ELSEVIER

Journal of Pure and Applied Algebra 145 (2000) 293–308

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Formal completion of the Jacobians of plane curves and higher real K-theories

V. Gorbounov [a,*], M. Mahowald [b]

[a] *University of Kentucky Lexington, KY 40506, USA*

[b] *Northwestern University Evanston, IL 60208, USA*

Communicated by E.M. Friedlander; received 19 October 1997; received in revised form 23 February 1998

Abstract

In this note we will study the formal completion of the Jacobian of a certain class of curves over p-adic rings. These curves generalize the Legendre family of elliptic curves. As an immediate application, we will describe the representation which is crucial for calculating the initial term of the spectral sequence, converging to the homotopy groups of the higher real K-theories $\mathbb{E}O_n$.

MSC: 55; 14

1. Introduction

Let p be a fixed prime number. Let E_n be Lubin and Tate's [7] ring representing deformations to complete local $\mathbb{W}(F_{p^n})$-algebras of a standard formal group of the Morava $K(n)$ theory, see, for example, [10]. Then there is a 2-periodic ring spectrum $\mathbb{E}_n$ such that $\pi_{\text{odd}}\mathbb{E}_n = 0$ and $\pi_0\mathbb{E}_n \cong E_n$. Lubin and Tate show in [7, 3.4] that the Morava stabilizer group $\mathbb{S}_n$ acts on E_n. We call this representation the Lubin–Tate representation. Recently, Hopkins and Miller show that this action is induced by an action of $\mathbb{S}_n$ on the spectrum $\mathbb{E}_n$. Let $\mathbb{G}_n$ denote a maximal finite subgroup of the Morava stabilizer group $\mathbb{S}_n$. Hopkins and Miller define $\mathbb{E}O_n$ to be the homotopy fixed point spectrum of the action of $\mathbb{G}_n$ on $\mathbb{E}_n$. There is a spectral sequence which abuts to $\pi_*\mathbb{E}O_n$ with E_2 term $H^*(\mathbb{G}_n, E_n)^{\text{Gal}}$. $\mathbb{E}O_2$ agrees with the usual elliptic cohomology when 2 is inverted [9].

* Corresponding author.

0022-4049/100/$ - see front matter
PII: S0022-4049(98)00134-0

In this paper we will study a formal group which can be used to construct $\mathbb{E}O_n$ for $n = p - 1$, and describe explicitly the Lubin–Tate representation of $\mathbb{G}_n$. In [8] Manin proved that every formal group of finite height defined over a field of finite characteristic is a summand in the formal completion of the Jacobian of a certain curve. It was suggested to the authors by Mike Hopkins that a universal lift of a formal group of height n over $\mathbb{F}_p$ should come as a summand in the formal completion of the Jacobian of a certain curve with p marked points. There is an action of $\mathbb{G}_{p-1}$ on such a curve, which can be expressed in terms of permutations of the marked points. This leads to a precise description of the Lubin–Tate action of $\mathbb{G}_{p-1}$ on the ring E_{p-1}. This representation was also studied using different techniques in [1, 6, 9].

2. Overview of the Honda theory

We recall briefly the Honda classification of formal group laws from [4]. If K is a ring or a field we denote by $K[[x]]_n^0 = K[[x_1, \ldots, x_m]]_n^0$ the set of n-dimensional vectors over the ring of series over K with constant term equal to zero.

Let K be a discrete valuation field. Denote by $\mathfrak{v}$, $\mathfrak{p}$ and $\mathfrak{v}_\mathfrak{p}$ the ring of integers of K, the maximal ideal of $\mathfrak{v}$, and the completion of $\mathfrak{v}$ with respect to $\mathfrak{p}$, respectively. We assume that the residue class field is of characteristic $p > 0$. Suppose also that there is an endomorphism σ of K and a power q of p such that $a^\sigma = a^q \bmod \mathfrak{p}$ for any $a \in \mathfrak{v}$. Introduce a variable T such that $Ta = a^\sigma T$ for any $a \in \mathfrak{v}$, and define the twisted power series ring $M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ as the ring of series $M_n(\mathfrak{v}_\mathfrak{p})[[T]]$ in which T and $M_n(\mathfrak{v}_\mathfrak{p})$ commute according to this rule. Define an action of this twisted power series ring on the vector space of n-dimensional vectors over the ring $K[[x_1, \ldots, x_m]]$ by

$$(u * f)(x) = \sum_{\eta=0}^{\infty} C_\eta f^{\sigma^\eta}(x^{q^\eta}),$$

where $u = \Sigma_\eta C_\eta T^\eta$, $f \in K[[x]]_n^0$.

We say that an element $u \in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ is *special* for $f \in K[[x]]_n^0$ if $u \cong \pi I_n \bmod$ degree 1 and $(u * f)(x) \equiv 0 \bmod \mathfrak{p}$, where π is a uniformizer for $\mathfrak{p}$ and I_n is the $n \times n$ identity matrix. Let F be an n-dimensional abelian formal group law over $\mathfrak{v}$ and $f = (f_1, \ldots, f_n)$ denote its logarithm. An element $u \in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ is said to be *special* for F if it is a special element for f. We say in this case that F is of type u. Call elements $u_1, u_2 \in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$, equivalent if $u_1 = vu_2$, where $v \in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ is a unit.

The following theorem is proved in [4].

