J. Fac. Sci. Univ. Tokyo
Sect. IA, Math.
37 (1990), 151-170.

*Galois extensions associated to deformations of formal A-modules**)

By Kevin KEATING

Abstract. Let A be the ring of integers in a finite extension $\mathcal{K}$ of $\boldsymbol{Q}_p$ with residue field k_0. Let $\bar{G}/k_0$ be a formal A-module of height $h<\infty$ and let $\Gamma/k_0[[t]]$ be a universal deformation of $\bar{G}$ to height $h-1$. In this paper we study the kernel of the Galois character associated to Γ. Our main tool is Fontaine and Wintenberger's theory of the field of norms.

Let $\bar{G}/\boldsymbol{F}_p$ be a one-parameter formal group law of height 2 and let $\Gamma/\boldsymbol{F}_p[[t]]$ be a universal deformation of $\bar{G}$ to complete noetherian local rings of characteristic p. Set $F=\boldsymbol{F}_p((t))$ and let F^{ab} be a maximal abelian extension of F. There is a character $\chi: \mathrm{Gal}(F^{ab}/F)\rightarrow \boldsymbol{Z}_p^{\times}$ given by the action of Galois on the p^n-torsion of Γ. Let $F'\subset F^{ab}$ be the fixed field of $\ker\chi$, and let $F^{nr}\subset F^{ab}$ be the maximal unramified extension of F. In [4, Th. 1] and [7, Th. 3.3] the compositum $F'F^{nr}$ is characterized in terms of the action of $\mathrm{Aut}_{\boldsymbol{F}_p}(\bar{G})$ on F. The purpose of this paper is to generalize these results to the case where $\bar{G}$ is a formal A-module of height $h<\infty$ and Γ is a universal deformation of $\bar{G}$ to height $h-1$. As applications we give independent computations of the ramification breaks of the Galois character associated to Γ [6, Th. 3.5 2b], and of the endomorphism ring of the reduction of $\Gamma\ (\mathrm{mod}\ t^n)$ [8, Th. 1.2].

1. Preliminaries and statement of the theorem

Let $\mathcal{K}$ be a complete discretely valued field with ring of integers A, uniformizer π_A, and finite residue field $k_0\cong\boldsymbol{F}_q$. Let K be a finite separable extension of $\mathcal{K}$ of degree $h>1$, with ring of integers $\mathcal{O}$, uniformizer $\pi_{\mathcal{O}}$, and residue field k. Let $(\bar{G}, \bar{\alpha})$ be a pair consisting of a formal A-module $\bar{G}/k$ and an A-algebra homomorphism $\bar{\alpha}: \mathcal{O}\hookrightarrow\mathrm{End}_k(\bar{G})$ which makes $\bar{G}$ a formal $\mathcal{O}$-module of height 1 (see [1, § 1A]).

Let $\mathcal{R}$ be a complete noetherian local $\mathcal{O}$-algebra with residue field k. A deformation of the formal A-module $\bar{G}$ over $\mathcal{R}$ is a pair $(\tilde{G}, i)$, where $\tilde{G}/\mathcal{R}$ is a formal A-module and $i: \tilde{G}\otimes_{\mathcal{R}}k\xrightarrow{\sim}\bar{G}$ is an isomorphism of formal A-modules.

*) The author was partially supported by NSF contract DMS 88-05216.

A morphism between the deformations $(\tilde{G}, i)/\mathcal{R}$ and $(\tilde{G}', i')/\mathcal{R}'$ of $\bar{G}$ consists of a homomorphism $\phi: \mathcal{R} \to \mathcal{R}'$ of local $\mathcal{O}$-algebras and a map $f: \tilde{G} \otimes_{\mathcal{R}} \mathcal{R}' \to \tilde{G}'$ of formal A-modules whose special fiber $\bar{f}$ satisfies $i = i' \circ \bar{f}$. Usually we have $\tilde{G} \otimes_{\mathcal{R}} k = \bar{G}$ and $i = id$, in which case we write $\tilde{G}$ for $(\tilde{G}, i)$. Given $\tilde{G}/\mathcal{R}$ and $a \in A$ we denote by $[a]_{\tilde{G}}$ the endomorphism of $\tilde{G}$ induced by a. (We also use this notation for formal $\mathcal{O}$-modules.) If $\tilde{G}$ and $\tilde{G}'$ are isomorphic in the category of deformations of $\bar{G}$ we say that they are $*$-isomorphic, and write $\tilde{G} \cong^* \tilde{G}'$.

Let R denote the $\mathcal{O}$-algebra $k[[t]]$, let $F = k((t))$ denote the field of fractions of R, and let v_t denote the normalized valuation on F. By the proof of [1, Prop. 4.2] there exists a deformation Γ/R of $\bar{G}$ such that

$$[\pi_A]_\Gamma(x) = a_0 x^{q^{h-1}} + \cdots,$$

with $v_t(a_0) = 1$. Let F^{sep} be a separable closure of F, and denote by F^{ab}/F the maximal abelian subextension of F^{sep}/F. We will associate to Γ a Galois character $\chi: \mathrm{Gal}(F^{ab}/F) \to A^\times$, as follows.

Let $\mathcal{R}$ be a ring of characteristic p. For $n \geqq 0$ let $q^n: \mathcal{R} \to \mathcal{R}$ denote the base change $x \mapsto x^{q^n}$. Then for $r \geqq 1$ the power series $[\pi_A^r]_\Gamma^{q^{(h-1)r}}$ is the endomorphism of $\Gamma^{q^{(h-1)r}}$ induced by π_A^r. The F^{ab}-valued points in the kernel of $[\pi_A^r]_\Gamma^{q^{(h-1)r}}$ form a free (A/π_A^r)-module of rank 1. The group $\mathrm{Gal}(F^{ab}/F)$ acts on this (A/π_A^r)-module, giving a map $\chi_r: \mathrm{Gal}(F^{ab}/F) \to (A/\pi_A^r)^\times$. By taking the projective limit of the χ_r we get the character $\chi: \mathrm{Gal}(F^{ab}/F) \to A^\times$.

By [1, Prop. 4.2] we see that Γ is a universal deformation of $\bar{G}$ to height $h-1$: Given any deformation $(\tilde{G}, i)/\mathcal{R}$ of $\bar{G}$ to height h or $h-1$, there is a unique map of deformations from Γ/R to $(\tilde{G}, i)/\mathcal{R}$. Let $\phi \in \mathrm{Aut}_k(\bar{G})$. Then $(\Gamma, \phi)/R$ is a deformation of $\bar{G}$ to height $h-1$, so there is a unique $\mathcal{O}$-algebra homomorphism $\phi^*: R \to R$ such that ϕ lifts to an isogeny $\tilde{\phi}: \Gamma \to \Gamma^{\phi^*}$. By the uniqueness of ϕ^* we see that the map $\phi \mapsto \phi^*$ is an anti-homomorphism from $\mathrm{Aut}_k(\bar{G})$ to $\mathrm{Aut}_k(R)$.

Of course ϕ^* extends uniquely to a k-automorphism of F. Hence ϕ^* induces a map $\phi^\cdot: \mathrm{Gal}(F^{ab}/F) \to \mathrm{Gal}(F^{ab}/F)$. Let χ^{ϕ^*} denote the Galois character associated to Γ^{ϕ^*}. By the functoriality of χ we easily see that $\chi^{\phi^*} \circ \phi^\cdot = \chi$. Since Γ^{ϕ^*} is isomorphic (but not $*$-isomorphic) to Γ, we have $\chi^{\phi^*} = \chi$ as well. It follows that $\chi \circ \phi^\cdot = \chi$.

Let $F' \subset F^{ab}$ be the fixed field of $\ker \chi$, and let $F^{nr} \subset F^{ab}$ be the maximal unramified extension of F. The identity $\chi \circ \phi^\cdot = \chi$ and the k-linearity of ϕ^* imply that $\phi^\cdot$ acts trivially on $\mathrm{Gal}(F'F^{nr}/F)$, for every $\phi \in \mathrm{Aut}_k(\bar{G})$. Our main result shows that $F'F^{nr}$ is the largest abelian extension of F with this property.

