Canad. J. Math. Vol. **68** (2), 2016 pp. 334–360
http://dx.doi.org/10.4153/CJM-2015-024-7

Kernels in the Category of Formal Group Laws

Oleg Demchenko and Alexander Gurevich

Abstract. Fontaine described the category of formal groups over the ring of Witt vectors over a finite field of characteristic p with the aid of triples consisting of the module of logarithms, the Dieudonné module, and the morphism from the former to the latter. We propose an explicit construction for the kernels in this category in term of Fontaine's triples. The construction is applied to the formal norm homomorphism in the case of an unramified extension of $\mathbb{Q}_p$ and of a totally ramified extension of degree less or equal than p. A similar consideration applied to a global extension allows us to establish the existence of a strict isomorphism between the formal norm torus and a formal group law coming from L-series.

Introduction

The fundamental result of Cartier theory [Ca] provides a classification of the formal group laws over a commutative ring A by means of Cartier modules over the Cartier ring $\mathrm{Cart}(A)$. A detailed exposition of this theory can be found in [Zi]. In general, $\mathrm{Cart}(A)$ has a quite complicated structure; however, in the case where $A = k$ is a finite field, it becomes rather simple. In this special case, another description was suggested by Dieudonné who assigned to a formal group law over k a certain module (Dieudonné module). It can be shown that both theories are closely related. In the case where $A = W$ is the ring of the Witt vectors over k, Fontaine [Fo] associated with a formal group law F over A a triple $(\mathcal{L}, M, \rho)$ where M is the Dieudonné module of the reduction of F. It provides an alternative description of the category of formal group laws. Similar results formulated in terms of the logarithm types were obtained by Honda [Ho]. It turns out that the category of Fontaine's triples is easier to work with than the category of Cartier modules.

The goal of this paper is to give an explicit construction of kernels in the category of formal group laws over k and W in terms of Dieudonné modules and Fontaine's triples, respectively. This construction can be applied, in particular, to the subcategory of formal group laws of finite height, which is in turn equivalent to the category of connected p-divisible groups. The existence of kernels in the category of p-divisible groups over W follows from the result about the extension of a p-divisible group over the fraction field of W to a p-divisible group over W (the uniqueness of such extension is due to Tate [Ta] and the existence is due to Raynaud [Ra]). The desired kernel

Received by the editors October 6, 2014; revised April 27, 2015.
Published electronically October 21, 2015.
AMS subject classification: **14L05**.
Keywords: formal groups, p-divisible groups, Dieudonne modules, norm tori.

can be obtained by applying this result to the kernel of the generic fiber of the morphism of p-divisible groups. However, this construction is not explicit; in particular, it does not allow one to calculate Honda's type and the Dieudonné module of (the special fiber of) the kernel. Our approach corrects this deficiency. Moreover, we manage to deduce some well-known results on kernels in two special cases: homomorphisms between formal group laws of finite height and pure homomorphisms that are introduced within the scope of this note. The dual problem related to explicit construction of cokernels in the same categories is left for future investigation.

The technique developed is applied to the computation of Honda's type of the kernel of the formal norm homomorphism on the Weil restriction of the multiplicative formal group law with respect to an extension of $\mathbb{Q}_p$. When the extension is tamely ramified, this homomorphism is pure, which allows one to obtain the result in terms of the Jacobian matrix of the homomorphism. We also treat the case of a general totally ramified extension of degree p that vividly demonstrates the power of our explicit construction. Besides, a similar computation is performed for the formal norm homomorphism with respect to the extension of $\mathbb{Q}$ generated by q-th root of unity. This consideration implies the main result of Childress and Grant [CG], which establishes a strict isomorphism between a formal norm torus and a formal group law coming from L-series. Unlike [CG] where the global approach is exercised and heavy computations with formal power series are required, we easily deduce the existence of the isomorphism from rather simple local arguments. Finally, given an algebraic torus split over a tamely ramified extension, we consider the corresponding Galois action on the Weil restriction and prove that $\sigma - \mathrm{id}$ is pure for any Galois group element σ. This result is closely related to the smoothness of the subscheme of the Néron model for the Weil restriction of a split torus fixed by σ and allows one to find Honda's type of its formal completion explicitly (see [DGX]).

The outline of the paper is as follows. In Section 1, the main definitions related to formal group laws are introduced, and the classification results of Honda and Fontaine are recalled. Sections 2 is devoted to an explicit construction of kernels. The formal group laws of finite height are studied in Section 3. We show that in this case, the construction of the kernels can be essentially simplified. In particular, kernel commutes with the reduction modulo p. The pure homomorphisms are studied in Section 4. We prove that for such homomorphisms, Honda's type of kernel can be found as a submatrix of an appropriate conjugate of the type of the domain. As a consequence, any kernel of a pure homomorphism is strong, *i.e.*, coincides with the kernel in the category of formal group schemes. Finally, a necessary and sufficient condition for a homomorphism between formal group laws to be a (strong) monomorphism is given. In Section 5, several applications to formal group laws coming from algebraic tori are presented. The section is divided into three subsections. The first one is devoted to the formal norm homomorphism corresponding to extensions of local fields. For unramified extensions of $\mathbb{Q}_p$ and totally ramified extensions of $\mathbb{Q}_p$ of degree less or equal to p, Honda's type of the formal norm torus is calculated explicitly. In the second subsection, the formal norm homomorphism is studied for the extension of $\mathbb{Q}$ generated by a root of unity, and the result of Childress and Grant [CG] is deduced. The Galois action associated with an algebraic torus is considered in the third subsection.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Throughout the paper, the following notation is used. If M is a module and $S \subset M$, the submodule of M generated by S is denoted by $\langle S \rangle$. If N is a submodule of M, then $\mathrm{red}_N \colon M \to M/N$ is the reduction modulo N, *i.e.,* $\mathrm{red}_N(m) = m + N$.

1 Formal Group Laws

Basic Definitions

Denote by X and Y the sets of variables $x_1, \dots, x_d$ and $y_1, \dots, y_d$, respectively. A d-dimensional *formal group law* over a ring A is a d-tuple of formal power series $F \in A[\![X, Y]\!]^d$ such that

(a) $F(X, 0) = X$;
(b) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;
(c) $F(X, Y) = F(Y, X)$.

The one-dimensional *additive formal group law* and *multiplicative formal group law* are defined as $F_a(x, y) = x + y$ and $F_m(x, y) = x + y + xy$, respectively.

Denote by $A[\![X]\!]_0$ the subalgebra of $A[\![X]\!]$ of formal power series without constant term. Let F and G be d- and e-dimensional formal group laws over A. An e-tuple of formal power series $f \in A[\![X]\!]_0^e$ is a *homomorphism* from F to G if $f(F(X, Y)) = G(f(X), f(Y))$. The category of formal group laws over A is denoted by $\mathcal{FG}(A)$.

A matrix $D \in \mathrm{M}_{e,d}(A)$ such that $f(X) = DX \mod \deg 2$ is called the *Jacobian matrix* of the homomorphism f and denoted by $J(f)$. Formal group laws are *strictly isomorphic* if there exists an isomorphism between them with identity Jacobian matrix.

Denote by $\mathcal{N}il_A$ the category of nilpotent commutative associative A-algebras. If $N \in \mathcal{N}il_A$ and F is a d-dimensional formal group law over A, the *group of points* $F(N)$ is an abelian group with underlying set equal to N^d and addition defined by F, *i.e.,* $a +_F b = F(a, b)$ for $a, b \in N^d$. It is clear that any morphism $\phi \colon N_1 \to N_2$ of nilpotent A-algebras induces a homomorphism $F(\phi) \colon F(N_1) \to F(N_2)$. Similarly, any homomorphism $f \in \mathrm{Hom}_A(F, G)$ of formal group laws induces a homomorphism $f(N) \colon F(N) \to G(N)$. It is clear that $f(N_2) \circ F(\phi) = G(\phi) \circ f(N_1)$.

Yoneda lemma *Let F and G be formal group laws over A. Suppose that for any nilpotent A-algebra N, there is a homomorphism $f_N \colon F(N) \to G(N)$ such that for any morphism $\phi \colon N_1 \to N_2$ of nilpotent A-algebras, $f_{N_2} \circ F(\phi) = G(\phi) \circ f_{N_1}$. Then there exists a unique $f \in \mathrm{Hom}_A(F, G)$ such that $f(N) = f_N$ for any nilpotent A-algebra N.*

A formal group law over a $\mathbb{Q}$-algebra possesses a distinguished homomorphism that plays an important role in the subsequent exposition.

Proposition 1.1 ([Ho, Theorem 1]) *For any d-dimensional formal group law F over a $\mathbb{Q}$-algebra B, there exists a unique $\lambda \in \mathrm{Hom}_B(F, F_a^d)$ such that $J(\lambda) = I_d$.*

If F is a formal group law over A and B is an A-algebra, we denote by F_B the formal group law over B obtained by the extension of scalars.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Suppose that $\operatorname{char} A = 0$. Then $A \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra. If F is a formal group law over A, then application of Proposition 1.1 to $F_{A\otimes_{\mathbb{Z}}\mathbb{Q}}$ yields a unique $\lambda \in A \otimes_{\mathbb{Z}} \mathbb{Q}[[X]]_0^d$ which is called the *logarithm* of F. Since $F(X, Y) = \lambda^{-1}(\lambda(X)+\lambda(Y))$, a formal group law is uniquely defined by its logarithm.

Proposition 1.2 ([Ho, Proposition 1.6]) *If F, G are formal group laws over A with logarithms λ, μ, respectively, and $f \in \operatorname{Hom}_A(F, G)$, then $f = \mu^{-1} \circ J(f)\lambda$.*

Honda Theory

Honda theory [Ho] gives an explicit description up to strict isomorphism of formal group laws over finite fields and their rings of Witt vectors.

Let K be a finite unramified extension of $\mathbb{Q}_p$ with residue field k, integer ring $\mathcal{O}_K$, and Frobenius automorphism Δ. Let $\blacktriangle: K[[X]]_0 \to K[[X]]_0$ be a $\mathbb{Q}_p$-algebra map defined by $\blacktriangle(x_i) = x_i^p$, $1 \le i \le d$ and $\blacktriangle(a) = \Delta(a)$, $a \in K$. Denote by $\mathcal{E} = \mathcal{O}_K[[\blacktriangle]]$ a non-commutative $\mathbb{Q}_p$-algebra of formal power series in $\blacktriangle$ with multiplication rule $\blacktriangle a = \Delta(a)\blacktriangle$ for $a \in \mathcal{O}_K$. Then $K[[X]]_0$ has a left $\mathcal{E}$-module structure that induces a left $\mathrm{M}_d(\mathcal{E})$-module structure on $K[[X]]_0^d$.

If $u \in \mathrm{M}_d(\mathcal{E})$, $u \equiv pI_d \mod \blacktriangle$, and $\lambda \in K[[X]]_0^d$, $J(\lambda) = I_d$ are such that $u\lambda \in p\mathcal{O}_K[[X]]_0^d$, we say that λ is *of type* u. It is obvious that the logarithm of the additive formal group law $\lambda_a(x) = x$ is of type p. If $u \in \mathrm{M}_d(\mathcal{E})$, $u \equiv pI_d \mod \blacktriangle$, then $(u^{-1}p)(X) \in K[[X]]_0^d$ is of type u.

The following are the main results of Honda theory.

(1) If $\lambda \in K[[X]]_0^d$ is of type u, then λ is the logarithm of a formal group law over $\mathcal{O}_K$.

(2) If $\lambda \in K[[X]]_0^d$ is of type u and $v\lambda \in p\mathcal{O}_K[[X]]_0^d$ for some $v \in \mathrm{M}_{e,d}(\mathcal{E})$, then there exists $w \in \mathrm{M}_{e,d}(\mathcal{E})$ such that $v = wu$. In particular, if u, v are types of λ, then there is $w \in \mathrm{M}_d(\mathcal{E})$ such that $v = wu$.

(3) For any formal group law F over $\mathcal{O}_K$ with logarithm $\lambda \in K[[X]]_0^d$, there exists $u \in \mathrm{M}_d(\mathcal{E})$ such that λ is of type u.

(4) Any formal group law over k is the reduction of a formal group law over $\mathcal{O}_K$.

(5) Let F, G be d- and e-dimensional formal group laws over $\mathcal{O}_K$ with logarithms λ, μ of types u, v, respectively, and $D \in \mathrm{M}_{e,d}(\mathcal{O}_K)$. Then $\mu^{-1} \circ D\lambda \in \mathcal{O}_K[[X]]^d$ if and only if there exists $w \in \mathrm{M}_{e,d}(\mathcal{E})$ such that $vD = wu$. In this case, $\mu^{-1} \circ D\lambda \in \operatorname{Hom}_{\mathcal{O}_K}(F, G)$ and any homomorphism between F and G can be obtained in this way. In particular, formal group laws with logarithms of the same type are strictly isomorphic.

(6) Let F, G be d- and e-dimensional formal group laws over $\mathcal{O}_K$ with logarithms λ, μ of types u, v, respectively, and $w \in \mathrm{M}_{e,d}(\mathcal{E})$. Then $\mu^{-1} \circ w\lambda \in \mathcal{O}_K[[X]]^d$ if and only if there exists $t \in \mathrm{M}_{e,d}(\mathcal{E})$ such that $vw = tu$. In this case the reduction modulo p of $\mu^{-1} \circ w\lambda$ belongs to $\operatorname{Hom}_k(F_k, G_k)$, and any homomorphism between F_k and G_k can be obtained in this way.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Dieudonné Modules

Our exposition of the theory of Dieudonné modules follows an explicit approach of Fontaine [Fo, Chap. V, § 2] based on results of Honda.

Let F be a d-dimensional formal group law over $\mathcal{O}_K$. Denote

$$\mathcal{M}(F) = \Big\{ l \in K[[X]]_0 : \partial l/\partial x_i \in \mathcal{O}_K[[X]],\ 1 \le i \le d,\\ l\big(F(X,Y)\big) - \big(l(X) + l(Y)\big) \in p\mathcal{O}_K[[X]]_0 \Big\}.$$

One can show that $\mathcal{M}(F)$ is an $\mathcal{E}$-submodule of $K[[X]]_0$, and $p\mathcal{O}_K[[X]]_0$ is an $\mathcal{E}$-submodule of $\mathcal{M}(F)$. Then $M(F) = \mathcal{M}(F)/p\mathcal{O}_K[[X]]_0$ depends only on F_k and is called its *Dieudonné module*. It possesses the following properties:

(a) $M(F)$ is a finitely generated $\mathcal{E}$-module;
(b) $\blacktriangle: M(F) \to M(F)$ is injective;
(c) $pM(F) \subset \blacktriangle M(F)$.

