Galois Representations Arising from p-Divisible Groups

by
Max David Lieblich

a thesis
presented to the Department of Mathematics
in partial fulfillment
of the requirements for the degree
of Bachelor of Arts with Honors

Harvard University
Cambridge, Massachusetts
April 3, 2000

Contents

1 General Introduction

A primary goal of modern number theory is to understand the absolute Galois groups of certain classes of fields, among them number fields and their completions. During the 20th Century, it became clear that one of the best ways to study a group is to study its representations, and one of the best places to look for representations is in algebraic geometry. Even before Grothendieck's theory of schemes, algebraic geometers could think of an abelian variety A "defined over a field K," and thus number theorists could represent the Galois group $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$ by its action on (what we now call) the geometric points $A(\overline{K})$. It is in this context that the Galois representation which we now know as the "ℓ-adic Tate module" $T_\ell(A)$ was first studied by Weil. Classically, $T_\ell(A) = \varprojlim A(\overline{K})[\ell^n]$, the limit taken with respect to the maps $A(\overline{K})[\ell^n] \to A(\overline{K})[\ell^{n-1}]$ induced by multiplication by ℓ. If K is the field of fractions of a mixed characteristic $(0,p)$ discrete valuation ring R and A is "defined over R" with good reduction, then $T_\ell(A)$ for $\ell \neq p$ turns out to be an unramified $\mathscr{G}$-module. Thus, when R has *finite* residue field k, the $\mathscr{G}$-action in such cases is determined by the action of a fixed choice of arithmetic Frobenius element in $\mathscr{G}/I = \mathrm{Gal}(\bar{k}/k) \cong \widehat{\mathbf{Z}}$. Weil proved that this action has characteristic polynomial in $\mathbf{Z}[x]$ independent of $\ell \neq p$, encoding the number of k-rational points on the "reduction" of A.

However, $T_p(A)$ is much more mysterious. The reason became apparent during the development of the theory of group schemes: the finite flat p^n-torsion group schemes $\mathscr{A}[p^n]$ of the Néron model of A over R are not étale (whereas $\mathscr{A}[\ell^n]$ *is* étale for $\ell \neq p$). From the modern point of view, we find that the *R-group scheme* $\mathscr{A}[p^n]$ encodes a lot of subtle information about A. On the other hand, since $\mathrm{char}\, K = 0$, the generic fiber of $\mathscr{A}[p^n]$ is étale, so there is a fully faithful functor $\mathscr{A}_K[p^n] \rightsquigarrow A[p^n](\overline{K})$ which identifies the p-power torsion *generic fiber group scheme* $\mathscr{A}_K[p^n]$ with the *Galois module* structure on its geometric points $A(\overline{K})[p^n]$. Thus, as we will discuss in Part II, studying the Tate module $T_p(A)$ is equivalent to studying the generic fibers $\mathscr{A}_K[p^n]$. However, the p-adic Tate module Galois representation is highly ramified and so can only be understood through a study of the structure of the various schemes $\mathscr{A}[p^n]$. This interplay between relative geometry and (generic) Galois modules allowed Tate to prove several remarkable theorems [11]. Before we discuss Tate's theorems, we provide some motivation.

If A is a compact connected complex Lie group of dimension g (e.g., $A = X^{\mathrm{an}}$ for an abelian variety X over $\mathbf{C}$), then there is an isomorphism of complex Lie groups $A \cong V/\Lambda$, where $V = \mathrm{H}^0(A,\Omega^1)^\vee$ is a g-dimensional $\mathbf{C}$-vector space and $\Lambda = \mathrm{H}_1(A,\mathbf{Z})$ is a full lattice in V. It is a classical (*analytical*) result that there is a canonical decomposition

$$\mathrm{H}^1(A,\mathbf{C}) = \mathrm{H}^0(A,\overline{\Omega}^1) \oplus \mathrm{H}^0(A,\Omega^1), \tag{1}$$

where Ω^1 is the sheaf of holomorphic 1-forms on A and $\overline{\Omega}^1$ is the sheaf of anti-holomorphic 1-forms. If $A^\vee$ is the dual complex torus (constructed classically as $\overline{V}^\vee/\Lambda^\perp$ if $A = V/\Lambda$) and t (resp. t^*) denotes the tangent space (resp. cotangent space) at the identity, we may rewrite (1) as

$$\mathrm{Hom}_{\mathbf{Z}}(\mathrm{H}_1(A,\mathbf{Z}),\mathbf{C}) = t_{A^\vee} \oplus t_A^*.$$

In the case of an abelian variety over a local field K, Tate proved that there is a similar decomposition in the étale cohomology after extending scalars to $\mathbf{C}_K$ (the completion of an algebraic closure of K). To understand the statement, we recall what it means to *twist* a Galois module by a multiplicative character of the Galois group. If $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$ and $\chi : \mathscr{G} \to K^*$ is any continuous multiplicative character of $\mathscr{G}$, then given a $\mathscr{G}$-module M we define the *twist of M by χ*, denoted $M(\chi)$, to be the same underlying K-vector space with a new action given by $(s, m) \mapsto \chi(s)s(m)$. In the case where χ is the *p-adic cyclotomic character* $\varepsilon_p : \mathscr{G} \to \mathrm{Aut}(\boldsymbol{\mu}_{p^\infty}(\overline{K})) = \mathbf{Z}_p^\times$, we will write $M(n)$ for $M(\varepsilon_p^n)$. Tate showed that for the natural $\mathscr{G}$-action on $\mathbf{C}_K$, there is a canonical *$\mathscr{G}$-equivariant* decomposition, now called the *Hodge-Tate decomposition*,

$$\mathrm{Hom}_{\mathbf{Z}_p}(T_p(A), \mathbf{C}_K) = (t_{A^\vee} \underset{K}{\otimes} \mathbf{C}_K) \oplus (t_A^* \underset{K}{\otimes} \mathbf{C}_K(-1)). \tag{2}$$

(The analogy with the classical Hodge decomposition (1) over $\mathbf{C}$ is made clearer when we observe that for $A = V/\Lambda$, $T_p(A) \cong \mathbf{Z}_p \otimes_{\mathbf{Z}} \mathrm{H}_1(A, \mathbf{Z})$.) Like the classical Hodge decomposition, the proof of the Hodge-Tate decomposition relies heavily on (rigid) analytic techniques. For a finite-dimensional K-vector space V with a continuous $\mathscr{G}$-action, the property (generalizing (2)) that the semi-linear representation $V \otimes_K \mathbf{C}_K$ break up as a direct sum of various twists $\mathbf{C}_K(n)$ is a strong condition (as we will see in Part II). Therefore Tate's analytic result gives some insight into the Galois-module structure of the p-adic Tate module $T_p(A)$ (which is an *algebraic* object).

Tate proved the Hodge-Tate decomposition in the more general context of *p-Barsotti-Tate groups*. Given a base scheme S and an abelian scheme $\mathscr{A}$ of relative dimension g over S, the first step in forming a "p-adic Tate module over S" is the formation of the (scheme-theoretic) kernels $\mathscr{A}[p^n]$. These are finite locally free S-group schemes of order p^{2gn} and the canonical closed immersion $\mathscr{A}[p^n] \hookrightarrow \mathscr{A}[p^{n+1}]$ identifies $\mathscr{A}[p^n]$ with the kernel of $[p^n]$ on $\mathscr{A}[p^{n+1}]$. For reasons which will become clear shortly, it is to our advantage to view $(\mathscr{A}[p^n])$ as a *directed system* of finite locally free commutative S-group schemes. If $\mathscr{A}'$ is another abelian scheme over S, then any map of abelian schemes $\mathscr{A} \to \mathscr{A}'$ over S induces a compatible collection of maps $\mathscr{A}[p^n] \to \mathscr{A}'[p^n]$ over S, so there is a functor pBT_S from abelian schemes over S to certain directed systems of finite locally free commutative S-group schemes. In general, a directed system of finite locally free commutative S-group schemes $G = (G_n, i_n)$ such that G_n has order p^{nh} (for a fixed h) and $i_n : G_n \to G_{n+1}$ is a closed immersion identifying G_n with $G_{n+1}[p^n]$ will be called a *p-Barsotti-Tate group over S*. Homomorphisms between p-Barsotti-Tate groups $G \to H$ are just compatible systems of morphisms $G_n \to H_n$. We see that the functor pBT_S takes values in the category of p-Barsotti-Tate groups over S. Any p-Barsotti-Tate group is automatically equipped with faithfully flat group morphisms $j_n : G_n \to G_{n-1}$ generalizing "multiplication by p" $\mathscr{A}[p^n] \to \mathscr{A}[p^{n-1}]$ for abelian schemes.

In the case of an abelian scheme over R, taking points in $\overline{K}$ yields the inverse system of Galois modules $(G_n(\overline{K}), j_n(\overline{K}))$ whose limit is exactly $T_p(\mathscr{A}_K)$, and therefore we see that we may recover $T_p(\mathscr{A}_K)$ from $\mathrm{pBT}_R(\mathscr{A})$. By analogy with the case of an abelian scheme over R, given a p-Barsotti-Tate group $G = (G_n)$ over R, we define the *generic fiber* G_K of G to be the system $((G_n)_K, (i_n)_K)$ formed by the generic fibers of the finite stages and we define the *Tate module* $T(G)$ of G to be $T(G_K) = \varprojlim G_n(\overline{K})$, a finite free $\mathbf{Z}_p$-module with continuous $\mathscr{G}$-action. Tate's general result says that for any p-Barsotti-Tate group (G_n) over R,

$$\mathrm{Hom}_{\mathbf{Z}_p}(T(G), \mathbf{C}_K) \cong (t_{G^\vee} \underset{K}{\otimes} \mathbf{C}_K) \oplus (t_G^* \underset{K}{\otimes} \mathbf{C}_K(-1))$$

(where t_G and $t_{G^\vee}$ are the "tangent spaces" of G and its "dual" p-Barsotti-Tate group $G^\vee$). Most of this thesis is devoted to proving this result and explaining the numerous tools from algebraic geometry and number theory (not all of which are easily accessible in the literature) which are required for the proof.

Having established the Hodge-Tate decomposition for arbitrary p-Barsotti-Tate groups, Tate was then able to use it to prove the astonishing fact (which we will call the Isogeny Theorem) that the generic fiber functor $G \rightsquigarrow G_K$ is *fully faithful* on the category of p-Barsotti-Tate groups over R. Because $\mathrm{char}\, K = 0$, the generic fiber of any p-Barsotti-Tate group is étale, and it follows that $G \rightsquigarrow T(G_K)$ defines a fully faithful functor. Thus, we see that *a p-Barsotti-Tate group G over R is completely determined by its Tate module $T(G)$* (or, equivalently, by G_K). Such an equivalence with the generic fiber is manifestly untrue for finite flat group schemes over R (e.g., both the constant group $\underline{\mathbf{Z}/p\mathbf{Z}}$ and the group $\boldsymbol{\mu}_p$ have the same generic fiber over $\mathbf{Z}[\zeta_p]$, but they are quite different on the closed fiber, so the generic isomorphism determined by $1 \mapsto \zeta_p$ will *not* extend to an isomorphism over the entire base). Thus, the Isogeny Theorem is a deep theorem about the *entire system* (G_n). In Part I, we will develop a theory of *formal groups* over R which will allow us to encapsulate all of the data about the system (G_n) in a single object, the "direct limit formal group" $\varinjlim G_n$. In order to allow such natural constructions as the connected-étale sequence in the formal case, we will need to work over rather general (highly non-Noetherian) base rings when setting up the theory. The direct limit formal group of a p-Barsotti-Tate group will be called a *p-divisible group*.

The proof of Tate's theorems proceeds in two general stages. We will first study the formal properties of p-divisible groups which become apparent only in the limit. In particular, we will attach an invariant, the "dimension," to a p-Barsotti-Tate group $G = (G_n)$ by showing that the "connected" p-divisible group G^0 arising from the connected components of the G_n is a "formal Lie group." (The "formal smoothness" property inherent in G^0 is invisible at every finite stage, and is an example of a property which can only be seen in the limit.) After looking at the formal properties of p-divisible groups, we will use the formally smooth structure of connected p-divisible groups to give an *analytic* connection between the finite stages of p-Barsotti-Tate groups and the limiting p-divisible groups. In particular, we will attach a rigid analytic group G^{an} over K (arising from the "connected component") to a p-Barsotti-Tate group G over R. Given such an analytic group G^{an}, we will define a *logarithm* which analytically identifies a neighborhood of the identity of G^{an} with a neighborhood of the origin in the tangent space t_G of G^{an} at the identity. Using Cartier duality, we will prove the essential result relating the dual of the Tate module of G_K to t_G, and this will imply the remarkable fact that $\mathrm{Hom}_{\mathbf{Z}_p}(T(G_K), \mathbf{C}_K)$ admits a Hodge-Tate decomposition which encodes the *dimension* of G (over R). This provides the crucial link between $T(G)$ and the global properties of G over R. Finally, the smoothness of the connected component of G will enable us to calculate the discriminant of the "finite flat" map $[p^n] : G \to G$ by an analysis of the differential forms on G. This calculation, combined with the "dimension sensitivity" of $T(G)$, will imply the Isogeny Theorem.

Notation and prerequisites

We maintain the usual conventions regarding the rational integers, rational numbers, and complex numbers, denoting these by $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{C}$ respectively.

We assume familiarity with several non-trivial topics (we list each with its relevant notation):

1) Local class field theory and Galois cohomology (e.g., [10]).

Notation. A *local field* K will always be a field of characteristic zero complete with respect to a discrete valuation, with residue field of positive characteristic. (In general, we say that a discrete valuation ring R is *mixed characteristic* $(0, p)$ to indicate that the fraction field of R has characteristic zero, while the residue field has characteristic p.) We will denote by $\mathbf{C}_K$ the completion of an algebraic closure $\overline{K}$ of K.

The symbol $\mathscr{G}$ will be reserved for the absolute Galois group of K (i.e., $\mathrm{Gal}(\overline{K}/K)$); we will usually use $\mathscr{H}$ to denote either an open or closed subgroup of $\mathscr{G}$. We will use K_∞ to denote a $\mathbf{Z}_p$-extension of K, and we will write $\mathfrak{g} = \mathrm{Gal}(K_\infty/K)$.

The *p-adic cyclotomic character* of $\mathscr{G}$ will be denoted by $\varepsilon_p : \mathscr{G} \to \mathbf{Z}_p^\times$; it is determined by the action of $\mathscr{G}$ on the p-power roots of unity in $\overline{K}$. In general, given a $\mathscr{G}$-action on an $\mathscr{O}_K$-module M and a continuous multiplicative character $\chi : \mathscr{G} \to \mathscr{O}_K^\times$, the *twist* of M by χ, denoted $M(\chi)$, is defined to be the same underlying $\mathscr{O}_K$-module with the new action $g.m = \chi(g)g(m)$. In the case of the p-adic cyclotomic character, the twist $M(\varepsilon_p^n)$ will be written $M(n)$.

2) Basic elements of the theory of schemes.

Notation. Given an S-scheme X and a morphism $T \to S$, we will denote by X_T the base change $X \times_S T$. Given maps $f : T \to S$ and $g : X \to S$, we will use $T \times_{f,S,g} X$ to denote the fiber product $T \times_S X$ when we want to make the maps explicit.

3) Knowledge of finite group schemes, at least at the level of Tate's article [12] (including the connected-étale sequence over a Henselian local base) or the appropriate sections of Waterhouse's book [13], especially the theory of Cartier duality for finite locally free commutative group schemes. More generally, we expect that the reader has at least heard of affine group schemes and is aware of the Hopf-algebraic dual formulation of the theory.

Notation. A *finite S-group scheme* will always be assumed to be a finite locally free commutative group scheme over S. (We will drop the commutativity hypothesis on rare occasions; this will be made explicit when it happens.) We will write $|G|$ for the order of a finite group scheme G. We will often refer to an S-group scheme as an S-group. If G is an ordinary finite abelian group, we will let $\underline{G}_S$ (or simply $\underline{G}$ when the base is clear from context) denote the constant S-group sending an S-scheme T to locally constant functions $T \to G$.

Finally, we use the symbols □, ◊, and ⧫ to denote the end of proofs, examples, and remarks, respectively.

Acknowledgements

Without the continual advice and encouragement of Professor Brian Conrad, I would be hopelessly lost. His vision of mathematics and dedication to his students are a constant source of inspiration; I spent many more hours than I deserved in his office, and I am the better for it. For his superhuman attention to detail and his endless patience, I owe him a great debt.

I am also indebted to my parents. Without their love and support I would not be where I am today. They have helped shape my view of the world and implanted in me the values I hold dear: education, empathy, and a will to make things better.

Were it not for the continued vigilance of June Spector, neither this thesis nor its author would ever have seen the light of day. Her unflagging faith in me helped me see beyond the difficult moments.

Yu Yasufuku and Jacob Lurie provided helpful conversation at various points in this long process.

Part I
Formal groups

Let $\mathcal{A}_R$ be the category of (commutative unitary) R-algebras. Given a p-Barsotti-Tate group (G_n) over R and an object $A \in \mathrm{Obj}\,\mathcal{A}_R$, the groups $G_n(A)$ form a directed system of $\mathbf{Z}$-modules, so there is a covariant functor $G : A \rightsquigarrow \varinjlim G_n(A)$. Unfortunately, G is not represented by an R-scheme, essentially because there is no scheme large enough to simultaneously encode $G(A)$ for all R-algebras A. However, when R belongs to a certain class of rings (including complete local Noetherian rings) we will see that by restricting our attention to the category $\mathcal{F}_R$ of finite Artinian R-algebras, we can successfully "represent" G. Geometrically, this is the same as restriction our attention to infinitesimal neighborhoods of points of the various G_n. We call a set-valued functor on $\mathcal{F}_R$ a *formal functor*.

In this Part, we will rigorously construct formal functors and describe the ways in which we can represent them. Restricting our attention to group-valued formal functors, we will formulate a theory of commutative *formal groups* which we will use in Part II to assemble p-Barsotti-Tate groups, initially defined as directed systems of finite groups, into single group objects, *p-divisible groups*, which we can study geometrically (using smoothness, differential forms, etc.). Our study of formal groups will produce results which are parallel to standard results in the theory of finite group schemes.

Following our construction of the general theory of (commutative) formal groups, we will consider two important specializations: formal groups in positive characteristic and formal Lie groups. These two specializations will come together in Part II (Theorem 6.2.1) when we prove the crucial theorem of Serre and Tate that over a complete Noetherian local ring with residue characteristic p, "connected" p-divisible groups are identified with formal Lie groups for which multiplication by p is an "isogeny." (Our proof actually applies to a slightly larger class of base rings.) Finally, we will study discriminants in locally free ring extensions in order to calculate the discriminants of isogenies of formal Lie groups. These calculations will be essential for the proof of Tate's Isogeny Theorem.

2 Generalities

Before we define formal groups, we give some "pro-algebraic" preliminaries. For the most part, we will only state the basic properties and theorems of pro-algebra, indicating with a few words the essence of a proof or an especially important technique which we will use in the sequel. The most accessible source for this material is [1], where the reader will find a clear and enlightening treatment which collects in a single document the relevant material (with complete proofs) from Gabriel's development of these topics in SGA_3.

After our discussion of pro-algebra, we define formal groups and discuss their general properties in preparation for a more detailed study beginning in Section 3.

2.1 Pro-algebra and formal functors

Let us begin our study of pro-algebra with some motivation. Suppose R is a commutative ring. In the theory of finite R-groups, it is entirely natural to consider the *constant group* $\underline{G}$ for an ordinary finite abelian group G which represents the functor sending an R-scheme T to the locally constant functions $T \to G$. The affine algebra of $\underline{G}$ is $\prod_{g\in G} R = \mathrm{Hom}_{\mathrm{sets}}(G, R)$ with the obvious Hopf structure. If $f : G \hookrightarrow G'$ is an injection of finite groups, the corresponding map on R-algebras is the surjection $\prod_{g'\in G'} R \twoheadrightarrow \prod_{g\in G} R$ given by projection (identifying G with $f(G)$).

In the case of the constant p-Barsotti-Tate group $(\underline{\frac{1}{p^n}\mathbf{Z}/\mathbf{Z}})$, we expect by analogy with ordinary groups that the corresponding "constant p-divisible group" should be $\underline{\mathbf{Q}_p/\mathbf{Z}_p}$ and we naturally expect the "affine algebra" of $\underline{\mathbf{Q}_p/\mathbf{Z}_p}$ to be

$$\varprojlim_n \prod_{\frac{1}{p^n}\mathbf{Z}/\mathbf{Z}} R = \prod_{\mathbf{Q}_p/\mathbf{Z}_p} R,$$

which we notice is *highly* non-Noetherian. Furthermore, it is natural to impose a topology on $\prod_{\mathbf{Q}_p/\mathbf{Z}_p} R$ which allows us to retain the information that this group was assembled from a particular system of finite groups.

The natural category of topological rings to work in is the category of *pseudocompact rings*, which we will discuss before we use them as a tool to "geometrize" the theory of formal groups in Section 2.2.

2.1.1 Pseudocompact rings and profinite modules

We begin with a topological ring R which possesses a base for the topology at 0 defined by a collection $\mathfrak{I}_R$ of (open) ideals of R. Requiring that the ring operations be continuous with respect to this topology is the same as saying that a base at any $x \in R$ is given by $\{x + I : I \in \mathfrak{I}_R\}$. We say that R is *separated* if $\cap_{I\in\mathfrak{I}_R} I = (0)$ and *complete* if it is separated and the natural map of topological rings $R \to \varprojlim_{I\in\mathfrak{I}_R} R/I$ is an isomorphism. We will write $(R, \mathfrak{I}_R)$ when $\mathfrak{I}_R$ is not clear from context.

Definition 2.1.1. A topological ring $(R, \mathfrak{I}_R)$ is *pseudocompact* if R is complete and R/I is Artinian for all $I \in \mathfrak{I}_R$.

Example 2.1.2. The most natural examples of pseudocompact rings are Artinian rings and complete Noetherian local rings. In fact, any Noetherian pseudocompact local ring must actually have the maximal-adic topology [1, Corollary 1.2.7]. ◊

A *linearly topologized* R-module is a topological R-module M (i.e., $R \times M \to M$ is continuous) whose topology is defined at 0 by a set of open submodules Λ_M. We say that M is *separated* if $\cap_{N\in\Lambda_M} N = (0)$ and *complete* if M is separated and the natural map of topological R-modules $M \to \varprojlim_{N\in\Lambda_M} M/N$ is an isomorphism. A *topological R-algebra* is a topological R-module which is simultaneously a topological ring.

Definition 2.1.3. Given a pseudocompact ring R, a topological R-module M is *profinite* over R if M is complete and M/M' is finite over R for every $M' \in \Lambda_M$. A *profinite R-algebra* is a topological R-algebra B which is profinite as an R-module. Write $\mathfrak{P}_R$ for the category of profinite R-modules (with continuous module maps) and $\mathcal{P}_R$ for the category of profinite R-algebras (with continuous R-algebra maps).

Remarks 2.1.4. 1) We did not require that the topology on a profinite R-algebra A be defined by a base of open ideals. However, for future reference, we note that this is in fact the case. It suffices to show that any open R-submodule $M \subset A$ contains an open ideal of A. But the multiplication map $A \times A \to A$ is *continuous*, so there is an open R-submodule $N \subset A$ such that $N \cdot N \subset M$. By profiniteness, A/N has finitely many generators over R; choose $e_1, \dots, e_r$ in A whose images generate A/N. Since $e_i \cdot 0 = 0$ for all i, we see that there is a some open R-submodule $N' \subset N$ such that $e_i \cdot N' \subset M$ for all i, and therefore $N' \subset A \cdot N' \subset M$, so $A \cdot N'$ is the desired open ideal contained in M. Thus, we have shown that *if A is a profinite algebra over a pseudocompact ring, then A is pseudocompact.*

2) If M is profinite and $M' \subset M$ is open, then M/M' is actually finite over one of the Artinian quotients R/I of R. Indeed, the map $R \times M \to M \to M/M'$ is continuous and M/M' has the discrete topology, so for any $m \in M$, $\{r \in R : rm \equiv m \pmod{M'}\} \subset R$ is open. The rest follows because M/M' is finitely generated over R. Thus, M/M' has finite length over R. ♦

Example 2.1.5. While it is not true that any *finite* module over R is profinite, it is true that any *finitely presented* R-module admits a unique profinite R-module structure (this follows from Proposition 2.1.9). Profiniteness depends upon the topology and not just on the module: given a field k, the power series ring $k[\![\{X_i\}]\!]$ in countably many indeterminates is profinite with the topology determined by the ideals

$$\{(X_{i_1}^{a_1}, \dots, X_{i_n}^{a_n}, X_j \; (j \notin \{i_1, \dots, i_n\}))\},$$

but not with the maximal-adic topology. (The quotient of $k[\![\{X_i\}]\!]$ by the non-closed ideal $(\{X_i\})$ gives an example of a finite module over a pseudocompact ring which is not profinite.) ◊

Example 2.1.6. If A is a finite R-algebra, finitely presented as an R-module (or equivalently, as an R-algebra), then A with its unique profinite R-module structure is a profinite R-algebra (and therefore a pseudocompact ring by Remark 2.1.4(1)). ◊

Defining tensor products in such a way as to yield a useful theory of base change requires some care.

Definition 2.1.7. Given two linearly topologized R-modules M and N, we define the *completed tensor product* $M \widehat{\otimes}_R N$ to be the limit

$$\varprojlim (M/M' \underset{R/I}{\otimes} N/N'),$$

taken over triples $(M', N', I) \in \Lambda_M \times \Lambda_N \times \mathcal{I}_R$ such that I annihilates both M' and N'. This is linearly topologized with the inverse limit topology (with each $M/M' \otimes_{R/I} N/N'$ discrete).

It is not hard to see that $\widehat{\otimes}$ is an associative and commutative bifunctor on $\mathfrak{P}_R$.

For arbitrary linearly topologized R-modules, the completed tensor product is not very useful because there may not be any open ideal I which annihilates an open submodule M'. However, when M and N are profinite, the required triples (M', N', I) abound. We see that in the definition of $M \widehat{\otimes}_R N$, we could just as easily have formed the limit over triples (M', N', I) drawn from *any* (R-module) bases for topologies of M, N, and R and produced the same result.

Proposition 2.1.8. *The category $\mathfrak{P}_R$ is closed under*

(1) *product and finite direct sum (using the product topology),*

(2) *inverse limit,*

(3) *completed tensor product.*

Furthermore, we see that the bifunctor $\widehat{\otimes}$ satisfies the usual universal property with respect to bilinear maps in $\mathfrak{P}_R$.

The basic Proposition governing maps in $\mathfrak{P}_R$ is the following [1, Theorem 1.2.2].

Proposition 2.1.9. *Let R be a pseudocompact ring and M and N two profinite R-modules. Suppose $K \subset M$ is a closed submodule.*

(1) *Giving K the induced topology and M/K the quotient topology, K and M/K are profinite R-modules.*

(2) *If $u : M \to N$ is a continuous map of modules, then u is closed. In particular, injections coincide with closed embeddings and surjections coincide with topological quotient maps.*

(3) *The category $\mathfrak{P}_R$ is abelian if we take monomorphisms to be injections and epimorphisms to be surjections.*

Corollary 2.1.10. *If R is a pseudocompact ring, a map $f : M \to N$ of profinite R-modules is a topological isomorphism if and only if it is a continuous bijection. Furthermore, any continuous map of profinite R-modules with dense image is a surjection.*

We see immediately that if M and N are profinite R-modules and J is a closed ideal of R which annihilates both M and N, then the natural map $M \widehat{\otimes}_R N \to M \widehat{\otimes}_{R/J} N$ is an isomorphism.

Corollary 2.1.11. *If (M_i) is an inverse system of profinite R-modules with surjective transition maps, then the natural map $\varprojlim M_i \to M_i$ is surjective. In particular, $\varprojlim$ is an exact functor on the category of short exact sequences of profinite R-modules.*

Proposition 2.1.9 and its Corollaries make essential use of the non-trivial fact that given an inverse system of R-module surjections $u_i : M_i \to N_i$ with Artinian kernels, the induced map $u : \varprojlim M \to \varprojlim N$ is a surjection. See [1, Theorem 1.2.2] for the details.

One basic consequence of the definition of pseudocompact rings is that they behave in many ways like Artinian rings.

Proposition 2.1.12. *Let R be a pseudocompact ring. Given an open maximal ideal $\mathfrak{m} \subset R$, the natural map $R \to R_{\mathfrak{m}}$ is surjective and the kernel is a closed ideal. The resulting quotient topology on $R_{\mathfrak{m}}$ makes it a profinite R-algebra and the map*

$$\Pi : R \to \prod R_{\mathfrak{m}}$$

(where the product is taken over the open maximal ideals) is a topological isomorphism.

Using Proposition 2.1.12, we can give the fundamental properties of $\widehat{\otimes}$ [1, Theorem 1.1.8 and Theorem 1.3.1]. Given a profinite R-module M, define $M_{\mathfrak{m}} = M \widehat{\otimes}_R R_{\mathfrak{m}}$.

Proposition 2.1.13. *Let $R \to S$ be a (continuous) map of pseudocompact rings and let M and N be profinite R-modules.*

(0) *The natural map $R \widehat{\otimes}_R M \to M$ is an isomorphism.*

(1) *The operation $M \rightsquigarrow M \widehat{\otimes}_R S$ gives a functor $\mathfrak{P}_R \to \mathfrak{P}_S$, naturally compatible with composites of maps of pseudocompact rings.*

(2) *The functor $M \widehat{\otimes}_R(\,\cdot\,) : \mathfrak{P}_R \to \mathfrak{P}_R$ is right-exact.*

(3) *Given an inverse system N_i of profinite R-modules, the natural map*

$$M \underset{R}{\widehat{\otimes}} \varprojlim N_i \to \varprojlim (M \widehat{\otimes} N_i)$$

is a topological isomorphism. In particular, $M \widehat{\otimes} \prod N_i \xrightarrow{\sim} \prod (M \widehat{\otimes} N_i)$.

(4) *For each open maximal ideal $\mathfrak{m} \subset R$, the natural map $M \to M_{\mathfrak{m}}$ is surjective with closed kernel. The resulting quotient topology makes $M_{\mathfrak{m}}$ a profinite $R_{\mathfrak{m}}$-module and the natural map $M \to \prod M_{\mathfrak{m}}$ over $R \xrightarrow{\sim} \prod R_{\mathfrak{m}}$ is a topological isomorphism. Thus, for any open ideal $\mathfrak{m} \subset R$, the natural map $R_{\mathfrak{m}} \otimes_R M \to R_{\mathfrak{m}} \widehat{\otimes}_R M$ is an isomorphism. Similarly, there is a natural isomorphism*

$$\mathrm{Hom}_{\mathfrak{P}_R}(M, N) \xrightarrow{\sim} \prod \mathrm{Hom}_{\mathfrak{P}_{R_{\mathfrak{m}}}}(M_{\mathfrak{m}}, N_{\mathfrak{m}}).$$

(Proposition 2.1.13(4) follows from Proposition 2.1.12 and parts (0) and (3) of Proposition 2.1.13.)

Remark 2.1.14. One can also show that for any profinite R-algebra A and any pseudocompact ring S, the profinite S-algebra $A \widehat{\otimes}_R S$ represents the functor

$$\mathrm{Hom}_{\mathrm{cont}}(A, \,\cdot\,)$$

on $\mathcal{P}_S$ (the category of profinite S-algebras). This gives a good notion of base change, which we will exploit in our study of formal schemes (cf. Proposition 2.1.26). ◆

Corollary 2.1.15. *If R is pseudocompact, M is a profinite R-module, and $\mathfrak{r} \subset R$ is a closed ideal, then $(R/\mathfrak{r}) \widehat{\otimes}_R M \xrightarrow{\sim} M/\overline{\mathfrak{r}M}$.*

Definition 2.1.16. Given a pseudocompact ring R and a profinite R-module M, M is *topologically flat* (resp. *topologically faithfully flat*) if and only if for every sequence $\mathscr{S} : 0 \to N_1 \to N_2 \to N_3 \to 0$ of profinite R-modules, $M \widehat{\otimes}_R \mathscr{S}$ is exact if $\mathscr{S}$ is exact (resp. if and only if $\mathscr{S}$ is exact). We call M *topologically free* if there is a topological isomorphism $M \cong \prod_{j \in J} R$ for some index set J (where $\prod R$ is given the product topology).

Lemma 2.1.17. *A profinite A-algebra $\sigma : A \to B$ is topologically faithfully flat if and only if the structure map σ is injective and topologically flat, and this is the same as requiring that for each open maximal ideal $\mathfrak{m} \subset A$ the profinite $A_{\mathfrak{m}}$-algebra $B_{\mathfrak{m}}$ is non-zero and topologically flat.*

Proposition 2.1.18. *Over a complete Noetherian local ring, topological (faithful) flatness is equivalent to (faithful) flatness. If R is any pseudocompact ring and M a finite profinite R-module (resp. -algebra), then M is topologically (faithfully) flat if and only if M is (faithfully) flat.*

The following Proposition will prove useful in Part II and illustrates some of the technical workings of this subject. We will use this result to show that the limit of a direct system of surjections of finite group schemes is a surjection of formal groups.

Proposition 2.1.19. *Fix a pseudocompact base ring R. If $A_n \to B_n$ is an inverse system of topologically faithfully flat maps of profinite R-algebras then $A = \varprojlim A_n \to \varprojlim B_n = B$ is topologically faithfully flat. In particular, an inverse limit of topologically flat profinite R-algebras is topologically flat.*

Proof. For any profinite A-module T and any collection T_n of closed submodules of T, call $\{T_n\}$ a *defining collection* if $\cap T_n = (0)$. It is not hard to see that $\{T_n\}$ is a defining collection of closed submodules of T if and only if the natural map $T \to \varprojlim T/T_n$ is an isomorphism.

By definition the canonical map $A \to A_n$ has closed kernel I_n. Therefore, given a profinite A-module M, defining M_n to be $\overline{I_n M}$, we have

$$M = M \underset{A}{\widehat{\otimes}} A = \varprojlim (M \underset{A}{\widehat{\otimes}} A_n) = \varprojlim M/M_n.$$

Suppose

$$\mathscr{S} : 0 \to N \to M \xrightarrow{f} P \to 0$$

is a short exact sequence of profinite A-modules containing M. Define $N_n = M_n \cap N$ and $P_n = f(M_n)$. For every n, the sequence

$$\mathscr{S}_n : 0 \to N/N_n \to M/M_n \to P/P_n \to 0$$

is exact. Because $\cap M_n = (0)$, we see that $\{N_n\}$ is a defining collection of closed submodules of N. By the exactness of $\varprojlim$ on $\mathfrak{P}_A$, where therefore see that $\{P_n\}$ is a defining collection of closed submodules of P. By Corollary 2.1.10, it is not hard to see that

$$B \underset{A}{\widehat{\otimes}} \mathscr{S} \cong \varprojlim (B_n \underset{A}{\widehat{\otimes}} \mathscr{S}_n) \cong \varprojlim (B_n \underset{A_n}{\widehat{\otimes}} \mathscr{S}_n),$$

the first isomorphism following because $\widehat{\otimes}$ commutes with $\varprojlim$ and $\{B_n \widehat{\otimes}_A \mathscr{S}_n\}$ is coinitial in the inverse system for $B \widehat{\otimes}_A \mathscr{S}$. But B_n is topologically flat over A_n, so $B_n \widehat{\otimes}_{A_n} \mathscr{S}_n$ is exact. By the exactness of $\varprojlim$ on short exact sequences of profinite A-modules, we see that B is topologically flat over A. Similarly, by the left-exactness of $\varprojlim$, we see that $A \to B$ is injective, and therefore B is topologically faithfully flat over A by Lemma 2.1.17. □

The following Proposition will be useful in our study of the connected-étale sequence for formal groups. Recall that a local ring A is *Henselian* if every finite A-algebra breaks up as a product of finite local A-algebras (which are then themselves Henselian).

Proposition 2.1.20. *A pseudocompact local ring R is Henselian.*

Proof. Given a finite R-algebra B, we see that B is a quotient of a finite free R-algebra B'. It clearly suffices to show that B' breaks up as a product of finite local R-algebras, so we may assume that B is finitely presented as an R-module. By Example 2.1.6, B is a profinite R-algebra, hence pseudocompact as a topological ring. Therefore, $B \cong \prod B_{\mathfrak{m}}$, indexed by the open maximal ideals $\mathfrak{m} \subset B$. On the other hand, every open maximal ideal of B must contract to the unique (open) maximal ideal $\mathfrak{m}_R$ of R by integrality. Because open ideals are closed and continuous maps of profinite R-algebras are closed, we see that $B/\mathfrak{m}_R B$ is a finite profinite $R/\mathfrak{m}_R$-algebra. Thus, there can be only finitely many open maximal ideals of B, so B breaks up as a product of finitely many finite local R-algebras. □

A more profound example of the resonance between Artinian and pseudocompact rings is the following Proposition, which will prove to be essential in the theory of formal groups.

Proposition 2.1.21. *Given a pseudocompact ring R and a profinite R-module M, the following are equivalent*

(1) *M is a projective object in $\mathfrak{P}_R$;*

(2) *M is topologically flat over R;*

(3) *for any open maxmial ideal $\mathfrak{m} \subset R$, $M_{\mathfrak{m}}$ is topologically free over $R_{\mathfrak{m}}$.*

We see from the proof in [1, Theorem 1.3.6] that topologically free profinite R-modules are projective in $\mathfrak{P}_R$.

The relationship with Artinian rings suggests one final Proposition which will prove to be a useful tool.

Proposition 2.1.22 (Formal Nakayama's Lemma). *If $(R, \mathfrak{m}, k)$ is a pseudocompact local ring and M is a profinite R-module such that $M/\overline{\mathfrak{m}M} = M \widehat{\otimes}_R k$ vanishes, then $M = 0$.*

Proof. Choosing an open submodule $M' \subset M$, applying $(\cdot) \widehat{\otimes}_R k$ to the exact sequence

$$0 \to M' \to M \to M/M' \to 0$$

yields a surjection $M \mathbin{\widehat{\otimes}}_R k \twoheadrightarrow (M/M') \mathbin{\widehat{\otimes}}_R k$, so $(M/M') \mathbin{\widehat{\otimes}}_R k = 0$. But M/M' is discrete, so there is an initial object $(M/M)' \otimes_R k$ in the inverse system for $(M/M') \mathbin{\widehat{\otimes}}_R k$ and therefore $0 = (M/M') \mathbin{\widehat{\otimes}}_R k = (M/M') \otimes_R k$. But M/M' is finite over R, so by the usual form of Nakayama's Lemma, $M/M' = 0$. By completeness, $M = 0$. $\square$

The following argument will be used often.

Corollary 2.1.23. *Let $(R, \mathfrak{m}, k)$ be a pseudocompact local ring. If $f : M \to N$ is a map of topologically flat profinite R-modules, then f is an isomorphism if and only if $f \mathbin{\widehat{\otimes}} k : M \mathbin{\widehat{\otimes}} k \to N \mathbin{\widehat{\otimes}} k$ is an isomorphism.*

Proof. By the Formal Nakayama's Lemma, f is surjective if and only if $f \mathbin{\widehat{\otimes}} k$ is surjective. But if this holds, then f splits by topological flatness (which is the same as projectivity), so therefore f is injective if and only if $f \mathbin{\widehat{\otimes}} k$ is injective. $\square$

Having given the proof, we will refer to this as a "standard Formal Nakayama's Lemma argument" from now on.

We conclude this rapid but unpleasantly dry review of pseudocompact rings and profinite modules with a *caveat* to the reader: in order to make a natural and efficient summary of the results we will use, we have not stated the results in "logical dependence" order. It is advisable that a reader who wants a detailed understanding of this material carefully read [1].

2.1.2 Formal functors and pro-representability

Let R be a pseudocompact ring. Let $\mathcal{F}_R$ denote the category of finite Artinian R-algebras (viewed as discrete profinite R-algebras by Example 2.1.2 and Remark 2.1.4(1)).

Definition 2.1.24. A *formal functor* is a set-valued functor on $\mathcal{F}_R$.

In algebraic geometry, the study of schemes over a ring k is tantamount to the study of a specific full subcategory of the category of set-valued functors on $\mathcal{A}_k$. Abstractly, we could define an *affine k-scheme* to be a set-valued functor on $\mathcal{A}_k$ which is *representable* by an object of $\mathcal{A}_k$, and an arbitrary k-scheme is then a functor which is "locally affine." In a similar way, we single out a full "geometric" subcategory of the formal functors to serve as the category of *formal schemes*. However, we will not be able to represent a formal scheme with an object of $\mathcal{F}_R$. Instead, we will "pro-represent" it with an object of $\mathcal{P}_R$ (the category of profinite R-algebras).

Observe that for objects $A, B \in \operatorname{Obj} \mathcal{P}_R$, $\operatorname{Hom}_{\mathcal{P}_R}(A, B) = \varprojlim \operatorname{Hom}_{\mathcal{P}_R}(A, B/\mathfrak{b})$, where $\mathfrak{b}$ ranges over the open ideals of B. Therefore, we can recover A by Yoneda's Lemma if we know the restriction of $\operatorname{Hom}_{\mathcal{P}_R}(A, \cdot)$ to $\mathcal{F}_R$. We call the formal functor $\operatorname{Hom}_{\mathcal{P}_R}(A, \cdot)|_{\mathcal{F}_R}$ the *formal spectrum* of A, denoted $\operatorname{Spf}_R A$. We call $\operatorname{Spf}_R A$ topologically (faithfully) flat over R if A topologically (faithfully) flat over R.

Definition 2.1.25. A formal functor $\mathfrak{X} : \mathcal{F}_R \to \mathbf{Set}$ is *pro-representable* if there is an $A \in \operatorname{Obj} \mathcal{P}_R$ such $\mathfrak{X} \cong \operatorname{Spf}_R A$. A pro-representable formal functor is called a *formal R-scheme*. We write $A = \mathscr{O}(\mathscr{X})$.

The usual arguments using Yoneda's Lemma apply to formal schemes. In particular, we see that the category of formal schemes is equivalent to the opposite category $\mathcal{P}_R^{\mathrm{op}}$. Let $\mathfrak{S}ch_R$ denote the category of formal R-schemes.

Proposition 2.1.26. *The category $\mathfrak{S}ch_R$ has the following properties:*

(1) Fiber products. $\mathrm{Spf}_R(A) \times_{\mathrm{Spf}_R(C)} \mathrm{Spf}_R(B) = \mathrm{Spf}_R(A \mathbin{\widehat{\otimes}}_C B)$.

