Journal of the Inst. of Math. Jussieu (2012) **11**(2), 363–419
doi:10.1017/S1474748011000132

HIGHER-LEVEL CANONICAL SUBGROUPS FOR p-DIVISIBLE GROUPS

JOSEPH RABINOFF

Department of Mathematics, Harvard University, One Oxford Street, Cambridge, MA 02138, USA (rabinoff@post.harvard.edu)

(Received 4 December 2009; revised 15 October 2010; accepted 15 October 2010)

Abstract Let R be a complete rank-1 valuation ring of mixed characteristic $(0, p)$, and let K be its field of fractions. A g-dimensional truncated Barsotti–Tate group G of level n over R is said to have a *level-n canonical subgroup* if there is a K-subgroup of $G \otimes_R K$ with geometric structure $(\boldsymbol{Z}/p^n\boldsymbol{Z})^g$ consisting of points 'closest to zero'. We give a non-trivial condition on the Hasse invariant of G that guarantees the existence of the canonical subgroup, analogous to a result of Katz and Lubin for elliptic curves. The bound is independent of the height and dimension of G.

Keywords: abelian varieties; p-divisible groups; canonical subgroups; automorphic forms; tropical geometry

AMS 2010 *Mathematics subject classification:* Primary 11G10
Secondary 14L05

Contents

1. Introduction

1.1. Motivation. Let K be a field that is complete with respect to a non-trivial non-Archimedean valuation, with residue characteristic p. The level-n canonical subgroup of

an abelian variety A of dimension g defined over K is a certain distinguished K-subgroup of $A[p^n]$ with geometric structure $(\boldsymbol{Z}/p^n\boldsymbol{Z})^g$; it should exist when the reduction type of A is 'not too far from ordinary'. The classical theory of the canonical subgroup (for elliptic curves) as introduced by Katz [**22**], building on ideas of Lubin, has seen important applications in the study of overconvergent p-adic modular forms; see for instance the work of Buzzard and Taylor [**7**], Buzzard [**6**] and Kassaei [**21**]. In an effort to extend these overconvergent methods to the study of p-adic automorphic forms, there has been much work in the past several years towards a better understanding of the canonical subgroup of a higher-dimensional abelian variety.

1.2. In this paper we give an intrinsic geometric construction of the level-n canonical subgroup of an arbitrary truncated Barsotti–Tate group G of level n defined over the valuation ring R of K, subject to a universal bound on its 'Hasse invariant' that is independent of the height and dimension of G. Building on these results, our construction can be relativized and extended to algebraic families of abelian varieties over K with arbitrary fibral reduction types, still under the same Hasse invariant bound; this is the subject of ongoing work in collaboration with Brian Conrad. (Working with truncated Barsotti–Tate groups over R effectively restricts our present focus to the case of good reduction.)

1.3. Two important advantages of our approach are its generality, and the fact that our bounds are nearly as good as possible, in the sense of § 1.10. Abbes and Mokrane [**1**] and Andreatta and Gasbarri [**2**] have methods for constructing level-1 canonical subgroups of abelian varieties, subject to more restrictive Hasse invariant bounds than ours. Tian [**30**] and Fargues and Tian [**13**] extend Abbes and Mokrane's work to construct the level-n canonical subgroup of an arbitrary level-n truncated Barsotti–Tate group, again subject to more restrictive bounds and over noetherian base rings. Kisin and Lai [**23**] and Kassaei [**20**] also have theories of the level-1 canonical subgroup for certain universal families of abelian varieties; their methods rely on the integral structure of certain Shimura varieties. Recently, in an extension of their 'subgroup-free' methods [**15**], Goren and Kassaei have made a construction of the canonical subgroup of any level of a certain class of abelian varieties with real multiplication, with better bounds than ours in terms of partial Hasse invariants; again, the advantage of our approach is that it works for arbitrary abelian varieties (independent of any level structure) while remaining quite explicit.

1.4. We expect that our results, along with certain compatibility properties with respect to isogenies and the Frobenius endomorphism that will appear in a future paper, should be useful in the application of overconvergent methods to the study of p-adic automorphic forms on quite general modular varieties such as Hilbert modular varieties, Siegel modular varieties, and more general Shimura varieties of PEL type. We expect that the explicit nature of our bounds will be important in such applications. One might hope in particular to find classical modular forms in p-adic families of p-adic modular forms as in [**23**], and

in the long term perhaps to prove a 'control theorem' in certain settings generalizing results of Coleman [**8**, **9**] and Kassaei [**21**].

Our methods are also entirely different from those used in the literature mentioned in § 1.3. They involve some fairly explicit calculations with Zink's displays, and they use the language of tropical algebraic geometry in a crucial way. We expect that these methods and some of the related intermediate results will prove useful in other contexts.

1.5. Overview of results. Let R be a complete rank-1 valuation ring of mixed characteristic $(0, p)$, with valuation ord normalized so that $\mathrm{ord}(p) = 1$ and absolute value $|\cdot| = p^{-\mathrm{ord}(\cdot)}$. We do not require R to be discretely valued; this generality will be useful for avoiding perfectness hypotheses on the residue field. Let G be a p-divisible group of height h and dimension g over R, and let $G^\circ \cong \mathrm{Spf}(R[\![X_1, \ldots, X_g]\!])$ be the connected component of G. Let $G_0 = G \otimes_R (R/pR)$. For $r \in R/pR$ we let $\tilde{r}$ denote any lift to R; observe that $\min\{\mathrm{ord}(\tilde{r}), 1\}$ depends only on r. Let $V\colon G_0^{(p)} \to G_0$ be the Verschiebung homomorphism over R/pR, and let $\mathrm{d}V$ be the associated map on tangent spaces. Choosing bases, we may identify $\mathrm{d}V$ with a $g \times g$ matrix with entries in R/pR. The *Hasse invariant* of G is defined to be

$$H(G) = \min\{\mathrm{ord}(\det(\mathrm{d}V)^\sim), 1\}.$$

One can show (Remark 7.9.1 (ii)) that $H(G) = 0$ if and only if the Cartier dual of G° is étale, which is the case exactly when the height of G° is equal to g.

1.6. The p-power torsion levels $G^\circ[p^n]$ are truncated Barsotti–Tate groups over $\mathrm{Spec}(R)$, in the sense of [**27**, Chapter 1] or § 2.7. For $\xi \in G^\circ[p^n](\bar{K})$ let $|\xi| = \max\{|X_1(\xi)|, \ldots, |X_g(\xi)|\} < 1$; this is the distance of ξ from the origin, and is independent of the choice of R-parameters X_i for G°. For $\rho > 0$ let $G^\circ[p^n]_{\leqslant\rho}$ be the K-subgroup of $G^\circ[p^n]$ whose geometric points are

$$G^\circ[p^n]_{\leqslant\rho}(\bar{K}) = \{\xi \in G^\circ[p^n](\bar{K})\colon |\xi| \leqslant \rho\},$$

and let

$$G^\circ[p^\infty]_{\leqslant\rho} = \bigcup_{n=1}^{\infty} G^\circ[p^n]_{\leqslant\rho}.$$

Obviously, $G^\circ[p^n]_{\leqslant 1} \cong (\boldsymbol{Z}/p^n\boldsymbol{Z})^h$, and for small enough ρ we have $G^\circ[p^n]_{\leqslant\rho}(\bar{K}) = \{0\}$. Also note that if $\rho \leqslant \mu$ then $G^\circ[p^n]_{\leqslant\rho} \subset G^\circ[p^n]_{\leqslant\mu}$. If $G^\circ[p^n]_{\leqslant\rho}(\bar{K}) \cong (\boldsymbol{Z}/p^n\boldsymbol{Z})^g$ for some $\rho > 0$ then we call $G^\circ[p^n]_{\leqslant\rho}$ the *level-n canonical subgroup of G*, and we say that this canonical subgroup *admits the radius ρ*.

1.7. Such a subgroup, if it exists, does not depend on the choice of ρ: it is the unique subgroup with geometric group structure $(\boldsymbol{Z}/p^n\boldsymbol{Z})^g$ whose geometric points are closer to the origin than all other points of $G^\circ[p^n](\bar{K})$. If $H(G) = 0$ then $h = g$, so $G^\circ[p^n] = G^\circ[p^n]_{\leqslant 1}$ serves as the level-n canonical subgroup for any n. Conversely, if the level-n canonical subgroup exists for all n then $H(G) = 0$ (Remark 11.6). In general it is not true

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

that even the level-1 canonical subgroup exists, even when $h = 2$ and $g = 1$, although it is clear from the definition that if there exists a level-n canonical subgroup G_n of G then for all $1 \leqslant m \leqslant n$ the K-subgroup $G_n[p^m]$ is the level-m canonical subgroup of G. Also note that the canonical subgroup of G depends only on the connected component G°, and that its existence and formation are insensitive to valued extensions of K.

1.8. We will see (Remark 7.9.1 (i) and § 7.5.2) that the Hasse invariant and level-n canonical subgroup of G are notions that are intrinsic to the truncated Barsotti–Tate group $G[p^n]$. The main goal of this paper is to prove the following result.

Theorem 1.9. *Let G be a truncated Barsotti–Tate group of level $N \geqslant 1$ defined over a complete mixed characteristic $(0, p)$ valuation ring R, and let $H(G)$ be its Hasse invariant. If $H(G) < (p-1)/p^N$ then the level-N canonical subgroup of G exists, and it admits the radius $\rho = p^{-r}$ where*

$$r = \frac{1}{p^{N-1}(p-1)} - \frac{H(G)}{p-1}.$$

1.9.1. The analogous statement for p-divisible groups G over R then follows; this statement (with R fixed) is slightly weaker than Theorem 1.9 over R, since we do not know if a truncated Barsotti–Tate group of level N over R is necessarily isomorphic to the p^N-torsion of a p-divisible group over R when the residue field of R is not perfect. An elementary argument will reduce Theorem 1.9 to the special case when G is the p^N-torsion in a p-divisible group.

1.10. Theorem 1.9 is a partial generalization of results of Katz and Lubin [**22**] on level-1 canonical subgroups of elliptic curves (see in particular Theorem 3.10.7 of [**22**]), as extended by Buzzard [**6**, § 3] to higher levels (see [**10**, Theorem 4.2.5] for a proof that Buzzard's higher-level canonical subgroups agree with ours). Katz proves in particular that if E is an elliptic curve over R and if $G = E[p^\infty]$, then the level-N canonical subgroup of G exists if and only if $H(G) < 1/p^{N-2}(p+1)$, with the radius as in Theorem 1.9. This (sharp) bound is better than our bound by a factor of $p^2/(p^2-1)$; see Remark 1.12. Katz also analyses the behaviour of the canonical subgroup with respect to degree-p isogenies of elliptic curves, and proves that the level-N canonical subgroup lifts the kernel of the N-fold relative Frobenius on $G \otimes_R (R/p^\lambda R)$ for an explicit value of $\lambda \in (0, 1)$ depending on p, N and $H(G)$. In future work we will prove analogous results in our situation.

1.11. Here we give a brief overview of the proof of Theorem 1.9. Zink [**32**] has defined a category of semi-linear algebraic objects over the ring of Witt vectors $W(R)$ called displays, as well as a functor $\mathcal{P} \rightsquigarrow \mathrm{BT}_\mathcal{P}$ from the category of (nilpotent) displays over R to the category of connected p-divisible groups over R, which is an equivalence of categories [**25**, Theorem 1.1]. We will first prove Theorem 1.9 in the case when G° extends to a p-divisible group over R, in which case $G^\circ \cong \mathrm{BT}_\mathcal{P}[p^N]$ for some display $\mathcal{P}$ over R, and then in § 12 we will reduce Theorem 1.9 to this case.

If $\mathcal{P}$ is a display over R, the p-divisible formal group $\mathrm{BT}_\mathcal{P}$ is given in terms of its functor of points; § 3 makes explicit how to recover a g-dimensional formal group law from such an

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

object. In §§ 4–5, we calculate the logarithm of $\mathrm{BT}_{\mathcal{P}}$ in terms of the structure coefficients of $\mathcal{P}$. Then in § 6 we review the fact that the kernel of the logarithm is the p-power torsion $\mathrm{BT}_{\mathcal{P}}[p^\infty]$ of $\mathrm{BT}_{\mathcal{P}}$ as a K-analytic subspace of a p-adic open unit ball of dimension g.

By the above considerations, we need to understand the valuations of the points of the kernel of the logarithm. Thinking of the logarithm as a g-tuple of power series $\log_1, \dots, \log_g$ in g variables, this amounts to finding the valuations of the common zeros of the power series $\log_i$. The theory of tropical algebraic geometry is ideally suited for such a task; we briefly recall the relevant parts of the theory in § 8. In § 9 we study the tropicalizations of the $\log_i$ in enough detail to justify making a rather drastic deformation of $\ker(\log)$ in § 10, the end result of which is a way of counting the number of common zeros of the $\log_i$ contained in the ball of radius ρ. In particular we show that under the Hasse invariant bound in the above theorem, the K-group $\mathrm{BT}_{\mathcal{P}}[p^\infty]_{\leqslant\rho}$ has order p^{Ng} for ρ as in the theorem; in § 11 we show that $\mathrm{BT}_{\mathcal{P}}[p^\infty]_{\leqslant\rho}(\bar{K}) \cong (\boldsymbol{Z}/p^N\boldsymbol{Z})^g$.

Remark 1.12. Our methods depend on the fact that when G is a connected p-divisible group over R with $H(G) < (p-1)/p^N$ then $G[p^\infty]_{\leqslant\rho} = G[p^N]_{\leqslant\rho}$ with $\rho = p^{-r}$, $r = 1/p^{N-1}(p-1) - H(G)/(p-1)$. This is *false* in general when $H(G) \geqslant (p-1)/p^N$: for instance, let E be an elliptic curve over R with ordinary reduction and let E' be an elliptic curve with supersingular reduction and Hasse invariant $H(E') = (p-1)/p$. By the work of Katz and Lubin in [**22**] E' has a level-1 canonical subgroup with radius $\rho = p^{-1/p(p-1)}$, and E has a level-2 canonical subgroup with the same radius. Therefore, $(E\times E')[p^\infty]_{\leqslant\rho} \neq (E\times E')[p]_{\leqslant\rho}$ (although $(E\times E')[p]_{\leqslant\rho}$ is the level-1 canonical subgroup of $E \times E'$). Thus our methods break down when $H(G) \geqslant (p-1)/p^N$. It is unclear to us whether this bound is sharp in general, or whether Katz and Lubin's bound holds in higher dimensions.

1.13. General notation. In this paper, all rings are commutative, and contain a unit element unless noted otherwise; rings without a unit element will generally be denoted by a calligraphic symbol. If R is a ring, $\mathcal{N}(R)$ will denote its nilradical. We fix a prime p once and for all.

The symbol $\subset$ means subset inclusion; $\subsetneq$ means strict inclusion. For $r \in \boldsymbol{R}$ let

$$\boldsymbol{R}_{>r} = \{x \in \boldsymbol{R} \colon x > r\}, \qquad \boldsymbol{R}_{\geqslant r} = \{x \in \boldsymbol{R} \colon x \geqslant r\},$$

and similarly for $\boldsymbol{R}_{<r}$, $\boldsymbol{R}_{\leqslant r}$, $\boldsymbol{Z}_{\leqslant r}$, $\boldsymbol{Z}_{<r}$, $\boldsymbol{Z}_{>r}$ and $\boldsymbol{Z}_{\geqslant r}$. We let $\boldsymbol{N} = \boldsymbol{Z}_{\geqslant 1}$.

We will use other bold capital letters $\boldsymbol{X}, \boldsymbol{Y}, \dots$ to denote a sequence of indeterminates, that is, $\boldsymbol{X} = X_1, \dots, X_g$, $\boldsymbol{Y} = Y_1, \dots, Y_g$, etc.

1.13.1. We use the following notation for Witt vectors. If R is any ring,

$$W(R) = \{(x_0, x_1, x_2, \dots) \colon x_i \in R\}$$

denotes the ring of p-Witt vectors. For $x \in W(R)$, the *Witt components* of x will be denoted $x_0, x_1, \dots$, i.e. $x = (x_0, x_1, x_2, \dots) \in W(R)$. For $n \in \boldsymbol{Z}_{\geqslant 0}$ the *nth ghost component* map is the ring homomorphism $w_n \colon W(R) \to R$ defined by

$$w_n(x) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^{n-1}x_{n-1}^p + p^n x_n.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

We set

$$I_R = \ker(w_0) = \{(x_0, x_1, x_2, \dots) \in W(R) \colon x_0 = 0\},$$

and for $x \in R$ we let $[x]$ denote the Witt vector $(x, 0, 0, \dots) \in W(R)$. The Frobenius and Verschiebung endomorphisms are denoted ${}^{\mathrm{F}}(\cdot), {}^{\mathrm{V}}(\cdot) \colon W(R) \to W(R)$, respectively, and are defined by the relations

$$w_n({}^{\mathrm{F}}x) = w_{n+1}(x), \qquad w_n({}^{\mathrm{V}}x) = \begin{cases} 0 & \text{if } n = 0, \\ p w_{n-1}(x) & \text{otherwise,} \end{cases}$$

and by functoriality in R. More explicitly, ${}^{\mathrm{V}}(x_0, x_1, \dots) = (0, x_0, x_1, \dots)$ (so $I_R = {}^{\mathrm{V}}(W(R))$), and when $pR = 0$ we have ${}^{\mathrm{F}}(x_0, x_1, \dots) = (x_0^p, x_1^p, \dots)$. When R is not an $\boldsymbol{F}_p$-algebra then the formula for ${}^{\mathrm{F}}x$ is difficult to write explicitly; for instance, the first two components of ${}^{\mathrm{F}}x$ are given by

$${}^{\mathrm{F}}(x_0, x_1, \dots) = \left(x_0^p + p x_1,\ x_1^p + p x_2 - \sum_{i=0}^{p-1} \binom{p}{i} p^{p-i-1} x_0^{ip} x_1^{p-i},\ \dots \right).$$

The reader who is unfamiliar with Witt vectors over arbitrary rings may want to do the exercise in [**24**] on this topic (the exercise number varies by edition, but can be found under the 'Witt vectors' entry in the index), with the caveat that Lang's definition of the Frobenius endomorphism is different from ours. A more complete treatment can be found in § 17 of [**18**].

1.13.2. Let R be a ring, let G be an R-group scheme, and let $n \in \boldsymbol{N}$. We will denote the multiplication-by-n map by $[n]_G \colon G \to G$, and its kernel by $G[n]$. If $G = \mathrm{Spec}(A)$ is affine then we will also write $[n]_G \colon A \to A$ for the corresponding R-algebra homomorphism. When no confusion is likely we will drop the subscript and write $[n] = [n]_G$. If $\mathfrak{G} \cong \mathrm{Spf}(R[\![X_1, \dots, X_g]\!])$ is a formal group over R then we define $[n] = [n]_{\mathfrak{G}}$ and $\mathfrak{G}[n]$ likewise. If $G = \mathrm{Spec}(A)$ is an affine R-group scheme (respectively $G \cong \mathrm{Spf}(R[\![X_1, \dots, X_g]\!])$ is a formal group over R) and $I \subset A$ is the augmentation ideal then the *cotangent space* to G is the R-module I/I^2, and the *tangent space* is $\mathrm{Lie}(G) = \mathrm{Hom}_R(I/I^2, R)$.

2. Generalities concerning p-divisible groups

2.1. Here we fix our ideas concerning formal Lie groups, p-divisible groups and truncated Barsotti–Tate groups. For details see [**27**, Chapters I and II], [**29**] and [**19**].

2.2. Let R be a ring endowed with the discrete topology. A *formal Lie variety of dimension g* over R is a pointed formal scheme $\mathfrak{X} = \mathrm{Spf}(A)$ over $\mathrm{Spf}(R)$ such that $A \cong R[\![\boldsymbol{X}]\!]$, where $\boldsymbol{X} = (X_1, \dots, X_g)$ is a set of g indeterminates and $R[\![\boldsymbol{X}]\!]$ is given the $(\boldsymbol{X})$-adic topology. We call such an isomorphism $A \cong R[\![\boldsymbol{X}]\!]$ a *choice of parameters* for $\mathfrak{X}$. A *formal Lie group* over R is a formal Lie variety $\mathfrak{G}$ over R which is a group object in the category of pointed formal schemes over $\mathrm{Spf}(R)$. Given a formal Lie group

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

$\mathfrak{G}$ and a choice of parameters $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$, the group structure on $\mathfrak{G}$ is given by a g-dimensional formal group law F on $R[\![\boldsymbol{X}]\!]$. Note that the tangent space of a g-dimensional formal Lie group $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ is the rank-g free R-module $\mathrm{Hom}_R((\boldsymbol{X})/(\boldsymbol{X})^2, R)$. In this paper, all formal group laws and all formal Lie groups will be assumed commutative.

2.3. A *p-divisible group* or *Barsotti–Tate group* over R is a directed system $G = \{G(n)\}_{n\in\boldsymbol{N}}$ of finite locally free commutative group schemes over $\mathrm{Spec}(R)$ such that for all $n \in \boldsymbol{N}$,

(i) the map $G(n) \to G(n+1)$ is a closed immersion identifying $G(n)$ with $G(n+1)[p^n]$, and

(ii) the resulting map $[p]\colon G(n+1) \to G(n)$ is faithfully flat.

If $G = \{G(n)\}_{n\in\boldsymbol{N}}$ is a p-divisible group then we will write $G[p^n] = G(n)$. Suppose that R is a p-adically separated and complete local ring. For all $n \geqslant 1$ the R-group scheme $G[p^n]$ is finite and flat* with constant order p^{nh} for some number $h \in \boldsymbol{Z}_{\geqslant 0}$ (not depending on n), called the *height* of G. The *connected component* of a p-divisible group G over R is the p-divisible group $G^\circ = \{G[p^n]^\circ\}_{n\in\boldsymbol{N}}$, where $G[p^n]^\circ$ is the connected component of the identity section in $G[p^n]$. If $G = G^\circ$ we say that G is *connected*, or that G is a *p-divisible formal group*.

2.4. We continue to assume R is a p-adically separated and complete local ring. By [**27**, Chapter II], a p-divisible formal group G over R is a formal Lie group in the sense that there exists a formal Lie group $\mathfrak{G}$ over $\mathrm{Spf}(R)$, canonically determined by G, such that $\mathfrak{G}[p^n]$ is a finite flat group scheme over $\mathrm{Spec}(R)$ and $G \cong \mathfrak{G}[p^\infty] := \{\mathfrak{G}[p^n]\}_{n\in\boldsymbol{N}}$ naturally. The *tangent space* to a p-divisible group G is the finite free R-module $\mathrm{Lie}(G) := \mathrm{Lie}(\mathfrak{G})$, where $\mathfrak{G}$ is the formal Lie group determined by the p-divisible formal group G° as above, and the *dimension* of G is the R-rank of $\mathrm{Lie}(G)$.

Remark 2.5. Let $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ be a formal Lie group over R, and suppose that R is a complete local *noetherian* ring with residue characteristic p. By [**29**, Proposition 2.2.1], $G = \{\mathfrak{G}[p^n]\}_{n\in\boldsymbol{N}}$ is a p-divisible formal group over R if and only if $[p]\colon \mathfrak{G} \to \mathfrak{G}$ is an *isogeny*, i.e. $[p]\colon R[\![\boldsymbol{X}]\!] \to R[\![\boldsymbol{X}]\!]$ makes $R[\![\boldsymbol{X}]\!]$ into a finite free module over itself. This condition can be checked after base change to the residue field k, or to any field extension of k.

Remark 2.6. Suppose that R is a local $\boldsymbol{F}_p$-algebra. Let G be a p-divisible formal group over R, and let $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ be the associated formal Lie group. Let $I = (\boldsymbol{X}) \subset R[\![\boldsymbol{X}]\!]$ be the augmentation ideal and let $J \subset R[\![\boldsymbol{X}]\!]$ be the ideal defining $\mathfrak{G}[p]$. Since the relative Frobenius $F\colon \mathfrak{G} \to \mathfrak{G}^{(p)}$ factors through $[p]\colon \mathfrak{G} \to \mathfrak{G}$, we have $J \subset (X_1^p, \ldots, X_g^p) \subset I^2$. Thus $G[p]$ 'captures' the tangent space $\mathrm{Lie}(G)$ in the sense that the canonical map $\mathrm{Lie}(G[p]) \to \mathrm{Lie}(G)$ is an isomorphism. It follows that $\mathrm{Lie}(G[p^n]) \to \mathrm{Lie}(G)$ is an isomorphism for all $n \geqslant 1$.

* A finitely generated module over a local ring R is flat if and only if it is free by [**26**, Theorem 7.10]. Hence a finite R-scheme $X = \mathrm{Spec}(A)$ is flat if and only if A is a free R-module.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

More generally, if p is nilpotent in R then $\mathrm{Lie}(G[p^n]) \to \mathrm{Lie}(G)$ is an isomorphism for large enough n; see [**27**, § II.3].

2.7. Let R be any ring, let G be a finite locally free group scheme over R, and let $n \geqslant 1$. We say that G is a *truncated p-divisible group of level n*, or a *truncated Barsotti–Tate group of level n*, or a BT_n, provided that G is killed by p^n, and for $0 \leqslant i \leqslant n$ the map $p^i \colon G \to G[p^{n-i}]$ is faithfully flat. If $n = 1$ we also require the following condition.

> Let $G_0 = G \otimes_R (R/pR)$, and let $F \colon G_0 \to G_0^{(p)}$ and $V \colon G_0^{(p)} \to G_0$ be the relative Frobenius and Verschiebung homomorphisms, respectively (see [**3**, Exposé VII_A.4] for the definition). We require that $\ker(F), \ker(V)$ be finite locally free (R/pR)-group schemes and that $F \colon G_0 \to \ker(V)$ and $V \colon G_0^{(p)} \to \ker(F)$ be faithfully flat.

Suppose again that R is a p-adically separated and complete local ring with residue field k. If G is a BT_n for some $n \geqslant 1$ and $G_k := G \otimes_R k$ then $\mathrm{Lie}(G_k)$ is a finite-dimensional k-vector space; its k-dimension is defined to be the *dimension* of G. The order of $G[p]$ is equal to p^h for some number $h \geqslant 0$, called the *height* of G. Note that if G is a BT_n of dimension g over R and G° is the connected component of the identity section in G then G° is also a BT_n of dimension g over R.

2.8. If G is a BT_n of dimension g and height h for $n \geqslant 2$ then $G[p^{n-1}]$ is a BT_{n-1} of dimension g and height h by [**27**, Proposition II.3.3.11], and if G is a p-divisible group of dimension g and height h then $G[p^n]$ is a BT_n of dimension g and height h for all $n \geqslant 1$. Conversely, if R is noetherian and its residue field is perfect then by a theorem of Grothendieck [**19**, Theorem 4.4(e)], any BT_n over R is isomorphic to the p^n-torsion subgroup of a Barsotti–Tate group over R.

3. Formal groups and formal group laws

3.1. In [**31**], Zink develops an algebraic theory of formal groups which is well-adapted to calculations with displays. Here we make explicit the relation between Zink's formal groups and classical formal group laws.

In this section, R is any ring.

Definition 3.2. A *nilpotent R-algebra* is an R-algebra $\mathcal{N}$ (generally without unit) such that for some $r \geqslant 0$, a product of any r elements of $\mathcal{N}$ is equal to zero. In other words, if $\mathcal{N}^r$ denotes the ideal generated by $\{x_1 x_2 \cdots x_r \colon x_i \in \mathcal{N}\}$, then $\mathcal{N}^r = 0$. We let Nil_R denote the category of nilpotent R-algebras.

A *topologically nilpotent R-algebra* is a topological R-algebra $\mathcal{N}$ such that

(i) $\bigcap_{r=1}^{\infty} \mathcal{N}^r = 0$ and

(ii) the natural map $\mathcal{N} \to \varprojlim_r \mathcal{N}/\mathcal{N}^r$ is a topological isomorphism, where $\mathcal{N}/\mathcal{N}^r$ is given the discrete topology.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Let $\mathrm{Nil}_R^\wedge$ denote the category whose objects are the topologically nilpotent R-algebras and whose morphisms are R-algebra homomorphisms.

Remark 3.3.

(i) If $\mathcal{N}$ is a nilpotent (respectively topologically nilpotent) R-algebra, we put a ring structure on $R \oplus \mathcal{N}$ by setting $(r,n)\cdot(r',n') = (rr', rn' + r'n + nn')$. Thus Nil_R is equivalent to the category of augmented R-algebras with nilpotent augmentation ideals, and similarly for $\mathrm{Nil}_R^\wedge$.

(ii) An R-module M can be viewed as a nilpotent R-algebra by setting $M^2 = 0$; in this way we think of the category Mod_R of R-modules as a full subcategory of Nil_R.

(iii) The category Nil_R is naturally an abelian category. It is a full subcategory of $\mathrm{Nil}_R^\wedge$.

