Journal of Number Theory **70**, 37–61 (1998)
Article No. NT982224

Deformations for Function Fields

David T. Ose*, †

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail: ose-d@member.ams.org

Communicated by D. Goss

Received July 31, 1997; revised November 24, 1997

We consider a question of describing the one-dimensional P-adic representations that lift a given representation over a finite field of the absolute Galois group of a function field. In this case, the characterization of abelian p-power extensions of

those representations which can be realized as the action of the Galois group on the division points of a rank one Drinfeld module, discussing both results and a conjecture about the form of the representations that arise in this manner. © 1998 Academic Press

Key Words: Function field; deformations; deformation theory; Galois representations.

1. INTRODUCTION

Galois representations have played a large role in recent advances in number theory, most notably in Wiles' proof of Fermat's Last Theorem [17]. Here we recall a construction on algebraic function fields called *Drinfeld modules*, and how we may construct Galois representations from them. We also recall the definition and a few basic facts about *deformations* of Galois representations.

1.1. *Drinfeld modules.* A function field, for our purposes, is a field $\mathbf{k}$ that is finitely generated over its finite prime field $\mathbb{F}_p$ and has transcendence

* I thank Nigel Boston, my thesis advisor, for introducing me to his work, the University of Illinois, for making it possible for me to visit the Isaac Newton Institute at Cambridge, England, where this work really began and for supporting me through the Department of Education National Needs Fellowship, and my wife Kerry, for her love, support and encouragement. I thank the referee for improving this paper. And finally, I thank God for leading me to the results of this paper.

† Current address: Department of Mathematical Sciences, Lycoming College, Williamsport, PA 17701.

0022-314X/98 $25.00

degree one over $\mathbb{F}_p$. Since the field $\mathbf{k}$ can be viewed as the field of functions on a curve over $\mathbb{F}_q$ (the algebraic closure of $\mathbb{F}_p$ in $\mathbf{k}$), we may refer to the elements of $\mathbf{k}$ as functions. Let P be a place (and v be its corresponding valuation) and let $\mathcal{O}_P$ be the ring of elements $a \in \mathbf{k}$ that do not have a pole at P (that is, $v(a) \geqslant 0$). See [5, 15] for the basic properties of function fields.

Let ∞ be a fixed place of $\mathbf{k}$, and let $\mathscr{A}$ be the subring of $\mathbf{k}$ consisting of the elements whose only pole is ∞. Then $\mathscr{A}$ is a Dedekind domain, with $\mathbf{k}$ its field of fractions. The obvious example is where $\mathbf{k}$ is the field $\mathbb{F}_q(T)$ of rational functions in one variable over a finite field, the distinguished place ∞ is the unique valuation for which $v(T) = -1$. In this case, the ring $\mathscr{A}$ is the ring $\mathbb{F}_q[T]$ of polynomials in one variable over a finite field. Now if we let S be a set consisting of places of $\mathbf{k}$, then we can define $\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_P$. If we let S be the set of all places of $\mathbf{k}$ except ∞, then $\mathscr{A}$ is $\mathcal{O}_S$.

If we have a fixed $\mathbb{F}_q$-algebra homomorphism $\gamma: \mathscr{A} \to \mathbf{K}$ for a field $\mathbf{K}$, we call $\mathbf{K}$ an $\mathscr{A}$-field. Usually, γ will be an inclusion map, such as the ring homomorphism from $\mathbb{F}_q[T]$ into $\mathbf{F}_q(T)$ (or even into a finite extension of $\mathbb{F}_q(T)$), or a reduction modulo a prime ideal.

Let $\mathbf{K}\{\mathscr{F}\}$ denote the twisted ring of polynomials in the indeterminate $\mathscr{F}$ with coefficients in $\mathbf{K}$ written on the left and in which multiplication follows the rule $\mathscr{F} w = w^q \mathscr{F}$ when $w \in \mathbf{K}$. Let i be the inclusion map of $\mathbf{K}$ into $\mathbf{K}\{\mathscr{F}\}$, and let D be the map from $\mathbf{K}\{\mathscr{F}\}$ to $\mathbf{K}$ induced by $\mathscr{F} \mapsto 0$. Note that, for any commutative $\mathbf{K}$-algebra $\mathscr{R}$, $\mathbf{K}\{\mathscr{F}\}$ acts on $\mathscr{R}$ via $w \cdot r = wr$ for $w \in \mathbf{K}$ and $\mathscr{F} \cdot r = r^q$. Hence $\mathscr{F}$ acts as the q-power map on $\mathscr{R}$. In fact, one can show that $\mathbf{K}\{\mathscr{F}\}$ is isomorphic to the ring of $\mathbb{F}_q$-linear endomorphisms of the additive group scheme over $\mathbf{K}$. The ring $\mathbf{K}\{\mathscr{F}\}$ possesses a right division algorithm, and hence every left ideal is principal [5, Proposition 1.6.2].

DEFINITION 1. Let $\mathbf{K}$ be an $\mathscr{A}$-field. A Drinfeld $\mathscr{A}$-module over $\mathbf{K}$ is a ring homomorphism $\phi: \mathscr{A} \to \mathbf{K}\{\mathscr{F}\}$ for which $D\phi = \gamma$, but $\phi \neq i\gamma$.

Notice that a Drinfeld module gives an action of $\mathscr{A}$ on any commutative $\mathbf{K}$-algebra $\mathscr{R}$ that is different from the action given by γ. For an element $a \in \mathscr{A}$, we will write ϕ_a for the image of a under ϕ. Since $\phi_a \in \mathbf{K}\{\mathscr{F}\}$, we will denote the action of ϕ_a on $x \in \mathscr{R}$ (where $\mathscr{R}$ is a $\mathbf{K}$-algebra) by $\phi_a(x)$.

Two invariants of a Drinfeld module ϕ are its *rank* and its *characteristic*. The characteristic of a Drinfeld module is the (prime) ideal $\ker(\gamma)$ of $\mathscr{A}$. If the kernel is (0), then we say the characteristic is "generic" or sometimes that the Drinfeld module "has no characteristic." The rank of a Drinfeld module is a positive integer r, which is easiest to explain when $\mathscr{A}$ is $\mathbb{F}_q[T]$, in which case r is the degree in $\mathscr{F}$ of ϕ_T. The reader may consult [5, 7] for more information.

EXAMPLE 2 (Carlitz Module). Let $\mathscr{A}$ be $\mathbb{F}_q[T]$ and let $\mathbf{K}$ be $\mathbb{F}_q(T)$ and let γ be the natural inclusion. The Carlitz module (the first example of what later became known as Drinfeld modules) ϕ is defined by $T \mapsto \mathscr{F} + T$. One can see that $\phi \neq i\gamma$ as $\phi_T = \mathscr{F} + T \neq T = i\gamma(T)$. One can also see that $\gamma = D\phi$. The rank of the Carlitz module is one, since $\deg \phi_T = 1$. It has generic characteristic, since γ is an inclusion. See [6] for a fascinating and readable account of an explicit construction of class field theory for rational function fields using the Carlitz module.

Let ϕ be a Drinfeld $\mathscr{A}$-module over $\mathbf{K}$ of rank r, and let $a \in \mathscr{A}$ where a is not in the characteristic of ϕ. Let $\mathscr{R}$ be a $\mathbf{K}$-algebra, and recall that $\mathbf{K}\{\mathscr{F}\}$ acts on the polynomial ring $\mathscr{R}$ by $w(z) = wx$ for $w \in \mathbf{K}$ and by $\mathscr{F}(x) = x^q$ for any $x \in \mathscr{R}$. Thus if $f = w_0 + w_1\mathscr{F} + \cdots + w_n\mathscr{F}^n$, $f(x) = w_0x + w_1x^q + \cdots + w_nx^{q^n}$. In this way, $\phi_a(x)$ is a polynomial over $\mathbf{K}$ with only q-power exponents, and since the coefficient of x is $\gamma(a) = D\phi(a)$, $\phi'_a(x) = \gamma(a) \neq 0$, $\phi_a(x)$ has no repeated roots, and thus the field extension generated by adjoining the roots of $\phi_a(x)$ to $\mathbf{K}$ is separable. The a-division points of ϕ are the roots of this polynomial in the algebraic closure of $\mathbf{K}$. Now let I be a nonzero ideal of $\mathscr{A}$ not divisible by the characteristic of ϕ. We can define the I-division points, $\phi[I]$, as $\{x \in \bar{\mathbf{K}} \mid \phi_a(x) = 0 \text{ for every } a \in I\}$. One can show that $\phi[I] \cong (\mathscr{A}/I)^r$ by first examining the case where I is a prime ideal, then the case where I is a power of a prime ideal, and finally the general case [7, p. 8]. As $\mathbf{K}\{\mathscr{F}\}$ is a left principal ideal ring, the annihilator of $\phi[I]$ is a left ideal generated by one element ϕ_I, which is monic in $\mathscr{F}$. Note that ϕ_I is not necessarily in the image of ϕ.

The group $G_{\mathbf{K}} := \mathrm{Gal}(\mathbf{K}^{\mathrm{sep}}/\mathbf{K})$ acts naturally on $\phi[I]$, producing a representation

$$G_{\mathbf{K}} \to \mathrm{Aut}(\phi[I]) \cong \mathrm{GL}_r(\mathscr{A}/I)$$

which is, of course, continuous.

Suppose P is a prime ideal in $\mathscr{A}$, different from the characteristic of ϕ. Then ϕ_P provides an $\mathscr{A}$-module epimorphism $\phi[P^{n+1}] \to \phi[P^n]$ by $x \mapsto \phi_P(x)$. We define the Tate module $\mathbf{T}(\phi, P)$ to be the inverse limit of this system. The action of $G_{\mathbf{K}}$ commutes with the action of ϕ_P, since the action of ϕ_P is a polynomial action with coefficients in $\mathbf{K}$, hence we have a continuous representation

$$G_K \to \mathrm{Aut}\ \mathbf{T}(\phi, P) \cong \mathrm{GL}_r(\mathscr{A}_P)$$

where $\mathscr{A}_P$ is the completion of $\mathscr{A}$ at the prime ideal P. Thus Drinfeld modules, in a way completely analogous to the construction for elliptic curves and more general abelian varieties, lead to both finite and P-adic Galois representations.