(2) Base change. *Given a profinite R-algebra R', consider the embedding $\mathcal{F}_{R'} \hookrightarrow \mathcal{F}_R$. The restriction of* $\mathrm{Spf}_R(B)$ *to $\mathcal{F}_{R'}$, denoted* $\mathrm{Spf}_R(B)_{R'}$, *is* $\mathrm{Spf}_{R'}(B \mathbin{\widehat{\otimes}}_R R')$. *If $(R, \mathfrak{m}, k)$ is local, we call $\mathrm{Spf}_R(B)_k = \mathrm{Spf}_k(B \mathbin{\widehat{\otimes}}_R k)$ the* formal closed fiber *of B. More generally, if $R \to R'$ is any continuous map of pseudocompact rings, $R' \mathbin{\widehat{\otimes}}_R B$ is a profinite R'-algebra, so we may define the* base change *of $\mathrm{Spf}_R(B)$ to R' by $\mathrm{Spf}_R(B)_{R'} = \mathrm{Spf}_{R'}(B \mathbin{\widehat{\otimes}}_R R')$; see Remark 2.1.14. Base change is compatible with fiber products.*

(3) Direct limits. *If* $\mathrm{Spf}_R(B_i)$ *is a directed system of formal schemes, then*

$$\varinjlim \mathrm{Spf}_R(B_i) = \mathrm{Spf}_R(\varprojlim B_i).$$

(4) Formalization of finite, finitely presented R-schemes. *Let $\mathbf{Fin}_R$ denote the category of finite, finitely presented R-schemes. There is a fully faithful embedding $\mathbf{Fin}_R \hookrightarrow \mathfrak{S}ch_R$ which takes (faithfully) flat finite R-schemes to topologically (faithfully) flat R-schemes.*

Proposition 2.1.26(3) and Proposition 2.1.26(4) (together with Proposition 2.1.19) are precisely what we need to assemble our p-Barsotti-Tate groups into formal limits with good properties (e.g., topological flatness).

Definition 2.1.27. If $f : \mathrm{Spf}_R A \to \mathrm{Spf}_R B$ is a map of formal schemes, then by Yoneda's Lemma f is induced by a unique a map $f^* \in \mathrm{Hom}_{\mathcal{P}_R}(B, A)$. We will call f *topologically (faithfully) flat* if f^* is topologically (faithfully) flat.

By analogy with ordinary algebraic geometry, we have the following Proposition.

Proposition 2.1.28 (Formal fiberwise criterion). *If A and B are topologically flat over R, then a map $f : \mathrm{Spf}_R A \to \mathrm{Spf}_R B$ is topologically (faithfully) flat if and only if the base change $f_{\mathfrak{m}} : \mathrm{Spf}_R(A)_{R/\mathfrak{m}} \to \mathrm{Spf}_R(B)_{R/\mathfrak{m}}$ is topologically (faithfully) flat (as a map of formal $R/\mathfrak{m}$-schemes) for all open maximal ideals $\mathfrak{m} \subset R$.*

Proposition 2.1.29. *If $f : A \to B$ is a map of profinite R-algebras and C is a topologically faithfully flat profinite A-algebra, then f is finite (resp. finite free of rank d, topologically flat, topologically faithfully flat, injective, surjective) if and only if the same is true for $C \to C \mathbin{\widehat{\otimes}}_A B$.*

Sketch of a proof. The result for injectivity, surjectivity, topological flatness, and topological faithful flatness follow easily from the definition of topological faithful flatness once we note that the profinite R-module cokernel of f is a profinite A-module. The result for finiteness follows by reducing to the case where A is local and then using the Formal Nakayama's Lemma to reduce to the closed fiber, where all profinite modules are topologically free. (We use the fact in this case that if $B_\mathfrak{m}$ is finite over $A_\mathfrak{m}$ for all open maximal ideals $\mathfrak{m} \subset A$ and there is an upper bound on the number of generators as $\mathfrak{m}$ varies, then B is finite over A.) The result in the case of a finite free map of rank d follows by reducing to the case where A is local (with some care) and combining the finite and topologically flat cases. □

None of the Propositions of this section is especially difficult to prove, but they would all entail a great digression from the purpose of this thesis. Complete proofs may be found in [1].

2.2 Formal groups

We are now ready to construct the objects which are of principal interest to us. Fix a pseudocompact ring R throughout this section.

Definition 2.2.1. A *formal R-group scheme* (or simply *formal R-group*) is a topologically flat formal R-scheme taking values in the category of groups.

While this all seems rather convoluted, formal R-group schemes arise quite naturally.

Example 2.2.2. Suppose R is a complete Noetherian local ring. Let G be any flat algebraic group scheme over R (so that G is locally of finite type) with identity section $\varepsilon : \operatorname{Spec} R \to G$, and let $\mathfrak{m}$ denote the closed point on the identity section of G. Given an R-scheme T, call a point $x \in G(T)$ a *small point* if T is a finite Artinian R-scheme and the image of $x : T \to G$ is supported at the closed point of the identity section. It is easy to see (because $\varepsilon \cdot \varepsilon = \varepsilon$ in the group law on $G(\operatorname{Spec} R)$) that restricting G to small points gives a functor $\widehat{G} : \mathcal{F}_R \to \mathbf{Grp}$. Furthermore, since any small point factors uniquely through (an Artinian quotient) of the local scheme $\operatorname{Spec} \mathscr{O}_{\mathfrak{m},G}$, we see that $\widehat{G}$ is pro-represented by the maximal-adic completion $\widehat{\mathscr{O}}_{\mathfrak{m},G}$. But G is flat and locally of finite type over R, so $\mathscr{O}_{\mathfrak{m},G}$ is a Noetherian ring and is faithfully flat over R because $\mathfrak{m}$ lies over the closed point of $\operatorname{Spec} R$. By the basic theory of Noetherian local rings, $\widehat{\mathscr{O}}_{\mathfrak{m},G}$ is faithfully flat over $\mathscr{O}_{\mathfrak{m},G}$. By the finite type hypothesis and Proposition 2.1.18, we see that $\widehat{\mathscr{O}}_{\mathfrak{m},G}$ is a topologically faithfully flat profinite R-algebra, and therefore $\widehat{G} = \operatorname{Spf}_R(\widehat{\mathscr{O}}_{\mathfrak{m},G})$ is a formal R-group.

The construction of a formal group encoding the group law near the identity was first done in the context of Lie groups as a way of creating an object intermediate between the group and its Lie algebra. For algebraic groups over fields of characteristic zero, the formal group so constructed (with small points) yields no more information than the Lie algebra of the group. However, when the base field has positive characteristic p, the formal group can detect non-reduced phenomena which do not appear in the Lie algebra (which can only see the reduced structure on the group). In particular, the formal group $\widehat{G}$ stores information about p-power torsion on G, which may not appear geometrically in the form of classical points. We will see an important application of this idea in Part II when we study p-divisible groups (e.g., those arising from abelian schemes). ◊

Example 2.2.3. Applying Example 2.2.2 to the multiplicative group $\mathbf{G}_m$, we get the *formal multiplicative group* $\widehat{\mathbf{G}}_m$. Writing $\mathbf{G}_m = \operatorname{Spec} R[x, x^{-1}]$, we see by making the change of variable $x = t + 1$ that $\widehat{\mathbf{G}}_m = \operatorname{Spf}_R R[\![t]\!]$.

Similarly, we may construct the *formal additive group* $\widehat{\mathbf{G}}_a$, and we see that if $\mathbf{G}_a = \operatorname{Spec} R[x]$, then $\widehat{\mathbf{G}}_a = \operatorname{Spf}_R R[\![x]\!]$. $\Diamond$

As in the case of a finite (or affine) group scheme over R, the theory of formal R-groups admits a dual formulation in terms of *formal Hopf algebras*. Suppose $G = \operatorname{Spf}_R A$ is a formal R-group. Using Yoneda's Lemma, we see that the multiplication, the inversion morphism, and the identity section give rise to maps of profinite R-algebras

$$m^* : A \to A \mathbin{\widehat{\otimes}} A \qquad i^* : A \to A \qquad \varepsilon^* : A \to R,$$

called the (formal) *comultiplication*, *antipode*, and *augmentation*, respectively. Conversely, given three such maps which satisfy the usual group axioms when viewed as maps of formal schemes (i.e., given a formal Hopf algebra A), $G = \operatorname{Spf}_R A$ is a formal R-group.

Example 2.2.4. The formal Hopf maps for the formal multiplicative group are:

$$\begin{aligned} m^*(t) &= 1 \mathbin{\widehat{\otimes}} t + t \mathbin{\widehat{\otimes}} 1 + t \mathbin{\widehat{\otimes}} t, \\ i^*(t) &= -\frac{t}{1+t}, \\ \varepsilon^*(t) &= 0. \end{aligned}$$

(This comes from the usual Hopf maps for the multiplicative group: $m^*(x) = x \otimes x$, $i^*(x) = x^{-1}$, and $\varepsilon^*(x) = 1$, after our change of variable $x = t + 1$.)

Similarly, the formal Hopf maps for the formal additive group are the usual ones: $m^*(x) = x \mathbin{\widehat{\otimes}} 1 + 1 \mathbin{\widehat{\otimes}} x$, $i^*(x) = -x$, and $\varepsilon^*(x) = 0$. $\Diamond$

Using the Hopf-theoretic approach, we can also construct formal group schemes which are not otherwise "geometrically intuitive."

Example 2.2.5. As an example, we can construct a type of formal group which often arises in an arithmetic context: a discrete (constant) commutative group. Given a commutative (set-theoretic) group G, we may define the constant group $\underline{G}$ over R by declaring $\underline{G} = \operatorname{Spf}_R A$, where $A = \prod_{g \in G} Re_g$ with the formal Hopf structure given by

$$\begin{aligned} m^* &: e_g \mapsto \sum_{h\ell = g} e_h \mathbin{\widehat{\otimes}} e_\ell, \\ i^* &: e_g \mapsto e_{g^{-1}}, \\ \varepsilon^* &: e_g \mapsto \delta_{g,1}, \end{aligned}$$

and extended by continuity and linearity. In Theorem 3.1.6, we will see how to construct "twisted forms" of these constant groups (which become untwisted over a suitable extension ring). $\Diamond$

We will encounter numerous examples of formal groups in Part II, where we will assemble p-Barsotti-Tate groups into formal limits.

2.2.1 Duality

Recall that for finite locally free commutative group schemes over R, the usual module-theoretic dualizing functor sending the finite locally free algebra A to the locally free module

$$A^\vee \stackrel{\text{def}}{=} \operatorname{Hom}_{R\text{-mod}}(A, R)$$

actually establishes a duality on the category of finite commutative R-group schemes. This arises because the module-theoretic dualizing functor switches the algebra maps with the Hopf maps, and the resulting object $A^\vee$ is a commutative cocommutative Hopf algebra because $\operatorname{Spec} A$ is a commutative R-group.

When we try to extend this to the case of commutative formal groups, we have serious difficulty if we try to work over an arbitrary pseudocompact base. Let us restrict ourselves to the case where R is actually an Artinian local ring. Given a profinite R-module M, the module $M^\vee = \operatorname{Hom}_{\mathfrak{P}_R}(M, R)$ is no longer profinite; it is merely an R-module. In fact, we will see in a moment that it could be *any* R-module. On the other hand, because R is Artinian, given an arbitrary R-module N, the module $N' = \operatorname{Hom}_R(N, R)$ has a natural profinite structure given by $N' = \varprojlim \operatorname{Hom}_R(N_i, R)$, where N_i ranges over all finite R-submodules of N. Thus, $M \rightsquigarrow M^\vee$ gives a functor $\mathfrak{P}_R \to R\text{-}\mathbf{mod}$ and $N \rightsquigarrow N'$ gives a functor $R\text{-}\mathbf{mod} \to \mathfrak{P}_R$. This suggests the following proposition. For technical reasons, we restrict our functors to topologically flat (equivalently, topologically free) profinite modules $\mathfrak{P}_{R,\text{top. flat}}$ and flat (equivalently, free) R-modules $R\text{-}\mathbf{mod}_{\text{flat}}$. (Part (1) of the following proposition states that these restrictions are respected by the dualizing functors.)

Proposition 2.2.6 (Formal duality). *Let R be an Artinian local ring, and let M be a profinite topologically flat R-module and N a flat R-module.*

(1) *$M^\vee$ is flat and N' is topologically flat.*

(2) *There is a natural isomorphism $M \xrightarrow{\sim} (M^\vee)'$ and a natural isomorphism $N \xrightarrow{\sim} (N')^\vee$ given in both cases by sending an element of M (resp. N) to evaluation of maps on that element. As functors between $\mathfrak{P}_{R,\text{top. flat}}$ and $R\text{-}\mathbf{mod}_{\text{flat}}$, $M \rightsquigarrow M^\vee$ and $N \rightsquigarrow N'$ are exact, interchange direct products and direct sums, and there are natural isomorphisms*

$$M_1^\vee \otimes M_2^\vee \xrightarrow{\sim} (M_1 \widehat{\otimes} M_2)^\vee$$

and

$$N_1' \widehat{\otimes} N_2' \xrightarrow{\sim} (N_1 \otimes N_2)'.$$

(3) *The functors $(\,\cdot\,)^\vee$ and $(\,\cdot\,)'$ are compatible with local Artinian base change.*

The proof of Proposition 2.2.6 is straightforward. The reader may again consult [1, Theorem 1.3.4] for details.

Corollary 2.2.7. *Given an Artinian local ring R, there is a duality between commutative affine group schemes over R and commutative formal R-groups.*

Composing with the formalization functor (Proposition 2.1.26(4)), we see that Cartier duality over R is nothing more than a restriction of the dualization between affine and formal group schemes over R to a subcategory which is in "the intersection" of the two.

The duality established in Corollary 2.2.7 will prove to be essential in several of our constructions, notably in our analysis of the Frobenius and Verschiebung morphisms in Theorem 3.2.4 below.

2.2.2 Exact sequences

Now that we have constructed formal groups, we will briefly look at the maps between them. In particular, we will formulate the indispensible notion of an *exact sequence* and check that exact sequences have good properties.

Definition 2.2.8. Given a morphism $g : G \to H$ of formal R-groups, we say that g is *injective* if $g^* : \mathscr{O}(H) \to \mathscr{O}(G)$ is surjective (i.e., g is a "formal closed immersion"); we say that g is *surjective* if $g^* : \mathscr{O}(H) \to \mathscr{O}(G)$ is topologically faithfully flat. The *kernel* of g is defined to be $G \times_{H,\varepsilon_H} S$ (the "formal scheme-theoretic kernel").

Recall in the case of affine flat algebraic R-groups that $G \to H$ is a closed immersion if the corresponding ring map is surjective, and is called "a quotient map" if the corresponding ring map is faithfully flat.

It is not always true that $\ker g$ is a formal R-group because topological flatness is not guaranteed by the formation of the formal scheme-theoretic kernel unless $G \to H$ is topologically flat. However, when R is a field, topological flatness *is* automatic.

The formation of cokernels is a slighly more complicated affair. We give a brief sketch. For the sake of simplicity, we only treat the case where R is local, which suffices for our purposes.

Lemma 2.2.9. *Let R be a local pseudocompact ring. A map of flat formal Hopf R-algebras $A \to B$ is topologically faithfully flat if and only if it is injective on the closed fiber. Similarly, if R is also Artinian then a map of affine Hopf R-algebras is faithfully flat if and only if it is injective on the closed fiber.*

Sketch of proof. By the (formal) fiberwise criterion for faithful flatness, we can assume in the formal case that R is a field k. Writing $G = \mathrm{Spf}_k\, B$ and $H = \mathrm{Spf}_k\, A$, we have a map $\xi : G \to H$ corresponding to $A \to B$. Because k is a field, we can form the kernel $K = \ker \xi$ in the category of formal k-groups. We see by Yoneda's Lemma that $G \times_H G \xrightarrow{\sim} G \times_k K$, and therefore we conclude that $G \times_H G$ is topologically faithfully flat over G by the first projection. The rest of the proof is a (slightly difficult) exercise in pro-algebra [1, Theorem 2.1.3]. In the affine case, the proof is much more involved. One uses [7, Theorem 22.3(α)] and the fact that the maximal ideal of R is nilpotent to reduce to the case where R is a field. For details when R is a field, see [1, Theorem 2.1.3] (or [13, §§14.1, 14.2] for a more elementary treatment). □

Lemma 2.2.10. *If $(R, \mathfrak{m}, k)$ is an Artinian local ring, and $g : G \to H$ is a morphism of formal R-groups, then g is a surjection if and only if $g^\vee : H^\vee \to G^\vee$ is an injection.*

Proof. Write $B = \mathscr{O}(G)$ and $A = \mathscr{O}(H)$. If $g^\vee$ is an injection, then dualizing shows that the induced map $g^* : A \to B$ is a split injection, hence g is a surjection by Lemma 2.2.9. On the other hand, suppose g is a surjection, so that $g^* : A \to B$ is topologically faithfully flat. By compatibility with base change, we see that $g_k^* : A_k \to B_k$ is a topologically faithfully flat map of profinite k-algebras, hence injective. But every profinite k-module is topologically free, so we can apply Proposition 2.2.6 to conclude that the dual map $(g_k^*)^\vee : (B_k)^\vee \to (A_k)^\vee$ is a surjection. By Proposition 2.2.6(3), we see that $(g^*)_k^\vee : (B^\vee)_k \to (A^\vee)_k$ is surjective. Since $\mathfrak{m}$ is nilpotent and $A^\vee$ is flat over R, we see that $(g^*)^\vee = (g^\vee)^*$ is surjective [7, Theorem 7.10], so $g^\vee$ is an injection of affine R-group schemes. □

Construction. Suppose $f : G \to H$ is an injection of commutative formal R-groups. By Lemma 2.2.10, we may dualize after changing the base to $R/\mathfrak{r}$ for an open ideal $\mathfrak{r} \subset R$ to yield $f_{R/\mathfrak{r}}^\vee : H_{R/\mathfrak{r}}^\vee \to G_{R/\mathfrak{r}}^\vee$, which is a surjection of affine $R/\mathfrak{r}$-group schemes by Lemma 2.2.9. Since faithful flatness is stable under base change, we may form the kernel $g^\vee : K_{R/\mathfrak{r}}^\vee \hookrightarrow H_{R/\mathfrak{r}}^\vee$ of $f_{R/\mathfrak{r}}^\vee$ in the category of affine $R/\mathfrak{r}$-groups. Dualizing yields a surjection $H_{R/\mathfrak{r}} \twoheadrightarrow K_{R/\mathfrak{r}}$ of formal $R/\mathfrak{r}$-groups by Lemma 2.2.10. Using the universal property of the kernel for $K_{R/\mathfrak{r}}^\vee$ (which follows by Yoneda's Lemma), we see that the $K_{R/\mathfrak{r}}$ form a directed system of formal R-groups (with varying $\mathfrak{r}$). Taking the direct limit yields a formal group scheme K (topologically flat by [1, Theorem 1.3.12]) and a map $\pi : H \to K$ which is topologically faithfully flat (as this is true over each $R/\mathfrak{r}$). The composite $G \to H \to K$ is zero and $G \to \ker \pi$ is an isomorphism (again working over each $R/\mathfrak{r}$). We will call $\pi : H \to K$ a *cokernel for* f; we will write H/G to denote the cokernel of an injection $G \hookrightarrow H$. □

We note that formation of kernels and cokernels is compatible with base change.

Definition 2.2.11. Given commutative formal R-group schemes G, H, and K, a complex

$$\mathscr{S} : 0 \to K \xrightarrow{f} G \xrightarrow{g} H \to 0$$

is an *exact sequence* if g is a surjection and f is an injection identifying K with $\ker g$.

The fundamental reason for Definition 2.2.8 and Definition 2.2.11 is that when R is a field they make the category of formal R-groups into an abelian category (and similarly for affine R-groups). We omit the proof [1, Theorem 2.1.4].

In general, we can form the cokernel of a morphism $f : H \to G$ if the kernel of f is topologically flat over R: there is an induced injection $\bar{f} : H/\ker f \to G$, and we let the cokernel of f be $\operatorname{coker} \bar{f}$.

Note that by the formal fiberwise criterion for topological (faithful) flatness, a sequence $\mathscr{S}$ is exact if and only if $g \circ f = 0$ and $\mathscr{S}_{R/\mathfrak{m}}$ is exact for all open maximal ideals $\mathfrak{m} \subset R$. We define longer exact sequences in terms of factorization into short exact subsequences.

From the construction of cokernels (and considerations on the closed fiber, where the category is abelian, and Artinian fibers, where we have formal duality), we easily deduce the following basic fact which allows us to work with exact sequences.

Theorem 2.2.12. *Let R be an Artinian local ring and S an arbitrary pseudocompact local ring.*

(1) *A diagram $0 \to K \to G \to H \to 0$ of commutative formal R-groups is short exact if and only if the dual diagram of affine (flat) commutative R-groups is short exact.*

(2) *If $0 \to K \to G \to H \to 0$ is a short exact sequence of commutative formal S-groups and $f : G \to G'$ is a map to a commutative formal S-group which kills K, then f uniquely factors through $G \to H$.*

3 Specializations

The goal of this section is to study the different fibers of a commutative formal group scheme over a pseudocompact local ring $(R, \mathfrak{m}, k)$ with positive characteristic closed point. We first introduce a fundamental tool, the *connected-étale sequence*, and carefully construct it. Then we will look at one particular class of connected formal R-groups, *formal Lie groups*. Finally, we will exhibit certain morphisms which only exist in positive characteristic, the *Frobenius* and *Verschiebung* morphisms. These two morphisms will help us relate formal Lie groups to the formal limits of p-Barsotti-Tate groups in Part II.

3.1 The Connected-Étale Sequence

Over a local pseudocompact base ring $(R, \mathfrak{m}, k)$, any commutative formal group scheme fits into a canonical exact sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0,$$

where G^0 is *connected* and $G^{\text{ét}}$ is *étale*. These parts correspond to the connected component and component group of a Lie group or an algebraic group. As described below in Theorem 3.1.6, the étale quotient $G^{\text{ét}}$ is equivalent to a certain kind of $\text{Gal}(k_s/k)$-module. The connected component G^0 has a more subtle structure, which we will only understand in certain special cases.

3.1.1 The étale dictionary

Given a morphism of formal R-schemes $f : \text{Spf}_R B \to \text{Spf}_R A$, we can construct the *module of formal differentials* $\widehat{\Omega}^1_{B/A}$, which represents the functor taking a profinite B-module M to the profinite B-module of continuous A-linear derivations $B \to M$. Concretely, $\widehat{\Omega}^1_{B/A} = \varprojlim \Omega^1_{(B/\mathfrak{b})/(A/\mathfrak{a})}$, where $(\mathfrak{b}, \mathfrak{a})$ ranges over pairs of open ideals such that $(f^*)^{-1}(\mathfrak{b}) \supset \mathfrak{a}$, and we see that $\widehat{\Omega}^1_{B/A}$ is a profinite B-module. The properties of the module of differentials familiar from elementary commutative algebra carry over to the formal category. In particular, the formation of $\widehat{\Omega}^1_{B/A}$ is compatible with base change on A and base change by an arbitrary continuous map of pseudocompact rings $R \to R'$, as an easy argument using Yoneda's Lemma shows. For psychological reasons, we will write $\Omega^1_{T/S}$ for $\widehat{\Omega}^1_{B/A}$ when $T = \text{Spf}_R B$ and $S = \text{Spf}_R A$.

Lemma 3.1.1. *If $f : T = \mathrm{Spf}_R(B) \to \mathrm{Spf}_R(A) = S$ is a map of formal schemes with a section s, then there is a natural isomorphism of profinite A-modules*

$$s^*\Omega^1_{T/S} \overset{\text{def}}{=} A \mathop{\widehat{\otimes}}_B \Omega^1_{T/S} \cong t^*_s \overset{\text{def}}{=} I/\overline{I^2},$$

compatible with base change in S, where t^*_s is the formal relative cotangent space along the section s and I is the augmentation ideal of the section s.

Proof. The proof follows easily from Yoneda's Lemma once we note that $s^*\widehat{\Omega}^1_{B/A}$ represents A-linear continuous derivations from B to B-modules on which B acts through the augmentation given by s. □

Definition 3.1.2. A map $T \to S$ of formal R-schemes is *formally étale* if it is topologically flat and $\Omega^1_{T/S} = 0$.

By functoriality, it is easy to see that the property of being formally étale is stable under base change on A, pseudocompact base change on R, and that it descends through topologically faithfully flat base change. When R is a field k, the property of being formally étale descends through base change by an arbitrary field extension k'/k.

Lemma 3.1.3. *If k is a field and A a profinite k-algebra, then $\mathrm{Spf}_k A$ is formally étale over $\mathrm{Spf}_k k$ if and only if A is a product of finite separable extensions of k.*

Proof. By descent along field extensions, we may assume k is algebraically closed. Because A is profinite, $A = \prod A_{\mathfrak{m}}$, the product taken over all open maximal ideals of A, so we may assume A is local by functoriality. We are then done by Lemma 3.1.1 and the Formal Nakayama's Lemma. □

Proposition 3.1.4. *If G is a topologically flat formal scheme over R, then G is formally étale over R if and only if the (formal) closed fiber of G is formally étale over k.*

Proof. By functoriality, $\Omega^1_{G_k/k} = \Omega^1_{G/A} \widehat{\otimes}_A k$, and this is the zero module if and only if $\Omega^1_{G/A} = 0$ by the Formal Nakayama's Lemma (because $\Omega^1_{G/A}$ is also a profinite A-module). □

Recall that pseudocompact local rings are Henselian (Lemma 2.1.20). In the theory of schemes, it is natural to think of Henselian local rings as analytic neighborhoods of their closed points. The same intuition carries over into the formal category. Fix a local pseudocompact ring $(R, \mathfrak{m}, k)$ and fix a separable closure k_s of k. In the case of ordinary schemes over a Henselian local base $(R, \mathfrak{m}, k)$, the closed fiber functor establishes an equivalence of categories between finite étale R-schemes and finite étale k-schemes, which are in turn identified with finite sets with a continuous action of the Galois group $\mathrm{Gal}(k_s/k)$. A similar fact is true for formally étale formal R-schemes.

Proposition 3.1.5. *The closed fiber functor establishes an equivalence of categories between formally étale formal R-schemes G and formally étale formal k-schemes G_k.*

Proof. Because the property of being formally étale is stable under base change, if G is formally étale over R then G_k is formally étale over k. Conversely, given some formally étale G_k over k, write $G_k = \mathrm{Spf}_k(\prod_{i \in I} k_i)$, where k_i is a finite separable extension of k. Let $A_i = R[\![x]\!]/(f_i(x))$, where f_i is any (monic) lift of the minimal polynomial for a primitive element α_i for k_i/k. It is easy to see that A_i is finite free (hence profinite topologically flat) and local, and that the residue field of A_i is precisely k_i. Thus, $G = \mathrm{Spf}_R(\prod A_i)$ is a formally étale lift of G_k to R by Proposition 3.1.4.

It remains to check that this lift is unique up to unique isomorphism. If G' is another lift, then by the Formal Nayakama's Lemma and the fact that k_i/k is finite for all $i \in I$, G' must have the form $\mathrm{Spf}_k(\prod_{i \in I} B_i)$ for finite local R-algebras B_i. But then B_i is a finite local algebra over a Henselian local ring, so B_i is itself Henselian. Furthermore, f_i has a root α_i in the residue field k_i of B_i, so by Hensel's Lemma there is a unique R-algebra map $\phi_i : A_i \to B_i$ lifting the residue field identification. Since B_i is topologically flat and the induced map $\phi_i \widehat{\otimes} k$ is an isomorphism, we see that ϕ_i is an isomorphism. □

Let $\widehat{\mathcal{E}}_k$ be the category of formally étale formal k-schemes and $\widehat{\mathcal{S}}_k$ the category of discrete sets admitting a continuous $\mathscr{G}$-action, where $\mathscr{G} = \mathrm{Gal}(k_s/k)$.

Theorem 3.1.6. *There is an equivalence of categories $\widehat{\mathcal{E}}_k \to \widehat{\mathcal{S}}_k$ defined by*

$$G \rightsquigarrow G(k_s) \overset{\mathrm{def}}{=} \varinjlim_{L \subset k_s, [L:k] < \infty} G(L). \tag{3.1.1}$$

Over an algebraically closed field, the category of formally étale formal k-schemes is equivalent to the category of sets.

Proof. For a formally étale formal k-scheme G and k_s endowed with the discrete topology,

$$\mathrm{Hom}_{k\text{-alg., cont}}(\mathscr{O}_G, k_s) = \varinjlim \mathrm{Hom}_{k\text{-alg., cont}}(\mathscr{O}_G, L) \tag{3.1.2}$$

as L ranges over finite Galois subextensions of k_s/k. The transition maps in (3.1.2) are clearly maps of sets functorial in G which respect the functorial $\mathscr{G}$-action induced by the action on k_s (and all of its finite normal subextensions), and any point in the limit is fixed by an open subgroup of $\mathscr{G}$. Thus, $G \rightsquigarrow G(k_s)$ determines a functor $\widehat{\mathcal{E}}_k \to \widehat{\mathcal{S}}_k$.

On the other hand, suppose H is a discrete set with a continuous $\mathscr{G}$-action. Let I be the set of orbits under the $\mathscr{G}$-action. For each $i \in I$, continuity ensures that i is finite and stabilized by an open subgroup $\mathscr{H}_i \subset \mathscr{G}$. Let $k_i \subset k_s$ be the fixed field of $\mathscr{H}_i$ and let $A_H = \prod_{i \in I} k_i$. We see that $\mathrm{Spf}_k A_H$ is a formally étale formal k-scheme such that $(\mathrm{Spf}_k A_H)(k_s) = H$ as $\mathscr{G}$-sets. It is not difficult to see that $\mathrm{Spf}_k A_{G(k_s)} \cong \mathscr{O}(G)$, so we have defined a quasi-inverse functor to $G \rightsquigarrow G(k_s)$. □

By universal properties, we see that the equivalence in Theorem 3.1.6 takes products to products and therefore takes (commutative) group objects to (commutative) group objects.

Theorem 3.1.6 is the "étale dictionary" which may be used to reduce questions about étale group schemes to questions about groups in the category of sets. We will use this dictionary to translate between commutative formal groups over fields of characteristic zero and Galois modules. We remind the reader that a similar dictionary exists between finite étale R-schemes and finite discrete $\mathscr{G}$-sets with a continuous action.

3.1.2 Connected components and the connected-étale sequence

Fix a local pseudocompact ring $(R, \mathfrak{m}, k)$.

Definition 3.1.7. Given a formal R-group G with identity section factoring through $\mathscr{O}(G)_{\mathfrak{m}}$, the *connected component* of G, denoted G^0, is $\mathrm{Spf}_R(\mathscr{O}(G)_{\mathfrak{m}})$.

Proposition 3.1.8. *The connected component G^0 is a closed sub-formal R-group. If $R \to R'$ is a local pseudocompact base change, then $(G^0)_{R'} = (G_{R'})^0$. In particular, $(G^0)_k = (G_k)^0$.*

Proof. The first statement follows by restricting G to small points and using the pseudocompactness of the factor rings in the canonical decomposition of $\mathscr{O}(G)$. The second statement follows because the closed point of G^0 is k-rational. □

We can now construct the connected-étale sequence.

Proposition 3.1.9. *If G is a commutative formal group over R, the quotient $G^{\text{ét}} = G/G^0$ is formally étale over R.*

Proof. By Proposition 3.1.4 and Proposition 3.1.8, we may assume the base R is a field k, and by descent along field extensions we may assume that k is algebraically closed. By an elementary translation argument, because k is algebraically closed we see that every factor ring of $\mathscr{O}(G/G^0)$ is isomorphic. Thus, by functoriality and the Formal Nakayama's Lemma, if we can show that $\varepsilon^*\widehat{\Omega}^1_{\mathscr{O}(G/G^0)/k} = 0$ then we will be done. If I is the augmentation ideal of $\mathscr{O}(G/G^0)$, it suffices (by Lemma 3.1.1) to show that $I/\overline{I^2} = 0$. Writing $\mathscr{O}(G) = A \times \mathscr{O}(G^0)$, we see that $\overline{I\mathscr{O}(G)} = A \times \{0\}$, so $\overline{I\mathscr{O}(G)} = \overline{I^2\mathscr{O}(G)}$, and therefore $(I/\overline{I^2})\,\widehat{\otimes}_{\mathscr{O}(G/G^0)}\,\mathscr{O}(G) = 0$. By the topological faithful flatness of $G \to G/G^0$, we are done. □

Proposition 3.1.10. *The connected-étale sequence is functorial, i.e., a morphism $\phi : G \to H$ uniquely fits into a commutative diagram*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & G^0 & \longrightarrow & G & \longrightarrow & G^{\text{ét}} & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow{\scriptstyle \phi} & & \big\downarrow & & \\
0 & \longrightarrow & H^0 & \longrightarrow & H & \longrightarrow & H^{\text{ét}} & \longrightarrow & 0.
\end{array}
$$

Proof. This immediately follows from the fact that restricting to small points is functorial with respect to morphisms of formal groups, along with the cokernel property for the étale quotient $G^{\text{ét}}$ (by Theorem 2.2.12(2)). □

Proposition 3.1.11. *If $R = K$ is a perfect field, then the connected-étale sequence for G uniquely splits as a sequence of formal groups.*

Proof. Suppose A is a local profinite K-algebra. Because A is profinite and K is perfect, the residue field L of A is a finite separable extension of K. Fixing a choice of primitive element α for L/K and lifting the minimal polynomial f of α to the unique pre-image in $A[x]$ with coefficients in K, we see that there is a unique lift of α to a root of f in A because A is Henselian, and therefore the residue map $A \to L$ has a unique section (in the category of K-algebras). This implies that for each local factor A_i of $\mathscr{O}(G)$, we can find a unique K-subalgebra isomorphic to the residue field L_i of A_i. Furthermore, any formally étale subalgebra B of A_i is clearly a finite (separable) field extension of K (by Lemma 3.1.3), and hence it is easy to see that B must map injectively into the residue field L_i of A_i under the canonical quotient map $A_i \to L_i$. We therefore conclude that $B \subset L_i$ by uniqueness, so L_i is the *maximal formally étale subalgebra* of A_i. By applying this argument to the local factors of arbitrary profinite K-algebras, we see that every profinite K-algebra possesses a maximal formally étale subalgebra (containing all others) and that maps between profinite K-algebras induce maps between the maximal formally étale subalgebras.

Because K is perfect, $L_i \widehat{\otimes}_K L_j$ is identified with a formally étale subalgebra of $A_i \widehat{\otimes}_K A_i$ under the canonical injection $L_i \widehat{\otimes}_K L_j \hookrightarrow A_i \widehat{\otimes}_K A_j$. On the other hand, any open maximal ideal of $A_i \widehat{\otimes}_K A_j$ must contain $\mathfrak{m}_i \subset A_i \hookrightarrow A_i \widehat{\otimes}_K A_j$ and $\mathfrak{m}_j \subset A_j \hookrightarrow A_i \widehat{\otimes}_K A_j$ (under the canonical injections), so we see that the quotient of $A_i \widehat{\otimes}_K A_j$ by its ideal of topological nilpotents is a quotient of $L_i \widehat{\otimes}_K L_j$. We conclude that $L_i \widehat{\otimes}_K L_j$ must be the maximal formally étale subalgebra of $A_i \widehat{\otimes} A_j$. By the obvious generalization of this argument, we see that the formal comultiplication and antipode on $\mathscr{O}(G)$ induce compatible Hopf maps on $\prod L_i$. We conclude that $\prod L_i$ is canonically a formal Hopf subalgebra of $\mathscr{O}(G)$, and it is easy to see that $\mathscr{O}(G)$ is topologically faithfully flat over $\prod L_i$. The induced surjection $G \to \mathrm{Spf}(\prod L_i)$ has kernel G^0, and therefore we have explicitly realized the map $G \to G^{\text{ét}}$. Finally, it is easy to see that the product of the reduction maps $\prod A_i \to \prod L_i$ gives a map of formal Hopf algebras which is a section to $G \to G^{\text{ét}}$. Since $\mathrm{Hom}(G^{\text{ét}}, G^0) = 0$, this is the unique splitting of the connected-étale sequence by a map of formal groups. □

As an application of the splitting of the connected-étale sequence, we prove a proposition relating short exact sequences of commutative formal groups with short exact sequences of commutative finite group schemes. This will help us to study the formal limits of p-Barsotti-Tate groups in Theorem 6.1.3 below.

Proposition 3.1.12. *Let R be a pseudocompact ring. If G', G, and G'' are formal R-groups such that G' and G'' are finite free of constant ranks d' and d'' respectively and there is an exact sequence*

$$0 \to G' \to G \to G'' \to 0$$

of formal R-groups, then G is finite free of rank $d'd''$.

Remark 3.1.13. Note that by Proposition 2.1.12, finite locally free profinite R-modules of constant rank must be globally free. ♦

Proof. Because the ranks of G' and G'' are constant over R, we may reduce to the case where R is local. By a standard topological flatness argument, we may further reduce to the case where $R = k$ is a field, and it is easy to see that we may take k to be algebraically closed. In this case, the connected-étale sequences split. By functoriality, we need only prove the Proposition when the three groups are all connected or all formally étale. In the formally étale case, the proof is trivial by the étale dictionary. Suppose G', G, and G'' are all connected. We easily see by the Formal Nakayama's Lemma that $\mathscr{O}(G'') \to \mathscr{O}(G)$ is finite, so we are done by Proposition 2.1.18 and the usual multiplicativity of orders in short exact sequences of finite locally free group schemes. □

Remark 3.1.14. The usefulness of exact sequences of formal groups necessitates that we work in the general category of pseudocompact rings. Indeed, the étale quotient of a formal group could easily be the constant group $\underline{\mathbf{Q}_p/\mathbf{Z}_p}$ (we will see many examples in Part II; even over $\mathbf{Z}_p$, the profinite algebra of $\underline{\mathbf{Q}_p/\mathbf{Z}_p}$ is highly non-Noetherian.) ♦

3.2 The Special Fiber

Over a field k of positive characteristic a great amount of new information about a formal k-group G is encoded in a diagram

(3.2.1)
$$\begin{array}{ccccc} G & \xrightarrow{F} & G^{(p)} & & \\ & \searrow^{p} & \downarrow{\scriptstyle V} & \searrow^{p} & \\ & & G & \xrightarrow{F} & G^{(p)}, \end{array}$$

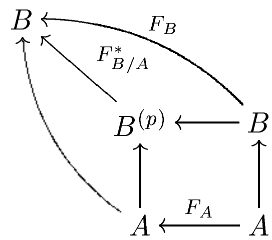
where F is the *Frobenius* morphism and V is the dual *Verschiebung* morphism. We will now define and study these group morphisms.

3.2.1 Frobenius and Verschiebung

Throughout this section, k will be a field of characteristic $p > 0$.

Given an $\mathbf{F}_p$-algebra A, the map $A \to A$ given by $x \mapsto x^p$ is called the *absolute Frobenius morphism* of A and denoted F_A; if A is pseudocompact, we see that F_A is continuous. Given an A-algebra B, let $B^{(p^n)}$ denote the base change by F_A^n. Likewise, if A is pseudocompact and B is a profinite A-algebra, define $B^{(p^n)} = B \widehat{\otimes}_{A, F_A^n} A$. This is a profinite A-algebra, but it is important to note that F_A need not make A a profinite algebra over itself (e.g., consider a field k with $[k : k^p] = \infty$). We will also write $(\mathrm{Spf}_A B)^{(p^n)} \stackrel{\mathrm{def}}{=} \mathrm{Spf}_A(B^{(p^n)})$ and similarly in the affine case. By the universal property of (completed) tensor products, we may make the following definition.

Definition 3.2.1. Let B be a (profinite) A-algebra (with A pseudocompact in the formal case). There is a unique map of (profinite) A-algebras $F^*_{B/A} : B^{(p)} \to B$, the *relative Frobenius of B over A*, such that the diagram



commutes. Concretely, $F^*_{B/A}$ is given on elements of the form $b \mathbin{\widehat{\otimes}} a$ by $F^*_{B/A}(b \mathbin{\widehat{\otimes}} a) = b^p a$.

We see from the universal properties of base change and from uniqueness that the relative Frobenius of B over A is compatible with base change (to another pseudocompact ring over A) and with the formation of products, and therefore when $\operatorname{Spf}_A B$ is a formal A-group or $\operatorname{Spec} B$ is an affine group scheme over $\operatorname{Spec} A$, the relative Frobenius is a group morphism.

Remark 3.2.2. The usual construction of the relative Frobenius for schemes can be given in geometric form, unlike the construction we give in Definition 3.2.1. In the formal case, the possibility that $F_A : A \to A$ might not be a "pro-finite" algebra map forces us to use the ring-theoretic version in the category of pseudocompact rings. Having made the construction, we see that $F^*_{B/A}$ is in fact a continuous map of profinite A-algebras, and therefore we may restate the result: Given a formal A-scheme $\mathfrak{X}$, the relative Frobenius gives a morphism $F_{\mathfrak{X}/\operatorname{Spf}_A A} : \mathfrak{X} \to \mathfrak{X}^{(p)}$ of formal A-schemes, compatible with base change on A. When $\mathfrak{X}$ is a formal A-group, $F_{\mathfrak{X}/\operatorname{Spf}_A A}$ is a group morphism. ♦

If A is a local Artinian ring, employing the duality of Corollary 2.2.7 and the duality built into Definition 3.2.1 allows us to define the *relative Verschiebung*:

Definition 3.2.3. Given a formal or affine (topologically) flat A-scheme Y, the *relative Verschiebung* $V_{Y/A} : Y^{(p)} \to Y$ is the dual to the relative Frobenius.

We will drop the "relative" in what follows, using only the words "Frobenius" and "Verschiebung." When the base is understood, we also omit it from the notation and write simply $F_{\mathfrak{X}}$, or even F, if everything else is clear. We may inductively define the base changes $\mathfrak{X}^{(p^n)}$, the nth relative Frobenius $F^n : \mathfrak{X} \to \mathfrak{X}^{(p^n)}$, and the nth relative Verschibung $V^n : \mathfrak{X}^{(p^n)} \to \mathfrak{X}$.

In the case where the base ring is a field k of characteristic p, we will now prove that (3.2.1) above is a commutative diagram. This will allow us to analyze the multiplication-by-p map $[p]$ using the F and V maps. In particular, both F and V can be written somewhat explicitly, and this will help us greatly in Part II. In fact, it is by finding a concrete expression for V that we will prove the following basic theorem relating F and V. The proof we give here is taken from [1]; it makes essential use of the duality between affine and formal k-groups.

Theorem 3.2.4. *If G is a formal or affine commutative group scheme over a field k of positive characteristic p, then $F \circ V = [p]_{G^{(p)}}$ and $V \circ F = [p]_G$.*

We see from the compatibility properties of the Frobenius that it suffices to prove Theorem 3.2.4 when k is perfect. Therefore, for the rest of this section, we assume k is perfect; this will help us because the absolute Frobenius $\varphi : k \to k$ becomes an *automorphism*. It should be noted, however, that the statement of the theorem does not require a perfect base field.