Theorem 2.1. *Suppose that K is a discrete totally unramified valuation field (in addition to the conditions stated above), then the strict isomorphism classes of formal group laws over $\mathfrak{v}$ correspond bijectively to the equivalence classes of elements $u \in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ of the form $u \cong \pi I_n \bmod$ degree 1.*

We intend to study the formal completion of the Jacobian of a certain class of curves. Let us state the connection, established in [5], between the formal completion of the Jacobian of a curve and the space of holomorphic differentials on it. Let Γ be a curve of genus $n>0$ over K. Denote by J the Jacobian of Γ, and by Λ the canonical map $\Gamma\to J$. Let $\omega_1,\dots,\omega_n$ be a basis of holomorphic differentials on Γ, each defined over K. Choose a local parameter $z\in K(\Gamma)$ at some point P, and denote by $\omega_i(z)$ the expansion of ω_i at P. There are $\psi_i(z)\in K[[z]]$, $1\le i\le n$, such that $\psi_i(0)=0$ and $\omega_i(z)=\mathrm{d}\psi_i(z)$. Let $y=(y_1,\dots,y_n)\subset K(J)$ be a system of local parameters at the origin of J and let $v_1,\dots,v_n$ be the invariant differentials on J such that

$$v_i\circ\Lambda=\omega_i\quad(1\le i\le n).$$

Denote by $v_i(y)$ the expansion of v_i at the origin. There are $\phi_i(y)\in K[[y]]$, $1\le i\le n$, such that $\phi_i(0)=0$ and $v_i(y)=\mathrm{d}\phi_i(y)$. The vector $\phi(y)=(\phi_i(y))$ is the logarithm of the formal group law F of J, associated to the system of local parameters y. Let S_1 be the set of primes at which Γ, Λ, J, z, or y has a bad reduction, and S_0 be the set of ramified primes of K.

Proposition 2.2 (Honda [3, Theorem 1]). *There is a finite set S of primes of K satisfying the following conditions*:

- *S contains $S_0\cup S_1$.*
- *If $\mathfrak{p}\notin S$ and $u\in M_n(\mathfrak{v}_\mathfrak{p})[[T]]^\sigma$ is a special element for $\psi(z)=(\psi_i(z))$, then u is also a special element for the vector $(\phi_i(y))$, so that F is of type u as a formal group law over $\mathfrak{v}_\mathfrak{p}$.*

Let A be a ring of characteristic zero that is also a $\mathbb{Z}_{(p)}$-algebra, and $K=A\otimes\mathbb{Q}$. Suppose there is a ring endomorphism $\sigma:K\to K$, such that $\sigma(a)=a^p \bmod pA$ for all $a\in A$.

Lemma 2.3. *Let A be a ring as above.*

(i) *There is a special element for every formal group law over A.*

(ii) *If there is a special element u for a series $f\in K[[x]]_n^0$, $f\equiv x \bmod \text{degree } 2$, then the formal group law $f^{-1}(f(x)+f(y))$ is a formal group law over A.*

(iii) *The strict isomorphism classes of formal group laws over A correspond bijectively to the equivalence classes of elements $u\in M_n(A)[[T]]^\sigma$ of the form $u\equiv\pi I_n \bmod \text{degree one}$.*

Proof. (i) It is proved in [2] that every formal group F over A has a logarithm defined by a functional equation, and Eq. (20.3.11) of [2] shows that it is equivalent to the existence of a special element for F.

(ii) The direct check shows that the proofs of the Lemmas 2.3 and 2.4, and Theorem 2 from [5] go without a change when K and A are as above.

(iii) The proof of the Proposition 2.6 from [5] goes through without change as well. Note that for a given special element u the formal group law, F, associated to it is defined by the logarithm $f=(p/u)*(i)$. □

3. Motivating example: points on elliptic curves and the Lubin–Tate representation

In this section we assume that $p=3$. We will use the properties of the Legendre curve to describe the Lubin–Tate representation of $\mathbb{G}_2$, a maximal finite subgroup of $\mathbb{S}_2$. The general strategy here will be to work with lifts of elliptic curves to the appropriate moduli space rather than with lifts of formal groups.

In order to describe the action of $\mathbb{G}_2$ on the moduli space of deformations, we need to choose a specific deformation of a formal group of height two. Consider the following elliptic curve $\bar{C}$:

$$y^2 = x^3 - x. \tag{3.1}$$

The formal completion of this elliptic curve is a formal group of height two, therefore the group of its automorphisms over a suitable extension of $\mathbb{F}_3$ is isomorphic to $\mathbb{S}_2$. We will present a convenient model for the moduli space of lifts of $\bar{C}$ to Artinian rings.

The Legendre curve is a plane curve defined by the equation

$$y^2 = x(x-1)(x-\lambda)$$

over the ring $\bar{E} = \mathbb{Z}[\frac{1}{2}, \lambda]$. Denote this curve by C and rewrite its equation as

$$y^2 = x(x-1)(x-u_1+1). \tag{3.2}$$

Complete $\bar{E}$ with respect to the ideal $(3, \lambda+1)$ and denote the resulting ring E.

Lemma 3.1. *The pair (E, F_C), where F_C denotes the formal completion of C, is a universal deformation of the formal completion of $\bar{C}$.*

Proof. Choose $z = x/y$ as a local parameter at infinity. As a simple computation shows the formal completion of C is a series in two variables

$$F(z_1, z_2) = z_1 + z_2 + u_1(z_1^2 z_2 + z_1 z_2^2) \bmod (z_1, z_2)^4.$$

According to [7] this is a universal deformation. □

The pair (E, F_C) is the model of the Lubin–Tate lift we will use.

Now we are ready to describe the Lubin–Tate representation of $\mathbb{G}_2$.