1.2. *Deformations of Galois representations.* Let G be a profinite group, and fix a continuous representation

$$\bar{\rho}\colon G \to \mathrm{GL}_r(\mathbf{F})$$

where $\mathbf{F}$ is a finite field. Let $\mathcal{O}$ be a commutative complete local noetherian ring with residue field $\mathbf{F}$, and let $\mathsf{C}(\mathcal{O})$ be the category of commutative local topological $\mathcal{O}$-algebras $\mathscr{R}$ with continuous local $\mathcal{O}$-algebra homomorphisms for morphisms, for which the natural map $\mathcal{O} \to \mathscr{R}/\wp_{\mathscr{R}}$ is a surjection ($\wp_{\mathscr{R}}$ is the maximal ideal of $\mathscr{R}$), and for which the homomorphism from $\mathscr{R}$ to the inverse limit of its discrete artinian quotients is a topological isomorphism. The last condition guarantees that $\mathscr{R}$ is complete and its topology is determined by the collection of open ideals I for which $\mathscr{R}/I$ is artinian. Given an object $\mathscr{R}$ of this category, define $\pi_{\mathscr{R}}$ to be the map from $\mathrm{GL}_r(\mathscr{R})$ to $\mathrm{GL}_r(\mathbf{F})$ induced by reducing the entries modulo the maximal ideal of $\mathscr{R}$. A continuous homomorphism

$$\rho\colon G \to \mathrm{GL}_r(\mathscr{R})$$

is called a *lift* of $\bar{\rho}$ to $\mathscr{R}$ if $\bar{\rho} = \pi_{\mathscr{R}} \cdot \rho$.

Let $\Gamma_r(\mathscr{R}) = \ker(\pi_{\mathscr{R}})$. We may define a strict equivalence relation between two representations ρ_1 and ρ_2 if $g^{-1}\rho_1 g = \rho_2$ for some $g \in \Gamma_r(\mathscr{R})$. We call the strict equivalence class of a lift of $\bar{\rho}$ a *deformation* of $\bar{\rho}$ to $\mathscr{R}$. Finally we can define Mazur's functor, A from $\mathsf{C}(\mathcal{O})$ to the category of sets, by setting

$$\mathsf{A}(\mathscr{R}) = \{\text{deformations of } \bar{\rho} \text{ to } \mathscr{R}\}$$

and with the obvious definition of A on morphisms.

In Mazur's original work [12], he shows that this functor is representable on the full subcategory of complete local noetherian $\mathcal{O}$-algebras when $\bar{\rho}$ is absolutely irreducible and G satisfies the finiteness condition that, for every open subgroup H, the maximal pro-p quotient of H is topologically finitely generated. That is, there is an equivalence class of representations $[\xi]$ to some ring $\mathscr{R}_{\bar{\rho}}$ that is universal. When working with number fields, these conditions are not restrictive, because $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, where $\mathbb{Q}_S$ is the maximal Galois extension of $\mathbb{Q}$ that is unramified off the finite set of primes S, possesses this finiteness condition, and representations constructed "geometrically" only ramify at a finite set of primes. This is not the case for the representations constructed by Drinfeld modules. Hayes proved that if $\mathbf{K}$ is the maximal abelian extension of $\mathbb{F}_p(T)$ unramified outside the set of places $\{T, \infty\}$, and only tamely ramified at ∞, the group $\mathrm{Gal}(\mathbf{K}/\mathbb{F}_q(T))$ is isomorphic to $\mathbb{F}_q[[T]]^*$ [6], whose maximal pro-p quotient is *not* finitely generated (this is Lemma 25 when $q = p$). Recently de Smit and Lenstra

[3] found an explicit construction for Mazur's universal deformation ring. Their approach constructs a ring, and only uses the finiteness condition to verify that the ring is noetherian, rather than simply an object in $\mathsf{C}(\mathcal{O})$. As a consequence, we know that absolutely irreducible representations of $\mathrm{Gal}(\mathbf{K}_S/\mathbf{K})$ have universal deformation rings.

We can see this rather easily for a one dimensional representation. The proof of de Smit and Lenstra is a careful and thoughtful generalization of this construction.

PROPOSITION 3. *Let G be a profinite group, and let $\bar{\rho}$ be a continuous homomorphism*

$$\bar{\rho}: G \to \mathbf{F}^*$$

where $\mathbf{F}$ is finite. Let $\mathcal{O}$ be any complete noetherian local ring with residue field $\mathbf{F}$. Then Mazur's functor A is representable.

Proof. The proof in [1, Section 1.5] was written for the case where G satisfied the finiteness condition and for the subcategory of noetherian $\mathcal{O}$-algebras, but it proves the more general result. We will outline the construction of the universal deformation.

Let P be the maximal abelian pro-p quotient of G. Let Λ be the ring

$$\Lambda = \mathcal{O}[[P]] = \varprojlim \mathcal{O}[P/H]$$

where the inverse limit is taken over the set of open subgroups H of P. We can construct the representation $\xi: G \to \Lambda^*$ as a product of two representations. First, let ρ_0 be the composition of $\bar{\rho}$ with the Teichmüller lift $\mathbf{F}^* \hookrightarrow \mathcal{O}^*$. Let $\pi: G \to P$ be the natural surjection. Thus $\xi(g) = \rho_0(g)\,\pi(g)$ defines the map $G \to \Lambda^*$.

Let $\rho: G \to \mathscr{R}^*$ be a continuous lift of $\bar{\rho}$ to $\mathscr{R}$, an object in $\mathsf{C}(\mathcal{O})$. The natural map $\mathscr{R}^* \to \mathbf{F}^*$ splits, because we have the map

$$\mathbf{F}^* \hookrightarrow \mathcal{O}^* \to \mathscr{R}^*.$$

Thus $\mathscr{R}^* \cong \mathbf{F}^* \times \Gamma_1(\mathscr{R})$. We have a continuous map $G \to \Gamma_1(\mathscr{R})$ which factors through P since $\Gamma_1(\mathscr{R})$ is an abelian pro-p group (see Lemma 4). The ring $\mathscr{R}$ is also an $\mathcal{O}$-algebra, hence there is a canonical ring homomorphism $\mathcal{O} \to \mathscr{R}$. These two maps define the homomorphism $p_{\mathscr{R}}: \Lambda \to \mathscr{R}$ so that $\rho = p_{\mathscr{R}} \cdot \xi$. ∎

We end this section with two lemmas that will be important later.

LEMMA 4. *For any object $\mathscr{R}$ in $\mathsf{C}(\mathcal{O})$, the group $\Gamma_r(\mathscr{R})$ is a pro-p group.*

Proof. The case where $\mathscr{R}$ is an artinian ring (in fact, where $\mathscr{R}$ is noetherian) is handled in [2, Lemma 1.2]. In fact, when $\mathscr{R}$ is artinian, the same proof shows that $\Gamma_r(\mathscr{R})$ is a finite p-group. Now suppose that $\mathscr{R}$ is an arbitrary object in $\mathsf{C}(\mathscr{R})$, so that $\mathscr{R}$ is isomorphic to $\varprojlim \mathscr{R}/I$ where I runs through the open ideals for which the quotient $\mathscr{R}/I$ is artinian. One can check that $\Gamma_r(\mathscr{R})$ is isomorphic to $\varprojlim \Gamma_r(\mathscr{R}/I)$, a projective limit of finite p-groups, i.e., a pro-p group. ∎

LEMMA 5. *If U is an abelian pro-p group, then $\mathbf{F}[[U]]$ (defined in the proof of Proposition 3) is an object in $\mathsf{C}(\mathscr{O})$ where $\mathscr{O}$ is a complete noetherian local ring with residue field $\mathbf{F}$ and the natural map of U to $\Gamma_1(\mathbf{F}[[U]])$ is injective.*

Proof. The ring $\mathbf{F}[[U]]$ is by definition a projective limit of the rings $\mathbf{F}[U/V]$ for all open subgroups V of finite index. Each of the rings $\mathbf{F}[U/V]$ has the discrete topology, is finite (hence artinian), and is local, since the augmentation ideal is the only maximal ideal (to see this, let $\alpha = \sum_{x \in U/V} a_x x$ for which $\sum a_x = 0$, and check that $(1+\alpha)^{p^e} = 1$ for some nonnegative integer e). To define the $\mathscr{O}$-algebra structure, we simply define

$$\mathscr{O} \to \mathscr{O}/\wp_{\mathscr{O}} \cong \mathbf{F} \hookrightarrow \mathbf{F}[[U]].$$

Finally, define the homomorphism $U \to \Gamma_1(\mathbf{F}[[U]])$ by $x \mapsto x$, since

$$x = 1 + (1-x) \in (1 + \wp_{\mathbf{F}[[U]]}).$$

This is obviously injective. ∎

2. ABELIAN PRO-P EXTENSIONS

2.1. *Artin–Schreier extensions.* For any commutative ring $\mathscr{R}$ of characteristic p, let $\mathscr{P}: \mathscr{R} \to \mathscr{R}$ be defined by $\mathscr{P}(x) = x^p - x$. We notice that the polynomial map $\mathscr{P}$ is an $\mathbb{F}_p$-linear map with kernel $\mathbb{F}_p$, when $\mathscr{R}$ is a domain.

As a first step, we recall some facts about extensions of degree p of fields of characteristic p, including the usual theorem of Artin–Schreier. (See [9, Proposition 7.8 of Chapter V].)

THEOREM 6. *Let $\mathbf{K}$ be a field of characteristic p. The extension $\mathbf{L}/\mathbf{K}$ is cyclic of degree p if and only if $\mathbf{L}$ is the splitting field over $\mathbf{K}$ of an irreducible polynomial of the form $\mathscr{P}(x) - a \in \mathbf{K}[x]$, in which case $\mathbf{L} = \mathbf{K}(\alpha)$ where α is a root of $\mathscr{P}(x) - a = 0$. Also another equation over $\mathbf{K}$, $\mathscr{P}(x) - b$, has the same splitting field if and only if, for some nonzero $i \in \mathbb{F}_p$ and $y \in \mathbf{K}$, $b = ia + \mathscr{P}(y)$.*

2.2. *Witt extensions.* In this section, we recall the definition of Witt vectors, and how they are used to characterize abelian p-power extensions of fields of characteristic p. We refer the reader to standard texts, such as Jacobson's *Basic Algebra II* [10, Section 8.10 and Section 8.11] for the definitions of addition and multiplication in $W_m(\mathscr{R})$, as well as the proofs of the various facts and equations that we quote throughout this section.

2.2.1. *Witt vectors.* We recall the definition of the Witt functor of length n from the category of commutative rings of characteristic $p>0$ to the category of commutative rings of characteristic p^n. As a set, the ring of Witt vectors over $\mathscr{R}$ is simply the n-dimensional Cartesian product $\mathscr{R}^n$, usually indexed by the set $\{0, 1, ..., n-1\}$. Please refer to [10, Section 8.10] for the definitions of addition, multiplication and the action of W_n on ring homomorphisms. We will only note that $(0, ..., 0)$ is the zero element, $(1, 0, ..., 0)$ is the multiplicative identity, and that the ith coordinate of $(a_0, ..., a_{n-1}) + (b_0, ..., b_{n-1})$ is

$$a_i + b_i + F_{p,i}(a_0, ..., a_{i-1}, b_0, ..., b_{i-1})$$

where $F_{p,i}$ is a polynomial with integer coefficients and zero constant term that depends only on p and i.

Three important maps on rings of Witt vectors are the following.

Restriction map: R: $W_n\mathscr{R} \to W_{n-1}\mathscr{R}$ via $(a_0, ..., a_{n-1}) \mapsto (a_0, ..., a_{n-2})$.

