LECTURE NOTES ON LUBIN-TATE SPACES

JOHANNES ANSCHÜTZ

Contents

1. Local class field theory via Lubin-Tate theory

In the first part of the course we want to discuss local class field theory via Lubin-Tate theory following [LT65], [Gol81] and [Ser13].

1.1. The global and local Kronecker-Weber theorem.

For $N \geq 1$ we set

$$\mu_N := \{z \in \mathbb{C} \mid z^N = 1\} = \{e^{2\pi i k/N} \in \mathbb{C} \mid k \in \{0, \dots, N-1\}\} \cong \mathbb{Z}/N$$

as the subgroup group in $\mathbb{C}^\times$ of N-roots of unity. Clearly, each element of μ_N is algebraic over $\mathbb{Q}$, and therefore lies in the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$. The subfield

$$\mathbb{Q}(\mu_N) \subseteq \overline{\mathbb{Q}}$$

generated by the elements of μ_N is called the N-th cyclotomic field, and it is the prototypical example of a Galois extension of $\mathbb{Q}$ with an *abelian* Galois group. Indeed, there exists a chain of canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \mathrm{Aut}(\mu_N) \cong (\mathbb{Z}/N)^\times.$$

Let us mention the following famous theorem of Kronecker-Weber.

Theorem 1.1 (Kronecker-Weber)**.** *Let $L/\mathbb{Q}$ be a finite abelian extension, i.e., a finite Galois extension with abelian Galois group. Then there exists an $N \geq 1$ and an embedding $L \subseteq \mathbb{Q}(\mu_N)$.*

In other words,

$$\mathbb{Q}(\mu_\infty) := \bigcup_N \mathbb{Q}(\mu_N)$$

is the maximal abelian extension of $\mathbb{Q}$. Theorem 1.1 is a massive generalization of the fact that each quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic field. For example, if $p \in \mathbb{Z}_{\geq 0}$ is an odd prime and $p^* = (-1)^{(p-1)/2}p$, then $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$ as $\mathbb{Q}(\zeta_p)$ contains a unique quadratic field by Galois theory and this field can only be ramified at p.

Now fix a prime p and consider the p-adic field $\mathbb{Q}_p$, which is defined as the completion of $\mathbb{Q}$ for the p-adic norm

$$|-|_p \colon \mathbb{Q} \to \mathbb{R}_{\geq 0},\ x \mapsto p^{-\nu_p(x)},$$

where

$$\nu_p(x) := \begin{cases} \infty, & x = 0 \\ a, & \text{if } x = p^a \frac{m}{n},\ m, n \in \mathbb{Z} \setminus \{0\},\ p \nmid mn, \end{cases} \tag{1}$$

is the p-adic valuation.

The theorem of Kronecker-Weber admits the following "local" analog over $\mathbb{Q}_p$.

Theorem 1.2 (local Kronecker-Weber)**.** *Let $L/\mathbb{Q}_p$ be a finite abelian extension. Then there exists an $N \geq 1$ and an embedding $L \subseteq \mathbb{Q}_p(\mu_N)$. In other words,*

$$\mathbb{Q}_p(\mu_\infty)$$

is the maximal abelian extension of $\mathbb{Q}_p$.

Here, $\mathbb{Q}_p(\mu_N)$ denotes the composite of $\mathbb{Q}_p$ and $\mathbb{Q}(\mu_N)$ inside an algebraic closure of $\mathbb{Q}_p$, and similarly for $\mathbb{Q}_p(\mu_\infty)$.

Actually, the conjunction of the local Kronecker-Weber theorem for all primes p implies the Kronecker-Weber theorem for $\mathbb{Q}$, cf. [Sut17, Lecture # 20].

It is one aim of the course to generalize Theorem 1.2 to arbitrary finite extensions of $\mathbb{Q}_p$ (or finite extensions of $\mathbb{F}_p((t))$), i.e., to describe the maximal abelian extension K^{ab} for any non-archimedean local field. We want to explain in the following how this description looks like, but first we will provide a reminder on (non-archimedean) local fields.

1.2. **Reminder on (non-archimedean) local fields.** The p-adic valuation

$$\nu_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

introduced in (Equation (1)) has the following properties:

(1) $\nu_p(x) = \infty$ if and only if $x = 0$.
(2) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ for $x, y \in \mathbb{Q}$.[1]
(3) $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$ for $x, y \in \mathbb{Q}$ (the "triangle inequality").

A field K equipped with a function $\nu \colon K \to \mathbb{Z} \cup \{\infty\}$ satisfying these properties for $\mathbb{Q}$ replaced by K is called a discretely valued field. Examples are $\mathbb{Q}$ with the p-adic valuation ν_p, $\mathbb{Q}_p$ with the canonical extension of ν_p (which we will still denote ν_p) or $\mathbb{F}_p((t))$ with the t-adic valuation

$$\nu_t \colon \mathbb{F}_p((t)) \to \mathbb{Z} \cup \{\infty\}, \quad \sum_{i \gg -\infty}^{\infty} a_i t^i \mapsto \inf\{i |\ a_i \neq 0\}.$$

Let (K, ν) be a discretely valued field. Then

$$\mathcal{O}_K := \{x \in K \mid \nu(x) \geq 0\}$$

is a subring of K (called "its ring of integers"), which satisfies the following properties:

(1) $\mathcal{O}_K$ is local with maximal ideal $\mathfrak{m}_K := \{x \in K \mid \nu(x) > 0\}$, in particular
$$\mathcal{O}_K^\times = \mathcal{O}_K \setminus \mathfrak{m}_K = \{x \in K \mid \nu(x) = 0\},$$
where the LHS denotes the units in $\mathcal{O}_K$,
(2) $\mathfrak{m}_K$ is generated over $\mathcal{O}_K$ by each element $\pi \in K$ with $\nu(x) = 1$ (such a π is called a "uniformizer").
(3) The non-zero ideals of $\mathcal{O}_K$ are indexed by $\mathbb{N}$ via
$$n \mapsto (\pi^n).$$
(4) The ring $\mathcal{O}_K$ is normal, i.e., integrally closed in K.

In other words, $\mathcal{O}_K$ is a discrete valuation ring, i.e., a local noetherian ring which is regular of Krull dimension 1. We see that for each uniformizer $\pi \in K$ the map

$$\mathbb{Z} \times \mathcal{O}_K \to K^\times, \ (n, u) \mapsto \pi^n u$$

is an isomorphism.

Exercise 1.3. Deduce all the above statements from the properties of ν.

The triangle inequality for ν has the following, maybe surprising, corollary.

Lemma 1.4 ("strong triangle inequality")**.** *If $x, y \in K$ and $\nu(x) \neq \nu(y)$, then*

$$\nu(x + y) = \min\{\nu(x), \nu(y)\}.$$

[1]Here we set $\infty + n = \infty$ for all $n \in \mathbb{Z}$.

Proof. We may assume $\nu(x) < \nu(y)$. Then

$$\nu(x) \geq \min\{\nu(x+y), \nu(y)\},$$

and $\nu(x) < \nu(y)$ together with the triangle inequality imply $\nu(x) \geq \nu(x+y) \geq \nu(x)$ and thus $\nu(x) = \nu(x+y)$ as desired. □

Let $a > 1$ be any real number, then the map

$$d\colon K \times K \to \mathbb{R},\ (x,y) \mapsto a^{-\nu(x-y)}$$

defines a metric on K and we say that K is complete if the metric space (K,d) is complete, i.e., Cauchy sequences in (K,d) converge to a unique limit. Each metric space admits a completion $(\hat{K},\hat{d})$, and in the case of (K,d) one can check that $\hat{K}$ is again naturally a field. The valuation ν on K extends uniquely to a valuation $\hat{\nu}$ on $\hat{K}$, and this makes $(\hat{K},\hat{\nu})$ into a discretely valued field (called the "completion" of (K,ν)). For example, $\mathbb{Q}_p$ was defined as the completion of $(\mathbb{Q},\nu_p)$ while the field $\mathbb{F}_p((t))$ of Laurent series with coefficients in $\mathbb{F}_p$ is already complete for its t-adic valuation. A different construction of the completion is the following: Take any element $x \in \mathfrak{m}_K \setminus \{0\}$ and define

$$\widehat{\mathcal{O}_K} := \varprojlim_{n \geq 1} \mathcal{O}_K/(x)^n$$

(the "(x)-adic completion" of $\mathcal{O}_K$). One checks that $\widehat{\mathcal{O}_K}$ is an integral domain, and that

$$\widehat{K} \cong \mathrm{Frac}(\widehat{\mathcal{O}_K}) \cong \widehat{\mathcal{O}_K}[\frac{1}{x}].$$

The essential point is that the subspace topology of $\mathcal{O}_K$ for the metric topology on K agrees with the (x)-adic topology of $\mathcal{O}_K$.

The following statement is an important property of complete discretely valued fields. It fails without assuming completeness.

Proposition 1.5. *Let (K,ν) be a complete discretely valued field, and L/K a finite extension of degree n. Then ν admits a unique extension to a valuation $\nu'\colon L \to \frac{1}{n}\mathbb{Z} \cup \{\infty\}$. For each $x \in L$ we have*

$$\nu'(x) = \frac{1}{n}\nu(N_{L/K}(x)),$$

where $N_{L/K}\colon L \to K$ is the norm, and L is complete.

The proof can be found in [Tia, Theorem 8.5.1.]. The critical point is to show that the function

$$\nu'(-) = \frac{1}{n}\nu(N_{L/K}(-))\colon L \to \frac{1}{n}\mathbb{Z} \cup \{\infty\}$$

satisfies the triangle inequality.

This in turn uses Hensel's lemma, which we recall here for later use.

Lemma 1.6 (Hensel's lemma)**.** *Let K be a complete discretely valued field with residue field k, $g(X) \in \mathcal{O}_K[X]$ a monic polynomial with reduction $\overline{g}(X) \in k[X]$. Assume that $\overline{g} = \overline{h}_1 \cdot \overline{h}_2$ for $\overline{h}_1, \overline{h}_2 \in k[X]$ such that $(\overline{h}_1, \overline{h}_2) = 1$. Then there exists a factorization*

$$g = h_1 \cdot h_2 \in \mathcal{O}_K[X]$$

with $\deg(h_i) = \deg(\overline{h}_i)$, $i = 1,2$, and $h_i \equiv \overline{h}_i$ mod $\mathfrak{m}_K$. Moreover, h_1, h_2 are unique with these properties up to multiplication by a unit in $\mathcal{O}_K$.

A sample application of Hensel's lemma is that for a prime p the field $\mathbb{Q}_p$ contains the $p-1$-th roots of unity as the polynomial $X^{p-1}-1 \in \mathbb{Z}_p[X]$ reduces to

$$X^{p-1}-1 = \prod_{\alpha \in \mathbb{F}_p^\times} (X-\alpha) \in \mathbb{F}_p[X].$$

Proof. The proof can be found in [Tia, Proposition 8.4.1.] (or more generally in [Sta17, Tag 0ALJ] for any ring R which is I-adically complete for an ideal $I \subseteq R$). We only sketch the proof of the special (actually, equivalent, cf. [Sta17, Tag 03QH]) case that

$$\overline{h}_1 = X - \beta$$

for some $\beta \in k$. We then have to show the existence of some $\alpha \in \mathcal{O}_K$ lifting β, which is a zero of g. The assumption $(\overline{h}_1, \overline{h}_2) = 1$ is equivalent to $g'(\beta) \neq 0$. Let $\alpha_0 \in \mathcal{O}_K$ be any lift of β. The idea of proof is to show that the Newton algorithm

$$\alpha_{n+1} := \alpha_n - \frac{g(\alpha_n)}{g'(\alpha_n)}, \quad n \geq 0,$$

for finding zeros of polynomials yields a Cauchy sequence $\{\alpha_n\}_{n\geq 0}$ in K whose limit α (which exists by completeness of K!) fulfils the requirements. We leave the details as an exercise. □

The ring of integers $\mathcal{O}_L$ agrees with the integral closure of $\mathcal{O}_K$ in L (this appears in the proof of Proposition 1.5). We record the following statement, which again needs completeness.

Lemma 1.7. *Let L/K be a finite extension of complete discretely valued fields of degree n. Then the ring $\mathcal{O}_L$ is a finite free $\mathcal{O}_K$-module of rank n.*

Proof. Cf. [Tia, Lemma 9.1.1.]. □

Let us now give the definition of a (non-archimedean) local field.

Definition 1.8. *A (non-archimedean) local field is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ for some prime p.*

Equivalently, a (non-archimedean) local field is the field of fractions of a complete discrete valuation ring A with *finite* residue field $k = A/\mathfrak{m}_A$. For a local field K we denote by

$$\nu_K \colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$$

its (normalized) valuation. By definition, finite extensions of local fields are again local fields.

We now recall some terminology concerning finite extensions of local fields.

Definition 1.9. *Let L/K be a finite extension of local fields of degree n, let $\mathcal{O}_K \subseteq \mathcal{O}_L$ be their rings of integers, and let $\pi_K \in \mathcal{O}_K$, $\pi_L \in \mathcal{O}_L$ be uniformizers.*

- *We call the ramification index of L/K the unique natural number $e := e(L/K) \geq 1$ such that $\pi_K \cdot \mathcal{O}_L = (\pi_L)^e$.*
- *We call the residue degree $f := f(L/K)$ of L/K the degree of the (finite) field extension $k := \mathcal{O}_K/(\pi_K) \to k_L := \mathcal{O}_L/(\pi_L)$.*
- *We call L/K unramified if $f = n$, and we call L/K totally ramified if $e = n$.*

Using Lemma 1.7 it is not difficult to see that $n = e \cdot f$. An extension L/K of degree n is totally ramified if and only if $L \cong K[X]/(g(X))$ for some polynomial

$$g(X) \in \mathcal{O}_K[X],$$

which is Eisenstein, i.e., $\nu_K(g(0)) = 1$ and $g(X) \equiv X^n \bmod \pi_K$. In this case, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ for each uniformizer $\pi_L \in L$. Indeed, we leave it as an exercise that for an Eisenstein polynomial $g(X) \in \mathcal{O}_K[X]$ the ring $L = K[X]/(g(X))$ is a field, whose valuation subring $\mathcal{O}_L$ is given by $\mathcal{O}_K[X]/(g(X))$. Conversely, assume L/K is totally ramified of degree n and $\pi_L \in L$ a uniformizer. Let

$$\nu' \colon L \to \frac{1}{n}\mathbb{Z} \cup \{\infty\}$$

be the unique extension of the normalized valuation $\nu = \nu_K$ on K. Then

$$1 = \nu_L(\pi_L) = e_{L/K}\nu'(\pi_L) = n\nu'(\pi_L) = \nu(N_{L/K}(\pi_L)),$$

which implies that the constant coefficient of the minimal polynomial $g(X) \in \mathcal{O}_K[X]$ of π_L equals π up to a unit in $\mathcal{O}_K$. As L/K is totally ramified, all other coefficients are divisible by π. The inclusion $\mathcal{O}_K[\pi_L] \subseteq \mathcal{O}_L$ must then be an equality as the residue fields of both local rings agree and both contain π_L. A reference for these facts is [Tia, Section 9.1.].

The unramified extensions are classified by finite extensions of the residue field.

Proposition 1.10. *Let K be a local field with residue field $k = \mathcal{O}_K/\mathfrak{m}_K$. Then the functor*

$$\begin{aligned} \{L \text{ finite, unramified extension of } K\} &\to \{l \text{ finite extension of } k\} \\ L &\mapsto k_L := \mathcal{O}_L/\mathfrak{m}_L \end{aligned}$$

is an equivalence of categories.

Proof. We provide a short sketch of proof, more details can be found in [Tia, Section 9.2.]. Each finite unramified extension L/K is separable, i.e., of the form

$$L \cong K[X]/(g(X))$$

for some separable polynomial $g(X) \in K[X]$, which we may assume to be monic and lie in $\mathcal{O}_K[X]$. Argueing a bit more carefully, we can arrange that

$$k_L \cong k[X]/(\overline{g}(X)),$$

where $\overline{g}(X) \in k[X]$ denotes the reduction of $g(X)$. Note that $\overline{g}(X)$ is then irreducible and thus automatically separable as k is a finite field. For any finite field extension L' of K we then have to see that the map

$$\begin{aligned} &\mathrm{Hom}_K(L, L') \\ &\cong \mathrm{Hom}_K(K[X]/(g(X)), L') \\ \cong &\{\alpha \in \mathcal{O}_{L'} \mid g(\alpha) = 0\} \\ \to &\{\beta \in k_{L'} \mid \overline{g}(\beta) = 0\} \\ \cong &\mathrm{Hom}_k(k_L, k_{L'}) \end{aligned}$$

is bijective. But this follows from Hensel's lemma Lemma 1.6 applied to L'. This finishes the proof of fully faithfulness. Essential surjectivity then follows by lifting the minimal polynomial of a generator of a finite (separable) extension l of k to a monic polynomial $g(X) \in \mathcal{O}_K[X]$ and setting $L = K[X]/(g(X))$. □

Exercise 1.11. Let (K, ν) be a complete, discretely valued field, and let $\mathcal{O}_K = \{x \in K \mid \nu(x) \geq 0\}$ be its ring of integers, $\mathfrak{m}_K \subseteq \mathcal{O}_K$ the maximal ideal, and $k = \mathcal{O}_K/\mathfrak{m}_K$ the residue field. Let $\pi \in \mathcal{O}_K$ be a uniformizer.

(1) Let $S \subseteq \mathcal{O}_K$ be a system of representatives for the residue classes in k, i.e., the map $\mathcal{O}_K \to k$ restricts to a bijection $S \cong k$. Prove that

$$\prod_{\mathbb{N}} S \to \mathcal{O}_K,\ (a_n)_n \mapsto \sum_{n=0}^{\infty} a_n \cdot \pi^n$$

is a well-defined homeomorphism, when the LHS is equipped with the product topology.

(2) Assume that $\mathrm{char}(k) = p > 0$ and that k is perfect. Then there exists a unique multiplicative map

$$[-]\colon k \to \mathcal{O}_K,$$

such that $\lambda \equiv [\lambda] \bmod (\pi)$ for all $\lambda \in K$.
Hint: Try $[\lambda] = \lim_{n\to\infty} (\tilde{\lambda^{1/p^n}}^{p^n})$ *with* $\tilde{\lambda^{1/p^n}}$ *a lift of* λ^{1/p^n}.

(3) Assume that $\mathrm{char}\, K = p > 0$ and that k is perfect. Prove that

$$K \cong k((\pi)).$$

1.3. **The maximal abelian extension of a local field.** Fix a prime p. Let K be a local field (with residual characteristic p) and fix a separable closure $\overline{K}$ of K. In this section, we want to analyze the maximal abelian extension

$$K^{\mathrm{ab}} := \bigcup_{L \subseteq \overline{K},\ L/K \text{ finite abelian}} L \subseteq \overline{K}$$

and see what Lubin-Tate theory can tell us about it.

Let $k = \mathcal{O}_K/\mathfrak{m}_K$ be the residue field of K. Recall that for each $m \geq 1$ the (finite) field $k \cong \mathbb{F}_q$ has a unique extension k_m of degree m (up to isomorphism). By Proposition 1.10 we obtain that for each $m \geq 1$ the local field K has a unique unramified extension

$$K_m^{\mathrm{nr}}$$

of degree m. From Proposition 1.10 we can conclude that

$$\mathrm{Gal}(K_m^{\mathrm{nr}}/K) \cong \mathrm{Gal}(k_m/k) \cong \mathrm{Frob}_q^{\mathbb{Z}/m},$$

where

$$\mathrm{Frob}_q\colon k_m \to k_m,\ x \mapsto x^q$$

is the q-Frobenius of k_m, which is known to generate $\mathrm{Gal}(k_m/k)$. Set

$$K^{\mathrm{nr}} := \bigcup_{m \geq 1} K_m^{\mathrm{nr}} \subseteq \overline{K},$$

which is the maximal unramified extension of K.

We can explicitly describe K^{nr}. Namely, let $\overline{k}$ be an algebraic closure of k. Then

$$\overline{k} = \bigcup_{(N,p)=1} k(\mu_N(\overline{k})),$$

where we set for any ring R

$$\mu_N(R) := \{y \in R \mid y^N = 1\}$$

as the group of N-roots of unity in R. We can conclude that

$$K^{\mathrm{nr}} = \bigcup_{(N,p)=1} K(\mu_N(\overline{K})).$$

Clearly, each K^{nr}_m is abelian and thus

$$K^{\mathrm{nr}} \subseteq K^{\mathrm{ab}}.$$

On Galois groups we therefore obtain an exact sequence

$$0 \to \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}}) \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(K^{\mathrm{nr}}/K) \to 0,$$

where

$$\mathrm{Gal}(K^{\mathrm{nr}}/K) = \varprojlim_{m\geq 1} \mathrm{Gal}(K_m/K) \cong \varprojlim_{m\geq 1} \mathbb{Z}/m =: \widehat{\mathbb{Z}}.$$

Because $\widehat{\mathbb{Z}}$ is a free profinite group it follows that we can pick a (non-canonical) splitting

$$s\colon \mathrm{Gal}(K^{\mathrm{nr}}/K) \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Therefore we can write

$$K^{\mathrm{ab}} = K^{\mathrm{nr}} \cdot K_s$$

with K_s the fixed field of the (closed) subgroup $s(\mathrm{Gal}(K^{\mathrm{nr}}/K)) \subseteq \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Note that K_s is necessarily totally ramified as $K = K_s \cap K^{\mathrm{nr}}$. Before we try to describe K_s, let us pause and analyze the case $K = \mathbb{Q}_p$ assuming the local Kronecker-Weber theorem Theorem 1.2. Then

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_\infty),$$

while

$$\mathbb{Q}_p^{\mathrm{nr}} = \bigcup_{(N,p)=1} \mathbb{Q}_p(\mu_N).$$

This suggest to look at the "missing part"

$$\mathbb{Q}_p(\mu_{p^\infty}) = \bigcup_{n\geq 1} \mathbb{Q}_p(\mu_{p^n})$$

as $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_{p^\infty})\mathbb{Q}_p^{\mathrm{nr}}$ (we leave it as an exercise to check that $\mathbb{Q}_p(\mu_{p^\infty}) = K_s$ for a suitable section s).

In this case, there exists a canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \cong \varprojlim_n (\mathbb{Z}/p^n)^\times \cong \mathbb{Z}_p^\times.$$

In particular, there exists a non-canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

Local class field theory asserts that such an isomorphism exists for an arbitrary local field K.

Theorem 1.12. *Let K be a local field. Then the Galois group of K^{ab} over K is (non-canonically) isomorphic to*

$$\mathcal{O}_K^\times \times \widehat{\mathbb{Z}},$$

where $\mathcal{O}_K \subseteq K$ denotes the ring of integers. In fact, there exists a canonical morphism $K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, which identifies the target with the profinite completion of $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$.

Let us elaborate a bit more on the canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times.$$

For this, let us fix some $n \geq 1$ and consider the polynomial

$$X^{p^n} - 1$$

and its factorization

$$X^{p^n} - 1 = \Phi_{p^n}(X)\Phi_{p^{n-1}}(X)\dots\Phi_p(X)\Phi_1(X)$$

into the cyclotomic polynomials (e.g., $\Phi_1(X) = X-1$, $\Phi_p(X) = X^{p-1}+\ldots+X+1$). We get the decomposition

$$\mathbb{Q}_p[X]/(X^{p^n}-1) \cong \mathbb{Q}_p(\mu_{p^n}) \times \mathbb{Q}_p(\mu_{p^{n-1}}) \times \ldots \times \mathbb{Q}_p(\mu_p) \times \mathbb{Q}_p. \tag{2}$$

Clearly, given $a \in \mathbb{Z}$ the map

$$X \mapsto X^a$$

induces a homomorphism

$$\varphi_a \colon \mathbb{Q}_p[X]/(X^{p^n}-1) \to \mathbb{Q}_p[X]/(X^{p^n}-1)$$

of $\mathbb{Q}_p$-algebras, which only depends on the residue class of a modulo p^n.[2] The resulting map

$$\iota \colon \mathbb{Z}/p^n \to \mathrm{End}_{\mathbb{Q}_p}(\mathbb{Q}_p[X]/(X^{p^n}-1)),\ a \mapsto \varphi_a$$

is a map of multiplicative monoids, i.e., $\varphi_{a\cdot b} = \varphi_a \circ \varphi_b$, and we get a natural homomorphism of groups

$$\iota \colon (\mathbb{Z}/p^n)^\times \to \mathrm{Aut}_{\mathbb{Q}_p}(\mathbb{Q}_p[X]/(X^{p^n}-1)).$$

But each automorphism of $\mathbb{Q}_p[X]/(X^{p^n}-1)$ has to respect the decomposition (Equation (2)), and thus preserve each factor. In particular, we obtain the natural morphism

$$(\mathbb{Z}/p^n)^\times \to \mathrm{Aut}_{\mathbb{Q}_p}(\mathbb{Q}_p(\mu_{p^n}))$$

which yields the canonical isomorphism

$$\mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$$

by passing to the inverse limit over n.

We will see that the above situation generalizes to an arbitrary local field K if we do the twist of rewriting everything in terms of $Y := X - 1$. The decomposition (Equation (2)) then reads

$$\mathbb{Q}_p[Y]/((1+Y)^{p^n}-1) \cong \mathbb{Q}_p(\mu_{p^n}) \times \ldots \times \mathbb{Q}_p$$

according to the factorization

$$(1+Y)^{p^n} - 1 = pY + \binom{p}{2}Y^2 + \ldots + pY^{p^n-1} + Y^{p^n} = \Phi_{p^n}(1+Y)\cdots\Phi_0(1+Y).$$

For $a \in \mathbb{Z}$ the endomorphism φ_a becomes the morphism

$$Y \mapsto (1+Y)^a - 1.$$

[2] $\mathbb{Q}_p[X]/(X^{p^n}-1)$ is isomorphic to the group algebra $\mathbb{Q}_p[\mu_{p^n}]$ and φ_a is induced by the multiplication by a on μ_{p^n}.

It is convenient to formulate the situation independently of n by passing to power series. For this it is worth noting that the $\mathbb{Z}$-action $a \mapsto \varphi_a$ is actually defined over $\mathbb{Z}_p$ as for each $a \in \mathbb{Z}$ the polynomial

$$(1+Y)^a - 1$$

has coefficients in $\mathbb{Z}$.

Let us set for $a \in \mathbb{Z}$ and $n \geq 1$

$$\varphi_{a,n} := \varphi_{\overline{a}} \colon \mathbb{Z}_p[Y]/((1+Y)^{p^n} - 1) \to \mathbb{Z}_p[Y]/((1+Y)^{p^n} - 1),$$

with $\overline{a} \in \mathbb{Z}/p^n$ the residue class of a. Then the diagram

$$\begin{array}{ccc} \mathbb{Z}_p[Y]/((1+Y)^{p^n} - 1) & \xrightarrow{\varphi_{a,n}} & \mathbb{Z}_p[Y]/((1+Y)^{p^n} - 1) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[Y]/((1+Y)^{p^{n-1}} - 1) & \xrightarrow{\varphi_{a,n-1}} & \mathbb{Z}_p[Y]/((1+Y)^{p^{n-1}} - 1) \end{array}$$

with vertical arrows being the canonical projections commutes for any $a \in \mathbb{Z}$ and $n \geq 1$.

Lemma 1.13. *The natural projections constitute an isomorphism*

$$\mathbb{Z}_p[[Y]] \cong \varprojlim_n \mathbb{Z}_p[Y]/((1+Y)^{p^{n-1}} - 1)$$

Proof. We first need to construct the morphism

$$\mathbb{Z}_p[[Y]] \to \varprojlim_n \mathbb{Z}_p[Y]/((1+Y)^{p^n} - 1).$$

For $m, n \geq 0$ the element $Y \in \mathbb{Z}/p^m[Y]/((1+Y)^{p^n} - 1)$ is nilpotent because

$$(1+Y)^{p^n} - 1 \equiv Y^{p^n} \bmod (p).$$

Therefore the canonical morphism $\mathbb{Z}_p[Y] \to \mathbb{Z}/p^m[Y]/((1+Y)^{p^n} - 1)$ extends uniquely to a morphism

$$\mathbb{Z}_p[[Y]] \to \mathbb{Z}/p^m[Y]/((1+Y)^{p^n} - 1)$$

taking the limit over m, n yields the desired morphism, and this morphism is easily seen to be injective and continuous, when $\mathbb{Z}_p[[Y]] \cong \prod_{\mathbb{N}} \mathbb{Z}_p$ is equipped with the product topology. For each $n \geq 1$ the morphism

$$\mathbb{Z}_p[[Y]] \to \mathbb{Z}_p[Y]/((1+Y)^{p^{n-1}} - 1)$$

is surjective. By compactness of $\mathbb{Z}_p[[Y]]$ this implies surjectivity in the limit. This finishes the proof. □

Let us note that the same statement is wrong when $\mathbb{Z}_p$ is replaced by $\mathbb{Q}_p$, e.g., the ring

$$\varprojlim \mathbb{Q}_p[Y]/((1+Y)^{p^n} - 1)$$

is has Krull dimension 0. By Lemma 1.13 we get an endomorphism (as a $\mathbb{Z}_p$-algebra)

$$\varphi_{a,\infty} \colon \mathbb{Z}_p[[Y]] \to \mathbb{Z}_p[[Y]].$$

for each $a \in \mathbb{Z}$ by taking the limit of the $\varphi_{a,n}$. This endomorphism is given by the map

$$\varphi_{a,\infty} \colon \mathbb{Z}_p[[Y]] \to \mathbb{Z}_p[[Y]],\ Y \mapsto (1+Y)^a - 1 := \sum_{i \geq 1} \binom{a}{i} Y^i$$

with

$$\binom{a}{i} := \frac{a(a-1)\cdot(a-i+1)}{i!}.$$

We can do better. Namely, for each $a \in \mathbb{Z}_p$ and each $i \geq 1$ the binomial coefficient $\binom{a}{i}$ lies in $\mathbb{Z}_p$ because $\binom{a}{i}$ is continuous in a, $\mathbb{Z} \subseteq \mathbb{Z}_p$ is dense, $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is closed and $\binom{b}{i} \in \mathbb{Z} \subseteq \mathbb{Z}_p$ for $b \in \mathbb{Z}$. Hence, we get by the exact same formula an endomorphism $\varphi_{a,\infty}$ of $\mathbb{Z}_p[[Y]]$ for each $a \in \mathbb{Z}_p$.

The resulting map

$$\iota \colon \mathbb{Z}_p \to \mathrm{End}_{\mathbb{Z}_p}(\mathbb{Z}_p[[Y]]),\ a \mapsto \varphi_{a,\infty}$$

satisfies again

$$\varphi_{a\cdot b,\infty} = \varphi_{a,\infty} \circ \varphi_{b,\infty}.$$

Now we arrived at a concise viewpoint on the field extension

$$\mathbb{Q}_p(\mu_{p^\infty})$$

of $\mathbb{Q}_p$ and Lubin-Tate were able to generalize this viewpoint to all local fields. Before going into their resuls, let us pause and summarize how the data of ι allows to reconstruct for a given $n \geq 1$ the field extension

$$\mathbb{Q}_p(\mu_{p^n})$$

of $\mathbb{Q}_p$. Namely, $\mathbb{Q}_p(\mu_{p^n})$ is the largest field extension occuring in the decomposition of

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[Y]]/(\iota(p^n))$$

into fields. Note the interplay of $\mathbb{Q}_p$ and $\mathbb{Z}_p$: The $\mathbb{Z}_p$-algebra

$$\mathbb{Z}_p[[Y]]/((1+Y)^{p^n} - 1)$$

is local with maximal ideal (p, Y), and does in particular not decompose into a product of fields. However, after tensoring with $\mathbb{Q}_p$ it does!

For a general local field K Lubin-Tate constructed a similar datum, namely a map

$$\iota \colon \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_K[[Y]])$$

converting multiplication into composition. The map ι is not unique but depends on two input data:

(1) a uniformizer $\pi \in K$,
(2) a power series $[\pi](Y) \in \mathcal{O}_K[[Y]]$ satisfying

$$[\pi](Y) \equiv \pi Y \bmod (Y)^2, \quad [\pi](Y) \equiv Y^q \bmod (\pi_K),$$

where $q := \sharp k$ with $k := \mathcal{O}_K/\mathfrak{m}_K$ the residue field of K.

For example, if $K = \mathbb{Q}_p$, $\pi = p$ and

$$[p](Y) = (1+Y)^p - 1 = pY + \binom{p}{2} Y + \ldots + pY^{p-1} + Y^p.$$

In this case

$$\iota(p)(Y) = [p](Y),$$

and in general we will have

$$\iota(\pi)(Y) = [\pi](Y).$$

Let us write

$$\iota_{\pi,[\pi]}$$

for ι if we want to point out the dependence of ι on π and $[\pi]$. Then $\iota_{\pi,[\pi]}$ will be uniquely determined by multiplicativity and the requirement

$$\iota_{\pi,[\pi]}(\pi)(Y) = [\pi](Y).$$

To ease notation, let us define

$$A := \mathcal{O}_K,$$

and

$$\mathcal{F}_\pi := \{f \in A[[Y]] \mid f \equiv \pi Y \bmod (Y)^2,\ f \equiv Y^q \bmod (\pi)\}.$$

The construction of $\iota_{\pi,[\pi]}$ (and much more) will rest on the following beautiful lemma of Lubin-Tate.

Lemma 1.14 ([LT65, Lemma 1])**.** *Let $f(Y), g(Y) \in \mathcal{F}_\pi, n \geq 1$ and let*

$$L(Y_1, \dots, Y_n) = \sum_{i=1}^{n} a_i Y_i$$

be a linear form with $a_1, \dots, a_n \in A$. Then there exists a unique power series $F(Y_1, \dots, Y_n) \in A[[Y_1, \dots, Y_n]]$ such that

$$F(Y_1, \dots, Y_n) \equiv L(Y_1, \dots, Y_n) \text{ mod } (Y_1, \dots, Y_n)^2,$$

and

$$f(F(Y_1, \dots, Y_n)) = F(g(Y_1), \dots, g(Y_n)).$$

For example, pick $a \in A$, $f = g = [\pi]$ and $L(Y) = aY$. Then the F provided by Lemma 1.14 will yield $\iota_{\pi,[\pi]}(a)$!

Proof. The proof will be by inductively finding a power series $F_r(Y_1, \dots, Y_n) \in A[[Y_1, \dots, Y_n]]$ satisfying

$$f(F(Y_1, \dots, Y_n)) = F(g(Y_1), \dots, g(Y_n)) \bmod (Y_1, \dots, Y_n)^r.$$

For $r = 1$ we can take $F_r = 0$, and less trivially for $r = 2$ we can take $F_2(Y_1, \dots, Y_n) = L(Y_1, \dots, Y_n)$. Indeed,

$$f(Y) \equiv \pi Y \equiv g(Y) \bmod (Y)^2,$$

which implies

$$f(F_2(Y_1, \dots, Y_n)) \equiv \pi(L(Y_1, \dots, Y_n)) \equiv F_2(g(Y_1), \dots, g(Y_n)) \bmod (Y_1, \dots, Y_n)^2.$$

Now assume that F_r has been found for $r \geq 2$. Our solution F_{r+1} must have the form

$$F_{r+1} = F_r + G_r$$

with $G_r \in (Y_1, \dots, Y_n)^r$. We can calculate

$$f(F_{r+1}(Y_1, \dots, Y_n)) \equiv f(F_r(Y_1, \dots, Y_n)) + \pi G_r(Y_1, \dots, Y_n) \bmod (Y_1, \dots, Y_n)^{r+1}$$

because $f \in \mathcal{F}_\pi$. For the similar reason $g \in \mathcal{F}_\pi$ we get

$$F_{r+1}(g(Y_1), \dots, g(Y_n)) = F_r(g(Y_1), \dots, g(Y_n)) + \pi^r G_r(Y_1, \dots, Y_n) \bmod (Y_1, \dots, Y_n)^{r+1}.$$

The equality

$$f(F_{r+1}(Y_1, \dots, Y_n)) \equiv F_{r+1}(g(Y_1), \dots, g(Y_n)) \bmod (Y_1, \dots, Y_n)^{r+1} \tag{3}$$

is therefore equivalent to

$$(\pi^r-\pi)G_r(Y_1,\dots,Y_n) \equiv f(F_r(Y_1,\dots,Y_n))-F_r(g(Y_1),\dots,g(Y_n)) \bmod (Y_1,\dots,Y_n)^{r+1}.$$

The element $\pi^{r-1}-1 \in A$ is a unit (because A π lies in the Jacobson ideal of A), and $\pi \in A$ is a non-zerodivisor on

$$A[[Y_1,\dots,Y_n]]/(Y_1,\dots,Y_n)^{r+1}.$$

Therefore, G_r solving (Equation (3)) exists (and is then uniquely determined modulo $(Y_1,\dots,Y_n)^{r+1}$) if and only of

$$f(F_r(Y_1,\dots,Y_n)) - F_r(g(Y_1),\dots,g(Y_n)) \in A[[Y_1,\dots,Y_n]]/(Y_1,\dots,Y_n)^{r+1}$$

is divisible by π. But

$$f(F_r(Y_1,\dots,Y_n))-F_r(g(Y_1),\dots,g(Y_n)) \equiv (F_r(Y_1,\dots,Y_n))^q-F_r(Y_1^q,\dots,Y_n^q)) \equiv 0 \bmod \pi$$

because the map $z \mapsto z^q$ is an *A-algebra* homomorphism modulo π. Having found the F_r we can set $F \in A[[Y_1,\dots,Y_n]]$ as the unique power series satisfying

$$F \equiv F_r \bmod (Y_1,\dots,Y_n)^r.$$

This finishes the proof.[3] □

Remark 1.15. Note that we only used the facts that A is π-complete and π-torsion free, that π divides p and that the map $x \mapsto x^q$ is the identity on A/π. Moreover, it works if we replace q be some power $q^h, h \geq 1$..

Let us now fix $f \in \mathcal{F}_\pi$, e.g.,

$$f = \pi Y + Y^q$$

is a perfectly valid choice. For each $a \in A$ Lemma 1.14 yields a uniquely determined power series

$$[a]_f \in A[[Y]],$$

such that

$$[a]_f(Y) \equiv aY \bmod (Y)^2$$

and

$$f \circ [a]_f = [a]_f \circ f.$$

Here, we defined

$$g \circ h(Y) := g(h(Y)) \in A[[Y]]$$

for two power series $g, h \in A[[Y]]$ with vanishing constant term. The uniqueness in Lemma 1.14 and the equality

$$a(bY) \equiv (ab)Y \bmod (Y)^2$$

implies that

$$[ab]_f = [a]_f \circ [b]_f$$

for $a, b \in A$. We can record this as the following corollary.

Corollary 1.16. *For each uniformizer $\pi \in A$ and each $f = [\pi] \in \mathcal{F}_\pi$ there exists a unique multiplicative map*

$$\iota_{\pi,[\pi]} \colon A \to \mathrm{End}_A(A[[Y]]),\ a \mapsto (Y \mapsto [a]_f(Y))$$

such that $\iota_{\pi,[\pi]}(\pi)(Y) = f(Y)$ and $\iota_{\pi,[\pi]}(a) \equiv aY$ mod $(Y)^2$ for each $a \in A$.

[3] These calculations are faciliated using the following general fact: Let S be any ring and $F(X) \in S[X]$ a polynomial. If $\varepsilon \in S$ satisfies $\varepsilon^2 = 0$, then $F(X+\varepsilon) = F(X) + \varepsilon \cdot \frac{\partial}{\partial X} F(X)$.

For $A = \mathbb{Z}_p, \pi = p$ and $f(Y) = pY + \binom{p}{2}Y^2 + \ldots + Y^p$ we, of course, recover our previous ι. Back in the general case, the quotient

$$A[[Y]]/([\pi^n](Y))$$

is a finite free A-module of rank q^n (with basis $1, Y, \ldots, Y^{q^n-1}$). Recall that $K = \mathrm{Frac}(A)$. In complete analogy to (Equation (2)) we want to find a decomposition

$$K[[Y]]/([\pi]^n](Y)) \cong K_{\pi,n} \times K_{\pi,n-1} \times \ldots \times K_{\pi,1} \times K \tag{4}$$

for a nested sequence (inside some fixed separable closure $\overline{K}$ of K)

$$K \subseteq K_{\pi,1} \subseteq K_{\pi,2} \subseteq \ldots$$

of abelian extensions $K_{\pi,n}$ with Galois group

$$\mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi)^n)^\times.$$

If $f = [\pi]$ is a polynomial, then this means to factor the polynomial

$$[\pi^n](Y)$$

into analogs of the cyclotomic polynomials. The isomorphism $\mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi)^n)^\times$ will be constructed in the same way as for $K = \mathbb{Q}_p$: The multiplicative morphism

$$\iota_{\pi,[\pi]} \colon \mathcal{O}_K \to \mathrm{End}_K(K[[Y]]), a \mapsto (Y \mapsto [a]_f(Y))$$

induces for each $n \geq 1$ (because of the crucial identity $[p]_f \circ [a]_f = [a]_f \circ [p]!$) a morphism of groups

$$\iota_n \colon \mathcal{O}_K^\times \to \mathrm{Aut}_K(K[[Y]]/([\pi]^n)),$$

and the resulting $\mathcal{O}_K^\times$-action must preserve the decomposition (Equation (4)) which yields the desired isomorphism

$$\mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi)^n)^\times.$$

using that

$$\mathcal{O}_K^\times/1 + (\pi)^n \cong (\mathcal{O}_K/(\pi)^n)^\times.$$

Setting

$$K_{\pi,\infty}$$

yields then the desired description

$$K^{\mathrm{ab}} = K_{\pi,\infty}K^{\mathrm{nr}}.$$

There is however no reason to expect that

$$K_{\pi,\infty} = K_{\pi',\infty}$$

for different uniformizer $\pi, \pi' \in K$, and it is thus a bit surprising that the composite

$$K_{\pi,\infty}K^{\mathrm{nr}}$$

will turn out to be independent of π. Before handling this question (and also to derive the decomposition (Equation (4))) we will make a short interlude on the notion of a *formal A-module*, which is one of the central notions appearing in this course.

1.4. **Formal groups and formal A-modules.** Slightly lightening the notation of Section 1.3 we let A denote a complete discrete valuation ring with finite residue field k of characteristic p. We fix as before a uniformizer $\pi \in A$, and set $q := \sharp k$. As before, define

$$\mathcal{F}_\pi := \{f \in A[[X]] \mid f(X) \equiv \pi X \bmod (X)^2,\ f(X) \equiv X^q \bmod (\pi)\}.$$

The starting point for this subsection are the following nearly obvious corollaries of Lemma 1.14.

Lemma 1.17. *For each $f \in \mathcal{F}_\pi$ there exists a unique power series $F_f(X,Y) \in A[[X,Y]]$ such that*

$$F_f(X,Y) \equiv X + Y \ mod\ (X,Y)^2,$$

and

$$f(F_f(X,Y)) \equiv F_f(f(X), f(Y)).$$

For each $f, g \in \mathcal{F}_\pi$ and $a \in A$ there exists a unique power series $[a]_{f,g}(X) \in A[[X]]$ such that

$$[a]_{f,g}(X) \equiv aX \ mod\ (X)^2,$$

and

$$f([a]_{f,g}(X)) = [a]_{f,g}(g(X)).$$

For brevity, we will write $[a]_f = [a]_{f,f}$.

Proof. This is a direct consequence of Lemma 1.14. In the first case, one considers

$$f, g = f, \quad L(X,Y) = X + Y,$$

and in the second

$$f, g, L(X) = aX. \qquad \square.$$

For example, if $A = \mathbb{Z}_p$ and $f(Y) = (1+Y)^p - 1$, then

$$F_f(X,Y) = X + Y + XY.$$

Indeed,

$$\begin{aligned} & f(F_f(X,Y)) \\ =& f(X + Y + XY) \\ =& (1 + X + Y + XY)^p - 1 \\ =& ((1+X)(1+Y))^p - 1 \\ =& (1+X)^p (1+Y)^p - 1 \end{aligned}$$

while

$$\begin{aligned} & F_f(f(X), f(Y)) \\ =& (1+X)^p - 1 + (1+Y)^p - 1 + ((1+X)^p - 1)((1+Y)^p - 1)) \\ =& (1+X)^p + (1+Y)^p - 2 + (1+X)^p (1+Y)^p - (1+Y)^p - (1+X)^p + 1 \\ =& (1+X)^p (1+Y)^p - 1. \end{aligned}$$

In general, we can record the following properties of the $F_f, [a]_{f,g}$.

Theorem 1.18 ([LT65, Theorem 1])**.** *For $f, g, h \in \mathcal{F}_\pi$ and $a, b \in A$, the following properties hold true:*

1. $F_f(X,0) = X, F_f(0,Y) = Y$,
2. $F_f(F_f(X,Y), Z) = F_f(X, F_f(Y,Z))$
3. $F_f(X,Y) = F_f(Y,X)$,

(4) $F_f([a]_{f,g}(X), [a]_{f,g}(Y)) = [a]_{f,g}(F_g(X,Y))$
(5) $[a]_{f,g}([b]_{g,h}(X)) = [ab]_{f,h}(X)$
(6) $[a+b]_{f,g}(X) = F_f([a]_{f,g}(X), [b]_{f,g}(X))$
(7) $[\pi]_f(X) = f(X), [1]_f(X) = X.$

Proof. All of these statements follow from Lemma 1.14 and Lemma 1.17 by the same pattern (which was already used for the construction of ι in the previous section): First check that both sides of an equation commute in the appropriate sense with f, g or h, and then check the identity modulo degree 2, where they reduce to the equalities

$$\begin{aligned} X + 0 = X, 0 + Y = Y, \\ (X + Y) + Z = X + (Y + Z), \\ X + Y = Y + X, \\ aX + aY = aX + aY, \\ a(bX) = (ab)X, \\ (a + b)X = aX + bX, \\ \pi X = \pi X, \\ 1 \cdot X = X. \end{aligned}$$

We leave the details as an exercise. □

Item 1, Item 2 imply that F_f is a so-called (one-dimensional) *formal group law* over A, Item 3 implies that this formal group is commutative, while Item 4 implies that $[a]_{f,g}$ defines a homomorphism between the formal group laws F_f and F_g. Finally, Item 4, Item 5, Item 6, Item 7 imply that $a \mapsto [a]_f$ defines a *ring* homomorphism

$$A \to \mathrm{End}_{\mathrm{FGL}(A)}(F_f),$$

where the RHS denotes the endomorphism ring of the formal group law F_f over A. Let us now give the relevant general definitions.

Definition 1.19. *Let R be any (commutative, unital) ring. Then a power series $F \in R[[X,Y]]$ is called a (one-dimensional) formal group law if*

(1) *$F(X,0) = X$, $F(0,Y) = Y$. In particular, $F(X,Y) \equiv X + Y$ mod $(X,Y)^2$.*
(2) *$F(X, F(Y,Z)) = F(F(X,Y), Z) \in R[[X,Y,Z]]$.*
(3) *It is called commutative, if additionally the equality $F(X,Y) = F(Y,X)$ holds true.*

Note that Item 2 is well-defined because $F(X,Y)$ has no constant term. The easiest example for a formal group law is the power series

$$F_{\mathrm{add}}(X,Y) := X + Y,$$

which defines the so-called "additive" formal group law.

Let us check explicitly that these conditions hold for any ring R and the power series

$$F_{\mathrm{mul}}(X,Y) := X + Y + XY$$

from before (F_{mul} is the so-called "multiplicative" formal group law). Indeed, Item 1, Item 3 are obvious and for Item 2 we can calculate

$$\begin{aligned} & F(X, F(Y,Z)) \\ =& X + F(Y,Z) + X \cdot F(Y,Z) \\ =& X + (Y + Z + Y \cdot Z) + X(Y + Z + Y \cdot Z) \\ =& (X + Y + X \cdot Y) + Z + (X + Y + X \cdot Y)Z \\ =& F(F(X,Y),Z). \end{aligned}$$

We now define homomorphisms between formal group laws.

Definition 1.20. *Let R be a ring and $F_1, F_2 \in R[[X,Y]]$ two formal group laws. A homomorphism*

$$\varphi \colon F_1 \to F_2$$

is a power series $\varphi(X) \in R[[X]]$ such that

(1) $\varphi(X) \equiv 0$ *mod* (X)
(2) $F_2(\varphi(X), \varphi(Y)) = \varphi(F_1(X,Y)) \in R[[X,Y]]$.

With this notion of homomorphisms we can consider the category

$$\mathrm{FGL}(R)$$

of formal group laws over R. For example, $\varphi(X) = X$ defines the identity.

To enlighten the definition of a formal group law we now discuss a different viewpoint on them. This viewpoint will help to clarify later how formal group laws relate to (formal) schemes. The crucial point is to interpret rings of power series functorially.

Let us fix a ring R and let

$$\mathrm{Alg}_R$$

be the category of (commutative, unital) R-algebras (thus formally Alg_R is the under category $R/(\mathrm{Ring})$). Let us equip $R[[X]]$ with the (X)-adic topology, i.e., the uniqe topology with a basis of open neighborhoods of 0 given by $\{(X)^n\}_{n \geq 1}$, which makes $R[[X]]$ into a topological ring. For any R-algebra $S \in \mathrm{Alg}_R$ we can consider the set

$$\mathrm{Hom}_{\mathrm{cts},R}(R[[X]], S)$$

of continuous R-algebra homomorphisms, where S is equipped with the discrete topology. As $\{0\} \subseteq S$ is open, for every continuous morphism $\varphi \colon R[[X]] \to S$ there must exist an $n \geq 1$ such that

$$\varphi(X^n) = 0.$$

In particular, $f(X) \in S$ is nilpotent. For each element

$$s \in \mathcal{N}il(S) := \{x \in S \mid s \text{ nilpotent } \}.$$

there exists conversely a unique continuous R-algebra homomorphism

$$\varphi \colon R[[X]] \to S$$

sening X to s. We obtain a natural isomorphism

$$\mathrm{Hom}_{\mathrm{cts},R}(R[[X]], -) \cong \mathcal{N}il(-)$$

of functors $\mathrm{Alg}_R \to (\mathrm{Sets})$. More generally, we get

$$\mathrm{Hom}_{\mathrm{cts},R}(R[[X_1, \ldots, X_n]], -) \cong \mathcal{N}il^n(-)$$

for any $n \geq 1$, when $R[[X_1, \dots, X_n]]$ is equipped with the $(X_1, \dots, X_n)$-adic topology.

Now consider a formal group law $F \in R[[X, Y]]$ over a ring R. Pulling back a continuous homomomorphism

$$\varphi \colon R[[X, Y]] \to S$$

along the continuous map

$$R[[X]] \to R[[X, Y]], \ X \mapsto F(X, Y)$$

we get a natural transformation

$$\eta^F \colon \mathcal{N}il \times \mathcal{N}il \to \mathcal{N}il$$

(this only uses the F has no constant term). The definition of a formal group law implies now that for each R-algebra S the resulting operation

$$\eta^F_S \colon \mathcal{N}il(S) \times \mathcal{N}il(S) \to \mathcal{N}il(S)$$

turns $\mathcal{N}il(S)$ into a *group with unit* $0 \in \mathcal{N}il(S)$*!*

For $S \in \mathrm{Alg}_R$ and $x, y \in \mathcal{N}il(S)$ let us set

$$x +_F y := \eta^F((x, y)) = F(x, y) \in \mathcal{N}il(S).$$

From Definition 1.19 it is clear that

$$0 +_F y = y,$$
$$x +_F 0 = x$$

and

$$(x +_F y) +_F z = x +_F (y +_F z)$$

for any $x, y, z \in \mathcal{N}il(S)$. In order to obtain that $\mathcal{N}il(S)$ is really a group we have to prove that inverses exists. This is provided by the next lemma.

Lemma 1.21. *Let R be a ring and $F \in R[[X, Y]]$ be a formal group law. Then there exists a unique power series $\varphi \in R[[X]]$ such that*

$$F(\varphi(X), X) = 0.$$

Having φ, it is clear that

$$\varphi(x) +_F x = 0$$

for any $S \in \mathrm{Alg}_R, x \in \mathcal{N}il(S)$, which is sufficient to see that each element in $\mathcal{N}il(S)$ has an inverse with respect to $+_F$.

Proof. We construct inductively a power series $\varphi_n \in R[[X]]$ such that

$$F(\varphi_n(X), X)) \equiv 0 \bmod X^n. \tag{5}$$

Clearly, we can set $\varphi_0(X) = -X$. Now given $\varphi_n(X)$ satisfying (Equation (5)) write

$$F(\varphi_n(X), X) \equiv r \cdot X^n \bmod X^{n+1}$$

for some $r \in R$. We can deduce that for $s \in R$ arbitrary

$$\begin{aligned} &F(\varphi_n(X) + sX^n, X) \\ \equiv &F(\varphi_n(X), X) + sX^n \bmod X^{n+1} \\ \equiv &rX^n + sX^n \bmod X^{n+1} \end{aligned}$$

because $F(X, Y) = X + Y +$ higher terms. Thus we can set

$$\varphi_{n+1}(X) = \varphi_n(X) - rX^n.$$

This is moreover the unique possible choice, and the proof is finished. □

We call the functor

$$\mathcal{G}_F\colon \mathrm{Alg}_R \to (\mathrm{Grp}),\ S \mapsto (\mathcal{N}il(S), (-) +_F (-))$$

the "formal group associated to the formal group law F". It is clear that for each $S \in \mathrm{Alg}_R$ the group $\mathcal{G}_F(S)$ is commutative if F is commutative (in fact, only if).