THEOREM 1. *For* $a \in \mathcal{O}^\times$ *let* $\phi_a = [a]_{\bar{G}} \in \mathrm{Aut}_k(\bar{G})$. *Let* F''/F *be the maximal subextension of* F^{ab}/F *such that* ϕ_a *acts trivially on* $\mathrm{Gal}(F''/F)$ *for every* $a \in \mathcal{O}^\times$. *Then* $F'' = F'F^{nr}$.

REMARK. The cases with $A = \boldsymbol{Z}_p$ and $h=2$ are treated in [4, Th. 1] and [7, Th. 3.3 and Th. 3.4].

2. The field of norms

The proof of Theorem 1 depends on the theory of the field of norms, developed by Fontaine [2] and Wintenberger [13]. We outline a special case of this theory here, in which all the field extensions are abelian.

Let K be a complete discretely valued field with finite residue field and let L be an infinite abelian extension of K which induces a finite extension of the residue field of K. By class field theory [11, XV § 2, Th. 2] the higher ramification subgroups of $\mathrm{Gal}(L/K)$ have finite index in $\mathrm{Gal}(L/K)$. Therefore the extension L/K is arithmetically profinite in the sense of [13, 1.2.1]. Let $\mathcal{E}$ denote the set of finite extensions of K which are contained in L. We define

$$X_K(L)^\times = \varprojlim_{M \in \mathcal{E}} M^\times,$$

where the limit is taken with respect to the norms. The group $X_K(L)^\times$ is the multiplicative group of a field $X_K(L)$ in a natural way. More precisely, $X_K(L)$ is a complete discretely valued field of characteristic p whose residue field is isomorphic to the residue field of L [13, Th. 2.1.3]. In § 4 we will describe the additive structure of $X_K(L)$ more explicitly.

Let L_1 be a finite extension of L such that L_1 is abelian over K. By [13, Th. 3.1.2] there is an embedding

$$X_K(L) \longrightarrow X_K(L_1)$$

which makes $X_K(L_1)$ a Galois extension of $X_K(L)$. The action of $\mathrm{Gal}(L_1/L)$ on the subextensions of L_1/K induces an action of $\mathrm{Gal}(L_1/L)$ on $X_K(L_1)$. By [13, Th. 3.1.2] this action induces an isomorphism

$$\mathrm{Gal}(L_1/L) \xrightarrow{\sim} \mathrm{Gal}(X_K(L_1)/X_K(L)).$$

If L' is an infinite extension of L such that L'/K is abelian define

$$X_{L/K}(L') = \varinjlim X_K(L_1),$$

with the limit taken over the finite subextensions of L'/L. By [13, Th. 3.2.2] we have

$$\mathrm{Gal}(L'/L) \xrightarrow{\sim} \mathrm{Gal}(X_{L/K}(L')/X_K(L)).$$

In the case that interests us K is the field we considered in § 1. To describe L we let $G/\mathcal{O}$ be a formal $\mathcal{O}$-module such that $G\otimes_{\mathcal{O}}k=\bar{G}$. (The existence and uniqueness of G will be proved in Proposition 2.) Let K^{sep} be a separable closure of K, let $K'_s\subset K^{sep}$ be the extension of K generated by the roots of $[\pi_A^s]_G$, and let L' be the union of the K'_s for $s\geqq 1$. By the theory of Lubin-Tate [10, p. 386] L' is a maximal totally ramified abelian extension of K, and $\mathrm{Gal}(L'/K)\cong\mathcal{O}^\times$. Define $L\subset L'$ to be the fixed field of $A^\times\subset\mathcal{O}^\times$; then $\mathrm{Gal}(L/K)\cong\mathcal{O}^\times/A^\times$. Let $L^{nr}\subset K^{sep}$ denote the maximal unramified extension of L. By class field theory we see that the compositum $L'L^{nr}\subset K^{sep}$ is equal to the maximal abelian extension K^{ab} of K.

In § 6 we show that $X_K(L)$ is isomorphic to the field F defined in § 1. Then in § 7 we prove the following (non-canonical) isomorphisms of fields over $F\cong X_K(L)$:

$$F'\cong X_{L/K}(L')$$

$$F''\cong X_{L/K}(K^{ab}).$$

(The first follows from Proposition 10, and the second follows from Proposition 9.) Since the residue field of $X_K(L_1)$ is isomorphic to the residue field of L_1, we also have

$$F^{nr}\cong X_{L/K}(L^{nr}).$$

Then by [13, Th. 3.2.2] we get

$$X_{L/K}(L')X_{L/K}(L^{nr})=X_{L/K}(L'L^{nr})$$

$$=X_{L/K}(K^{ab}).$$

Since all of our fields are abelian extensions of F, we conclude that $F'F^{nr}=F''$, which gives Theorem 1.

REMARK. Let F be a complete discretely valued field of characteristic p with perfect residue field, and let $\mathcal{G}$ be a closed subgroup of $\mathrm{Aut}(F)$ which is an abelian p-adic Lie group. By [12] there exists an infinite abelian extension of local fields L/K such that the pairs $(F,\mathcal{G})$ and $(X_K(L),\mathrm{Gal}(L/K))$ are isomorphic. It seems likely that in the present case (with $F=k((t))$ and $\mathcal{G}\cong\mathcal{O}^\times/A^\times$) one might be able use this result to prove Theorem 1 without determining L and K explicitly. Such an approach would depend heavily on the ramification data computed in [6, Th. 3.5 2b] and [8, Th. 1.2]. The method presented here is preferable in that it is more explicit, and yields independent proofs of [6, Th. 3.5 2b] and [8, Th. 1.2].

3. Canonical and quasi-canonical liftings

In order to construct the field isomorphisms of the previous § we need to develop a generalization of the theory of canonical and quasi-canonical liftings (cf. [5]). We say that the deformation $G/\mathcal{O}$ of $\bar{G}$ is the canonical lifting associated to $\bar{\alpha}: \mathcal{O} \hookrightarrow \mathrm{End}_k(\bar{G})$ if G lifts $\bar{G}$ as a formal $\mathcal{O}$-module.

PROPOSITION 2. *There exists a canonical lifting $G/\mathcal{O}$ of $\bar{G}$ associated to $\bar{\alpha}$. This lifting is unique up to $*$-isomorphism.*

PROOF. By [10, Th. 1] there exists a formal $\mathcal{O}$-module (G', α') of height 1 defined over $\mathcal{O}$. Let $K^{nr} \subset K^{sep}$ be the maximal unramified extension of K, with residue field k^{nr}. Then $(\bar{G}, \bar{\alpha})$ is isomorphic over k^{nr} to the special fiber $(\bar{G}', \bar{\alpha}')$ of (G', α'), and hence corresponds to an element of $H^1(\mathrm{Gal}(k^{nr}/k), \mathrm{Aut}(\bar{G}', \bar{\alpha}'))$. Since $\mathrm{Aut}(\bar{G}', \bar{\alpha}') \cong \mathrm{Aut}(G', \alpha') \cong \mathcal{O}^\times$ there is an isomorphism

$$H^1(\mathrm{Gal}(k^{nr}/k), \mathrm{Aut}(\bar{G}', \bar{\alpha}')) \xrightarrow{\sim} H^1(\mathrm{Gal}(K^{nr}/K), \mathrm{Aut}(G', \alpha')).$$

Therefore there exists a formal $\mathcal{O}$-module $(G, \alpha)/\mathcal{O}$ whose special fiber is $(\bar{G}, \bar{\alpha})$. By [1, Prop. 4.2] the moduli space of deformations of (G, α) is trivial. Therefore G is determined up to $*$-isomorphism. □