Shift map: V: $W_n\mathscr{R} \to W_{n+1}\mathscr{R}$ via $(a_0, ..., a_{n-1}) \mapsto (0, a_0, ..., a_{n-1})$.

Frobenius map: $\mathscr{F}$: $W_n\mathscr{R} \to W_n\mathscr{R}$ via $(a_0, ..., a_{n-1}) \mapsto (a_0^p, ..., a_{n-1}^p)$.

The restriction and Frobenius maps are ring homomorphisms, but the shift map is only a homomorphism of the additive group structure. All three maps commute with each other. Note that (VR) is an endomorphism of the additive group of $W_n\mathscr{R}$ whose effect on $(a_0, ..., a_{n-1})$ is $(0, a_0, ..., a_{n-2})$, so $(VR)^n$ is the zero map on $W_n(\mathscr{R})$.

2.2.2. *Abelian p-power extensions.* Now we recall the characterization of abelian pro-p extensions in terms of additive subgroups of rings of Witt vectors. As before, we refer the reader to [10, Section 8.11] for the proofs of these facts. First we extend the definition of $\mathscr{P}$ to a map on $W_n\mathscr{R}$, defined by $\mathscr{P} = \mathscr{F} - I$, where I is the identity map. That is,

$$\mathscr{P}(a_0, ..., a_{n-1}) = (a_0^p, ..., a_{n-1}^p) - (a_0, ..., a_{n-1}).$$

Let $\mathbf{L}/\mathbf{K}$ be an extension of fields of characteristic $p>0$, with Galois group G, an abelian group of exponent p^e. Let $m \geqslant e$ be an integer, and define

$$SW_m\mathbf{L} = \{l \in W_m\mathbf{L} \mid \mathscr{P}(l) \in W_m\mathbf{K}\}.$$

This is a subgroup of the additive group $W_m\mathbf{L}$ that contains $W_m\mathbf{K}$. The usual proof shows that there is an epimorphism from $SW_m\mathbf{L}$ to

$$\hat{G} := \{\text{continuous bounded homomorphisms of } G \text{ into } \mathbb{C}^*\}$$

(the character group of G). The kernel of this epimorphism is $W_m\mathbf{K}$.

If G is cyclic of degree p^e, and $l = (l_0, ..., l_{m-1})$ maps to a generator of $\hat{G}$, then $\mathbf{L} = \mathbf{K}(l_0, ..., l_{m-1})$, and $\mathbf{K}(l_0, ..., l_j)/\mathbf{K}(l_0, ..., l_{j-1})$ is either trivial or is an Artin–Schreier extension satisfying $\mathscr{P}(l_j) = k_j + m_{j-1}$, where k_i is the ith coordinate of $k = \mathscr{P}(l)$, and m_{j-1} is the element of $\mathbf{K}(l_0, ..., l_{j-1})$ from the definition of subtraction in $W_m\mathscr{R}$.

Back to the more general situation, where $\mathbf{L}/\mathbf{K}$ is an abelian p-power extension of exponent p^e, and $m \geqslant e$, we set $QW_m\mathbf{L} = \mathscr{P}SW_m\mathbf{L} \subset W_m\mathbf{K}$. We now have $QW_m\mathbf{L}/\mathscr{P}W_m\mathbf{K} \cong \hat{G}$, a characterization of $\mathbf{L}/\mathbf{K}$ solely in terms of $\mathbf{K}$. Finally, there is a converse theorem, which says that any subgroup Q of $W_m\mathbf{K}^+$ that contains $\mathscr{P}W_m\mathbf{K}$ as a subgroup of finite index is $QW_m\mathbf{L}$ for some abelian p-power extension $\mathbf{L}$ of exponent p^e, where $e \leqslant m$.

2.3. *Ramification.* When we restrict our attention to extensions of algebraic function fields over $\mathbb{F}_p$, then we can say more about which places ramify in the extension. The following proposition is simply a restatement of parts of [15, Lemma III.7.7 and Proposition III.7.8].

PROPOSITION 7. *Let* $\mathbf{K}$ *be an algebraic function field of characteristic* $p > 0$, *and* $\mathbf{L}$ *be an Artin–Schreier extension of* $\mathbf{K}$ *as in Theorem* 6, *where* $\mathbf{L}$ *is the splitting field over* $\mathbf{K}$ *of* $\mathscr{P}(x) - a$. *Let* P *be a place of* $\mathbf{K}$. *Then either*

1. P *is unramified in* $\mathbf{L}$ *if and only if* $a \in \mathscr{P}\mathbf{K} + \mathcal{O}_P$; *or*
2. P *is totally ramified in* $\mathbf{L}$ *if and only if* $a \notin \mathscr{P}\mathbf{K} + \mathcal{O}_P$.

We may extend this to abelian p-power extensions, by keeping track of the ramification information in each of the Artin–Schreier subextensions. Using the notation as in subsection 2.2.2, we have the following lemma.

LEMMA 8. *Let* $\mathbf{L} = \mathbf{K}(\alpha_0, ..., \alpha_{m-1})$ *be an extension of the function field* $\mathbf{K}$ *such that*

$$\mathscr{P}(\alpha_0, ..., \alpha_{m-1}) = (a_0, ..., a_{m-1}),$$

where $a_i \in \mathbf{K}$. *Let* P *be a place of* $\mathbf{K}$. *Then* P *ramifies in* $\mathbf{L}$ *if and only if*

$$(a_0, ..., a_{m-1}) \notin \mathscr{P}W_m\mathbf{K} + W_m\mathcal{O}_P.$$

Proof. For a choice of $z \in W_m\mathbf{K}$ to be made later, let $\beta = \alpha + z$ and $\mathscr{P}(\beta) = b$. Let $\mathbf{L}_1 = \mathbf{K}(\alpha_0) = \mathbf{K}(\beta_0)$ and $\mathbf{L}_{i+1} = \mathbf{L}_i(\alpha_i) = \mathbf{L}_i(\beta_i)$ for $1 \leqslant i < m$. Also, let P_i be any place of $\mathbf{L}_i$ that lies over P_{i-1}, where $P_0 = P$.

Choose $z \in W_m\mathbf{K}$, if possible, so that $b = a + \mathscr{P}(z) \in W_m\mathcal{O}_P$. We will show that the ramification index of P_{i+1} over P_i is one for each i, implying that P is unramified in $\mathbf{L}$. First, P is unramified in $\mathbf{L}_1$ by Proposition 7 since β_0 has minimal polynomial $f(X) = \mathscr{P}(X) - b_0 \in \mathcal{O}_P[X]$ and $f'(X) = -1$. Notice also that $\{1, \beta_0, ..., \beta_0^{p-1}\}$ is an integral basis for $\mathbf{L}_1/\mathbf{K}$, by [15, Corollary III.5.11]. Hence we may assume that P is unramified in $\mathbf{L}_i$ and that $\{1, \beta_{i-1}, ..., \beta_{i-1}^{p-1}\}$ is an integral basis for $\mathbf{L}_i/\mathbf{L}_{i-1}$. The minimal polynomial for β_i over $\mathbf{L}_i$ is $f(X) = \mathscr{P}(X) - b_i - \mu$, where μ is a polynomial with integer coefficients in $\{\beta_0, ..., \beta_{i-1}\}$. Hence $\mu \in \mathcal{O}_{P_i}$, and thus $f(X) \in \mathcal{O}_{P_i}[X]$. Since $f'(X) = -1$, [15, Corollary III.5.11] again tells us that $P_{i+1} \mid P_i$ is unramified and that $\{1, \beta_i, ..., \beta_i^{p-1}\}$ is an integral basis. Thus by induction, P is unramified in $\mathbf{L}$.

Conversely, assume that $(a_0, ..., a_{m-1}) \notin \mathscr{P}W_m\mathbf{K} + W_m\mathcal{O}_P$. Let i be the maximal nonnegative integer for which $(a_0, ..., a_{i-1}) \in \mathscr{P}W_i\mathbf{K} + W_i\mathcal{O}_P$, and choose $(z_0, ..., z_{i-1}) \in W_i\mathbf{K}$ such that $(a_0, ..., a_{i-1}) + (z_0, ..., z_{i-1}) \in W_i\mathcal{O}_P$. The ith coordinate of $(a_0, ..., a_i) + (z_0, ..., z_{i-1}, 0)$ is $a_i + Z$ for some $Z \in \mathbf{K}$. By [15, Lemma III.7.7] there is a $z_i \in \mathbf{K}$ for which $v_P(a_i + Z + \mathscr{P}(z_i)) = -m < 0$ and $\gcd(m, p) = 1$. Let $z = (z_0, ..., z_i) \in W_{i+1}\mathbf{K}$, $(\beta_0, ..., \beta_i) = (\alpha_0, ..., \alpha_i) + z$, and $(b_0, ..., b_i) = \mathscr{P}(\beta_0, ..., \beta_i)$. From above, P is unramified in $\mathbf{L}_i$ and that $\{\beta_0, ..., \beta_{i-1}\}$ are integral over $\mathcal{O}_P$. The extension $\mathbf{L}_{i+1}/\mathbf{L}_i$ is an Artin–Schreier extension, generated by β_i. The minimal polynomial for β_i is $f(X) = \mathscr{P}(X) - b_i - \gamma$, where γ is a polynomial with integer coefficients in $\{\beta_0, ..., \beta_{i-1}\}$. Thus

$$v_{P_i}(b_i + \gamma) = v_{P_i}(b_i) = v_P(b_i) = -m < 0,$$

where $\gcd(m, p) = 1$. Hence, $b_i + \gamma \notin \mathscr{P}\mathbf{L}_i + \mathcal{O}_{P_i}$, by [15, Lemma III.7.7], P_i ramifies in $\mathbf{L}_{i+1}$, and thus P ramifies in $\mathbf{L}$. ∎

As a result, an abelian p-power extension $\mathbf{L}/\mathbf{K}$ is unramified at every place in a set T if and only if $(a_0, ..., a_{m-1}) \in \bigcap_{P \in T}(W_m\mathcal{O}_P + \mathscr{P}W_m\mathbf{K})$. The next proposition characterizes the additive subgroup of $W_m\mathbf{K}$ formed by this intersection.