We will see later that if conversely

$$\mathcal{G}\colon \mathrm{Alg}_R \to (\mathrm{Grp})$$

is a functor, such that on underlying set-valued functors $\mathcal{G} = \mathcal{N}il$ and

$$0\colon * \to \mathcal{G} = \mathcal{N}il$$

is the unit for this group structure, then $\mathcal{G} = \mathcal{G}_F$ for a uniquely determined formal group law $F \in R[[X, Y]]$.

Example 1.22. The functor

$$\mathbb{G}_m\colon \mathrm{Alg}_R \to (\mathrm{Ab}),\ S \mapsto S^\times$$

is called the "multiplicative group" over R. For each $S \in \mathrm{Alg}_R$ and each $x \in \mathcal{N}il(S)$ we get $1 + x \in S^\times$. This defines a natural inclusion(=monomorphism)

$$\mathcal{N}il \to \mathbb{G}_m,\ x \in \mathcal{N}il(S) \mapsto 1 + x \in X^\times,$$

which endows the functor $\mathcal{N}il$ with a group structure. From the equation

$$(1 + x)(1 + y) = 1 + x + y + xy$$

we can see that this group structure is induced by the multiplicative formal group law

$$F_{\mathrm{mul}}(X, Y) = X + Y + XY.$$

This can be reinterpreted as saying that the formal multiplicative group

$$\widehat{\mathbb{G}}_m := G_{F_{\mathrm{mul}}}(X, Y)$$

was obtained from the (algebraic) multiplicative group $\mathbb{G}_m$ by "completing at the identity section $1 \in \mathbb{G}_m$". Similarly, the formal additive group

$$\widehat{\mathbb{G}_a} := G_{F_{\mathrm{add}}(X,Y)}$$

with $F_{\mathrm{add}}(X, Y) = X + Y$ arises from the (algebraic) additive group

$$\mathbb{G}_a\colon \mathrm{Alg}_R \to (\mathrm{Ab}),\ S \mapsto S$$

by completing at the zero-sectio $0 \in \mathbb{G}_a$.

Given any endomorphism $\varphi\colon F_1 \to F_2$ of formal group laws, then

$$\eta^\varphi\colon \mathcal{G}_{F_1} \to \mathcal{G}_{F_2},\ x \in \mathcal{G}_{F_1}(S) = \mathcal{N}il(S) \mapsto \varphi(x) \in \mathcal{N}il(S) = \mathcal{G}_{F_2}$$

defines a natural transformation of functors $\mathrm{Alg}_R \to (\mathrm{Ab})$ (and conversely any morphism $\mathcal{G}_{F_1} \to \mathcal{G}_{F_2}$ is of this form as we will discuss later).

Exercise 1.23. Let R be a ring, and for $c \in R$ set $F_c(X, Y) := X + Y + cXY$.

(1) Show that $F_c(X, Y) := X + Y + cXY$ is a formal group law over R.
(2) Assume that R is reduced. Show that each formal group law F, which is a polynomial, is equal to F_c for some $c \in R$.

(3) Assume that R is a $\mathbb{Q}$-algebra. Show that the "additive formal group law" $F_0(X,Y) = X + Y$ and the "multiplicative formal group law" $F_1(X,Y) = X + Y + XY$ are isomorphic.

Let us turn back to our case of interest, i.e., let A be a complete discretely valued with finite residue field k of characteristic p with q elements, and let us fix a uniformizer $\pi \in A$. Recall that

$$\mathcal{F}_\pi = \{f \in A[[X]] \mid f(X) \equiv \pi X \bmod (X)^2, \quad f(X) \equiv X^q \bmod (\pi)\},$$

and that for any $f \in \mathcal{F}_\pi$ we constructed in Lemma 1.17 a formal group law

$$F_f(X,Y) \in A[[X,Y]].$$

The formal group law $F_f(X,Y)$ is special as it is equipped with many endomorphisms, namely the

$$[a]_f \in A[[X]]$$

for any $a \in A$ ("$F_f(X,Y)$ has formal complex multiplication by A").

We abstract this data to a general definition for any A-algebra R.

Definition 1.24. *A formal A-module*[4] *over R is a formal group law F over R together with a ring homomorphism*

$$\iota\colon A \to \mathrm{End}_{\mathrm{FGL}(R)}(F)$$

such that for each $a \in A$ we have

$$\iota(a) \equiv a \cdot X \ \mathit{mod}\ (X)^2,$$

We will usually write $[a]$ instead of $\iota(a)$.

Clearly, formal A-modules are functorial in R in the following sense. If $\alpha\colon R \to S$ is a morphism of A-algebras and F a formal A-module over R, then by applying α to the coefficients of F and the $\iota(a), a \in A$, we obtain a formal A-module $\alpha_* F$ over S. Instead of $\alpha_* F$ we will also write $F\hat{\otimes}_R S$ occasionally.

Let us note that for a formal A-module F over R and any $S \in \mathrm{Alg}_R$ the abelian group

$$(\mathcal{N}il(S), (-) +_F (-))$$

is naturally an A-module via

$$a \cdot_F x := [a](x).$$

This viewpoint makes it clear how we should define morphisms of formal A-modules. Namely, a morphism $f\colon F \to G$ between formal A-modules over R is a power series $f(X) \in R[[X]]$, which is a morphism of the underlying formal group laws, such that

$$f([a]_F(X)) = [a]_G(f(X))$$

for each $a \in A$. Similarly to the case of formal group laws we get the category $\mathrm{FGL}_A(R)$ of formal A-modules over $\mathrm{Spec}(R)$ which is naturally enriched in A-modules by pointwise taking the addition (for the formal group law)/scalar multiplication of homomorphisms. For the moment, the case $R = A$ is the most important one for us. By Theorem 1.18 we know that for $f, g \in \mathcal{F}_\pi$ the formal group laws F_f and F_g are isomorphic via the homomorphism

$$[1]_{g,f}\colon F_f \to F_g$$

[4]Or better, formal A-module law.

from Lemma 1.17 (with inverse $[1]_{f,g}$). We will now continue our discussion of local class field theory.

1.5. **Back to local class field theory.** We continue to use the usual notation $A, \pi, q, k, \mathcal{F}_\pi$ from before.

Let us consider again the case $A = \mathbb{Z}_p$, $f(X) = pX + \binom{p}{i}X^2 + \ldots + pX^{p-1} + X^p$ with associated formal group law

$$F_f(X,Y) = X + Y + XY.$$

Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. For $n \geq 1$ the field

$$\mathbb{Q}_p(\mu_{p^n})$$

arises by adjoining the p^n-torsion points

$$\mu_{p^n}(\overline{\mathbb{Q}}_p)$$

of the $\overline{\mathbb{Q}}_p$-valued points

$$\mathbb{G}_m(\overline{\mathbb{Q}}_p) = \overline{\mathbb{Q}}_p^\times$$

of the algebraic multiplicative group $\mathbb{G}_m$. For more general A there does not exist an analog of $\mathbb{G}_m$, and so let us try to reconsider the situation with $\mathbb{G}_m$ by $\widehat{\mathbb{G}}_m$.

There is a different reason why we should switch to $\widehat{\mathbb{G}}_m$. Let $\mathbb{G}_m, \widehat{\mathbb{G}}_m \colon \mathrm{Alg}_{\mathbb{Z}_p} \to (\mathrm{Ab})$ be the algebraic resp. formal multiplicative group over $\mathbb{Z}_p$. Then

$$\mathrm{End}(\mathbb{G}_m) \cong \mathbb{Z},$$

while

$$\mathrm{End}(\widehat{\mathbb{G}}_m) \cong \mathbb{Z}_p,$$

where the $\mathrm{End}(-)$ refers to natural transformations of functors $\mathrm{Alg}_{\mathbb{Z}_p} \to (\mathrm{Ab})$, cf. Exercise 1.35.

The immediate problem is that naively

$$\widehat{\mathbb{G}}_m(\overline{\mathbb{Q}}_p) = \mathcal{N}il(\overline{\mathbb{Q}}_p) = 0$$

if we consider $\overline{\mathbb{Q}}_p$ a "discrete" $\mathbb{Z}_p$-algebra. There are two ways to fix this problem. In the first (which is the one used in [LT65]) one uses that the p-adic valuation on $\mathbb{Q}_p$ extends uniquely to a valution

$$\nu \colon \overline{\mathbb{Q}}_p \to \mathbb{Q} \cup \{\infty\}$$

(using Proposition 1.5), and that this yields an associated (non-discrete) metric topology on $\overline{\mathbb{Q}}_p$. If $x \in \overline{\mathbb{Q}}_p$ satisfies $\nu(x) > 0$, then for a power series $\varphi(x) = \sum\limits_{i \geq 0} a_i X \in \mathbb{Z}_p[[X]]$ the series

$$\varphi(x) = \sum_{i \geq 0} a_i x^i$$

converges, even if $\overline{\mathbb{Q}}_p$ is not complete. Namely, x lies in some finite extension L of $\mathbb{Q}_p$, and then $\varphi(x)$ converges in L as L is complete by Proposition 1.5. Argueing similarly for $F_f(X,Y)$ we can therefore define a group structure (even a $\mathbb{Z}_p$-module structure) on

$$\widehat{\mathbb{G}}_m(\overline{\mathbb{Q}}_p) := \{x \in \overline{\mathbb{Q}}_p \mid \nu(x) > 0\}$$

using F_f, and the p^n-torsion points in this group define the field $\mathbb{Q}_p(\mu_n)$.

In the second approach one just passes to the completion

$$\mathbb{C}_p := \widehat{\overline{\mathbb{Q}}}_p$$

of $\overline{\mathbb{Q}}_p$, and defines

$$\widehat{\mathbb{G}}_m(\mathbb{C}_p) = \mathfrak{m}_{\mathbb{C}_p} := \{x \in \mathbb{C}_p \mid \nu(x) > 0\}.$$

By completeness of $\mathbb{C}_p$ the relevant power series converge and yield a $\mathbb{Z}_p$-module structure on $\widehat{\mathbb{G}}_m(\mathbb{C}_p)$. Note that although

$$\widehat{\mathbb{G}}_m(\overline{\mathbb{Q}}_p) \subsetneq \widehat{\mathbb{G}}_m(\mathbb{C}_p)$$

the subgroups of p^n-torsion points agree for each $n \geq 1$ as torsion points are algebraic over $\mathbb{Q}_p$.

Let us generalize this to arbitrary A. Fix a separable closure

$$\overline{K}$$

of K, and $\pi \in A, f \in \mathcal{F}_\pi$ as before. For any algebraic extension L of K we set

$$\mathcal{G}_{F_f}(L) := \mathfrak{m}_L := \{x \in L \mid \nu(x) > 0\},$$

where $\nu\colon L \to \mathbb{Q} \cup \infty$ is the unique extension of the valuation on K. The formal group law F_f and its endomorphisms $[a]_f$ for $a \in A$ define a functorial A-module structure on

$$\mathcal{G}_{F_f}(L) := \mathfrak{m}_L := \{x \in L \mid \nu(x) > 0\}.$$

In particular, if L/K is Galois the Galois action of $\mathrm{Gal}(L/K)$ on

$$\mathcal{G}_{F_f}(L)$$

is A-linear.

We can now (finally) define the Lubin-Tate extensions of K.

Definition 1.25. *For $n \geq 1$ we define*

$$\Lambda_{f,n} := \ker(\mathcal{G}_{F_f}(\overline{K}) \xrightarrow{[\pi^n]_f} \mathcal{G}_{F_f}(\overline{K})) \subseteq \overline{K}$$

as the π^n-torsion in the A-module $\mathcal{G}_{F_f}(\overline{K})$, and

$$K_{\pi,n} = K(\Lambda_{f,n}).$$

If $f, g \in \mathcal{F}_\pi$, then the (A-linear) isomorphism $[1]_{f,g}\colon F_g \cong F_f$ from Theorem 1.18 restricts to an isomorphism

$$[1]_{f,g}\colon \Lambda_{g,n} \to \Lambda_{f,n},\ x \mapsto [1]_{f,g}(x).$$

Therefore even if the subset $\Lambda_{f,n} \subseteq \overline{K}$ depends on f, the resulting field extension

$$K_{\pi,n}$$

does not. The natural action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathcal{G}_{F_f}(\overline{K})$ preserves $\Lambda_{f,n}$ and therefore the field $K_{\pi,n}$ is Galois over K. As we can take $f(X) = \pi X + X^q$, we see that $K_{\pi,n}$ is very concretely the splitting field of the polynomial

$$[\pi^n]_f(X) = \underbrace{f(f(\ldots(f(X))\ldots)}_{n-\text{fold composition}} \in K[X]$$

We want to analyze the field $K_{\pi,n}$ further, and in particular prove that the natural morphism

$$\mathrm{Gal}(K_{\pi,n}/K) \to \mathrm{Aut}_A(\Lambda_{f,n})$$

and

$$(A/\pi^n)^\times \to \mathrm{Aut}_A(\Lambda_{f,n})$$

are isomorphisms (proving that $K_{\pi,n}/K$ is abelian with Galois group $(A/\pi^n)^\times$).

Theorem 1.26 ([LT65, Theorem 2])**.** *Let $A, \pi, f \in \mathcal{F}_\pi$ as before, and set $M := \mathcal{G}_{F_f}(\overline{K})$. The following hold true:*

1. *The A-module M is divisible, i.e., for each $a \in A \setminus \{0\}$ the multiplication $M \xrightarrow{a} M$ is surjective.*
2. *For each $n \geq 1$ there exists an isomorphism $\Lambda_{f,n} = M[\pi^n] \cong A/\pi^n$.*
3. *The A-module $\Lambda_f := \bigcup_{n\geq 0} \Lambda_{f,n} = M[\pi^\infty]$ is isomorphic to K/A.*
4. *For $\sigma \in \mathrm{Gal}(\overline{K}/K)$ there exists a unique $x_\sigma \in A^\times$ such that*

$$\sigma(\lambda) = x_\sigma \cdot \lambda := [x_\sigma](\lambda)$$

for all $\lambda \in \Lambda_f$.

Proof. As the formal A-modules F_f, F_g for different choice $f, g \in \mathcal{F}_\pi$ are all isomorphic (via $[1]_{f,g}$), we may assume that

$$f(X) = \pi X + X^q.$$

For any $z \in M \subseteq \overline{K}$ the zeros of the polynomial

$$f(X) - z = X^q + \pi X - z$$

lie in $\mathfrak{m}_{\overline{K}}$ as $f(X) \equiv X^q \bmod \mathfrak{m}_{\overline{K}}$. Moreover, $f(X)$ is separable as its derivative

$$f'(X) = qX^{q-1} + \pi$$

does not have a zero in $\mathfrak{m}_{\overline{K}}$ because $\nu(q) \geq \nu(\pi)$. Clearly,

$$\Lambda_{f,1} = \{x \in M \mid f(x) = 0\}$$

because $f(X) = [\pi]_f$. In particular,

$$\sharp\Lambda_{f,1} = q = \sharp k.$$

As A-action on $\Lambda_{f,1}$ factors over $A/\pi = k$, this implies

$$\Lambda_{f,1} \cong k$$

as A-modules. Lemma 1.27 below implies Item 2 and Item 3. As the $\mathrm{Gal}(\overline{K}/K)$-action on $\Lambda_f = M[\pi^\infty]$ is A-linear the existence of x_σ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$ follows from another application of Lemma 1.27. This finishes the proof. □

Lemma 1.27. *Let N be a divisible A-module such that $N[\pi] \cong A/\pi$. Then*

$$N[\pi^\infty] \cong K/A,$$

and in particular,

$$A \cong \mathrm{End}_A(N[\pi^\infty]).$$

Proof. By the assumption $N[\pi] \cong A/\pi$ and the structure theory of finitely generated A-modules each finitely generated A-submodule $M_0 \subseteq N[\pi^\infty]$ must be isomorphic to A/π^n for some $n \geq 0$. The multiplication $\pi\colon N \to N$ induces (by divisibility of N) a short exact sequence

$$0 \to N[\pi] \to M_1 \to M_0 \to 0$$

for a finitely generated A-submodule $M_1 \subseteq N[\pi^\infty]$. We can conclude that $M_1 \cong A/\pi^{n+1}$. Continuing we find that

$$N[\pi^\infty] \cong \varinjlim_{n\geq 0} \pi^{-n}A/A \cong K/A.$$

For the last statement note that

$$\begin{aligned}
&\mathrm{Hom}_A(K/A, K/A)\\
\cong&\mathrm{Hom}_A(\varinjlim_{n\geq 0} \pi^{-n}A/A, K/A)\\
\cong&\varprojlim_{n\geq 0} \mathrm{Hom}_A(\pi^{-n}A/A, K/A)\\
\cong&\varprojlim_{n\geq 0} \mathrm{Hom}_A(\pi^{-n}A/A, \pi^{-n}A/A)\\
\cong&\varprojlim_{n\geq 0} A/\pi^n\\
\cong&A
\end{aligned}$$

by completeness of A. □

We obtain as a consequence a description of $\mathrm{Gal}(K_{\pi,n}/K)$.

Lemma 1.28. *For $n \geq 1$ we have*

1. $[K_{\pi,n} : K] = (q-1)q^{n-1}$
2. *$K_{\pi,n}$ is totally ramified over K*
3. *The map $\sigma \mapsto x_\sigma$ induces an isomorphism*

$$\mathrm{Gal}(K_{\pi,n}/K) \cong A^\times/(1+\pi^n A).$$

Proof. Assume as in Theorem 1.26 that $f(X) = X^q + \pi X$. Write

$$f^n(X) = f(f(\ldots(f(X))\ldots)) = X^{q^n} + \ldots + \pi^n X$$

for the n-fold composition of f. Note that by definition we have

$$\Lambda_{f,n} = \{x \in \mathcal{G}_{F_f}(\overline{K}) \mid f^n(x) = 0\}.$$

We can factor $f^n(X)$ (similarly to factoring $X^{p^n} - 1$ into cyclotomic polynomials!) as

$$\Phi_n(X)\Phi(X)_{n-1}\cdots\Phi_1(X)\Phi_0(X)$$

with $\Phi_0(X) = X$ and

$$\Phi_i(X) = \frac{f^i(X)}{f^{i-1}(X)} = \frac{f(f^{i-1}(X))}{f^{i-1}(X)} = (f^{i-1}(X))^{q-1} + \pi$$

for $i \geq 1$. We see that $\Phi_i(X)$ is an Eisenstein polynomial, therefore irreducible, and of degree $(q-1)q^{i-1}$. As $K_{\pi,i}$ is the splitting field of $\Phi_i(X)$ for each i, it follows that

$$[K_{\pi,n} : K] = (q-1)q^{n-1}$$

and that $K_{\pi,n}$ is totally ramified over K. The natural morphism

$$\mathrm{Gal}(K_{\pi,n}/K) \to \mathrm{Aut}_A(\Lambda_{f,n}) \cong A^\times/(1+\pi^n A)$$

is injective as $\Lambda_{f,n}$ generates $K_{\pi,n}$. We can then conclude because

$$\sharp(\mathrm{Gal}(K_{\pi,n}/K)) = [K_{\pi,n} : K] = (q-1)q^{n-1} = \sharp(A^\times/(1+\pi^n A))$$

using Theorem 1.26. □

Passing to the colimit we therefore obtain the natural isomorphism

$$\mathrm{Gal}(K_\pi/K) \cong A^\times,\ \sigma \mapsto x_\sigma.$$

for $K_\pi = K(\Lambda_f) = \bigcup_{n\geq 0} K_{\pi,n}$. As $K_{\pi,n}$ is totally ramified over K by Lemma 1.28, we obtain an isomorphism

$$A^\times \times \widehat{\mathbb{Z}} \cong \mathrm{Gal}(K_\pi K^{\mathrm{nr}}/K).$$

Our next aim will be to prove that for each uniformizer $\pi \in A$ we have

$$K^{\mathrm{ab}} = K_\pi K^{\mathrm{nr}}.$$

Following [Gol81] we will deduce this from the theorem of Hasse-Arf.

1.6. **Higher ramification groups.** In order to prove that

$$K^{\mathrm{ab}} = K_\pi K^{\mathrm{nr}}$$

for a (non-archimedean) local field, we need at least one statement concerning *all* abelian extensions of K. This statement will be the theorem of Hasse-Arf, cf. Theorem 1.40. In order to state it, we need to introduce the higher ramification groups of K, cf. [Ser13, Chapter IV], which in the case of $K_{\pi,n}$ mimick the filtration

$$\{0\} \subseteq (1+\pi^{n-1}A)/(1+\pi^n A) \subseteq \ldots \subseteq (1+\pi A)/(1+\pi^n A) \subseteq A^\times/(1+\pi^n A)$$

on

$$A^\times/(1+\pi^n A) \cong \mathrm{Gal}(K_{\pi,n}/K).$$

In the following, let A be any complete discrete valuation ring, that is we don't assume that the residue field k of A is finite. Let

$$K := \mathrm{Frac}(A),$$

and fix a uniformizer $\pi \in A$. We still assume that k is perfect. This has the consequence that for each finite extension L/K with ring of integers $B = \mathcal{O}_L$ and uniformizer π_L the extension

$$k_L := B/(\pi_L)$$

of k is separable, and therefore Proposition 1.10 holds true as well.

We denote by

$$\nu_L \colon L \to \mathbb{Z} \cup \{\infty\}$$

the *normalized* valuation of L, i.e., $\nu_L(\pi_L) = 1$. Assume in addition that L/K is Galois (not necessarily abelian) and set

$$G := \mathrm{Gal}(L/K).$$

Let $L_0 \subseteq L$ be the maximal subextension of L/K such that L_0/K is unramified. By Proposition 1.10 we get a natural isomorphism

$$\mathrm{Gal}(L_0/K) \cong \mathrm{Gal}(k_L/k),$$

and thus a short exact sequence

$$1 \to I_{L/K} \to G \to \mathrm{Gal}(k_L/k) \to 1$$

with $I_{L/K} = \mathrm{Gal}(L/L_0)$ the so-called inertia subgroup of G. In other words,

$$I_{L/K} = \ker(G \to \mathrm{Aut}(B/(\pi_L))).$$

More generally, we can define the higher ramification subgroups $G_i \subseteq G$, $i \geq -1$.

Definition 1.29. *For $i \geq -1$ we set*

$$G_i := \ker(G \to \mathrm{Aut}(B/(\pi_L)^{i+1})).$$

In particular, the G_i form a decreasing sequence of normal subgroups in G and $G_{-1} = G, G_0 = I_{L/K}$.

As $B \cong \varprojlim_i B/(\pi_L)^{i+1}$ by π_L-adic completeness of B, we get

$$\bigcap_i G_i = \{1\},$$

i.e., $G_i = \{1\}$ for $i \gg -1$. We call the $i \geq -1$ such that $G_i \neq G_{i+1}$ the "jumps" of the filtration $G_i, i \geq -1$.

Let $H \subseteq G$ be a subgroup with corresponding subfield

$$K' = L^H.$$

It is clear that for each $i \geq -1$

$$H_i = G_i \cap H,$$

where the LHS denotes the ramification filtration of the Galois group $H = \mathrm{Gal}(L/K')$ of the field extension L/K'.

For simplicity we may therefore assume that L/K is totally ramified, i.e, $L_0 = K$ (or equivalently, $G_0 = G$) by replacing K with L_0. Then

$$B = A[\pi_L]$$

as follows from the fact that the minimal polynomial of π_L over K is Eisenstein.

Let us define the function

$$i_G \colon G \to \mathbb{Z}_{\geq 0} \cup \{\infty\},\ s \mapsto \nu_L(s(\pi_L) - \pi_L).$$

Then

$$i_G(s) \geq i + 1 \Leftrightarrow s \in G_i$$

for $s \in G$ as follows easily from the definitions and the fact that $B = A[\pi_L]$. In particular, i_G is independent of the choice of π_L. For a subgroup $H \subseteq G$ we clearly have $i_H = (i_G)_{|H}$.

Let us now calculate the function i_G (and thus the ramification filtration) for the field $K_{\pi,n}$ from Section 1.5.

Example 1.30. Assume that K, $L = K_{\pi,n}, f$ are as in Section 1.5. To compute the ramification filtration on

$$G = \mathrm{Gal}(K_{\pi,n}/K) \cong A^\times/(1 + \pi^n A),\ s \mapsto x_s$$

we first have to find a suitable uniformizer $\pi_L \in L$. From the proof of Lemma 1.28 we can take as π_L any π^n-torsion point in $\Lambda_{f,n}$ of "exact order n", i.e., $\pi_L \in \Lambda_{f,n} \setminus \Lambda_{f,n-1}$. As the choice of f does not matter, we may take $f(X) = X^q + \pi X$ in the following. We will see later that in general $G_1 \subseteq G = G_0$ is the unique p-Sylow subgroup of G. This implies that

$$G_1 \cong (1 + \pi A)/(1 + \pi^n A).$$

Let $s \in G_1$ and write $x_s = 1 + a\pi^i A$ with $a \in A^\times$. Then

$$s(\pi_L) = [x_s](\pi_L) = [1](\pi_L) +_{F_f} [a\pi^i](\pi_L) = \pi_L +_{F_f} [a\pi^i](\pi_L),$$

and using $F_f(X,Y) = X + Y +$ higher terms we have to find

$$i_G(s) = \nu_L([a\pi^i](\pi_L)).$$

As $[a](x) = ax +$ higher terms in x with $a \in A^\times$, we get

$$\nu_L([a\pi^i](\pi_L)) = \nu_L([\pi^i](\pi_L)).$$

We claim that

$$\nu_L([\pi^i](\pi_L)) = q^i \tag{6}$$

for $1 \leq i < n$. Indeed, for $i = 1$ (which forces $n \geq 2$) we have

$$[\pi](\pi_L) = \pi_L^q + \pi\pi_L$$

and $\nu_L(\pi\pi_L) = (q-1)q^{n-1}+1 > q = \nu_L(\pi_L^q)$ by Lemma 1.28. For $i > 1$ we compute

$$[\pi^i](\pi_L) = ([\pi^{i-1}](\pi_L))^q + \pi[\pi^{i-1}](\pi_L)$$

and by induction

$$\nu_L(\pi[\pi^{i-1}](\pi_L)) = (q-1)q^{n-1} + q^{i-1},$$

which is strictly greater than

$$q^i = \nu_L(([\pi^{i-1}](\pi_L))^q)$$

because $n > i$. This proves (Equation (6)). We get that for any $s \in G_1$

$$i_G(s) = q^i$$

if $x_s \in (1+\pi^i A) \setminus (1+\pi^{i+1}A)$. We therefore obtain that the jumps of the filtration $G_i, i \geq 0$, are exactly the values

$$0 = q^0 - 1, q^1 - 1, q^2 - 1, \ldots, q^{n-1} - 1$$

and that the quotient G_j/G_{j+1} at a jump j is $k^\times = A^\times/(1+\pi A)$ if $j = 0$ or $k \cong (1+\pi^i)/(1+\pi^{i+1}A)$ if $j = q^i - 1 \geq 1$. For completeness let us mention that

$$i_G(s) = 1$$

if $s \in G_0 \setminus G_1$ because if $x_s = a + b\pi$ with $a \in A^\times \setminus 1 + \pi A, b \in A$, then

$$\nu_L(s(\pi_L) - \pi_L) = \nu_L((a-1)\pi_L) = 1.$$

In general, the function $i_G(s)$ is constant on the subset $G_i \setminus G_{i+1}$. Now assume that $H \subseteq G$ is a normal subgroup, or equivalently that

$$K' := L^H$$

is Galois over K.

We want to relate i_G and $i_{G/H}$ (and thus the ramification filtration of G with that of G/H).

Lemma 1.31 ([Ser13, Chapter 3, Proposition 3])**.** *For every $\overline{s} = sH \in G/H$ we have*

$$i_{G/H}(\overline{s}) = \frac{1}{e_{L/K'}} \sum_{t \in sH} i_G(t),$$

where $e_{L/K'} = [L : K'] = \sharp H$ is the ramification index of L/K'.

Proof. We may assume that $\overline{s} \neq 1 \in G/H$ as otherwise both sides equal ∞. Let $\pi_{K'} \in K'$ be a uniformizer. Then

$$i_{G/H}(\overline{s}) = \nu_{K'}(s(\pi_{K'}) - \pi_{K'}) = e_{L/K'}^{-1}\nu_L(s(\pi_{K'}) - \pi_{K'}),$$

while

$$\sum_{t \in sH} i_G(t) = \sum_{t \in H} \nu_L(st(\pi_L) - \pi_L) = \nu_L(\prod_{t \in H}(st(\pi_L) - \pi_L)).$$

Hence it suffices to see that

$$a := s(\pi_{K'}) - \pi_{K'}$$

and

$$b := \prod_{t \in H}(st(\pi_L) - \pi_L)$$

generate the same ideal in $B = \mathcal{O}_L$. Let

$$f(X) \in \mathcal{O}_{K'}[X]$$

be the minimal polynomial of π_L over K', and let $s(f) \in B[X]$ be the polynomial obtained from $f(X)$ by applying s to the coefficients of f. The element $a = s(\pi_{K'}) - \pi_{K'}$ divides

$$s(f) - f$$

as each coefficient of f can be written as a polynomial (with A-coefficents) in $\pi_{K'}$ and s fixes each element in A. This in turn implies that a divides $s(f)(\pi_L) - f(\pi_L) = s(f)(\pi_L) = \pm b$ because

$$f(X) = \prod_{t \in H}(X - t(\pi_L)).$$

Because $B = A[\pi_L]$ we can write $\pi_{K'} = g(\pi_L)$ for some polynomial $g(X) \in A[X]$. The polynomial $g(X) - \pi_{K'} \in \mathcal{O}_{K'}$ is divisible by f because it has π_L as a root. Hence, we can write

$$g(X) - \pi_{K'} = f(X)h(X)$$

for some $h(X) \in \mathcal{O}_{K'}[X]$. We get

$$\begin{aligned} & a \\ =& s(\pi_{K'}) - \pi_{K'} \\ =& s(f)(X)s(h)(X) + s(g)(X) - f(X)h(X) - g(X) \\ =& s(f)(X)s(h)(X) - f(X)h(X) \end{aligned}$$

because g has coefficients in A. Substituting π_L for X we obtain

$$a = s(f)(\pi_L)s(h)(\pi_L) = \pm bs(h)(\pi_L)$$

as desired. □

From Lemma 1.31 it is not difficult to conclude that if $H = G_j, j \geq -1$, then

$$(G/H)_i = G_iH/H = \begin{cases} \{1\} & \text{if } i \geq j \\ G_i/H & \text{if } i < j. \end{cases}$$

Indeed, if $i < j$ we can calculate for $s \in G_i \setminus G_{i+1}$

$$i_{G/H}(\overline{s}) = \frac{1}{e_{L/K'}} \sum_{t \in H} i_G(st) = i_G(s)$$

because i_G is constant on the coset $sH \subseteq G_i \backslash G_{i+1}$. On the other hand $i_{G/H}(\overline{s}) = \infty$ if $s \in G_j = H$. As

$$i_{G/H}(\sigma) \geq i+1 \Leftrightarrow \sigma \in (G/H)_i$$

we can conclude.

Before describing the filtration $(G/H)_i, i \geq -1$, for more general H, we describe the quotients

$$G_i/G_{i+1},\ i \geq 0.$$

Lemma 1.32. *Let $s \in G = G_0$. Then*

$$s \in G_i \Leftrightarrow i_G(s) = \nu_L(\nu(\pi_L) - \pi_L) \geq i+1 \Leftrightarrow \frac{s(\pi_L)}{\pi_L} \equiv 1 \ mod\ (\pi_L)^i.$$

Proof. This follows directly from the definitions. □

For $i \geq 0$ set

$$U_L^i := 1 + \pi^i B,$$

which is a subgroup of $B^\times = U_L^0$. By π_L-adic completeness of B we get

$$U_L^0/U_L^1 \cong (B/\pi_L)^\times,\ B^\times = \varprojlim_i U_L^0/U_L^i.$$

For each $i \geq 1$ we have an isomorphism

$$U_L^i/U_L^{i+1} \cong B/\pi_L,\ x \bmod U_L^{i+1} \mapsto \frac{x-1}{\pi^i} \bmod (\pi_L)$$

of additive groups.

We get the following interesting consequence.

Corollary 1.33. *For $i \geq 0$ the map (of sets)*

$$G_i \to U_L^i,\ s \mapsto \frac{s(\pi_L)}{\pi_L}$$

induces an injective homomorphism

$$\theta_i \colon G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1},$$

which is independent of the choice of π_L.

Proof. By Lemma 1.32 the map is well-defined. We first prove independence of π_L of the map

$$G_i \to U_L^i/U_L^{i+1},\ s \mapsto \frac{s(\pi_L)}{\pi_L}.$$

For this let $\pi' = u\pi_L \in B$ be another uniformizer with $u \in B^\times$. Then

$$s(u) = u \bmod (\pi^{i+1})$$

for $s \in G_i$. This implies $\frac{s(u)}{u} \equiv 1 \bmod (\pi^{i+1})$ and hence

$$\frac{s(\pi')}{\pi'} = \frac{s(u)}{u}\frac{s(\pi_L)}{\pi_L} \equiv \frac{s(\pi_L)}{\pi_L} \bmod U_L^{i+1}.$$

Now we can prove additivity of $G_i \to U_L^i/U_L^{i+1}$. If $s,t \in G_i$, then $t(\pi_L) \in B$ is a uniformizer, and hence by the proven independence

$$\frac{st(\pi_L)}{\pi_L} = \frac{s(t(\pi_L))}{t(\pi_L)}\frac{t(\pi_L)}{\pi_L} \equiv \frac{s(\pi_L)}{\pi_L}\frac{t(\pi_L)}{\pi_L} \bmod U_L^{i+1}$$

as desired. □

Corollary 1.33 has interesting consequence. Namely,

(1) The quotient G_0/G_1 is cyclic of order prime to the characteristic of k because this holds for each finite subgroup of $k^\times \cong U_L^0/U_L^1$.
(2) If $\mathrm{char}(k) = 0$, then for each $i \geq 1$ we must have $G_i/G_{i+1} = \{1\}$ as $k \cong U_L^i/U_L^{i+1} \cong B/\pi_L$ has no non-trivial finite subgroups.
(3) If $\mathrm{char}(k) = p > 0$, then for $i \geq 1$ the group G_i/G_{i+1} must be a finite direct sum of copies of $\mathbb{F}_p$ as it embeds into the additive subgroup k. In particular, G_1 is the unique p-Sylow subgroup of G_0.
(4) The group G_0 is solvable, which combined with the fact that unramified extensions of *local* fields are abelian, implies that if K is a local field, and L/K finite Galois, then $\mathrm{Gal}(L/K)$ is solvable.

Let as before K be a complete discretely valued field (with perfect residue field k), and L/K a finite Galois extension (not necessarily totally ramified). Then $G_1 = \{1\}$ if and only of $e_{L/K}$ is prime to the characteristic of k. Such an extension is called tamely ramified. We give the following exercise describing these.

Exercise 1.34. Assume that L/K is tamely ramifed with $e = [L : K]$ and that the residue field of K is algebraically closed. Then

$$L = K(\sqrt[e]{\pi})$$

for a suitable uniformizer $\pi \in K$.

In particular, if $p = \mathrm{char}(k)$ (possibly $p = 0$)

$$\bigcup_{n \geq 1,\ p \nmid n} K^{\mathrm{nr}} K(\sqrt[n]{\pi})$$

is the maximal tamely ramified extension of K. This implies that for $K = k((t))$ with k algebraically closed and of characteristic 0, the field

$$\bigcup_{n \geq 1} k((t^{1/n}))$$

is algebraically closed.

After having described the G_i/G_{i+1} our next task is to describe the ramification filtration on G/H for a general subgroup $H \subseteq G = \mathrm{Gal}(L/K)$.

Exercise 1.35.

(1) Prove the Yoneda lemma: Let $\mathcal{C}$ be a category and for $c \in \mathcal{C}$ let $h_c(-) := \mathrm{Hom}_{\mathcal{C}}(-, c)$ be its contravariant Hom-functor. Let $F \colon \mathcal{C}^{\mathrm{op}} \to (\mathrm{Sets})$ be a functor. Then there exists a natural bijection

$$\mathrm{Hom}_{\mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, (\mathrm{Sets}))}(h_c, F) \cong F(c).$$

(2) Let R be a ring. Show that the natural transformations $\eta \colon \mathcal{N}il \to \mathcal{N}il$ are in natural bijection with the set $\{f(X) \in R[[X]] \mid f(0) \in \mathcal{N}il(R)\}$.
(3) Let p be a prime and let

$$\mathbb{G}_m, \widehat{\mathbb{G}}_m \colon (\mathrm{Alg}_{\mathbb{Z}_p}) \to (\mathrm{Sets})$$

be the algebraic and formal multiplicative group over $\mathbb{Z}_p$. Then $\mathrm{End}_{\mathbb{Z}}(\mathbb{G}_m) \cong \mathbb{Z}$, while $\mathrm{End}_{\mathbb{Z}}(\widehat{\mathbb{G}}_m) \cong \mathbb{Z}_p$.

1.7. **The theorems of Herbrand and Hasse-Arf.** As in the previous section we let $K = \mathrm{Frac}(A)$ be a complete discretely valued field with perfect residue field k, and L/K a finite Galois extension (not necessarily totally ramified) with $G := \mathrm{Gal}(L/K)$ equipped with its higher ramification filtration $G_i,\ i \geq -1$, and associated function i_G.

We also fix a normal subgroup $H \subseteq G$ with corresponding subfield

$$K' := L^H \subseteq L,$$

which is Galois over K.

Roughly, Herbrand's theorem implies that for each $i \geq -1$ the ramification subgroup

$$(G/H)_i$$

for $G/H = \mathrm{Gal}(K'/K)$ is of the form

$$G_jH/H$$

for some $j \geq -1$, *which might be different from* i. In order to state the result precisely we set

$$G_u := G_i$$

for $u \in \mathbb{R}, u \geq -1$, where $i \geq u$ is as the smallest integer.

Now set

$$\varphi := \varphi_{L/K}(u) := \int_0^u \frac{1}{[G_0 : G_t]} dt$$

for $u \geq -1$. Here, we defined

$$[G_0 : G_{-1}] = [G_{-1} \colon G_0].$$

Note that $\varphi(u) = u$ for $-1 \leq u \leq 0$.

Let us directly give an example by computing the case K local and $L = K_{\pi,n},\ n \geq 1$, from Section 1.5.

Example 1.36. In Example 1.30 we computed the higher ramification groups for the extension $K_{\pi,n}$ of a local field K with uniformizer $\pi \in K$. The function

$$\mathbb{R}_{\geq -1} \to \mathbb{R}, t \mapsto \frac{1}{[G_0 : G_t]}$$

is piecewise constant by definition. From here, one obtains that

$$\varphi \colon \mathbb{R}_{\geq -1} \to \mathbb{R},$$

is the unique, concave polygon starting at $(-1, -1)$ with slopes

$$1, 1/(q-1), 1/(q-1)q, \ldots, 1/(q-1)q^{n-1}.$$

and break points $0, q-1, q^2-1, \ldots, q^n-1$.

In general,

$$\varphi(u) = \frac{1}{\sharp g_0}(g_1 + g_2 + \ldots + (u-i)g_{i+1})$$

for $u \in \mathbb{R}_{\geq 0}, i \in \mathbb{Z}$, such that $i \leq u \leq i+1$, and $g_i := \sharp G_i$.

We can now state Herbrand's theorem precisely.

Theorem 1.37 (Herbrand)**.** *For any $u \geq -1$ we have*

$$(G/H)_v = G_u H/H$$

if $v = \varphi_{L/K'}(u)$.

Before proving Herbrand's theorem let us introduce the *upper* numbering of the higher filtration groups.

Lemma 1.38. *The function $\varphi_{L/K} \colon \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$ is a piecewise linear, concave, increasing homeomorphism with $\varphi(0) = 0$.*

For $u \in \mathbb{R}_{\geq -1} \setminus \mathbb{Z}$ the function φ is differentiable at u with derivative $\frac{1}{[G_0 : G_u]}$. For $u \in \mathbb{Z}_{\geq 0}$ the left derivative of φ is $\frac{1}{[G_0 : G_u]}$ while its right derivative is $\frac{1}{[G_0 : G_{u+1}]}$. Let

$$\psi := \psi_{L/K} := (\varphi_{L/K})^{-1} \colon \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$$

be the inverse of φ.

Via ψ we can define ramification groups in the upper numbering of G via

$$G^v := G_{\psi(v)}$$

for $v \in \mathbb{R}_{\geq -1}$. Theorem 1.37 can then nicely be reformulated as saying that

$$(G/H)^v = G^v H/H$$

for all $v \in \mathbb{R}_{\geq -1}$. Indeed, we will prove this in Lemma 1.44.

Example 1.39. Let us continue Example 1.30, Example 1.36 and compute the ramification filtration on $G = \mathrm{Gal}(K_{\pi,n}/K)$ in the *upper* numbering. The jumps of $G^v = G_{\psi(v)}, v \geq -1$, are precisely the values

$$\varphi(u)$$

for $u \geq -1$ a jump for the filtration G_u. We computed that these are precisely

$$0, q-1, q^2-1, \ldots, q^{n-1}-1$$

with

$$G_0 = A^\times/(1+\pi^n A) \supseteq G_1 = G_{q-1} = (1+\pi A)/(1+\pi^n A)$$

and for $1 \leq i < n$

$$G_{q^i-1} = (1+\pi^i A)/(1+\pi^n A).$$

Now we calculate for $1 \leq i < n$

$$\begin{aligned}
&\varphi(q^i - 1) \\
=&\int_0^{q^i-1} \frac{1}{[G_0 : G_u]} du \\
=&\sum_{j=1}^{i} \int_{q^{j-1}-1}^{q^j-1} \frac{1}{[G_0 : G_{q^j-1}]} \\
=&\sum_{j=1}^{i} (q^j - q^{j-1}) \frac{1}{(q-1)q^{j-1}} \\
=&\sum_{j=1}^{i} 1 \\
=&i.
\end{aligned}$$

Hence, $G^v, v \geq -1$, has its jumps precisely at

$$0, 1, 2, \ldots, n-1.$$

and

$$\psi(i) = q^i - 1$$

for $0 \leq i < n$. For $v \geq n-1$ we have

$$\psi(v) = (q-1)q^{n-1}(v - n + 1) + q^{n-1} - 1,$$

i.e., the final slope of ψ is $(q-1)q^{n-1}$.

In particular, we see that the jumps in the upper numbering filtration on $\mathrm{Gal}(K_{\pi,n}/K)$ are integers (rather than rationals). The theorem of Hasse-Arf implies that this is the case for *all* abelian extensions of a complete discretely valued field K.

Theorem 1.40 (Hasse-Arf)**.** *Let L/K be an abelian extension. Then the jumps for the upper ramification filtration $G^v, v \in \mathbb{R}_{\geq -1}$, on $G := \mathrm{Gal}(L/K)$ lie in $\mathbb{Z}$.*

Here a jump in the filtration $G^v,\ v \in \mathbb{R}_{\geq -1}$ is a real number $v \in \mathbb{R}_{\geq -1}$ such that

$$G^v \neq G^{v+\varepsilon}$$

for all $\varepsilon > 0$.

Note that by Theorem 1.37 the local Kronecker-Weber theorem, cf. Theorem 1.46, and Example 1.39 imply Theorem 1.40 if K is a (non-archimedean) local field.

We will present a proof of Theorem 1.40 in Section 1.9. Now we turn to the proof of Theorem 1.37.

We have to establish some lemmata. We continue to write $g_i = \sharp G_i$ for $i \geq 0$.

Lemma 1.41. *For $u \geq 0$ we have*

$$\varphi_{L/K}(u) = \theta(u) := \frac{1}{g_0} \sum_{s \in G} (\min\{i_G(s), u+1\} - 1)$$

with $i_G(s) = \nu_L(s(\pi_L) - \pi_L)$ the function discussed in Section 1.6.

Proof. For $s \in G$ the function $\min\{i_G(s), u+1\}$ is concave, continuous and piecewise linear. This implies the same for θ. Moreover,

$$\theta(u) = 0 = \varphi(u).$$

Hence, it suffices to see that for $i < u < i+1$ the derivatives of θ and φ agree. For φ the derivative is $\frac{g_{i+1}}{g_0}$. For θ the derivative is

$$\frac{1}{g_0} \sum_{s \in G,\ i_G(s) \geq i+2} 1 = \frac{g_{i+1}}{g_0}$$

as desired. □

Lemma 1.42. *For $\sigma = sH \in G/H$ set*

$$j(\sigma) := \max\{i_G(t) \mid t \in sH\}.$$

Then

$$i_{G/H}(\sigma) - 1 = \varphi_{L/K'}(j(\sigma) - 1).$$

Proof. We may assume that

$$j(\sigma) = i_G(s) := m.$$

If $t \in H$ with $t \in H_{m-1}$, then $st \in H_{m-1}$ by construction of s. Thus $i_G(st) \geq m$, and hence $i_G(st) = m$. For $t \in H \setminus H_{m-1}$. we obtain

$$i_G(st) = i_G(t)$$

because for $i < m-1$ we have $st \in H_i$ if and only if $t \in H_i$. Combining both cases we obtain

$$i_G(st) = \min\{i_G(t), m\}$$

for each $t \in H$. By Lemma 1.31 we get

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{t \in H} i_G(st) = \frac{1}{h_0} \sum_{t \in H} \min\{i_G(st), m\}.$$

By Lemma 1.41 for H and $i_G(t) = i_H(t)$ the last term equals

$$\frac{1}{h_0} \sum_{t \in H} \min\{i_G(st), m\} = 1 + \varphi_{L/K'}(m-1).$$

This finishes the proof. □

Now we can prove Theorem 1.37

Proof of Theorem 1.37. With the notations in Lemma 1.42 we get for $\sigma \in G/H$

$$\begin{aligned} &\sigma \in G_u H/H \\ \Leftrightarrow &j(\sigma) - 1 \geq u \\ \overset{\varphi_{L/K'} \text{ strictly increasing}}{\Leftrightarrow} &\varphi_{L/K'}(j(\sigma) - 1) \geq \varphi_{L/K'}(u) \\ \overset{\text{Lemma 1.42}}{\Leftrightarrow} &i_{G/H}(\sigma) - 1 \geq \varphi_{L/K'}(u) \\ \Leftrightarrow &\sigma \in (G/H)_v \end{aligned}$$

as $v = \varphi_{L/K'}(u)$. □

The functions $\varphi_{L/K}$, $\psi_{L/K}$ enjoy the following transitivity in field extensions.

Lemma 1.43. *We have*

$$\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'}$$

and

$$\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}.$$

Proof. We only have to prove the statement for φ. For $u = -1$ we get

$$\varphi_{L/K}(-1) = -1 = \varphi_{K'/K} \circ \varphi_{L/K'}(-1).$$

As both sides are continuous it suffices to show that for any $u \in \mathbb{R}_{\geq -1} \setminus \mathbb{Z}$ the derivatives coincide. Set $v := \varphi_{L/K'}(u)$. We get

$$\begin{aligned}
&(\varphi_{K'/K} \circ \varphi_{L/K'})'(u) \\
=&\varphi'_{K'/K}(v) \cdot \varphi'_{L/K'}(u) \\
=&\frac{\sharp(G/H)_v}{e_{K'/K}} \frac{\sharp(H_u)}{e_{L/K'}} \\
\overset{Theorem\ 1.37}{=}&\frac{\sharp(G_u H/H}{e_{K'/K}} \frac{\sharp(H_u)}{e_{L/K'}} \\
\overset{e_{L/K}=e_{K'/K}e_{L/K'}}{=}&\frac{\sharp G_u}{e_{L/K}} \\
=&\varphi'_{L/K}(u).
\end{aligned}$$

This finishes the proof. □

Now we can prove the desired compatibility of the *upper* numbering filtration with passage to quotients.

Lemma 1.44. *We have*

$$(G/H)^v = G^v H/H$$

for all $v \in \mathbb{R}_{\geq -1}$.

Proof. We have

$$\begin{aligned}
&(G/H)^v \\
\overset{x:=\psi_{K'/K}(v)}{=}&(G/H)_x \\
\overset{w:=\psi_{L/K'}(x)}{=}&G_w H/H \\
\overset{u:=\varphi_{L/K}(w)}{=}&G^u H/H
\end{aligned}$$

Lemma 1.43 implies

$$u = \varphi_{L/K}(\psi_{L/K'}(\psi_{K'/K}(v))) = \varphi_{L/K}(\psi_{L/K}(v)) = v$$

and we win. □

Lemma 1.44 has the pleasant consequence that for we can extend the *upper* numbering ramification filtration to infinite Galois extensions. Namely, if L/K is an arbitrary, possibly infinite, Galois extension and $G = \mathrm{Gal}(L/K)$, then we can set

$$G^v := \varprojlim_H (G/H)^v$$

for $v \geq -1$, where the limit runs over all open, normal subgroups $H \subseteq G$. Then the $G^v \subseteq G, v \geq -1$, are a decreasing sequence of normal closed subgroups, and $G^v H/H = (G/H)^v$ for any $H \subseteq G$ open, normal and $v \geq -1$. Moreover,

$$\bigcap_{v \geq -1} G^v = \{1\}$$

as the intersection must be contained in the intersection of all open, normal subgroups $H \subseteq G$.

Example 1.45. For $K_\pi = \bigcup_{n \geq 1} K_{\pi,n}$ the infinite Lubin-Tate extension from Section 1.5 we conclude from Example 1.39 that the jumps of $G = \mathrm{Gal}(K_\pi/K)$ in the upper numbering filtration are nicely given by

$$0, 1, 2, \ldots.$$

1.8. **Proof of the local Kronecker-Weber theorem.** In this section we want to deduce the local Kronecker-Weber theorem from the Hasse-Arf theorem. Let us recall its statement.

Theorem 1.46 (local Kronecker-Weber)**.** *Let K be a (non-archimedean) local field and $\pi \in K$ a uniformizer. Then*

$$K_\pi K^{\mathrm{nr}}$$

is the maximal abelian extension of K.

Here, K^{nr} is the maximal unramified extension of K (inside some fixed separable closure of K), and K_π the Lubin-Tate extension associated with π from Section 1.5.

Proof. The proof follows [Gol81]. Let L/K be an abelian extension. We want to prove that

$$L \subseteq M := K_\pi K^{\mathrm{nr}}.$$

Consider the short exact sequence

$$1 \to \mathrm{Gal}(L \cdot M/M) \to \mathrm{Gal}(M \cdot L/K_\pi) \to \mathrm{Gal}(M/K_\pi) \to 1$$

of abelian profinite groups. As

$$\mathrm{Gal}(M/K_\pi) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K) \cong \widehat{\mathbb{Z}}$$

there exists a splitting $s\colon \mathrm{Gal}(M/K_\pi) \to \mathrm{Gal}(M \cdot L/K_\pi)$. The fixed field

$$F$$

for the (closed) image of s is a totally ramified extension of K_π with $F \cdot M = L \cdot M$ and F/K (infinite) abelian. Now the claim follows from Lemma 1.47. □

Lemma 1.47. *Let F/K_π be a totally ramified extension with F/K abelian. Then $F \subseteq K_\pi$.*

The field K_π is no longer *discretely* valued (due to its infinite ramification). With F/K_π totally ramified we therefore mean $F \cap K_\pi K^{\mathrm{nr}} = K_\pi$.[5]

Proof. Set $H := \mathrm{Gal}(F/K_\pi) \subseteq G := \mathrm{Gal}(F/K)$. As F/K_π is totally ramified

$$G = G^0.$$

For $v \geq -1$ let us write

$$G^{v+} := \bigcup_{\varepsilon > 0} G^{v+\varepsilon}.$$

Hence, $G^v \neq G^{v+}$ if and only if v is a jump. It is sufficient to show that for any jump $v \in \mathbb{R}_{\geq 0}$ of the filtration $G^v, v \geq 0$, we have

$$G^v \cap H = G^{v+} \cap H.$$

Indeed, if true this implies

$$H \subseteq G^v$$

for each $v \geq 0$, and hence $H = \{1\}$ as $\bigcap_{v \geq 0} G^v = \{1\}$. But $H = \{1\}$ implies $F = K_\pi$ and hence the lemma. Let $v \geq 0$. Then

$$[G^v : G^{v+}] = [(G/H)^v : (G/H)^{v+}][G^v \cap H : G^{v+} \cap H] \tag{7}$$

[5]Alternatively, each element $\mathrm{Gal}(F/K_\pi)$ acts trivially on the residue field of F.

using $(G/H)^v = G^v H/H$, cf. Lemma 1.44. We have

$$G/H \cong \mathrm{Gal}(K_\pi/K)$$

and thus by Example 1.45 we know that

$$[(G/H)^v : (G/H)^{v+}] = \begin{cases} q-1, & v = 0 \\ q, & v \in \mathbb{Z}_{\geq 1} \\ 1, & v \in \mathbb{R}_{\geq 0} \setminus \mathbb{Z}. \end{cases}$$

In particular,

$$[(G/H)^v : (G/H)^{v+}] \geq q - 1$$

if $[(G/H)^v : (G/H)^{v+}] \neq 1$. From Corollary 1.33 we know that

$$[G^v : G^{v+}] \leq q$$

for each $v \geq -1$. Hence, if

$$[G^v \cap H \colon G^{v+} \cap H] \neq 1,$$

then by (Equation (7)) we can conclude that

$$[(G/H)^v : (G/H)^{v+}] = 1,$$

i.e., that v is not an integer, and that v is a jump of $G^v, v \geq 0$. However, this is a contradiction to Theorem 1.40 as we assumed that F/K is abelian. □

In the proof of Lemma 1.47 we used the assumption that $G = \mathrm{Gal}(F/K)$ is abelian only to conclude by the theorem of Hasse-Arf that the jumps $G^v, v \geq 0$, are integers. In particular, for any totally ramified extenstion F/K_π with $\mathrm{Gal}(F/K)$ not abelian, not all jumps on $G = \mathrm{Gal}(F/K)$ can be integers.