Lemma 3.2. *$\mathbb{G}_2$ is isomorphic to the group of automorphisms of the elliptic curve $\bar{C}$ over the field $\mathbb{F}_9$ via the functor of the formal completion.*

Proof. $\mathbb{G}_2$ is known to be isomorphic to $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$. The group of automorphisms of $\bar{C}$ over the field $\mathbb{F}_9$ is given by the substitutions

$$s_1\colon\ x = x' + 1, \quad y = y',$$
$$s_2\colon\ x = -x', \quad y = -\mathrm{i}y',$$

where $\mathrm{i}^4 = 1$. This group is isomorphic to $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$. The functor of formal completion provides a monomorphism $\mathrm{Aut}_{\mathbb{F}_9}(\bar{C}) \to \mathbb{S}_2$. □

Proposition 3.3. *There are six automorphisms of the complete local $W(\mathbb{F}_9)$-algebra $W(\mathbb{F}_9)\hat{\otimes}E$ which preserve the isomorphism class of the curve C.*

Proof. This is a standard fact in elliptic curve theory, (cf. [12, p. 54]). In particular, if one adds to the moduli space E a forth root of unity i, then it admits six automorphisms which preserve the isomorphism class of C. Because this example illustrates our later work (see Section 6), we will outline the proof. We have three marked points on our curve with x coordinates $\{0, 1, \lambda\}$. Any automorphism g of the moduli space takes the triple $\{0, 1, \lambda\}$ to an unordered triple $\{0, 1, g(\lambda)\}$. Let

$$x' = w^2 x + r, \qquad y' = w^3 y$$

be an algebraic transformation from C to g^*C. It, in its turn, takes the triple $\{0, 1, \lambda\}$ to an unordered triple $\{r, w^2 + r, w^2\lambda + r\}$. There are six way to match these two unordered triples, which produce the following values for λ:

$$\left\{\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{\lambda-1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}\right\}. \qquad \square$$

All we need now is to replace λ with $u_1 - 1$ and take into account the fact that g fixes elements of the base ring $W(\mathbb{F}_9)$. Here are possible values for $g(u_1)$:

$$\left\{u_1, 3-u_1, \frac{u_1}{u_1-1}, \frac{2u_1-3}{u_1-1}, \frac{u_1-3}{u_1-2}, \frac{2u_1-3}{u_1-2}\right\}.$$

Remark 3.4. By definition, $g(u) = u/w$. The appropriate values of w are easy to calculate. For the substitutions of Proposition 3.3 they are

$$\sqrt{-\frac{1}{\lambda}}, \quad \sqrt{\frac{1}{\lambda}}.$$

Remark 3.5. The fact that we found only six automorphisms of the moduli space E means that the center of the group $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$ acts trivially on it. It always happens this way as is proved in [6].

Remark 3.6. We can handle the Lubin–Tate representation of $\mathbb{G}_2$ for $p = 2$ in a similar fashion.

4. The generalized Legendre family

Fix a prime number p from now on. Then any maximal finite subgroup of $\mathbb{S}_{p-1}$, $\mathbb{G}_{p-1}$, is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}/(p-1)^2$ [3]. The important points in the example with the Legendre curve C are:

(i) C is a 2-cover of the projective line with three marked points on it. The reduction of this curve mod the ideal $(\lambda+1)$ has $\mathbb{G}_2$ as a subgroup of its group of automorphisms by Proposition 3.3.

(ii) The formal completion of the Jacobian of C is a universal Lubin–Tate lift of a formal group of height two.

We would like to realize universal Lubin–Tate lifts of formal groups of other heights in a similar "algebraic" fashion. In particular, we would like to obtain them as summands in the formal completion of the Jacobian of curves. The work of Manin [8] suggests considering curves of the form

$$y^{p^a-1} = x^p - x,$$

defined over $\mathbb{F}_p$. He showed in [8] that, at least up to isogeny, the formal completion of the Jacobians of such a curve contains a one-dimensional summand, whose height divides $a(p-1)$. Here we will study the case when $a=1$.

Denote by E the ring $\mathbb{Z}_p[[u_1,\dots,u_{p-2}]]$.

Definition 4.1. Let the generalized Legendre curve C be the plane curve over E defined by the following equation:

$$y^{p-1} = x^p + u_1x^{p-1} + \cdots + u_{p-2}x^2 + \left(-1 - \sum_{i=1}^{p-2} u_i\right)x. \tag{4.1}$$

Denote $-1-\sum_{i=1}^{p-2} u_i$ by b.

If we factor out the ideal $I=(p,u_1,\dots,u_{p-2})$, then the reduction of the curve C will be a curve $\bar{C}$ over $\mathbb{F}_p$ defined by the equation

$$y^{p-1} = x^p - x.$$

The roots of the right-hand side are $0,1,2,\dots,p-1 \bmod p$.

Hensel's lemma implies the following lemma.

Lemma 4.2. *All the roots of the polynomial in the right-hand side of* (4.1) *are in E, so the curve C may be defined by the following equation*:

$$y^{p-1} = x(x-1)(x-e_1)\cdots(x-e_{p-2}),$$

where $e_i = i+1 \bmod I$.

As we see from the above remark C is a $p-1$ covering of the projective line with p marked points on it. Over the ring $\mathbb{F}_{p^{p-1}}$ the group of automorphisms of $\bar{C}$ contains $\mathbb{G}_{p-1}$. Indeed, $\mathbb{Z}/p$ and $\mathbb{Z}/(p-1)^2$ act on the curve $\bar{C}$ via a substitutions:

$$x = x'+1, \quad y = y', \quad x = \zeta^{p-1}x', \quad y = \zeta^p y', \tag{4.2}$$

where $\zeta^{(p-1)^2} = 1$.

Proposition 4.3. *The curves C and $\bar{C}$ are non-singular curves of genus $m=(p-1)(p-2)/2$. The differentials*

$$\omega_{i,j}=\frac{x^i\,\mathrm{d}x}{y^j},\quad 0\le i\le j-1\le p-3$$

form a basis of the space of holomorphic differentials.