Choose $s \geqq 1$. Then $\ker[\pi_A^s]_G$ is a free $(\mathcal{O}/\pi_A^s)$-module of rank 1 and a free (A/π_A^s)-module of rank h, with an action by $\mathrm{Gal}(K^{sep}/K)$. Let $D \subset \ker[\pi_A^s]_G$ be a free (A/π_A^s)-submodule of rank 1 such that $\mathcal{O} \cdot D = \ker[\pi_A^s]_G$. We say that D is a generic submodule of G of level s. Let I_s' denote the ring of integers of the field $K_s' \subset K^{sep}$ generated over K by the roots of $[\pi_A^s]_G$. By [9, Th. 1.4] there exists over I_s' a formal A-module G_D and an isogeny $g: G \to G_D$ with kernel D. The isogeny g may be written explicitly as

$$g(x) = \prod_{\delta \in D} G(x, \delta).$$

The special fiber of g is $\bar{g}(x) = x^{q^s}$, so G_D is a deformation of $\bar{G}^{q^s}$. We say that G_D is a quasi-canonical lifting of $\bar{G}^{q^s}$ of level s. (This generalizes [5, § 5].) The endomorphism ring of G_D is the A-subalgebra of $\mathcal{O}$ which stabilizes D. The constraints on D imply that

$$\mathrm{End}(G_D) = A + \pi_A^s \mathcal{O}.$$

We denote this A-algebra by $\mathcal{O}_s$.

PROPOSITION 3 (cf. [5, Prop. 5.3]). a) *All of the quasi-canonical liftings of* $\bar{G}^{q^s}$ *of level s are defined over the ring of integers* I_s *of a totally ramified abelian extension* K_s *of* K *of degree*

$$|\mathcal{O}^\times/\mathcal{O}_s^\times| = \frac{q^f-1}{q-1}\cdot q^{(h-1)s-f+1}.$$

The norm group $N_s \subset K^\times$ *of* K_s *satisfies* $N_s \cap \mathcal{O}^\times = \mathcal{O}_s^\times$.

b) *The group* $\mathrm{Gal}(K_s/K) \cong \mathcal{O}^\times/\mathcal{O}_s^\times$ *acts simply transitively on the set of quasi-canonical liftings of* $\bar{G}^{q^s}$ *of level s.*

c) *For each* $a \in \mathcal{O}^\times$ *the automorphism* $[a]_{\bar{G}}^{q^s}$ *of* $\bar{G}^{q^s}$ *lifts to an isogeny* $\tilde{a}: G_D \to G_{D'}$, *where* $D' = [a]_G(D)$.

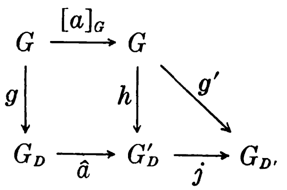
REMARK. The union of the K_s for $s \geqq 1$ is the field L defined in § 2.

PROOF. The formal $\mathcal{O}$-module structure on G gives a transitive action of $\mathcal{O}^\times$ on the roots of $[\pi_A^s]_G$. This induces a transitive action of $\mathcal{O}^\times$ on the set of generic submodules of G of level s. For $a \in \mathcal{O}^\times$ let σ_a be the element of $\mathrm{Gal}(K^{ab}/K)$ which corresponds to a via class field theory. By the theory of Lubin-Tate [10, p. 386] we see that $\sigma_a\delta = [a^{-1}]_G(\delta)$ for every $\delta \in \ker[\pi_A^s]_G$. Therefore the stabilizer of D in $\mathrm{Gal}(K_s'/K) \cong \mathcal{O}^\times/(1+\pi_A^s\mathcal{O})^\times$ is $\mathcal{O}_s^\times/(1+\pi_A^s\mathcal{O})^\times$. Thus g and G_D can be defined over the ring of integers I_s of the subfield K_s of K_s' fixed by $\mathcal{O}_s^\times$. This proves a) and b).

To prove c) choose $a \in \mathcal{O}^\times$ and lift $[a]_{\bar{G}}^{q^s} \in k[[x]]$ arbitrarily to a power series $\hat{a} \in I_s[[x]]$ such that $\hat{a}(0)=0$. Then $\hat{a}$ is an invertible power series, so there is a unique formal A-module G_D'/I_s such that $\hat{a}: G_D \to G_D'$ is an isogeny. Since $[a]_{\bar{G}}^{q^s}$ is an automorphism of $\bar{G}^{q^s}$ we see that G_D' is a deformation of $\bar{G}^{q^s}$. Define $h: G \to G_D'$ by the formula $h = \hat{a}\circ g \circ [a^{-1}]_G$. The special fiber of h is $\bar{h}(x) = x^{q^s}$, and the kernel of h is $D' = [a]_G(D)$. Let g': $G \to G_{D'}$ be the isogeny

$$g'(x) = \prod_{\delta \in D'} G(x, \delta).$$

Since $\ker g' = \ker h$, by [9, Th. 1.5] there exists an isomorphism of formal A-modules $j: G_D' \to G_{D'}$ such that $j \circ h = g'$.



The special fiber of j is the identity. Therefore $\tilde{a} = j\circ\hat{a}$ lifts $[a]_{\bar{G}}^{q^s}$ to an isogeny $G_D \to G_{D'}$. □

4. Construction of $X_K(L)$

For $s \geqq 2$ set $n_s = q^{(h-1)s-h}$ and define $\bar{I}_s = I_s/(\pi_s^{n_s})$. For $s' > s \geqq 2$ let $\bar{N}_{s',s}$: $\bar{I}_{s'} \to \bar{I}_s$ denote the map induced by the norm $N_{K_{s'}/K_s}$: $I_{s'} \to I_s$. In this § we use the results of [13] to show that $\bar{N}_{s',s}$ is a surjective ring homomorphism. We then show that $\varprojlim \bar{I}_s$ is naturally identified with the ring of integers of $X_K(L)$. In § 6 we will use this explicit construction to give isomorphisms between F and $X_K(L)$.

PROPOSITION 4. *For $s' > s \geqq 2$ the map $\bar{N}_{s',s}$: $\bar{I}_{s'} \to \bar{I}_s$ is a surjective ring homomorphism.*

PROOF. It suffices to consider the case $s' = s+1$. For $s \geqq 1$ let v_s denote the valuation on K^{sep} normalized so that $v_s(K_s^{\times}) = \boldsymbol{Z}$. For $\sigma \in \mathrm{Gal}(K_{s+1}/K_s)$ define

$$i(\sigma) = \min_{y \in I_{s+1}} v_{s+1}(\sigma y - y).$$

By [13, Prop. 2.2.1] the proposition is true for $s' = s+1$ as long as

$$(*) \qquad n_s \leqq \frac{p-1}{p} \cdot (i(\sigma) - 1)$$

for every $\sigma \in \mathrm{Gal}(K_{s+1}/K_s)$. This inequality is a consequence of the following lemma.

LEMMA 5. *For $\sigma \in \mathrm{Gal}(K_{s+1}/K_s)$ we have*

$$i(\sigma) \geqq \frac{q^{(h-1)s}}{q-1}.$$

PROOF. Let $\pi'_{s+1} \in K^{sep}$ be a generator for the $\mathcal{O}$-module $\ker[\pi_A^{s+1}]_G$, and set $K'_{s+1} = K(\pi'_{s+1})$. Let v'_{s+1} denote the normalized valuation on K'_{s+1}, and let I'_{s+1} denote the ring of integers of K'_{s+1}. For $\tau \in \mathrm{Gal}(K'_{s+1}/K_s)$ define

$$i'(\tau) = \min_{y \in I'_{s+1}} v'_{s+1}(\tau y - y).$$

The group

$$\mathrm{Gal}(K'_{s+1}/K_{s+1}) \cong \mathcal{O}_{s+1}^{\times}/(1 + \pi_A^{s+1}\mathcal{O})^{\times}$$

has order $(q-1)q^s$. Therefore by [11, IV § 1, Prop. 3], for $\sigma \in \mathrm{Gal}(K_{s+1}/K_s)$ we have

$$i(\sigma) = \frac{1}{(q-1)q^s} \sum i'(\tau),$$

where the sum is taken over all $\tau\in\mathrm{Gal}(K'_{s+1}/K_s)$ whose image in $\mathrm{Gal}(K_{s+1}/K_s)$ is σ.