Serre gave an example of a non-abelian extension L/K with jumps in the upper numbering not all integral. In fact it is sufficient that

$$G = \mathrm{Gal}(L/K)$$

is isomorphic to the quaternion group of order 8 and $G_4 = \{1\}$, cf. [Ser13, Chapter 3, §3, Exercise 2].[6] The jumps occur at

$$1, 3/2.$$

1.9. **Proof of the Hasse-Arf theorem.** We now want to give the proof for the Hasse-Arf Theorem 1.40 following [Sen69], cf. [Yos08, Theorem 6.11]. Let us recall the situation and thus fix a complete discretely valued field K with ring of integers $A = \mathcal{O}_K$ and perfect residue field k. Let L/K be a finite Galois extension with *abelian* Galois group $G := \mathrm{Gal}(L/K)$ and set $B := \mathcal{O}_L$. Set

$$n := [L : K] = \sharp G.$$

We want to see that if $v \geq -1$ is a jump for the ramification filtration G^v of G in the upper numbering, i.e.,

$$G^v \neq G^{v+} := \bigcup_{\varepsilon > 0} G^{v+\varepsilon},$$

then v is an integer. Equivalently, we want to see that if $G_i \neq G_{i+1}$ in the lower numbering with $i \in \mathbb{Z}_{\geq -1}$, then

$$v := \varphi_{L/K}(i) \in \mathbb{Z}.$$

[6] I used [Ser13, Chapter 3, Proposition 11] when solving this exercise.

The cases $i = -1, 0$ are clear as $\varphi_{L/K}(-1) = -1$ and $\varphi_{L/K}(0) = 0$. If $i \geq 0$, then

$$\varphi_{L/K}(i) = \frac{1}{g_0}(g_1 + g_2 + \dots g_i),$$

where $g_i := \sharp G_i$ as was remarked in Section 1.7.

One can make the following initial reductions.

- If $G^v \neq G^{v+}$, then by the structure theorem of finite abelian groups, there exists a subgroup $H \subseteq G$ with G/H cyclic and $G^vH/H \neq G^{v+}H/H$. Using Herbrand's theorem Theorem 1.37 and replacing L by L^H reduces us to the case that G is cyclic.
- Writing G as a product of cyclic subgroups of prime power order reduces us by the same argument as before to the case that $\sharp G$ is a prime power.
- If L/K is tamely ramified, i.e., $\sharp G$ is prime to the characteristic of k, then $G_1 = \{1\}$ and we are done.

Hence, we reduced to the case that G is a cyclic p-group of order p^m for some $m \geq 1$, where $p > 0$ is the characteristic of k. In particular, $G_0 = G_1$ and L/K is wildly ramified.

Fix a generator

$$\sigma \in G,$$

and for $0 \leq j \leq m$ let

$$G(j) \subseteq G$$

be the unique subgroup of order p^{m-j}, i.e., $G(j) = \langle \sigma^{p^j} \rangle$ and

$$G = G(0) \supsetneq G(1) \supsetneq G(2) \supsetneq \dots.$$

From Corollary 1.33 and the structure of the subgroups of G we can conclude that each subgroup $G(j) \subseteq G$ equals a higher ramification subgroup of G. Hence, there exist jumbs $0 < n_0 < \dots < n_{m-1}$ with

$$\begin{aligned} G(0) = G_0 = \dots = G_{n_0} \\ G(1) = G_{n_0+1} = \dots = G_{n_1} \\ \dots \\ G(j) = G_{n_{j-1}+1} = \dots = G_{n_j} \\ \dots \\ G(m) = G_{n_{m-1}+1} = \dots. \end{aligned}$$

We get

$$\varphi_{L/K}(n_0) = \frac{1}{g_0}(g_1 + \dots + g_{n_0}) = \frac{1}{p^m} n_0 p^m = n_0,$$

$$\varphi_{L/K}(n_1) = n_0 + \frac{1}{g_0} \sum_{t=n_0+1}^{n_1} g_i = n_0 + \frac{(n_1 - n_0)p^{m-1}}{p^m} = n_0 + \frac{(n_1 - n_0)}{p}$$

and in general

$$\varphi_{L/K}(n_j) = n_0 + \frac{(n_1 - n_0)}{p} + \dots + \frac{(n_j - n_{j-1})}{p^j}$$

for $1 \leq j \leq m-1$. Thus, in the end we have to prove the congruences

$$n_j \equiv n_{j-1} \bmod p^j$$

for $1 \leq j \leq m-1$.

Recall the function

$$i_G \colon G \to \mathbb{Z}_{\geq 0} \cup \{\infty\},\ \tau \mapsto \nu_L(\tau(\pi_L) - \pi_L)$$

from Section 1.6. It has the decisive property that

$$i_G(s) \geq i+1 \text{ if and only if } s \in G_i$$

for $s \in G, i \geq -1$. We can conclude

$$\begin{aligned} & G(j) \subseteq G_i \\ \Leftrightarrow & \sigma^{p^j} \in G_i \\ \Leftrightarrow & i_G(\sigma^{p^j}) \geq i+1. \end{aligned}$$

We get

$$n_j + 1 = i(\sigma^{p^j})$$

for $0 \leq j \leq m-1$ as $\sigma^{p^j} \in G_{n_j} \setminus G_{n_j+1}$. Hence, in order to finish the proof of the Hasse-Arf theorem Theorem 1.40 it suffices to prove the congruences

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

for $1 \leq j \leq m$. For this we follow [Sen69] and consider the following slightly more general situation. Let A be a complete discrete valuation ring with perfect residue field k of characteristic p, fraction field $K = \mathrm{Frac}(A)$, normalized valuation ν_K and let us fix a uniformizer $\pi \in A$. Let

$$\sigma \colon K \to K$$

be a "wildly ramified" automorphism, i.e., σ is an automorphism of K preserving A, and $\nu_K(\sigma(x) - x) > 1$ for $x \in A$. Define

$$i(\sigma) := \nu_K(\sigma(\pi)/\pi - 1) = \nu_K(\sigma(\pi) - \pi) - 1 \in \mathbb{Z} \cup \{\infty\}$$

The function $\sigma \mapsto i(\sigma)$ has the following important property.

Lemma 1.48. *For $n \in \mathbb{Z}$ with p-adic valuation a we have*

$$i(\sigma^n) = i(\sigma^{p^a}).$$

Proof. Write $n = p^a m$ with $p \nmid m$. Then with $\tau := \sigma^{p^a}$ we get

$$\sigma^n - 1 = (\tau - 1)(\tau^{m-1} + \ldots + \tau + 1)$$

in the polnyomial ring $\mathbb{Z}[\sigma]$. As σ (and hence τ) is wildly ramified, τ acts trivially on

$$(\pi)^i/(\pi)^{i+1}$$

for each $i \geq 0$. Hence, $(\tau^{m-1} + \ldots + \tau + 1)$ acts via multiplication by m on $(\pi)^i/(\pi)^{i+1}$. As $p \nmid m$ we can conclude that $(\tau^{m-1} + \ldots + \tau + 1)$ preserves valuations, and thus that

$$i(\sigma^n) = \nu_K((\sigma^n - 1)\pi) - 1 = \nu_K((\tau - 1)\pi) - 1 = i(\tau)$$

as desired. □

Applying the following theorem in our previous setup with $K = L$ and $\sigma \colon L \to L$ the chosen generator of $G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/p^m$ finishes the proof of the Hasse-Arf Theorem 1.40 (and thereby of the local Kronecker-Weber Theorem 1.12).

Theorem 1.49 ([Sen69, Theorem 1])**.** *We have*

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

for each $j \geq 1$*.*

It is possible that $i(\sigma^{p^j}) = \infty$. In this case, ∞ is supposed to be equivalent to each natural number. In other words, if $i(\sigma^{p^j}) = \infty$, then nothing has to be proven.

Proof. By induction on $n \geq 1$ we prove that for any wildly ramified automorphism $\tau\colon K \to K$

$$i(\tau^{p^{j-1}}) \equiv i(\tau^{p^j}) \bmod p^j$$

for $1 \leq j < n$. If $n = 1$, then nothing has to be proven. Hence, assume that the statement is wrong for some $n \geq 2$ and σ, i.e.,

$$i(\sigma^{p^{n-1}}) \not\equiv i(\sigma^{p^n}) \bmod p^n.$$

Applying the induction hypothesis to σ^p we get

$$i(\sigma^{p^{n-1}}) = i((\sigma^p)^{p^{n-2}}) \equiv i((\sigma^p)^{p^{n-1}}) = i(\sigma^{p^n}) \bmod p^{n-1}.$$

Set

$$s := i(\sigma^{p^{n-1}}) - i(\sigma^{p^n}) \in \mathbb{Z}.$$

By Lemma 1.50 (applied to $\mu = s$ and σ^p) there exists an element $z \in K$ such that

$$\nu_K(z) = s,\ \nu_K(\sigma^p(z) - z) = s + i((\sigma^p)^s).$$

By Lemma 1.48 $i((\sigma^p)^s) = i((\sigma^p)^{p^{n-1}})$ because s has p-adic valuation $n-1$. Hence,

$$\nu_K(\sigma^p(z) - z) = s + i(\sigma^{p^n}) = i(\sigma^{p^{n-1}}).$$

Set

$$x := \sigma^{p-1}(z) + \ldots + \sigma(z) + z.$$

We have

$$\sigma^{p-1} + \ldots + \sigma + 1 \equiv (\sigma - 1)^{p-1} \bmod p$$

in the polynomial ring $\mathbb{Z}[\sigma]$. Hence, write

$$\sigma^{p-1} + \ldots + \sigma + 1 = (\sigma - 1)^{p-1} + pf(\sigma)$$

with $f(\sigma) \in \mathbb{Z}[\sigma]$. We can conclude

$$\nu_K(x) \geq \min\{\nu_K((\sigma(z) - z)^{p-1}, pf(\sigma)(z))\} > \nu_K(z)$$

as σ is wildly ramified and $\nu_K(p) > 0$. Moreover,

$$\nu_K(\sigma(x) - x) = \nu_K(\sigma^p(z) - z) = i(\sigma^{p^{n-1}}).$$

Write

$$x = \sum_{\mu=\nu_K(x)}^{\infty} x_\mu$$

as in Lemma 1.50, and define

$$y := \sigma(x) - x,\ y_\mu := \sigma(x_\mu) - x_\mu.$$

Let $\nu_p\colon \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ be the p-adic valuation and set

$$y_1 := \sum_{\nu_p(\mu)<n} y_\mu,$$

$$y_2 := \sum_{\nu_p(\mu) \geq n} y_\mu.$$

Consider a non-zero summand y_μ in y_2, in particuluar $\mu \in \mathbb{Z}, \mu \geq \nu_K(x)$ and $\nu_p(\mu) \geq n$. Then

$$\nu_K(y_\mu) = \mu + i(\sigma^\mu) \overset{Lemma\ 1.48}{=} \mu + i(\sigma^{p_p^\nu(\mu)}) \geq \nu_K(x) + i(\sigma^{p^n}) > s + i(\sigma^{p^n}) = i(\sigma^{p^{n-1}})$$

by our construction of x and the fact that $i(\sigma^{p^{\nu_p(\mu)}}) \geq i(\sigma^{p^n})$. In particular, each summand of y_2 has valuation $> \nu_K(y) = i(\sigma^{p^{n-1}})$. We can conclude

$$\nu_K(y) = \nu_K(y_1).$$

The crucial point in the proof is the observation that the

$$\nu_K(y_\mu) = \mu + i(\sigma^\mu)$$

for $\mu \in \mathbb{Z}, \nu_p(\mu) < n, x_\mu \neq 0$ and $i(\sigma^{p^{n-1}})$ are all *pairwise distinct*. Granting this, the valuation of y_1 must be distinct from y, which then finishes the proof. Therefore assume that

$$\mu + i(\sigma^\mu) = \lambda + i(\sigma^\lambda)$$

for $\mu, \lambda \in \mathbb{Z}$ with $\nu_p(\mu), \nu_p(\lambda) < n$. If $\nu_p(\mu) = \nu_p(\lambda)$, then by Lemma 1.48 $i(\sigma^\mu) = i(\sigma^\lambda)$, which then implies $\mu = \lambda$. Hence, we may assume that $\nu_p(\mu) > \nu_p(\lambda)$. Then

$$\nu_p(\mu + \lambda) = \min\{\nu_p(\mu), \nu_p(\lambda)\} = \nu_p(\lambda).$$

By the induction hypothesis we know that

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

for $1 \leq j < n$. As $\nu_p(\lambda) < \nu_p(\mu) < n$ we can conclude that

$$i(\sigma^\mu) \equiv i(\sigma^\lambda) \bmod p^{\nu_p(\mu)}.$$

This implies that

$$\nu_p(i(\sigma^\mu) - i(\sigma^\lambda)) \geq \nu_p(\mu) > \nu_p(\lambda).$$

Therefore, $i(\sigma^\mu) - i(\sigma^\lambda) \neq \lambda - \mu$ as desired. If $\nu_p(\mu) < n$ and $i(\sigma^{p^{n-1}}) = \mu + i(\sigma^\mu)$, then

$$i(\sigma^\mu) \equiv i(\sigma^{p^{n-1}}) \bmod p^{n-1},$$

which implies $p^{n-1} \mid \mu$, i.e., $\nu_p(\mu) = n + 1$. But then $i(\sigma^{p^{n-1}} = i(\sigma^\mu)$ and thus $\mu = 0$, which is contradicting $\nu_p(\mu) < n$. Thus, the proof is finished. □

We used the following lemma in the proof of Theorem 1.49.

Lemma 1.50. *For each $\mu \in \mathbb{Z}$ there exists an element $x_\mu \in K$, such that $\nu_K(x_\mu) = \mu$ and $\nu_K(\sigma(x_\mu) - x_\mu) = \mu + i(\sigma^\mu)$. Moreover, each $x \in K$ can be written as*

$$x = \sum_{\mu = \nu_K(x)}^{\infty} x_\mu$$

with x_μ for $\mu \geq \nu_K(x)$ being zero or satisfying $\nu_K(x_\mu) = \mu$ and $\nu_K(\sigma(x_\mu) - x_\mu) = \mu + i(\sigma^\mu)$.

Proof. Assume $\mu \geq 0$. Then set

$$x_\mu := \prod_{i=0}^{\mu-1} \sigma^i(\pi).$$

Then $\nu_K(x_\mu) = \mu$. Moreover,

$$\nu_K(\sigma(x_\mu) - x_\mu) = \nu_K(x_\mu) + \nu_K(\frac{\sigma(x_\mu)}{x_\mu} - 1) = \mu + \nu_K(\frac{\sigma(x_\mu)}{x_\mu} - 1)$$

and

$$\frac{\sigma(x_\mu)}{x_\mu} = \frac{\sigma^\mu(\pi)}{\pi}.$$

This implies

$$\nu_K(\frac{\sigma(x_\mu)}{x_\mu} - 1) = \nu_K(\frac{\sigma^\mu(\pi)}{\pi} - 1) = i(\sigma^\mu)$$

and therefore $\nu_K(\sigma(x_\mu) - x_\mu) = \mu + i(\sigma^\mu)$ as desired. If $\mu < 0$ set $x_\mu = \frac{1}{x_{-\mu}}$ with the previously defined $x_{-\mu}$. Then $\nu_K(x_\mu) = \mu$ and

$$\begin{aligned}
&\nu_K(\sigma(x_\mu) - x_\mu) \\
=&\mu + \nu_K(\frac{\sigma(x_\mu)}{x_\mu} - 1) \\
=&\mu + \nu_K(\frac{\pi}{\sigma^{-\mu}(\pi)} - 1) \\
=&\mu + \nu_K(\frac{\sigma^\mu(\pi)}{\pi} - 1) \\
=&\mu + i(\sigma^\mu),
\end{aligned}$$

which finishes the proof of the first assertion. For the last statement let $x \in K$ and let

$$[-] \colon k \to A$$

be the Teichmüller lift, cf. [Tia, Proposition 8.3.5.]. Note that

$$\sigma([\lambda]) = [\lambda]$$

for each $\lambda \in k$ as σ is wildly ramified. If x_μ satisfies

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

then $[\lambda]x_\mu$ is therefore zero or satisfies the same statements. Now it is clear by successive approximation that desired expression for x exists. □

Exercise 1.51. Let A be a complete discrete valuation ring with perfect residue field k and $K := \mathrm{Frac}(A)$ its fraction field.

(1) Let L/K be a totally ramified finite Galois extension with Galois group $G := \mathrm{Gal}(L/K)$. Let $f(X) \in A[X]$ be the minimal polynomial of a uniformizer $\pi_L \in L$ over K. Show that

$$\nu_L(f'(\pi_L)) = \sum_{s \neq 1} i_G(s) = \sum_{i=0}^{\infty} (\sharp(G_i) - 1).$$

(2) Assume that k is finite with $q := \sharp k$. Show that the Galois group of the maximal tamely ramified extension of K (inside some fixed algebraic closure of K) is isomorphic to the semidirekt product

$$\widehat{\mathbb{Z}}' \rtimes \widehat{\mathbb{Z}}$$

with $1 \in \widehat{\mathbb{Z}}$ acting on $\widehat{\mathbb{Z}}' := \varprojlim_{(n,q)=1} \mathbb{Z}/n$ by multiplication with q.

1.10. **Supplements on local class field theory.** We mention several statements that also fall in the realm of "local class field theory". The first is the computation of the Brauer group of a local field.

The (cohomological) Brauer group of a field K is defined as the second Galois cohomology group

$$\mathrm{Br}(K) = H^2_{\mathrm{cts}}(\mathrm{Gal}(\overline{K}/K), K^\times)$$

and it identifies with the (Azumaya) Brauer group of equivalence classes of central simple algebras over K.

If K is a non-archimedean local field, then there exists an isomorphism

$$\mathrm{inv}\colon \mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z},$$

cf. [Ser13, Chapter XII, §.3].

When discussing formal A-modules of height $h \geq 1$ we will construct explicit central division algebras D_h with $\mathrm{inv}(D_h) = 1/h$.

Another topic which was left over is the independece of the morphism

$$r := r_\pi\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

in Section 1.5. We may come back to this question after discussing deformation theory of formal A-modules.

We did not show (and don't plan to do so) that for a finite abelian extension L/K the kernel of the composition

$$r\colon K^\times \to \mathrm{Gal}(K_\pi/K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

is given by the norm subgroup $N_{L/K}(L^\times) \subseteq K^\times$. We won't discuss functoriality of r if K changes either.

2. Lubin-Tate spaces

We want to study formal A-modules and in particular formal group laws further. It is clear that the definition of a formal A-module Definition 1.24 generalizes to any ring A, i.e., if A is any ring, R an A-algebra, then a (commutative) formal group law

$$F \in R[[X, Y]]$$

together with a ring homomorphism $[-]_F \colon A \to \mathrm{End}_{\mathrm{FGL}(R)}(F)$ can be called a formal A-module if

$$[a]_F(X) \equiv aX \bmod (X)^2$$

for any $a \in A$. Let us denote by

$$\mathrm{FGL}_A(R)$$

the category of formal A-modules (with the natural choice for morphisms, cf. Section 1.4). Clearly each morphism $\varphi \colon R \to S$ of A-algebras induces a functor, denoted by φ_* or $-\hat{\otimes}_R S$,

$$\mathrm{FGL}_A(R) \to \mathrm{FGL}_A(S),$$

by applying φ to the coefficients of $F \in R[[X, Y]]$ and $[a]_F \in R[[X]], a \in A$.

The typical example of a formal A-module is the formal additive A-module $\widehat{\mathbb{G}_a}$ given by

$$F(X, Y) := X + Y,\ [a]_F(X) := aX,\ a \in A,$$

and for a general A each formal A-module will be isomorphic to this, e.g., if A contains an infinite field.[7] Therefore we will mostly assume that $A = \mathbb{Z}$, where formal A-modules are just formal group laws, or A a (not necessarily complete) discrete valuation ring with finite residue field, which captures localisations $\mathbb{Z}_{(p)}$ or rings of integers in (non-archimedean) local fields. It may be possible that the results presented here admit suitable generalizations to the case that A is a Dedeking ring with finite residue fields at maximal ideals, but we don't pursue this question here.

We leave the following as an exercise.

Exercise 2.1. Let A be any ring, R an A-algebra and $a \in A$.

(1) If a is invertible in R, then the category $\mathrm{FGL}_A(R)$ is equivalent to the category $\mathrm{FGL}_{A[1/a]}(R)$ of formal $A[1/a]$-modules.
(2) If a is nilpotent in R, then the category $\mathrm{FGL}_A(R)$ is equivalent to the category $\mathrm{FGL}_{\widehat{A}_a}$ of formal $\widehat{A}_a$-modules, with $\widehat{A}_a$ the (a)-adic completion of A.

Thus depending on R we may change A without any trouble. Let us note that formal A-module *laws* exist in abundance and the problem is to classify them up to isomorphism. More formally, for $R \in \mathrm{Alg}_A$ set

$$G(R) := \{g(X) \in R[[X]] \mid f(0) = 0, f'(0) \in R^\times\}.$$

For any $g \in G(R)$ the substitution

$$g \colon R[[X]] \to R[[X]],\ X \mapsto g(X)$$

[7] This will implicitly be proven in this chapter.

defines an R-algebra isomorphism (this is implicit in Exercise 2.1). Let us write g^{-1} for its inverse, i.e., $g^{-1}(X) \in G(R)$ is the unique power series satisfying

$$g^{-1}(g(X)) = X,\ g(g^{-1}(X)) = X.$$

On checks that the set $G(R)$ is naturally a group for the binary operation

$$g \circ h := g(h(X)).$$

Moreover, it acts on $\mathrm{FGL}_A(R)$: Given any formal A-module (law) $F \in R[[X,Y]]$ we obtain the new formal A-module (law)

$$F^g := g^{-1}(F(g(X), g(Y))) \in R[[X,Y]]$$

with formal multiplication

$$[a]_{F^g}(X) := g^{-1}([a]_F(g(X)) \in R[[X]],\ a \in A.$$

By construction the power series $g(X) \in R[[X]]$ defines an isomorphism

$$g\colon F^g \xrightarrow{\simeq} F$$

of formal A-modules. The classification of formal A-modules amounts therefore to understanding the $G(R)$-orbits on $\mathrm{FGL}_A(R)$.[8]

For the rest of this chapter we will follow (at least) [HG94], [Dri74] and lecture notes of Fargues [Far] resp. Lurie [Lur10].

As a start, we discuss the height of a formal A-module.

2.1. **The height of a formal A-module.** Assume that A is a (not necessarily complete) discrete valuation ring with uniformizer $\pi \in A$ and finite residue field $k = A/\pi$ of characteristic p and cardinality $q = p^c$.

Assume that R is an A-algebra with $\pi R = 0$ and that

$$F \in R[[X,Y]]$$

is a formal A-module, whose multiplication we denote by

$$\iota\colon A \to \mathrm{End}_{\mathrm{FGL}(R)}(F)$$

or

$$[a] = [a]_F = \iota(a) \in R[[X]].$$

Let us note that although $\pi R = 0$ we need not have $\iota(\pi) = 0$. All we know is that

$$\iota(\pi)(X) \equiv \pi X \equiv 0 \bmod (X)^2.$$

In order to state the next lemma we have to discuss the Frobenius twists of formal A-modules. Let

$$\mathrm{Frob}_p\colon R \to R,\ r \mapsto r^p$$

be the p-Frobenius of R and

$$\mathrm{Frob}_q = \mathrm{Frob}_p^c\colon R \to R,\ r \mapsto r^q$$

be its q-Frobenius for $q = p^c$. Note that Frob_q is a morphism of A-algebras but Frob_p not if $q \neq p$. Applying for $b \geq 1$ the morphism Frob_p^b to the coefficients of a formal A-module F over R and its A-multiplication $\iota(a), a \in A$, we obtain a formal group (the "b-th Frobenius twist of F")

$$F^{(p^b)} := \mathrm{Frob}_{p_*}^b F,$$

[8]The functors $R \mapsto \mathrm{FGL}_A(R),\ R \mapsto G(R)$ are corepresentable (the latter by $R[r_1^{\pm}, r_2, r_3, \ldots]$). Therefore the better aim should be to understand the stack quotient $[\mathrm{FGL}_A/G]$.

which is equipped with the ring morphism

$$\iota^{(p^b)}\colon A \to \mathrm{End}_{\mathrm{FGL}(R)}(F^{(p^b)})$$

by raising the coefficients of $[a]_F(X), a \in A$, to their p^b-th power. If $c \mid b$ the pair $(F^{(p^b)}, \iota^{(p^b)})$ is again a formal A-module. Indeed,

$$\iota^{(p^b)}(a)(X) \equiv a^{p^b} X \equiv aX \bmod (X)^2$$

for $a \in A$ in this case. The map ("the b-the Frobenius of F")

$$\varphi_{F,p^b}\colon F \to F^{(p^b)},\ X \mapsto X^{p^b}$$

is a morphism of formal groups and A-linear with respect to $\iota, \iota^{(p^b)}$. Indeed,

$$(F(X,Y))^{p^b} = F^{(p^b)}(X^{(p^b)}, Y^{(p^b)})$$

as follows from the fact that $\mathrm{Frob}_p^b\colon R[[X,Y]] \to R[[X,Y]]$ is a ring homomorphism. If $c \mid b$, then φ_F^b is even a morphism of formal A-modules.

In the following we let

$$f' \in R[[X]]$$

be the formal derivative of a power series $f \in R[[X]]$.

Lemma 2.2 ([HG94, Lemma 4.1.], [Far, 1.8.2.])**.** *Let $f\colon F_1 \to F_2$ be a morphism of formal A-modules over k'. If $f'(0) = 0$, then*

$$f(X) = g \circ \varphi_{F^{(q)}}(X) = g(X^q)$$

for some morphism $g\colon F^{(q)} \to F$. In particular, if $R = k'$ is a field extension of k, then either $f = 0$ or there exist a unique $h \in \mathbb{Z}_{\geq 0}$, and a morphism $g\colon F_1^{q^h} \to F_2$ of formal A-modules such that

$$f(X) = g \circ \varphi_{F^{(q^h)}}(X) = g(X^{q^h})$$

and $g'(0) \neq 0$.

In the case that $R = k'$ is a field we call h the height of the homomorphism f and write $\mathrm{ht}(f)$ for it. By convention we set $\mathrm{ht}(0) := \infty$. Clearly, if $f_1\colon F_1 \to F_2$ is of height h_1 and $f_2\colon F_2 \to F_3$ of height h_2, then $f_2 \circ f_1$ is of height $h_1 + h_2$. Moreover, a homomorphism is of height 0 if and only if it is an isomorphism.

Proof. By Exercise 2.1 we may assume that A is complete. We first prove that $f' = 0$. Let us take the derivative of

$$f(F_1(X,Y)) = F_2(f(X), f(Y))$$

with respect to X. This yields

$$f'(F_1(X,Y))\frac{\partial F_1}{\partial X}(X,Y) = \frac{\partial F_2}{\partial X}(f(X), f(Y))f'(X).$$

and thus by setting $X = 0$ (using $F_1(0,Y) = Y, f(0) = 0, f'(0) = 0$)

$$f'(Y)\frac{\partial F_1}{\partial X}(0,Y) = \frac{\partial F_2}{\partial X}(0, f(Y))f'(0) = 0.$$

But

$$\frac{\partial F_1}{\partial X}(0,Y) = 1 \bmod (X,Y)$$

and thus $\frac{\partial F_1}{\partial X}(0,Y) \in R[[X]]^\times$ is a unit, which implies that

$$f'(Y) = 0.$$

This implies that we can write

$$f(X) = g_1(X^p)$$

with $g_1 \in R[[X]] \in k'$ because $p = 0 \in R$ and each $n \in \mathbb{Z}$ prime to p is invertible in R. We claim that

$$g_1(F_1^{(p)}(X,Y)) = F_2(g_1(X), g_1(Y)) \in R[[X,Y]], \tag{8}$$

i.e., that $g_1 \colon F_1^{(p)} \to F_2$ is a morphism of formal groups. But the R-algebra morphism

$$R[[X,Y]] \to R[[X,Y]],\ X,Y \mapsto X^p, Y^p$$

is injective and maps (8) to

$$g_1(F_1^{(p)}(X^p,Y^p)) = g_1((F_1(X,Y))^p) = f(F_1(X,Y))$$

resp.

$$F_2(g_1(X^p), g_1(Y^p)) = F_2(f(X), f(Y)).$$

As $f \colon F_1 \to F_2$ is a morphism, we can conclude that (8) holds. Similarly, one checks that morphism g_1 is A-linear, i.e.,

$$g_1(\iota_{F_1}^{(p)}(a)(X)) = \iota_{F_2}(a)(g_1(X))$$

for $a \in A$. Write $q = p^c$ with $c \geq 1$. Iterating the above argument with f replaced by g_1, it suffices to show the following claim. If for $1 \leq b < c$ there exists an A-linear morphism

$$g \colon F_1^{(p^b)} \to F_2$$

such that

$$f(X) = g \circ \varphi_{F,p^b}(X) = g(X^{(p^b)}),$$

then $g'(0) = 0$. Write

$$f(X) = dX^{p^b} \bmod (X^{p^b+1})$$

with $d = g'(0)$. The ring A contains a primitive $q-1$-th root of unity $\zeta \in A$. By A-linearity of f we know that

$$[\zeta]_{F_2}(f(X)) = f([\zeta]_{F_1}(X)).$$

Now looking at the coefficients of X^{p^b} on both sides we find

$$\zeta d = \zeta^{p^b} d.$$

As $b < c$ the element $1 - \zeta^{p^b-1} \in A$ is a unit. This implies $d = 0$ as desired. □

We can now define the *height* of a formal A-module.

Definition 2.3. *Let k' be a field extension of k and let F be a formal A-module over k'. Then we define the height h of F as the height of the endomorphism $[\pi]_F \colon F \to F$.*

As the height can also be defined as the largest integer such that $[\pi]_F \colon F \to F$ factors over $F^{(q^h)}$ we see that the height does not depend on the choice of the uniformizer π. By construction the Lubin-Tate formal A-module in Section 1.3 is of height 1. The formal A-module $\hat{\mathbb{G}}_a$ associated to

$$F(X,Y) = X + Y \in k[[X,Y]]$$

and

$$[a](X) = aX,\ a \in A,$$

is of height ∞ as $\pi \equiv 0 \in k$.

Let us now produce examples of formal A-modules of height $h \in \mathbb{Z}_{\geq 1}$.

Lemma 2.4. *For $1 \leq h < \infty$ there exists a unique formal A-module $F_h \in A[[X,Y]]$ with $[\pi]_{F_h}(X) = X^{q^h} + \pi X$. Moreover, $F_h \hat{\otimes}_A k$ is of height h and $A \cong \mathrm{End}_{\mathrm{FGL}_A(A)}(F_h)$.*

Note that we could replace $X^{q^h} + \pi X$ here by any other $f(X) \in A[[X,Y]]$ such that $f(X) \equiv \pi X \bmod (X)^2$ and $f(X) \equiv X^{q^h} \bmod (\pi)$.

Proof. Using Remark 1.15 all statements follow from Lemma 1.14. □

In particular, over $k = A/\mathfrak{m}_A$ there exists formal A-modules of arbitrary height $h \geq 1$, and then by base change over any field extension of k. The height is an interesting invariant of formal A-modules over fields.

Theorem 2.5. *Assume that k'/k is a separably closed field. Then two formal A-modules $F_1, F_2 \in k'[[X,Y]]$ are isomorphic if and only if they have the same height.*

The "only if" statement is easy. More generally, there do not exist any non-zero morphisms of formal A-modules of different height as the height is additive under composition. We will prove this theorem in Theorem 2.29. For mention the following applications of heights.

Exercise 2.6. Assume that A is complete and let $h \in \mathbb{Z}_{\geq 1}$. Let $\overline{F}_h \in k[[X,Y]]$ be the reduction of the formal A-module F_h from Lemma 2.4. Show that

$$\mathrm{End}_{\mathrm{FGL}_A(k)}(\overline{F}_h) \cong A[\Pi]/(\Pi^h - \pi)$$

with Π the endomorphism X^q of $\overline{F}_h$.

2.2. **Lubin-Tate spaces via formal group laws.** Let us now give the definition of Lubin-Tate spaces. Let A be a complete discrete valuation ring with finite residue field k of characteristic p and cardinality q. Fix a uniformizer $\pi \in A$. We let

$$\mathrm{Nilp}_A$$

be the category of A-algebras R such that π is nilpotent in R. Thus Nilp_A is the "union" of the categories of A/π^n-algebras for $n \geq 0$.

Let us fix a formal A-module $F_h \in k[[X,Y]]$ of height $h \in \mathbb{Z}_{\geq 1}$, e.g., the reduction of the F_h constructed in Lemma 2.4 with

$$[\pi]_{F_h}(X) = X^{q^h} \in k[[X]].$$

Definition 2.7. *Let $R \in \mathrm{Nilp}_A$, and $f\colon F \to G$ a morphism of formal A-modules given by the power series $f(X) \in R[[X]]$. Then f is called a $\star$-isomorphism if there exists a nilpotent ideal $I \subseteq R$ such that*

$$f(X) \equiv X \ \mathit{mod}\ I,$$

i.e., if f reduces to the identity modulo $I \subseteq R$.

Note that $f'(0) \in R^\times$ as I is nilpotent. In particular, each $\star$-isomorphism is an isomorphism of formal A-module(law)s. Moreover, the existence of a $\star$-isomorphism $f\colon F \to G$ forces $F \equiv G \bmod I$.

We can now define the Lubin-Tate space (for height h) as the space of $\star$-deformations of F_h.

Definition 2.8. *For $R \in \mathrm{Nilp}_A$ we set*

$$\mathcal{M}_{F_h}(R)$$

as the set of $\star$-isomorphism classes of formal A-module laws $F \in R[[X,Y]]$ such that $F \equiv F_h \in R/I[[X,Y]]$ for some nilpotent ideal $I \subseteq R$ with $\pi \in I$. The functor

$$\mathcal{M}_{F_h}\colon \mathrm{Nilp}_A \to (\mathrm{Sets})$$

is called the Lubin-Tate space (for F_h).

Let us call a formal A-module $F \in R[[X,Y]]$ such that $F \equiv F_h \bmod I$ for some finitely generated nilpotent ideal $I \subseteq R$ containing π a $\star$-deformation of F_h over R.

The next aim of this course is to prove the following (version of a) theorem of Lubin and Tate, cf. [LT66, Theorem 3.1.], [HG94, Proposition 12.10].

Theorem 2.9 (Representability of Lubin-Tate space)**.** *For $h \in \mathbb{Z}_{\geq 1}$ there exists an isomorphism*

$$\mathrm{Spf}(A[[X_1,\dots,X_{h-1}]]) \cong \mathcal{M}_{F_h},$$

where $\mathrm{Spf}(A[[X_1,\dots,X_{h-1}]])$ denotes the functor

$$\mathrm{Nilp}_A \to (\mathrm{Sets}),\ R \mapsto \mathrm{Hom}_{A,\mathrm{cts}}(A[[X_1,\dots,X_{h-1}]], R)$$

with R viewed as a discrete A-algebra.

In particular, we can construct many $\star$-deformations over an A-algebra $R \in \mathrm{Nilp}_A$. From another viewpoint Theorem 2.9 equips the $\mathrm{Spf}(A[[X_1,\dots,X_{h-1}]])$ with more structure, namely a (pro-)universal $\star$-deformation of F_h. This additional structure is highly interesting as it leads to the Gross-Hopkins period morphism and the higher level Lubin-Tate spaces.

The following lemma is a critical place where the assumption that $h \in \mathbb{Z}_{\geq 1}$ is used.

Lemma 2.10. *Assume $h \in \mathbb{Z}_{\geq 1}$. Let $R \in \mathrm{Nilp}_A$, $I \subseteq R$ a nilpotent ideal and let $f\colon F_1 \to F_2$ be a morphism of formal A-modules over R. If F is a $\star$-deformation of F_h with $h \in \mathbb{Z}_{\geq 1}$ and $f \equiv 0$ mod I, then $f = 0$.*

Proof. Assume $I^n = 0$. Considering the surjections

$$R = R/I^n \to R/I^{n-1} \to \ldots \to R/I$$

we can reduce to the case that $I^2 = 0$. Let $J \subseteq R$ be a nilpotent ideal containing π such that $F \equiv F_h \bmod I$. Using the filtration

$$0 = J^i I \subseteq \ldots \subseteq J^i I \subseteq \ldots \subseteq JI \subseteq I$$

for some $i \geq 0$, we may assume that $JI = 0$. In particular, $\pi I = 0$. By assumption the power series

$$f(X) \in R[[X]]$$

has coefficients in I. Write

$$[\pi]_{F_1} = aX^{q^h} + h(X)$$

with $a \in R^\times$ and $h(X) \in R[[X]]$ having coefficients in $J = (\pi, J)$ (this is possible by our assumption that $F_1 \equiv F_h \bmod J$). Because $0 = \pi I = JI$ we can conclude that

$$f([\pi]_{F_1}(X)) = f(aX^{q^h}).$$

On the other hand,

$$f([\pi]_{F_1}(X)) = [\pi]_{F_2}(f(X)) = \pi f(X) = 0$$

because $I^2 = \pi I = 0$ and $[\pi]_{F_2}(X) \equiv \pi X \bmod (X)^2$. Because

$$R[[X]] \to R[[X]],\ X \mapsto aX^{q^h}$$

is injective we can conclude that $f = 0$ as desired. □

Lemma 2.10 implies that each morphism

$$f \colon F \to \hat{\mathbb{G}}_a$$

of formal A-modules over R is zero if F is a $\star$-deformation of F_h with $h \in \mathbb{Z}_{\geq 1}$. Indeed, by Lemma 2.10 we may replace R by $R/(\pi, J)$, and then use that

$$f([\pi]_{F_h}(X)) = f(X^{q^h})$$

while

$$[\pi]_{\widehat{\mathbb{G}}_a}(f(X)) = \pi f(X) = 0.$$

Another corollary of Lemma 2.10 is that there exists at most one $\star$-isomorphism between two $\star$-deformations of F_h.

If $R \in \mathrm{Nilp}_A$ is local artinian, then its maximal ideal $\mathfrak{m}_R \subseteq R$ is nilpotent. From Lemma 2.10 we obtain that the sets of isomorphism classes of $\star$-deformations over R identifies with

$$\{F \in R[[X, Y]] \mid F = F_h \bmod \mathfrak{m}_R\}/\simeq,$$

where two such F_1, F_2 are called equivalent if there exists an isomorphism $f \colon F_1 \to F_2$ reducing to the identity modulo $\mathfrak{m}_R$.

This explains the link between Definition 2.8 and the viewpoint taken in the references [LT66], [HG94] and [Far]. We choose this different presentation as it closer to the definition of a Rapoport-Zink space.

2.3. **Lazard's theorem for formal A-modules.** The proof of Theorem 2.9 requires a detailed understanding of formal A-modules. Let us assume that A is a (not necessarily complete) discrete valuation ring with finite residue field as before or $A = \mathbb{Z}$.

Let R be an A-algebra. We will analyze formal A-modules

$$F \in R[[X,Y]], [a]_F(X) \in R[[X]], a \in A,$$

by approximating them modulo powers of $(X,Y) \subseteq R[[X,Y]]$.

Definition 2.11. *Let $n \geq 2$. An n-truncated (commutative, one-dimensional) formal group law is an element $F \in R[[X,Y]]/(X,Y)^n$ such that*

1. $F(X,0) = X, F(0,Y) = Y$,
2. $F(X,F(Y,Z)) = F(F(X,Y),Z) \in R[[X,Y,Z]]/(X,Y,Z)^n$
3. $F(X,Y) = F(Y,X) \in R[[X,Y]]/(X,Y)^n$.

Let $\mathrm{FGL}_{\leq n}(R)$ be the category of n-truncated formal group laws (with the natural notion of morphisms, cf. Definition 1.24). An n-truncated formal group law F together with a ring homomorphism

$$\iota_F \colon A \to \mathrm{End}_{\mathrm{FGL}_{\leq n}(R)}(F),\ a \mapsto [a]_F$$

is called an n-truncated formal A-module if $[a]_F(X) = aX \mod (X)^2$ for all $a \in A$. We let $\mathrm{FGL}_{\leq n,A}(R)$ be the category o n-truncated formal A-modules (with morphisms the A-linear morphisms of n-truncated formal group laws).

Here as for the case of formal group laws

$$\mathrm{FGL}_{\leq n}(R)$$

denotes the category of n-truncated formal group laws, which is naturally enriched in abelian groups. It is clear that modding out the degree n part everywhere yields a functor

$$\mathrm{FGL}_{\leq n+1,A}(R) \to \mathrm{FGL}_{\leq n,A}(R)$$

from the category of $n+1$-truncated formal A-modules to n-truncated formal A-modules for any A-algebra R. Moreover, the category of formal A-modules can be reconstructed via

$$\mathrm{FGL}_A(R) \cong \varprojlim_n \mathrm{FGL}_{\leq n,A}(R).$$

A key ingredient in understanding formal A-module laws is to understand the fibers of

$$\mathrm{FGL}_{\leq n+1,A}(R) \to \mathrm{FGL}_{\leq n,A}(R).$$

This is partly answered by the following lemma, which is a combination of [Laz55, Proposition 1] and [Dri74, §1].

Lemma 2.12. *Let $n \geq 2$. Let*

$$F_1 \in R[[X,Y]]/(X,Y)^{n+1}, [a]_{F_1} \in R[[X]]/(X)^{n+1},$$

be an $(n+1)$-truncated formal A-module and let

$$F_2 \in R[[X,Y]]/(X,Y)^{n+1}, [a]_{F_2}(X) \in R[[X]]/(X)^{n+1}, a \in A,$$

be elements such that $F_1 \equiv F_2 \mod (X,Y)^n, [a]_{F_1} \equiv [a]_{F_2} \mod (X)^n$ for $a \in A$. Then F_2 is an $(n+1)$-truncated formal A-module with multiplication $[-]_{F_2}$ if and only if for

$$\Gamma(X,Y) := F_2(X,Y) - F_1(X,Y)$$

and

$$[a]_{F_2}(X) - [a]_{F_1}(X) = h(a)X^n, a \in A,$$

the following equations are satisfied:

(1) $\Gamma(X,0) = 0$, $\Gamma(0,Y) = 0$,
(2) $\Gamma(Y,X) + \Gamma(X,Y+Z) = \Gamma(X,Y) + \Gamma(X+Y,Z)$,
(3) $\Gamma(X,Y) = \Gamma(Y,X)$,
(4) $h(a)(X^n + Y^n) + a^n\Gamma(X,Y) = h(a)(X+Y)^n + a\Gamma(X,Y)$,
(5) $h(a+b)X^n = h(a)X^n + h(b)X^n + \Gamma(aX,bY)$,
(6) $h(ab) = ah(b) + h(a)b^n$

for $a, b \in A$.

Proof. This follows directly by plugging in the definitions and using repeatedly that all terms of degree $\geq n+1$ vanish. For example,

$$F_2(X,Y) \equiv F_2(Y,X)$$

if and only if $\Gamma(X,Y) \equiv \Gamma(Y,X)$ as $F_1(X,Y) \equiv F_1(Y,X)$. As another example we can calculate

$$\begin{aligned} &F_2([a]_2(X), [a]_2(Y)) \\ \equiv &F_1([a]_{F_1}(X), [a]_{F_1}(Y)) + a^n\Gamma(X,Y) + h(a)(X^n + Y^n) \bmod (X,Y)^{n+1} \end{aligned}$$

while

$$\begin{aligned} &[a]_{F_2}(F_2(X,Y)) \\ \equiv &[a]_{F_1}(F_1(X,Y)) + a\Gamma(X,Y) + h(a)(X+Y)^n \bmod (X,Y)^{n+1} \end{aligned}$$

for $a \in A$. The required equations

$$[a+b]_{F_2}(X) = F_2([a]_{F_2}(X), [b]_{F_2}(X))$$

and

$$[ab]_{F_2}(X) = [a]_{F_2}([b]_{F_2}(X))$$

for $a, b \in A$ yield the other conditions. □

Note that in these formulas we did not use the multiplication in R, only its A-linear structure. If M is any A-module and $n \geq 2$, then we therefore set

$$\mathcal{D}_{n,A}(M)$$

as the A-module of elements $m_i \in M, 0 < i < n, h(a) \in M, a \in A$, such that with the formal expression

$$\Gamma(X,Y) := \sum_{0<i<n} m_i X^i Y^{n-i}$$

the equations in Lemma 2.12 are satisfied. It is easy to write down elements in $\mathcal{D}_{n,A}(M)$. Set

$$B_n(X,Y) := (X+Y)^n - X^n - Y^n \in \mathbb{Z}[X,Y],$$

and let

$$\gamma_n \in \mathcal{D}_{n,A}(A)$$

be the element given by the collection

$$\{\Gamma(X,Y) := B_n(X,Y), h(a) := (a^n - a), a \in A\}.$$

It is easily checked that γ_n is well-defined, i.e., the equations in Lemma 2.12 are satisfied. For any $m \in M$ we therefore obtain the element

$$\gamma_n \cdot m \in \mathcal{D}_{n,A}(M).$$

The following lemma is the crucial point in the proof of Lazard's theorem. For $A = \mathbb{Z}$ it is [Laz55, Lemme 3] and for A a discrete valuation ring with finite residue field it will be extracted from [Dri74, Proposition 1.3.]. We will give the proof of Lemma 2.13 in Section 2.4.

Lemma 2.13 (Lazard, Drinfeld)**.** *Let $n \geq 2$.*

1. *Assume $A = \mathbb{Z}$. If n is not a prime power, then set $\gamma_{\mathrm{div},n} = \gamma_n \in \mathcal{D}_{n,A}(A)$. If $n = p^h$ is a prime power, then there exists a unique $\gamma_{\mathrm{div},n} \in \mathcal{D}_{n,A}(A)$ such that $p\gamma_{\mathrm{div},n} = \gamma_n$. In both cases, the element $\gamma_{\mathrm{div},n} \in \mathcal{D}_{n,A}(A)$ represents the functor $\mathcal{D}_{n,A}(-)$.*
2. *Assume that A is a discrete valuation ring with finite residue field k having q elements. Let $\pi \in A$ be a uniformizer. If n is not a power of q set $\gamma_{\mathrm{div},n} := \gamma_n \in \mathcal{D}_{n,A}(A)$. If n is a power of q, then there exists a unique element $\gamma_{\mathrm{div},n} \in \mathcal{D}_{n,A}(A)$ such that $\pi\gamma_{\mathrm{div},n} = \gamma_n$. In both cases, the element $\gamma_{\mathrm{div},n} \in \mathcal{D}_{n,A}(A)$ represents the functor $\mathcal{D}_{n,A}(-)$.*

In other words, if M is an arbitrary A-module and $\gamma \in \mathcal{D}_{n,A}(M)$, then there exists a unique $m \in M$, such that

$$\gamma = \gamma_{\mathrm{div},n} \cdot m.$$

By Lemma 2.12 we can conclude that if

$$F \in R[[X,Y]], [a]_F(X), a \in A,$$

is an $n+1$-truncated formal A-module, then the $n+1$-truncated formal A-modules agreeing with F modulo $(X,Y)^n$ differ from $F, [a]_F$ by a multiple (in R) of the generator $\gamma_{n,\mathrm{div}} \in \mathcal{D}_{n,A}(A)$.

Let us make this explicit for small $n \geq 2$ if $A = \mathbb{Z}$. For this let d_n be the greatest common divisor of the coefficients of $B_n(X,Y)$. When proving Lemma 2.13 we will prove that

$$d_n = \begin{cases} 1, & \text{if } n \text{ is not a prime power,} \\ p, & \text{if } n \text{ is a power of the prime } p. \end{cases}$$

For $A = \mathbb{Z}$ it follows from Lemma 2.13 that the canonical element $\gamma_{\mathrm{div},n}$ is given by

$$C_n(X,Y) := \frac{1}{d_n} B_n(X,Y).$$

By definition, $X + Y \in R[[X,Y]]/(X,Y)^2$ is the only 2-truncated formal group law. It is easily checked that the 3-truncated formal group laws are exactly the

$$F(X,Y) = X + Y + a_1 XY$$

for some $a_1 \in R$ where

$$XY = C_2(X,Y),$$

and that these define actual formal group laws (and not just truncated ones). This implies that the 4-truncated formal group laws are exactly the

$$F(X,Y) = X + Y + a_1 XY + a_2(X^2Y + XY^2)$$

with $a_1, a_2 \in R$ where

$$X^2Y + XY^2 = C_3(X,Y).$$

It is *not* true that each $n+1$-truncated (commutative) formal group is of the form

$$X + Y + a_1 C_2(X,Y) + a_2 C_3(X,Y) + \ldots + a_{n-1} C_n(X,Y)$$

for some $a_1, a_2, \ldots, a_n \in R$. Namely, we leave as an exercise to show that this does not happen for the general 5-truncated formal group law.

We are now heading to Lazard's theorem. Let

$$F = X+Y+\sum_{i,j=1}^{\infty} c_{i,j}X^iY^j \in R[[X,Y]], [a]_F(X) = aX+\sum_{i=2}^{\infty} d_{a,i}X^i \in R[[X]], a \in A,$$

be a collection of power series. Then F is a formal A-module with multiplication by the $[a]_F, a \in A$, if and only if certain equations in the $c_{i,j}, i,j \geq 1, d_{l,a}, l \geq 2$, are satisfied. For example, $c_{i,j} = c_{j,i}$ for $i,j \geq 1$. If

$$I \subseteq A[c_{i,j}, d_{l,a} \mid i,j \geq 1, l \geq 2, a \in A]$$

denotes the ideal generated by these equations, then the ring

$$\Lambda_A := A[c_{i,j}, d_{l,a} \mid i,j \geq 1, l \geq 2, a \in A]/I$$

carries the natural formal A-module group

$$F_{\text{univ}}(X,Y) = X + Y + \sum_{i,j=1}^{\infty} c_{i,j}X^iY^j \in \Lambda[[X,Y]]$$

with multiplication

$$[a]_{F_{\text{univ}}} = aX + \sum_{i=2}^{\infty} d_{l,a}X^i, a \in A,$$

and for any A-algebra R the map

$$\text{Hom}_{(\text{Alg}_A)}(\Lambda_A, R) \to \text{ob}(\text{FGL}_A(R)),\ (f\colon \Lambda \to R) \mapsto f_*F_{\text{univ}}$$

is a bijection, where $\text{ob}(-)$ denotes the objects in a category. In other words, the ring Λ_A (together with F_{univ}) represents the functor of formal A-module laws.

Our aim is the proof of the following fundamental theorem of Lazard, cf. [Laz55, Théoème II] and [Dri74, Proposition 1.4.].

Theorem 2.14 (Lazard, Drinfeld)**.** *There exists an isomorphism* $\Lambda_A \cong A[t_1, t_2, \ldots]$.

Of course, we want to produce a (more or less) explicit isomorphism. The structure of proof for Theorem 2.14 is a bit complicated. Namely, we will simultaneously prove

(1) over $R_n := A[t_1, \ldots, t_{n-2}]$ exists an n-truncated formal A-module, which represents the functor of n-truncated formal A-modules,
(2) each n-truncated formal A-module over an R-algebra can be extended to an $n+1$-truncated formal A-module,
(3) if $K = \text{Frac}(A)$ and R is a K-algebra, then each formal A-module is isomorphic to the additive formal A-module $\widehat{\mathbb{G}}_{a,R}$.

Set

$$R_{n,K} := R_n \otimes_A K \cong K[t_1, \ldots, t_{n-2}]$$

and, if A is a complete discrete valuation ring with finite residue field, fix a uniformizer $\pi \in A$. By Lemma 2.13 we get generators

$$\gamma_{\text{div},n} \in \mathcal{D}_{n,A}(A)$$

corresponding to data $\Gamma_{\text{div},n}(X,Y), h_{\text{div},n}(a), a \in A$, satisfying the equations in Lemma 2.12. A first application of Lemma 2.13 is the following proposition.

Proposition 2.15 ([Laz55, Proposition 3] if $A = \mathbb{Z}$)**.** *There exists sequences*

$$F_n(X,Y) \in R_n[[X,Y]], [a]_{F_n}(X) \in R_n[[X]], n \geq 2,$$

and $\varphi_n(X) \in R_{n,K}[[X]], n \geq 2$, *such that*

1. $F_n(X,Y)$ *mod* $(X,Y)^n$ *is an* n*-truncated formal* A*-module with multiplication by the* $[a]_{F_n}(X), a \in A$,
2. $\varphi_n(F_n(X,Y)) \equiv \varphi_n(X) + \varphi_n(Y)$ *in* $R_{n,K}[[X,Y]]/(X,Y)^n$,
3. $\varphi_n([a]_{F_n}(X)) \equiv a\varphi_n(X)$ *in* $R_{n,K}[[X,Y]]/(X,Y)^n$,
4. $F_{n+1}(X,Y) \equiv F_n(X,Y)$ *mod* $(X,Y)^n$,
5. $\varphi_{n+1}(X) \equiv \varphi_n(X)$ *mod* $(X)^n$,
6. $F_n(X,Y) - t_{n-2}\Gamma_{\mathrm{div},n-1}(X,Y) \in R_{n-1}[[X,Y]]$ *if* $n \geq 3$,
7. $[a]_{F_n}(X) - t_{n-2}h_{\mathrm{div},n-1}(a)X^{n-1} \in R_{n-1}[[X,Y]]$ *if* $n \geq 3$.