PROPOSITION 9. *If T is a set of places of $\mathbf{K}$ that does not contain every place, then*

$$W_m\mathcal{O}_T + \mathscr{P}W_m\mathbf{K} = \bigcap_{P \in T}(W_m\mathcal{O}_P + \mathscr{P}W_m\mathbf{K}).$$

Proof. Since $\mathcal{O}_T = \bigcap_{P \in T}\mathcal{O}_P$, one inclusion is immediate. To show the other inclusion, we shall first assume $m = 1$. Let $a \in \bigcap_{P \in T}(\mathcal{O}_P + \mathscr{P}\mathbf{K})$. As a has only finitely many poles, let $P_1, ..., P_r$ be the poles of a that lie in T. Let v_i be the corresponding normalized valuation for P_i. By [15, Lemma III.7.7], $v_i(a) = -pl_i$ for some positive integer l_i, since we know that for

some $z \in \mathbf{K}$, $v_i(a + \mathscr{P}(z)) \geqslant 0$. Using the strong approximation theorem, we can find t, $y \in \mathbf{K}$ for which $v_i(t) = -l_i$ and $v_i(y) = 0$ for every $i = 1, ..., r$ and $v_P(t) \geqslant 0$ and $v_P(y) \geqslant 0$ for every $P \in T - \{P_1, ..., P_r\}$. One can check that $v_i(a + \mathscr{P}(yt)) > -pl_i$ for each i and that $v_P(a + \mathscr{P}(yt)) \geqslant 0$ for every $P \in T - \{P_1, ..., P_r\}$. Set $a_1 = a + \mathscr{P}(yt)$, and notice that the poles of a_1 that are contained in T are in fact contained in the set $\{P_1, ..., P_r\}$, and the order of the pole of a_1 at P_i is less than the order of the pole of a at P_i. Inductively define a_i so that the poles of a_i that are in T are in $\{P_1, ..., P_r\}$ with orders less than the orders of the poles of a_{i-1}. In at most $\max\{l_j\}$ steps, we will have found an element $z \in \mathbf{K}$ for which $v_P(a + \mathscr{P}(z)) \geqslant 0$ for every $P \in T$. Hence $a + \mathscr{P}(z) \in \mathscr{O}_T$, so $a \in \mathscr{O}_T + \mathscr{P}\mathbf{K}$.

To prove the full generality, suppose $(a_0, ..., a_{m-1}) \in \bigcap_{P \in T} (W_m \mathscr{O}_P + \mathscr{P} W_m \mathbf{K})$, and, if possible, choose j minimally so that

$$(a_0, ..., a_j) + \mathscr{P}(z_0, ..., z_j) \notin W_{j+1} \mathscr{O}_T + \mathscr{P} W_{j+1} \mathbf{K}$$

for every $z_i \in \mathbf{K}$. By the minimality of j, we know that there exists $(z_0, ..., z_{j-1})$ such that $(a_0, ..., a_{j-1}) + (z_0, ..., z_{j-1}) \in W_j \mathscr{O}_T$. Let

$$(b_0, ..., b_j) = (a_0, ..., a_j) + \mathscr{P}(z_0, ..., z_{j-1}, 0).$$

Now b_j has poles $\{P_1, ..., P_r\} \subseteq T$ (and perhaps some poles that are not in T). By the previous paragraph, we may find a $z_j \in \mathbf{K}$ such that $v_P(b_j + \mathscr{P}(z_j)) \geqslant 0$ for every $P \in T$. Hence,

$$(a_0, ..., a_j) + \mathscr{P}(z_0, ..., z_j) \in W_{j+1} \mathscr{O}_T,$$

contradicting the minimality of j. Hence the two subgroups are equal. ∎

As any place that ramifies in a finite abelian p-power extension must ramify in one of its cyclic subextensions, we have the following theorem.

THEOREM 10. *Let* $\mathbf{L}/\mathbf{K}$ *be a finite abelian p-power extension of exponent dividing* p^m, *and let* $QW_m\mathbf{L}$ *be the subgroup of* $W_m\mathbf{K}$ *that contains* $\mathscr{P}W_m\mathbf{K}$, *as in Section* 2.2.2. *Let* T *be a set of places of* $\mathbf{K}$. *If every place of* $\mathbf{K}$ *that lies in* T *is unramified in* $\mathbf{L}$, *then* $QW_m\mathbf{L} \subset \bigcap_{P \in T} (W_m \mathscr{O}_P + \mathscr{P} W_m \mathbf{K})$. *Conversely, any additive subgroup* Q *of* $\bigcap_{P \in T} (W_m \mathscr{O}_P + \mathscr{P} W_m \mathbf{K})$ *that contains* $\mathscr{P}W_m\mathbf{K}$ *with finite index corresponds to an abelian p-power field extension in which no place in the set* T *ramifies.*

2.4. *Galois correspondence.* Let $\mathbf{K}$ be a function field, S a set of places of $\mathbf{K}$, and T the complement of S. Let

$$X_{\mathbf{K}, S, m} = \left(\bigcap_{P \in T} W_m \mathscr{O}_P + \mathscr{P} W_m \mathbf{K} \right) \Big/ \mathscr{P} W_m \mathbf{K},$$

where we understand that if T is empty, $X_{\mathbf{K},S,m} = W_m\mathbf{K}/\mathscr{P}W_m\mathbf{K}$. Theorem 10 says that the finite subgroups of $X_{\mathbf{K},S,m}$ are in a one-to-one correspondence with the finite abelian p-power extensions of $\mathbf{K}$ with exponent dividing p^m and whose ramified places lie in the set S. To characterize all abelian p-power extensions (in fact, all abelian pro-p extensions), we need to glue these sets together. The key is that every finite subgroup Q of $X_{\mathbf{K},S,m}$ is canonically isomorphic to the character group of a Galois group for some extension $\mathbf{L}/\mathbf{K}$. Suppose $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$ is a tower of fields, unramified at each place of $\mathbf{K}$ that is not in S, and so that $\widehat{\mathrm{Gal}}(\mathbf{M}/\mathbf{K})$ is a finite abelian p-group of exponent dividing p^m. Suppose also that $Q_{\mathbf{L}}$ and $Q_{\mathbf{M}}$ are the corresponding subgroups of $X_{\mathbf{K},S,m}$. The natural surjection $\mathrm{Gal}(\mathbf{M}/\mathbf{K}) \to \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ induces a natural injection on character groups $\widehat{\mathrm{Gal}}(\mathbf{M}/\mathbf{K}) \to \widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K})$. Since $Q_{\mathbf{L}}$ is canonically isomorphic to $\widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K})$, we have $Q_{\mathbf{L}} \hookrightarrow Q_{\mathbf{M}}$, where the monomorphism is simply the inclusion map. Thus when dealing with finite extensions of $\mathbf{K}$, all of whose exponents divide p^m, it suffices to deal with Witt vectors of length m.

The following lemma pieces together Witt characterizations of different lengths.

LEMMA 11. *The homomorphism* $V\colon W_m\mathbf{K} \hookrightarrow W_{m+1}\mathbf{K}$ *induces a monomorphism of additive groups*

$$X_{\mathbf{K},S,m} \hookrightarrow X_{\mathbf{K},S,m+1}.$$

Proof. Consider $(W_m\mathscr{O}_T + \mathscr{P}W_m\mathbf{K}) \xrightarrow{\bar{V}} X_{\mathbf{K},S,m}$, and let $a = (a_0, ..., a_{m-1})$ be an element of the kernel of this map. Then

$$V(a) = (0, a_0, ..., a_{m-1}) = \mathscr{P}(b_0, ..., b_m).$$

Thus $\mathscr{P}(b_0) = 0$, implying that $b_0 \in \mathbb{F}_p$. Notice that

$$(b_0, ..., b_m) - (b_0, 0, ..., 0) = (0, c_1, ..., c_m) \in W_{m+1}\mathbf{K},$$

so $\mathscr{P}(0, c_1, ..., c_m) = (0, a_0, ..., a_{m-1})$. Since V and $\mathscr{P}$ commute,

$$\mathscr{P}V(c_1, ..., c_m) = \mathscr{P}(0, c_1, ..., c_m) = V(a)$$

implies that $a = \mathscr{P}(c_1, ..., c_m) \in \mathscr{P}W_m\mathbf{K}$. ∎

Thus $\{X_{\mathbf{K},S,m}, \bar{V}\}$ forms a direct system, and we let $X_{\mathbf{K},S}$ be its direct limit. We may refer to elements of $X_{\mathbf{K},S}$ by a representative Witt vector whose first coordinate is *not* in $\mathscr{P}\mathbf{K}$. We now have justified the following proposition.

PROPOSITION 12. *There is an inclusion-preserving, bijective correspondence between the set of finite abelian p-power extensions of* $\mathbf{K}$ *unramified outside* S *and the set of finite subgroups of* $X_{\mathbf{K},S}$ *given by* $\mathbf{L} \mapsto [Q_{\mathbf{L}}]$. *Also, for each extension* $\mathbf{L}/\mathbf{K}$, *the corresponding* $Q_{\mathbf{L}}$ *is naturally isomorphic to* $\widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K})$.

2.5. *Functoriality.* As the preceding characterizations of abelian p-power extensions involved character groups, we need an important fact about the character functor: on the category of locally compact abelian groups, the character functor is fully faithful. This may be proved using the duality theorem of Pontryagin and Van Kampen [8, Theorem 24.8].

Let $\mathbf{K}$ be an algebraic function field with characteristic p and let S be a set of places of $\mathbf{K}$. We will define two functors from the category of abelian pro-p groups to the category of sets. Define $C(*) := \hom(G_{\mathbf{K},S}, *)$, where $G_{\mathbf{K},S}$ is the Galois group of the maximal unramified Galois extension of $\mathbf{K}$ that is unramified outside S, and where the homomorphisms are understood to be continuous homomorphisms of profinite groups. The other functor $D(*) := \hom(\hat{*}, X_{\mathbf{K},S})$, where $X_{\mathbf{K},S}$ is defined in Section 2.4.

Let U be an abelian pro-p group, and let $\rho \in C(U)$. In the category of profinite groups, monomorphisms are injective and epimorphisms are surjective (the proofs are essentially as for groups, see [10, Proposition 1.1]). Thus ρ factors as $m_\rho e_\rho$, an epimorphism followed by a monomorphism. Let $G = e_\rho(G_{\mathbf{K},S})$, which is a quotient of $G_{\mathbf{K},S}$, hence $G \cong \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ for some $\mathbf{L}$. Now

$$\{\mathbf{N} \mid \mathbf{N}/\mathbf{K} \text{ is finite subextension of } \mathbf{L}/\mathbf{K}\}$$

is a direct system, ordered by inclusion. Proposition 12 says this corresponds to a direct system (with the same index set) of finite subgroups $Q_{\mathbf{N}}$ of $X_{\mathbf{K},S}$. Let $Q_{\mathbf{L}} = \varinjlim Q_{\mathbf{N}}$. Notice that $\{\widehat{\mathrm{Gal}}(\mathbf{N}/\mathbf{K})\}$ also forms a direct system, isomorphic to $\{Q_{\mathbf{N}}\}$, and hence that

$$\widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K}) \cong \varinjlim \widehat{\mathrm{Gal}}(\mathbf{N}/\mathbf{K}) \cong Q_{\mathbf{L}}.$$