(iv) If $\mathcal{N}_1, \mathcal{N}_2 \in \mathrm{Nil}_R^\wedge$ and $f\colon \mathcal{N}_1 \to \mathcal{N}_2$ is an R-algebra homomorphism then $\mathcal{N}_1^r \subset f^{-1}(\mathcal{N}_2^r)$ for all $r \geqslant 1$, so f is continuous.

(v) A topologically nilpotent R-algebra is by definition an inverse limit of nilpotent R-algebras. Hence any functor $G\colon \mathrm{Nil}_R \to \mathrm{Ab}$ canonically extends to $\mathrm{Nil}_R^\wedge$ by setting

$$G(\mathcal{N}) = \varprojlim_r G(\mathcal{N}/\mathcal{N}^r).$$

Example 3.4. Let $\boldsymbol{X} = X_1, \ldots, X_g$ be indeterminates, and let $\mathcal{N}$ be the ideal $(\boldsymbol{X})R[\![\boldsymbol{X}]\!]$. Then $\mathcal{N}$ is a topologically nilpotent R-algebra, and for all $r \geqslant 1$ the quotient $\mathcal{N}/\mathcal{N}^r = (\boldsymbol{X})R[\![\boldsymbol{X}]\!]/(\boldsymbol{X})^r$ is a nilpotent R-algebra.

3.5. Let $\Lambda_R \in \mathrm{Nil}_R$ be the R-module R regarded as a nilpotent R-algebra, so $\Lambda_R \cong \varepsilon R[\varepsilon]/\varepsilon^2$.

Definition 3.6 (Zink [32, Definition 80]). A *finite-dimensional abelian formal group* over R is a functor G from Nil_R to the category Ab of abelian groups, satisfying:

(i) $G(0) = 0$,

(ii) G takes exact sequences of R-algebras to exact sequences of abelian groups,

(iii) G naturally commutes with arbitrary direct sums in Mod_R, and

(iv) the tangent space $t_G = G(\Lambda_R)$ is a finite free R-module.

A *morphism* of finite-dimensional abelian formal groups is a natural transformation of functors.

3.6.1. Property (iv) requires some explanation. Let $\mathcal{N}$ be an R-algebra such that $\mathcal{N}^2 = 0$. Multiplication by $r \in R$ induces an R-algebra endomorphism of $\mathcal{N}$, and hence an endomorphism of $G(\mathcal{N})$. The other axioms imply that this is an R-module structure on $G(\mathcal{N})$. In particular, t_G is naturally an R-module.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

3.6.2. In this paper, a *formal group over* R is a finite-dimensional abelian formal group over R in the above sense, unless specified otherwise. The *dimension* of G is the rank of t_G. We will implicitly extend such G to a functor on $\mathrm{Nil}_R^\wedge$ as in Remark 3.3 (v).

Remark 3.7. Zink in fact only requires that t_G be a (finitely generated) projective R-module. In the sequel we will assume that R is local, so all projective R-modules are free [**26**, Theorem 2.5].

3.8. There is a natural functor $\mathcal{A}$ from the category of formal Lie groups over R to the category of formal groups over R, defined as follows. Let $\mathfrak{G} = \mathrm{Spf}(A)$ be a formal Lie group, and let $G = \mathcal{A}(\mathfrak{G})\colon \mathrm{Nil}_R \to \mathrm{Ab}$ be the functor

$$G(\mathcal{N}) = \ker(\mathrm{Hom}_R(\mathrm{Spec}(R \oplus \mathcal{N}), \mathfrak{G}) \to \mathrm{Hom}_R(\mathrm{Spec}(R), \mathfrak{G})) = \mathrm{Hom}_R(I, \mathcal{N}),$$

where $R \oplus \mathcal{N}$ is the augmented R-algebra defined in Remark 3.3 (i) and I is the augmentation ideal of A. It is easily checked that G is a formal group over R, and moreover that there is a natural identification of R-modules $\mathrm{Lie}(\mathfrak{G}) \cong t_G$. Given a choice of parameters $\boldsymbol{X} = X_1, \dots, X_g$ for $A \cong R[\![\boldsymbol{X}]\!]$, let F be the formal group law on $R[\![\boldsymbol{X}]\!]$ defining the group structure on $\mathfrak{G}$. Then an element of $G(\mathcal{N})$ is a homomorphism $R[\![\boldsymbol{X}]\!] \to R \oplus \mathcal{N}$ such that the image of each X_i is contained in $\mathcal{N}$; hence $G(\mathcal{N}) \cong \mathcal{N}^{\oplus g}$, with $G(\mathcal{N})$ imposing the law of composition $(\boldsymbol{x}, \boldsymbol{y}) \mapsto F(\boldsymbol{x}, \boldsymbol{y})$ on $\mathcal{N}^{\oplus g}$ via this bijection.

Remark 3.9. Let G be a p-divisible formal group over a local ring R that is p-adically separated and complete, and let $\mathfrak{G}$ be the canonically associated formal Lie group such that $G \cong \mathfrak{G}[p^\infty]$ as in § 2.4. Then $\mathcal{A}(\mathfrak{G})$ is a formal group which is naturally associated with G; in later sections we will identify G with the formal group $\mathcal{A}(\mathfrak{G})$ without mentioning $\mathfrak{G}$.

3.10. By [**31**, II.2.32], $\mathfrak{G} \rightsquigarrow \mathcal{A}(\mathfrak{G})$ is an equivalence of categories. In other words, if G is a g-dimensional formal group then there is a formal group law F on $R[\![\boldsymbol{X}]\!]$ and a functorial isomorphism of abelian groups $G(\mathcal{N}) \cong \mathcal{N}^{\oplus g}$, where the group law on $\mathcal{N}^{\oplus g}$ is defined by F as above. In the sequel we will be given an explicit description of an (abstract) formal group G for which we will want to recover such a formal group law. The remainder of this section is devoted to the construction of a (non-canonical) formal Lie group $\mathfrak{G}$ such that $G \cong \mathcal{A}(\mathfrak{G})$ for a formal group G.

3.11. To motivate this construction, suppose that $G = \mathcal{A}(\mathfrak{G})$ for some formal Lie group $\mathfrak{G} = \mathrm{Spf}(A)$ over R. We can recover $\mathfrak{G}$ from G in the following way. Let $I \subset A$ be the augmentation ideal, let $I' = \prod_{i=1}^\infty \mathrm{Sym}^i(t_G^*)$, and let $A' = R \oplus I'$. We have a natural isomorphism $t_G^* := \mathrm{Hom}_R(t_G, R) \cong I/I^2$, and hence a (non-canonical) isomorphism of R-algebras $\alpha\colon I' \xrightarrow{\sim} I$. The choice of isomorphism α gives rise to functorial isomorphisms

$$\mathrm{Hom}_R(I', \mathcal{N}) \xrightarrow{\sim} \mathrm{Hom}_R(I, \mathcal{N}) = G(\mathcal{N}),$$

which recovers the structure of formal Lie group on $\mathrm{Spf}(A') \cong \mathfrak{G}$. Choosing a basis for t_G then gives a choice of parameters $A' \cong R[\![\boldsymbol{X}]\!]$, giving rise to a functorial isomorphism

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

of pointed sets $G(\mathcal{N}) \cong \mathcal{N}^{\oplus g}$. The formal group law F defining the group structure on $\mathfrak{G}$ can then be recovered by substituting $\mathcal{N} = (\boldsymbol{X}, \boldsymbol{Y})R[\![\boldsymbol{X}, \boldsymbol{Y}]\!]$ and calculating $F(\boldsymbol{X}, \boldsymbol{Y}) = \boldsymbol{X} +_{G(\mathcal{N})} \boldsymbol{Y} \in \mathcal{N}^{\oplus g}$.

Definition 3.12. Let G be a g-dimensional formal group, and let $I = \prod_{i=1}^{\infty} \mathrm{Sym}^i(t_G^*)$. A *choice of Hopf algebra* for G is functorial isomorphism of pointed sets

$$\mathrm{Hom}_{\mathrm{Nil}_R^\wedge}(I, \mathcal{N}) \xrightarrow{\sim} G(\mathcal{N}),$$

and *choice of parameters* for G is a functorial isomorphism of pointed sets

$$\mathcal{N}^{\oplus g} \xrightarrow{\sim} G(\mathcal{N}).$$

3.13. Let I be a choice of Hopf algebra for a formal group G, let $A = R \oplus I$, and let $\mathfrak{G} = \mathrm{Spf}(A)$. Then $\mathfrak{G}$ has a structure of formal Lie group such that $G \cong \mathcal{A}(\mathfrak{G})$, as in § 3.11. A choice of parameters for G is equivalent to a choice of Hopf algebra along with a choice of basis for t_G, which is in turn equivalent to a choice of parameters for $\mathfrak{G}$. Conversely, let $\mathfrak{G} = \mathrm{Spf}(A)$ be a formal Lie group, and let $I \subset A$ be the augmentation ideal. An isomorphism $I \cong \prod_{i=1}^{\infty} \mathrm{Sym}^i(I/I^2)$ gives rise to a choice of Hopf algebra for $G = \mathcal{A}(\mathfrak{G})$; this along with a choice of basis for I/I^2 gives rise to a choice of parameters for G. Since $\mathcal{A}$ is an equivalence of categories § 3.10, every formal group G admits a choice of Hopf algebra and a choice of parameters.

Example 3.14. If $\mathfrak{G} = \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ then a choice of parameters for $\mathcal{A}(\mathfrak{G})$ is equivalent to a choice of elements $\boldsymbol{Y} = Y_1, \ldots, Y_g \in (\boldsymbol{X})R[\![\boldsymbol{X}]\!]$ inducing an isomorphism $R[\![\boldsymbol{Y}]\!] \xrightarrow{\sim} R[\![\boldsymbol{X}]\!]$.

3.15. By Yoneda's lemma, any natural transformation of pointed set-valued functors $\mathrm{Hom}_{\mathrm{Nil}_R^\wedge}(I, \cdot) \to G$ is of the form $f \mapsto G(f)(\alpha)$ for a unique element $\alpha \in G(I)$. We will use the following criterion for a particular $\alpha \in G(I)$ to determine a choice of Hopf algebra.

Lemma 3.16. *With the notation in Definition 3.12, choose $\alpha \in G(I)$, and let $\Phi\colon \mathrm{Hom}_{\mathrm{Nil}_R^\wedge}(I, \cdot) \to G$ be the natural transformation $f \mapsto G(f)(\alpha)$. Then Φ is a choice of Hopf algebra for G if and only if the composite map*

$$\theta\colon t_G \cong \mathrm{Hom}_{\mathrm{Mod}_R}(t_G^*, R) = \mathrm{Hom}_{\mathrm{Nil}_R^\wedge}(I, R) \xrightarrow{\Phi} G(\Lambda_R) = t_G$$

is bijective.

Proof. Since G admits a choice of parameters, we may assume that $G(\mathcal{N}) = \mathrm{Hom}_{\mathrm{Nil}_R^\wedge}((\boldsymbol{X}), \mathcal{N})$, where $(\boldsymbol{X}) = (X_1, \ldots, X_g) \subset R[\![X_1, \ldots, X_g]\!]$. Using the identification of $(\boldsymbol{X})/(\boldsymbol{X})^2$ with t_G^*, we also identify I with $(\boldsymbol{X})$. Then $\alpha \in G(I) = \mathrm{Hom}_{\mathrm{Nil}_R^\wedge}((\boldsymbol{X}), (\boldsymbol{X}))$, and θ is a bijection if and only if the R-module endomorphism α_1 of $(\boldsymbol{X})/(\boldsymbol{X})^2$ induced by α is bijective. This is equivalent to α being an R-algebra automorphism of $(\boldsymbol{X})$. □

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

3.16.1. Let $\alpha_1 \in G(t_G^*)$ be the image of α under the quotient map $I \to t_G^*$, so $f \mapsto G(f)(\alpha_1)$ is a functorial isomorphism of R-algebras $\mathrm{Hom}_R(t_G^*, \mathcal{N}) \xrightarrow{\sim} G(\mathcal{N})$ when $\mathcal{N}^2 = 0$. The map θ in Lemma 3.16 only depends on α_1, so any $\alpha \in I$ lifting α_1 gives rise to a choice of Hopf algebra for G.

For completeness we remark that the functor $\mathcal{A}$ respects extension of scalars, in the following sense.

Definition 3.17. Let $\varphi\colon R \to R'$ be a ring homomorphism, and let G be a formal group over R. Define the *base change* $G_{R'}$ *of* G *to* R' to be the functor on $\mathrm{Nil}_{R'}$ defined by $G_{R'}(\mathcal{N}) = G(\mathcal{N})$, where we view a nilpotent R'-algebra $\mathcal{N}$ as a nilpotent R-algebra via φ.

3.17.1. Note that $G_{R'}$ is likewise a formal group over R'. If $G \cong \mathcal{A}(\mathfrak{G})$ for a formal Lie group $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ over R with formal group law F, then $\mathfrak{G}_{R'} := \mathfrak{G} \mathbin{\widehat{\otimes}_R} R'$ is a formal Lie group over R' with formal group law $\varphi(F)$, and $G_{R'} \cong \mathcal{A}(\mathfrak{G}_{R'})$.

4. A choice of parameters from a display

4.1. Displays. In this section, R is a p-adically complete and separated local ring. Recall from § 1.13.1 that $W(R)$ denotes the ring of p-Witt vectors over R and that $I_R = \ker(w_0) \subset W(R)$. A *display* over R consists of the data $\mathcal{P} = (P, Q, F, V^{-1})$, where P is a finite projective $W(R)$-module, $Q \subset P$ is a $W(R)$-submodule, and $F\colon P \to P$, $V^{-1}\colon Q \to P$ are ${}^{\mathrm{F}}$-linear maps, satisfying the following conditions.

(i) We can write P as a direct sum of projective $W(R)$-modules $P = T \oplus L$ such that $Q = I_R T \oplus L$.

(ii) The $W(R)$-linear map $W(R) \otimes_{W(R),{}^{\mathrm{F}}} Q \to P$ induced by V^{-1} is surjective.

(iii) For $x \in P$ and $w \in W(R)$, we have $V^{-1}({}^{\mathrm{V}}w)x) = wFx$.

It follows from (iii) that

$$Fy = V^{-1}({}^{\mathrm{V}}1y) = {}^{\mathrm{FV}}1V^{-1}y = pV^{-1}y \tag{4.1.1}$$

for $y \in Q$. A decomposition as in (i) is called a *normal decomposition** of P. The $W(R)$-rank of P is called the *height* of $\mathcal{P}$, and the R-rank of P/Q (or equivalently the $W(R)$-rank of T) is its *dimension*. There is an evident notion of morphism of displays, so we can speak of the category of displays over R.

4.1.2. A *nilpotent display* is a display that satisfies an additional nilpotence condition; see [**32**, Definitions 1, 11, 13]. Nilpotent displays correspond to connected p-divisible groups, so all displays in this paper will be assumed to be nilpotent.

* Be aware that Zink [**32**] writes a normal decomposition as $P = L \oplus T$, yet always chooses a basis $e_1, \dots, e_h$ for P such that $e_1, \dots, e_g$ is a basis for T and $e_{g+1}, \dots, e_h$ is a basis for L.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

4.2. By [**32**, Proposition 3], $W(R)$ is complete and separated in the I_R-adic topology. Hence I_R is contained in the Jacobson radical of $W(R)$, so the maximal ideals of $W(R)$ are the same as the maximal ideals of $W(R)/I_R = R$. Therefore, $W(R)$ is local ring, so any projective $W(R)$-module is free [**26**, Theorem 2.5]. This allows us to choose bases for our displays.

4.3. If R is a perfect ring of characteristic p then (nilpotent) displays over R and (covariant) Dieudonné modules over R such that V is topologically nilpotent are equivalent notions [**32**, Proposition 15]. In fact, if $\mathcal{P} = (P, Q, F, V^{-1})$ is a display over such a ring then V^{-1} has an ${}^{\mathrm{F}^{-1}}$-linear inverse $V\colon P \to Q$. When R is not a perfect ring of characteristic p then ${}^{\mathrm{F}}\colon W(R) \to W(R)$ is not an automorphism, and an operator V does not exist in general. Nonetheless it is helpful when doing calculations to think of displays as Dieudonné modules and V^{-1} as the inverse of V.

Example 4.4. The datum $\mathcal{G}_m = (W(R), {}^{\mathrm{V}}W(R), {}^{\mathrm{F}}, {}^{\mathrm{V}^{-1}})$ forms a display of height 1 and dimension 1. See [**32**, Example 16], as well as Examples 4.8 and 5.6.

4.5. Let $\mathcal{P}$ be a display over R and let $R \to R'$ be a homomorphism of p-adically separated and complete local rings. The display $\mathcal{P}_{R'} = (P_{R'}, Q_{R'}, F_{R'}, V_{R'}^{-1})$ obtained from $\mathcal{P}$ by base change is defined as follows (see [**32**, Definition 20]):

- $P_{R'} = W(R') \otimes_{W(R)} P$;
- $Q_{R'} = \ker[w_0 \otimes (\mathrm{proj})\colon W(R') \otimes_{W(R)} P \to R' \otimes_R (P/Q)] = \mathrm{im}[(W(R') \otimes_{W(R)} Q) \oplus (I_{R'} \otimes_{W(R)} P) \to P_{R'}]$;
- $F_{R'} = {}^{\mathrm{F}}(\cdot) \otimes F\colon P_{R'} \to P_{R'}$;
- $V_{R'}^{-1}\colon Q_{R'} \to P_{R'}$ is the unique ${}^{\mathrm{F}}$-linear homomorphism satisfying

$$V_{R'}^{-1}(w \otimes y) = {}^{\mathrm{F}}w \otimes V^{-1}y, \qquad V_{R'}^{-1}({}^{\mathrm{V}}w \otimes x) = w \otimes Fx \tag{4.5.1}$$

  for all $w \in W(R')$, $y \in Q$, and $x \in P$ (recall from § 1.13.1 that ${}^{\mathrm{V}}(W(R)) = \ker(w_0)$).

This sets up a functor from the category of displays over R to the category of displays over R'. Note that if $P = T \oplus L$ is a normal decomposition then

$$Q_{R'} = I_{R'}(W(R') \otimes_{W(R)} T) \oplus (W(R') \otimes_{W(R)} L).$$

Definition 4.6. If A is any ring and $\mathcal{N} \in \mathrm{Nil}_A$, we let $\hat{W}(\mathcal{N})$ denote the $W(A)$-algebra of finite-length Witt vectors: that is,

$$\hat{W}(\mathcal{N}) = \{(x_0, x_1, \dots)\colon x_n \in \mathcal{N},\ x_n = 0 \text{ for large enough } n\}.$$

We will view $\hat{W}$ as an infinite-dimensional formal group over A under addition of Witt vectors, as in [**18**, § 17.1.8]. If $\mathcal{N}$ is a nilpotent A-algebra and $x \in \mathcal{N}$, we denote by $[x]$ the Witt vector $(x, 0, 0, \dots) \in \hat{W}(\mathcal{N})$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

4.7. There is a functor $\mathrm{BT}\colon \mathcal{P} \rightsquigarrow \mathrm{BT}_{\mathcal{P}}$ from the category of (nilpotent) displays over a ring R as in § 4.1 to the category of p-divisible formal groups over R, which is an equivalence of categories [**25**, Theorem 1.1]. This functor is compatible with change of base and respects the notions of height and dimension. The p-divisible formal group $\mathrm{BT}_{\mathcal{P}}$ is given in terms of its corresponding formal group; it is constructed as follows. Suppose for the moment that $p^n R = 0$ for some $n \geqslant 1$. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, let $\mathcal{N}$ be a nilpotent R-algebra, and define

$$\hat{P}_{\mathcal{N}} = \hat{W}(\mathcal{N}) \otimes_{W(R)} P,$$
$$\hat{Q}_{\mathcal{N}} = \ker[w_0 \otimes (\mathrm{proj})\colon \hat{W}(\mathcal{N}) \otimes_{W(R)} P \to \mathcal{N} \otimes_R (P/Q)].$$

Let $R' = R \oplus \mathcal{N}$ be the augmented R-algebra as defined in Remark 3.3 (i). We can regard $\hat{Q}_{\mathcal{N}}$ (respectively $\hat{P}_{\mathcal{N}}$) as a submodule of the base change $Q_{R'}$ (respectively $P_{R'}$). As explained in [**32**, § 3.1], the map $V_{R'}^{-1}\colon Q_{R'} \to P_{R'}$ restricts to a map $V_{\mathcal{N}}^{-1}\colon \hat{Q}_{\mathcal{N}} \to \hat{P}_{\mathcal{N}}$. We define $\mathrm{BT}_{\mathcal{P}}(\mathcal{N})$ to be the cokernel of the map $V_{\mathcal{N}} - \mathrm{Id}\colon \hat{Q}_{\mathcal{N}} \to \hat{P}_{\mathcal{N}}$, where $\mathrm{Id}\colon \hat{Q}_{\mathcal{N}} \to \hat{P}_{\mathcal{N}}$ is the natural inclusion. By [**32**, Corollary 84] the sequence of abelian groups

$$0 \to \hat{Q}_{\mathcal{N}} \xrightarrow{V_{\mathcal{N}}^{-1} - \mathrm{Id}} \hat{P}_{\mathcal{N}} \to \mathrm{BT}_{\mathcal{P}}(\mathcal{N}) \to 0 \tag{4.7.1}$$

is exact on the left as well. We will often write V^{-1} for $V_{\mathcal{N}}^{-1}$ when it is unlikely to cause confusion.

Now suppose that p is not nilpotent in R. Let $\mathcal{P}$ be a display over R, let $R_n = R/p^{n+1}R$, let $\mathcal{P}_n$ be the base change of $\mathcal{P}$ to R_n, and let $\mathrm{BT}_{\mathcal{P}_n}$ be the associated p-divisible formal group. Then $\{\mathrm{BT}_{\mathcal{P}_n}\}_{n=1}^{\infty}$ is a compatible inverse system of p-divisible formal groups, so by [**27**, Lemma II.4.16] there is a unique p-divisible formal group over R whose base change to R_n is isomorphic to $\mathrm{BT}_{\mathcal{P}_n}$ for all n. We define $\mathrm{BT}_{\mathcal{P}}$ to be this p-divisible formal group. Concretely, given a choice of compatible systems of parameters $\boldsymbol{X} = X_1, \dots, X_g$ for the formal groups $\mathrm{BT}_{\mathcal{P}_n}$ (i.e. a choice of formal group laws F_n on $R_n[\![\boldsymbol{X}]\!]$ giving rise to $\mathrm{BT}_{\mathcal{P}_n}$ and such that $F_n = F_{n+1} \pmod{p^{n+1}}$ for all $n \geqslant 0$), the p-divisible formal group $\mathrm{BT}_{\mathcal{P}}$ is given by the formal group law $F = \lim F_n$ on $R[\![\boldsymbol{X}]\!]$.

Example 4.8. Suppose that p is nilpotent in R. Let $\mathcal{G}_m$ be the display from Example 4.4, and let $G = \mathrm{BT}_{\mathcal{G}_m}$. If $\mathcal{N}$ is a nilpotent R-algebra then

$$G(\mathcal{N}) = \hat{W}(\mathcal{N})/(V^{-1} - \mathrm{Id})^{\mathrm{V}}(\hat{W}(\mathcal{N})).$$

We claim that $G(\mathcal{N}) \cong (1 + \mathcal{N})^{\times} \subset (R \oplus \mathcal{N})^{\times}$. The Artin–Hasse exponential [**18**, § 17.5] is the power series

$$\mathrm{hexp}(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \frac{X^{p^3}}{p^3} + \cdots\right) \in 1 + \boldsymbol{Z}_{(p)}[\![X]\!].$$

Define a map $h\colon \hat{W}(\mathcal{N}) \to (1+\mathcal{N})^{\times}$ by $h(x_0, x_1, \dots) = \prod_{i=0}^{\infty} \mathrm{hexp}(x_i)$. Formally we have

$$h(x_0, x_1, \dots) = \exp\left(\sum_{i=0}^{\infty} \frac{w_n(x_0, x_1, \dots)}{p^n}\right),$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

so h is a group homomorphism. Then $h(V^{-1}x) = h(x)$ for $x \in {}^{\mathrm{V}}\hat{W}(\mathcal{N})$ since $V^{-1}(0, x_0, x_1, \dots) = (x_0, x_1, \dots)$, so h descends to a map $G(\mathcal{N}) \to (1+\mathcal{N})^\times$. Since hexp is an invertible power series, the map $y \mapsto h([y]) = \mathrm{hexp}(y) \colon \mathcal{N} \to (1+\mathcal{N})^\times$ is bijective, so by Proposition 4.9 below, h is an isomorphism. This shows that $G \cong \hat{\boldsymbol{G}}_m = \boldsymbol{\mu}_{p^\infty}$.

Proposition 4.9. *Suppose that p is nilpotent in R. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, let $P = T \oplus L$ be a normal decomposition, and let $e_1, \dots, e_g$ be a basis for T. The map*

$$(x_1, x_2, \dots, x_g) \mapsto [x_1] \otimes e_1 + [x_2] \otimes e_2 + \cdots + [x_g] \otimes e_g \mod (V_{\mathcal{N}}^{-1} - \mathrm{Id})\hat{Q}_{\mathcal{N}} \quad (4.9.1)$$

a functorial bijection of pointed sets $\mathcal{N}^{\oplus g} \xrightarrow{\sim} \mathrm{BT}_{\mathcal{P}}(\mathcal{N})$, i.e. it is a choice of parameters for $\mathrm{BT}_{\mathcal{P}}$.

4.9.2. To prove Proposition 4.9, we will make use of Zink's exp map, which is constructed as follows (still under the assumption that p is nilpotent in R). Let M be an R-module, thought of as a square-zero R-algebra, and let $R' = R \oplus M$, so M is identified with the augmentation ideal in R'. As in [**32**, § 1.4] (or as an exercise) one can show that if $w = (w_0, w_1, \dots) \in \hat{W}(M)$ then ${}^{\mathrm{F}}w = p(w_1, w_2, \dots)$. By (4.1.1) and (4.5.1), for $w \in \hat{W}(M)$ and $y \in Q$ we have

$$V_M^{-1}(w \otimes y) = {}^{\mathrm{F}}w \otimes V^{-1}y = (w_1, w_2, \dots) \otimes p \cdot V^{-1}y = (w_1, w_2, \dots) \otimes Fy,$$

and for $x \in P$,

$$V_M^{-1}({}^{\mathrm{V}}w \otimes x) = V_M^{-1}((0, w_0, w_1, \dots) \otimes x) = (w_0, w_1, \dots) \otimes Fx.$$

Hence it is natural to extend V_M^{-1} to an endomorphism of $\hat{P}_M = \hat{W}(M) \otimes_{W(R)} P$ by the formula

$$V_M^{-1}((w_0, w_1, \dots) \otimes x) = (w_1, w_2, \dots) \otimes Fx \quad (4.9.3)$$

(compare Lemma 38 and the proof of Lemma 83 in [**32**]). Define a functorial homomorphism

$$\exp \colon M \otimes_R (P/Q) \to \mathrm{BT}_{\mathcal{P}}(M)$$

via the commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \hat{Q}_M & \longrightarrow & \hat{W}(M) \otimes_{W(R)} P & \xrightarrow{w_0 \otimes (\mathrm{proj})} & M \otimes_R (P/Q) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle V_M^{-1} - \mathrm{Id}} & & \downarrow{\scriptstyle \exp} & & \\
0 & \longrightarrow & \hat{Q}_M & \xrightarrow{V_M^{-1} - \mathrm{Id}} & \hat{W}(M) \otimes_{W(R)} P & \longrightarrow & \mathrm{BT}_{\mathcal{P}}(M) & \longrightarrow & 0
\end{array}$$

Zink [**32**, Proof of Theorem 81] shows that exp is an R-linear isomorphism.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

4.10. Proof of Proposition 4.9. Let $G = \mathrm{BT}_{\mathcal{P}}$ (so $t_G = \mathrm{BT}_{\mathcal{P}}(\Lambda_R)$), and let $I = \prod_{i=1}^{\infty} \mathrm{Sym}^i(t_G^*)$. Let $\bar{e}_i \in P/Q$ be the residue of e_i, so $\bar{e}_1, \dots, \bar{e}_g$ is an R-basis for P/Q, and hence $\exp(\bar{e}_1), \dots, \exp(\bar{e}_g)$ form a basis of t_G. Let $\varepsilon_1, \dots, \varepsilon_g \in t_G^*$ be the dual basis, and let

$$\bar{\alpha}_1 = \varepsilon_1 \otimes \bar{e}_1 + \varepsilon_2 \otimes \bar{e}_2 + \cdots + \varepsilon_g \otimes \bar{e}_g \in t_G^* \otimes_R (P/Q).$$

Then for $x = \sum_{i=1}^{g} a_i \bar{e}_i \in P/Q$, if $\mathrm{ev}_x \colon t_G^* \to R$ denotes the evaluation map at $\exp(x) \in t_G$, we have

$$(\mathrm{ev}_x \otimes \mathrm{Id})\biggl(\sum_{i=1}^{g} \varepsilon_i \otimes \bar{e}_i \biggr) = \sum_{i=1}^{g} \varepsilon_i(\exp(x))\bar{e}_i = \sum_{i=1}^{g} a_i \bar{e}_i = x.$$

Let $\alpha_1 = \exp(\bar{\alpha}_1) \in G(t_G^*)$. By Lemma 3.16 and the above calculation, any lift of α_1 to $G(I)$ determines a choice of Hopf algebra for G.