The universal formal A-module over $A[t_1, t_2, \ldots]$ will be given by

$$F_{\mathrm{univ}} := \varinjlim_n F_n \in A[t_1, t_2, \ldots][[X,Y]],$$

with multiplication

$$[a]_{F_{\mathrm{univ}}}(X) := \varinjlim_n [a]_{F_n}(X) \in A[t_1, t_2, \ldots][[X,Y]],\ a \in A,$$

and $\varphi := \varinjlim_n \varphi_n$ will define an isomorphism

$$F_{\mathrm{univ}} \hat{\otimes}_A K \cong \widehat{\mathbb{G}}_{a,K[t_1,t_2,\ldots]}$$

of formal A-modules.

Proof. We can set

$$F_2(X,Y) = X + Y, [a]_{F_2}(X) = aX, \varphi_2(X) = X.$$

Thus we may assume that we have constructed $F_n, [a]_{F_n}, a \in A, \varphi_n$ with the desired properties and that they are polynomials of degree $< n$. Set

$$G(X,Y) = \varphi_n^{-1}(\varphi_n(X) + \varphi_n(Y)) \in R_{n,K}[[X,Y]]$$

and

$$[a]_G(X) := \varphi_n^{-1}(a\varphi_n(X)), a \in A,$$

(this makes sense as $\varphi_n(X) = X + \ldots \in R_{n,K}[[X,Y]]$). Then G is a formal A-module in $R_{n,K}[[X,Y]]$ and

$$G(X,Y) \equiv F_n(X,Y) \in R_{n,K}[[X,Y]]/(X,Y)^n.$$

Let

$$\Gamma(X,Y) \in R_{n,K}, h(a)X^n, a \in A,$$

be the degree n-part of $G(X,Y)$ and $[a]_G(X)$, i.e.,

$$G(X,Y) \equiv F_n(X,Y) + \Gamma(X,Y) \in R_{n,K}[[X,Y]]/(X,Y)^{n+1}$$

and

$$[a]_G(X) \equiv [a]_{F_n}(X) + h(a)X^n \in R_{n,K}[[X,Y]]/(X,Y)^{n+1}.$$

As in Lemma 2.12 consider

1. $E_1 := \Gamma(Y,X) + \Gamma(X,Y+Z) - \Gamma(X,Y) - \Gamma(X+Y,Z)$,
2. $E_2 := h(a)(X^n + Y^n) + a^n\Gamma(X,Y) - h(a)(X+Y)^n - a\Gamma(X,Y)$,
3. $E_3 := h(a+b)X^n - h(a)X^n - h(b)X^n - \Gamma(aX,bY)$,
4. $E_4 := h(ab) - ah(b) - h(a)b^n$

for $a, b \in A$. As $G(X,Y)$ is a formal A-module with multiplication by $[a]_G(X)$ and $F_n(X,Y) \in R_n[[X,Y]], [a]_{F_n}(X) \in R_n[[X]], a \in A$, all the polynomials $E_1, \ldots, E_4$ have coefficients in R_n. For example,

$$0 = G(X, G(Y,Z)) - G(G(X,Y), Z)$$

implies that

$$E_1 = F_n(F_n(X,Y), Z) - F_n(X, F_n(Y,Z))$$

has coefficients in R_n, while

$$0 = [a]_G(G(X,Y)) - G([a]_G(X), [a]_G(Y))$$

implies that

$$E_2 = F_n([a]_{F_n}(X), [a]_{F_n}(Y)) - [a]_{F_n}(F_n(X,Y))$$

has coefficients in R_n. As φ_n has only finitely many denominators modulo $(X)^{n+1}$, there exists an $m \in A$ such that $m\Gamma(X,Y), mh(a)X^n, a \in A$, have coefficients in R_n (and not $R_{n,K}$).

This implies that

$$mE_i \in mR_n[[X,Y,Z]],$$

for $i = 1, \ldots, 4$, i.e., that

$$mE_i \equiv 0 \bmod m$$

for $i = 1, \ldots, 4$. Set

$$\Gamma'(X,Y) := m\Gamma(X,Y)$$

and

$$h'(a) := mh(a), a \in A.$$

We can conclude that the mod m residue classes of $\Gamma'(X,Y), h'(a), a \in A$, define an element of

$$\mathcal{D}_{n,A}(R_n/m)$$

as $mE_1 = \ldots mE_4 \equiv 0 \bmod m$. By Lemma 2.13 we find some $r \in R_n$ (unique modulo m), a homogeneous polynomial

$$\Gamma''(X,Y) \in R_n[[X,Y]]$$

of degree n, and

$$h''(a) \in R_n, a \in A,$$

such that

$$\Gamma'(X,Y) = r\Gamma_{\mathrm{div},n}(X,Y) + m\Gamma''(X,Y)$$

and

$$h'(a) = rh_{\mathrm{div},n}(a) + mh''(a), a \in A.$$

Now define

$$F_{n+1}(X,Y) = F_n(X,Y) + \Gamma''(X,Y) + t_{n-1}\Gamma_{\mathrm{div},n}(X,Y) \in R_{n+1}[[X,Y]],$$
$$[a]_{F_{n+1}}(X) = [a]_{F_n} + h''(a)X^n + t_{n-1}h_{\mathrm{div},n}(a)X^n,\ a \in A.$$

We have to find some element $a_n \in R_{n,K}$ such that

$$\varphi_{n+1}(X) = \varphi_n(X) + a_nX^n \in R_{n+1,K}[[X]]$$

satisfies

$$\varphi_{n+1}(F_{n+1}(X,Y)) \equiv \varphi_{n+1}(X) + \varphi_{n+1}(Y) \in R_{n+1,K}[[X]],$$
$$\varphi_{n+1}([a]_{F_{n+1}}(X)) = a\varphi_{n+1}(X),\ a \in A$$

(these equations imply that $F_{n+1}(X,Y)$ is an $n+1$-truncated formal A-module with multiplication by the $[a]_{F_{n+1}},\ a \in A$.). We calculate

$$\begin{aligned}
&\varphi_{n+1}(F_{n+1}(X,Y))\\
\equiv&\varphi_n(F_{n+1}(X,Y)) + a_n(X+Y)^n\\
\equiv&\varphi_n(F_n(X,Y) + \Gamma''(X,Y) + t_{n-1}\Gamma_{\mathrm{div},n}(X,Y)) + a_n(X+Y)^n\\
\equiv&\varphi_n(F_n(X,Y)) + \Gamma''(X,Y) + t_{n-1}\Gamma_{\mathrm{div},n}(X,Y) + a_n(X+Y)^n\\
\equiv&\varphi_n(X) + \varphi_n(Y) - \Gamma(X,Y) + \Gamma''(X,Y) + t_{n-1}\Gamma_{\mathrm{div},n}(X,Y) + a_n(X+Y)^n\\
\equiv&\varphi_n(X) + \varphi_n(Y) - \frac{r}{m}\Gamma_{\mathrm{div},n}(X,Y) + t_{n-1}\Gamma_{\mathrm{div},n}(X,Y) + a_n(X+Y)^n
\end{aligned}$$

in $R_{n+1,K}[[X,Y]]/(X,Y)^{n+1}$, while

$$\begin{aligned}
&\varphi_{n+1}(X) + \varphi_{n+1}(Y)\\
\equiv&\varphi_n(X) + \varphi_n(Y) + a_nX^n + a_nY^n.
\end{aligned}$$

We therefore get the requirement

$$a_n((X+Y)^n - X^n - Y^n) = a_nB_n(X,Y) = (\frac{r}{m} - t_{n-1})\Gamma_{\mathrm{div},n}.$$

Moreover, we calculate

$$\begin{aligned}
&\varphi_{n+1}([a]_{F_{n+1}}(X))\\
\equiv&\varphi_n([a]_{F_{n+1}}) + a_na^nX^n\\
\equiv&\varphi_n([a]_{F_n}(X) + h''(a)X^n + t_{n-1}h_{\mathrm{div},n}(a)X^n) + a_na^nX^n\\
\equiv&\varphi_n([a]_{F_n}(X)) + h''(a)X^n + t_{n-1}h_{\mathrm{div},n}(a)X^n + a_na^nX^n\\
\equiv&a\varphi_n(X) - h(a)X^n + h''(a)X^n + t_{n-1}h_{\mathrm{div},n}(a)X^n + a_na^nX^n\\
\equiv&a\varphi_n(X) - \frac{r}{m}h_{\mathrm{div},n}(a)X^n + t_{n-1}h_{\mathrm{div},n}(a)X^n + a_na^nX^n
\end{aligned}$$

and

$$a\varphi_{n+1}(X) \equiv a\varphi_n(X) + aa_nX^n$$

for $a \in A$. Thus we get the additional equations

$$(a^n - a)a_n = (\frac{r}{m} - t_{n-1})h_{\mathrm{div},n}(a)$$

for $a \in A$. By Lemma 2.13 we see that there exists a unique choice for $a_n \in R_{n,K}$. □

Let us fix sequences $F_n, [a]_{F_n}, a \in A, \varphi_n$ as in Proposition 2.15 (they are not unique as the $r \in R_n$ in the proof of Proposition 2.15 is only unique modulo m). We now check that the $F_n \in R_n[[X,Y]]$ with multiplication $[a]_{F_n}(X), a \in A$, are in fact universal n-truncated formal A-module. By the Yoneda lemma this n-truncated formal A-module defines a natural transformation

$$\eta_n \colon \mathrm{Hom}_{(\mathrm{Alg}_A)}(R_n, -) \to \mathrm{FGL}_{\leq n,A}(-)$$

and Proposition 2.15 implies that the diagram

$$\begin{array}{ccc}
\mathrm{Hom}_{(\mathrm{Alg}_A)}(R_{n+1}, -) & \longrightarrow & \mathrm{Hom}_{(\mathrm{Alg}_A)}(R_n, -)\\
\downarrow{\scriptstyle \eta_n} & & \downarrow{\scriptstyle \eta}\\
\mathrm{FGL}_{\leq n+1,A}(-) & \longrightarrow & \mathrm{FGL}_{\leq n,A}(-)
\end{array}$$

commutes as $F_{n+1} \equiv F_n \bmod (X,Y)^n$, $[a]_{F_{n+1}}(X) \equiv [a]_{F_n}(X) \bmod (X,Y)^n$.

Theorem 2.16 (Lazard's theorem for n-truncated formal A-modules)**.** *For $n \geq 2$ the natural transformation η_n is an isomorphism, i.e, the ring R_n with the n-truncated formal A-module $F_n \in R_n[[X,Y]]/(X,Y)^n$ represents the functor $\mathrm{FGL}_{\leq n,A}(-)$ on A-algebras.*

As was explained before this implies Theorem 2.14.

Proof. The statement is clear for $n = 2$. Hence, we assume the statement for n and deduce the statement for $n+1$. Let S be any A-algebra and

$$G_{n+1}(X,Y) \in S[[X,Y]]/(X,Y)^{n+1}$$

an $n+1$-truncated formal group law, and

$$G_n(X,Y) \in S[[X,Y]]/(X,Y)^n$$

its n-truncation. Let $f_n \colon R_n \to S$ be the unique homomorphism such that

$$f_{n,*}F_n(X,Y) \equiv G_n(X,Y) \bmod (X,Y)^n$$

and

$$f_{n,*}[a]_{F_n}(X) \equiv [a]_G(X,Y) \bmod (X,Y)^n.$$

We can extend

$$f_n \colon R_n = A[t_1, \ldots, t_{n-2}] \to S$$

to a homomorphism

$$f'_n \colon R_{n+1} = A[t_1, \ldots, t_{n-1}] \to S$$

by sending t_{n-1} to 0. Then

$$f'_{n,*}F_{n+1}, G_{n+1}$$

are two lifts of G_n to an $n+1$-truncated formal A-module. By Lemma 2.12 there exists a unique $s \in S$ such that

$$f'_{n,*}F_{n+1}(X,Y) + s\Gamma_{\mathrm{div},n}(X,Y) = G_{n+1}(X,Y) \in S[[X,Y]]/(X,Y)^{n+1}$$

and

$$f'_{n,*}[a]_{F_{n+1}}(X) + sh_{\mathrm{div},n}(a)X^n = [a]_{G_{n+1}}(X) \in S[[X,Y]]/(X,Y)^{n+1}$$

for $a \in A$, where $\Gamma_{\mathrm{div},n}, h_{\mathrm{div},n}$ have the same meaning as in Proposition 2.15. Define

$$f_{n+1} \colon R_{n+1} \to S$$

by sending t_{n-1} to s. Then

$$\begin{aligned} & f_{n+1,*}F_{n+1}(X,Y) \\ \equiv & f_{n+1,*}(F_{n+1}(X,Y) - t_{n-1}\Gamma_{\mathrm{div},n}(X,Y)) + s\Gamma_{\mathrm{div},n}(X,Y) \\ \equiv & f'_n(F_{n+1}(X,Y)) + s\Gamma_{\mathrm{div},n}(X,Y) \\ \equiv & G_{n+1}(X,Y) \end{aligned}$$

using that $F_{n+1} - t_{n-1}C_n(X,Y)$ has coefficients in R_n. Similarly, we get that

$$f_{n+1,*}([a]_{F_{n+1}}(X)) \equiv [a]_{G_{n+1}}(X)$$

for $a \in A$. By Lemma 2.13 we see that this is also our unique choice for f_{n+1}. This finishes the proof. □

Theorem 2.16 implies that *commutative* n-truncated formal group laws can be lifted to formal group laws. This is wrong for non-commutative n-truncated formal group laws. Indeed,

$$F(X,Y) = X + Y + XY^2 \in \mathbb{F}_2[X,Y]/(X,Y)^4$$

is a non-commutative truncated formal group law, which cannot be lifted as any formal group law over $\mathbb{F}_2[[X,Y]]$ is commutative, cf. [Laz55, Théoréme 1].

Unfortunately, the proof of Theorem 2.14 is a bit inexplicit as it does not provide a very concrete formula for a universal (commutative) formal A-module

$$F_{\mathrm{univ}}(X,Y) \in A[t_1, t_2, \ldots][[X,Y]]$$

and its formal multiplication. From Proposition 2.15 and Theorem 2.16 we at least see that we can arrange that

$$F_{\mathrm{univ}}(X,Y) \equiv X + Y + t_{n-1}\Gamma_{\mathrm{div},n}(X,Y) \bmod (t_1, \ldots, t_{n-2}) + (X,Y)^{n+1}$$

and

$$[a]_{F_{\mathrm{univ}}}(X) \equiv X + t_{n-1}h_{\mathrm{div},n}(a)X^n \bmod (t_1, \ldots, t_{n-2}) + (X,Y)^{n+1}.$$

As a concrete example

$$F_{\mathrm{univ}}(X,Y) \equiv X + Y + t_1XY + t_2(X^2Y + XY^2) \bmod (X,Y)^3$$

if $A = \mathbb{Z}$.

Exercise 2.17. We close this section with an exercise on the endomorphisms of the additive formal A-module.

(1) Let $A = \mathbb{Z}$ or a discrete valuation ring with finite residue field, and R a torsion free A-algebra. Show that

$$R \to \mathrm{End}_{\mathrm{FGL}_A(R)}(\widehat{\mathbb{G}}_a),\ r \mapsto rX$$

is an isomorphism.

(2) Let A be a complete discrete valuation ring with finite residue field k of characteristic p and cardinality q, and let R be a k-algebra. Show that

$$R\{\{\tau\}\} \to \mathrm{End}_{\mathrm{FGL}_A(R)}(\widehat{\mathbb{G}}_a),\ \sum_{i=0}^{\infty} r_i\tau^i \mapsto \sum_{i=0}^{\infty} r_i X^{q^i}$$

is an isomorphism, where $R\{\{\tau\}\}$ denotes the non-commutative ring of power series in τ and coefficients in R such that

$$\tau \cdot r = r^q \cdot \tau$$

for $r \in R$.

2.4. **Proof of the lemma of Lazard and Drinfeld.** We now turn to the proof of the crucial, yet technical Lemma 2.13.

Given an A-module M we want to understand the A-module

$$\mathcal{D}_{n,A}(M)$$

given by $\Gamma(X,Y) \in M[X,Y] = M \otimes_A A[X,Y]$ homogeneous of degree n, $h(a) \in M,\ a \in A$, such that the equations

(1) $\Gamma(X,0) = 0$, $\Gamma(0,Y) = 0$,
(2) $\Gamma(Y,Z) + \Gamma(X,Y+Z) = \Gamma(X,Y) + \Gamma(X+Y,Z)$,
(3) $\Gamma(X,Y) = \Gamma(Y,X)$,

(4) $h(a)(X^n + Y^n) + a^n\Gamma(X,Y) = h(a)(X+Y)^n + a\Gamma(X,Y)$,
(5) $h(a+b)X^n = h(a)X^n + h(b)X^n + \Gamma(aX, bX)$,
(6) $h(ab) = ah(b) + h(a)b^n$

are satisfied for $a, b \in A$.

Let

$$\gamma_n \in \mathcal{D}_{n,A}(A)$$

be the collection

$$\{B_n(X,Y), (a^n - a), a \in A\}.$$

If $A = \mathbb{Z}$ Lemma 2.13 reduces to the following statement.

Lemma 2.18. *If $A = \mathbb{Z}$, then for any abelian group M we have*

$$\mathcal{D}_{n,\mathbb{Z}}(M) = \gamma_{\mathrm{div},n} \cdot M$$

for $\gamma_{\mathrm{div},n}$ given by the collection $\{C_n(X,Y), \frac{(a^n-a)}{d_n}, a \in A\}$.

Here,

$$C_n(X,Y) = \frac{1}{d_n} B_n(X,Y)$$

with $d_n = 1$ if n is not a prime power and p if $n = p^h$ for some prime p as in Section 2.3.

Before proving Lemma 2.18 let us deduce Lemma 2.13 from Lemma 2.18.

Lemma 2.19. *Let A be a complete discrete valuation ring with finite residue field k having q-elements. Let $K := \mathrm{Frac}(A)$ be the fraction field of A. Assuming Lemma 2.18 the second statement of Lemma 2.13 holds true.*

Proof. We first prove the existence of $\gamma_{\mathrm{div},n} \in \mathcal{D}_{n,A}(A)$ if n is a power of q. Let $p := \mathrm{char}(k)$. Then

$$B_n(X,Y) = pC_n(X,Y)$$

and $\pi \mid p$. Moreover, $\mathrm{Frob}_q \colon k \to k$ is the identity, which implies that

$$\pi \mid (a^n - a)$$

for all $a \in A$ as n is a power of q. Now, let M be an A-module and $\{\Gamma(X,Y), h(a), a \in A\}$ an element in $\mathcal{D}_{n,A}(M)$. We know that

$$(a^n - a)\Gamma(X,Y) = h(a)B_n(X,Y)$$

by equation (4). If n is not a power of p, then by Lemma 2.18 we know

$$\Gamma(X,Y) = B_n(X,Y)m$$

for a unique $m \in M$ as d_n is invertible in A in this case. Therefore we get

$$(a^n - a)m = h(a)$$

as desired. Next assume that n is a power of p, but not of q. Then there exists $a \in A$ such that

$$a^n - a \notin (\pi).$$

Set

$$m := \frac{1}{(a^n - a)} h(a) \in M.$$

Then for each $b \in A$

$$ah(b) + b^n h(a) = h(ab) = h(ba) = bh(a) + a^n h(b),$$

which implies

$$h(b) = (b^n - b)\frac{h(a)}{(a^n - a)} = (b^n - b)m$$

for each $b \in B$. Moreover,

$$\Gamma(X, Y) = B_n(X, Y)m$$

as we saw above. Finally, assume that n is a power of q. Set

$$m := \frac{h(\pi)}{\pi^{n-1} - 1}.$$

Substracting

$$m \cdot \gamma_{\mathrm{div},n}$$

from the data $\{\Gamma(X, Y), h(a), a \in A\}$ reduces us to the case that $h(\pi) = 0$. We have to show that $\Gamma(X, Y) = 0$ and $h(a) = 0$ for $a \in A$. We then know that

$$\pi h(b) = (b^n - b)\frac{h(\pi)}{(\pi^{n-1} - 1)} = 0$$

for $b \in B$. This implies

$$h(\pi b) = 0$$

for $b \in B$. In particular, $h(p) = 0$ as $\pi | p$. By Lemma 2.18, i.e., the case $A = \mathbb{Z}$, we know that

$$\Gamma(X, Y) = C_n(X, Y)m'$$

for a unique $m' \in M$ and that

$$h(p) = (p^{n-1} - 1)m'.$$

As $p^{n-1} - 1$ is a unit in A we can conclude that $m' = 0$. We know $\pi h(a) = 0$ for all $a \in A$ thus

$$b^n h(a) = bh(a)$$

for all $b \in A$ as n is a power of q. In particular, h defines a derivation $A \to M$ with image in the π-torsion $M[\pi]$ of M. Because $h(\pi b) = 0$ for all $b \in B$, this derivation factors over a derivation

$$\overline{h} \colon k \to M[\pi].$$

Any such derivation is trivial as k is a perfect field. Indeed, each $x \in k$ admits a p-th root y and

$$\overline{h}(x) = py^{p-1}\overline{h}(y) = 0.$$

This finishes the proof. □

Thus, we have reduced to the case that $A = \mathbb{Z}$. Let us show that in this case only the equations $1), 2), 3)$ are relevant. Let M be an abelian group and let $\Gamma(X, Y), h(a), a \in A$, be an element of $\mathcal{D}_{n,\mathbb{Z}}(M)$. If we write

$$\Gamma(X, Y) = \sum_{0<i<n} m_i X^i Y^{n-i},$$

then the first three imposed relations reduce to

$$m_i = m_{n-i}, 0 < i < n,$$

and

$$\binom{j+k}{j} m_i = \binom{i+j}{j} m_{i+j}$$

for $0 < i, j, k < n, i + j + k = n$. The forth relation becomes

$$(a^n - a)m_i = h(a)\binom{n}{i}$$

for $0 < i < n$ while the fifth relation becomes

$$h(a + b) = h(a) + h(b) + \sum_{0<i<n} m_i a^i b^{n-i}.$$

Assume now that

$$\Gamma(X, Y) = mC_n(X, Y) = \sum_{0<n<n} m\frac{1}{d_n}\binom{n}{i}X^i Y^{n-1}$$

for some necessarily unique $m \in M$. Then we get by induction

$$h(a) = \frac{1}{d_n}(a^n - a)m.$$

Indeed, $h(1) = 0$ and

$$\begin{aligned} &h(a+1)\\ =&h(a) + \sum_{0<i<n} m\frac{1}{d_n}\binom{n}{i}a^i\\ =&\frac{1}{d_n}(a^n - a)m + m(\frac{1}{d_n}((a+1)^n - a^n - 1)\\ =&\frac{1}{d_n}((a+1)^n - a - 1)m \end{aligned}$$

using induction on a. Similarly, one checks the statement for $a < 0$ using downward induction starting with the case $a = 0$. In particular, Lemma 2.18 follows from Lemma 2.20

Lemma 2.20 (Lucas' theorem)**.** *Let M be an abelian group and let $m_{i,j} \in M, 0 \leq i, j \leq n, i + j = n$, satisfying*

$$m_{n,0} = m_{0,n} = 0, m_{i,j} = m_{j,i}$$

for all $0 \leq i, j \leq n$, and

$$\binom{i+j}{j}m_{i+j,k} = \binom{j+k}{j}m_{i,j+k}$$

for all $0 < i, j, k < n$. Then there exists a unique $m \in M$, such that

$$m_i := m_{i,n-i} = \frac{1}{d_n}\binom{n}{i}m$$

for $0 < i < n$.

For the proof we follow [Lur10, Lecture 3].

Proof of Lemma 2.20. Uniqueness follows from the fact that the greatest common divisor of the coefficients of $C_n(X, Y)$ is 1, cf. Lemma 2.21. We can assume that M is finitely generated by considering the subgroup generated by the $m_{i,j}, 0 \leq i, j \leq n$. Then M is isomorphic to the kernel of the map

$$M \oplus_{\mathbb{Z}} \mathbb{Q} \oplus \prod_p M \otimes_{\mathbb{Z}} \mathbb{Z}_p \to M \otimes_{\mathbb{Z}} \mathbb{Q}_p,\ (a, b) \mapsto a - b,$$

where the product runs over all primes p and we identified

$$(M \otimes_{\mathbb{Z}} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong M \otimes_{\mathbb{Z}} \mathbb{Q}_p \cong (M \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

By uniqueness of M we may therefore replace M by $M \otimes_{\mathbb{Z}} \mathbb{Z}_p$ or $M \otimes_{\mathbb{Z}} \mathbb{Q}$ and assume that M is a $\mathbb{Z}_{(p)}$-module for some prime p. The assumption on the collection $\{m_i\}_{0 \leq i \leq n}$ implies that if $m_i = 0$ for some $0 < i < n$ and $k = i + j < n$ satisfies

$$\binom{k}{i} \not\equiv 0 \bmod p,$$

then $m_k = 0$. Indeed, $\binom{k}{i}$ is a unit in $\mathbb{Z}_{(p)}$ in this case. By Lemma 2.21 $\binom{i+j}{j} \not\equiv 0 \bmod p$ if in p-adic expansion the sum $i + j$ can be calculated without carrying, i.e., the p-adic digits in $i + j$ are larger than the p-adic digits of i (or j) First let us assume that $n = p^h$ for some $h \geq 1$. Lemma 2.21 implies that

$$\frac{1}{p}\binom{p^h}{p^{h-1}} \not\equiv 0 \bmod p.$$

Hence replacing $m_{i,j}$ by $m_{i,j} + a\frac{1}{p}\binom{n}{i} m_{p^{(h-1)}}$ for a suitable $a \in \mathbb{Z}_{(p)}$ we may assume that $m_{p^{h-1}} = 0$. Let

$$p^{h-1} \leq k < p^h.$$

By Lemma 2.21

$$\binom{k}{p^{h-1}} \not\equiv 0 \bmod p$$

as the sum $k = p^{h-1} + (k - p^{h-1})$ is computed without carrying in the p-adic expansion (as $k < (p-1)p^{h-1}$) and $k \geq p^{h-1}$. As we saw above this yields $m_k = 0$. If $0 < k < p^{h-1}$, then

$$m_k = m_{p^h - k} = 0$$

as $p^{h-1} \leq p^h - k < p^h$. This finishes the proof in the case that $n = p^h$ is a power of p. Next assume that n is not a power of p and write $n = p^h n'$ with $n' > 1$ and $p \nmid n'$. By Lemma 2.21 we know that

$$\binom{n}{p^h} \not\equiv 0 \bmod p.$$

As above we may then assume that $m_{p^h} = 0$. If $h \geq 1$, then $m_{n-p^h} = 0$ by symmetry. By Lemma 2.21

$$\binom{n - p^{h-1}}{(p-1)p^{h-1}} \not\equiv 0 \bmod p$$

as $n - p^{h-1} = n - p^h + (p-1)p^{h-1}$ can be calculated in its p-adic expansion without carrying. From the remark made at the beginning of the proof we get that

$$m_{n-p^{h-1}} = 0,$$

from which we deduce that $m_{p^{h-1}} = m_{p^h} = 0$ if $h \geq 1$. Now let $0 < i, j < n$ with $i + j = n$. We need to see that $m_i = 0$ or by symmetry equivalently $m_j = 0$. By assumption we have

$$n = a_h p^h + \sum_{i=h+1}^{\infty} a_i p^i$$

in p-adic expansion with $0 < a_h < p$. Either i or j must have a non-trivial p-adic digit in front of p^{h-1} (only possible if $h \geq 1$) or p^h. Assume this is the case for i and the coefficient in front of p^h. By Lemma 2.21 we can conclude that

$$\binom{i}{p^h} \not\equiv 0 \bmod p$$

and thus $m_i = 0$ because $m_{p^h} = 0$ and the remark made at the beginning of the proof. If the p-adic digit in front of p^{h-1} (if $h \geq 1$) of i is non-zero, then similarly

$$\binom{i}{p^{h-1}} \not\equiv \bmod$$

and thus $m_i = 0$ using $m_{p^{h-1}} = 0$. This finishes the proof. □

Lemma 2.21. *Let p be a prime. Let $a = \sum_{i=0}^{\infty} a_i p^i, b = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_{\geq 0}$ be two natural numbers in their p-adic expansion, i.e., $a_i, b_i \in \{0, \ldots, p-1\}$. Then*

$$\binom{a}{b} \equiv \prod_{i=0}^{\infty} \binom{a_i}{b_i} \text{ mod } p.$$

Moreover, for $h \geq 1$ and we have $\frac{1}{p}\binom{p^h}{p^{h-1}} \not\equiv 0$ mod p.

Here, $\binom{a}{b} = 0$ if $b > a$ and $\binom{0}{0} = 1$. Lemma 2.21 can be used to give a proof that

$$d_n = \begin{cases} 1, \text{ if } n \text{ is not a prime power} \\ p, \text{if } n \text{ is a power of the prime } p. \end{cases}$$

Namely, if n is not a power of p, then write $n = \sum_{i=0}^{h} a_i p^i$ with $a_h \neq 0$, and set $i := a_h p^h, j := n - i > 0$. Lemma 2.21 implies that $\binom{n}{i}$ is not divisible by p.

Proof. Consider the set

$$S = \coprod_{k=1}^{a_0} \mathbb{Z}/p^0 \sqcup \coprod_{k=1}^{a_1} \mathbb{Z}/p^1 \sqcup \coprod_{i=1}^{a_2} \mathbb{Z}/p^2 \sqcup \ldots \tag{9}$$

of cardinality a with its evident action of the group

$$G := \prod_{i=0}^{\infty} (\mathbb{Z}/p^i)^{a_i}.$$

Let T be the set of subsets of S of cardinality b. Then $\sharp T = \binom{a}{b}$ and G acts on T. As G is a p-group

$$\sharp T \equiv \sharp T^G \bmod p,$$

where T^G is the fixed point set of G. But a b-element subset $S' \subseteq S$ is fixed under G if and only if it is a union of G-orbit. From ((9)) we can conclude that there are

$$\prod_{i=0}^{\infty} \binom{a_i}{b_i}$$

possible choices for choosing orbits, such that their union has b-elements. This proves the first assertion. Let us prove that

$$\frac{1}{p}\binom{p^h}{p^{h-1}} \not\equiv 0 \bmod p.$$

This is clear if $h = 1$ as then $\binom{p}{1} = p$. For $h \geq 2$ note that

$$(X+Y)^{p^{h-1}} \equiv X^{p^{h-1}} + Y^{p^{h-1}} \bmod p,$$

which implies

$$(X+Y)^{p^h} \equiv (X^{p^{h-1}} + Y^{p^{h-1}})^p \bmod p^2$$

as the p-th power map is p-adically contracting. From here we can conclude

$$C_{p^h}(X,Y) \equiv C_p(X^{p^{h-1}}, Y^{p^{h-1}}) = (C_p(X,Y))^{p^{h-1}} \not\equiv 0 \bmod p$$

and by looking at the coefficient of $X^{p^{h-1}}Y^{(p-1)p^{h-1}} = (XY^{p-1})^{p^{h-1}}$

$$\frac{1}{p}\binom{p^h}{p^{h-1}} \equiv \frac{1}{p}\binom{p}{1} \not\equiv 0 \bmod p.$$

This finishes the proof. □

2.5. **Consequences for formal A-modules.** We let again A denote $\mathbb{Z}$ or a discrete valuation ring with finite residue field (in which case we fix a uniformizer π).

For $n \geq 2$ let

$$\gamma_n, \gamma_{\mathrm{div},n} \in \mathcal{D}_{n,A}(A)$$

denote the elements from Lemma 2.13 with corresponding data

$$\{B_n(X,Y), (a^n - a), a \in A\}, \{\Gamma_{\mathrm{div},n}(X,Y), h_{\mathrm{div},n}(a), a \in A\}$$

satisfying the equations in Lemma 2.12. In the following we fix an A-algebra R.

Most of the following results rest on the following lemma, cf. [Vla76, Propositon 1.5.].

Lemma 2.22. *Let $F \in R[[X,Y]]/(X,Y)^{n+1}$ be an $n+1$-truncated formal A-module, let $r \in R$ and let*

$$\varphi_n(X) := X + rX^n \in R[[X]]/(X)^{n+1}.$$

Then

$$\varphi_n^{-1}(F(\varphi_n(X), \varphi_n(Y))) \equiv F(X,Y) - rB_n(X,Y) \ \mathit{mod}\ (X,Y)^{n+1}$$

and

$$\varphi_n^{-1}([a]_F(\varphi_n(X)) \equiv [a]_F(X) - r(a^n - a)X^n \ \mathit{mod}\ (X,Y)^{n+1}$$

for $a \in A$.

Here, $\varphi_n^{-1}(X) \in R[[X]]/(X)^{n+1}$ denotes the inverse R-algebra morphism to

$$X \mapsto \varphi_n(X).$$

In other words, Lemma 2.22 explains how we can change truncated formal A-modules by changing the coordinate, namely exactly by some multiple of γ_n.

Proof. We calculate

$$\begin{aligned} &F(\varphi_n(X), \varphi_n(Y)) \\ \equiv &F(X + rX^n, Y + rY^n) \\ \equiv &F(X,Y) + rX^n + rY^n \end{aligned}$$

and

$$\begin{aligned}&\varphi_n(F(X,Y)-rB_n(X,Y))\\ \equiv&\varphi_n(F(X,Y))-rB_n(X,Y)\\ \equiv&F(X,Y)+r(X+Y)^n-rB_n(X,Y)\\ \equiv&F(X,Y)+rX^n+rY^n.\end{aligned}$$

If $a \in A$ we get

$$\begin{aligned}&[a]_F(\varphi_n(X))\\ \equiv&[a]_F(X)+arX^n\end{aligned}$$

and

$$\begin{aligned}&\varphi_n([a]_F(X)-r(a^n-a)X^n)\\ \equiv&\varphi_n([a]_F(X))-r(a^n-a)X^n\\ \equiv&[a]_F(X)+ra^nX^n-r(a^n-a)X^n\\ \equiv&[a]_F(X)+raX^n.\end{aligned}$$

This finishes the proof. □

Let K be the fraction field of A.

Lemma 2.23. *Assume that R is a K-algebra, and $F \in R[[X,Y]]$ a formal A-module. Then there exists a unique power series $\log_F \in R[[X]]$ with $\log_F(0) = 0, \log_F'(0) = 1$ and*

$$\log_F(F(X,Y)) = \log_F(X) + \log_F(Y)$$

and

$$\log_F([a]_F(X)) = a\log_F(X)$$

for a. Moreover,

$$\mathrm{End}_{\mathrm{FGL}_A(R)}(\widehat{\mathbb{G}}_a) \cong R,\ g(X) \mapsto g'(0)$$

In other words, if R is a K-algebra, then each formal A-module over R is isomorphic to the additive one.

Proof. By Exercise 2.17

$$\mathrm{End}_{\mathrm{FGL}_A(R)}(\widehat{\mathbb{G}}_a) \cong R,\ g(X) \mapsto g'(0)$$

which implies uniqueness of $\log_F$. The existence of $\log_F$ for the universal formal A-module was implicitly proven in Proposition 2.15. Alternatively, it follows from Lemma 2.22. Namely, as R is a K-algebra γ_n generates $\mathcal{D}_{n,A}(R)$ by Lemma 2.13. By Lemma 2.22 we see that we can iteratively find an isomorphism $F \cong \widehat{\mathbb{G}}_a$. □

Let us now fix a prime p, and assume that R is $\mathbb{Z}_{(p)}$-algebra. We may then replace A by $A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ if we consider formal A-modules over R. Hence, assume from now on that A is a (not necessarily complete) discrete valuation ring with finite residue field k of characteristic p and cardinality q. In this case we will analyze a formal A-module by analyzing its endomorphism $[\pi]$ for $\pi \in A$ a fixed uniformizer.

Recall that in Section 2.1 we introduced the height of a formal A-module over a field extension k' of k. Namely, $F \in k'[[X,Y]]$ is of height h if and only if

$$[\pi]_F(X) \equiv aX^{q^h} \bmod (X)^{q^h+1}$$

with $a \in k'^{,\times}$.

Let

$$F_{\mathrm{univ}}(X,Y) \in \Lambda_A[[X,Y]] \cong A[t_1,t_2,\ldots][[X,Y]]$$

be a universal formal group law as constructed via Proposition 2.15. Then we know that for $h \geq 1$

$$[\pi]_F(X) \equiv t_{q^h-1}(\pi^{q^h-1}-1)X^{q^h} \bmod (\pi, t_1, \ldots, t_{q^h-2}) + (X,Y)^{q^h+1}$$

because $h_{\mathrm{div},q^h}(\pi) = \pi^{q^h-1}-1$. Set

$$v_0 := \pi$$

and

$$v_i := (\pi^{q^i-1}-1)t_{q^i-1}$$

for $i \geq 1$. Note that

$$\Lambda_A \cong A[t_0, t_1, \ldots, t_{q-2}, v_1, t_q, \ldots, t_{q^i-2}, v_i, t_{q^i}, \ldots]$$

as $\pi^{q^i-1}-1 \in A^\times$ for $i \geq 1$.

Now we generalize the notion of a height to an arbitrary A-algebra R.

Definition 2.24. *Let $h \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$. Let $F \in R[[X,Y]]$ be a formal A-module. Then F is called of height $\geq h$ (resp. height h) if*

$$[\pi]_F(X) \equiv 0 \ \mathit{mod}\ (X^{q^h})$$

(resp.

$$[\pi]_F(X) \equiv rX^{q^h} \ \mathit{mod}\ (X)^{q^h+1}$$

with $r \in R^\times$).

A formal A-module over R is of height 0 if and only if R is a K-algebra. Equivalently, F is of height ≥ 1 if and only of $\pi R = 0$, i.e., R is a k-algebra. If F is of height 0, then by Lemma 2.23

$$F \cong \widehat{\mathbb{G}}_{a,R}.$$

Clearly, the formal A-module $F_h \in k[[X,Y]]$ constructed in Lemma 2.4 is of height $h \geq 1$. If R is a k-algebra, then the formal A-module

$$\widehat{\mathbb{G}}_{a,R}$$

is of height ∞.

The following lemma implies that Definition 2.24 is invariant under isomorphisms of formal A-modules and that it does not depend on the choice of F_{univ}.

Lemma 2.25. *Let R be a k-algebra, $F \in R[[X,Y]]$ a formal A-module and $1 \leq h < \infty$. Then the following are equivalent:*

1. *F is of height $\geq h$,*
2. *$[\pi]_F$ factors over $\mathrm{Frob}_q^h \colon F^{(q^h)} \to F$, cf. Section 2.1,*
3. *F is isomorphic to a formal A-module F' such that $[\pi]_{F'}(X) = 0 \ \mathit{mod}\ (X)^{q^h+1}$,*
4. *if $F = f_*F_{\mathrm{univ}}$ for $f \colon \Lambda_A \to R$, then $f(v_i) = 0$ for $i < h$,*
5. *F is isomorphic to $\widehat{\mathbb{G}}_a$ modulo $(X,Y)^{q^h}$, i.e., there exists $\varphi \in X + X^2R[[X]]$ with $\varphi'(0) \in R^\times$ such that*

$$\varphi(F(X,Y)) \equiv \varphi(X) + \varphi(Y) \ \mathit{mod}\ (X,Y)^{q^h},$$

and

$$\varphi([a]_F(X)) \equiv a\varphi(X) \ \mathit{mod}\ (X)^{q^h}$$

In particular, F is of height ∞ if and only if $[\pi]_F(X) = 0$ if and only if $F \cong \widehat{\mathbb{G}}_{a,R}$.

Proof. 1) $\Rightarrow$ 2) follows from the proof of Lemma 2.2. 2) $\Rightarrow$ 1) is clear as Frob_q^h is represented by the series X^{q^h}. As 2) is invariant under isomorphisms we see that 3) is equivalent to 1). Alternatively, we could argue that substituting X by some power series $\varphi(X)$ with $\varphi(0) = 0, \varphi'(0)$ preserves the ideal $(X)^{q^h}$. From the argument for 1) $\Rightarrow$ 2) we see that if $[\pi]_F(X) = 0 \bmod X^n$, then $[\pi]_F(X) = 0 \bmod (X)^{q^{i+1}}$ if $q^i \leq n < q^{i+1}$. Moreover, if $[\pi]_F(X) = 0 \bmod (X^{q^i})$, then we can conclude that $[\pi]_F(X) \equiv v_i X^{q^i} \bmod (X)^{q^i+1}$. This implies that 4) is equivalent to 1). As

$$[\pi]_{\hat{\mathbb{G}}_a}(X) = \pi \cdot X = 0$$

we see that 5) $\Rightarrow$ 3). Thus assume that F is of height $\geq h$. We may argue via induction on $m < q^h$ that we find $\varphi(X) \in X + X^2 R[[X]]$ with

$$\varphi(F(X,Y)) \equiv \varphi(X) + \varphi(Y) \bmod (X,Y)^m$$

and similarly for the formal multiplication. The case $m = 2$ is clear and we may assume that

$$F(X,Y) \equiv X + Y \bmod (X,Y)^m.$$

By Lemma 2.12 and Lemma 2.13 we know that

$$F(X,Y) \equiv X + Y \equiv r\Gamma_{\mathrm{div},m}(X,Y) \bmod (X,Y)^{m+1}$$

and

$$[a]_F(X) \equiv aX + r h_{\mathrm{div},n}(a) X^m \bmod (X)^{m+1}$$

for $a \in A$. If m is not a power of q, then by Lemma 2.22 we may take

$$\varphi(X) = X - rX^m.$$

If $m = q^i$ with $i < h$, then we know that

$$[\pi]_F(X) \equiv v_i X^{q^i} \equiv r(\pi^{q^i-1} - 1) X^{q^i} \equiv rX^{q^i} \bmod (X)^{m+1}.$$

As $v_i = 0$ this implies that $r = 0$ and automatically.

$$F(X,Y) \equiv X + Y \bmod (X,Y)^{m+1}.$$

This finishes the proof. □

Recall that in Exercise 2.17 we computed the endomorphisms $\widehat{\mathbb{G}}_a$ over some k-algebra R. Thereby the infinite height case is completely understood.

If A is of characteristic p and R any A-algebra, then Lemma 2.25 implies that the underlying formal group law of each formal A-module $F \in R[[X,Y]]$ is isomorphic to $\widehat{\mathbb{G}}_a$. Indeed, as

$$[p]_F(X) = 0$$

as $p = 0 \in A$, the underlying formal $\mathbb{Z}_{(p)}$-module is of height ∞. This does of course not imply that the formal A-module F is of height ∞.

Recall that we constructed for $h \in \mathbb{Z}_{\geq 1}$ in Lemma 2.4 a formal A-module $F_h \in k[[X,Y]]$ of height h such that

$$[\pi]_{F_h}(X) = X^{q^h} \in k[[X,Y]].$$

It is nearly true that each formal A-module over a k-algebra R of height h is isomorphic to F_h. It is true after passing to a faithfully flat ind-finite étale R-algebra. Let us give the relevant definitions.

Definition 2.26. *Let $f\colon R \to S$ be a map of arbitrary rings. Then f is called finite étale if S is a finite projective R-module and the trace bilinear form*

$$\mathrm{Tr}_{S/R}\colon S \times S \to R,$$

which exists by finite projectivity of S over R, is non-degenerate, i.e., its adjoint $S \to \mathrm{Hom}_R(S, R)$ is an isomorphism. We call f ind-finite étale if $S = \varinjlim_i S_i$ is a filtered colimit of R-algebras S_i, which are finite étale over R. We call f flat if f is S is a flat R-module, and faithfully flat if f is flat and $S \otimes_R M = 0$ implies $M = 0$ for any R-module M.

Let us give examples of (ind-)finite étale morphisms.

Example 2.27. (1) Let R be any ring and assume that $f(X) \in R[X]$ is a monic polynomial with derivative $f'(X) \in R[X]$ such that

$$(f(X), f'(X)) = R[X].$$

Then

$$S := R[X]/(f(X))$$

is a finite étale R-algebra. Indeed, S is finite free over R and we have to see that the adjoint of the trace bilinear form

$$S \to \mathrm{Hom}_R(S, R)$$

is an isomorphism. This amounts to checking that the determinant of a matrix is invertible. But this can be checked after base change to fields, and then to algebraiclly closed fields. Thus we may assume that $L = R$ is an algebraically closed field. In this case the condition $(f(X), f'(X))$ means that the polynomial $f(X)$ is multiplicity free. This implies that S is a finite product of copies of L. But then the trace bilinear form is clearly non-degenerate.

(2) By base change to an algebraically closed extension it is easy to see that if $R = L$ is a field, then a commutative finite dimensional L-algebra S is finite étale if and only if it is a product of separable field extensions. In particular, if L is separably closed, then each (non-zero) finite étale L-algebra S admits a retraction $S \to L$ as L-algebras.

Let us say that a formal A-module $F \in R[[X, Y]]$ of height $h \in \mathbb{Z}_{\geq 1}$ over a k-algebra R is normalized if

$$[\pi]_F(X) = X^{q^h}.$$

As $F([\pi]_F(X), [\pi]_F(Y)) = [\pi]_F(F(X, Y))$ and $[\pi]_F([a]_F(X)) = [a]_F([\pi]_F(X))$ for $a \in A$, it follows that a normalized formal A-module and its formal multiplication have coefficients in the subring

$$R^{\mathrm{Frob}_{q^h}=\mathrm{Id}} := \{x \in R \mid x^{q^h} = x\} \subseteq R.$$

For example, the module $F_h \in k[[X, Y]]$ from Lemma 2.4 is normalized. More generally, we have the following.

Lemma 2.28. *Let R be a k-algebra, $h \in \mathbb{Z}_{\geq 1}$ and $F \in R[[X, Y]]$ a formal A-module of height h. Then there exists a faithfully flat ind-finite étale R-algebra S such that $F \hat{\otimes}_R S$ is isomorphic to a normalized formal A-module $F' \in S[[X, Y]]$.*

Proof. By Lemma 2.25 we can assume that

$$F(X,Y) \equiv \widehat{\mathbb{G}}_a \bmod (X,Y)^{q^h}.$$

By assumption

$$[\pi]_F(X) \equiv aX^{q^h} \bmod (X)^{q^h+1}$$

with $a \in R^\times$. As $q^h = 0$ in R and $a \in R^\times$ the R-algebra

$$S := R[T]/(T^{q^h-1} - a)$$

is finite étale over R by Example 2.27. After replacing R by S we may therefore assume that there exists $b \in R$ with $b^{q^h-1} = a$. Set

$$\varphi(X) = b^{-1}X.$$

Then

$$\varphi^{-1}([\pi]_F(\varphi(X))) \equiv X^{q^h} \bmod (X)^{q^h+1}$$

and we may replace F by $\varphi^{-1}(F(\varphi(X),\varphi(Y)))$ and assume that

$$[\pi]_F(X) \equiv X^{q^h} \bmod (X)^{q^h+1}.$$

Let $m \geq q^h$. By induction we may assume that

$$[\pi]_F(X) \equiv X^{q^h} \bmod (X)^m.$$

By Lemma 2.2 we know that $[\pi]_F(X) = g(X^{q^h})$ for some power series g. Hence, we only have to deal with $m = kq^h$ with $k \geq 2$. In this case write

$$[\pi]_F(X) \equiv X^{q^h} + aX^{kq^h} \bmod (X)^{m+1}.$$

If we set

$$\varphi(X) = X - bX^k,$$

then

$$\begin{aligned}
&\varphi([\pi]_F(\varphi^{-1}(X)))\\
\equiv&[\pi]_F(\varphi^{-1}(X)) - bX^{kq^h}\\
\equiv&X^{kq^h} + b^{q^h}X^{kq^h} + aX^{kq^h} - bX^{kq^h}\\
\equiv&X^{kq^h} + (b^{q^h} - b + a)X^{kq^h}
\end{aligned}$$

mod $(X)^{kq^h+1}$ as

$$\varphi^{-1}(X) = X + bX^k \bmod X^{k+1}.$$

The R-algebra $S := R[X]/(X^{q^h} - X + a + 1)$ is finite étale over R. Hence, we may enlarge R an assume that there exists $b \in R$ with

$$b^{q^h} - b + a + 1 = 0.$$

This concludes the proof. □

We can now prove a generalization of the previously announced Theorem 2.5.

Theorem 2.29. *Let $h \in \mathbb{Z}_{\geq 1}$ and R a k-algebra. Any two normalized formal A-modules $F_1, F_2 \in R[[X,Y]]$ of height h are isomorphic. In particular, any two formal A-modules of height h become isomorphic over a faithfully flat ind-finite étale R-algebra, and if $R = k'$ is a separably closed field extension of k, then two formal A-modules are isomorphic if and only if they have the same height.*

Proof. This follows from Lemma 2.22, Lemma 2.28 and the fact that every faithfully flat ind-finite étale algebra S over some separably closed field k' admits a retraction $S \to k'$. Namely, we may assume that

$$R^{\mathrm{Frob}_{q^h}=\mathrm{Id}} = R,$$

which implies that for $\varphi(X) \in X \cdot R[[X]]$ with $\varphi'(0) \in R^\times$, the R-algebra automorphism

$$\varphi\colon R[[X]] \to R[[X]],\ X \mapsto \varphi(X)$$

transforms normalized formal A-modules to normalized A-modules. Using the usual arguments the crucial point is to see that if F_1, F_2 are normalized formal A-modules of height h and

$$F_1(X,Y) \equiv F_2(X,Y) \bmod (X,Y)^m$$

for some power $m = q^i, i \geq 0$, of q, then

$$F_1(X,Y) \equiv F_2(X,Y) \bmod (X,Y)^{m+1}.$$

We know that

$$[\pi]_{F_2}(X) \equiv [\pi]_{F_1}(X) + aX^m \bmod (X)^{m+1}$$

for some $a \in R$. As F_1, F_2 are normalized we get $a = 0$ because $h_{\mathrm{div},m}(\pi) = 1 - \pi^{m-1}$ is a unit in R. □

Lemma 2.25 and Lemma 2.13 imply that there exists a normalized formal A-module $F_h \in k[[X,Y]]$ of height $h \in \mathbb{Z}_{\geq 1}$ with

$$F_h(X,Y) \equiv X + Y - \frac{p}{\pi} C_{q^h}(X,Y) \bmod (X,Y)^{q^h+1}$$

and

$$[a]_{F_h}(X) \equiv aX - \frac{a^{q^h} - a}{\pi} X^{q^h} \bmod (X,Y)^{q^h+1}.$$

We shortly discuss another structure of the Lazard ring, namely its grading.

Let

$$\mathbb{G}_m\colon (\mathrm{Alg}_A) \to (\mathrm{Grp}),\ R \mapsto R^\times.$$

be the multiplicative group over A. Then $\mathbb{G}_m$ acts on the functor

$$\mathrm{FGL}_A(-).$$

Indeed, given $R \in \mathrm{Alg}_A$ and a formal A-module $F \in R[[X,Y]], [a]_F(X) \in R[[X]], a \in A$, then

$$r.F(X,Y) := r^{-1}F(rX, rY), [a]_{r.F}(X) := r^{-1}[a]_F(rX), a \in A,$$

is another formal A-module.[9] If F is classified by the map

$$g_F\colon \Lambda_A \cong A[t_1, t_2, \ldots] \to R,$$

then by Proposition 2.15 and the proof of Lazard's theorem we see that

$$g_{r.F}(t_i) = r^i g_F(t_i)$$

as

$$r^{-1}t_i\Gamma_{\mathrm{div},i+1}(rX, rY) = r^i t_i \Gamma_{\mathrm{div},i+1}, r^{-1}t_i h_{\mathrm{div},i+1}(a) r^{i+1} X^{i+1} = r^i h_{\mathrm{div},i+1}(a) X^i.$$

for $i \geq 1, a \in A$. In other words,

$$\Lambda_A \cong A[t_1, t_2, \ldots]$$

[9]This is a special case of the action of the group G, which was discussed after Exercise 2.1

as graded rings if t_i has degree i (and Λ_A its graduation coming from the $\mathbb{G}_m$-action on FGL_A).

To complete the discussion of formal A-modules of height $h \in \mathbb{Z}_{\geq 1}$ we have to calculate the endomorphism

$$\mathrm{End}_{\mathrm{FGL}_{A(R)}}(F)$$

for such a formal A-module F. For this we may assume that A is complete. By Theorem 2.29 it suffices to consider the case that F is normalized and describe

$$\mathrm{End}_{\mathrm{FGL}_{A(R)}}(F).$$

The general case will be given by twists with a torsor under the functor of units in $\mathrm{End}_{\mathrm{FGL}_{A(R)}}(F)$. As F is assumed to be normalized each endomorphism of F over R is already defined over the subring

$$R^{\mathrm{Frob}_{q^h}=\mathrm{Id}} \subseteq R.$$

Let us discuss the structure of this subring. For $a \geq 1$ we let k_a/k be an extension of degree a over k (which is unique up to isomorphism).

