COMPOSITIO MATHEMATICA

KEVIN KEATING

# Galois characters associated to formal $A$-modules

*Compositio Mathematica*, tome 67, n° 3 (1988), p. 241-269
<http://www.numdam.org/item?id=CM_1988__67_3_241_0>

Compositio Mathematica 67: 241–269 (1988)



# Galois characters associated to formal $A$-modules

KEVIN KEATING
*Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA*

Received 25 August 1987; accepted in revised form 3 February 1988

**Abstract.** Let $F_0/\mathbf{F}_p$ be a formal group law of height 2, and let $F/\mathbf{F}_p[[t]]$ be a universal deformation of $F_0$ to the category of complete noetherian local $\mathbf{F}_p$-algebras. Associated to $F$ is a character $\gamma_F$: $\mathrm{Gal}(K_s/K) \to \mathbf{Z}_p^\times$, where $K = \mathbf{F}_p((t))$. By class field theory this character is identified with a continuous homomorphism $\chi_F$: $K^\times \to \mathbf{Z}_p^\times$. In this paper we give generators for $U_K \cap \ker \chi_F$. This result is used to give an abstract characterization of the Igusa tower.

## Introduction

Let $\kappa$ be a complete discretely valued field with finite residue field $\mathbf{F}_q$ and let $A$ be the ring of integers in $\kappa$. Let $S$ be an $A$-algebra, with structure map $\gamma$: $A \to S$. A *formal $A$-module $F/S$* is defined to be a 1-parameter formal group law $\tilde{F}/S$ together with a homomorphism

$$\phi\colon A \to \mathrm{End}_S(\tilde{F})$$

such that the induced map

$$\phi_*\colon A \to \mathrm{End}_S(\mathrm{Lie}\,\tilde{F}) \cong S$$

is the same as $\gamma$: $A \to S$. Given formal $A$-modules defined over $S$ we define $\mathrm{Hom}_S(F, G)$ to consist of those group-law homomorphisms $f \in \mathrm{Hom}_S(\tilde{F}, \tilde{G})$ such that

$$f \circ \phi_F(a) = \phi_G(a) \circ f$$

for every $a \in A$. Let $\pi = \pi_A$ be a uniformizer for the discretely valued ring $A$. If the endomorphism $\phi_F(\pi)(x) = [\pi]_F(x)$ is zero we say that $F$ has infinite height. If this endomorphism is not zero it can be written in the form

$$[\pi]_F(x) = s(x^{q^h})$$

with $h > 0$ and $s'(0) \neq 0$. In this case we say that $F$ has (finite) height $h$.

Assume now that $S$ is a local $A$-algebra, with maximal ideal $\mathcal{M}_S$ and residue field $k$. Let $F_0$ be a formal $A$-module over $k$. A *deformation* of $F_0$ over $S$ is a formal $A$-module $F/S$ whose reduction (mod $\mathcal{M}_S$) is $F_0$. Let $F_0$ be a formal $A$-module of height $h < \infty$ over the field $k$ and let $F$ be a deformation of $F_0$ over $R = k[[t]]$ of height $g = h - 1$. We write

$$[\pi]_F(x) = a_0 x^{q^g} + \cdots$$

and set $e = v_t(a_0)$. In the case $e = 1$ Lubin-Tate [11, Prop. 3.3] associate to $F$ an action of $\mathrm{Aut}_k(F_0)$ on $R$. The purpose of this paper is to study this action by using the results of [7]. The most interesting theorems which arise from this study give data about the Galois character $\chi_F$ associated to $F$. A related approach to the study of $\chi_F$ can be found in [3].

The work presented here is part of the author's 1987 Harvard Ph.D. thesis, written under the inspiring direction of Professor Benedict Gross.

## 1. Universal deformations of formal $A$-modules

Again we let $S$ be a complete noetherian local $A$-algebra, with maximal ideal $\mathcal{M}_S$ and residue field $k$. Let $F_0/k$ be a formal $A$-module and let $F$ and $F'$ be two deformations of $F_0$ defined over $S$. A $*$-*isomorphism* $\psi\colon F \to F'$ is an isomorphism between the $A$-modules $F$ and $F'$ which satisfies

$$\psi(x) \equiv x \pmod{\mathcal{M}_S}.$$

The deformations $F$ and $F'$ are isomorphic if there exists a $*$-isomorphism between them. Assume that $F_0$ has finite height $h$ and let $F/S$ be a deformation of $F_0$ of height $g < h$. We say that $F$ is a universal height-$g$ deformation of $F_0$ if, given another height-$g$ deformation $F'$ of $F_0$ over a complete noetherian local $A$-algebra $S'$, there exists a unique $A$-algebra homomorphism $\sigma\colon S \to S'$ such that $F^\sigma$ is $*$-isomorphic to $F'$.

Let $k$ be a field extension of $A/(\pi) \cong \mathbf{F}_q$, and let $R = k[[t]]$. Then $k$ and $R$ can be made into $A$-algebras in an obvious way. Let $F_0/k$ be a formal $A$-module of height $h$, and let $F/R$ be a deformation of $F_0$ of height $h - 1$. We write

$$[\pi]_F(x) = a_0 x^{q^{h-1}} + \cdots$$

and set $e = v_t(a_0) > 0$.

THEOREM 1.1. *Let $h \geqslant 2$ and $g = h - 1$. There exist universal height-$g$ deformations of $F_0$ defined over $R = k[[t]]$. The deformation $F/R$ is universal if and only if $e = 1$.*

REMARKS:

1. If $g = h - d$ with $0 < d < h$ then the universal height-$g$ deformation of $F_0$ is defined over $k[[t_1, \ldots, t_d]]$.
2. As this theorem makes evident, there isn't a unique universal deformation of $F_0$ of height $h - 1$. However, if $F/R$ and $F'/R$ are two such deformations there is a unique $\sigma \in \mathrm{Aut}\,(R/k)$ such that $F^\sigma$ is $*$-isomorphic to $F'$.

*Proof.* This theorem is essentially a special case of [2, Prop. 4.2]. If $A = \mathbf{Z}_p$ so that $F$ is a formal group law, $F$ is $*$-isomorphic to

$$\Gamma(0, \ldots, 0, -a_0),$$

for some Lubin-Tate universal deformation $\Gamma(t_1, \ldots, t_{h-1})$ of $F_0$ (see [11, Prop. 1.1 and Th. 3.1]). □

Henceforth we take $g = h - 1$ and assume that $F$ is a universal height-$g$ deformation of $F_0$. If $F'/R$ is any deformation of $F_0$ of height $g$ we write

$$[\pi]_{F'}(x) = a'_0 x^{q^g} + \cdots .$$

There exists a homomorphism $\sigma$: $R \to R$ such that $F'$ is $*$-isomorphic to $F^\sigma$. The formal $A$-module $F^\sigma$ is defined over $\sigma(R) \subset R$, and is a universal height-$g$ deformation of $F_0$ over $\sigma(R)$. If $v_t(a'_0) > 1$ the deformation $F^\sigma$ is not universal over $R$.

Recall that $\kappa = \mathrm{Frac}\,(A)$ and let $D_{1/h}$ be the central division algebra of degree $h^2$ over $\kappa$ with invariant $1/h$. By [2, Prop. 1.7], $\mathrm{End}_k(F_0)$ is isomorphic to an $A$-subalgebra of the maximal order $B$ in $D_{1/h}$. Henceforth we identify $\mathrm{End}_k(F_0)$ with a subalgebra of $B$. Choose $f \in \mathrm{Aut}_k(F_0)$. We are interested in lifting $f$ to an isogeny defined over $R$. Since $\mathrm{Aut}_k(F) = A^\times$, $f$ cannot in general be lifted to an automorphism of $F$; however, we can lift $f$ to an isomorphism between two different universal deformations of $F_0$ (cf. [11, Prop. 3.3]). Since $k \hookrightarrow R$ we may consider $f$ as an invertible power series with coefficients in $R$. Set

$$F'(x, y) = f \circ F(f^{-1}(x), f^{-1}(y))$$

$$[a]_{F'}(x) = f \circ [a]_F \circ f^{-1}(x) \qquad (a \in A).$$

This gives another formal $A$-module $F'/R$ which is isomorphic to $F/R$ (but not necessarily $*$-isomorphic). Since $f$ is an automorphism of $F_0$, the special fiber of $F'$ is $F_0$. Theorem 1.1 implies that $F'$ is a universal deformation of $F_0$. Therefore we get a unique $k$-linear automorphism $\sigma$ of $R$ such that there exists a $*$-isomorphism $\alpha$: $F' \to F^\sigma$. Let $\tilde{f}$: $F \to F^\sigma$ be the composition of $\alpha$ with $f$.

$$F \xrightarrow{f} F' \xrightarrow{\alpha} F^\sigma$$

The isomorphism $\tilde{f}$ induces the automorphism $f$: $F_0 \to F_0$ on the special fiber $F_0$ of $F$ and $F^\sigma$. Since $\sigma \in \mathrm{Aut}_k(R)$ is unique, there is a well-defined map

$$\begin{aligned} \Psi_F\colon \mathrm{Aut}_k(F_0) &\to \mathrm{Aut}_k(R). \\ f &\mapsto \sigma_f \end{aligned}$$

Since $\Psi_F$ is well-defined it follows easily that $\Psi_F$ is an anti-homomorphism, with kernel $\mathrm{Aut}_k(F) = A^\times$.