Next we calculate a lift $\tilde{\alpha}_1$ of α_1 to $\hat{W}(t_G^*) \otimes_{W(R)} P$ using the commutative square

$$\begin{array}{ccc} \hat{W}(t_G^*) \otimes_{W(R)} P & \longrightarrow & t_G^* \otimes_R (P/Q) \\ \Big\downarrow{\scriptstyle V^{-1}-\mathrm{Id}} & & \Big\downarrow{\scriptstyle \exp}\cong \\ \hat{W}(t_G^*) \otimes_{W(R)} P & \longrightarrow & G(t_G^*) \end{array}$$

Let

$$\tilde{\alpha}_1 = -([\varepsilon_1] \otimes e_1 + [\varepsilon_2] \otimes e_2 + \cdots + [\varepsilon_g] \otimes e_g) \in \hat{W}(t_G^*) \otimes_{W(R)} P.$$

By construction, $\tilde{\alpha}_1$ lifts $-\bar{\alpha}_1$ under the quotient map $\hat{W}(t_G^*) \otimes_{W(R)} P \twoheadrightarrow t_G^* \otimes_R (P/Q)$, so $(V^{-1} - \mathrm{Id})(-\tilde{\alpha}_1)$ lifts α_1. But $V^{-1}((\varepsilon_i, 0, 0, \dots) \otimes e_i) = 0$ by (4.9.3), so $V^{-1}\tilde{\alpha}_1 = 0$. Therefore, $\tilde{\alpha}_1 = (V^{-1} - \mathrm{Id})(-\tilde{\alpha}_1)$ lifts α_1.

Using Remark 3.3 (v) to extend G and $\hat{W}$ to functors on the category $\mathrm{Nil}_R^{\wedge}$, we have

$$\hat{W}(I) = \{(x_0, x_1, x_2, \dots) \in W(I) \colon x_n \to 0 \text{ as } n \to \infty\}$$

and a natural map $\varphi \colon \hat{W}(I) \otimes_{W(R)} P \to G(I)$. Using the inclusion $t_G^* \hookrightarrow I$ to view $\hat{W}(t_G^*)$ (respectively $G(t_G^*)$) as a subgroup of $\hat{W}(I)$ (respectively $G(I)$), if

$$\tilde{\alpha} = -([\varepsilon_1] \otimes e_1 + \cdots + [\varepsilon_g] \otimes e_g) \in \tilde{W}(I) \otimes_{W(R)} P$$

we see that $\alpha := \varphi(\tilde{\alpha}) \in G(I)$ lifts α_1 because $\tilde{\alpha}$ lifts $\tilde{\alpha}_1$. Therefore, α determines a choice of Hopf algebra for G, so by the results of § 3, for any nilpotent R-algebra $\mathcal{N}$ the map

$$f \mapsto G(f)(\alpha) \colon \mathrm{Hom}_{\mathrm{Nil}_R^{\wedge}}(I, \mathcal{N}) \to G(\mathcal{N})$$

is a bijection of pointed sets. Since $G(f)(\alpha)$ is the image of

$$(\tilde{W}(f) \otimes \mathrm{Id})(\tilde{\alpha}) = (\tilde{W}(f) \otimes \mathrm{Id})\biggl(-\sum_{i=1}^{g} [\varepsilon_i] \otimes e_i \biggr) = -\sum_{i=1}^{g} [f(\varepsilon_i)] \otimes e_i \in \hat{W}(\mathcal{N}) \otimes_{W(R)} P$$

in $G(\mathcal{N})$, we have that the map

$$(x_1, \dots, x_g) \mapsto \sum_{i=1}^{g} [x_i] \otimes e_i \mod (V_{\mathcal{N}}^{-1} - \mathrm{Id})\hat{Q}_{\mathcal{N}} \colon \mathcal{N}^{\oplus g} \xrightarrow{\sim} G(\mathcal{N})$$

is a bijection. □

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

4.11. Now suppose that p is not necessarily nilpotent in R, and let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R. We would like an analogue of Proposition 4.9 for $\mathcal{P}$, which is not generally true as stated in this context since the associated p-divisible formal group is not constructed in the same way.

Remark 4.12. Let $\mathcal{N}$ be a nilpotent R-algebra such that the natural map $\mathcal{N} \to \varprojlim_n \mathcal{N}/p^n\mathcal{N}$ is an isomorphism, and define

$$\tilde{W}(\mathcal{N}) = \varprojlim_n \hat{W}(\mathcal{N}/p^n\mathcal{N}) = \{(x_0, x_1, x_2, \dots) \in W(\mathcal{N})\colon x_i \to 0\},$$

where the convergence is taken in the p-adic topology. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, and set

$$\begin{aligned}\tilde{P}_{\mathcal{N}} &= \tilde{W}(\mathcal{N}) \otimes_{W(R)} P,\\ \tilde{Q}_{\mathcal{N}} &= \ker[w_0 \otimes (\mathrm{proj})\colon \tilde{W}(\mathcal{N}) \otimes_{W(R)} P \to \mathcal{N} \otimes_R (P/Q)].\end{aligned}$$

With some work one can show that $\mathrm{BT}_{\mathcal{P}}(\mathcal{N})$ is naturally isomorphic to $\tilde{P}_{\mathcal{N}}/(V^{-1} - \mathrm{Id})\tilde{Q}_{\mathcal{N}}$. With a great deal of work one can even prove an analogous formula for $\mathcal{N}[p^{-1}]$ in place of $\mathcal{N}$ when $\mathcal{N}$ has no p-torsion. As we do not need these refinements, we will not say more about them here.

4.13. Let $P = T \oplus L$ be a normal decomposition, let $e_1, \dots, e_g$ be a $W(R)$-basis for T, and let $e_{g+1}, \dots, e_h$ be a $W(R)$-basis for L. Let $\mathcal{N}$ be a nilpotent R-algebra such that $p^n\mathcal{N} = 0$ for some n. Our choice of basis allows us to identify $\hat{P}_{\mathcal{N}}$ with $\hat{W}(\mathcal{N})^{\oplus h}$ and $\hat{Q}_{\mathcal{N}}$ with the subgroup ${}^{\mathrm{V}}(\hat{W}(\mathcal{N}))^{\oplus g} \oplus \hat{W}(\mathcal{N})^{\oplus(h-g)}$; under these identifications the exact sequence (4.7.1) becomes an exact sequence

$$0 \to {}^{\mathrm{V}}\hat{W}(\mathcal{N})^{\oplus g} \oplus \hat{W}(\mathcal{N})^{\oplus(h-g)} \xrightarrow{V_{\mathcal{N}}^{-1} - \mathrm{Id}} \hat{W}(\mathcal{N})^{\oplus h} \to \mathrm{BT}_{\mathcal{P}}(\mathcal{N}) \to 0,$$

which is functorial in $\mathcal{N}$. It is not hard to show that the above sequence uniquely extends to a diagram of homomorphisms of formal groups over R (i.e. of functors $\mathrm{Nil}_R \to \mathrm{Ab}$)

$${}^{\mathrm{V}}\hat{W}^{\oplus g} \oplus \hat{W}^{\oplus(h-g)} \xrightarrow{V^{-1} - \mathrm{Id}} \hat{W}^{\oplus h} \xrightarrow{\pi} \mathrm{BT}_{\mathcal{P}} \tag{4.13.1}$$

whose composite is zero.

Theorem 4.14. *Let R be a p-adically complete and separated local ring. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, let $P = T \oplus L$ be a normal decomposition, let $e_1, \dots, e_g$ be a $W(R)$-basis for T, and let $e_{g+1}, \dots, e_h$ be a $W(R)$-basis for L. Let $\pi\colon \hat{W}^{\oplus h} \to \mathrm{BT}_{\mathcal{P}}$ be the homomorphism (4.13.1) determined by our choice of basis. For a nilpotent R-algebra $\mathcal{N}$, the map*

$$(x_1, \dots, x_g) \mapsto \pi([x_1], \dots, [x_g], 0, \dots, 0)\colon \mathcal{N}^{\oplus g} \to \mathrm{BT}_{\mathcal{P}}(\mathcal{N}) \tag{4.14.1}$$

is a choice of parameters for $\mathrm{BT}_{\mathcal{P}}$ in the sense of Definition 3.12.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Proof. For $n \geqslant 0$ let $R_n = R/p^{n+1}R$ and let $\mathcal{P}_n$ be the base change to R_n. When $p^{n+1}\mathcal{N} = 0$ for some n (i.e. $\mathcal{N}$ is an R_n-algebra), the map (4.14.1) agrees with the bijection (4.9.1) after identifying $\mathrm{BT}_{\mathcal{P}}(\mathcal{N})$ with $\mathrm{BT}_{\mathcal{P}_n}(\mathcal{N})$. If G is any formal group over R then a choice of parameters for G is equivalent to a compatible system of choices of parameters for the formal groups G_{R_n}, so our basis does give rise to a choice of parameters for $\mathrm{BT}_{\mathcal{P}}$. Furthermore, a functorial map $\mathcal{N}^{\oplus g} \to G(\mathcal{N})$ is determined by its behaviour on nilpotent algebras $\mathcal{N}$ such that $p^{n+1}\mathcal{N} = 0$ for some n (in fact one only needs to consider $\mathcal{N}$ of the form $(X_1, \dots, X_g)R_n[\![X_1, \dots, X_g]\!]/(X_1, \dots, X_g)^m$), so (4.14.1) agrees with the choice of parameters for $\mathrm{BT}_{\mathcal{P}}$ induced by our basis. □

4.15. In choosing a basis for a display $\mathcal{P}$ over R, we will implicitly make the corresponding choice of parameters for $\mathrm{BT}_{\mathcal{P}}$ given by Theorem 4.14.

5. The logarithm of a display

5.1. In this section R is a complete rank-1 valuation ring of mixed characteristic $(0, p)$ with field of fractions K. Fix a display $\mathcal{P} = (P, Q, F, V^{-1})$ over R, a normal decomposition $P = T \oplus L$ (so $Q = I_R T \oplus L$), and $W(R)$-bases $e_1, \dots, e_g$ for T and $e_{g+1}, \dots, e_h$ for L. Let $G = \mathrm{BT}_{\mathcal{P}}$ be the formal group over R associated with $\mathcal{P}$. With respect to our basis the ${}^{\mathrm{F}}$-linear maps $F\colon P \to P$ and $V^{-1}\colon Q \to P$ are determined by formulae

$$\left.\begin{aligned} Fe_j &= \sum_{i=1}^{h} \alpha_{ij} e_i, \quad j = 1, \dots, g, \\ V^{-1}e_j &= \sum_{i=1}^{h} \alpha_{ij} e_i, \quad j = g+1, \dots, h, \end{aligned}\right\} \tag{5.1.1}$$

for $\alpha_{ij} \in W(R)$. The matrix $M = (\alpha_{ij}) \in \mathrm{M}_h(W(R))$ is called the *structure matrix* for $\mathcal{P}$ with respect to $e_1, \dots, e_h$; its determinant $\det(M)$ is a unit in $W(R)$ by [**32**, Lemma 9].

5.1.2. In terms of the structure matrix M, the map $V^{-1}\colon {}^{\mathrm{V}}\hat{W}^{\oplus g} \oplus \hat{W}^{\oplus(h-g)} \to \hat{W}^{\oplus h}$ of (4.13.1) is given by

$$V^{-1}({}^{\mathrm{V}}x_1, \dots, {}^{\mathrm{V}}x_g, x_{g+1}, \dots, x_h) = M(x_1, \dots, x_g, {}^{\mathrm{F}}x_{g+1}, \dots, {}^{\mathrm{F}}x_h)^{\mathrm{t}}$$

for $\mathcal{N} \in \mathrm{Nil}_R$ and $x_1, \dots, x_h \in \hat{W}(\mathcal{N})$; here we are using the relation $V^{-1}(({}^{\mathrm{V}}x_i) \otimes e_i) = x_i \otimes Fe_i \in \hat{P}_{\mathcal{N}}$ for $1 \leqslant i \leqslant g$ (see (4.5.1)).

Notation 5.2. If $A = (\beta_{ij})$ is a matrix with coefficients in $W(R)$, we write $w_n(A)$ for the matrix over R whose entries are $w_n(\beta_{ij})$. Note that $w_n(AB) = w_n(A)w_n(B)$ since w_n is a ring homomorphism.

5.3. By [**18**, Corollary 11.1.6], the g-dimensional formal group G_K over the field K of characteristic zero is isomorphic (as a formal group) to the formal additive group $\hat{\boldsymbol{G}}_{a,K}^{\oplus g}$; this isomorphism is unique if we require (as we may) that a choice of parameters for G_K

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

map to the standard parameters for $\hat{\boldsymbol{G}}_{a,K}^{\oplus g}$. We call such an isomorphism $G_K \xrightarrow{\sim} \hat{\boldsymbol{G}}_{a,K}^{\oplus g}$ a *logarithm*. After making a choice of parameters, we can view the logarithm as a collection of g power series $\log_1, \ldots, \log_g$ in g variables with entries in K. The valuations of the coefficients of the logarithm will be important in the sequel; we will now calculate these coefficients in terms of the structure coefficients α_{ij} from (5.1.1).

5.4. Let $\log = (\log_1, \ldots, \log_g) \colon G_K \xrightarrow{\sim} \hat{\boldsymbol{G}}_{a,K}^{\oplus g}$ be the unique logarithm mapping the ith parameter provided by Theorem 4.14 and our choice of basis $e_1, \ldots, e_h$ for P to the ith standard parameter. We will denote by $\mathbf{log}$ the composition of log with the map $\pi \colon \hat{W}^{\oplus h} \to G_K$ from (4.13.1). We can think of $\mathbf{log}$ as a $g \times h$ matrix of homomorphisms $\log_{ij} \colon \hat{W} \to \hat{\boldsymbol{G}}_{a,K}$: that is,

$$\mathbf{log}(x_1, \ldots, x_h) = \left(\sum_{j=1}^{h} \log_{1j}(x_j), \ldots, \sum_{j=1}^{h} \log_{gj}(x_j) \right)$$

for a nilpotent R-algebra $\mathcal{N}$ and elements $x_1, \ldots, x_h \in \hat{W}(\mathcal{N})$. It is a basic theorem of Cartier theory ('Cartier's first theorem', [**18**, Theorem 27.7.5]) that $\hat{W}$ represents the 'formal curves functor' for a formal group. What this means concretely in the case of $\hat{\boldsymbol{G}}_{a,K}$ is that if $f \colon \hat{W} \to \hat{\boldsymbol{G}}_{a,K}$ is a homomorphism of formal groups then there are uniquely determined $a_n \in K$ such that $f(x) = \sum_{n=0}^{\infty} a_n w_n(x)$ for all nilpotent R-algebras $\mathcal{N}$ and all $x \in \hat{W}(\mathcal{N})$ (this is a finite sum because for all $x \in \hat{W}(\mathcal{N})$ we have $w_n(x) = 0$ when $n \gg 0$). Hence we may write $\log_{ij}(x) = \sum_{n=0}^{\infty} a_{n,ij} w_n(x)$. Letting $\boldsymbol{a}_n$ be the $g \times h$ matrix $(a_{n,ij})$, we have

$$\mathbf{log}(x_1, \ldots, x_h) = \sum_{n=0}^{\infty} \boldsymbol{a}_n \begin{bmatrix} w_n(x_1) \\ \vdots \\ w_n(x_h) \end{bmatrix}. \tag{5.4.1}$$

In terms of the formal group parameters $(y_1, \ldots, y_g) \mapsto \pi([y_1], \ldots, [y_g], 0, \ldots, 0)$ on G (and hence on G_K) provided by Theorem 4.14, we have

$$\begin{aligned} \log(y_1, \ldots, y_g) &= \mathbf{log}([y_1], \ldots, [y_g], 0, \ldots, 0) \\ &= \sum_{j=1}^{g} (\log_{1j}([y_j]), \ldots, \log_{gj}([y_j])) \\ &= \sum_{n=0}^{\infty} \sum_{j=1}^{g} (a_{n,1j} y_j^{p^n}, \ldots, a_{n,gj} y_j^{p^n}) \quad \text{since } w_n([y_j]) = y_j^{p^n} \\ &= \sum_{n=0}^{\infty} \boldsymbol{a}_n (y_1^{p^n}, \ldots, y_g^{p^n}, 0, \ldots, 0)^{\mathrm{t}}. \end{aligned}$$

In particular, since $\log(y) = y + O(y^2)$ we have that $a_{0,ij} = \delta_{ij}$ for $1 \leqslant i, j \leqslant g$.

5.5. By (4.13.1), the image of

$$V^{-1} - \mathrm{Id} \colon {}^{\mathrm{V}}\hat{W}^{\oplus g} \oplus \hat{W}^{\oplus (h-g)} \to \hat{W}^{\oplus h}$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

is contained in the kernel of **log**. Hence for every nilpotent K-algebra $\mathcal{N}$ and all $x, y \in \hat{W}(\mathcal{N})$, we have

$$\left.\begin{aligned}\mathbf{log}((^{\mathrm{V}}x)\boldsymbol{e}_i) = \mathbf{log}(V^{-1}((^{\mathrm{V}}x)\boldsymbol{e}_i)) = \mathbf{log}(xF\boldsymbol{e}_i) = \mathbf{log}(xM\boldsymbol{e}_i),\\ \mathbf{log}(y\boldsymbol{e}_j) = \mathbf{log}(V^{-1}(y\boldsymbol{e}_j)) = \mathbf{log}((^{\mathrm{F}}y)V^{-1}\boldsymbol{e}_j) = \mathbf{log}((^{\mathrm{F}}y)M\boldsymbol{e}_j)\end{aligned}\right\} \tag{5.5.1}$$

for $i = 1, \dots, g$ and $j = g+1, \dots, h$, where $\boldsymbol{e}_i$ is the ith standard basis vector in $W(R)^{\oplus h}$. Expanding **log** using (5.4.1), the left-hand sides of (5.5.1) are

$$\begin{aligned}\mathbf{log}((^{\mathrm{V}}x)\boldsymbol{e}_i) &= \sum_{n=0}^{\infty} w_n(^{\mathrm{V}}x)\boldsymbol{a}_n\boldsymbol{e}_i = \sum_{n=1}^{\infty} pw_{n-1}(x)\boldsymbol{a}_n\boldsymbol{e}_i,\\ \mathbf{log}(y\boldsymbol{e}_j) &= \sum_{n=0}^{\infty} w_n(y)\boldsymbol{a}_n\boldsymbol{e}_j\end{aligned}$$

and the right-hand sides of (5.5.1) are

$$\begin{aligned}\mathbf{log}(xM\boldsymbol{e}_i) &= \sum_{n=0}^{\infty} w_n(x)\boldsymbol{a}_n w_n(M)\boldsymbol{e}_i,\\ \mathbf{log}((^{\mathrm{F}}y)M\boldsymbol{e}_j) &= \sum_{n=0}^{\infty} w_{n+1}(y)\boldsymbol{a}_n w_n(M)\boldsymbol{e}_j.\end{aligned}$$

Therefore,

$$\left.\begin{aligned}\sum_{n=1}^{\infty} pw_{n-1}(x)\boldsymbol{a}_n\boldsymbol{e}_i = \sum_{n=0}^{\infty} w_n(x)\boldsymbol{a}_n w_n(M)\boldsymbol{e}_i,\\ \sum_{n=0}^{\infty} w_n(y)\boldsymbol{a}_n\boldsymbol{e}_j = \sum_{n=0}^{\infty} w_{n+1}(y)\boldsymbol{a}_n w_n(M)\boldsymbol{e}_j.\end{aligned}\right\} \tag{5.5.2}$$

As these equalities hold for all $\mathcal{N}$, they are in fact equalities of tuples of power series in the Witt coordinates of x and y. Examining the equation

$$w_n(x_0, x_1, \dots) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^{n-1}x_{n-1}^p + p^n x_n,$$

we see that the sets of monomials appearing in the polynomials $w_n(x_0, x_1, \dots)$ and $w_{n'}(x_0, x_1, \dots)$ are disjoint when $n \neq n'$. Thus we may separate the sums in (5.5.2) to obtain:

$$\begin{aligned}pw_n(x)\boldsymbol{a}_{n+1}\boldsymbol{e}_i &= w_n(x)\boldsymbol{a}_n w_n(M)\boldsymbol{e}_i,\\ w_{n+1}(y)\boldsymbol{a}_{n+1}\boldsymbol{e}_j &= w_{n+1}(y)\boldsymbol{a}_n w_n(M)\boldsymbol{e}_j,\\ \boldsymbol{a}_0\boldsymbol{e}_j &= 0,\end{aligned}$$

for all $n \geqslant 0$, $1 \leqslant i \leqslant g$ and $g+1 \leqslant j \leqslant h$. Cancelling the $w_n(x)$ and $w_{n+1}(y)$, and recalling that $a_{0,ij} = \delta_{ij}$ for $1 \leqslant i, j \leqslant g$, we obtain the fundamental recursive equation:

$$\left.\begin{aligned}\boldsymbol{a}_0 &= [I_g \;\; 0],\\ \boldsymbol{a}_{n+1} &= \boldsymbol{a}_n w_n(M)\boldsymbol{p}^{-1},\end{aligned}\right\} \tag{5.5.3}$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

where I_g is the identity matrix and $\boldsymbol{p}$ is the $h \times h$ diagonal matrix whose diagonal entries are $(p, p, \dots, p, 1, \dots, 1)$ (g entries are p). Note that (5.5.3) uniquely determines $\mathbf{log}$ in terms of the structure matrix M of $\mathcal{P}$ with respect to $e_1, \dots, e_h$.

Example 5.6. Let $\mathcal{G}_m$ be the display from Examples 4.4 and 4.8. Its structure matrix is $M = (1)$ with respect to the canonical basis $e_1 = 1$ of $P = W(R)$, so by (5.5.3), its logarithm is

$$\log(x) = x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \frac{x^{p^3}}{p^3} + \cdots .$$

We recognize this as the p-typical logarithm for the formal group $\hat{\boldsymbol{G}}_m$, in the sense of [**18**, § 16.3]. This means that $\mathrm{hexp} = \exp \circ \log \colon \mathrm{BT}_{\mathcal{G}_m} \to \hat{\boldsymbol{G}}_m$ is an isomorphism of formal groups defined over R, as in Example 4.8.

6. The rigid generic fibre of a p-divisible formal group

6.1. In this section we give a geometric interpretation of a p-divisible formal group G, and in particular of the kernel of its logarithm. We also derive the well-known fact that $\ker(\log) = G[p^\infty]$, in an appropriate geometric sense.

6.2. Let K be a field of characteristic zero that is complete with respect to a non-Archimedean valuation $\mathrm{ord} \colon K \to \boldsymbol{R} \cup \{\infty\}$ satisfying $\mathrm{ord}(p) = 1$. Let $|x| = p^{-\mathrm{ord}(x)}$ be the associated absolute value. Let R be the ring of integers in K and let k be its residue field. It is convenient at this point to set our notation involving rigid geometry; our primary reference for rigid K-analytic spaces is [**5**].

Notation 6.3. Let $|K^\times| = \{|x| \colon x \in K^\times\}$ be the *value group* of K, and let

$$\sqrt{|K^\times|} = |\bar{K}^\times| = \{x \in \boldsymbol{R}_{>0} \colon x^n \in |K^\times| \text{ for some } n\},$$

where $\bar{K}$ is an algebraic closure of K. For $\rho \in \sqrt{|K^\times|}$ we define

$$T_{K,g,\rho} = T_{g,\rho} = \Big\{ \sum a_\nu X^\nu \in K[\![X_1, \dots, X_g]\!] \colon |a_\nu| \rho^{|\nu|} \to 0 \text{ as } |\nu| \to \infty \Big\}$$

(we omit K from the notation when the ground field is clear from the context), which is equipped with the norm $|\sum a_\nu X^\nu|_\rho = \max\{|a_\nu| \rho^{|\nu|}\}$, where $|\nu| = \nu_1 + \cdots + \nu_g$. The associated affinoid space is the closed g-ball of radius ρ, and is denoted $\boldsymbol{B}^g_K(\rho) = \mathrm{Sp}(T_{K,g,\rho})$. Likewise we set $\boldsymbol{D}^g_K(\rho) = \bigcup_{\mu < \rho} \boldsymbol{B}^g_K(\mu)$, the open ball of radius ρ. For brevity we write $T_g = T_{K,g} = T_{K,g,1}$, $\boldsymbol{B}^g_K = \boldsymbol{B}^g_K(1)$ and $\boldsymbol{D}^g_K = \boldsymbol{D}^g_K(1)$.

If $\mathscr{X}$ is a rigid space and $x \in \mathscr{X}$ is a point then we denote the residue field at x by $\kappa(x)$; this is a finite extension of K.

6.4. Let G be a p-divisible formal group over R of height h and dimension $g > 0$, and let $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ (where $\boldsymbol{X} = X_1, \dots, X_g$) be the associated formal Lie group over R with $G \cong \mathfrak{G}[p^\infty] = \{\mathfrak{G}[p^n]\}_{n \in \boldsymbol{N}}$. In particular, $G[p^n] \cong \mathfrak{G}[p^n] = \mathrm{Spec}(A_n)$, where $A_n = R[\![\boldsymbol{X}]\!]/[p^n](\boldsymbol{X})$ is a free R-module of rank p^{nh}. Let F be the formal group

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

law on $R[\![\boldsymbol{X}]\!]$ determining the group structure on $\mathfrak{G}$. Let $\mathscr{G} = \boldsymbol{D}_K^g$, and endow $\mathscr{G}$ with the structure of K-analytic group via the convergent power series F. We call $\mathscr{G}$ the *rigid generic fibre* of G (with respect to a choice of parameters for G). The p^n-torsion $\mathscr{G}[p^n]$ is the closed analytic subspace of $\mathscr{G}$ defined by the equations $[p^n](\boldsymbol{X})$. For any $\rho \in \sqrt{|K^\times|}$, $0 < \rho < 1$, the natural inclusion $R[\![\boldsymbol{X}]\!] \to T_{g,\rho}$ induces a homomorphism $K \otimes_R A_n \to T_{g,\rho}/[p^n](\boldsymbol{X})$, whence we obtain a natural morphism of K-analytic groups $\mathscr{G}[p^n] \cap \boldsymbol{B}_K^g(\rho) \to G[p^n] \otimes_R K$. Passing to the direct limit, we have a natural morphism $\mathscr{G}[p^n] \to G[p^n] \otimes_R K$.

Lemma 6.5. *The natural map $\mathscr{G}[p^n] \to G[p^n] \otimes_R K$ of finite (étale) K-analytic groups is an isomorphism for all $n \geqslant 1$.*

Proof. For $\xi \in G[p^n](\bar{K})$ let $\xi_i = X_i(\xi) \in \bar{K}$. Since A_n is local, we have $|\xi_i| < 1$. Let $\rho \in \sqrt{|K^\times|}$, $0 < \rho < 1$, be such that $|\xi_i| \leqslant \rho$ for all $\xi \in G[p^n](\bar{K})$. Let x_i be the image of X_i under the quotient map $R[\![\boldsymbol{X}]\!] \to A_n$, and define a homomorphism $T_{g,\rho} \to K \otimes_R A_n$ by $\sum a_\nu X^\nu \mapsto \sum a_\nu x^\nu$. This is well defined because $K \otimes_R A_n \cong \prod K_i$ is a product of finite field extensions K_i of K, and by the above the series $\sum a_\nu x^\nu$ converges in each K_i. Thus we obtain a map $T_{g,\rho}/[p^n](\boldsymbol{X}) \to K \otimes_R A_n$, which is easily seen to be inverse to the natural map defining the morphism $\mathscr{G}[p^n] \cap \boldsymbol{B}_K^g(\rho) \to G[p^n] \otimes_R K$. □

Remark 6.6. Suppose that the valuation on K is discrete. Then Berthelot has defined a 'rigid generic fibre' functor $\mathfrak{X} \rightsquigarrow \mathfrak{X}_{\mathrm{rig}}$ from the category of locally noetherian adic formal schemes $\mathfrak{X}$ over $\mathrm{Spf}(R)$ whose reduction is a scheme locally of finite type over $\operatorname{Spec} k$, to the category of rigid analytic spaces over K; this is explained in [**12**, § 7]. In this case $\mathscr{G}$ is identified with $\mathfrak{G}_{\mathrm{rig}}$, and Lemma 6.5 follows from the fact that Berthelot's functor is compatible with fibre products.