Let W be a k-vector space. Let $TS^j(W)$ be the fixed points of $W^{\otimes j}$ under the action of the symmetric group S_j on the tensor factors (for $j = 0$, take $TW^0(W) = k$). Call $TS^j(W)$ the *symmetric j-tensors*. Define a linear map $\Sigma_j : W^{\otimes n} \to TS^j(W)$ by

$$w_{i_1} \otimes \cdots \otimes w_{i_j} \mapsto \sum_{\sigma \in S_j} w_{\sigma(i_1)} \otimes \cdots \otimes w_{\sigma(i_j)}.$$

Our constructions are clearly functorial in W and are therefore stable under passage to the direct limit.

Lemma 3.2.5. *Every symmetric p-tensor $v \in TS^p(W)$ can be uniquely written in the form $v = w^{\otimes p} + t$, where $t \in \Sigma_p(W^{\otimes p})$ and $w \in W$.*

Proof. It suffices to prove the Lemma for finite-dimensional W; the general result follows by passage to the direct limit. Looking at orbits for the action of S_j, it is not too hard to see that

$$\Sigma_j((W_1 \oplus W_2)^{\otimes j}) = \bigoplus_{i=0}^{j} \left(\Sigma_i W_1^{\otimes i} \oplus \Sigma_{j-i} W_2^{\otimes (j-i)} \right)$$

inside of $W^{\otimes j}$. There is a compatible isomorphism

$$TS^j(W_1 \oplus W_2) \cong \bigoplus_{i=0}^{j} \left(TS^i(W_1) \oplus TS^{j-i}(W_2) \right).$$

For $0 \leq j \leq p-1$, it is clear that Σ_j is an isomorphism and therefore

$$\frac{TS^p(W_1 \oplus W_2)}{\Sigma_p(W_1 \oplus W_2)^{\otimes p}} \cong \frac{TS^p(W_1)}{\Sigma_p W_1^{\otimes p}} \oplus \frac{TS^p(W_2)}{\Sigma_p W_2^{\otimes p}}.$$

Using induction on $\dim_k W < \infty$, it follows that the k-linear map

$$W^{(p)} \to TS^p(W)/\Sigma_p(W^{\otimes p}) : \lambda \otimes w \mapsto \lambda w^{\otimes p}$$

is an isomorphism. Because k is perfect, the Lemma is proven. □

If W is a profinite k-module, there is a unique continuous action of S_j on $W^{\widehat{\otimes} j}$ determined by

$$w_1 \widehat{\otimes} \cdots \widehat{\otimes} w_j \mapsto w_{\sigma(1)} \widehat{\otimes} \cdots \widehat{\otimes} w_{\sigma(j)}.$$

Define the profinite k-module $TS^j(W)$ to be the fixed points for continuous k-linear action (it is profinite because it is closed). As above, call $TS^j(W)$ the *symmetric j-tensors*. The map Σ_j of Lemma 3.2.5 extends by continuity to give a continuous linear map of profinite k-modules $W^{\widehat{\otimes} j} \to TS^j(W)$. The profinite analogue of Lemma 3.2.5 is the following:

Lemma 3.2.6. *If W is a profinite k-module, any element $v \in TS^j(W)$ has a unique expression as $v = w^{\widehat{\otimes} p} + t$, where $t \in \Sigma_j(W^{\widehat{\otimes} j})$ and $w \in W$. Moreover, w and t are continuous functions of v.*

Proof. It suffices to show that the continuous linear map of profinite k-modules

$$\psi_W : W^{(p)} \to TS^p(W)/\Sigma_p W^{\widehat{\otimes} p}$$

determined by $\lambda \widehat{\otimes} w \mapsto \lambda w^{\widehat{\otimes} p}$ is bijective. Note that ψ is functorial in W. If U ranges over a base of open subspaces of W, it is easy to see that

$$U \widehat{\otimes} W \widehat{\otimes} \cdots \widehat{\otimes} W + W \widehat{\otimes} U \widehat{\otimes} W \widehat{\otimes} \cdots \widehat{\otimes} W + \cdots + W \widehat{\otimes} \cdots \widehat{\otimes} W \widehat{\otimes} U$$

ranges over a cofinal system of open subspaces of $W^{\widehat{\otimes} j}$. By the definition of Σ_p it is not hard to see that the functors $W \rightsquigarrow W^{(p)}$ and $W \rightsquigarrow TS^p(W)/\Sigma_p W^{\widehat{\otimes} p}$ and the natural transformation ψ_W are compatible with inverse limits. (The key to showing this for $W \rightsquigarrow TS^p(W)/\Sigma_p W^{\widehat{\otimes} p}$ is the right-exactness of $\varprojlim$ on profinite k-modules.) Thus, we are reduced to the case where $\dim_k W < \infty$, and we are done by Lemma 3.2.5. □

Proof of Theorem 3.2.4. We will prove the result in the formal case; the affine case follows by duality. Let $A = \mathscr{O}(G)$. Writing $[p] = m_p \Delta_p$, where $m_p : G^p \to G$ is the p-fold multiplication and Δ_p is the p-fold diagonal map, Lemma 3.2.6 shows that the map $m_p^* : A \to A^{\widehat{\otimes} p}$ on k-algebras has the property that for any $a \in A$,

$$m_p^*(a) = V(a)^{\widehat{\otimes} p} + t \tag{3.2.2}$$

for some unique $V(a)$, continuous in a, and some $t \in \Sigma_p(A^{\widehat{\otimes} p})$. (The map m_p^* takes symmetric values because the multiplication is commutative.) It is easy to see that for t in the dense submodule of $\Sigma_p(A^{\widehat{\otimes} p})$ given by finite sums of elementary tensors, $\Delta_p^*(t) = 0$ because $pA = 0$. By continuity and density, we therefore see that

$$[p]^*(a) = V(a)^p.$$

Obviously, V is our candidate for the Verschiebung morphism. By uniqueness, it is clear that $V : A \to A$ is a continuous ring map which is semilinear with respect to the inverse of the absolute Frobenius of k (i.e., $V(\lambda a) = \lambda^{1/p} V(a)$), and therefore (by base change by the absolute Frobenius φ of k) it defines a continuous k-algebra map $V_\varphi : A \to A^{(p)}$. We claim that $V_\varphi = V_G^*$. (In the remainder of this proof, we will let the subscript φ denote base change by the absolute Frobenius of k.) This will conclude the proof that $F_G \circ V_G = [p]$. Since the pth-power map commutes with any ring homomorphism, we can also conclude that $V_G \circ F_G = [p]$.

To verify that $V_\varphi = V_G^*$, we will use linear algebra. Let

$$\langle \cdot, \cdot \rangle : A \otimes A^\vee \to k$$

denote the canonical pairing, and let the base change by the absolute Frobenius be denoted by $\langle \cdot, \cdot \rangle_\varphi$. Recall that the k-algebra structure on the (discrete dual)

$A^\vee$ comes from the formal Hopf structure on A. With this in mind, we see by the definition of the Verschiebung that for all $a \in A$ (topologically identified with $A^{(p)}$ by $a \mapsto 1 \widehat{\otimes} a$ because k is perfect) and all $\psi \in A^\vee$,

$$\langle V_G^*(a), \psi_\varphi\rangle_\varphi = \langle a, F_{G^\vee}^*(\psi_\varphi)\rangle = \langle m_p^*(a), \psi^{\otimes p}\rangle$$

the last pairing taking place between $A^{\widehat{\otimes} p}$ and $(A^\vee)^{\otimes p}$. But any element of $\Sigma_p(A^{\widehat{\otimes} p})$ pairs to zero with $\psi^{\otimes p}$ because $\psi^{\otimes p}$ clearly pairs to zero with a dense submodule of $\Sigma_p(A^{\widehat{\otimes} p})$ (as $\operatorname{char} k = p$). By (3.2.2),

$$\langle m_p(a), \psi^{\otimes p}\rangle = \langle V(a)^{\widehat{\otimes} p}, \psi^{\otimes p}\rangle = \langle V(a), \psi\rangle^p = \langle V_\varphi(a), \psi_\varphi\rangle_\varphi.$$

Because k is perfect, all elements of $(A^\vee)_\varphi$ have the form ψ_φ. Because the pairing $\langle\,\cdot\,,\,\cdot\,\rangle_\varphi$ is perfect, we conclude that $V_\varphi(a) = V_G^*(a)$ for all $a \in A$, so $V_\varphi = V_G^*$. □

As a consequence of Theorem 3.2.4, we can prove a basic fact about connected formal groups in characteristic $p > 0$.

Proposition 3.2.7. *If G is a connected commutative formal group over a field k of characteristic $p > 0$, then the natural injection of formal groups*

$$\xi : \varinjlim G[p^n] \to G$$

is an isomorphism.

Proof. By Yoneda's Lemma and the right-exactness of $\varprojlim$ on the category of short exact sequences of profinite k-modules, ξ is easily seen to exist and be a formal closed immersion. If we can show that every point of G is annihilated by p^n for some n, we will be done. Because any Artinian k-algebra breaks up into finitely many local factors, we easily reduce to the case of a local (Artinian) point of G.

Let R be a finite local Artinian k-algebra. Since the maximal ideal $\mathfrak{m}$ of R is nilpotent, we may choose n such that $\mathfrak{m}^{p^n} = 0$, and therefore the nth relative Frobenius $F_G^n : G \to G^{(p^n)}$ kills $G(R)$ because G is connected. Since $V_G^n \circ F_G^n = [p^n]_G$ by induction, we are done. □

Corollary 3.2.8. *If A is a pseudocompact local ring with residue characteristic $p > 0$ and G is a connected commutative formal group scheme over A such that $[p] : G \to G$ is topologically flat, then the natural map of formal groups*

$$\xi : \varinjlim G[p^n] \to G$$

is an isomorphism.

Remark 3.2.9. By Proposition 2.1.19, $\varinjlim G[p^n]$ is topologically flat over A. ◆

Proof. This follows from Proposition 3.2.7 by a standard argument using the Formal Nakayama's Lemma along with the fact that $\varinjlim G[p^n]$ and G are topologically flat over A. (It is possible to prove this result when G and the map $[p] : G \to G$ are not assumed to be topologically flat, but we will not need it, and the proof is somewhat involved: one proceeds by reducing the problem to the case where A is Artinian and then inducting on the length of A, using Proposition 3.2.7 to handle the case where A is a field.) □

Remark 3.2.10. The proof of Corollary 3.2.8 shows that analyzing the closed fiber of G using F and V can yield non-trivial results, even over a base which is not of characteristic p. In Part II we will use the closed fiber to show that formal groups constructed from certain p-Barsotti-Tate groups are formally smooth, i.e., are "formal Lie groups." ♦

3.2.2 The structure of connected finite group schemes

Since connected groups over a perfect field of characteristic $p > 0$ are easier to understand than connected groups over an arbitrary local ring (or even an arbitrary field), the following theorem is another illustration of the use of passage to the closed fiber. We will not prove it here, as it is a well-known result [13, §11.3].

Theorem 3.2.11. *If k is a perfect field of characteristic $p \geq 0$ and G is a finite (not necessarily commutative) connected finite group scheme over k, then $\mathscr{O}(G)$ has the form $k[x_1, \dots, x_n]/(x_i^{p^{m_i}})$ for some integers $m_i \geq 0$. In particular, if k has characteristic 0 then all finite (not necessarily commutative) group schemes over k are étale and if k is an* arbitrary *field of characteristic $p > 0$, then every finite connected k-group scheme has p-power order.*

3.3 Smoothness and Formal Lie Groups

Let $(A, \mathfrak{m}, k)$ be a pseudocompact local ring. For our purposes, we will say that a connected formal A-scheme X with a k-rational closed point is *formally smooth* (*over A*) if there is an isomorphism $\mathscr{O}(X) \cong A[\![\{X_i\}]\!]$ for some collection of indeterminates. (See [1] for a more functorial definition and a proof of the equivalence with the definition given here.) If $\{X_i\}$ is finite, we call $|\{X_i\}|$ the (*relative*) *dimension of X* and write $\dim X$. When $\{X_i\}$ is infinite, we will write $\dim X = \infty$. It is clear that $\dim X = \dim_k \mathfrak{m}/\mathfrak{m}^2$, so the dimension is intrinsic to X. In our study of formal limits of connected p-Barsotti-Tate groups in Part II, an analysis of the closed fiber of such a limit will reveal it to be formally smooth of finite relative dimension on the gometric closed fiber. We therefore provide a useful mechanism for descending this information over the closed fiber and lifting it to the entire formal group.

Proposition 3.3.1. *Let k'/k be an extension of the residue field of A. If B is a topologically flat local profinite A-algebra with residue field k, then B is formally smooth over A if and only if $B \widehat{\otimes}_A k'$ is formally smooth over k'.*

Proof. The 'only if' direction is trivial. Now suppose that $B \widehat{\otimes}_A k'$ is formally smooth over k'. If we can show that $B \widehat{\otimes}_A k$ is formally smooth over k, then we can lift the isomorphism $k[\![\{X_i\}]\!] \xrightarrow{\sim} B \widehat{\otimes}_A k$ to a continuous map of topologically flat profinite A-algebras $A[\![\{X_i\}]\!] \to B$, and we will be done by a standard Formal Nakayama's Lemma argument. Thus, we may assume $A = k$ and that $B \widehat{\otimes}_k k'$ is formally smooth over k', and we wish to show that this property descends over k. We prove this in the special case where $\dim \mathrm{Spf}_{k'}(B \widehat{\otimes}_k k')$ is finite. The proof in general is in [1]; the finite-dimensional case is all that we need, so we give a simpler proof for that case (which, unfortunately, does not easily generalize).

Let $\mathfrak{n}$ be the (open) maximal ideal of B. By faithful flatness, $\mathfrak{n}/\overline{\mathfrak{n}^2}$ is a finite-dimensional k-vector space. Lifting a basis gives a continuous surjection

$$k[\![X_1, \ldots, X_n]\!] \twoheadrightarrow B$$

for some X_i. To show this is an isomorphism, we may extend scalars to k', which yields a surjection

$$k'[\![X_1, \ldots, X_n]\!] \twoheadrightarrow B \mathop{\widehat{\otimes}}_k k' \cong k'[\![Y_1, \ldots, Y_n]\!].$$

But any surjective self-map of a *Noetherian* ring must be an isomorphism. $\square$

Definition 3.3.2. A *formal Lie group over* A is a connected formally smooth formal group over A.

Example 3.3.3. The formal multiplicative group $\widehat{\mathbf{G}}_m$ is represented by $A[\![X]\!]$, so it is a formal Lie group. Similarly, the formal additive group $\widehat{\mathbf{G}}_a$ is a formal Lie group. If G is a smooth algebraic k-group scheme of dimension n, Example 2.2.2 shows that the formal completion $\widehat{G}$ of G at the identity is a formal Lie group of dimension n (commutative if G is). $\diamondsuit$

Remark 3.3.4. It is trivial to check that for any formal Lie group, the comultiplication map $A[\![\{X_i\}]\!] \rightarrow A[\![\{Y_i, Z_i\}]\!]$ (with $Y_i = 1 \widehat{\otimes}_A X_i$ and $Z_i = X_i \widehat{\otimes}_A 1$) sends X_i to $Y_i + Z_i$ modulo terms of degree two and higher. This simple observation will become important later (cf. Theorem B.2.3). $\blacklozenge$

4 Discriminants

In general, a map $f : G \rightarrow H$ between finite group schemes over a mixed characteristic discrete valuation ring R with fraction field K need not be an isomorphism if f_K is an isomorphism. (For example, consider $R = \mathbf{Z}_p[\zeta_p]$, $G = \underline{\mathbf{Z}/p\mathbf{Z}}$, and $H = \boldsymbol{\mu}_p$ with $f(1) = \zeta_p$.) When f_K is an isomorphism (so f^* is injective by R-flatness), the failure of the lattice injection $f^* : \mathscr{O}(H) \rightarrow \mathscr{O}(G)$ to be an isomorphism is measured by failure of the (non-zero) discriminant ideals $\mathrm{disc}_{\mathscr{O}(H)/R}, \mathrm{disc}_{\mathscr{O}(G)/R} \subset R$ to coincide (they are non-zero because the generic point has characteristic zero, so G_K and H_K are étale over K). In studying the analogous question for p-Barsotti-Tate groups, Tate was able to use invariant differentials on formal Lie groups to *compute* the discriminant ideals of the finite stages of p-Barsotti-Tate groups. This analysis, which we present in Part II, uses several basic properties of discriminants, which we now review. We will conclude this section with the calculation of discriminant ideals for certain isogenies of formal Lie groups; this calculation will be essential in Section 6.2.2.

4.1 A Geometric Construction

Given a finite locally free morphism of schemes $f : T \rightarrow S$ of constant rank d (e.g., a finite locally free S-group), we may define a trace form $\mathrm{Tr}_{T/S} : f_*\mathscr{O}_T \rightarrow \mathscr{O}_S$. Using the $\mathscr{O}_S$-structure on $f_*\mathscr{O}_T$, we get a bilinear pairing $f_*\mathscr{O}_T \otimes_{\mathscr{O}_S} f_*\mathscr{O}_T \rightarrow \mathscr{O}_S$. This induces a natural pairing $\wedge^d f_*\mathscr{O}_T \otimes_{\mathscr{O}_S} \wedge^d f_*\mathscr{O}_T \rightarrow \mathscr{O}_S$ whose image is a locally principal ideal sheaf on S called the *discriminant* and denoted $\mathrm{disc}_{T/S}$.

Example 4.1.1. If f is étale (which in this case just adds the hypothesis that the $\mathscr{O}_T$-module $\Omega^1_{T/S}$ vanishes), then we see by computing in the fibers that $\mathrm{disc}_{T/S} = \mathscr{O}_S$. If S is a Dedekind scheme, what we have constructed is precisely the discriminant of classical number theory. $\Diamond$

The closed subscheme determined by the discriminant is just the locus of points over which the trace form on the fiber is degenerate. A better measure of such degeneracy would be provided by some analogue of the *different* of classical number theory, which would indicate points of T where the structure map is "ramified" rather than just the fibers which contain the ramification points. When the fibers of f are Gorenstein, such a different may in fact be defined (see Section 4.3 for a treatment of the formal case).

In the same way that we defined the trace, we may define the norm $\mathrm{N}_{T/S} : f_*\mathscr{O}_T \to \mathscr{O}_S$. In particular, if $\mathscr{I} \subset f_*\mathscr{O}_S$ is a locally principal ideal sheaf, then we may define the locally principal ideal sheaf $\mathrm{N}_{T/S}(\mathscr{I})$ in $\mathscr{O}_S$. If $X \to T \to S$ is a tower of finite locally free morphisms of constant rank, it follows from Theorem 4.2.1 below that

$$\mathrm{disc}_{X/S} = \mathrm{N}_{T/S}(\mathrm{disc}_{X/T})\,\mathrm{disc}_{T/S}^{\mathrm{rk}_T X}\,. \tag{4.1.1}$$

This extends the transitivity of discriminants from classical number theory to a much more general situation.

To verify (4.1.1), it clearly suffices to work locally over S, so we need only prove (4.1.1) when $S = \operatorname{Spec} A$ is a local scheme. Because $X \to T$ and $T \to S$ are finite, localizing the base reduces us to the affine case, where $S = \operatorname{Spec} A$, $T = \operatorname{Spec} B$, and $X = \operatorname{Spec} C$. In the affine case, (4.1.1) just says that transitivity of discriminants holds for a tower of finite locally free ring extensions. This purely algebraic point of view will make things slightly clearer when we treat discriminants of isogenies between formal Lie groups.

4.2 Transitivity of the Discriminant

Theorem 4.2.1. *If $A \to B \to C$ is a tower of finite locally free free ring extensions of constant ranks $\mathrm{rk}_B C = r$ and $\mathrm{rk}_A B = \ell$, then $\mathrm{disc}_{C/A} = \mathrm{N}_{B/A}(\mathrm{disc}_{C/B})\,\mathrm{disc}^r_{B/A}$ as ideals of A.*

Proof. It suffices to prove this after localizing A, in which case it is an easy exercise in commutative algebra that $A \to B$ and $B \to C$ must be free. Note that the transitivity of the trace shows that the trace form $C \otimes_A C \to A$ is the composite

$$C \underset{A}{\otimes} C \to C \underset{B}{\otimes} C \xrightarrow{\mathrm{Tr}_{C/B}(\cdot,\cdot)} B \xrightarrow{\mathrm{Tr}_{B/A}} A.$$

Therefore, we may consider the problem in a slightly more general form: let $A \to B$ be a finite free ring extension and M a non-zero finite free module over B of rank r equipped with a bilinear pairing $\mathfrak{B} : M \otimes_B M \to B$. A new pairing $\mathfrak{B}' : M \otimes_B M \to A$ results by composing $\mathfrak{B}$ with $\mathrm{Tr}_{B/A}$. We want to prove that

$$\mathrm{disc}(\mathfrak{B}') = \mathrm{N}_{B/A}(\mathrm{disc}(\mathfrak{B}))\,\mathrm{disc}^r_{B/A}\,.$$

Using the adjointness of Hom and $\otimes$, $\mathfrak{B}$ corresponds to a B-linear map

$$M \to \operatorname{Hom}_B(M, B),$$

both sides of which are free of rank r over B. Furthermore, choosing a basis $e_1, \dots, e_r$ for M (and its dual for $\operatorname{Hom}_B(M, B)$), it is easy to see that the induced map on top exterior powers is just multiplication by $\operatorname{disc}(\mathfrak{B})$ up to a unit of B. Rephrasing the problem in these terms, consider the sequence

$$M \to \operatorname{Hom}_B(M, B) \to \operatorname{Hom}_A(M, B) \to \operatorname{Hom}_A(M, A), \tag{4.2.1}$$

where the second map comes from the forgetful functor from B-modules to A-modules and the third map is composition with the trace from B to A. An easy computation shows that

$$\operatorname{rk}_A M = r\ell = \operatorname{rk}_A \operatorname{Hom}_B(M, B) = \operatorname{rk}_A \operatorname{Hom}_A(M, A),$$

while

$$\operatorname{rk}_A \operatorname{Hom}_A(M, B) = r\ell^2.$$

Exterior powers over B and over A commute in the sense that for a free B module N of rank r, there is a natural isomorphism

$$\wedge_A^{r\ell} N \cong \wedge_A^{\ell}(\wedge_B^r N). \tag{4.2.2}$$

For the first map in (4.2.1), the top exterior B-power is multiplication by $\operatorname{disc}(\mathfrak{B})$ (up to a unit of B). Thus, by the isomorphism (4.2.2) and the definition of the norm, the top exterior A-power of this map is just multiplication by $\mathrm{N}_{B/A}(\operatorname{disc}_{M/B})$. Choosing a B-basis for M, the last part of diagram (4.2.1) becomes

$$B^r \to \operatorname{Hom}_A(B, B)^r \to \operatorname{Hom}_A(B, A)^r,$$

which is naturally just the direct sum of r copies of the map $B \to \operatorname{Hom}_A(B, A)$ corresponding to the trace form on B. Hence, using the basic relations between exterior powers and direct sum, the induced map on top exterior powers is just multiplication by a generator of $\operatorname{disc}_{B/A}^r$. The composition of both pieces of (4.2.1) yields the result. □

4.3 The Gorenstein condition and isogenies of formal Lie groups

Let $f : T \to S$ be a finite locally free morphism of schemes.

Definition 4.3.1. We say that T is *Gorenstein over S* or satifies the *relative S-Gorenstein condition* (*is S-Gorenstein*) if $\mathscr{H}om_{\mathscr{O}_S}(f_*\mathscr{O}_T, \mathscr{O}_S)$ is a locally free $f_*\mathscr{O}_T$-module of rank one.

Note that because f is locally free, given any base change $S' \to S$, if T is S-Gorenstein then $T \times_S S'$ is S'-Gorenstein; similarly, we see that T is S-Gorenstein if and only if $T \times_S \operatorname{Spec} \kappa(s)$ is $\operatorname{Spec} \kappa(s)$-Gorenstein for all $s \in S$, i.e., the property holds if and only if it holds in every (geometric) fiber. It is also clear that if T and T' are S-Gorenstein, then $T \times_S T'$ is S-Gorenstein. When S is local, it suffices to check the S-Gorenstein condition on the closed fiber.

Remark 4.3.2. Let us consider the affine case for a moment. Because f is finite, by $\varinjlim$ considerations we may immediately reduce to the case where $\operatorname{Spec} B \to \operatorname{Spec} A$ is a finite locally free morphism of Noetherian affine schemes. We claim that if A is a Gorenstein ring, then $\operatorname{Spec} B$ is $\operatorname{Spec} A$-Gorenstein if and only if B is a Gorenstein ring. To see this, we can further reduce to the case where A is local by the definition of Gorenstein rings. Now, by freeness, any A-regular sequence is a B-regular sequence (considering A as a subring of B by way of the structure map), so we may again reduce to the case where A is Artinian. But then B breaks up as a product of finite free local A-algebras, and therefore we are reduced to the case where $(A, \mathfrak{m}_A, k_A) \hookrightarrow (B, \mathfrak{m}_B, k_B)$ is a finite free map of local Artinian rings. Let E signify injective hull. By the basic theory of duality for Artinian rings, we see that a local Artinian ring $(A, \mathfrak{m}, k)$ is Gorenstein if and only if $A \cong E_A(k_A)$. By the uniqueness of dualizing functors (for finite modules over an Artinian local ring), there is a B-module isomorphism $\operatorname{Hom}_A(B, E_A(k_A)) \cong E_B(k_B)$. But then, since A is Gorenstein, $E_A(k_A) \cong A$, so $E_B(k_B) \cong \operatorname{Hom}_A(B, A)$ as B-modules. This completes the proof. ♦

Remark 4.3.3. Using Remark 4.3.2, we may prove that a finite (not necessarily commutative) group scheme $T \to S$ is S-Gorenstein. Indeed, we reduce to the case where $S = \operatorname{Spec} k$ for some algebraically closed field k. Using translation arguments (because k is algebraically closed), we reduce to a consideration of connected group schemes. By the structure theorem for finite connected group schemes (Theorem 3.2.11), we are done. ♦

Definition 4.3.4. If T is S-Gorenstein then the $f_*\mathscr{O}_T$-annihilator of

$$\mathscr{H}om_{\mathscr{O}_S}(f_*\mathscr{O}_T, \mathscr{O}_S)/(\operatorname{Tr}_{T/S})$$

is a locally principal ideal sheaf $\delta_{T/S} \subset f_*\mathscr{O}_T$ called the *different of T over S*. We view the different as a quasi-coherent ideal sheaf on T.

When S is a Dedekind scheme, its local rings are discrete valuation rings, hence are Gorenstein. Thus, T is S-Gorenstein if and only if the local rings of T are Gorenstein rings by Remark 4.3.2. In particular, if T is also a Dedekind scheme, we see that T is S-Gorenstein and the different $\delta_{T/S}$ corresponds to the different of classical number theory.

Lemma 4.3.5. *If T is S-Gorenstein, then*

$$\mathrm{N}_{T/S}(\delta_{T/S}) = \operatorname{disc}_{T/S}$$

as ideals in $\mathscr{O}_S$.

Proof. We immediately reduce to the case where $S = \operatorname{Spec} A$ for a local ring and $T = \operatorname{Spec} B$ for a finite free extension ring. Let $e_1, \ldots, e_n$ be an ordered basis for B over A. Letting $\pi_j : B \to A$ be the projection to the jth summand of B, we see that $\mathrm{N}_{B/A}(\delta_{B/A}) = \det(\pi_j(\delta_{B/A} e_i))$. On the other hand, if λ is a B-basis for $\operatorname{Hom}_A(B, A)$, so $\operatorname{Tr}_{B/A} = \delta_{B/A}\lambda$ (where $\delta_{B/A}$ generates the different ideal of B), then $\pi_j = \alpha_j \lambda$ implies

$$\begin{aligned} \pi_j(\delta_{B/A} e_i) &= \lambda(\alpha_j \delta_{B/A} e_i) \\ &= \lambda(\delta_{B/A} \alpha_j e_i) \\ &= \mathrm{Tr}_{B/A}(\alpha_j e_i). \end{aligned}$$

It is clear that $\alpha_1, \ldots, \alpha_n$ is another A-basis for B, so there is an invertible matrix M with $Me_j = \alpha_j$. Thus, $(\mathrm{Tr}_{B/A}(\alpha_j e_i)) = M(\mathrm{Tr}_{B/A}(e_j e_i))$. Taking determinants shows that $\mathrm{N}_{B/A}(\delta_{B/A}) = u \det(\mathrm{Tr}_{B/A}(e_i e_j))$ for some $u \in A^\times$. □

We now wish to apply these ideas to formal groups.

4.3.1 Discriminants of isogenies of formal Lie groups

Fix a pseudocompact local base ring R. Let G and H be two (finite-dimensional) formal Lie groups over R.

Definition 4.3.6. An *isogeny* $\phi : G \to H$ is a topologically faithfully flat morphism of formal groups with a finite kernel (which is topologically flat over R by base change, hence finite free because R is local). The order of the kernel is called the *degree* of ϕ.

Example 4.3.7. For Noetherian R, let A be an abelian scheme of relative dimension g over R and $\widehat{A}$ the completed local ring at the closed identity point (viewed as the formal completion of A as a formal R-group). Multiplication by $N \geq 1$ on $\widehat{A}$ is an isogeny of degree equal to the order of $\mathscr{A}[N]^0$. ♢

We will show that the different of an isogeny $f : G \to H$ of commutative formal Lie groups parametrizes the points of G where f is not (formally) étale. In Corollary 4.3.11, we will need some results about the module of formal differentials of a formal R-group. We develop the theory (with proofs) in Appendix A. However, without the theory at hand, it is difficult to even accurately state the results which we will use. The reader is advised to read the relevant statements from Appendix A when reading the proof of Corollary 4.3.11; if time permits, it is ideal to read the entire appendix, as the ideas developed there are essential for understanding the classical motivation behind Tate's proof of the Isogeny Theorem (Theorem 7.2.1).

Lemma 4.3.8. *If $\phi : G \to H$ is an isogeny of formal groups over R, then the induced map $\phi^* : \mathscr{O}(H) \to \mathscr{O}(G)$ is finite free of rank $\deg \phi$ and ϕ is Gorenstein. If G and H are formal Lie groups, then $\dim H = \dim G$.*

Proof. We see by topological flatness considerations that it suffices to prove the Lemma after changing the base to the residue field k of R. The map $(\ell, g) \mapsto (\ell g^{-1}, g)$ on the level of points shows that there is an isomorphism

$$\ker \phi \times_k G \xrightarrow{\sim} G \times_H G \tag{4.3.1}$$

which is compatible with the second projection maps. Since $\ker \phi$ is finite free over k, we conclude that $p_2 : G \times_H G \to G$ (which is just the base change of ϕ by G over

H) is a finite topologically faithfully flat map with constant rank. By Proposition 2.1.29, we see that ϕ^* is finite free.

Similarly, (4.3.1) shows that $\mathrm{Hom}_{\mathscr{O}(H)}(\mathscr{O}(G), \mathscr{O}(H))$ is locally free of rank one over $\mathscr{O}(G)$ if and only if $\mathrm{Hom}_{\mathscr{O}(G)}(\mathscr{O}(\ker\phi) \widehat{\otimes}_k \mathscr{O}(G), \mathscr{O}(G))$ is locally free of rank one over $\mathscr{O}(\ker\phi) \widehat{\otimes}_k \mathscr{O}(G)$, and this holds if and only if $\mathrm{Hom}_R(\mathscr{O}(\ker\phi), R)$ is locally free of rank one over $\mathscr{O}(\ker\phi)$. But we showed in Remark 4.3.3 that this is the case, and therefore ϕ is Gorenstein.

When G and H are formal Lie groups over R, the dimension result follows from finiteness of ϕ^* [7, Theorem 15.1(i)]. □

Tate's calculation of the discriminants of isogenies rests upon considerations of invariant differentials. The following theorem provides the first link in a chain of results culminating in Tate's calculation, which appears as Corollary 4.3.11.

Theorem 4.3.9. *Let $\mathscr{O}$ be a ring, and $\mathscr{O}' = \mathscr{O}[\![T_1, \dots, T_n]\!]/(f_1, \dots, f_n)$ for some regular sequence $f_1, \dots, f_n$ in $\mathscr{O}[\![T_1, \dots, T_n]\!]$. If $\mathscr{O}'$ is finite and free over $\mathscr{O}$, then there is an $\mathscr{O}'$-linear isomorphism*

$$\mathrm{Hom}_{\mathscr{O}}(\mathscr{O}', \mathscr{O}) \simeq \mathscr{O}'$$

such that

$$\mathrm{Tr}_{\mathscr{O}'/\mathscr{O}} \mapsto \det\left(\frac{\partial f_i}{\partial T_j}\right).$$

Thus,

$$\delta_{\mathscr{O}'/\mathscr{O}} = \det\left(\frac{\partial f_i}{\partial T_j}\right)\mathscr{O}'.$$

We will give the most important consequences of Theorem 4.3.9 before we give the proof.

Let G and H be formal Lie groups of dimension n over a pseudocompact local ring R and suppose $\psi : H \to G$ is an isogeny. There is an induced map of invertible $\mathscr{O}(H)$-modules $\psi^*(\Omega^n_{G/R}) \to \Omega^n_{H/R}$. The annihilator of the cokernel is a principal ideal in $\mathscr{O}(H)$, denoted (a).

Corollary 4.3.10. *In this situation,* $\mathrm{disc}_{G/H} = \mathrm{N}_{\mathscr{O}_H/\mathscr{O}_G}(a)$.

Proof. By Lemma 4.3.8, $\mathscr{O}(H)$ is finite and free over $\mathscr{O}(G)$. Writing $\mathscr{O}(G)$ in the form $R[\![Y_1, \dots, Y_n]\!]$ and $\mathscr{O}(H)$ in the form $\mathscr{O}(G)[\![X_1, \dots, X_n]\!]/(f_i(X_1, \dots, X_n) - Y_i)$, where the structure map ψ^* sends Y_i to f_i, it is easy to see that we may choose $a = \det(\partial f_i(Y_1, \dots, Y_n)/\partial Y_j)$. By the "formal division algorithm," it is clear that $\{f_i(X_1, \dots, X_n) - Y_i\}$ is a regular sequence in $R[\![X_1, \dots, X_n, Y_1, \dots, Y_n]\!]$. We are done by Theorem 4.3.9. □

We will use the following corollary to study the "connected component" of a p-divisible group in Part II, Section 6.2.2.

Corollary 4.3.11. *If G is a commutative formal Lie group over R of relative dimension n and $[m] : G \to G$ is an isogeny of degree ν, then* $\mathrm{disc}(G[m]) = m^{\nu n}$.

Proof. It clearly suffices to show that the discriminant of $\mathscr{A} = \mathscr{O}(G)$ over itself under the map $[m]^* : \mathscr{A} \to \mathscr{A}$ is $m^{\nu n}$. By the results of Appendix A, $\Omega^1_{G/\operatorname{Spf} R}$ has a basis $\omega_1, \dots, \omega_n$ consisting of invariant differentials, and since G is commutative Corollary A.2.7 shows that

$$[m]^*\omega_i = m\omega_i.$$

Hence, if $\alpha = \omega_1 \wedge \cdots \wedge \omega_n$, we see that $[m]^*\alpha = m^n\alpha$. Thus, by Corollary 4.3.10 (because the ω_i are a basis for the module of differentials $\widehat{\Omega}^1_{\mathscr{A}/R}$),

$$\operatorname{disc}_{\mathscr{A}/[m]^*\mathscr{A}} = \mathrm{N}_{\mathscr{A}/[m]^*\mathscr{A}}(m^n) = m^{\nu n}.$$

□

To prove Theorem 4.3.9, it is conceptually clearer to invoke a more general result, due to Tate (see the appendix to [8]).

Proposition 4.3.12 (Tate). *Suppose R is a ring, A an R-algebra, $f_1, \dots, f_N$ a regular A-sequence, $\alpha : A \to A/(f_i) = C$ the canonical projection. Suppose further that C is finite free over A and that the kernel of*

$$\beta : B = A \underset{R}{\otimes} C \xrightarrow{\alpha \otimes 1_C} C$$

is generated by a regular B-sequence $g_1, \dots, g_N$. Writing $1 \otimes f_i = \sum b_{ij} g_j$, $d = \det(b_{ij})$, and $\lambda' = \mathrm{id}_A \otimes_R \lambda$,

1. *C is R-Gorenstein;*
2. *there is a C-module generator $\lambda \in \operatorname{Hom}_R(C, R)$ such that $\alpha(\lambda'(d)) = 1$;*
3. *for any $c \in C$, $\alpha(c\lambda'(d)) = c$;*
4. *$\delta_{C/R} = \beta(d)$.*

With the exception of a few typographical errors, the proof presented in [8] is quite clear. The reader is therefore referred to [8, Appendix] for the proof.

Proof of Theorem 4.3.9. We wish to apply Proposition 4.3.12 with $R = \mathscr{O}$, $A = \mathscr{O}[[T_1, \dots, T_n]]$, and $C = \mathscr{O}'$. It is easy to see by finiteness that

$$A \underset{R}{\otimes} C = \mathscr{O}'[[T_1, \dots, T_n]].$$

The map $\beta = \alpha \otimes \mathrm{id}_C : B \to C$ takes X_i to T_i, and it is easy to see (using the "formal division algorithm") that $\ker \beta$ is generated by $X_i - T_i$, which is clearly a B-regular sequence. Therefore, the hypotheses of Proposition 4.3.12 are satisfied. Write $f_i = \sum b_{ij}(T_j - \bar{T}_j)$, and let $d = \det(b_{ij})$. Differentiating,

$$\frac{\partial f_i}{\partial T_j} = b_{ij} + \sum_{\ell=1}^{n} \frac{\partial b_\ell}{\partial T_\ell}(T_\ell - \bar{T}_\ell),$$

so $\partial f_i/\partial T_j = \beta(\partial f_i/\partial T_j) = \beta(b_{ij})$, which means that $\beta(d) = \det(\partial f_i/\partial T_j)$. □

Part II
Tate's Theorems

5 Definitions

Fix a prime p.

5.1 p-Barsotti-Tate groups

Given an abelian scheme $\mathscr{A} \to S$, the system $(\mathscr{A}[p^n], i_n)$ with natural maps $i_n : \mathscr{A}[p^n] \to \mathscr{A}[p^{n+1}]$ is the motivating example of a p-Barsotti-Tate group. While we will primarily study these objects in the abstract for purposes of conceptual clarity and technical flexiblity, we will occasionally turn to the theory of abelian schemes as a source of motivating examples. In everything that follows, $(R, \mathfrak{m}, k)$ is a local pseudocompact ring with char $k = p > 0$. When extra hypotheses are necessary, we will impose them.

We recall the definition we made in the General Introduction.

Definition 5.1.1. A *p-Barsotti-Tate group of height h* over a scheme S is an inductive system $(G_n, i_n)_{n\geq 0}$ of finite locally free commutative S-group schemes and closed immersions $i_n : G_n \to G_{n+1}$ such that

1) $|G_n| = p^{nh}$;

2) i_n identifies G_n with $G_{n+1}[p^n]$.

It is clear that the category of p-Barsotti-Tate groups is closed under the formation of finite products (in the obvious manner) and there is an evident notion of base change. In particular, given a p-Barsotti-Tate group over a discrete valuation ring, we can speak of the *generic fiber* and the *closed fiber*.

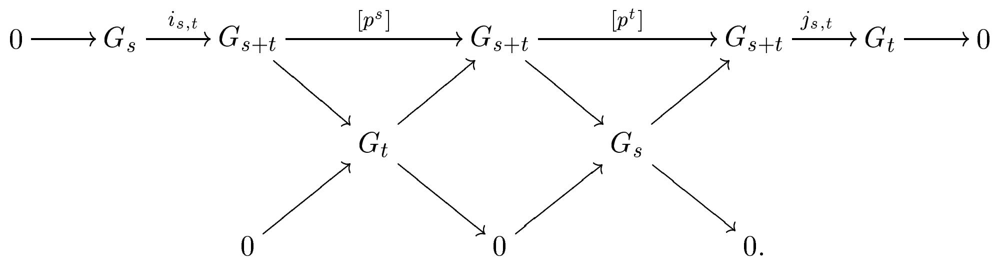
Remark 5.1.2. We could alternately require of our system of groups G_n that for all s and t, there exist exact sequences

$$0 \to G_s \xrightarrow{i_{s,t}} G_{s+t} \xrightarrow{[p^s]} G_{s+t} \xrightarrow{[p^t]} G_{s+t} \xrightarrow{j_{s,t}} G_t \to 0. \tag{5.1.1}$$

Let us show that this is equivalent to Definition 5.1.1. Given sequences (5.1.1), taking the system $(G_n, i_{n,1})$ yields the first definition. On the other hand, setting $i_{s,t} = i_{s+t} \circ \cdots \circ i_{s+1} \circ i_s$ clearly identifies G_s with $G_{s+t}[p^s]$. Furthermore, by definition, $[p^n]G_n = 0$, i.e., $[p^n]|_{G_n}$ factors through the identity section. Therefore, $[p^s]|_{G_{s+t}}$ factors through $G_t \hookrightarrow G_{s+t}$. The induced sequence

$$0 \to G_s \to G_{s+t} \to G_t \to 0$$

is then exact by (*a priori* left-exactness and) an order calculation, so we have an exact diagram



♦

Definition 5.1.3. Given a p-Barsotti-Tate group $G = (G_n)$ over a Henselian local ring, the *connected component* G^0 of G is the system formed by the G_n^0 and functoriality of the connected-étale sequence.

We see that G^0 is itself a p-Barsotti-Tate group (of height at most $\operatorname{ht} G$): it is clear that the i_n induce closed immersions $G_n^0 \to G_{n+1}^0$. To calculate the order $|G_n^0|$, we may pass to the geometric closed fiber, and we are done by the splitting of the connected-étale sequence and an easy inductive argument using Remark 5.1.2. Note that G^0 has height zero (i.e., is trivial) unless the local base has residue characteristic p.

Example 5.1.4. Suppose G is a commutative algebraic group scheme over a base S and the map $[p] : G \to G$ is finite locally free of rank p^h (e.g., G could be an abelian scheme over S or $\mathbf{G}_{m/S}$). The map $[p^n] : G \to G$ is then finite locally free of rank p^{nh}, and we see by changing the base of $[p]$ to $G[p^{n-1}]$ that there are exact sequences

$$0 \to G[p] \to G[p^n] \to G[p^{n-1}] \to 0.$$

By induction, we see that $|G[p^n]| = p^{nh}$ and that the canonical closed immersion $i_n : G[p^n] \to G[p^{n+1}]$ identifies $G[p^n]$ with $G[p^{n+1}][p^n]$. Thus, the system $(G[p^n], i_n)$ is a p-Barsotti-Tate group, the *p-Barsotti-Tate group associated to* G, which we will denote by $G(p)$. This is the fundamental example of a p-Barsotti-Tate group which arises geometrically.