Both $\mathrm{Aut}_k(F_0)$ and $\mathrm{Aut}_k(R)$ have natural filtrations. To describe the filtration of $\mathrm{Aut}_k(F_0)$ we observe that the ring $B$ has a valuation $v_B$ such that $v_B(\pi_A) = h$. We choose $\pi_B \in B$ such that $v_B(\pi_B) = 1$. Then $\mathrm{Aut}_k(F_0)$ is filtered by the subgroups

$$\mathrm{Aut}_k(F_0) \cap (A + \pi_B^n B)^\times \quad (n \geqslant 0).$$

In order to define a filtration on $\mathrm{Aut}_k(R)$ we set

$$i(\sigma) = v_t\left(\frac{\sigma t - t}{t}\right)$$

for $\sigma \in \mathrm{Aut}_k(R)$. Then $\mathrm{Aut}_k(R)$ has a filtration by the subgroups

$$G_n = \{\sigma\colon i(\sigma) \geqslant n\} \quad (n \geqslant 0).$$

The filtrations of $\mathrm{Aut}_k(F_0)$ and $\mathrm{Aut}_k(R)$ are related by $\Psi_F$. To describe this relationship we define $R_n = R/(t^{n+1})$ and set

$$a(gm) = \frac{(q^{gm} - 1)(q^h - 1)}{(q^g - 1)(q - 1)}$$

with $g = h - 1$ so that we may quote the following crucial theorem.

THEOREM 1.2. ([7, Th. 3.3]) *Let $F_0/k$ be a formal A-module of height h and let $F/R$ be a universal height-g deformation of $F_0$. Choose $f \in \mathrm{End}_k(F_0)$ such that*

$$f \in (A + \pi_B^l B) \setminus (A + \pi_B^{l+1} B)$$

*for some $l \geqslant 0$. Then f lifts to $\mathrm{End}_{R_{n-1}}(F)$ but not to $\mathrm{End}_{R_n}(F)$, where*

$$l = hm + b \quad (0 \leqslant b < h)$$

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

REMARKS:

1. By [2, Prop. 4.1] we know there exists at most one lifting of $f$ to $\mathrm{End}_{R_n}(F)$.
2. The nonnegative integers $a(gm)$ are the upper ramification breaks of the Galois character $\gamma_F$ associated to $F$. They play an important role in what follows.

The following proposition relates liftings of endomorphisms of $F_0$ to the filtration of $\mathrm{Aut}_k(R)$. When combined with Theorem 1.2 it gives the relation between the filtrations of $\mathrm{Aut}_k(F_0)$ and $\mathrm{Aut}_k(R)$ that we are looking for.

PROPOSITION 1.3. *Assume that $f \in \mathrm{Aut}_k(F_0)$ lifts to $\mathrm{Aut}_{R_{n-1}}(F)$ but not to $\mathrm{Aut}_{R_n}(F)$. Then $\sigma = \Psi_F(f)$ satisfies $i(\sigma) = n - 1$.*

*Proof.* As before we set $F' = f \circ F \circ f^{-1}$. For $i \geqslant 0$ let $F_i' = F' \otimes_R R_i$ be the reduction of $F'$ $(\mathrm{mod}\,(t^{i+1}))$. For each $i$ there is a unique map $\sigma_i\colon R \to R_i$ such that $F_i'$ is $*$-isomorphic to $F^{\sigma_i}$. Since $\sigma_i$ is unique and $F'$ is $*$-isomorphic to $F^{\sigma}$, $\sigma_i$ must be the composition of $\sigma$ with reduction $(\mathrm{mod}\,(t^{i+1}))$. For $i = n - 1$ this implies that $\sigma_{n-1}\colon R \to R_{n-1}$ is reduction $(\mathrm{mod}\,(t^n))$ since $f$ lifts to an automorphism of $F_{n-1}$. Therefore

$$\sigma t \equiv \sigma_{n-1} t \quad (\mathrm{mod}\,(t^n))$$

$$\equiv t \quad (\mathrm{mod}\,(t^n)).$$

For $i = n$ we know that $f$ does not lift to an automorphism of $F_n$; therefore $\sigma_n\colon R \to R_n$ is not the reduction map. Hence

$$\sigma t \equiv \sigma_n t \quad (\mathrm{mod}\,(t^{n+1}))$$

$$\not\equiv t \quad (\mathrm{mod}\,(t^{n+1})).$$

We conclude that $i(\sigma) = n - 1$. □

COROLLARY 1.4. *Let $f$ be an automorphism of $F_0$ which is an element of $(A + \pi_B^l B)^\times$ but not an element of $(A + \pi_B^{l+1} B)^\times$, for some $l \geqslant 0$. Write $l = mh + b$ with $0 \leqslant b < h$, and let $\Psi_F(f) = \sigma$. Then*

$$i(\sigma) = a(gm) + q^{gm} \cdot \frac{q^b - 1}{q - 1}.$$

*Proof.* This follows easily from Proposition 1.3 and Theorem 1.2. □

REMARK. Sen [12, Th. 1] proves that if $j \geqslant 1$ and $\sigma^{p^j}$ is not the identity then

$$i(\sigma^{p^j}) \equiv i(\sigma^{p^{j-1}}) \pmod{p^j}.$$

Since $\Psi_F(f)^{p^j} = \Psi_F(f^{p^j})$ we can calculate $i(\sigma^{p^j})$ explicitly when $\sigma = \Psi_F(f)$. For example, let $F$ be a universal deformation of a formal group law $F_0$ of height 2 over a field $k$ of characteristic $p > 3$. Choose $f \in \mathrm{Aut}_k(F_0)$ which satisfies $v_B(f - 1) = 1$ and let $\sigma = \Psi_F(f)$. We have then

$$v_B(f^{p^j} - 1) = 1 + 2j$$

$$i(\sigma^{p^j}) = a(j) + p^j$$

$$= \frac{2p^{j+1} - p - 1}{p - 1}.$$

If $i(\sigma) > 0$ the inequality $i(\sigma^{p^j}) > i(\sigma^{p^{j-1}})$ and Sen's formula imply that $i(\sigma^{p^j}) - i(\sigma^{p^{j-1}})$ is a positive multiple of $p^j$. In this example,

$$i(\sigma^{p^j}) - i(\sigma^{p^{j-1}}) = 2p^j,$$

so the $i(\sigma^{p^j})$ are not quite as small as Sen's formula allows.

Sen also points out that if $i(\sigma) > 0$ and $\sigma$ has infinite order, the limit

$$\lim_{j \to \infty} i(\sigma^{p^j}) \in \mathbf{Z}_p$$

is defined. When $\sigma = \Psi_F(f)$ this limit depends only on $A$ and $h$ and not on $f$ or $F$. If $i(\sigma) > 0$ then

$$\lim_{j \to \infty} i(\sigma^{p^j}) = \lim_{m \to \infty} \left[ a(gm) + q^{gm} \cdot \frac{q^b - 1}{q - 1} \right]$$

$$= \lim_{m \to \infty} a(gm)$$

$$= \lim_{m\to\infty} \frac{(q^h - 1)(q^{gm} - 1)}{(q^g - 1)(q - 1)}$$

$$= \frac{1 - q^h}{(1 - q^g)(1 - q)}.$$

The meaning of these numbers is obscure.

## 2. The Galois character associated to $F$

Let $F/R$ be a deformation of the type considered previously. In this section we construct the Galois character $\gamma_F$ associated to $F$ and compute certain elements of $\ker \gamma_F$. In the next section we will show that in certain cases these elements generate $I \cap \ker \gamma_F$, where $I$ is the inertia subgroup of $\mathrm{Gal}(K_s/K)$.