Using Berthelot's functor, it is not necessary to choose parameters for $\mathfrak{G}$ in order to define $\mathscr{G}$. We prefer to use an ad-hoc construction in this case instead of imposing noetherian hypotheses on R, especially since we will need to choose parameters for $\mathfrak{G}$ in § 7.

6.7. By Lemma 6.5, $\mathscr{G}[p^n]$ is a finite étale K-analytic group of order p^{nh}. The following proposition relates the logarithm from § 5 with $\mathscr{G}[p^\infty] := \bigcup_{n=1}^\infty \mathscr{G}[p^n]$ when G comes from a display.

Proposition 6.8. *Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, let $P = T \oplus L$ be a normal decomposition, and choose bases for T and L. Let $\log\colon G_K \xrightarrow{\sim} \hat{\boldsymbol{G}}_{a,K}^{\oplus g}$ be the logarithm of $G = \mathrm{BT}_{\mathcal{P}}$ with respect to the induced choice of parameters for G, as in § 5. Let F be the formal group law for G and let $\mathscr{G}$ be its rigid generic fibre, as above.*

The g-tuple of power series $\log = (\log_1, \dots, \log_g)$ converges on the analytic open unit ball $\boldsymbol{D}_K^g$ and defines a homomorphism $\log\colon \mathscr{G} \to \mathscr{G}_a^{\oplus g}$ of K-analytic groups, where $\mathscr{G}_a$ is the additive group on the rigid affine line. Let $\ker(\log)$ be its kernel, and let $\rho \in \sqrt{|K^\times|}$, $0 < \rho < 1$. For $n \gg 0$ (depending on ρ) we have an equality

$$\ker(\log) \cap \boldsymbol{B}_K^g(\rho) = \mathscr{G}[p^n] \cap \boldsymbol{B}_K^g(\rho)$$

of (finite) K-analytic subspaces of $\boldsymbol{B}_K^g(\rho)$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Proof. Using (5.5.3), one sees that $\operatorname{ord} a_{n,ij} \geqslant -n$, from which it follows immediately that the radius of convergence of log is at least 1, i.e. that $\log_i \in \Gamma(\boldsymbol{D}_K^g, \mathscr{O}_{\boldsymbol{D}_K^g})$. Therefore, $\log_i$ defines a map $\boldsymbol{D}_K^g \to \mathscr{G}_a$, so we obtain a K-analytic morphism $\log\colon \mathscr{G} \to \mathscr{G}_a^g$. Since $\log(F(X,Y)) = X + Y$, log is a homomorphism of K-analytic groups.

To prove the second assertion, first we show that $\ker(\log)(\bar{K}) = \bigcup_{n\geqslant 1} \mathscr{G}[p^n](\bar{K})$. As $\mathscr{G}_a^g$ has no additive torsion, any point $x \in \boldsymbol{D}_K^g(\bar{K})$ such that $[p^n](x) = 0$ must satisfy $\log(x) = 0$. Conversely, suppose that $\log(x) = 0$ for $x = (x_1, \ldots, x_g) \in \boldsymbol{D}_K^g(\bar{K})$. By the non-Archimedean inverse function theorem, the power series inverse exp to log has non-zero radius of convergence, so log is injective on some ball $\boldsymbol{B}_K^g(\rho_0)$ around 0 with $\rho_0 > 0$. Since $[p^n](\boldsymbol{X}) = p^n\boldsymbol{X} + O(\boldsymbol{X}^2)$ as power series over R, we have $[p^n]x \to 0$ as $n \to \infty$, so for some n we have $[p^n]x \in \boldsymbol{B}_K^g(\rho_0)$. Then $0 = [p^n]\log(x) = \log([p^n]x)$ implies $[p^n]x = 0$. Moreover, the value of n can be bounded in terms of $|x| = \max\{|x_1|, \ldots, |x_g|\}$, so $\mathscr{G}[p^\infty] \cap \boldsymbol{B}_K^g(\rho) \subset \mathscr{G}[p^n]$ for large enough n.

Since log has a local inverse near the identity, the K-analytic group $\ker(\log)$ is étale. Thus for fixed ρ and sufficiently large n depending on ρ, $\ker(\log) \cap \boldsymbol{B}_K^g(\rho)$ and $\mathscr{G}[p^n] \cap \boldsymbol{B}_K^g(\rho)$ are equal, being étale subspaces of $\boldsymbol{B}_K^g(\rho)$ with the same geometric points. □

Remark 6.9. Proposition 6.8 is not surprising in view of the fact that $\log = \lim_{n\to\infty}[p^n]/p^n$ in the sense of [**18**, p. 64].

7. Statement of the main theorem and preliminary reductions

7.1. In this section we define the canonical subgroup of a truncated p-divisible group G, we define a measure of non-ordinarity of G, and we state our main theorem (Theorem 7.10) relating these. We also make some preliminary reductions regarding the proof.

Notation 7.2. For the rest of this paper R is a complete rank-1 valuation ring of mixed characteristic $(0, p)$ with fraction field K, residue field k, valuation ord normalized so that $\operatorname{ord}(p) = 1$, and absolute value $|\cdot| = p^{-\operatorname{ord}(\cdot)}$. We do *not* assume that R is noetherian or that its residue field is perfect.

7.3. Let G be a connected p-divisible group over R of dimension g and let $\mathscr{G} \cong \boldsymbol{D}_K^g$ be its rigid generic fibre in the sense of § 6.4. As indicated in the introduction, we would like to define the level-n canonical subgroup of G to be a K-subgroup of $G[p^n] \otimes_R K = \mathscr{G}[p^n]$ with geometric structure $(\boldsymbol{Z}/p^n\boldsymbol{Z})^g$ whose geometric points are smaller than all other points of $\mathscr{G}[p^n](\bar{K})$ with respect to the size function $|(x_1, \ldots, x_g)| = \max\{|x_i|\}_{i=1}^g$. This size function is in fact determined by the R-group structure on $G[p^n]$, as follows.

7.4. Let $G = \operatorname{Spec}(A)$ be a finite flat connected R-group scheme, let I be the augmentation ideal of A, and let $\xi \in G(\bar{K})$. Since A is local, we have $|f(\xi)| < 1$ for all $f \in I$. For $r_1, \ldots, r_n \in A$ and $f_1, \ldots, f_n \in I$ we have

$$\left|\sum_{i=1}^n r_i f_i(\xi)\right| \leqslant \max\{|f_i(\xi)|\}_{i=1}^n,$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

so if the residues of $f_1, \dots, f_n$ generate I/I^2 as an R-module then

$$|\xi| := \sup_{f \in I} |f(\xi)| = \max\{|f_i(\xi)|\}_{i=1}^n < 1.$$

Suppose that $\xi, \xi' \in G(\bar{K})$ and $|\xi|, |\xi'| \leqslant \rho$ for some $0 < \rho \leqslant 1$. Let $f \in I$, and let $1 \otimes f + f \otimes 1 + \sum_{i=1}^n f_i \otimes f_i' \in A \otimes_R A$ be the image of f under the comultiplication map, where $f_i, f_i' \in I$. Then

$$|f(\xi + \xi')| = \left| f(\xi) + f(\xi') + \sum_{i=1}^n f_i(\xi) f_i'(\xi') \right| \leqslant \rho,$$

so $\{\xi \in G(\bar{K}) \colon |\xi| \leqslant \rho\}$ is a subgroup of $G(\bar{K})$. Since $|\xi| = |\sigma(\xi)|$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, this subgroup descends to a K-subgroup of $G \otimes_R K$, denoted $G_{\leqslant \rho}$. To summarize, we have the following definition.

Definition 7.5. Let $G = \mathrm{Spec}(A)$ be a finite flat connected R-group scheme, let I be the augmentation ideal of A, and let $\xi \in G(\bar{K})$. We define the *size of* ξ to be

$$|\xi| = \sup_{f \in I} |f(\xi)| < 1,$$

and for $0 < \rho \leqslant 1$ we let $G_{\leqslant \rho}$ be the K-subgroup of $G \otimes_R K$ whose geometric points are

$$G_{\leqslant \rho}(\bar{K}) = \{\xi \in G(\bar{K}) \colon |\xi| \leqslant \rho\}.$$

Remark 7.5.1. Let G be a finite flat connected R-group scheme.

(i) Let $H \subset G$ be a finite flat closed R-subgroup scheme. For $\xi \in H(\bar{K})$ with image ξ' in $G(\bar{K})$, we have $|\xi| = |\xi'|$.

(ii) Let K' be a complete valued field extension of K with valuation ring R' and let $G' = G \otimes_R R'$. Let $\xi \in G(\bar{K})$, and let ξ' be the image of ξ in $G(\bar{K}') = G'(\bar{K}')$ under some embedding $\bar{K} \hookrightarrow \bar{K}'$. Then $|\xi| = |\xi'|$. In particular, if $0 < \rho \leqslant 1$ then $G_{\leqslant \rho} \otimes_K K' = G'_{\leqslant \rho}$.

(iii) If $\rho \leqslant \mu$ then $G_{\leqslant \rho}$ is a K-subgroup of $G_{\leqslant \mu}$.

7.5.2. Let G be a g-dimensional connected p-divisible group over R, let $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ be the associated formal Lie group with $G = \mathfrak{G}[p^\infty]$, and let $\mathscr{G} \cong \boldsymbol{D}_K^g$ be its rigid generic fibre. By Lemma 6.5, for all $n \geqslant 1$ we have a natural isomorphism $G[p^n] \otimes_R K \xrightarrow{\sim} \mathscr{G}[p^n]$. By definition $G[p^n] = \mathrm{Spec}(A)$ where $A = R[\![\boldsymbol{X}]\!]/[p^n](\boldsymbol{X})$, and the augmentation ideal I of A is generated by the residues of $X_1, \dots, X_g$. Hence if $\xi \in G[p^n](\bar{K})$ and if $x = (x_1, \dots, x_g)$ is its image in $\boldsymbol{D}_K^g$ then $|\xi| = \max\{|x_i|\}_{i=1}^g$. It follows that $G[p^n]_{\leqslant \rho} = \mathscr{G}[p^n] \cap \boldsymbol{B}_K^g(\rho)$.

Definition 7.6. Let $N \geqslant 1$, and let G be a BT_N over R of dimension g. If there exists $\rho \leqslant 1$ such that $G^\circ_{\leqslant \rho}(\bar{K}) \cong (\boldsymbol{Z}/p^N\boldsymbol{Z})^g$ then we call $G^\circ_{\leqslant \rho}$ the *level-N canonical subgroup of G*, and we say that this canonical subgroup admits the *radius* ρ.

If G is a p-divisible group over R of dimension g then the *level-N canonical subgroup of G* is defined to be the level-N canonical subgroup of $G[p^N]$, if it exists.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

7.6.1. Note that Definition 7.6 only depends on G° and is insensitive to valued field extension of K.

Remark 7.6.2. Let G be a connected BT_N over R of dimension g and height h.

(i) Note that $G_{\leqslant 1}(\bar{K}) = G(\bar{K}) \cong (\boldsymbol{Z}/p^n\boldsymbol{Z})^h$, and $G_{\leqslant \rho}(\bar{K}) = \{0\}$ for small enough $\rho > 0$. In particular, if $g = h$ then $G_{\leqslant 1}$ is the level-N canonical subgroup of G.

(ii) If $G_{\leqslant \rho}$ is the level-N canonical subgroup of G then $G[p^n]_{\leqslant \rho}$ is the level-n canonical subgroup of $G[p^n]$ for all $1 \leqslant n \leqslant N$.

7.7. The main theorem of this paper is a non-trivial condition on a truncated p-divisible group G of level n that is sufficient for the canonical subgroup of level n to exist. This involves the Hasse invariant of G, defined as follows.

7.8. Let $G = \mathrm{Spec}(A)$ be a connected BT_n over R for some $n \geqslant 1$. Let $R_0 = R/pR$, let $A_0 = A \otimes_R R_0$, let I_0 be the augmentation ideal of A_0, let $G_0 = G \otimes_R R_0 = \mathrm{Spec}(A_0)$, and let $F\colon G_0 \to G_0^{(p)}$ and $V\colon G_0^{(p)} \to G_0$ be the relative Frobenius and Verschiebung homomorphisms, respectively. By [**27**, Propositions II.2.1.2 and II.3.3.11], I_0/I_0^2 is a finite free R_0-module, so $\mathrm{Lie}(G_0)$ (respectively $\mathrm{Lie}(G_0^{(p)})$) is a finite free R_0-module of the same rank. After choosing bases for $\mathrm{Lie}(G_0)$ and $\mathrm{Lie}(G_0^{(p)})$, we can regard the map $\mathrm{d}V\colon \mathrm{Lie}(G_0^{(p)}) \to \mathrm{Lie}(G_0)$ as a square matrix with entries in R_0; the determinant $\det(\mathrm{d}V)$ is then defined up to multiplication by a unit in R_0. For $r \in R_0$ let $\tilde{r} \in R$ be any lift of r, and note that $\min\{\mathrm{ord}(\tilde{r}), 1\}$ only depends on the ideal rR_0.

Definition 7.9. If G is a truncated p-divisible group over R, the *Hasse invariant* of G is defined to be

$$H(G) = H(G^\circ) = \min\{\mathrm{ord}(\det(\mathrm{d}V)^\sim), 1\}.$$

If G is a p-divisible group over R, the *Hasse invariant* of G is defined to be $H(G[p])$.

Remark 7.9.1.

(i) If G is a truncated p-divisible group over R then $H(G) = H(G[p])$ because $\mathrm{Lie}(G_0) = \mathrm{Lie}(G_0[p])$; see Remark 2.6.

(ii) Let G be a connected BT_N over R of dimension $g > 0$ and height h for some $N \geqslant 1$. We have $H(G) = 0$ if and only if the Verschiebung V is an isomorphism on the tangent space of G_0, which is to say that $V\colon G_0^{(p)} \to G_0$ is an isomorphism, or equivalently the Frobenius F is an isomorphism on the Cartier dual group G_0^*. Equivalently the dual G^* is étale, which is to say $\dim(G^*) = 0$. As $\dim(G^*) + \dim(G) = h$, this says exactly that $h = g$, i.e. that G is multiplicative. In this case we say that G is *ordinary*; the theory of the canonical subgroup is uninteresting when G is ordinary, as $\mathscr{G}[p^N]_{\leqslant 1}$ is trivially the level-N canonical subgroup G for all $n \geqslant 1$. In general we consider $H(G)$ as a measure of non-ordinarity of G.

(iii) As a converse to (ii), if G is a p-divisible group over R such that the canonical subgroup of level N exists for all $N \geqslant 1$, then $H(G) = 0$; see Remark 11.6.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

(iv) Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, and let $G = \mathrm{BT}_{\mathcal{P}}$ be the associated p-divisible group. We can calculate the Hasse invariant of G in terms of the display $\mathcal{P}$ as follows. Choose a normal decomposition $P = T \oplus L$, choose $W(R)$-bases for T and L, and let $M = (\alpha_{ij})$ be the structure matrix for $\mathcal{P}$ with respect to these bases, as in (5.1.1). Let $A = (\alpha_{ij})_{i,j=1}^{g}$ be the upper-left $g \times g$ submatrix of M, the matrix for the composite map $T \to P \xrightarrow{F} P \to T$. The tangent space $\mathrm{Lie}(G_0)$ of $G_0 = G \otimes_R R_0$ is identified with $(P/Q) \otimes_R R_0 \cong T_0 := T \otimes_R R_0$, and likewise $\mathrm{Lie}(G_0^{(p)}) \cong T_0 \otimes_{R_0,\mathrm{Frob}} R_0$. Hence $\mathrm{d}V\colon \mathrm{Lie}(G_0^{(p)}) \to \mathrm{Lie}(G_0)$ is given by the matrix $w_0(A) \mod p$ with respect to our choice of basis, so

$$H(G) = \min\{\mathrm{ord}(\det(w_0(A))), 1\}.$$

See [**32**, Example 23].

Our goal is to prove the following.

Theorem 7.10. *Let G be a truncated p-divisible group of level $N \geqslant 1$ over R. If $H(G) < (p-1)/p^N$ then the level-N canonical subgroup of G exists, and it admits the radius $\rho = p^{-r}$ where*

$$r = \frac{1}{p^{N-1}(p-1)} - \frac{H(G)}{p-1}.$$

Remark 7.10.1.

(i) It is important to note that the bound in Theorem 7.10 is independent of the height and dimension of G.

(ii) As mentioned in § 1.10, when $g = 1$ and $h \leqslant 2$ Katz *et al.* have shown that the canonical subgroup of level N exists if and only if $H(G) < 1/p^{N-2}(p+1)$ (with the same radius). This bound is larger than the bound in Theorem 7.10 by a factor of $p^2/(p^2-1)$; we do not know if it holds in higher dimensions. See Remark 1.12.

(iii) Since the Hasse invariant and canonical subgroup of G are intrinsic to G°, Theorem 7.10 is in fact a statement about *connected* truncated Barsotti–Tate groups. Furthermore, if K' is a complete valued field extension of K with valuation ring R' and if $G' = G \otimes_R R'$, then $H(G) = H(G')$ and $G^\circ_{\leqslant\rho}$ is the level-N canonical subgroup of G if and only if $(G')^\circ_{\leqslant\rho}$ is the level-N canonical subgroup of G', so Theorem 7.10 is insensitive to valued field extensions.

(iv) Theorem 7.10 can be extended to give a criterion for the existence of the canonical subgroup of an abelian variety over K of arbitrary reduction type. In addition, a relative version of Theorem 7.10 holds for algebraic families of abelian varieties over K. This is a subject of forthcoming work with Brian Conrad.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

7.11. We would like to use the theory of logarithms of displays developed in § 5 to prove Theorem 7.10. However, since we are not assuming the residue field of R to be perfect, we cannot apply [**19**, Theorem 4.4(e)] to identify G with the p^N-torsion of a p-divisible group over R. In § 12 we will prove (Proposition 12.2) that any connected level-N truncated p-divisible group G is isomorphic to $\mathrm{BT}_{\mathcal{P}}[p^N]$ for some display $\mathcal{P}$ over R when K is algebraically closed; passing to the completion of the algebraic closure of K and using Remark 7.10.1 (iii), we see that it suffices to prove the slightly weaker theorem that follows.

Theorem 7.12. *Let $\mathcal{P}$ be a display over R, and let $G = \mathrm{BT}_{\mathcal{P}}$. If $H(G) < (p-1)/p^N$ then the level-N canonical subgroup of G exists, and it admits the radius $\rho = p^{-r}$ where*

$$r = \frac{1}{p^{N-1}(p-1)} - \frac{H(G)}{p-1}.$$

7.13. The strategy for proving Theorem 7.12 is as follows. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R, let $P = T \oplus L$ be a normal decomposition, let $e_1, \dots, e_g$ and $e_{g+1}, \dots, e_h$ be $W(R)$-bases for T and L respectively, and let $M = (\alpha_{ij})$ be the structure matrix for $\mathcal{P}$ with respect to this basis, as in (5.1.1). Let $G = \mathrm{BT}_{\mathcal{P}}$ be the associated p-divisible formal group over R (of dimension g and height h), and let $\mathscr{G}$ be its rigid generic fibre. Recall that the choice of basis $e_1, \dots, e_g$ of T provides a homomorphism of K-analytic groups $\log\colon \mathscr{G} \to \mathscr{G}_{a,K}^{\oplus g}$, which is given by g power series $(\log_1, \dots, \log_g)$ in g variables calculated in terms of $\mathcal{P}$ using (5.5.3).

The kernel of log being the p-power torsion of $\mathscr{G}$, we would like to understand the valuations of the coordinates of the *points* of $\ker(\log)$. The theory of tropical geometry is ideally set up to solve such a problem: in what is essentially a higher-dimensional analogue of a Newton polygon, the ultrametric inequality will allow us to pinpoint the only possible points $x = (x_1, \dots, x_g) \in (\boldsymbol{R} \cup \{\infty\})^g$ such that $x_i = \mathrm{ord}(\xi_i)$ for some simultaneous root $\xi = (\xi_1, \dots, \xi_g) \in \boldsymbol{D}_K^g(\bar{K})$ of $\log_1, \dots, \log_g$. More precisely, we will be able to say where these points *cannot* lie, and then make a deformation to count the number of points of $\ker(\log)$ contained in $\boldsymbol{B}_K^g(\rho)$ for suitable ρ. This will allow us to prove that $\mathscr{G}[p^\infty] \cap \boldsymbol{B}_K^g(\rho)$ is the level-N canonical subgroup of G.

We start by making a preliminary reduction.

Lemma 7.14. *Let T be a finite free $W(R)$-module of rank g, and let $F\colon T \to T$ be an ${}^{\mathrm{F}}$-linear map. After possibly making a finite extension of K, there is a $W(R)$-basis $e_1, \dots, e_g$ for T such that, if A is the matrix for F with respect to this basis, then $w_0(A)$ is upper triangular modulo pR.*

Proof. Let $T_0 = T \otimes_{W(R), w_0} R_0$ where $R_0 = R/pR$. Since ${}^{\mathrm{F}}(\cdot)$ preserves the ideal $W(pR) + I_R \subset W(R)$, F preserves the submodule $(W(pR) + I_R)T$ and hence F induces an additive map $F_0\colon T_0 \to T_0$ satisfying $F(\lambda v) = \lambda^p F(v)$ for $\lambda \in R_0$ and $v \in T_0$. By § 4.2 and Nakayama's lemma, it suffices to find a basis for T_0 with respect to which the matrix for F_0 is upper-triangular. This statement is intrinsic to the p-linear endomorphism F_0 of the finite free R_0-module T_0, so it suffices to prove the following.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

(*) Let M_0 be a finite free R_0-module of rank g and let $F_0\colon M_0 \to M_0$ be a p-linear endomorphism. After possibly extending scalars to R'/pR', where R' is the ring of integers in a finite field extension of K, there is a basis for M_0 with respect to which F_0 is upper-triangular.

By the standard inductive argument, we need only exhibit a 'basis eigenvector' for F_0, i.e. an element $v \in M_0$ such that $F_0 v = \lambda v$ for some $\lambda \in R_0$, and such that $\{v\}$ extends to a basis for M_0.

Let M be a finite free R-module such that $M/pM \cong M_0$, and denote the map $M \to M_0$ by $v \mapsto \bar{v}$. Let $x_1, \dots, x_g \in M$ be any basis, so $\bar{x}_1, \dots, \bar{x}_g$ is a basis of M_0, and $F_0(\bar{x}_i) = \sum_{i=1}^g \bar{\mu}_{ij}\bar{x}_j$ for some $\bar{\mu}_{ij} \in R_0$. Let $\mu_{ij} \in R$ be a lift of $\bar{\mu}_{ij}$ (which may be chosen such that $\det(\mu_{ij}) \neq 0$), and define a map $F\colon M \to M$ by

$$F\left(\sum_{i=1}^g a_i x_i\right) = \sum_{i=1}^g a_i^p \sum_{j=1}^g \mu_{ij} x_j. \tag{7.14.1}$$

Then $F_0(\bar{v}) = F(v) \mod p$ and $F(\lambda v) = \lambda^p F(v)$ for $v \in M$ and $\lambda \in R$. Suppose that $F(w) = \lambda w$ for $w \in M$ non-zero and $\lambda \in R$. Write $w = \sum_{i=1}^g a_i x_i$, and let $\pi \in K$ be an element with $\operatorname{ord}(\pi) = -\max\{\operatorname{ord}(a_i)\}_{i=1}^g$. Let $v = \pi w$. Note that

$$\lambda\pi^{-1}v = \lambda w = F(w) = F(\pi^{-1}v) = \pi^{-p}F(v) \implies F(v) = \pi^{p-1}\lambda v,$$

with $\pi^{p-1}\lambda \in R$ because $\pi^{p-1}\lambda v \in M$. Since $M/(Rv)$ is a finite torsion-free R-module, it is flat (use [**26**, Theorem 7.8(3)], noting that every finitely generated ideal of R is principal) and hence free by [**26**, Theorem 7.10], so $\{v\}$ extends to a basis of M and hence $\bar{v}$ is a basis eigenvector for F_0. Thus we are reduced to finding $w \in M$ such that $F(w) = \lambda w$. If $F(w) = 0$ for some non-zero $w \in M$ then we are done, so we may assume that there is no such w, even after a finite field extension of K.

Let $M_K = M \otimes_R K$, and let $\boldsymbol{P} = \boldsymbol{P}(M_K) \cong \boldsymbol{P}_K^g$ be the associated projective space over $\operatorname{Spec}(K)$. Since $F(w) \neq 0$ for all non-zero $w \in M$ even after finite extension of K, the homogeneous polynomials (7.14.1) define a morphism $F_K\colon \boldsymbol{P} \to \boldsymbol{P}$. By [**14**, Example 16.2.2], any self-map of $\boldsymbol{P}$ has a fixed point, so after extending scalars we may assume that F_K has a rational fixed point. Of course the rational points of $\boldsymbol{P}$ correspond to the lines in M_K, so there exists a non-zero element $w \in M$ such that $F_K(w) = \lambda w$ for some $\lambda \in K^\times$. Choosing $\pi \in R$ such that $\pi^{p-1}\lambda \in R$, we have $F(\pi w) = \pi^{p-1}\lambda \cdot \pi w$, as required. □

7.15. Recall that we have chosen a normal decomposition $P = T \oplus L$, and that T is a rank-g free module over $W(R)$. Let A be the matrix for the composite $T \hookrightarrow P \xrightarrow{F} P \to T$, so $H(G) = \min\{\operatorname{ord}(\det(w_0(A))), 1\}$ by Remark 7.9.1 (iv). After making a finite extension of K and choosing a basis for T as in Lemma 7.14, we will *assume from now on that* $w_0(A)$ *is upper-triangular modulo* pR. In this case,

$$H(G) = \operatorname{ord}(\det(w_0(A))) = \sum_{i=1}^g \operatorname{ord}(w_0(\alpha_{ii}))$$

assuming $H(G) < 1$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

8. A survey of some concepts from tropical geometry

8.1. In this section we review the dual concepts of the tropical hypersurface and the Newton polytope of a power series. This theory can be seen as a direct generalization of the theory of Newton polygons; see Example 8.13. For a more complete theory see [**28**] and the references contained therein.

Notation 8.2. Let S be a set and $T \subset S$ a subset, and let $f\colon S \to \boldsymbol{R}$ be any function. Define

$$\operatorname{minset}(f, T) := \Big\{ t \in T\colon f(t) = \inf_{t' \in T} f(t') \Big\}.$$

Note that this set could be empty.

8.3. First we introduce some notions from convex geometry. We will make a great deal of definitions, stating facts without proof. A good reference for this material is [**4**]. Let $\langle \cdot, \cdot \rangle$ denote the standard inner product on $\boldsymbol{R}^g$. The convex hull of a set of points $S \subset \boldsymbol{R}^g$ will be denoted $\operatorname{conv}(S)$. A *polyhedron* P is a non-empty intersection of finitely many half-spaces in $\boldsymbol{R}^g$, i.e. a non-empty subset of the form

$$P = \bigcap_{i=1}^{r} \{ x \in \boldsymbol{R}^g\colon \langle x, u_i \rangle \geqslant a_i \}$$

for some elements $u_1, \ldots, u_r \in \boldsymbol{R}^g$ and $a_1, \ldots, a_r \in \boldsymbol{R}$. A *polytope* is a bounded polyhedron. For $w \in \boldsymbol{R}^g$ we define

$$\operatorname{face}_w(P) = \operatorname{minset}(\langle \cdot, w \rangle, P);$$

this is the locus in P where a linear form attains its infimum on P. A *face* of a polyhedron P is a non-empty subset of P of the form $\operatorname{face}_w(P)$; this is again a polyhedron. A *vertex* of P is a one-point face; we let $\operatorname{vertices}(P)$ be the set of vertices of P. A polyhedron has finitely many faces (hence finitely many vertices), and a polytope is the convex hull of its vertices. The *affine span* of a polyhedron P is the smallest affine subspace containing P. The *dimension* of P is the dimension of its affine span, and the *relative interior* $\operatorname{relint}(P)$ of P is the interior of P as a subset of its affine span. The relative interior of a face of P is the set of points not contained in a strictly smaller face.

A *polyhedral complex* is a non-empty finite collection Π of polyhedra satisfying the following.

(i) If $P \in \Pi$ then every face of P is in Π.

(ii) If $P, Q \in \Pi$ and $P \cap Q \neq \emptyset$ then $P \cap Q$ is a face of P and a face of Q.

An element of Π is called a *cell*; the *support* $|\Pi|$ of Π is the union of its cells. A *polytopal complex* is a polyhedral complex whose cells are polytopes (i.e. bounded).