In the case where the base $S = \operatorname{Spec} R$ with R a complete Noetherian local ring and G is flat over R, then the completed local ring $\widehat{\mathscr{O}}_{\mathfrak{m},G}$ of the closed point on the identity section is topologically flat over R and the connected component $G(p)^0$ has a very concrete interpretation. Recall from Example 2.2.2 that restricting G to "small points" (Artinian points supported on the identity section) yields a formal R-group $\widehat{G}$.

It is easy to see that $\widehat{G}[p^n] = \widehat{G[p^n]} = G[p^n]^0$ (the last identified with its image in the category of formal group-functors *via* Proposition 2.1.26(4)). If G is smooth over R then $[p^n] : \widehat{G} \to \widehat{G}$ is an isogeny of formal Lie groups over R. By Corollary 3.2.8, the natural monomorphism $\varinjlim \widehat{G}[p^n] \to \widehat{G}$ is an isomorphism, and therefore the connected p-Barsotti-Tate group $G(p)^0$ is identified with the p-power torsion levels of a formal Lie group $\widehat{G}$ for which $[p]$ is an isogeny. A crucial fact to be proven later is that all connected p-Barsotti-Tate groups over R are "the same" as formal Lie groups on which $[p]$ is an isogeny (see Theorem 6.1.3 and Theorem 6.2.1 below.) ◊

Example 5.1.5. Choosing $G = \mathbf{G}_m$ in Example 5.1.4 shows that over R we may view the *multiplicative p-torsion* p-Barsotti-Tate group $(\boldsymbol{\mu}_{p^n}, i_n)$ with the canonical closed immersions $\boldsymbol{\mu}_{p^n} \to \boldsymbol{\mu}_{p^{n+1}}$ as the p-power torsion levels of $\widehat{\mathbf{G}}_m$. (We may observe this concretely:

$$\varprojlim \mathscr{O}(\boldsymbol{\mu}_{p^n}) = \varprojlim R[\![X]\!]/((1+X)^{p^n} - 1) \cong R[\![X]\!] \cong \mathscr{O}(\widehat{\mathbf{G}}_m)$$

because R has residue characteristic p.) In general, over any base scheme, $\mathbf{G}_m(p)$ is a p-Barsotti-Tate group of height one. ◊

Definition 5.1.6. A p-Barsotti-Tate group is *formally étale* if G_n is étale for every n.

Example 5.1.7 (Formally étale p-Barsotti-Tate groups). Given a connected scheme S, formally étale p-Barsotti-Tate groups G over S have a simple underlying structure: if $\operatorname{ht} G = h$, then we see that G_n is identified with the abelian group $(\mathbf{Z}/p^n\mathbf{Z})^h = (\frac{1}{p^n}\mathbf{Z}_p/\mathbf{Z}_p)^h$, equipped with a continuous action of the étale fundamental group of S (using a generalization of the étale dictionary). In particular, when $S = \operatorname{Spec} R$, a formally étale p-Barsotti-Tate group is identified with a continuous $\operatorname{Gal}(k_s/k)$-action on the discrete group $(\mathbf{Q}_p/\mathbf{Z}_p)^h$. ◊

Example 5.1.8 (Dual p-Barsotti-Tate groups). Dualizing Remark 5.1.2, we see that $(G_n^\vee, j_{1,n}^\vee)$ is another p-Barsotti-Tate group, the *dual p-Barsotti-Tate group*. Clearly, $\operatorname{ht} G^\vee = \operatorname{ht} G$ and there is a unique natural isomorphism $\alpha_G : G \to G^{\vee\vee}$ compatible with Cartier duality on torsion levels. Formation of the dual p-Barsotti-Tate group is clearly compatible with base change. Given an abelian scheme $\mathscr{A}$, we have already described the associated p-Barsotti-Tate group, $\mathscr{A}(p)$. If $\mathscr{A}^\vee$ denotes the dual abelian scheme, the Cartier-Nishi duality theorem yields natural isomorphisms $\mathscr{A}[p^n]^\vee \cong \mathscr{A}^\vee[p^n]$ compatible with change in n (where the first $(\cdot)^\vee$ stands for the Cartier dual), so we see that $\mathscr{A}(p)^\vee \cong \mathscr{A}^\vee(p)$. ◊

As Examples 5.1.4 and 5.1.7 make clear, when working with p-Barsotti-Tate groups over R, it is quite natural to consider them as functors and to examine their images in the category of formal group-functors over R with a view toward assemblimg the direct limits in the formal category. We will construct such limits and characterize them in Sections 6.1 and 6.2. We will see that Definition 5.1.3 and Definition 5.1.6 will accord with the formal group terminology of part I. However, we see from Example 5.1.8 that the p-Barsotti-Tate viewpoint is also indispensable, for there is no natural construction of the dual in the formal category. Similarly, the formation of the generic fiber of a p-Barsotti-Tate group (i.e., making non-local base change) is much easier to understand on the level of p-Barsotti-Tate groups.

5.2 The Tate module

Let K be a field of characteristic zero (e.g., the field of fractions of a p-adic integer ring).

Given a p-Barsotti-Tate group $G = (G_n, i_n)$ over K, we can construct the abstract version of the p-adic Tate module of an abelian scheme. Let $\overline{K}/K$ be a fixed separable closure.

Definition 5.2.1. The *Tate module* of G is $\varprojlim G_n(\overline{K})$, taken with respect to the $j_{1,n-1} : G_n \twoheadrightarrow G_{n-1}$ of Remark 5.1.2

By functoriality, we view $T(G)$ as a $\mathbf{Z}_p[\mathrm{Gal}(\overline{K}/K)]$-module. It is easy to see that the underlying module is a free $\mathbf{Z}_p$-module of rank $\mathrm{ht}\, G$ on which $\mathrm{Gal}(\overline{K}/K)$ acts continuously.

Example 5.2.2. We define $\mathbf{Z}_p(1) = T(\mathbf{G}_m(p))$. It is easy to see that this is just the representation of $\mathrm{Gal}(\overline{K}/K)$ on $\mathbf{Z}_p$ defined by the p-adic cyclotomic character $\varepsilon_p : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\boldsymbol{\mu}_{p^\infty}(\overline{K})) = \mathbf{Z}_p^\times$. ◊

Using the functoriality of Cartier duality and the étale dictionary, we see that $T(G^\vee) = T(G)^\vee \stackrel{\text{def}}{=} \mathrm{Hom}_{\mathbf{Z}_p}(T(G), \mathbf{Z}_p(1))$ with the natural $\mathrm{Gal}(\overline{K}/K)$-action.

Let G be a p-Barsotti-Tate group over K. Given $T(G)$, we may recover $G_n(\overline{K})$ by forming $T(G)/p^n T(G)$ (because $j_{1,n-1}$ is induced by multiplication by p). On the other hand, since $\mathrm{char}\, K = 0$, we recall that the étale dictionary is nothing more than the "$\overline{K}$-valued points functor." Thus, we have shown the following.

Proposition 5.2.3. *The functor $G \rightsquigarrow T(G)$ gives an equivalence of categories between p-Barsotti-Tate groups over K and finite free $\mathbf{Z}_p$-modules with continuous* $\mathrm{Gal}(\overline{K}/K)$*-action.*

A variant of the Tate module which will appear in the proof of the Hodge-Tate decomposition is the module $\Phi(G) = \varinjlim G_n(\overline{K})$ with transition maps given by the transition maps of G. As above, we find that $G_n(\overline{K}) = \Phi(G)[p^n]$, and consequently, we arrive at a similar proposition expressing the fact that $G \rightsquigarrow \Phi(G)$ is fully faithful on p-Barsotti-Tate groups over K. This implies that there is a similar relationship between $\Phi(G)$ and $T(G)$. In fact, we may make this explicit.

Proposition 5.2.4. *As functors on the category of p-Barsotti-Tate groups over K, there are natural* $\mathrm{Gal}(\overline{K}/K)$*-isomorphisms*

$$T(G) \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\sim} \Phi(G) \qquad\qquad T(G) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \Phi(G)).$$

Proof. The isomorphism $T(G) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\sim} \Phi(G)$ follows from the fact that $\varinjlim$ and $\otimes$ commute, combined with the fact that $T(G)/p^n T(G) = G_n(\overline{K})$.

The isomorphism $T(G) \to \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \Phi(G))$ comes about as follows: there is a natural isomorphism

$$\mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \varinjlim G_n(\overline{K})) \xrightarrow{\sim} \varprojlim \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Z}_p/p^n\mathbf{Z}_p, \varinjlim G_n(\overline{K})).$$

But the system (G_n, i_n) has injective transition maps and each $G_n(\overline{K})$ is a finite p-group, so it is easy to see that there are natural isomorphisms

$$G_n(\overline{K}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Z}_p, G_n(\overline{K})) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Z}_p/p^n\mathbf{Z}_p, \varinjlim G_n(\overline{K})),$$

and therefore the projection maps $T(G) \to T(G)/p^n T(G)$ yield a natural isomorphism $T(G) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \Phi(G))$. It is easy to check that all of the isomorphisms are $\mathrm{Gal}(\overline{K}/K)$-equivariant. □

Thus, for a p-Barsotti-Tate group G over K, the Tate module $T(G)$ and the module $\Phi(G)$ carry information equivalent to G, and one may easily move among G, $T(G)$ and $\Phi(G)$. This easily understood mutual relationship will play an important role in Proposition 7.1.2, where we exploit all three objects simultaneously.

5.3 Statement of the results

Let R be a complete mixed characteristic $(0,p)$ discrete valuation ring with fraction field K. For a p-Barsotti-Tate group G over R, we let G_K denote the generic fiber of G, and we define $T(G) \stackrel{\text{def}}{=} T(G_K)$. We write $G^\vee$ for the dual p-Barsotti-Tate group to G.

Our goal is to prove the theorems alluded to in the General Introduction in the context of p-Barsotti-Tate groups. In particular, we will show two fundamental results:

Hodge-Tate Decomposition (Theorem 7.1.3). *There are finite dimensional K-vector spaces $t_{G^\vee}$ attached to $G^\vee$ and t_G^* attached to G such that there is a canonical* $\mathrm{Gal}(\overline{K}/K)$*-equivariant decomposition*

$$\mathrm{Hom}_{\mathbf{Z}_p}(T(G), \mathbf{C}_K) = (t_{G^\vee} \underset{K}{\otimes} \mathbf{C}_K) \oplus (t_G^* \underset{K}{\otimes} \mathbf{C}_K(-1))$$

Isogeny Theorem (Theorem 7.2.1). *The generic fiber functor $G \rightsquigarrow G_K$ is fully faithful.*

It is difficult and conceptually unsatisfying to try to prove these theorems without leaving the context of p-Barsotti-Tate groups. Therefore, we will first see how to assemble p-Barsotti-Tate groups into formal limits called p-divisible groups. We will see that the connected components of p-divisible groups are actually formal Lie groups (the Smoothness Theorem). Given this information, we will do two things:

1) We will see how to define "points" of a p-divisible group in such a way that the points in the connected component form an analytic group. Given such an analytic group, we will define a logarithm function which, in conjunction with a crucial input from Cartier duality, will connect the Tate module of a p-Barsotti-Tate group to the global geometry of the limit p-divisible group. This will furnish a proof of the Hodge-Tate decomposition.

2) We will use our results about formal Lie groups (e.g., Corollary 4.3.11) to compute the discriminant ideals of the finite stages of p-Barsotti-Tate groups; these calculations, along with data produced by the Hodge-Tate decomposition, will form the basis for a proof of the Isogeny Theorem.

With this plan in mind, we begin our discussion of

6 The connection to formal groups

Restricting our attention to Artinian points, we may view the finite stages G_n of any p-Barsotti-Tate group G over our complete discrete valuation ring R as formal group-functors (pro-represented by the R-algebras $\mathscr{O}(G_n)$ with their unique profinite R-algebra topologies). This allows us to form the limit $\varinjlim G_n$, which we will also denote by G (a minor abuse of notation; see Theorem 6.1.3). In this section we will show that the category of p-Barsotti-Tate groups is equivalent, under this limit operation, to a category of formal groups which we will call *p-divisible groups*. The primary advantage of this point of view is embodied in the Smoothness Theorem, which shows that the connected component of a p-divisible group is actually a formal Lie group. Given this crucial piece of information, we can define a second invariant of a p-divisible group, the *dimension*. The remarkable fact, proved in the Pairing Proposition (Proposition 7.1.2), is that the Tate module $T(G) = T(G_K)$, depending only upon the *generic* fiber, is sensitive to this dimension, which depends upon the global structure of G over R.

6.1 p-divisible groups

In this section, we drop the hypothesis that R be a complete discrete valuation ring, requiring only that R be a pseudocompact ring. Given a p-Barsotti-Tate group (G_n, i_n) over R, write $G = \varinjlim G_n$ in the category of formal R-groups. In the case of ordinary groups, inductive limits G of "p-Barsotti-Tate groups of height h" are easily classified by the three properties: 1) $p : G \to G$ is a surjection; 2) $G = \varinjlim G[p^n]$; 3) $G[p]$ has order p^h. By standard arguments, these three properties also characterize the formally étale limits of formally étale p-Barsotti-Tate groups. The following two definitions extend properties 1), 2), and 3) to the category of formal R-groups.

Definition 6.1.1. A commutative formal R-group G is a *formal p-group* if the morphism $[p] : G \to G$ is topologically faithfully flat and the natural formal closed immersion $\varinjlim G[p^n] \to G$ is an isomorphism.

Note that if R is a local pseudocompact ring with residue characteristic p, Corollary 3.2.8 shows that every commutative formal R-group G such that $[p] : G \to G$ is topologically faithfully flat is a formal p-group.

Definition 6.1.2. A commutative formal R-group G is a *p-divisible group of height h* if G is a formal p-group and $G[p]$ is a finite group of order p^h.

Having written down the definitions in general, the formally étale situation also generalizes as follows. Given a pseudocompact ring R, let $\mathcal{B}_p$ denote the category of p-Barsotti-Tate groups over R and let $\widehat{\mathcal{B}}_p$ denote the category of p-divisible groups over R.

Theorem 6.1.3. *There is a height-preserving equivalence of categories between $\mathcal{B}_p$ and $\widehat{\mathcal{B}}_p$ sending a p-Barsotti-Tate group (G_n, i_n) to $\varinjlim G_n$ and a p-divisible group G to $(G[p^n], i_n)$, where i_n is the obvious closed immersion.*

Proof. Given a p-divisible group, taking the fiber product of $[p] : G \to G$ with $G[p^{n-1}] \hookrightarrow G$ gives an exact sequence

$$0 \to G[p] \to G[p^n] \to G[p^{n-1}] \to 0 \tag{6.1.1}$$

for each n. By Proposition 3.1.12 and induction on n, we see from (6.1.1) that $G[p^n]$ is a finite R-group for all n. Since $|G[p]| = p^h$, we see that $|G[p^n]| = p^{nh}$. Taking the fiber of $G[p^n] \hookrightarrow G$ over $G[p^{n+1}] \hookrightarrow G$ shows that $i_n : G[p^n] \to G[p^{n+1}]$ is a closed immersion. Thus, $(G[p^n], i_n)$ is a p-Barsotti-Tate group over R. Because G is formal p-group, we see that $\varinjlim G[p^n] = G$.

On the other hand, suppose (G_n, i_n) is a p-Barsotti-Tate group over R. Letting $G = \varinjlim G_n$, we see by Yoneda's Lemma that $G_n = G[p^n]$. Because each G_n is topologically flat over R, G is also topologically flat over R. Finally, we claim that $[p] : G \to G$ is an isogeny of degree p^h. Since $G[p]$ is a finite R-group of order p^h, it remains to prove that $[p]$ is topologically faithfully flat. However, Remark 5.1.2 shows that the map $j_{1,n-1} : G_n \to G_{n-1}$ induced by $[p]$ is topologically faithfully flat. By Proposition 2.1.19, we see that $[p] : G \to G$ is topologically faithfully flat. Thus, G is a p-divisible group, and $(G[p^n], i_n) = (G_n)$. It is clear that both $G \rightsquigarrow (G[p^n], i_n)$ and $(G_n) \rightsquigarrow \varinjlim G_n$ are functorial, and we have just verified that they are quasi-inverses. $\square$

Now that we have characterized, in some degree of generality, exactly which formal groups arise as limits of p-Barsotti-Tate groups (by which we will always mean "limits of torsion levels of p-Barsotti-Tate groups"), we reinstate the hypothesis that R is a *local* pseudocompact ring with residue characteristic p. Because R is Henselian, we may consider the *connected component* of a p-divisible group, and it is clear by functoriality and the comments following Definition 5.1.3 that the connected-étale sequence of a p-divisible group is a sequence of p-divisible groups. The usual arguments show that a formally étale p-divisible group may be viewed as a discrete Galois module for the absolute Galois group of the residue field of R. It turns out that connected p-divisible are also well-behaved.

Example 6.1.4. Recall from Example 5.1.4 that for a flat commutative algebraic group scheme G over a complete Noetherian local ring R for which $[p] : G \to G$ is finite locally free of rank p^h, the connected component $G(p)^0$ (viewed as a formal group *via* Theorem 6.1.3) is represented by $\widehat{\mathscr{O}}_{\mathfrak{m},G}$. When $\mathfrak{m}$ is a smooth point of G, we see that $G(p)^0$ is formally smooth.

In particular, when $G = \mathbf{G}_m$, we see by making the change of variable $x = t+1$ in the algebra $R[x, x^{-1}]$ of $\mathbf{G}_{m/R}$ that $\mathbf{G}_m(p)^0 = \widehat{\mathbf{G}}_m$ is represented by $R[\![t]\!]$ (with the usual formal Hopf structure as given in Example 2.2.4), hence is formally smooth. Similarly, when G is an abelian scheme over R, we see by smoothness that $G(p)^0$ is represented by the completed local ring at $\mathfrak{m}$, which has (relative) dimension equal to $\dim G$. In both of these cases, none of the finite stages $G[p^n]^0$ is smooth, in contrast to the formal smoothness of the limit. $\Diamond$

Example 6.1.4 demonstrates that the connected component of a p-divisible group over R has a rich structure which is not apparent at finite stages. In general, as we will prove in Theorem 6.2.1 below, the connected component of any p-divisible group is *always* formally smooth. This crucial result (due to Serre and Tate) will let us use ideas from Lie theory (e.g., invariant differentials) in the study of connected p-divisible groups.

6.2 The smoothness theorem

We retain the notation that $(R, \mathfrak{m}, k)$ is an arbitrary local pseudocompact ring with $\operatorname{char} k = p$. Recall that "formal Lie group over R" and "formally smooth formal group over R of finite relative dimension" are synonomous.

Theorem 6.2.1 (Smoothness Theorem). *If G is a connected p-divisible group over R, then G is a formal Lie group over R.*

By Proposition 3.3.1, if G is a formal group over a pseudocompact ring R with residue field k and k' is a field extension of k, then G is a formal Lie group over R if and only if $G_{k'}$ is a formal Lie group over k'. Therefore, it suffices to prove the Smoothness Theorem on the geometric closed fiber, so we may assume that the base R is a field k of characteristic $p > 0$. (If $\operatorname{char} k \neq p$, then the only connected p-divisible group over k is the trivial group, as we easily see from the p-Barsotti-Tate vantage point.) In what follows, k will be a field of characteristic $p > 0$. Using the fact that $\operatorname{char} k = p > 0$, we will reduce the proof of the Smoothness Theorem over k to the following:

Proposition 6.2.2. *If G is a connected formal group over k, then G is a formal Lie group if and only if the relative Frobenius $F : G \to G^{(p)}$ is an isogeny.*

Lemma 6.2.3. *Proposition 6.2.2 implies Theorem 6.2.1.*

Proof. Having reduced our base to k, we recall that the commutative formal groups over k form an abelian category where epimorphisms (called "surjections") are topologically faithfully flat maps.

If G is a connected p-divisible group, then so is the base change $G^{(p)}$. Since any p-divisible group is a formal p-group, the map $[p] : G^{(p)} \to G^{(p)}$ is a surjection, but by Theorem 3.2.4 this factors as

$$G^{(p)} \xrightarrow{V} G \xrightarrow{F} G^{(p)},$$

so F must be a surjection. Furthermore, by definition, $G[p]$ is finite of order p^h and $\ker F \subset G[p]$, so F is an isogeny. □

Therefore, it remains to prove Proposition 6.2.2. In what follows, G is a connected formal group over k. Given a morphism $f : G \to H$, we will let $G[f]$ denote $\ker f$.

Lemma 6.2.4. *If the relative Frobenius $F : G \to G^{(p)}$ is an isogeny, then $\deg F = p^h$ for some $h \geq 0$, $|G[F^n]| = p^{nh}$ for all n, and the natural monomorphism $\varinjlim G[F^n] \to G$ is an isomorphism.*

Proof. The final ismomorphism is easily extractable from the proof of Proposition 3.2.7. That $\deg F = p^h$ for some integer $h \geq 0$ follows from the structure theorem for finite connected group schemes (Theorem 3.2.11) and the fact that any closed subgroup of G must be connected. To compute the order of $G[F^n]$ we will show that there is an exact sequence

$$E_n : 0 \to G[F] \to G[F^n] \to G^{(p)}[F^{n-1}] \to 0$$

for each n. By base change, $G^{(p)}[F^{n-1}] = G[F^{n-1}]^{(p)}$, so by induction we may assume that $G^{(p)}[F^{n-1}]$ is a finite k-group of order $p^{(n-1)h}$. By Proposition 3.1.12, we see that $G[F^n]$ is also a finite k-group, and we are done by the multiplicativity of orders in an exact sequence.

To see that there is such a sequence E_n, recall that topological faithful flatness is stable under base change. Therefore, we see that $F^n : G \to G^{(p^n)}$ is also an isogeny. Considering the triangle

$$\begin{array}{ccc} G & \xrightarrow{\;F\;} & G^{(p)} \\ & {\scriptstyle F^n}\searrow \quad \swarrow{\scriptstyle F^{n-1}} & \\ & G^{(p^n)} & \end{array}$$

completes the proof. ☐

Proof of Proposition 6.2.2. Let $(A, \mathfrak{m})$ be the (local) profinite (augmented) k-algebra of G, and let $(B_n, \mathfrak{m}_n)$ be the finite k-algebra of $G[F^n]$. Compatibility of the group laws shows that the splittings induced by the augmentations $A = k \oplus \mathfrak{m}$ and $B_n = k \oplus \mathfrak{m}_n$ are compatible (for all n) and that $\mathfrak{m} = \varprojlim \mathfrak{m}_n$. Furthermore, the maps $A \to B_n$ corresponding to the natural injection $G[F^n] \hookrightarrow G$ are all surjective (as this is true of kernel morphisms in general). By finiteness we may choose $x_1, \ldots, x_\ell \in \mathfrak{m}$ such that their images in $\mathfrak{m}_1/\mathfrak{m}_1^2$ are a k-basis. Composing the transition maps gives a map $B_n \twoheadrightarrow B_1$ which identifies $G[F]$ with $G[F^n][F]$ (e.g., by Yoneda's Lemma), and therefore we have a natural induced isomorphism $B_n/F(\mathfrak{m}_n) \xrightarrow{\sim} B_1$. Since $F(\mathfrak{m}_n)$ is generated by $\{x^p : x \in \mathfrak{m}_n\}$ and $p \geq 2$, there is an isomorphism of cotangent spaces $\mathfrak{m}_n/\mathfrak{m}_n^2 \xrightarrow{\sim} \mathfrak{m}_1/\mathfrak{m}_1^2$. We thus see that the images of $x_1, \ldots, x_\ell$ are a k-basis for each $\mathfrak{m}_n/\mathfrak{m}_n^2$.

The result of all of this is that the maps $u_n : k[X_1, \ldots, X_\ell] \to B_n$ sending $X_i \mapsto x_i$ are a compatible system of surjections. Because $B_n = \mathscr{O}(G[F^n])$, we see that $(X_1^{p^n}, \ldots, X_\ell^{p^n}) \subset \ker u_n$. On the other hand, $\dim_k(B_n) = p^{\ell n}$ by Lemma 6.2.4, so $(X_1^{p^n}, \ldots, X_\ell^{p^n}) = \ker u_n$ and the u_n induce a compatible system of isomorphisms $k[X_1, \ldots, X_\ell]/(X_1^{p^n}, \ldots, X_\ell^{p^n}) \to B_n$. Passing to the inverse limit, we get an isomorphism $k[\![X_1, \ldots, X_n]\!] \xrightarrow{\sim} A$ of profinite k-algebras.

The converse follows by an explicit calculation (using the concrete description of the morphism F). ☐

Corollary 6.2.5. *If the residue field k of R is perfect and G is a p-divisible group over R, then the connected-étale sequence $0 \to G^0 \to G \to G^{\text{ét}} \to 0$ splits as a sequence of formal R-functors. In other words, there is an isomorphism of profinite R-algebras $\mathscr{O}(G) = \mathscr{O}(G^0) \widehat{\otimes}_R \mathscr{O}(G^{\text{ét}})$ compatible with the connected-étale sequence.*

Proof. Because k is perfect, the closed fiber of the connected-étale sequence uniquely splits, and this says that there is an isomorphism of profinite $\mathscr{O}(G^{\text{ét}})_k$-algebras

$$\mathscr{O}(G_k) \cong \mathscr{O}(G^{\text{ét}})_k[\![X_1, \ldots, X_\ell]\!] = \mathscr{O}(G^{\text{ét}})_k \mathop{\widehat{\otimes}}_k \mathscr{O}(G^0)_k. \tag{6.2.1}$$

On the other hand, both $\mathscr{O}(G^{\text{ét}})[\![X_1, \ldots, X_\ell]\!]$ and $\mathscr{O}(G)$ are topologically faithfully flat over $\mathscr{O}(G^{\text{ét}})$, which is itself topologically flat over R. We may lift the closed fiber isomorphism (6.2.1) to a map

$$\mathscr{O}(G^{\text{ét}}) \mathop{\widehat{\otimes}}_R \mathscr{O}(G^0) = \mathscr{O}(G^{\text{ét}})[\![X_1, \ldots, X_\ell]\!] \to \mathscr{O}(G)$$

of topologically flat profinite R-algebras, and this is an isomorphism by a Formal Nakayama's Lemma argument. ☐

Corollary 6.2.5 will play a critical role in our study of the analytic groups attached to p-divisible groups in Section 6.3.

Remark 6.2.6. The use of $\mathscr{O}(G^{\text{ét}})$ and topological flatness considerations over this ring in the proof of Corollary 6.2.5 demonstrates once again the importance of the concept of topological flatness over non-Noetherian pseudocompact rings, even for an analysis of formal groups over a complete Noetherian local ring. ♦

Definition 6.2.7. Given a p-divisible group G over R, we define the *dimension of* G, denoted $\dim G$, to be the (finite) relative dimension of the formal Lie group G^0.

Equivalently, writing $\mathscr{O}(G^0) = R[\![X_1, \ldots, X_\ell]\!]$, we see that $\dim G$ is the rank of the finite free R-module I/I^2, where I is the augmentation ideal of $\mathscr{O}(G^0)$. Similarly (see Appendix A), the dimension of G is rank of the finite free $\mathscr{O}(G^0)$-module $\Omega^1_{G^0/R}$.

6.2.1 The behavior of the dimension under dualization

When our local ring R is Noetherian, Example 6.1.4 shows that an abelian scheme $\mathfrak{G}$ over R of relative dimension g has associated p-divisible group $\mathfrak{G}(p)$ of height $2g$ and dimension g. If $\mathfrak{G}^\vee$ denotes the dual abelian scheme to $\mathfrak{G}$, then $\mathfrak{G}^\vee$ has dimension g and Cartier-Nishi duality (see Example 5.1.8) identifies $\mathfrak{G}^\vee(p)$ with the dual p-divisible group $\mathfrak{G}(p)^\vee$, so this dual p-divisible group has dimension g as well. Thus,

$$\dim \mathfrak{G}(p) + \dim \mathfrak{G}(p)^\vee = \operatorname{ht} \mathfrak{G}(p).$$

Similarly, the multiplicative group $\mathbf{G}_m$ has associated p-divisible group $\mathbf{G}_m(p)$ of height one and dimension one. On the other hand, since $\boldsymbol{\mu}_{p^n}^\vee = \underline{\mathbf{Z}/n\mathbf{Z}}$, we see that $\mathbf{G}_m(p)^\vee$ is formally étale, so $\dim \mathbf{G}_m(p)^\vee = 0$ by definition. Therefore,

$$\dim \mathbf{G}_m(p) + \dim \mathbf{G}_m(p)^\vee = \operatorname{ht} \mathbf{G}_m(p).$$

In general, we have the following proposition.

Proposition 6.2.8. *Suppose G is a p-divisible group over R. If $n = \dim G$, $n^\vee = \dim G^\vee$, and $h = \operatorname{ht} G$, then*

$$n + n^\vee = h.$$

Proof. Because the height and dimension are invariant under local base change, we may work over the closed point and assume that $R = k$. By a faithfully flat base extension, we may take k to be perfect. Because $[p]$ is an isogeny and we are in an abelian category, every map in diagram (3.2.1) is a surjection. Therefore, there is an exact sequence

$$0 \to G[F] \to G[p] \xrightarrow{F} G^{(p)}[V] \to 0. \tag{6.2.2}$$

Clearly, $|G[F]| = |G[p][F]| = p^n$ by Proposition 6.2.2 and the splitting of the connected-étale sequence, with F an isomorphism on the étale factor. By Theorem 3.2.4, we see that there is an exact sequence

$$0 \to G^{(p)}[V] \to G^{(p)}[p] \xrightarrow{V} G[p].$$

By duality, we see that

$$0 \to G[p]^\vee[F] \to G[p]^\vee \xrightarrow{F} G^{(p)}[p]^\vee \to G^{(p)}[p][V]^\vee \to 0$$

is exact. The middle two terms have the same order, so using the definition of the dual p-Barsotti-Tate group, the compatibility properties base change, and the multiplicativity of orders, $|G^{(p)}[V]| = |G^\vee[F]| = p^{n^\vee}$. By (6.2.2), $p^h = p^{n+n^\vee}$. □

Proposition 6.2.8 will help us to relate G and $G^\vee$ in the proof of the Hodge-Tate decomposition.

6.2.2 Using smoothness to compute discriminants of p-Barsotti-Tate groups

Our strategy for proving the Isogeny Theorem will be to reduce the problem to showing that a morphism $f : G \to H$ of p-divisible R-groups which is an isomorphism on generic fibers is in fact an isomorphism. As we discussed in the beginning of Section 4, given that $f : G \to H$ induces an isomorphism on generic fibers, we can prove that f is an isomorphism of p-divisible groups over the entire base R by showing that $\operatorname{disc} G[p^t] = \operatorname{disc} H[p^t]$ for all t. We will show in Proposition 6.2.12 that $\operatorname{disc} G[p^t]$ depends only upon t, $\dim G$, and $\operatorname{ht} G$. The key point is to show that $T(G)$ "knows" $\dim G$. With this in mind, we proceed.

Given a p-Barsotti-Tate group over R, the calculation of $\operatorname{disc} G_n$ reduces to a computation of $\operatorname{disc} G_n^0$ (see Corollary 6.2.11), and the Smoothness Theorem (Theorem 6.2.1) relates $\operatorname{disc} G_n^0$ to the discriminant of the isogeny $[p^n] : G^0 \to G^0$, which we can understand using our results about formal Lie groups.

Lemma 6.2.9. *If $0 \to G_1 \to G_2 \to G_3 \to 0$ is a short-exact sequence of finite locally free group schemes over a base S, then*

$$\operatorname{disc}(G_2) = \operatorname{disc}(G_1)^{|G_3|} \operatorname{disc}(G_3)^{|G_1|}.$$

Proof. We immediately reduce to the case where the base is a local ring A. Let $B = \mathscr{O}(G_3)$ and $C = \mathscr{O}(G_2)$. By the definition of a short exact sequence, there is a tower $A \hookrightarrow B \hookrightarrow C$ of finite locally free ring extensions of constant ranks, and $\operatorname{rk}_B C = |G_1|$ (it is an exercise in commutative algebra to see that such a tower must in fact be free). By the transitivity of discriminants (Theorem 4.2.1),

$$\operatorname{disc}_{C/A} = \mathrm{N}_{B/A}(\operatorname{disc}_{C/B}) \operatorname{disc}_{B/A}^{\operatorname{rk}_C B}.$$

Thus, it remains to show that $\mathrm{N}_{B/A}(\operatorname{disc}_{C/B}) = \operatorname{disc}_{\overline{C}/A}^{\operatorname{rk}_A B}$, where $\overline{C} = C/I_B C$, for I_B the augmentation ideal of B. By Yoneda's Lemma, there is an isomorphism compatible with second projections

$$G_1 \times_S G_2 \cong G_2 \times_{G_3} G_2$$

given on points by $(x, y) \mapsto (xy, y)$. Translating this into algebra and using compatibility of the norm with base extension, this says exactly that $(\operatorname{disc}_{\overline{C}/A})C = \operatorname{disc}_{C/B}$. Therefore, by the definition of the norm, $\mathrm{N}_{B/A}(\operatorname{disc}_{C/B}) = \operatorname{disc}_{\overline{C}/A}^{\operatorname{rk}_A B}$. □

Lemma 6.2.10. *If $X \to S$ is finite locally free, then X is étale over S if and only* $\operatorname{disc}(X)$ *is the unit ideal.*

Proof. It is easy to see that $\operatorname{disc}(X)$ is the unit ideal if and only if $\operatorname{disc}(X_k)$ is a unit in every geometric fiber $X \times_S \operatorname{Spec} k$. Because $X \to S$ is finite locally free, we easily reduce to the case where $X = \operatorname{Spec} A$ for some finite local k-algebra $(A, \mathfrak{m})$, and we are reduced to proving that $\operatorname{disc}_k A = 0$ if $A \neq k$ (the converse is clear). Multiplication by any $a \in \mathfrak{m}$ is a nilpotent k-endomorphism of A, hence $\operatorname{Tr}_{A/k}(a) = 0$. Thus, taking a k-basis $e_1, \ldots, e_n$ for A with $e_1 = 1$ and $e_i \in \mathfrak{m}$ for $i > 1$, we see that the matrix $\operatorname{Tr}_{A/k}(e_i e_j)$ has determinant zero if $n > 1$. □

Corollary 6.2.11. *For a finite group scheme G over R, $\operatorname{disc} G = (\operatorname{disc} G^0)^{|G^{\text{ét}}|}$.*

Proposition 6.2.12. *Given a p-divisible group of height h and dimension n over R, $\operatorname{disc}(G[p^\nu]) = p^{n\nu p^{\nu h}}$.*

Proof. By Corollary 6.2.11, it suffices to show that $\operatorname{disc}(G[p^\nu]^0) = p^{n\nu|G^0[p^\nu]|}$. But we know that $[p] : G^0 \to G^0$ is an isogeny of formal Lie groups by the Smoothness Theorem, and therefore we are done by Corollary 4.3.11. □

6.3 An analytic interpretation

In this section, we suppose that R is a complete mixed characteristic $(0, p)$ discrete valuation ring with fraction field K and that $G = \operatorname{Spf}_R A$ is a formal group over R.

6.3.1 Points and the logarithm: generalities

Definition 6.3.1. Given a topological R-algebra S, the group of *points of G in S*, denoted $G(S)$, is defined to be the group $\operatorname{Hom}_{\text{cont}}(A, S)$ of continuous R-algebra maps $A \to S$.

If S is the ring of integers in the completion L of an algebraic extension of K and G is a formal Lie group over R with relative dimension n, we see upon choosing formal coordinates for G that $G(S)$ is identified with the open unit ball in L^n (under the d_∞ metric, where $d_\infty(y_1, \ldots, y_n) = \max\{|y_i|\}$), and the formal analyticity (*with R-coefficients*) of the group law for G gives an analytic group structure to $G(S)$. In other words, taking points of a formal Lie group results in a "rigid Lie group." Using *p-adic Lie theory*, one can construct a canonical local analytic isomorphism $\log : G(S) \to t_G(L)$, with $t_G(L)$ as in Definition 6.3.3 below, and there is a p-adic "Cambell-Baker-Hausdorff formula" which explains why the logarithm map $G(S) \to t_G(L)$ is a group homomorphism. While this may be more satisfying from an analytic perspective, we will not take the p-adic Lie theory approach here. Instead, we will use a formal "generic fiber" isomorphism which exists in the commutative case (which is all that we need here) to construct the canonical logarithm:

Lemma 6.3.2. *If Γ is a commutative formal Lie group of dimension n over a field K of characteristic zero, then there is an isomorphism of formal K-groups $\Gamma \cong \prod_{i=1}^n \mathbf{G}_a$.*

Proof. The methods involved in this proof are rather orthogonal to our purposes, so we refer the reader to Appendix B. □

Definition 6.3.3. For a formal Lie group G over R with augmentation ideal I, the *tangent space* t_G *to* G *at the identity* is defined to be the functor on topological R-modules represented by $I/\overline{I^2}$. By Proposition A.2.1, this is equivalent to the functor represented by the R-module $\Omega^{1,\ell}_{G/R}$ of left-invariant differential forms on G, and $t_G(R)$ is a finite free R-module. The *points of* t_G in a topological R-algebra L, denoted by $t_G(L)$, is the set $\mathrm{Hom}_{R\text{-mod}}(I/\overline{I^2}, L)$.

Given L, the natural map $L \otimes_R t_G(R) \to t_G(L)$ of (finite free) L-modules is an isomorphism, where $t_G(L)$ is canonically topologized by the product topology.

Proposition 6.3.4. *If G is a commutative formal Lie group of dimension n over R and L is the completion of an algebraic extension of K with integer ring $S \subset L$, then there is a natural homomorphism of topological groups*

$$\log : G(S) \to t_G(L),$$

functorial in the pair $S \subset L$ as well as in G. Upon choosing an isomorphism $\mathscr{O}(G) = R[\![X_1, \ldots, X_n]\!]$ and letting

$$B \stackrel{\text{def}}{=} \{(x_1, \ldots, x_n) \in G(S) : |x_i| < |p|^{-1/(p-1)}\}$$
$$B' \stackrel{\text{def}}{=} \{\tau \in t_G(L) : |\tau(\omega)| < |p|^{-1/(p-1)} \text{for all } \omega \in \Omega^{1,\ell}_{G/R}\},$$

the logarithm yields a topological (analytic) isomorphism $B \cong B'$.

To prove Proposition 6.3.4, we will first prove a formal analogue of Poincaré's Lemma. Given antiderivatives for the invariant 1-forms on G, we will construct the logarithm and show that it satisfies functorial properties. Finally, we will establish that it is a local isomorphism.

Lemma 6.3.5. *Given any invariant differential form $\omega \in \Omega^1_{G/R}$, there exists a unique formal power series $\Omega_\omega \in K[\![X_1, \ldots, X_n]\!]$ such that $\Omega_\omega(0) = 0$ and $d\Omega_\omega = \omega$.*

Proof. We may "formally change the base" to K by way of the canonical continuous injection $R \hookrightarrow K$. By Lemma 6.3.2, we then see that there is an isomorphism $\Omega^{1,\ell}_{G_K/K} \cong \Omega^{1,\ell}_{\prod \mathbf{G}_a/K}$. By the functorial properties of left-invariant differentials (or by Proposition A.2.1), we see that $\Omega^{1,\ell}_{\prod \mathbf{G}_a/K} \stackrel{\sim}{\to} \prod \Omega^{1,\ell}_{\mathbf{G}_a/K}$ under the natural map $\Omega^1_{\prod \mathbf{G}_a/K} \stackrel{\sim}{\to} \prod p_i^* \Omega^1_{\prod \mathbf{G}_a/K}$, and now it is easy to see that we are done. □

Remark 6.3.6. Because $\partial\Omega_\omega/\partial X_i \in R[\![X_1, \ldots, X_n]\!]$ for all i, we see that each Ω_ω has the property

(†) if a is a coefficient of a term of total degree m, then $ma \in R$.

Therefore, the usual estimates show that Ω_ω converges to an analytic (hence continuous) function on $G(S)$. By Proposition A.2.5 and Remark A.2.6, we see that $m^*\Omega_\omega = p_1^*\Omega_\omega + p_2^*\Omega_\omega$, and therefore for $x_1, x_2 \in G(S)$, $\Omega_\omega(x_1 + x_2) = \Omega_\omega(x_1) + \Omega_\omega(x_2)$. ♦

Definition 6.3.7. The *logarithm* is the topological group homomorphism

$$\log = \log_G : G(S) \to t_G(L) = \mathrm{Hom}_R(\Omega^{1,\ell}_{G/R}, L)$$

defined by

$$x \mapsto (\omega \mapsto \Omega_\omega(x)).$$

This is easily seen to be independent of the isomorphism $\mathscr{O}(G) \cong R[\![X_1, \dots, X_n]\!]$.

Remark 6.3.8. We will prove in Lemma 6.3.12 below that for a p-divisible group G over R, $G(S)$ has a unique topological $\mathbf{Z}_p$-module structure such that the analytic group $G^0(S)$ is an open subgroup. Having established that log is continuous in Remark 6.3.6, we conclude by continuity that if G is a p-divisible group, log is actually $\mathbf{Z}_p$-linear. ♦

Because group morphisms pull back left-invariant differentials to left-invariant differentials and $\Omega_{\phi^*\omega} = \phi^*\Omega_\omega$, the functoriality of $\log_G$ in G is clear. Functoriality in $S \subset L$ follows from the fact that Ω_ω has coefficients in K. To complete the proof of Proposition 6.3.4, it remains to show that log establishes a local analytic isomorphism.

Proof of the local isomorphism. We will proceed by constructing a *formal* inverse function and then checking that both sides converge on appropriate balls.

Write $\mathscr{O}(G) = R[\![X_1, \dots, X_n]\!]$. We know that there exist left-invariant differentials $\omega_1, \dots, \omega_n$ freely generating $\Omega^1_{G/R} = \bigoplus R[\![X_1, \dots, X_n]\!]dX_i$. Therefore, there exist $a_{ij} \in R[\![X_1, \dots, X_n]\!]$ such that $\omega_i = \sum a_{ij} dX_j$ and $\det(a_{ij}) \in R[\![X_1, \dots, X_n]\!]^\times$. Reducing modulo $(X_1, \dots, X_n)$, we see that we may assume after a homogeneous linear change of coordinates that $a_{ij} \equiv \delta_{ij} \pmod{X_1, \dots, X_n}$. Thus, we may write

$$\Omega_i \stackrel{\text{def}}{=} \Omega_{\omega_i} = X_i + \text{higher order terms}.$$

We also know that Ω_i has the property (†) of Remark 6.3.6. By an inductive calculation, given that $\Omega_i \equiv X_i \pmod{X_1, \dots, X_n}$, we see that there is a formal inverse $\Omega^{-1} = (\Omega_{-1}, \dots, \Omega_{-n})$ to $\Omega = (\Omega_1, \dots, \Omega_n)$ which has the weaker property

(‡) if a is a coefficient of a term of total degree m, then $m!a \in R$.