Let $K = k((t))$. Gross [5, p. 86] associates to $F$ a Galois character

$$\gamma_F\colon \mathrm{Gal}(K_s/K) \to A^\times.$$

To describe this character we first define characters

$$\gamma_n\colon \mathrm{Gal}(K_s/K) \to (A/\pi^n)^\times$$

for each $n \geqslant 1$. Since $[\pi]_F(x)$ is a power series in $x^{q^g}$ with $g = h - 1$, $[\pi^n]_F(x)$ is a power series in $x^{q^{gn}}$. By the Weierstrass preparation theorem $[\pi^n]_F(x)$ factors into

$$[\pi]_F(x) = u_n(x^{q^{gn}}) \cdot c_n(x^{q^{gn}})$$

with $u_n(x^{q^{gn}})$ a unit in $R[[x]]$ and $c_n(x^{q^{gn}})$ a distinguished polynomial of degree $q^{hn}$. The polynomial $c_n(x^{q^{gn}})$ has $q^n$ distinct roots in $\bar{K}$ which form a principal $A/(\pi^n)$-module under the action of $F$. The group $\mathrm{Aut}(\bar{K}/K)$ acts on these roots. Since $\mathrm{Aut}(\bar{K}/K) \cong \mathrm{Gal}(K_s/K)$, this action defines a character

$$\gamma_n\colon \mathrm{Gal}(K_s/K) \to (A/(\pi^n))^\times.$$

Then since $\gamma_n$ is the reduction $(\mathrm{mod}\,(\pi^n))$ of $\gamma_{n+1}$, by taking the inverse limit of these finite characters we get a character

$$\gamma_F\colon \mathrm{Gal}(K_s/K) \to A^\times.$$

When $k$ is a finite field local class field theory identifies $K^\times$ with a dense subgroup of the abelianization of $\mathrm{Gal}(K_s/K)$; by composing the class field theory map with $\gamma_F$ we get a character

$$\chi_F\colon K^\times \to A^\times.$$

Henceforth we asume that $k$ is a finite field and we work with $\chi_F$ rather than $\gamma_F$.

As our notation suggests, $\chi_F$ depends on the choice of $F$. However, if we choose another universal height-$g$ deformation $F'$ of $F_0$ there is a unique $k$-linear automorphism $\sigma$ of $R$ such that $F^\sigma$ is $*$-isomorphic to $F'$. It follows that $\chi_{F'} = \chi_{F^\sigma}$. On the other hand, if $\sigma$ is any $k$-linear automorphism of $K$ then the functoriality of class field theory [13, p. 178] and the functoriality of $\gamma_n$ imply that $\chi_F = \chi_{F^\sigma} \circ \sigma$. Therefore $\chi_{F'} = \chi_F \circ \sigma^{-1}$, which shows that $\chi_F$ and $\chi_{F'}$ differ only by an automorphism of $K$.

Let $f$ be a $k$-automorphism of $F_0$. We can lift $f$ to an isomorphism $\tilde{f}\colon F \to F^\sigma$, where $\sigma = \Psi_F(f)$ is a $k$-linear automorphism of $R$ (and $K$). Since $F$ and $F^\sigma$ are isomorphic we have $\chi_F = \chi_{F^\sigma}$. This implies

$$\chi_F \circ \sigma = \chi_F.$$

In particular, if $\alpha \in K^\times$ and $\sigma = \Psi_F(f)$ for $f \in \mathrm{Aut}_k(F_0)$ then $\sigma\alpha/\alpha \in \ker \chi_F$. This gives us a method of finding elements of $\ker \chi_F$; in some cases we can calculate these elements explicitly (see Section 4). What is remarkable is that in certain important cases the subgroup

$$\left\{\frac{\sigma\alpha}{\alpha} : \alpha \in K^\times, \sigma = \Psi_F(f), f \in \mathrm{Aut}_k(F_0)\right\}$$

is dense in $U_K \cap \ker \chi_F$. This surprising fact is the subject of Section 3.

## 3. The kernel of $\chi_F$

Before we attempt to find generators for $U_K \cap \ker \chi_F$ we would like to identify some elements of $U_K$ which are not in $\ker \chi_F$. The theory of higher ramification groups is a tool which allows us to find such elements. We review here the relevant facts about ramification groups.

Let $k$ be a finite field, let $K = k((t))$, and let $L$ be an abelian extension of $K$ with $G = \mathrm{Gal}(L/K)$. The group $G$ has a filtration by the "upper ramification groups" $G_n$ ($n \geqslant 0$). One way to describe these groups uses class field theory: Let $\omega_{L/K}\colon K^\times \to G$ be the reciprocity map of class field theory, and set

$$U_K^n = \{x \in U_K\colon v_K(x - 1) \geqslant n\}$$

for $n \geqslant 0$. Then we define

$$G^n = \omega_{L/K}(U_K^n).$$

We say that $n$ is a ramification break of $G$ if $G^n \neq G^{n+1}$.

In [5, Th. 3.5] the ramification breaks of the abelian extension of $K = k((t))$ cut out by $\chi_F$ are calculated. It is shown that

$$\chi_F(U_K^{a(gm)}) = (1 + \pi^m A)^\times$$

$$\chi_F(U_K^{a(gm)+1}) = (1 + \pi^{m+1} A)^\times$$

where $a(gm)$ is given by

$$a(gm) = \frac{(q^h - 1)(q^{gm} - 1)}{(q^g - 1)(q - 1)}.$$

(As usual, $g = h - 1$ here.) For $m = 0$ this result implies that $\chi_F$ maps $U_K/U_K^1 \cong k^\times$ onto $A^\times/(1 + \pi A)^\times \cong \mathbf{F}_q^\times$; for $m > 0$ it implies that $\chi_F$ maps $U_K^n/U_K^{n+1} \cong k^+$ onto $(1 + \pi^m A)^\times/(1 + \pi^{m+1} A)^\times \cong \mathbf{F}_q^+$, where $n = a(gm)$. If $k = \mathbf{F}_q$, it follows that $U_K^n \cap \ker \chi_F \subset U_K^{n+1}$. In particular, if $\beta \in U_K^n \smallsetminus U_K^{n+1}$ with $n = a(gm)$ then $\beta \notin \ker \chi_F$. If $k \cong \mathbf{F}_{q^f}$ with $f > 1$ the situation is more complicated: The image of $U_K^n \cap \ker \chi_F$ in $U_K^n/U_K^{n+1}$ has order at most $q^{f-1}$ (or $(q^f - 1)/(q - 1)$ if $n = 0$).

Now we let $F_0/k$ be a formal group law of height 2 with $k = \mathbf{F}_p$ or $k = \mathbf{F}_{p^2}$, and let $F$ be a universal deformation of $F_0$ over $R = k[[t]]$. We wish to find generators for $U_K \cap \ker \chi_F$. We begin by quoting a lemma of Sen which allows us to say something about the units $\sigma\alpha/\alpha \in \ker \chi_F$.

LEMMA 3.1. ([12, Lemma 1]). *Let $k$ be a field and let $K = k((t))$. Choose $\sigma \in \mathrm{Aut}_k(K)$ and set*

$$x_\mu = t \cdot \sigma t \cdot \ldots \cdot \sigma^{\mu-1} t$$

*for* $\mu > 0$. *Then*

$$v_K(\sigma x_\mu - x_\mu) = \mu + i(\sigma^\mu)$$

$$v_K\left(\frac{1 + \sigma x_\mu}{1 + x_\mu} - 1\right) = \mu + i(\sigma^\mu).$$

$$v_K\left(\frac{\sigma x_\mu}{x_\mu} - 1\right) = i(\sigma^\mu).$$

*Proof.* Since $\sigma x_\mu = (\sigma^\mu t/t) \cdot x_\mu$ we have

$$\begin{aligned} v_K(\sigma x_u - x_u) &= v_K\left(\left(\frac{\sigma^\mu t}{t} - 1\right) x_\mu\right) \\ &= v_K(x_\mu) + v_K\left(\frac{\sigma^\mu t}{t} - 1\right) \\ &= \mu + i(\sigma^\mu), \end{aligned}$$

which gives the first equation. The second and third equations follow easily from the first. □

REMARK. This lemma has a partial converse: If $i(\sigma) > 0$ and there exists $\alpha \in K^\times$ such that

$$v_K\left(\frac{\sigma\alpha}{\alpha} - 1\right) = n$$

then $n$ can be written either as $\mu + i(\sigma^\mu)$ or as $i(\sigma^\mu)$ for some $\mu > 0$.

The following lemma is useful in conjunction with Lemma 3.1.