Proof. Direct computation shows that the curves C and $\bar{C}$ are non-singular. To calculate the genus note that

$$div(x)=(p-1)(0)-(p-1)(\infty),$$

$$div(y)=(0)+(1)+(e_1)+\cdots+(e_{p-2})-p(\infty),$$

$$div(dx)=(p-2)(0)+(p-2)(1)+(p-2)(e_1)+\cdots+(p-2)(e_{p-2})-p(\infty).$$

So the above differentials are indeed holomorphic. A standard argument shows that these form a basis for the space of holomorphic differentials. The Riemann–Roch theorem implies that the genus is as indicated in the proposition. □

Corollary 4.4. *The order of the zero at infinity of $\omega_{i,j}$ is equal to $p(j-1)-(p-1)i$. If we choose $z=x/y$ as a local parameter at infinity than the expansion of $\omega_{i,j}$ is a power series $\sum_{k\ge 0} g_k z^{n_k}\,\mathrm{d}z$ where g_k is in E, and $n_k\equiv j-1 \bmod p-1$.*

Proof. Introduce the following coordinates $z=x/y$ and $w=1/y$. In these coordinates the equation of the curve is

$$w=z^p+u_1z^{p-1}w+\cdots+u_{p-2}z^2w^{p-2}+bz\,w^{p-1}. \tag{4.3}$$

Out of this equation we immediately get that

$$w=z^p\sum_{k\ge 0}a_kz^{m_k},\qquad y=z^{-p}\sum_{k\ge 0}b_kz^{l_k},$$

$$x=z^{1-p}\sum_{k\ge 0}b_kz^{l_k},\qquad \mathrm{d}x=z^{-p}\sum_{k\ge 0}c_kz^{l_k},$$

where $m_k, l_k\equiv 0 \bmod p-1$. This implies the statement of the corollary. □

5. The splitting of the formal completion of the Jacobian

The ring E is of the type described in Lemma 2.3. Indeed, we can define the required endomorphism σ of $E\otimes_{\mathbb{Z}_{(p)}}\mathbb{Q}$ by the formulas:

$$\sigma(u_i)=u_i^p,\quad \sigma(a)=a,\quad a\in\mathbb{Q}_p.$$

Therefore, the formal group law associated to a choice of coordinates on $J(C)$ is determined by the equivalence class of special elements for its logarithm. We will study the properties of this class of special elements.

Denote by $\psi_{i,j}(z)$ the formal anti-derivative of the formal expansion of $\omega_{i,j}$ around infinity, and by ψ the vector with the coordinates $\psi_{i,j}(z)$, ordered in such a way that $(i,j)>(i_1,j_1)$ if $j>j_1$. Recall that $m=(p-1)(p-2)/2$ is the number of entries in the vector ψ.

Theorem 5.1. (i) *Define the formal group law F_ψ of $J(C)$ in terms of the coordinates on $J(C)$ determined by ψ. Then this is a formal group law over E, therefore, there is a special element for F_ψ, which is also a special element for the vector ψ.*

(ii) *If $u\in M_m(E)[[T]]^\sigma$ is a special element for the vector ψ, then it is also a special element for F_ψ, so that F_ψ is of type u as a formal group over E.*

Proof. (i) We need to prove that the Jacobian is smooth at the origin. This follows from the general theory of reduction of algebraic varieties [11]. In our case the statement follows from the fact that the curve C_p is non-singular and its reduction is non-singular. In the terminology of [11] it means that the objects we deal with are I-simple.

It follows from Lemma 2.3 that there is a special element for F_ψ. Pulling the logarithm of F_ψ back using the canonical embedding $C\to J(C)$, we see that it is also a special element for ψ.

(ii) We will show that the following version of Lemma 1 from [5] holds in our setting. Then the proof of part (ii) will follow exactly as the proof of Proposition 2.2 of [5]. □

Lemma 5.2. *Let ψ be as above. If $u,v\in M_m(E)[[T]]^\sigma$ are special elements for ψ, then there is a unit in $M_m(E)[[T]]^\sigma$ such that $v=tu$.*

Proof. Suppose

$$u=pI_m+\sum_{k=1}^{\infty}C_kT^k,\quad v=pI_m+\sum_{k=1}^{\infty}D_kT^k,$$

$C_k,D_k\in M_m(E)$. We will show that if $C_k=D_k$, $0\le k\le l-1$ with some $l\ge 1$, then $C_l=D_l \bmod p$. We have

$$\sum_{k=l}^{\infty}(C_k-D_k)\psi^{\sigma^k}(z^{p^k})\equiv 0 \bmod p.$$

It follows from Corollary 4.6 by direct computation that all the entries of C_l-D_l are divisible by p. Put now

$$t_l=I_m-\frac{1}{p}(C_l-D_l)T^l,$$

t_l is a unit in $M_m(E)[[T]]^\sigma$ and $t_l u = v \bmod \text{degree } l+1$. In this way we can find units $t_1, \ldots, t_l$ successively for each $l > 0$, so that $t_l \ldots t_1 u = v \bmod \text{degree } l+1$. The limit of $t_l \ldots t_1$ clearly satisfies the requirement of our lemma. □

Theorem 5.3. *The isomorphism class of F_ψ over E contains a formal group law, which splits into $p-2$ summands of dimensions $1, 2, \ldots, p-2$, respectively. The reduction of the one-dimensional summand* mod I *has the height $p-1$.*