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

8.4. The following example illustrates the idea behind using tropical geometry to determine the valuations of the zeros of a power series. To motivate our choice of power series, let $\mathcal{P}$ be the display of dimension 2 and height 2 over the valuation ring R of K given by the structure matrix $M = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, and let $\log = (\log_1, \log_2)$ be the logarithm of $\mathrm{BT}_{\mathcal{P}}$ as in § 5. Using (5.5.3) we see that

$$\log_1(X, Y) \equiv X + p^{-1}X^p + p^{-1}Y^p + p^{-2}X^{p^2} + 2p^{-2}Y^{p^2} \pmod{X^{p^3}, Y^{p^3}}.$$

Example 8.5. Let $f = X + p^{-1}X^p + p^{-1}Y^p \in K[X, Y]$, and choose $(\xi, \eta) \in (\bar{K}^\times)^2$. If $f(\xi, \eta) = 0$ then at least two of the three quantities $|\xi|$, $|p^{-1}\xi^p|$ and $|p^{-1}\eta^p|$ are equal and are at least as large as the third. In terms of valuations, if $(u, v) = (\mathrm{ord}(\xi), \mathrm{ord}(\eta))$, this says that at least two of the quantities u, $pu - 1$, $pv - 1$ are equal to $\min\{u, pu-1, pv-1\}$. The locus where $pu-1 = pv-1$ is the line $L_1 = \{u = v\}$, the locus where $u = pu-1$ is the line $L_2 = \{u = 1/(p-1)\}$, and the locus where $u = pv-1$ is the line $L_3 = \{v = (u-1)/p\}$; we have $u = pu-1 = pv-1$ at the point $(u, v) = (1/(p-1), 1/(p-1))$. This is illustrated in the right-hand side of figure 1; we now explain the significance of the half-lines in that picture.

When $(u, v) \in L_1$ and $u = v > 1/(p-1)$ then $u = v > pv - 1$, so (ξ, η) cannot be a zero of f; hence if (ξ, η) is a zero of f and $(u, v) \in L_1$ then (u, v) is contained in the ray $R_1 = (1/(p-1), 1/(p-1)) + \boldsymbol{R}_{\geqslant 0}(-1, -1)$. Similar reasoning shows that if (ξ, η) is a zero of f then (u, v) is contained in one of the rays R_1, $R_2 = (1/(p-1), 1/(p-1)) + \boldsymbol{R}_{\geqslant 0}(0, 1)$, or $R_3 = (1/(p-1), 1/(p-1)) + \boldsymbol{R}_{\geqslant 0}(p, 1)$. In other words, there are 'piecewise linear' necessary conditions on (u, v) for (ξ, η) to be a zero of f; we will use tropical geometry as a language to express these conditions. (In fact, we will see in a moment that the 'tropicalization' of f, to be defined shortly, is essentially equal to $R_1 \cup R_2 \cup R_3$.)

8.6. Choose $\rho > 0$, let $r = -\log_p(\rho) \in \boldsymbol{R}$, and let $\boldsymbol{T}^g_K(\rho) = (\boldsymbol{B}^1_K(\rho) \setminus \{0\})^g$. For non-zero $f = \sum_\nu a_\nu X^\nu \in T_{g,\rho}$ let

$$H(f) = \{(\nu, \mathrm{ord}(a_\nu)) \colon a_\nu \neq 0\} \subset \boldsymbol{Z}^g_{\geqslant 0} \times \boldsymbol{R};$$

this is called the *height graph* of f. For $w \in \boldsymbol{R}^g_{\geqslant r}$ let $\mathrm{In}_w(f) = \mathrm{minset}(\langle (w, 1), \cdot \rangle, H(f))$, where we are denoting the inner product on $\boldsymbol{R}^{g+1}$ by $\langle \cdot, \cdot \rangle$ as well; by [**28**, § 8], $\mathrm{In}_w(f)$ is a non-empty finite set for all $w \in \boldsymbol{R}^g_{\geqslant r}$. In Example 8.7 we work this out for f as in Example 8.5. For $w \in \boldsymbol{R}^g_{\geqslant r}$, define the *initial form* $\mathrm{in}_w(f)$ of f to be

$$\mathrm{in}_w(f) = \sum_{(\nu, \mathrm{ord}(a_\nu)) \in \mathrm{In}_w(f)} a_\nu X^\nu,$$

so $H(\mathrm{in}_w(f)) = \mathrm{In}_w(f)$. In other words, $\mathrm{in}_w(f)$ is the (non-zero) sum of those monomials $a_\nu X^\nu$ such that

$$\mathrm{ord}(a_\nu) + \langle w, \nu \rangle = \min_{\mu \in \boldsymbol{Z}^g_{\geqslant 0}} \{\mathrm{ord}(a_\mu) + \langle w, \mu \rangle\}.$$

In particular, if $w = (\mathrm{ord}(\xi_1), \ldots, \mathrm{ord}(\xi_g))$ for $\xi = (\xi_1, \ldots, \xi_g) \in \boldsymbol{T}^g_K(\rho)(\bar{K})$ then $\mathrm{in}_w(f)$ is the sum of those monomials $a_\nu X^\nu$ such that $a_\nu \xi^\nu$ has minimal valuation among all

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

monomials of $f(\xi)$. Define the *tropicalization* of f to be

$$\mathrm{Trop}(f) = \{w \in \boldsymbol{R}^g_{\geqslant r} \colon \mathrm{in}_w(f) \text{ is not a monomial}\}.$$

Example 8.7. Continuing with Example 8.5, let $\rho = 1$ (so $r = 0$) and $g = 2$, so $f \in T_{g,\rho}$ and

$$H(f) = \{(1,0,0),(p,0,-1),(0,p,-1)\}.$$

For w in the part of the relative interior of R_1 that lies in $\boldsymbol{R}^2_{\geqslant 0}$ we have $\mathrm{In}_w(f) = \{(p,0,-1),(0,p,-1)\}$ and $\mathrm{in}_w(f) = p^{-1}X^p + p^{-1}Y^p$; equivalently, if $w = (u,v) = (\mathrm{ord}(\xi),\mathrm{ord}(\eta))$ then $\mathrm{ord}(p^{-1}\xi^p) = \mathrm{ord}(p^{-1}\eta^p) < \mathrm{ord}(\xi)$. Likewise, for $w \in \mathrm{relint}(R_2) \subset \boldsymbol{R}^2_{\geqslant 0}$ we have $\mathrm{In}_w(f) = \{(1,0,0),(p,0,-1)\}$ and $\mathrm{in}_w(f) = X + p^{-1}X^p$, for $w \in \mathrm{relint}(R_3) \subset \boldsymbol{R}^2_{\geqslant 0}$ we have $\mathrm{In}_w(f) = \{(1,0,0),(0,p,-1)\}$ and $\mathrm{in}_w(f) = X + p^{-1}Y^p$, and if $w = (1/(p-1),1/(p-1))$ then $\mathrm{In}_w(f) = H(f)$ and $\mathrm{in}_w(f) = f$. As we saw in Example 8.5, if $w = (\mathrm{ord}(\xi),\mathrm{ord}(\eta))$ for $(\xi,\eta) \in \boldsymbol{T}^2_K(0)(\bar{K})$ then $\mathrm{in}_w(f)$ is the sum of those monomials of f for which some 'internal cancellation' has to occur in order for (ξ,η) to be a zero of f.

On the other hand, let U_{ij} denote the interior of the polytope bounded by the rays R_i and R_j for $i,j = 1,2,3$, $i \neq j$. If $w \in U_{12} \cap \boldsymbol{R}^2_{\geqslant 0}$ then $\mathrm{in}_w(f) = X$, if $w \in U_{23}$ then $\mathrm{in}_w(f) = p^{-1}X^p$, and if $w \in U_{13} \cap \boldsymbol{R}^2_{\geqslant 0}$ then $\mathrm{in}_w(f) = p^{-1}Y^p$. This proves that $\mathrm{Trop}(f) = (R_1 \cup R_2 \cup R_3) \cap \boldsymbol{R}^2_{\geqslant 0}$. As we worked out in Example 8.5, if $(\xi,\eta) \in \boldsymbol{T}^2_K(1)(\bar{K})$ is a zero of f then $(\mathrm{ord}(\xi),\mathrm{ord}(\eta)) \in \mathrm{Trop}(f)$. This is true in general, as we will see in § 8.8.

8.8. We use the notation in § 8.6. Let $\mathrm{ord}\colon \boldsymbol{T}^g_K(\rho)(\bar{K}) \to \boldsymbol{R}^g_{\geqslant r}$ be the map defined by

$$\mathrm{ord}(\xi_1,\ldots,\xi_g) = (\mathrm{ord}(\xi_1),\ldots,\mathrm{ord}(\xi_g)).$$

If $\xi = (\xi_1,\ldots,\xi_g) \in \boldsymbol{T}^g_K(\rho)(\bar{K})$ is a zero of $f \in T_{g,\rho}$ then we claim that $\mathrm{ord}(\xi) \in \mathrm{Trop}(f)$. Letting $w = \mathrm{ord}(\xi)$, we have $\mathrm{ord}(a_\nu\xi^\nu) = \mathrm{ord}(a_\nu) + \langle w,\nu\rangle$, so if $\mathrm{in}_w(f)$ is a monomial $a_\nu X^\nu$ then $a_\nu\xi^\nu$ has strictly smaller valuation than $a_\mu\xi^\mu$ for all $\mu \neq \nu$, and thus $|f(\xi)| = |a_\nu\xi^\nu| \neq 0$ by the ultrametric inequality. Hence ord restricts to a map $\mathrm{ord}\colon V(f)(\bar{K}) \to \mathrm{Trop}(f)$, where $V(f)$ is the closed subspace of $\boldsymbol{T}^g_K(\rho)$ cut out by f. It is a fundamental fact that the closure of $\mathrm{ord}(V(f)(\bar{K}))$ is exactly $\mathrm{Trop}(f)$, and if $w \in \mathrm{Trop}(f)$ has coordinates in $\mathrm{ord}(\bar{K}^\times)$ then there is a zero ξ of f such that $\mathrm{ord}(\xi) = w$; see [**28**, § 8] for a proof in this context. This is why we are interested in $\mathrm{Trop}(f)$.

8.9. For $f \in T_{g,\rho}$ non-zero, the set $\mathrm{Trop}(f)$ has the following natural polyhedral complex structure. For $w \in \boldsymbol{R}^g_{\geqslant r}$ define

$$\begin{aligned} P_w &= \{w' \in \boldsymbol{R}^g_{\geqslant r} \colon \mathrm{In}_{w'}(f) \supset \mathrm{In}_w(f)\} \\ &= \bigcap_{\substack{(\nu,\mathrm{ord}(a_\nu)) \in \mathrm{In}_w(f) \\ \mu \in \boldsymbol{Z}^n_{\geqslant 0}}} \{w' \in \boldsymbol{R}^g_{\geqslant r} \colon \langle w', \nu - \mu\rangle \leqslant \mathrm{ord}(a_\mu) - \mathrm{ord}(a_\nu)\}; \end{aligned}$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

note that $w \in P_w$ and if $w' \in P_w$ then $P_{w'} \subset P_w$. It is proved in [**28**, § 8] that $\bigcup_{v \in \boldsymbol{R}^g_{\geqslant r}} \mathrm{In}_v(f)$ is a finite set. It follows that P_w is a polyhedron, and that the collection $\mathcal{C} = \{P_w \colon \mathrm{in}_w(f) \text{ is not a monomial}\}$ of polyhedra in $\boldsymbol{R}^g_{\geqslant r}$ is finite. In fact $\mathcal{C}$ is a polyhedral complex (at least in $\boldsymbol{R}^g_{>r}$), and its support is clearly

$$|\mathcal{C}| = \{w \in \boldsymbol{R}^g_{\geqslant r} \colon \mathrm{in}_w(f) \text{ is not a monomial}\} = \mathrm{Trop}(f).$$

From now on we will use $\mathrm{Trop}(f)$ to denote both $\mathcal{C}$ and its support. See Example 8.11 for a description of the polyhedra P_w for f as in Example 8.5.

8.10. Recall that the height graph $H(f)$ for non-zero $f \in T_{g,\rho}$ lies in $\boldsymbol{Z}^g_{\geqslant 0} \times \boldsymbol{R}$, with the initial g coordinates encoding the monomials appearing in f, and that the $\mathrm{In}_w(f)$ are subsets of $H(f)$. Let $\pi \colon \boldsymbol{R}^{g+1} \to \boldsymbol{R}^g$ be the projection onto the first g coordinates. The *Newton complex* $\mathrm{New}(f)$ of f is the collection of polytopes in $\boldsymbol{R}^g$ consisting of the convex hulls

$$C_w = \mathrm{conv}(\pi(\mathrm{In}_w(f)))$$

of the finite sets $\pi(\mathrm{In}_w(f))$ for $w \in \boldsymbol{R}^g_{\geqslant r}$; it is shown in [**28**, § 8] that the Newton complex is 'almost' a polytopal complex. What we will use is the fact that the complex $\mathrm{New}(f)$ controls the combinatorics of $\mathrm{Trop}(f)$, in the following sense.

8.10.1. By definition $P_w = P_{w'}$ if and only if $\mathrm{In}_{w'}(f) \subset \mathrm{In}_w(f)$ and $\mathrm{In}_w(f) \subset \mathrm{In}_{w'}(f)$, i.e. if and only if $\mathrm{In}_w(f) = \mathrm{In}_{w'}(f)$. We leave the equality

$$\mathrm{In}_w(f) = H(f) \cap \mathrm{conv}\{x \in H(f) \colon \pi(x) \in \mathrm{vertices}(C_w)\} \tag{8.10.2}$$

as an exercise to the reader; in particular, $C_w = C_{w'}$ if and only if $\mathrm{In}_w(f) = \mathrm{In}_{w'}(f)$. Therefore, the association $P_w \leftrightarrow C_w$ for $w \in \mathrm{Trop}(f)$ is a bijective correspondence between the cells of $\mathrm{Trop}(f)$ and the positive-dimensional cells of $\mathrm{New}(f)$ (of course C_w is a point if and only if $\mathrm{in}_w(f)$ is a monomial). We call C_w the *dual cell* to P_w, and vice versa; this terminology is justified by the following paragraphs.

8.10.3. We can interpret (8.10.2) as follows. Let $C = C_w$ be a cell of $\mathrm{New}(f)$, and let $\nu_1, \dots, \nu_n$ be the vertices of C. Then $\mathrm{In}_w(f) = H(f) \cap \mathrm{conv}\{(\nu_i, \mathrm{ord}(a_{\nu_i})) \colon i = 1, \dots, n\}$, and hence the dual cell $P = P_w$ is exactly

$$\begin{aligned} P &= \{w' \in \mathrm{Trop}(f) \colon \pi(\mathrm{In}_{w'}(f)) \supset \{\nu_1, \dots, \nu_n\}\} \\ &= \Big\{w' \in \mathrm{Trop}(f) \colon \langle w', \nu_i\rangle + \mathrm{ord}(a_{\nu_i}) = \min_{\nu \in \boldsymbol{Z}^g_{\geqslant 0}} \{\langle w', \nu\rangle + \mathrm{ord}(a_\nu)\} \text{ for all } i = 1, \dots, n\Big\}. \end{aligned}$$

This allows us to recover P from C and f without reference to w. *Note in particular that*

$$\langle w', \nu_1\rangle + \mathrm{ord}(a_{\nu_1}) = \cdots = \langle w', \nu_n\rangle + \mathrm{ord}(a_{\nu_n}) \tag{8.10.4}$$

for all w' in the cell P of $\mathrm{Trop}(f)$ dual to the cell C of $\mathrm{New}(f)$ with vertices $\{\nu_1, \dots, \nu_n\}$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

8.10.5. For $w \in \mathrm{Trop}(f)$ the cells C_w and P_w are orthogonal to each other (in the sense that the vector subspaces of $\boldsymbol{R}^g$ associated to their affine spans are orthogonal); this can be seen as follows. Let $(\nu_1, \mathrm{ord}(a_{\nu_1}))$ and $(\nu_2, \mathrm{ord}(a_{\nu_2}))$ be in $\mathrm{In}_w(f)$ and let $w_1, w_2 \in P_w$. Then $(\nu_i, \mathrm{ord}(a_{\nu_i})) \in \mathrm{In}_{w_j}(f)$ for $i, j = 1, 2$, so since

$$\mathrm{In}_{w_j}(f) = \mathrm{minset}((\nu, \mathrm{ord}(a_\nu)) \mapsto \mathrm{ord}(a_\nu) + \langle w_j, \nu \rangle, H(f)),$$

it follows that

$$\begin{aligned} \mathrm{ord}(a_{\nu_1}) + \langle w_1, \nu_1 \rangle &= \mathrm{ord}(a_{\nu_2}) + \langle w_1, \nu_2 \rangle, \\ \mathrm{ord}(a_{\nu_1}) + \langle w_2, \nu_1 \rangle &= \mathrm{ord}(a_{\nu_2}) + \langle w_2, \nu_2 \rangle, \end{aligned}$$

and hence $\langle w_1 - w_2, \nu_1 - \nu_2 \rangle = 0$. We leave as an exercise to the reader to derive that $\langle w_1 - w_2, v_1 - v_2 \rangle = 0$ for all $v_1, v_2 \in C_w$ using the fact that any element $v \in C_w$ is of the form $v = \sum_{i=1}^r \alpha_i \mu_i$ where $\alpha_i \geqslant 0$, $\sum_{i=1}^r \alpha_i = 1$, and $(\mu_i, \mathrm{ord}(a_{\mu_i})) \in \mathrm{In}_w(f)$ for $i = 1, \ldots, r$.

8.10.6. The 'duality' between $\mathrm{Trop}(f)$ and $\mathrm{New}(f)$ satisfies other nice properties. For example, $\dim(C_w) + \dim(P_w) = g$ (at least when P_w is not contained in the boundary of $\boldsymbol{R}^g_{\geqslant r}$ in $\boldsymbol{R}^g$), and C_w is a face of $C_{w'}$ if and only if $P_{w'}$ is a face of P_w for $w, w' \in \mathrm{Trop}(f)$. However, $\mathrm{Trop}(f)$ and $\mathrm{New}(f)$ are not dual in any intrinsic way—it is more accurate to say that they are both expressions of the combinatorial properties of f (really of $H(f)$) that live in dual vector spaces.

Example 8.11. Continuing Example 8.7, we have $\mathrm{In}_w(f) = \{(p, 0, -1), (0, p, -1)\}$ for $w \in \mathrm{relint}(R_1) \cap \boldsymbol{R}^2_{\geqslant 0}$, and hence

$$P_w = \{w' \in \mathrm{Trop}(f) \colon \{(p, 0, -1), (0, p, -1)\} \subset \mathrm{In}_{w'}(f)\} = R_1 \cap \boldsymbol{R}^2_{\geqslant 0}.$$

Likewise $P_w = R_2$ for $w \in \mathrm{relint}(R_2)$, $P_w = R_3$ for $w \in \mathrm{relint}(R_3)$, and $P_{(1/(p-1), 1/(p-1))} = \{(1/(p-1), 1/(p-1))\}$.

For $w \in \mathrm{relint}(R_1) \cap \boldsymbol{R}^2_{\geqslant 0}$ we have

$$C_w = \mathrm{conv}(\pi(\mathrm{In}_w(f))) = \mathrm{conv}(\pi(\{(p, 0, -1), (0, p, -1)\})) = \mathrm{conv}\{(p, 0), (0, p)\};$$

this is the line segment $R_1' := \overline{(p, 0)(0, p)}$. Likewise $C_w = R_2' := \overline{(1, 0)(p, 0)}$ for $w \in \mathrm{relint}(R_2)$, $C_w = R_3' := \overline{(1, 0)(0, p)}$ for $w \in \mathrm{relint}(R_3)$, and $C_{(1/(p-1), 1/(p-1))}$ is the triangle τ with vertices $(1, 0)$, $(0, p)$, $(0, p)$. For $i = 1, 2, 3$ the cells R_i and R_i' are dual; note that they are orthogonal and have complementary dimension. The triangle τ is dual to the vertex $\{(1/(p-1), 1/(p-1))\} \in \mathrm{Trop}(f)$. The vertices of $\mathrm{New}(f)$ correspond to the connected components of $\boldsymbol{R}^2_{\geqslant 0} \setminus \mathrm{Trop}(f)$ (these are the U_{ij} of Example 8.7); they do not have dual cells in $\mathrm{Trop}(f)$. See figure 1.

Example 8.12. Extending the previous example, suppose that $p \neq 2$, and let

$$f = X + p^{-1}X^p + p^{-1}Y^p + p^{-2}X^{p^2} + 2p^{-2}Y^{p^2},$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

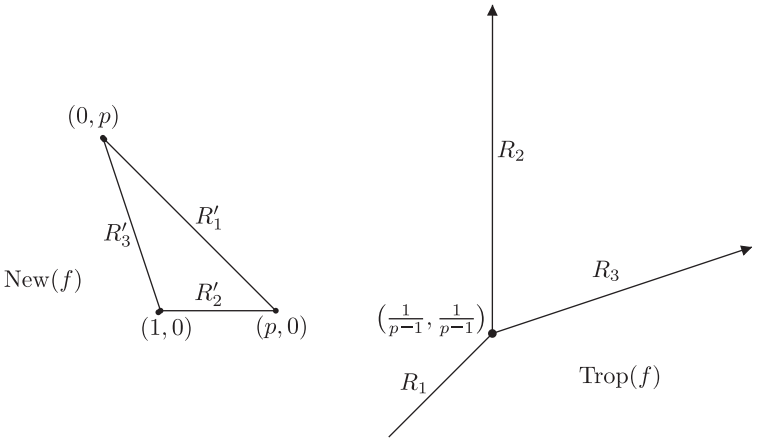

Figure 1. The Newton complex and tropicalization of the polynomial f of Examples 8.5, 8.7 and 8.11. The cell R_i of $\mathrm{Trop}(f)$ is dual to the line segment $R_i' \in \mathrm{New}(f)$ for $i = 1, 2, 3$.

(see § 8.4), so

$$H(f) = \{(1,0,0), (p,0,-1), (0,p,-1), (p^2,0,-2), (0,p^2,-2)\}.$$

We claim that the line segment $\overline{(p,0)(p^2,0)}$ is a cell of $\mathrm{New}(f)$, i.e. that there exists $w \in \boldsymbol{R}^2_{\geqslant 0}$ such that $\mathrm{In}_w(f) = \{(p,0,-1), (p^2,0,-2)\}$. Any such $w = (u,v)$ must satisfy $pu - 1 = p^2u - 2$ (see (8.10.4)), i.e. $u = 1/p(p-1)$, in addition to $pu - 1 < \min\{u, pv - 1, p^2v - 2\}$; this is true for all $v \gg 0$, which proves the claim. We can calculate all of the cells of $\mathrm{New}(f)$ in the same way: first we choose a subset $S \subset H(f)$, then we solve a system of linear equations and inequalities to determine if there exists $w \in \boldsymbol{R}^g_{\geqslant 0}$ such that $S = \mathrm{In}_w(f)$; if so, then $\mathrm{conv}(\pi(S))$ is a cell of $\mathrm{New}(f)$. The complex $\mathrm{New}(f)$ is drawn in figure 2.

Once we have drawn $\mathrm{New}(f)$, it is much easier to draw $\mathrm{Trop}(f)$. For instance, the cell P dual to $\overline{(0,p^2)(p^2,0)}$ is contained in the line

$$\{(u,v) \colon p^2u - 2 = p^2v - 2\} = \{(u,v) \colon u = v\} \quad \text{(again see (8.10.4))}.$$

Since $\overline{(0,p^2)(p^2,0)}$ is a face of the trapezoid with vertices $\{(p,0), (p^2,0), (0,p), (0,p^2)\}$, we know that P has the unique vertex (u,v) satisfying $pu - 1 = pv - 1 = p^2u - 2 = p^2v - 2$. Since $p^2u - 2 \ll 0$ when $u \ll 0$, we see that P is the ray $(1/p(p-1), 1/p(p-1)) + \boldsymbol{R}_{\geqslant 0}(-1,-1)$ intersected with $\boldsymbol{R}^2_{\geqslant 0}$. One can calculate all of the cells of $\mathrm{Trop}(f)$ in this way: any $P \in \mathrm{Trop}(f)$ is dual to a unique positive-dimensional cell $P' \in \mathrm{New}(f)$, and P can be recovered from P' as in § 8.10.3. The tropicalization of f is also illustrated in figure 2.

Example 8.13. When $g = 1$, tropical geometry basically reduces to the classical theory of the Newton polygon, as follows. For a non-zero $f = \sum_{\nu \geqslant 0} a_\nu X^\nu \in T_{1,\rho}$, the Newton polygon of f is by definition the set $\mathcal{N}(f) = \bigcup_{w \in \boldsymbol{R}_{\geqslant r}} \mathrm{conv}(\mathrm{In}_w(f))$. Hence the support of Newton complex is the projection of $\mathcal{N}(f)$ onto $\boldsymbol{R}$; the polytopal complex structure

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

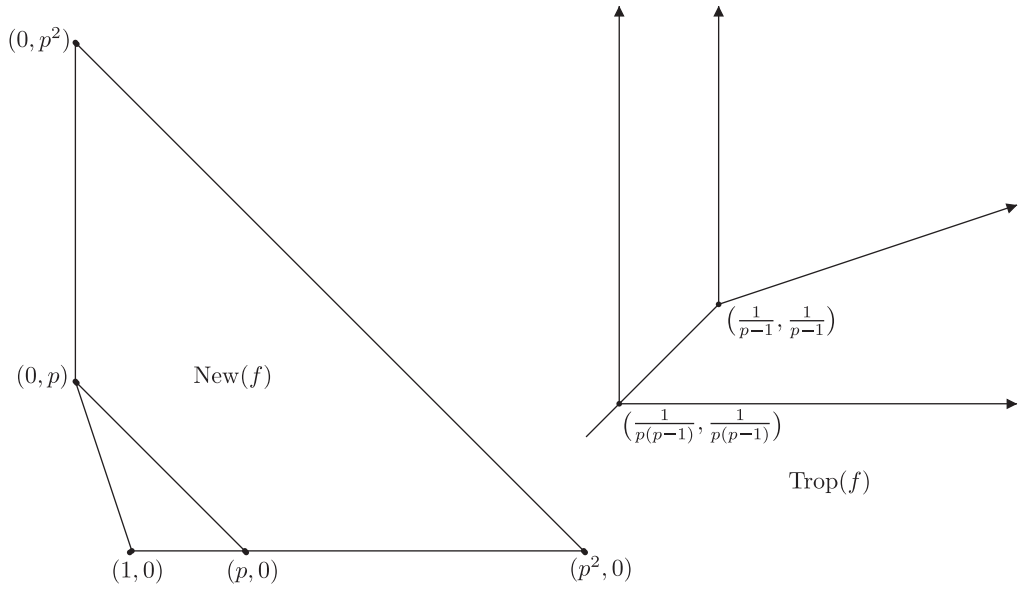

Figure 2. The Newton complex and tropicalization of the polynomial f of Example 8.12.

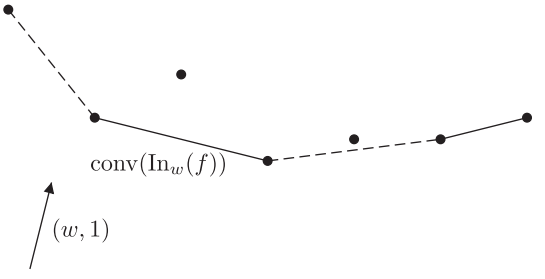

Figure 3. The Newton polygon of a polynomial f. The vertices in the figure are the points of the height graph $H(f)$, and the union of the (dotted and solid) lines is the Newton polygon of f. For the choice of w indicated in the figure, $\mathrm{In}_w(f)$ contains two points, so $w \in \mathrm{Trop}(f)$; the slope of the line segment $\mathrm{conv}(\mathrm{In}_w(f))$ joining these two points is $-w$.

simply remembers the horizontal lengths of the line segments $\mathrm{conv}(\mathrm{In}_w(f))$. As illustrated in figure 3, an element $w \in \boldsymbol{R}_{\geqslant r}$ is in $\mathrm{Trop}(f)$ if and only if $-w$ is the slope of a line segment (of positive length) in $\mathcal{N}(f)$; this recovers the fact that if ξ is a zero of f then $-\operatorname{ord}(\xi)$ is the slope of a line segment of $\mathcal{N}(f)$. In fact, the tropicalization of f along with its Newton complex is enough to recover the valuations and multiplicities of all of the zeros of f using the theory of the Newton polygon.

There is an analogue of this fact in higher dimensions. Namely, if $f_1, \ldots, f_g \in T_{g,\rho}$ are non-zero and $w \in \bigcap_{i=1}^{g} \mathrm{Trop}(f_i)$ is an isolated point contained in $\boldsymbol{R}^g_{>r}$ then there is a formula based on the 'sizes' of the cells of the Newton complexes of the f_i that calculates the (finite, non-zero) number of points $\xi \in \boldsymbol{T}^g_K(\rho)(\bar{K})$ (counted with multiplicity) such that $\operatorname{ord}(\xi) = w$ and $f_i(\xi) = 0$ for all i. This follows from an analogous result for Laurent

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

polynomials proved by Eric Katz, Sam Payne and Brian Osserman; see [**28**, § 11] for a statement and proof.