Exercise 2.30. If R is a k-algebra of finite type, then $R^{\mathrm{Frob}_{q^h}=\mathrm{Id}}$ is isomorphic to a finite product of k_a's for $1 \leq a \leq h$. The number of factors equals $\sharp\pi_0(\mathrm{Spec}(R))$.

Writing R as a colimit of k-algebras of finite type, we can conclude that if R is a k_h-algebra, then

$$R^{\mathrm{Frob}_{q^h}=\mathrm{Id}} \cong \mathrm{Hom}_{\mathrm{cts}}(\pi_0(\mathrm{Spec}(R)), k_h)$$

with

$$\pi_0(\mathrm{Spec}(R))$$

the profinite set of connected components of $\mathrm{Spec}(R)$, cf. [Sta17, Tag 0906].

Note that $S := R^{\mathrm{Frob}_{q^h}=\mathrm{Id}}$ is a perfect ring, i.e., its Frobenius is bijective. In particular, there exists a π-complete, π-torsion free A-algebra $A(S)$ unique up to unique isomorphism with a fixed isomorphism

$$A/\pi \cong S,$$

cf. [FF18, Proposition 2.1.7.]. For example, $A(k_a)$ is isomorphic to the ring of integers in the unramified extension of K of degree a. In general, each element in $A(S)$ can be represented as a power series

$$\sum_{i=0} [s_i]\pi^i$$

with s_i in S and $[-]\colon S \to A(S)$ the Teichmüller lift, which can be constructed as in Exercise 1.11. The q-Frobenius on S lifts uniquely to an A-algebra homomorphism

$$\sigma\colon A(S) \to A(S),$$

which is functorial in S. We can give the desired description of

$$\mathrm{End}_{\mathrm{FGL}_{A(R)}}(F)$$

if $F \in R[[X, Y]]$ is normalized. By Theorem 2.29 (and Lemma 2.4) we may assume that F and its formal multiplication are defined over k.

Lemma 2.31. *Let R be a k-algebra and set $S := R^{\mathrm{Frob}_{q^h}=1}$. Let $F \in R[[X,Y]]$ be a normalized formal A-module with coefficients in k. Then*

$$\mathrm{End}_{\mathrm{FGL}_A(R)}(F) = A(S) \oplus A(S)\Pi \oplus \ldots \oplus A(S)\Pi^{h-1}$$

with $\Pi(X) = X^q$ satisfying $\Pi^h = \pi$ and

$$a\Pi = \Pi\sigma(a)$$

for $a \in A(S)$.

If $R = k$, then this lemma was Exercise 2.6.

Proof. We may assume $R = S$ as F is normalized and therefore its addition, formal multiplication and endomorphisms are already defined over S. Replacing A by $A(S)$ (and q by q^h) in Lemma 1.14 the same proof works, cf. Remark 1.15 and Theorem 1.26. In particular, we can deduce the existence of a natural injective homomorphism

$$\iota\colon A(S) \to \mathrm{End}_A(F).$$

As F is defined over k it is clear that $\Pi(X) = X^q$ defines an endomorphism of F. As F is normalized it is clear that

$$\Pi^h(X) = [\pi]_F(X).$$

Moreover, for $a \in A(S)$

$$\iota(a) \circ \Pi(X) = \Pi \circ \iota(\sigma(a))$$

by definition of Π and σ. In particular, ι extends to a morphism

$$\iota\colon A(S) \oplus A(S)\Pi \oplus \ldots \oplus A(S)\Pi^{h-1} \to \mathrm{End}_{\mathrm{FGL}_A(R)}(F)$$

of A-algebras. Let $f\colon F \to F$ be an endomorphism over S. After subtracting some $\iota(a)$ with $a \in A(S)$ we may assume that $f'(0) = 0$. By Lemma 2.2 we see that we can write

$$f = g \circ \Pi$$

for a morphism $g\colon F \to F$ of formal A-modules. Continuing we find that we can write

$$f = \iota(\sum_{i=0}^{\infty} a_i \Pi^i)$$

for some $a_i \in A(S)$. Replacing Π^h by π we even get a unique expansion of the form

$$f = \iota(\sum_{i=0}^{h-1} a_i \Pi^i)$$

with $a_0, \ldots, a_{h-1} \in A(S)$. We use that the A-algebra $\mathrm{End}_{\mathrm{FGL}_A(S)}(F)$ is π-complete and π-torsion free. This last statement follows easily using that $\mathrm{End}_{\mathrm{FGL}_A(R)}(F) \subseteq R[[X]]$ is X-adically closed. □

If $R = k_h$, then $\mathrm{End}_{\mathrm{FGL}_A(k_h)}(F)$ is isomorphic to the maximal order of the division algebra of invariant $1/h$ over $K = \mathrm{Frac}(A)$, cf. Section 1.10.

Exercise 2.32. Assume that A is any field, that $R \in \mathrm{Alg}_A$, and F is a formal A-module law over R (in the sense discussed in beginning of Section 2). Show that

$$F \cong \widehat{\mathbb{G}}_a$$

as formal A-modules.
Hint: Reduce to $F(X,Y) = X + Y$ *and* $\operatorname{char}(A) = p > 0$. *Then consider*

$$\iota\colon A \to \operatorname{End}_{\mathrm{FGL}(R)}(\widehat{\mathbb{G}}_a) = R\{\{\tau\}\}$$

with $R\{\{\tau\}\}$ *as in Exercise 2.17. Now prove by induction on* i *that up to isomorphism one can arrange* $\iota(a) \equiv a \bmod (\tau)^i$ *for all* $a \in A$.

2.6. **Proof of representability of Lubin-Tate spaces.** We are now ready to start the proof of the representability of the Lubin-Tate spaces. Let us recall the setup. We suppose that A is a complete discrete valuation ring with finite residue field k of characteristic p, and $q := \sharp k$. Let $\pi \in A$ be a fixed uniformizer. Let

$$F_h \in k[[X, Y]]$$

be a formal A-module of height h. Let

$$\mathrm{Nilp}_A$$

be the category of A-algebras R such that π is nilpotent in R.

The results (and proofs) in this section work the same if we replace k, F_h by any perfect k-algebra k' and $F_h \in k'[[X, Y]]$ any formal A-module of (exact) height $h \in \mathbb{Z}_{\geq 1}$ and replace accordingly Nilp_A by the category $\mathrm{Nilp}_{A(k')}$ of $A(k')$-algebras R with π nilpotent in R and $A[[X_1, \ldots, X_{h-1}]]$ by $A(k')[[X_1, \ldots, X_{h-1}]]$, for $A(k')$ the unique π-complete, π-torsion free A-algebra with $A(k')/\pi \cong k'$. For simplicity in notation we stick to the case $k' = k$.

Let us recall the definition of the Lubin-Tate space associated with F_h, cf. Section 2.2.

Definition 2.33. *For $R \in \mathrm{Nilp}_A$ we set*

$$\mathcal{M}_{F_h}(R)$$

as the set of $\star$-isomorphism classes of formal A-module laws $F \in R[[X, Y]]$ such that $F \equiv F_h \in R/I[[X, Y]]$ for some nilpotent ideal $I \subseteq R$ with $\pi \in I$. The functor

$$\mathcal{M}_{F_h} \colon \mathrm{Nilp}_A \to (\mathrm{Sets})$$

is called the Lubin-Tate space (for F_h).

Let us construct a (non-canonical) morphism

$$\eta \colon \mathrm{Spf}(A[[X_1, \ldots, X_{h-1}]]) \to \mathcal{M}_{F_h}.$$

For this let

$$\overline{g}_{F_h} \colon \Lambda_A \to k$$

be the morphism classifying the formal A-module $F_h \in k[[X, Y]]$. As F_h is of height h we know

$$\overline{g}_{F_h}(v_i) = 0,\ i = 0, \ldots, h-1.$$

Therefore, we can choose a morphism

$$g_{F_h} \colon \Lambda_A \to A[[X_1, \ldots, X_{h-1}]]$$

with

$$g_{F_h}(v_i) = X_i,\ i = 1, \ldots, h-1$$

lifting $\overline{g}_{F_h}$ along the surjection $A[[X_1, \ldots, X_{h-1}]] \to k$ sending X_i to 0 for $i = 1, \ldots, h-1$. For each $n \geq 1$ the formal A-module over

$$A[[X_1, \ldots, X_{h-11}]]/(\pi^n, X_1^n, \ldots, X_{h-1}^n)$$

is a $\star$-deformation of F_h by construction, and this defines by the Yoneda lemma a morphism

$$\eta_n \colon \mathrm{Spec}(A[[X_1, \ldots, X_{h-1}]]/(\pi^n, X_1^n, \ldots, X_{h-1}^n) \to \mathcal{M}_{F_h}.$$

Passing to the colimits of the compatible morphisms η_n yields the desired morphism

$$\eta \colon \mathrm{Spf}(A[[X_1, \ldots, X_{h-1}]]) \to \mathcal{M}_{F_h}.$$

Definition 2.33 is now implied by the following theorem, which will be the main result of this section and its proof will occupy us till the end of this section.

Theorem 2.34 (Lubin-Tate/Drinfeld)**.** *The above morphism*

$$\eta\colon \mathrm{Spf}(A[[X_1,\dots,X_{h-1}]]) \to \mathcal{M}_{F_h}.$$

is an isomorphism.

The following lemma will help to get rid of the $\star$-isomorphisms.

Lemma 2.35. *Let $R \to S$ in Nilp_A be a surjection with nilpotent kernel, and $F \in \mathcal{M}_{F_h}(S)$ be $\star$-deformation of F_h. Then the fiber of*

$$\mathcal{M}_{F_h}(R) \to \mathcal{M}_{F_h}(S)$$

over F is given by the set of equivalence classes of formal A-modules $\tilde{F} \in R[[X,Y]]$ reducing to $F \in S[[X,Y]]$, where $\tilde{F}_1, \tilde{F}_2$ are called equivalent if there exists an isomorphism $f\colon \tilde{F}_1 \to \tilde{F}_2$ reducing to the identity in S.

Proof. Given formal A-modules $\tilde{F}_1, \tilde{F}_2 \in R[[X,Y]]$ lifting F, then by Lemma 2.10 each $\star$-isomorphism $f\colon \tilde{F}_1 \to \tilde{F}_2$ reduces to the identity in S. Furthermore, if $\tilde{F} \in R[[X,Y]]$ is a formal A-module and $g\colon \tilde{F}\hat{\otimes}_R S \cong F$ a $\star$-isomorphism, then we can lift the power series $g \in S[[X]]$ to a power series $h \in R[[X]]$. As $R \to S$ has a nilpotent kernel, the power series h defines an automorphism of $R[[X]]$. Replacing $\tilde{F}$ by $h(\tilde{F}(h^{-1}(X), h^{-1}(Y)))$ we may then assume that $\tilde{F}(X,Y)$ (and its formal multiplication) reduces to F. □

The functor $\mathcal{M}_{F_h}$ satisfies the (formal) Mayer-Vietoris property and is formally smooth as we know explain. Let

$$G\colon \mathrm{Nilp}_A \to (\mathrm{Sets})$$

be a functor.

Definition 2.36. *The functor G satisfies the (formal) Mayer-Vietoris property if for any morphism $R_1 \to S, R_2 \to S$ in Nilp_A with $R_1 \to S$ surjective with nilpotent kernel the natural morphism*

$$G(R_1 \times_S R_2) \to G(R_1) \times_{G(S)} G(R_2)$$

is a bijection. The functor G is called formally smooth if for any surjection $R \to S$ in Nilp_A with nilpotent kernel the map

$$G(R) \to G(R/I)$$

is surjective.

Clearly,

$$\mathrm{Spf}(A[[X_1,\dots,X_n]]) = \mathrm{Hom}_{A,\mathrm{cts}}(A[[X_1,\dots,X_n]], -)\colon \mathrm{Nilp}_A \to (\mathrm{Sets})$$

satisfies the Mayer-Vietoris property and is formally smooth. As a prerequisite to Definition 2.33 we show that the Lubin-Tate spaces $\mathcal{M}_{F_h}$ satisfy the (formal) Mayer-Vietoris property and are formally smooth as well.

Lemma 2.37. *The functor*

$$\mathcal{M}_{F_h}\colon \mathrm{Nilp}_A \to (\mathrm{Sets})$$

satisfies the (formal) Mayer-Vietoris property and is formally smooth.

Proof. Let $\varphi_1 \colon R_1 \to S, \varphi_2 \colon R_2 \to S$ be morphisms in Nilp_A with φ_1 surjective with nilpotent kernel. Set $R := R_1 \times_S R_2$ and let $\pi_i \colon R \to R_i$ the respective projections. We have to prove that the morphism

$$\mathcal{M}_{F_h}(R) \to \mathcal{M}_{F_h}(R_1) \times_{\mathcal{M}_{F_h}(S)} \mathcal{M}_{F_h}(R_2)$$

is a bijection. For this it suffices to see that for each $\star$-deformation $F_2 \in R_2[[X,Y]]$ of F_h the fibers N_1, N_2 of

$$\mathcal{M}_{F_h}(R) \to \mathcal{M}_{F_h}(R_2)$$

and

$$\mathcal{M}_{F_h}(R_1) \to \mathcal{M}_{F_h}(S)$$

over $F \in \mathcal{M}_{F_h}(R_2)$ resp. $\varphi_{2,*}F \in \mathcal{M}_{F_h}(S)$ are in bijection (via φ_1). Note that $R \to R_2, R_1 \to S$ are surjections with nilpotent kernels. By Lemma 2.35 we can conclude that N_1 identifies with isomorphism classes of formal A-modules $G \in R[[X,Y]]$ with second component F, while N_2 identifies with isomorphism classes of formal A-modules $G' \in R_1[[X,Y]]$ reducing to $\varphi_{2,*}F$. By the definition of the fiber product

$$R = R_1 \times_S R_2$$

we see that φ_1 induces a bijection $N_1 \to N_2$ as desired. The formal smoothness of $\mathcal{M}_{F_h}$ follows directly from Lemma 2.35 and Theorem 2.14. Indeed, Lazard's theorem implies that formal A-modules can be lifted along any surjection of rings. □

Lemma 2.37 explains why we have to put this strange condition on the existence of the nilpotent ideal I in the definition of $\mathcal{M}_{F_h}$. The functor sending $R \in \mathrm{Nilp}_A$ to the set of $F \in R[[X,Y]]$ reducing to F_h module π (taken up to isomorphisms reducing to the identity mod π) does not satisfy the Mayer-Vietors property as in general the morphism

$$(R_1 \times_S R_2)/(\pi) \to R_1/\pi \times_{S/\pi} R_2/\pi$$

is not injective.

We first reduce the question whether

$$\eta_R \colon \mathrm{Spf}(A[[X_1, \dots, X_n]])(R) \to \mathcal{M}_{F_h}(R)$$

is a bijection for any $R \in \mathrm{Nilp}_A$ to the case that R has a particular shape.

Lemma 2.38. *Assume that*

$$\eta_R \colon \mathrm{Spf}(A[[X_1, \dots, X_n]])(R) \to \mathcal{M}_{F_h}(R)$$

is a bijection for any local A-algebra R with residue field k whose maximal ideal contains π and is nilpotent. Then η_S is a bijection for any $S \in \mathrm{Nilp}_A$.

In the more general situation with k replaced by any perfect k'-algebra, the conditions on R have to be replaced by the conditions that $\mathcal{N}il(R)$ is nilpotent, contains π and that $k' \to R/\mathcal{N}il(R)$ is an isomorphism. The proof of Lemma 2.38 works as well (even though the ring S' appearing there need not be a subring of S anymore).

Proof. Let $S \in \mathrm{Nilp}_A$ and $F \in S[[X,Y]]$ be a $\star$-deformation of F_h. By definition there exists a nilpotent ideal $I \subseteq S$ containing π such that

$$F \equiv F_h \bmod I.$$

In particular, F has coefficients in the subring

$$S' := k \times_{S/I} S.$$

of elements in S reducing to some element in $k \subseteq S/I$. Note that S' is a local A-algebra with nilpotent maximal ideal $k \times_{S/I} I \cong I$ containing π. In particular, F lies in the image of

$$\mathcal{M}_{F_h}(S') \to \mathcal{M}_{F_h}(S).$$

and thus η_S is surjective as $\eta_{S'}$ is assumed to be surjective. Now assume that

$$g_1, g_2 \in \mathrm{Spf}(A[[X_1, \dots, X_{h-1}]])(S)$$

map to the same element in $\mathcal{M}_{F_h}(S)$. Let $I \subseteq S$ be the ideal generated by $\pi, X_i, g_1(X_i) - g_2(X_{h-1}), i = 1, \dots, h-1$. Then $I \subseteq S$ is nilpotent, and the compositions

$$A[[X_1, \dots, X_{h-1}]] \xrightarrow{g_j} S \to S/I$$

agree for $j = 1, 2$. Let again

$$S' = k \times_{S/I} S.$$

Then g_1, g_2 factor over morphisms

$$g_1', g_2' \colon A[[X_1, \dots, X_{h-1}]] \to S'.$$

Using that $\eta_{S'}$ is injective, it suffices to see that the images of g_1', g_2' in $\mathcal{M}_{F_h}(S')$ agree. By Lemma 2.37

$$\mathcal{M}_{F_h}(S') \cong \mathcal{M}_{F_h}(k) \times_{\mathcal{M}_{F_h}(S/I)} \mathcal{M}_{F_h}(S),$$

and both components of $\eta_{S'}(g_1') = \eta_{S'}(g_2')$ agree. This finishes the proof. □

Let S be any ring, and let M be any S-module. Then we define the S-algebra

$$S[M]$$

with underlying S-module $S \oplus M$ and multiplication

$$(s, m)(s', m') := (ss', sm' + s'm)$$

for $s, s' \in S, m, m' \in M$. Note $M \subseteq S[M]$ is an ideal with $M^2 = 0$. We sometimes will write $S[M] = S \oplus \varepsilon M$ with $\varepsilon^2 = 0$.

Lemma 2.39. *Let M be any k-module. Then the map*

$$\eta_{k[M]} \colon \mathrm{Spf}(A[[X_1, \dots, X_{h-1}]])(k[M]) \to \mathcal{M}_{F_h}(k[M])$$

is a bijection.

Proof. The LHS is given by the set of continuous morphisms

$$f \colon A[[X_1, \dots, X_{h-1}]] \to k[M].$$

As $M^2 = 0$, this set identifies with

$$\mathrm{Hom}_k((X_1, \dots, X_{h-1})/(X_1, \dots, X_{h-1})^2, M) \cong M^{h-1}.$$

By Lemma 2.35 $\mathcal{M}_{F_h}(k[M])$ identifies with the set of isomorphism classes of formal A-modules $F \in k[M][[X, Y]]$ lifting F_h in k. We now construct a natural map

$$\theta_M \colon \mathcal{M}_{F_h}(k[M]) \to M^{h-1}$$

recording the $v_1, \dots, v_{h-1}$. Namely, let

$$F \in \mathcal{M}_{F_h}(k[M])$$

be a $\star$-deformation of F_h over $k[M]$. As k is reduced, we can conclude that $F\hat{\otimes}_{k[M]}k = F_h$. Now set

$$\theta_M(F) := (v_1, \dots, v_{h-1}) \in (\varepsilon M)^{h-1} \cong M^{h-1},$$

where v_i is the coefficient of X^{q^i} in $[\pi]_F(X)$. This is well-defined as

$$[\pi]_{F_h}(X) \equiv 0 \bmod (X)^{q^h}$$

and only depends on the $\star$-deformation class of F because if $\varphi(X) \in k[M][[X]]$ is a power series with $\varphi(X) \equiv X \bmod \varepsilon M$, we have

$$\varphi^{-1}([\pi]_F(\varphi(X)) \equiv [\pi]_F \bmod (X^{q^h})$$

as follows from the facts that $\varepsilon^2 = 0, \pi\varepsilon M = 0$. It is clear that θ_M is natural in M.

By construction of η the composition

$$M^{h-1} \cong \mathrm{Hom}_k((X_1, \dots, X_{h-1})/(X_1, \dots, X_{h-1})^2, M) \to \mathcal{M}_{F_h}(k[M]) \xrightarrow{\theta_M} M^{h-1}$$

is the identity for any k-vector space. To prove the lemma it therefore suffices to see that θ_M is injective. By Lemma 2.37 the functor

$$M \mapsto \mathcal{M}_{F_h}(k[M])$$

commutes with finite products as $k[M_1 \oplus M_2] \cong k[M_1] \times_k k[M_2]$ for k-vector spaces M_1, M_2. This implies that $\mathcal{M}_{F_h}(k[M])$ is naturally a k-module (as functors commuting with finite products preserve k-module objects) and that θ_M is a morphism of k-module. In particular, it suffices to check that its kernel is trivial. If $F \in \mathcal{M}_{F_h}(k[M])$ lies in the kernel of θ_M. Then by definition of θ_M the formal A-module F is of (exact) height h. Let $F_0 = F_h \in \mathcal{M}_{F_h}(k[M])$ be the trivial deformation of F_h. Lemma 2.40 implies that the functor on F_h lifts to an isomorphism $F \cong F_0$. This proves that θ_M is injective as desired. □

We used the following lemma.

Lemma 2.40. *Let R be a k-algebra and $F_1, F_2 \in R[[X, Y]]$ two formal A-modules of height $h \in \mathbb{Z}_{\geq 1}$, and let $I \subseteq R$ be a nilpotent ideal. Then each isomorphism $F_1\hat{\otimes}_R R/I \cong F_2\hat{\otimes}R/I$ admits a unique lift to an isomorphism $F_1 \to F_2$.*

Proof. It is clear that the functor

$$\mathrm{Alg}_R \to (\mathrm{Sets}),\ S \mapsto \mathrm{Isom}_{\mathrm{FGL}_A(R)}(F_1\hat{\otimes}_R S, F_2\hat{\otimes}_R S)$$

is corepresentable by some R-algebra R'. By Lemma 2.28, Theorem 2.29 and Lemma 2.31 there exists a faithfully flat ind-finite étale R-algebra S such that the S-algebra $S' := R' \otimes_R S$ is formally étale over S, i.e.,

$$\mathrm{Hom}_S(S', T) \cong \mathrm{Hom}_S(S', T/J)$$

for any S-algebra T and $J \subseteq T$ a nilpotent ideal (this boils down to the fact that $T^{\mathrm{Frob}_{q^h}=\mathrm{Id}} = (T/J)^{\mathrm{Frob}_{q^h}=\mathrm{Id}}$ by nilpotence of J). By faithfully flat descent we can conclude that R' is a formally étale R-algebra as desired. □

The conclusion of Theorem 2.34 is now a formal consequence of the following general proposition. Let

$$\mathcal{C}_A$$

be the category of local A-algebras R with residue field k and nilpotent maximal ideal (containing π).

Proposition 2.41. *Let $G_1, G_2 \colon \mathcal{C}_A \to (\mathrm{Sets})$ be two functors which satisfy the Mayer-Vietoris property and are formally smooth. Then a natural transformation*

$$\eta \colon G_1 \to G_2$$

is an isomorphism if and only if $\eta_{k[M]} \colon G_1(k[M]) \to G_2(k[M])$ is a bijection for all k-modules M.

By Lemma 2.37, Lemma 2.38 and Lemma 2.39 this implies Theorem 2.34.

Proof. For simplicity we assume that $G_1(k) = \{*\} = G_2(k)$ is a singleton. Let $R \in \mathcal{C}_A$ with maximal ideal $\mathfrak{m}_R$. Let $n \geq 1$ such that $\mathfrak{m}_R^n = 0$. If $n = 0$, we are finished by assumption. By induction we may assume that η_S is a bijection for all $S \in \mathcal{C}_A$ such that $\mathfrak{m}_S^{n-1} = 0$. Set $J := \mathfrak{m}_R^{n-1}$. Then $J \subseteq R$ is a square zero ideal with $\mathfrak{m}_R \cdot J = 0$. This implies that

$$R \times_k k[J] \cong R \times_{R/J} R, (r, (a, j)) \mapsto (r, r + j)$$

and more generally

$$R \times_k k[J] \times_k \ldots \times_k k[J] \cong R \times_{R/J} \ldots \times_{R/J} R.$$

From the Mayer-Vietoris property we can deduce that

$$G_1(R) \times_{G_1(k)} \ldots \times_{G_1(k)} G_1(k[J]) \cong G_1(R) \times_{G_1(R/J)} \ldots \times_{G_1(R/J)} G_1(R).$$

This implies that the fibers of

$$G_1(R) \to G_1(R/J)$$

are principal homogeneous spaces under the group $G_1(k[J])$. The same discussion applies for G_2. By assumption

$$\eta_{k[J]} \colon G_1(k[J]) \to G_2(k[J])$$

is an isomorphism. Using formal smoothness of G_2 and induction we can conclude that the diagram

$$\begin{array}{ccc} G_1(R) & \xrightarrow{\eta_R} & G_2(R) \\ \downarrow & & \downarrow \\ G_1(R/J) & \xrightarrow{\eta_{R/J}} & G_2(R/J) \end{array}$$

is cartesian. As by induction $\eta_{R/J}$ is an isomorphism, we get that η_R is an isomorphism. □

3. Formal schemes

Let A be a complete discrete valuation ring with finite residue field k and let $F_h \in k[[X,Y]]$ be a formal A-module of height $h \in \mathbb{Z}_{\geq 1}$.

Our next aim is to construct the étale and surjective Gross-Hopkins period morphism

$$\pi_{\mathrm{GH}} \colon \mathcal{M}_{F_h,\eta} \to \mathbb{P}_K^{h-1,\mathrm{ad}}$$

from the adic generic fiber of the Lubin-Tate space $\mathcal{M}_{F_h,\eta}$, a rigid analytic open unit ball over $K := \mathrm{Frac}(A)$, to the (adic) projective space of dimension $h-1$. The existence of π_{GH} is quite surprising. Indeed, it is not just étale surjective, but an infinite covering space (in a suitable sense). In complex geometry a map like π_{GH} can therefore not exist as the projective space is simply connected. To rigorously present the construction of π_{GH} we need a geometric framework incorporating rigid-analytic spaces like $\mathbb{P}_K^{h-1,\mathrm{ad}}$ and formal schemes like $\mathcal{M}_{F_h}$. For this reason we aim to discuss Huber's category of adic spaces. As an introduction we discuss formal schemes (a bit). This will lead to a different, useful viewpoint on formal A-modules and Lubin-Tate spaces.

3.1. **Formal schemes.** Let us recall that there exist (at least) two viewpoints on schemes. Namely,

(1) a scheme X is a locally ringed space, which locally is isomorphic to the locally ringed space $\mathrm{Spec}(R)$ associated with some ring R,
(2) a scheme X is a (covariant) functor on rings, which locally agrees with the functor corepresented by some ring R.

The first viewpoint is more geometric while the second is powerful for discussing group schemes etc.. The link between both viewpoints is the Yoneda lemma.

We will now develop similar viewpoints on (affine) formal schemes.

Example 3.1. Recall the functor

$$\mathcal{N}il \colon (\mathrm{Alg}_A) \to (\mathrm{Sets})$$

from Section 1.4. We saw that

$$\mathcal{N}il(R) = \mathrm{Hom}_{A,\mathrm{cts}}(A[[X]], R),$$

where $A[[X]]$ is considered as a *topological* A-algebra for its (X)-adic topology, and $R \in \mathrm{Alg}_A$ is given the discrete topology. More generally, consider any topological A-algebra B. Then we obtain a functor

$$\mathrm{Spf}(B) := \mathrm{Hom}_{A,\mathrm{cts}}(B, -) \colon (\mathrm{Alg}_A) \to (\mathrm{Sets})$$

sending R to the set of continuous A-algebra homomorphisms $B \to R$ with R equipped with the discrete topology. This construction is too general, and we should assume that B is linearly topologized, i.e., admits a fundamental system $I_j, j \in J$, of neighborhoods of 0, which are ideals.

Note that in this case the functor $\mathrm{Hom}_{A,\mathrm{cts}}(B,-)$ only depends on the completion

$$\widehat{B} := \widehat{B} := \varprojlim_{j \in J} B/I_j$$

which is a complete ring when equipped with its inverse limit topology as

$$\mathrm{Hom}_{A,\mathrm{cts}}(B,-) \cong \mathrm{Hom}_{A,\mathrm{cts}}(\widehat{B},-).$$

Indeed, if R is any A-algebra (equipped with the discrete topology) and $f\colon B \to \widehat{B}$ the natural morphism, then precomposition by f induces a bijection

$$\mathrm{Hom}_{A,\mathrm{cts}}(B,R) \cong \mathrm{Hom}_{A,\mathrm{cts}}(\widehat{B},R)$$

as both sides evaluate to

$$\varinjlim_j \mathrm{Hom}_A(B/I_j,R)$$

by the definition of the topologies on B and $\widehat{B}$. We leave it as an exercise to check that the functor $\mathrm{Hom}_{A,\mathrm{cts}}(B,-)$ is corepresentable if and only if the topology on $\widehat{B}$ is discrete.

Useful examples are the n-dimensional formal affine space over A, which

$$\hat{\mathbb{A}}^n_A := \mathrm{Spf}(A[[X_1,\dots,X_n]]),$$

or the formal multiplicative group over A

$$\hat{\mathbb{G}}_{m,A} := \mathrm{Spf}(A[[T-1]])$$

with $A[[T-1]]$ the $(T-1)$-adic completion of $A[T,T^{-1}]$ (or $A[T]$).

We want to single out the class of topological rings, which are relevant for formal schemes.

Definition 3.2 ([Sta17, Tag 07E8])**.** *Let R be a topological ring.*

1. *R is called linearly topologized if $0 \in R$ has a basis of neighborhoods, which are ideals.*
2. *If R is linearly topologized, then an ideal $I \subseteq R$ is called an ideal of definition, if $I \subseteq R$ is open and every neighborhood of 0 contains I^n for some $n \geq 0$.*
3. *R is called admissible if R is linearly topologized, contains an ideal of definition and R is complete (i.e., as topological rings $R \cong \varprojlim_J R/J$, where J is running through a fundamental system of open neighborhoods of 0, which are ideals, and the RHS is equipped with the inverse limit topology).*
4. *R is called adic if R is complete and its topology is I-adic for some ideal $I \subseteq R$.*

For example, $R = \mathbb{R}$ with its classical topology is not linearly topologized. Let

$$R = \mathbb{Z}[X_1,X_2,\dots] \supseteq I := (X_1,X_2,\dots)$$

as in [Sta17, Tag 05JA]. Then the ring

$$\hat{R}_I = \varprojlim_n R/I^n$$

(with its inverse limit topology) is admissible, but not adic (as is proven in [Sta17, Tag 05JA]). In general, if R is any ring and $I \subseteq R$ a finitely generated ideal, then the inverse limit topology on $\hat{R}_I$ is $I\cdot\hat{R}_I$-adic and in particular, $\hat{R}_I$ is $I\cdot\hat{R}_I$-adically complete, cf. [Sta17, Tag 05GG]. As a special case, we leave the following as an exercise.

Exercise 3.3. Assume that R is a ring and $\pi \in R$ a non-zero divisor. Let $I := (\pi)$ and $n \geq 0$. Show that the image of $\pi \in \hat{R}_I$ is a non-zero divisor, that $\pi^n \cdot \hat{R}_I = \ker(\hat{R}_I \to R/I^\pi)$ and that $\hat{R}_I$ is π-adically complete.

The definition of an admissible ring traces back to Grothendieck's definition of a formal scheme, cf. [Sta17, Tag 0AHY] and certain generalizations of the definition are possible, cf. [Sta17, Tag 0A16]. For us the most important case is that of an adic ring containing a finitely generated ideal of definition. For an admissible ring A let

$$\mathrm{Adm}_A$$

be the category of admissible A-algebras B (with $A \to B$ continuous). Let us set

$$\mathrm{Nilp}_A$$

as the category of continuous ring morphisms $A \to R$ with R discrete.[10] The morphisms in Adm_A are by definition the continuous morphisms of A-algebras. If $B \in \mathrm{Adm}_A$, then we have an equality

$$\mathrm{Spf}(B) = h^B_{\mathrm{cts}} = \varinjlim_{n \geq 0} h^{B/I^n} \tag{10}$$

of functors $(\mathrm{Nilp}_A) \to (\mathrm{Sets})$. Indeed, the category $\mathrm{Fun}(\mathrm{Alg}_A, (\mathrm{Sets}))$ has all (small) limits and colimits, and these are computed pointwise.

Lemma 3.4. *The functor*

$$\mathrm{Adm}_A^{\mathrm{op}} \to \mathrm{Fun}(\mathrm{Nilp}_A, (\mathrm{Sets})),\ B \mapsto \mathrm{Spf}(B) = h^B_{\mathrm{cts}}$$

is fully faithful.

Lemma 3.4 is an example of the Yoneda lemma for pro-objects.

Proof. Let $B, B' \in \mathrm{Adm}_A$ and let $I_i \subseteq B', i \in I$, be a fundamental system of open neighborhoods of 0, which are ideals in B'. Then we can calculate

$$\begin{aligned}
&\mathrm{Hom}_{\mathrm{Fun}(\mathrm{Nilp}_A,(\mathrm{Sets}))}(h^{B'}_{\mathrm{cts}}, h^B_{\mathrm{cts}}) \\
\cong &\mathrm{Hom}_{\mathrm{Fun}(\mathrm{Nilp}_A,(\mathrm{Sets}))}(\varinjlim_j h^{B'/I'_j}, h^B_{\mathrm{cts}}) \\
\cong &\varprojlim_j \mathrm{Hom}_{\mathrm{Fun}(\mathrm{Nilp}_A,(\mathrm{Sets}))}(h^{B'/I'_j}, h^B_{\mathrm{cts}}) \\
\cong &\varprojlim_j \mathrm{Hom}_{A,\mathrm{cts}}(B, B'/I'_j) \\
\cong &\mathrm{Hom}_{A,\mathrm{cts}}(B, B')
\end{aligned}$$

using the Yoneda lemma and the fact the colimits of functors are computed pointwise. □

At this point we did not use the assumption on the existence of an ideal of definition. This assumption will be important when introducing the topological space of a formal scheme, cf. Definition 3.10.

Exercise 3.5. A functor $F\colon \mathrm{Alg}_A \to (\mathrm{Sets})$ is called an fpqc-sheaf if for any faithfully flat morphism $R \to S$ of A-algebras the morphism $F(R) \to F(S)$ is an equalizer of the two natural morphisms $p_1, p_2\colon F(S) \to F(S \otimes_R S)$. If $B \in \mathrm{Adm}_A$, then h^B_{cts} is an fpqc-sheaf.

We can now finish our discussion about viewing formal group laws as group structures on the functor $\mathcal{N}il$, cf. Section 1.4.

[10] If A is a complete discrete valuation ring, this recovers the category Nilp_A of A-algebras R, such that the uniformizers are nilpotent in R.

Example 3.6. Let R be any ring and consider the functor

$$\mathcal{N}il \cong \mathrm{Spf}(R[[X]])\colon \mathrm{Alg}_R \to (\mathrm{Sets}).$$

By Lemma 3.4 we see that natural transformations of functors

$$\eta\colon \mathcal{N}il \to \mathcal{N}il$$

are in bijection to

$$\mathrm{Hom}_{R,\mathrm{cts}}(R[[X]], R[[X]]).$$

In general, $\mathrm{Hom}_{R,\mathrm{cts}}(R[[X]], B)$ with $B \in \mathrm{Adm}_R$ identifies with the set

$$B^{\circ\circ} := \{b \in B \mid b^n \to 0, n \to \infty\}$$

of topologically nilpotent elements in B. Now assume that $B = R[[X]]$. Then we get

$$B^{\circ\circ} = \{f(X) \in R[[X]] \mid f(0) \in \mathcal{N}il(R)\}.$$

Given $f \in B^{\circ\circ}$ the induced natural transformation η preserves the zero section $0\colon \mathrm{Spec}(R) \to \mathcal{N}il$ if and only if $f(0) = 0$. From here it is now clear (thanks to Lemma 1.21) that formal group laws correspond bijectively to group structures on the functor $\mathcal{N}il$ whose two sided unit is $0\colon \mathrm{Spec}(R) \to \mathcal{N}il$. Note that the restriction that 0 is a two sided unit for the group structure on $\mathcal{N}il$ is not serious as we can translate any section $s\colon \mathrm{Spec}(R) \to \mathcal{N}il$ to the zero section. If A is a discrete valuation ring with finite residue field, then we see similarly that formal A-module(law)s $F \in R[[X, Y]]$ for $R \in \mathrm{Alg}_A$ correspond bijectively to A-module structures on the functor

$$\mathcal{N}il\colon \mathrm{Alg}_R \to (\mathrm{Sets}),$$

whose additive unit is $0 \in \mathcal{N}il$.

An important way of constructing formal schemes is via completion of schemes along (closed) subschemes. More generally, let A be any ring, let

$$X\colon \mathrm{Alg}_A \to (\mathrm{Sets})$$

be a functor, and $Y \subseteq X$ a subfunctor. Then we can define the formal completion

$$\widehat{X}_Y$$

of X along Y as the subfunctor of X given by all $s \in X(R), R \in \mathrm{Alg}_A$, such that there exists a nilpotent ideal $I \subseteq R$ such that the image of s in $X(R/I)$ lies in $Y(R/I)$. We leave it as an exercise to see that if R is any A-algebra and $I \subseteq R$ an ideal, then the formal completion of $\mathrm{Spec}(R)$ along its (closed) subscheme $\mathrm{Spec}(R/I)$ is the formal affine scheme

$$\mathrm{Spf}(\widehat{R}_I) \subseteq \mathrm{Spec}(R).$$

If X is a group valued functor, and Y a subgroup functor, then the formal completion is pointwise stable under the group structure, and hence again a group valued functor. This generalizes Example 1.22. As a concrete example for a formal completion assume $R = \mathrm{Sym}_A^\bullet M$ for an A-module M, and set

$$A[[M]]$$

as the admissible ring representing the formal completion of R at the ideal generated by M. If M is a finite free A-module of rank n, then

$$\mathrm{Spf}(A[[M]]) \cong \mathrm{Spf}(A[[X_1, \ldots, X_n]])$$

and if M is finite projective such an isomorphism exists locally on $\mathrm{Spec}(A)$, cf. Lemma 3.7. Therefore we can call $\mathrm{Spf}(A[[M]])$ a formal vector bundle over A. Note that for any $R \in \mathrm{Nilp}_A$ there exists a natural bijection between

$$\mathrm{Spf}(A[[M]])(R)$$

and the set

$$\mathrm{Hom}_A(M, \mathcal{N}il(R))$$

of A-linear homomorphisms $M \to \mathcal{N}il(R)$. In particular, there exists the natural zero section $0\colon \mathrm{Spf}(A) \to \mathrm{Spf}(A[[M]])$.

Let us now compute some fiber products of formal (affine) schemes.

Lemma 3.7. *Let $A \to R$ be a morphism of rings and M an A-module. Then*

$$\mathrm{Spec}(R) \times_{\mathrm{Spec}(A)} \mathrm{Spf}(A[[M]]) \cong \mathrm{Spf}(R[[M \otimes_A R]]).$$

Proof. Given an A-algebra S, then

$$\mathrm{Spf}(A[[M]])(S)$$

identifies with A-linear maps $M \to \mathcal{N}il(S)$. Given now an R-algebra S, then naturally in S

$$\mathrm{Hom}_A(M, \mathcal{N}il(S)) \cong \mathrm{Hom}_R(R \otimes_A M, \mathcal{N}il(S)),$$

which proves the claim. □

In general,

$$\mathrm{Spf}(R) \times_{\mathrm{Spf}(A)} \mathrm{Spf}(B) \cong \mathrm{Spf}(R \hat{\otimes}_A B),$$

where $R \hat{\otimes}_A B$ is the completed tensor product of the admissible A-algebras R, B, cf. [Gro60, §0.(7.7.6.)]. For example,

$$\mathrm{Spf}(A[[M_1]]) \times_{\mathrm{Spf}(A)} \mathrm{Spf}(A[[M_2]]) \cong \mathrm{Spf}(A[[M_1 \otimes_A M_2]])$$

as can also be calculated by hand.

Exercise 3.8. Let A be a ring and let $X\colon \mathrm{Alg}_A \to (\mathrm{Sets})$ be a functor. Then $X \cong \mathrm{Spf}(A[[M]])$ for a finite projective A-module M if and only if the following conditions are satisfied

(1) $X \cong \mathrm{Spf}(B)$ for some admissible A-algebra B,
(2) X is formally smooth, cf. Definition 2.36,
(3) there exists a section $s \in X(A)$ and X is the formal completion of X along s,
(4) X commutes with filtered colimits in Alg_A.

If these conditions are satisfied we call X a formal Lie variety over A.

The critical point in Exercise 3.8 is to find a candidate for the A-module M. This works as follows: Recall that for an A-module N we defined the A-algebra

$$A[N] = A \oplus \varepsilon N$$

with $\varepsilon^2 = 0$. If $X = \mathrm{Spf}(A[[M]])$ and $s\colon \mathrm{Spec}(A) \to X$ the zero section, then there exists a natural isomorphism

$$\mathrm{Hom}_A(M, N) \cong X(A[N]) \times_{X(A)} \{*\}$$

with $\{*\} \to X(A)$ the unique map with image $s \in X(A) = \mathrm{Hom}_A(\mathrm{Spec}(A), X)$ and by the Yoneda lemma this characterizes M up to isomorphism. Given an

isomorphism $X \cong \mathrm{Spf}(B)$, and $f\colon B \to A$ the morphism corresponding to the section s, then $M \cong I/I^2$ with $I := \ker(B \to A)$.

Definition 3.9. *With the above notation we call*

$$T_s X := X(A[A]) \times_{X(A)} \{*\} \cong \mathrm{Hom}_A(M, A)$$

the tangent space of X at s, and the rank of M the relative dimension of X over A.

It is clear that the category of formal Lie varieties admits products. Let us now introduce a locally (topologically) ringed space associated to an admissible ring A. We set (abusing notation)

$$\mathrm{Spf}(A)$$

as the set of *open* prime ideals in A (which can be much smaller than $\mathrm{Spec}(A)$). If $I \subseteq A$ is an ideal of definition, then

$$\mathrm{Spf}(A) \cong \mathrm{Spec}(A/I)$$

as each open prime ideal in A must contain I. In particular, the Zariski topology on $\mathrm{Spec}(A/I)$ can be transported to $\mathrm{Spf}(A)$. One can check that this topology is independet of the choice of I. More canonically, pick $f \in A$ and set

$$D(f) \subseteq \mathrm{Spf}(A)$$

as the subset of open prime ideals $\mathfrak{p} \subseteq A$ with $f \notin \mathfrak{p}$. The subsets $D(f), f \in A$, form then a basis for the previously constructed topology, and the topological space $\mathrm{Spf}(A)$ is functorial in morphisms $A \to B$ of admissible rings. Given $f \in A$ there exists an admissible A-algebra $A\langle 1/f\rangle$ such that a morphism $g\colon A \to B$ of admissible rings factors over $A\langle 1/f\rangle$ if and only if $\mathrm{Spf}(B) \xrightarrow{\mathrm{Spf}(g)} \mathrm{Spf}(A)$ factors over $D(f)$. More concretely, if

$$A \cong \varprojlim_{i \in J} A/I_i$$

for a fundamental system of open ideals of definition $I_i \subseteq A, i \in J$, then

$$A\langle 1/f\rangle := \varprojlim_{i \in J} A/I_i[1/f].$$

In particular, $A\langle 1/f\rangle$ depends only on $D(f)$ and we obtain a presheaf $\mathcal{O}_{\mathrm{Spf}(A)}$

$$D(f) \mapsto A\langle 1/f\rangle$$

of topological rings on (a basis of) $\mathrm{Spf}(A)$. Alternatively, $\mathcal{O}_{\mathrm{Spf}(A)}$ is the inverse limit (in presheaves of topological rings) of the structure sheaves

$$\mathcal{O}_{\mathrm{Spec}(A/I_i)}$$

on the topological spaces $\mathrm{Spec}(A/I_i) \cong \mathrm{Spf}(A)$. As limits of sheaves are again sheaves, we see that $\mathcal{O}_{\mathrm{Spf}(A)}$ is a sheaf of topological rings on $\mathrm{Spf}(A)$. If A is discrete this sheaf need not be a sheaf of *discrete* topological rings as infinite products/limits of discrete topological spaces are not necessarily discrete. This subtle point is usually not relevant.

Let us finish this subsection with the definition of a formal scheme.

Definition 3.10. *A locally topologically ringed space $(X, \mathcal{O}_X)$ is called a formal scheme if it is locally isomorphic to $(\mathrm{Spf}(A), \mathcal{O}_{\mathrm{Spf}(A)})$ for some admissible ring A.*

We leave it as an exercise to check that for any formal scheme X over some $\mathrm{Spf}(A)$ the functor

$$h_X \colon \mathrm{Nilp}_A \to (\mathrm{Sets}),\ R \mapsto \mathrm{Hom}_A(\mathrm{Spec}(R), X)$$

is an fpqc-sheaf and that the functor

$$h \colon (\text{Formal schemes over } \mathrm{Spec}(R)) \to \mathrm{Fun}(\mathrm{Alg}_A, (\mathrm{Sets}))$$

is fully faithful.

3.2. **Formal A-modules revisited.** Assume that A is any ring.

Definition 3.11. *Let R be an A-algebra.*

(1) *A (commutative, infinitesimal, formally smooth) formal group over R (of topologically finite type) is a (commutative) group object $\mathcal{G}$ in the category of formal Lie varieties over R. A morphism of formal groups is a morphism of group objects. We denote by $\mathrm{FG}^{\mathrm{arb}}(R)$ the category of commutative formal groups over R (of arbitrary relative dimension).*

(2) *For $\mathcal{G} \in \mathrm{FG}(R)$ we call*

$$\mathrm{Lie}(\mathcal{G}) := T_0\mathcal{G},$$

with $0 \colon \mathrm{Spec}(R) \to \mathcal{G}$ the zero section, the Lie algebra of $\mathcal{G}$. Clearly, the Lie algebra is functorial in morphisms of formal groups.

(3) *A formal A-module over R an A-module object $(\mathcal{G}, \iota \colon A \to \mathrm{End}_{\mathrm{FG}^{\mathrm{arb}}(R)}(\mathcal{G})$ in the category $\mathrm{FG}^{\mathrm{arb}}(R)$ of commutative formal groups over R such that the action of A on $\mathrm{Lie}(\mathcal{G})$ coincides with the natural A-action coming from R. More precisely, this means that the diagram*

$$\begin{array}{ccc} A & \xrightarrow{\iota} & \mathrm{End}_{\mathrm{FG}^{\mathrm{arb}}(R)}(\mathcal{G}) \\ \downarrow & & \downarrow \\ R & \longrightarrow & \mathrm{End}_{\mathrm{Mod}_R}(\mathrm{Lie}(\mathcal{G})) \end{array}$$

commutes. A morphism of formal A-modules is a morphism of A-module objects in $\mathrm{FG}^{\mathrm{arb}}(R)$. We denote by $\mathrm{FG}_A^{\mathrm{arb}}(R)$ the category of formal A-modules (of arbitrary relative dimension).

Given a formal A-module $(\mathcal{G}, \iota)$ we set

$$[a] := [a]_{\mathcal{G}}\iota(a) \colon \mathcal{G} \to \mathcal{G}$$

for $a \in A$. We let $\mathrm{FG}(R), \mathrm{FG}_A(R)$ be the categories of formal groups/formal A-modules of relative dimension 1. These are the formal groups/formal A-modules we are mostly interested in. In Section 1.4 we associated a formal A-module to any formal A-module law, and similarly a morphism of formal A-modules to any morphism of formal A-module laws. By Lemma 3.4 we can deduce that the resulting functor

$$\mathrm{FGL}_A(R) \to \mathrm{FG}_A(R)$$

is fully faithful. Its essential image consists precisely of those formal A-module $\mathcal{G}$ such that $\mathrm{Lie}(\mathcal{G})$ is a *free* A-module (of rank 1). In particular, each formal A-module lies Zariski-locally on $\mathrm{Spec}(R)$ in the essential image.

Assume from now on that A is a complete discrete valuation ring with finite residue field k of characteristic p and cardinality q. We let K be the fraction field of A.

Definition 3.12. *Let $R \in \mathrm{Alg}_A$ and $\mathcal{G} \in \mathrm{FG}_A(R)$. Then we call $\mathcal{G}$ a π-divisible formal A-module if $\ker([\pi]\colon \mathcal{G} \to \mathcal{G})$ is represented by a finite, locally free scheme over $\mathrm{Spec}(R)$.*

Lemma 3.13. *Let $R \in \mathrm{Alg}_A$ and $\mathcal{G} \in \mathrm{FG}_A(R)$. The following conditions are equivalent:*

(1) *$\mathcal{G}$ is a π-divisible formal A-module.*
(2) *The function*

$$\mathrm{ht}_{\mathcal{G}}\colon \mathrm{Spec}(R) \to \mathbb{Z}_{\geq 0} \cup \{\infty\},\ x \mapsto \mathrm{ht}(\mathcal{G} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(k(x)))$$

is locally constant and takes values in $\mathbb{Z}_{\geq 0}$.

If these conditions are satisfied and $\mathrm{ht}_{\mathcal{G}}$ is constant of value h we say that $\mathcal{G}$ is a π-divisible formal A-module of height h.

Proof. We prove a more general statement in Lemma 3.15. □

For example, if R is a K-algebra, then $[\pi]$ is invertible on $\mathcal{G}$ and each formal A-module over R is π-divisible of height 0. As a consequence if R is an A-algebra and $\mathcal{G} \in \mathrm{FG}_A(R)$ π-divisible of height $h \geq 1$, then π must be nilpotent in R.

The following "rigidity of quasi-isogenies" between π-divisible formal A-modules allows us to reinterpret the Lubin-Tate space as a moduli space of formal A-modules in a quasi-isogeny class.

Lemma 3.14. *Let $R \in \mathrm{Nilp}_A$, $I \subseteq R$ a nilpotent ideal and $\mathcal{G}_1, \mathcal{G}_2$ two π-divisible formal A-modules over R. Then the map*

$$\mathrm{Hom}_{\mathrm{FG}_A(R)}(\mathcal{G}_1, \mathcal{G}_2) \to \mathrm{Hom}_{\mathrm{FG}_A(R/I)}(\mathcal{G}_1 \hat{\otimes}_R R/I, \mathcal{G}_{2,} \hat{\otimes}_R R/I)$$

is an injection of π-torsion free modules with cokernel π^n-torsion for some $n \geq 1$.

The injectivity can be deduced from Lemma 2.10.

Proof. We may assume that $I^2 = 0$ and $\pi \cdot I = 0$ and that $\mathcal{G}_1, \mathcal{G}_2$ arise from formal A-module laws F_1, F_2. Let $g \in R[[X]]$ be a power series with coefficients in I. Then we can conclude that

$$[\pi]_{F_2}(g(X)) = 0.$$

If g is moreover a morphism of formal A-modules, then

$$[\pi]_{F_2}(g(X)) = g([\pi]_{F_1}(X)) = 0,$$

which forces $g = 0$ as $\mathcal{G}_1$ is π-divisible. Assume now that $f \in R[[X]]$ reduces to a morphism of formal A-modules over R/I. Then we can conclude that

$$[\pi]_{F_2}(f(F_1(X,Y)) - F_2(f(X), f(Y))) = 0$$

as $f(F_1(X,Y)) - F_2(f(X), f(Y))$ has coefficients in I. We can write

$$0 = [\pi]_{F_2}(f(F_1(X,Y)) - F_2(f(X), f(Y))) = [\pi]_{F_2}(f(F_1(X,Y))) - [\pi]_{F_2}(F_2(f(X), f(Y))) + g(X,Y)$$

with $g(X,Y)$ having coefficients in I. This implies that

$$\begin{aligned}&[\pi^2]_{F_2}(f(F_1(X,Y)))\\ =&[\pi]_{F_2}([\pi]_{F_2}(F_2(f(X),f(Y)))+g(X,Y))\\ =&[\pi]_{F_2}([\pi]_{F_2}(F_2(f(X),f(Y))))+\pi g(X,Y)\\ =&F_2([\pi^2]_{F_1}(f(X)),[\pi^2]_{F_1}(f(Y))),\end{aligned}$$

i.e., that $[\pi^2]_{F_2}\circ f(X)$ defines a morphism $\mathcal{G}_1\to\mathcal{G}_2$. □

Lemma 3.15. *Let $R\in\mathrm{Alg}_A$ and let $f\colon\mathcal{G}_1\to\mathcal{G}_2$ be a morphism. Then the following conditions are equivalent:*

1. $\ker(f)$ *is represented by a finite, locally free scheme over* $\mathrm{Spec}(R)$,
2. *The height function* $\mathrm{ht}(f)\colon\mathrm{Spec}(R)\to\mathbb{Z}_{\geq 0}\cup\{\infty\}$ *mapping x to* $\mathrm{ht}(f\hat{\otimes}_R k(x))$ *is locally constant with value in* $\mathbb{Z}_{\geq 1}$.

If these conditions are satisfied, we call f an isogeny.