Clearly, property (†) implies (‡). But it is clear that any n-tuple of formal power series $\Omega = (\Omega_1, \dots, \Omega_n)$ with property (‡) converges to an analytic function in the ball of radius $|p|^{-1/(p-1)}$ in the d_∞ metric on L^n. Using $\omega_1, \dots, \omega_n$ to identify $t_G(L)$ with L^n, we see that Ω^{-1} gives an analytic inverse to Ω on the open ball of radius $|p|^{-1/(p-1)}$ around the origin in $t_G(L)$ (which must be a group homomorphism). (Because we cannot be sure that Ω^{-1} satisfies any stronger property than (‡), we cannot *a priori* extend the analytic isomorphism to a larger ball of $t_G(L)$.) □

Example 6.3.9. We saw in Example 6.1.4 that $G = \mathbf{G}_m(p) = \widehat{\mathbf{G}}_m$ is a connected p-divisible of height one and dimension one. Given S and choosing a basis for $\mathscr{O}(\mathbf{G}_m(p))$, it is not too hard to see that there is a topological isomorphism $G(S) \to U_S : x \mapsto 1 + x$, where U_S is the (topological) group of principal units of S. Classically, we have the ordinary p-adic logarithm $\log_p : U_S \to L$. Writing

$\mathscr{O}(\mathbf{G}_m(p)) = R[\![T]\!]$, we see that $dT/(T+1)$ is an invariant differential on $\mathbf{G}_m(p)$ with antiderivative $\log_p(1+T)$ (as a formal power series), and therefore we see that $\log_G : G(S) \to t_G(L)$ is identified with $\log_p : U_S \to L$ by choosing the basis $T \pmod{T^2}$ for $t_G(L)$. This identification will play a crucial role in the sequel. $\Diamond$

6.3.2 Points and the logarithm: p-divisible groups

While we cannot easily generalize Proposition 6.3.4 to an arbitrary commutative formal group, the étale quotient of a p-divisible group is nice enough to allow us to extend our construction. We will show in Lemma 6.3.12 that $G^{\text{ét}}(S)$ is actually a p-power torsion group. Assume for the moment that this is true. By Corollary 6.2.5, we see that for any S as above, there is an exact sequence

$$0 \to G^0(S) \to G(S) \to G^{\text{ét}}(S) \to 0, \tag{6.3.1}$$

functorial in G and S. Given this information, we see that we may extend the logarithm uniquely as follows:

Definition 6.3.10. Given $x \in G(S)$, choose m such that $p^m x \in G^0(S)$. Define

$$\log(x) = \tfrac{1}{p^m}\log(p^m x).$$

It is clear that this definition is independent of m and that we have given the unique extension of $\log_{G_0}$ to a continuous $\mathbf{Z}_p$-linear function

$$\log = \log_G : G(S) \to t_{G^0}(L).$$

(In particular, we see that $\log_G$ kills the torsion subgroup $G(S)_{\text{tors}}$ of $G(S)$.) This construction is clearly functorial in $S \subset L$ and G. In what follows, $t_G \stackrel{\text{def}}{=} t_{G^0}$.

Proposition 6.3.11. *The logarithm induces an isomorphism of* $\mathbf{Q}_p$*-vector spaces*

$$G(S) \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p \to t_G(L).$$

The kernel $\ker\log$ *is precisely* $G(S)_{\text{tors}}$*, the torsion subgroup. If the valuation on* S *is discrete, then* $\log G(S)$ *is contained in a finitely generated* S*-submodule of* $t_G(L)$*. If* L *is algebraically closed, then* $\log G(S) = t_G(L)$*.*

Proof. We will first prove that $\ker\log = G(S)_{\text{tors}}$. As we noted above (using Lemma 6.3.12 below and (6.3.1)), for any $x \in G(S)$ there is some n such that $p^n x \in G^0(S)$. Since $G(S)_{\text{tors}} \subset \ker\log$, we clearly need only prove that there exists m such that $p^{n+m}x \in B$, the open ball where log is an isomorphism. We claim that for $y \in G^0(S)$, the sequence $p^m y$ tends to 0. Recall that

$$[p]^*(X_i) = pX_i + \text{ higher order terms.}$$

For all $y = (y_1, \ldots, y_n) \in G^0(S)$, we have $|y_i| < 1$ for all i. It follows from this information (and the fact that $|p| < 1$) that $p^m y \to 0$ in $G^0(S)$ as $m \to \infty$, so there is some m such that $p^{n+m}x \in B$. Therefore, $\ker\log = G(S)_{\text{tors}}$ because all torsion is p-power torsion by Lemma 6.3.12 below.

In fact, when the valuation on S is discrete, there is a maximal value for $|y_i| < 1$ among all coordinates of all points of $G^0(S)$, and therefore there is some N such that $p^N x \in B$ for all $x \in G^0(S)$. On the other hand, we see that $\log G(S) = \log G^0(S)$, so we conclude that $\log G(S) \subset p^{-N}B'$, and B' is a finitely generated S-submodule of $t_G(L)$ (because S is Noetherian). Thus, when the valuation on S is discrete, $\log G(S)$ is contained in a finitely generated S-submodule of $t_G(L)$.

When L is algebraically closed, the fact that $\log G(S) = t_G(L)$ clearly follows from the fact that $G(S)$ is p-divisible, which we will establish in Lemma 6.3.13 below.

Finally, since it is clear by the local isomorphism of Proposition 6.3.4 that coker log is p-power torsion, tensoring the exact sequence

$$0 \to \ker \log \to G(S) \xrightarrow{\log} t_G(L) \to \operatorname{coker} \log \to 0$$

with $\mathbf{Q}_p$ over $\mathbf{Z}_p$ and using the fact that $t_G(L)$ is already a $\mathbf{Q}_p$-module yields the exact sequence

$$0 \to G(S) \underset{\mathbf{Z}_p}{\otimes} \mathbf{Q}_p \to t_G(L) \to 0.$$

□

It remains to verify that $G^{\text{ét}}(S)$ is p-power torsion and that $G(S)$ is divisible when L is algebraically closed.

Lemma 6.3.12. *The topological group $G(S)$ admits a unique topological $\mathbf{Z}_p$-module structure and $G(S)_{\text{tors}} = \varinjlim G_n(S)$ functorially in G and S. If G is formally étale, then $G(S)$ is p-power torsion. The analytic group $G^0(S)$ is an open subgroup of G.*

Proof. Because the discrete topological R-algebra $S/\mathfrak{m}^i S$ has a maximal ideal consisting of nilpotents, it is a direct limit of discrete finite Artinian R-algebras T_j. By definition, we have

$$G(T_j) = \varinjlim G_n(T_j) \tag{6.3.2}$$

for all j. Using (6.3.2), it is easy to see that

$$G(S/\mathfrak{m}^i S) = \varinjlim G_n(S/\mathfrak{m}^i S). \tag{6.3.3}$$

We have thus shown that $G(S/\mathfrak{m}^i S)$ consists of p-power torsion elements, with

$$G_n(S/\mathfrak{m}^i S) = G(S/\mathfrak{m}^i S)[p^n].$$

By continuity, it is clear that

$$G(S) = \varprojlim G(S/\mathfrak{m}^i S), \tag{6.3.4}$$

as topological groups (with each $G(S/\mathfrak{m}^i S)$ discrete), so the topological group $G(S)$ has a unique compatible topological $\mathbf{Z}_p$-module structure and

$$G(S)[p^n] = \varprojlim G(S/\mathfrak{m}^i S)[p^n] = \varprojlim G_n(S/\mathfrak{m}^i S) = G_n(S).$$

Thus, we find that $G(S)_{\text{tors}} = G(S)[p^\infty] = \varinjlim G_n(S)$.

Suppose G is formally étale. From our proof of Proposition 3.1.5, we see that the affine algebra of G_n is a product of integer rings in unramified extensions of K, and it is clear that the map $\eta_i : G_n(S/\mathfrak{m}^{i+1}S) \to G_n(S/\mathfrak{m}^i S)$ is a bijection for all i. Therefore, $G(S/\mathfrak{m}^i S) = G(S/\mathfrak{m}S)$ for all i, and passing to the inverse limit on i shows that $G(S) = G(S/\mathfrak{m}S)$ is a discrete p-power torsion group.

It remains to show that $G^0(S)$ is open. By functoriality there is a commutative diagram of continuous maps of topological groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G^0(S) & \longrightarrow & G(S) & \longrightarrow & G^{\text{ét}}(S) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha^0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^{\text{ét}}} & & \\ 0 & \longrightarrow & G^0(S/\mathfrak{m}S) & \longrightarrow & G(S/\mathfrak{m}S) & \longrightarrow & G^{\text{ét}}(S/\mathfrak{m}S) & \longrightarrow & 0. \end{array}$$

We have just seen that $\alpha^{\text{ét}}$ is an isomorphism, so $\ker \alpha \subset G^0(S)$. By the definition of the topology on $G(S)$, we see that $G^0(S)$ is an open subgroup of $G(S)$. □

Lemma 6.3.13. *When L is algebraically closed, $G(S)$ is p-divisible.*

Proof. We will prove a more precise statement: given $S \subset L$ for any completion L of an algebraic extension of K, and given $x \in G(S)$, there is a finite extension L'/L and $y \in G(S')$ such that $py = x$ (and clearly L' is the completion of an algebraic extension of K).

By (6.3.1), it suffices to check this separately for the connected and étale cases. In the étale case, the proof of Lemma 6.3.12 shows that $G^{\text{ét}}(S) = \varinjlim G_n(S) = \varinjlim G_n(S/\mathfrak{m}S)$. Writing $S/\mathfrak{m}S$ as a direct limit of finite local $R/\mathfrak{m} = k$-algebras and using the fact that G_n is finite over R, we see that $G_n(S/\mathfrak{m}S) = G_n(k_S)$, where k_S denotes the residue field of S (which is an algebraic extension of k). But for a separable closure k_s of k_S, we know from the étale dictionary that $\varinjlim G_n(k_s) = (\mathbf{Q}_p/\mathbf{Z}_p)^h$ for some h. Since $G_n(k_s) = \varinjlim_{k'} G_n(k')$ with $k' \subset k_s$ ranging through finite separable extensions of k_S, we are done if we can show that every finite separable extension of k_S arises as the residue field of the valuation ring in some finite extension L'/L (which admits a unique extension of the valuation on L). We see this as follows: given k'/k_S, we may lift a minimal polynomial for a primitive element for k' over k_S to an irreducible monic polynomial $f \in S[x]$. Letting L' be the field of fractions of $S[x]/(f(x))$, we see that $[L' : L] = [k' : k_S]$ and that the valuation ring S' of L' must contain $S[x]/(f(x))$. We conclude from the standard inequalities of valuation theory (for valuation rings which are not necessarily discrete, e.g., S) [7, Exercise 10.8] that the residue field of S' must be k'. This settles the étale case.

In the connected case, we recall that $[p] : G^0 \to G^0$ is an isogeny of degree $p^{h'}$ for some h'. Thus, $[p]^* : \mathscr{O}(G^0) \to \mathscr{O}(G^0)$ is a finite free R-algebra extension of rank $p^{h'}$. Therefore, by integrality, embedding S in $\overline{L}$ we see that any continuous R-algebra map $\mathscr{O}(G^0) \to S$ extends along $[p]^*$ to an R-algebra map $\mathscr{O}(G^0) \to L'$ for a finite extension L'/L. This extension is automatically continuous: choosing coordinates $X_1, \dots, X_n$ for $\mathscr{O}(G^0)$, it is easy to see (using the properties of non-archimedean valuations) that the X_i must land in the maximal ideal of the valuation ring S' of L'. □

With this extension to the case of an arbitrary p-divisible group, we have developed all of the analytic tools which we will need to establish the Hodge-Tate decomposition of $\mathrm{Hom}_{\mathbf{Z}_p}(T(G), \mathbf{C}_K)$ for an arbitrary p-divisible group G over our mixed characteristic $(0, p)$ complete discrete valuation ring R. (We note in passing that it is not surprising that we should need analysis, as the Hodge decomposition of the cohomology of an abelian variety in the classical (complex) case is itself an *analytic*, rather than an *algebraic*, fact.)

As a consequence of the analysis in the proof of Lemma 6.3.12, we deduce the following.

Lemma 6.3.14. *The construction $G \rightsquigarrow G(S)$ is naturally a functor from p-Barsotti-Tate groups over R to topological $\mathbf{Z}_p$-modules, natural in G and S. Given a map $f : G \to H$ of p-Barsotti-Tate groups over R, the induced map $f^0(S) : G^0(S) \to H^0(S)$ is a map of analytic groups over L, functorial in L.*

7 The main results

7.1 The Hodge-Tate decomposition

We assume for the rest of Part II that the residue field k of our mixed characteristic $(0, p)$ complete discrete valuation ring R is perfect.

7.1.1 Statements from Part III

In Part III, we will investigate the continuous cohomology of $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$ with coefficients in $\mathbf{C}_K$. Briefly, we will define a cochain complex consisting of continuous cochains and we will define H^0 and H^1 in the usual manner (using the familiar Hochschild coboundary maps). The results which we prove are essential for proof of the Hodge-Tate decomposition. In particular, we will prove:

Fixed Points Theorem (Theorem 10.3.1).

$$\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K) = K \text{ and } \dim_K \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K) = 1.$$

Twisting Theorem (Theorem 10.3.2). *If ε_p is the p-adic cyclotomic character on $\mathscr{G}$, then for all $n \neq 0$,*

$$\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(n)) = 0 = \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(n)).$$

(Recall that $\mathbf{C}_K(n) = \mathbf{C}_K(\varepsilon_p^n)$ is the twist of $\mathbf{C}_K$ by ε_p^n.)

Hodge-Tate Lemma. *If W is a finite-dimensional $\mathbf{C}_K$-vector space admitting a continuous semi-linear $\mathscr{G}$-action, then the natural $\mathbf{C}_K$-linear map $W^{\mathscr{G}} \otimes_K \mathbf{C}_K \to W$ of $\mathscr{G}$-modules is injective. In particular, $\dim_K W^{\mathscr{G}} < \infty$.*

7.1.2 Proof of the Hodge-Tate decomposition

Let D be the ring of integers of $\mathbf{C}_K$ with $U_D = \{x \in D : |x - 1| < 1\} \subset D^{\times}$. Suppose G is a p-divisible group over R of height h and dimension N. Let $T = T(G)$ and

$T^\vee = T(G^\vee)$, and let $W = \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{C}_K)$, $W^\vee = \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, \mathbf{C}_K)$ (as $\mathbf{C}_K$-semilinear $\mathscr{G}$-representations). Note that while $T^\vee = \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p(1))$, it is not the case with our notation that $W^\vee = \mathrm{Hom}_{\mathbf{Z}_p}(W, \mathbf{Z}_p(1))$.

Before we study the Hodge-Tate decomposition, we will use the logarithm to show that the dual generic fiber Tate module $T^\vee$ actually encodes global information about G *over* R. In particular, we will prove

Theorem 7.1.1. *There are natural isomorphisms*

$$G(R) \xrightarrow{\alpha_R} \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, U_D)^{\mathscr{G}}$$

of groups and

$$t_G(K) \xrightarrow{d\alpha_R} (W^\vee)^{\mathscr{G}}$$

of K-vector spaces.

The Hodge-Tate decomposition will arise as a corollary of the methods we employ to prove Theorem 7.1.1. The essential input is Cartier duality, which relates points of $G_n^\vee$ to morphisms $G_n \to \mathbf{G}_m$. Let us make this more precise:

We see by the definition of Cartier duality that for each n there is an isomorphism of $\mathscr{G}$*-modules*

$$G_n^\vee(D) \xrightarrow{\sim} \mathrm{Hom}_{D\text{-gps}}(G_{n/D}, \mathbf{G}_{m/D}) = \mathrm{Hom}_{D\text{-gps}}(G_{n/D}, \boldsymbol{\mu}_{p^{nh}/D}) \tag{7.1.1}$$

by functoriality in D (where the $\mathscr{G}$-action on the right is by base change). This isomorphism is compatible with change in n, so we get a natural isomorphism

$$\varprojlim G_n^\vee(D) \xrightarrow{\sim} \mathrm{Hom}_{p\text{-B.T.}/D}(G_D, \mathbf{G}_{m/D}(p)) \tag{7.1.2}$$

compatible with the $\mathscr{G}$-actions. On the other hand, it is easy to see by integrality that $G_n^\vee(D) = G_n^\vee(\overline{K})$, so we see that the left side of (7.1.2) is actually $T(G^\vee)$. Using Lemma 6.3.14 with $S = D$ gives a map of $\mathscr{G}$-modules

$$T(G^\vee) \to \mathrm{Hom}(G(D), \widehat{\mathbf{G}}_m(D)), \tag{7.1.3}$$

where the right side consists of maps $G(D) \to \widehat{\mathbf{G}}_m(D)$ of topological $\mathbf{Z}_p$-modules whose restriction to $G^0(D)$ induces a map of analytic groups $G^0(D) \to \widehat{\mathbf{G}}_m^0(D)$. (The $\mathscr{G}$-action preserves the analyticity of the maps $G^0(D) \to \widehat{\mathbf{G}}_m^0(D)$ because the formal group laws are defined over R).

By functoriality and analyticity, the logarithm gives a map of $\mathscr{G}$-modules

$$\mathrm{Hom}(G(D), \widehat{\mathbf{G}}_m(D)) \xrightarrow{\log} \mathrm{Hom}_{\mathbf{C}_K}(t_G(\mathbf{C}_K), t_{\widehat{\mathbf{G}}_m}(\mathbf{C}_K)).$$

Writing this more symmetrically and using Example 6.3.9, Proposition 6.3.11, and

Lemma 6.3.12 gives a functorial diagram of pairings

$$
\begin{array}{ccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
(7.1.4) & & T(G^\vee) \times \Phi(G) & \longrightarrow & \Phi(\widehat{\mathbf{G}}_m) & \xrightarrow{\sim} & (U_D)_{\mathrm{tors}} \\
 & & \downarrow{\scriptstyle \mathrm{id}_{T(G^\vee)}} & & \downarrow & & \downarrow \\
 & & T(G^\vee) \times G(D) & \longrightarrow & \widehat{\mathbf{G}}_m(D) & \xrightarrow{\sim} & U_D \\
 & & \downarrow{\scriptstyle \mathrm{id}_{T(G^\vee)} \,|\, \log} & & \downarrow{\scriptstyle \log} & & \downarrow{\scriptstyle \log_p} \\
 & & T(G^\vee) \times t_G(\mathbf{C}_K) & \longrightarrow & t_{\widehat{\mathbf{G}}}(\mathbf{C}_K) & \xrightarrow{\sim} & \mathbf{C}_K \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0.
\end{array}
$$

Diagram (7.1.4) gives rise to a smaller commutative diagram of $\mathbf{Z}_p$-linear maps

(7.1.5)

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \Phi(G) & \longrightarrow & G(D) & \xrightarrow{\log} & t_G(\mathbf{C}_K) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle d\alpha} & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, (U_D)_{\mathrm{tors}}) & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, U_D) & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, \mathbf{C}_K) & \longrightarrow & 0.
\end{array}
$$

We see that α_0, α, and $d\alpha$ are $\mathscr{G}$-homomorphisms (with respect to the usual action on $\mathrm{Hom}_{\mathbf{Z}_p}(\,\cdot\,,\,\cdot\,)$) by chasing the functoralities in diagram (7.1.4). Similarly, we see that $d\alpha$ is $\mathbf{C}_K$-linear. By analyzing (7.1.5), we will prove the following Proposition.

Proposition 7.1.2 (Pairing Proposition). *In diagram* (7.1.5)*, α_0 is a bijection and α and $d\alpha$ are injective.*

We defer the proof of Proposition 7.1.2 to Section 7.1.3. Let us prove Theorem 7.1.1 using the Pairing Proposition. Note that by the Fixed Points Theorem, $G(R) = G(D)^{\mathscr{G}}$ and $t_G(K) = t_G(\mathbf{C}_K)^{\mathscr{G}}$.

Proof of Theorem 7.1.1. We will prove the Theorem by using the "differential" $d\alpha$ to reduce the question to one of (semi)-linear algebra, where a dimension computation will suffice to prove the result.

By $\mathscr{G}$-equivariance and Proposition 7.1.2, we see that α and $d\alpha$ induce injective maps

$$\alpha_R : G(R) \to \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, U_D)^{\mathscr{G}}$$

of groups and

$$d\alpha_R : t_G(K) \to (W^\vee)^{\mathscr{G}}$$

of K-vector spaces. By left-exactness of the fixed-points functor $\mathrm{H}^0(\mathscr{G}, \cdot)$, we see that $\mathrm{coker}\,\alpha_R \to (\mathrm{coker}\,\alpha)^{\mathscr{G}}$ and $\mathrm{coker}\,d\alpha_R \to (\mathrm{coker}\,d\alpha)^{\mathscr{G}}$ are injective. But Proposition 7.1.2 and the Snake Lemma show that $\mathrm{coker}\,\alpha \to \mathrm{coker}\,d\alpha$ is a bijection, so $\mathrm{coker}\,\alpha_R \to \mathrm{coker}\,d\alpha_R$ is injective.

Therefore, to prove the Theorem it suffices to prove that $d\alpha_R$ is surjective. But $d\alpha_R : t_G(K) \to \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, \mathbf{C}_K)^{\mathscr{G}}$ is a K-linear map with $\dim_K t_G(K) = \dim G$, so it suffices (by the Hodge-Tate Lemma) to prove that $\dim_K \mathrm{Hom}(T^\vee, \mathbf{C}_K)^{\mathscr{G}} = N = \dim G$. Recall that W and $W^\vee$ are h-dimensional $\mathbf{C}_K$-vector spaces with semi-linear $\mathscr{G}$-action. If $d = \dim_K W^{\mathscr{G}}$ and $d^\vee = \dim_K (W^\vee)^{\mathscr{G}}$, then we know by injectivity of $d\alpha_R$ (in general, i.e., for both G *and* $G^\vee$) that $N \leq d^\vee$ and $N^\vee \leq d$, where $N^\vee = \dim G^\vee$. Therefore, by Proposition 6.2.8 we see that $h \leq d + d^\vee$, and to show that $\operatorname{coker} d\alpha_R = 0$, we need only show that $d + d^\vee \leq h$.

Since $T \cong \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, \mathbf{Z}_p(1))$ it is an exercise in algebra to show that there is a $\mathscr{G}$-equivariant isomorphism

$$W^\vee \cong T \underset{\mathbf{Z}_p}{\otimes} \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{Z}_p(1), \mathbf{C}_K) \cong T \underset{\mathbf{Z}_p}{\otimes} \mathbf{C}_K(-1).$$

Thus, we get a $\mathscr{G}$-equivariant $\mathbf{C}_K$-bilinear pairing

$$\mathfrak{B} : W \times W^\vee \to \mathbf{C}_K(-1)$$

defined by $(f, t \otimes \alpha) \mapsto f(t)\alpha$. It is easy to see that $\mathfrak{B}$ is a perfect pairing of $\mathbf{C}_K$-vector spaces. But $W^{\mathscr{G}}$ and $(W^\vee)^{\mathscr{G}}$ clearly pair into $\mathbf{C}_K(-1)^{\mathscr{G}}$, which vanishes by the Fixed Points Theorem. Furthermore, the map $W^{\mathscr{G}} \otimes_K \mathbf{C}_K \to W$ given by scalar multiplication is injective by the Hodge-Tate Lemma. Hence, a d-dimensional subspace of W annihilates a $d^\vee$-dimensional subspace of $W^\vee$. Because $\mathfrak{B}$ is perfect, we see that $d + d^\vee \leq \dim_{\mathbf{C}_K} W = h$, completing the proof. □

Theorem 7.1.3 (Hodge-Tate decomposition). *There is a canonical $\mathbf{C}_K$-linear $\mathscr{G}$-equivariant decomposition*

$$\mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{C}_K) \cong t_{G^\vee}(\mathbf{C}_K) \oplus t_G^*(\mathbf{C}_K)(-1).$$

Proof. Since it is clear that $t_G(K) \otimes_K \mathbf{C}_K \xrightarrow{\sim} t_G(\mathbf{C}_K)$ (and similarly for $t_{G^\vee}$), we see from the proof of Theorem 7.1.1 and the Hodge-Tate Lemma that $d\alpha$ (resp. $d\alpha^\vee$) injects $t_G(\mathbf{C}_K)$ (resp. $t_{G^\vee}(\mathbf{C}_K)$) onto subspaces of $W^\vee$ and W which are orthogonal complements for the perfect pairing $\mathfrak{B}$. This says precisely that the pairing $\mathfrak{B}$ induces an exact sequence

$$(7.1.6) \quad 0 \to t_{G^\vee}(\mathbf{C}_K) \xrightarrow{d\alpha^\vee} W \to \mathrm{Hom}_{\mathbf{C}_K}(t_G(\mathbf{C}_K), \mathbf{C}_K(-1)) = t_G^*(\mathbf{C}_K)(-1) \to 0.$$

To complete the proof, it remains to show that the sequence (7.1.6) splits uniquely (compatibly with the $\mathscr{G}$-actions). Twisting (7.1.6) by ε_p, we see that it suffices to show that for any m and n, a sequence of semi-linear $\mathbf{C}_K$-spaces with continuous semi-linear $\mathscr{G}$-actions

$$(7.1.7) \qquad 0 \to \mathbf{C}_K(1)^m \to V \to \mathbf{C}_K^n \to 0$$

splits uniquely. Since $\mathrm{Hom}_{\mathbf{C}_K}(\mathbf{C}_K, \mathbf{C}_K(1)) \cong \mathbf{C}_K(1)$, the Twisting Theorem shows that such a splitting is unique if it exists. On the other hand, it is easy to see that we may form the functor $\mathrm{Ext}^1(\cdot, \cdot)$ classifying extensions on the category of finite-dimensional $\mathbf{C}_K$-vector spaces with continuous semi-linear $\mathscr{G}$-action and that $\mathrm{Ext}^1(\bigoplus V_i, \bigoplus W_j) = \bigoplus \mathrm{Ext}^1(V_i, W_j)$, so we see by the Twisting Theorem that

$$\mathrm{Ext}^1(\mathbf{C}_K^n, \mathbf{C}_K(1)^m) = \bigoplus \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(1)) = 0,$$

and the extension splits. □

7.1.3 Proof of the pairing proposition

Following Tate [11, Proposition 11], we prove the Pairing Proposition in steps.
Step 1. *The map α_0 is bijective.* Because $\operatorname{char} K = 0$, we see that there is a natural isomorphism of $\mathscr{G}$-modules

$$\begin{aligned} G_n^\vee(\mathbf{C}_K) &\cong \operatorname{Hom}(G_n(\mathbf{C}_K), \mathbf{G}_m(\mathbf{C}_K)) \\ &= \operatorname{Hom}(G_n(\mathbf{C}_K), \boldsymbol{\mu}_{p^\infty}(\mathbf{C}_K)) \\ &= \operatorname{Hom}(G_n(\mathbf{C}_K), (U_D)_{\text{tors}}). \end{aligned}$$

Therefore, Cartier duality provides a perfect pairing of abelian groups

$$G_n(\mathbf{C}_K) \times G_n^\vee(\mathbf{C}_K) \to \boldsymbol{\mu}_{p^{nh}}(D) \hookrightarrow (U_D)_{\text{tors}}, \tag{7.1.8}$$

so there is an isomorphism of $\mathscr{G}$-modules

$$G_n(\mathbf{C}_K) \xrightarrow{\sim} \operatorname{Hom}(G_n^\vee(\mathbf{C}_K), (U_D)_{\text{tors}}). \tag{7.1.9}$$

Note that $T^\vee$ is a finitely generated $\mathbf{Z}_p$-module, while $(U_D)_{\text{tors}}$ is torsion, so any map $T^\vee \to (U_D)_{\text{tors}}$ must factor through some $T^\vee/p^n T^\vee$, i.e., through some $G_n^\vee(\mathbf{C}_K)$. Thus, passing to the limit in (7.1.9), we see that there is a natural isomorphism of $\mathscr{G}$-modules

$$\Phi(G) \xrightarrow{\sim} \varinjlim \operatorname{Hom}(G_n^\vee(\mathbf{C}_K), (U_D)_{\text{tors}}) \xrightarrow{\sim} \operatorname{Hom}(T^\vee, (U_D)_{\text{tors}}),$$

and this is exactly the map α_0.
Step 2. *The $\mathbf{Z}_p$-modules* $\ker\alpha$ *and* $\operatorname{coker}\alpha$ *are $\mathbf{Q}_p$-vector spaces.* Applying the Snake Lemma to diagram (7.1.5), we see that $\ker\alpha \to \ker d\alpha$ and $\operatorname{coker}\alpha \to \operatorname{coker} d\alpha$ are isomorphisms of $\mathbf{Z}_p[\mathscr{G}]$-modules. Thus, we need only show that $d\alpha$ is $\mathbf{Q}_p$-linear, and this follows from functoriality (it is even $\mathbf{C}_K$-linear).
Step 3. *We have $G(R) = G(D)^{\mathscr{G}}$ and $t_G(K) = t_G(\mathbf{C}_K)^{\mathscr{G}}$.* This is clear from the Fixed Points Theorem, for $\mathbf{C}_K^{\mathscr{G}} = K$ and $D^{\mathscr{G}} = R$, and the $\mathscr{G}$-action on $G(D)$ (resp. $t_G(\mathbf{C}_K)$) is induced by the action on D (resp. $\mathbf{C}_K$).
Step 4. *The map α is injective on $G(R)$.* By step 3 and the left-exactness of the fixed-points functor, we see that $\ker\alpha|_{G(R)} = (\ker\alpha)^{\mathscr{G}}$. By step 2, we see that $\ker\alpha$ is a $\mathbf{Q}_p$-vector space, so $\ker\alpha \cap G(R) = (\ker\alpha)^{\mathscr{G}}$ is a $\mathbf{Q}_p$-vector space and therefore is p-divisible. If G is *connected* then because the valuation on R is discrete, we see (as in the proof of Proposition 6.3.11) that $\cap p^n G(R) = 0$, and therefore $\ker\alpha \cap G(R) = 0$.

If G is arbitrary, then given $x \in \ker\alpha \cap G(R)$, we see from Lemma 6.3.12 that $p^n x \in \ker\alpha \cap G^0(R)$ for some n. Note that the closed immersion $G^0 \hookrightarrow G$ yields an injection $G^0(D) \hookrightarrow G(D)$ and a surjection $T(G^\vee) \twoheadrightarrow T((G^0)^\vee)$ (because $\varprojlim$ is exact on the category of finite abelian groups). By the functoriality in G of the formation of α and the proof of the connected case, we therefore see that $p^n x = 0$, so $x = 0$ because $\ker\alpha$ has no p-torsion.
Step 5. *The map $d\alpha|_{t_G(K)}$ is injective.* By steps 1 and 4, along with the Snake Lemma, we see that $d\alpha|_{\log G(R)}$ is injective. But $\mathbf{Q}_p \log G(R) = t_G(K)$ by Proposition 6.3.11, so step 5 follows because $t_G(K)$ is torsion-free.

Step 6. *The map $d\alpha$ is injective.* We can factorize $d\alpha$ as

$$t_G(\mathbf{C}_K) \cong t_G(K) \underset{K}{\otimes} \mathbf{C}_K \to \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, \mathbf{C}_K)^{\mathscr{G}} \underset{K}{\otimes} \mathbf{C}_K \to \mathrm{Hom}_{\mathbf{Z}_p}(T^\vee, \mathbf{C}_K).$$

By step 5, the middle map is an injection, and by the Hodge-Tate Lemma, the last map is an injection.

Using the Snake Lemma now shows that α is injective, completing the proof.

7.2 The Isogeny Theorem

Let R be a normal Noetherian domain with fraction field K of characteristic different from p.

Theorem 7.2.1 (Isogeny Theorem). *If G and H are p-Barsotti-Tate groups over R, then any generic morphism $f_K : G_K \to H_K$ uniquely extends to a morphism $f : G \to H$. In other words, the functor $G \rightsquigarrow G_K$ is fully faithful.*

Fix a separable closure $\overline{K}$ of K and let $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$.

Corollary 7.2.2. *The natural transformation $\mathrm{Hom}(G, H) \to \mathrm{Hom}_{\mathscr{G}}(T(G), T(H))$ of bifunctors is an isomorphism.*

If $R = K$, then the Isogeny Theorem is trivial. Furthermore, if $\mathrm{char}\, K \neq 0$, then $p \in R^\times$ so p-Barsotti-Tate groups are formally étale and the Isogeny Theorem follows from a normalization argument (working locally, completing, and using the structure of finite étale algebras over a complete discrete valuation ring). Therefore, we assume in what remains that $\mathrm{char}\, K = 0$ and $R \neq K$.

Theorem 7.2.1 is very similar to the theorem, originally conjectured by Tate and proven by Faltings, that for abelian varieties A and B over a finitely generated extension K of $\mathbf{Q}$, the map $\mathrm{Hom}_K(A, B) \otimes_{\mathbf{Z}} \mathbf{Z}_p \to \mathrm{Hom}_{\mathscr{G}}(T_p(A), T_p(B))$ is an isomorphism. In fact, Tate proved Theorem 7.2.1 as part of his attempt to adduce evidence for his conjecture (and Tate's work plays an essential role in Faltings's proof).

The strategy for proving Theorem 7.2.1 is to deduce it from the apparently weaker statement:

Proposition 7.2.3. *If $g : G \to H$ is a morphism of p-Barsotti-Tate groups over R such that the generic fiber map $g_K : G_K \to H_K$ is an isomorphism, then g is an isomorphism.*

(Beware that Propostion 7.2.3 is false if we replace "isomorphism" by "closed immersion" or "topologically faithfully flat.") We will get all of Theorem 7.2.1 from Proposition 7.2.3 by using a standard graph construction to extend certain generic fiber p-Barsotti-Tate groups to p-Barsotti-Tate groups over the entire base R *via* "closure." In fact, we will show the following result in Section 7.2.1.

Proposition 7.2.4. *Let R be a complete discrete valuation ring. If F is a p-divisible group over R and $M \subset T(F)$ is a $\mathbf{Z}_p$-direct summand which is a $\mathscr{G}$-submodule, then there is a p-divisible group Γ over R and a morphism $\phi : \Gamma \to F$ such that ϕ induces an isomomorphism $T(\Gamma) \xrightarrow{\sim} M$.*

(Beware that the ϕ in Proposition 7.2.4 does *not* factor through a closed immersion into F.) Let us show how the Isogeny Theorem reduces to Proposition 7.2.3.

Lemma 7.2.5. *Proposition* 7.2.3 *implies Theorem* 7.2.1.

Proof. Let $F = G \times H$. Clearly, $T(F) = T(G) \times T(H)$, so letting M be the graph of the induced map $T(f_K) : T(G) \to T(H)$, we see that $T(F) = M \oplus (\{0\} \times T(H))$. By Proposition 7.2.4, there is a p-Barsotti-Tate group Γ over R and a morphism $\phi : \Gamma \to G \times H$ such that $T(\phi) : T(\Gamma) \tilde{\to} M \subset T(F)$. But since M is the graph of $T(f_K) : T(G) \to T(H)$, we see that $p_1 \circ \phi$ induces an isomorphism $T(\Gamma) \to T(G)$, and therefore $(p_1 \circ \phi)_K$ is an isomorphism of generic fibers by Proposition 5.2.3. Thus, Proposition 7.2.3 shows that $p_1 \circ \phi : \Gamma \to G$ is an isomorphism. By construction, we see that

$$\psi = p_2 \circ \phi \circ (p_1 \circ \phi)^{-1} : G \to H$$

is a morphism extending the given morphism f_K of generic fibers. Because each torsion level is flat over R, it is clear that such an extension is unique ($A \to A \otimes_R K$ is injective for any flat R-algebra A). □

It remains to prove Proposition 7.2.4 and Proposition 7.2.3.

7.2.1 Extending generic fibers: the proof of Proposition 7.2.4

The main idea of the proof is to take the scheme-theoretic closure in F of the generic fiber p-Barsotti-Tate group corresponding to M, but the resulting directed system of finite R-groups may fail to be a p-Barsotti-Tate group. Therefore, we will need to alter it slightly without disturbing the generic fiber to produce a p-Barsotti-Tate group Γ and a map $\Gamma \to F$ which realizes the injection $M \to T(F)$ on the level of generic fiber Tate modules. This is a bit delicate because Γ usually does not come from a (system of) closed subgroup(s) of F.

Because M is a $\mathbf{Z}_p$-direct summand of $T(F)$, we see that $M/p^n M$ injects into $T(F)/p^n T(F)$, which means precisely that M corresponds to a closed p-divisible subgroup E' of the *generic fiber* F_K. If $F = (F_n)$ and $E' = (E'_n)$, write B_n for the affine R-algebra of F_n and A'_n for the affine K-algebra of E'_n. There is a surjective map $u_n : B_n \otimes_R K \to A'_n$ corresponding to the generic closed immersion $E'_n \hookrightarrow F_n \times \operatorname{Spec} K$. If we let $A_n = u_n(B_n)$, an R-subalgebra of A'_n, we see that A_n must be a free R-module because B_n is free and R is a principal ideal domain. In fact, $\operatorname{Spec} A_n \hookrightarrow \operatorname{Spec} B_n$ is precisely the scheme-theoretic closure of the open subscheme $E'_n \hookrightarrow (F_n)_K$ in F_n ($(F_n)_K$ is open in F_n because R is a discrete valuation ring). Letting $E_n = \operatorname{Spec} A_n$, we see by R-flatness that in fact E_n is a closed sub*group* of F_n (so E_0 is the trivial group), and it is not hard to see that the closed immersions $F_n \to F_{n+1}$ induce closed immersions $E_n \to E_{n+1}$.

Because (E_n) is generically p-Barsotti-Tate , we see that $[p]$ annihilates the R-flat quotient E_n/E_{n+1} because it annihilates the generic fiber. Therefore, we see that for all n, $[p]$ induces morphisms $\psi_{n,i} : E_{i+n+1}/E_{i+1} \to E_{i+n}/E_i$ which are generic isomorphisms. Therefore, if D_i is the affine algebra of E_{i+1}/E_i, then for each i $\psi_{1,i} : D_i \to D_{i+1}$ induces an isomorphism $D_i \otimes K \tilde{\to} D_{i+1} \otimes K$. If A denotes the common affine algebra of the $D_i \otimes K$, we see by flatness that $D_i \to A$ is injective, so we can identify D_i with its image in A, where there is a compatible system of injections $D_i \hookrightarrow D_{i+1}$. Therefore, we see that (D_i) is an increasing sequence of finitely generated R-submodules of the finite K-algebra A. But A is étale, so the normalization of R in A is a finite R-module. Thus, (D_i) must stabilize, i.e., there is i_0 such that $D_{i+1} = D_i$ for $i \geq i_0$ (under the identifications of $D_i \otimes K$ with A). If we let $\Gamma_n = E_{i_0+n}/E_{i_0}$, we then see that $[p^{i_0}]$ induces a system of group morphisms $\Gamma_n \to E_n/E_0 = E_n$ which are generic isomorphisms. Furthermore, we see that there are closed immersions $i_n : \Gamma_n \hookrightarrow \Gamma_{n+1}$ which correspond on the generic fiber to the closed immersions $E'_n \hookrightarrow E'_{n+1}$. If we can show that (Γ_n) is p-Barsotti-Tate , the morphism $\phi : \Gamma \to E \to F$ will complete the proof.

By an easy argument with the generic fiber, all we have to check is that i_n identifies Γ_n with $\Gamma_{n+1}[p^n]$. Consider the diagram

(7.2.1)
$$\begin{array}{ccccccc} \Gamma_{n+1} & = & E_{i_0+n+1}/E_{i_0} & \xrightarrow{[p^n]} & E_{i_0+n+1}/E_{i_0} & = & \Gamma_{n+1} \\ & & \downarrow \alpha & & \uparrow \gamma & & \\ & & E_{i_0+n+1}/E_{i_0+n} & \xrightarrow{\beta} & E_{i_0+1}/E_{i_0}, & & \end{array}$$

where α is the canonical projection, β the map induced by $[p^n]$, and γ the canonical closed immersion. Checking on the generic fiber, we see that (7.2.1) commutes. On the other hand, by our choice of i_0, we see that β is an isomorphism, and therefore $\ker[p^n] = \ker \alpha$, which is nothing more than Γ_n.

Remark 7.2.6. Tate [11] gives an example due to Serre showing that it is not the case that $\phi : \Gamma \to F$ is necessarily a closed immersion. ♦

7.2.2 The proof of Proposition 7.2.3

Because R is a normal Noetherian domain, $R = \cap_P R_P \subset K$ as P ranges over the height one prime ideals of R and each R_P is a discrete valuation ring. In particular, for finite locally free R-modules M and N in a fixed finite-dimensional K-vector space, we see that $M \subset N$ if and only if $M_P \subset N_P$ for all primes P of height one. Since our goal is to show that $f_K^* : \mathscr{O}(H_n)_K \to \mathscr{O}(G_n)_K$ takes $\mathscr{O}(H_n)$ into $\mathscr{O}(G_n)$ for all $n \geq 1$, it therefore suffices to prove Proposition 7.2.3 for a discrete valuation ring $(R, \mathfrak{m}, k)$.

It is clear that there is a faithfully flat extension R' of R which is a discrete valuation ring with algebraically closed residue field, and completing R' produces a complete discrete valuation ring $R'' \supset R$ which is also faithfully flat over R. Hence, we may assume that R is complete with algebraically closed residue field. If $p \neq \operatorname{char} k$, then G and H must be formally étale over R. Consider the finite stages $g_n : G_n \to H_n$. Because G_n and H_n are étale, looking at our proof of Proposition 3.1.5 shows that $\mathscr{O}(G_n)$ and $\mathscr{O}(H_n)$ are exactly products of integer rings in finite unramified extensions of K. Thus, by an easy integrality argument, we deduce the Isogeny Theorem in the formally étale case. We are reduced to the difficult case: R is a complete discrete valuation ring with perfect residue field k of characteristic p.