Proof. According to Theorem 5.1(ii), we need to study special elements for the vector ψ. To prove the theorem we will show that there is a special element for ψ which is made out of diagonal blocks of dimensions $1, 2, \ldots, p-2$. Let $u = pI_m + \sum_{k=1}^{\infty} C_k T^k$ be a special element for ψ, which exists according to 5.1. Recall that the order of zero at infinity of $\omega_{i,j}$, reduced mod $p-1$, is equal to $j-1$. Expanding $\omega_{i,j} = x^i \, dx/y^j$ around infinity into a power series and integrating the result, we see from Corollary 4.4 that $\psi_{i,j}$ is a formal series in powers of z congruent to $j \bmod p-1, 1 \le j \le p-2$. At this point it is convenient to introduce the following notation. If ϕ is any column vector with m entries and $1 \le i \le p-2$, let $\phi(i)$ be the column vector with i entries such that

$$\phi = \begin{bmatrix} \phi(1) \\ \phi(2) \\ \vdots \\ \phi(p-2) \end{bmatrix}.$$

With this notation each entry of $\psi(i)$ is a power series in z with exponents congruent to i modulo $p-1$.

Similarly, if C is an $m \times m$ matrix, then for $1 \le i,\ j \le p-2$ let $C(i,j)$ be the $i \times j$ matrix such that

$$C = \begin{bmatrix} C(1,1) & \ldots & C(1,p-2) \\ \vdots & \vdots & \vdots \\ C(p-2,1) & \ldots & C(p-2,p-2) \end{bmatrix}.$$

Then

$$C_k \psi(i)^{\sigma^k}(i) = \sum_{j=1}^{p-2} C_k(i,j) \psi(j)^{\sigma^k}.$$

The summand $C_k(i,j)\psi(j)^{\sigma^k}$ has as its entries power series in z with exponents congruent to j modulo $p-1$.

Now consider an entry $r(z)$ of $(u * \psi)(i)$. It is easy to see that $r(z)$ can be written as a sum of power series

$$r(z) = \sum_{j=1}^{p-2} r_j(z),$$

such that

(i) the exponent occurring in $r_j(z)$ are congruent to j modulo $p-1$.

(ii) $r_j(z)$ depends only on the block matrix $C_k(i,j)$, and is zero if $C_k(i,j)=0$.

Indeed r_j is just the appropriate entry of

$$\sum_k C_k(i,j)\psi^{\sigma^k}(j)(z^{p^k}).$$

This implies that the element $u'=pI_m+\sum_{k=1}^{\infty} C'_k T^k$, where each C'_k is a block matrix

$$\begin{bmatrix} C_k(1,1) & 0 & \dots \\ 0 & C_k(2,2) & \dots \\ \dots & \dots & \dots \\ \dots & 0 & C_k(p-2,p-2) \end{bmatrix}$$

is a special element for the vector ψ.

Consider now the vector $f(x)=(p/u')*\boldsymbol{i}(x)$, where x is a vector of variables $(x_1,\dots x_m)$, and $\boldsymbol{i}(x)=x$. The Lemma 2.3 implies that the formal group law $H(x,y)=f^{-1}(f(x)+f(y))$ is defined over E, and, by construction, is a sum of $p-2$ summands of dimensions $1,\dots,p-2$. Theorem 5.1 guarantees that it is isomorphic to F.

According to [8, p. 74, Theorem 4.2], the reduction of $F_\psi \bmod I$ contains a one-dimensional summand of the height $p-1$. Since the maximal dimension of an indecomposable summand of the reduction of F_ψ is less or equal to $p-2$, using [8, (4.7), p. 71] we see that the height of the reduction of the one-dimensional summand must be $p-1$. □

Now we present a certain deformation of a formal group of height $p-1$ over $\mathbb{F}_p$. Later we will prove that this is a universal deformation in the sense of Lubin–Tate [7].

Corollary 5.4. *Denote by F_C the one-dimensional formal group law with the logarithm $\psi_{0,1}(z)$. This is a formal group law over E, and the height of the reduction of $F_C \bmod$ the ideal I is $p-1$.*

Proof. We have proved above that the vector $\psi(z)=(\psi_{i,j}(z))$ has a special element $u=pI_m+\sum_{k=1}^{\infty} C_k T^k$, such that for all k, C_k is a block diagonal matrix with the blocks of dimensions $1,\dots,p-2$. By definition of the $*$-product it means that $\psi_{0,1}$ has a special element. It is made out of the blocks C_k^1 of C_k of the size one by one. In other words, it is given by the formula $u=p+\sum_{k=1}^{\infty} C_k^1 T^k$. The Honda theory [4] and Remark 2.3 imply that the formal group law $F_C(x,y)=\psi_{0,1}^{-1}(\psi_{0,1}(x)+\psi_{0,1}(y))$ is defined over E. Moreover, the very same series u is a special element for the one-dimensional summand of the formal group law $H(x,y)$, defined above. Therefore, according to the Honda theory, these two one-dimensional formal group laws are isomorphic over E. Thus, the height of the reduction $\bmod I$ of F_C is $p-1$. □

6. A useful representation of $\mathbb{G}_{p-1}$

From now on $\log_F$ denotes the logarithm of a formal group F. Denote by E_1 the ring $W(\mathbb{F}_{p^{p-1}})[[u_1,\dots,u_{p-2}]]$. In this section we will describe a certain action of $\mathbb{G}_{p-1}$ on the ring E_1. The result of the next section will imply that this action is the Lubin–Tate action. In order to obtain the formulas for this representation of $\mathbb{G}_{p-1}$ we will use the generalized Legendre curve C in the same way we used the Legendre curve in section three.