Let

$$\mathcal{L}(F) = \big\{ l \in K[[X]]_0 : \partial l/\partial x_i \in \mathcal{O}_K[[X]], 1 \le i \le d, l\big(F(X,Y)\big) = l(X) + l(Y) \big\}.$$

Then $\mathcal{L}(F)$ is a free $\mathcal{O}_K$-module of rank d. Denote by $\rho(F): \mathcal{L}(F) \to M(F)$ the composition of the inclusion of $\mathcal{L}(F)$ in $\mathcal{M}(F)$ and the reduction modulo $p\mathcal{O}_K[[X]]_0$. It is an $\mathcal{O}_K$-morphism, and the induced morphism $\mathcal{L}(F)/p\mathcal{L}(F) \to M(F)/\blacktriangle M(F)$ is an isomorphism.

If F, G are formal group laws over $\mathcal{O}_K$ and $f \in \mathrm{Hom}(F,G)$, define $\mathcal{M}(f)(l) = l \circ f \in \mathcal{M}(F)$ for $l \in \mathcal{M}(G)$. Then f induces morphisms $M(f): M(G) \to M(F)$, $\mathcal{L}(f): \mathcal{L}(G) \to \mathcal{L}(F)$ such that $\rho(F) \circ \mathcal{L}(f) = M(f) \circ \rho(G)$.

Denote by $\mathcal{C}$ the category of finitely generated $\mathcal{E}$-modules M such that $\blacktriangle: M \to M$ is injective and $pM \subset \blacktriangle M$. Define by $\mathcal{CT}$ the category of triples $(\mathcal{L}, M, \rho)$ such that

(a) $\mathcal{L}$ is a free $\mathcal{O}_K$-module of finite rank;
(b) $M \in \mathcal{C}$;
(c) $\rho: \mathcal{L} \to M$ is an $\mathcal{O}_K$-morphism which induces an isomorphism $\mathcal{L}/p\mathcal{L} \to M/\blacktriangle M$.

The finite-generatedness of M implies that M is a complete topological $\mathcal{E}$-module in $\blacktriangle$-adic topology; *i.e.,* for any sequence $\{m_i\}$ in M there exists $\sum \blacktriangle^i m_i \in M$.

A morphism from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$ is a pair (ψ, Ψ), where $\psi: \mathcal{L}' \to \mathcal{L}$ is an $\mathcal{O}_K$-morphism, $\Psi: M' \to M$ is an $\mathcal{E}$-morphism, and $\Psi \circ \rho' = \rho \circ \psi$.

Theorem ([Fo, Chap. III, Prop. 6.1 and Chap. IV, Th. 1])

(i) *For any formal group law Φ over k there exists a formal group law F over $\mathcal{O}_K$ such that $\Phi = F_k$. The correspondence $\Phi \mapsto M(F)$ is an anti-equivalence between $\mathcal{FG}(k)$ and $\mathcal{C}$;*
(ii) *The correspondence $F \mapsto (\mathcal{L}(F), M(F), \rho(F))$ is an anti-equivalence between $\mathcal{FG}(\mathcal{O}_K)$ and $\mathcal{CT}$;*
(iii) *The reduction functor from $\mathcal{FG}(\mathcal{O}_K)$ to $\mathcal{FG}(k)$ corresponds to the forgetful functor from $\mathcal{CT}$ to $\mathcal{C}$,* i.e., *to the functor $(\mathcal{L}, M, \rho) \mapsto M$.*

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Let F be a d-dimensional formal group law over $\mathcal{O}_K$ with logarithm λ of type u. Define $\mathcal{H}(F) = (\mathcal{O}_K^d, \mathcal{E}^d/\mathcal{E}^d u, \kappa)$, where $\kappa\colon \mathcal{O}_K^d \to \mathcal{E}^d/\mathcal{E}^d u$ is induced by the inclusion of $\mathcal{O}_K^d$ into $\mathcal{E}^d$. One can easily show that $\mathcal{H}(F)$ is an object in the category $\mathcal{CT}$. If $F, G \in \mathcal{FG}(\mathcal{O}_K)$ and $f \in \mathrm{Hom}(F, G)$, $J(f) = D$, then the mapping $l \mapsto lD, l \in \mathcal{O}_K^e$ induces a morphism $\mathcal{H}(G) \to \mathcal{H}(F)$ in $\mathcal{CT}$, which defines a functor from $\mathcal{FG}(\mathcal{O}_K)$ to $\mathcal{CT}$.

Let F be a d-dimensional formal group law F over $\mathcal{O}_K$ with logarithm $\lambda = (\lambda_1, \ldots, \lambda_d)$. The correspondence $(a_1, \ldots, a_d) \mapsto (a_1\lambda_1, \ldots, a_d\lambda_d)$ induces a morphism $\mathcal{H}(F) \to (\mathcal{L}(F), M(F), \rho(F))$ in $\mathcal{CT}$. One can see that it gives a natural isomorphism between $\mathcal{H}$ and Fontaine functor $(\mathcal{L}, M, \rho)$.

Kernels in $\mathcal{FG}(k)$ have very easy construction. The proof of the following theorem is straightforward.

Theorem 1.3 *Let $M, M' \in \mathcal{C}$, $\Psi \in \mathrm{Hom}(M', M)$, and*

$$M_{\blacktriangle} = \{m \in M : \blacktriangle^h m \in \mathrm{Im}\,\Psi \text{ for some } h \geq 0\}.$$

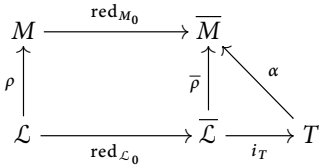
Then $M/M_{\blacktriangle} \in \mathcal{C}$ along with $\mathrm{red}_{M_{\blacktriangle}}\colon M \to M/M_{\blacktriangle}$ is a cokernel of the morphism Ψ.

2 Kernels in $\mathcal{FG}(\mathcal{O}_K)$

Let (ψ, Ψ) be a morphism from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$ in the category $\mathcal{CT}$. Define $\mathcal{L}_0 = \{l \in \mathcal{L} : al = \psi(l') \text{ for some } a \in \mathcal{O}_K, a \neq 0 \text{ and } l' \in \mathcal{L}'\}$. Then $\overline{\mathcal{L}} = \mathcal{L}/\mathcal{L}_0$ is a torsion-free and therefore free $\mathcal{O}_K$-module.

Let $M_0 = \langle \rho(\mathcal{L}_0) \rangle \subset M$. Clearly, $\mathrm{Im}\,\Psi \subset M_0$. For the quotient module $\overline{M} = M/M_0$, there is a uniquely defined $\mathcal{O}_K$-homomorphism $\overline{\rho}\colon \overline{\mathcal{L}} \to \overline{M}$ such that $\overline{\rho} \circ \mathrm{red}_{\mathcal{L}_0} = \mathrm{red}_{M_0} \circ \rho$. Notice that $\blacktriangle$ may or may not be injective on $\overline{M}$.

Let $T = \mathcal{E}\widehat{\otimes}_{\mathcal{O}_K}\overline{\mathcal{L}}$ and $i_T\colon \overline{\mathcal{L}} \to T$ be the canonical inclusion, $i_T(l) = 1 \otimes l$. Define homomorphisms $\alpha\colon T \to \overline{M}$ by $\alpha(\sum \blacktriangle^k \otimes l_k) = \sum \blacktriangle^k \overline{\rho}(l_k)$ and $j_T\colon T \to \overline{\mathcal{L}}$ by $j_T(\sum \blacktriangle^k \otimes l_k) = l_0$. Clearly, α is surjective.



Denote $J = \{m \in T : \blacktriangle^h \alpha(m) = 0 \text{ for some } h \geq 0\}$ and $J^0 = j_T(J)$. Then J is a submodule of T containing $\mathrm{Ker}\,\alpha$, and J^0 is a submodule of $\overline{\mathcal{L}}$. Notice that $\blacktriangle$ is injective on T/J.

Lemma 2.1 $p\overline{\mathcal{L}} \subset J^0$.

Proof The properties of the triple $(\mathcal{L}, M, \rho)$ imply that $p\rho(\mathcal{L}) \subset \blacktriangle M$. Hence $p\overline{\rho}(\overline{\mathcal{L}}) \subset \blacktriangle\overline{M}$, *i.e.*, $\alpha \circ i_T(pl) \in \blacktriangle\overline{M}$ for any $l \in \overline{\mathcal{L}}$. Since α is surjective, $i_T(pl) \in \mathrm{Ker}\,\alpha + \blacktriangle T$. As $\mathrm{Ker}\,\alpha \subset J$, we have $pl \in J^0$. ∎

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Lemma 2.1 implies that $T/J \in \mathcal{C}$. However, the triple $(\overline{\mathcal{L}}, T/J, \mathrm{red}_J \circ i_T)$ may or may not belong to $\mathcal{CT}$. Thus, one needs to modify T/J.

Lemma 2.2 *Let A be an $\mathcal{O}_K$-module and let B be its submodule. Let C be a maximal submodule among the submodules C' of B satisfying the condition*

$$a \in A, pa \in C' \Longrightarrow a \in C'.$$

Then for any $b \in B$, there exists $c \in C$ such that $b - c \in pA$.

Proof Put $C' = C + \mathcal{O}_K b$. If $C' = C$, then $b \in C$, and we are done. Otherwise, there is $a \in A \setminus C'$ such that $pa = c + tb$ for some $c \in C, t \in \mathcal{O}_K$. If $t = pt'$ for $t' \in \mathcal{O}_K$ then $c = p(a - t'b)$. It gives $a - t'b \in C$, *i.e.*, $a \in C'$, a contradiction. Therefore, $t \in \mathcal{O}_K^*$ and $b + t^{-1}c \in pA$, as required. ∎

Let $\mathcal{L}^+$ be a submodule of J^0 such that

(a) for any $l \in J^0$ there exists $l_1 \in \mathcal{L}^+$ with $l - l_1 \in p\overline{\mathcal{L}}$;
(b) if $l \in \overline{\mathcal{L}}, pl \in \mathcal{L}^+$ then $l \in \mathcal{L}^+$.

The latter condition implies that there exists a submodule $\mathcal{L}^-$ of $\overline{\mathcal{L}}$ such that $\mathcal{L}^+ \oplus \mathcal{L}^- = \overline{\mathcal{L}}$.

Lemma 2.2 proves the existence of $\mathcal{L}^+$. An equivalent and more explicit construction can be given as follows. Let $r: \overline{\mathcal{L}} \to \overline{\mathcal{L}}/p\overline{\mathcal{L}}$ be the reduction modulo p. Let $y_1, \dots, y_n$ be an $\mathbb{F}_p$-basis of $r(J^0)$. Choose any $l_1, \dots, l_n \in J^0$ such that $r(l_k) = y_k, 1 \le k \le n$. Then $\mathcal{L}^+ = \langle l_1, \dots, l_n \rangle$.

Define an endomorphism $\tau_0: \overline{\mathcal{L}} \to \overline{\mathcal{L}}$ by

$$\tau_0(l) = \begin{cases} pl, & l \in \mathcal{L}^+, \\ l, & l \in \mathcal{L}^-. \end{cases}$$

Lemma 2.3 $\tau_0(J^0) = p\overline{\mathcal{L}}$.

Proof For any $l \in J^0$, there is $l_1 \in \mathcal{L}^+$ such that $l - l_1 \in p\overline{\mathcal{L}}$, which gives $\tau_0(l) \in p\overline{\mathcal{L}}$. In order to prove the inclusion $p\overline{\mathcal{L}} \subset \tau_0(J^0)$, we consider separately two cases: $l \in \mathcal{L}^+$ and $l \in \mathcal{L}^-$. If $l \in \mathcal{L}^+$, then $l \in J^0$ and $pl = \tau_0(l) \in \tau_0(J^0)$. If $l \in \mathcal{L}^-$ then $pl = \tau_0(pl) \in \tau_0(J^0)$ by Lemma 2.1. ∎

Extend τ_0 to $\tau \in \mathrm{End}\ T$ so that $\tau \circ i_T = i_T \circ \tau_0$. Denote $\overline{M}^\tau = T/\tau(J)$ and $\overline{\rho}^\tau = \mathrm{red}_{\tau(J)} \circ i_T$. Since α is surjective and $\mathrm{Ker}\,\alpha \subset J$, there is a unique homomorphism $\tau^*: \overline{M} \to \overline{M}^\tau$ such that $\tau^* \circ \alpha = \mathrm{red}_{\tau(J)} \circ \tau$.

$$\begin{array}{ccccc} J & \hookrightarrow & T & \xrightarrow{\ \tau\ } & T \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{red}_{\tau(J)}} \\ & & \overline{M} & \xrightarrow[\ \tau^*\ ]{} & \overline{M}_\tau \end{array}$$

Proposition 2.4 $(\overline{\mathcal{L}}, \overline{M}^\tau, \overline{\rho}^\tau) \in \mathcal{CT}$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

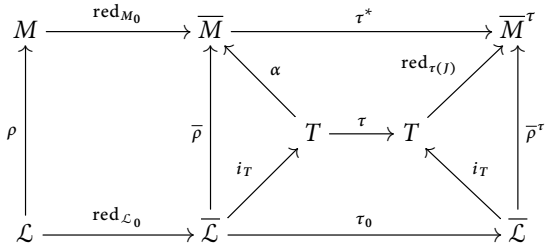
Proof Only the following properties are not obvious:

(1) $\blacktriangle$ is injective on $\overline{M}^{\tau}$. Let $\blacktriangle m = \tau(m_1)$ for $m \in T, m_1 \in J$. Then $m_1 = \blacktriangle m_2$ and $m = \tau(m_2)$ for some $m_2 \in T$. Since $m_1 = \blacktriangle m_2 \in J$, it follows that $m_2 \in J$. Thus, $m \in \tau(J)$, as required.

(2) $p\overline{M}^{\tau} \subset \blacktriangle \overline{M}^{\tau}$. If $l \in \overline{\mathcal{L}}$, then $pl \in \tau_0(J^0)$ by Lemma 2.3, *i.e.*, $pi_T(l) = \tau(m_1) + m_2$ for $m_1 \in J, m_2 \in \blacktriangle T$, which gives the desired conclusion.