LEMMA 3.2. *Assume* $\sigma \in \mathrm{Aut}_k(K)$ *and let* $\alpha$ *and* $\beta$ *be 1-units of* $K$ *such that*

$$\alpha = 1 + x$$

$$v_K(\sigma x - x) = n$$

$$v_K(\beta - 1) = n.$$

*Then there exists* $s \in k^\times$ *such that* $\alpha' = 1 + sx$ *satisfies*

$$\frac{\sigma\alpha'}{\alpha'} \equiv \beta \pmod{(t^{n+1})}.$$

*Proof.* Let $\sigma x = x + \varepsilon$. Then

$$\varepsilon = at^n + \ldots \qquad (a \in k^\times)$$

$$\beta = 1 + bt^n + \ldots \quad (b \in k^\times).$$

Choose $s \in k^\times$ such that $sa = b$ and set $\alpha' = 1 + sx$. Then we have

$$\begin{aligned}\frac{\sigma\alpha'}{\alpha'} &= \frac{1 + sx + s\varepsilon}{1 + sx} \\ &= 1 + \frac{s\varepsilon}{1 + sx} \\ &\equiv 1 + sat^n \pmod{(t^{n+1})} \\ &\equiv \beta \pmod{(t^{n+1})}\end{aligned}$$

as claimed. □

We now give topological generators for $U_K \cap \ker\chi_F$ in the case $k = \mathbf{F}_p$.

THEOREM 3.3. *Let* $F_0$ *be a formal group law of height 2 over* $k = \mathbf{F}_p$ *and let* $F$ *be a universal height-1 deformation of* $F_0$ *over* $R = \mathbf{F}_p[[t]]$. *Choose* $f \in \mathrm{Aut}_{\mathbf{F}_p}(F_0)$ *such that*

$$f^{p^m} \in (\mathbf{Z}_p + \pi_B^{2m+1}B) \setminus (\mathbf{Z}_p + \pi_B^{2m+2}B)$$

*for every* $m \geqslant 0$, *and set* $\sigma = \Psi_F(f) \in \mathrm{Aut}(K)$, *where* $K = \mathbf{F}_p((t))$. *Then given* $\beta \in U_K \cap \ker\chi_F$ *with* $v_K(\beta - 1) = n$ *there exists* $\alpha \in K^\times$ *such that*

$$\frac{\sigma\alpha}{\alpha} \equiv \beta \pmod{(t^{n+1})}.$$

*Therefore the subgroup*

$$\left\{\frac{\sigma\alpha}{\alpha}: \alpha \in K^{\times}\right\}$$

*is dense in* $U_K \cap \ker\chi_F$.

REMARKS.

1. If $p > 3$ and

$$f \in (\mathbf{Z}_p + \pi_B B)\setminus(\mathbf{Z}_p + \pi_B^2 B)$$

the hypothesis of the theorem is satisfied. For instance, let

$$\begin{aligned} f(x) &= F_0(x, x^p) \\ &= (1 + \mathrm{Fr})(x) \end{aligned}$$

where Fr is the frobenius endomorphism of $F_0$.

2. Fujiwara [3, Th. 1] proves essentially the same theorem by a different but related method.

*Proof.* We give the proof only for odd $p$; the case $p = 2$ is handled similarly. Let $n = v_K(\beta - 1) = a(m)$ with $\beta \in U_K \cap \ker\chi_F$. If $n = a(m)$ is a ramification break for $\chi_F$ then

$$\chi_F(\beta) \in (1 + p^m\mathbf{Z}_p)^{\times}\setminus(1 + p^{m+1}\mathbf{Z}_p)^{\times}.$$

Since we're assuming $\chi_F(\beta) = 1$ we conclude that $n = v_K(\beta - 1)$ is not a ramification break for $\chi_F$. In particular, $n$ is not zero, so we write

$$\beta = 1 + bt^n + \ldots$$

with $b \in \mathbf{F}_p^{\times}$.

We intend to apply Lemma 3.1 and Lemma 3.2 with $\mu = p^m r$, where $m$ and $r$ are defined as follows. If $n \not\equiv 1 \pmod p$ set $r = n - 1$ and $m = 0$. If $n \equiv 1 \pmod p$ then by considering the $p$-adic expansion of $n$ we find $r$ and $m$ which satisfy

$$n = (r + 2)p^m + 2p^{m-1} + \cdots + 2p + 1$$

$$m > 0$$

$$r \geqslant -2$$

$$r \not\equiv 0 \pmod p.$$

In both cases we have

$$n = (r + 1)p^m + a(m).$$

If $r > 0$ set $\mu = p^m r$. By Lemma 3.1 and Lemma 3.2 it suffices to show that $n = \mu + i(\sigma^\mu)$. Since $(r, p) = 1$,

$$\begin{aligned} i(\sigma^\mu) &= i((\sigma^{p^m})^r) \\ &= i(\sigma^{p^m}). \end{aligned}$$

Using Corollary 1.4 and the assumption about $f^{p^m}$ we find that

$$\begin{aligned} \mu + i(\sigma^\mu) &= p^m r + i(\sigma^{p^m}) \\ &= p^m r + a(m) + p^m \\ &= n, \end{aligned}$$

which is just what we need.

If $r = -2$ we let $\mu = p^{m-1}$. By Lemma 3.1,

$$\begin{aligned} v_K\left(\frac{\sigma x_\mu}{x_\mu} - 1\right) &= i(\sigma^{p^{m-1}}) \\ &= a(m - 1) + p^{m-1} \\ &= n. \end{aligned}$$

Therefore there is $s > 0$ such that

$$\frac{\sigma x_\mu^s}{x_\mu^s} \equiv \beta \pmod{(t^{n+1})}.$$

Finally, if $r = -1$ then $n = a(m)$ is a ramification break for $\chi_F$. □

By repeated use of Theorem 3.3 we find $\alpha_m \in K^\times$ such that

$$\frac{\sigma \alpha_m}{\alpha_m} \equiv \beta \pmod{(t^{n+m})}$$

for any given $m > 0$. Unfortunately, it may happen that

$$\lim_{m\to\infty} v_K(\alpha_m) = \infty$$

which means that we can't define

$$\alpha = \lim_{m\to\infty} \alpha_m$$

such that $\sigma\alpha/\alpha = \beta$. In order to get a complete set of generators for $U_K \cap \ker\chi_F$ we need to use class field theory descent.

THEOREM 3.4. *Let $F_0$ be a formal group law of height 2 over $k = \mathbf{F}_{p^2}$ with $p > 2$ and let $F$ be a universal height-1 deformation of $F_0$ over $R = \mathbf{F}_{p^2}[[t]]$. Let $K = \mathbf{F}_{p^2}((t))$ and assume that there exists $f \in \mathrm{Aut}_k(F_0)$ such that*
*a) $f$ generates $B^\times/(\mathbf{Z}_p + \pi_B B)^\times \cong \mathbf{F}_{p^2}^\times/\mathbf{F}_p^\times$.*
*b) $f^{p+1} \in (\mathbf{Z}_p + \pi_B^2 B)\setminus(\mathbf{Z}_p + \pi_B^3 B)$.*
*Let $\sigma = \Psi_F(f)$ and choose $\beta \in U_K \cap \ker\chi_F$ with $v_K(\beta - 1) = n$.*
1. *If $n$ is not a ramification break for $\chi_F$ there exists $\alpha \in U_K$ such that*

$$\frac{\sigma\alpha}{\alpha} \equiv \beta \pmod{(t^{n+1})}.$$

2. *If $n$ is a ramification break for $\chi_F$ there exists $\alpha \in K^\times$ such that*

$$\frac{\sigma\alpha}{\alpha} \equiv \beta \pmod{(t^{n+1})}.$$

*Therefore the subgroup*

$$\left\{\frac{\sigma\alpha}{\alpha} : \alpha \in K^\times\right\}$$

*is dense in $U_K \cap \ker\chi_F$.*
3. *Let $K_0 = \mathbf{F}_p((t))$ and assume that there exists a continuous character*

$$\chi_0 : K_0^\times \to \mathbf{Z}_p^\times$$

*such that $\chi_F = \chi_0 \circ \mathrm{N}_{K/K_0}$. Then there exists $\alpha \in U_K$ and*

$$c \in \ker(\mathrm{N}_{K/K_0} : K^\times \to K_0^\times)$$

*such that $\beta = c \cdot \sigma\alpha/\alpha$. This holds in particular if $F$ can be defined over $\mathbf{F}_p[[t]]$.*

REMARKS.