For notation, let $j_{\mathbf{L}}$ be the isomorphism from $\widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K})$ to $Q_{\mathbf{L}}$, and let $i_{\mathbf{L}}$ be the inclusion of $Q_{\mathbf{L}}$ into $X_{\mathbf{K},S}$. Also recall that the character functor on abelian pro-p groups is exact. Thus we can define the natural transformation η on objects by $\eta_U(\rho) = i_{\mathbf{L}} j_{\mathbf{L}} \widehat{m_\rho}$. Now let $f\colon U \to V$ be a homomorphism of abelian pro-p groups. Thus we have a map $C(f)\colon C(U) \to C(V)$ defined by $\rho \mapsto f\rho$. And we have $D(f)$ defined by $\alpha \mapsto \alpha \hat{f}$. Thus $D(f)(\eta_U(\rho)) = D(f)(i_{\mathbf{L}} j_{\mathbf{L}} \widehat{m_\rho}) = i_{\mathbf{L}} j_{\mathbf{L}} \widehat{m_\rho} \hat{f}$ and $\eta_V(C(f)) = \eta_V(f_\rho) = i_{\mathbf{M}} j_{\mathbf{M}} \widehat{m_{f\rho}}$, where $\mathbf{M}$ is the fixed field of the kernel of $f\rho$. Upon examining the following diagram, we see it commutes.

$$\begin{array}{ccccccc}
\hat{V} & \xrightarrow{\widehat{m_{fp}}} & \widehat{\mathrm{Gal}}(\mathbf{M}/\mathbf{K}) & \xrightarrow{j_{\mathbf{M}}} & Q_{\mathbf{M}} & \xrightarrow{i_{\mathbf{M}}} & X_{\mathbf{K},S} \\
\downarrow{\scriptstyle \hat{f}} & & \downarrow & & \downarrow & & \downarrow \\
\hat{U} & \xrightarrow{m_p} & \widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K}) & \xrightarrow{j_{\mathbf{L}}} & Q_{\mathbf{L}} & \xrightarrow{i_{\mathbf{L}}} & X_{\mathbf{K},S}
\end{array}$$

The leftmost rectangle commutes by the functoriality of the character functor, the middle rectangle commutes by the Galois correspondence, and the right rectangle commutes since the arrows are inclusions of subgroups, and the rightmost vertical arrow is an equality. Hence η is a natural transformation from C to D.

THEOREM 13. *The natural transformation η is an equivalence of functors.*

Proof. To show it is an isomorphism, we construct an inverse. To do this, we use the Duality Theorem [8, Theorem 24.8]. Given a map $g\colon \hat{V} \to \hat{U}$, and $\alpha \in D(U)$, we have the image of $\alpha(\hat{U}) = Q_{\mathbf{L}}$ and $\alpha g(\hat{V}) = Q_{\mathbf{M}}$. These respectively are canonically isomorphic to $\widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K})$ and $\widehat{\mathrm{Gal}}(\mathbf{M}/\mathbf{K})$, so we have

$$\begin{array}{ccc}
\hat{V} & \xrightarrow{\alpha g} & \widehat{\mathrm{Gal}}(\mathbf{M}/\mathbf{K}) \\
{\scriptstyle g}\downarrow & & \downarrow \\
\hat{U} & \xrightarrow[\alpha]{} & \widehat{\mathrm{Gal}}(\mathbf{L}/\mathbf{K}).
\end{array}$$

Applying the character functor, and the natural isomorphism of the duality theorem, we have

$$\begin{array}{ccc}
V & \longleftarrow & \mathrm{Gal}(\mathbf{M}/\mathbf{K}) \\
\uparrow & & \uparrow \\
U & \longleftarrow & \mathrm{Gal}(\mathbf{L}/\mathbf{K}).
\end{array}$$

To define the inverse, compose the natural map $G_{\mathbf{K},S} \to \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ with the maps in the $\hat{\alpha}$ and $\widehat{\alpha g}$. ∎

3. DEFORMATIONS ASSOCIATED TO DRINFELD MODULES

We examine specific cases of deformations of a fixed Galois representation $\bar{\rho}\colon G \to \mathbb{F}_p^*$ where G is either the absolute Galois group of a local function field $\mathbf{K}$, or the Galois group of the maximal Galois extension of a global function field $\mathbf{K}$ unramified outside a set of places S. We will use the notation $\mathbf{K}_S$ to denote both the algebraic closure of a local function field, or the

maximal Galois extension unramified outside the set of places S. Using the theory of Section 2, we explore which deformations are the G-actions on the division points of Drinfeld modules over $\mathbf{K}$. Throughout the chapter, we will focus on deformations to $\mathscr{R} = \mathbb{F}_p[T]/(T^n)$ for $n > 0$ and to $\mathscr{R} = \varprojlim \mathbb{F}_p[T]/(T^n) \cong \mathbb{F}_p[[T]]$. A rank one Drinfeld $\mathbb{F}_p[T]$-module over $\mathbf{K}$ produces representations to these rings by the action of G on its (T^n)-division points, or on its (T)-adic Tate module.

3.1. *Isolating the pro-p part.* Recall subsection 1.2, and let $\mathscr{R}$ be an object in the category $\mathsf{C}(\mathscr{O})$ where $\mathscr{O}$ has residue field $\mathbb{F}_p$. The exact sequence,

$$1 \to U \to \mathscr{R}^* \xrightarrow{\pi_{\mathscr{R}}} \mathbb{F}_p^* \to 1$$

where $\pi_{\mathscr{R}}$ is induced by reduction modulo the maximal ideal, splits via a Teichmüller lifting (in subsection 1.2, we used the notation $\Gamma_1(\mathscr{R})$ rather than U). Thus

$$\mathscr{R}^* \cong \mathbb{F}_p^* \times U.$$

Let θ be the projection of $\mathscr{R}^*$ onto U, and recall that U is an abelian pro-p group (Lemma 4).

If ρ is a continuous homomorphism of G to $\mathscr{R}^*$ that lifts $\bar{\rho}$ we have a continuous homomorphism $\rho' = \theta \cdot \rho \colon G \to U$. Conversely a continuous homomorphism

$$\rho' \colon G \to U$$

can be used to define a deformation $\rho \colon G \to \mathscr{R}^*$ by setting $\rho(g) = \bar{\rho}(g) \cdot \rho'(g)$ for every $g \in G$. In this manner we will transfer questions about one dimensional representations to questions about abelian pro-p extensions, for which we have the results of Section 2.

3.2. *Representations produced by Drinfeld modules.* We will now restrict our attention to the case where $\mathscr{A}$ is the polynomial ring $\mathbb{F}_p[T]$. Let ϕ be a rank one Drinfeld $\mathscr{A}$-module over $\mathbf{K}$, a global or local function field, where ϕ is defined by $\phi_T = a\mathscr{F} + b$ for $a, b \in \mathbf{K} - \{0\}$, hence $\gamma(T) = b \neq 0$ and the characteristic of ϕ is not (T). Let P be a monic irreducible polynomial in $\mathscr{A}$, relatively prime to the characteristic of ϕ. Then for each $n > 0$, $\phi_P \colon \phi[P^{n+1}] \to \phi[P^n]$ is a surjective map of cyclic $\mathscr{A}$-modules. We can choose a generator λ_n of each $\phi[P^{n+1}]$ $(n \geqslant 0)$ so that $\phi_P(\lambda_{n+1}) = \lambda_n$.

Now we will restrict our attention further to the case where $P = T$. Then $\phi_T(x) = ax^p + bx$, so the (T)-division points are 0 and the solutions of the Kummer equation $x^{p-1} = -b/a$. The action of G on $\phi[T]$ produces a representation

$$\rho_T \colon G \to \operatorname{Aut} \phi[T] \cong \mathbb{F}_p^*.$$

Let $n>0$. We notice that $\phi_T(\lambda_n)=a\lambda_n^p+b\lambda_n=\lambda_{n-1}$. Dividing by $a\lambda_0^p$ yields

$$\left(\frac{\lambda_n}{\lambda_0}\right)^p+\frac{b}{a\lambda_0^{p-1}}\left(\frac{\lambda_n}{\lambda_0}\right)=\frac{1}{a\lambda_0^{p-1}}\left(\frac{\lambda_{n-1}}{\lambda_0}\right). \tag{3.1}$$

Let $x_n=\lambda_n/\lambda_0$ and $c=-1/b$, and recall that $\lambda_0^{p-1}=-b/a$. This reduces (3.1) to

$$x_n^p-x_n=cx_{n-1}. \tag{3.2}$$

In this way, $\mathbf{K}(\phi[T^{n+1}])/\mathbf{K}(\phi[T^n])$ is an Artin–Schreier extension for each $n\geqslant 1$. A standard tool in what follows will be the following hypothesis.

HYPOTHESIS 14. *Let*

$$\mathbf{K}=\mathbf{K}_0\subset\mathbf{K}_1\subset\cdots\subset\mathbf{K}_n\subset\cdots$$

be a tower of field extensions where, for a fixed $c\in\mathbf{K}$, $x_0=1\in\mathbf{K}$ *and, for* $n>0$, x_n *is a root of* $\mathscr{P}(x)-cx_{n-1}$ *and* $\mathbf{K}_n=\mathbf{K}_{n-1}(x_n)$.

THEOREM 15. *If* ϕ *is a rank one Drinfeld* $\mathscr{A}$*-module over* $\mathbf{K}$, *and* ρ *is the action of* $G=\mathrm{Gal}(\mathbf{K}_S/\mathbf{K})$ *on* $\phi[T^m]$ *for some* $m\geqslant 1$ (*or on the Tate module* $\mathbf{T}(\phi,(T))$), *then* ρ *is the pointwise product of* $\bar{\rho}\colon G\to\mathbb{F}_p^*$ *and* $\rho'\colon G\to\Gamma_1(\mathscr{R})$ *where* $\mathscr{R}$ *is* $\mathbb{F}_p[T]/(T^m)$ (*or* $\mathscr{A}_{(T)}\cong\mathbb{F}_p[[T]]$, *respectively*), *and the extension of* $\mathbf{K}$ *determined by* ρ' *satisfies Hypothesis* 14.

Proof. See subsection 3.1 for the first statement. The extension determined by ρ' is the tower of splitting fields of the equations (3.2) from above. ∎

We examine the ramification of places in extensions that satisfy Hypothesis 14 in the next theorem, and derive some information about representations constructed by the action of G on the (T)-adic Tate module of ϕ in its corollary.

THEOREM 16. *Let* $\mathbf{K}$ *be a local field of characteristic* p, *and* $c\in\mathbf{K}$. *If Hypothesis* 14 *holds, then, for each* $n>0$, $\mathbf{K}_n/\mathbf{K}$ *is unramified or totally ramified, depending on whether* $c=-1/\gamma(T)\in\mathscr{O}+\mathscr{P}\mathbf{K}$ *or not, respectively.*

Proof. We will prove this by induction, the case $n=1$ being a local version of Proposition 7. Now, according to [15, Lemma III.7.7], we may assume that c is chosen so that either $v(c)\geqslant 0$ or $v(c)=\max_{z\in\mathbf{K}}(v(c+\mathscr{P}(z))=-m$ where m is a positive integer not divisible by p.