Let us again view this from the p-Barsotti-Tate viewpoint. In this case, we are given a family $u_n : A_n \to B_n$ of maps between finite free generically étale R-algebras such that $u_n \otimes_R K$ is an isomorphism. This certainly implies that u_n is injective. Because R is a discrete valuation ring (and in particular, a principal ideal domain), it is easy to see that u_n is an isomorphism if and only if $\mathrm{disc}_{A_n/R} = \mathrm{disc}_{B_n/R}$ (these discriminant ideals being non-zero because G_n and H_n are generically étale). By Proposition 6.2.12, $\mathrm{disc}\, G_n$ depends only upon n, $\dim G$, and $\mathrm{ht}\, G$, and similarly for $\mathrm{disc}\, H_n$. But by Theorem 7.1.3 and the Twisting Theorem, $T(G)$ and $T(H)$ encode the dimensions of G and H respectively, and since f is a generic isomorphism, $\dim G = \dim H$. Similarly, it is trivial that generically isomorphic p-divisible groups have equal heights. Therefore, we see that u_n is an isomorphism for all n.

Remarks 7.2.7. 1) As we will see in Part III, without Serre's geometric local class field theory (which is needed instead of the usual local class field theory to prove the Twisting Theorem if the perfect residue field of R is not finite), the proof we have given for Theorem 7.1.3 (and hence Theorem 7.2.1) only works for Noetherian domains R with finite residue field at the height one primes whose residue characteristic is p. This includes integer rings of number fields and p-adic fields (finite extensions of $\mathbf{Q}_p$).

2) In the case where $\mathrm{char}\, K = p$, we can reduce just as in the beginning of the proof of Proposition 7.2.3 to the case where $R \cong k[\![t]\!]$ for an algebraically closed field k of characteristic p (by the structure theorem for equicharacteristic complete discrete valuation rings). Unfortunately, the analytic tools Tate used in his proof (e.g., the logarithm) are only available in characteristic zero. The equicharacteristic case remained unsolved until 1996, when de Jong proved it using techniques of crystalline cohomology. ♦

Part III
Galois Modules

8 Introduction

Let A be a mixed characteristic complete discrete valuation ring of absolute ramification index e with perfect residue field k of characteristic $p > 0$ and fraction field K (a local field). Write $\mathscr{G}$ for the absolute Galois group of K. These notations (in addition to the notations introduced at the beginning of this thesis) will remain in effect throughout this Part.

The study of étale groups in Part I showed that the generic fiber of a (formal or finite) group scheme over A may be studied as a Galois module, or, conversely, that a Galois module may be viewed as a geometric object, namely, an étale group over K. Part II showed that for a p-divisible group G over A, the generic fiber Galois representation decomposes after extending scalars to $\mathbf{C}_K$ in a fashion reminiscent of the Hodge decomposition of the de Rham cohomology of a complex abelian variety. In other words, the geometry of an abelian scheme over A (e.g., an elliptic curve with good reduction) constrains the generic fiber Tate module representation of $\mathscr{G}$. This Part will focus on the cohomological issues which arose in Section 7.1.1 (and provide the proofs for the facts which are necessary to Part II).

Call M a *topological $\mathscr{G}$-module* if M is a $\mathscr{G}$-module with a topology such that $\mathscr{G} \times M \to M$ is continuous. Given a topological $\mathscr{G}$-module M, define the *continuous* cohomology to be the cohomology of the complex $C^*(\mathscr{G}, M)$ given by continuous cochains $f : \mathscr{G}^r \to M$. (This is usually not a derived functor.) On the rare occasions when the topology on M is discrete, the complex will be notated C^*_{disc} and the cohomology groups will be written $\mathrm{H}^r_{\text{disc}}$. Where necessary, the r-cocycles and r-coboundaries are denoted $\mathrm{Z}^r(\mathscr{G}, M)$ and $\mathrm{B}^r(\mathscr{G}, M)$, respectively.

When M has the additional structure of R-module for some ring R and the $\mathscr{G}$-action is R-linear, the continuous cohomology naturally lives in the category of R-modules. Especially important for us will be semi-linear representations of $\mathscr{G}$ on F-modules for topological rings F (usually subfields of $\mathbf{C}_K$) admitting semi-linear $\mathscr{G}$-actions. Letting $F\{\mathscr{G}\}$ denote the "semi-linear group ring" (such that for $\alpha \in F$ and $g \in \mathscr{G}$, $g\alpha = g(\alpha)g$), a left $F\{\mathscr{G}\}$-module V is precisely an F-module with a semi-linear left $\mathscr{G}$-action. When V is a topological F-module with an $F\{\mathscr{G}\}$-structure such that $\mathscr{G}$ acts continuously, we say that V is a *topological $F\{\mathscr{G}\}$-module* (we do not put a topology on the ring $F\{\mathscr{G}\}$).

We may produce inflation and restriction maps by composing cochains with quotient maps $\mathscr{G} \to \mathscr{G}/\mathscr{H}$ by closed groups or restricting cochains to closed subgroups $\mathscr{H} \subset \mathscr{G}$. The direct computational proof of the exactness of the low-degree inflation-restriction sequence carries over to continuous cohomology: if $\mathscr{H} \subset \mathscr{G}$ is a closed subgroup and M is a topological $\mathscr{G}$-module, then there is an exact sequence

$$0 \to \mathrm{H}^1(\mathscr{G}/\mathscr{H}, M^{\mathscr{H}}) \to \mathrm{H}^1(\mathscr{G}, M) \to \mathrm{H}^1(\mathscr{H}, M).$$

As usual, $\mathrm{H}^0(\mathscr{G}, M) = M^{\mathscr{G}}$ and if M is a topological $R\{\mathscr{G}\}$-module then $\mathrm{H}^1(\mathscr{G}, M)$

classifies topological short exact sequences

$$0 \to M \to N \to \mathbf{1} \to 0$$

up to isomorphism, i.e., continuous extension classes of $\mathbf{1}$ by M, where $\mathbf{1}$ is the trivial semi-linear representation of $\mathscr{G}$ on R.

The fundamental result of this Part is that

$$\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(1)) = 0, \tag{8.0.2}$$

which shows that topological $\mathbf{C}_K\{\mathscr{G}\}$-module extensions of the form

$$E : 0 \to \mathbf{C}_K^m \to V \to \mathbf{C}_K(-1)^n \to 0$$

are split.

We will also show that twisting by ε_p and taking fixed points allows us to recover the splitting of an extension such as E. The fundamental result in this direction is

$$\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(n)) = \begin{cases} 0 & \text{if } n \neq 0; \\ K & \text{if } n = 0. \end{cases} \tag{8.0.3}$$

Thus, for example, given a topological sequence E, we can recover m (resp. n) by computing $\dim_K V^{\mathscr{G}}$ (resp. $\dim_K V(1)^{\mathscr{G}}$). (By combining these two pieces of information, we can recover the splitting.) This shows that if G is a p-Barsotti-Tate group over A, then $\dim G = \dim_K \mathrm{Hom}_{\mathbf{Z}_p}(T(G), \mathbf{C}_K)(1)^{\mathscr{G}}$, so $T(G)$ "knows" the dimension of G.

The goal of this Part is two-fold: first, to prove (8.0.2) and (8.0.3), which will be done in slightly greater generality than is stated here (and which will be completed in Section 10.3); second, to give some indication of the general properties shared by Galois modules which admit "Hodge-Tate decompositions" (e.g., the generic fiber Tate module of a p-Barsotti-Tate group). To motivate the discussion, we will carry out these tasks in the reverse order.

9 Modules of Hodge-Tate type

Given a field F with a non-archimedean valuation, A_F will denote the ring of integers. For the fixed base field K the ring of integers may also be denoted simply by A, depending upon the context. These conventions will hold throughout the remainder of Part III.

9.1 The action

It is a standard result that the valuation on K extends uniquely to (a non-discrete valuation on) $\overline{K}$ and that $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$ acts on $\overline{K}$ by isometries with respect to this metric. It is also well known [4, Chapter III, §4] that $\overline{K}$ is not complete, but that its completion $\mathbf{C}_K$ is algebraically closed. By uniform continuity, the $\mathscr{G}$-action extends to an isometric action on $\mathbf{C}_K$.

Lemma 9.1.1. *Let X be the completion of any algebraic extension L of K. If X has the valuation topology and $\mathscr{G}$ the usual profinite topology, then the action $\mathscr{G} \times X \to X$ is continuous.*

Proof. It suffices to show that given a point $x \in X$, the set of $s \in \mathscr{G}$ which stabilize an arbitrarily small open ball around x is open. Because L is dense in X, given n there is an $\alpha \in L$ and a $\beta \in A_X$ such that x may be written as $\alpha + p^n\beta$. By the definition of the Krull topology, α is fixed by some open subgroup $\mathscr{H} \subset \mathscr{G}$, so $\mathscr{H}$ stabilizes the ball $x + p^n A_X$. ☐

This complements the familiar result from infinite Galois Theory that the action $\mathscr{G} \times \overline{K} \to \overline{K}$ is continuous when $\overline{K}$ has the discrete topology.

9.2 The Hodge-Tate property

Given a ring R with a $\mathscr{G}$-action and an $R\{\mathscr{G}\}$-module M, we may consider the action of $\mathscr{G}$ *twisted* by a multiplicative character $\chi : \mathscr{G} \to R^\times$. It is easy to see that $M(\chi) = R(\chi) \otimes_R M$ as an $R\{\mathscr{G}\}$-module, and that there is a natural isomorphism $M(\chi_1)(\chi_2) = M(\chi_1\chi_2)$. When R is topologized such that the action $\mathscr{G} \times R \to R$ is continuous and χ is continuous, twisting a topological $R\{\mathscr{G}\}$-module by χ produces another topological $R\{\mathscr{G}\}$-module.

Suppose V is a finite-dimensional $\mathbf{C}_K$-vector space admitting a semi-linear continuous $\mathscr{G}$-action. Since the underlying spaces of V and $V(\chi^{-1})$ are the same, $V^\chi \stackrel{\text{def}}{=} V(\chi^{-1})^{\mathscr{G}}$ is canonically a sub-K-vector space of V. Explicitly, V^χ is the set of $v \in V$ such that $s(v) = \chi(s)v$ for all $s \in \mathscr{G}$. There is a natural $\mathbf{C}_K\{\mathscr{G}\}$-linear map

$$\mathbf{C}_K \underset{K}{\otimes} V^\chi \to V$$

given by scalar multiplication, where $\mathbf{C}_K \otimes_K V^\chi$ is given the obvious $\mathbf{C}_K\{\mathscr{G}\}$-module structure.

Fixing a choice of character χ, let V^i (resp. $V[i]$) denote V^{χ^i} (resp. $\mathbf{C}_K \otimes_K V^i$). There is certainly a $\mathbf{C}_K\{\mathscr{G}\}$-module map $\Theta_V^\chi : \bigoplus_{i\in\mathbf{Z}} V[i] \to V$. For a certain class of characters, we can show that Θ_V^χ is injective. This is quite a strong statement, as in general we cannot even be sure that *any* V^i has finite K-dimension.

Definition 9.2.1. Let $\chi : \mathscr{G} \to A^\times$ be a continuous multiplicative character. If the fixed field of χ is a totally ramified $\mathbf{Z}_p$-extension of a finite subextension K_0/K of $\overline{K}$, then χ will be called *ramified*.

The p-adic cyclotomic character ε_p is the most important example of a ramified character (see Lemma 10.1.3). If χ is ramified then χ^n is also ramified, for $\operatorname{im}\chi^n$ is infinite and any sub-$\mathbf{Z}_p$-extension of a ramified $\mathbf{Z}_p$-extension is itself ramified. Furthermore, if χ is ramified and $\mathscr{H}$ is an open subgroup of $\mathscr{G}$, then $\chi|_{\mathscr{H}}$ is ramified. (See Section 10.1 for a brief discussion of $\mathbf{Z}_p$-extensions.)

Using the continuous cohomology introduced in Section 8, we will prove two essential results in Section 10.3. Because we will use these results in this section, we give the statements here.

Fixed Points Theorem (Theorem 10.3.1).

$$\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K) = K \text{ and } \dim_K \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K) = 1.$$

Twisting Theorem (Theorem 10.3.2). *If χ is ramified, then*

$$\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(\chi)) = 0 = \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(\chi)).$$

Using these Theorems, we prove a Lemma which is fundamental to the rest of this section.

Lemma 9.2.2. *The map $\Theta_V^\chi : \bigoplus V[i] \to V$ is injective if χ is ramified.*

Proof. For each i, let $\{\alpha_{ij}\}$ be a (possibly infinite) K-basis for V^i, viewed as a K-subspace of V. If Θ_V^χ is not injective, then there is some linear dependence $L = \sum c_{ij}\alpha_{ij} = 0$ where at least one $c_{ij} \neq 0$ and a minimal number of coefficients are non-zero. Without loss of generality, we may assume that $c_{i_0 j_0} = 1$ for some pair of indices. Applying $s \in \mathscr{G}$ to the relation L yields

$$\sum_{i,j} s(c_{ij})\chi^i(s)\alpha_{ij} = 0.$$

Now, $L - s(L)/\chi^{i_0}(s) = 0$ gives another linear dependence with strictly fewer non-zero coefficients because $c_{i_0 j_0} = 1$. By minimality, $s(L) = \chi^{i_0}(s)L$ for all $s \in \mathscr{G}$. Expanding this out and using linear independence of the α_{ij}, it must be case that

$$s(c_{ij})\chi^i(s) = \chi^{i_0}(s)c_{ij}$$

for all i and j. In other words, $c_{ij} \in \mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(\chi^{i-i_0}))$. By Theorem 10.3.2, $c_{ij} = 0$ unless $i = i_0$, in which case $c_{i_0 j} \in K$ by Theorem 10.3.1(1). But the $\alpha_{i_0 j}$ are K-linearly independent by construction, so all of the coefficients must vanish, resulting in a contradiction. Therefore, no such dependence is possible, and the Lemma is proven. □

Remarks 9.2.3. 1) In practice, the chosen character will be the p-adic cyclotomic character ε_p (cf. Section 10.1). In general, if $\chi : \mathscr{G} \to \mathbf{Z}_p^\times$ is any continuous multiplicative character of $\mathscr{G}$ with infinite image, $\mathscr{G}/\ker\chi$ must contain an open subgroup topologically isomorphic to $\mathbf{Z}_p$. (This follows because $\operatorname{im}\chi$ is an infinite closed subgroup of $\mathbf{Z}_p^\times$, there is a continuous split surjection $\mathbf{Z}_p^\times \to \mathbf{Z}_p$ with finite kernel, and any closed subgroup of $\mathbf{Z}_p$ is an ideal.) Thus, the fixed field of $\ker\chi$ is always a $\mathbf{Z}_p$-extension of a finite subextension K_0/K; the hypothesis of Lemma 9.2.2 simply adds the condition that this $\mathbf{Z}_p$-extension be ramified. This property separates ramified characters χ from arbitrary continuous characters with infinite image.

2) Because Θ_V^χ is injective, the infinite direct sum in the definition of Θ_V^χ actually has only finitely many non-zero terms and $\sum_i \dim_K V^i \leq \dim_{\mathbf{C}_K} V$. This is the essential point of choosing a character of infinite order. If χ were a continuous character to the discrete topology of $K^\times$ (so that $\operatorname{im}\chi$ would be finite, among other things), Hilbert's Theorem 90 (i.e., $\mathrm{H}^1_{\mathrm{disc}}(\mathscr{G}, K^\times) = 0$) shows that $\mathbf{C}_K(\chi^n) \cong \mathbf{C}_K$ as $\mathbf{C}_K\{\mathscr{G}\}$-modules for all n, so twisting by different powers of χ does not pick out distinct K-subspaces of $\mathbf{C}_K$. ♦

If T is the Tate module of a p-divisible group over A and $\chi = \varepsilon_p$, let $T' = \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{C}_K)$ as a $\mathbf{C}_K\{\mathscr{G}\}$-module. Theorem 7.1.3 of Part II shows that $T' = T'[0] \oplus T'[1]$ as a $\mathbf{C}_K\{\mathscr{G}\}$-module. In other words, not only does the injection of Lemma 9.2.2 hold, but the map $\Theta_{T'}^{\varepsilon_p}$ is actually surjective, and this corresponds precisely to the "Hodge-like" decomposition of T'. This motivates the following definition.

Definition 9.2.4. Given a ramified character χ, a $\mathbf{C}_K\{\mathscr{G}\}$-module V is *of* χ*-Hodge-Tate type* (or simply is χ*-Hodge-Tate* or *Hodge-Tate for* χ) if Θ_V^{χ} is a bijection. More generally, given a finite dimensional K-vector space V with a linear $\mathscr{G}$-action, V will be called *pre-*χ*-Hodge-Tate* if the semi-linear representation $\mathbf{C}_K \otimes_K V$ is of χ-Hodge-Tate type. The χ will be dropped if it is clear from the context. (The standard case is $\chi = \varepsilon_p$.)

9.2.1 An alternative point of view

Instead of looking at the Hodge-Tate property "one twist at a time," consider the following reformulation of the Hodge-Tate condition. Let χ be a ramified character, and define $\mathrm{B_{HT}}(\chi) = \bigoplus_{n \in \mathbf{Z}} \mathbf{C}_K(\chi^n)$. Given a topological $K[\mathscr{G}]$-module V with finite K-dimension, Lemma 9.2.2 shows that there is an injection

$$\mathrm{B_{HT}}(\chi) \underset{K}{\otimes} (\mathrm{B_{HT}}(\chi) \underset{K}{\otimes} V)^{\mathscr{G}} \hookrightarrow \mathrm{B_{HT}}(\chi) \underset{K}{\otimes} V$$

which is functorial in V. Let $\underline{\mathrm{D}}_{\mathrm{HT}}^{\chi}$ denote the functor sending V to $(\mathrm{B_{HT}}(\chi) \otimes_K V)^{\mathscr{G}}$; in the case where V is a topological $\mathbf{C}_K\{\mathscr{G}\}$-module, we will write $\underline{\mathrm{D}}_{\mathrm{HT}}^{\chi}(V) = (\mathrm{B_{HT}}(\chi) \otimes_{\mathbf{C}_K} V)^{\mathscr{G}}$. In either case $\underline{\mathrm{D}}_{\mathrm{HT}}^{\chi}(V)$ is a finite-dimensional K-vector space; writing $V_{\mathbf{C}_K} = \mathbf{C}_K \otimes_K V$ when V is a K-vector space and $V_{\mathbf{C}_K} = V$ when V is a $\mathbf{C}_K$-vector space, Lemma 9.2.2 shows that $\dim_K \underline{\mathrm{D}}_{\mathrm{HT}}^{\chi}(V) \leq \dim_{\mathbf{C}_K} V_{\mathbf{C}_K}$. We see that V is χ-Hodge-Tate or χ-pre-Hodge-Tate (depending upon the scalar field) if and only if $\dim_K \underline{\mathrm{D}}_{\mathrm{HT}}^{\chi}(V) = \dim_{\mathbf{C}_K} V_{\mathbf{C}_K}$. More functorially, If $\underline{\mathrm{V}}_{\mathrm{HT}}^{\chi}$ denotes the functor $V \rightsquigarrow \mathrm{B_{HT}}(\chi) \otimes_K \underline{\mathrm{D}}_{\mathrm{HT}}^{\chi}(V)$ and B^{χ} denotes the functor $V \rightsquigarrow \mathrm{B_{HT}}(\chi) \otimes_{\mathbf{C}_K} V_{\mathbf{C}_K}$, Lemma 9.2.2 shows that there is an injection of functors $\iota : \underline{\mathrm{V}}_{\mathrm{HT}}^{\chi} \hookrightarrow \mathrm{B}^{\chi}$. The condition that V be χ-Hodge-Tate is then equivalent to the condition that $\iota(V)$ be an isomorphism.

9.2.2 Basic properties of Hodge-Tate modules

In this section, we consider the relationship between the Hodge-Tate condition and certain natural constructions of topological $\mathbf{C}_K\{\mathscr{G}\}$-modules from other topological $\mathbf{C}_K\{\mathscr{G}\}$-modules. We implicitly assume in what follows that all $\mathbf{C}_K\{\mathscr{G}\}$-modules have finite $\mathbf{C}_K$-dimension.

Given two $\mathbf{C}_K\{\mathscr{G}\}$-modules V and W, several other $\mathbf{C}_K\{\mathscr{G}\}$-modules may naturally be constructed out of them:

(i) $V^{\vee} = \mathrm{Hom}_{\mathbf{C}_K}(V, \mathbf{C}_K)$ with action $(s.\phi)(v) = s(\phi(s^{-1}(v)))$;

(ii) $V \otimes_{\mathbf{C}_K} W$ with action $s.(v \otimes w) = s(v) \otimes s(w)$ (extended by semi-linearity);

(iii) $\mathrm{Hom}_{\mathbf{C}_K}(V, W)$ with action $(s.\phi)(v) = s(\phi(s^{-1}(v)))$.

It is easy to check that the action on $V^\vee \otimes_{\mathbf{C}_K} W$ is identified with the action on $\mathrm{Hom}_{\mathbf{C}_K}(V, W)$ under the natural isomorphism $V^\vee \otimes_{\mathbf{C}_K} W \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{C}_K}(V, W)$.

Lemma 9.2.5. *Suppose V and W are topological $\mathbf{C}_K\{\mathscr{G}\}$-modules. There are natural injections*

(1) $\underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(V) \otimes \underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(W) \hookrightarrow \underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(V \otimes W)$

(2) $\underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(V)^\vee \hookrightarrow \underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(V^\vee)$

(3) $\mathrm{Hom}_K(\underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(V), \underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(W)) \hookrightarrow \underline{\mathrm{D}}^{\chi}_{\mathrm{HT}}(\mathrm{Hom}_{\mathbf{C}_K}(V, W))$.

Proof. Part (1) is clear. To prove (2), it suffices show that if $\phi \in (V^i)^\vee$ (the K-vector space dual), then ϕ naturally defines an element of $(V^\vee)^{-i}$. But this is clear by a simple computation. Part (3) follows from parts (1) and (2). □

Fix a ramified character χ. In what follows, "Hodge-Tate" will mean "χ-Hodge-Tate."

Lemma 9.2.6. *If V and W are of Hodge-Tate type, then*

(1) $V^\vee$ *is of Hodge-Tate type;*

(2) $V \otimes_{\mathbf{C}_K} W$ *is of Hodge-Tate type;*

(3) $\mathrm{Hom}_{\mathbf{C}_K}(V, W)$ *is of Hodge-Tate type.*

Proof. This is a trivial consequence of Lemma 9.2.5, and it shows the usefulness of having defined the functor $\underline{\mathrm{D}}_{\mathrm{HT}}$. □

Thus, all of the "natural constructions" preserve the Hodge-Tate condition. Here is an interesting example of a non-Hodge-Tate $\mathbf{C}_K\{\mathscr{G}\}$-module which may be constructed "non-algebraically" from one which is Hodge-Tate.

Example 9.2.7. Consider the p-adic cyclotomic character $\varepsilon_p : \mathscr{G} \to \mathbf{Z}_p^\times$. Using the p-adic logarithm, write $\mathbf{Z}_p^\times = G \times \mathbf{Z}_p$ for some finite group G (which depends upon p). Because G is finite, there is some n_p such that $\varepsilon_p^{n_p}$ takes values in the open subgroup of $\mathbf{Z}_p^\times$ isomorphic to $\mathbf{Z}_p$. Let $i \in \mathbf{Z}_p - \mathbf{Z}$, and define $\chi = (\varepsilon_p^{n_p})^i$. Form the $\mathbf{C}_K\{\mathscr{G}\}$-module $\mathbf{C}_K(\chi)$. For every integer n, $\chi\varepsilon_p^n$ remains ramified, and therefore, by Theorem 10.3.2,

$$\mathbf{C}_K(\chi)(n)^{\mathscr{G}} = \mathbf{C}_K(\chi\varepsilon_p^n)^{\mathscr{G}} = 0.$$

So, starting with a Hodge-Tate module $\mathbf{C}_K(1)$, performing a very "non-algebraic" twisting construction yields a non-Hodge-Tate module. Part II gives evidence that this unnatural construction does not arise algebro-geometrically. ◊

Proposition 9.2.8. *If V is of Hodge-Tate type then*

$$\mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V, W) \cong \prod_{i \in \mathbf{Z}} \mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V[i], W[i]) \cong \prod_{i \in \mathbf{Z}} \mathrm{Hom}_K(V^i, W^i).$$

In particular, $\dim_K \mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V, W) < \infty$.

Proof. Because $V = \bigoplus V(i)$ as $\mathbf{C}_K\{\mathscr{G}\}$-modules and only finitely many summands are non-zero, there is a natural isomorphism

$$\mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V, W) \to \prod_{i \in \mathbf{Z}} \mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V[i], W)$$

given by the product of the restriction maps $f \mapsto f|_{V[i]}$. But it is clear from $\mathbf{C}_K\{\mathscr{G}\}$-linearity that the natural injection

$$\mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V[i], W[i]) \hookrightarrow \mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V[i], W)$$

is an isomorphism.

To complete the proof, it suffices to show that the natural map

$$\mathrm{Hom}_K(V^i, W^i) \to \mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(V[i], W[i])$$

is an isomorphism, and this reduces to showing that the natural map

$$\mathrm{Hom}_K(K(\chi^i), K(\chi^i)) \to \mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(\mathbf{C}_K(\chi^i), \mathbf{C}_K(\chi^i))$$

is an isomorphism. But $\mathrm{Hom}_K(K(\chi^i), K(\chi^i))$ is just K and it is easy to see that

$$\mathrm{Hom}_{\mathbf{C}_K\{\mathscr{G}\}}(\mathbf{C}_K(\chi^i), \mathbf{C}_K(\chi^i)) = \mathbf{C}_K^{\mathscr{G}} = K$$

by Theorem 10.3.1. □

Pre-Hodge-Tate modules are not as easily classified as those of Hodge-Tate type because some information is lost upon extending scalars to $\mathbf{C}_K$, as the following example demonstrates concretely.

9.2.3 An example

In this example we work with continuous cohomology. The group $U \subset A^\times$ of *principal units* is defined to be the kernel of the reduction map $A^\times \to k^\times$.

Lemma 9.2.9. *Let $\mathscr{G}$ be a profinite group, and M a normed $\mathbf{Q}_p$-vector space with a continuous $\mathbf{Q}_p$-linear $\mathscr{G}$-action such that $\mathscr{G}$ preserves the open unit ball $N \subset M$. For all $r \geq 0$, the natural map of $\mathbf{Q}_p$-vector spaces*

$$\mathbf{Q}_p \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^r(\mathscr{G}, N) \to \mathrm{H}^r(\mathscr{G}, M)$$

is an isomorphism. In particular, $\mathrm{H}^1(\mathscr{G}, K(\chi)) = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathrm{H}^1(\mathscr{G}, A(\chi))$.

Proof. When $r = 0$, this follows from the fact that the $\mathscr{G}$-action is $\mathbf{Q}_p$-linear. Now suppose $r \geq 1$. By the compactness of $\mathscr{G}$, given any cochain $f : \mathscr{G}^r \to M$ there is some $n \geq 0$ such that the image of f lies in $\frac{1}{p^n}N$. If f is a coboundary, then there is some continuous g such that $f = \delta g$. But then, again by compactness of $\mathscr{G}$, there is some $m \geq n$ such that g takes values in $\frac{1}{p^m}N$. Thus, any element of $\mathrm{H}^r(\mathscr{G}, \frac{1}{p^n}N)$ which maps to a coboundary in M maps to one in $\frac{1}{p^m}N$ for some m. The net effect of this is that

$$\mathrm{H}^1(\mathscr{G}, M) = \varinjlim \mathrm{H}^1(\mathscr{G}, \tfrac{1}{p^n}N).$$

To prove the Lemma, it therefore suffices to show that the natural map

$$\iota : \tfrac{1}{p^n}\mathbf{Z}_p \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^1(\mathscr{G}, N) \to \mathrm{H}^r(\mathscr{G}, \tfrac{1}{p^n}N)$$

is an isomorphism. Note that every element of $\frac{1}{p^n}\mathbf{Z}_p \otimes_{\mathbf{Z}_p} \mathrm{H}^1(\mathscr{G}, N)$ may be written in the form $\frac{1}{p^n} \otimes_{\mathbf{Z}_p} [f]$ for some cocycle f (where the brackets denote the equivalence class). The map ι simply sends $\frac{1}{p^n} \otimes_{\mathbf{Z}_p} [f]$ to $[\frac{1}{p^n} f]$. If there is some $\frac{1}{p^n}N$-valued continuous $(r+1)$-cochain g such that $\frac{1}{p^n} f = \delta g$, then $f = \delta(p^n g)$, and therefore $[f] = 0$, so ι is injective. On the other hand, given an r-cocycle $f : \mathscr{G}^r \to \frac{1}{p^n}N$, $[f] = \iota(\frac{1}{p^n} \otimes_{\mathbf{Z}_p} [p^n f])$, and therefore ι is surjective. □

Lemma 9.2.10. *Let N be a topological $\mathbf{Z}_p[\mathscr{G}]$-module which is linearly topologized and complete as a $\mathbf{Z}_p$-module. Suppose there is a countable cofinal set $N_1 \supset N_2 \supset \cdots$ of open submodules, each of which is stabilized by $\mathscr{G}$. For any $r \geq 1$, if $\mathrm{H}^{r-1}_{\mathrm{disc}}(\mathscr{G}, N/N_i) = 0$ for all i then natural map of $\mathbf{Z}_p$-modules*

$$\phi : \mathrm{H}^r(\mathscr{G}, N) \to \varprojlim \mathrm{H}^r_{\mathrm{disc}}(\mathscr{G}, N/N_i)$$

is an isomorphism.

Proof. If (f_i) is a representative of an element of the inverse limit, then there is a coboundary g such that $f_2(s) \equiv f_1(s) + g(s) \pmod{N_1}$ for all s. Replacing f_2 by $f_2 - g$ and continuing inductively in this manner produces a system of cochains representing the same element in the inverse system of cohomology groups such that for all $i > j$ and all $s \in \mathscr{G}$, $f_i(s) \equiv f_j(s) \pmod{N_j}$. By the completeness of N, there is a cochain $f : \mathscr{G} \to N$ such that $f \equiv f_i \pmod{N_i}$ for all i. Because N is separated, f satisfies the cocycle condition and therefore $\phi([f]) = (f_i)$.

Furthermore, we claim that if a cochain f is a coboundary modulo N_i for all i then it is a coboundary. Indeed, suppose $f \equiv \delta g_i \pmod{N_i}$ for some coboundaries δg_i. By assumption, we see that $g_2 \equiv g_1 + \delta f_1 \pmod{N_1}$ for some cochain f_1. Replacing g_2 by $g_2 - \delta f_1$ yields a cochain g_2' such that $g_2' \equiv g_1 \pmod{N_1}$ and $\delta g_2' = \delta g_2 \equiv f \pmod{N_2}$. Continuing in this manner (and renaming) produces a system of cochains g_i such that $g_{i+1} \equiv g_i \pmod{N_i}$ and $f \equiv \delta g_i \pmod{N_i}$ for all i. By completeness there is some cochain $g : \mathscr{G}^r \to N$ such that $f \equiv \delta g \pmod{N_i}$ for all i, which means that $f = \delta g$ by separatedness. Thus, ϕ is injective. □

Remark 9.2.11. We will only apply Lemma 9.2.10 in the case where $r = 1$, and in our application the vanishing of the discrete zeroth cohomology is clear. ♦

Lemma 9.2.12. *There is a natural short exact sequence of K-vector spaces*

$$0 \to K \underset{\mathbf{Z}_p}{\otimes} U \to \mathrm{H}^1(\mathscr{G}, K(1)) \to K \to 0.$$

In particular, $\mathrm{H}^1(\mathscr{G}, K(1)) \neq 0$.

Proof. By Lemma 9.2.9,

$$\mathrm{H}^1(\mathscr{G}, K(1)) = \mathbf{Q}_p \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^1(\mathscr{G}, A(1)).$$

Furthermore, since A is finite and free over $\mathbf{Z}_p$, it is easy to see that the natural map

$$A \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^1(\mathscr{G}, \mathbf{Z}_p(1)) \to \mathrm{H}^1(\mathscr{G}, A(1))$$

is an isomorphism (recall that $\mathscr{G}$ is the Galois group of K, not of $\mathbf{Q}_p$). Finally, Lemma 9.2.10 shows that

$$\mathrm{H}^1(\mathscr{G}, \mathbf{Z}_p(1)) \cong \varprojlim \mathrm{H}^1(\mathscr{G}, \mathbf{Z}_p(1)/p^n\mathbf{Z}_p(1)) = \varprojlim \mathrm{H}^1(\mathscr{G}, \boldsymbol{\mu}_{p^n}).$$

By Kummer Theory, there is an isomorphism

$$K^\times/(K^\times)^{p^n} \to \mathrm{H}^1(\mathscr{G}, \boldsymbol{\mu}_{p^n})$$

which is compatible with the quotient maps in the system $K^\times/(K^\times)^{p^n}$ and the maps $\boldsymbol{\mu}_{p^n} \to \boldsymbol{\mu}_{p^{n-1}}$ induced by the pth power map. On the other hand, there is an inverse system of short exact sequences

$$1 \to U/U^{p^n} \to K^\times/(K^\times)^{p^n} \to \mathbf{Z}/p^n\mathbf{Z} \to 0$$

with surjective transition maps. Passing the inverse limit and using the Mittag-Lefler condition gives an exact sequence

$$1 \to U \to \mathrm{H}^1(\mathscr{G}, \mathbf{Z}_p(1)) \to \mathbf{Z}_p \to 0$$

of $\mathbf{Z}_p$-modules. Now, $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} A = K$, so the Lemma follows by flatness after tensoring through with K. □

It is now possible to give an indication of how much information gets lost by extending scalars on a pre-Hodge-Tate $K[\mathscr{G}]$-module. Choose a continuous 1-cocycle $c : \mathscr{G} \to K(1)$ which represents a non-trivial cohomology class (cf. Lemma 9.2.12). Let V be a two-dimensional K-space with a fixed basis e_1, e_2, and let $\mathscr{G}$ act by the matrices

$$\begin{pmatrix} \varepsilon_p & c \\ 0 & \mathbf{1} \end{pmatrix}.$$

Since c is a continuous cocycle, this gives a continuous left action of $K[\mathscr{G}]$ on V. The topological exact sequence of $K[\mathscr{G}]$-modules

$$S : 0 \to \varepsilon_p \to V \to \mathbf{1} \to 0$$

is non-split, for otherwise c would be a continuous coboundary. Upon extending scalars to $\mathbf{C}_K$, Theorem 10.3.2 below shows that the sequence S *splits*, and therefore V is pre-Hodge-Tate.

Thus, even though V (over K) may not may not have an especially obvious structure, its isomorphism class after extending scalars to $\mathbf{C}_K$ is uniquely determined by the sequence of numbers which may be read off after twisting $\mathbf{C}_K \otimes_K V$ by various powers of ε_p. However, such a massive scalar extension has disadvantages (cf. Proposition 10.3.4 and Remark 10.3.7), and it would be nice to find a refinement of the Hodge-Tate condition.

Proving the results used in Section 9.2 will occupy the remainder of this Part.

10 The $\mathscr{G}$-action on $\mathbf{C}_K$

10.1 Analysis of $\mathbf{Z}_p$-extensions

10.1.1 Existence of $\mathbf{Z}_p$-extensions

Definition 10.1.1. A $\mathbf{Z}_p$-*extension* of a field E is a Galois extension L/E with Galois group topologically isomorphic to $\mathbf{Z}_p$.

As usual, given a $\mathbf{Z}_p$-extension E_∞/E, the filtration $\mathbf{Z}_p \supset p\mathbf{Z}_p \supset p^2\mathbf{Z}_p \supset \cdots \supset 0$ corresponds to a tower $E = E_0 \subset E_1 \subset \cdots \subset E_\infty$ of fixed fields. By infinite Galois theory this tower is in fact the complete lattice of finite sub-extensions of K_∞, all of which are Galois because every subgroup of an abelian group is normal. The fact that this lattice is a chain implies that every $\mathbf{Z}_p$-extension is either unramified or corresponds to a finite unramified extension followed by *a totally ramified* $\mathbf{Z}_p$-*extension*, since $p^n\mathbf{Z}_p \cong \mathbf{Z}_p$.

Lemma 10.1.2. *Let $F \hookrightarrow L$ be an isometric embedding of local fields of residue characteristic $p > 0$. If F_∞ is a ramified $\mathbf{Z}_p$-extension of F, then the quotient fields of $F_\infty \otimes_F L$ by its maximal ideals are ramified $\mathbf{Z}_p$-extensions of L.*

Proof. Fixing algebraic closures $\overline{F}$ of F and $\overline{L}$ if L, it suffices to prove that for (necessarily isometric) embeddings $F_\infty \hookrightarrow \overline{F} \hookrightarrow \overline{L}$, the compositum $F_\infty L$ has Galois group $\mathbf{Z}_p$. Because L is a local field, the ramification index of L/F is finite, and this implies that $L \cap F_\infty = F_n$ for some $n < \infty$ because F_∞/F is ramified. But then L and F_∞ are linearly disjoint over F_n, so there is a topological isomorphism

$$\mathrm{Gal}(F_\infty L/L) = \mathrm{Gal}(F_\infty/F_n) \cong \mathbf{Z}_p.$$

It is clear that $F_\infty L/L$ must be ramified. □

By standard results [10, Chapter II, §5], there is a local field F of absolute ramification index 1 such that K is a finite totally ramified extension of F. To establish the existence of a ramified $\mathbf{Z}_p$-extension of K, it suffices by Lemma 10.1.2 to find a ramified $\mathbf{Z}_p$-extension for local fields of absolute ramification index 1.

Lemma 10.1.3. *If F is a local field of absolute ramification index 1, then F admits a ramified $\mathbf{Z}_p$-extension. In fact, the p-adic cyclotomic character ε_p is ramified.*

Proof. Let $F(\boldsymbol{\mu}_{p^\infty})$ denote the totally ramified extension of F given by adjoining all p-power roots of unity. It is easy to prove using the Eisenstein irreducibility criterion that the cyclotomic polynomials $\Phi_{p^n}(x)$ are irreducible over F. An elementary order calculation then shows that $\mathrm{Gal}(F(\boldsymbol{\mu}_{p^n})/F) \cong (\mathbf{Z}_p/p^n\mathbf{Z}_p)^\times$, which in turn implies that there is a topological isomorphism $\mathrm{Gal}(F(\boldsymbol{\mu}_{p^\infty})/F) \cong \mathbf{Z}_p^\times$. Using the p-adic logarithm shows that there is a canonical continuous split surjection $\mathbf{Z}_p^\times \to \mathbf{Z}_p$ with finite kernel. Thus, $F(\boldsymbol{\mu}_{p^\infty})/F$ is finite over a totally ramified $\mathbf{Z}_p$-extension (the *cyclotomic* $\mathbf{Z}_p$-*extension*) of F.

On the other hand, the restriction map $\mathscr{G} \to \mathrm{Gal}(F(\boldsymbol{\mu}_{p^\infty})/F) = \mathbf{Z}_p^\times$ is just the p-adic cyclotomic character, and the splitting of the surjection $\mathbf{Z}_p^\times \to \mathbf{Z}_p$ shows that the fixed field of $\ker \varepsilon_p$ is a totally ramified $\mathbf{Z}_p$-extension of a finite subextension, i.e., that ε_p is ramified. (That $\varepsilon_p|_{\mathrm{Gal}(\overline{K}/K)}$ is ramified follows because $\mathrm{Gal}(\overline{K}/K)$ is an open subgroup of $\mathrm{Gal}(\overline{K}/F)$.) □

Remark 10.1.4. It is not too hard to verify that $F(\boldsymbol{\mu}_{p^\infty}) \cong F \otimes_{\mathbf{Q}_p} \mathbf{Q}_p(\boldsymbol{\mu}_{p^\infty})$, and that the $\mathbf{Z}_p$-extension F_∞ constructed in Lemma 10.1.3 is just tensor product over $\mathbf{Q}_p$ of F with the subextension $\mathbf{Q}_p^{\text{cycl}} \subset \mathbf{Q}_p(\boldsymbol{\mu}_{p^\infty})$ given by the p-adic logarithm, as in Lemma 10.1.3. The $\mathbf{Z}_p$-extensions of K coming from F_∞ are just the factor fields of the finite $\mathbf{Q}_p^{\text{cycl}}$-algebra $K \otimes_{\mathbf{Q}_p} \mathbf{Q}_p^{\text{cycl}}$. ♦

10.1.2 The absolute trace

Further study of $\mathbf{Z}_p$-extensions requires some tools constructed by local class field theory. Fix a $\mathbf{Z}_p$-extension K_∞/K. The goal of this section is to construct a continuous function from K_∞ to K, the *absolute trace*, which will be useful in computing cohomology for $\mathfrak{g} = \mathrm{Gal}(K_\infty/K)$ acting on the completion X of K_∞. Denote the fixed field of $p^n\mathbf{Z}_p \subset \mathfrak{g}$ by K_n and let $A_n \subset K_n$ be the ring of integers, with maximal ideal $\mathfrak{m}_n$. Let $\mathfrak{D}_n = \mathfrak{D}_{K_n/K}$ denote the different of A_{K_n} over A; this is an ideal of A_{K_n}. Where necessary, σ denotes a topological generator of the Galois group $\mathfrak{g} = \mathbf{Z}_p$. In what follows, the valuation v is taken to be normalized on the base field K.

Definition 10.1.5. Let L be a field of characteristic 0 and let L_∞/L be an algebraic extension. Given $\alpha \in L_\infty$, define *the absolute trace* associated to L_∞/L to be

$$t(\alpha) = \frac{1}{[L' : L]} \operatorname{Tr}_{L'/L}(\alpha),$$

where L' is any finite subextension of L_∞/L containing α. By transitivity of the trace, $t(\alpha)$ is independent of the choice of L' and is an L-linear operator on L_∞.

Proposition 10.1.6. *There a constant c (independent of n) and a bounded sequence (a_n) such that $v(\mathfrak{D}_n) = (en + c + p^{-n}a_n) \cdot \epsilon$, where $\epsilon = 1$ if K_∞/K is ramified and $\epsilon = 0$ otherwise.*

Proof. When K_∞/K is unramified, the result is clear. Suppose that the extension is ramified. Passing to a finite subextension (and adjusting finitely many of the constants a_n), we may assume by the transitivity of the different that K_∞/K is totally ramified.