8.14. The tropicalization and Newton complex of a non-zero power series f only depend on its height graph, and are therefore insensitive to extension of the ground field. More precisely, let K' be a complete valued extension of K, let $f \in T_{K,g,\rho}$, and let f' be the image of f in $T_{K',g,\rho}$. Then $\mathrm{Trop}(f) = \mathrm{Trop}(f')$ and $\mathrm{New}(f) = \mathrm{New}(f')$.

8.15. Let f be a non-zero power series converging on the open unit g-ball $\boldsymbol{D}_K^g$, and for $0 < \rho < 1$ let f_ρ be the image of f in $T_{g,\rho}$. Let $0 < \rho' < \rho$, let $r = -\log_p(\rho) > 0$, and let $r' = -\log_p(\rho') > r$. It is clear that $\mathrm{Trop}(f_\rho) \cap \boldsymbol{R}^g_{\geqslant r'} = \mathrm{Trop}(f_{\rho'})$, so if we define

$$\mathrm{Trop}(f) = \bigcup_{\rho > 0} \mathrm{Trop}(f_\rho)$$

(as a subset of $\boldsymbol{R}^g_{>0}$) then $\mathrm{Trop}(f) \cap \boldsymbol{R}^g_{\geqslant r} = \mathrm{Trop}(f_\rho)$ for all ρ. This set is the union

$$\bigcup_{w \in \boldsymbol{R}^g_{>0}} P_w, \quad \text{where } P_w = \{w' \in \boldsymbol{R}^g_{>0} \colon \mathrm{in}_w(f) \subset \mathrm{in}_{w'}(f)\},$$

the intersection of a polyhedron with $\boldsymbol{R}^g_{>0}$. Hence $\mathrm{Trop}(f)$ is a 'polyhedral complex' with infinitely many cells. We also let $\mathrm{New}(f) = \bigcup_{\rho>0} \mathrm{New}(f_\rho)$; again this would 'almost' be a polyhedral complex if it had finitely many cells. In any case we have a bijective correspondence $P_w \leftrightarrow C_w$, so we will still say that P_w and C_w are *dual cells*. We will call $\mathrm{Trop}(f)$ the tropicalization of f and $\mathrm{New}(f)$ the infinite Newton complex of f. In what follows all power series f will converge on $\boldsymbol{D}_K^g$, so this ambiguity of notation will hopefully not cause confusion.

Alternatively, in the calculations in the following sections involving $\mathrm{Trop}(f)$ and $\mathrm{New}(f)$, we could always work with $\mathrm{Trop}(f_\rho)$ and $\mathrm{New}(f_\rho)$ for a fixed (small) value of ρ.

8.16. Suppose that $f_1, \dots, f_g$ are non-zero power series in g variables converging on $\boldsymbol{D}_K^g$. Clearly, if $\xi = (\xi_1, \dots, \xi_g) \in (\boldsymbol{D}_K^1(\bar{K}) \setminus \{0\})^g$ is a common root of the f_i then $\mathrm{ord}(\xi)$ must be contained in the intersection $\bigcap_{i=1}^g \mathrm{Trop}(f_i)$. Let $\mathscr{X}_i \subset (\boldsymbol{D}_K^1 \setminus \{0\})^g$ be the hypersurface cut out by f_i and let $\mathscr{X} = \bigcap_{i=1}^g \mathscr{X}_i$. We will denote by ord the map $\mathscr{X}(\bar{K}) \to \bigcap_{i=1}^g \mathrm{Trop}(f_i)$.

9. The tropicalizations of $\log_1, \dots, \log_g$

9.1. Let $\mathcal{P}$ be a display over R and let $\log = (\log_1, \dots, \log_g)$ be its logarithm with respect to some choice of basis, as in § 5. In view of Proposition 6.8 and § 8.16, we would like to draw the tropical hypersurfaces $\mathrm{Trop}(\log_i)$ and locate their intersection points explicitly. However, this is a difficult problem in geometry and combinatorics when $g > 2$, so instead we will learn enough about the structure of $\mathrm{Trop}(\log_i)$ to allow us to perturb the coefficients of $\log_i$ without changing the number of roots in a suitable $\boldsymbol{B}_K^g(\rho)$. In this

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

spirit, we will study the tropical hypersurfaces of general g-tuples of convergent power series

$$f_i(X_1,\dots,X_g)=\sum_{j=1}^{g}\sum_{n=0}^{\infty}a_{n,ij}X_j^{p^n}\in K[\![X_1,\dots,X_g]\!],\quad i=1,\dots,g, \tag{9.1.1}$$

under specific hypotheses on the valuations $\mathrm{ord}(a_{n,ij})\in \boldsymbol{R}\cup\{\infty\}$ of the coefficients $a_{n,ij}$ for $n\geqslant 0$, $0\leqslant i,j\leqslant g$ which will be satisfied by the perturbations to be considered later on the coefficients of the $\log_i$. To this end, we fix the following data.

Data 9.2.

(i) Fix numbers $u_{n,ij}\in \boldsymbol{R}\cup\{\infty\}$ for $n=0,1,\dots$ and $i,j=1,2,\dots,g$ ($u_{n,ij}$ will be $\mathrm{ord}(a_{n,ij})$).

(ii) Fix an integer $N\geqslant 1$ (to be the level of the canonical subgroup we wish to find).

(iii) Fix a non-negative real number $H<(p-1)/p^N$ (to be the Hasse invariant).

(iv) Fix non-negative real numbers $U_1,\dots,U_g$ with

$$\sum_{i=1}^{g}U_i=H$$

(U_i will be $\mathrm{ord}(w_0(\alpha_{ii}))$).

9.2.1. Let N_i be the largest integer such that

$$\frac{p^{N_i}-1}{p-1}U_i<1$$

(if $U_i=0$ we set $N_i=\infty$). Since

$$\frac{p^N-1}{p-1}U_i\leqslant\frac{p^N-1}{p-1}H<\frac{p^N-1}{p^N}<1,$$

we see that $N_i\geqslant N$ for all i. We require the following.

Hypotheses 9.2.2.

(i) $u_{0,ii}=0$ for $i=1,\dots,g$ and $u_{0,ij}=\infty$ for $i\neq j$.

(ii) $u_{n,ii}=((p^n-1)/(p-1))U_i-n$ for $1\leqslant n\leqslant N_i$.

(iii) $u_{n,ii}\geqslant 1-n$ whenever $n>N_i$.

(iv) $u_{n,ij}\geqslant -n$ for all $1\leqslant i,j\leqslant g$ and all $n\geqslant 0$, and furthermore $u_{n,ij}\geqslant 1-n$ when $i>j$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

9.2.3. Let f_i be any power series of the form (9.1.1) such that the data $(u_{n,ij}, N, H, U_i)$ satisfy Hypotheses 9.2.2 with $u_{n,ij} = \operatorname{ord}(a_{n,ij})$. Note that Hypotheses (ii) and (iii) imply Hypothesis (iv) for $i = j$, and Hypothesis (iv) guarantees that the f_i converge on the open unit g-ball. As another immediate consequence of Hypotheses 9.2.2, we have the following lemma.

Lemma 9.2.4. *Let $\mathcal{U} = (u_{n,ij}, N, H, U_i)$ be a set of data satisfying Hypotheses 9.2.2.*

(i) *If $1 \leqslant N' < N$ then $(u_{n,ij}, N', H, U_i)$ is also a set of data satisfying Hypotheses 9.2.2.*

(ii) *If $u'_{n,ij} \geqslant u_{n,ij}$ for all $n \geqslant 0$ and all $i \neq j$ and $u'_{n,ii} = u_{n,ii}$ for all $n \geqslant 0$ and all i then $(u'_{n,ij}, N, H, U_i)$ is also a set of data satisfying Hypotheses 9.2.2.*

(iii) *Suppose that $g > 1$. Choose $i \in \{1, \dots, g\}$, and let $H' = \sum_{j \neq i} U_j$. Then*

$$(\{u_{n,i'j}\}_{i',j \neq i}, N, H', \{U_{i'}\}_{i' \neq i})$$

is a set of data satisfying Hypotheses 9.2.2 for $g - 1$.

9.3. The first step in understanding $\operatorname{Trop}(f_i)$ is to analyse the infinite Newton complex $\operatorname{New}(f_i)$. It is clear that all of the vertices of $\operatorname{New}(f_i)$ are contained on the coordinate axes, since there are no mixed monomials in (9.1.1). Let $\boldsymbol{x}_i$ be the ith standard basis vector in $\boldsymbol{R}^g$ and let $L_i = \boldsymbol{R}\boldsymbol{x}_i$ be the $\boldsymbol{x}_i$-axis. Let

$$\Delta_i = \{\sigma \cap L_i \colon \sigma \in \operatorname{New}(f_i) \text{ and } \sigma \cap L_i \neq \emptyset\}.$$

Then Δ_i is a collection of line segments and vertices in L_i. As an exercise one can prove that Δ_i is naturally identified with the infinite Newton complex of the power series

$$\tilde{f}_i(X) = f_i(0, \dots, X, \dots, 0) = \sum_{n=0}^{\infty} a_{n,ii} X^{p^n}, \tag{9.3.1}$$

and that any cell in Δ_i is a cell in $\operatorname{New}(f_i)$. Note that by Lemma 9.2.4 (iii), $\tilde{f}_i$ satisfies Hypotheses 9.2.2 for $g = 1$. The following proposition is illustrated in figure 4.

Proposition 9.4. *Choose $1 \leqslant i \leqslant g$ and n such that $0 \leqslant n < N_i$. The line segment joining $p^n \boldsymbol{x}_i$ and $p^{n+1} \boldsymbol{x}_i$ is a cell in Δ_i.*

Proof. By the above remarks, we may replace f_i with $f_i(0, \dots, X_i, \dots, 0)$; hence we may and do assume that $g = 1$ and $f = f_1$. This is now a question about the Newton polygon of f (see Example 8.13). Let $u_n = u_{n,11}$ and $U = U_1$. We need to show that the line passing through the points (p^n, u_n) and (p^{n+1}, u_{n+1}) lies strictly below every point (p^m, u_m) with $m \neq n, n+1$, i.e. that the linear form $\omega \colon (x, y) \mapsto (u_n - u_{n+1})x + p^n(p-1)y$ evaluated at points (p^m, u_m) for $m \geqslant 0$ achieves its minimum at (p^n, u_n) and (p^{n+1}, u_{n+1}). If $1 \leqslant n < N_i$ then

$$u_n - u_{n+1} = \frac{p^n - 1}{p - 1} U - n - \frac{p^{n+1} - 1}{p - 1} U + n + 1 = 1 - p^n U,$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

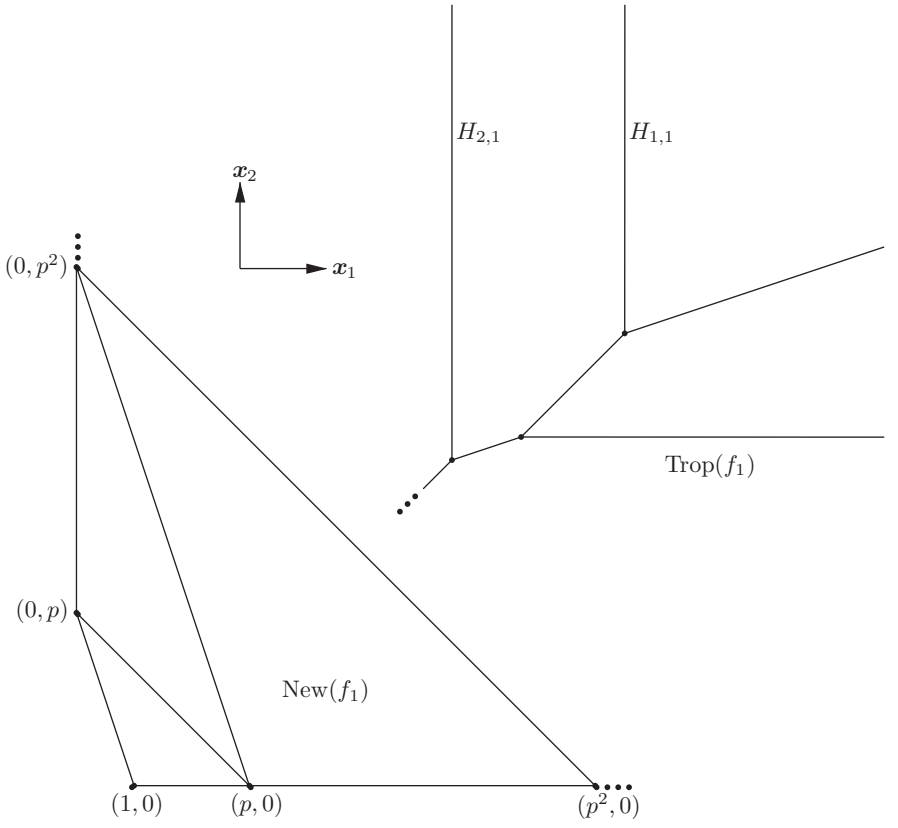

Figure 4. An example of what finite approximations to $\mathrm{New}(f_1)$ and $\mathrm{Trop}(f_1)$ can look like for f_1 as in (9.1.1) when $g = 2$ (the ellipses indicate that the full infinite Newton complex, respectively tropicalization, continue in the given direction). Since there are no mixed monomial terms in the power series f_1, all of the vertices of $\mathrm{New}(f_1)$ are contained on the coordinate axes. The infinite Newton complex of the power series $\tilde{f}_1$ of (9.3.1) is identified with the part of $\mathrm{New}(f_1)$ contained in the line $\boldsymbol{x}_2 = 0$, as in Proposition 9.4. The ray $H_{n,1}$ is the dual cell to the line segment $\overline{(p^{n-1},0)(p^n,0)}$ in $\mathrm{New}(f_1)$.

and if $n = 0$ then

$$u_0 - u_1 = 0 - (U - 1) = 1 - p^n U$$

as well. Choose any point (m, u_m) with $m \neq n, n+1$. We want the quantity

$$\omega(p^m, u_m) - \omega(p^n, u_n) = (1 - p^n U)(p^m - p^n) + p^n(p-1)(u_m - u_n) \tag{9.4.1}$$

to be positive.

9.4.2. We treat the case $n = 0$ separately. In this case $m > 1$, and (9.4.1) becomes

$$\omega(p^m, u_m) - \omega(1, 0) = (1 - U)(p^m - 1) + (p-1)u_m.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Suppose that $u_m = ((p^m-1)/(p-1))U - m$. Then (9.4.1) is equal to

$$(1-U)(p^m-1) + (p^m-1)U - m(p-1) = p^m - 1 - m(p-1),$$

which is positive because $p^m - 1 > m(p-1)$ for $m \geqslant 2$, since $((p^m-1)/(p-1)) = 1+p+\cdots+p^{m-1}$. If $u_m \neq ((p^m-1)/(p-1))U - m$ then $m > N_1$, and by Hypothesis 9.2.2 (iii) we have $u_m \geqslant 1-m$. Hence (9.4.1) becomes

$$(1-U)(p^m-1) + (p-1)u_m \geqslant (1-U)(p^m-1) - (p-1)(m-1).$$

Now $U \leqslant H < (p-1)/p^N \leqslant (p-1)/p$, so $1-U \geqslant 1/p$. Hence

$$(1-U)(p^m-1) + (p-1)u_m \geqslant \frac{1}{p}(p^m-1) - (p-1)(m-1).$$

Again one can check that $p^m - 1 > p(p-1)(m-1)$ for $m \geqslant 2$.

9.4.3. Now assume $n \geqslant 1$, and suppose that $u_m = ((p^m-1)/(p-1))U - m$. Then (9.4.1) is equal to

$$(1-p^nU)(p^m-p^n) + p^n(p-1)\left(\frac{p^m-1}{p-1}U - \frac{p^n-1}{p-1}U - m + n\right) \\ = p^m - p^n + p^n(p-1)(n-m). \quad (9.4.4)$$

When $m \geqslant n+2$ this quantity is positive because

$$\frac{p^{m-n}-1}{p-1} = p^{m-n-1} + p^{m-n-2} + \cdots + p + 1 > m - n.$$

When $m < n$, (9.4.4) is also positive since

$$(p-1)(n-m) > 1 - p^{m-n}.$$

9.4.5. If $u_m \neq ((p^m-1)/(p-1))U - m$ then either $m = 0$ (so $u_m = 0$) or else $m > N_1$ (so $m \geqslant n+2$), in which case $u_m \geqslant 1-m$. First suppose that $m > N_1$, so (9.4.1) is greater than or equal to

$$\begin{aligned}(1-p^nU)(p^m-p^n) - p^n(p^n-1)U + p^n(p-1)(n-m+1) \\ &= (1-p^nU)p^m - (1-U)p^n + p^n(p-1)(n-m+1) \\ &> \left(1 - \frac{p-1}{p}\right)p^m - p^n + p^n(p-1)(n-m+1) \\ &= p^{m-1} - p^n + p^n(p-1)(n-m+1),\end{aligned}$$

where the second-to-last step comes from the fact that

$$U \leqslant H < \frac{p-1}{p^N} \leqslant \frac{p-1}{p^{n+1}}.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

But $p^{m-1} - p^n + p^n(p-1)(n-m+1)$ is non-negative because

$$\frac{p^{m-n-1}-1}{p-1} \geqslant m-n-1$$

for all $m \geqslant n+2$. If instead $m=0$ then (9.4.1) is

$$\begin{aligned}(1-p^nU)(1-p^n) - p^n(p-1)u_n &= (1-p^nU)(1-p^n) - p^n(p-1)\left(\frac{p^n-1}{p-1}U - n\right)\\ &= 1 + p^n(n(p-1)-1) \geqslant 1\end{aligned}$$

because $n(p-1) \geqslant 1$ when $n \geqslant 1$. □

Example 9.5. Suppose that $g=1$, and let $U = U_1 = H$ and $u_n = u_{n,11}$. Let $N=1$, and assume that $u_0 = 0$, $u_1 = U-1$ and $u_2 = -1$. If the line segment joining $\boldsymbol{x}_1$ and $p\boldsymbol{x}_1$ is a cell in $\Delta = \Delta_1$ then the point (p, u_1) is below the line segment joining $(1, u_0)$ and (p^2, u_2); an elementary calculation shows that this happens precisely when $U = H < p/(p+1)$. It is not a coincidence that $p/(p+1)$ is Katz's bound on the Hasse invariant of an elliptic curve that suffices for its level-1 canonical subgroup to exist; see § 1.10, Remark 7.10.1 (ii) and Remark 9.8.

9.6. Proposition 9.4 says that the line segment joining $p^{n-1}\boldsymbol{x}_i$ and $p^n\boldsymbol{x}_i$ is a cell in $\mathrm{New}(f_i)$ when $1 \leqslant n \leqslant N$; let $H_{n,i}$ be its dual cell in $\mathrm{Trop}(f_i)$.

Lemma 9.7. *Let $1 \leqslant i \leqslant g$ and let $1 \leqslant n \leqslant N$ (so $n \leqslant N_i$).*

(i) *The cell $H_{n,i}$ is contained in the affine hyperplane defined by the equation*

$$x_i = \frac{1}{p^{n-1}(p-1)} - \frac{U_i}{p-1} \geqslant \frac{1}{p^{N-1}(p-1)} - \frac{H}{p-1} > \frac{1}{p^N(p-1)}.$$

(ii) *If H is the dual cell in $\mathrm{Trop}(f_i)$ to any other cell of Δ_i then it is contained in the affine hyperplane defined by the equation $x_i = r$ for some $r \leqslant 1/(p^N(p-1))$.*

Proof. For $m', m \in \boldsymbol{Z}_{\geqslant 0}$ with $m' < m$ let $I_{m',m}$ be the line segment joining $p^{m'}\boldsymbol{x}_i$ and $p^m\boldsymbol{x}_i$, and when $u_{m',ii}, u_{m,ii} \neq \infty$ let $r_{m',m} = (u_{m',ii} - u_{m,ii})/p^{m'}(p^{m-m'}-1)$, so $-r_{m',m}$ is the slope of the line segment joining $(p^{m'}, u_{m',ii})$ and $(p^m, u_{m,ii})$ in $\boldsymbol{R}^2$. (For the first part of the lemma, we will be interested in the case $m' = m-1$ with $1 \leqslant m \leqslant N$.) As explained in § 8.10.3, if $I_{m',m}$ is a cell in Δ_i and $x = (x_1, \ldots, x_g) \in \boldsymbol{R}^g_{>0}$ is contained in its dual cell H then $p^{m'}x_i + u_{m',ii} = p^m x_i + u_{m,ii}$, i.e. $x_i = r_{m',m}$. Hence by Example 8.13, this is a question about the Newton polygon of the power series $f_i(0, \ldots, X_i, \ldots, 0)$, so as in the proof of Proposition 9.4 we can assume $g=1$. Let $\Delta = \Delta_1$, let $u_n = u_{n,11}$ and $U = U_1$. Part (i) now follows immediately from the calculation

$$r_{n-1,n} = \frac{u_{n-1} - u_n}{p^{n-1}(p-1)} = \frac{1-p^{n-1}U}{p^{n-1}(p-1)} = \frac{1}{p^{n-1}(p-1)} - \frac{U}{p-1}.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Let $I_{m,m'}$ be a cell in Δ for some $m, m' \in \boldsymbol{Z}$ such that $N \leqslant m' < m$, so its dual cell is the point $\{r_{m',m}\}$. If $I_{m'',m'}$ is also a cell in Δ for some $N \leqslant m'' < m'$ then $-r_{m'',m'} < -r_{m',m}$ (i.e. $r_{m',m} < r_{m'',m'}$) because the slopes of the line segments in a Newton polygon are monotonically increasing; thus we may assume that $m' = N$. If $N < N_i$ then $m = N+1$ and $r_{N,N+1} = 1/p^N(p-1) - U/(p-1)$ as above, so we may assume that $N = N_i$ (unless $N_i = \infty$, in which case we are done), and hence $u_m \geqslant 1-m$ by Hypothesis 9.2.2 (iii). We therefore have (by Hypotheses 9.2.2 (ii),(iii))

$$\begin{aligned} r_{N,m} &= \frac{u_N - u_m}{p^N(p^{m-N}-1)} \\ &\leqslant \frac{((p^N-1)/(p-1))U - N + m - 1}{p^N(p^{m-N}-1)} \\ &< \frac{m-N}{p^N(p^{m-N}-1)} \quad \left(\text{using } U \leqslant H < \frac{p-1}{p^N}\right). \end{aligned}$$

But this quantity is at most $1/p^N(p-1)$ since for $k \geqslant 1$ we have

$$\frac{k}{p^N(p^k-1)} \leqslant \frac{1}{p^N(p-1)},$$

as one easily checks. □

Remark 9.8. When $\mathcal{P}$ is a display of dimension $g = 1$ over R, Proposition 9.4 and Lemma 9.7 effectively calculate the Newton polygon of the logarithm $\log = \log_1$ with respect to some choice of basis, as follows. We will prove (Proposition 10.6) that if $\log = \sum a_n X^n$ then the data $(\mathrm{ord}(a_n), N, H, H)$ satisfy Hypotheses 9.2.2, so Proposition 9.4 shows that for $1 \leqslant n \leqslant N$ the line segment σ_n joining $(p^{n-1}, \mathrm{ord}(a_{n-1}))$ and $(p^n, \mathrm{ord}(a_n))$ is in $\mathcal{N}(\log)$. By Lemma 9.7 the slope of σ_n is $-(1/p^{n-1}(p-1) - H/(p-1)) < -1/p^N(p-1)$, and the slope of any other line segment in $\mathcal{N}(\log)$ is at least $-1/p^N(p-1)$. Hence $\log$ has $p^n - p^{n-1}$ roots with valuation $1/p^{n-1}(p-1) - H/(p-1)$, and this accounts for all non-zero roots of $\log$ with valuation at least $r := 1/p^{N-1}(p-1) - H/(p-1)$. Therefore, $\log$ has a total of

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

roots in the ball $\boldsymbol{B}_K^g(\rho)$ where $\rho = p^{-r}$. We will also show (Lemma 11.7) that $(\mathscr{G}[p^\infty] \cap \boldsymbol{B}_K^g(\rho))(\bar{K}) \cong \boldsymbol{Z}/p^n\boldsymbol{Z}$ (so $\mathscr{G}[p^\infty] \cap \boldsymbol{B}_K^g(\rho) = G[p^N]_{\leqslant\rho}$), which proves Theorem 7.12 for $g = 1$.

Proposition 9.9. *Let $r = 1/p^N(p-1)$, let $1 \leqslant i \leqslant g$, and let $x = (x_1, \ldots, x_g) \in \mathrm{Trop}(f_i) \cap \boldsymbol{R}^g_{>r}$. Suppose that $x \notin H_{n,i}$ for $n = 1, \ldots, N$ (so $g \geqslant 2$; see Remark 9.8). Then there exists $j \neq i$ such that*

$$x_i - x_j \geqslant \frac{\varepsilon_{i>j}}{p^N} - \frac{U_i}{p-1},$$

where $\varepsilon_{i>j} = 1$ if $i > j$ and is 0 otherwise.

Proposition 9.9 is illustrated in figure 5.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Proof. To say that $x \in \mathrm{Trop}(f_i)$ means that $\mathrm{in}_x(f_i)$ is not a monomial. Hence there are m, m' and j, j' with $(m,j) \neq (m',j')$ such that $p^m x_j + u_{m,ij} = p^{m'} x_{j'} + u_{m',ij'}$, and $p^m x_j + u_{m,ij} \leqslant p^{m''} x_{j''} + u_{m'',ij''}$ for all m'', j''. Since $x_i > r$, either $j \neq i$ or $j' \neq i$, because otherwise x would be contained in the dual cell to a cell of Δ_i and hence would lie on some $H_{n,i}$ by Lemma 9.7 (ii). Therefore, without loss of generality we can assume that $j \neq i$. Then we have

$$p^m x_j + u_{m,ij} \leqslant p^n x_i + u_{n,ii}$$

for all $n \geqslant 0$. We now consider two separate cases.

(i) Suppose that $m \leqslant N$ (so $m \leqslant N_i$). Then $p^m x_j + u_{m,ij} \leqslant p^m x_i + u_{m,ii}$ implies

$$\begin{aligned} x_i - x_j &\geqslant \frac{u_{m,ij} - u_{m,ii}}{p^m} \\ &\geqslant \frac{\varepsilon_{i>j} - m + m - ((p^m-1)/(p-1))U_i}{p^m} \quad \text{(by Hypotheses 9.2.2 (ii),(iii))} \\ &= \frac{\varepsilon_{i>j}}{p^m} - \frac{p^m-1}{p^m}\frac{U_i}{p-1} \\ &\geqslant \frac{\varepsilon_{i>j}}{p^m} - \frac{U_i}{p-1} \\ &\geqslant \frac{\varepsilon_{i>j}}{p^N} - \frac{U_i}{p-1}. \end{aligned}$$

(ii) Now suppose that $m > N$. Then $p^m x_j + u_{m,ij} \leqslant p^N x_i + u_{N,ii}$ implies

$$\begin{aligned} x_i - x_j &\geqslant (p^{m-N}-1)x_j + \frac{1}{p^N}(u_{m,ij} - u_{N,ii}) \\ &\geqslant \frac{p^{m-N}-1}{p^N(p-1)} + \frac{\varepsilon_{i>j} - m + N - ((p^N-1)/(p-1))U_i}{p^N} \\ &\geqslant \frac{p^{m-N} - 1 - (p-1)(m-N)}{p^N(p-1)} + \frac{\varepsilon_{i>j}}{p^N} - \frac{U_i}{p-1}, \end{aligned}$$

where we have used $x_j > r = 1/p^N(p-1)$. Hence we need only show that for $k = m - N \geqslant 1$ we have $p^k - 1 \geqslant (p-1)k$, which is easily checked.

□

The main result concerning the structure of $\mathrm{Trop}(f_i)$ is as follows.

