = \prod_{x \in k \cup \{\infty\}} (\pi_x)^{u_{x,n}}$$

and

$$p^{\min\{n_c, n\}}(2g_n - 2) = -2p^n + \sum_{x \in k \cup \{\infty\}} \sum_{j=0}^n \varphi(p^j)u_{x,j}.$$

Proof. The results follow from the discussions before, and most importantly, Theorem 4.1. □

In the above proposition, one can easily deduce when the tower is genus stable with the help of Proposition 4.4.

Example 4.10. Consider the unit root \mathbb{Z}_p -extension (called the Artin-Schreier-Witt extension in [2]) given by the unit root coefficient polynomial

$$x = \sum_{(i,p)=1}^d [b_i X^i] = \sum_{(i,p)=1}^d [b_i][X^i] \in W(K)$$

with $b_i \in k$ and $b_d \neq 0$, $d > 0$ not divisible by p . By the above equation, this defines a \mathbb{Z}_p -extension which is totally ramified at ∞ . One finds for $n \geq 1$:

$$u_{\infty,n} = 1 + dp^{n-1}$$

and this gives

$$2g_n - 2 = \frac{d}{p+1}p^{2n} - p^n - \frac{p+1+d}{p+1}.$$

This is an example of a genus-stable tower.

Remark 4.11. Let $a = (a_0, a_1, \dots) \in W(K)$ with $a_0 \notin \wp K$. Consider the corresponding \mathbb{Z}_p -extension given by a . Let \mathfrak{p} be a prime of $K(X)$ of degree d' over \mathbb{F}_p which does not ramify in the tower. We give a geometric way to compute the Frobenius element $(\mathfrak{p}, K_\infty/K)$. Let $z \in \mathbb{P}^1(\bar{k})$ be a representative of \mathfrak{p} . Assume that z is not a pole of the a_i (otherwise, we have to find another representative of $a \pmod{\wp W(K)}$); or one can assume a is in our unique reduced form). Set $a(z) = (a_0(z), a_1(z), \dots) \in W(k(z))$. Let $y \in \wp^{-1}z \in W(\bar{k})$. One has

$$F^{d'} y = y + \sum_{j=0}^{d'-1} F^j(Fy - y) = y + \text{Tr}_{W(k(z))/W(\mathbb{F}_p)}(a(z)).$$

This shows that the Frobenius is equal to

$$(\mathfrak{p}, K_\infty/K) = (\bar{a} \mapsto -\text{Tr}_{W(k(z))/\mathbb{Z}_p}(a(z))) \subseteq \text{Hom}(\mathbb{Z}_p\bar{a}, \mathbb{Z}_p) \cong \text{Gal}(K(\wp^{-1}a)/K).$$

A similar formula works for primes which are not ramified in say K_n/K . Furthermore, this formula generalizes when K is replaced by another function field.

ACKNOWLEDGMENTS

We would like to thank Chris Davis for his help with Witt-vectors and for his proofreading of parts of this manuscript. We would also like to thank the referee for comments on this paper.

REFERENCES

- [1] Enrico Bombieri, *On exponential sums in finite fields* (English, with French summary), *Les Tendances Géom. en Algèbre et Théorie des Nombres*, Éditions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 37–41. MR0204413
- [2] Christopher Davis, Daqing Wan, and Liang Xiao, *Newton slopes for Artin-Schreier-Witt towers*, *Math. Ann.* **364** (2016), no. 3–4, 1451–1468, DOI 10.1007/s00208-015-1262-4. MR3466874
- [3] R. Gold and H. Kisilevsky, *On geometric \mathbf{Z}_p -extensions of function fields*, *Manuscripta Math.* **62** (1988), no. 2, 145–161, DOI 10.1007/BF01278975. MR963002
- [4] M. Kusters and D. Wan, *On the arithmetic of \mathbf{Z}_p -extensions*, arXiv:1607.00523.
- [5] M. Kusters and H.J. Zhu, *On slopes of L -functions of \mathbf{Z}_p -covers over the projective line*, arXiv:1701.08733.
- [6] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556
- [7] Chaoqun Li and Jianqiang Zhao, *Class number growth of a family of \mathbf{Z}_p -extensions over global function fields*, *J. Algebra* **200** (1998), no. 1, 141–154, DOI 10.1006/jabr.1997.7233. MR1603268
- [8] J. Rabinoff, *The theory of Witt vectors*, arXiv preprint arXiv:1409.7445, (2014).
- [9] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237
- [10] Lara Thomas, *Ramification groups in Artin-Schreier-Witt extensions* (English, with English and French summaries), *J. Théor. Nombres Bordeaux* **17** (2005), no. 2, 689–720. MR2211314
- [11] J. T. Tate, *p -divisible groups*, *Proc. Conf. Local Fields (Driebergen, 1966)*, Springer, Berlin, 1967, pp. 158–183. MR0231827

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, IRVINE, 340 ROWLAND HALL, IRVINE, CALIFORNIA 92697

E-mail address: `kusters@gmail.com`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, IRVINE, 340 ROWLAND HALL, IRVINE, CALIFORNIA 92697

E-mail address: `dwan@math.uci.edu`