If L/K is finite, recall the formula [10, p. 64]

$$v_K(\mathfrak{D}_{L/K}) = e_{L/K}^{-1} \sum_{i=0}^{\infty} (|G_i| - 1), \tag{10.1.1}$$

where (G_i) is the sequence of ramification groups contained in the Galois group $G = \mathrm{Gal}(L/K)$ and $e_{L/K}$ is the ramification index of L/K. For our purposes, the "upper numbering" of the ramification groups [10, Chapter IV] is more useful because of its compatibility with quotients. To rewrite this formula using the upper numbering we use calculus. If ψ is the Herbrand function, so that $G^\mu = G_{\psi(\mu)}$, we know that outside of a discrete set ψ is differentiable with derivative $[G^0 : G^\mu]$. Equation (10.1.1) can be written as the integral

$$v_K(\mathfrak{D}_{L/K}) = e \int_{-1}^{\infty} (|G_\nu| - 1)\, d\nu,$$

and making the change of variable $\nu = \psi(\mu)$ yields

$$\begin{aligned} v_K(\mathfrak{D}_{L/K}) &= e^{-1} \int_{-1}^{\infty} (|G^{\mu}| - 1) \frac{|G^0|}{|G^{\mu}|}\, d\mu \\ &= e^{-1} \int_{-1}^{\infty} \left(1 - \frac{1}{|G^{\mu}|}\right) |G^0|\, d\mu. \end{aligned}$$

In the case where $L = K_n$, the ramification assumption on K_∞ means that $|G^0| = e$, so

$$v_K(\mathfrak{D}_n) = \int_{-1}^{\infty} \left(1 - \frac{1}{|G^{\mu}|}\right) d\mu. \tag{10.1.2}$$

The integrand is a step function, so to integrate it we need to determine where the jumps occur. The fundamental result in this direction is the Hasse-Arf Theorem, which states that the jumps occur at integer values. Since K_∞/K is a $\mathbf{Z}_p$-extension, $\mathfrak{g}_n = \mathrm{Gal}(K_n/K) = \mathbf{Z}/p^n\mathbf{Z}$. By the definition of the upper numbering (and the obvious inverse limits), $\mathfrak{g}^{\mu}\mathfrak{g}_n = \mathfrak{g}_n^{\mu}$. Let t_m denote the integer where the upper ramification jumps from $p^{m-1}\mathfrak{g}$ to $p^m\mathfrak{g}$. If $t_{m+1} - t_m = e$ for sufficiently large m, then for $t_0 = -1$ and $n > m$ we have

$$\begin{aligned} v(\mathfrak{D}_n) &= (t_1 - t_0)\left(1 - \frac{1}{p^n}\right) + (t_2 - t_1)\left(1 - \frac{1}{p^{n-1}}\right) + \cdots \\ &\qquad + e\left(1 - \frac{1}{p^{n-m}} + 1 - \frac{1}{p^{n-m-1}} + \cdots + 1 - \frac{1}{1}\right) \\ &= (t_m - t_0) - \left((t_1 - t_0)\frac{1}{p^n} + \cdots (t_m - t_{m-1})\frac{1}{p^{n-m+1}}\right) + \\ &\qquad en - em - e\left(\frac{1}{p^{n-m}} + \frac{1}{p^{n-m-1}} + \cdots + 1\right) \\ &= en + \left(t_m - t_0 - em - e\frac{p}{p-1}\right) + \\ &\qquad p^{-n}\left(e\frac{p^{m+2}}{p-1} + (t_1 - t_0) + \frac{1}{p}(t_2 - t_1) + \cdots + \frac{1}{p^{m+1}}(t_m - t_{m-1})\right) \\ &= en + c + p^{-n}a_n. \end{aligned} \tag{10.1.3}$$

When $n \le m$, this calculation is nonsense, but for those finitely many values we may adjust the a_n to make the formula valid.

Thus, to establish the Proposition, it suffices to demonstrate that the distance $t_m - t_{m-1}$ between the jumps "stabilizes" to e as m increases. The proof given below works in the case where the residue field of K is finite. Other cases may be deduced from the case of an algebraically closed residue field (Serre's "geometric local class field theory") after changing the base to the completion of the maximal unramified extension of K (recall that K_∞/K is totally ramified). The methods for handling this case will not be touched upon in this thesis.

By the assumption that the residue field k is finite, it is easy to see that K is a finite extension of $\mathbf{Q}_p$ with ramification index e, the absolute ramification index of K. If π is a uniformizer for A_K and α is a lift of a generator for k over $\mathbf{F}_p$ then A_K is a free $\mathbf{Z}_p$-module with basis $\{\alpha^i\pi^j : 0 \le i \le f-1, 0 \le j \le e-1\}$, where $f = [k : \mathbf{F}_p]$.

The reciprocity isomorphism of local class field theory can be used to relate the natural filtration $U_K^m = 1 + \pi^m A_K$ of the group of units $A_K^\times$ with the filtration of $\mathfrak{g}$ by the sequence of ramification groups with the upper numbering. In particular, U_K^m is taken onto $\mathfrak{g}^m$ [10, Chapter XV, §2, Theorem 2]. On the other hand, for $m > e/(p-1)$, the (isometric) p-adic logarithm yields an isomorphism $U_K^m \cong A_K$ such that the filtration $U_K^m \supset U_K^{m+1} \supset \cdots$ corresponds to the filtration $A_K \supset \pi A_K \supset \pi^2 A_K \supset \cdots$. Since $\mathfrak{g}^m \cong \mathfrak{g}$, for large enough m the reciprocity isomorphism is identified with a continuous surjection $f : A_K \twoheadrightarrow \mathbf{Z}_p$.

Let g_{ij} denote the basis element $\alpha^i\pi^j$ for A_K over $\mathbf{Z}_p$. The index j will be taken from the set $\{0, 1, \ldots, e-1\}$, viewed as representatives for $\mathbf{Z}/e\mathbf{Z}$. It is clear that $\pi g_{ij} = p^\varepsilon g_{i,j+1}$, where $\varepsilon = \lfloor (j+1)/e \rfloor$. If j_0 is the minimal index such that there is some i_0 with $f(g_{i_0,j_0}) \notin p\mathbf{Z}_p$, then replacing A_K by $\pi^{j_0}A_K$ and rescaling, we may clearly assume that there is some i_0 such that $f(g_{i_0,0}) \notin p\mathbf{Z}_p$. But then $f(\pi^j A) = p\mathbf{Z}_p$ for all $j = 1, \ldots, e$ because $\pi^j g_{i,-j} = pg_{i,0}$, and $f(pg_{i_0,0}) \notin p^2\mathbf{Z}_p$ for $j = e$. Rescaling and proceeding inductively shows that the remaining jumps in the ramification filtration are equally spaced e integers apart. □

Corollary 10.1.7. *The absolute trace is continuous.*

Proof. By linearity, it suffices to produce a constant λ such that $|t(x)| \le \lambda|x|$ for all $x \in K_\infty$. The estimate established in Proposition 10.1.6 shows that $v(\mathfrak{D}_{K_{n+1}/K_n}) = (e + p^{-n}b_n)\cdot\epsilon$, where ϵ is 0 or 1 depending upon ramification. Given fractional ideals $\mathfrak{a} \subset K_{n+1}$ and $\mathfrak{b} \subset K_n$, $\mathrm{Tr}_{K_{n+1}/K_n}(\mathfrak{a}) \subset \mathfrak{b}$ if and only if $\mathfrak{a} \subset \mathfrak{b}\mathfrak{D}^{-1}_{K_{n+1}/K_n}$. Hence, if $\mathfrak{D}_{K_{n+1}/K_n} = \mathfrak{m}_{n+1}^d$ then $\mathrm{Tr}_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}_n^j$, where $j = \lceil (i+d)/p \rceil$ [10, Chapter III, §3, Prop. 7]. It is easy to see that given any constant B, there is an $a < 0$ such that

$$ep^{n+1}(1 - ap^{-n}) + i \ge \frac{i+e+B}{p} + 1 \ge \left\lceil \frac{i+e+B}{p} \right\rceil \tag{10.1.4}$$

for all n. Since b_n is bounded, say by B, and $(p) = \mathfrak{m}_\ell^{ep^\ell}$, (10.1.4) shows that

$$|\,\mathrm{Tr}_{K_{n+1}/K_n}(x)| \le |p|^{1-ap^{-n}}|x| \tag{10.1.5}$$

for all $x \in K_{n+1}$. (Using $-e$ for B shows (10.1.5) for the unramified case, i.e., $\epsilon = 0$.) Letting $c = ap/(p-1)$ and using transitivity of the trace, we find that

$$|\,\mathrm{Tr}_{K_n/K}(x)| \le |p|^{n-c}|x|$$

for all $x \in K_n$, so taking $\lambda = |p|^{-c}$ shows that $|t(x)| \le \lambda|x|$. □

Corollary 10.1.8. *There is a constant $d > 0$ such that for all $x \in K_\infty$ and all $n \ge 0$,*

$$|x - p^n t(x)| \le d|\sigma^{p^n}x - x|. \tag{10.1.6}$$

Proof. It will suffice to prove the Corollary for σ as long as d is independent of n. This corresponds to replacing K by K_n as the base field, making this result "base field independent."

The first thing we will prove is an "approximation" of (10.1.6): there is a constant c independent of n such that for $x \in K_{n+1}$,

$$|x - p^{-1}\operatorname{Tr}_{K_{n+1}/K_n}(x)| \le c|\sigma^{p^n}x - x|. \tag{10.1.7}$$

Writing $\tau = \sigma^{p^n}$, we have

$$px - \operatorname{Tr}_{K_{n+1}/K_n}(x) = px - \sum_{i=0}^{p-1}\tau^i x = \sum_{i=0}^{p-1}(1-\tau^i)x.$$

But $(1-\tau)$ divides $(1-\tau^i)$ for every $i \ge 1$ (and the $i = 0$ term vanishes), so the right side is a sum of conjugates of $(1-\tau)x$. Since all conjugates of $(1-\tau)x$ have the same valuation it follows by the ultrametric property that $|px - \operatorname{Tr}_{K_{n+1}/K_n}(x)| \le |(1-\tau)x|$, so one can even take $c = |p|^{-1}$ in (10.1.7).

The proof of the Corollary follows by an induction from the first-order approximation (10.1.7). More precisely, induction will furnish a sequence c_n such that for $x \in K_n$,

$$|x - t(x)| \le c_n|\sigma x - x|. \tag{$S(n)$}$$

The constants c_n will satisfy the recursion $c_{n+1} = |p^{-ap^{-n}}|c_n$ for some $a < 0$ which does not depend on n. Taking $d = |p|^{-1-ap/(p-1)}$ completes the proof.

Letting $c_1 = |p|^{-1}$ and using (10.1.7) proves $S(1)$. Suppose $S(n)$ holds. Given $x \in K_{n+1}$, observe that $t(\operatorname{Tr}_{K_{n+1}/K_n}(x)) = t(x)$. Thus, by (10.1.5) in the proof of Corollary 10.1.7, there is some $a < 0$ such that

$$\begin{aligned} |\operatorname{Tr}_{K_{n+1}/K_n}(x) - pt(x)| &\le c_n|\sigma \operatorname{Tr}_{K_{n+1}/K_n}(x) - \operatorname{Tr}_{K_{n+1}/K_n}(x)| \\ &= c_n|\operatorname{Tr}_{K_{n+1}/K_n}(\sigma x - x)| \\ &\le c_n|p|^{1-ap^{-n}}|\sigma x - x|, \end{aligned} \tag{10.1.8}$$

Write $x - t(x) = x - p^{-1}\operatorname{Tr}_{K_{n+1}/K_n}(x) + p^{-1}\operatorname{Tr}_{K_{n+1}/K_n} - t(x)$. Using the ultrametric property and applying (10.1.7) and (10.1.8) yields

$$\begin{aligned} |x - t(x)| &\le \max(|x - p^{-1}\operatorname{Tr}_{K_{n+1}/K_n}(x)|, |p|^{-ap^{-n}}c_n|\sigma x - x|) \\ &\le \max(c_1, |p|^{-ap^{-n}}c_n)|\sigma x - x| \\ &= |p|^{-ap^{-n}}c_n|\sigma x - x|, \end{aligned}$$

the final step following from the inequality $\prod_{i=2}^n |p|^{-ap^{-i}} \ge 1$, which holds because $a < 0$. Thus, $S(n+1)$ holds. □

10.1.3 The completion of a $\mathbf{Z}_p$-extension and its cohomology

In the usual way, the isometric action of $\mathfrak{g}$ on K_∞ extends to an action on the completion X of K_∞ with respect to the valuation metric. We will now use the continuity of the absolute trace to study the cohomology of this action.

Theorem 10.1.9. *Let $\chi : \mathfrak{g} \to K^\times$ be a character of $\mathfrak{g}$.*

(1) $\mathrm{H}^0(\mathfrak{g}, X) = K$ *and* $\dim_K \mathrm{H}^1(\mathfrak{g}, X) = 1$;

(2) *If $\chi(\mathfrak{g})$ is infinite, then* $\mathrm{H}^0(\mathfrak{g}, X(\chi)) = 0 = \mathrm{H}^1(\mathfrak{g}, X(\chi))$.

The proof relies heavily on Corollary 10.1.7 to study the linear operators $\sigma - 1$ and $\sigma - \lambda$ on X, where λ is a principal unit of A_K which is not a root of unity:

Lemma 10.1.10. *Let $X_0 \subset X$ be the kernel of the absolute trace t and let λ be a principal unit of A_X which is not a root of unity.*

(1) $X = X_0 \oplus K$ *as topological $K[\mathfrak{g}]$-modules;*

(2) $K = \ker(\sigma - 1)$ *and $\sigma - 1$ has a continuous inverse on X_0;*

(3) *$\sigma - \lambda$ has a continuous inverse on X.*

Proof. (1) We simply note that $t : X \to K$ is a continuous $\mathscr{G}$-equivariant surjection.

(2) That $\sigma - 1$ annihilates K is trivial. It remains to prove that $\sigma - 1$ has a continuous inverse on X_0. Consider the subspaces $K_{n,0} = K_n \cap X_0$ consisting of the trace zero elements of each K_n. Letting $K_{\infty,0} = \cup K_{n,0} = K_\infty \cap X_0$, it is easy to see as in (1) that $K_n = K \oplus K_{n,0}$ for $0 \le n \le \infty$, and that all such decompositions are compatible with the natural injections $K_n \hookrightarrow K_{n+1}$.

Because $\operatorname{char} K = 0$, $\sigma - 1$ is injective on each $K_{n,0}$, and therefore invertible on each $K_{n,0}$ because $\dim_K K_{n,0} < \infty$. Thus, $\sigma - 1$ is invertible on $K_{\infty,0}$. Furthermore, Corollary 10.1.8 shows that the inverse ρ of $\sigma - 1$ is continuous on $K_{\infty,0}$, because $|\rho(x)| \le d|x|$ for some d independent of x. If we can show that $K_{\infty,0}$ is dense in X_0, then ρ will extend to a continuous inverse to $\sigma - 1$ on all of X_0.

Given $\alpha_\infty \in X_0$, choose a Cauchy sequence (α_n) in K_∞ tending to α_∞. Write $\alpha_m = \beta_m + \gamma_m$ with $\beta_m \in K$ for all $0 \le m \le \infty$, $\gamma_m \in K_{\infty,0}$ for $m < \infty$, and $\gamma_\infty \in X_0$. We claim that $\beta_n \to \beta_\infty$ and $\gamma_n \to \gamma_\infty$. Indeed, $t(\alpha_\infty) = t(\beta_\infty) = \beta_\infty$ and $t(\alpha_n) = t(\beta_n) = \beta_n$. Since $\alpha_n \to \alpha_\infty$, continuity of t shows that $\beta_n \to \beta$. Thus, $\gamma_n \to \gamma$. Applying this to $\alpha \in X_0$ shows that $\beta_n \to 0$ and $\gamma_n \to \alpha$, which means that $K_{\infty,0}$ is dense in X_0.

(3) For $\lambda \ne 1$, $\sigma - \lambda$ is trivially bijective on K. Thus, it remains to show that $\sigma - \lambda$ has a continuous inverse on X_0.

As in (2), if ρ denotes the inverse to $\sigma - 1$ on X_0, then

$$(\sigma - \lambda)\rho = ((\sigma - 1) - (\lambda - 1))\rho = 1 - (\lambda - 1)\rho.$$

Choose d such that for all x, $|\rho(x)| \le d|x|$. If $|\lambda - 1|d < 1$ then $|(\lambda - 1)\rho(y)| < |y|$, which means that $1 - (\lambda - 1)\rho$ acts as an isometry. Hence, $1 - (\lambda - 1)\rho$ has a continuous inverse, and therefore so does $\sigma - \lambda$.

When $|\lambda - 1|$ is too large (i.e., $\ge 1/d$), we use the fact that λ is a principal unit. Writing $\lambda = 1 + \pi^\ell \alpha$ shows that $|\lambda^{p^n} - 1|$ may be made arbitrarily small.

In fact, for some n, $|\lambda^{p^n} - 1|d < 1$. Furthermore, because λ is not a root of unity, $\lambda^{p^n} \neq 1$. In this case, replacing the base field by K_n and σ by σ^{p^n}, the base field independence of Corollary 10.1.8 allows us to reason as we did when $|\lambda - 1|d < 1$ to conclude that $\sigma^{p^n} - \lambda^{p^n}$ has a continuous inverse on X_0. Writing $\sigma^{p^n} - \lambda^{p^n} = (\sigma - \lambda)f(\sigma)$, where f is a polynomial with coefficients in $\mathbf{Z}$, we see that $\sigma - \lambda$ has a continuous inverse on X_0.

□

Proof of Theorem 10.1.9. Let $\lambda = \chi(\sigma^{-1})$. If Y is a $\mathfrak{g}$-stable subspace of X, then $\mathrm{H}^0(\mathfrak{g}, Y(\chi)) = \ker(\sigma - \lambda)$. Indeed, one inclusion is obvious. In the other direction, if $y \in \ker(\sigma - \lambda)$, then $\sigma(y) = \lambda y$, so $\chi(\sigma)\sigma(y) = \sigma.y = y$ and y is a fixed point for σ (with the twisted action). Thus,

$$\sigma^\ell.y = \chi(\sigma^\ell)\sigma^\ell(y) = \chi(\sigma^\ell)\lambda^\ell y = y$$

for all ℓ. By Lemma 9.1.1, the action $\mathfrak{g} \times Y \to Y$ is continuous, so $s.y = y$ for all $s \in \mathfrak{g}$ because $\langle\sigma\rangle$ is dense in $\mathfrak{g}$.

Similarly, by continuity, any (continuous!) 1-cocycle of $\mathfrak{g}$ is determined by its value at σ, and therefore there is a K-linear injection

$$\phi : \mathrm{Z}^1(\mathfrak{g}, Y(\chi)) \to Y(\chi).$$

If $\alpha = \sigma(\beta) - \lambda\beta \in \mathrm{im}(\sigma - \lambda)$, then applying ϕ to the 1-cocycle $f(s) = s.(\lambda\beta) - \lambda\beta$ yields α. On the other hand, if $f(s) = s.\beta - \beta$ is a 1-cocycle, then $f(\sigma) = \sigma(\lambda\beta) - \beta = \lambda^{-1}(\sigma(\beta) - \lambda\beta)$, so $\phi(\lambda f) = \sigma(\beta) - \lambda\beta$. Therefore,

$$\phi|_{\mathrm{B}^1(\mathfrak{g}, Y(\chi))} : \mathrm{B}^1(\mathfrak{g}, Y(\chi)) \xrightarrow{\sim} \mathrm{im}(\sigma - \lambda),$$

and thus ϕ induces an identification of $\mathrm{H}^1(\mathfrak{g}, Y(\chi))$ with a K-subspace of $\mathrm{coker}(\sigma - \lambda)$.

By Lemma 10.1.10(2), for $\lambda = 1$ (the untwisted action) and $Y = X$, $\ker(\sigma - 1) = K$ and $\mathrm{coker}(\sigma - 1) = K$. Thus, $\mathrm{H}^0(\mathfrak{g}, X) = K$ and $\dim_K \mathrm{H}^1(\mathfrak{g}, X) = 1$ because $\dim_K \mathrm{coker}(\sigma - 1) = 1$ and the "identity" mapping $\chi : \mathfrak{g} \to \mathbf{Z}_p \subset K$ yields a continuous non-zero additive character of $\mathfrak{g}$. (That the cohomology class of χ is non-vanishing follows from the fact that $\mathrm{im}(\sigma - 1) \cap K = 0$.) Thus, (1) is proven.

To prove (2), note that if $\chi(\mathfrak{g})$ is infinite, then $\lambda = \chi(\sigma^{-1})$ cannot possibly be a root of unity. Furthermore, λ must actually be a principal unit. To see this, note that the reduction map $A^\times \to k^\times$ is continuous from the valuation topology to the discrete topology. Thus, the composite $\mathfrak{g} \to k^\times$ must be continuous from the profinite topology to the discrete topology. If the kernel is a proper open subgroup, then the image is isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$ for some $n > 0$. But $\mathrm{char}\, k = p$, so any finite subgroup of $k^\times$ has order prime to p. Thus, $\mathfrak{g} \to k^\times$ must send all of $\mathfrak{g}$ to $1 \in k^\times$, and this says precisely that $\chi(\sigma)$ is a principal unit. Therefore, by Lemma 10.1.10(3), $\mathrm{H}^0(\mathfrak{g}, X(\chi)) = 0 = \mathrm{H}^1(\mathfrak{g}, X(\chi))$. □

Remark 10.1.11. None of the results of Section 10.1 require any ramification hypotheses on K_∞/K. For an application of Theorem 10.1.9 which requires that K_∞ be *unramified*, see Proposition 10.3.5. ♦

10.2 Translating the base field by a $\mathbf{Z}_p$-extension

10.2.1 The use of ramification

While the results of Section 10.1.3 do not require ramification in the $\mathbf{Z}_p$-extension K_∞, the rest of our results use ramification in an essential way. Thus, for the remainder of Part III, K_∞ will be a *ramified* $\mathbf{Z}_p$-extension of K. Such a K_∞ exists by Section 10.1.1.

The goal of this section is to study what remains of the extension $\mathbf{C}_K/K$ over K_∞, or more precisely to study $\mathbf{C}_K/X$. The methods will again be based upon skillful approximation. Let $\mathscr{H} = \mathrm{Gal}(\overline{K}/K_\infty)$. Instead of considering $\mathbf{C}_K$ directly, we will use ramification to demonstrate that the continuous cohomology of $\mathscr{H}$ with coefficients in $\mathbf{C}_K$ is adequately approximated by the discrete cohomology with coefficients in $\overline{K}$. In some sense, we are rescuing the usual use of inflation from finite stages in the study of Galois cohomology.

Lemma 10.2.1. *If M is a direct limit of fields M_i, then for any finite extension F of M, there is some index i and some finite extension F_i/M_i such that $F_i \otimes_{M_i} M \cong F$. In particular, F_i and M are linearly disjoint over M_i.*

Proof. Write $F = M[x_1, \dots, x_n]/I$, where I is a finitely generated ideal. Fixing a finite set of generators $g_1, \dots, g_m$ for I, the coefficients of the g_j all lie in some M_i because $M = \varinjlim M_i$. Thus, writing $F_i = M_i[x_1, \dots, x_n]/(g_1, \dots, g_m)$, we see that $M \otimes_{M_i} F_i = F$ is a field. But extensions of fields are faithfully flat, so F_i must also be a field, linearly disjoint from M over M_i. We easily note in passing that F_i is separable over M_i if F is separable over M, and F_i may be taken to be Galois over M_i if F is Galois over M. □

Now let L be a finite extension of K_∞. The ring of integers of K_∞ will be denote A_∞, with maximal ideal $\mathfrak{m}_\infty$.

Lemma 10.2.2. $\mathrm{Tr}_{L/K_\infty}(A_L) \supset \mathfrak{m}_\infty$.

Proof. By the transitivity of the trace, if the Lemma is true after enlarging L to a finite Galois extension, it is certainly true for arbitrary L. Thus, we may assume that L/K_∞ is Galois. By Lemma 10.2.1, there is some L_0/K_n finite such that $L_0 \otimes_{K_n} K_\infty = L$. Replacing K by K_n we may assume from the start that $L = L_0 K_\infty$ for some L_0/K linearly disjoint from K_∞.

Let $L_n = L_0 K_n$. By the transitivity of the different (i.e., $\mathfrak{D}_{L_n/K_n} \cdot \mathfrak{D}_{K_n/K} = \mathfrak{D}_{L_n/K}$) and (10.1.2) in the proof of Proposition 10.1.6,

$$v(\mathfrak{D}_{L_n/K_n}) = \int_{-1}^{\infty} \left(|\,\mathrm{Gal}(K_n/K)^v|^{-1} - |\,\mathrm{Gal}(L_n/K)^v|^{-1} \right) dv. \tag{10.2.1}$$

Since L_0/K is finite, there is some h such that $\mathrm{Gal}(L_0/K)^v = 1$ for all $v \geq h$. By linear disjointness, $\mathrm{Gal}(L_n/K) = \mathrm{Gal}(L_0/K) \times \mathrm{Gal}(K_n/K)$, and therefore

$$\mathrm{Gal}(L_0/K)^v = \frac{\mathrm{Gal}(L_n/K)^v\,\mathrm{Gal}(K_n/K)}{\mathrm{Gal}(K_n/K)}.$$

We see that $\mathrm{Gal}(L_0/K)^v = (1)$ if and only if $\mathrm{Gal}(L_n/K)^v \subset \mathrm{Gal}(K_n/K)$. If this is the case, then the subgroups $\mathrm{Gal}(L_n/K)^v$ and $\mathrm{Gal}(L_0/K)$ of $\mathrm{Gal}(L_n/K)$ commute and intersect only at $\{1\}$, which means that

$$\text{(10.2.2)} \qquad \mathrm{Gal}(K_n/K)^v = \frac{\mathrm{Gal}(L_n/K)^v\,\mathrm{Gal}(L_0/K)}{\mathrm{Gal}(L_0/K)} = \mathrm{Gal}(L_n/K)^v.$$

Applying (10.2.2) to (10.2.1) shows that

$$v(\mathfrak{D}_{L_n/K_n}) \leq \int_{-1}^{h} |\,\mathrm{Gal}(K_n/K)^v|\, dv.$$

By a calculation almost identical to (10.1.3) in the proof of Proposition 10.1.6, we find that $v(\mathfrak{D}_{L_n/K_n}) = p^{-n}a_n$, where a_n is bounded, say $|a_n| \leq a$ for all n. Given $\alpha \in \mathfrak{m}_\infty$, there is some n_0 such that $\alpha \in K_n$ for all $n \geq n_0$. Furthermore, *because* K_∞ *is totally ramified*, writing $(\alpha) = \mathfrak{m}_n^{i_n}$ shows that $i_n \to \infty$ as $n \to \infty$. On the other hand, as remarked in the proof of Corollary 10.1.7, if e_n is the ramification index of L_n/K_n, then $\mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n}^{\ell}) = \mathfrak{m}_n^{j}$ where $j = \lceil (\ell + v_{L_n}(\mathfrak{D}_{L_n/K_n}))/e_n \rceil$. In particular, $j \leq a+1$ for $\ell = 0$, so $\mathrm{Tr}_{L_n/K_n}(A_{L_n}) \supset \mathfrak{m}_n^{a+1}$. Since $i_n \to \infty$, there is some $m(\alpha)$ such that $i_{m(\alpha)} > a+1$, and therefore for any $n \geq m(\alpha)$ there is a $\beta \in A_{L_n} \subset A_L$ such that $\mathrm{Tr}_{L_n/K_n}(\beta) = \alpha$. Since $\mathrm{Gal}(L_n/K_n) = \mathrm{Gal}(L_0/K) = \mathrm{Gal}(L/K_\infty)$, this means that $\mathrm{Tr}_{L/K_\infty}(\beta) = \alpha$. □

For purposes of clarity, we prove the remaining results in some degree of generality. To do this, we first introduce some terminology.

Suppose F is a field admitting a non-trivial non-archimedean valuation. Let $\mathscr{N}$ be a profinite group which acts on F, and let M be an ultrametric normed F-vector space which is a topological $F\{\mathscr{N}\}$-module. Let $\widehat{M}$ be the completion of M. If the $\mathscr{N}$-action on M extends to a continuous action on $\widehat{M}$ (note that such an extension is unique if it exists), then we will refer to the collection $R = (F, \mathscr{N}, M, \widehat{M})$ as a *continuous representation*. If $\mathrm{char}\, F = 0$, then we will say that R *has characteristic zero*. The notation will be shortened to M in an unambiguous context.

Example 10.2.3. If L is an algebraic extension of K and $\mathscr{N}$ a closed subgroup of $\mathscr{G}$, then for any subextension $F/K \subset L/K$, $(F, \mathscr{N}, L, \widehat{L})$ is a continuous representation such that $\mathscr{N}$ acts by isometries. ◊

In order to simplify notation, given a continuous representation $(F, \mathscr{N}, M, \widehat{M})$, the *discrete cohomology* will always refer to the discrete cohomology with coefficients *in* M and the *continuous cohomology* will always mean the continuous cohomology with coefficients *in* $\widehat{M}$.

Given a continuous r-cochain of $\mathscr{N}$ with coefficients in $\widehat{M}$, compactness of $\mathscr{N}$ shows that there is a maximal value for $|f(s)|$ as s ranges over $\mathscr{N}$. Define a metric on the cochains as usual: $|f| = \max\{|f(s)|\}_{s \in \mathscr{N}}$. The usual uniform continuity arguments show that $C^r(\mathscr{N}, \widehat{M})$ is complete with respect to this metric. Discrete cochains are certainly continuous, so limits of sequences of discrete cochains belong to the continuous cochains.

Lemma 10.2.4. *If $(F, \mathscr{N}, M, \widehat{M})$ is a continuous representation, then the discrete cochains are dense in the continuous cochains. In particular, if L is an algebraic extension of K and $\mathscr{N}$ is a closed subgroup of $\mathscr{G}$, then $C^r_{\text{disc}}(\mathscr{N}, L)$ is dense in $C^r(\mathscr{N}, \widehat{L})$.*

Proof. Let $B_n \subset \widehat{M}$ be the open ball of radius $1/n$ around 0. By density, $\widehat{M} = M + B_n$ for all n, so if $\psi_n : \widehat{M} \to \widehat{M}/B_n$ is the canonical map (of groups), it is easy to see that there is a set-theoretic map $\phi_n : \widehat{M}/B_n \to M$ such that $\psi_n \phi_n = \text{id}$. Since B_n is open, $\widehat{M}/B_n$ is discrete, so the ϕ_n are all continuous to the discrete topology on M. Given a continuous r-cochain $f : \mathscr{H}^r \to \widehat{M}$, setting $f_n = \phi_n \psi_n f$ yields a sequence of discrete cochains (with values in M) such that $\psi_n f_n = \psi_n f$, i.e., $|f - f_n| < 1/n$. □

Notation 10.2.5. When dealing with finite extensions L/K_∞, a (discrete) (-1)-cochain will be an element y of L, and the coboundary of such a cochain will be $\delta y = \text{Tr}_{L/K_\infty}(y)$.

Proposition 10.2.6. *Let $\mathscr{H}$ act in the usual way on $\overline{K}$ and let $(\overline{K}, \mathscr{H}, M, \widehat{M})$ be a continuous representation for which $\mathscr{H}$ acts by isometries. Suppose further that M is a discrete $\mathscr{H}$-module, i.e., that $M = \cup M^{\mathscr{U}}$ as $\mathscr{U}$ ranges over open subgroups of $\mathscr{H}$. Given a discrete r-cochain $f \in C^r_{\text{disc}}(\mathscr{H}, M)$ and a constant $c > 1$,*

(1) *if $r = 0$, there is an element $x \in M^{\mathscr{H}}$ such that $|f - x| \leq c|\delta f|$ (in particular, when $M = \overline{K}$, $x \in K_\infty$);*

(2) *if $r > 0$, there is a discrete $(r-1)$-cochain g such that $|f - \delta g| \leq c|\delta f|$ and $|g| \leq c|f|$.*

Proof. Because M is discrete, the stabilizer of any element of M is an open subgroup of $\mathscr{H}$, and this implies that the natural map

$$\varinjlim \mathrm{H}^1_{\text{disc}}(\text{Gal}(L/K^\infty), M^{\mathscr{U}}) \to \mathrm{H}^1_{\text{disc}}(\mathscr{H}, M)$$

is an isomorphism, where the limit is taken with respect to the inflation maps as L ranges over finite subextensions $L = \overline{K}^{\mathscr{U}}$ of $\overline{K}/K_\infty$. Since the inflation maps are all injective, the big cohomology group may simply be viewed as a union. Therefore, it suffices to prove the following:

Let L/K_∞ be finite with Galois group G, and let M be an ultrametric normed L-vector space which admits a semi-linear G-action by isometries. For any r-cochain f and any $c > 1$, there is an $(r-1)$-cochain g such that $|f - \delta g| \leq c|\delta f|$ and $|g| \leq c|f|$. (This includes $r = 0$!)

The point is that a single c may be chosen, independent of the finite subextension L/K_∞. This independence depends heavily upon the fact that K_∞/K is ramified. By Lemma 10.2.2, there is a (-1)-cochain $y \in L$ such that $|y| \leq 1$ and $|\delta y| > c^{-1}$ for any value of $c > 1$. Given such an element, we can even *construct* a g for any f. To do this, we define a product $(y, f) \mapsto y.f$ as follows:

$r = 0$: $y.f = yf$

$r > 0\colon (y.f)(s_1, \dots, s_{r-1}) = (-1)^r \sum_{s \in G} s_1 s_2 \cdots s_{r-1} s(y) f(s_1, s_2, \dots, s_{r-1}, s)$.

Because G acts by isometries and the metric on M is an ultrametric, it is clear that if $|y| \leq 1$ then $|y.f| \leq |f|$.

By a routine calculation, one easily verifies that $(\delta y)f - \delta(y.f) = y.\delta f$. Hence, setting $\mathrm{Tr}_{L/K_\infty}(y) = x$ and $g = x^{-1}(y.f)$, we have $f - \delta g = x^{-1}(y.\delta f)$. Since $|x^{-1}| < c$ and $|y| \leq 1$, $|x^{-1}(y.\delta f)| \leq c|\delta f|$. □

10.2.2 The cohomology of $\mathscr{H}$ with coefficients in $\mathbf{C}_K$

If $R = (F, \mathscr{N}, M, \widehat{M})$ is a continuous representation, call R *acyclic* if the continuous cohomology of R vanishes for indices ≥ 1.

Approximation Lemma. *A continuous representation $(\overline{K}, \mathscr{H}, M, \widehat{M})$ satisfying the hypotheses of Proposition 10.2.6 is acyclic.*

Proof. The proof proceeds by successive approximations by discrete coboundaries of a continuous cochain representing a cocycle.

Let f be a continuous cochain representing some cocycle of $\mathrm{H}^r(\mathscr{H}, \widehat{M})$ (with $r > 0$, of course). Take any sequence of discrete cochains (with coefficients in M) $F_\nu \to f$. Since δ is continuous and $\delta f = 0$, we may assume that $|F_\nu - f| \leq 2^{-\nu}$ and $|\delta F_\nu| \leq 2^{-\nu}$. Fixing a constant $c > 0$, let G_ν be chosen as in Proposition 10.2.6, so that $|F_\nu - \delta G_\nu| \leq c|\delta F_\nu|$ and $|G_\nu| \leq c|F_\nu|$. If $f_n = \frac{1}{m_n}\sum_{\nu=1}^{n} F_\nu$ and $g_n = \frac{1}{m_n}\sum_{\nu=1}^{n} G_\nu$, where $m_n \in \mathbf{Z} \subset F$ is a sequence of integers such that $|m_n| \to \infty$ as $n \to \infty$, then

$$|f - f_n| \leq \frac{1}{|m_n|}\sum_{\nu=1}^{n} |f - F_\nu| \leq \frac{1}{|m_n|},$$

so $f_n \to f$. Similarly,

$$|g_{n+\ell} - g_n| \leq \left|\frac{1}{m_{n+\ell}} - \frac{1}{m_n}\right| + \left|\frac{1}{m_{n+\ell}}\right|,$$

and the right-hand side tends to 0 as $n \to \infty$ for arbitrary fixed ℓ. Thus, the g_n form a Cauchy sequence, so $g_n \to g$ for some continuous $(r-1)$-cochain g. It is easy to see that $|f_n - \delta g_n| \leq \frac{c}{|m_n|}$, so in the limit $f = \delta g$. □

Proposition 10.2.7. $\mathrm{H}^0(\mathscr{H}, \mathbf{C}_K) = X$ *and* $\mathrm{H}^r(\mathscr{H}, \mathbf{C}_K) = 0$ *for* $r > 0$.

Proof. When $r = 0$, the result follows immediately from Proposition 10.2.6(1). By Example 10.2.3, the proof for $r > 0$ follows from the Approximation Lemma. □

10.3 The Main Results

10.3.1 Fixed points

Theorem 10.3.1. $\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K) = K$ *and* $\dim_K \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K) = 1$.

Proof. To prove the first statement, note that $\mathbf{C}_K^{\mathscr{G}} = (\mathbf{C}_K^{\mathscr{H}})^{\mathfrak{g}}$. By Proposition 10.2.7 and Theorem 10.1.9(1), this equals K.

To prove the second statement, recall the inflation-restriction sequence

$$0 \to \mathrm{H}^1(\mathfrak{g}, X) \to \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K) \to \mathrm{H}^1(\mathscr{H}, \mathbf{C}_K). \tag{10.3.1}$$

By Theorem 10.1.9(1) and Proposition 10.2.7, the result is proven. □

10.3.2 Twists

Fix a multiplicative character $\chi : \mathscr{G} \to K^\times$. (By compactness, χ must actually take its values in $A^\times$.) Let K_∞ denote the fixed field of $\ker \chi$.

Theorem 10.3.2. *If χ is ramified, then* $\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(\chi)) = 0 = \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(\chi))$.

Proof. Because χ is ramified, there is some finite K_0/K such that K_∞/K_0 is a totally ramified $\mathbf{Z}_p$-extension.

Suppose first that $K_0 = K$. Since $(\mathbf{C}_K(\chi))^{\mathscr{G}} = ((\mathbf{C}_K(\chi))^{\mathscr{H}})^{\mathfrak{g}}$ and $\mathscr{H}$ acts on $\mathbf{C}_K(\chi)$ without a twist, Proposition 10.2.7 and Theorem 10.1.9(2) show that $\mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(\chi)) = 0$. For the second result, the inflation-restriction sequence works just as in (10.3.1) above, except that Proposition 10.2.7 and Theorem 10.1.9(2) make the outer terms both vanish, yielding $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(\chi)) = 0$.

Now suppose that K_0 is any arbitrary finite extension of K. Let $\mathscr{U}$ be the open subgroup fixing K_0. By the case just proven, $\mathrm{H}^0(\mathscr{U}, \mathbf{C}_K(\chi)) = 0 = \mathrm{H}^1(\mathscr{U}, \mathbf{C}_K(\chi))$. Therefore, in the inflation-restriction sequence

$$0 \to \mathrm{H}^1(\mathscr{G}/\mathscr{H}, \mathrm{H}^0(\mathscr{U}, \mathbf{C}_K(\chi))) \to \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K(\chi)) \to \mathrm{H}^1(\mathscr{U}, \mathbf{C}_K(\chi)),$$

the outer terms are zero, completing the proof. □

Remark 10.3.3. Sen's paper [9] contains a proof of the non-existence of transcendental invariants in $\mathbf{C}_K$ (Theorem 10.3.1) which requires no class field theory and is completely elementary. However, for Tate's results, one also needs the vanishing in Theorem 10.3.2, which Sen does not obtain by elementary methods. ♦

10.3.3 An amusing application of the main results

Proposition 10.3.4. $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$ *is non-zero and torsion-free.*

Proof. To see that $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$ is non-zero, consider the p-adic cyclotomic character ε_p. A $K^\times$-valued character is certainly a 1-cocycle, so ε_p represents an element of $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$. If $\varepsilon_p(s) = s(\alpha)/\alpha$, then $\alpha \in \mathrm{H}^0(\mathscr{G}, \mathbf{C}_K(\varepsilon_p^{-1}))$, so $\alpha = 0$ by Theorem 10.3.2. This means that ε_p represents a non-trivial element of $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$.

It remains to show that the torsion submodule of $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$ is trivial. If a cocycle f represents an n-torsion cohomology class, then there is a $\beta \in \mathbf{C}_K^\times$ such that for all $s \in \mathscr{G}$, $f(s)^n = s(\beta)/\beta$. If α is any nth root of β, then $f'(s) = f(s) \cdot \alpha / s(\alpha)$ takes values in $\boldsymbol{\mu}_n$. Since $\mathbf{C}_K$ is Hausdorff in the valuation topology, $\boldsymbol{\mu}_n$ is discrete because it is finite. Thus, by continuity, f' must factor through the quotient of $\mathscr{G}$ by an open subgroup, and therefore f' is a discrete cocycle. (We have implicitly used Lemma 9.1.1.) By Hilbert's Theorem 90, there is some $\beta \in \overline{K}^\times$ such that $f'(s) = s(\beta)/\beta$, and therefore f is a coboundary. □

It seems quite unlikely that $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$ is finitely generated. In the special case where K is a finite unramified extension of $\mathbf{Q}_p$ for some odd prime p, it is possible to use Theorem 10.1.9 to produce an enormous subgroup of $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$. The proof below shows a use of the Theorem when X is the completion of an *unramified* $\mathbf{Z}_p$-extension of K.

Proposition 10.3.5. *Let K be a finite unramfied extension of $\mathbf{Q}_p$ with $p > 2$. If K_∞ is an unramified $\mathbf{Z}_\ell$-extension of K with Galois group $\mathfrak{g}$ and completion X, then $\mathrm{H}^1(\mathfrak{g}, X^\times)$ is naturally a torsion-free $\mathbf{Z}_p$ module, and*

$$\dim_{\mathbf{Q}_p}(\mathbf{Q}_p \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^1(\mathfrak{g}, X^\times)) = [K : \mathbf{Q}_p].$$

In particular, $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$ contains a subgroup isomorphic to $\mathbf{Z}_p^{[K:\mathbf{Q}_p]}$.

Proof. Because the residue field of K is finite, there is an unramified $\mathbf{Z}_p$-extension K_∞/K, fixed by some closed $\mathscr{H} \subset \mathscr{G}$. Write $\mathfrak{g}$ for $\mathrm{Gal}(K_\infty/K)$ and let X be the completion of K_∞. By a Theorem of Sen (see [9]), $\mathbf{C}_K^{\mathscr{H}} = X$. Using the inflation-restriction sequence

$$0 \to \mathrm{H}^1(\mathfrak{g}, X^\times) \to \mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times) \to \mathrm{H}^1(\mathscr{H}, \mathbf{C}_K^\times)$$

shows that the second statement follows from the first.