Theorem 9.10. *Let*

$$r = \frac{1}{p^N(p-1)} \quad \text{and} \quad r' = \frac{1}{p^{N-1}(p-1)} - \frac{H}{p-1},$$

so $r' > r$ since $H < (p-1)/p^N$. Then

$$\bigcap_{i=1}^{g} \mathrm{Trop}(f_i) \cap \boldsymbol{R}^g_{>r} = \bigcap_{i=1}^{g} \mathrm{Trop}(f_i) \cap \boldsymbol{R}^g_{\geqslant r'} \quad \text{and} \quad \bigcap_{i=1}^{g} \mathrm{Trop}(f_i) \cap \boldsymbol{R}^g_{>1/(p-1)} = \emptyset.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

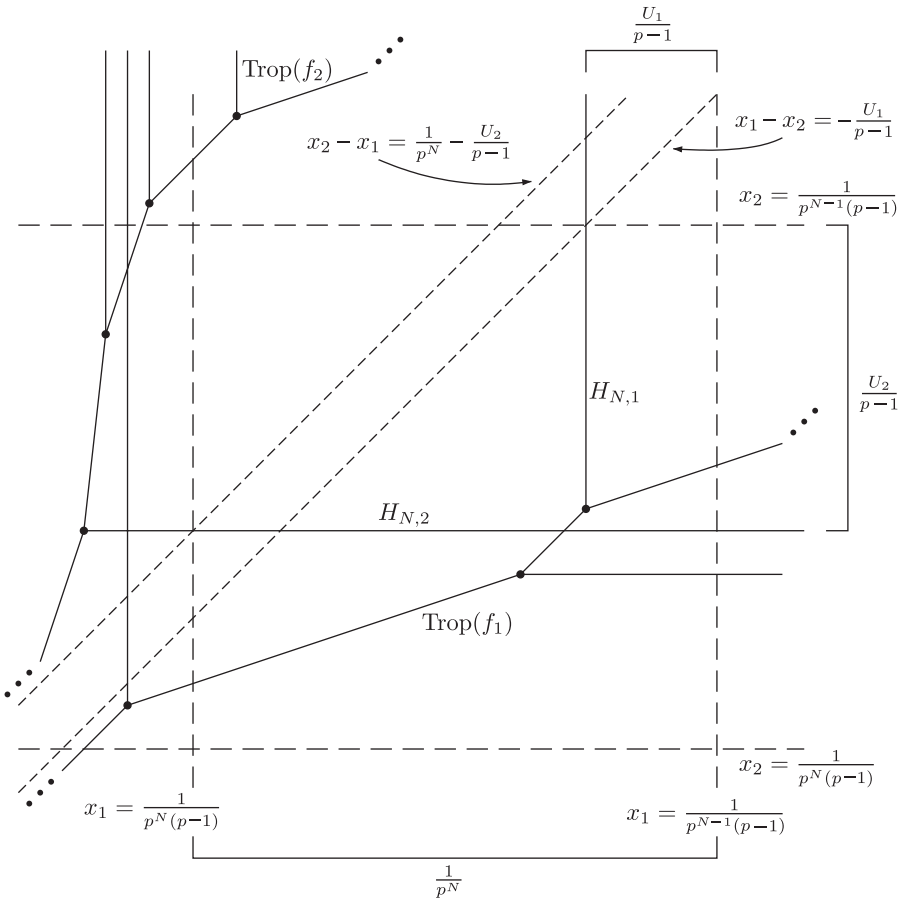

Figure 5. This figure illustrates Proposition 9.9. Let $r = 1/p^N(p-1)$. The vertical rays in $\mathrm{Trop}(f_1) \cap \boldsymbol{R}^2_{>r}$ are the cells $H_{n,1}$, and the horizontal rays in $\mathrm{Trop}(f_2) \cap \boldsymbol{R}^2_{>r}$ are the cells $H_{n,2}$, see § 8.10.5 and Lemma 9.7. In the region $x_1, x_2 > r$, every point on $\mathrm{Trop}(f_1)$ not contained in $H_{n,1}$ for $1 \leqslant n \leqslant N$ lies below the dotted line $x_1 - x_2 = -U_1/(p-1)$, and any point on $\mathrm{Trop}(f_2)$ not contained in $H_{n,2}$ for $1 \leqslant n \leqslant N$ lies above the dotted line $x_2 - x_1 = 1/p^N - U_2/(p-1)$. As the regions $\{(x_1, x_2) \colon x_1 - x_2 \geqslant -U_1/(p-1)\}$ and $\{(x_1, x_2) \colon x_2 - x_1 \geqslant 1/p^N - U_2/(p-1)\}$ do not intersect, this implies that any point of $\mathrm{Trop}(f_1) \cap \mathrm{Trop}(f_2) \cap \boldsymbol{R}^2_{>r}$ is located on some ray $H_{n,1}$ or $H_{n,2}$, as in the proof of Theorem 9.10. (Note that many such intersection points will lie above or to the right of the figure.)

Proof. Let $x = (x_1, \dots, x_g) \in \bigcap_{i=1}^g \mathrm{Trop}(f_i) \cap \boldsymbol{R}^g_{>r}$. Choose $1 \leqslant i_1 \leqslant g$; we want to show that $x_{i_1} \geqslant r'$. If $x \in H_{m,i_1}$ for some $1 \leqslant m \leqslant N$ then $x_i \geqslant r'$ by Lemma 9.7, so we may restrict our attention to the case $x \notin \bigcup_{m=1}^N H_{m,i_1}$. By Proposition 9.9, there exists $1 \leqslant i_2 \leqslant g$ with $i_2 \neq i_1$ such that

$$x_{i_1} - x_{i_2} \geqslant \frac{\varepsilon_{i_1 > i_2}}{p^N} - \frac{U_{i_1}}{p-1}.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Continuing in this fashion, there are pairwise distinct integers $i_1, i_2, \ldots, i_n \in \{1, \ldots, g\}$ for some $2 \leqslant n \leqslant g$ such that for each $j < n$ we have

$$x \notin \bigcup_{m=1}^{N} H_{m,i_j} \quad \text{and} \quad x_{i_j} - x_{i_{j+1}} \geqslant \frac{\varepsilon_{i_j > i_{j+1}}}{p^N} - \frac{U_{i_j}}{p-1}. \tag{$*$}$$

We may assume that there is no $i_{n+1} \notin \{i_1, \ldots, i_n\}$ such that $i_1, \ldots, i_{n+1}$ satisfies $(*)$ for all $j < n+1$, which is to say that either

(i) there exists an $i_{n+1} = i_\ell$ for some $\ell < n$ satisfying $(*)$ for $j = n$, or

(ii) $x \in \bigcup_{m=1}^{N} H_{m,i_n}$.

We claim that case (i) cannot happen. If (i) occurs then

$$0 = \sum_{j=\ell}^{n} (x_{i_j} - x_{i_{j+1}}) \geqslant \frac{\sum_{j=\ell}^{n} \varepsilon_{i_j > i_{j+1}}}{p^N} - \frac{\sum_{j=\ell}^{n} U_{i_j}}{p-1}.$$

Since $i_\ell = i_{n+1}$, at least one $\varepsilon_{i_j > i_{j+1}}$ is 1, and since $\sum_{j=1}^{g} U_j = H$ we have $\sum_{j=\ell}^{n} U_{i_j} \leqslant H$. Hence

$$0 \geqslant \frac{1}{p^N} - \frac{H}{p-1} > 0,$$

a contradiction. Therefore, $x \in H_{m,i_n}$ for some $1 \leqslant m \leqslant N$, so

$$x_{i_n} = \frac{1}{p^{m-1}(p-1)} - \frac{U_{i_n}}{p-1} \geqslant \frac{1}{p^{N-1}(p-1)} - \frac{U_{i_n}}{p-1}.$$

Hence

$$\begin{aligned} x_{i_1} &= (x_{i_1} - x_{i_n}) + x_{i_n} \\ &= \sum_{j=1}^{n-1} (x_{i_j} - x_{i_{j+1}}) + x_{i_n} \\ &\geqslant \frac{\sum_{j=1}^{n-1} \varepsilon_{i_j > i_{j+1}}}{p^N} - \frac{\sum_{j=1}^{n-1} U_{i_j}}{p-1} + \frac{1}{p^{N-1}(p-1)} - \frac{U_{i_n}}{p-1} \\ &\geqslant \frac{1}{p^{N-1}(p-1)} - \frac{\sum_{j=1}^{n} U_{i_j}}{p-1} \\ &\geqslant \frac{1}{p^{N-1}(p-1)} - \frac{H}{p-1} \\ &= r'. \end{aligned}$$

For the final assertion, since

$$\frac{1}{p-1} \geqslant \frac{1}{p^{m-1}(p-1)} - \frac{U_i}{p-1}$$

for $1 \leqslant m \leqslant N$, any point $x \in \bigcap_{i=1}^{g} \mathrm{Trop}(f_i) \cap \boldsymbol{R}^g_{>1/(p-1)}$ is not contained on any hyperplane $H_{m,i}$ by Lemma 9.7 (i). But we showed above that this is impossible. □

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

10. Counting the common roots of $(\log_1, \dots, \log_g)$

10.1. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R and let $P = T \oplus L$ be a normal decomposition, let $e_1, \dots, e_g$ and $e_{g+1}, \dots, e_h$ be $W(R)$-bases for T and L, respectively, and let $M = (\alpha_{ij})$ be the structure matrix for $\mathcal{P}$ with respect to this basis, as in (5.1.1). Let $G = \mathrm{BT}_{\mathcal{P}}$ be the associated p-divisible formal group over R (of dimension g and height h), and let $\mathscr{G}$ be its rigid generic fibre. Let $\log = (\log_1, \dots, \log_g)$ be the logarithm of G, calculated in terms of $\mathcal{P}$ using (5.5.3).

Notation 10.2. We will use the following notation in this section and the next. For $n \geqslant 0$, define

$$r_n = \frac{1}{p^n(p-1)} \quad \text{and} \quad r'_n = \frac{1}{p^{n-1}(p-1)} - \frac{H}{p-1},$$

where $H = H(G)$. We also set $\rho_n = p^{-r_n}$ and $\rho'_n = p^{-r'_n}$. Note that if $H < (p-1)/p^n$ then $r_n < r'_n$ and $\rho_n > \rho'_n$.

If $\mathscr{X} \subset \boldsymbol{D}_K^g$ is any analytic subspace and $\rho \in \sqrt{|K^\times|}$, $0 < \rho \leqslant 1$, we define

$$\mathscr{X}_{\leqslant \rho} := \mathscr{X} \cap \boldsymbol{B}_K^g(\rho) \quad \text{and} \quad \mathscr{X}_{<\rho} := \mathscr{X} \cap \boldsymbol{D}_K^g(\rho).$$

10.3. We will use the results of § 9 and a continuity of roots argument to count the number of points in the set $\mathscr{G}[p^\infty]_{\leqslant \rho'_n}(\bar{K})$ when $H < (p-1)/p^n$, i.e. to count the number of common zeros of $(\log_1, \dots, \log_g)$ whose coordinates have absolute value at most ρ'_n. (It will turn out that $\mathscr{G}[p^\infty]_{\leqslant \rho'_n} = G[p^n]_{\leqslant \rho'_n}$ when $H(G) < (p-1)/p^n$.) Specifically, we will prove the following proposition.

Proposition 10.4. *Fix an integer $N \geqslant 1$, and assume that $H(G) < (p-1)/p^N$. For $0 < n \leqslant N$, the group $\mathscr{G}[p^\infty]_{\leqslant \rho'_n}(\bar{K})$ has exactly p^{ng} points.*

10.5. Recall that we have defined $g \times h$ matrices $\boldsymbol{a}_n = (a_{n,ij})$ with entries in K for $n \geqslant 0$, calculated in terms of M using the equations (5.5.3), such that

$$\log_i(X_1, \dots, X_g) = \sum_{j=1}^{g} \sum_{n=0}^{\infty} a_{n,ij} X_j^{p^n} \in K[\![X_1, \dots, X_g]\!], \quad i = 1, \dots, g.$$

Our first task is to show that the coefficients $a_{n,ij}$ of $\log_1, \dots, \log_g$ satisfy Hypotheses 9.2.2. To this end, for the rest of this section we *fix an integer* $N \geqslant 1$, and we *assume that* $H = H(G) < (p-1)/p^N$. We also let $U_i = \mathrm{ord}(w_0(\alpha_{ii}))$, so $\sum_{i=1}^g U_i = H$ (see § 7.15). Let $u_{n,ij} = \mathrm{ord}(a_{n,ij}) \in \boldsymbol{R} \cup \{\infty\}$ for $i = 1, 2, \dots, g$ and $j = 1, 2, \dots, h$. Note that $(\{u_{n,ij}\}_{i,j=1,\dots,g}, N, H, U_i)$ forms a system of data as in § 9.2.

Proposition 10.6. *The data $(\{u_{n,ij}\}_{i,j=1,\dots,g}, N, H, U_i)$ satisfy Hypotheses 9.2.2.*

Proof. Hypothesis (i) is clear by (5.5.3). We will prove Hypotheses (ii)–(iv) by induction on n, the base case $n = 0$ being Hypothesis (i). We will also need the following inductive hypothesis:

$$u_{n,ij} \geqslant -n + 1 \quad \text{for } j > g, \tag{$*$}$$

which is satisfied for $n = 0$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

10.6.1. Suppose that Hypotheses (ii)–(iv) and (∗) are satisfied for some $n \geqslant 0$. Express the $h \times h$ structure matrix M in block-matrix form:

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

where A is a $g \times g$ matrix, D is an $(h-g) \times (h-g)$ matrix, C is an $(h-g) \times g$ matrix, and B is a $g \times (h-g)$ matrix. We also write $\boldsymbol{a}_n$ in the block form

$$\boldsymbol{a}_n = \begin{bmatrix} \boldsymbol{a}'_n & \boldsymbol{b}_n \end{bmatrix},$$

where $\boldsymbol{a}'_n$ is a $g \times g$ matrix and $\boldsymbol{b}_n$ is a $g \times (h-g)$ matrix. For brevity, if E is a matrix with coefficients in R, we will write $\mathrm{ord}(E) \geqslant \delta$ to mean that the valuation of every coefficient of E is at least δ. Hence Hypotheses (ii)–(iv) and (∗) imply

$$\mathrm{ord}(\boldsymbol{a}'_n) \geqslant -n, \qquad \mathrm{ord}(\boldsymbol{b}_n) \geqslant -n+1.$$

10.6.2. First we prove (∗) and Hypothesis (iv) for $n+1$. Writing out (5.5.3), we have

$$\begin{bmatrix} \boldsymbol{a}'_{n+1} & \boldsymbol{b}_{n+1} \end{bmatrix} = \begin{bmatrix} p^{-1}(\boldsymbol{a}'_n w_n(A) + \boldsymbol{b}_n w_n(C)) & \boldsymbol{a}'_n w_n(B) + \boldsymbol{b}_n w_n(D) \end{bmatrix}.$$

Since $\mathrm{ord}(\boldsymbol{a}'_n) \geqslant -n$, $\mathrm{ord}(\boldsymbol{b}_n) \geqslant 1-n$, and $\mathrm{ord}(w_n(M)) \geqslant 0$, we see that $\mathrm{ord}(\boldsymbol{b}_{n+1}) \geqslant -n = 1-(n+1)$, which proves (∗) for $n+1$. The same argument shows that $\mathrm{ord}(\boldsymbol{a}'_{n+1}) \geqslant -(n+1)$, i.e. $u_{n+1,ij} \geqslant -(n+1)$ for all i, j. Since $\mathrm{ord}(\boldsymbol{b}_n) \geqslant 1-n$, we have

$$a_{n+1,ij} = \frac{1}{p}\left(\sum_{\ell=1}^{g} a_{n,i\ell} w_n(\alpha_{\ell j})\right) + (\text{terms with valuation at least } -n).$$

Hypothesis (iv) for n says that $\mathrm{ord}(a_{n,i\ell}) \geqslant 1-n$ when $i > \ell$, and since $w_0(A)$ is upper-triangular modulo p, $w_n(\alpha_{\ell j})$ is divisible by p for $\ell > j$, so $\mathrm{ord}(w_n(\alpha_{\ell j})) \geqslant 1$. If $i > j$ then either $i > \ell$ or $\ell > j$, so $u_{n+1,ij} \geqslant 1-(n+1)$ in this case. This proves Hypothesis (iv) for $n+1$.

10.6.3. It remains to prove Hypotheses (ii) and (iii) for $n+1$. We have

$$a_{n+1,ii} = \frac{1}{p}\left(\sum_{\ell=1}^{g} a_{n,i\ell} w_n(\alpha_{\ell i})\right) + (\text{terms with valuation at least } -n),$$

with $\mathrm{ord}(a_{n,i\ell} w_n(\alpha_{\ell i})) \geqslant 1-n$ when $\ell \neq i$ as above, since $\mathrm{ord}(a_{n,i\ell}) \geqslant 1-n$ when $i > \ell$ by Hypothesis (iv) and $\mathrm{ord}(w_n(\alpha_{\ell i})) \geqslant 1$ when $\ell > i$. Assume that $n+1 \leqslant N_i$ (i.e. we are in the situation of Hypothesis (ii)), so

$$\frac{p^{n+1}-1}{p-1} U_i < 1$$

and, by induction,

$$\mathrm{ord}(a_{n,ii}) = \frac{p^n-1}{p-1} U_i - n.$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Write $\alpha_{ij} = (\alpha_{ij,0}, \alpha_{ij,1}, \dots)$ in its Witt coordinates, so $U_i = \operatorname{ord}(\alpha_{ii,0})$. Then

$$p^n \operatorname{ord}(\alpha_{ii,0}) = p^n U_i < \frac{p^{n+1}-1}{p-1} U_i < 1$$

so

$$\operatorname{ord}(w_n(\alpha_{ii})) = \operatorname{ord}\left(\sum_{j=0}^{n} p^j \alpha_{ii,j}^{p^{n-j}}\right) = \operatorname{ord}(\alpha_{ii,0}^{p^n}) = p^n U_i.$$

Hence

$$\operatorname{ord}(a_{n,ii} w_n(\alpha_{ii})) = \frac{p^n-1}{p-1} U_i + p^n U_i - n = \frac{p^{n+1}-1}{p-1} U_i - n < 1 - n.$$

We conclude that

$$u_{n+1,ii} = \operatorname{ord}(a_{n+1,ii}) = \frac{p^{n+1}-1}{p-1} U_i - (n+1),$$

which proves Hypothesis (ii) for $n+1$.

Now assume $n+1 > N_i$ (i.e. we are in the situation of Hypothesis (iii)), so

$$\frac{p^{n+1}-1}{p-1} U_i \geqslant 1.$$

The formula $w_n(\alpha_{ii}) = \sum_{j=0}^{n} p^j \alpha_{ii,j}^{p^{n-j}}$ gives $\operatorname{ord}(w_n(\alpha_{ii})) \geqslant \min\{p^n U_i, 1\}$ since $U_i = \operatorname{ord}(\alpha_{ii,0})$, so if $n = N_i$ then by Hypothesis (ii) for n,

$$\operatorname{ord}(a_{n,ii} w_n(\alpha_{ii,0})) \geqslant \frac{p^n-1}{p-1} U_i - n + \min\{p^n U_i, 1\} = \min\left\{\frac{p^{n+1}-1}{p-1} U_i,\ 1\right\} - n \geqslant 1 - n.$$

If $n > N_i$ then by Hypothesis (iii) for n,

$$\operatorname{ord}(a_{n,ii} w_n(\alpha_{ii,0})) \geqslant 1 - n + \operatorname{ord}(w_n(\alpha_{ii,0})) \geqslant 1 - n.$$

Therefore, $u_{n+1,ii} \geqslant -n = 1 - (n+1)$, which proves Hypothesis (iii) for $n+1$. □

10.7. As mentioned above, we will perturb the coefficients of the power series $\log_i$ to simplify the combinatorics. The following kind of power series will serve as the perturbations (recall § 10.5 that we have fixed N, H and $\{U_i\}_{i=1,\dots,g}$).

Definition 10.8. Let

$$f_i(X_1, \dots, X_g) = \sum_{j=1}^{g} \sum_{n=0}^{\infty} b_{n,ij} X_j^{p^n} \in K'[\![X_1, \dots, X_g]\!]$$

be power series with coefficients in a finite extension field K' of K for $i = 1, \dots, g$. We say that $(f_1, \dots, f_g)$ *satisfies Hypotheses 9.2.2* if the data $(\operatorname{ord}(b_{n,ij}), N, H, U_i)$ satisfy Hypotheses 9.2.2.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

The following lemma is basically a translation of Theorem 9.10. We use the notation of § 10.2.

Lemma 10.9. *Let K' be a finite extension of K, let $f_1, \dots, f_g \in K'[\![X_1, \dots, X_g]\!]$ be power series satisfying Hypotheses 9.2.2, and let $\mathscr{X} \subset \boldsymbol{D}^g_{K'}$ be the analytic subspace defined by $(f_1, \dots, f_g)$. Then for $1 \leqslant n \leqslant N$ we have $\mathscr{X} \cap \boldsymbol{D}^g_{K'}(\rho_n) = \mathscr{X} \cap \boldsymbol{B}^g_{K'}(\rho'_n)$. In addition, $\mathscr{X} \cap \boldsymbol{D}^g_{K'}(\rho_0) = \{0\}$.*

Proof. By decreasing N we may assume that $n = N$; see Lemma 9.2.4 (i). The case $g = 1$ is handled by Remark 9.8, so assume by induction on g that $g > 1$. Let $\xi = (\xi_1, \dots, \xi_g) \in \mathscr{X} \cap \boldsymbol{D}^g_{K'}(\rho_N)$. If all ξ_i are non-zero then

$$\operatorname{ord}(\xi) = (\operatorname{ord}(\xi_1), \dots, \operatorname{ord}(\xi_g)) \in \bigcap_{i=1}^{g} \operatorname{Trop}(f_i) \cap \boldsymbol{R}^g_{>r_N},$$

so by Theorem 9.10, $\xi \in \boldsymbol{B}^g_{K'}(\rho'_N)$. Now suppose that $\xi_i = 0$ for some i. Let

$$\tilde{f}_j(X_1, \dots, \hat{X}_i, \dots, X_g) = f_j(X_1, \dots, X_{i-1}, 0, X_{i+1}, \dots, X_g)$$

for $j \neq i$. Then by Lemma 9.2.4 (iii), the power series $\{\tilde{f}_j\}_{j \neq i}$ satisfy Hypotheses 9.2.2 for $g - 1$. But $(\xi_1, \dots, \hat{\xi}_i, \dots, \xi_g)$ is a root of each $\tilde{f}_j$, $j \neq i$, so by induction on g we have $\xi \in \boldsymbol{B}^g_{K'}(\rho'_N) \cap \{\xi_i = 0\}$.

The same argument shows that $\mathscr{X} \cap \boldsymbol{D}^g_{K'}(\rho_0) = \{0\}$. □

10.9.1. In particular, taking $(f_1, \dots, f_g) = (\log_1, \dots, \log_g)$ and using Propositions 6.8 and 10.6, we see that for all $1 \leqslant n \leqslant N$,

$$\mathscr{G}[p^\infty]_{\leqslant \rho'_n} = \mathscr{G}[p^\infty]_{<\rho_n} \quad \text{and} \quad \mathscr{G}[p^\infty]_{<\rho_0} = \{0\}. \tag{10.9.2}$$

Lemma 10.9 and the following proposition allow us to make drastic modifications to our power series without affecting the number of roots in $\boldsymbol{B}^g_K(\rho'_n)$.

Proposition 10.10 (continuity of roots). *Let $\rho, \mu \in \sqrt{|K^\times|}$ be such that $\rho < \mu$. Let $\mathscr{X} \subset \boldsymbol{B}^g_K(\mu) \times \boldsymbol{B}^1_K$ be a closed analytic subspace contained in $\boldsymbol{B}^g_K(\rho) \times \boldsymbol{B}^1_K$, and let $\varphi\colon \mathscr{X} \to \boldsymbol{B}^1_K$ be projection onto the second factor. Suppose that $\mathscr{X}$ is defined by an ideal of the form $(f_1, \dots, f_g) \subset T_{g,\mu}\langle t \rangle$. Then φ is a finite, flat map. In particular, each fibre of $\mathscr{X}$ over $\boldsymbol{B}^1_K$ is finite and has the same length.*

Proof. It is harmless to make a finite extension of K, so we can reduce to the case $\mu = 1$. Let $A = T_g\langle t \rangle / \mathfrak{a}$, where $\mathfrak{a}$ is the ideal generated by $f_1, \dots, f_g$, so $\mathscr{X} = \operatorname{Sp}(A)$. First we show that A is a finite $K\langle t \rangle$-module. By the rigid-analytic direct image theorem [**5**, Theorem 9.6.3/1], we need only show that φ is proper. Using Kiehl's definition of properness for rigid spaces, it suffices to show that there are affinoid generators $h_1, \dots, h_n$ of A over $K\langle t \rangle$ such that $|h_i|_{\sup} < 1$. Since $\mathscr{X} \subset \boldsymbol{B}^g_K(\rho) \times \boldsymbol{B}^1_K$ with $\rho < 1$, the standard generators of T_g satisfy this property.

Since $\mathfrak{a}$ has g generators, by Krull's principal ideal theorem every irreducible component of $\operatorname{Spec}(A)$ has dimension at least one, so since the fibres of φ have dimension zero, $\mathscr{X}$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

is pure dimension 1 by [**26**, Theorem 15.1]. Since $T_{g,\mu}$ is a regular ring, it is Cohen–Macaulay, so by the unmixedness theorem [**26**, Theorem 17.6], $\mathrm{Spec}(A)$ has no embedded points. Thus every associated point of $\mathrm{Spec}(A)$ lies over the generic point of $\mathrm{Spec}(K\langle t\rangle)$. Since $K\langle t\rangle$ is Dedekind, A is a flat $K\langle t\rangle$-module. □

Definition 10.11. Let K' be a finite extension of K, let $(f_1,\dots,f_g)$ be a g-tuple of power series in g variables converging on $\boldsymbol{D}^g_{K'}$, and choose $\rho\in\sqrt{|K^\times|}$, $0<\rho<1$. By the *number of roots* of $(f_1,\dots,f_g)$ in $\boldsymbol{B}^g_{K'}(\rho)$ we mean the K'-dimension of $T_{K',g,\rho}/(f_1,\dots,f_g)$ (which may be infinite).

When $(f_1,\dots,f_g)$ cut out an étale subspace $\mathscr{X}\subset\boldsymbol{B}^g_{K'}(\rho)$, the number of roots of $(f_1,\dots,f_g)$ in $\boldsymbol{B}^g_{K'}(\rho)$ is simply the number of geometric points of $\mathscr{X}$.

Corollary 10.12. *Let $f_1,\dots,f_g$ be analytic functions on $\boldsymbol{D}^g_K\times\boldsymbol{B}^1_K$ such that for each $t_0\in\boldsymbol{B}^1_K$, the specializations $f_{1,t_0},\dots,f_{g,t_0}$ satisfy Hypotheses 9.2.2 over $\kappa(t_0)$ (in the sense of § 10.8). Then for any $1\leqslant n\leqslant N$, $(f_{1,t_0},\dots,f_{g,t_0})$ has a finite number of roots in $\boldsymbol{B}^g_K(\rho'_n)$, and this number is independent of $t_0\in\boldsymbol{B}^1_K$.*

Proof. Decreasing N if necessary, we may assume that $n=N$. Let $\mathscr{X}\subset\boldsymbol{D}^g_K\times\boldsymbol{B}^1_K$ be the analytic subspace cut out by $f_1,\dots,f_g$, and for $t_0\in\boldsymbol{B}^1_K$ let $\mathscr{X}_{t_0}$ be the fibre over t_0. By Lemma 10.9, $\mathscr{X}_{t_0}\subset\boldsymbol{B}^g_{\kappa(t_0)}(\rho'_N)$ for all t_0, so $\mathscr{X}\subset\boldsymbol{B}^g_K(\rho'_N)\times\boldsymbol{B}^1_K$. The result now follows from Proposition 10.10 with $\rho=\rho'_N$ and any $\mu\in(\rho'_N,1)\cap\sqrt{|K^\times|}$. □

10.13. Proof of Proposition 10.4. We define

$$f_i(X_1,\dots,X_g;t)=\sum_{n=0}^{\infty}a_{n,ii}X_i^{p^n}+t\sum_{j\neq i}\sum_{n=0}^{\infty}a_{n,ij}X_j^{p^n}.$$

By Lemma 9.2.4 (ii), for every $t_0\in\boldsymbol{B}^1_K$ the specializations $f_{1,t_0},\dots,f_{g,t_0}$ satisfy Hypotheses 9.2.2. Thus by Corollary 10.12, for every $1\leqslant n\leqslant N$, $(f_{1,0},\dots,f_{g,0})$ has the same number of roots in $\boldsymbol{B}^g_K(\rho'_n)$ as $(f_{1,1},\dots,f_{g,1})=(\log_1,\dots,\log_g)$. Let

$$h_i=f_{i,0}=\sum_{n=0}^{\infty}a_{n,ii}X_i^{p^n};$$

we want to show that $(h_1,\dots,h_g)$ has p^{ng} roots in $\boldsymbol{B}^g_K(\rho'_n)$. Thinking of h_i as a power series in one variable, let $\mathscr{X}_i\subset\boldsymbol{B}^1_K(\rho'_n)$ be the subspace cut out by h_i, so the ideal $(h_1,\dots,h_g)$ cuts out the product $\mathscr{X}_1\times\cdots\times\mathscr{X}_g\subset\boldsymbol{B}^g_K(\rho'_n)$. Thus it suffices to show that the length of $\mathscr{X}_i$ is p^n for $i=1,\dots,g$, so we are reduced to the case $g=1$. This is handled by Remark 9.8. □

11. The group structure on $\mathscr{G}[p^\infty]_{\leqslant\rho'_N}(\bar{K})$

11.1. We keep the notation of § 10. The only remaining step in the proof of Theorem 7.12 is to show that the group $\mathscr{G}[p^\infty]_{\leqslant\rho'_N}(\bar{K})$ of size p^{Ng} is in fact equal to $\mathscr{G}[p^N]_{\leqslant\rho'_N}(\bar{K})$, and is isomorphic to $(\boldsymbol{Z}/p^N\boldsymbol{Z})^g$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

11.2. Let $\boldsymbol{X} = (X_1, \dots, X_g)$ and let $\mathfrak{G} \cong \mathrm{Spf}(R[\![\boldsymbol{X}]\!])$ be the canonical formal Lie group with $G \cong \mathfrak{G}[p^\infty]$, as in § 2.4. Let $[p](\boldsymbol{X}) \in (\boldsymbol{X})R[\![\boldsymbol{X}]\!]^g$ be the g-tuple of power series defining the multiplication-by-p map on $\mathfrak{G}$. Let $R_0 = R/pR$, let $\mathfrak{G}_0 = \mathfrak{G} \otimes_R R_0$ and $G_0 = G \otimes_R R_0$, and let V be the relative Verschiebung map $\mathfrak{G}_0^{(p)} \to \mathfrak{G}_0$ over R_0. We have chosen a basis for the tangent space $\mathrm{Lie}(G_0)$ of G_0, which induces a basis for $\mathrm{Lie}(G_0^{(p)}) \cong \mathrm{Lie}(G_0) \otimes_{R_0,\mathrm{Frob}} R_0$; with respect to these bases, we can view $\mathrm{d}V\colon \mathrm{Lie}(G_0^{(p)}) \to \mathrm{Lie}(G_0)$ as a $g \times g$ matrix with coefficients in R_0. Choose a lift of $\widetilde{\mathrm{d}V} \in \mathrm{M}_g(R)$ of this matrix. The following is a slight generalization of a result in [**22**, § 3.6].