1. Class field theory implies that $\ker N_{K/K_0} \subset \ker \chi_F$. Therefore $c \in \ker \chi_F$.
2. Let $\mathcal{O}$ be the ring of integers in the unramified quadratic extension of $\mathbf{Q}_p$. If $\mathrm{End}_{\mathbf{F}_{p^2}}(F_0)$ contains a subring isomorphic to $\mathcal{O}$ we may construct $f$ which satisfies a) and b) as follows. Let $\zeta \in \mathcal{O} \subset \mathrm{End}_{\mathbf{F}_{p^2}}(F_0)$ be a primitive $p^2 - 1$ root of unity and set $f = \zeta + p$. The smallest power of $f$ which lies in $\mathbf{Z}_p + \pi_B B$ is

$$\begin{aligned} f^{p+1} &= \zeta^{p+1} + (p+1)p\zeta^p + \dots \\ &\equiv \zeta^{p+1} + p\zeta^p \pmod{p^2} \\ &\in (\mathbf{Z}_p + \pi_B^2 B) \setminus (\mathbf{Z}_p + \pi_B^3 B). \end{aligned}$$

   Therefore $f$ satisfies a) and b).
3. Let $F$ be a universal height $g$ deformation of the formal $A$-module $F_0/k$ of height $h$. If $A \neq \mathbf{Z}_p$ or $h > 2$ then the methods presented here are not sufficient to determine $U_K \cap \ker \chi_F$. In such cases it would be interesting to know the group structure of the quotient of $U_K$ by the closure of

$$\left\{ \frac{\sigma\alpha}{\alpha} : \alpha \in K^\times, \quad \sigma = \Psi_F(f), \quad f \in \mathrm{Aut}_k(F_0) \right\}.$$

*Proof.* We have $\sigma t = at + \dots$ with $\alpha \in k^\times$. Since

$$\sigma^n t = a^n t + \dots,$$

$a^n = 1$ if and only if $i(\sigma^n) > 0$. Hence by Corollary 1.4, $a^n = 1$ if and only if $f^n \in \mathbf{Z}_p + \pi_B B$. Hypothesis a) implies that this holds if and only if $p + 1 \mid n$. Therefore $\alpha$ is a primitive $p + 1$ root of unity.

If $n = v_K(\beta - 1)$ is not a ramification break then $\beta$ is a 1-unit (since $a(0) = 0$) and we can write

$$\beta = 1 + bt^n + \dots \quad (b \in \mathbf{F}_{p^2}^\times).$$

If $p + 1 \nmid n$ then $v_K(\sigma(t^n) - t^n) = n$. Hence by Lemma 3.2 there exists $\alpha \in U_K^n$ such that

$$\frac{\sigma\alpha}{\alpha} \equiv \beta \pmod{(t^{n+1})},$$

which proves the first statement in this case.

To handle the cases with $p + 1 \mid n$ we need the following lemma.

LEMMA 3.5. *Let* $\tau = \sigma^{p+1}$ *and choose* $\alpha, \beta \in U_K$ *such that*

$$\frac{\tau\alpha}{\alpha} \equiv \beta \pmod{(t^{n+1})}.$$

*Then* $\alpha' = \alpha \cdot \sigma\alpha \cdot \ldots \cdot \sigma^p\alpha$ *satisfies*

$$\frac{\sigma\alpha'}{\alpha'} \equiv \beta \pmod{(t^{n+1})}.$$

*Proof.* This follows from the equation $\sigma\alpha'/\alpha' = \sigma^{p+1}\alpha/\alpha = \tau\alpha/\alpha$. □

Assume $p + 1 \mid n$ so that $n = (p + 1)n'$. By considering its $p$-adic expansion we write $n'$ uniquely in the form

$$n' = (r + 1)p^m + p^{m-1} + \cdots + p + 1$$

with $r = 0$ or $r > 0, p \nmid r$. If $r = 0$ then $n = (p + 1)n'$ is the ramification break $a(m + 1)$. If $r > 0$ we let $\mu = p^m(p + 1)r$. Then by Lemma 3.1,

$$\begin{aligned} v_K(\tau x_\mu - x_\mu) &= \mu + i(\tau^\mu) \\ &= p^m r(p + 1) + i(\tau^{p^m}). \end{aligned}$$

Since $p > 2$ and

$$f^{p+1} \in (\mathbf{Z}_p + \pi_B^2 B) \setminus (\mathbf{Z}_p + \pi_B^3 B),$$

it follows easily that

$$f^{(p+1)p^m} \in (\mathbf{Z}_p + \pi_B^{2m+2} B) \setminus (\mathbf{Z}_p + \pi_B^{2m+3} B).$$

Therefore Corollary 1.4 implies that

$$\begin{aligned} i(\tau^{p^m}) &= a(m + 1) \\ v_K(\tau x_\mu - x_\mu) &= p^m r(p + 1) + a(m + 1) \\ &= p^m r(p + 1) + \frac{(p + 1)(p^{m+1} - 1)}{p - 1} \\ &= (p + 1)n' \\ &= n. \end{aligned}$$

By Lemma 3.2 and Lemma 3.5 there exists $\alpha' \in U_K$ such that

$$\frac{\sigma\alpha'}{\alpha'} \equiv \beta \pmod{(t^{n+1})}.$$

This completes the proof of the first statement of the theorem.

To prove the second statement we consider $\beta \in U_K \cap \ker\chi_F$ such that $n = v_K(\beta - 1)$ is a ramification break for $\chi_F$. If $n = 0$ then

$$\beta = bt + \ldots$$

for some $b \in \mathbf{F}_{p^2}^{\times}$. In fact $b \in (\mathbf{F}_{p^2}^{\times})^{p-1} = \boldsymbol{\mu}_{p+1}$ because $\chi_F$ maps $\mathbf{F}_{p^2}^{\times}$ onto $\boldsymbol{\mu}_{p-1} \subset \mathbf{Z}_p^{\times}$. Since

$$\sigma t = at + \ldots$$

with $a$ a primitive $p + 1$ root of unity, there is a positive integer $s$ such that

$$\frac{\sigma t^s}{t^s} = b + \ldots$$

$$\equiv \beta \pmod{(t)}.$$

If $n = a(m) > 0$ we let $\tau = \sigma^{p+1}$ and $\mu = p^{m-1}$ so that

$$v_t\left(\frac{\tau x_\mu}{x_\mu} - 1\right) = v_t\left(\frac{\tau^{p^{m-1}}t}{t} - 1\right)$$

$$= i(\tau^{p^{m-1}})$$

$$= a(m).$$

The character $\chi_F$ induces a surjective map

$$U_K^n/U_K^{n+1} \to (1 + p^m\mathbf{Z}_p)^{\times}/(1 + p^{m+1}\mathbf{Z}_p)^{\times}.$$

The kernel of this map has order $p$, and is generated by $\tau x_\mu/x_\mu$. Therefore there is $s > 0$ such that

$$\beta \equiv \left(\frac{\tau x_\mu}{x_\mu}\right)^s \pmod{(t^{n+1})}$$

$$\equiv \frac{\tau(x_\mu^s)}{x_\mu^s} \pmod{(t^{n+1})}.$$

The second statement of the theorem now follows from Lemma 3.5.

To prove the third statement we take $\beta \in U_K \cap \ker\chi_F$ with $n = v_K(\beta - 1) = a(m)$. We wish to find $c \in \ker N_{K/K_0}$ such that

$$\beta \equiv c \pmod{(t^{n+1})}.$$

If $n = 0$ then

$$\beta = b + \ldots$$

with $b \in \mu_{p+1} \subset \mathbf{F}_{p^2}^{\times}$, so we set $c = b \in \ker N_{K/K_0}$. If $n > 0$ it is easy to see that $U_K^n \cap \ker N_{K/K_0}$ maps onto a subgroup of $U_K^n/U_K^{n+1}$ of order $p$. The image of $\beta$ is in this subgroup, because $\ker N_{K/K_0} \subset \ker\chi_F$ and $\chi_F$ maps $U_K^n/U_K^{n+1}$ onto

$$(1 + p^m\mathbf{Z}_p)^{\times}/(1 + p^{m+1}\mathbf{Z}_p)^{\times}.$$

Therefore we get $c \in \ker N_{K/K_0}$ such that

$$c \equiv \beta \pmod{(t^{n+1})}.$$

We have shown that any $\beta_0 \in U_K \cap \ker\chi_F$ can be approximated by some $c_0 \in \ker N_{K/K_0}$ or by $\sigma\alpha_0/\alpha_0$ for some $\alpha_0 \in U_K$. Also note that $v_K(c_0 - 1)$ and $v_K(\alpha_0 - 1)$ go to infinity as $n = v_K(\beta_0 - 1)$ goes to infinity. Given $\beta \in U_K \cap \ker\chi$ we make successive approximations to $\beta$ by elements of the form $c_0 \cdot \sigma\alpha_0/\alpha_0$ with $c_0 \in \ker N_{K/K_0}$ and $\alpha_0 \in U_K$. By taking the limit we find $c \in U_K \cap \ker N_{K/K_0}$ and $\alpha \in U_K$ such that $\beta = c \cdot \sigma\alpha/\alpha$. □

## 4. An explicit $\sigma$

In this section we give an example of a formal group law $F_0/\mathbf{F}_9$ and a universal deformation $F/\mathbf{F}_9[[t]]$ of $F_0$ such that a particular $\sigma = \Psi_F(f)$ ($f \in \mathrm{Aut}_{\mathbf{F}_9}(F_0)$) can be computed explicitly. We get $F_0$ and $F$ as the formal groups of elliptic curves, and $f$ is induced by an isogeny of elliptic curves.