Let F be a formal group law of dimension one over the ring E_1. Denote by $\bar{F}$ the reduction of $F \bmod I = (p, u_1, \dots, u_{p-2})$, and suppose that it has the height greater than or equal to one. Let G be a subgroup of the group of automorphisms of $\bar{F}$ over $\mathbb{F}_{p^{p-1}}$. Recall, that we can view G as a subgroup of the group of power series over $\mathbb{F}_{p^{p-1}}$ which are invertible under composition.

Denote $g^{-1}F(g(x), g(y))$ by $g^{-1}(F)$.

Definition 6.1. We say that F has the Lubin–Tate property with respect to G if for any $\bar{g} \in G$, there is a unique lift g of $\bar{g}$ to the ring $E_1[[x]]$, and an unique automorphism α_g of E_1 as a complete local $W(\mathbb{F}_{p^{p-1}})$-algebra, such that

$$g^{-1}(F) = \alpha_g^*(F(x, y)).$$

This lets us define an action of G on the ring E_1 as follows. For $\bar{g} \in G$, define a $W(\mathbb{F}_{p^{p-1}})$-linear ring automorphism of E_1 by the formula:

$$\bar{g}(u_i) = \alpha_g(u_i).$$

We call this representation of G, the representation defined by F.

Remark 6.2. For purposes in homotopy theory we need to consider formal groups over the ring $E_1[u^{-1}, u]$. If a formal group F defines a representation of G on E_1 as in Definition 6.1, then we can extend it to an action of G on $E_1[u^{-1}, u]$ by the formula

$$\alpha_g(u) = g'(0)u.$$

Remark 6.3. A formal group law F has the Lubin–Tate property if and only if for all $\bar{g} \in G$ there is a unique lift g of $\bar{g}$ to the ring $E_1[[x]]$, and an unique automorphism α_g of E_1 as a complete local $W(\mathbb{F}_{p^{p-1}})$-algebra, such that

$$\alpha_g^*(\log_F) = \frac{\log_F \circ g}{g'(0)}.$$

Let C be a plane curve over the ring A, given by the equation $C(x, y) = 0$, α is a ring homomorphism of A, and f is a transformation of A^2 given by a pair of polynomial functions $f(x, y) = (f_1(x, y), f_2(x, y))$. We denote by $\alpha^*(C)$ the inverse image of C under α, and by $f(C)$ the curve, defined by the equation $C(f_1(x, y), f_2(x, y)) = 0$.

Set $e_0 = 1$ and $e_{p-1} = 0$ and denote by $[m]$ the reduction of the integer $m \bmod p$. With this notation we have $e_i \equiv [i+1] \bmod I$, $0 \le i \le p-1$.

Recall that the group $\mathbb{G}_{p-1}$ is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}/(p-1)^2$. The last can be viewed as a group of automorphisms over $\mathbb{F}_{p^{p-1}}$ of the curve $\bar{C}$, defined in section 4. Choose i from the set $\{1,\dots,p-1\}$. One can see directly that the substitution $\bar{a}$ of order p

$$x_1 = x + i, \qquad y_1 = y$$

and $\bar{b}$ of order $(p-1)^2$

$$x_1 = \zeta^{p-1} x, \qquad y_1 = \zeta^p y,$$

where $\zeta^{(p-1)^2} = 1$, generate this group. A general form of a transformation a of C, which reduces $\bmod I$ to the automorphism $\bar{a}$ of $\bar{C}$ is

$$x_1 = v_i^{p-1} x + r_i, \qquad y_1 = v_i^p y,$$

where $r_i \equiv i$ and $v_i \equiv 1 \bmod I$, and a general form of a transformation b of C, which reduces $\bmod I$ to an automorphism of $\bar{C}$ of order $(p-1)^2$ is

$$x_1 = v^{p-1} x, \qquad y_1 = v^p y,$$

where $v_i \equiv 1$, $r_i \equiv i$, $v \equiv \zeta \bmod I$. We can always assume that $\zeta^{p-1} = k^{-1}$ were k is a generator of $\mathbb{F}_p^{\times}$.

Proposition 6.4. *For every $\bar{g} \in \mathbb{G}_{p-1}$ there is a $W(\mathbb{F}_{p^{p-1}})$-linear automorphisms α_g of the ring E, and a transformation g of the curve C, such that*

$$\alpha_g^*(C_p) = g^{-1}(C_p).$$

Proof. Since $\mathbb{G}_{p-1}$ is generated by $\bar{a}$ and $\bar{b}$, we will look for automorphisms α_a and α_b of the ring E_1, and transformations a and b of the form described above, such that

$$\alpha_a^*(C) = a^{-1}(C), \quad \alpha_b^*(C) = b^{-1}(C).$$

It is enough to look at the images of the marked points

$$(0,0),(1,0),(e_1,0),\dots,(e_{p-2},0)$$

of C under α_a, α_b and a, b. If we match the images of these points in the following way:

$$0 = v_i^{p-1} e_{[-1-i]} + r_i, \quad 1 = v^{p-1} e_{[k-1]},$$

$$1 = v_i^{p-1} e_{[-i]} + r_i, \quad \alpha_b(e_j) = v^{p-1} e_{[(j+1)k-1]},$$

$$\alpha_a(e_j) = v_i^{p-1} e_{[j-i]} + r_i$$

$1 \le j \le p-2$, we can solve the resulting equations for α_a and α_b. From the way we solved these equations it is clear that the solution is unique. In terms of the roots

$e_1,\dots,e_{p-2}$ these automorphisms are given by the formulas:

$$\alpha_a(e_j)=\frac{e_{[j-i]}-e_{[-i-1]}}{e_{[-i]}-e_{[-1-i]}},\qquad \alpha_b(e_j)=\frac{e_{[(j+1)i-1]}}{e_{[k-1]}},$$
$$\alpha_a(u)=(e_{[-i]}-e_{[-1-i]})^{1/(p-1)}u\quad \alpha_b(u)=(e_{[k-1]})^{1/(p-1)}u. \qquad \square$$

Remark 6.5. The series $(1+x)^{1/(p-1)}$ exists in $\mathbb{Z}_p[[x]]$.