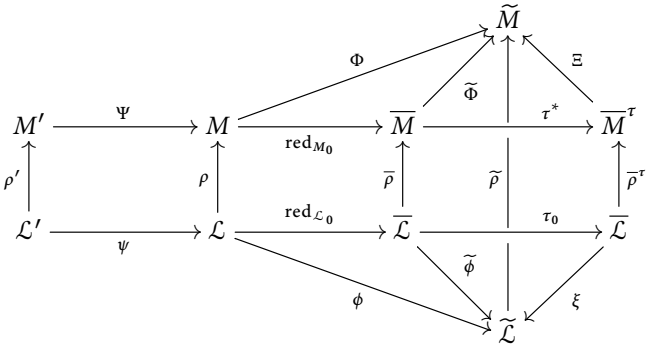
(3) The induced homomorphism $\overline{\mathcal{L}}/p\overline{\mathcal{L}} \to \overline{M}^{\tau}/\blacktriangle\overline{M}^{\tau}$ is injective. If $i_T(l) - \tau(m) \in \blacktriangle T$ for $l \in \overline{\mathcal{L}}, m \in J$, then $l = j_T \circ i_T(l) = j_T \circ \tau(m) = \tau_0 \circ j_T(m) \in \tau_0(J^0) = p\overline{\mathcal{L}}$ by Lemma 2.3. ■

The commutativity of the five inner diagrams implies that the outer diagram is also commutative, *i.e.*, $(\tau_0 \circ \mathrm{red}_{\mathcal{L}_0}, \tau^* \circ \mathrm{red}_{M_0})$ is a morphism from $(\mathcal{L}, M, \rho)$ to $(\overline{\mathcal{L}}, \overline{M}^{\tau}, \overline{\rho}^{\tau})$.



Theorem 2.5 *The triple* $(\overline{\mathcal{L}}, \overline{M}^{\tau}, \overline{\rho}^{\tau})$ *along with* $(\tau_0 \circ \mathrm{red}_{\mathcal{L}_0}, \tau^* \circ \mathrm{red}_{M_0})$ *is a cokernel of the morphism* (ψ, Ψ).

Proof Let (ϕ, Φ) be a morphism from $(\mathcal{L}, M, \rho)$ to a triple $(\widetilde{\mathcal{L}}, \widetilde{M}, \widetilde{\rho}) \in \mathcal{CT}$ such that $\phi \circ \psi = 0, \Phi \circ \Psi = 0$. One needs to show that there exists a unique morphism (ξ, Ξ) from $(\overline{\mathcal{L}}, \overline{M}^{\tau}, \overline{\rho}^{\tau})$ to $(\widetilde{\mathcal{L}}, \widetilde{M}, \widetilde{\rho})$ such that $(\phi, \Phi) = (\xi, \Xi) \circ (\tau_0 \circ \mathrm{red}_{\mathcal{L}_0}, \tau^* \circ \mathrm{red}_{M_0})$.



Since $\phi \circ \psi = 0$, one has $\phi(\mathcal{L}_0) = 0$, and there is a homomorphism $\widetilde{\phi}: \overline{\mathcal{L}} \to \widetilde{\mathcal{L}}$ such that $\phi = \widetilde{\phi} \circ \mathrm{red}_{\mathcal{L}_0}$. Similarly, $\phi(\mathcal{L}_0) = 0$ implies $\Phi(M_0) = 0$, hence there is a homomorphism $\widetilde{\Phi}: \overline{M} \to \widetilde{M}$ such that $\Phi = \widetilde{\Phi} \circ \mathrm{red}_{M_0}$ and $\widetilde{\Phi} \circ \overline{\rho} = \widetilde{\rho} \circ \widetilde{\phi}$.

Let $l \in \mathcal{L}^+ \subset J^0$. Then $i_T(l) - m \in \blacktriangle T$ for some $m \in J$. It gives $\widetilde{\rho} \circ \widetilde{\phi}(l) = \widetilde{\Phi} \circ \overline{\rho}(l) = \widetilde{\Phi} \circ \alpha \circ i_T(l) \in \blacktriangle \widetilde{M}$. From the properties of $(\widetilde{\mathcal{L}}, \widetilde{M}, \widetilde{\rho})$, we conclude that $\widetilde{\phi}(l) \in p\widetilde{\mathcal{L}}$,

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

which enables us to define a homomorphism $\xi\colon\overline{\mathcal{L}}\to\widetilde{\mathcal{L}}$ by

$$\xi(l)=\begin{cases} l_1 \text{ for } \widetilde{\phi}(l)=pl_1, & l\in\mathcal{L}^+,\\ \widetilde{\phi}(l), & l\in\mathcal{L}^-.\end{cases}$$

Clearly, $\widetilde{\phi}=\xi\circ\tau_0$.

We next construct a homomorphism $\Xi\colon\overline{M}^{\tau}\to\widetilde{M}$. For $m=\sum\blacktriangle^k i_T(l_k)\in T$, put $\Xi(m+\tau(J))=\sum\blacktriangle^k\widetilde{\rho}\circ\xi(l_k)$. If $\sum\blacktriangle^k i_T(l_k)\in\tau(J)$, then

$$\sum\blacktriangle^k i_T(l_k)=\tau\Big(\sum\blacktriangle^k i_T(l'_k)\Big)=\sum\blacktriangle^k i_T\circ\tau_0(l'_k)$$

for $\sum\blacktriangle^k i_T(l'_k)\in J$. It implies $l_k=\tau_0(l'_k)$, $k\ge 0$ and $\blacktriangle^h\alpha(\sum\blacktriangle^k i_T(l'_k))=0$ for some $h\ge 0$.

One needs to prove that $\sum\blacktriangle^k\widetilde{\rho}\circ\xi(l_k)=0$. Since $\widetilde{\Phi}\circ\alpha\circ i_T=\widetilde{\Phi}\circ\overline{\rho}=\widetilde{\rho}\circ\widetilde{\phi}=\widetilde{\rho}\circ\xi\circ\tau_0$, one gets $\sum\blacktriangle^k\widetilde{\rho}\circ\xi(l_k)=\sum\blacktriangle^k\widetilde{\rho}\circ\xi\circ\tau_0(l'_k)=\sum\blacktriangle^k\widetilde{\Phi}\circ\alpha\circ i_T(l'_k)=\widetilde{\Phi}\circ\alpha(\sum\blacktriangle^k i_T(l'_k))$. Therefore, $\blacktriangle^h(\sum\blacktriangle^k\widetilde{\rho}\circ\xi(l_k))=0$ and $\sum\blacktriangle^k\widetilde{\rho}\circ\xi(l_k)=0$, as required. It shows that Ξ is well defined.

Clearly, $\Xi\circ\mathrm{red}_{\tau(J)}\circ i_T=\widetilde{\rho}\circ\xi$, *i.e.*, (ξ,Ξ) is a morphism from $(\overline{\mathcal{L}},\overline{M}^{\tau},\overline{\rho}^{\tau})$ to $(\widetilde{\mathcal{L}},\widetilde{M},\widetilde{\rho})$.

Note that

$$\begin{aligned}\Xi\circ\mathrm{red}_{\tau(J)}\circ\tau\Big(\sum\blacktriangle^k i_T(l_k)\Big)&=\Xi\circ\mathrm{red}_{\tau(J)}\Big(\sum\blacktriangle^k i_T\circ\tau_0(l_k)\Big)\\&=\sum\blacktriangle^k\widetilde{\rho}\circ\xi\circ\tau_0(l_k)=\sum\blacktriangle^k\widetilde{\Phi}\circ\alpha\circ i_T(l_k)\\&=\widetilde{\Phi}\circ\alpha\Big(\sum\blacktriangle^k i_T(l_k)\Big).\end{aligned}$$

Finally, $\phi=\widetilde{\phi}\circ\mathrm{red}_{\mathcal{L}_0}=\xi\circ\tau_0\circ\mathrm{red}_{\mathcal{L}_0}$, and since α is surjective, the equality $\widetilde{\Phi}\circ\alpha=\Xi\circ\mathrm{red}_{\tau(J)}\circ\tau=\Xi\circ\tau^*\circ\alpha$ implies $\widetilde{\Phi}=\Xi\circ\tau^*$, which gives $\Phi=\widetilde{\Phi}\circ\mathrm{red}_{M_0}=\Xi\circ\tau^*\circ\mathrm{red}_{M_0}$.

What remains is to show the uniqueness of (ξ,Ξ). Suppose that there are homomorphisms $\xi'\colon\overline{\mathcal{L}}\to\widetilde{\mathcal{L}}$ and $\Xi'\colon\overline{M}^{\tau}\to\widetilde{M}$ such that $\Xi'\circ\overline{\rho}^{\tau}=\widetilde{\rho}\circ\xi'$, $\phi=\xi'\circ\tau_0\circ\mathrm{red}_{\mathcal{L}_0}$ and $\Phi=\Xi'\circ\tau^*\circ\mathrm{red}_{M_0}$. Clearly, $\xi'\circ\tau_0=\widetilde{\phi}=\xi\circ\tau_0$, which gives $\xi'=\xi$.

Now, $\Xi'\circ\mathrm{red}_{\tau(J)}\circ i_T=\Xi\circ\mathrm{red}_{\tau(J)}\circ i_T$ and $\Xi'\circ\mathrm{red}_{\tau(J)}=\Xi\circ\mathrm{red}_{\tau(J)}$, hence $\Xi'=\Xi$. ∎

Corollary 2.6 *Let $F,G\in\mathcal{FG}(\mathcal{O}_K)$ and $f\in\mathrm{Hom}(F,G)$. If (F_0,f_0) is a kernel of f, then* $\dim F_0=\dim F-\mathrm{rk}_K J(f)$ *and* $\mathrm{rk}_K J(f_0)=\dim F_0$.

Example Let F be a 3-dimensional formal group law over $\mathbb{Z}_p$ with logarithm

$$\lambda(x_1,x_2,x_3)=(x_1,x_2,x_3-x_1^p/p-x_2^{p^2}/p).$$

Then $f=(0\ 0\ p)\lambda$ for $f(x_1,x_2,x_3)=px_3-x_1^p-x_2^{p^2}$, which implies $f\in\mathrm{Hom}(F,F_a)$.

Consider a 2-dimensional formal group law H over $\mathbb{Z}_p$ with logarithm $\mu(y_1,y_2)=(y_1-y_2^p/p,y_2)$. Since $\lambda\circ h=D\mu$ for

$$h(y_1,y_2)=\Big(py_1-y_2^p,y_2,\big((py_1-y_2^p)^p+y_2^{p^2}\big)/p\Big)\quad\text{and}\quad D=\begin{pmatrix}p&0\\0&1\\0&0\end{pmatrix},$$

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

we obtain that $h \in \mathrm{Hom}(H, F)$ and $f \circ h = 0$.

In order to show that (H, h) is a kernel of the homomorphism f, we use the construction from Theorem 2.5. The logarithms λ and μ are of types u and v, respectively, where

$$u = \begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ \blacktriangle & \blacktriangle^2 & p \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} p & \blacktriangle \\ 0 & p \end{pmatrix}.$$

Let $\mathcal{L}_a$ be a free $\mathbb{Z}_p$-module with generator d; $\mathcal{L}$ be a free $\mathbb{Z}_p$-module with generators d_1, d_2, d_3 and $\psi(d) = pd_3$. Moreover,

$$M = \big\langle \rho(d_1), \rho(d_2), \rho(d_3) \big\rangle / \big\langle p\rho(d_1), p\rho(d_2), p\rho(d_3) + \blacktriangle\rho(d_1) + \blacktriangle^2\rho(d_2) \big\rangle.$$

It is clear that $\mathcal{L}_0$ is generated by d_3, thus $\overline{\mathcal{L}} = \langle \overline{d}_1, \overline{d}_2 \rangle$, where $\overline{d}_j = \mathrm{red}_{\mathcal{L}_0} d_j, 1 \le j \le 2$, and

$$\overline{M} \cong \big\langle \overline{\rho}(\overline{d}_1), \overline{\rho}(\overline{d}_2) \big\rangle / \big\langle p\overline{\rho}(\overline{d}_1), p\overline{\rho}(\overline{d}_2), \blacktriangle\overline{\rho}(\overline{d}_1) + \blacktriangle^2\overline{\rho}(\overline{d}_2) \big\rangle.$$

Denoting $D_j = i_T(\overline{d}_j), 1 \le j \le 2$, we have $T = \langle D_1, D_2 \rangle$. Moreover,

$$J = \langle D_1 + \blacktriangle D_2, pD_1, pD_2 \rangle = \langle D_1 + \blacktriangle D_2, pD_2 \rangle,$$

since $\blacktriangle\alpha(D_1 + \blacktriangle D_2) = \alpha(pD_1) = \alpha(pD_2) = 0$. Notice that $(\overline{\mathcal{L}}, T/J, \mathrm{red}_J \circ i_T)$ is not an object in $\mathcal{CT}$, since $\overline{\mathcal{L}}/p\overline{\mathcal{L}}$ is a $\mathbb{Z}/p\mathbb{Z}$-module of rank 2, while $(T/J)/\blacktriangle(T/J)$ is a $\mathbb{Z}/p\mathbb{Z}$-module of rank 1 generated by the image of $D_2 + J$. We have $J^0 = \langle \overline{d}_1, p\overline{d}_2 \rangle$, and we can choose $\mathcal{L}^+ = \langle \overline{d}_1 \rangle$, $\mathcal{L}^- = \langle \overline{d}_2 \rangle$. In this situation, $\tau_0(\overline{d}_1) = p\overline{d}_1, \tau_0(\overline{d}_2) = \overline{d}_2$. Therefore,

$$\tau(J) = \langle pD_1 + \blacktriangle D_2, pD_2 \rangle \quad \text{and} \quad \overline{M}^\tau = T/\tau(J) = \langle D_1, D_2 \rangle / \langle pD_1 + \blacktriangle D_2, pD_2 \rangle.$$

Thus, the logarithm of a kernel is of type v and the Jacobian matrix of the corresponding homomorphism is equal to D.

In some cases, the construction of kernel in the category $\mathcal{FG}(\mathcal{O}_K)$ can be significantly simplified as the following proposition shows.

Proposition 2.7 *The following conditions are equivalent:*

(i) $p\rho(\mathcal{L}_0) \subset \blacktriangle M_0$;
(ii) $\blacktriangle$ *is injective on* $\overline{M}$;
(iii) $J = \mathrm{Ker}\,\alpha$;
(iv) $J^0 = p\overline{\mathcal{L}}$;
(v) τ *is identical.*

Proof Implications (ii) $\Rightarrow$ (iii) and (iv) $\Leftrightarrow$ (v) are clear.

(i) $\Rightarrow$ (ii) Let $\blacktriangle m \in M_0$ for some $m \in M$. Then $\blacktriangle m = \rho(l_0) + m_1$, where $l_0 \in \mathcal{L}_0$, $m_1 \in \blacktriangle M_0$. Evidently, $l_0 = pl$ and $l \in \mathcal{L}_0$. It gives $\blacktriangle m \in \blacktriangle M_0$; thus, $m \in M_0$, as required.

(ii) $\Rightarrow$ (i) If $p\rho(l) = \blacktriangle m$ for $l \in \mathcal{L}_0, m \in M$, then $\blacktriangle\widetilde{m} = 0$ for $\widetilde{m} = \mathrm{red}_{M_0} m$. It gives $\widetilde{m} = 0$, *i.e.*, $m \in M_0$.