Since $K_{s+1}\cap K'_s=K_s$ there exists $\tau_0\in\mathrm{Gal}(K'_{s+1}/K'_s)$ whose image in $\mathrm{Gal}(K_{s+1}/K_s)$ is σ. By the theory of Lubin-Tate [10, Th. 2] there exists $u\in(1+\pi_A^s\mathcal{O})^\times$ such that

$$\tau_0\pi'_{s+1}=[u^{-1}]_G(\pi'_{s+1}).$$

Since $u^{-1}\in(1+\pi_A^s\mathcal{O})^\times$ and $\bar{G}$ is a formal A-module of height h we have

$$[u^{-1}]_G(x)\equiv x \qquad (\mathrm{mod}(x^{q^{sh}},\pi_{\mathcal{O}})).$$

The field K'_{s+1} is a totally ramified extension of K of degree $(q^f-1)q^{(s+1)h-f}\geqq q^{sh}$. Therefore

$$[u^{-1}]_G(\pi'_{s+1})\equiv\pi'_{s+1} \qquad (\mathrm{mod}(\pi'_{s+1})^{q^{sh}}).$$

Then since $I'_{s+1}=\mathcal{O}[\pi'_{s+1}]$ we have

$$i'(\tau_0)\geqq q^{sh}$$

$$i(\sigma)\geqq\frac{1}{(q-1)q^s}\cdot q^{sh},$$

which gives the lemma. □

Since $s\geqq 2$ and $i(\sigma)$ is an integer the lemma implies

$$\begin{aligned} i(\sigma)-1 &\geqq \frac{q^{(h-1)s}-1}{q-1} \\ &\geqq q^{(h-1)s-1} \\ \frac{p-1}{p}\cdot(i(\sigma)-1) &\geqq q^{-1}\cdot q^{(h-1)s-1} \\ &\geqq n_s, \end{aligned}$$

which proves (*). This completes the proof of the proposition. □

This proposition allows us to define

$$A_K(L)=\varprojlim \bar{I}_s.$$

By [13, Prop. 2.3.1], the ring of integers of $X_K(L)$ is

$$\varprojlim I_s\subset X_K(L),$$

and the map

$$\nu:\ \varprojlim I_s \longrightarrow A_K(L)$$

induced by the projections $I_s \to \bar{I}_s$ is an isomorphism. We wish to endow $X_K(L)$ with an $\mathcal{O}$-algebra structure by constructing a map j': $\mathcal{O} \to A_K(L)$. Let j_s: $\mathcal{O} \to \bar{I}_s$ denote the composition of natural maps $\mathcal{O} \hookrightarrow I_s \to \bar{I}_s$. Since we do not have $j_{s'} = j_s \circ \bar{N}_{s',s}$ in general, the j_s do not induce a map from $\mathcal{O}$ to $A_K(L)$. To remedy this we need to define an $\mathcal{O}$-algebra structure for the $\bar{I}_s$ which makes $\bar{N}_{s',s}$ an $\mathcal{O}$-algebra homomorphism.

Since K_s is a totally ramified extension of K of degree greater than n_s we see that j_s: $\mathcal{O} \to \bar{I}_s$ factors through the projection $\mathcal{O} \to k$. Therefore the map j'_s: $\mathcal{O} \to \bar{I}_s$ defined by $j'_s(x) = j_s(x^{q^s})$ is a ring homomorphism. Hencefoth we view $\bar{I}_s$ as an $\mathcal{O}$-algebra with structure map j'_s. Since $K_{s'}/K_s$ is a totally ramified extension of degree $q^{(h-1)(s'-s)}$, we see that

$$\bar{N}_{s',s}(j_{s'}(x^{q^{s'}})) = j_s((x^{q^{s'}})^{q^{(h-1)(s'-s)}})$$

$$= j_s(x^{q^s}).$$

Therefore $\bar{N}_{s',s}$ is an $\mathcal{O}$-algebra homomorphism. (However, the projection $I_s \to \bar{I}_s$ need not be an $\mathcal{O}$-algebra homomorphism.)

Our choice of $\mathcal{O}$-algebra structure for $\bar{I}_s$ has one more pleasant consequence. The map j'_s induces an isomorphism of k with the residue field of $\bar{I}_s$. We easily see that this isomorphism identifies the special fiber of $\bar{G}_D = G_D \otimes_{I_s} \bar{I}_s$ with $\bar{G}/k$. Thus $\bar{G}_D$ is a deformation of $\bar{G}$ (rather than $\bar{G}^{q^s}$).

5. Newton polygons

In this § we show that $\bar{G}_D$ has height $h-1$ or h. Since Γ/R is a universal deformation of $\bar{G}$ to height $h-1$ this implies that there is a unique $\mathcal{O}$-algebra homomorphism ε_D: $R \to \bar{I}_s$ such that $\bar{G}_D \cong^* \Gamma^{\varepsilon_D}$. In § 6 we will use the homomorphisms ε_D to construct isomorphisms between F and $X_K(L)$, as promised in § 2.

In order to determine the height of $\bar{G}_D$ we need to determine the Newton polygon of $[\pi_A]_{\bar{G}_D}$. The first step is to compute the Newton polygon of $[\pi_A]_G$. Let e denote the ramification degree of $K/\mathcal{K}$ and let f denote the degree of the residue field extension k/k_0 induced by $K/\mathcal{K}$. We have then $ef = h$.

LEMMA 6. *The vertices of the Newton polygon of* $[\pi_A]_G \in \mathcal{O}[[x]]$ *are the points* $(q^{if}, e-i)$ *for* $0 \leqq i \leqq e$.

REMARK. This shows that $[\pi_A]_G$ has $q^{if} - q^{(i-1)f}$ roots of K-valuation $\dfrac{1}{q^{if} - q^{(i-1)f}}$, for $1 \leqq i \leqq e$.

PROOF. We have $\pi_A=\pi_{\mathcal{O}}^e u$ for some $u\in\mathcal{O}^\times$. We easily see that the vertices of the Newton polygon of $[\pi_{\mathcal{O}}]_G\in\mathcal{O}[[x]]$ are the points $(1,1)$ and $(q^f,0)$, and that the only vertex of the Newton polygon of $[u]_G$ is the point $(1,0)$. Since

$$[\pi_A]_G=[\pi_{\mathcal{O}}]_G\circ\cdots\circ[\pi_{\mathcal{O}}]_G\circ[u]_G,$$

an easy calculation shows that the vertices of the Newton polygon of $[\pi_A]_G$ are the points $(q^{if},e-i)$ for $0\leqq i\leqq e$. □

We now compute the Newton polygon of G_D.

PROPOSITION 7. *The vertices of the Newton polygon of* $[\pi_A]_{G_D}\in I_s[[x]]$ *are the points*

$$P_i=\left(q^{if},(e-i)\cdot\frac{q^f-1}{q-1}\cdot q^{(h-1)s-f+1}-\frac{(q^{(h-1)s}-1)(q^{if}-1)}{q^{h-1}-1}\right)$$

for $0\leqq i\leqq e-1$, *plus the two points* $(q^{h-1},1)$ *and* $(q^h,0)$.

REMARKS. 1) If $f=1$ then the vertices P_{e-1} and $(q^{h-1},1)$ coincide.