If $v(c)\geqslant 0$, then x_1 is in the integral closure $\mathscr{O}_1$ of $\mathscr{O}$ in $\mathbf{K}_1$. Thus $v_1(cx_1)\geqslant 0$ where v_1 is the normalized valuation on $\mathbf{K}_1$. By induction, suppose that $\mathbf{K}_{n-1}/\mathbf{K}$ is unramified and that $x_{n-1}\in\mathscr{O}_{n-1}$. Then, by Proposition 7, we have that $\mathbf{K}_n/\mathbf{K}_{n-1}$, and thus $\mathbf{K}_n/\mathbf{K}$, are unramified.

Now suppose that $v(c) = -m$ is not divisible by p. Again, Proposition 7 proves the case $n = 1$. Notice that $v_1(c) = p \cdot v(c)$ as $\mathbf{K}_1/\mathbf{K}$ is a ramified extension of degree p. Also notice that $v_1(x_1^p - x_1) = p \cdot v_1(x_1)$ since $v(x+y) \geqslant \min\{v(x), v(y)\}$, with equality holding when $v(x) \neq v(y)$. Thus $v_1(x_1) = v(c)$, and as p does not divide $v(c)$,

$$v_1(c \cdot x_1) = v_1(c) + v_1(x_1) = p \cdot v(c) + v(c) \leqslant 0$$

is not divisible by p either. By induction, suppose that $\mathbf{K}_{n-1}/\mathbf{K}$ is totally ramified, and that $v_{n-1}(x_{n-1})$ is negative and not divisible by p. Thus

$$v_{n-1}(c \cdot x_{n-1}) = v_{n-1}(c) + v_{n-1}(x_{n-1}) = p^{n-1} \cdot v(c) + v_{n-1}(x_{n-1})$$

is negative and not divisible by p. Hence by Proposition 7, $\mathbf{K}_n/\mathbf{K}_{n-1}$ is totally ramified. Also, since $v_n(x_n^p - x_n) = p \cdot v_n(x_n) = v_n(c \cdot x_{n-1}) = p \cdot v_{n-1}(c \cdot x_{n-1})$,

$$v_n(x_n) = v_{n-1}(c) + v_{n-1}(x_{n-1}) = p^{n-1} \cdot v(c) + v_{n-1}(x_{n-1})$$

is negative and not divisible by p. By induction, $\mathbf{K}_n/\mathbf{K}$ is totally ramified. ∎

COROLLARY 17. *Let ϕ be a rank one Drinfeld $\mathscr{A}$-module over a global function field $\mathbf{K}$ and let $\rho: G \to \mathbb{F}_p[[T]]^*$ be the continuous representation constructed from the action of G on $\mathbf{T}(\phi, T)$. If $\rho' = \theta \cdot \rho: G \to U$ where $U = \Gamma_1(\mathbb{F}_p[[T]])$, then, for any place P of $\mathbf{K}$, the image of an inertia group at P under ρ' is either trivial or is the full image of the decomposition group at P.*

Proof. As before, a Drinfeld module produces a sequence of cyclic p-extensions as in the previous theorem that is cut out by ρ'. Applying the theorem to the decomposition group of P, we see that the image of the inertia group is either trivial or the full group. ∎

3.3. "*Small*" *examples.* In this section, we consider several cases of deformations of $\bar{\rho}: G \to \mathbb{F}_p^*$ and examine whether they can be realized by the Galois action of G on the division points of a rank one Drinfeld module. We will consider three cases: $\mathscr{R} = \mathbb{F}_p$, $\mathscr{R} = \mathbb{F}_p[\varepsilon]$, where $\varepsilon^2 = 0$ (the dual numbers), and $\mathscr{R} = \mathbb{F}_p[T]/(T^3)$.

PROPOSITION 18. *If $\bar{\rho}: G \to \mathbb{F}_p^*$ is a continuous homomorphism and if γ is a structure morphism of $\mathbb{F}_p[T]$ into $\mathbf{K}$, then we can choose $a, b \in \mathbf{K}$ so that $\bar{\rho} = \rho_T$, the Galois action of G on (T)-division points of a Drinfeld module ϕ defined by $\phi_T = a\mathscr{F} + b$, and so that γ is the structure morphism of ϕ.*

Proof. Let $\mathbf{L}$ be the fixed field of the kernel of $\bar{\rho}$. Since $\mathbf{L}/\mathbf{K}$ is a cyclic extension of degree dividing $p-1$ and $\mathbf{K}$ contains μ_{p-1}, it is a Kummer

extension, containing all the roots of $x^{p^{-1}}-d$ for some $d\in\mathbf{K}^*$ and for which $d\notin(\mathbf{K}^*)^{p-1}$. Let δ be a fixed root of $x^{p-1}-d$ and let $\bar{\sigma}$ generate $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$ so that $\bar{\sigma}(\delta)=\omega\delta$ and let $\sigma\in G$ so that $\bar{\sigma}=\sigma\mathrm{Gal}(\mathbf{K}_S/\mathbf{L})$ and $\bar{\rho}(\sigma)=\omega$. Now set $\lambda_0=\delta$, which allows us to arbitrarily choose one of a or $b\in\mathbf{K}$, and then solve $d=-b/a$ for other. This way we can choose the structure map γ which is determined by $\gamma(T)=b$. Also note that, having chosen b, we can still control the value of a somewhat, in that we could have set $\lambda_0=\delta z$ for some $z\in\mathbf{K}^*$ so that $-b/a=d\cdot z^{p-1}$. Using this technique, we could choose a to have positive valuation at almost every place of $\mathbf{K}$, if we wished, by choosing z properly. ∎

Remark 19. Joint work of Nigel Boston and this author, to be published elsewhere, explores the question of what representations may be produced by the Galois action on P-division points of Drinfeld $\mathbb{F}_q[T]$-modules when P is a prime with $\deg(P)>1$.

THEOREM 20. *A representation $\rho: G\to\mathscr{R}^*$ where $\mathscr{R}$ is $\mathbb{F}_p[T]/(T^n)$ (or $\mathbb{F}_p[[T]]$) can be realized as the action of G on the (T^n)-division points (or on the T-adic Tate module, respectively) of a rank one Drinfeld $\mathscr{A}$-module ϕ over $\mathbf{K}$ if the tower of fields cut by $\rho'=\theta\cdot\rho$ satisfies Hypothesis* 14.

Proof. We simply need to choose $a, b\in\mathbf{K}-\{0\}$ correctly. If ρ' cuts out a tower of fields satisfying Hypothesis 14, there is an element $c\neq 0$ of $\mathbf{K}$ that defines the tower. Let $b=-1/c$, and define the structure morphism $\gamma: \mathscr{A}\to\mathbf{K}$ so that $\gamma(T)=b$. Now we can use Proposition 18 to construct $\bar{\rho}$. ∎

We can now examine several "small" examples of representations ρ that lift a given $\bar{\rho}$. As the previous proposition says, we only need examine if the pro-p part of the representation cuts out a tower of fields that satisfies Hypothesis 14. Our first example has $\mathscr{R}=\mathbb{F}_p[\varepsilon]$, where $\varepsilon^2=0$.

PROPOSITION 21. *Every continuous homomorphism $\rho: G\to\mathbb{F}_p[\varepsilon]^*$ can be realized by the action of G on the (T^2)-division points of a rank one Drinfeld module.*

Proof. Looking at $\rho': G\to U$, where $U=\langle 1+T+(T^2)\rangle\cong\mathbb{Z}/p\mathbb{Z}$, suppose ρ' is not trivial. Thus ρ' determines an Artin–Schreier extension $\mathbf{L}$ in which x^p-x-e splits completely for some $e\in\mathbf{K}$. Choose an element $\sigma\in G$ for which $\rho'(\sigma)=1+T+(T^2)$ and choose a root of α of x^p-x-e for which $\sigma(\alpha)=\alpha+1$. Now let $x_1=\alpha$, so that $c=-1/b=e$. In the proof of Proposition 18, we have the latitude to choose b, which we now have, and still have the ability to solve for an appropriate value for a. Thus we can define ϕ by $\phi_T=a\mathscr{F}+b$.

If, on the other hand, ρ' is trivial, ρ' determines a trivial Artin–Schreier extension, thus there is an $e \in \mathbf{K}$ so that $\mathscr{P}(x) = e$ splits in $\mathbf{K}$. Set $b = -1/e$, and proceed as before. ∎

Notice that for this to work, we had to give up our ability to control the structure morphism γ as we no longer have complete freedom to choose the value of b. We could modify our choice of b somewhat, in that we would have the same extension as long as we set $c = -1/b = e + \mathscr{P}(y)$ for some $y \in \mathbf{K}$, in which case $x_1 = \alpha + y$.

As the last of the "small" examples, we have $\mathscr{R} = \mathbb{F}_p[T]/(T^3)$. Now, however, we have a distinction to make. When p is an odd prime, then U is elementary abelian with two generators, $1 + T + (T^3)$ and $1 + T^2 + (T^3)$, but when $p = 2$, $U = \langle 1 + T + (T^3) \rangle$ is cyclic of order 4. Suppose that $\mathbf{L}$ is the fixed field of the kernel of ρ', as before. In either case, there is an intermediate field $\mathbf{M}$. The difference between p odd and p even results in this: when p is an odd prime, then $\mathbf{L}/\mathbf{K}$ has $p+1$ intermediate fields that are linearly disjoint over $\mathbf{K}$, any two of which generate $\mathbf{L}$, whereas, when $p = 2$, $\mathbf{L}/\mathbf{K}$ is a cyclic degree four extension with only the one intermediate field, $\mathbf{M}$. Though the methods differ, the result is the same: not every continuous homomorphism $\rho: G \to \mathscr{R}^*$ can be realized as the action of G on the (T^3)-division points of a rank one Drinfeld module over $\mathbf{K}$.

For now, let p be an odd prime. As mentioned above, $\mathbf{L}/\mathbf{K}$ has $p+1$ intermediate fields, one of which is $\mathbf{M}$ and which, together with any of the other intermediate fields, will generate $\mathbf{L}$. Let $\mathbf{N}$ be any of the other intermediate fields. As $\mathbf{M}/\mathbf{K}$ and $\mathbf{N}/\mathbf{K}$ are Artin–Schreier extensions, they are the splitting fields of $\mathscr{P}(x) - m$ and $\mathscr{P}(x) - n$ respectively. Let μ and ν be the roots of these polynomials respectively. Also, $\mathbf{L}/\mathbf{M}$ is an Artin–Schreier extension, generated over $\mathbf{M}$ by λ, a root of $\mathscr{P}(x) - l$ where $l \in \mathbf{M}$. Since $\mathbf{L} = \mathbf{K}(\mu, \nu) = \mathbf{M}(\lambda)$, the polynomials $\mathscr{P}(x) - n$ and $\mathscr{P}(x) - l$ have the same splitting field $\mathbf{L}$ over $\mathbf{M}$. By Theorem 6, $n = il + \mathscr{P}(y)$ for some nonzero $i \in \mathbb{F}_p$ and some $y \in \mathbf{M}$. This is the key idea that we will use.