(iii) $\Rightarrow$ (ii) If $\blacktriangle\widetilde{m} = 0$ for $\widetilde{m} \in \overline{M}$, then for $m \in T$, $\widetilde{m} = \alpha(m)$ one gets $m \in J$, whence $\widetilde{m} = 0$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

(iii) $\Rightarrow$ (iv) If $l \in J^0$, then $i_T(l) = m_1 + m_2$, where $m_1 \in \operatorname{Ker}\alpha$, $m_2 \in \blacktriangle T$. It gives $\overline{\rho}(l) = \alpha(m_2) \in \blacktriangle\overline{M}$, which in turn implies $l \in p\overline{\mathcal{L}}$.

(iv) $\Rightarrow$ (iii) It suffices to show that any $m \in J$ can be represented as $m = m_1 + m_2$, where $m_1 \in \blacktriangle T$ and $m_2 \in \operatorname{Ker}\alpha$. Since $J^0 = p\overline{\mathcal{L}}$, one has $m - i_T(pl) \in \blacktriangle T$ for some $l \in \overline{\mathcal{L}}$. Furthermore, $\overline{\rho}(pl) \in \blacktriangle\overline{M}$, whence $i_T(pl) - m_2 \in \blacktriangle T$ for some $m_2 \in \operatorname{Ker}\alpha$. ■

If one of the equivalent conditions of Proposition 2.7 is satisfied, then $\overline{M}^\tau = \overline{M}$ and $\overline{\rho}^\tau = \overline{\rho}$.

Corollary 2.8 *Let $(\mathcal{L}', M', \rho'), (\mathcal{L}, M, \rho) \in \mathcal{CT}$ and (ψ, Ψ) is a morphism between them. If $M_\blacktriangle = M_0$, then $\blacktriangle$ is injective on $\overline{M}$ and $M/M_\blacktriangle \cong \overline{M}^\tau$.*

Proof If $m \in M$ and $\blacktriangle m \in M_0 = M_\blacktriangle$, then $\blacktriangle^h(\blacktriangle m) \in \operatorname{Im}\Psi$ for some $h \geq 0$. Thus, $m \in M_\blacktriangle = M_0$, as required. The last statement is clear. ■

Notice that for the multiplication by p in F_a, one has $M_0 = M$, $M_\blacktriangle = 0$, and $\blacktriangle$ is injective on $\overline{M}$, which shows that the conditions of Proposition 2.7 can be satisfied even if $M_\blacktriangle \neq M_0$. In addition, it provides an example where the reduction of the kernel is not isomorphic to the kernel of the reduction (*cf.* Corollary 3.7 and Corollary 4.4).

3 Formal Group Laws of Finite Height

A module $M \in \mathcal{C}$ or a triple $(\mathcal{L}, M, \rho) \in \mathcal{CT}$ are *of finite height* if M is torsion-free as $\mathcal{O}_K$-module. Correspondingly, a formal group law F over k or $\mathcal{O}_K$ has *finite height* if $M(F)$ is torsion-free as $\mathcal{O}_K$-module. A matrix $u \in \mathrm{M}_d(\mathcal{E})$ is of *finite height* if it satisfies one of the following equivalent conditions ([De, Proposition 10]).

(a) There exist $w \in \mathrm{M}_d(\mathcal{E})$ and an integer h such that $wu \equiv \blacktriangle^h I_d \mod p$.
(b) There exist $w \in \mathrm{M}_d(\mathcal{E})$ and an integer h such that $uw \equiv \blacktriangle^h I_d \mod p$.
(c) If $su \equiv 0 \mod p$ for $s \in \mathrm{M}_{e,d}(\mathcal{E})$, then $s \equiv 0 \mod p$.
(d) If $us \equiv 0 \mod p$ for $s \in \mathrm{M}_{d,e}(\mathcal{E})$, then $s \equiv 0 \mod p$.

Lemma 3.1 *A formal group law over $\mathcal{O}_K$ is of finite height if and only if its type is of finite height.*

Proof Let u be a type of a formal group law corresponding to the triple $(\mathcal{L}, M, \rho) \in \mathcal{CT}$. For a basis $l_1, \dots, l_d$ of $\mathcal{L}$ one has $u(\rho(l_1), \dots, \rho(l_d))^T = 0$. Let $m \in M$ and $pm = 0$. If $m = \sum_{i=1}^d t_i\rho(l_i)$, $t_1, \dots, t_d \in \mathcal{E}$, Honda theory implies that $p(t_1, \dots, t_d) = (s_1, \dots, s_d)u$ for some $s_1, \dots, s_d \in \mathcal{E}$. Since u is of finite height, one gets $s_i = p\widetilde{s}_i, 1 \leq i \leq d$. Thus $(t_1, \dots, t_d) = (\widetilde{s}_1, \dots, \widetilde{s}_d)u$, which gives $m = 0$.

Suppose M is torsion-free and $su \equiv 0 \mod p$ for $s \in \mathrm{M}_{e,d}(\mathcal{E})$. One can assume that $e = 1, s = (s_1, \dots, s_d)$ and $(s_1, \dots, s_d)u = p(t_1, \dots, t_d)$. Then $\sum_{i=1}^d t_i\rho(l_i) = 0$ which gives $(t_1, \dots, t_d) = (\widetilde{s}_1, \dots, \widetilde{s}_d)u$ for $\widetilde{s}_1, \dots, \widetilde{s}_d \in \mathcal{E}$. Thus $(s_1, \dots, s_d)u = p(\widetilde{s}_1, \dots, \widetilde{s}_d)u$, whence $(s_1, \dots, s_d) = p(\widetilde{s}_1, \dots, \widetilde{s}_d)$ as $u \in \mathrm{GL}_d(\mathcal{E} \otimes k)$. ■

Lemma 3.2 *For $(\mathcal{L}, M, \rho) \in \mathcal{CT}$ of finite height*

(i) *M/pM is a finite dimensional vector space over k;*

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

(ii) *there exists* $h > 0$ *such that* $\blacktriangle^h M \subset pM$.

Proof Let u be a type of a formal group law corresponding to $(\mathcal{L}, M, \rho)$. If $l_1, \dots, l_d$ is a basis of $\mathcal{L}$, then $u(\rho(l_1), \dots, \rho(l_d))^T = 0$. The type u is of finite height by Lemma 3.1; thus, there exist $w \in M_n(\mathcal{E})$ and an integer h such that $wu \equiv \blacktriangle^h I_n \mod p$. It yields $\blacktriangle^h(\rho(l_1), \dots, \rho(l_d))^T \in pM^d$, whence the set $\{\blacktriangle^j \rho(l_i)\}_{\substack{1\le i\le d \\ 0\le j\le h-1}}$ spans M/pM. ∎

Lemma 3.3 *For square matrices a and d, if a matrix $\left(\begin{smallmatrix} a & pb \\ c & d \end{smallmatrix}\right)$ is of finite height, then a and d are also of finite height.*

Proof If a is not of finite height then there exists a matrix $s \not\equiv 0 \mod p$ such that $sa \equiv 0 \mod p$. Then

$$(s \quad 0)\begin{pmatrix} a & pb \\ c & d \end{pmatrix} \equiv 0 \mod p,$$

a contradiction. A similar argument shows that d is also of finite height. ∎

Proposition 3.4 *Let F, G be d and e-dimensional formal group laws over $\mathcal{O}_K$, F be of finite height and $f \in \mathrm{Hom}(F, G)$. Then there are integers $0 \le s_1 < \cdots < s_k$, matrices $C_1 \in \mathrm{GL}_e(\mathcal{O}_K), C_2 \in \mathrm{GL}_d(\mathcal{O}_K)$ and a type $u = \{u_{ij}\}_{1\le i,j\le k+1}$ of the logarithm of F for $u_{ij} \in \mathrm{M}_{n_i,n_j}(\mathcal{O}_K)$ such that*

$$C_1 J(f) C_2 = \begin{pmatrix} p^{s_1} I_{n_1} & & & \\ & \ddots & & \\ & & p^{s_k} I_{n_k} & \\ & & & 0 \end{pmatrix}$$

and

(i) $u_{i,k+1} = 0$ *for* $1 \le i \le k$,
(ii) $u_{i,j} \equiv 0 \mod p^{s_j - s_i}$ *for* $1 \le i < j \le k$,
(iii) $u_{i,i}$ *is of finite height for* $1 \le i \le k+1$.

Proof Consider the corresponding situation in the category $\mathcal{CT}$. Let (ψ, Ψ) be a morphism from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$ and $(\mathcal{L}, M, \rho)$ be of finite height. In some bases of $\mathcal{L}'$ and $\mathcal{L}$ the matrix of ψ has Smith normal form

$$\begin{pmatrix} p^{s_1} I_{n_1} & & & \\ & \ddots & & \\ & & p^{s_k} I_{n_k} & \\ & & & 0 \end{pmatrix}$$

Let the lower-right zero submatrix belong to $\mathrm{M}_{n_{k+1},n'_{k+1}}(\mathcal{O}_K)$. For notation simplicity, put $n'_j = n_j$ for $1 \le j \le k$. Denote by ψ_n the $\mathcal{O}_K$-morphism from $\mathcal{L}'^n$ to $\mathcal{L}^n$ induced by ψ. Let $l'_j \in \mathcal{L}'^{n'_j}$, $1 \le j \le k+1$ and $l_j \in \mathcal{L}^{n_j}$, $1 \le j \le k+1$ be tuples of vectors whose components form the corresponding Smith normal bases in $\mathcal{L}'$ and $\mathcal{L}$ such that $\psi_{n_j}(l'_j) = p^{s_j} l_j$, $1 \le j \le k$, and $\psi_{n'_{k+1}}(l'_{k+1}) = 0$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

There are $a_{ij} \in \mathrm{M}_{n'_i,n'_j}(\mathcal{O}_K), 1 \le i \le k, 1 \le j \le k+1$ such that $\sum_{j=1}^{k+1} a_{ij}\rho'(l'_j) = 0$, $1 \le i \le k$, and

$$a_{ij} \equiv \begin{cases} 0 & \mod \blacktriangle \quad \text{if } i \ne j, \\ pI_{n_j} & \mod \blacktriangle \quad \text{if } i = j, \end{cases}$$

Then $\sum_{j=1}^{k} p^{s_j} a_{ij}\rho(l_j) = 0, 1 \le i \le k$. Since M is torsion-free, in particular we get $\sum_{j=1}^{k} p^{s_j - s_1} a_{1j}\rho(l_j) = 0$.

There are $b_{ij} \in \mathrm{M}_{n_i,n_j}(\mathcal{O}_K), 2 \le i \le k+1, 1 \le j \le k+1$ such that $\sum_{j=1}^{k+1} b_{ij}\rho(l_j) = 0$, $2 \le i \le k+1$, and

$$b_{ij} \equiv \begin{cases} 0 & \mod \blacktriangle \quad \text{if } i \ne j, \\ pI_{n_j} & \mod \blacktriangle \quad \text{if } i = j, \end{cases}$$

Then

$$\begin{pmatrix} a_{1,1} & p^{s_2-s_1}a_{1,2} & \cdots & p^{s_k-s_1}a_{1,k} & 0 \\ b_{2,1} & b_{2,2} & \cdots & b_{2,k} & b_{2,k+1} \\ \vdots & \vdots & & \vdots & \vdots \\ b_{k+1,1} & b_{k+1,2} & \cdots & b_{k+1,k} & b_{k+1,k+1} \end{pmatrix}$$

is a type of F and thus is of finite height by Lemma 3.1.

We show by induction on m that there exists a type $u^{(m)} = \{u_{ij}\}_{1 \le i, i \le k+1}$ of F such that $u_{i,k+1} = 0$ for $1 \le i \le m$ and $u_{i,j} \equiv 0 \mod p^{s_j - s_i}$ for $1 \le i \le m, i+1 \le j \le k$. The existence of $u^{(1)}$ is already proved. Suppose that $u^{(m)}$ exists. By Honda theory the equality $\sum_{j=1}^{k} p^{s_j} a_{m+1,j}\rho(l_j) = 0$ yields

$$\begin{pmatrix} p^{s_1}a_{m+1,1} & p^{s_2}a_{m+1,2} & \cdots & p^{s_k}a_{m+1,k} & 0 \end{pmatrix} = \begin{pmatrix} w_1 & w_2 & \cdots & w_{k+1} \end{pmatrix} u^{(m)}$$

for some $w_j \in \mathrm{M}_{n_j}(\mathcal{O}_K), 1 \le j \le k+1$.

Prove by induction on t that $w_t, \ldots, w_{k+1} \equiv 0 \mod p^{s_t}$ for $1 \le t \le m+1$. Suppose the assumption holds for all integers not exceeding the given $t \le m$. In particular, it implies that $w_i \equiv 0 \mod p^{s_i}$ for any $1 \le i \le t$. Then

$$\sum_{i=t+1}^{k+1} w_i u_{ij} = p^{s_j} a_{m+1,j} - \sum_{i=1}^{t} w_i u_{ij} \equiv 0 \mod p^{s_{t+1}}$$

for $t+1 \le j \le k+1$. Since $\{u_{ij}\}_{\substack{1 \le i \le t \\ t+1 \le j \le k+1}} \equiv 0 \mod p$, Lemma 3.3 implies that $\{u_{ij}\}_{t+1 \le i,j \le k+1}$ is of finite height, therefore the congruence

$$\{w_i\}_{t+1 \le i \le k+1} \{u_{ij}\}_{t+1 \le i,j \le k+1} \equiv 0 \mod p^{s_{t+1}}$$

yields $w_i \equiv 0 \mod p^{s_{t+1}}$, $t+1 \le i \le k+1$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Now, if $w_i = p^{s_i}\widehat{w}_i$ for $1 \le i \le m$, $w_i = p^{s_{m+1}}\widehat{w}_i$ for $m+1 \le i \le k+1$ and $u_{ij} = p^{s_j - s_i}\widehat{u}_{ij}$ for $1 \le i \le m$, $i+1 \le j \le k$, one gets

$$\begin{aligned}
0 &= \sum_{j=1}^{k} p^{s_j} a_{m+1,j}\rho(l_j) = \sum_{j=1}^{m} p^{s_j} a_{m+1,j}\rho(l_j) + \sum_{j=m+1}^{k} p^{s_j} a_{m+1,j}\rho(l_j) \\
&= \sum_{j=1}^{m}\sum_{i=1}^{k+1} w_i u_{ij}\rho(l_j) + \sum_{j=m+1}^{k} p^{s_j} a_{m+1,j}\rho(l_j) \\
&= \sum_{i=1}^{m} w_i \sum_{i=1}^{m} u_{ij}\rho(l_j) + \sum_{i=m+1}^{k+1} w_i \sum_{j=1}^{m} u_{ij}\rho(l_j) + \sum_{j=m+1}^{k} p^{s_j} a_{m+1,j}\rho(l_j) \\
&= -\sum_{i=1}^{m} w_i \sum_{j=m+1}^{k} u_{ij}\rho(l_j) + \sum_{i=m+1}^{k+1} w_i \sum_{j=1}^{m} u_{ij}\rho(l_j) + \sum_{j=m+1}^{k} p^{s_j} a_{m+1,j}\rho(l_j).
\end{aligned}$$

Dividing by $p^{s_{m+1}}$, we obtain

$$-\sum_{i=1}^{m}\sum_{j=m+1}^{k} p^{s_j - s_{m+1}}\widehat{w}_i\widehat{u}_{ij}\rho(l_j) + \sum_{i=m+1}^{k+1}\widehat{w}_i\sum_{j=1}^{m} u_{ij}\rho(l_j) + \sum_{j=m+1}^{k} p^{s_j - s_{m+1}} a_{m+1,j}\rho(l_j) = 0.$$

Since $\widehat{u}_{ij} \equiv 0 \mod \blacktriangle$, all the coefficients here other than $a_{m+1,m+1}$ are congruent to 0 modulo $\blacktriangle$. Thus, one can replace the $(m+1)$-th line of $u^{(m)}$ with these coefficients. It remains to observe that the coefficient at $\rho(l_{k+1})$ equals 0 and the coefficients at $\rho(l_j)$ are congruent to 0 modulo $p^{s_j - s_{m+1}}$ for $m+2 \le j \le k$. ∎

Denote $M_p = \{m \in M : am = \Psi(m') \text{ for some } a \in \mathcal{O}_K, a \ne 0 \text{ and } m' \in M'\}$.