2) Let (q^{h-2},y_0) denote the intersection of the Newton polygon with the line $x=q^{h-2}$. Then G_D has height $h-1$ as long as $1<n_s\leqq y_0$. If $f>1$ then

$$\begin{aligned}y_0&=1+\frac{q^{h-1}-q^{h-2}}{q^{h-1}-q^{h-f}}\cdot\left(\frac{q^f-1}{q-1}\cdot q^{(h-1)s-f+1}-\frac{(q^{(h-1)s}-1)(q^{h-f}-1)}{q^{h-1}-1}\right)\\&=1+\frac{q^f-1}{q^{f-1}-1}\cdot q^{(h-1)s-1}-\frac{q-1}{q^{f-1}-1}\cdot\frac{q^{h-f}-1}{q^{h-1}-1}\cdot(q^{(h-1)s}-1)\cdot q^{f-2}\\&\geqq 1+q\cdot q^{(h-1)s-1}-q^{2-f}\cdot q^{1-f}\cdot q^{(h-1)s}\cdot q^{f-2}\\&\geqq n_s,\end{aligned}$$

while if $f=1$ then

$$\begin{aligned}y_0&=2q^{(h-1)s}-\frac{(q^{(h-1)s}-1)(q^{h-2}-1)}{q^{h-1}-1}\\&\geqq 2q^{(h-1)s}-q^{(h-1)s}\cdot q^{-1}\\&\geqq n_s.\end{aligned}$$

Therefore $\bar{G}_D$ has height $h-1$ unless $s=h=2$, in which case $\bar{G}_D$ has height $h=2$.

PROOF. It suffices to show that the K_s-valuations of the roots of $[\pi_A]_{G_D}$ are given by the following table.

Valuation	Multiplicity
∞	1
$\frac{q^{(h-1)s-f+1}}{q-1}+\frac{q^{(h-1)s}-1}{q^{h-1}-1}$	q^f-1
$\frac{q^{(h-1)s-2f+1}}{q-1}+\frac{q^{(h-1)s}-1}{q^{h-1}-1}$	$q^{2f}-q^f$
$\vdots$	$\vdots$
$\frac{q^{(h-1)s-(e-1)f+1}}{q-1}+\frac{q^{(h-1)s}-1}{q^{h-1}-1}$	$q^{(e-1)f}-q^{(e-2)f}$
$\frac{q^{(h-1)s-ef+1}}{q-1}+\frac{q^{(h-1)s}-1}{q^{h-1}-1}$	$q^{ef-1}-q^{(e-1)f}$
$\frac{q^{1-h}}{q-1}$	$q^{ef}-q^{ef-1}$

Let $C_0\subset\ker[\pi_A]_G$ be the image of $\ker[\pi_A]_G$ under the map $[\pi_{\mathcal{O}}]_G$. Since D is a generic submodule of G we clearly have $D\cap C_0=\{0\}$. Let M be an A-submodule of $\ker[\pi_A]_G$ such that $M\supset C_0$, $M\cap D=\{0\}$, and M has index q in $\ker[\pi_A]_G$. The isogeny g maps M onto a submodule of $\ker[\pi_A]_{G_D}$ of index q. For $\mu\in M$ we have

$$v_s(g(\mu))=\sum_{\delta\in D} v_s(G(\mu,\delta)).$$

Let $\delta_0\in D\cap\ker[\pi_A]_G$ with $\delta_0\neq 0$. Since $\delta_0\notin C_0$, Lemma 6 implies that δ_0 has K-valuation $\frac{1}{q^{ef}-q^{(e-1)f}}$. Therefore

$$v_s(\delta_0)=[K_s:K]\cdot\frac{1}{q^{ef}-q^{(e-1)f}}$$
$$=\frac{q^{(h-1)s-h+1}}{q-1}.$$

Therefore if $\delta\in D$ satisfies $[\pi_A^{i-1}]_G(\delta)=\delta_0$ then $v_s(\delta)=\frac{q^{(h-1)s-ih+1}}{q-1}$.

The constraints on M imply that

$$v_s(G(\mu,\delta))=v_s(\delta)$$

for $\mu\in M, \delta\in D\setminus\{0\}$. Hence

$$\sum_{\delta\in D} v_s(G(\mu,\delta)) = v_s(\mu) + \sum_{i=1}^{s}(q^i - q^{i-1})\frac{q^{(h-1)s-ih+1}}{q-1}$$
$$= v_s(\mu) + q^{(h-1)s}\sum_{i=1}^{s} q^{-(h-1)i}$$
$$= v_s(\mu) + \frac{q^{(h-1)s}-1}{q^{h-1}-1}.$$

Lemma 6 gives the following values for $v_s(\mu)$, with the indicated multiplicities.

Valuation	Multiplicity
∞	1
$\dfrac{q^{(h-1)s-if+1}}{q-1}$	$q^{if}-q^{(i-1)f}$ $(1 \leq i < e)$
$\dfrac{q^{(h-1)s-ef+1}}{q-1}$	$q^{ef-1}-q^{(e-1)f}$

This confirms all but the last line of the table. To get that part let δ_1 be a generator for the A-module D and choose $\delta_2 \in \ker[\pi_A^{s+1}]_G$ with $[\pi_A]_G(\delta_2) = \delta_1$. Then $g(\delta_2) \in \ker[\pi_A]_{G_D}$. As above we compute $v_s(\delta_2) = \dfrac{q^{-h-s+1}}{q-1}$. It follows that

$$v_s(g(\delta_2)) = \sum_{\delta\in D} v_s(G(\delta_2,\delta))$$
$$= q^s v_s(\delta_2)$$
$$= \frac{q^{1-h}}{q-1}.$$

This gives the last line of the table. □

6. Isomorphisms of $X_K(L)$ with F

Let T denote the Tate module of G; then T is free of rank 1 over $\mathcal{O}$ and free of rank h over A. We say that V is a generic submodule of T if

1) V is free of rank 1 over A
2) $\mathcal{O}\cdot V = T$.

For each generic submodule V we will construct an isomorphism

$$\varepsilon_V : F \xrightarrow{\sim} X_K(L).$$

We first need to associate to the power series $[\pi_A]_{\bar{G}}$ an element $c \in \mathcal{O}^\times$ which is equal to 1 if and only if $[\pi_A]_{\bar{G}}(x) = x^{q^h}$. Since $\Phi(x) = x^{q^h}$ is a k-endomorphism of $\bar{G}$ which commutes with every element of $\mathrm{End}_k(\bar{G})$, we see that Φ is also an endomorphism of $(\bar{G}, \bar{\alpha})$. Therefore $\Phi = \bar{\alpha}(v)$ for some $v \in \mathcal{O}$. Since $\bar{G}$ is a formal A-module of height h we have $v = c \cdot \pi_A$ for some $c \in \mathcal{O}^\times$.

For $s \geqq 1$ let D be the image of $c^{-s}V$ in $\ker[\pi_A^s]_G$. Then D is a generic submodule of G of level s. Since $(\bar{G}, \bar{\alpha})$ determines c up to multiplication by $A^\times$, the module D is independent of the choice of π_A. As in § 3 we have a quasi-canonical lifting G_D of $\bar{G}^{q^s}$ of level s and an isogeny $g: G \to G_D$ with kernel D.

Now assume $s \geqq 2$. Recall from § 4 that $\bar{G}_D$ is a deformation of $\bar{G}$ with respect to the $\mathcal{O}$-algebra structure on $\bar{I}_s$ induced by j'_s. Proposition 7 implies that the height of $\bar{G}_D$ is $h-1$ or h. Therefore there exists a unique $\mathcal{O}$-algebra homomorphism $\varepsilon_D: R \to \bar{I}_s$ such that $\bar{G}_D \cong^* \Gamma^{\varepsilon_D}$. Choose $s' > s \geqq 1$ and let D' be the image of $c^{-s'}V$ in $\ker[\pi_A^{s'}]_G$. The following proposition shows that $\bar{N}_{s',s}$ is compatible with the maps $\varepsilon_D, \varepsilon_{D'}$.

PROPOSITION 8. *Let $s' > s \geqq 2$. Then the diagram*

$$\begin{array}{ccc} R & & \\ {\scriptstyle \varepsilon_{D'}}\downarrow & \searrow{\scriptstyle \varepsilon_D} & \\ \bar{I}_{s'} & \xrightarrow[\bar{N}_{s',s}]{} & \bar{I}_s \end{array}$$

commutes.