Corollary 6.6. *The formal group law F_C has the Lubin–Tate property with respect to $\mathbb{G}_{p-1}$.*

Proof. Let $\bar{g}\in\mathbb{G}_{p-1}$ and its lift, obtained in Proposition 6.4, be represented by the following substitution:

$$x_1=v^{p-1}x+r,\qquad y_1=v^p y.$$

Expanding this transformation we obtain a series $g(z_1)$, such that $z=g(z_1)$.

Recall that the series $\omega_{0,1}$ is the expansion with respect to the parameter $z=x/y$ of the differential $\mathrm{d}x/y$ on the curve C_p. Denote by ω^g the expansion with respect to the parameter $z_1=x_1/y_1$ of the differential $\mathrm{d}x_1/y_1$ on the curve $g(C_p)$. Then

$$\frac{\mathrm{d}x}{y}=\frac{\mathrm{d}(v^{1-p}(x_1+r))}{v^{-p}y_1}=v\frac{\mathrm{d}x_1}{y_1}.$$

Expanding both sides with respect to the parameter z_1, we obtain that

$$v^{-1}(g)'(z_1)\omega_{0,1}(g(z_1))=\omega^g(z_1).$$

On the one hand, Proposition 6.4 implies that $\alpha_g^*\mathrm{d}x/y=\mathrm{d}x_1/y_1$, therefore, after expanding both sides into series we obtain

$$\alpha_g^*\omega_{0,1}(z_1)=\omega^g(z_1).$$

To finish the proof we need to formally integrate both the identities for $\omega^g(z_1)$, and note that $v=(g)'(0)$. $\square$

Corollary 6.7. *Let F be a formal group law and $\gamma:F_C\to F$ be a strict isomorphism of formal group laws, both defined over E_1, then F has the Lubin–Tate property with respect to $\mathbb{G}_{p-1}$. The representation of $\mathbb{G}_{p-1}$ defined by F coincides with the one defined by F_C.*

Proof. Let $\bar{g}\in G$, then there are g and α_g, described above, such that $g^{-1}(F_C)=\alpha_g^*F_C$. Then we have $(\gamma\circ g\circ\alpha_g^*(\gamma^{-1}))^{-1}F=\alpha_g^*F$ Since γ was a strict isomorphism, we have $(\alpha_g^*(\gamma)g(\gamma^{-1}))'(0)=(g^{-1})'(0)$. $\square$

7. On the properties of the one-dimensional summand

Since our base ring E is a $Z_{(p)}$-algebra, F_C is strictly isomorphic over E to a p-typical formal group law, which we denote by G_C. We also denote by $\bar{G}_C$ ($\bar{F}_C$) the reductions of G_C (F_C) modulo the ideal I, and by G_C^0 (F_C^0) the reductions of G_C (F_C) modulo the ideal $I_0=(u_1,\dots,u_{p-2})$. So $\bar{G}_C$ and $\bar{F}_C$ are formal group laws defined over $\mathbb{F}_p$, and G_C^0 and F_C^0 are formal group laws defined over $\mathbb{Z}_p$.

Remark 7.1. According to Eq. (16.4.14) of [2] $\log_{G_C}$ is obtained from $\log_{F_C}$ by crossing out the terms $m_i z^i$ with $i\neq p^k$. Moreover, if $\phi(z)\in E[[z]]$ is the strict isomorphism between G_C and F_C, then $\log_{G_C}(z)=\log_{F_C}(\phi(z))$.

The purpose of this section is to prove the theorem.

Theorem 7.2. *The formal group law G_C is a universal Lubin–Tate lift of a formal group of height $p-1$ over $\mathbb{F}_p$.*

The proof will follow directly from the next two propositions.

Proposition 7.3. *There is an automorphism $\bar{g}$ of $\bar{G}_C(x,y)$ of order p, defined over $\mathbb{F}_p$, such that $\bar{g}(z)=z+z^p$ mod degree $p+1$.*

Proof. The formal group laws G_C and F_C are strictly isomorphic over E by construction, therefore $\bar{G}_C$ and $\bar{F}_C$ are isomorphic over $\mathbb{F}_p$. We claim that there is an isomorphism between $\bar{G}_C$ and $\bar{F}_C$, such that as a series in z it is equal to z mod degree $p+1$.

Note that $\log_{G_C^0}(z)=\log_{F_C^0}(\phi^0(z))$, where $\phi^0(z)$ is the reduction of $\phi(z)$ mod I_0. The logarithm of F_C^0 is the formal integral of the following differential form:

$$\omega=\frac{(1-p)\,\mathrm{d}z}{1+(p-1)\,zw^{p-2}}, \tag{7.1}$$

where the series $w(z)$ obeys the following functional equation:

$$w=z^p-zw^{p-1}.$$

This functional equation implies that w is a series in powers of z congruent to p modulo $(p-1)^2$ and, therefore, $\omega=\omega(z)\,\mathrm{d}z$ is the differential form such that $\omega(z)$ is a series in powers of z congruent to zero modulo $(p-1)^2$. From this we conclude that the series $\log_{F_C^0}$ and $\log_{G_C^0}$ are congruent to z mod degree $p+1$. Therefore, $\phi^0(z)$ is congruent to z mod degree $p+1$. Its reduction mod p gives an isomorphism between $\bar{G}_C$ and $\bar{F}_C$ with the stated above properties.