Proposition 3.5 *Let (ψ, Ψ) be a morphism from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$ in the category $\mathcal{CT}$.*

(i) *If $(\mathcal{L}, M, \rho)$ has finite height, then $p\rho(\mathcal{L}_0) \subset \blacktriangle M_0$;*
(ii) *If both $(\mathcal{L}, M, \rho)$ and $(\mathcal{L}', M', \rho')$ have finite height then $M_\blacktriangle = M_0 = M_p$.*

Proof (i) Apply Proposition 3.4. It suffices to notice that $\mathcal{L}_0$ equals to the span of the components of $l_0, \dots, l_k$.

(ii) Since $\mathcal{L}$ is of finite rank, there is an element $a \in \mathcal{O}_K$, $a \ne 0$ such that $a\mathcal{L}_0 \subset \operatorname{Im}\psi$. Then $aM_0 \subset \operatorname{Im}\Psi$, which implies $M_0 \subset M_p$.

Now let $m \in M_p$, *i.e.*, $am = \Psi(m')$ for some $a \in \mathcal{O}_K$, $a \ne 0$ and $m' \in M'$. According to Lemma 3.2 there is $h \ge 0$ and $m'' \in M'$ such that $\blacktriangle^h m' = am''$. It implies $\blacktriangle^h m = (a/a^{\Delta^h})\Psi(m'') \in \operatorname{Im}\Psi$, and thus $M_p \subset M_\blacktriangle$.

Finally, $\blacktriangle$ is injective on $\overline{M}$ by Proposition 2.7. So if $m \in M_\blacktriangle$, *i.e.*, $\blacktriangle^h m \in \operatorname{Im}\Psi \subset M_0$ for some $h \ge 0$, then $m \in M_0$. Thus, $M_\blacktriangle \subset M_0$, and we are done. ∎

Corollary 3.6 *If (ψ, Ψ) is a morphism in $\mathcal{CT}$ from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$ and $(\mathcal{L}, M, \rho)$ is of finite height, then $(\overline{\mathcal{L}}, \overline{M}, \overline{\rho})$ along with $(\operatorname{red}_{\mathcal{L}_0}, \operatorname{red}_{M_0})$ is a cokernel of (ψ, Ψ).*

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Proof The proof follows from Theorem 2.5 and Proposition 2.7. ∎

Corollary 3.7 *In the category of formal group laws of finite height, kernel commutes with the reduction modulo p.*

Proof This follows from Corollary 2.8. ∎

Corollary 3.8 *A kernel of a homomorphism between formal group laws of finite height is also of finite height.*

Proof Remark that $\overline{M} = M/M_0 = M/M_p$ is torsion-free. ∎

4 Pure Homomorphisms

Lemma 4.1 *For $D \in \mathrm{M}_{e,d}(\mathcal{O}_K)$ the following conditions are equivalent:*

(i) $\mathrm{rk}_K D = \mathrm{rk}_k(D \otimes k)$;

(ii) *If $x \in \mathcal{O}_K^d$, $y \in \mathcal{O}_K^e$ satisfy the equality $Dx = py$, then there exists $x' \in \mathcal{O}_K^d$ such that $Dx' = y$;*

(iii) *If $x \in \mathcal{O}_K^e$, $y \in \mathcal{O}_K^d$ satisfy the equality $xD = py$, then there exists $x' \in \mathcal{O}_K^e$ such that $x'D = y$;*

(iv) *There exist $0 \le r \le \min(e,d)$ and $Q \in \mathrm{GL}_d(\mathcal{O}_K)$ such that $DQ = (D' \quad 0)$, where $D' \in \mathrm{M}_{e,r}(\mathcal{O}_K)$ and $CD' = I_r$ for some $C \in \mathrm{M}_{r,e}(\mathcal{O}_K)$;*

(v) *There exist $0 \le r \le \min(e,d)$ and $Q \in \mathrm{GL}_e(\mathcal{O}_K)$ such that $QD = \binom{D'}{0}$, where $D' \in \mathrm{M}_{r,d}(\mathcal{O}_K)$ and $D'C = I_r$ for some $C \in \mathrm{M}_{d,r}(\mathcal{O}_K)$.*

Proof The matrix D has the Smith normal form, *i.e.,* there are invertible matrices C_1 and C_2 such that

$$C_1 D C_2 = \begin{pmatrix} p_1 & 0 & & \cdots & & 0 \\ 0 & \ddots & & & & 0 \\ & & p_r & & & \\ \vdots & & & 0 & & \vdots \\ & & & & \ddots & \\ 0 & 0 & & \cdots & & 0 \end{pmatrix},$$

where $p_1, \dots, p_r$ are non-decreasing p-powers. It is easy to see that all the conditions of the lemma are equivalent to the fact that $p_1 = \cdots = p_r = 1$. ∎

Let $\psi\colon \mathcal{L}_1 \to \mathcal{L}_2$ be a homomorphism of free $\mathcal{O}_K$-modules of finite rank. Then the p-divisible closure of $\mathrm{Im}\,\psi$ in $\mathcal{L}_2$ coincides with $\mathrm{Im}\,\psi$ (*i.e.,* if $al_2 \in \mathrm{Im}\,\psi$ for some $a \in \mathcal{O}_K$, $a \neq 0$, and $l_2 \in \mathcal{L}_2$, then $l_2 \in \mathrm{Im}\,\psi$) if and only if the matrix of ψ in some (and therefore in any) free $\mathcal{O}_K$-bases of $\mathcal{L}_1$ and $\mathcal{L}_2$ satisfies the equivalent conditions of Lemma 4.1. In this case, we say that ψ is *pure*.

A homomorphism of formal groups laws over $\mathcal{O}_K$ is called *pure*, if its Jacobian matrix satisfies the equivalent conditions of Lemma 4.1. A morphism (ψ, Ψ) in the category $\mathcal{CT}$ is called *pure*, if ψ is pure. Clearly, the notions of purity in $\mathcal{FG}(k)$ and $\mathcal{CT}$ agree in the sense of Fontaine's correspondence.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Proposition 4.2 *If (ψ, Ψ) is a pure morphism in the category $\mathcal{CT}$ from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$, then $p\rho(\mathcal{L}_0) \subset \blacktriangle M_0$ and $M_\blacktriangle = M_0$.*

Proof Since $\mathcal{L}_0 = \operatorname{Im}\psi$ we have $M_0 = \operatorname{Im}\Psi$, and hence $M_0 \subset M_\blacktriangle$. In order to show that $p\rho(\mathcal{L}_0) \subset \blacktriangle M_0$ let $l \in \mathcal{L}_0$, *i.e.*, $l = \psi(l')$ for some $l' \in \mathcal{L}'$. Then $p\rho'(l') = \sum_{k\geq 1} \blacktriangle^k \rho'(l'_k)$, $l'_k \in \mathcal{L}'$. It yields

$$p\rho(l) = p\rho \circ \psi(l') = \Psi(p\rho'(l')) = \sum_{k\geq 1} \blacktriangle^k \Psi \circ \rho'(l'_k) = \sum_{k\geq 1} \blacktriangle^k \rho(\psi(l'_k)) \in \blacktriangle M_0.$$

Now Proposition 2.7 implies that $\blacktriangle$ is injective on $\overline{M}$. Finally, if $m \in M_\blacktriangle$, *i.e.*, $\blacktriangle^h m \in \operatorname{Im}\Psi = M_0$ for some $h \geq 0$, then $m \in M_0$. Thus, $M_\blacktriangle \subset M_0$. ∎

sloppy Notice that for a pure morphism (ψ, Ψ), M_p may or may not coincide with $M_\blacktriangle = M_0$. Indeed, for the zero endomorphism of the additive formal group law, $M_\blacktriangle = M_0 = 0$ holds, whereas $M_p = M$ (*cf.* Proposition 3.5).

Corollary 4.3 *If (ψ, Ψ) is a pure morphism in $\mathcal{CT}$ from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$, then $(\overline{\mathcal{L}}, \overline{M}, \overline{\rho})$ along with $(\operatorname{red}_{\mathcal{L}_0}, \operatorname{red}_{M_0})$ is a cokernel of (ψ, Ψ).*

Proof This follows from Theorem 2.5 and Proposition 2.7. ∎

Corollary 4.4 *For a pure homomorphism in $\mathcal{FG}(\mathcal{O}_K)$, kernel commutes with the reduction modulo p.*

Proof This follows from Corollary 2.8. ∎

Proposition 4.5 *Let F, G be d- and e-dimensional formal group laws over $\mathcal{O}_K$, the logarithm of F be of type u and $f \in \operatorname{Hom}(F, G)$. Suppose that f is pure. In particular, there exists $Q \in \mathrm{GL}_d(\mathcal{O}_K)$ such that $J(f)Q = (D' \quad 0)$, where $D' \in \mathrm{M}_{e,r}(\mathcal{O}_K)$ and $CD' = I_r$ for some $C \in \mathrm{M}_{r,e}(\mathcal{O}_K)$. Then there is a kernel of f represented by a $(d-r)$-dimensional formal group law H and $h \in \operatorname{Hom}(H, F)$ such that the logarithm of H is of type equal to the lower-right $(d-r) \times (d-r)$-submatrix of $Q^{-1}uQ$ and $J(h) = Q(0 \quad I_{d-r})^T$.*

Proof Consider the formal group law $F'(X, Y) = Q^{-1}F(QX, QY)$ with the logarithm of type $u' = Q^{-1}uQ$ and the homomorphism $f'(X) = f(QX) \in \operatorname{Hom}(F', G)$ with $J(f') = J(f)Q$. Then $\mathcal{H}(F') = (\mathcal{O}_K^d, \mathcal{E}^d/\mathcal{E}^d u', \kappa)$. The first component of $\mathcal{H}(f')$ is the mapping $\psi\colon \mathcal{O}_K^e \to \mathcal{O}_K^d$, $\psi(m) = mJ(f')$ for which, in the case under consideration, $\operatorname{Im}\psi$ is the subset of the elements of $\mathcal{O}_K^d$ with the last $d-r$ coordinates equal to 0. Indeed, for any $m \in \mathcal{O}_K^e$, we have $\psi(m) = mJ(f)Q = (mD' \quad 0)$, and for any $y \in \mathcal{O}_K^r$, we get $\psi(yC) = (yCD' \quad 0) = (y \quad 0)$. Since ψ is pure, $\mathcal{L}_0 = \operatorname{Im}\psi$ and hence $M_0 = \langle\kappa(\operatorname{Im}\psi)\rangle$. Thus, by Corollary 4.3, the triple $(\mathcal{O}_K^d/\operatorname{Im}\psi, (\mathcal{E}^d/\mathcal{E}^d u')/\langle\kappa(\operatorname{Im}\psi)\rangle, \widehat{\kappa})$ gives a kernel of f', where $\widehat{\kappa}$ is induced from κ by factoring modulo $\operatorname{Im}\psi$. It corresponds to a formal group law H with the logarithm of the required type and a homomorphism $h' \in \operatorname{Hom}(H, F')$ with $J(h') = (0 \quad I_{d-r})^T$. A kernel of f can be given by H and $h = Qh'$, and we are done. ∎

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Let a group $\mathcal{G}$ act on a formal group law F, *i.e.,* there is a fixed homomorphism $\mathcal{G} \to \mathrm{Aut}_{\mathcal{O}_K}(F)$. We say that (H, h) is a universal fixed pair for $(F, \mathcal{G})$ if H is a formal group law over $\mathcal{O}_K$, $h \in \mathrm{Hom}(H, F)$ is such that $\sigma \circ f = f$ for any $\sigma \in \mathcal{G}$, and for any pair (H', h') satisfying the above properties, there exists a unique $g \in \mathrm{Hom}(H', H)$ such that $h' = h \circ g$.

Corollary *Let F be a d-dimensional formal group law over $\mathcal{O}_K$ provided with an action of a finite group $\mathcal{G}$. Suppose that there exists $0 \le r \le d$ and $Q \in \mathrm{GL}_d(\mathcal{O}_K)$ such that for any $\sigma \in \mathcal{G}$ one has $J(\sigma)Q = (D'_\sigma \quad 0)$, where $D'_\sigma \in M_{d,r}(\mathcal{O}_K)$ and $\sum_{\sigma\in\mathcal{G}} C_\sigma D'_\sigma = I_r$ for some $C_\sigma \in M_{r,d}(\mathcal{O}_K)$. Then there exists a universal fixed pair (H, h) for $(F, \mathcal{G})$ such that a type of the logarithm of H equals the lower-right $(d-r)\times(d-r)$-submatrix of $Q^{-1}uQ$ and $J(h) = Q(0 \quad I_{d-r})^T$, where u is a type of the logarithm of F.*

Proof Let $\mathcal{G} = \{\sigma^{(1)}, \dots, \sigma^{(m)}\}$ and let G be the direct sum of m copies of F. For $f = (\sigma^{(1)}, \dots, \sigma^{(m)}) \in \mathrm{Hom}(F, G)$ one has

$$J(f) = \begin{pmatrix} J(\sigma^{(1)}) \\ \vdots \\ J(\sigma^{(m)}) \end{pmatrix}.$$

Then $J(f)Q = (D' \quad 0)$ and $CD' = I_r$ for

$$D' = \begin{pmatrix} D'_{\sigma^{(1)}} \\ \vdots \\ D'_{\sigma^{(m)}} \end{pmatrix}$$

and $C = (C_{\sigma^{(1)}} \cdots C_{\sigma^{(m)}})$. According to Proposition 4.5 there exists a kernel (H, h) of f that satisfies the required conditions. Clearly, (H, h) is a universal fixed pair for $(F, \mathcal{G})$. ∎

The above corollary is essentially [DGX, Theorem 3.5].