Let us specialize to the case where we have a tower of fields of length two satisfying Hypothesis 14, where $\mathbf{K}_1 = \mathbf{M}$ is the splitting field over $\mathbf{K}$ of $\mathscr{P}(x) = c$ and $\mathbf{K}_2 = \mathbf{L}$ is the splitting field over $\mathbf{K}_1$ of $\mathscr{P}(x) = cx_1$. As above, we know that $n = icx_1 + \mathscr{P}(y) \in \mathbf{K}$ for some $i \in \mathbb{F}_p$ and some $y \in \mathbf{K}_1$. We can easily check that one possible choice of i and y is $p-2$ and x_1^2. Then

$$\begin{aligned} n &= (p-2)\, cx_1 + \mathscr{P}(x_1^2) \\ &= (p-2)\, cx_1 + (x_1^p)^2 - x_1^2 \\ &= (p-2)\, cx_1 + (x_1 + c)^2 - x_1^2 \\ &= c^2. \end{aligned}$$

Notice that $\mathscr{P}(x_1^2 - 2x_2) = c^2$. Hence, this tower of fields is generated by the roots of $\mathscr{P}(x) = c$ and $\mathscr{P}(x) = c^2$. So finally, for any element $d \in \mathbf{K}$ so that $c^2 \notin d + \mathscr{P}\mathbf{K}$, the field extension generated by the roots of $\mathscr{P}(x) - c$ and $\mathscr{P}(x) - d$ cannot satisfy Hypothesis 14. The existence of such a d can be guaranteed in some situations. For instance, when $\mathbf{K}$ is $\mathbb{F}_3(T)$, then we can look for nonzero values of c and values of d for which $c^2 = d + z^3 - z$ has no rational solutions. The following two lemmas give examples of values for d which $c^2 \notin d + \mathscr{P}\mathbf{K}$ for every nontrivial value for c, when $\mathbf{K}$ is the rational function field over $\mathbb{F}_3$.

LEMMA 22. *The equation*

$$y^2 = z^3 - z \tag{3.3}$$

has no solutions in $\mathbf{K} = \mathbb{F}_3(T)$ *except the trivial solutions where* $y = 0$.

Proof. This is an elliptic curve E over $\mathbf{K}$, with the only $\mathbf{K}$-rational torsion points being the 2-torsion points, where $y = 0$ or the point at infinity. To establish the result, we use the method of complete 2-descent [14, Chapter X, Proposition 1.4]. Let $y^2 = (x - e_1)(x - e_2)(x - e_3)$ be an elliptic curve E over $\mathbf{K}$. Let S is the set of place of $\mathbf{K}$ that divide ∞, or that divide 2, or where E has bad reduction, and let $\mathbf{K}(S, 2) = \{b \in \mathbf{K}^*/(\mathbf{K}^*)^2 \mid v(b) \equiv 0 \bmod 2 \text{ for every } v \in S\}$. Complete 2-descent constructs an injective homomorphism

$$E(\mathbf{K})/2E(\mathbf{K}) \to \mathbf{K}(S, 2)^2. \tag{3.4}$$

In our case of E, given by (3.3), S contains only the infinite place, as E has good reduction at all finite places, so $\mathbf{K}(S, 2) = \{1, 2\}$. One can check that the torsion points of E has only the trivial 2-torsion points. Now suppose that $E(\mathbf{K})$ has rank n, so that $E(\mathbf{K})/2E(\mathbf{K}) \cong (\mathbb{Z}/2\mathbb{Z})^{n+2}$. But the injective homomorphism (3.4) has its image in a group of order 4. Hence n must be zero, and the only rational points on E are the trivial points with $y = 0$. ∎

LEMMA 23. *The equation*

$$y^2 = 2 + z^3 - z \tag{3.5}$$

has no solutions in $\mathbf{K} = \mathbb{F}_3(T)$.

Proof. One can easily check that (3.5) has no solutions in $\mathbb{F}_3$. To show that is has no solutions in $\mathbf{K}$, we will use a formula for the genus of a function field [15, Proposition III.10.5 and the note]. The formula holds for the field $\mathbf{F}(x, y)$ when $\mathbf{F}(x, y)$ is a function field over $\mathbf{F}$, x and y are

transcendental over $\mathbf{F}$, and when the irreducible equation for y over $\mathbf{F}(x)$ has the form

$$y^n + f_1(x)\, y^{n-1} + \cdots + f_{n-1}(x)\, y + f_n(x) = 0$$

with $f_j(x) \in \mathbf{F}[x]$ and $\deg f_j(x) \leqslant j$ for each $j = 1, ..., n$, and when the equation gives a nonsingular projective curve embedded in $\mathbf{P}^2(\mathbf{F})$. If these hold, the genus of $\mathbf{F}(x, y)$ is $(n-1)(n-2)/2$. For us, we can see (3.5) is, after homogenizing, a nonsingular projective curve, and that, when rewritten as

$$z^3 - z + (2 - y^2) = 0$$

it satisfies the conditions of [15, Proposition III.5.10]. Thus the genus of $\mathbb{F}_3(y, z)$ is $(3-1)(2-1)/2 = 1$. But if y and z lie in $\mathbf{K}$, then $\mathbb{F}_3(y, z)$ is a genus one subfield of the genus zero field $\mathbf{K}$. This contradicts Lüroth's Theorem [15, Proposition III.5.9], which states that every subfield of a rational function field which properly contains the constant field is itself a rational function field (and hence has genus zero). ∎

Now let $p = 2$, and let us examine the tower of fields

$$\mathbf{K} \subset \mathbf{K}_1 \subset \mathbf{K}_2$$

that satisfies Hypothesis 14. Thus we have x_1 and x_2 so that $\mathscr{P}(x_2) = cx_1$ and $\mathscr{P}(x_1) = c$. A rather simple calculation shows that $\mathscr{P}(x_1, x_2) = (c, 0)$. Thus, any field extension of $\mathbf{K}$ generated by the coordinates of a solution to

$$\mathscr{P}(y_1, y_2) = (a, b),$$

where $(a, b) \notin (c, 0) + \mathscr{P}W_2\mathbf{K}$ for some $c \in \mathbf{K}$, cannot satisfy Hypothesis 14. Thus we have a similar result, that not every continuous homomorphism of G into $\mathbb{F}_2[T]/(T^3))^*$ can be constructed as the Galois action of G on the (T^3)-division points of a rank one Drinfeld $\mathscr{A}$-module over $\mathbf{K}$.

Remark 24. We actually could have proved this earlier, using our knowledge of ramification in representations produced by Drinfeld modules. As Corollary 17 says, the pro-p part of a representation produced by the action of G on the (T^n)-division points of a rank one Drinfeld module is either unramified or totally ramified at each place. To construct a representation that cannot be realized by the G-action on the division points of a Drinfeld module, we only need to construct a representation that is ramified, but not totally ramified, at some place.

3.4. *Deformations to* $\mathbb{F}_p[[T]]$. In this section, we examine which deformations might arise as the Galois action on the P-adic Tate module of a

rank one Drinfeld module. We concentrate, as before, on the case $P=(T)$, for which we have $\mathbb{F}_p[T]_{(T)} \cong \mathbb{F}_p[[T]]$. We can break a representation $\rho: G \to \mathbb{F}_p[[T]]^*$ into its projection $\bar{\rho}$ to $\mathbb{F}_p^*$ and its projection ρ' to $U = \{f(T) \in \mathbb{F}_p[[T]] \mid f(0)=1\}$. Thus we want to study continuous homomorphisms $\rho': G \to U$. To do so, we will study the structure of U, and, in order to use Section 2, we will study the structure of $\hat{U}$.

LEMMA 25. *As a pro-p group, U is isomorphic to a countable product of* $\mathbb{Z}_p$; *more explicitly*,

$$U \cong \prod_{i \in \mathbb{Z},\, i>0,\, (i,\, p)=1} \langle 1 + T^i \rangle.$$

Proof. We can find this result in [11] and in [16, Chapter 2, Proposition 10]. The proof in the latter reference gives the explicit product decomposition in a slightly more general setting. ∎

Since the parametrization of abelian pro-p extensions $\mathbf{L}/\mathbf{K}$ derived in subsection 2.4 depends on the character groups of $\mathrm{Gal}(\mathbf{L}/\mathbf{K})$, to examine $\rho': G \to U$, we need to understand the structure of $\hat{U}$.

LEMMA 26. *The character group of U is isomorphic to* $\coprod \mu_{p^\infty}$ *over a countably infinite index set.*

Proof. The facts about products, coproducts, and direct limits used in this proof are relatively standard, and can be found in [13, Chapter 2]. Since U is isomorphic to a countably infinite product of $\mathbb{Z}_p$ where I is the countable index set, we will consider the structure of $\hom(\prod \mathbb{Z}_p, \mu_{p^\infty})$. Now, $\mathbb{Z}_p$ is a compact, Hausdorff, and totally disconnected topological group, thus $\prod \mathbb{Z}_p$ is also compact, Hausdorff, and totally disconnected. This implies that if χ is a character of $\prod \mathbb{Z}_p$, its image is finite and its kernel is an open subgroup. Thus the kernel contains the subgroup $\prod_{i \in J} \mathbb{Z}_p$, where $J \subset I$ and $I - J$ is finite. So any character factors through a finite direct product. Hence $\hom(\prod_{i \in I} \mathbb{Z}_p, \mu_{p^\infty})$ is the direct limit over all the finite subsets I' of I of $\hom(\prod_{i \in I'} \mathbb{Z}_p, \mu_{p^\infty})$, since if χ factors through $\prod_{i \in I_1} \mathbb{Z}_p$, it certainly factors through $\prod_{i \in I_2} \mathbb{Z}_p$ where $I_1 \subset I_2$. However, finite direct products and finite direct sums are isomorphic, so each of the objects in the direct system is

$$\hom\left(\coprod_{i \in I'} \mathbb{Z}_p, \mu_{p^\infty}\right) \cong \prod_{i \in I'} \hom(\mathbb{Z}_p, \mu_{p^\infty}) \cong \coprod_{i \in I'} \hom(\mathbb{Z}_p, \mu_{p^\infty}).$$

Generally we have that $\coprod_{j \in J} M_j$ is isomorphic to the direct limit of $\coprod_{j \in J'} M_j$ over all finite subsets $J' \subset J$. Thus $\hat{U} \cong \coprod_{i \in I} \hom(\mathbb{Z}_p, \mu_{p^\infty})$. Since,

for any category of commutative $\mathscr{A}$-modules, $\hom(\mathscr{A}, M) \cong M$, we have the result. ∎

Recall our isomorphism η of functors from subsection 2.5. Using η and the previous lemma, the image of $\eta_U(\rho')$ in $X_{\mathbf{K},S}$ is the image of the countably infinite coproduct of μ_{p^∞}. The question is, what restrictions are placed on the map

$$\hat{U} \to X_{\mathbf{K},S}$$

by Hypothesis 14?