$\bar{F}_C$ has an automorphism of order p, such that as a series, it is congruent to z mod degree $p+1$. Take, for example, a_1 from Proposition 6.4, expand it into a series with respect to a local parameter x/y and reduce the resulting series mod I. This proves the proposition. □

Proposition 7.4.

$$\log_{G_C} = z + \sum_{i=1}^{p-2} \frac{t_i}{p} u_i z^{p^i} \tag{7.2}$$

$t_i \in \mathbb{Z}_p^{\times}, \bmod I_0^2$ and mod *degree p^{p-1}. This implies that G_C is a universal deformation of the formal group law $\bar{G}_C$.*

Proof. Recall that the logarithm of G_C is obtained in the following way: choosing a local parameter z as in Corollary 4.4 we obtain the following formula for the expansion of the differential $\omega = \mathrm{d}x/y$ on the curve C_p. If $\omega = \omega(z)\,\mathrm{d}z$, then

$$\omega(z) = \frac{(1-p)}{1 - \left(\sum_{i=1}^{p-2} i u_i z^{p-i} w^{i-1} + (p-1) b z w^{p-2} \right)}, \tag{7.3}$$

where w satisfies the following functional equation:

$$w = z^p + \sum_{i=1}^{p-2} u_i z^{p-i} w^i + b z w^{p-1}. \tag{7.4}$$

Integrate $\omega(z)$ and cross out the terms $m_i z^i$ with i not equal to a power of p.

We claim that (7.2) holds for some $t_i \in \mathbb{Q}_p, \bmod I_0^2$. This follows from the following facts:

(a) In the series $w(z)$ and $\omega(z)$, reduced $\bmod I_0$, the powers of z are congruent to p and zero $\bmod (p-1)^2$, respectively.

(b) In the series $w(z)$ the coefficient of z^k is equal to $u_i \bmod$ degree two if and only if $k = p - i + pi$ or zero $\bmod (p-1)^2$.

(c) In the series $\omega(z)$ the coefficient of z^k is equal to $u_i \bmod$ degree two if and only if k is congruent to $pi - i$ or zero $\bmod (p-1)^2$.

(d) $p^{i-1} = pi - p \bmod (p-1)^2$, $1 \le i \le p-1$.

The proof is direct and uses (7.3) and (7.4).

Now we will prove that $t_i \in \mathbb{Z}_p^{\times}$. Examining the above formula for the expansion of the differential $\mathrm{d}x/y$, we easily see that $t_1 \in \mathbb{Z}_p^{\times}$. Suppose we have proved the proposition for $j < i$. Since F_C is isomorphic to G_C, the Corollary 6.7 implies that G_C has the Lubin–Tate property with respect to $\mathbb{G}_{p-1}$. In particular, there is a lift g of $\bar{g}$ from Proposition 7.3, such that

$$\alpha_g^*(G_C) = g(G_C).$$

For $\log_{G_C}$ we get the identity

$$\alpha_g^*(\log_{G_C})(z) = \frac{\log_{G_C}(g(z))}{g'(0)}$$

and taking into account that $g(z) = z + z^p \bmod$ degree $p+1$, we see that

$$\alpha_g^*(t_i u_i) = t_i u_i + t_{i-1} u_{i-1},$$

mod I_0^2, and mod $p, u_1, \ldots, u_{i-2}$, and $t_{i-1} \in \mathbb{Z}_p^\times$. On the other hand, the formulas in Proposition 6.4 tell that

$$\alpha_g^*(u_i) = u_i + c_{i-1}u_{i-1}$$

$c_{i-1} \in \mathbb{Z}_p^\times$, mod $p, u_1, \ldots, u_{i-2}$, and I_0^2. This implies that t_i must be a unit in $\mathbb{Z}_p$.

Proposition 1.1 from [7] implies now that G_C is a universal deformation of $\bar{G}_C$. □

The following corollary shows that the formulas from Proposition 6.4 can be used for calculations with the cohomology theories represented by the spectra $\mathbb{E}O_{p-1}$.

Corollary 7.5. *The representation of $\mathbb{G}_{p-1}$ defined by F_C is the Lubin–Tate representation.*

Acknowledgements

The authors wish to thank Mike Hopkins for useful comments, Avinash Sathaye for helpful discussions during the preparation of this paper and the referee for carefully reading the paper and suggesting a number of improvements.

References

[1] E. Devinatz, M.J. Hopkins, The action of the Morava stabilizer group on the Lubin–Tate moduli space of lifts, Amer. J. Math 117 (3) (1995) 669–710.
[2] M. Hazewinkel, Formal Groups and Applications, Academic Press, New York, 1978.
[3] T. Hewett, Finite subgroups of the Morava stabilizer algebra, preprint.
[4] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970) 213–246.
[5] T. Honda, On the formal structure of the Jacobian variety of the Fermat curve over a p-adic integer ring, Symp. Math. INDAM 11 (1973) 271–284.
[6] M.J. Hopkins, B.H. Gross, The rigid analytic period mapping, Lubin–Tate space, and stable homotopy theory, Bull. Amer. Math. Soc. 30 (1) (1994) 76–86.
[7] J. Lubin, J. Tate, Formal moduli for one parameter formal Lie groups, Bull. Soc. Math. France 94 (1966) 49–60.
[8] Yu.I. Manin, The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surveys 18 (1963) 1–81.
[9] H. Miller, AMS Summer Research Institute, Seattle, 1996.
[10] D.C. Ravenel, Complex Cobordism and Stable Homotopy Groups of Spheres, Academic Press, New York, 1986.
[11] G. Shimura, Y. Taniyama, Complex multiplication of abelian varieties and its application to number theory, Publ. Math. Soc. Japan 6 (1960).
[12] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 106, Springer, Berlin, 1986.