Let F, G be formal group laws over $\mathcal{O}_K$. A homomorphism $f \in \mathrm{Hom}(F, G)$ is a *strong monomorphism* if for any $N \in \mathcal{N}il_{\mathcal{O}_K}$, the morphism $f(N)\colon F(N) \to G(N)$ is a monomorphism.

A pair (H, h), where $H \in \mathcal{FG}(\mathcal{O}_K)$, $h \in \mathrm{Hom}(H, F)$, is called a *strong kernel* of f if for any $N \in \mathcal{N}il_{\mathcal{O}_K}$ the homomorphism $h(N)$ is injective and the subgroup $h(N)(H(N))$ of $F(N)$ coincides with the kernel of $f(N)$. The Yoneda lemma implies that any strong kernel is a kernel and, therefore, any strong monomorphism is a monomorphism.

Proposition 4.6 *Let $F, G \in \mathcal{FG}(\mathcal{O}_K)$ and let $f \in \mathrm{Hom}(F, G)$. If f is pure, then any kernel of f is strong.*

Proof Let $Q \in \mathrm{GL}_d(\mathcal{O}_K)$ be such that $J(f)Q = (D' \quad 0)$ where $D' \in \mathrm{M}_{e,r}(\mathcal{O}_K)$ and $CD' = I_r$ for some $C \in \mathrm{M}_{r,e}(\mathcal{O}_K)$. Consider $F'(X, Y) = Q^{-1}F(QX, QY)$ and $f'(X) = f(QX)$. Then $f' \in \mathrm{Hom}(F', G)$, $J(f') = (D' \quad 0)$ and Proposition 4.5 implies that there is a kernel of f' represented by a $(d-r)$-dimensional formal group law H' and $h' \in \mathrm{Hom}(H', F')$ such that $J(h') = (0 \quad I_{d-r})^T$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Now it suffices to prove that this kernel is strong. Obviously, $h'(N)$ is injective for $N \in \mathcal{N}il_{\mathcal{O}_K}$. Pick any $\alpha \in N^r, \beta \in N^{d-r}$ satisfying $f'(\alpha, \beta) = 0$. Let $h' = (h_1, h_2)$ for $h_1 \in \mathcal{O}_K[[x_1, \dots, x_{d-r}]]^r, h_2 \in \mathcal{O}_K[[x_1, \dots, x_{d-r}]]^{d-r}$. Then $J(h_2) = I_{d-r}$, and therefore one can find $\gamma \in N^{d-r}$ such that $h_2(\gamma) = \beta$.

Denote $\psi(Z) = Cf'(Z, \beta)$ for $Z = (z_1, \dots, z_r)$. Then $J(\psi) = I_r$ and ψ is invertible. The equality $\psi(\alpha) = Cf'(\alpha, \beta) = 0 = Cf'(h_1(\gamma), h_2(\gamma)) = \psi(h_1(\gamma))$ gives $\alpha = 0 = h_1(\gamma)$, as required. ∎

We complete this section with necessary and sufficient conditions on a homomorphism in $\mathcal{FG}(\mathcal{O}_K)$, which guarantees that it is a (strong) monomorphism.

Let D be an $m \times n$-matrix with entries in a ring A. By abuse of notation, $\operatorname{Ker} D$ stands for the sub-A-module of A^n given by all $a = (a_1, \dots, a_n) \in A^n$ such that $Da^T = 0$.

Proposition 4.7 *Let $F, G \in \mathcal{FG}(\mathcal{O}_K)$, $f \in \operatorname{Hom}(F, G)$, and $D = J(f) \in \mathrm{M}_{e,d}(\mathcal{O}_K)$. Then*

(i) *f is a monomorphism if and only if $\operatorname{Ker} D = \{0\}$;*
(ii) *f is a strong monomorphism if and only if $\operatorname{Ker}(D \otimes k) = \{0\}$.*

Proof (i) This follows from Corollary 2.6.

(ii) First, suppose that f is a strong monomorphism. Consider k as an $\mathcal{O}_K$-algebra with zero multiplication and scalar multiplication induced by the reduction map. Then $F(k) = k^d$, $G(k) = k^e$ and $f(k)$ is a multiplication by $D \otimes k$. Since $f(k)$ is a monomorphism, $\operatorname{Ker}(D \otimes k) = \{0\}$.

Conversely, suppose that $\operatorname{Ker}(D \otimes k) = \{0\}$. Then $\operatorname{Ker} D = \{0\}$ and the zero homomorphism gives a kernel of f. Since $\operatorname{rk}_{\mathcal{O}_K} \operatorname{Ker} D = \dim_k \operatorname{Ker}(D \otimes k) = 0$, this kernel is strong by Proposition 4.6. It shows that f is a strong monomorphism. ∎

5 Formal Group Laws Coming From Tori

We present some applications of the above results to formal group law homomorphisms associated with homomorphisms of algebraic tori.

Let B be an algebra over a ring A and $e_1, \dots, e_n$ be a free basis of B as an A-module. For a one-dimensional formal group law F over B, the *Weil restriction* with respect to B/A and $e_1, \dots, e_n$ is defined as an n-dimensional formal group law $R = (R_1, \dots, R_n)$ over A such that $\sum_{i=1}^n R_i e_i = F(\sum_{i=1}^n x_i e_i, \sum_{i=1}^n y_i e_i)$. Similarly, the Weil restriction of a d-dimensional formal group law can be defined (see [DGX, Section 4] for details).

Local Norm Homomorphism

Let L/K be a finite extension and let $e_1, \dots, e_n$ be a free $\mathcal{O}_K$-basis of $\mathcal{O}_L$. Let R denote the Weil restriction of F_m with respect to $\mathcal{O}_L/\mathcal{O}_K$ and $e_1, \dots, e_n$. Put $P(X) = \mathcal{N}_{L/K}(1 + \sum_{i=1}^n x_i e_i) - 1$, where $\mathcal{N}_{L/K}$ stands for the norm map. Then $P \in \operatorname{Hom}_{\mathcal{O}_K}(R, F_m)$.

Proposition 5.1 *If L/K is tamely ramified, then P is pure.*

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Proof We have $P(X) \equiv \sum_{i=1}^{n} (\mathrm{tr}_{L/K} e_i) x_i \mod \deg 2$. If all the entries of $J(P)$ are divisible by p, then $\mathrm{tr}_{L/K} \mathcal{O}_L \subset p\mathcal{O}_K$, which is impossible, since L/K is tamely ramified. ∎

Let (H, h) denote a kernel of P.

Corollary *If L/K is tamely ramified, then* $\mathrm{Im}\, h(N) = \mathrm{Ker}\, P(N)$ *for any nilpotent $\mathcal{O}_K$-algebra N.*

Proof This follows from Proposition 4.6. ∎

This corollary can be interpreted as a consequence of a result on an integer model for the Weil restriction of the multiplicative group scheme with respect to a tamely ramified extension. Indeed, R can be identified with the formal completion of

$$\mathcal{W} = \mathrm{Sp}_{\mathcal{O}_K} \mathcal{O}_K[x_0, x_1, \dots, x_n]/x_0 \mathcal{N}_{L/K}\Big(1 + \sum_{i=1}^{n} x_i e_i\Big) - 1.$$

Further, if L/K is tamely ramified, $\mathcal{T} = \mathrm{Sp}_{\mathcal{O}_K} \mathcal{O}_K[X]/P(X)$ is smooth. Denote by H' its formal completion, and by h' the completion of the morphism $\iota\colon \mathcal{T} \to \mathcal{W}$, which is the kernel of the norm map from $\mathcal{W}$ to the multiplicative group scheme over $\mathcal{O}_K$. Since $\mathcal{T}$ is affine, for any nilpotent $\mathcal{O}_K$-algebra N, one has $\mathrm{Im}\, h'(N) = \mathrm{Im}\, \iota(N) = \mathrm{Ker}\, P(N)$, and hence (H', h') is also a kernel of P. This implies the required statement.

We proceed with the computation of Honda's type of H in three special cases. The base field $K = \mathbb{Q}_p$.

I. *Unramified case.*

Let L be an unramified extension of $\mathbb{Q}_p$ of degree n. According to the normal basis theorem, there is $\bar{\zeta} \in \mathbb{F}_{p^n}$ such that

$$\bar{\zeta}, \bar{\zeta}^p, \dots, \bar{\zeta}^{p^{n-1}}$$

are linearly independent over $\mathbb{F}_p$. If $\zeta \in \mathcal{O}_L$ is the Teichmüller representative of $\bar{\zeta}$, then $\delta = \mathrm{tr}_{L/\mathbb{Q}_p} \zeta = \zeta + \zeta^p + \dots + \zeta^{p^{n-1}} \in \mathbb{Z}_p^*$. Put $e_i = \zeta^{p^{i-1}}$.

The logarithm of R is of type $pI_n - V\blacktriangle$, where $V = \{v_{i,j}\}_{1 \le i,j \le n}$, $v_{i,j} = 1$ if $j = i - 1$ or $j = i + n - 1$ and $v_{i,j} = 0$ otherwise ([DGX, Proposition 7.2]), and the Jacobian matrix $J(P) = (\delta, \dots, \delta)$. Take $Q = \{q_{i,j}\}_{1 \le i,j \le n}$ with $q_{i,j} = 1$ if $j = i$, $q_{i,j} = -1$ if $i = 1$, $j > 1$, and $q_{i,j} = 0$ otherwise. Then $Q^{-1} = \{q'_{i,j}\}_{1 \le i,j \le n}$, where $q'_{i,j} = 1$ if $j = i$ or $i = 1$, and $q'_{i,j} = 0$ otherwise:

$$Q = \begin{pmatrix} 1 & -1 & -1 & \cdots & -1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad Q^{-1} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Proposition 4.5 implies that there is a kernel (H, h) of P such that the logarithm of H is of type $pI_{n-1} - S\blacktriangle$, where $S = \{s_{i,j}\}_{1 \le i,j \le n-1}$, $s_{i,j} = 1$ if $j = i - 1$, $s_{i,j} = -1$ if $i = 1$,

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

and $s_{i,j} = 0$ otherwise, and $J(h) = \widetilde{Q} = \{\widetilde{q}_{i,j}\}_{1\le i\le n, 1\le j\le n-1}$, where $\widetilde{q}_{i,j} = 1$ if $j = i-1$, $\widetilde{q}_{i,j} = -1$ if $i = 1$, $\widetilde{q}_{i,j} = 0$ otherwise:

$$S = \begin{pmatrix} -1 & -1 & -1 & \cdots & -1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \widetilde{Q} = \begin{pmatrix} -1 & -1 & \cdots & -1 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

II. *Totally ramified case of degree less than p.*

Let L be a totally ramified extension of $\mathbb{Q}_p$ of degree $n \le p-1$. One can choose a uniformizer $t \in \mathcal{O}_L$ such that $t^n + a = 0$, where $a \in \mathbb{Z}_p$, $v_p(a) = 1$. Put $e_i = t^{i-1}, 1 \le i \le n$. The logarithm of R is of type $pI_n - V\blacktriangle$, where $V = \{v_{i,j}\}_{1\le i,j\le n}$, $v_{i,j} = 1$ if $j = i = 1$, and $v_{i,j} = 0$ otherwise ([DGX, Proposition 7.2]), and the Jacobian matrix $J(P) = (n, 0, \ldots, 0)$. Proposition 4.5 implies ($Q = I_n$) that there is a kernel (H, h) of P such that the logarithm of H is of type pI_{n-1} and $J(h) = (0 \quad I_{n-1})^T$. This means that H is isomorphic to the direct sum of $n-1$ copies of F_a.

III. *Totally ramified case of degree equal to p.*

Let L be a totally ramified extension of $\mathbb{Q}_p$ of degree p. One can choose a uniformizer $t \in \mathcal{O}_L$ such that $t^p + a_1 t^{p-1} + \cdots + a_p = 0$, where $a_i \in \mathbb{Z}_p$, $v_p(a_i) \ge 1$ for any $1 \le i \le p$ and $v_p(a_p) = 1$. Put $e_i = t^{i-1}, 1 \le i \le p$.

Denote by $\Lambda = (\Lambda_0, \ldots, \Lambda_{p-1})$ the logarithm of R. Then $\log(1 + \sum_{i=0}^{p-1} x_i t^i) = \sum_{i=0}^{p-1} \Lambda_i t^i$ ([DGX, Proposition 4.3]). Our first purpose is to calculate Honda's type of Λ.

For any $\alpha \in \mathcal{O}_L$ there are $\{\alpha\}_0, \ldots, \{\alpha\}_{p-1} \in \mathbb{Z}_p$ such that $\alpha = \sum_{j=0}^{p-1} \{\alpha\}_j t^j$. Similarly, for any $\lambda \in \mathcal{O}_L[[x]]$ there are $\{\lambda\}_0, \ldots, \{\lambda\}_{p-1} \in \mathbb{Z}_p[[x]]$ such that $\lambda = \sum_{j=0}^{p-1} \{\lambda\}_j t^j$.

Lemma 5.2 *$v_p(\{t^n\}_j) \ge [\frac{n+p-1-j}{p}]$ for any $0 \le j \le p-1, n \ge 0$.*

Proof The proof is by induction on n. If $n \le p-1$, then $\{t^n\}_j = 0$ for $n \ne j$ and $\{t^n\}_j = 1$ for $n = j$. In both cases the inequality in question is evident. If $n \ge p$, then $\sum_{i=0}^{p-1} \{t^n\}_j t^j = (-\sum_{i=0}^{p-1} a_{p-i} t^i) \sum_{k=0}^{p-1} \{t^{n-p}\}_k t^k$ yields

$$\begin{aligned} \{t^n\}_j &= -\sum_{i,k=0}^{p-1} a_{p-i} \{t^{n-p}\}_k \{t^{i+k}\}_j \\ &= -\sum_{i+k=j} a_{p-i} \{t^{n-p}\}_k - \sum_{i+k\ge p} a_{p-i} \{t^{n-p}\}_k \{t^{i+k}\}_j. \end{aligned}$$

The induction assumption implies that $v_p(\{t^{n-p}\}_k) \ge [\frac{n-1-k}{p}] \ge [\frac{n-1-j}{p}]$ for $i + k = j$ and $v_p(\{t^{n-p}\}_k \{t^{i+k}\}_j) \ge [\frac{n-1-k}{p}] + 1 \ge [\frac{n-1-j}{p}]$ for $i + k \ge p$. ■

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Proposition 5.3 *If $p \neq 2$, then Λ is of type*

$$u = \begin{pmatrix} p - \blacktriangle & -z\blacktriangle^2 & 0 & \cdots & 0 \\ 0 & p & 0 & \cdots & 0 \\ 0 & 0 & p & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p \end{pmatrix},$$

where $z = \frac{a_p}{p}(1 - \frac{a_{p-1}}{p}\blacktriangle)^{-1}$.