Conjecture 27. Let $\rho'\colon G \to U$ be a continuous homomorphism. Let π_n be the projection of U onto U/U_n, where

$$U_n = \{ f(T) \in \mathbb{F}_p[[T]] \mid f(T) \equiv 1 \pmod{(T^{n+1})} \}.$$

Let $\mathbf{K}_n$ be the fixed field of the kernel of $\pi_n \cdot \rho'$. If the tower of fields

$$\mathbf{K} \subset \mathbf{K}_1 \subset \cdots$$

satisfies Hypothesis 14, then the image of $\eta_U(\rho')$ in $X_{\mathbf{K},S}$ is

$$\coprod_{i>0,\,(i,p)=1} C_i$$

where $C_i = \varinjlim_{m>0} \langle (c^i, 0, \ldots, 0) + \mathscr{P}W_m\mathbf{K} \rangle$.

The conjecture implies that each element of the image of $\eta_U(\rho')$ is represented by a coset $(A_0, \ldots, A_{m-1}) + \mathscr{P}W_m\mathbf{K}$ where each A_j is a polynomial in c with zero constant term, and conversely, that every such coset represents an element of the image of $\eta_U(\rho')$. Since $\mathscr{P}(x) = x^p - x \in \mathscr{P}\mathbf{K}$ whenever $x \in \mathbf{K}$,

$$x^p \equiv x \pmod{\mathscr{P}\mathbf{K}},$$

implying that we can rewrite any coset representative so that each A_j is a polynomial in c with zero constant term and where the only exponents of c are relatively prime to p.

3.5. *Evidence for the conjecture.* Suppose we have Hypothesis 14. For any $n < p$, we can use the definition of $\mathscr{P}$ and of x_n, to attempt to find a primitive element of the disjoint field extensions of $\mathbf{K}$ that generate $\mathbf{K}_n$. For example

$$\begin{aligned}\mathscr{P}(x_1^2) &= (x_1^2)^p - x_1^2 = (x_1^p)^2 - x_1^2 \\ &= (x_1 + c)^2 - x_1^2 = 2cx_1 + c^2\end{aligned}$$

along with the linearity of $\mathscr{P}$ gives, as mentioned before, that $\mathscr{P}(x_1^2 - 2x_2) = c^2$. Using calculations like this one, we can generate data such as the following.

$$
\begin{aligned}
c &= \mathscr{P}(x_1) \\
c^2 &= \mathscr{P}(x_1^2 - 2x_2) \\
c^3 &= \mathscr{P}(x_1^3 - 3x_1x_2 + 3x_3) \\
c^4 &= \mathscr{P}(x_1^4 - 4x_1^2x_2 + 4x_1x_3 + 2x_2^2 - 4x_4) \\
c^5 &= \mathscr{P}(x_1^5 - 5x_1^3x_2 + 5x_1^2x_3 - 5x_1x_4 + 5x_1x_2^2 - 5x_2x_3 + 5x_5) \\
c^6 &= \mathscr{P}(x_1^6 - 6x_1^4x_2 + 6x_1^3x_3 - 6x_1^2x_4 + 9x_1^2x_2^2 \\
&\qquad + 6x_1x_5 - 12x_1x_2x_3 - 2x_2^3 + 6x_2x_4 + 3x_3^2 - 6x_6) \\
c^7 &= \mathscr{P}(x_1^7 - 7x_1^5x_2 + 7x_1^4x_3 + 14x_1^3x_2^2 - 7x_1^3x_4 \\
&\qquad - 21x_1^2x_2x_3 + 7x_1^2x_5 - 7x_1x_2^3 + 14x_1x_2x_4 + 7x_1x_3^2 \\
&\qquad - 7x_1x_6 + 7x_2^2x_3 - 7x_2x_5 - 7x_3x_4 + 7x_7)
\end{aligned}
\tag{3.6}
$$

We can notice several patterns in these data. When $\mathscr{P}(y) = c^n$ for $n < p$, y is a polynomial in the x_i for $i \leqslant n$, and that x_1^n is the only term with coefficient 1. If we weight each of the x_i by its index, so that, for example, the weight of $x_1x_3^2$ is $1 + 2 \cdot 3 = 7$, then each of the summands has weight n. Also, every possible monomial of weight n is represented with some nonzero coefficient. As for the coefficients involved in y, we can see that the only prime divisors of the coefficients are less than or equal to n. If we consider the monomial $x_i^j x_k^l$ as a product of j i-cycles and l k-cycles, the sign of the coefficient of the monomial is the sign of the monomial, depending on whether the "cycle structure" of the monomial is even or odd. And, when n is an odd prime, the absolute value of the coefficient of the monomials that only involve x_1 and x_2 are given by the coefficients of $x_1 \cdot g_n(x_1^2 + 2)$ where g_n is the characteristic polynomial over $\mathbb{Q}$ of $\zeta_n + \zeta_n^{-1}$ (ζ_n is a primitive nth root of unity).[1] These observations suggest the question: for $n < p$, is there a formula for a $y \in \mathbf{K}_n$ in terms of the x_i for which $\mathscr{P}(y) = c^n$, and, if so, what is it?

When we consider Hypothesis 14 for values of $n \geqslant p$, we need the characterization using Witt vectors. For the data that follows, we fix the prime p, and compute the image of $\eta_{U_n}(\pi_n \cdot \rho')$ in $X_{\mathbf{K},S}$ for certain n, where U_n is the set of units congruent to 1 modulo (T^{n+1}).

In the case of $p = 2$, we can look at the tower of field extensions $\mathbf{K}_5/\mathbf{K}$ that satisfies Hypothesis 14 (i.e., setting $n = 5$ in the above discussion). In

[1] I thank the referee for finding this apparent connection to cyclotomic polynomials.

this case, U_5 is an abelian 2-group of type $(8, 2, 2)$, and we can compute the following data:

$$\begin{aligned}(c, 0, 0) &= \mathscr{P}(x_1, x_2, x_4 + x_1x_2 + x_1x_3 + cx_2)\\ (c^3) &= \mathscr{P}(x_3 + x_1x_2 + cx_1 + x_1 + c)\\ (c^5) &= \mathscr{P}(x_5 + x_1x_4 + x_2x_3 + x_1x_3 + cx_3\\ &\quad + cx_2 + cx_1x_2 + c^2x_1 + x_1 + c^2 + c)\end{aligned}$$

so that $\langle (c, 0, 0) + \mathscr{P}W_3\mathbf{K}, (c^3) + \mathscr{P}W_1\mathbf{K}, (c^5) + \mathscr{P}W_1\mathbf{K}\rangle$ generates the image of $\eta_{U_5}(\pi_5 \cdot \rho')$ in $X_{\mathbf{K}, S}$.

In the case of $p = 3$, we can compute the case for $n = 3$. In this case, U_3 is an abelian 3-group of type $(9, 3)$. The result is the following data:

$$\begin{aligned}(c, 0) &= \mathscr{P}(x_1, x_3 - x_1x_2)\\ (c^2) &= \mathscr{P}(x_1^2 - 2x_2)\end{aligned}$$

so that $\langle (c, 0) + \mathscr{P}W_2\mathbf{K}, (c^2) + \mathscr{P}W_1\mathbf{K}\rangle$ is the image of $\eta_{U_3}(\pi_3 \cdot \rho')$ in $X_{\mathbf{K}, S}$.

As a final example, when $p = 5$ and $n = 5$, U is an abelian 5-group of type $(25, 5, 5, 5)$. The data includes

$$(c, 0) = \mathscr{P}(x_1, x_5 - x_1x_4 - x_2x_3 + x_1^2x_3 + x_1x_2^2 - x_1^3x_2)$$

and the equations in (3.6) for c^i when $i < 5$.

We are left with several questions:

1. If the conjecture holds, is there a reasonable formula in terms of the x_i for the elements $y^{(j)}$ of $W_m\mathbf{K}_n$ for which $\mathscr{P}(y^{(j)}) = (c^i, 0, ..., 0)$?

2. What can we learn from looking at the images of decomposition group and inertia group at (T)? I.e., can we say something along the lines of the Fontaine–Mazur conjecture? Fontaine and Mazur conjecture in [4] that an irreducible p-adic Galois representation of a number field is "geometric" if and only if the representation is *potentially semi-stable at p*, which is essentially a condition on the restriction to the decomposition group at p. We have Corollary 17, but this is probably not enough to guarantee that a particular representation is "associated" to a Drinfeld module.

REFERENCES

1. Nigel Boston, "Deformation Theory of Galois Representations," Ph.D. thesis, Harvard University, 1987.
2. Nigel Boston, Explicit deformation of Galois representations, *Invent. Math.* **103** (1991), 181–196.

3. B. de Smit and H. W. Lenstra, Jr., Explicit construction of universal deformations rings, *in* "Modular Forms and Fermat's Last Theorem (New York)" (Cornell, Silverman, and Stevens, Eds.), Proceedings of a conference held at Boston University August 9–18, 1995, Springer-Verlag.
4. Jean-Marc Fontaine and Barry Mazur, Geometric Galois representations, *in* "Elliptic Curves, Modular Forms, and Fermat's Last Theorem (Cambridge, MA)" (John Coates and S. T. Yau, Eds.), Series in Number Theory, Vol. 1, International Press, 1995; Conference on Elliptic curves and Modular Forms, Hong Kong, December 18–21, 1993, pp. 41–78.
5. David Goss, "Basic Structures of Function Field Arithmetic," Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, Berlin, 1996.
6. David R. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
7. David R. Hayes, A brief introduction to Drinfeld modules, *in* "The Arithmetic of Function Fields (New York)" (David Goss, David R. Hayes, and Michael I. Rosen, Eds.), Ohio State University Mathematical Research Institute Publications, Vol. 2, Walter de Gruyter and Co., 1992; Proceedings of the Workshop at The Ohio State University, June 17–26, 1991, pp. 1–32.
8. Edwin Hewitt and Kenneth A. Ross, "Abstract Harmonic Analysis," Vol. 1, Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, no. 115, Springer-Verlag, Berlin, 1963.
9. Thomas W. Hungerford, "Algebra," Graduate Texts in Mathematics, no. 73, Springer-Verlag, New York, 1987.
10. Nathan Jacobson, "Basic Algebra II," W. H. Freeman and Company, San Francisco, 1980.
11. Helmut Koch, "Galoissche Theorie der p-Erweiterungen," Springer-Verlag, New York, 1970.
12. Barry Mazur, Deforming Galois representations, *in* "Galois Groups over **Q** (New York)" (Yasutaka Ihara, Kenneth Ribet, and Jean-Pierre Serre, Eds.), Mathematical Sciences Research Institute Publications, Vol. 16, Springer-Verlag; Proceedings of a Workshop Held March 23–27, 1987, pp. 385–438.
13. Joseph J. Rotman, "An Introduction to Homological Algebra," Academic Press, Orlando, 1979.
14. Joseph H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics, no. 106, Springer-Verlag, New York, 1986.
15. Henning Stichtenoth, "Algebraic Function Fields and Codes," Universitext, Springer-Verlag, New York, 1993.
16. André Weil, "Basic Number Theory," 3 ed., Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, no. 144, Springer-Verlag, New York, 1974.
17. Andrew Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141**(2) (1995); no. 3, 443–551.