REMARK. This proposition shows that the maps $\varepsilon_D: R \to \bar{I}_s$ induce an $\mathcal{O}$-algebra homomorphism

$$\varepsilon_V: R \longrightarrow \varprojlim \bar{I}_s = A_K(L).$$

The map ε_V is an isomorphism because the natural map

$$R \longrightarrow \varprojlim R/(t^{n_s})$$

is an isomorphism. Since $A_K(L)$ is the ring of integers of $X_K(L)$, it is clear that ε_V extends to an isomorphism of F with $X_K(L)$.

PROOF. It suffices to consider the case $s' = s+1$. By Lemma 5 we have

$$\begin{aligned} i(\sigma) &\geqq \frac{q^{(h-1)s}}{q-1} \\ &\geqq q^{(h-1)s-1} \\ &\geqq [K_{s+1}:K_s]\cdot n_s \end{aligned}$$

for every $\sigma \in \mathrm{Gal}(K_{s+1}/K_s)$. Therefore

$$N_{K_{s+1}/K_s}(x) \equiv x^{q^{h-1}} \qquad (\mathrm{mod}\, \pi_s^{n_s})$$

for every $x \in I_{s+1}$. By Proposition 7 we may choose uniformizers $\pi_D \in I_s$, $\pi_{D'} \in I_{s+1}$ whose images in $\bar{I}_s$, $\bar{I}_{s+1}$ are $\varepsilon_D(t), \varepsilon_{D'}(t)$. Since $\varepsilon_D, \varepsilon_{D'}$, and $\bar{N}_{s+1,s}$ are $\mathcal{O}$-algebra homomorphisms it suffices to show that

$$\pi_{D'}^{q^{h-1}} \equiv \pi_D \qquad (\mathrm{mod}\, \pi_s^{n_s}).$$

By the definition of D and D' we see that $\ker g' \subset \ker(g\circ[c\pi_A]_G)$. Therefore [9, Th. 1.5] implies that there is a unique isogeny of formal A-modules $w_s: G_{D'} \to G_D$, defined over I_{s+1}, such that $w_s \circ g' = g\circ[c\pi_A]_G$. By the definitions of g and c we have

$$\begin{aligned} g\circ[c\pi_A]_G(x) &= \prod_{\delta\in D} G([c\pi_A]_G(x), \delta) \\ &\equiv \prod_{\delta\in D} \bar{G}(x^{q^h}, \delta) \qquad (\mathrm{mod}\, \pi_{\mathcal{O}}). \end{aligned}$$

On the other hand,

$$\begin{aligned} g'(x)^{q^h} &= \prod_{\delta'\in D'} G(x, \delta')^{q^h} \\ &\equiv \prod_{\delta'\in D'} \bar{G}^{q^h}(x^{q^h}, (\delta')^{q^h}) \qquad (\mathrm{mod}\, \pi_{\mathcal{O}}) \\ &\equiv \prod_{\delta'\in D'} \bar{G}(x^{q^h}, [c\pi_A]_{\bar{G}}(\delta')) \qquad (\mathrm{mod}\, \pi_{\mathcal{O}}). \end{aligned}$$

Since $[c\pi_A]_G$ maps D' onto D and $v_s(\pi_{\mathcal{O}}) \geqq qn_s$ we get

$$\begin{aligned} g'(x)^{q^h} &\equiv \prod_{\delta\in D} \bar{G}(x^{q^h}, \delta)^q \qquad (\mathrm{mod}\, \pi_s^{qn_s}) \\ g'(x)^{q^{h-1}} &\equiv \prod_{\delta\in D} \bar{G}(x^{q^h}, \delta) \qquad (\mathrm{mod}\, \pi_s^{n_s}) \\ &\equiv g\circ[c\pi_A]_G(x) \qquad (\mathrm{mod}\, \pi_s^{n_s}). \end{aligned}$$

Since $w_s \circ g' = g\circ[c\pi_A]_G$ it follows that

$$w_s(x) \equiv x^{q^{h-1}} \qquad (\mathrm{mod}\, \pi_s^{n_s}).$$

By our choice of n_s, the inclusion $I_s \hookrightarrow I_{s+1}$ induces an inclusion $\iota_s: \bar{I}_s \hookrightarrow \bar{I}_{s+1}$ (but ι_s is not an $\mathcal{O}$-algebra homomorphism). The congruence for w_s implies

$$\bar{G}_D^{i_s} = \bar{G}_{D'}^{q^{h-1}}.$$

It follows that

$$\iota_s(\varepsilon_D(t)) = \varepsilon_{D'}(t)^{q^{h-1}}$$

$$\pi_D \equiv \pi_{D'}^{q^{h-1}} \qquad (\mathrm{mod}\, \pi_{s+1}^{n_{s+1}}).$$

Since $v_s(\pi_{s+1}^{n_{s+1}}) = q^{1-h} n_{s+1} = n_s$, this completes our proof. □

7. Extensions of F and $X_K(L)$

In this § we prove the isomorphisms of fields over $F \cong X_K(L)$,

$$F' \cong X_{L/K}(L')$$
$$F'' \cong X_{L/K}(K^{ab}).$$

This will complete the proof of Theorem 1.

Choose $a \in \mathcal{O}^\times$ and let $\sigma_a \in \mathrm{Gal}(L/K)$ be the image of a under class field theory. Then σ_a induces automorphisms of I_s, $\bar{I}_s$, $A_K(L)$, and $X_K(L)$. In § 1 we saw that $[a]_{\bar{G}} \in \mathrm{Aut}_k(\bar{G})$ induces an automorphism ϕ_a^* of F. The next proposition shows that the isomorphism $\varepsilon_V : F \xrightarrow{\sim} X_K(L)$ identifies ϕ_a^* with σ_a^{-1}.

PROPOSITION 9. *For every $a \in \mathcal{O}^\times$, the diagram*

$$\begin{array}{ccc} F & \xrightarrow{\varepsilon_V} & X_K(L) \\ {\scriptstyle \phi_a^*}\downarrow & & \downarrow{\scriptstyle \sigma_a^{-1}} \\ F & \xrightarrow[\varepsilon_V]{} & X_K(L) \end{array}$$

commutes.

REMARK. The maximal abelian subextension of K^{sep}/L whose Galois group has trivial action by $\mathrm{Gal}(L/K) \cong \mathcal{O}^\times/A^\times$ is K^{ab}/L. Therefore by [13, Th. 3.2.2], the field $X_{L/K}(K^{ab})$ is a maximal abelian extension of $X_K(L)$ whose Galois group has trivial $(\mathcal{O}^\times/A^\times)$-action. Recall that $F'' \subset F^{sep}$ is the maximal abelian extension of F with trivial action by ϕ_a^* for every $a \in \mathcal{O}^\times$. This proposition implies that the field extensions $X_{L/K}(K^{ab})/X_K(L)$ and F''/F are isomorphic.

PROOF. By Proposition 3 and the choice of $\mathcal{O}$-algebra structure on $\bar{I}_s$, the automorphism $[a]_{\bar{G}}$ of $\bar{G}$ lifts to an isogeny $\tilde{a}_s : \bar{G}_D \to \bar{G}_{D'}$, where $D' = [a]_G(D)$. By Lubin-Tate [10, p. 386] we have $D' = \sigma_a^{-1} D$, and hence $\bar{G}_{D'} = \bar{G}_D^{\sigma_a^{-1}}$. Since $G_D \cong^* \Gamma^{\varepsilon_D}$ and $G_{D'} \cong^* \Gamma^{\varepsilon_{D'}}$, there is an isogeny $\tilde{a}'_s : \Gamma^{\varepsilon_D} \to \Gamma^{\sigma_a^{-1} \circ \varepsilon_D}$ which corresponds to $\tilde{a}_s : G_D \to G_{D'}$. By Proposition 8, the maps ε_D induce an isomorphism $\varepsilon_V: R \to A_K(L)$. Therefore there is an isogeny $\tilde{a}: \Gamma^{\varepsilon_V} \to \Gamma^{\sigma_a^{-1} \circ \varepsilon_V}$ which lifts $[a]_{\bar{G}}$. Since $[a]_{\bar{G}}$ also lifts to an isogeny $\hat{a}: \Gamma \to \Gamma^{\phi_a^*}$, by the universal property of Γ we conclude that $\varepsilon_V \circ \phi_a^* = \sigma_a^{-1} \circ \varepsilon_V$. □