Proof According to the formula for Λ mentioned above, we have

$$\Lambda_j = \sum_{\substack{n_0+\cdots+n_{p-1}=p^k \\ k\geq 0}} \frac{1}{p^k}\binom{p^k}{n_0 \cdots n_{p-1}} \{t^{n_1+2n_2+\cdots+(p-1)n_{p-1}}\}_j x_0^{n_0} \cdots x_{p-1}^{n_{p-1}}.$$

We make use of an estimate for p-valuation of multinomial coefficients (Lemma 1.4 of [De])

$$v_p\left(\binom{p^k}{n_0 \ \cdots \ n_{p-1}}\right) \geq k - \min_{0\leq i\leq p-1} v_p(n_i).$$

Consider the summand

$$\frac{1}{p^k}\binom{p^k}{n_0 \ \cdots \ n_{p-1}} \{t^{n_1+2n_2+\cdots(p-1)n_{p-1}}\}_j x_0^{n_0} \cdots x_{p-1}^{n_{p-1}}$$

for any p-tuple $(n_0, \ldots, n_{p-1})$ other than $(p^k, 0, \ldots, 0)$. The inequality

$$v_p\left(\frac{1}{p^k}\binom{p^k}{n_0 \ \cdots \ n_{p-1}} \{t^{n_1+2n_2+\cdots(p-1)n_{p-1}}\}_j\right) \geq$$
$$- \min_{0\leq i\leq p-1} v_p(n_i) + \left[\frac{n_1 + 2n_2 + \cdots + (p-1)n_{p-1} + p - 1 - j}{p}\right]$$

shows that its coefficient is p-integer, since $v_p(n) \leq [\frac{n}{p}]$ for any $n \geq 1$. In particular, it gives $p\Lambda_j \equiv 0 \mod p, 1 \leq j \leq p-1$, *i.e.*, $p\Lambda_j \in p\mathbb{Z}_p[[x_0, \ldots, x_{p-1}]]_0$.

If $j = 0$, then

$$\left[\frac{n_1 + 2n_2 + \cdots + (p-1)n_{p-1} - 1}{p}\right] \geq \min v_p(n_i)$$

unless $(n_0, \ldots, n_{p-1}) = (p^k - p, p, 0 \ldots, 0)$.

If $j = 1$, then

$$\left[\frac{n_1 + 2n_2 + \cdots + (p-1)n_{p-1} - 2}{p}\right] \geq \min v_p(n_i)$$

unless $(n_0, \ldots, n_{p-1}) = (p^k - p, p, 0, \ldots, 0)$ or $(p^k - 1, 1, 0, \ldots, 0)$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Therefore, one has

$$\begin{aligned}\Lambda_0 &\equiv \sum_{k\geq 0}\frac{1}{p^k}x_0^{p^k}+\sum_{k\geq 1}\frac{1}{p^k}\binom{p^k}{p}\{t^p\}_0 x^{p^k-p}x_1^p\\ &\equiv \sum_{k\geq 0}\frac{1}{p^k}x_0^{p^k}-\frac{a_p}{p}\sum_{k\geq 1}x^{p^k-p}x_1^p \mod p\end{aligned}$$

and

$$\begin{aligned}\Lambda_1 &\equiv \sum_{k\geq 0}x_0^{p^k-1}x_1+\sum_{k\geq 1}\frac{1}{p^k}\binom{p^k}{p}\{t^p\}_1 x^{p^k-p}x_1^p\\ &\equiv \sum_{k\geq 0}x_0^{p^k-1}x_1-\frac{a_{p-1}}{p}\sum_{k\geq 1}x^{p^k-p}x_1^p \mod p.\end{aligned}$$

In both congruences, the fact that $\binom{p^k}{p}\equiv p^{k-1} \mod p^k$ is used. Denote

$$l=\sum_{k\geq 0}x_0^{p^k-1}x_1.$$

Then $\Lambda_1\equiv l-\frac{a_{p-1}}{p}\blacktriangle l \mod p$ whence $l\equiv(1-\frac{a_{p-1}}{p})^{-1}\Lambda_1 \mod p$. On the other hand,

$$\Lambda_0\equiv\sum_{k\geq 0}\frac{1}{p^k}x_0^{p^k}-\frac{a_p}{p}\blacktriangle l \mod p,$$

which results in

$$(p-\blacktriangle)\Lambda_0\equiv-\frac{a_p}{p}(p-\blacktriangle)\blacktriangle l\equiv\frac{a_p}{p}\blacktriangle^2 l\equiv\frac{a_p}{p}\Big(1-\frac{a_{p-1}}{\blacktriangle}\Big)^{-1}\blacktriangle^2\Lambda_1 \mod p,$$

as required. ■

The Jacobian matrix $J(P)=(p,-pb_1,\ldots,-pb_{p-1})$ for $b_i=-p^{-1}\operatorname{tr}_{L/\mathbb{Q}_p}t^i$, $1\leq i\leq p-1$. According to Newton's identities, the numbers $b_1,\ldots,b_{p-1}$ satisfy the following recurrent relations: $b_1=p^{-1}a_1$, $b_i=ip^{-1}a_i-\sum_{l=1}^{i-1}a_l b_{i-l}$, $2\leq i\leq p-1$. In particular, $b_i\in\mathbb{Z}_p$ and $b_i\equiv ip^{-1}a_i \mod p$, $1\leq i\leq p-1$.

Proposition 5.4

(i) *If $v_p(a_i)\geq 2$ for any $2\leq i\leq p-1$, then there is a kernel (H,h) of P such that the logarithm of H is of type pI_{p-1} and*

$$J(h)=\begin{pmatrix}pb_1 & b_2 & \cdots & b_{p-1}\\ p & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{pmatrix}.$$

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

(ii) *If there is* $2 \le j \le p-1$ *such that* $v_p(a_j) = 1$, *then there is a kernel* (H, h) *of* P *such that the logarithm of* H *is of type*

$$\begin{pmatrix} p & z\blacktriangle & 0 & \cdots & 0 \\ 0 & p & 0 & \cdots & 0 \\ 0 & 0 & p & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p \end{pmatrix},$$

where z *is as in Proposition* 5.3, *and*

$$J(h) = \begin{pmatrix} p & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ p/b_j & -b_1/b_j & \cdots & -b_{j-1}/b_j & -b_{j+1}/b_j & \cdots & -b_{p-1}/b_j \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Proof Denote Fontaine's triples corresponding to the formal group laws F_m and R by $(\mathcal{L}', M', \rho')$ and $(\mathcal{L}, M, \rho)$, respectively. Let (ψ, Ψ) be the morphism from $(\mathcal{L}', M', \rho')$ to $(\mathcal{L}, M, \rho)$ corresponding to P. One can choose a generator d of $\mathcal{L}'$ and generators $d_1, \dots, d_p$ of $\mathcal{L}$ so that $\psi(d) = pd_1 - pb_1d_2 - \cdots - pb_{p-1}d_p$. Then

$$M = \big\langle \rho(d_1), \dots, \rho(d_p) \big\rangle \big/ \big\langle p\rho(d_1) - \blacktriangle\rho(d_1) - z\blacktriangle^2 \rho(d_2), p\rho(d_2), \dots, p\rho(d_p) \big\rangle$$

and $\mathcal{L}_0$ is generated by $d_1 - b_1d_2 - \cdots - b_{p-1}d_p$. Denote $\overline{d}_i = \mathrm{red}_{\mathcal{L}_0} d_i \in \overline{\mathcal{L}}$, $D_i = i_T(\overline{d}_i) \in T, 1 \le i \le p$.

(i) If $v_p(a_i) \ge 2$ for any $2 \le i \le p-1$, then $v_p(b_i) \ge 1$ for any $2 \le i \le p-1$. In this case $\overline{\mathcal{L}} = \langle \overline{d}_2, \dots, \overline{d}_p \rangle$, $T = \langle D_2, \dots, D_p \rangle$, and

$$\overline{M} \cong \big\langle \overline{\rho}(\overline{d}_2), \dots, \overline{\rho}(\overline{d}_p) \big\rangle \big/ \big\langle -(b_1\blacktriangle + z\blacktriangle^2)\overline{\rho}(\overline{d}_2), p\overline{\rho}(\overline{d}_2), \dots, p\overline{\rho}(\overline{d}_p) \big\rangle.$$

Now if $v_p(b_1) \ge 1$,

$$\overline{M} \cong \big\langle \overline{\rho}(\overline{d}_2), \dots, \overline{\rho}(\overline{d}_p) \big\rangle \big/ \big\langle -z\blacktriangle^2 \overline{\rho}(\overline{d}_2), p\overline{\rho}(\overline{d}_2), \dots, p\overline{\rho}(\overline{d}_p) \big\rangle$$

and $J = \langle D_2, pD_3, \dots, pD_p \rangle$, since z is invertible. If $v_p(b_1) = 0$, then $b_1 + z\blacktriangle$ is invertible in $\mathcal{E}$ and again $J = \langle D_2, pD_3, \dots, pD_p \rangle$.

Further, $J^0 = \langle \overline{d}_2, p\overline{d}_3, \dots, p\overline{d}_p \rangle$, $\tau_0(\overline{d}_2) = p\overline{d}_2$, $\tau_0(\overline{d}_i) = \overline{d}_i$, $3 \le i \le p$. Finally, $\overline{M}^\tau = \langle D_2, \dots, D_p \rangle / \langle pD_2, \dots, pD_p \rangle$ which implies that there is a kernel (H, h) of P such that the logarithm of H is of type pI_{p-1}. Since

$$\tau_0 \circ \mathrm{red}_{\mathcal{L}_0}(d_i) = \begin{cases} pb_1\overline{d}_2 + b_2\overline{d}_3 + \cdots + b_{p-1}\overline{d}_p & \text{if } i = 1, \\ p\overline{d}_2 & \text{if } i = 2, \\ p\overline{d}_i & \text{if } 3 \le i \le p, \end{cases}$$

the Jacobian matrix of h has the required form.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

(ii) If there is $2 \le j \le p-1$ such that $v_p(a_j) = 1$, then $v_p(b_j) = 0$. In this case, $\overline{\mathcal{L}} = \langle \overline{d}_1, \dots, \overline{d}_j, \overline{d}_{j+2}, \dots, \overline{d}_p \rangle$, $T = \langle D_1, \dots, D_j, D_{j+2}, \dots, D_p \rangle$, and

$$\overline{M} \cong \left\langle \overline{\rho}(\overline{d}_1), \dots, \overline{\rho}(\overline{d}_j), \overline{\rho}(\overline{d}_{j+2}), \dots, \overline{\rho}(\overline{d}_p) \right\rangle / N$$

where

$$N = \left\langle - \blacktriangle \overline{\rho}(\overline{d}_1) - z \blacktriangle^2 \overline{\rho}(\overline{d}_2), p\overline{\rho}(\overline{d}_1), \dots, p\overline{\rho}(\overline{d}_j), p\overline{\rho}(\overline{d}_{j+2}), \dots, p\overline{\rho}(\overline{d}_p) \right\rangle.$$

Thus

$$\begin{aligned} J &= \langle D_1 + z \blacktriangle D_2, pD_1, pD_2, \dots, pD_j, pD_{j+2}, \dots, pD_p \rangle \\ &= \langle D_1 + z \blacktriangle D_2, pD_2, \dots, pD_j, pD_{j+2}, \dots, pD_p \rangle \end{aligned}$$

and $J^0 = \langle \overline{d}_1, p\overline{d}_2, \dots, p\overline{d}_j, p\overline{d}_{j+2}, \dots, p\overline{d}_p \rangle$, $\tau_0(\overline{d}_1) = p\overline{d}_1$, $\tau_0(\overline{d}_i) = \overline{d}_i$, for $2 \le i \le p$, $i \ne j+1$. Finally,

$$\overline{M}^{\tau} = \langle D_1, \dots, D_j, D_{j+2}, \dots, D_p \rangle / \langle pD_1 + z \blacktriangle D_2, pD_2, \dots, pD_j, pD_{j+2}, \dots, pD_p \rangle,$$

and we are done. ∎

Global Norm Homomorphism

Let q be a prime, $s \in \mathbb{Z}$ be a multiplicative generator modulo q and ζ be a primitive q-th root of unity. Let R be the Weil restriction of F_m with respect to the extension $\mathbb{Z}[\zeta]/\mathbb{Z}$ and the basis $\zeta, \zeta^s, \zeta^{s^2}, \dots, \zeta^{s^{q-2}}$. Then

$$P(X) = \mathcal{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\Big(1 + \sum_{i=1}^{q-1} x_i \zeta^{s^{i-1}}\Big) - 1 \in \mathrm{Hom}_{\mathbb{Z}}(R, F_m)$$

and $P(X) \equiv -\sum_{i=1}^{q-1} x_i \mod \deg 2$. Put $\overline{X} = (x_1, \dots, x_{q-2})$ and $\overline{Y} = (y_1, \dots, y_{q-2})$. By the implicit function theorem there exists a unique $\phi \in \mathbb{Z}[\![x_1, \dots, x_{q-2}]\!]$ such that $P(\phi(\overline{X}), \overline{X}) = 0$. Let $\alpha(\overline{X})$ denote the $(q-1)$-tuple $(\phi(\overline{X}), \overline{X})$. Define the $(q-2)$-tuple $\Omega(\overline{X}, \overline{Y}) = \big(\Omega_1(\overline{X}, \overline{Y}), \dots, \Omega_{q-2}(\overline{X}, \overline{Y})\big)$ by

$$\Omega_i(\overline{X}, \overline{Y}) = R_{i+1}(\alpha(\overline{X}), \alpha(\overline{Y})) \quad \text{for } 1 \le i \le q-2.$$

One obtains

$$P\big(R_1(\alpha(\overline{X}), \alpha(\overline{Y})), \dots, R_{q-1}(\alpha(\overline{X}), \alpha(\overline{Y}))\big) = 0,$$

since $P(R(X, Y)) = F_m(P(X), P(Y))$, thus

$$\phi\Big(R_2\big(\alpha(\overline{X}), \alpha(\overline{Y})\big), \dots, R_{q-1}\big(\alpha(\overline{X}), \alpha(\overline{Y})\big)\Big) = R_1\big(\alpha(\overline{X}), \alpha(\overline{Y})\big).$$