We consider the Legendre elliptic curve with full level-2 structure over the $\lambda$-line, with equation

$$y^2 = x(x - 1)(x - \lambda) \quad (\lambda \neq 0, 1, \infty).$$

There is an analogue to the classical modular equation for elliptic curves which applies to curves with level-2 structure. Consider the equation

$$X^2(1 - Y)^2 - 16(1 - X)Y = 0$$

whose generic solution is $(\lambda(\tau), \lambda(2\tau))$, where $\lambda(\tau)$ is the standard modular function of level 2. Corresponding to a solution $(\lambda_1, \lambda_2)(\lambda_i \neq 0, 1, \infty)$ of this equation are two elliptic curves

$$E_1 : y^2 = x(x - 1)(x - \lambda_1)$$

$$E_2 : y^2 = x(x - 1)(x - \lambda_2)$$

related by a 2-isogeny $\phi$: $E_1 \to E_2$ which maps (0, 0) and $(\lambda_1, 0)$ onto (0, 0) and maps (0, 1) onto $\infty$. (Warning: To define $\phi$ it may be necessary to extend the base field.)

Our plan is to find $\lambda_0 \in k$ such that

$$E_0 : y^2 = x(x - 1)(x - \lambda_0)$$

is a supersingular elliptic curve, and $(\lambda_0, \lambda_0)$ satisfies our analogue of the modular equation. We observe then that the elliptic curve

$$E : y^2 = x(x - 1)(x - \lambda_0 - t)$$

is a universal deformation of $E_0$ over $R = k[[t]]$, so the formal group $F$ of $E$ is a universal deformation of the formal group $F_0$ of $E_0$. Assuming $\phi \in \mathrm{End}(E_0)$ is defined over $k$, $\phi$ lifts to a map $E \to E^\sigma$, for some $\sigma \in \mathrm{Aut}_k(R)$. Therefore the induced endomorphism $\tilde{\phi}$ of $F_0$ lifts to a map $F \to F^\sigma$. To determine $\sigma$ we use our version of the modular equation. The pair $(\lambda_0 + t, \lambda_0 + \sigma t)$ must satisfy the equation

$$X^2(1 - Y)^2 - 16(1 - X)Y = 0.$$

The last step is to solve this equation for $Y = \lambda_0 + \sigma t$ in terms of $X = \lambda_0 + t$.

For our example we take $k = \mathbf{F}_9$ and $\lambda_0 = -1$. Then $\mathrm{End}(E_0)$ is defined over $k$. The point $(\lambda_0, \lambda_0)$ satisfies our modular equation, and the corresponding elliptic curve has

$$j_0 = 2^8 \cdot \frac{(\lambda_0^2 - \lambda_0 + 1)^3}{\lambda_0^2(1 - \lambda_0)^2}$$

$$= 0$$

which implies that

$$E_0 : y^2 = x(x-1)(x+1)$$

is supersingular. We define $E$ by the equation

$$y^2 = x(x-1)(x+1-t).$$

Then $E$ has $\lambda$-invariant $t-1$. When we solve the modular equation for $Y$ in terms of $X$ we find that

$$Y = \frac{X^2 - 8X + 8 \pm 4(X-2)\sqrt{1-X}}{X^2}$$

$$= \frac{X^2 + X - 1 \pm (X+1)\sqrt{1-X}}{X^2}.$$

Set $X = t - 1$ and $Y = \sigma t - 1$. It follows then that

$$\sigma t = 1 + \frac{t^2 - t - 1 \pm t\sqrt{-1-t}}{(t-1)^2}$$

$$= \frac{-t^2 \pm it\sqrt{1+t}}{(t-1)^2}$$

where $i \in \mathbf{F}_9$ is a square root of $-1$. The two different values of $\sigma t$ correspond to the liftings of two different endomorphisms of $E_0$ which have the same kernel $\{\infty, (0, 1)\}$. From now on we take

$$\sigma t = \frac{-t^2 + it\sqrt{1+t}}{(t-1)^2}$$

$$= it + (-1+i)t^2 + (1-i)t^3 + it^4 + (-1+i)t^5 + \ldots$$

We now want to show that $\tilde{\phi}$ satisfies the hypotheses of Theorem 3.4. Since $i$ is a primitive 4th root of unity, $\tilde{\phi}$ satisfies hypothesis a) of Theorem 3.4. To show that $\tilde{\phi}$ satisfies hypothesis b) we have to calculate the first few terms of $\sigma^4 t$:

$$\sigma^2 t = -t + it^2 + t^3 + (-1+i)t^5 + \ldots$$

$$\sigma^4 t = t - t^5 + \ldots.$$

Hence $i(\sigma^4) = 4 = a(1)$. Then by Corollary 1.4 we see that

$$\tilde{\phi}^4 \in (\mathbf{Z}_3 + \pi_B^2 B) \setminus (\mathbf{Z}_3 + \pi_B^3 B),$$

so $\tilde{\phi}$ satisfies hypothesis b) of Theorem 3.4.

Now we can invoke Theorem 3.4, which says that the power series of the form

$$\left\{ \frac{\sigma\alpha}{\alpha} : \alpha \in K = \mathbf{F}_9((t)) \right\}$$

are dense in $U_K \cap \ker \chi_F$, with $\sigma$ as given above. The theorem also says that every $\beta \in U_K \cap \ker \chi_F$ has the form $\beta = \sigma\alpha/\alpha \cdot c$ where $\alpha \in U_K$, $c \in \ker \mathrm{N}_{K/K_0}$, $K_0 = \mathbf{F}_3((t))$.

## 5. Igusa curves

In this section we outline how the techniques developed in Sections 1–3 may be used to derive an abstract characterization of the Igusa tower. In this section we always assume $p > 2$.

The Igusa tower is a collection of smooth projective curves $\{X_n\}_{n \geq 0}$ with covering maps $X_{n+1} \to X_n$ for each $n$. The curve $X_0$ is the projective $j$-line, and for $n$ positive $X_n$ is an abelian cover of $X_0$, with

$$\mathrm{Gal}(X_n/X_0) \cong (\mathbf{Z}/p^n)^\times/(\pm 1).$$

Since $X_n$ is a nonsingular curve over $\mathbf{F}_p$ it is determined by its field of $\mathbf{F}_p$-rational functions. In order to describe the function field $K_n$ of $X_n$ as an extension of $K_0 = \mathbf{F}_p(j)$ we construct a generic elliptic curve $E/K_0$ with invariant $j$. Associated to $E$ is a Galois character $\gamma_E$, analogous to the character $\gamma_F$ constructed in Section 2. To construct $\gamma_E$ we first observe that the $p^n$-torsion group of $E(\bar{K}_0)$ is isomorphic to $\mathbf{Z}/p^n$. The group $\mathrm{Aut}(\bar{K}_0/K_0) \cong \mathrm{Gal}((K_0)_s/K_0)$ acts on the $p^n$-torsion of $E$ and gives a character

$$\gamma_n : \mathrm{Gal}((K_0)_s/K_0) \to (\mathbf{Z}/p^n)^\times.$$

These $\gamma_n$ fit together to give a character

$$\gamma_E : \mathrm{Gal}((K_0)_s/K_0) \to \mathbf{Z}_p^\times.$$

The characters $\gamma_n$ and $\gamma_E$ actually depend on our choice of generic elliptic curve $E$, but if we compose these maps with the reduction maps

$$(\mathbf{Z}/p^n)^\times \to (\mathbf{Z}/p^n)^\times/(\pm 1)$$

$$\mathbf{Z}_p^\times \to \mathbf{Z}_p^\times/(\pm 1)$$

the resulting characters $\bar{\gamma}_n$ and $\bar{\gamma}_E$ depend only on the $j$-invariant of $E$. Therefore the subfield $K_n$ of $(K_0)_s$ cut out by

$$\bar{\gamma}_n : \mathrm{Gal}((K_0)_s/K_0) \to (\mathbf{Z}/p^n)^\times/(\pm 1)$$

is well-defined. The $n$th Igusa curve is the unique smooth curve over $\mathbf{F}_p$ with function field $K_n$. See [6, Ch. 12] for a systematic treatment of the Igusa curves.