Fix $r \geqq 1$ and let $F_r \subset F^{sep}$ be the extension of F generated by the roots of $[\pi_A^r]_\Gamma^{q^{(h-1)r}}$. We wish to determine the extension of $X_K(L)$ which corresponds to F_r/F. Let $K_s^r \subset K^{sep}$ denote the extension of K_s generated by the roots of $[\pi_A^r]_{G_D}$. We easily see that $K_s^r \subset L'$ is the fixed field of $(1+\pi_A^r A + \pi_A^{s+r}\mathcal{O})^\times$, and hence that

$$\begin{aligned}\mathrm{Gal}(K_s^r/K_{s+r}) &\cong \mathcal{O}_{s+r}^\times/(1+\pi_A^r A+\pi_A^{s+r}\mathcal{O})^\times \\ &\cong A^\times/(1+\pi_A^r A)^\times .\end{aligned}$$

Let $L_r = \bigcup_s K_s^r$. Then $L_r \subset L'$ is the fixed field of $(1+\pi_A^r A)^\times$, and

$$\mathrm{Gal}(L_r/L) \cong \mathrm{Gal}(K_s^r/K_{s+r}) .$$

PROPOSITION 10. *The fields F_r and $X_K(L_r)$ are isomorphic extensions of $F \cong X_K(L)$.*

REMARK. It follows from this proposition that $F' = \bigcup F_r$ and $X_{L/K}(L') = \bigcup X_K(L_r)$ are isomorphic extensions of $F \cong X_K(L)$.

PROOF. Choose $s \geqq 2$ and for $s \leqq i \leqq s+r$ let D_i denote the image of $c^{-i}V$ in $\ker[\pi_A^i]_G$. In the proof of Proposition 8 we defined an isogeny $w_i: G_{D_{i+1}} \to G_{D_i}$ such that

$$w_i(x) \equiv x^{q^{h-1}} \qquad (\mathrm{mod}\, \pi_i^{n_i}) .$$

Set $D = D_s$, $D' = D_{s+r}$ and let $W: G_{D'} \to G_D$ be the composition

$$\begin{aligned}W(x) &= w_s \circ w_{s+1} \circ \cdots \circ w_{s+r-1}(x) . \\ &\equiv x^{q^{(h-1)r}} \qquad (\mathrm{mod}\, \pi_s^{n_s}) .\end{aligned}$$

Let $\iota_s': \bar{I}_s \hookrightarrow \bar{I}_{s+r}$ be the map induced by $I_s \hookrightarrow I_{s+r}$. Then the congruence for W implies

$$\bar{G}_D^{\iota_s'} = \bar{G}_{D'}^{q^{(h-1)r}} .$$

Therefore

$$\bar{G}_D^{\iota_s'} \cong^* (\Gamma^{\varepsilon_{D'}})^{q^{r(h-1)}} .$$

Let I_s^r denote the ring of integers of K_s^r, and let $\bar{I}_s^r = I_s^r/(\pi_{s+r}^{n_{s+r}})$. Then G_D has rational π_A^r-torsion over K_s^r, and hence $(\Gamma^{\varepsilon_{D'}})^{q^{r(h-1)}}$ has rational π_A^r-torsion over $\bar{I}_s^r$. Since this holds for every $s \geqq 2$, we conclude that

$(\Gamma^{\varepsilon V})^{q^{r(h-1)}}$ has rational π_A^r-torsion over $A_K(L_r)=\varprojlim \bar{I}_s^r$. Since F_r is generated by the roots of $[\pi_A^r]_\Gamma^{q^{(h-1)r}}$, we see that F_r is isomorphic to a subextension of $X_K(L_r)/X_K(L)$. But since $[X_K(L_r): X_K(L)]=[F_r: F]=(q-1)q^{r-1}$, the extensions F_r/F and $X_K(L_r)/X_K(L)$ must be isomorphic. □

8. Applications

In this § we use the results of § 7 and the theory of the field of norms to give new proofs of two known results. First we deduce the ramification breaks of χ_Γ from the ramification data for $\mathrm{Gal}(L'/L)$. Afterwards we use the ramification structure of $\mathrm{Gal}(L/K)$ to determine the endomorphism ring of the reduction of Γ (mod t^n).

Let E be a complete discretely valued field with ring of integers T, uniformizer π_T, and finite residue field. Let H be an abelian extension of E, and set $\mathcal{F}=\mathrm{Gal}(H/E)$. For $i\geqq 0$ we define the ith ramification subgroup $\mathcal{F}^i$ of $\mathcal{F}$ to be the image of $(1+\pi_T^i T)^\times$ in $\mathcal{F}$. (This is equivalent to the usual definition—see [11, XV § 2, Th. 2].) For real $u\geqq 0$ we set $\mathcal{F}^u=\mathcal{F}^i$ whenever $i\geqq u>i-1$. Since $[\mathcal{F}^0: \mathcal{F}^i]$ is finite we may define the (inverse) Herbrand function $\psi_{H/E}: [0,\infty)\to[0,\infty)$ by the formula

$$\psi_{H/E}(x)=\int_0^x [\mathcal{F}^0: \mathcal{F}^u]\, du\,.$$

Now take $E=K$ and $H=L$ so that $\mathcal{F}\cong\mathcal{O}^\times/A^\times$. Let $m\geqq 0$ and $0\leqq b<e$ be integers which aren't both 0. By the definition of $\psi_{L/K}$ we see that

$$\frac{d}{dx}\psi_{L/K}(x)=|\mathcal{O}^\times/A^\times(1+\pi_{\mathcal{O}}^{me+b}\mathcal{O})^\times|$$

$$=\frac{q^f-1}{q-1}\cdot q^{(h-1)m+(b-1)f}$$

whenever $me+b-1<x<me+b$. From this formula we easily deduce the following lemma.

LEMMA 11. *Let m and b be integers such that $m\geqq 0$ and $0\leqq b<e$. Define*

$$a((h-1)m)=\frac{(q^h-1)(q^{(h-1)m}-1)}{(q-1)(q^{h-1}-1)}\,.$$

Then

$$\psi_{L/K}(me+b)=a((h-1)m)+q^{(h-1)m}\cdot\frac{q^{bf}-1}{q-1}\,.$$

Let F and F' be the fields defined in § 1, and set $\mathcal{H}=\mathrm{Gal}(F'/F)\cong A^{\times}$. Since F is a local field the ramification groups $\mathcal{H}^{i}\subset\mathcal{H}$ are defined. The following proposition determines $\mathcal{H}^{i}$ as a subgroup of $A^{\times}$.