Proof. After Zariski-localization on $\mathrm{Spec}(R)$ we may represent f via some powerseries $g\in R[[X]]$. If R is a field, then we see moreover that

$$q^{\mathrm{ht}(f)}=\dim_R(R[[X]]/(g)).$$

Assume that R is general. By the existence of fiber products in formal schemes,

$$\ker(f)\cong\mathrm{Spf}(R[[X]]/\overline{(g)}),$$

where $\overline{(g)}$ denotes the closure of (g). Under the first assumption, $\mathrm{Spf}(R[[X]]/\overline{(g)})\cong\mathrm{Spec}(S)$ for some finite locally free R-algebra S. As the kernel commutes with base change in R, we get that for each $x\in\mathrm{Spec}(R)$

$$\dim_{k(x)}S\otimes_R k(x)=q^{\mathrm{ht}(f)}.$$

But the LHS of this expression is locally constant.

For the converse direction, we may assume that $\mathrm{ht}(f)$ is constant of value h. Then

$$g(X)=a_0+a_1X+\ldots+a_{q^h}X^{q^h}+\ldots$$

with $a_0,\ldots,a_{q^h-1}$ nilpotent in R, and $a_{q^h}\in R^\times$. We leave as an exercise to check that this implies that

$$R[[X]]/(g(X))$$

is free over R (on $1,X,\ldots,X^{q^h-1}$). This in turn implies that $\overline{(g)}=(g)$ and therefore

$$\ker(f)\cong\mathrm{Spec}(R[[X]]/(g))$$

as desired. □

The second property in Lemma 3.15 implies that isogenies are stable under composition.

The function $\mathrm{ht}(f)$ is always semicontinuous (its value may jump under specialization).

Lemma 3.16. *Let $R\in\mathrm{Alg}_A$ and $f\colon\mathcal{G}_1\to\mathcal{G}_2$ an isogeny of π-divisible formal A-modules over R. Then there exists some $n\geq 1$ and an isogeny $g\colon\mathcal{G}_2\to\mathcal{G}_1$ with*

$$g\circ f=[\pi^n],\ f\circ g=[\pi^n].$$

Proof. By Lemma 3.14 we may check this over R/I for some nilpotent ideal $I \subseteq R$. As f is an isogeny we can conclude that the morphism

$$\mathcal{G}_1 \to \mathcal{G}_2$$

is an epimorphism of fpqc-sheaves on Alg_R (this only uses that $R[[X]]/(f(X))$ is a finite, locally free faithfully flat R-algebra). In particular, $\mathcal{G}_1/\ker(f) \cong \mathcal{G}_2$. We claim that there exists some $n \geq 1$ such that

$$[\pi]^n(\ker(f)) = 0.$$

We may check this Zariski-locally on $\mathrm{Spec}(R)$ (as $\mathrm{Spec}(R)$ is quasi-compact), and thus assume the $\mathcal{G}_i$ arises from some formal A-module law $F_i \in R[[X,Y]], i = 1,2$. By Lemma 3.14 we may check this over R/I for some nilpotent ideal $I \subseteq R$. As $\mathcal{G}_1, \mathcal{G}_2$ are π-divisible (necessarily of the same height) we may find some nilpotent $I \subseteq R$ such that F_1, F_2 are of exact height h (in the sense of definition Definition 2.24). By Lemma 2.28 we may assume, by passing to a faithfully flat ind-étale R-algebra, that F_1, F_2 are normalized and hence by Theorem 2.29 isomorphic. By Lemma 2.31 we can then conclude that there exists some $n \geq 1$ and some $g\colon \mathcal{G}_2 \to \mathcal{G}_1$ such that $g \circ f = [\pi]^n$, which proves our claim. Knowing that $[\pi]^n(\ker(f)) = 0$ there exists some morphism $g\colon \mathcal{G}_2 \to \mathcal{G}_1$ factoring $[\pi^n]\colon \mathcal{G}_1 \to \mathcal{G}_1$ into $g \circ f$. Reducing modulo some nilpotent ideal, we may deduce that g is an isogeny by Lemma 3.15. As f is an epimorphism for the fpqc-topology we can deduce that $f \circ g = [\pi]$ as well because

$$f \circ g \circ f = f \circ [\pi^n] = [\pi^n] \circ f.$$

This finishes the proof. □

The converse of Lemma 3.16 holds true as well, if f, g are morphisms between π-divisible formal A-modules satisfying $f \circ g = [\pi^n]$, then f, g are isogenies. Indeed, by semicontinuity of $\mathrm{ht}(f), \mathrm{ht}(g)$ we can deduce that both functions are actually locally constant as the height function for π^n is.

Definition 3.17. *Let $R \in \mathrm{Nilp}_A$. A quasi-isogeny $f\colon \mathcal{G}_1 \dashrightarrow \mathcal{G}_2$ of π-divisible formal A-modules is an element of $\mathrm{Hom}_{\mathrm{FG}_{A(R)}}(\mathcal{G}_1, \mathcal{G}_2) \otimes_A K$ such that $\pi^n \cdot f$ is an isogeny for some $n \geq 1$.*

By Lemma 3.16 a quasi-isogeny is equivalently an isomorphism in the isogeny category of π-divisible formal A-modules, i.e., in the category with objects π-divisible formal A-modules and morphisms $\mathrm{Hom}_{\mathrm{FG}_{A(R)}}(\mathcal{G}_1, \mathcal{G}_2) \otimes_A K$.

Given an isogeny $f\colon \mathcal{G}_1 \to \mathcal{G}_2$ we get by Lemma 2.2 the function

$$\mathrm{ht}_f\colon \mathrm{Spec}(R) \to \mathbb{Z}_{\geq 0},\ x \mapsto ht(f \hat{\otimes}_R k(x)\colon \mathcal{G}_1 \hat{\otimes}_R k(x) \to \mathcal{G}_2 \hat{\otimes}_R k(x)),$$

which is locally constant and called the height of f. Given a quasi-isogeny $f\colon \mathcal{G}_1 \dashrightarrow \mathcal{G}_2$ we define the locally constant function

$$\mathrm{ht}_f = \mathrm{ht}_{\pi^n f} - \mathrm{ht}_{\pi^n}\colon \mathrm{Spec}(R) \to \mathbb{Z}$$

if $n \geq 1$ satisfies that $\pi^n \cdot f$ is an isogeny.

We can now present an alternative description of Lubin-Tate spaces. Fix a formal A-module $\mathcal{G}_h$ of height h and some $n \geq 1$. We define the functor

$$\mathcal{M}_{\mathrm{RZ},\mathcal{G}_h,n}\colon \mathrm{Nilp}_A \to (\mathrm{Sets})$$

which maps $R \in \mathrm{Nilp}_A$ to the set

$$\mathcal{M}_{\mathrm{RZ},\mathcal{G}_h,n}(R)$$

of isomorphism class of pair $(\mathcal{G}, \alpha)$ with $\mathcal{G}$ a π-divisible formal A-module over R and

$$\alpha \colon \mathcal{G}\hat{\otimes}_R R/\pi \dashrightarrow \mathcal{G}_h\hat{\otimes}_k R/\pi$$

a quasi-isogeny of constant height n, and a morphism $R \to S$ in Nilp_A to the natural pullback morphism. The formal A-module $\mathcal{G}_h$ is associated with some formal A-module law $F_h \in k[[X, Y]]$ of height h.

Proposition 3.18. *The functors $\mathcal{M}_{F_h}, \mathcal{M}_{\mathrm{RZ},\mathcal{G}_h,0}$ are naturally isomorphic.*

The "RZ" is an abbreviation for Rapoport-Zink as the definition of $\mathcal{M}_{\mathrm{RZ},\mathcal{G}_h,0}$ is for $A = \mathbb{Z}_p$ a particular case of a Rapoport-Zink space, cf. [RZ96].

Proof. Let $R \in \mathrm{Nilp}_A$. Given a $\star$-deformation $F \in R[[X, Y]]$ of F_h let $\mathcal{G}_F$ be the associated formal A-module. By Lemma 3.14 we can lift the identity $F \equiv F_h \bmod I$ for the unspecified nilpotent ideal $I \subseteq R$ to a quasi-isogeny

$$\alpha_F \colon \mathcal{G}\hat{\otimes}_R R/\pi \dashrightarrow \mathcal{G}_h\hat{\otimes}_k R/\pi.$$

This quasi-isogeny has height 0 as the height of quasi-isogenies is invariant under passage to quotients by nilpotent ideals. It is clear that we get a natural transformation

$$\mathcal{M}_{F_h} \to \mathcal{M}_{\mathcal{RZ},\mathcal{G}_h,0},\ F \mapsto (\mathcal{G}_F, \alpha_F).$$

Assume that $(\mathcal{G}, \alpha) \in \mathcal{M}_{\mathcal{RZ},\mathcal{G}_h,0}(R)$. Then there exists a nilpotent ideal $I \subseteq R$ such that

$$\alpha\hat{\otimes}_R R/I \colon \mathcal{G}\hat{\otimes}_R R/I \dashrightarrow G_h\hat{\otimes}_k R/I$$

is an isomorphism. Indeed, assume that $\pi^n\alpha = f$ is an isogeny. Then there exists a nilpotent ideal $I \in R$ containing π such that Zariski-locally on $\mathrm{Spec}(R)$ the isogeny f can be represented by a power series whose coefficients before the first invertible coefficient lie in I. As $\mathrm{ht}_\alpha = 0$ we can conclude by Lemma 2.2 that we can write Zariski-locally $f = [\pi]^n \circ g$ for some isomorphism

$$g \colon \mathcal{G}\hat{\otimes}_R R/I \cong \mathcal{G}_h\hat{\otimes}_k R/I.$$

By uniqueness of g these local morphisms glue to the required isomorphism. In particular, we can conclude (as I is nilpotent) that $\mathrm{Lie}(\mathcal{G})$ is free and therefore $\mathcal{G}$ is associated to some formal A-module law $F \in R[[X, Y]]$. Doing a coordinate transform via some lift of the power series representing α, we can arrange that $F \equiv F_h \bmod I$. This proves surjectivity of

$$\mathcal{M}_{F_h}(R) \to \mathcal{M}_{\mathcal{RZ},\mathcal{G}_h,0}(R).$$

Injectivity follows from Lemma 3.14. □

Note that by passing to quasi-isogenies the unspecified nilpotent ideal in the definition of $\mathcal{M}_{F_h}$ disappeared. From the viewpoint of Rapoport-Zink spaces it is more natural to consider the space

$$\mathcal{M}_{\mathrm{RZ},\mathcal{G}} \cong \coprod_{n\in\mathbb{Z}} \mathcal{M}_{\mathrm{RZ},\mathcal{G},n},$$

which parametrizes formal A-modules $\mathcal{G}$ together with a quasi-isogeny

$$\alpha \colon \mathcal{G}\hat{\otimes}_R R/\pi \dashrightarrow \mathcal{G}_h\hat{\otimes}_k R/\pi$$

of arbitrary height. Clearly, the full group of quasi-isogenies of $\mathcal{G}_h$ acts on $\mathcal{M}_{\mathrm{RZ},\mathcal{G}}$ (and not just the isomorphisms).

3.3. **Invariant differentials.** We introduce now invariant differentials on formal A-modules.

Let S be any ring. Given the formal scheme $Z \cong \mathrm{Spf}(S[[X_1,\dots,X_n]])$ we define its (continuous) de Rham complex $\hat{\Omega}^\bullet_{Z/\mathrm{Spec}(S)}$ as the complex

$$\mathcal{O}_Z(Z) = S[[X_1,\dots,X_n]] \xrightarrow{d} \hat{\Omega}^1_{Z/\mathrm{Spec}(S)} := \bigoplus_{i=1}^n S[[X_1,\dots,X_n]]dX_i \xrightarrow{d} \hat{\Omega}^2_{Z/\mathrm{Spec}(R)} \to \dots,$$

where d denotes the exterior derivative of differentials. One checks that up to a canonical isomorphism the terms of this complex and the differential do depend only on Z and not the chosen isomorphism $\mathcal{O}_Z(Z) \cong S[[X_1,\dots,X_n]]$). In particular, we can glue these local complexes in the case that $Z \cong \mathrm{Spf}(S[[M]]))$ is a formal Lie variety with $M \cong T_0 Z$ a finite projective S-module. Given formal Lie varieties Z_1, Z_2 and a morphism $f\colon Z_1 \to Z_2$ of formal schemes over $\mathrm{Spec}(S)$ the pullback of differentials defines a morphism

$$f^*\colon \hat{\Omega}^\bullet_{Z_2/\mathrm{Spec}(S)} \to \hat{\Omega}^\bullet_{Z_1/\mathrm{Spec}(S)}$$

of complexes.

Assume now that A is a complete discrete valuation ring with finite residue field and that $R = S$ is an A-algebra. Let $\mathcal{G} \to \mathrm{Spec}(R)$ be a (one-dimensional) formal A-module. Let

$$m, \mathrm{pr}_1, \mathrm{pr}_2\colon \mathcal{G} \times_{\mathrm{Spec}(R)} \mathcal{G} \to \mathcal{G}$$

be the multiplication resp. first and second projection. We call a differential

$$\omega \in \Omega^1_{\mathcal{G}/\mathrm{Spec}(R)}$$

invariant if

$$m^*\omega = \mathrm{pr}_1^*\omega + \mathrm{pr}_2^*\omega \in \hat{\Omega}^1_{\mathcal{G}\times_{\mathrm{Spec}(R)}\mathcal{G}/\mathrm{Spec}(R)},$$

Let

$$\omega(\mathcal{G}) \subseteq \hat{\Omega}^1_{\mathcal{G}/\mathrm{Spec}(R)}$$

be the R-submodule of invariant differentials. For example, the differentials

$$dX, \quad \text{resp. } \frac{dX}{1+X}$$

on the formal $\mathbb{Z}_p$-modules $\hat{\mathbb{G}}_a$, resp. $\hat{\mathbb{G}}_m$ are invariant.

Given a morphism $f\colon \mathcal{G}_1 \to \mathcal{G}_2$ of formal A-modules and $\omega \in \omega(\mathcal{G}_2)$, then $f^*\omega \in \omega(\mathcal{G}_1)$ as is easily checked.

Lemma 3.19. *The R-module $\omega(\mathcal{G})$ is locally free of rank 1, canonically isomorphic to*

$$\mathrm{Lie}(\mathcal{G})^\vee := \mathrm{Hom}_R(\mathrm{Lie}(\mathcal{G}), R)$$

and $\mathcal{O}_\mathcal{G}(\mathcal{G}) \otimes_R \omega(\mathcal{G}) \cong \hat{\Omega}^1_{\mathcal{G}/\mathrm{Spec}(R)}$ via the natural morphism $f \otimes \omega \mapsto f \cdot \omega$. If $\omega \in \omega(\mathcal{G})$ and $a \in A$, then $[a]^*\omega = a\omega$.

Proof. First assume that $\mathcal{G} = \mathcal{G}_F$ for some formal A-module law F. Then we are seeking

$$\omega(X) = f(X)dX \in \hat{\Omega}^1_{\mathcal{G}/\mathrm{Spec}(R)}$$

such that

$$f(F(X,Y))d(F(X,Y)) = f(X)dX + f(Y)dY.$$

The first equation is equivalent to

$$f(F(X,Y))\frac{\partial F}{\partial X}F(X,Y) = f(X),\ f(F(X,Y))\frac{\partial F}{\partial Y}F(X,Y) = f(Y). \tag{11}$$

Setting $X = 0$ in the first yields

$$f(Y)\frac{\partial F}{\partial X}(0,Y) = f(0).$$

As $\frac{\partial F}{\partial X}(0,Y) \equiv 1 \bmod (X,Y)$ we get

$$f(Y) = \frac{f(0)}{\frac{\partial F}{\partial X}(0,Y)}.$$

In particular, each invariant differential $\omega(X) = f(X)d(X)$ is determined by $f(0)$. Let us check that the differential

$$\omega_F := \frac{dX}{\frac{\partial F}{\partial X}(0,X)}$$

is invariant. Taking the Z-derivative of $F(Z,F(X,Y)) = F(F(Z,X),Y)$ yields

$$\frac{\partial F}{\partial X}(Z,F(X,Y)) = \frac{\partial F}{\partial X}(F(Z,X),Y)\frac{\partial F}{\partial X}(Z,X).$$

Setting $Z = 0$ proves invariance of ω_F. Let $a \in A$. As $[a]\colon \mathcal{G} \to \mathcal{G}$ is an endomorphism of the formal group $\mathcal{G}$, the differentials

$$[a]^*\omega = a\omega$$

are invariant. As $[a](X) = aX \bmod (X^2)$ the coefficients of dX agree for both. Hence, both differentials have to be equal. The pairing

$$\omega(\mathcal{G}) \times \mathrm{Lie}(\mathcal{G}) \to R,\ (\omega = h(X)dX, \psi\colon (X)/(X)^2 \to R) \mapsto \psi(h(X)X \bmod (X)^2)$$

is A-linear and invariant under substituting X by some $g(X) \in R[[X]]$ with $g(0) = 0, g'(0) \in R^\times$. We can conclude that both claims extend by Zariski glueing to arbitrary formal A-modules over $\mathrm{Spec}(R)$. □

If $\mathcal{G} = \mathcal{G}_F$ for some formal A-module law F we note that the generator

$$\frac{1}{\frac{\partial F}{\partial X}(0,X)}dX \in \omega(\mathcal{G})$$

depends on F, and not just on $\mathcal{G}$. Let K be the fraction field of A. Recall that for any π-torsion free A-algebra R and $\mathcal{G} = \mathcal{G}_F$ the formal A-module associated with some formal A-module law $F \in R[[X,Y]]$, there exists a unique series, the "logarithm of F",

$$\log_F(X) \in (R \otimes_A K)[[X]]$$

such that

$$\log_F(0) = 0,\ \log_F'(0) = 1,\ \log_F(F(X,Y)) = \log_F(X) + \log_F(Y),$$

Lemma 2.23. In other words, $\log_F$ defines an isomorphism of

$$\mathcal{G}\hat{\otimes}_R(R \otimes_A K) \cong \widehat{\mathbb{G}}_{a,R\otimes_A K}.$$

As the differential dX is invariant on $\widehat{\mathbb{G}}_a$, we can conclude that

$$\log_F^*(dX) = d(\log_F(X)) = \log_F'(X)dX = \frac{1}{\frac{\partial F}{\partial X}(0,X)}dX$$

by comparing the coefficient of dX. In particular,

$$\log_F'(X) = \frac{1}{\frac{\partial F}{\partial X}(0,X)}$$

has coefficients in R.

4. Adic spaces

Formal schemes are not enough for our purpose as (naively) we cannot take their "generic fiber". Let us mention a typical operation that we would like to do. Let A be a complete discrete valuation ring, $\pi \in A$ a uniformizer. Then we get

$$\mathrm{Spf}(A) \subseteq \mathrm{Spec}(A)$$

and the base change of $\mathrm{Spec}(A[T])$ along this morphism is corepresented by the π-adic completion

$$A\langle T\rangle := \{f(T) = \sum_{i=0}^{\infty} \in A[[T]] \mid |a_i| \to 0,\ i \to \infty\}$$

of $A[T]$. Now the "rigid-analytic generic fiber" of $\mathrm{Spf}(A\langle T\rangle)$ should be corepresented by the $K := \mathrm{Frac}(A)$-algebra

$$K\langle T\rangle := A\langle T\rangle \otimes_A K.$$

The ring $K\langle T\rangle$ is no longer admissible. For this reason we have to enlarge our test category, and to discuss Huber rings.

4.1. **Huber rings.**

We now introduce Huber rings, which form the building block for Huber's category of adic spaces. References for Huber rings etc. are [Hub93][Hub94], [SW20], [Mor19].

Definition 4.1. *A Huber ring is a topological ring A for which there exists an open subring $A_0 \subseteq A$ whose subspace topology is I-adic for some finitely generated ideal $I \subseteq A_0$. Any such subring A_0 is called a ring of definition.*

The finite generation of I is important, e.g., to get that I-adic completions are well-behaved, cf. [Sta17, Tag 05GG].

Example 4.2. Let us give examples of Huber rings.

(1) Any discrete ring A is Huber with any subring a ring of definition (with $I = \{0\}$). This example relates to classical schemes.
(2) If A is any ring, $I \subseteq A$ a finitely generated ideal, then A with its I-adic topology is Huber. The example relates to formal schemes.
(3) Let A_0 be any ring, $g \in A_0$ a non-zero divisor and $A := A_0[1/g]$. Then we can make A into a topological group by requiring that $\{g^n A_0\}_{n\geq 0}$ is a fundamental system of open neighborhoods of 0. For this topology A is in fact a topological ring as one checks that multiplication by g is continuous. This example relates to rigid-analytic varieties.
(4) More concretely, let $(K, |-|)$ be a non-archimedean valued field and let $(A, |-|)$ be a (non-archimedean) Banach algebra over K. Then

$$A_0 := \{a \in A \mid |a| \leq 1\}$$

is a subring. If there exists an element $g \in K$ with $0 < |g| < 1$, then the subspace topology on A_0 is (g)-adic and $A = A_0[1/g]$.

The following exercise yields the main example from rigid-analytic geometry.

Exercise 4.3. Let K be a non-archimedean valued field with (multiplicative) valuation $|-|\colon K \to \mathbb{R}_{\geq 0}$. Define

$$K\langle T\rangle := \{\sum_{i=0}^{\infty} a_i T^i \mid |a_i| \to 0, i \to \infty\}.$$

Show that

$$|\sum_{i=0}^{\infty} a_i T^i| := \max\{|a_i| \mid i \geq 0\}$$

is a norm on $K\langle T\rangle$, and that $K\langle T\rangle$ is complete for this norm.

Similarly, we can define the Tate algebra $K\langle T_1, \ldots, T_n\rangle$ for $n \geq 1$.

Definition 4.4. *Let A be a topological ring. A subset $S \subseteq A$ is called bounded if for any open neighborhood U of 0 there exists an open neighborhood V of 0, such that $\{v \cdot s \mid v \in V, s \in S\} \subseteq U$.*

For example, in Item 3 a subset $S \subseteq A = A_0[1/g]$ is bounded if and only if $S \subseteq 1/g^n A_0$ for some $n \geq 0$.

Lemma 4.5. *Let A be a Huber ring, and $A_0 \subseteq A$ a subring. Then the following are equivalent:*

1. *A_0 is a ring of definition,*
2. *A_0 is open in A and adic, i.e., its subspace topology is adic,*
3. *A_0 is open and bounded.*

Proof. Clearly, 1) $\Rightarrow$ 2). If A_0 is open and adic, then there exists a fundamental system of neighborhoods of 0 in A_0, which are ideals. This implies boundedness of A_0. Thus, 2) $\Rightarrow$ 3). Let us prove 3) $\Rightarrow$ 1). Let $B \subseteq A$ be ring of definition, and let $J = (\pi_1, \ldots, \pi_n) \subseteq B$ be a finitely generated ideal of definition. Let

$$T := \{\pi_1, \ldots, \pi_n\}.$$

For $k \geq 1$ set

$$T(k) := \{t_1 \cdots t_k \mid t_i \in T\}.$$

Note that

$$J^{k+1} = T(k) \cdot J$$

for $k \geq 1$. As A_0 is open, there exists some $k \geq 1$, such that

$$T(k) \subseteq J^k \subseteq A_0.$$

Set

$$I := T(k) \cdot A_0.$$

Take $l \geq 1$, such that $J^l \subseteq A_0$. Then

$$I^n = T(nk)A_0 \supseteq T(nk)J^l = J^{nk+l},$$

i.e., $I^n \subseteq A_0$ is open. Let $V \subseteq A_0$ be an open neighborhood of 0. Then there exists some $m \geq 1$, such that

$$J^{mk} A_0 \subseteq V$$

as A_0 is bounded. Then

$$I^m = T(mk)A_0 \subseteq T(mk-1)J \cdot A_0 = J^{mk} A_0 \subseteq V,$$

which proves that the subspace topology on A_0 is I-adic. As by construction I is finitely generated, A_0 is a ring of definition. $\square$

Definition 4.6. *Let A be a Huber ring. Then an element $a \in A$ is power bounded if $\{a^n \mid n \geq 0\} \subseteq A$ is a bounded subset. We let*

$$A^\circ \subseteq A$$

be the subset of power bounded elements.

For example, if p is a prime and $A = \mathbb{Q}_p[T]/(T^2)$ (with ring of definition $\mathbb{Z}_p[T]/(T^2)$ and ideal of definition (p)), then

$$A^\circ = \mathbb{Z}_p + T\mathbb{Q}_p.$$

Lemma 4.7. *Let A be a Huber ring.*

1. *The subset $A^\circ \subseteq A$ of power bounded elements is a subring.*
2. *A° is the filtered union of all rings of definition $A_0 \subseteq A$. In particular, each ring of definition $A_0 \subseteq A$ is contained in A°.*

Proof. Clearly, each ring of definition $A_0 \subseteq A$ is contained in A° as A_0 is bounded. We first prove that if $A_0, A_0' \subseteq A$ are rings of definition, then the ring $B := A_0 \cdot A_0'$ generated by them is again a ring of definition. By Lemma 4.5 it suffices to see that B is bounded. Let $U \subseteq A$ be an open neighborhood of 0. By definition of an Huber ring, we may assume that U is a subgroup. As A_0, A_0' are bounded there exist open neighborhoods $V_1, V_2 \subseteq A$, which are subgroups, such that

$$V_1 \cdot A_0' \subseteq U$$

and

$$V_2 \cdot A_0 \subseteq V_1.$$

We can conclude that

$$V_2 \cdot B \subseteq V_2 \cdot A_0 \cdot A_0' \subseteq V_1 \cdot A_0' \subseteq U,$$

which proves that B is bounded. The same argument with A_0' replaced by the bounded set $\{x^n\}_{n \geq 0}$ for $x \in A^\circ$ implies that each power bounded element lies in some ring of definition. This finishes the proof. □

Definition 4.8. *Let A be a Huber ring. An element $a \in A$ is called topologically nilpotent if $a^n \to 0$ for $n \to \infty$. We let*

$$A^{\circ\circ} \subseteq A$$

be the subset of topologically nilpotent elements.

We leave it as an exercise to see that $A^{\circ\circ} \subseteq A^\circ$ is an ideal. If $A_0 \subseteq A$ is a ring of definition with ideal of definition $I \subseteq A_0$, then $\sqrt{I} \subseteq A^{\circ\circ}$ and $A^{\circ\circ}$ is the union of those. In particular, $A^{\circ\circ} \subseteq A$ is open.

Of particular importance are pseudo-uniformizers.

Definition 4.9. *Let A be a Huber ring. A topologically nilpotent unit $x \in A$ is called a pseudo-uniformizer. A Huber ring possessing a pseudo-uniformizer is called a Tate-Huber ring.*

Note that x is invertible in A, but never in any ring of definition (except $A = \{0\}$). For example, let A, A_0, g be as in Item 3. Then $A = A_0[1/g]$ is Tate and $g \in A$ a pseudo-uniformizer.

Conversely, each Tate-Huber ring is of this form.

Lemma 4.10. *Let A be a Tate-Huber ring, and $A_0 \subseteq A$ a ring of definition. Let $x \in A$ be a pseudo-uniformizer. Then $g := x^n \in A_0$ for some $n \geq 0$. Moreover, the subspace topology in A_0 is the (g)-adic topology and $A = A_0[1/g]$.*

Proof. Let $I \subseteq A_0$ be an ideal of definition. As I is an open neighborhood of 0 and $x^n \to 0, n \to \infty$, we can conclude that $x^n \in I$ for some $n \geq 0$. Choose such an n and set $g := x^n$. The multiplication by g is a homeomorphism on A. In particular, $g \cdot A_0$ is open in A, and hence in A_0 as $gA_0 \subseteq A_0$. In particular, there exists some $m \geq 0$ such that $I^m \subseteq gA_0$. As $gA_0 \subseteq I$, we see that the I-adic and (g)-adic topologies on A_0 agree. Let us show that $A = A_0[1/g]$ and pick any $a \in A$ for this. As g is topologically nilpotent, we can conclude that $g^n a \to 0, n \to \infty$. In particular, there exists $n \geq 0$ such that

$$g^n a \in A_0.$$

This proves that $a \in A_0[1/g] \subseteq A$ as desired. □

Let A be a discrete valuation ring with fraction field K and let $\pi \in A$ be a uniformizer. From Lemma 4.10 we can conclude that there exists no topology on

$$A[[T]][1/\pi]$$

making $A[[T]]$ an open subring whose topology is (π, T)-adic.

Definition 4.11. *Let A be a Huber ring. An open, integrally closed subring $A^+ \subseteq A$ is called a ring of integral elements if $A^+ \subseteq A^\circ$. A Huber pair is pair (A, A^+) of a Huber ring A and a subring $A^+ \subseteq A$ of integral elements. A morphism $(A, A^+) \to (B, B^+)$ of Huber pairs is a continuous ring homomorphism $A \to B$ sending A^+ to B^+.*

Lemma 4.12. *Let A be a Huber ring. Then $A^\circ \subseteq A$ is a ring of integral elements. Moreover, each ring of integral elements $A^+ \subseteq A$ contains $A^{\circ\circ}$ and $A^+ \mapsto A^+/A^{\circ\circ}$ defines a bijection between ring of elements in A and integrally closed subrings of $A^\circ/A^{\circ\circ}$.*

In particular, rings of integral elements exist in abundance.

Proof. We have to check that A° is integrally closed in A. But if $x \in A$ satisfies

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

with $a_1, \ldots, a_n \in A^\circ$, then x is again power bounded, i.e., lies in A°. Now let $A^+ \subseteq A$ be any ring of integral elements, and $x \in A^{\circ\circ}$. As A^+ is open there exists some $n \geq 0$ such that $x^n \in A^+$. As A^+ is integrally closed we can conclude that $x \in A^+$, i.e., $A^{\circ\circ} \subseteq A^+$. Let $D \subseteq A^\circ/A^{\circ\circ}$ be any subring with preimage $B \subseteq A^\circ$. Then an element $z \in A^\circ/A^{\circ\circ}$ is integral over D if and only if some preimage of it in A° is integral over B (as one can adjust the constant term by an element in $A^{\circ\circ}$). This proves the last assertion. □

From Lemma 4.7 we can conclude that each ring of integral elements is the filtered union of the rings of definition, which are contained in it. Lemma 4.12 implies that the an arbitrary intersection of rings of elements is again a ring of integral elements.

4.2. **Valuation spectra.** We want to associate a topological space of (continuous) valuations

$$\mathrm{Spa}(A, A^+)$$

to any Huber pair (A, A^+).

Definition 4.13. *A totally ordered abelian group is an abelian group Γ together with a total order $\leq$ on it such that for all $a, b, c \in \Gamma$ with $a \leq b$ we have*

$$a + c \leq b + c.$$

Clearly, subgroups of totally ordered abelian groups with the induced order are again totally ordered abelian groups, e.g., the trivial group $\{1\}$.

Example 4.14. Let us give examples of totally ordered abelian groups.

(1) $(\mathbb{R}, +)$ with its usual order is a totally ordered abelian group. The logarithm and exponential define mutually inverse isomorphisms

$$(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$$

of totally ordered abelian groups.

(2) Let I be any well-ordered set, e.g., $I = \{1, 2, \ldots, n\}$ with the natural order, and $\Gamma_i, i \in I$, a family of totally ordered abelian groups (each written multplicatively). Then the product

$$\prod_{i \in I} \Gamma_i$$

admits the lexicographic order: Let $a := (\gamma_i)_{i \in I}, b := (\gamma_i')_{i \in I} \in \prod_{i \in I} \Gamma_i$ be two distinct elements and let $i_0 \in I$ be the minimal element such that $\gamma_i \neq \gamma_i'$. Then set $a \leq b$ if $\gamma_{i_0} \leq \gamma_{i_0}$.

For a totally ordered abelian group Γ (written multiplicatively) we define the totally ordered abelian monoid

$$\Gamma \cup \{0\}$$

by setting $\gamma \cdot 0 := 0$ and $0 < \gamma$ for $\gamma \in \Gamma$.

We now present a huge generalization of the definition of the (multiplicative) valuations discussed in Section 1.2.

Definition 4.15. *Let A be any ring. A (multiplicative) valuation on A is a map*

$$|-| \colon A \to \Gamma \cup \{0\}$$

with Γ some totally ordered abelian group such that

(1) $|0| = 0, |1| = 1$,
(2) $|a \cdot b| = |a| \cdot |b|$
(3) $|a + b| \leq \max\{|a|, |b|\}$

for $a, b \in A$.

The support of a valuation $|-|$ is the prime ideal

$$\mathrm{supp}(|-|) := |-|^{-1}(\{0\}).$$

Two valuations

$$|-| \colon A \to \Gamma \cup \{0\}, \ |-|' \colon A \to \Gamma' \cup \{0\}$$

are equivalent if for all $a, b \in A$ we have

$$|a| \leq |b| \text{ if and only if } |a|' \leq |b|'.$$

Let us note that the same proof as in Lemma 1.4 works and thus each valuation satisfies the strong triangle inequality

$$|a+b| = \max\{|a|, |b|\}$$

if $|a| \neq |b|$ for $a, b \in A$. If A is a topological ring, then it makes sense to impose a continuity condition on the valuations.

Definition 4.16. *Let A be a topological ring. A valuation $|-|\colon A \to \Gamma \cup \{0\}$ is called continuous if for all $a \in A$ with $|a| \neq 0$ the set*

$$\{b \in A \mid |b| < |a|\}$$

is open in A.

We don't demand $\leq$ as we want that trivial valuations (i.e., those with $\Gamma = \{1\}$) have open prime ideals as support. In general the support of a continuous valuation is a closed prime ideal as it is an intersection of open, hence closed, subgroups. Note that the condition of continuity only depends on the equivalence class of $|-|$.

Definition 4.17. *Let (A, A^+) be Huber pair. We set*

$$\mathrm{Spa}(A, A^+)$$

as the set of equivalence classes of continuous valuations $|-|\colon A \to \Gamma \cup \{0\}$ for Γ some arbitrary totally ordered abelian group such that

$$|a| \leq 1$$

for all $a \in A^+$.

We will occasionally replace the A^+ in Definition 4.17 by any subset $S \subseteq A$ and write

$$\mathrm{Spa}(A, S)$$

for the equivalence classes of continuos valuations $|-|\colon A \to \Gamma \cup \{0\}$ such that $|a| \leq 1$ for $a \in S$. We leave it as an exercise to see that $\mathrm{Spa}(A, S) = \mathrm{Spa}(A, A^+)$ for A^+ the smallest ring of integral elements in A, which contains S. We also use the short notation $\mathrm{Spa}(A)$ for $\mathrm{Spa}(A, A^\circ)$, and

$$\mathrm{Spv}(A, S)$$

for the Spa of the underlying discrete ring A with its subset $S \subseteq A$ (which only depends on the integral closed subring generated by S, which may not be open).

We will use the following convenient notation: If $x \in \mathrm{Spa}(A, A^+)$ is the equivalence class of the valuation $|-|\colon A \to \Gamma \cup \{0\}$, then we write

$$|f(x)| := x(f) = |f| \in \Gamma \cup \{0\}.$$

for $f \in A$.

We now define a topology on $\mathrm{Spa}(A, A^+)$.

Definition 4.18. *For $f_1, \ldots, f_n, g \in A$ set*

$$U(\frac{f_1, \ldots, f_n}{g}) := \{x \in \mathrm{Spa}(A, A^+) \mid |f_i(x)| \leq |g(x)| \neq 0,\ i = 1, \ldots, n\}$$

The colletion of subsets $U(\frac{f_1,\dots,f_n}{g}) \subseteq \mathrm{Spa}(A,A^+)$ for $f_1,\dots,f_n,g \in A$ is stable under intersections because

$$U(\frac{f_1,\dots,f_n}{g}) \cap U(\frac{f_1',\dots,f_m'}{g'}) = U(\frac{f_1g',\dots,f_ng',f_1'g,\dots,f_m'g}{gg'}),$$

and hence they form the basis of a topology on $\mathrm{Spa}(A,A^+)$. If $\varphi\colon (A,A^+) \to (B,B^+)$ a morphism of Huber pairs, then

$$|-| \mapsto |-| \circ \varphi$$

defines a continuous map.

$$h\colon \mathrm{Spa}(B,B^+) \to \mathrm{Spa}(A,A^+)$$

Indeed,

$$h^{-1}(U(\frac{f_1,\dots,f_n}{g})) = U(\frac{\varphi(f_1),\dots,\varphi(f_n)}{\varphi(g)})$$

for $f_1,\dots,f_n,g \in B$.

Before giving examples let us describe $\mathrm{Spa}(A,A^+)$ via valuation rings. Given $x \in \mathrm{Spa}(A,A^+)$ with (equivalence class of the) valuation

$$|-|\colon A \to \Gamma \cup \{0\}$$

let

$$k(x) := \mathrm{Frac}(A/\mathrm{supp}(|-|))$$

be the "residue field of $\mathrm{Spa}(A,A^+)$ at x". The valuation $|-|$ extends naturally to a valuation

$$|-|_x\colon k(x) \to \Gamma \cup \{0\},$$

and

$$k(x)^+ := \{a \in k(x) \mid |a|_x \leq 1\}$$

is a valuation ring (with fraction field $k(x)$) in the sense of the following definition.

Definition 4.19. *A valuation ring is an integral domain R such that for each non-zero $x \in K := \mathrm{Frac}(R)$ we have $x \in R$ or and $x^{-1} \in R$.*

It is not difficult to see that if R is a valuation ring, then R is a local ring with maximal ideal

$$\mathfrak{m}_R := \{x \in R \mid x = 0 \text{ or } x^{-1} \notin R\}.$$

Moreover, each subring $S \subseteq K$ containing R is again a valuation ring, equal to the localization of R at the prime ideal $\mathfrak{m}_S \cap R$, and that the ideals in R are linearly ordered. The last point characterizes valuation rings as those integral domains whose set of ideals is linearly ordered via inclusion.

Valuation rings yield valuations.

Lemma 4.20. *Let R be a valuation ring and $K := \mathrm{Frac}(R)$ its fraction field. Set $\Gamma := K^\times/R^\times$. Let us write $\gamma \leq \eta$ for $\gamma,\eta \in \Gamma$ if $\gamma = x\eta$ for some $x \in R$. Then $(\Gamma,\leq)$ is a totally ordered abelian group and the natural projection*

$$|-|\colon K \to \Gamma \cup \{0\}$$

is a valuation whose associated valuation ring is R.

Proof. We leave the verification as an exercise. □

If Γ is a totally ordered abelian group, then the group algebra $\mathbb{Z}[\Gamma]$ has the natural (surjective) valuation

$$|-|\colon \mathbb{Z}[\Gamma] \to \Gamma \cup \{0\},\ \sum_{\gamma\in\Gamma} a_\gamma \gamma \mapsto \sup\{\gamma \mid a_\gamma \neq 0\}$$

and thus each totally ordered abelian group arises via Lemma 4.20.

From Lemma 4.20 it is easy to deduce that the ideals in a valuation ring are linearly ordered, the finitely generated ideals are principal, and moreover that radical ideals in valuation rings are prime.

Given a valuation ring we call its Krull dimension the rank of the associated valuation. If K is a field let us call a subring $R \subseteq K$ a valuation subring of K if R is a valuation ring with fraction field K.

As a corollary we get another description of $\mathrm{Spa}(A, S)$ for a discrete ring A and a subset $S \subseteq A$.

Corollary 4.21. *Let A be a (discrete) ring and $S \subseteq A$ a subset. The map*

$$x \mapsto (\mathrm{supp}(x), k(x)^+)$$

defines a bijection from $\mathrm{Spa}(A, S)$ *to the set of pairs*

$$(\mathfrak{p}, R)$$

with $\mathfrak{p} \subseteq A$ a prime ideal, $R \subseteq k(\mathfrak{p}) := \mathrm{Frac}(A/\mathfrak{p})$ a valuation subring such that R contains the image of S under $A \to k(\mathfrak{p})$.

Proof. This follows from Lemma 4.20. □

Phrased differently, the map

$$\mathrm{supp}\colon \mathrm{Spa}(A, S) \to \mathrm{Spec}(A)$$

has fiber over $\mathfrak{p}$ given by the set of valuation subrings in $k(\mathfrak{p})$ containing the image of S. The map supp admits a section

$$s\colon \mathrm{Spec}(A) \to \mathrm{Spa}(A, S)$$

sending $\mathfrak{p}$ to the trivial valuation $A \to k(\mathfrak{p}) \to \{1\} \cup \{0\}$ (or equivalently to the pair $(\mathfrak{p}, k(\mathfrak{p}))$). Both maps supp, s are continuous. Indeed, if $f, f_1, \ldots, f_n, g \in A$, then

$$\mathrm{supp}^{-1}(D(f)) = U(\frac{0}{f})$$

and

$$\mathrm{s}^{-1}(U(\frac{f_1, \ldots, f_n}{g})) = D(g).$$

Usually the fibers of supp are huge, and exactly the Riemann-Zariski spaces

$$\mathrm{Spa}(K, B)$$

for a (discrete) field K and a subring $B \subseteq K$. Note that for $f_1, \ldots, f_n, g \in K$ we get that

$$U(\frac{f_1, \ldots, f_n}{g})$$

identifies with the set of valuation subrings $R \subseteq K$ containing $B[\frac{f_1}{g}, \ldots, \frac{f_n}{g}]$, i.e.,

$$U(\frac{f_1, \ldots, f_n}{g}) = \mathrm{Spa}(K, B[\frac{f_1}{g}, \ldots, \frac{f_n}{g}]).$$

Example 4.22. Let us give some examples of adic spectra for discrete rings.

(1) By Ostrowski's theorem

$$\mathrm{Spa}(\mathbb{Q},\mathbb{Z}) = \{x_{\mathbb{Q}}, x_p \mid p \text{ prime}\}$$

with $x_{\mathbb{Q}}$ the trivial valuation on $\mathbb{Q}$ (corresponding to the valuation ring $\mathbb{Q} \subseteq \mathbb{Q}$), and $x_p = |-|_p \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ the (multplicative) p-adic norm (corresponding to the valuation subring $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$). The topological space $\mathrm{Spa}(\mathbb{Q},\mathbb{Z})$ is homeomorphic to $\mathrm{Spec}(\mathbb{Z})$.

(2) We can deduce

$$\mathrm{Spa}(\mathbb{Q},\mathbb{Z}) = \{x_{\mathbb{Q}}, x_p, x_{\mathbb{F}_p} \mid p \text{ prime}\}$$

with $x_{\mathbb{Q}}, x_p$ as before and $x_{\mathbb{F}_p}$ the trivial valuation $\mathbb{Z} \to \mathbb{F}_p \to \{0,1\}$ (corresponding to the valuation ring $\mathbb{F}_p \subseteq \mathbb{F}_p$).

(3) Let R be a valuation ring with fraction field K. Then the map

$$\varphi \colon \mathrm{Spa}(K,R) \to \mathrm{Spec}(R),\ |-| \mapsto \{a \in R \mid |a| < 1\}$$

is a homeomorphism. Indeed, as was mentioned after Definition 4.19 each valuation subring $S \subseteq K$ containing R is the localization $R_{\mathfrak{p}}$ of R at the prime ideal $\mathfrak{m}_S \subseteq R$, and conversely each localization of R at a prime ideal is a valuation ring. If $\mathfrak{p} \subseteq R$ is a prime ideal and $f \in R$, then $f \notin \mathfrak{p} = \mathfrak{p}R_{\mathfrak{p}}$ if and only if $f \in R_{\mathfrak{p}}$ and $1/f \in R_{\mathfrak{p}}$. In particular, $\varphi^{-1}(D(f)) = U(\frac{f}{1}) \cap U(\frac{1}{f})$ and φ is continuous. Conversely, let $f, g \in R$. If $f/g \in R$, then $U(\frac{f}{g}) = \mathrm{Spa}(K,R)$ and $\varphi(U(\frac{f}{g})) = \mathrm{Spec}(R)$. If $f/g \notin R$, then $g/f \in R$ and $|g(x)| \leq f(x)| \neq 0$ for $x \in \mathrm{Spa}(K,R)$. This implies that $U(\frac{f}{g}) = U(\frac{f}{g}) \cap U(\frac{g}{f}) = \varphi^{-1}(D(g/f))$.

(4) Let k be a field and K/k a field extension of finite transcendence degree. Then by the valuative criterion for properness

$$\mathrm{Spa}(K,k) \cong \varprojlim_{X/k} |X|$$

(as topological spaces) with the (cofiltered) inverse limit running over all integral proper k-schemes X with generic point identified with $\mathrm{Spec}(K)$. By the existence of blow-ups we see that $\mathrm{Spa}(K,k)$ is very huge if K has transcendence degree ≥ 2. If $\mathrm{trdeg}(K/k) = 1$, then $\mathrm{Spa}(K,k) \cong |X|$ for X the unique (up to isomorphism) normal, integral projective curve over k with field of functions K.

(5) Let us describe a way to produce valuations of higher rank. For this, let R be an arbitrary valuation ring with field of fractions K and residue field k. Let

$$\varphi \colon R \to k$$

be the natural projection. The maps $S \mapsto \varphi(S)$ and $B \mapsto \varphi^{-1}(B)$ define mutually inverse bijections between the set of valuation subrings $S \subseteq K$ contained in R and the set $\mathrm{Spa}(k,\{0\})$ of valuation subrings of k.

(6) Concretely consider a field L and set

$$R := L((x))[[t]] \subseteq K := L((x))((t)).$$

Then $B := L[[x]] \subseteq R/(t)$ is a valuation ring and

$$S = \{\sum_{i=0}^{\infty} a_i t^i \in R \mid a_0 \in L[[x]]\}$$

a valuation subring of rank 2 in K. The associated valuation can be described as follows: Consider $\Gamma = (1/2)^{\mathbb{Z}} \oplus \varepsilon^{\mathbb{Z}}$ with the lexicographic order such that ε is infinitesimally less than 1. Then

$$K \to \Gamma \cup \{0\},\ \sum_{i,j} a_{i,j} x^i t^j \mapsto \max\{(1/2)^j \varepsilon^i \mid a_{i,j} \neq 0\}.$$

Let us rephrase the continuity of valuations in terms of valuation rings. For this let us say that an element $\gamma \in \Gamma \cup \{0\}$ is cofinal, or topologically nilpotent, if for any $\delta \in \Gamma$ there exists an $n \geq 1$, such that $\gamma^n < \delta$. For example, in the totally ordered abelian group

$$\Gamma = (1/2)^{\mathbb{Z}} \oplus \varepsilon^{\mathbb{Z}}$$

appearing in Example 4.22 $1/2$ is cofinal, but ε not. Similarly, let us say that an element in the fraction field K of a valuation ring R is cofinal, or topologically nilpotent, if its class in $K^\times/R^\times \cup \{0\}$ is cofinal. Clearly, each cofinal element lies in $\mathfrak{m}_R$.

Lemma 4.23. *Let (A, A^+) be a Huber pair, let $|-|\colon A \to \Gamma \cup \{0\}$ be a valuation, and let $\mathfrak{p} := \operatorname{supp}(|-|)$ be its support and $R := k(|-|)^+ \subseteq k(\mathfrak{p})$ its associated valuation ring. Assume that $|a| \leq 1$ for $a \in A^+$. Then $|-|$ is continuous if and only if the image of each $b \in A^{\circ\circ}$ in $k(\mathfrak{p})$ is cofinal.*

Proof. The "only if" statement is clear. For the converse, let $a \in A$ with $|a| \neq 0$. Let $A_0 \subseteq A$ be a ring of definition and $I \subseteq A_0$ a finitely generated ideal of definition. We may assume that $A_0 \subseteq A^+$, and thus in particular, $|c| \leq 1$ for $c \in A_0$. From this and the fact that I is finitely generated and each $b \in I$ maps to a cofinal element in $k(\mathfrak{p})$, we deduce that there exists an $n \geq 1$, such that $I^n \subseteq \{b \in A \mid |b| \leq |a|\}$. This finishes the proof. □

As the proof of Lemma 4.23 it suffices to show cofinality for generators $b \in A^{\circ\circ}$ if an ideal of definition in some ring of definition $A_0 \subseteq A^+$.

Let us define a non-archimedean field as a complete non-discrete topological field K whose topology is induced by a valuation $|-|_K\colon K \to \mathbb{R}_{\geq 0}$. We let

$$\mathcal{O}_K = K^\circ = \{x \in K \mid |x| \leq 1\}$$

be its ring of integers, which agrees with the power bounded elements in K.

Example 4.24. (1) Assume that K is a non-archimedean field and let $K^+ \subseteq K$ be an open and bounded valuation subring. Then the map

$$\operatorname{Spa}(K, K^+) \cong \operatorname{Spec}(K^+/K^{\circ\circ}),\ |-| \mapsto \{a \in K^+ \mid |a| < 1\}$$

is a homeomorphism. Indeed, this follows from Example 4.22 because a valuation subring $S \subseteq K$ defines a continuous valuation if and only if $K^{\circ\circ} \subseteq \mathfrak{m}_S$. In particular, if $K^+ = \mathcal{O}_K$ is of rank 1, then

$$\operatorname{Spa}(K, \mathcal{O}_K) = \{*\}$$

is a singleton.

(2) Valuations $A \to \Gamma \cup \{0\}$ with $\Gamma = \{1\}$ the trivial group correspond bijectively to the set of open prime ideal in A. In particular, if A is an adic ring and $I \subseteq A$ a finitely generated ideal of definition, then we see that

$$\mathrm{Spf}(A) \subseteq \mathrm{Spa}(A, A)$$

is naturally a subspace, which is closed (as it is the vanishing locus of $A^{\circ\circ}$). Moreover, the map

$$r\colon \mathrm{Spa}(A, A) \to \mathrm{Spf}(A),\ x \mapsto \{f \in A \mid |f(x)| < 1\}$$

is a continuous retraction. Indeed,

$$r^{-1}(D(g)) = \{x \in \mathrm{Spa}(A, A) \mid |g(x)| = 1\} = \{x \in \mathrm{Spa}(A, A) \mid |g(x)| \geq 1\}.$$

(3) Let K be a non-archimedean field, $\mathcal{O}_K$ its ring of integers, $\pi \in K$ a pseudo-uniformizer and $|-|$ its valuation. Then consider

$$A := \mathcal{O}_K[[T]]$$

with its (π, T)-adic topology. The space $\mathrm{Spf}(A)$ has one point given by the open prime ideal $\sqrt{(\pi, T)}$. The space $\mathrm{Spa}(A, A)$ is much larger. Indeed, it is the union of the closed subspace $V(\pi) = \{x \in \mathrm{Spa}(A, A) \mid |\pi(x)| = 0\}$, which has two points, and the open complenent $U(\frac{0}{\pi})$. Given any $z \in \mathfrak{m}_K = K^{\circ\circ}$, we get the valuation

$$\mathcal{O}_K[[T]] \to \mathbb{R}_{\geq 0},\ f \mapsto |f(z)|,$$

where $f(z) \in K$ denotes the evaluation of f at $z \in K$. Later we will see that the "generic fiber of $\mathrm{Spa}(A, A)$" is the open rigid-analytic unit disc over K. This example is particularly interesting because of its relation to the Lubin-Tate spaces.

4.3. **The closed unit ball.** Let K be an algebraically closed, non-archimedean field and denote by

$$|-|\colon K \to \mathbb{R}_{\geq 0}$$

its valuation. Let

$$\mathcal{O}_K := \{x \in \mathcal{O}_K \mid |x| \leq 1\}$$

be its "unit ball", or ring of integers. Let

$$K\langle T\rangle := \{\sum_{i=0}^{\infty} x_i T^i \mid x_i \in K, |x_i| \to 0, i \to \infty\}$$

be the Tate algebra over K. More or less by definition we have

$$K\langle T\rangle \cong (\mathcal{O}_K[T])^{\wedge}_{\varpi}[1/\varpi],$$

where the RHS denotes the ϖ-adic completion of $\mathcal{O}_K[T]$ for some $\varpi \in C$ with $0 < |\varpi| < 1$.

We want to describe the adic space

$$\mathbb{B}_K := \mathrm{Spa}(K\langle T\rangle, \mathcal{O}_K\langle T\rangle)$$

in detail. By definition $\mathbb{B}_K$ is the space of (equivalence classes of) continuous valuations

$$\nu\colon K\langle T\rangle \to \Gamma \cup \{0\},$$

such that $\nu(x) \leq 1$ for $x \in \mathcal{O}_C\langle T\rangle$. Consider the Huber pair $(K[T], \mathcal{O}_K[T])$ such that $\mathcal{O}_K[T]$ is a ring of definition carrying the ϖ-adic topology. It is easy to see that the natural morphism $(K[T], \mathcal{O}_K[T]) \to (K\langle T\rangle, \mathcal{O}_K\langle T\rangle)$ induces a bijection

$$\mathbb{B}_K \cong \mathrm{Spa}(K[T], \mathcal{O}_K[T])$$

because continuous valuations extend uniquely to the completion as the following lemma shows.

If A is a Huber ring, let

$$\widehat{A} := \varprojlim_{U \subseteq A} A/U,$$

where U runs through the open subgroups of A. We may, by cofinality, assume that U is an ideal in some fixed ring of definition $A_0 \subseteq A$. The closure of the image of A_0 in $\widehat{A}$ is

$$\widehat{A_0} := \varprojlim_{U} A_0/U,$$

i.e., the completion of A_0 (for the I-adic topology for some finitely generated ideal of definition $I \subseteq A_0$). By [Sta17, Tag 05GG] the inverse limit topology on $\widehat{A_0}$ is $I \cdot \widehat{A_0}$-adic. Moreover, $\widehat{A_0} \subseteq \widehat{A}$ is open. From here it is not difficult to see that the multiplication on A extends uniquely to a continuous multiplication on $\widehat{A}$, i.e., the topological group $\widehat{A}$ is actually a ring, that it is complete and that it is Huber. If $A^+ \subseteq A$ is an integral ring, then the integral closure of its topological closure in $\widehat{A}$ is again a ring of integral $\widehat{A}^+$. We call $(\widehat{A}, \widehat{A}^+)$ the completion of (A, A^+).