Let $E_0/\bar{\mathbf{F}}_p$ be an elliptic curve, with invariant $j_0$. If $E_0(\bar{\mathbf{F}}_p)$ has no points of order $p$ we say that $E_0$ is a supersingular elliptic curve and $j_0$ is a supersingular $j$-invariant. If $E_0$ is supersingular then $j_0 \in \mathbf{F}_{p^2}$ ([6, Lemma 12.5.4]). The point on $X_0$ associated to $j_0 \in \bar{\mathbf{F}}_p$ is wildly ramified in the Igusa tower if and only if $j_0$ is supersingular. The other points of $X_0$ are called "ordinary". If $j_0 = 0$ is an ordinary point of $X_0$, it has ramification degree 3 in the Igusa tower; if $j_0 = 1728$ is an ordinary point it has ramification degree 2 in the Igusa tower. All other ordinary points of $X_0$ are unramified in the Igusa tower. In order to determine the cover $X_n$ of the genus-0 curve $X_0$, we wish to understand the cover locally near the finitely many points that ramify. To solve this local problem we use the methods of Section 3. Once we've solved the "local Igusa problem" at the supersingular points, we use class field theory to give a global characterization of the Igusa tower.

To see how these methods are applied we consider a supersingular $j_0$. To avoid unnecessary complications we assume $j_0 \in \mathbf{F}_p \setminus \{0, 1728\}$. (If $p \geqslant 13$ such a $j_0$ exists.) Since $j_0 \neq 0, 1728$, we may choose our generic elliptic curve $E/K_0$ to have good reduction $E_0$ at $(j - j_0)$. Setting $t = j - j_0$ we see that $E$ gives an elliptic curve $E_{j_0}$ over $R = \mathbf{F}_p[[t]]$ which is a universal deformation of $E_0$. The formal group $F$ of $E_{j_0}$ is a universal deformation of the formal group $F_0$ of $E_0$. Let $K_{j_0} = \mathbf{F}_p((t))$. It is easily seen that the Galois characters

$$\gamma_{E_{j_0}} : \mathrm{Gal}((K_{j_0})_s/K_{j_0}) \to \mathbf{Z}_p^\times$$

$$\gamma_F : \mathrm{Gal}((K_{j_0})_s/K_{j_0}) \to \mathbf{Z}_p^\times$$

are identical. Since $\mathrm{Gal}((K_{j_0})_s/K_{j_0})$ is isomorphic to the decomposition group of $\mathrm{Gal}((K_0)_s/K_0)$ at $(j - j_0)$, we can view $\gamma_{E_{j_0}} = \gamma_F$ as the restriction

of $\gamma_E$ to this decomposition group. Suppose we have an isogeny of degree prime to $p$ from $E_{j_0}$ to another universal deformation $E_{j_0'}$ of $E_0$. (Such an isogeny could be induced by an appropriate isogeny of $E$.) The methods of Section 3 allow us to use this isogeny to get data about $\ker\gamma_F$; this information is then interpreted in terms of $\ker\bar{\gamma}_E$.

The details of this program may be found in [8, Ch. 4]. Here we only wish to state our characterization precisely. To do this we replace $X_n$ by its $p$-part $Y_{n-1}$: Since for $n \geqslant 1$

$$\mathrm{Gal}(X_n/X_0) \cong (1 + p\mathbf{Z})^\times/(1 + p^n\mathbf{Z})^\times \times \boldsymbol{\mu}_{p-1}/(\pm 1),$$

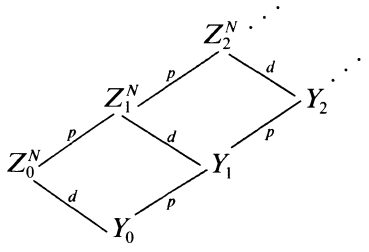
there is a curve $Y_{n-1}/\mathbf{F}_p$ lying between $X_n$ and $X_0$ such that $Y_{n-1}$ is an abelian cover of $X_0$ of degree $p^{n-1}$.

$$\begin{array}{c} X_n \\ \Big| \frac{p-1}{2} \\ Y_{n-1} \\ \Big| p^{n-1} \\ X_0 \end{array}$$

The curves $\{Y_n\}_{n \geqslant 0}$ form another tower of abelian covers of $X_0 = Y_0$, with $\mathrm{Gal}(Y_{n-1}/Y_0) \cong (1 + p\mathbf{Z})^\times/(1 + p^n\mathbf{Z})^\times$. We let $L_n$ denote the $\mathbf{F}_p$-rational function field of $Y_n$.

In order to characterize $Y_n$ we use the theory of modular curves. Choose $N > 1$ which is prime to $p$ and define the curve $Z_0^N/\mathbf{F}_p$ to be $X_0(N)$, the modular curve which parameterizes elliptic curves with a cyclic subgroup of order $N$. Let $Z_n^N$ be the lifting of $Y_n$ to a cover of $Z_0^N$. Then $Z_n^N/\mathbf{F}_p$ is a smooth curve which is a cover of $Y_n$ of degree

$$d = N \cdot \prod_{l \mid N} (1 + l^{-1}).$$



To keep our notation simple, in what follows we write $Z_n$ instead of $Z_n^N$.

Recall that we have chosen a generic elliptic curve $E$ defined over $\mathbf{F}_p(j) = L_0$. Let $M_n \supset L_n$ denote the field of $\mathbf{F}_p$-rational functions of $Z_n$. Over $M_0$ there exists another elliptic curve $E'$ and a cyclic $N$-isogeny $\phi$: $E \to E'$ corresponding to the generic point of $Z_0 = X_0(N)$. As before we define Galois characters

$$\gamma_E : \mathrm{Gal}((M_0)_s/M_0) \to \mathbf{Z}_p^\times$$

$$\gamma_{E'} : \mathrm{Gal}((M_0)_s/M_0) \to \mathbf{Z}_p^\times .$$

Since $E$ and $E'$ are related by an isogeny of degree prime to $p$, $\gamma_E$ and $\gamma_{E'}$ are identical. The formula $\gamma_E = \gamma_{E'}$ is the key to our characterization of the fields $L_n$, just as the formula $\chi_F = \chi_{F^\sigma}$ was the key to our characterization of $U_K \cap \ker \chi_F$.

The Fricke involution $w_N$ is an automorphism of order 2 of $Z_0 = X_0(N)$ which induces an involution of the function field $M_0$ of $Z_0$. The involution induced by $w_N$ interchanges the $j$-invariants of $E$ and $E'$–that is,

$$w_N(j_E) = j_{E'}$$

$$w_N(j_{E'}) = j_E.$$

Let $E'' = w_N(E)$ be the $w_N$-conjugate of $E$. The characters

$$\bar{\gamma}_{E'} : \mathrm{Gal}((M_0)_s/M_0) \to \mathbf{Z}_p^\times/(\pm 1)$$

$$\bar{\gamma}_{E''} : \mathrm{Gal}((M_0)_s/M_0) \to \mathbf{Z}_p^\times/(\pm 1)$$

are identical, since they depend only on the $j$-invariants of the elliptic curves used to define them. We let $W_0/\mathbf{F}_p$ be the quotient of $Z_0$ by the action of $w_N$, with function field $M_0' = M_0^{w_N}$. Combining the identities $\bar{\gamma}_{E''} = \bar{\gamma}_{E'}$ and $\gamma_E = \gamma_{E'}$ we get $\bar{\gamma}_E = \bar{\gamma}_{E''}$. Using this last formula one can show that $Z_n$ is Galois over $W_0$, with

$$\mathrm{Gal}(Z_n/W_0) \cong \mathbf{Z}/p^n \times \mathbf{Z}/2.$$

Therefore we may define curves $W_n/\mathbf{F}_p$ with

$$\begin{array}{c} Z_n \\ \Big| 2 \\ W_n \\ \Big| p^n \\ W_0 \end{array}$$

$\mathrm{Gal}(Z_n/W_n) \cong \mathbf{Z}/2$
$\mathrm{Gal}(W_n/W_0) \cong \mathbf{Z}/p^n$.

Hence the cover $Z_n$ of $Z_0$ comes from an abelian cover $W_n$ of $W_0$ and also from an abelian cover $Y_n$ of $Y_0$. These two descents combined with the local data described below suffice to characterize the Igusa tower.