PROPOSITION 12. *If* $a((h-1)(m-1))<i\leqq a((h-1)m)$ *then*

$$\mathcal{H}^{i}\cong(1+\pi_{A}^{m}A)^{\times}.$$

PROOF. Let L' be the maximal totally ramified abelian extension of K associated to the Lubin-Tate group (G,α) (cf. § 2). Set $\mathcal{G}=\mathrm{Gal}(L'/K)\cong\mathcal{O}^{\times}$. Then by Proposition 10 the group $\mathcal{H}$ is identified with the subgroup $A^{\times}$ of $\mathcal{G}\cong\mathcal{O}^{\times}$. By [13, Cor. 3.3.6] the ramification groups of $\mathcal{H}$ and $\mathcal{G}$ are related by the formula $\mathcal{H}^{\phi_{L/K}(u)}=\mathcal{G}^{u}\cap\mathcal{H}$. For $m\geqq 0$ and $0\leqq b<e$ we have

$$\begin{aligned}\mathcal{G}^{me+b}\cap\mathcal{H}&\cong(1+\pi_{\mathcal{O}}^{me+b}\mathcal{O})^{\times}\cap A^{\times}\\&\cong(1+\pi_{A}^{m}A)^{\times}.\end{aligned}$$

Therefore $\mathcal{H}^{i}\cong(1+\pi_{A}^{m}A)^{\times}$ whenever $\phi_{L/K}((m-1)e)<i\leqq\phi_{L/K}(me)$. The proposition now follows from Lemma 11. □

Let A be the ring of integers of a complete discretely valued field $\mathcal{K}$ with finite residue field $k_0\cong\mathbf{F}_q$, as in § 1. Let k_0^{nr} be an algebraic closure of k_0, and let $\bar{G}/k_0^{nr}$ be a formal A-module of height $1<h<\infty$. Define $S=k_0^{nr}[[t]]$ and $S_n=S/(t^{n+1})$, and let Γ/S be a universal deformation of $\bar{G}$ to height $h-1$. Set $B=\mathrm{End}_{k_0^{nr}}(\bar{G})$ and $D=B\otimes_A\mathcal{K}$. By [1, Prop. 1.7] the ring D is a division algebra of rank h^2 over $\mathcal{K}$ with invariant $1/h$. By [1, Prop. 4.1] the natural map $\mathrm{End}_{S_n}(\Gamma)\to\mathrm{End}_{k_0^{nr}}(\bar{G})$ is injective. Therefore $\mathrm{End}_{S_n}(\Gamma)$ may be viewed as an A-subalgebra of $\mathrm{End}_{k_0^{nr}}(\bar{G})=B$.

The following proposition allows us to determine $\mathrm{End}_{S_n}(\Gamma)$ as an A-subalgebra of B. Let $\pi_B\in B$ be an endomorphism of $\bar{G}$ of height 1. Then π_B is a uniformizer for B, so the powers of π_B induce a filtration on B.

PROPOSITION 13. *Let* π_B *be a uniformizer for* B *and choose* $\phi\in\mathrm{End}_{k_0^{nr}}(\bar{G})=B$ *such that*

$$\phi\in(A+\pi_B^{l}B)\smallsetminus(A+\pi_B^{l+1}B)\qquad(l\geqq 0).$$

Write $l=hm+b$ *with* $0\leqq b<h$ *and set*

$$n=a((h-1)m)+q^{(h-1)m}\cdot\frac{q^{b}-1}{q-1}+1.$$

Then ϕ *lifts to* $\mathrm{End}_{S_{n-1}}(\Gamma)$ *but not to* $\mathrm{End}_{S_n}(\Gamma)$.

PROOF. We may assume that $\phi\in \mathrm{Aut}_k(\bar{G})$. (Otherwise replace ϕ by $1+\phi$.) Let $\phi^*\in \mathrm{Aut}_k(R)$ be such that ϕ lifts to an isogeny $\tilde{\phi}: \Gamma\to(\Gamma)^{\phi^*}$. Define

$$i(\phi^*)=v_t(\phi^*(t)-t).$$

One easily sees (cf. [7, Prop. 1.3]) that the conclusion of the proposition is equivalent to the statement

$$i(\phi^*)=a((h-1)m)+q^{(h-1)m}\cdot\frac{q^b-1}{q-1}+1.$$

Let $K\subset D$ be a field extension of $\mathcal{K}$ such that $\phi\in K$ and $[K:\mathcal{K}]=h$. We will construct an extension L/K as in § 3 and show that the automorphism ϕ^* of $R\cong A_K(L)$ is induced by an element of $\mathrm{Gal}(L/K)$.

Let $\mathcal{O}$ be the ring of integers of K, and let $k\cong \mathbf{F}_{q^f}$ be the residue field of $\mathcal{O}$. The embedding $K\hookrightarrow D$ induces an embedding $\bar{\alpha}: \mathcal{O}\hookrightarrow B$, and hence an action of $\mathcal{O}$ on the tangent space of $\bar{G}$. This action induces an inclusion of k into k_0^{nr} and gives k_0^{nr} an $\mathcal{O}$-algebra structure such that the pair $(\bar{G},\bar{\alpha})$ is a formal $\mathcal{O}$-module. By [10, Th. 1] there exists a formal $\mathcal{O}$-module $(\bar{G}',\bar{\alpha}')$ which is defined over k. Set $R=k[[t]]$ and let Γ'/R be a universal deformation of the formal A-module $\bar{G}'$ to height $h-1$. By [1, Prop. 1.7] there exists an isomorphism ψ from $(\bar{G},\bar{\alpha})$ to $(\bar{G}',\bar{\alpha}')$ defined over k_0^{nr}. Then ψ induces an isomorphism between the filtered rings $\mathrm{End}(\bar{G})$ and $\mathrm{End}(\bar{G}')$.

By the universal property of Γ' there is a homomorphism $\tau: R\to S$ such that

$$(\Gamma')^{\tau}\cong^* \psi\circ\Gamma\circ\psi^{-1}.$$

It follows that ϕ lifts to $\mathrm{End}_{S_i}(\Gamma)$ if and only if $\psi\circ\phi\circ\psi^{-1}$ lifts to an endomorphism of $\Gamma'\otimes_R(R/t^{i+1})$. Therefore we may assume that $(\bar{G},\bar{\alpha})$ is defined over k, and that Γ is defined over $k[[t]]$.

Just as in § 2 we associate to $(\bar{G},\bar{\alpha})$ a totally ramified abelian extension L of K. Class field theory gives an onto map $\mathcal{O}^\times\to\mathcal{G}=\mathrm{Gal}(L/K)$ whose kernel is $A^\times$. Let $\sigma\in\mathcal{G}$ denote the image of $\phi\in\mathcal{O}^\times$ under this map. By Proposition 9 we see that ϕ^* is the automorphism of $R\cong A_K(L)$ induced by σ^{-1}. The hypothesis on ϕ and the choice of K imply that σ lies in $\mathcal{G}^i\setminus\mathcal{G}^{i+1}$, where $i=l/f$. Then by [13, Cor. 3.3.4] we have $i(\phi^*)=\psi_{L/K}(l/f)+1$. The proposition now follows from Lemma 11. □

References

[1] Drinfeld, V. G., Elliptic modules (Russian), Mat. Sb. **94**(136) (1974), 594-627, 656; English translation: Math. USSR-Sb. **23** (1976), 561-592.

[2] Fontaine, J. M., Corps de séries formelles et extensiones galoisiennes des corps locaux, Séminaire de Théorie des Nombres de Grenoble, Université de Grenoble-I, 1971-1972, 28-38.
[3] Fröhlich, A., Formal Groups, Lecture Notes in Math. vol. 74, Springer-Verlag, Berlin, 1968.
[4] Fujiwara, Y., On Galois actions on p-power torsion points of some one-dimensional formal groups over $\mathbf{F}_p[[t]]$, J. Algebra **113** (1988), 491-510.
[5] Gross, B., On canonical and quasi-canonical liftings, Invent. Math. **84** (1986), 321-326.
[6] Gross, B., Ramification in p-adic Lie extensions, Astérisque **65** (1979), 81-102.
[7] Keating, K., Galois characters attached to formal A-modules, Compositio Math. **67** (1988), 241-269.
[8] Keating, K., Lifting endomorphisms of formal A-modules, Compositio Math. **67** (1988), 211-239.
[9] Lubin, J., Finite subgroups and isogenies of one-parameter formal Lie groups, Ann. of Math. **85** (1967), 296-302.
[10] Lubin, J. and J. Tate, Formal complex multiplication in local fields, Ann. of Math. **81** (1965), 380-387.
[11] Serre, J.-P., Corps Locaux, Hermann, Paris, 1962.
[12] Wintenberger, J.-P., Extensions abéliennes et groupes d'automorphisms des corps locaux, C. R. Acad. Sci. Paris **290** (1980), A201-A203.
[13] Wintenberger, J.-P., Le corps des normes de certaines extensions infinies de corps locaux; applications, Ann. Sci. École. Norm. Sup. (4) **16** (1983), 59-89.

(Received January 25, 1989)

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
U. S. A.