Let σ be a topological generator for $\mathfrak{g}$. Given a continuous cocycle $f : \mathfrak{g} \to X^\times$, if $n > 0$ then $f(\sigma^n) = \prod_{i=0}^{n-1} \sigma^i f(\sigma)$. Thus, if $|f(\sigma)| \neq 1$, then there is a sequence in $\mathfrak{g}$ tending to the identity which does not tend to 1 in $X^\times$, contradicting continuity. Therefore, $|f(\sigma)| = 1$, and this means that the image of $\langle\sigma\rangle$ is contained in $A_X^\times$, so by density $f(\mathscr{G}) \subset A_X^\times$. If $f = s(\alpha)/\alpha$, then multiplying α by a suitable power of p (which is a uniformizer for X) shows that we may take $\alpha \in A_X^\times$. Thus, $\mathrm{H}^1(\mathfrak{g}, X^\times) = \mathrm{H}^1(\mathfrak{g}, A_X^\times)$. But $A_X^\times = S \times U_X$, where S is the group of Teichmüller representatives for the multiplicative group of the residue field of X and U_X is the group of principal units. This factorization of $A_X^\times$ is Galois-compatible, which means that $\mathrm{H}^1(\mathfrak{g}, A_X^\times) = \mathrm{H}^1(\mathfrak{g}, k^\times) \times \mathrm{H}^1(\mathfrak{g}, U_X)$. Because K_∞ is unramified and X and K_∞ have the same residue field, $\mathfrak{g}$ is the Galois group of the residue field extension, and therefore by Hilbert's Theorem 90 (along with the fact that S-valued cocycles are continuous for the discrete topology on S) the first factor is the trivial module.

As for the second factor, because X is unramified and p is odd, the p-adic logarithm provides a $\mathfrak{g}$-module isomorphism $U_X \cong A_X$. Now, by Lemma 9.1.1, Lemma 9.2.9 and Theorem 10.1.9(1),

$$\mathbf{Q}_p \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^1(\mathfrak{g}, X^\times) = \mathbf{Q}_p \underset{\mathbf{Z}_p}{\otimes} \mathrm{H}^1(\mathfrak{g}, A_X) = \mathrm{H}^1(\mathfrak{g}, X) \cong K.$$

By Proposition 10.3.4, $\mathrm{H}^1(\mathfrak{g}, X^\times) \cong \mathrm{H}^1(\mathfrak{g}, A_X)$ is a torsion-free $\mathbf{Z}_p$-module. □

Corollary 10.3.6. *If K is a finite Galois extension of $\mathbf{Q}_p$ with $p > 2$ and L is a subfield of K such that $L/\mathbf{Q}_p$ is unramified, then $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times)$ contains a subgroup isomorphic to $\mathbf{Z}_p^{[L:\mathbf{Q}_p]}$.*

Proof. This follows from the inflation-restriction sequence and Hilbert's Theorem 90 for finite Galois extensions. □

Remark 10.3.7. Consider the diagonal embedding $\mathbf{C}_K^\times \to \mathrm{GL}_n(\mathbf{C}_K)$. Let $f : \mathscr{G} \to \mathrm{GL}_n(\mathbf{C}_K)$ be a cocycle taking values in the image of $\mathbf{C}_K^\times$. If f is a coboundary in $\mathrm{H}^1(\mathscr{G}, \mathrm{GL}_n(\mathbf{C}_K))$, then there is some matrix α such that for all $s \in \mathscr{G}$, $f(s) = \alpha^{-1} s(\alpha)$. Writing $\overline{f(s)}$ for the element along the diagonal of $f(s)$, one has $s(\alpha) = \overline{f(s)}\alpha$ for all s. This holds if and only if for each coordinate α_{ij}, $s(\alpha_{ij}) = \overline{f(s)}\alpha_{ij}$. Invertibility of α implies that some $\alpha_{ij} \neq 0$, so it follows that $\overline{f(s)}$ is a coboundary. This shows that the diagonal embedding induces an injection $\mathrm{H}^1(\mathscr{G}, \mathbf{C}_K^\times) \to \mathrm{H}^1(\mathscr{G}, \mathrm{GL}_n(\mathbf{C}_K))$ for all $n > 0$, so $\mathrm{H}^1(\mathscr{G}, \mathrm{GL}_n(\mathbf{C}_K)) \neq 0$ for all n by Proposition 10.3.4. Thus, in spite of naïve expectations which may arise from the fact that $\mathbf{C}_K^{\mathscr{G}} = K$, attempts at a continuous analogue of "Galois descent" from the enormous scalar extension from K to $\mathbf{C}_K$ is futile. This further shows (cf. Section 9.2.3) the desirability of a refinement of the Hodge-Tate condition to involve something less drastic than applying the "non-invertible" functor $\mathbf{C}_K \otimes_K (\,\cdot\,)$ to $K[\mathscr{G}]$-modules (with finite K-dimension and continuous $\mathscr{G}$-action). ♦

A Invariant Differentials on Group Schemes

Motivated by the classical theory of Lie groups, it is reasonable to expect that "invariant differentials" should play a useful role in the study of group schemes. However, in this more general context it takes some work to properly define and prove the correct adaptations of the classical results. The purpose of this appendix is to construct invariant differentials on formal group schemes and to show that they freely generate the module of differentials. Using this information, we can compute the discriminants of certain isogenies between formal Lie groups (cf. Section 4.3.1).

The proofs we give here apply to both affine and formal group schemes. We give the proofs in the formal case because we make heavy use of it in Part II. Translating the results into the affine language simply involves removing " $\widehat{\ }$ " symbols and erasing the words "profinite" and "formal" whenever they occur. (With some care, these methods can be adapted to suitable non-affine group schemes, but this is not necessary for our purposes.)

We refer the reader to Section 2.1.1 and Section 2.1.2 for the basic facts and notations from the theory of pseudocompact rings and formal functors, as we use these extensively without comment in what follows.

A.1 Definitions

Fix a pseudocompact base ring A and let $G = \mathrm{Spf}_A(B)$ be a formal group over $S = \mathrm{Spf}_A(A)$. We work in the category of formal S-schemes; to simplify notation, "T-scheme" will always mean "formal T-scheme" for a formal S-scheme T. As usual, $G_T = G \times_S T$ is the notation for base change. There is a natural identification $G(T) = G_T(T)$.

Definition A.1.1. Given $g \in G(T)$, define the *left-translation by g* to be the functorial map

$$\lambda_g : G_T = G_T \times_T T \xrightarrow{\mathrm{id} \times g} G_T \times_T G_T \xrightarrow{m_T} G_T.$$

Equivalently, λ_g is the unique morphism $G_T \to G_T$ such that for any T-scheme $T' \to T$ and any point $h \in G_T(T')$, $\lambda_g(T')(h) = g_{T'}h$, where $g_{T'}$ is the image of g in $G_T(T')$ under the base change (pullback) map. The *right translation by g*, written ρ_g, is defined similarly. It is clear that the formation of λ_g and ρ_g are compatible with base change and are functorial in G.

Because G is a *group* scheme, the left-translations λ_g (for $g \in G(T)$) are automorphisms of the formal T-scheme G_T. Yoneda's Lemma shows that translation by the G-valued point $\mathrm{id}_G : G \to G$, the *universal point*, acts as a *universal translation* in the following sense: $\lambda_{\mathrm{id}_G} : G \times_S G \to G \times_S G$ sends a point (x, y) to the point (yx, y). Given any $h \in G(T)$, λ_h is just the base change of λ_{id_G} by h, i.e., the diagram

$$\begin{array}{ccc} G \times_S T & \xrightarrow{\lambda_h} & G \times_S T \\ \downarrow{\scriptstyle \mathrm{id}_G \times h} & & \downarrow{\scriptstyle \mathrm{id}_G \times h} \\ G \times_S G & \xrightarrow{\lambda_{\mathrm{id}_G}} & G \times_S G \end{array} \qquad \text{(A.1.1)}$$

is cartesian.

Definition A.1.2. A differential $\omega \in \Omega^1_{G/S} = \widehat{\Omega}^1_{B/A}$ is *left-invariant* if for all S-schemes $T \to S$ and all points $g \in G(T)$, $\lambda_g^* \omega_T = \omega_T$ under the canonical isomorphism $\lambda_g^* \Omega_{G/S} \cong \Omega_{G/S}$ induced by λ_g. The set of all left-invariant differential forms on G will be denoted by $\Omega^{1,\ell}_{G/S}$.

Remark A.1.3. It is clear that for any $h \in G(T)$, $\omega_T = (\mathrm{id}_G \times h)^* \omega_G$. By (A.1.1),

$$(\mathrm{id}_G \times h) \circ \lambda_h = \lambda_{\mathrm{id}_G} \circ (\mathrm{id}_G \times h),$$

so we see that

$$\lambda_h^* \omega_T = \lambda_h^* (\mathrm{id}_G \times h)^* \omega_G = (\mathrm{id}_G \times h)^* \lambda_{\mathrm{id}_G}^* \omega_G,$$

and therefore ω is left-invariant if and only if it is invariant under left-translation by the universal point id_G. This shows that $\Omega^{1,\ell}_{G/S}$ is identified with the kernel of the module map

$$\xi : \Omega^1_{G/S} \to \Omega^1_{G \times G/G}$$

defined by

$$\omega \mapsto \lambda_{\mathrm{id}_G}^* \omega_G - \omega_G.$$

It is easy to see that ξ is a continuous map of profinite A-modules, and therefore $\Omega^{1,\ell}_{G/S}$ is a closed (and hence profinite) A-submodule of $\Omega^1_{G/S}$. Similarly, it is straightforward to see that $\Omega^{1,\ell}_{G/S} \hookrightarrow \Omega^1_{G/S}$ is a "subfunctor" in the formal group G. It is not obvious that $\Omega^{1,\ell}_{G/S}$ is of formation compatible with base change on S (or that it is nonzero in general), but the next section will settle these points. ♦

A.2 Existence of invariant differentials

We will now show that the formal relative cotangent space of G at the identity section can be "propogated by translation" to construct all of the left-invariant differential forms on G. Let $\varepsilon : S \to G$ be the identity section and let $I \in B$ be the augmentation ideal. Given $\omega_0 \in \varepsilon^* \Omega^1_{G/S}$, the strategy will be to choose *any* "lift" $\omega \in \Omega^1_{G/S}$ such that $\varepsilon^* \omega = \omega_0$ and to construct from ω a *left-invariant* lift. The following elegant method is an adaptation to the formal case of the ordinary scheme-theoretic method in [6, Proposition 1, §4.2].

Suppose for a moment that G is a smooth classical Lie group. If we accept that the space of global 1-forms is freely spanned by the left-invariant 1-forms, then we may write any 1-form ω as

$$\omega(x) = \sum a_i(x) \omega_i(x)$$

for all $x \in G$, where the a_i are global smooth functions on G and the ω_i are global left-invariant 1-forms. We wish to construct a global left-invariant 1-form ω' such that $\omega'(0) = \omega(0)$. In other words, we want

$$\omega'(x) = \lambda_x^* \left(\sum a_i(0) \omega_i(0) \right) = \sum a_i(0) \omega_i(x).$$

We desire a functorial construction of ω' from ω which is less dependent upon points and generalizes to (formal) schemes. Given $x \in G$, if $j_2 : G \to G \times G$ sends y to (x, y), then for a *left-invariant* form ω_i we have $j_2^*(m^*\omega_i) = \lambda_x^*\omega_i = \omega_i$. Thus, using the canonical decomposition

$$\Omega^1_{G\times G} = p_1^*\Omega^1_G \oplus p_2^*\Omega^1_G, \tag{A.2.1}$$

we see that

$$(m^*\omega_i)(x, y) = \eta(x, y) + \omega_i(y),$$

where $\eta = \sum b_j(x, y)\alpha_j(x)$ for some 1-forms $\alpha_j(x)$ in the cotangent space at x. We have therefore shown that the "second component" of $m^*\omega_i(x, y)$ in (A.2.1) is $\omega_i(y)$. Thus,

$$(m^*\omega)(x, y) = \eta' + \sum a_i(xy)\omega_i(y)$$

where $\tilde{\omega} = \sum a_i(xy)\omega_i(y)$ is the second component of $(m^*\omega)(x, y)$. If $\delta : G \to G \times G$ is the "twisted diagonal map" which sends x to (x^{-1}, x) then pulling back $\tilde{\omega}$ by δ yields

$$(\delta^*\tilde{\omega})(x) = \sum a_i(0)\omega_i(x) = \omega'(x).$$

This gives a way of constructing a left-invariant 1-form ω' agreeing with ω at 0.

The following is a functorial revision of this point-theoretic argument.

Proposition A.2.1. *Given $\omega_0 \in \varepsilon^*\Omega^1_{G/S}$, there is a unique $\omega \in \Omega^{1,\ell}_{G/S}$ such that $\varepsilon^*\omega = \omega_0$.*

Proof. To prove existence, let ω be any lift of ω_0 (i.e., $\varepsilon^*\omega = \omega_0$). (This step uses the "affineness" of our formal schemes.) Using the natural isomorphism

$$p_1^*\Omega^1_{G/S} \oplus p_2^*\Omega^1_{G/S} \xrightarrow{\sim} \Omega^1_{G\times_S G/S}, \tag{A.2.2}$$

write $m^*\omega = \omega_1 \oplus \omega_2$. Let $\delta : G \to G \times_S G$ be the twisted diagonal map given on the level of points by $x \mapsto (x^{-1}, x)$. We claim that $\omega' = \delta^*\omega_2$ is a left-invariant lift of ω_0. To see that ω' lifts ω_0, we need to show that

$$\varepsilon^*\delta^*\omega_2 = \varepsilon^*\omega.$$

Consider the base change ε_G of the identity section $\varepsilon : S \to G$ by $G \to S$; that is, $\varepsilon_G(x) = (1, x)$ on the level of points. Then $p_1 \circ \varepsilon_G$ factors through the identity section, so

$$\varepsilon_G^*(\omega_2) = \varepsilon_G^*(\omega_1 + \omega_2) = \varepsilon_G^* m^*\omega = \omega$$

because $m \circ \varepsilon_G = \mathrm{id}_G$. Therefore, it suffices to show that $\varepsilon^*\delta^* = \varepsilon^*\varepsilon_G^*$ to show that ω' lifts ω_0. But it is easy to see that $\delta \circ \varepsilon = \varepsilon_G \circ \varepsilon$ as morphisms $S \to G \times_S G$, so the result follows by functoriality.

It remains to show that ω' is left-invariant. By base change, it suffices to prove invariance under left-translation by points of $G(S)$. Consider the diagram

$$\begin{array}{ccc} G & \xrightarrow{\lambda_g} & G \\ \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\delta} \\ G \times_S G & \xrightarrow{\rho_{g^{-1}} \times \lambda_g} & G \times_S G. \end{array} \tag{A.2.3}$$

This commutes by the definition of δ. Clearly, $p_1 \circ (\rho_{g^{-1}} \times \lambda_g) = \rho_{g^{-1}} \circ p_1$ and $p_2 \circ (\rho_{g^{-1}} \times \lambda_g) = \lambda_g \circ p_2$, so the map $(\rho_{g^{-1}} \times \lambda_g)^*$ respects the decomposition (A.2.2). Furthermore, $m \circ (\rho_{g^{-1}} \times \lambda_g) = m$, so writing $\tilde{\omega}_i = (\rho_{g^{-1}} \times \lambda_g)^* \omega_i$ yields

$$\omega_1 \oplus \omega_2 = m^* \omega = \tilde{\omega}_1 \oplus \tilde{\omega}_2,$$

and therefore $\omega_i = \tilde{\omega}_i$. But then commutativity of (A.2.3) shows that $\delta^* \omega_2$ is left-invariant under translations by points of $G(S)$, as desired.

If ω and ω' are left-invariant lifts of ω_0, then $\varepsilon^* \omega = \varepsilon^* \omega'$. Since $g = \lambda_g \circ \varepsilon$ for any $g \in G(S)$, left-invariance shows that

$$g^* \omega = g^* \omega',$$

and functoriality extends the argument to all points of G. Using the universal point of G, we conclude that $\omega = \omega'$. □

Corollary A.2.2. *The formation of $\Omega^{1,\ell}_{G/S}$ is naturally compatible with base change on S as a subfunctor of $\Omega^1_{G/S}$.*

Proof. Since $\varepsilon^* \Omega^1_{G/S}$ is compatible with base change on S, this follows from Proposition A.2.1. □

Finally, we can prove that the left-invariant differentials span $\Omega^1_{G/S}$. Let $\pi : G \to S$ be the structure morphism.

Theorem A.2.3. *There is a unique isomorphism of $\mathscr{O}_G$-modules*

$$\alpha_G : \pi^* \varepsilon^* \Omega^1_{G/S} \to \Omega^1_{G/S}$$

satisfying $\varepsilon^*(\alpha_G) = \mathrm{id}$. This is functorial in G and of formation compatible with base change on S.

Proof. By uniqueness, Proposition A.2.1 shows that there is an $\mathscr{O}_S$-module map

$$\varepsilon^* \Omega^1_{G/S} \to \Omega^{1,\ell}_{G/S} \subset \Omega^1_{G/S}$$

of formation compatible with base change on S (and functorial in G). Note that by construction, $\varepsilon^* \alpha_G$ is the identity on $\varepsilon^* \Omega^1_{G/S}$ (using $\varepsilon^* \pi^* = 1$). Thus, pulling back by π yields an $\mathscr{O}_G$-module map

$$\alpha_G : \pi^* \varepsilon^* \Omega^1_{G/S} \to \Omega^1_{G/S}.$$

By the usual functoriality and base change arguments (using Corollary A.2.2), to show α_G is an isomorphism it suffices to prove that $g^* \alpha_G$ is an isomorphism for all $g \in G(S)$. Consider the diagram

$$\text{(A.2.4)} \qquad \begin{array}{ccc} \lambda_g^* \pi^* \varepsilon^* \Omega^1_{G/S} & \xrightarrow{\lambda_g^* \alpha_G} & \lambda_g^* \Omega^1_{G/S} \\ \downarrow & & \downarrow \\ \pi^* \varepsilon^* \Omega^1_{G/S} & \xrightarrow{\alpha_G} & \Omega^1_{G/S}, \end{array}$$

where the left column is the isomorphism defined using $\pi \circ \lambda_g = \pi$ and the right column is the isomorphism given by functoriality of Ω^1. If we can show that this diagram commutes then we will be done, for applying ε^* to the rows yields the identity map on the bottom and $g^*\alpha_G$ on the top.

By continuity, it suffices to chase an element of the form $x = b \widehat{\otimes} \omega_0$, starting in the upper left of (A.2.4). The left map sends x to $x' = (\lambda_g^{-1})^*(b) \widehat{\otimes} \omega_0$ and the bottom map sends x' to $(\lambda_g^{-1})^*(b)\omega$, where ω is the unique left-invariant lift of ω_0. On the other hand, the top map takes x to $y = b \widehat{\otimes} \omega$ and the right map takes y to $(\lambda_g^{-1})^*(b)(\lambda_g^{-1})^*\omega = (\lambda_g^{-1})^*(b)\omega$ because ω is left-invariant.

By the uniqueness in Proposition A.2.1, α_G is uniquely characterized by the condition $\varepsilon_G^*(\alpha_G) = \mathrm{id}$. From the above construction we deduce functoriality in G and the uniqueness of α_G ensures base change compatibility on S. □

Corollary A.2.4. *If $B = \mathscr{O}(G)$, there is a unique isomorphism of profinite B-modules*

$$B \mathop{\widehat{\otimes}}_A \Omega^{1,\ell}_{G/S} \xrightarrow{\sim} \Omega^1_{G/S}$$

inducing the natural map along the identity section. This is functorial in G and of formation compatible with base change on A. Similarly, there is a natural isomorphism

$$B \mathop{\widehat{\otimes}}_A I/\overline{I^2} \xrightarrow{\sim} \Omega^1_{G/S}.$$

Proof. This is simply definition chasing in Theorem A.2.3, along with the fact that $\Omega^{1,\ell}_{G/S} \cong \varepsilon^*\Omega^1_{G/S} \cong I/\overline{I^2}$ by Proposition A.2.1 and Lemma 3.1.1. □

The finite (or even affine) cases of Theorem A.2.3 and Corollary A.2.4 are formally identical, as the properties of the sheaf of relative differentials and base change are the same in the category of schemes affine over a fixed base S.

The abstract methods used in this section also yield some concrete results.

Proposition A.2.5. *Let $G \to S$ be a formal group. Given $\omega \in \Omega^1_{G/S}$, write $m^*\omega = \omega_1 \oplus \omega_2$.*

(1) *If ω is left-invariant, $\omega_2 = p_2^*\omega$.*

(2) *If ω is right-invariant, $\omega_1 = p_1^*\omega$.*

Proof. We consider the case of left-invariance. (The right-invariant case follows from the obvious alteration of the proof of Proposition A.2.1.) Applying the construction of Proposition A.2.1 to ω, we deduce that $\delta^*\omega_2 = \omega$. Thus, $p_2^*\omega = p_2^*\delta^*\omega_2 = \omega_2$. □

Remark A.2.6. When G is commutative (the case of interest to us), left-invariant forms ω are automatically right-invariant because inversion is a group morphism which interchanges left- and right-translation. In fact, one can show that the forms which are simultaneously left- and right-invariant are precisely those forms satisfying $m^*\omega = p_1^*\omega + p_2^*\omega$ [1, Theorem 4.1.3]. ♦

Corollary A.2.7. *Let G be a commutative formal group scheme over S, and let $[N] : G \to G$ be the map sending $x \to Nx$ on the level of points. If $\omega \in \Omega^{1,\ell}_{G/S}$, then the natural map $[N]^*\Omega^1_{G/S} \to \Omega^1_{G/S}$ sends $[N]^*(\omega)$ to $N\omega$.*

Proof. Write $[N] = m_N \circ \Delta_N$ where Δ_N is the N-fold diagonal map and m_N is the N-fold multiplication map. The obvious extension of Proposition A.2.5 and Remark A.2.6 shows that

$$m_N^*(\omega) = p_1^*\omega + \cdots + p_N^*\omega. \tag{A.2.5}$$

On the other hand, it is clear that under the natural map $\Delta_N^*(\Omega^1_{G\times_S\cdots\times_S G/S}) \to \Omega^1_{G/S}$,

$$\Delta_N^*(p_1^*\omega_1 + \cdots + p_N^*\omega_N) \mapsto \omega_1 + \cdots + \omega_N, \tag{A.2.6}$$

so combining (A.2.5) and (A.2.6) yields the Corollary. □

B Connected formal groups in characteristic 0

Throughout this appendix, K is a field of characteristic 0.

We will prove that every connected formal group over K is a formal Lie group and that every commutative formal Lie group of relative dimension ℓ over K is isomorphic to $\prod_{i=1}^{\ell} \widehat{\mathbf{G}}_a$.

B.1 Connected formal groups over K are smooth

Proposition B.1.1. *Any connected formal group scheme over K is formally smooth.*

Proof. Let $\mathscr{O}(G) = A$, and let $\mathfrak{m}$ denote the augmentation ideal of A. Choose a topological basis $\{x_i\}$ for $\mathfrak{m}/\overline{\mathfrak{m}^2}$. Since $A/\mathfrak{m} = K$, it is elementary that any lift of this basis to a set $\{y_i\} \subset \mathfrak{m}$ gives rise to a unique continuous surjection of profinite K-algebras

$$\xi : K[\![\{Y_i\}]\!] \to A$$

such that Y_i maps to y_i. We claim that ξ is injective. If $\mathfrak{n} = \overline{(\{Y_i\})}$ is the augmentation ideal of $K[\![\{Y_i\}]\!]$, then $\cap\overline{\mathfrak{n}^t} = (0)$, so if $\ker\xi \neq 0$ there is $t \geq 0$ such that $\ker\xi \subset \overline{\mathfrak{n}^t}$ but $\ker\xi \not\subset \overline{\mathfrak{n}^{t+1}}$; by the definition of the y_is, $t \geq 2$. Let $f \in \ker\xi - \overline{\mathfrak{n}^{t+1}}$. We know by Corollary A.2.4 that $\Omega^1_{G/K}$ is a topologically free profinite A-module and the dy_i lift a topological basis of $\Omega^1_{G/K}$, so by the Formal Nakayama's Lemma and topological flatness arguments over the local pseudocompact ring A, we conclude that $\Omega^1_{G/K}$ has topological basis dy_i. Similarly, $\widehat{\Omega}^1_{K[\![\{Y_i\}]\!]/K}$ is a topologically free $K[\![\{Y_i\}]\!]$-module with topological generators dY_i. The induced map on differentials is $d\xi : dY_i \mapsto dy_i$, so we see that if $f \in \ker\xi$, then $\partial f/\partial Y_i \in \ker\xi$ as well. But then $\partial f/\partial Y_i \in \overline{\mathfrak{n}^t}$ for all Y_i so *because K has characteristic zero* we must have $f \in \overline{\mathfrak{n}^{t+1}}$, which is a contradiction. □

B.2 The "formal logarithm"

Given a classical Lie group G, the exponential mapping determines a local isomorphism between the Lie algebra of G and a neighborhood of the identity $e \in G$. Given two points x and y sufficiently close to e, their product xy will also be close to e, and similarly with inversion. The Campbell-Baker-Hausdorff formula shows that the local group structure of G is determined by the structure of the Lie algebra of G. Because the group law on G is analytic, the power series expansion for xy in terms of x and y (in local coordinates) and the power series expansion for the inversion map gives us a formal Lie group $\widehat{G}$ (the "completion of G at the identity"), and in the commutative case the Campbell-Baker-Hausdorff formula gives an isomorphism between $\widehat{G}$ and $\widehat{\mathbf{G}}_a^n$, where $n = \dim G$. We have seen in Proposition B.1.1 that any connected formal group over K is a formal Lie group. We will now show that the local isomorphism of G with its tangent space has a formal analogue for connected commutative formal groups over our field K of characteristic zero.

Example B.2.1. Consider the formal groups $\mathbf{G}_a$ and $\mathbf{G}_m$ over K. Because char $K = 0$, we may define a map

$$\exp : \widehat{\mathbf{G}}_a \to \widehat{\mathbf{G}}_m$$

given on the level of algebras by $X \mapsto \sum_{n=1}^{\infty} Y^n/n!$. Similarly, we may define

$$\log : \widehat{\mathbf{G}}_m \to \widehat{\mathbf{G}}_a$$

by $Y \mapsto \sum_{n=1}^{\infty} (-1)^{n+1} X^n/n$. The usual formal relations show that these are in fact morphisms of formal groups over K and that they are mutual inverses. $\diamondsuit$

Remark B.2.2. As noted in Remark 3.3.4, for a formally smooth formal K-group with algebra $K[\![\{X_i\}]\!]$, the image of X_i under the comultiplication is $X_i \mathbin{\widehat{\otimes}} 1 + 1 \mathbin{\widehat{\otimes}} X_i +$ higher order terms. ♦

Theorem B.2.3. *Any (smooth) connected commutative formal group G over K is isomorphic to a direct sum of copies of $\widehat{\mathbf{G}}_a$.*

The idea of the proof is to alter the situation of Remark B.2.2 in order to get rid of the higher order terms in the comultiplication. We will do this in a series of steps, using "Hochschild cohomology," which is a functorial version of group cohomology. Our version will be tailored to suit our needs; for a more comprehensive version of the theory, see [2, II, §3] and [3, Chapter I, §10]. We omit many routine details in what follows. All functors below are formal K-functors; that is to say, functors on the category of finite (Artinian) K-algebras. *In this appendix, and in this appendix only*, the word *group* will signify a group in the category of sets (i.e., a classical group), *group-functor* will denote a (possibly non-representable) group-valued formal functor, and *group scheme* will denote a pro-representable group-valued formal functor. (In other words, "group scheme" here means what "formal group scheme" means everywhere else.)

B.2.1 Hochschild cohomology

Given a commutative group-functor $\mathscr{M}$ and an arbitrary group-functor $\mathfrak{G}$ which acts (functorially) on $\mathscr{M}$, define the group of *n-cochains*, denoted $C^n(\mathfrak{G}, \mathscr{M})$, to be the group of morphisms (natural transformations) $\mathfrak{G}^n \to \mathscr{M}$, with the group structure provided by the group structure on the functor $\mathscr{M}$. An n-cochain f is then equivalent to a family of n-cochains from $\mathfrak{G}(R)^n$ to $\mathscr{M}(R)$ which varies covariantly with the finite Artinian K-algebra R.

As usual, define coboundary homomorphisms, $\partial^n : C^n(\mathfrak{G}, \mathscr{M}) \to C^{n+1}(\mathfrak{G}, \mathscr{M})$ given on the level of points by

$$(\partial f)(g_1, \dots, g_{n+1}) = g_1 f(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n).$$

Define $\mathrm{Z}^n(\mathfrak{G}, \mathscr{M}) = \ker \partial^n$ and define $\mathrm{B}^n(\mathfrak{G}, \mathscr{M}) = \operatorname{im} \partial^{n-1}$. The *n-th Hochschild cohomology group* is defined to be

$$\mathrm{H}^n(\mathfrak{G}, \mathscr{M}) = \mathrm{Z}^n(\mathfrak{G}, \mathscr{M}) / \mathrm{B}^n(\mathfrak{G}, \mathscr{M}).$$

This is evidently functorial in $\mathscr{M}$ and $\mathfrak{G}$. Using the convention that $\mathfrak{G}^0 = \operatorname{Spf} K$, we see that $\mathrm{H}^0(\mathfrak{G}, \mathscr{M}) = \mathscr{M}^{\mathfrak{G}}(K)$ is the group of $\mathfrak{G}$-invariant elements in $\mathscr{M}(K)$. Similarly, $\mathrm{H}^1(\mathfrak{G}, \mathscr{M})$ is the group of crossed homomorphisms modulo the trivial crossed homomorphisms (suitably functorially defined). The primary object of interest to us is the second cohomology $\mathrm{H}^2(\mathfrak{G}, \mathscr{M})$. In this case, we may use the commutativity of $\mathscr{M}$ to define a *symmetric* cohomology group as follows. All elements f of B^2 are symmetric, i.e., on points they satisfy $f(u, v) = f(v, u)$. Define the *symmetric n-cochains* $C^n_s(\mathfrak{G}, \mathscr{M})$ to be n-cochains f such that $f(u_1, \dots, u_n) = f(u_{\sigma(1)}, \dots, u_{\sigma(n)})$ for all $\sigma \in S_n$, the symmetric group on n letters. Because $\mathrm{B}^2 \subset C^2_s$, if we define $\mathrm{Z}^2_s = C^2_s \cap \mathrm{Z}^2$, we may define

$$\mathrm{H}^2_s(\mathfrak{G}, \mathscr{M}) = \mathrm{Z}^2_s(\mathfrak{G}, \mathscr{M}) / \mathrm{B}^2(\mathfrak{G}, \mathscr{M}).$$

This is covariant in $\mathscr{M}$, contravariant in $\mathfrak{G}$. The following result is not surprising.

Proposition B.2.4. *Given a $\mathfrak{G}$-module $\mathscr{M}$ as above,*

(1) *there is a bijection between $\mathrm{H}^2(\mathfrak{G}, \mathscr{M})$ and equivalence classes of extensions*

$$\mathscr{M} \xrightarrow{i} E \xrightarrow{p} \mathfrak{G} \tag{B.2.1}$$

of group-functors such that i is an injection giving the kernel of p, p has a section (which is not required to be a map of group-functors), and the action of $\mathfrak{G}$ on the normal subgroup functor $\mathscr{M}$ induced by this extension is the given action;

(2) *if $\mathfrak{G}$ is commutative and acts trivially on $\mathscr{M}$, there is a bijection between $\mathrm{H}^2_s(\mathfrak{G}, \mathscr{M})$ and extensions* (B.2.1) *where E is commutative.*

Proof. The proof is straightforward and proceeds in just the same way as the classical proof, except that one works with points of the functors and must check (straightforward) functoriality at several points in the proof. □

Corollary B.2.5. *If $\mathfrak{G} = \bigoplus_{j \in J} \mathfrak{G}_j$, then the natural map of groups*

$$\kappa : \mathrm{H}^2_s(\mathfrak{G}, \mathscr{M}) \to \prod \mathrm{H}^2_s(\mathfrak{G}_j, \mathscr{M}).$$

is an isomorphism.

Proof. Given a "symmetric extension" $S : \mathscr{M} \xrightarrow{i} E \xrightarrow{p} \mathfrak{G}$, $\kappa(S)$ is represented by the family of symmetric extensions $S_j : \mathscr{M} \xrightarrow{i} E_j = p^{-1}(\mathfrak{G}_j) \xrightarrow{p} \mathfrak{G}_i$ given by restricting the corresponding cochain to the various subgroups $\mathfrak{G}_j$ of $\mathfrak{G}$.

Note that for any finite K-algebra R, the exactness of all of the $S_j(R)$ and of $S(R)$ show that $E(R)$ is isomorphic as a group to $(\bigoplus E_j(R))/N(R)$, where $N(R) \subset \mathscr{M}(R)^{\oplus J}$ is the subgroup formed by tuples (u_j) such that all but finitely many of the u_j are zero and $\sum u_j = 0$ in $\mathscr{M}(R)$. In other words, the kernel of the map $\bigoplus E_j(R) \to E(R)$ comes from identifying the copies of $\mathscr{M}(R)$ inside each $E_j(R)$. Therefore, if $E_j(R) = \mathscr{M}(R) \times \mathfrak{G}_j(R)$ for all j we see that there is a natural isomorphism $E(R) \cong \mathscr{M}(R) \times \mathfrak{G}(R)$ and therefore κ is injective.

On the other hand, given a family of extensions S_j, we may simply form the group functor $E(R) = (\bigoplus E_j(R))/N(R)$, and one easily checks that $E \to \mathfrak{G}$ is split as a map of formal functors and that $p^{-1}(\mathfrak{G}_j) = E_j$. This shows that κ is surjective. □

B.2.2 An analysis of $\mathrm{H}^2(\mathfrak{G}, \widehat{\mathbf{G}}_a)$

To prove Theorem B.2.3, we will be interested only in the case where $\mathscr{M} = \widehat{\mathbf{G}}_a$ and where $\mathfrak{G}$ is a group scheme G acting trivially on $\widehat{\mathbf{G}}_a$. If $B = \mathscr{O}(G)$, then the cochain complex $C^n(G, \widehat{\mathbf{G}}_a)$ may clearly be realized concretely as the group $B^{\widehat{\otimes} n}$ and the coboundary maps become

$$\partial^n(b_1 \widehat{\otimes} \cdots \widehat{\otimes} b_n) = 1 \widehat{\otimes} b_1 \widehat{\otimes} \cdots \widehat{\otimes} b_n + \sum_{i=1}^{n} (-1)^i b_1 \widehat{\otimes} \cdots \widehat{\otimes} m^* b_i \widehat{\otimes} b_{i+1} \widehat{\otimes} \cdots \widehat{\otimes} b_n + (-1)^{n+1} b_1 \widehat{\otimes} \cdots \widehat{\otimes} b_n \widehat{\otimes} 1$$

extended by continuity to all of $C^n(G, \widehat{\mathbf{G}}_a)$. We will denote this group by $C^n(G)$ in what follows. Similarly, we will write $\mathrm{Z}^n(G)$ for cocycles, $\mathrm{B}^n(G)$ for coboundaries, and $\mathrm{H}^n(G)$ for cohomology (all taking values in $\widehat{\mathbf{G}}_a$).

Suppose $G \cong \bigoplus_{i \in I} \widehat{\mathbf{G}}_a$. In this case, $C^n(G)$ naturally breaks up as a product $\prod C^{n,r}(G)$, where $C^{n,r}(G) \subset C^n(G)$ is the closed subspace of given by homogeneous polynomials of degree r. Furthermore, because m^* is homogeneous, this decomposition is respected by the coboundary operator ∂, so we see that

$$\mathrm{H}^n(G) \cong \prod_{r=0}^{\infty} \mathrm{H}_0^{n,r}(G)$$

and

$$\mathrm{H}_s^2(G) \cong \prod_{r=0}^{\infty} \mathrm{H}_s^{2,r}(G).$$

Lemma B.2.6. *If $G = \bigoplus_{i \in I} \widehat{\mathbf{G}}_a$, then $\mathrm{H}_s^{2,r}(G) = 0$ for all $r \geq 2$.*

Proof. This relies on a computational Lemma due to Lazard, a special case of which says that if K has characteristic zero and P is a symmetric homogeneous polynomial of degree r in two variables satisfying $P(Y,Z) - P(X+Y,Z) + P(X,Y+Z) - P(X,Y) = 0$, then there is a $c \in K$ such that $P = c((X+Y)^r - X^r - Y^r)$. For details (which are a long string of uninspiring calculations), see [5, p. 44].

By Corollary B.2.5, we reduce the statement to be proven to the case where $G = \widehat{\mathbf{G}}_a$. In this case, using our explicit version of $C^n(G)$, we see that any homogeneous $(2,r)$-cochain is a symmetric homogeneous polynomial P of degree r in two variables, and translating the 2-cocycle condition yields $P(Y,Z) - P(X+Y,Z) + P(X,Y+Z) - P(X,Y) = 0$. By Lazard's Lemma, there is a $c \in K$ such that $P = c((X+Y)^r - X^r - Y^r)$, and this says precisely that P is a $(2,r)$-coboundary. $\square$

B.2.3 The proof of Theorem B.2.3

Now suppose that G is any connected commutative formal K-group. By Proposition B.1.1, we know that $\mathscr{O}(G)$ is isomorphic to $K[\![\{X_i\}_{i\in I}]\!]$ for some index set I.

We may again realize the cochain complex $C^*(G)$ explicitly, but since m^* is no longer *a priori* homogeneous, there is no longer a ∂-compatible gradation $C^n(G) = \prod C^{n,r}(G)$. Instead, because m^* has no constant term, there is a ∂-compatible *filtration* $C^n_r(G)$ consisting of tensors (polynomials) with no terms of degree less than r. We similarly define $C^n_{s,r}$, Z^n_r, $\mathrm{Z}^n_{s,r}$, B^n_r, and $\mathrm{B}^2_{s,r}$. There is an induced filtration on cohomology, and we let $\mathrm{H}^2_{s,r}$ denote the rth piece of the graded group associated to (the filtered group) H^2_s.

Lemma B.2.7. *Given a connected commutative formal K-group G, $\mathrm{H}^2_{s,r}(G) = 0$ for all $r \geq 2$.*

Proof. View $\mathscr{O}(G)$ as the algebra for $G' = \oplus_{i\in I}\widehat{\mathbf{G}}_a$ (with formal comultiplication $X_i \mapsto Y_i + Z_i$). As noted in Remark B.2.2, $m^*(X_i) \equiv Y_i + Z_i \pmod{\deg \geq 2}$. Therefore the identity map $\mathscr{O}(G) \to \mathscr{O}(G)$ induces an isomorphism of complexes of graded objects $\mathrm{gr}\, C^*(G') \to \mathrm{gr}\, C^*(G)$. The Lemma follows from Lemma B.2.6. $\square$

Lemma B.2.8. *Let G be a connected commutative formal K-group with algebra B and augmentation ideal I. Let J be the maximal ideal of $B \widehat{\otimes} B$. If $B = K[\![\{X_i\}]\!]$ such that $m^*X_i \equiv X_i \widehat{\otimes} 1 + 1 \widehat{\otimes} X_i \pmod{\overline{J^n}}$, then there is an automorphism of B determined by $X_i \mapsto X_i'$ such that $X_i' \equiv X_i \pmod{\overline{I^n}}$ and $m^*X_i' \equiv X_i' \widehat{\otimes} 1 + 1 \widehat{\otimes} X_i' \pmod{\overline{J^{n+1}}}$.*

Proof. Writing $m^*X_i = X_i \widehat{\otimes} 1 + 1 \widehat{\otimes} X_i + b_i$, we see by definition that $b_i = -\partial X_i$, so b_i is a 2-cocycle. By Lemma B.2.7, there is some homogeneous $c_i \in \overline{I^n}$ such that $\partial c_i \equiv b_i \pmod{\overline{J^{n+1}}}$. Letting $X_i' = X_i + c_i$ and using the fact that the c_i are homogeneous of degree n shows that $X_i \mapsto X_i'$ gives an isomorphism $K[\![\{X_i\}]\!] \xrightarrow{\sim} K[\![\{X_i'\}]\!]$ such that (identifying the two rings) $m^*X_i' \equiv X_i' \widehat{\otimes} 1 + 1 \widehat{\otimes} X_i' \pmod{\overline{J^{n+1}}}$. $\square$

Proof of Theorem B.2.3. This follows from Remark B.2.2 and induction on Lemma B.2.8; the congruence condition on X_i and X_i' shows that in the limit of the induction, we have written $\mathscr{O}(G)$ as $K[\![\{X_i\}]\!]$ such that $m^*X_i = X_i \widehat{\otimes} 1 + 1 \widehat{\otimes} X_i$, as desired. The point is that if $\{X_{i,n}\}$ denotes the formal coordinates at the nth stage of the induction, then $X_i = \lim X_{i,n} \in \mathscr{O}(G)$ makes sense and $K[\![\{X_i\}]\!] \to \mathscr{O}(G)$ is an isomorphism by the Formal Nakayama's Lemma. Since

$$m^* X_i \equiv m^* X_{i,n} \equiv X_{i,n} \mathbin{\widehat{\otimes}} 1 + 1 \mathbin{\widehat{\otimes}} X_{i,n} \equiv X_i \mathbin{\widehat{\otimes}} 1 + 1 \mathbin{\widehat{\otimes}} X_i \pmod{\overline{J^n}}$$

for all $n \geq 1$, we see that in fact $m^* X_i = X_i \mathbin{\widehat{\otimes}} 1 + 1 \mathbin{\widehat{\otimes}} X_i$. □

References

[1] B. Conrad. Background Notes on p-Divisible Groups over Local Fields. Unpublished notes, available from Prof. de Jong's website `http://www-math.mit.edu/~dejong`.

[2] M. Demazure and P. Gabriel. *Groupes Algébriques, Tome I.* Masson et Cie, 1970.

[3] J.-M. Fontaine. *Groupes p-Divisibles sur les Corps Locaux*, volume 47–48 of *Astérisque*. Société Mathématique de France, 1977.

[4] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Springer-Verlag, 1984.

[5] M. Lazard. *Commutative Formal Groups.* Springer-Verlag, 1975.

[6] S. Bosch, W. Lütkebohmert and M. Raynaud. *Néron Models.* Springer-Verlag, 1980.

[7] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1986.

[8] B. Mazur and L. Roberts. Local Euler Characteristics. *Inventiones Mathematicae*, 9:201–234, 1970.

[9] S. Sen. On Automorphisms of Local Fields. *The Annals of Mathematics*, 90:33–46, 1969.

[10] J.-P. Serre. *Local Fields.* Springer-Verlag, 1995. (Translated from French by M. Greenberg).

[11] J. Tate. p-Divisible groups. In T. A. Springer, editor, *Proceedings of a Conference on Local Fields, Driebergen (The Netherlands) in 1966*, pages 158–183. Springer-Verlag, 1966.

[12] J. Tate. Finite Flat Group Schemes. In G. Cornell, J. Silverman and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 121–154. Springer-Verlag, 1997.

[13] W. Waterhouse. *Introduction to Affine Group Schemes.* Springer-Verlag, 1979.