Lemma 11.3. *We have*

$$[p](\boldsymbol{X}) = p\boldsymbol{X} + \widetilde{\mathrm{d}V}(X_1^p, \dots, X_g^p) + pf(\boldsymbol{X}) + O(\boldsymbol{X}^{p^2}),$$

where f is a g-tuple of power series with no terms of total degree less than p.

The proof is left to the reader; one uses the fact that for $\zeta \in R$ a primitive $(p-1)$th root of unity, we have $\log(\zeta \boldsymbol{X}) = \zeta \log(\boldsymbol{X})$, so

$$\begin{aligned}
[p](\zeta\boldsymbol{X}) &= \exp(p \cdot \log(\zeta\boldsymbol{X})) \\
&= \exp(\zeta p \cdot \log(\boldsymbol{X})) \\
&= \exp(\zeta \log([p]\boldsymbol{X})) \\
&= \exp(\log(\zeta[p](\boldsymbol{X}))) \\
&= \zeta[p](\boldsymbol{X}).
\end{aligned}$$

(In fact Lemma 11.3 is true for any formal Lie group $\mathfrak{G}$ equipped with a choice of parameters such that the total degree of any monomial in $\log(\boldsymbol{X})$ is a power of p.)

11.4. By Remark 7.9.1 (iv), the matrix for $\mathrm{d}V$ (with respect to our choice of basis) is given $w_0(A) \mod p$ where A is the upper-left $g \times g$ submatrix of the structure matrix M of our display $\mathcal{P}$. Recall from § 7.15 that we are assuming that $w_0(A)$ is upper-triangular mod p, so $\widetilde{\mathrm{d}V} \pmod p$ is an upper-triangular matrix.

Notation 11.5. For $\xi = (\xi_1, \dots, \xi_g) \in \boldsymbol{B}_K^g(\bar{K}) \setminus \{0\}$ let $\mathrm{size}(\xi) = \min\{\mathrm{ord}(\xi_i)\}_{i=1}^g$ and for $n \in \boldsymbol{Z}_{\geqslant 0}$ let $\xi^{(n)} = (\xi_1^n, \dots, \xi_g^n)$.

In other words, if $\xi \in \boldsymbol{B}_K^g(\bar{K}) \setminus \{0\}$ and $r = \mathrm{size}(\xi)$ then $\rho = p^{-r}$ is the radius of the smallest ball $\boldsymbol{B}_K^g(\rho)$ containing ξ.

Remark 11.6. Lemma 11.3 implies that if $\xi \in \boldsymbol{D}_K^g(\bar{K}) \setminus \{0\}$ then

$$\mathrm{size}([p]\xi) \geqslant \min\{p\,\mathrm{size}(\xi), 1 + \mathrm{size}(\xi)\},$$

or equivalently,

$$\mathrm{size}(\xi) \leqslant \max\{p^{-1}\,\mathrm{size}([p]\xi), \mathrm{size}([p]\xi) - 1\}.$$

Consequently, if $\xi_1, \xi_2, \dots \in \boldsymbol{D}_K^g(\bar{K})$ satisfy $\xi_1 \neq 0$ and $[p]\xi_{n+1} = \xi_n$ for all $n \geqslant 1$, then $\mathrm{size}(\xi_n) \to 0$ as $n \to \infty$.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Suppose that the level-n canonical subgroup G_n of G exists for all n, and that G_n admits the radius μ_n. Then $[p]\colon G_{n+1}(\bar{K}) \to G_n(\bar{K})$ is a surjection, so there exist $\xi_n \in G_n(\bar{K}) = G[p^n]_{\leqslant \mu_n}(\bar{K})$ for $n \geqslant 1$ with $\operatorname{size}(\xi_n) \to 0$. Hence $\mu_n \to 1$, so $\mathscr{G}[p^\infty] = \bigcup_{n\geqslant 1} G_n \otimes_R K$. This implies that G is ordinary, since

$$G[p](\bar{K}) \subset \bigcup_{n\geqslant 1} G_n[p](\bar{K}) = G_1(\bar{K}).$$

Lemma 11.7. *Choose $\xi \in \boldsymbol{B}_K^g(\bar{K}) \setminus \{0\}$ and suppose that for some integer $n \geqslant 1$ we have*

$$\frac{1}{p^{n+1}(p-1)} < \operatorname{size}(\xi) \leqslant \frac{1}{p(p-1)}.$$

If $H = H(G) < (p-1)/p^{n+1}$ then $[p](\xi) \neq 0$.

Proof. First we will show by induction on g that if $B = (b_{ij}) \in \mathrm{M}_g(R)$ is any upper-triangular matrix with non-zero diagonal entries and $\nu \in \boldsymbol{B}_K^g(\bar{K}) \setminus \{0\}$ is any point then

$$\operatorname{size}(B\nu) = \min\left\{ \operatorname{ord}\left(\sum_{j\geqslant i} b_{ij}\nu_j \right) \right\}_{i=1}^{g} \leqslant h + \operatorname{size}(\nu), \tag{$*$}$$

where $h = \sum_{i=1}^g \operatorname{ord}(b_{ii})$ (note that $B\nu \neq 0$ since $\det(B) \neq 0$). The assertion is clear when $g = 1$, so assume $g > 1$.

(i) If $\operatorname{size}(\nu) < \operatorname{ord}(\nu_1)$ then $\operatorname{size}(\nu) = \operatorname{size}(\nu_2, \dots, \nu_g)$, so we are done by induction on g.

(ii) If $\operatorname{size}(\nu) = \operatorname{ord}(\nu_1)$ and $\operatorname{ord}(\sum_{i=1}^g b_{1i}\nu_i) \leqslant \operatorname{ord}(b_{11}\nu_1)$ then we are done.

(iii) Otherwise, for some $i > 1$ we have $\operatorname{ord}(\nu_i) \leqslant \operatorname{ord}(\nu_i) + \operatorname{ord}(b_{1i}) \leqslant \operatorname{size}(\nu) + \operatorname{ord}(b_{11})$. Hence if $\nu' = (\nu_2, \dots, \nu_g)$, $h' = \sum_{i=2}^g \operatorname{ord}(b_{ii})$, and $B' = (b_{ij})_{i,j\geqslant 2}$, then by induction we have

$$\begin{aligned} \operatorname{size}(B\nu) &\leqslant \operatorname{size}(B'\nu') \leqslant h' + \operatorname{size}(\nu') \leqslant h' + \operatorname{ord}(\nu_i) \\ &\leqslant h' + \operatorname{size}(\nu) + \operatorname{ord}(b_{11}) = h + \operatorname{size}(\nu). \end{aligned}$$

This proves the assertion.

Write $\mathrm{d}V = (a_{ij})$, and choose lifts $\tilde{a}_{ij}$ of a_{ij} to R such that the matrix $\widetilde{\mathrm{d}V} := (\tilde{a}_{ij})$ is also upper-triangular. Since $H = \sum_{i=1}^g \operatorname{ord}(\tilde{a}_{ii}) < 1$, the diagonal entries of $\widetilde{\mathrm{d}V}$ are non-zero so by $(*)$ we have $\operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)})) \leqslant H + p\operatorname{size}(\xi)$. We also have

$$H + (p-1)\operatorname{size}(\xi) < \frac{p-1}{p^{n+1}} + \frac{1}{p} \leqslant \frac{p-1}{p^2} + \frac{1}{p} = \frac{2}{p} - \frac{1}{p^2} \leqslant 1 - \frac{1}{p^2} < 1,$$

so $\operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)})) \leqslant H + p\operatorname{size}(\xi) < \operatorname{size}(\xi) + 1$. By Lemma 11.3,

$$[p](\boldsymbol{X}) = \widetilde{\mathrm{d}V}(X_1^p, \dots, X_g^p) + pf(\boldsymbol{X}) + O(\boldsymbol{X}^{p^2}) \tag{11.7.1}$$

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

for some $f \in (\boldsymbol{X})R[\![\boldsymbol{X}]\!]$. Write $[p](\boldsymbol{X}) = ([p]_1(\boldsymbol{X}), \ldots, [p]_g(\boldsymbol{X}))$, and let cX^μ be a monomial occurring in $[p]_i(\boldsymbol{X})$ for some $1 \leqslant i \leqslant g$ such that $c\xi^\mu \neq 0$ (i.e. $\xi_i \neq 0$ when $\mu_i \neq 0$). If $c \equiv 0 \pmod p$ then $\operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)})) < \operatorname{size}(\xi) + 1 \leqslant \operatorname{ord}(c\xi^\mu)$. If instead $|\mu| \geqslant p^2$ then

$$\operatorname{ord}(c\xi^\mu) \geqslant p^2 \operatorname{size}(\xi) > \frac{p-1}{p^{n+1}} + p\operatorname{size}(\xi) > H + p\operatorname{size}(\xi) \geqslant \operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)})),$$

where the second inequality holds because $p(p-1)\operatorname{size}(\xi) > (p-1)/p^{n+1}$ since $\operatorname{size}(\xi) > 1/p^{n+2}$. Hence in (11.7.1), we have $\operatorname{size}(f(\xi)) > \operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)}))$, and the $O(\boldsymbol{X}^{p^2})$-term also evaluates at $\boldsymbol{X} = \xi$ with size greater than $\operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)}))$. Thus $\operatorname{size}([p]\xi) = \operatorname{size}(\widetilde{\mathrm{d}V}(\xi^{(p)}))$, and in particular $[p]\xi \neq 0$. □

Proposition 11.8. *Assume that* $H = H(G) < (p-1)/p^N$. *Then* $\mathscr{G}[p^\infty]_{\leqslant \rho'_N}(\bar{K}) \cong (\boldsymbol{Z}/p^N\boldsymbol{Z})^g$.

Proof. First we show that for $1 \leqslant n \leqslant N$, $\mathscr{G}[p^\infty]_{\leqslant \rho'_n} = \mathscr{G}[p^n]_{\leqslant \rho'_n}$. We will prove by induction on n that $\mathscr{G}[p^\infty]_{\leqslant \rho'_n}(\bar{K}) = \mathscr{G}[p^\infty]_{<\rho_n}(\bar{K})$ is killed by p^n (see (10.9.2)). Let $\xi \in \mathscr{G}[p^\infty]_{<\rho_n}(\bar{K})$. By Lemma 11.3,

$$\operatorname{size}([p]\xi) \geqslant \min\{p\operatorname{size}(\xi),\ 1 + \operatorname{size}(\xi)\} > \min\{pr_n, 1 + r_n\} \geqslant \frac{1}{p^{n-1}(p-1)}.$$

If $n = 1$ then $\operatorname{size}([p]\xi) > 1/(p-1)$, so $[p]\xi = 0$ by (10.9.2). Otherwise $[p]\xi \in \mathscr{G}[p^\infty]_{<\rho_{n-1}}(\bar{K})$, so $[p^n]\xi = [p^{n-1}][p]\xi = 0$ by induction.*

In order to prove that the p^N-torsion abelian group $\mathscr{G}[p^\infty]_{\leqslant \rho'_N}(\bar{K})$ of order p^{Ng} is isomorphic to $(\boldsymbol{Z}/p^N\boldsymbol{Z})^g$, it suffices to show that $\mathscr{G}[p^\infty]_{\leqslant \rho'_N}(\bar{K})$ has p^g points of p-torsion. It is clear from the above that $\mathscr{G}[p^\infty]_{\leqslant \rho'_1} \subset \mathscr{G}[p^\infty]_{\leqslant \rho'_N}$ has order p^g and is killed by p, so we must show that for $\xi \in \mathscr{G}[p^\infty]_{\leqslant \rho'_N}(\bar{K})$, $[p]\xi = 0$ implies $\xi \in \mathscr{G}[p^\infty]_{\leqslant \rho'_1}(\bar{K})$. By (10.9.2), $\mathscr{G}[p^\infty]_{\leqslant \rho'_1} = \mathscr{G}[p^\infty]_{<\rho_1}$, so if $\xi \in \mathscr{G}[p^\infty]_{\leqslant \rho'_N}(\bar{K})$ is not contained in $\mathscr{G}[p^\infty]_{\leqslant \rho'_1}(\bar{K})$ then $\operatorname{size}(\xi) \leqslant 1/p(p-1)$. By Lemma 11.7, this implies that $[p]\xi \neq 0$. □

The proof of Theorem 7.12 is now complete.

12. Elimination of noetherian hypotheses

12.1. As mentioned in § 7.11, the goal of this section is to prove the following proposition.

Proposition 12.2. *Let G be a connected level-N truncated p-divisible group over R. If the fraction field K of R is algebraically closed then G extends to a p-divisible group over R.*

In particular, there is a display $\mathcal{P}$ over R such that $G \cong \mathrm{BT}_{\mathcal{P}}[p^N]$.

We will use a standard noetherian approximation argument.

* See [**11**, Lemma 2.2.6] for another proof of this fact.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Proposition 12.3. *Suppose that the fraction field K of R is algebraically closed. Let $(A, \mathfrak{m})$ be a local noetherian ring with residue field κ and let $\varphi\colon A \to R$ be a local homomorphism. Let κ' be a subfield of the residue field k of R, and assume $\kappa \subset \kappa'$. There exists a flat local noetherian A-algebra B and commutative diagram of local homomorphisms*

$$\begin{array}{ccc} B & \xrightarrow{\psi} & R \\ \uparrow & \nearrow_{\varphi} & \\ A & & \end{array}$$

such that $\mathfrak{m}B$ is the maximal ideal of B, and the map $B/\mathfrak{m}B \to k$ has image κ'.

Proof. The existence of a flat local noetherian A-algebra B such that $B/\mathfrak{m}B$ is isomorphic to a given field extension of κ is a standard fact proved in [$\mathrm{EGA0_{III}}$, Proposition 10.3.1]. Here we give an indication of how to modify that proof to include a construction of the map $\psi\colon B \to R$.

12.3.1. Suppose that $\kappa' = \kappa(t)$ where $t \in \kappa'$ is a transcendental element. Let $A' = A[T]$, let $\mathfrak{p} = \mathfrak{m}A'$, and let $B = A'_{\mathfrak{p}}$. Let $\psi\colon A' \to R$ be the A-algebra homomorphism sending $T \mapsto t$. If $f(T) \notin \mathfrak{p}$ then the residue of $\psi(f(T))$ in k is non-zero because t is transcendental over κ. Thus ψ extends to an A-map $B \to R$, and we are done in this case.

12.3.2. Suppose that $\kappa' = \kappa(\alpha)$ where $\alpha \in \kappa'$ is an algebraic element with (monic) minimal polynomial $f \in \kappa[T]$. Let $F \in A[T]$ be a monic polynomial reducing to $f \in k[T]$, let $A' = A[T]$, and let $B = A'/(F)$. Since K is algebraically closed, there exists $\tilde{\alpha} \in R$ lifting α such that $F(\tilde{\alpha}) = 0$. The map $\psi\colon A' \to R$ sending $T \mapsto \tilde{\alpha}$ factors through an A-map $\psi\colon B \to R$, which settles this case.

12.3.3. In general there exists an ordinal γ and, for all ordinals $\lambda \leqslant \gamma$, a subfield κ_λ of κ' containing κ such that

(a) for each $\lambda < \gamma$, $\kappa_{\lambda+1}$ is an extension of κ_λ generated by a single element,

(b) for every ordinal μ without a predecessor, we have $\kappa_\mu = \bigcup_{\lambda<\mu} \kappa_\lambda$, and

(c) $\kappa = \kappa_0$ and $\kappa' = \kappa_\gamma$.

By transfinite recursion we will construct local noetherian rings B_λ for $\lambda \leqslant \gamma$ and local homomorphisms $\sigma_{\mu\lambda}\colon B_\lambda \to B_\mu$ for $\lambda \leqslant \mu$ and $\psi_\lambda\colon B \to R$ such that

(1) $(B_\lambda, \sigma_{\lambda\mu})$ is a directed system with $B_0 = A$;

(2) for all λ the map ψ_λ induces a κ-isomorphism $B_\lambda/\mathfrak{m}B_\lambda \xrightarrow{\sim} \kappa_\lambda$;

(3) for $\lambda \leqslant \mu$, B_μ is B_λ-flat.

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

Let $\xi \leqslant \gamma$, and suppose that B_λ, $\sigma_{\mu\lambda}$ and ψ_λ have been constructed satisfying (1)–(3) for $\lambda \leqslant \mu < \xi$. If $\xi = \mu + 1$ is a successor then k_ξ is generated over k_μ by a single element, so we can construct B_ξ and ψ_ξ as in the previous two paragraphs. If ξ is not a successor then we set $B_\xi = \varinjlim_{\mu<\xi} B_\mu$, and we let $\psi_\xi \colon B_\xi \to R$ be the natural map. Then B_ξ satisfies (1)–(3) by [EGA0_{III}, Lemma 10.3.1.3]. □

Proposition 12.4. *Suppose that the fraction field K of R is algebraically closed. Let G be a BT_n over R for some $n \geqslant 1$. There exists a complete local noetherian ring R', a local homomorphism $R' \to R$ inducing an isomorphism on residue fields, and a level-n truncated p-divisible group G' over R' such that $G' \otimes_{R'} R \cong G$.*

Proof. First we show that there exists a local noetherian subring R_0 of R with local structure map $R_0 \to R$ and a finite flat R_0-group scheme G_0 such that $G_0 \otimes_{R_0} R \cong G$. We will use the standard techniques of noetherian approximation from [**17**, § 8].

12.4.1. Let $G = \mathrm{Spec}(A)$, and let $m \colon A \otimes_R A \to A$ and $\mu \colon A \to A \otimes_R A$ denote the multiplication and comultiplication, respectively. Let $\iota \colon A \to R$ be the coidentity, and let $I = \ker(\iota)$, so $A = R \oplus I$. Choosing an R-basis for I we obtain isomorphisms $I \cong R^M$ and $A \cong R^{M+1}$, and hence matrix representations $m = (m_{ij})$ and $\mu = (\mu_{ij})$. The augmentation ideal I and the structure coefficients m_{ij}, μ_{ij} determine the Hopf algebra structure on A. Let R_0 be a subring of R that is finitely generated over $\boldsymbol{Z}$ and contains the m_{ij} and μ_{ij}, let $I_0 = R_0^M$ and let $A_0 = R_0 \oplus I_0$. We define maps $m_0 \colon A_0 \otimes_{R_0} A_0 \to A_0$ and $\mu_0 \colon A_0 \to A_0 \otimes_{R_0} A_0$ using the matrices (m_{ij}) and (μ_{ij}), respectively, and we let $R_0 \to A_0 = R_0 \oplus I_0$ (respectively $\iota_0 \colon A_0 \to R_0$) be inclusion into (respectively projection onto) the first factor. It is not hard to see that these data endow A_0 with the structure of Hopf algebra over R_0. If $G_0 = \mathrm{Spec}(A_0)$ then $G_0 \otimes_{R_0} R \cong G$ by construction, and G_0 is commutative since $R_0 \to R$ is an injection. Replacing R_0 with its localization at $R_0 \cap \mathfrak{m}_R$, we may assume that R_0 is local.

12.4.2. Let $\{R_\alpha\}_{\alpha \in \mathcal{I}}$ be the directed system of local noetherian subrings of R containing R_0 and having local structure map $R_\alpha \to R$, and for $\alpha \in \mathcal{I}$ let $G_\alpha = G_0 \otimes_{R_0} R_\alpha$. Suppose that $n \geqslant 2$, and let $0 \leqslant i \leqslant n$. Then $[p^i]_{G_\alpha} \colon G_\alpha \to G_\alpha[p^{n-i}]$ is faithfully flat for large enough α by [**17**, Theorems 8.10.5 and 11.2.6], so G_α is a BT_n. A similar argument shows that G_α is a BT_1 for large enough α when $n = 1$.

12.4.3. Fix a large α as in § 12.4.2 and let $R_1 = R_\alpha$. This is a local noetherian ring with maximal ideal $\mathfrak{m}_1$ and local structure map $R_1 \to R$. Let R_2 be a local noetherian ring with maximal ideal $\mathfrak{m}_2$, equipped with a local homomorphism $R_1 \to R_2$ such that $\mathfrak{m}_2 = \mathfrak{m}_1 R_2$ and a local R_1-algebra homomorphism $R_2 \to R$ inducing an isomorphism on residue fields, as in Proposition 12.3. For $r \in \boldsymbol{R}_{\geqslant 0}$ let $\mathfrak{a}_r = \{x \in R_2 \colon \mathrm{ord}(x) \geqslant r\}$, so $\mathfrak{a}_1 \subset \mathfrak{a}_{1/2} \subset \mathfrak{a}_{1/3} \subset \cdots$ with $\bigcup_{i=1}^{\infty} \mathfrak{a}_{1/i} = \mathfrak{m}$. Since R_2 is noetherian, there is some $\pi \in R$ with non-zero valuation such that $\mathrm{ord}(x) \leqslant \mathrm{ord}(\pi)$ for all $x \in \mathfrak{m}_2$. It follows that $\mathrm{ord}(x) \leqslant \mathrm{ord}(\pi^n)$ for all $x \in \mathfrak{m}_2^n$, so the $\mathfrak{m}_2$-adic completion R' of R_2 maps into R. The ring R' and the truncated p-divisible group $G' = G_\alpha \otimes_{R_\alpha} R'$ satisfy the properties of Proposition 12.4. □

https://doi.org/10.1017/S1474748011000132 Published online by Cambridge University Press

12.5. Proof of Proposition 12.2. Let G be a connected BT_N over R for some $N \geqslant 1$. Since K is algebraically closed, the residue field k of R is perfect. Let R' be a complete local noetherian ring with a local homomorphism $R' \to R$ inducing an isomorphism of residue fields and such that there exists a connected truncated p-divisible group G' of level N over R' with $G' \otimes_{R'} R \cong G$, as in Proposition 12.4. By [**19**, Theorem 4.4(e)], there is a connected p-divisible group H' over R' such that $H'[p^N] \cong G'$. Let $H = H' \otimes_{R'} R$. Then

$$G \cong G' \otimes_{R'} R \cong (H' \otimes_{R'} R)[p^N] \cong H[p^N].$$

□

Acknowledgements. This work was completed as part of the author's doctoral degree program. The author would like to express sincere gratitude to his advisor Brian Conrad for suggesting this problem as a thesis topic and for all of his guidance. He is equally indebted to his advisor Ravi Vakil for his consistent support and advice throughout the previous five years. The author also thanks Sam Payne and Mark Kisin who provided key input and interesting conversations, and the referee for pointing out some errors and inaccuracies.

References

1. A. Abbes and A. Mokrane, Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes, *Publ. Math. IHES* **99** (2004), 117–162.
2. F. Andreatta and C. Gasbarri, The canonical subgroup for families of abelian varieties, *Compositio Math.* **143**(3) (2007), 566–602.
3. M. Artin, J. E. Bertin, M. Demazure, P. Gabriel, A. Grothendieck, M. Raynaud and J.-P. Serre, *Schémas en groupes.*, Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques (SGA 3) (Institut des Hautes Études Scientifiques, Paris, 1962–1964).
4. A. Barvinok, *A course in convexity*, Graduate Studies in Mathematics, Volume 54 (American Mathematical Society, Providence, RI, 2002).
5. S. Bosch, U. Güntzer and R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften, Volume 261 (Springer, 1984).
6. K. Buzzard, Analytic continuation of overconvergent eigenforms, *J. Am. Math. Soc.* **16**(1) (2003), 29–55.
7. K. Buzzard and R. Taylor, Companion forms and weight one forms, *Annals Math. (2)* **149**(3) (1999), 905–919.
8. R. F. Coleman, Classical and overconvergent modular forms, *Invent. Math.* **124**(1–3) (1996), 215–241.
9. R. F. Coleman, Classical and overconvergent modular forms of higher level, *J. Théorie Nombres Bordeaux* **9**(2) (1997), 395–403.
10. B. Conrad, Modular curves and rigid-analytic spaces, *Pure Appl. Math. Q.* **2**(1) (2006), 29–110.
11. B. Conrad, Higher-level canonical subgroups in abelian varieties, preprint (available at http://math.stanford.edu/~conrad/papers/subgppaper.pdf).
12. A. J. de Jong, Crystalline Dieudonné module theory via formal and rigid geometry, *Publ. Math. IHES* **82** (1995), 5–96.
13. L. Fargues and Y. Tian, La filtration canonique des points de torsion des groupes p-divisibles, preprint (2009).

14. W. Fulton, *Intersection theory*, 2nd edn (Springer, 1998).
15. E. Z. Goren and P. L. Kassaei, The canonical subgroup: a 'subgroup-free' approach, *Comment. Math. Helv.* **81**(3) (2006), 617–641.
16. A. Grothendieck, Éléments de géométrie algébrique, III, Étude cohomologique des faisceaux cohérents, I, *Publ. Math. IHES* **11** (1961), 167.
17. A. Grothendieck, Éléments de géométrie algébrique, IV, Étude locale des schémas et des morphismes de schémas, III, *Publ. Math. IHES* **28** (1966), 255.
18. M. Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, Volume 78 (Academic Press, 1978).
19. L. Illusie, Déformations de groupes de Barsotti–Tate (d'après A. Grothendieck), *Astérisque* **127** (1985), 151–198.
20. P. L. Kassaei, $\mathcal{P}$-adic modular forms over Shimura curves over totally real fields, *Compositio Math.* **140**(2) (2004), 359–395.
21. P. L. Kassaei, A gluing lemma and overconvergent modular forms, *Duke Math. J.* **132**(3) (2006), 509–529.
22. N. M. Katz, p-adic properties of modular schemes and modular forms, Modular functions of one variable, III, in *Proc. Int. Summer School, Univ. Antwerp, Antwerp, 1972*, Lecture Notes in Mathematics, Volume 350, pp. 69–190 (Springer, 1973).
23. M. Kisin and K. F. Lai, Overconvergent Hilbert modular forms, *Am. J. Math.* **127**(4) (2005), 735–783.
24. S. Lang, *Algebra*, 2nd edn (Addison-Wesley, Reading, MA, 1984).
25. E. Lau, Displays and formal p-divisible groups, *Invent. Math.* **171**(3) (2008), 617–628.
26. H. Matsumura, *Commutative ring theory* (transl. from Japanese by M. Reid), 2nd edn, Cambridge Studies in Advanced Mathematics, Volume 8 (Cambridge University Press, 1989).
27. W. Messing, *The crystals associated to Barsotti–Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, Volume 264 (Springer, 1972).
28. J. Rabinoff, Tropical analytic geometry, newton polygons, and tropical intersections, preprint (arXiv:1007.2665).
29. J. T. Tate, p-divisible groups, in *Proc. Conf. Local Fields, Driebergen, 1966*, pp. 158–183 (Springer, 1967).
30. Y. Tian, Canonical subgroups of Barsotti–Tate groups, *Annals Math.* **172**(2) (2010), 955–988.
31. T. Zink, *Cartiertheorie kommutativer formaler Gruppen*, Teubner-Texte zur Mathematik, Volume 68 (B. G. Teubner, Leipzig, 1984).
32. T. Zink, The display of a formal p-divisible group, *Astérisque* **278** (2002), 127–248.