Let $P$ be any supersingular point on the $j$-line $Y_0$. For each $n$ there is a unique point $P_n$ of $Y_n$ lying over $P$, because the supersingular points are totally ramified in the Igusa tower. Conversely, every point in $Y_0$ which ramifies in $Y_n$ lies over a supersingular point, because only the supersingular points are wildly ramified in the Igusa tower. By [6, Th. 12.7.1(1)], we know that the point $\infty$ on $Y_0$ splits completely in each of the curves $Y_n$.

We now state our characterization of (the $p$-part of) the Igusa curves. The proof of this theorem may be found in [8, Ch. 4].

THEOREM 5.1. *Let $p > 2$ and choose $N > 1$ with $(N, p) = 1$. The tower $(Y_n/\mathbf{F}_p)$ is the maximal abelian pro-p tower over $Y_0$ for which*
*a) the only ramification is over the supersingular points,*
*b) the lifting of the tower over $Z_0 = X_0(N)$ comes from an abelian tower over $W_0 = X_0(N)/w_N$, and*
*c) $\infty$ splits completely.*

REMARKS.
1. The key is condition b). The theorem essentially says that invariance under $N$-isogenies determines the Igusa tower.
2. Let $\omega$ be an invariant differential on the generic elliptic curve $E/\mathbf{F}_p(j)$ and let $H$ be the Hasse invariant of the pair $(E, \omega)$. The function field of $X_1$ is generated over $\mathbf{F}_p(j)$ by any root of the equation

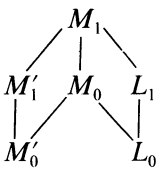
$$x^{(p-1)/2} - H = 0.$$

(The field extension is well-defined because $E$ determines $H$ up to multiplication by $(\mathbf{F}_p(j)^\times)^{(p-1)/2}$.) This fact combined with Theorem 5.1 gives a complete characterization of the Igusa tower.

3. The only abelian cover of $Y_0$ of degree $p^n$ satisfying a), b), and c) is $Y_n$.

## 6. Another example

Let $p = 3$ and $N = 2$. We give here explicit Artin–Schreier generators for the function fields $L_1$, $M_1$, $M_1'$ over $L_0$, $M_0$, $M_0'$.




The function field of $Y_0 = X_0$ is $L_0 = \mathbf{F}_p(j)$. Since $p = 3$ we can identify $Y_1$ with $X_2$. To find the function field of this curve we construct the unique generic elliptic curve $E$ over $\mathbf{F}_3(j)$ such that $E^{(3)}$ has rational 3-torsion (cf. [4, §5]). This curve has Weierstrass equation

$$y^2 = x^3 + j^2x^2 - j^5.$$

A laborious calculation shows that if $P_0 = (x_0, y_0)$ is a point on $E$ then

$$x(3P_0) = \frac{x_0^9 + j^{11}x_0^3 - j^{15}}{j^4(x_0^6 + j^5x_0^3 + j^{10})}.$$

We get the corresponding equations for $E^{(3)}$ by cubing the coefficients in the formulas for $E$. Therefore $E^{(3)}$ has Weierstrass equation

$$y^2 = x^3 + j^6x^2 - j^{15}$$

and rational 3-torsion points $(j^5, \pm j^8)$.

The function field $L_1$ of $Y_1 = X_2$ is the 9-division field of $E^{(9)}$. After we cube our coefficients a second time we find that $E^{(9)}$ has rational 3-torsion points $(j^{15}, \pm j^{25})$. Therefore there exists a point $P_0 = (x_0, y_0)$ of order 9 on

$E^{(9)}((L_0)_s)$ which satisfies

$$\begin{aligned} j^{15} &= x(3P_0) \\ &= \frac{x_0^9 + j^{99}x_0^3 - j^{135}}{j^{36}(x_0^6 + j^{45}x_0^3 + j^{90})}. \end{aligned}$$

We rewrite this as

$$\begin{aligned} 0 &= x_0^9 - j^{51}x_0^6 + (j^{99} - j^{96})x_0^3 - j^{141} - j^{135} \\ 0 &= (x_0^3 - j^{17}x_0^2 + (j^{33} - j^{32})x_0 - j^{47} - j^{45})^3 \\ 0 &= x_0^3 - j^{17}x_0^2 + (j^{33} - j^{32})x_0 - j^{47} - j^{45}. \end{aligned}$$

The substitution

$$x_0 = j^{16}X^{-1} - j^{16} + j^{15}$$

transforms the last equation into the irreducible Artin-Schreier equation

$$X^3 - X + \frac{1}{j} = 0.$$

Let $\alpha$ be a root of this equation. Since $L_1$ has degree 3 over $L_0$ we have $L_1 = L_0(\alpha)$.

Since $Z_0 = X_0(2)$ is a genus-0 cover of $Y_0$, its function field $M_0$ has the form $\mathbf{F}_3(t)$, with $\mathbf{F}_3(j) \subset \mathbf{F}_3(t)$. By [1, p. 179], we can choose $t$ such that

$$\begin{aligned} j &= \frac{(t + 256)^3}{t^2} \\ &= \frac{(t + 1)^3}{t^2}, \end{aligned}$$

and such that the Fricke involution $w_2$ of $Z_0 = X_0(2)$ induces the map

$$\begin{aligned} t &\mapsto \frac{2^{12}}{t} \\ &= \frac{1}{t} \end{aligned}$$

on $M_0$. The function field $M_0'$ of $W_0$ is the fixed field of this involution–that is, $M_0' = \mathbf{F}_3(t + t^{-1})$.

Since $1/j = t^2/(t + 1)^3$, $M_1$ is generated over $M_0 = \mathbf{F}_3(t)$ by the roots of the equation

$$X^3 - X + \frac{t^2}{(t + 1)^3} = 0.$$

We observe that

$$\begin{aligned} \frac{t^2}{(t + 1)^3} - \left(\frac{1}{(t + 1)^3} - \frac{1}{t + 1}\right) &= \frac{-t}{(t + 1)^2} \\ &= \frac{1}{1 - \left(t + \frac{1}{t}\right)} \\ &= \frac{1}{1 - \alpha}, \end{aligned}$$

where $\alpha = t + t^{-1} \in M_0'$. Therefore the roots of the Artin–Schreier equation

$$X^3 - X + \frac{1}{1 - \alpha} = 0$$

generate $M_1$ over $M_0$. Since $1/(1 - \alpha) \in M_0'$, the extension $M_1$ of $M_0$ comes from the extension $M_1'$ of $M_0'$ generated by the roots of the equation above.

We have shown that the $\mathbf{Z}/3$-extension $M_1/M_0$ comes from the $\mathbf{Z}/3$-extension $M_1'/M_0'$. This means that the extension $L_1/L_0$ satisfies hypothesis b) of Theorem 5.1. Since $L_1$ is generated over $L_0$ by the roots of the equation

$$X^3 - X + \frac{1}{j} = 0$$

it follows that $L_1/L_0$ is ramified only over $j = 0$, and that the prime $j = \infty$ splits completely in this extension. Thus our extension satisfies all the hypotheses of Theorem 5.1. It follows from the theorem that $L_1$ is the unique $\mathbf{Z}/3$-extension of $L_0$ with these properties.

## References


1. B. Birch: Some calculations of modular relations, *Lecture Notes in Math.* 320 (1973) 175–186.
2. V.G. Drinfield: Elliptic modules (Russian), *Math. Sbornik* 94 (136) (1974) 594–627, 656; English translation: *Math. USSR-Sob.* 23 (1976) 561–592.
3. Y. Fujiwara: 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.
4. B. Gross: Heegner points and the modular curve of prime level, *J. Math. Soc. Japan* 39 (1987) 345–362.
5. B. Gross: Ramification in $p$-adic Lie extensions, *Astérisque* 65 (1979) 81–102.
6. N. Katz and B. Mazur: *Arithmetic Moduli of Elliptic Curves*, Princeton University Press (1985).
7. K. Keating: Lifting endomorphisms of formal $A$-modules, *Comp. Math.* 67 (1988) 211–239.
8. K. Keating: Lifting endomorphisms of formal groups, Harvard Ph.D. thesis, 1987.
9. J. Lubin, J.-P. Serre and J. Tate: Seminar at Woods Hole Institute on algebraic geometry (1964).
10. J. Lubin and J. Tate: Formal complex multiplication in local fields, *Ann. of Math.* (2) 81 (1965) 380–387.
11. J. Lubin and J. Tate: Formal moduli for one-parameter formal Lie groups, *Bull. Soc. Math. France* 94 (1966) 49–59.
12. S. Sen: On automorphismes of local fields, *Ann. of Math.* (2) 90 (1969) 33–46.
13. J.-P. Serre: *Corps Locaux*, Hermann, Paris (1962).