Lemma 4.25. *Let (A, A^+) be a Huber pair. Then the natural morphism*

$$\mathrm{Spa}(\widehat{A}, \widehat{A}^+) \to \mathrm{Spa}(A, A^+)$$

is a homeomorphism.

Proof. Each continuous valuation $\nu\colon A \to \Gamma \cup \{0\}$ satisfying $\nu(a) \leq 1$ for $a \in A^+$ extends uniquely to a valuation $\widehat{A} \to \Gamma \cup \{0\}$ which is ≤ 1 on $\widehat{A^+}$. This proves bijectivity. The continuity of the inverse follows from Lemma 4.43. □

Let us start by describing the continuous rank 1 valuations

$$\nu\colon K[T] \to \mathbb{R}_{\geq 0}$$

with $\nu(x) \leq 1$ for $x \in \mathcal{O}_K[T]$. We will always implicitly assume that ν extends the valuation $|-|$ on K. An important example is the valuation defining the "Gauss point", i.e., the valuation

$$\nu_{0,1}\colon K[T] \to \mathbb{R}_{\geq 0}, f = \sum_{i=0}^{n} x_i T^i \mapsto \max_i\{|x_i|\}$$

(the notation will be clear later). More generally, we have the following examples of valuations.

Lemma 4.26. *Let $c \in \mathcal{O}_K$. For each $r \in [0, 1]$ the function*

$$\nu_{c,r}\colon K[T] \to \mathbb{R}_{\geq 0}, f = \sum_{i=0}^{n} x_i (T-c)^i \mapsto \max_i\{|x_i| r^i\}$$

is a continuous valuation. Moreover,

$$\nu_{c,r}(f) = \sup\{|f(x)| \mid x \in \mathbb{B}(c, r)\}$$

for $f \in K[T]$, where

$$\mathbb{B}(c,r) := \{x \in K \mid |x-c| \leq r\}$$

is the "closed" ball of radius r centered at $c \in K$.

Proof. Except

$$\nu_{c,r}(fg) = \nu_{c,r}(f) + \nu_{c,r}(g)$$

for $f, g \in K[T]$ all properties of a continuous valuation are easily verified. We may assume $c = 0$ and show that $\nu_{0,r}$ is a valuation. In particular, $\nu_{0,r}$ satisfies the strong triangle inequality. We may assume that $f = T - a$ for some $a \in K$ by factoring f (here we use our assumption that K is algebraically closed). First, assume that

$$\nu_{0,r}(a) = |a| \neq \nu_{0,r}(T) = r.$$

Then

$$\nu_{0,r}(Tg) = r\nu_{0,r}(g) \neq \nu_{0,r}(ag) = |a|\nu_{0,r}(g).$$

This implies

$$\nu_{0,r}((T-a)g) = \max\{r+\nu_{0,r}(g), |a|+\nu_{0,r}(g)\} = \max\{r,|a|\}+\nu_{0,r}(g) = \nu_{0,r}(T-a)+\nu_{0,r}(g)$$

by the strong inequality. The case $r = |a|$ follows from this as the function

$$r \in [0,1] \mapsto \nu_{0,r}(h) \in \mathbb{R}_{\geq 0}$$

is continuous for any $h \in K[T]$. Similarly the functions

$$f \mapsto \sup\{|f(x)| \mid x \in \mathbb{B}(0,r)\}$$

for $r \in [0,1]$ are continuous valuations, i.e., satisfy multiplicativity. That they agree with the $\nu_{0,r}$ follows by equating both on $T - a, a \in K$. □

We can now classify the rank 1 points in $\mathbb{B}_K$.

Lemma 4.27. *Let $\nu\colon K[T] \to \mathbb{R}_{\geq 0}$ be a continuous rank 1 valuation with $\nu(f) \leq 1$ for $f \in \mathcal{O}_K[T]$. Then there exists a family $\mathbb{B}(x_i, r_i), i \in I$, of nested discs with $x_i \in \mathcal{O}_K, r_i \in [0,1]$, such that*

$$\nu(f) = \inf_I \{\nu_{x_i,r_i}(f)\}.$$

Proof. We set $I = \mathcal{O}_K$, $x_i := i \in \mathcal{O}_K$ and $r_i = \nu(T - x_i) \in [0,1]$. If $r_i \leq r_j$, then

$$\mathbb{B}(x_i, r_i) \subseteq \mathbb{B}(x_j, r_j).$$

Indeed, if $a \in \mathbb{B}(x_i, r_i)$, then

$$|a - x_j| \leq \max\{|a - x_i|, |x_i - x_j|\} \leq \max\{|a - x_i|, \nu(T - x_i), \nu(T - x_j)\} = r_j,$$

i.e., the family $\mathbb{B}(x_i, r_i)$ consists of nested discs. Note that the disc $\mathbb{B}(x_i, r_i)$ depends only on $r_i = \nu(T - x_i)$. Let $y \in K$ and $i \in I$. If $\nu(T - y) > r_i$, then

$$|z - y| = \max\{\nu(z - T), \nu(T - y)\} = \nu(T - y)$$

for $z \in \mathbb{B}(x_i, r_i)$ as by the above calculation $\nu(z - T) \leq r_i$. Thus,

$$\nu(T - y) = \nu_{x_i,r_i}(T - y).$$

If $\nu(T - y) \leq r_i$, then $\mathbb{B}(y, \nu(T - y)) \leq \mathbb{B}(x_i, r_i)$ and

$$\nu(T - y) = \sup_{z \in \mathbb{B}(y,\nu(T-y))} \{|z - y|\} \leq \nu_{x_i,r_i}(T - y).$$

It suffices to test equality on the $T - y, y \in K$. This implies the claim. □

Note that from the proof we see that

$$\nu(f) = \inf_{y \in \mathbb{B}_{n,r_n}} \{|f(y)|\}$$

with discs

$$\mathbb{B}_{1,r_1} \supseteq \mathbb{B}_{2,r_2} \supseteq ...$$

for $n \in \mathbb{N}$ such that their radii r_n are a decreasing sequence of elements in $[0,1]$.

With Lemma 4.27 proven, we can classify the rank 1 points on $\mathbb{B}_K$. They fall into four types of points.

1) Assume that $r_n \to 0, n \to \infty$ and $\bigcap_n \mathbb{B}_{n,r_n} = \{x\}$ for some (necessarily unique) $x \in \mathcal{O}_K$. Then ν is the valuation
$$\nu_{x,0} \colon K[T] \to \mathbb{R}_{\geq 0}, f \mapsto |f(x)|.$$
2) Assume that $r_n \to r > 0, n \to \infty$ with $r \in |K^\times|$. Then
$$\nu = \nu_{x,r}$$
for some $x \in K$.
3) Assume that $r_n \to r > 0, n \to \infty$ with $r \notin |K^\times|$ (such points can only exist if K has not value group $\mathbb{R}_{>0}$). Then
$$\nu = \nu_{x,r}$$
for some $x \in K$.
4) Assume that $r_n \to 0, n \to \infty$, but $\bigcap_n \mathbb{B}_{n,r_n} = \emptyset$ (this strange property can happen if K is not so-called spherically complete). Then
$$\nu = \inf_n \{\nu_{x_n,r_n}\}$$
if $\mathbb{B}_{n,r_n} = \mathbb{B}(x_n, r_n)$.

For $x \in \mathcal{O}_K$ define

$$f_x \colon [0,1] \to \mathbb{B}_K, r \mapsto \nu_{x,r}.$$

The map f_x is not continuous as the open subsets in $\mathbb{B}_K$ are defined via non-strict inequalities. It is anticontinuous in the sense that the preimages of quasi-compact, open subsets are closed.

Clearly,

$$f_x(1) = \nu_{0,1}$$

is the Gauss point for all $x \in \mathcal{O}_K$. Thus, for each $x \in \mathcal{O}_K$ we can draw an interval from it to the Gauss point. Note that

$$\nu_{x,r} = \nu_{y,r}$$

if and only if

$$\mathbb{B}(x,r) = \mathbb{B}(y,r).$$

In other words, the functions f_x, f_y meet at $r = |x-y|$ (the tree is "branching"). Note that a branch point is of type 2). Let us now look at a type 4) point which is given by a nested sequence of discs

$$\mathbb{B}(x_1, r_1) \supseteq \mathbb{B}(x_2, r_2) \supseteq \dots$$

with $r_i \to 0, n \to \infty$. Then we can picture it as the "dead end of the tree", which is given by first moving from the Gauss point $f_{x_1}(1)$ to $f_{x_1}(|x_1 - x_2|)$, then switching to the branch determined by x_2 and move from $f_{x_1}(|x_1 - x_2|) = f_{x_2}(|x_1 - x_2|)$ to $f_{x_2}(|x_2 - x_3|)$, then switch to the branch determined by x_3 and so on.

We now classify the higher rank valuations on $\mathbb{B}_K$ by relating them to the rank 1 points, which we already know. We use the following observation. Let (A, A^+) be a Tate-Huber pair (like $(K[T], \mathcal{O}_K[T])$) and let $\varpi \in A$ a pseudo-uniformizer, i.e., a topologically nilpotent unit in A. For each $x \in \mathrm{Spa}(A, A^+)$ the image of $\varpi \in k(x)^+$ is a non-zero, cofinal element. A valuation ring R possessing a non-zero, cofinal element is called microbial.

Lemma 4.28. *Let R be a microbial valuation ring, and $\varpi \in R$ a non-zero cofinal element. Then*

$$\mathfrak{p} := \sqrt{(\varpi)}$$

is a prime ideal, which is the unique prime ideal of R of height 1.

Proof. As radical ideals in valuation rings are prime, $\mathfrak{p}$ is a prime ideal. Assume that

$$\{0\} \subsetneq \mathfrak{q}$$

is a prime ideal. We claim that $\mathfrak{p} \subseteq \mathfrak{q}$. Let $x \in \mathfrak{q} \setminus \{0\}$. As ϖ is cofinal, there exists some $n \geq 1$, such that $\varpi^n \in (x)$. In particular,

$$\mathfrak{p} = \sqrt{(\varpi)} \subseteq \sqrt{(x)} \subseteq \mathfrak{q}$$

as desired. □

In particular, $R_{\mathfrak{p}} \subseteq K := \mathrm{Frac}(R)$ is a valuation ring of rank 1.

Exercise 4.29. Let T be a valuation ring of Krull dimension 1 with fraction field L. Show that there exists an injection

$$L^\times / T^\times \to \mathbb{R}_{>0}$$

of totally ordered abelian groups.

Note that $R_{\mathfrak{p}}$ defines another continuous valuation of A and this point $\tilde{x}$ of $\mathrm{Spa}(A, A^+)$ is the unique rank 1 generalization of $x \in \mathrm{Spa}(A, A^+)$ whose residue field is $k(x)$. In fact, this condition is automatic.

Lemma 4.30. *Let (A, A^+) be a Tate-Huber pair and $z, y \in \mathrm{Spa}(A, A^+)$ be two points such that y is a specialization of z. Then*

$$k(y) = k(z),$$

i.e., specializations in $\mathrm{Spa}(A, A^+)$ only happen in the fibers of $\mathrm{Spa}(A, A^+) \to \mathrm{Spec}(A)$.

Proof. Assume that $k(y) \neq k(z)$. As $\mathrm{Spa}(A, A^+) \to \mathrm{Spec}(A)$ is continuous and thus preserves specializations, we can conclude that there exists some $f \in A$ such that $f(y) = 0 \in k(y)$ and $f(z) \neq 0 \in k(z)$. Let $\varpi \in A$ be a pseudo-uniformizer. Then we know that

$$|\varpi^n(z)| \leq |f(z)|$$

for some $n \geq 1$. In particular, $z \in U(\frac{\varpi^n}{f})$. On the other hand, $y \notin U(\frac{\varpi^n}{f})$ as $|\varpi^n(y)| \neq 0$ because ϖ is a unit in A. This shows that y is not a specialization of z, which is a contradiction. □

Given $\tilde{x}$ we can find back x via Example 4.22. Indeed by Lemma 4.30 and Lemma 4.23 the $y \in \mathrm{Spa}(A, A^+)$, which are a specialization of $\tilde{x}$ are in bijection with valuation subrings $S \subseteq k(\tilde{x})$ contained in $k(\tilde{x})^+$, which contain the image of A^+. This set is by Example 4.22 in bijection with

$$\mathrm{Spa}(\kappa(\tilde{x}), A^+_{\tilde{x}}),$$

where $\kappa(\tilde{x})$ is the residue field of the local ring $k(\tilde{x})^+$ and $A^+_{\tilde{x}}$ the image of A^+ under the composition

$$A^+ \to k(\tilde{x})^+ \to \kappa(\tilde{x}).$$

Let us come back to $\mathbb{B}_K = \mathrm{Spa}(A, A^+)$ with $A = K[T]$, $A^+ = K[T]$, and calculate the specialization for all rank 1 points $x \in \mathbb{B}_K$. We denote by κ the residue field of $\mathcal{O}_K$.

1) Let $c \in \mathcal{O}_K$. Then $x := \nu_{c,0}$ has residue field $K \cong K[T]/(T-c)$. As $\mathcal{O}_K$ is of rank 1, the point $\nu_{c,0}$ does not admit any specialization. In this case, $\kappa(x) = A^+_x = \kappa$.
2) Let $c \in \mathcal{O}_K$, and $r \in (0,1] \cap |K^\times|$. Let us first assume that $r = 1$, i.e., $x := \nu_{c,1}$ is the Gauss point. In this case,

$$\kappa(x) = \kappa(T),\ A^+_x = \kappa[T].$$

Therefore,

$$\mathrm{Spa}(\kappa(x), A^+_x) \cong \mathbb{A}^1_\kappa(\kappa).$$

If $r < 1$, then $(\kappa(x), A^+_x) = (\kappa(T'), \kappa)$ where $T' = \frac{T}{c}$ with $|c| = r$. Indeed,

$$\mathbb{B}(x, r) = \mathrm{Spa}(K\langle T/c\rangle, \mathcal{O}_K\langle T/c\rangle),$$

but the relevant A^+_x is not the image of $\mathcal{O}_K\langle T/c\rangle$ but of $\mathcal{O}_K[T]$. But $\nu_{x,r}(T) = r < 1$, i.e., the image of $\mathcal{O}_K[T]$ in k is just κ as claimed. Thus,

$$\mathrm{Spa}(\kappa(x), A^+_x) \cong \mathbb{P}^1_\kappa(\kappa)$$

in this case.

3),4) In these cases the point becomes a point of type 2) over some extension K' of K (which can assumed to have the same residue field κ) and using the case 2) one checks that the relevant pair is $(\kappa(x), A^+_x) = (\kappa, \kappa)$. Thus there are no non-trivial specializations of these points.

The points on $\mathbb{B}_K$ corresponding to valuations of rank > 1 are called of type 5). Concretely, if $\Gamma = \gamma^{\mathbb{Z}} \times \mathbb{R}_{>0}$ with γ infinitesimally less than 1, then the specializations of the point $\nu_{x,r}$ are given by

$$f = \sum_{i=0}^{\infty} x_i (T-a)^i \mapsto \max_i \{|x_i|(r\gamma)^i\}$$

for $|a - x| = r$, and, if $r < 1$, the point

$$f = \sum_{i=0}^{\infty} x_i (T-a)^i \mapsto \max_i \{|x_i|(r\gamma)^{-i}\}$$

for $|a - x| = r$ (for $r = 1$ this valuation does not satisfy that it takes value ≤ 1 on $\mathcal{O}_K[T]$). From the above we now finished the classification of points on $\mathbb{B}_K$.

4.4. $\mathrm{Spa}(A, A^+)$ **is a spectral space.** In this section we want to prove that the topological space

$$\mathrm{Spa}(A, A^+)$$

of continuous valuations for a Huber pair is a spectral space. Let us define what this means.

Definition 4.31. *A topological space X is spectral if it is quasi-compact, has a basis of quasi-compact open subsets, which is stable under finite intersections, and every irreducible closed subset admits a unique generic point.*

The typical example of a spectral space is the spectrum $\mathrm{Spec}(R)$ for some ring R. Here, the required basis for the topology is given by the sets $D(f)$ with $f \in R$. Up to homeomorphism each spectral space is of this form. In fact we have the following characterization of spectral spaces. Recall that topological space X is called T_0 if for any $x, y \in X$ distinct there exists an open subset $U \subseteq X$ such that $x \in U$ and $y \notin U$ or $y \in U$ and $x \notin U$.

Theorem 4.32 (Hoechster, cf. [Sta17, Tag 08YF])**.** *Let X be a topological space. The following conditions are equivalent:*

(1) *X is a spectral space,*
(2) *X is homeomorphic to $\mathrm{Spec}(R)$ for some ring R,*
(3) *X is the topological inverse limit of finite T_0-spaces.*

A morphism $f\colon Y \to X$ of spectral spaces is called spectral if it is quasi-compact, i.e., $f^{-1}(U) \subseteq Y$ is quasi-compact open if $U \subseteq X$ is quasi-compact and open.

We will need the following statements, which describe valuations via their divisibility relation.

Lemma 4.33. *Let R be a ring, $\nu\colon R \to \Gamma \cup \{0\}$ a valuation and $|$ the binary relation*

$$a|b := \nu(a) \leq \nu(b)$$

for $a, b \in R$. Then $|$ depends only on the equivalence class of ν and satisfies

(1) *$a|b$ or $b|a$,*
(2) *if $a|b$ and $b|c$, then $a|c$,*
(3) *if $a|b$ and $a|c$, then $a|b + c$,*
(4) *if $a|b$, then $ac|bc$,*
(5) *if $ac|bc$ and $0 \nmid c$, then $a|b$,*
(6) *$0 \nmid 1$*

for $a, b, c \in R$. Conversely, each binary relations on R satisfying these equations arises from some unique equivalence class of valuations.

Proof. This is clear except that a binary relation satisfying these equations defines a unique equivalence of class of valuations on R. Let M be the set of equivalences for the relation

$$a \simeq b \text{ if and only if } a|b \text{ and } b|a,$$

and for $a \in R$ let $[a] \in M$ be its equivalence class. The multiplication on R defines the commutative monoid structure

$$[a] \cdot [b] := [ab]$$

on M. If $[a], [b] \neq 0$, then $[ab] \neq 0$ and thus $M \setminus \{0\}$ is a monoid (with unit 1) as well. Moreover, in $M \setminus \{0\}$ multiplication is cancelable. Set

$$[a] \leq [b] \text{ if } b|a.$$

Then $M \setminus \{0\}$ is a totally ordered abelian monoid, and its group completion Γ is a totally ordered abelian group. The map

$$R \to \Gamma \cup \{0\},\ a \mapsto [a]$$

defines the desired valuation. □

Lemma 4.34. *Let (A, A^+) be a Huber pairs. Then each closed irreducible subset of $\mathrm{Spa}(A, A^+)$ contains a unique generic point.*

Proof. We first show that $\mathrm{Spa}(A, A^+)$ is T_0, which implies that generic points are unique (if they exist). If $x, y \in \mathrm{Spa}(A, A^+)$ are distinct valuations, then (up to permuting x, y) by the definition of equivalence of valuations there exists $f, g \in A$ with

$$|f(x)| \leq |g(x)|,$$

but

$$|f(y)| > |g(y)|.$$

If $g(x) \neq 0$, then $U(\frac{f}{g})$ is open and contains x, but not y. If $g(x) = 0$, then $f(x) = 0$ and $U(\frac{0}{f})$ contains y but not x. Let $Z \subseteq \mathrm{Spa}(A, A^+)$ be a closed irreducible subset. We use Lemma 4.33 and define the binary relation $|$ on A by requiring that

$$a|b$$

for $a, b \in A$ if $Z \subseteq V(b) \cap V(a)$ or $U(\frac{b}{a}) \cup Z \neq \emptyset$, where

$$V(c) = \mathrm{Spa}(A, A^+) \setminus U(\frac{0}{c})$$

is the vanishing locus of some $c \in A$. It is easy but tedious to see that $|$ satisfies the assumptions of Lemma 4.33, and thus defines a continuous valuation $\nu\colon A \to \Gamma \cup \{0\}$. The irreducibilty of Z is needed to ensure that two open non-empty open subsets have non-empty intersection. □

Let us now introduce the desired basis of quasi-compact open subsets. Here the following subtelty arises: for $f_1, \ldots, f_n, g \in A$ the open subset $U(\frac{f_1, \ldots, f_n}{g})$ need not be quasi-compact. For example, if $A = K\langle T\rangle$ for a non-archimedean field K, then

$$U(\frac{0}{T}) = \mathbb{B}_K \setminus \{0\} \subseteq \mathbb{B}_K = \mathrm{Spa}(K\langle T\rangle, \mathcal{O}_K\langle T\rangle)$$

is the punctured closed unit disc, which is not quasi-compact (in particular, the inclusion $\mathrm{Spa}(A, A^+) \to \mathrm{Spv}(A, A^+)$ is not spectral in general).

To circumvent this problem we introduce rational open subsets. Namely, we call the distinguished open subset

$$U(\frac{f_1, \ldots, f_n}{g}) \subseteq \mathrm{Spa}(A, A^+)$$

a rational open subset if $f_1, \ldots, f_n$ generate an open ideal of A.

Proposition 4.35. *Let (A, A^+) be a Huber pair, let $f_1, \ldots, f_n, g \in A$ such that $f_1, \ldots, f_n \in A$ generate an open ideal in A. Then*

$$U(\frac{f_1, \ldots, f_n}{g}) \cong \mathrm{Spa}(B, B^+)$$

(as topological spaces) for a Huber pair (B, B^+).

The Huber pair (B, B^+) constructed in the proof depends on $f_1, \ldots, f_n, g \in A$, but we will see in Proposition 4.46 that its completion only depends on $U(\frac{f_1, \ldots, f_n}{g})$.

Proof. If A is discrete it is clear that

$$U(\frac{f_1, \ldots, f_n}{g}) \cong \mathrm{Spv}(A[\frac{1}{g}], A^+[\frac{f_1, \ldots, f_n}{g}])$$

(as sets) because any valuation $\nu\colon A \to \Gamma \cup \{0\}$ with $\nu(g) \neq 0$ extends uniquely to the localization $A[\frac{1}{g}]$, and the condition

$$\nu(f_i) \leq \nu(g) \neq 0$$

is equivalent to $\nu(\frac{f_i}{g}) \leq 1$. Clearing denominators of elements in $A[1/g]$ shows that

$$U(\frac{f_1, \dots, f_n}{g}) \cong \mathrm{Spv}(A[\frac{1}{g}], A^+[\frac{f_1, \dots, f_n}{g}])$$

as topological spaces. Thus, we have to endow $A[\frac{1}{g}]$ with a ring topology $\mathcal{T}$ making $A[1/g]$ into a Huber ring such that some point

$$x \in \mathrm{Spv}(A[\frac{1}{g}], A^+[\frac{f_1, \dots, f_n}{g}])$$

restricts to a continuous valuation on A along $A \to A[1/g]$ if and only if x is continuous. Let $A_0 \subseteq A$ be a ring of definition with finitely generated ideal of definition $I \subseteq A_0$. Set

$$B_0 := A_0[\frac{f_1}{g}, \dots, \frac{f_n}{g}] \subseteq B := A[1/g]$$

and equip B_0 with the $J := I \cdot B$-adic topology. We equip B with the unique topology making B into a topological group such that the $J^n, n \geq 0$, form a fundamental system of neighborhoods of 0. We have to see that B is a topological ring, i.e., that the multiplication $B \times B \to B$ is continuous. It suffices to show that for each $h \in B$ the multiplication by h is continuous. This is clear for elements in the image of $A \to B$. Hence, it suffices to prove that multiplication by $1/g$ is continuous on B. We need to to see that

$$f_1 I^l + \ldots + f_n I^l \subseteq A$$

is open for any $l \geq 1$. Because granting this, there exists some $m \geq 1$ such that

$$I^m \subseteq f_1 I^l + \ldots + f_n I^l,$$

which implies

$$1/g I^m \subseteq \frac{f_1}{g} I^l + \ldots + \frac{f_n}{g} I^l \subseteq I^l \cdot A_0[\frac{f_1}{g}, \dots, \frac{f_n}{g}] = J^l,$$

thus $1/g \cdot J^m \subseteq J^l$ and therefore continuity of multiplication by $1/g$. Let $T := \{f_1, \dots, f_n\}$. By assumption the set

$$T \cdot A = f_1 A + \ldots + f_n A$$

is open in A. Let $k \geq 1$ such that $I^k \subseteq T \cdot A$. Replacing I by I^k we may assume that $I \subseteq T \cdot A$. Let $S \subseteq I$ be a finite set of generators and $V \subseteq A$ finite such that $S \subseteq T \cdot V$. As each finite set is bounded there exists $m \geq 1$ such that $V \cdot I^m \subseteq I^l$. Now

$$I^{m+1} = S \cdot I^m \subseteq T \cdot V \cdot I^m \subseteq T \cdot I^l$$

proves that $T \cdot I^l$ is open as desired. □

As rings/ideals of definition are cofinal the topology introduced on B in the proof of Proposition 4.35 does not depend on the choice of A_0, I.

Lemma 4.36. *Let (A, A^+) be a Huber pair. The rational open subsets form a basis for the topology on A, stable under finite intersections.*

Proof. Let $f_1, \dots, f_n = g, g, f_1', \dots, f_m' = g', g' \in A$ such that

$$(f_1, \dots, f_n)_A, (f_1', \dots, f_m')_A \subseteq A$$

are open. We have

$$U(\frac{f_1, \dots, f_n}{g}) \cap U(\frac{f_1', \dots, f_m'}{g'}) = U(\frac{f_1 f_1', \dots, f_n f_m'}{gg'}),$$

and the ideal

$$(f_1 f_1', \dots, f_n f_m')_A = \subseteq (f_1, \dots, f_n)_A \cdot (f_1', \dots, f_m')_A$$

is open. This proves that the rational open subsets are closed under intersection. Fix a ring of definition $A_0 \subseteq A$ and a finitely generated ideal of definition $I = (\pi_1, \dots, \pi_n) \subseteq A_0$. If $f, g \in A$ are arbitrary, then

$$U(\frac{f}{g}) = \bigcup_{m \geq 1} U(\frac{f, \pi_1^m, \dots, \pi_n^m}{g})$$

by continuity of valuations, and

$$(f, \pi_1^m, \dots, \pi_n^m)_A$$

is open. This proves that the rational open subsets are a basis for the topology. □

We want to present the following theorem of Huber, cf. [Hub93, Theorem 3.1.].

Theorem 4.37. *Let (A, A^+) be a Huber pair. The topological space $\mathrm{Spa}(A, A^+)$ is spectral, and its rational open subsets are a basis for the topology consisting of quasi-compact open subsets, which is stable under intersections.*

Proof. By Lemma 4.36, Proposition 4.35, Lemma 4.34 it suffices to see that $\mathrm{Spa}(A, A^+)$ is quasi-compact. This will be proved in Proposition 4.42. □

To finish the argument we introduce the constructible topology on spectral spaces.

Definition 4.38. *Let X be a spectral space. Then the constructible topology on X is the topology generated by U and $X \setminus U$ for $U \subseteq X$ quasi-compact and open. We let X_{cons} be X equipped with its constructible topology.*

Clearly, there exists a natural morphism

$$X_{\mathrm{cons}} \to X$$

and a spectral morphism $f \colon Y \to X$ of spectral spaces induces a continuous morphism $f_{\mathrm{cons}} \colon Y_{\mathrm{cons}} \to X_{\mathrm{cons}}$. When

$$X \cong \varprojlim_i X_i$$

with X_i finite T_0, then $X_{\mathrm{cons}} \cong \varprojlim_i X_{i,\mathrm{disc}}$ and in particular, X_{cons} is profinite. From here it is not difficult to deduce that if $Z \subseteq X$ is closed in the constructible topology, i.e., "pro-constructible", then Z with the subspace topology on X is a spectral space.

For more details, see [Sta17, Tag 08YF].

To prove the missing quasi-compacity of $\mathrm{Spa}(A, A^+)$ we construct now a continuous retraction $r \colon \mathrm{Spv}(A, A^+)_{\mathrm{cons}} \to \mathrm{Spa}(A, A^+)$, where

$$\mathrm{Spv}(A, A^+)_{\mathrm{cons}}$$

is (a posteriori) the spectral space $\mathrm{Spv}(A, A^+)$ with its constructible topology (but beware that we don't know yet that $\mathrm{Spv}(A, A^+)$ is spectral). Let $A_0 \subseteq A^+$ be a ring of definition and $I \subseteq A_0$ a finitely generated ideal of definition. For $x \in \mathrm{Spv}(A, A^+)$ let

$$R_x := k(x)^+ \subseteq k(x)$$

be the associated valuation ring, and

$$\varphi_x \colon A^+ \to R_x$$

the natural morphism. We set

$$\overline{R}_x := R_x/(\bigcap_{n\geq 1} \varphi_x(I)^n).$$

By Lemma 4.39 the elements in I map to cofinal elements in the valuation ring $\overline{R}_x$. By Lemma 4.23 this implies that the morphism

$$A^+ \to R_x \to \overline{R}_x$$

defines a continuous valuation on A^+.

Lemma 4.39. *Let S be a valuation ring, and $J \subseteq S$ a finitely generated ideal. Then $\mathfrak{p} := \bigcap_{n\geq 1} J^n \subseteq S$ is a prime ideal, $\overline{S} := S/\mathfrak{p}$ is a valuation ring, each $j \in J$ maps to a cofinal element in $\overline{S}$ and $\overline{S}$ is the largest quotient of S with this property.*

Proof. The ideal J is principal, say $J = (s)$. It suffices to see that $\mathfrak{p}$ is a radical ideal, but if $\nu \colon S \to \Gamma \cup \{0\}$ is the valuation of S, and $f \in S, m \geq 1$, with $f^m \in \mathfrak{p}$, then $\nu(f) \leq \nu(s^n)$ for all $n \geq 1$ as

$$m\nu(f) = \nu(f^m) \leq \nu(s^{m+n}) = m \leq \nu(s^n).$$

Quotients of valuation rings, which are integral domains are again valuation rings as their ideals are linearly ordered, cf. Definition 4.19. The cofinality of s in $\overline{S}$ is clear and also that $\overline{S}$ is the largest quotient having this property. □

We need to extend the continuous valuation

$$\nu_x \colon A^+ \to \Gamma_x \cup \{0\}$$

associated with the morphism

$$A^+ \to \overline{R}_x$$

to a continuous valuation on A. If $|\pi(x)| = 0$ for all $\pi \in I$, then $\overline{R}_x = R_x$ and nothing has to be done. Otherwise, ν_x extends uniquely to a continuous valuation on A as the next lemma shows.

Lemma 4.40. *Let $\nu \colon A^+ \to \Gamma \cup \{0\}$ be a continuous valuation, and assume that there exists some $\pi \in A^{\circ\circ}$ such that $\nu(\pi) \neq 0$. Then ν extends uniquely to a valuation on A.*

Proof. For each $a \in A$ there exists some $n \geq 1$ such that $\pi^n a \in A^+$. The unique extension of π is then given by

$$a \mapsto \nu(\pi)^{-n}\nu(\pi^n a).$$

□

Altogether we constructed for each $x \in \mathrm{Spv}(A, A^+)$ an element

$$r(x) \in \mathrm{Spa}(A, A^+). \tag{12}$$

We denote by $\mathrm{Spv}(A, A^+)_{\mathrm{cons}}$ the set $\mathrm{Spv}(A, A^+)$ equipped with the "constructible" topology for which the sets

$$U(\frac{f_1, \dots, f_n}{g})$$

for $f_1, \dots, f_n, g \in A$ are open *and* closed. The next lemma finishes the case that A is discrete.

Lemma 4.41. *The space* $\mathrm{Spv}(A, A^+)_{\mathrm{cons}}$ *is profinite, and thus in particular quasi-compact.*

Proof. For $x \in \mathrm{Spv}(A, A^+)_{\mathrm{cons}}$ let $|_x$ the associated binary relation

$$a|_x b \text{ if and only if } |a(x)| \geq |b(x)|$$

on A. By definition a binary relation on A is a subset of $A \times A$. Let $\mathcal{P}(A \times A) \cong \prod_{A \times A} \{0, 1\}$ be the power set of $A\times$, which is naturally a profinite set. By Lemma 4.33 the map

$$\iota \colon \mathrm{Spv}(A, A^+)_{\mathrm{cons}} \to \mathcal{P}(A \times A),\ x \mapsto |_x$$

is a closed embedding. Indeed, for $f, g \in A$ let $\pi_{f,g} \colon \mathcal{P}(A \times A) \to \{0, 1\}$ be the projection on the (f, g)-component. Then $\pi_{f,g}^{-1}(1)$ identifies with binary relations $|$ on A satisfying $f|g$. Let $f, g \in A$. Then the set

$$\iota^{-1}(\pi_{g,f}^{-1}(1)) \subseteq \mathrm{Spv}(A, A^+)_{\mathrm{cons}}$$

is open as it is the union of the open sets

$$U(\frac{f}{g}),\ \mathrm{Spv}(A, A^+)_{\mathrm{cons}} \setminus U(\frac{0}{g}) \cap \mathrm{Spv}(A, A^+)_{\mathrm{cons}} \setminus U(\frac{0}{f}).$$

Given $f, g \in A$ we see that

$$U(\frac{f}{g}) = \iota^{-1}(\pi_{g,f}^{-1}(1) \setminus \pi_{0,g}^{-1}(1)).$$

This implies that $\mathrm{Spv}(A, A^+)_{\mathrm{cons}}$ carries the subspace topology of $\mathcal{P}(A \times A)$. The set of binary relations $|$ satisfying that for all $f, g \in A$ we have $f|g$ or $f|g$ is therefore the closed subset

$$\bigcup_{f,g \in A} [\pi_{f,g}^{-1}(1) \cup (\pi_{f,g}^{-1}(0) \cap \pi_{g,f}^{-1}(1))],$$

and similarly for the other equations from Lemma 4.33. In particular, the image of ι is closed and hence $\mathrm{Spv}(A, A^+)_{\mathrm{cons}}$ is profinite. □

The next proposition finishes the proof of Theorem 4.37.

Proposition 4.42. *The map*

$$r \colon \mathrm{Spv}(A, A^+)_{\mathrm{cons}} \to \mathrm{Spa}(A, A^+)$$

constructed in (Equation (12)*) is continuous. In particular,* $\mathrm{Spa}(A, A^+)$ *is quasi-compact.*

Proof. By Lemma 4.36 it suffices to show that $r^{-1}(U)$ is open for every rational open subset $U \subseteq \mathrm{Spa}(A, A^+)$. Let $f_1, \dots, f_n, g \in A$ such that $(f_1, \dots, f_n)_A \subseteq A$ is open. Then

$$r^{-1}(U_{\mathrm{Spa}(A,A^+)}(\frac{f_1, \dots, f_n}{g})) = U_{\mathrm{Spv}(A,A^+)}(\frac{f_1, \dots, f_n}{g}),$$

where the subscript is added for clarifying where we consider the distinguished open subset. The map r is natural with respect to the morphism $(A, A^+) \to (B, B^+)$ constructed in Proposition 4.35. This implies that

$$r(U_{\mathrm{Spv}(A,A^+)}(\frac{f_1, \dots, f_n}{g})) \subseteq U_{\mathrm{Spa}(A,A^+)}(\frac{f_1, \dots, f_n}{g}).$$

Conversely, assume that $x \in r^{-1}(U_{\mathrm{Spa}(A,A^+)}(\frac{f_1,\dots,f_n}{g}))$. Then

$$x \in \{y \in \mathrm{Spv}(A, A^+) \mid |f_i(y)| \leq |g(y)|, i = 1, \dots, n\}$$

and we have to show that $g(x) \neq 0$. Let $I \subseteq A_0$ be an ideal of definition in a ring of definition of A. If $g(x) = 0$, then $\pi(x) = 0$ for all $\pi in I$ as $(f_1, \dots, f_n)_A$ is open. In particular, $r(x) = x$, and thus $g(x) \neq 0$, which is a contradiction. Hence, r is continuous. By Lemma 4.23 the map r is a retraction for the inclusion

$$\mathrm{Spa}(A, A^+) \to \mathrm{Spv}(A, A^+),$$

in particular, we can deduce from Lemma 4.41 that $\mathrm{Spa}(A, A^+)$ is quasi-compact. □

We mention the following compatibility of rational open subsets under completions.

Lemma 4.43. *Let (A, A^+) be a Huber pair. Then the natural map (a bijection by Lemma 4.25)*

$$\mathrm{Spa}(\widehat{A}, \widehat{A^+}) \to \mathrm{Spa}(A, A^+)$$

identifies the sets of rational open subsets.

Proof. This is [Hub93, Proposition 3.9] or [Mor19, Theorem III.3.1.]. The crucial point is to approximate $f_1, \dots, f_n, g \in \widehat{A}$ such that $(f_1, \dots, f_n)_A$ by elements in A without changing $U(\frac{f_1,\dots,f_n}{g})$. □

In the complete case we get that $\mathrm{Spa}(A, A^+)$ is "large enough".

Lemma 4.44. *Let (A, A^+) be a complete Huber pair, i.e., A is complete. Then*

1. *$\mathrm{Spa}(A, A^+) = \emptyset$ if and only $A = 0$,*
2. *$A^+ = \{f \in A \mid |f(x)| \leq 1$ for all $x \in \mathrm{Spa}(A, A^+)\}$,*
3. *an element $f \in A$ is invertible if and only if $|f(x)| \neq 0$ for all $x \in \mathrm{Spa}(A, A^+)$.*

Proof. This can be found in [Hub93, Proposition 3.6.], [Mor19, Section III.4.4.] and [SW20, Proposition 2.3.10.]. The last statement also follows from Lemma 4.45. □

Moreover, we note the following.

Lemma 4.45. *Let (A, A^+) be a complete Huber pair, and $T = \{t_1, \dots, t_n\} \subseteq A$ a finite subset. Then the following are equivalent:*

1. *The ideal generated by T is A.*
2. *For each $x \in \mathrm{Spa}(A, A^+)$ there exists some $t \in T$ with $|t(x)| \neq 0$.*

In this case, $U(\frac{t_1,\dots,t_n}{t_i})$ *for* $i = 1,\dots,n$ *form a covering of* $\mathrm{Spa}(A,A^+)$ *by rational open subsets.*

Proof. This is [Mor19, Corollary III.4.4.3.]. □

4.5. **The adic spectrum of a Huber pair.** Let (A,A^+) be a Huber pair. We want to endow

$$X := \mathrm{Spa}(A,A^+)$$

with a structure presheaf X (of complete topological rings), and prove that it is a sheaf if A admits a noetherian ring of definition. As rational open subsets $U \subseteq X$ form a basis of the topology on X by Lemma 4.36 it suffices to discuss them.

The crucial statement is then the following.

Proposition 4.46. *Let* (A,A^+) *be a Huber pair and* $U \subseteq X := \mathrm{Spa}(A,A^+)$ *a rational open subset. Then there exists a complete Huber pair* $(A,A^+) \to (A_U,A_U^+)$ *such that* $\mathrm{Spa}(A_U,A_U^+)$ *has image* U *and for every complete Huber pair* $(A,A^+) \to (C,C^+)$ *such that* $\mathrm{Spa}(C,C^+) \to \mathrm{Spa}(A,A^+)$ *has image in* U *there exists a unique factorization*

$$\begin{array}{ccc} (A,A^+) & \longrightarrow & (A_U,A_U^+) \\ & \searrow & \downarrow \\ & & (C,C^+). \end{array}$$

Proof. Let $f_1,\dots,f_n,g \in A$ such that $(f_1,\dots,f_n)_A \subseteq A$ is open and

$$U = U(\frac{f_1,\dots,f_n}{g}).$$

The crucial point is the following. If (C,C^+) is complete such that $\mathrm{Spa}(C,C^+) \to \mathrm{Spa}(A,A^+)$ has image in U, then by Lemma 4.44 g is invertible in C, and $\frac{f_i}{g} \in C^+$ for all $i = 1,\dots,n$. This implies that there exists a unique morphism

$$(B,B^+) \to (C,C^+)$$

with $(B = A[1/g],B^+)$ the Huber ring constructed in Proposition 4.35. By Lemma 4.43 the completion (A_U,A_U^+) of (B,B^+) satisfies the desired properties. □

If $V \subseteq U$ is an inclusion of rational open subsets of X, then by the universal property of (A_U,A_U^+) we get a natural morphism

$$r_{UV} \colon (A_U,A_U^+) \to (A_V,A_V^+)$$

of Huber pairs over (A,A^+).

Definition 4.47. *The structure presheaf* $\mathcal{O}_X$ *on* X *is the presheaf on the basis of rational open subsets given by*

$$U \mapsto A_U$$

and the restriction r_{UV}*. Similarly, the* $+$*-version of the structure presheaf* $\mathcal{O}_X^+$ *on* X *is*

$$U \mapsto A_U^+.$$

A Huber pair (A,A^+) *is called sheafy if* $\mathcal{O}_X$ *is a sheaf.*

For each $x \in X$ the valuation

$$|-(x)|\colon A \to \Gamma \cup \{0\}$$

extends naturally to a valuation $|-(x)|$ on the stalk

$$\mathcal{O}_{X,x} := \varinjlim_{U \subseteq X \text{ rational open}, x \in U} \mathcal{O}_X(U)$$

of $\mathcal{O}_X$ at x. By Lemma 4.44

$$\mathcal{O}_X^+(U) = \{f \in \mathcal{O}_X(U) \mid |f(x)| \leq 1\}.$$

In particular, $\mathcal{O}_X^+$ is a sheaf if $\mathcal{O}_X$ is a sheaf.

We mention the following criterion for sheafiness.

Theorem 4.48. *Let (A, A^+) be a Huber pair. Then (A, A^+) is sheafy if*

1. *A is discrete, or*
2. *A is finitely generated over a noetherian ring of definition.*

There do exist more (important) cases when (A, A^+) is sheafy, for example when A is a strongly noetherian Tate ring, i.e., A is Tate and $A\langle T_1, \dots, X_n\rangle$ is noetherian for each $n \geq 0$, cf. [Mor19, Theorem IV.1.1.5.].

Sending a *complete* Huber pair (R, R^+) to the adic space $\mathrm{Spa}(R, R^+)$ is fully faithful, cf. [Mor19, Proposition III.6.4.4].

Our case of interest are adic spaces associated to locally noetherian schemes, i.e., adic spaces which are locally of the form $\mathrm{Spa}(A_0, A_0)$ for an adic noetherian ring, or rigid-analytic varieties over some discretely valued non-archimedean field K, i.e., adic spaces which are locally of the form $\mathrm{Spa}(A, A^\circ)$ with A a quotient of some Tate algebra $K\langle X_1, \dots, X_n\rangle$ over K.

Given the category of adic spaces, we can now achieve our aim to pass to "generic fibers" of formal schemes. Fix a discretely valued non-archimedean field K with ring of integers $\mathcal{O}_K$. In the affine case, the passage to the generic fiber is the following. Let A_0 be a noetherian adic ring. Instead of $\mathrm{Spf}(A_0)$ we consider the adic space $X := \mathrm{Spa}(A_0, A_0)$. The "generic fiber of $\mathrm{Spf}(A_0)$" is then the fiber product

$$X_\eta := X \times_{\mathrm{Spa}(O_K, O_K)} \mathrm{Spa}(K, \mathcal{O}_K)$$

in the category of adic spaces. Alternatively, the generic fiber is the open sublocus

$$\{x \in X \mid |\pi(x)| \neq 0\} \subseteq X$$

for $\pi \in \mathcal{O}_K$ a uniformizer. As a concrete example, the generic fiber of the formal scheme $\mathrm{Spf}(\mathcal{O}_K\langle T\rangle)$ is the closed unit ball $\mathrm{Spa}(K\langle T\rangle, \mathcal{O}_K\langle T\rangle)$. In general the generic fibers of affine formal schemes need not be affinoid, e.g., the generic fiber of $\mathrm{Spf}(\mathcal{O}_K[[T]])$ (with $\mathcal{O}_K[[T]]$ given the (π, T)-adic topology) is the non-quasi-compact open unit disc

$$\mathbb{D}_K,$$

which is the interior of the closed (!) locus

$$\{x \in \mathbb{B}_K \mid |x| < 1\}.$$

If (R, R^+) is a complete Huber pair over $(K, \mathcal{O}_K)$ we can describe the (R, R^+)-valued points of $\mathrm{Spa}(A)_\eta$ for A a noetherian adic $\mathcal{O}_K$-algebra. Namely,

$$\begin{aligned} & \mathrm{Spf}(A)_\eta(R, R^+) \\ = \quad & \mathrm{Hom}_{(\mathcal{O}_K, \mathcal{O}_K)}((A, A), (R, R^+)) \\ = \quad & \varinjlim_{R_0 \subseteq R^+ \text{ ring of definition}} \mathrm{Hom}_{\mathcal{O}_K, \mathrm{cts}}(A, R_0) \\ = \quad & \varinjlim_{R_0 \subseteq R^+ \text{ ring of definition}} \mathrm{Spf}(A)(R_0), \end{aligned}$$

cf. [SW13, Proposition 2.2.2]. Note that the topological ring R^+ need not be admissible, and thus evaluating $\mathrm{Spf}(A)$ on R^+ does not in general make sense. However, each ring of definition $R_0 \subseteq R^+$ is π-adic, and hence

$$\mathrm{Spf}(A)(R_0) \cong \varprojlim_n \mathrm{Spf}(A)(R_0/\pi^n).$$

5. The Gross-Hopkins period morphism

Let A be a complete discrete valuation ring with finite resiude field k of characteristic p and cardinality q. Let $K := \mathrm{Frac}(A)$ be the fraction field of A. Fix a uniformizer $\pi \in A$ and a π-divisible formal A-module $\mathcal{G}_h$ over $\mathrm{Spec}(k)$ of height $h \in \mathbb{Z}_{\geq 1}$. Let

$$\mathcal{M} := \mathcal{M}_{\mathrm{RZ},\mathcal{G}} \cong \coprod_{n \in \mathbb{Z}} \mathcal{M}_{\mathrm{RZ},\mathcal{G},n}$$

be the associated Rapoport-Zink/Lubin-Tate space. In this section we want to present the construction of the Gross-Hopkins period morphism

$$\pi_{\mathrm{GH}} \colon \mathcal{M}_\eta^{\mathrm{ad}} \to \mathbb{P}_K^{h-1,\mathrm{ad}},$$

which is an étale surjective covering of the adic $h-1$-dimensional projective space by the adic generic fiber $\mathcal{M}_\eta^{\mathrm{ad}}$ of $\mathcal{M}$, and which is equivariant for some to be defined action of the quasi-isogenies of $\mathcal{G}_h$.

5.1. **Outline of the construction.** Let (B, B^+) be a complete sheafy Huber pair over (K, A). By construction,

$$\mathcal{M}_\eta^{\mathrm{ad}}(B, B^+) = \varinjlim_{B_0 \subseteq B^+} \mathcal{M}(B_0) = \varinjlim_{B_0 \subseteq B^+} \varprojlim_n \mathcal{M}(B_0/\pi^n),$$

where B_0 runs through the rings of definition contained in B^+. On the other hand

$$\mathbb{P}_K^{h-1,\mathrm{ad}}(B, B^+)$$

parametrizes the set of isomorphism classes of invertible B-modules $\mathcal{L}$ together with a surjection

$$B^h \to \mathcal{L}.$$

In other words, we have to associate with any π-complete π-torsion free A-algebra R (like B_0) and any pair

$$(\mathcal{G}, \alpha) \in \mathcal{M}(R)$$

of a formal A-module $\mathcal{G}$ over R with a quasi-isogeny

$$\alpha \colon \mathcal{G} \hat{\otimes}_R R/\pi \dashrightarrow \mathcal{G}_h \hat{\otimes}_k R/\pi,$$

a natural invertible $R[1/\pi]$-module $\mathcal{L}$ together with generating (over $R[1/\pi]$) elements

$$c_0, \ldots, c_{h-1} \in \mathcal{L}.$$

The line bundle $\mathcal{L}$ is easy to construct: As $\mathcal{G}$ is one-dimensional its Lie algebra $\mathrm{Lie}(\mathcal{G})$ is an invertible R-module, and we can set

$$\mathcal{L} := \mathrm{Lie}(\mathcal{G})[1/\pi].$$

We saw in Proposition 3.18 that necessarily $\mathrm{Lie}(\mathcal{G}) \cong R$ is free. In particular, there exists a lot of possible choices for the $c_0, \ldots, c_{h-1}$ and our task is to find some particularly interesting ones. This will be done as follows. For any π-complete π-torsion free A-algebra R we construct a functor (for $A = \mathbb{Z}_p$ this is an instance of the covariant crystalline Dieudonné functor for p-divisible groups)

$$M(-) \colon \mathrm{FG}_{A,\pi-\mathrm{div}}(R/\pi) \to \{\text{finite, locally free } R-\text{modules}\}$$

from the category of π-divisible formal A-modules to finite locally free R-modules such that

$$M(\mathcal{G})$$

has (constant) rank h if $\mathcal{G}$ has (constant) height h, and $M(-)$ is compatible with base change in R. Moreover, given a π-divisible formal A-module $\mathcal{G}$ over R we construct a natural surjection

$$M(\mathcal{G}\hat{\otimes}_R R/\pi) \twoheadrightarrow \mathrm{Lie}(\mathcal{G}).$$

Given this data the construction of the Gross-Hopkins period morphism can be finished as follows. Let R be a π-complete, π-torsion free A-algebra and $(\mathcal{G},\alpha) \in \mathcal{M}(R)$. Then the quasi-isogeny

$$\alpha\colon \mathcal{G}\hat{\otimes}_R R/\pi \dashrightarrow \mathcal{G}_h\hat{\otimes}_k R/\pi$$

defines an isomorphism

$$M(\mathcal{G}_h)\otimes_A R[1/\pi] \cong M(\mathcal{G}_h\hat{\otimes}_k R/\pi)[1/\pi] \overset{M(\alpha)}{\cong} M(\mathcal{G}\hat{\otimes}_R R/\pi)[1/\pi],$$

and the surjection

$$M(\mathcal{G}_h)\otimes_A R[1/\pi] \cong M(\mathcal{G}\hat{\otimes}_R R/\pi)[1/\pi] \twoheadrightarrow \mathcal{L} = \mathrm{Lie}(\mathcal{G})[1/\pi]$$

defines the desired point in

$$\mathbb{P}_K^{h-1,\mathrm{ad}} \cong \mathbb{P}(M(\mathcal{G}_h)[1/\pi])^{\mathrm{ad}}$$

Using the Lubin-Tate formal A_h-module for the ring of integers in the unramified degree h extension of K, we can then find explicit generators of

$$M(\mathcal{G}_h)[1/\pi],$$

which yield the desired sections $c_0,\dots,c_{h-1}$ of $\mathcal{L}$.

5.2. **Quasi-logarithms.** Let R be a π-complete π-torsion free A-algebra and $\mathcal{G}$ a formal A-module over R. We assume that

$$\mathcal{G} = \mathcal{G}_F$$

for some formal A-module law $F \in R[[X,Y]]$, $[a]_F \in R[[X]], a \in A$, and later explain how the following constructions can be made to depend only on $\mathcal{G}$.

We set

$$R_K := R\otimes_A K.$$

Definition 5.1. *We call a series $g(X) \in R_K[[X]]$ with $g(0)=0$ a quasi-logarithm for F if its derivative $g'(X)$,*

$$\Delta g(X,Y) := g(X) + g(Y) - g(F(X,Y))$$

and

$$\delta_a g(X) := a\cdot g(X) - g([a]_F(X)),\ a\in A,$$

have coefficients in $R[[X]]$. We call a quasi-logarithm integral if $g(X)$ has coefficients in R.

Clearly, the quasi-logarithms form an R-submodule of $R_K[[X]]$. For example, each R-multiple of $\log_F(X) \in R_K[[X]]$ is a quasi-logarithm. In fact, the R-multiples of the logarithm are precisely those quasi-logarithms $g(X)$ such that

$$\Delta g(X,Y) = 0,\ \delta_a g(X) = 0,\ a\in A$$

as we require that $g'(0)$ lies in R.

Definition 5.2. *We set*

$$M(\mathcal{G})^\vee := \{\textit{quasi-logarithms for } F\}/\{\textit{integral quasi-logarithms}\},$$

and call it the contravariant Dieudonné module of $\mathcal{G}$.