The latter equality implies $R(\alpha(\overline{X}), \alpha(\overline{Y})) = \alpha(\Omega(\overline{X}, \overline{Y}))$, *i.e.,* Ω is a formal group law over $\mathbb{Z}$, $\alpha \in \mathrm{Hom}(\Omega, R)$, and $J(\alpha) = \widetilde{Q} = \{\widetilde{q}_{i,j}\}_{1 \le i \le q-1, 1 \le j \le q-2}$, where $\widetilde{q}_{i,j} = 1$ if $j = i-1$, $\widetilde{q}_{i,j} = -1$ if $i = 1$, $\widetilde{q}_{i,j} = 0$ otherwise. To find Honda's type of the logarithm of Ω as a formal power series over $\mathbb{Q}_p$ (Honda's *p-type*), denote by $r(p)$ an integer such that $p \equiv s^{r(p)} \mod q$ and notice that the logarithm of R is of p-type $pI_{q-1} - V^{r(p)} \blacktriangle$, where $V = \{v_{i,j}\}_{1 \le i,j \le q-1}$, $v_{i,j} = 1$ if $j = i-1$ or $j = i+q-2$, and $v_{i,j} = 0$ otherwise for $p \ne q$, and of p-type $pI_{q-1} - (pI_{q-1} - Z) \blacktriangle$, where $Z = \{z_{i,j}\}_{1 \le i,j \le q-1}$, $z_{i,j} = 1$ for any i, j for $p = q$ ([DGX, Proposition 9.1]). Take $Q = \{q_{i,j}\}_{1 \le i,j \le q-1}$ such that $q_{i,j} = 1$ if $j = i$,

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

$q_{i,j} = -1$ if $j \neq 1$, $i = 1$ and $q_{i,j} = 0$ otherwise. For $p \neq q$, let $S(p) = \{s(p)_{i,j}\}_{1\le i,j\le q-2}$, $s(p)_{i,j} = 1$ if $j = i - r(p)$ or $j = i - r(p) + q - 1$; $s(p)_{i,j} = -1$ if $i = r(p)$ and $s(p)_{i,j} = 0$ otherwise. By Proposition 4.5 there is a kernel (H_p, h_p) of P such that $J(h_p) = Q(0 \quad I_{q-2})^T = \widetilde{Q}$ and the logarithm of H_p has p-type $pI_{q-2} - S(p)\blacktriangle$ if $p \neq q$ and $pI_{q-2} - pI_{q-2}\blacktriangle$ if $p = q$. Remark that the latter type can be replaced by pI_{q-2}. Since $P \circ \alpha = 0$, there is $g_p \in \mathrm{Hom}_{\mathbb{Z}_p}(\Omega, H_p)$ such that $\alpha = h_p \circ g_p$. It implies $J(g_p) = I_{q-2}$, *i.e.*, Ω and H_p are strictly isomorphic over $\mathbb{Z}_p$ and the logarithm of Ω has the same Honda's p-type as H_p.

Matrices $S(p)$ are defined for any prime $p \neq q$, put $S(q) = 0$. One can show that $S(p)$ and $S(p')$ commute for any primes p, p'. For a positive integer $l = \prod_{i=1}^{m} p_i^{k_i}$, where $p_1, \dots, p_m$ are distinct primes, define $S(l) = \prod_{i=1}^{m} S(p_i)^{k_i}$. Let

$$\xi(\overline{X}) = \sum_{l=1}^{\infty} \frac{1}{l} S(l)\overline{X}^l \in \mathbb{Q}[[\overline{X}]]^{q-2} \quad \text{and} \quad \Xi(\overline{X}, \overline{Y}) = \xi^{-1}\big(\xi(\overline{X}) + \xi(\overline{Y})\big).$$

Then ξ is of p-type $pI_{q-2} - S(p)\blacktriangle$ for any prime p, and Ξ is a formal group law over $\mathbb{Z}$ ([Ho, Theorem 8], [DGX, Proposition 2.5]). Thus Ω and Ξ have the same p-type for any prime p, and therefore are strictly isomorphic over $\mathbb{Z}$. This is [CG, Theorem 1].

Galois Action Associated with a Torus

Let L/K be a finite Galois extension of degree n, $\mathfrak{M}$ be a free $\mathcal{O}_K$–module with $\mathcal{O}_K[\mathrm{Gal}(L/K)]$- and $\mathcal{O}_L$-module structure extending the $\mathcal{O}_K$-module structure such that $\tau(lm) = l^{\tau}\tau(m)$ for any $\tau \in \mathrm{Gal}(L/K)$, $l \in \mathcal{O}_L$ and $m \in \mathfrak{M}$. Let $m_1, \dots, m_s$ be a free $\mathcal{O}_K$-basis of $\mathfrak{M}$, $\sigma \in \mathrm{Gal}(L/K)$, $D \in \mathrm{M}_s(\mathcal{O}_K)$ be the matrix of $\sigma - \mathrm{id}$ in the basis $m_1, \dots, m_s$.

Lemma 5.5 *If L/K is tamely ramified, then D satisfies the conditions of Lemma 4.1.*

Proof It suffices to prove that if $x, y \in \mathfrak{M}$ and $\sigma x - x = py$, then there exists $x' \in \mathfrak{M}$ such that $\sigma x' - x' = y$. Let $\widetilde{K}$ be the subfield of L fixed by σ. Then $L/\widetilde{K}$ is also tamely ramified, and hence, $\mathrm{tr}_{L/\widetilde{K}}\colon \mathcal{O}_L \to \mathcal{O}_{\widetilde{K}}$ is surjective. Chose $z \in \mathcal{O}_L$ so that $\mathrm{tr}_{L/\widetilde{K}}(z) = 1$ and denote the order of σ by q. Then $z + \sigma z + \dots + \sigma^{q-1}z = 1$. Finally, $\sigma x - x = py$ implies $y + \sigma y + \dots + \sigma^{q-1}y = 0$ and

$$x' = -y \cdot \sigma z - (y + \sigma y)\sigma^2 z - (y + \sigma y + \sigma^2 y)\sigma^3 z - \dots \\ - (y + \sigma y + \sigma^2 y + \dots + \sigma^{q-2}y)\sigma^{q-1}z$$

satisfies the required condition. ∎

Let $e_1 = 1, \dots, e_n$ be a free $\mathcal{O}_K$-basis of $\mathcal{O}_L$ and let T be an algebraic torus over K of dimension d split over L. Let $x_1, \dots, x_d$ be a free basis in the group $\mathfrak{X}$ of characters of T, which allows one to identify T_L with $(\mathbb{G}_m^d)_L$ and its Hopf algebra with $L[x_1, x_1^{-1}, \dots, x_d, x_d^{-1}]$. The natural action of $\mathrm{Gal}(L/K)$ on the Hopf algebra of T_L induces an action on its formal completion with respect to the local parameters $x_1 - 1, \dots, x_d - 1$, that is, on $L[[x_1, \dots, x_d]]$.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

Let R be the Weil restriction of F_m^d with respect to $\mathcal{O}_L/\mathcal{O}_K$ and $e_1, \dots, e_n$. For any nilpotent $\mathcal{O}_K$-algebra N, one can identify $R(N)$ with $\mathbb{F}_m^d(N \otimes_{\mathcal{O}_K} \mathcal{O}_L)$ by

$$(s_1, \dots, s_{nd}) \longleftrightarrow \Big(\sum_{i=1}^{n} s_{(i-1)d+1} \otimes e_i, \dots, \sum_{i=1}^{n} s_{(i-1)d+d} \otimes e_i \Big).$$

Then a right action of $\mathrm{Gal}(L/K)$ on R can be defined as follows: for

$$s \in \mathrm{Hom}_{\mathcal{O}_L}\big(\mathcal{O}_L[[x_1, \dots, x_d]], N \otimes_{\mathcal{O}_K} \mathcal{O}_L\big),$$

put $s\sigma = \widehat{\sigma}^{-1} \circ s \circ \widetilde{\sigma}$, where $\widetilde{\sigma} \in \mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_L[[x_1, \dots, x_d]])$ is the restriction of the action of σ on $L[[x_1, \dots, x_d]]$, and $\widehat{\sigma} \in \mathrm{End}_{\mathcal{O}_K}(N \otimes_{\mathcal{O}_K} \mathcal{O}_L)$ is induced by σ. This right action can be considered as a (left) action of $\mathrm{Gal}(L/K)^\circ$ on R, where $\mathrm{Gal}(L/K)^\circ$ denotes the opposite group of $\mathrm{Gal}(L/K)$.

Proposition 5.6 *If L/K is tamely ramified, $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma - \mathrm{id}$ is pure as an endomorphism of the formal group law R.*

Proof Denote $\mathfrak{M} = \mathcal{X} \otimes_{\mathcal{O}_K} \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$. Then $\mathfrak{M}$ has an $\mathcal{O}_L$-module structure induced from the $\mathcal{O}_L$-module structure on $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$. The group $\mathcal{X}$ is invariant with respect to the $\mathrm{Gal}(L/K)$-action on the Hopf algebra of T_L. Besides, there is a unique $\mathrm{Gal}(L/K)$-action on $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ such that $h^\tau(l^\tau) = h(l)$ for any $l \in \mathcal{O}_L$, $h \in \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$, $\tau \in \mathrm{Gal}(L/K)$. Then there is a unique $\mathcal{O}_K[\mathrm{Gal}(L/K)]$-module structure on $\mathfrak{M}$ that satisfies $\tau(x \otimes h) = \tau(x) \otimes h^\tau$ for any $x \in \mathcal{X}$, $h \in \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$, $\tau \in \mathrm{Gal}(L/K)$. Clearly, $\tau(lm) = l^\tau \tau(m)$ for any $m \in \mathfrak{M}$, $l \in \mathcal{O}_L$, $\tau \in \mathrm{Gal}(L/K)$. Moreover, according to [DGX, Proposition 6.3], $J(\sigma)$ is equal to the matrix of σ considered as an endomorphism of $\mathfrak{M}$ in the basis $m_1, \dots, m_{dn}$, where $m_{(i-1)d+l} = x_l \otimes \widetilde{e}_i$, $1 \le i \le n$, $1 \le l \le d$, and $\widetilde{e}_1, \dots, \widetilde{e}_n$ is the basis of $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ dual to $e_1, \dots, e_n$. Lemma 5.5 completes the proof. ∎

Let (H, h) denote a kernel of $\sigma - \mathrm{id}$.

Corollary *If L/K is tamely ramified, then $\mathrm{Im}\, h(N) = \mathrm{Ker}(\sigma - \mathrm{id})(N)$ for any nilpotent $\mathcal{O}_K$-algebra N.*

This corollary can be interpreted as a consequence of a result on the Néron model for an algebraic torus split over a tamely ramified extension. Indeed, recall that R can be identified with the formal completion of the Weil restriction of $(\mathbb{G}_m^d)_{O_L}$ with respect to $\mathcal{O}_L/\mathcal{O}_K$. The latter scheme is canonically isomorphic to the connected component $\mathcal{U}_0$ of the Néron model $\mathcal{U}$ for the Weil restriction of $(\mathbb{G}_m^d)_L$ with respect to L/K. An action of $\mathrm{Gal}(L/K)$ on these Weil restrictions can be defined as above, and due to the universal property of the Néron model, we get an action of $\mathrm{Gal}(L/K)$ on $\mathcal{U}$. According to [Ed], the fixed subscheme $\mathcal{U}^\sigma$ of $\mathcal{U}$ is smooth, provided L/K is tamely ramified. The connected component of $(\mathcal{U}_0)^\sigma$ is canonically isomorphic to that of $\mathcal{U}^\sigma$ (see [DGX, Proposition 5.6]), and in particular, $(\mathcal{U}_0)^\sigma$ is also smooth. Denote by H' the formal completion of $(\mathcal{U}_0)^\sigma$, and by h' the completion of the morphism $\iota\colon (\mathcal{U}_0)^\sigma \to \mathcal{U}_0$, which is the kernel of the endomorphism $\sigma - \mathrm{id}$ of $\mathcal{U}_0$. Since $(\mathcal{U}_0)^\sigma$ is affine, $\mathrm{Im}\, h'(N) = \mathrm{Im}\, \iota(N) = \mathrm{Ker}(\sigma - \mathrm{id})(N)$ for any nilpotent $\mathcal{O}_K$-algebra N, and hence (H', h') is also a kernel of $\sigma - \mathrm{id}$. This implies the required statement.

https://doi.org/10.4153/CJM-2015-024-7 Published online by Cambridge University Press

References

[Ca] P. Cartier, *Modules associés à un groupe formel commutatif. Courbes typiques.* C.R. Acad. Sci. Paris **265**(1967), A129–A132.

[CG] N. Childress and D. Grant, *Formal groups of twisted multiplicative groups and L-series.* In: *K*-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992), Proc. Symp. Pure Math., 58, American Mathematical Society, Providence, RI, 1995, pp. 89–102.

[De] O. Demchenko, *Covariant Honda theory.* Tohoku Math. J. **57**(2005), no. 3, 303–319. http://dx.doi.org/10.2748/tmj/1128702999

[DGX] O. Demchenko, A. Gurevich, and X. Xarles, *Formal completions of the Néron models for algebraic tori.* Proc. London Math. Soc. **100**(2010), no. 3, 607–638. http://dx.doi.org/10.1112/plms/pdp039

[Ed] B. Edixhoven, *Néron models and tame ramification.* Compositio Math. **81**(1992), no. 3, 291–306.

[Fo] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux.* Astérisque, 47–48, Société Mathématique de France, Paris, 1977.

[Ho] T. Honda, *On the theory of commutative formal groups.* J. Math. Soc. Japan **22**(1970), 213–246. http://dx.doi.org/10.2969/jmsj/02220213

[Ra] M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$. Bull Soc. Math. Fr. **102**(1974), 241–280.

[Ta] J. Tate, *p-divisible groups.* 1967 Proc. Conf. Local Fields (Driebergen, 1966) Springer, Berlin, 1967, pp. 158–183.

[Zi] T. Zink, *Cartiertheorie kommutativer formaler Gruppen.* Teubner Verlagsgesellschaft, Leipzig, 1984.

Department of Mathematics and Mechanics, St.Petersburg State University, Universitetsky pr. 28, Stary Petergof, St.Petersburg, 198504, Russia
e-mail: vasja@eu.spb.ru

Einstein Institute of Mathematics, Hebrew University of Jerusalem, Givat Ram, Jerusalem, 91904, Israel
e-mail: gurevich@math.huji.ac.il