The searched for functor $M(-)$ will map a π-divisible formal A-module $\mathcal{G}_0$ over R/π to

$$\mathrm{Hom}_R(M(\mathcal{G})^\vee, R),$$

where $\mathcal{G}$ is any lift of $\mathcal{G}_0$ to R. Using abuse of notation this means that

$$M(\mathcal{G}) := \mathrm{Hom}_R(M(\mathcal{G})^\vee, R) = M(\mathcal{G}\hat{\otimes}_R R/\pi)$$

for a π-divisible formal A-module $\mathcal{G}$ over R. For this construction to make sense and satisfy our desiderata from Section 5.1 we have to prove the following statements for π-divisible formal A-modules:

(1) $M(\mathcal{G})^\vee$ is a finite, locally free R-module of rank h if the π-divisible formal A-module $\mathcal{G}$ over R is of constant height h,
(2) $M(\mathcal{G})^\vee$ depends, up to canonical isomorphism, only on the reduction $\mathcal{G}/\pi$ of $\mathcal{G}$,
(3) $M(-)^\vee$ is functorial in morphisms of π-divisible formal A-modules over R/π,
(4) there exists a natural surjection

$$M(\mathcal{G}) \to \mathrm{Lie}(\mathcal{G}).$$

It is clear that there is a natural exact sequence

$$0 \to \mathrm{Hom}_R(\mathcal{G}, \hat{\mathbb{G}}_a) \to R \cdot \log_F \to M(\mathcal{G})^\vee.$$

If $\mathcal{G}$ is π-divisible then

$$\mathrm{Hom}_R(\mathcal{G}, \widehat{\mathbb{G}}_a) = 0,$$

and thus we get an injection

$$R \cdot \log_F \to M(\mathcal{G})^\vee$$

is injective. Note that canonically

$$\omega(\mathcal{G}) \cong R \log_F$$

by "integrating" invariant differential forms, cf. Section 3.3. We want to describe the cokernel of

$$\omega(\mathcal{G}) \to M(\mathcal{G})^\vee$$

concretely via deformations of $\mathcal{G}$. Recall that

$$R[\varepsilon] = R \oplus \varepsilon R$$

with $\varepsilon^2 = 0$.

Lemma 5.3. *Let* $g(X) \in R[[X]]$ *with* $g(0) = g'(0) = 0$, *and let* $f(X) = \log_F(X) \in R_K[[X]]$ *be the logarithm of* F. *Then* $g(X)$ *is a quasi-logarithm for* F *if and only if the series*

$$f_g(X) := f(X) + \varepsilon g(X)$$

is the logarithm of formal A*-module law* $F_g(X, Y) \in R[\varepsilon][[X, Y]]$.

Necessarily,

$$F_g(X, Y) = f_g^{-1}(f_g(X) + f_g(Y)),\ [a]_{F_g}(X) = f_g^{-1}(a \cdot f_g(X))$$

for $a \in A$.

Proof. Write

$$f_g^{-1}(X) = f^{-1}(X) + \varepsilon \cdot g_1(X)$$

with $g_1(X) \in R_K[[X]]$. Then

$$g_1(X) = -f'(f^{-1}(X))^{-1} \cdot g(f^{-1}(X)).$$

We get (using $\varepsilon^2 = 0$)

$$\begin{aligned} & F_g(X,Y) \\ =& f_g^{-1}(f_g(X) + f_g(Y)) \\ =& f^{-1}(f_g(X) + f_g(Y)) - \varepsilon \frac{1}{f'(F(X,Y))} g(F(X,Y)) \\ =& F(X,Y) + \varepsilon(\frac{1}{f'(F(X,Y))}(g(X) + g(Y) - g(F(X,Y)))). \end{aligned}$$

We know that

$$f'(Y) = (\frac{\partial F}{\partial X}(0,Y))^{-1} \in R[[X]]$$

by Section 3.3. In particular, $f'(F(X,Y))$ is unit in the ring $R[[X,Y]]$. We can deduce that $F_g(X,Y)$ has coefficients in R if and only if

$$g(X) + g(Y) - g(F(X,Y)) \in R[[X]].$$

Let $a \in A$. Then we similarly see that

$$[a]_{F_g}(X) = f_g^{-1}(a f_g(X))$$

has coefficients in R if and only if $ag(X) - g([a]_F(X)$ has coefficients in R. If f_g is the logarithm of a formal A-module over $R[\varepsilon]$, then its derivative has coefficients in $R[\varepsilon]$ by Section 3.3. This finishes the proof. □

From the proof we see that in Definition 5.1 we could equivalently demand that $g'(0) \in R$ instead of $g'(X) \in R[[X]]$.

From the proof of Lemma 5.3 we can record:

$$\begin{aligned} F_g(X,Y) &= F(X,Y) + \varepsilon \Delta g(X,Y) h(F(X,Y)) \\ [a]_{F_g}(X) &= [a]_F(X) + \delta_a g(X) h([a]_F(X)) \end{aligned} \tag{13}$$

for $a \in A$, where

$$h(Y) = \frac{\partial F}{\partial X}(0,Y) \in R[[Y]].$$

Note that the formal A-module $F_g, [a]_{F_g}, a \in A$ can be defined for any quasi-logarithm g for F, i.e., not just for those with $g'(0) = 0$.

Definition 5.4. *We let*

$$\mathcal{D}ef_F(R[\varepsilon])$$

be the set of equivalence classes of formal A-module laws $F' \in R[\varepsilon][[X,Y]]$ reducing to F modulo ε, with equivalence given by isomorphisms inducing the identity modulo ε.

As a finite projective $R[\varepsilon]$-module M is finite free if and only its base change $M \otimes_{R[\varepsilon]} R$ is finite free, $\mathcal{D}ef_F(R[\varepsilon])$ could equivalently be defined via deformations $\mathcal{D}ef_{\mathcal{G}}(R[\varepsilon])$ of the formal A-module $\mathcal{G}$.

As in the proof of Theorem 2.34 we see that $\mathcal{D}ef_F(R[\varepsilon])$ is naturally an R-module.

Lemma 5.5. *If $\mathcal{G}$ is π-divisble of constant height h, then the R-module $\mathcal{D}ef_F(R[\varepsilon])$ is finite free of rank $h-1$, and for a morphism $R \to R'$ of π-complete, π-torsion free A-algebras the natural map*

$$\mathcal{D}ef_F(R[\varepsilon]) \otimes_R R' \to \mathcal{D}ef_{F\hat{\otimes}_R R'}(R'[\varepsilon])$$

is an isomorphism.

Proof. Passing to the limit of R/π^n we may prove the with R replaced by some $R/\pi^n, n \geq 1$. If F is a $\star$-deformation of a normalized formal A-module of height h, we may argue as in the proof of Lemma 2.39. The general case follows from this by faithfully flat descent, Lemma 2.28 and the fact that ind-finite étale algebras lift uniquely along nilpotents, cf. [Sta17, Tag 09ZL]. □

We set

$$h(X) := \frac{\partial F}{\partial X}(0, X) \in R[[X]].$$

From Lemma 5.3 we can deduce the following statement.

Lemma 5.6. *The map $g \mapsto F_g(X,Y) \otimes \frac{1}{h(X)}dX$ with F_g as in (Equation (13)) fits into an exact sequence*

$$0 \to \mathrm{Hom}_R(\mathcal{G}, \hat{\mathbb{G}}_a) \to \omega(\mathcal{G}) \to M(\mathcal{G})^\vee \to \mathcal{D}ef_{\mathcal{G}}(R[\varepsilon]) \otimes_R \omega(\mathcal{G}) \to 0.$$

In particular, if $\mathcal{G}$ is π-divisible of height h, then

1. *$M(\mathcal{G})^\vee$ is a finite free R-module of rank h depending only on $\mathcal{G}$ (and not F),*
2. *for a morphism $R \to R'$ of π-complete π-torsion free R-modules the natural map*
$$M(\mathcal{G})^\vee \otimes_R R' \to M(\mathcal{G}\hat{\otimes}_R R')^\vee$$
is an isomorphism.

Proof. We already discussed exactness at $\mathrm{Hom}_R(F, \hat{\mathbb{G}}_a), \omega(\mathcal{G})$. Surjectivity on the right follows from Lemma 5.3 and the fact that $R[\varepsilon]$ is π-torsion free (which implies that each formal A-module law over it is associated to some logarithm). It is clear that

$$g \mapsto F_g(X,Y)$$

is R-linear for the R-linear structure on $\mathcal{D}ef_F(R[\varepsilon])$. Let us prove that the kernel of $g \mapsto F_g$ is generated by the integral quasi-logarithms and the multiples of the logarithm. Thus, assume that F_g for a quasi-logarithm g is equivalent to $F_0 = F$. Then there exists some $\alpha(X) = X + \varepsilon\beta(X) \in R[\varepsilon][[X]], \beta(X) \in R[[X]]$, such that

$$\alpha(F_g(X,Y)) = F(\alpha(X), \alpha(Y)), \alpha([a]_{F_g}(X)) = [a]_F(\alpha(X)).$$

A short calculation shows that

$$\Delta g(X,Y)h(F(X,Y)) + \beta(F(X,Y)) = \frac{\partial F}{\partial X}(X,Y)\beta(X) + \frac{\partial F}{\partial Y}(X,Y)\beta(Y)$$

and

$$\delta_a g(X) \cdot h([a]_F(X)) + \beta([a]_F(X)) = \frac{\partial [a]_F}{\partial X}(X) \cdot \beta(X).$$

Rewrite now both equations in terms of $\beta(X) = h(X)\gamma(X)$ with $\gamma(X) \in R[[X]]$ (this is possible as $h(X) \in R[[X]]^\times$). By (Equation (11))

$$h(F(X,Y)) = \frac{\partial F}{\partial X}(X,Y)h(X),\ h(F(X,Y)) = \frac{\partial F}{\partial Y}(X,Y)h(Y)$$

and similarly[11]

$$a \cdot h([a]_F(X)) = \frac{\partial [a]_F}{\partial X}(X) \cdot h(X)$$

which yields that

$$\Delta g(X,Y)h(F(X,Y))+h(F(X,Y))\gamma(F(X,Y)) = h(F(X,Y))\gamma(X)+h(F(X,Y))\gamma(Y)$$

and

$$\delta_a g(X)h([a]_F(X)) + h([a]_F(X))\gamma([a]_F(X)) = ah([a]_F(X))\gamma(X)$$

Thus,

$$\Delta g(X,Y) = \Delta\gamma(X,Y),\ \delta_a g(X) = \delta_a\gamma(X),\ a \in A,$$

as $h(X) \in R[[X]]^\times$. We can conclude that

$$g(X) = \gamma(X) + r\log_F(X)$$

for some $r \in R$ (as $g'(0) \in R$). Similarly, the final assertions follow from Lemma 5.5 and the 5-lemma. □

In order to analyze $M(-)^\vee$ further we develop a suitable normal form for formal A-module laws over π-torsion free A-algebras.

[11]This follows by taking the derivative of $f([a]_F(X)) = af(X)$ using $f'(X) = \frac{1}{h(X)}$.

5.3. **A-typical formal A-modules.** Let A be as before a complete discrete valuation ring with finite residue field k of characteristic p and cardinality q. We fix a uniformizer $\pi \in A$. Let K be the fraction field of A. Let R be an A-algebra and let $F \in R[[X,Y]]$ be a formal A-module law. If R is π-torsion free we need a suitable normal form for F in the following.

Definition 5.7. *Assume that R is π-torsion free. We call F an A-typical formal A-module if*

$$\log_F(X) = \sum_{i=0}^{\infty} b_i X^{q^i}.$$

for some $b_0, b_1, \ldots \in R_K := R \otimes_A K$.

In particular, we can deduce that

$$[\zeta]_F(X) = \zeta \cdot X$$

for each $q-1$-th root of unity in A, and that

$$[\pi]_F(X) = \sum_{i=0}^{\infty} r_i X^{q^i}$$

for some $r_0, r_1, \ldots \in R$.

Lemma 5.8. *Assume that R is π-torsion free, and that $F \in R[[X,Y]]$ is an A-typical formal A-module law. Then there exist $b_0 = 1, b_1, \ldots R, v_0 = \pi, v_1, \ldots \in R$ such that*

$$\log_F(X) = \sum_{i=0}^{\infty} b_i X^{q^i},$$

$$[\pi]_F(X) \equiv v_i X^{q^i} \bmod (v_0, \ldots, v_{i-1}) + (X,Y)^{q^i+1},\ i \geq 0,$$

and

$$\pi b_k = b_0 v_k + b_1 v_{k-1}^q + b_2 v_{k-2}^{q^2} \ldots + b_{k-1} v_1^{q^{k-1}}$$

for $k \geq 1$. In particular, $\pi^i \cdot b_i \in R$ for $i \geq 1$.

This proves that our definition of being A-typical agrees with the one used in [HG94].

Proof. We already know that

$$\log_F(X) = b_0 X + b_1 X^q + b_2 X^{q^2} + \ldots$$

for some $b_0 = 1, b_1, b_2, \ldots \in R$. Writing F as the image of the universal formal A-module we find $v_0 = \pi, v_1, \ldots \in R$ such that

$$[\pi]_F(X) \equiv v_i X^{q^i} \bmod (v_0, v_1, \ldots, v_{i-1}) + (X,Y)^{q^i+1}.$$

Assume that

$$\pi \cdot b_k = b_0 v_k + b_1 v_{k-1}^q + b_2 v_{k-2}^{q^2} \ldots + b_{k-1} v_1^{q^{k-1}}$$

for some $k \geq 0$. We know that

$$\pi \log_F(X) = \log_F([\pi]_F(X)).$$

Write

$$[\pi]_F(X) = \sum_{i=0}^{\infty} w_i X^{q^i}.$$

Then we can conclude

$$\pi \cdot b_{k+1} \equiv b_0 w_{k+1} + b_1 w_k^q + \ldots + b_k w_1^{q^{k-1}} \bmod (\pi).$$

Using that w_i lies in the ideal $(v_0, v_1, \ldots, v_k)$ of R it is clear that we can redefine v_{k+1}, such that

$$\pi \cdot b_{k+1} \equiv b_0 v_{k+1} + b_1 v_k^q + \ldots + b_k v_1^{q^k}$$

and

$$[\pi]_F(X) \equiv v_{k+1} X^{q^{k+1}} \equiv w_{k+1} X^{q^{k+1}} \bmod (v_0, v_1, \ldots, v_k) + (X, Y)^{q^{k+1}+1}.$$

By induction we can prove the final statement that $\pi^i b_i \in R$. This finishes the proof. □

We will use the following fact.

Lemma 5.9. *Each formal A-module over R is isomorphic to an A-typical one. Moreover, we may assume that the isomorphism reduces to the identity on some quotient R/I of R, if the base change to R/I is already A-typical for some ideal $I \subseteq R$.*

Proof. Cf. [HG94, Section 5] resp. [Haz78, 21.5.6]. □

Remark 5.10. Set $R = A[v_1, v_2, \ldots]$ and define $f(X) \in R_K[[X]]$ as the unique power series satisfying

$$f(X) = X + \sum_{i=1}^{\infty} \frac{v_i}{\pi} f^{q^i}(X^{q^i}),$$

where f^{q^i} denotes the power series with v_j replaced by $v_j^{q^i}$ for $j \geq 1$. Equivalently,

$$f(X) = \sum_{i=0}^{\infty} b_i X^{q^i}$$

with $b_0 = 1, b_1, \ldots \in R$, and

$$\pi b_k = b_0 v_k + b_1 v_{k-1}^q + b_2 v_{k-2}^{q^2} \ldots + b_{k-1} v_1^{q^{k-1}}$$

for $k \geq 1$. Then f is the logarithm of a formal A-module F over $A[v_1, v_2, \ldots]$, called the universal formal A-module (law). This is a particular case of Hazewinkel's integrality lemma in this case, cf. [Haz78, Section 2], [HG94, Proposition 5.7.].

Remark 5.11. Let $h \geq 1$ and with the notation from Remark 5.10 consider the A-algebra homomorphism

$$R \to A$$

sending v_j to 0 if $j \neq h$ and v_h to 1. The image $g(X) \in A[[X]]$ of $f(X) \in R[[X]]$ under this homomorphism satisfies

$$g(X) = X + \frac{1}{\pi} g(X^{q^h}),$$

i.e.,

$$g(X) = X + \frac{X^{q^h}}{\pi} + \frac{X^{q^{2h}}}{\pi^2} + \ldots.$$

We claim that[12]

$$g^{-1}(\pi g(X)) \equiv X^{q^h} \bmod \pi,$$

or equivalently

$$\pi g(X) = g(X^{q^h} + \pi\gamma(X))$$

for some $\gamma(X) \in A[[X]]$. We prove the last statement via approximation modulo powers of X. Thus assume that $\gamma_n(X) \in A[[X]]$ is found such that

$$\pi g(X) \equiv g(X^{q^h} + \pi\gamma_n(X)) \bmod (X)^n$$

(clearly this can be done for $n = 1$). Set

$$\gamma_{n+1}(X) = \gamma_n(X) + a_n X^n.$$

Then

$$g(X^{q^h} + \pi\gamma_{n+1}(X)) \equiv g(X^{q^h} + \pi\gamma_n(X)) + \pi a_n X^n \bmod (X)^{n+1}$$

as $g'(0) = 1$, and we want that this agrees with

$$\pi g(X) = \pi X + g(X^{q^h})$$

modulo $(X)^{n+1}$. Hence it suffices to see that $g(X^{q^h} + \pi\gamma_n(X)) - g(X^{q^h})$ has coefficients in πA. Let $i \geq 0$. Then

$$(X^{q^h} + \pi\gamma_n(X))^{q^i} = X^{q^{h+i}} + \pi^{i+1}\delta_n(X)$$

for some $\delta(X) \in A[[X]]$ by the binomial formula. This implies that

$$\frac{1}{\pi^i}(X^{q^h} + \pi\gamma_n(X))^{q^i} - \frac{1}{\pi^i}X^{q^{h\,i}} = \pi \cdot \delta_n(X)$$

as desired.

We can conclude that one of the formal A-modules F_h of height h, whose existence we proved in Lemma 2.4 via the Lubin-Tate lemma Lemma 1.14, can be chosen to have logarithm $g(X)$, i.e.,

$$F_h(X,Y) := g^{-1}(g(X) + g(Y)),\ [a]_{F_h}(X) = g^{-1}(ag(X)),\ a \in A,$$

because we proved that with this definition $F_h, [a]_{F_h}, a \in A$, have coefficients in A and

$$g^{-1}(\pi g(X)) \equiv X^{q^h} \bmod \pi.$$

In [HG94, Section 13] this formal A-module is also called the canonical lifting.

In the A-typical case we can derive an easier description of the module of quasi-logarithms $M(\mathcal{G})^\vee$.

Lemma 5.12 ([HG94, Proposition 8.12])**.** *Let R be π-torsion free, and $F \in R[[X,Y]]$ an A-typical π-divisible formal A-module law. Then each class in*

$$M(\mathcal{G}_F)^\vee$$

can be represented by a quasi-logarithm which has the form $g(X) = \sum_{i=0}^{\infty} m_i X^{q^i}$ with $\pi^i \cdot m_i \in R$ for each $i \geq 0$.

Proof. This follows from Lemma 5.9 and Lemma 5.3 by Lemma 5.8. □

[12]We think that the argument for this in [Haz78, (8.3.4.)] is wrong as the calculation is made mod π, but the $f(X)$ in loc. cit. has coefficients in K.

We now explain why $M(\mathcal{G})^\vee$ only depends on the reduction of $\mathcal{G}$ resp. F to R/π. The following lemma is crucial for everything that follows.

Lemma 5.13. *Let $g(X) \in R_K[[X]]$ be a quasi-logarithm for F, $f_1, f_2 \in R[[X,Y]]$ power series with no constant term with $f_1 \equiv f_2 \ mod\ \pi$. Then*

$$g(f_2(X,Y)) - g(f_1(X,Y))$$

has coefficients in R.

Proof. By Lemma 5.9 we may assume that F is A-typical. Write

$$f_2(X,Y) = f_1(X,Y) + h(X,Y)$$

with $h \in R[[X,Y]]$ having coefficients in $\pi \cdot R$, and

$$g(X) = \sum_{i=0}^{\infty} m_i X^{q^i},$$

cf. Lemma 5.12. Then (supressing the variables X, Y)

$$\begin{aligned} & g(f_2) - g(f_1) \\ =& g(f_1 + h) - g(f_1) \\ =& \sum_{i=0}^{\infty} m_i ((f_1+h)^{q^i} - f_1^{q^i}) \\ =& \sum_{i=0}^{\infty} m_i \sum_{j=1}^{q^i-1} \binom{q^i}{j} h^j f_1^{q^i-j}. \end{aligned}$$

Now the claim follows from the fact that $\pi^i m_i \in R$ and

$$\binom{q^i}{j} \pi^j \in \pi^{i+1} R$$

for all $1 \leq j \leq q^i - 1$, cf. Lemma 5.8.[13] □

Proposition 5.14. *Let $F_1, F_2 \in R[[X,Y]]$ two formal A-modules laws with $\mathcal{G}_i := \mathcal{G}_{F_i}, i = 1,2$. Let $f_1, f_2 \in R[[X]]$ such that*

$$f_j(F_1(X,Y)) \equiv F_2(f_j(X), f_j(Y)) \ mod\ \pi,$$

$$f_j([a]_{F_1}(X)) \equiv [a]_{F_2}(f_j(X)) \ mod\ \pi,$$

and

$$f_1 \equiv f_2 \ mod\ \pi.$$

Then $g(X) \mapsto (g(f_j(X)), j = 1,2$, induce the same, well-defined R-linear map

$$M(\mathcal{G}_2)^\vee \to M(\mathcal{G}_1)^\vee$$

This proposition can interpreted as the statement that the functor $M(-)^\vee$ is "crystalline".

[13] To see this last statement apply the following observation to $R = A[X]$, $a = 1 + \pi \cdot X, b = 1$: Let R be some A-algebra and $a, b \in R$ such that $a \equiv b \bmod \pi$. Then $a^{q^i} \equiv b^{q^i} \bmod \pi^{i+1}$.

Proof. Let $g(X) \in R_K[[X]]$ be a quasi-logarithm for F_2. We first show that

$$g(f_1(X))$$

is a quasi-logarithm for F_1. Lemma 5.13 applied to $f_1(F_1(X,Y)), F_2(f_1(X), f_1(Y))$ shows that

$$g(f_1(F_1(X,Y)) - g(F_2(f_1(X), f_1(Y))$$

has coefficients in R, and similarly for the formal multiplication. This implies that $g \mapsto g(f_1(X))$ defines a well-defined map

$$f_1^* \colon M(\mathcal{G}_2)^\vee \to M(\mathcal{G}_1)^\vee.$$

Lemma 5.13 applied to f_1, f_2 shows then that $f_1^* = f_2^*$ on $M(\mathcal{G}_2)^\vee$. □

Let $\mathcal{G}_0$ be a π-divisible formal A-module over R/π. In particular, we can deduce that

$$\mathcal{G}_0 \to M(\mathcal{G})^\vee$$

is functorial for morphisms between formal A-modules over R/π, and that

$$\mathcal{G}_0 \mapsto M(\mathcal{G}_0)^\vee := M(\mathcal{G})^\vee$$

with $\mathcal{G}$ any lift of $\mathcal{G}_0$ to R, defines a well-defined functor. We set

$$M(\mathcal{G}_0) := \mathrm{Hom}_R(M(\mathcal{G}_0)^\vee, R).$$

If $\mathcal{G}$ is any lift of $\mathcal{G}_0$, then by Lemma 5.6 we have a natural surjection

$$M(\mathcal{G}_0) \to \mathrm{Lie}(\mathcal{G}).$$

Morever, $M(\mathcal{G}_0)$ is of rank equal to the height of the π-divisible formal A-module $\mathcal{G}_0$.

In particular, the construction of the Gross-Hopkins period morphism

$$\pi_{\mathrm{GH}} \colon \mathcal{M}_\eta^{\mathrm{ad}} \to \mathbb{P}(M(\mathcal{G}_h) \otimes_A K)^{\mathrm{ad}}$$

is finished, cf. Section 5.1.

Let us note that there a priori exist two A-module structures on $M(\mathcal{G}_0)$: one via the A-action on $\mathcal{G}_0$ and the other via the natural R-module structure on quasi-isomorphisms and the homomorphism $A \to R$. As $ag(X) - g([a]_F(X))$ has coefficients in R for any quasi-logarithm g, we see that both A-actions coincide.

5.4. π_{GH} **is étale and surjective.** Fix $A, F_h, \pi, K, \mathcal{M}$ etc. as in Section 5.1. We want to show that the Gross-Hopkins period morphism

$$\pi_{\mathrm{GH}} \colon \mathcal{M}_\eta^{\mathrm{ad}} \to \mathbb{P}(M(\mathcal{G}_h) \otimes_A K)^{\mathrm{ad}}$$

is étale and surjective.

We first prove that it is étale in the sense that π_{GH} induces an isomorphism on tangent spaces. Let us recall how to describe the tangent space of projective space. Let S be any ring and let M be a finite, projective S-module. The projective space $\mathbb{P}(M)$ associated with M represents the functor

$$\mathrm{Alg}_S \to (\mathrm{Sets})$$

sending an S-algebra T to the isomorphism class of pairs (L, γ) with L an invertible T-module and $\gamma \colon M \otimes_S T \twoheadrightarrow L$ a surjection. Given any section $z \in \mathbb{P}(M)(T)$ represented by the surjection $\varphi \colon M \twoheadrightarrow L$ the tangent space at z

$$T_z(\mathbb{P}(M)) := \mathbb{P}(M)(T[\varepsilon]) \times_{\mathbb{P}(M)(T)} \{z\}$$

identifies canonically with

$$\mathrm{Hom}_R(M,L)/(T\cdot\varphi)$$

by sending $\psi\colon \mathrm{M}\to L$ to the surjection

$$\varphi+\varepsilon\cdot\psi\colon M[\varepsilon]\to L[\varepsilon].$$

We can similarly describe the tangent space of a section of an adic projective space. Given a complete sheafy Huber pair (B,B^+) over (K,A), and a section $x\in\mathcal{M}_\eta^{\mathrm{ad}}(B,B^+)$ represented by a pair

$$(\mathcal{G},\alpha)\in\mathcal{M}(B_0)$$

for some ring of definition $B_0\subseteq B^+\subseteq B$, then the tangent space

$$T_x\mathcal{M}_\eta^{\mathrm{ad}}$$

identifies with

$$\mathcal{D}ef_{\mathcal{G}}(B_0[\varepsilon])\otimes_{B_0}B.$$

The étaleness of π_{GH} is then implied by the following statement.

Lemma 5.15. *For any $x,B_0,\mathcal{G},\dots$ as above the map B-linear map*

$$T_x\mathcal{M}_\eta^{\mathrm{ad}}\to T_{\pi_{\mathrm{GH}}}\mathbb{P}(M(\mathcal{G}_h)\otimes_A K)^{\mathrm{ad}}$$

is an isomorphism.

Proof. The Gross-Hopkins period morphims is induced by the natural surjection

$$\varphi\colon M:=M(\mathcal{G}_h)\otimes_A B\cong M(\mathcal{G})\otimes_{B_0}B\to L:=\mathrm{Lie}(\mathcal{G})\otimes_{B_0}B$$

dual to the inclusion $\omega(\mathcal{G})\to M(\mathcal{G})^\vee$ By Lemma 5.6 we get

$$\mathrm{Hom}(M,L)/B\varphi\cong M^\vee\otimes_B L/B\varphi\cong\mathcal{D}ef_{\mathcal{G}}(B_0[\varepsilon])\otimes_{B_0}B,$$

which is $T_x\mathcal{M}_\eta^{\mathrm{ad}}$. Unravelling the definitions of these identifications shows that π_{GH} induces the identity on tangent spaces. □

To show surjectivity of π_{GH} we will make π_{GH} more explicit. Recall that

$$\mathcal{M}=\coprod_{n\in\mathbb{Z}}\mathcal{M}_{\mathrm{RZ},n}$$

is a disjoint union and that

$$\mathcal{M}_0:=\mathcal{M}_{\mathrm{RZ},0}\cong\mathcal{M}_{F_h}\cong\mathrm{Spf}(A[[X_1,\dots,X_{h-1}]]),$$

where $\mathcal{M}_{F_h}$ is the Lubin-Tate space defined in Section 2.2.

Let R be a π-complete, π-torsion free A-algebra and set $R_K:=R\otimes_A K$. Assume that $(\mathcal{G},\alpha)\in\mathcal{M}(R)$, i.e., $\mathcal{G}$ is a formal A-module over R and

$$\alpha\colon\mathcal{G}\hat{\otimes}_R R/\pi\dashrightarrow\mathcal{G}_h\hat{\otimes}_k R/\pi$$

is a quasi-isogeny. Fix some $n\gg 0$ such that $[\pi]^n_{\mathcal{G}}\circ\alpha^{-1}=\alpha^{-1}\circ[\pi]^n_{\mathcal{G}_h}$ is an isogeny

$$[\pi]^n_{\mathcal{G}}\circ\alpha^{-1}\colon\mathcal{G}_h\hat{\otimes}_k R/\pi\to\mathcal{G}\hat{\otimes}_R R/\pi.$$

We may write $\mathcal{G}=\mathcal{G}_F$ associated to some formal A-module law $F\in R[[X,Y]]$, and then lift $[\pi]^n_{\mathcal{G}}\circ\alpha^{-1}$ to some power series

$$f_{[pi]^n_{\mathcal{G}}\circ\alpha^{-1}}(X)\in R[[X]].$$

The pullback $g(X)\mapsto g(f_{[\pi]^n_{\mathcal{G}}\circ\alpha^{-1}}(X))$ defines the morphism

$$M([\pi]^n_{\mathcal{G}}\circ\alpha^{-1})^\vee\colon M(\mathcal{G})^\vee=M(\mathcal{G}\hat{\otimes}_R R/\pi)^\vee\to M(\mathcal{G}_h)^\vee\otimes_A R$$

and then $M(\alpha^{-1})^\vee = \frac{1}{\pi^n} M([\pi]^n_{\mathcal{G}} \circ \alpha^{-1})^\vee$. Assume now that

$$c_0, c_1, \dots, c_{h-1} \colon M(\mathcal{G}_h)^\vee \to A$$

form a basis of $M(\mathcal{G}_h) = \mathrm{Hom}_A(M(\mathcal{G}_h)^\vee, A)$. Let R_K^+ be the integral closure of R in R_K, and assume that R_K is sheafy. Then

$$\mathcal{M}(R) \subseteq \mathcal{M}_\eta^{\mathrm{ad}}(R_K, R_K^+)$$

and

$$\pi_{\mathrm{GH}}(\mathcal{G}, \alpha) \in \mathbb{P}(M(\mathcal{G}_h) \otimes_A K)^{\mathrm{ad}}(R_K, R^+) \overset{(c_0,\dots,c_{h-1})}{\cong} \mathbb{P}_K^{h-1,\mathrm{ad}}(R_K, R^+)$$

is given by the point

$$[c_0(M(\alpha)^{-1}(\log_F)) : c_1(M(\alpha)^{-1} \log_F) : \dots : c_{h-1}(M(\alpha)^{-1}(\log_F)]$$

because $R \cdot \log_F(X) \subseteq M(\mathcal{G})^\vee$ is the image of the canonical morphism $\omega(\mathcal{G}) \subseteq M(\mathcal{G})^\vee$. As a side remark we can see here very concretely that the image of $(\mathcal{G}, \alpha)$ does not depend on the formal A-module law F because for different choices of F the logarithm $\log_F(X)$ changes by a multiple.

Assume now that $(\mathcal{G}, \alpha) \in \mathcal{M}_0(R) \subseteq \mathcal{M}(R)$. By Proposition 3.18 we may then find a $\star$-deformation $F \in R[[X, Y]]$ of F_h such that $\mathcal{G} = \mathcal{G}_F$ and α corresponds to identity modulo some ideal $I \subseteq R$ with $\pi \in I$ and $I/(\pi) \subseteq R/\pi$ nilpotent. The same holds then for α^{-1} and because $[\pi]_{\mathcal{G}_h}(X) = X^{q^h}$ we may take

$$f_{[\pi]^n_{\mathcal{G}} \circ \alpha^{-1}}(X) = X^{q^{nh}}$$

for some $n \gg 0$ (the power series $X^{q^{nh}}$ is the n-fold composition of X^{q^h}). Concretely, if $I^{q^{mh}} \subseteq (\pi)$, then $X^{q^{mh}}$ defines a morphism $F \to F_h$ over $R/(\pi)$. By arguments as in Lemma 3.16 we may then find n. The map

$$M(\alpha^{-1})^\vee \colon M(\mathcal{G})^\vee \otimes_R R_K \cong M(\mathcal{G}_h)^\vee \otimes_A R_K$$

sends a quasi-logarithm $g(X)$ for F to

$$\frac{1}{\pi^n} g(X^{q^{nh}}).$$

More canonically, we can write this as

$$g(X) \mapsto \lim_{n \to \infty} \frac{1}{\pi^n} g(X^{q^{nh}}) \in M(\mathcal{G}_h)^\vee \otimes_A R_K$$

and the limit is eventually constant.

Now we have to calculate $M(\mathcal{G}_h)^\vee$ and construct a suitable basis

$$c_0, c_1, \dots, c_{h-1} \in M(\mathcal{G}_h).$$

For this we calculate the quasi-logarithms in the universal A-typical case. Let

$$F_{\mathrm{A-typ}} \in A[v_1, v_2, \dots]$$

be the universal A-typical formal A-module constructed in Remark 5.10, i.e., the logarithm $f_{\mathrm{A-typ}} \in X \cdot K[v_1, v_2, \dots][[X]]$ of $F_{\mathrm{A-typ}}$ satisfies the functional equation

$$f_{\mathrm{A-typ}}(X) = X + \sum_{i=1}^{\infty} \frac{v_i}{\pi} f_{\mathrm{A-typ}}^{q^i}(X^{q^i}).$$

For each $i \geq 1$ consider the base change F_i of $F_{\mathrm{A-typ}}$ along the map

$$A[v_1, v_2, \dots] \to A[v_1, v_2, \dots][\varepsilon],$$

which maps v_j to v_j if $i \neq j$ and v_i to $v_i + \varepsilon$. We can write the logarithm of F_i in the form

$$f_{\mathrm{A-typ}}(X) + \varepsilon g_i(X)$$

with $g_i(X)$ a quasi-logarithm for $F_{\mathrm{A-typ}}$ by Lemma 5.3. Concretely,

$$g_i(X) = \frac{\partial f}{\partial v_i}(X) \in K[v_1, v_2, \ldots][[X]].$$

Let $F_{\mathrm{LT,h}} \in A[[X, Y]]$ be the Lubin-Tate formal A-module whose logarithm is

$$f_0(X) := X + \frac{X^{q^h}}{\pi} + \frac{X^{q^{2h}}}{\pi^2} + \ldots,$$

cf. Remark 5.11. This is the specialization of the universal A-typical formal A-module along the map

$$A[v_1, \ldots] \to A$$

sending v_j to 0 if $j \neq h$ and v_h to 1 because $f_0(X)$ is the unique solution of the functional equation

$$f_0(X) = X + \frac{1}{\pi} f_0(X^{q^h})$$

with vanishing constant term. For $i \geq 1$ the above quasi-logarithm $g_i(X)$ specializes and yields the quasi-logarithm

$$f_i(X) := \frac{1}{\pi} f_0(X^{q^i}),\ i = 1, \ldots, h-1.$$

for $F_{\mathrm{LT},h}$. Indeed, this follows easily from the functional equation for $f_{\mathrm{A-typ}}$ and the fact that $g_i(X)$ is the v_i-derivative of $f_{\mathrm{A-typ}}$. By Lemma 5.6 and the construction of the g_i we can deduce that

$$M(\mathcal{G}_h)^\vee = \langle f_0, f_1, \ldots, f_{h-1} \rangle_A,$$

or more precisely that the classes of $f_0, f_1, \ldots, f_{h-1}$ form a basis of $M(\mathcal{G}_h)^\vee$. Note that the map $g(X) \mapsto g(X^q)$ defines an endomorphism $\varphi_{M(\mathcal{G}_h)^\vee}$ of $M(\mathcal{G}_h)^\vee$ by Proposition 5.14 (as X^q lifts the Frobenius on $\mathcal{G}_h$). Let A_h be the ring of integers in the unramified extension K_h of K of degree h and let k_h be the residue field of A. Then A_h acts on $F_{\mathrm{LT},h} \hat{\otimes}_k k_h$. Concretely, if $\zeta \in A_n$ is a $q^h - 1$-th root of unity, then ζ acts via the power series ζX. Namely, it follows directly from the functional equation

$$f_0(X) = X + \frac{1}{\pi} f_0(X^{q^h})$$

for the logarithm $f_0(X)$ of $F_{\mathrm{LT},h}$ that $f_0(\zeta X) = \zeta f_0(X)$. Let $\sigma \colon A_h \to A_h$ the lift of the q-Frobenius. Then A_h acts on $f_i \in M(\mathcal{G}_h) \otimes_A A_h$ via the morphism σ^i. Indeed, it suffices to check this for a $q^h - 1$-th root of unity $\zeta \in A_h$, where it follows from the fact that $\sigma(\zeta) = \zeta^q$ and the definition of f_i.

Let $c_0, \ldots, c_{h-1} \in M(\mathcal{G}_h) \otimes_A K$ be the dual basis of $f_0, \ldots, f_{h-1} \in M(\mathcal{G}_h)^\vee$. From the definition of the f_i we see that

$$c_0(g(X)) = \lim_{n \to \infty} \pi^n m_{hn} \in K$$

and

$$c_i(g(X)) = \lim_{n \to \infty} \pi^{n+1} m_{hn+1} \in K$$

for $i = 1, \leq, h-1$, if $g(X) = \sum_{i=0}^{\infty} m_i X^{q^i}$ is a quasi-logarithm for $F_{\mathrm{LT},h}$, cf. Lemma 5.12. In particular, the limit above exists for $i = 0, \dots, h-1$ and only depends on the class of $g(X)$ in $M(\mathcal{G}_h)^\vee$.

Let us come back to the pair $(\mathcal{G}, \alpha) \in \mathcal{M}_0(R)$ represented by the $\star$-deformation F of F_h. We may assume that F is A-typical by Lemma 5.9. Let

$$g(X) = \sum_{i=0} m_i X^{q^i}$$

be a quasi-logarithm for F. We can conclude that

$$\begin{aligned} & M(\alpha^{-1})(g(X)) \\ =& \lim_{n\to\infty} \frac{1}{\pi^n} g(X^{q^{hn}}) \\ =& \frac{1}{\pi^n} \sum_{i=0}^{\infty} m_i X^{q^{hn+i}} \end{aligned}$$

for $n \gg 0$ and thus

$$\begin{aligned} & c_0(M(\alpha^{-1})(g(X))) \\ =& \lim_{j\to\infty} \frac{1}{\pi^n} \pi^j m_{h(j-n)} \\ =& \lim_{j\to\infty} \pi^j m_{hj} \end{aligned}$$

and

$$\begin{aligned} & c_k(M(\alpha^{-1})(g(X))) \\ =& \lim_{j\to\infty} \frac{1}{\pi^n} \pi^{j+1} m_{h(j-n)+k} \\ =& \lim_{j\to\infty} \pi^{j+1} m_{hj+k} \end{aligned}$$

for $k = 1, \dots, h-1$. Appyling this to $g(X) = \log_F(X)$ yields the homogeneous coordinates of $\pi_{\mathrm{GH}}(\mathcal{G}, \alpha)$. For example, the canonical lifting $\mathcal{G}_{F_{\mathrm{LT},h}}$ is sent to the point $[1 : 0 : \dots : 0]$. In general, we can be more concrete. Namely, consider the formal A-module

$$F_u \in A[[u_1, \dots, u_{h-1}]][[X, Y]],$$

which is the specialization of $F_{\mathrm{A-typ}} \in A[v_1, v_2, \dots][[X, Y]]$ along the morphism

$$A[v_1, v_2, \dots] \to A[[u_1, \dots, u_{h-1}]]$$

sending $v_i \mapsto u_i$ for $i = 1, \dots, h-1$, $v_h \mapsto 1$, and $v_i \mapsto 0$ for $i > h$. By Theorem 2.34 the resulting morphism

$$\mathrm{Spf}(A[[u_1, \dots, u_{h-1}]]) \to \mathcal{M}_0$$

is an isomorphism. The logarithm of $F_{\mathrm{A-typ}}$ has the form

$$f_{\mathrm{A-typ}}(X) = \sum_{i=0}^{\infty} b_i X^{q^i}$$

with $b_0 = 1$, and $b_k,\ k \geq 1$, defined via the recursive formula

$$\pi b_k = b_0 v_k + b_1 v_{k-1}^q + \dots + b_{k-1} v_1^{q^{k-1}}.$$

Let

$$\mathbb{D} := \mathrm{Spa}(K\langle \frac{u_1^h}{\pi^{h-1}}, \dots, \frac{u_{h-1}^h}{\pi^{h-(h-1)}}\rangle) \subseteq \mathrm{Spf}(A[[u_1, \dots, u_{h-1}]])^{\mathrm{ad}}_\eta,$$

i.e., $\mathbb{D}$ is the "polydisc" parametrizing (automatically topologically nilpotent) elements $u_1, \dots, u_{h-1}$ in a (complete, sheafy) Huber pair (B, B^+) over (K, A) such that $|u_i(x))|^h \leq |\pi(x)|^{h-i}$ for all $x \in \mathrm{Spa}(B, B^+)$ and $i = 1, \dots, h-1$.

For $\mathbb{P}_K^{h-1,\mathrm{ad}}$ we take the homogeneous coordinates $c_0, c_1, \dots, c_{h-1}$, i.e., generating sections of $\mathcal{O}(1)$. Let

$$w_i := \frac{c_i}{c_0},$$

which are coordinates of $\mathbb{A}_K^{h-1,\mathrm{ad}} \subseteq \mathbb{P}_K^{h-1,\mathrm{ad}}$. Set

$$\mathbb{D}' := \mathrm{Spa}(K\langle \frac{w_1^h}{\pi^{h-1}}, \dots, \frac{w_{h-1}^h}{\pi^{h-(h-1)}}\rangle) \subseteq \mathbb{P}_K^{h-1,\mathrm{ad}}.$$

Proposition 5.16. *The Gross-Hopkins period morphism restricts to an isomorphism*

$$\pi_{\mathrm{GH}} \colon \mathbb{D} \to \mathbb{D}'.$$

Proof. Set

$$R := A\langle \frac{u_1^h}{\pi^{h-1}}, \dots, \frac{u_{h-1}^h}{\pi^{h-(h-1)}}\rangle \cong A\langle T_1, \dots, T_{n-1}\rangle$$

with $T_i := u_i^h/\pi^{h-i}$, $i = 1, \dots, h-1$, and let $F \in R[[X, Y]]$ be the base change of the A-typical formal A-module F_u over $A[[u_1, \dots, u_{h-1}]]$ with its logarithm

$$\log_F(X) = \sum_{i=0}^{\infty} b_i X^{q^i}.$$

Set

$$c_0 := \lim_{n\to\infty} \pi^n b_{hn} \in R_K := R \otimes_A K$$

and

$$c_i := \lim_{n\to\infty} \pi^{n+1} b_{hn+i} \in R_K := R \otimes_A K$$

for $i = 1, \dots, h-1$. Define $u_h := 1$. We know by construction of the universal A-typical formal A-module $F_{\mathrm{A-typ}}$ that

$$\pi \cdot b_n = \sum_{0<j\leq h} u_j \sigma^j(b)_{n-j}, \tag{14}$$

with

$$\sigma \colon R \to R$$

the A-algebra homomorphism induced by $\sigma(u_i) = u_i^q$ for $i = 1, \dots, h-1$, and $b_n = 0$ for $n < 0$. We let

$$|-| := |-|_{\mathbb{D}}$$

be the maximum norm on R_K, cf. Lemma 4.26. In particular,

$$|u_i|^h = |\pi|^{h-i}$$

for $i = 1, \dots, h$. Let

$$\nu \colon R_K \to \mathbb{Q} \cup \{\infty\}$$

be the associated additive valuation, which we assume to be normalized such that $\nu(\pi) = 1$. This implies

$$\nu(u_i) = \frac{h-i}{h}$$

for $i = 1, \dots, h$. We claim that

$$\nu(\pi^{n+1} b_{hn+i}) = \frac{h-i}{h} \tag{15}$$

for $i = 1, \dots, h$, and $n \geq 0$. In the case $i = 1, n = 0$ we have

$$\nu(\pi b_1) = \nu(u_1) = \frac{h-1}{h}$$

as $b_1 = \frac{u_1}{\pi}$ by (Equation (14)). Thus assume that the statement is proven for every number $hm + j < hn + i$ with $j = 1, \dots, h$. Then we know that $\pi^{m+1} b_{hm+j} \in R$ and

$$\sigma(\pi^{m+1} b_{hm+j}) \equiv (\pi^{m+1} b_{hm+j})^q \bmod \pi R.$$

From the strong triangle inequality we can deduce

$$\nu(\sigma(\pi^{m+1} b_{hm+j})) = q\nu(\pi^{m+1} b_{hm+j})$$

From (Equation (14)) we get

$$\pi^{n+1} b_{hn+i} = \sum_{0 \to j \leq h} u_j \pi^n \sigma^j(b_{hn+i-j}).$$

We claim that for $i = 1, \dots, h$

$$\nu(\pi^{n+1} b_{hn+i}) = \nu(u_i \pi^n \sigma^i(b_{hn})),$$

which using induction (or that $b_0 = 1$ if $n = 0$) equals

$$\frac{h-i}{h} + q^i \frac{h}{h} = \frac{h-i}{h}.$$

To prove this last claim it suffices to see that

$$\nu(u_j \pi^n \sigma^j(b_{hn+i-j}) - \frac{h-i}{h} > 0$$

If $i < j$, then

$$\nu(u_j \pi^n \sigma^j(b_{hn+i-j})) - \frac{h-i}{h} = \frac{h-j}{h} + q^j \frac{h-(h-j+i)}{h} = \frac{(q^j-1)(j-1)}{h} > 0.$$

If $i > j$, then

$$\nu(u_j \pi^n \sigma^j(b_{hn+i-j})) - \frac{h-i}{h} = \frac{h-j}{h} + q^j \frac{h-i+j}{h} - 1 - \frac{h-i}{h} = \frac{(q^j-1)(h-(i-j))}{h} > 0.$$

This finishes the proof that

$$\nu(\pi^{n+1} b_{hn+i}) = \frac{h-i}{h}$$

for $i = 1, \dots, h$. In particular, we can deduce that

$$\nu(c_0) = 0, \nu(c_1) = \frac{h-1}{h}, \dots, \nu(c_{h-1}) = \frac{1}{h}$$

by passing to the limit over n. In particular, π_{GH} maps $\mathbb{D}$ to $\mathbb{D}'$. If we write

$$\mathbb{D}' \cong \mathrm{Spa}(K\langle w_1, \dots, w_{h-1} \rangle)$$

with indeterminants $w_1, \dots, w_{h-1}$, then π_{GH} is induced by the morphism

$$\alpha \colon A\langle w_1^h/\pi^{h-1}, \dots, w_{h-1}^h/\pi \rangle \to R \cong A\langle T_1, \dots, T_{h-1} \rangle, \ w_i \mapsto \frac{c_i}{c_0}$$

for $i = 1, \dots, h-1$. We saw above that

$$\nu(\pi^{n+1} b_{hn+i} - u_i \sigma^j(b_{hn})) > \frac{h-i}{h},$$

which together with $\nu(\sigma^j(b_{hn}) - 1) > 0$ (as was proven implicitly above) implies that

$$\nu(\alpha(w_i) - u_i) > \frac{h-i}{h}.$$

This in turn proves that α is an isomorphism. Indeed, as

$$A\langle w_1^h/\pi^{h-1}, \dots, w_{h-1}^h/\pi^1 \rangle, R$$

are π-complete and π-torsion free it suffices to prove this modulo π, where it follows from the fact that $\alpha(w_i^h/\pi^{h-i}) \equiv u_i^h/\pi^{h-i}$ for $i = 1, \dots, h-1$. This finishes the proof. □

In [Far10, Corollaire 11] Fargues reinterprets the domain $\mathbb{D}$ as the locus in $\mathcal{M}_{\text{ét}}^{\text{ad}}$ parametrizing the locus where the π-torsion in $\mathcal{G}$ is semistable (in the sense developed in [Far10]). We can now finish the proof the the main theorem of this course.

Theorem 5.17 ([HG94, Section 23])**.** *The Gross-Hopkins period map*

$$\pi_{\text{GH}} \colon \mathcal{M}_\eta^{\text{ad}} \to \mathbb{P}(M(\mathcal{G}_h) \otimes_A K)^{\text{ad}} \cong \mathbb{P}_K^{h-1,\text{ad}}$$

is étale and surjective. The same holds for its restriction to $\mathcal{M}_{\eta,0}^{\text{ad}}$.

Proof. Étaleness was proven in Lemma 5.15. Let

$$\Pi \colon \mathcal{G}_h \to \mathcal{G}_h$$

be the Frobenius isogeny. For surjectivity of π_{GH} it suffices to show that

$$\mathbb{P}_K^{h-1,\text{ad}} \subseteq \bigcup_{n \in \mathbb{Z}} \Pi^n \cdot \mathbb{D}'$$

for $\mathbb{D}'$ as in Proposition 5.16. Let C/K be any non-archimedean field extension and let

$$\nu \colon C \to \mathrm{R} \cup \{\infty\}$$

be its additive valuation, normalized such that $\nu(\pi) = 1$. For

$$[c_0 : c_1 : \ldots : c_{h-1}] \in \mathbb{P}_K^{h-1,\text{ad}}$$

any field valued point we have

$$\Pi \cdot [c_0 : c_1 : \ldots : c_{h-1}] = [\pi^{-1} c_1 : c_2 : \ldots : c_{h-1} : c_0] \in \mathbb{P}_K^{h-1,\text{ad}}.$$

Choose $i = 0, 1, \dots, h-1$ such that

$$\nu(c_i) + \frac{i}{h}$$

is minimal. Then

$$\Pi^i \cdot [c_0 : c_1 : \ldots : c_{h-1}] = [\pi^{-1} c_i : c_{i+1} : \ldots : c_{h-1} : c_0 : \pi^{-1} c_1 : \ldots : \pi^{-1} c_{i-1}]$$

lies in $\mathbb{D}'$. Indeed, we know that

$$\nu(c_j) + \frac{j}{h} \geq \nu(c_i) + \frac{i}{h}$$

for $j = 0, \dots, h-1$. If $j > i$, we can conclude

$$\nu(c_j) - \nu(\pi^{-1} c_i) \geq 1 + \frac{i}{h} - \frac{j}{h} = \frac{h - (j-i)}{h}.$$

If $i < j$, we can conclude

$$\nu(\pi^{-1} c_j) - \nu(\pi^{-1} c_i) \geq \frac{i}{h} - \frac{j}{h} = \frac{i-j}{h}$$

as desired. We are left with the statement that the restriction

$$\pi_{\mathrm{GH}} \colon \mathcal{M}_{\eta,0}^{\mathrm{ad}} \to \mathbb{P}_K^{h-1,\mathrm{ad}}$$

is surjective, too. For this it suffices by the above argument to show that if R is the ring of integers in a sufficiently large finite extension of K and

$$(\mathcal{G}, \alpha) \in \mathcal{M}_0(R),$$

then there exists a point $(\mathcal{G}', \alpha') \in \mathcal{M}_0(R)$ such that

$$\pi_{\mathrm{GH}}(\mathcal{G}, \Pi^{-1} \cdot \alpha) = \pi_{\mathrm{GH}}(\mathcal{G}', \alpha').$$

By [HG94, (23.19)] resp. [Lub67] there exists (for R sufficiently large) an isogeny

$$f \colon \mathcal{G} \to \mathcal{G}'$$

reducing to the Frobenius isogeny, with $\mathcal{G}' = \mathcal{G}_{F'}$ a $\star$-deformation of F_h. Let α' the unique quasi-isogeny such that we arrive at the commutative diagram

$$\begin{array}{ccccc}
M(\mathcal{G}_h)_K & \xrightarrow{M(\alpha^{-1})} & M(\mathcal{G})_K & \xrightarrow{\psi_{\mathcal{G}}} & \mathrm{Lie}(\mathcal{G})_K \\
\downarrow{\scriptstyle M(\Pi)} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\
M(\mathcal{G}_h)_K & \xrightarrow{M((\alpha')^{-1})} & M(\mathcal{G}')_K & \xrightarrow{\psi_{\mathcal{G}'}} & \mathrm{Lie}(\mathcal{G})_K,
\end{array}$$

where the subscripts denote base extension, and all vertical morphisms are isomorphisms. The composition

$$\psi_{\mathcal{G}} \circ M(\alpha^{-1}) \circ M(\Pi)$$

defines the point $\pi_{\mathrm{GH}}(\mathcal{G}, \Pi^{-1}\alpha)$ while the composition

$$\psi_{\mathcal{G}} \circ M((\alpha')^{-1})$$

defines the point $\pi_{\mathrm{GH}}(\mathcal{G}', \alpha')$. From the above commutative diagram we can conclude that both points define the same point in $\mathbb{P}(M(\mathcal{G}_h)_K)^{\mathrm{ad}}$. □

Via further calculations Gross and Hopkins prove in [HG94, Section 23] furthermore that via the action of the quasi-isogenies of $\mathcal{G}_h$ each point on $\mathcal{M}_\eta^{\mathrm{ad}}$ can be translated to lie in $\mathbb{D}$, cf. [HG94, Corollary 23.26], and they describe the fibers of π_{GH}, cf. [HG94, Proposition 23.28]. Namely, given any algebraically closed non-archimedean field extension C/K and a point $z \in \mathbb{P}_K^{h-1,\mathrm{ad}}(C)$ there is a non-canonical isomorphism

$$\pi_{\mathrm{GH}}^{-1}(x) \cong \mathrm{GL}_h(K)/\mathrm{GL}_h(A).$$

More precisely, by the argument in the end of Theorem 5.17 one can see that quasi-isogenious formal A-modules over $\mathcal{O}_C$ map to the same point under the Gross-Hopkins period morphism. Given any formal A-module $\mathcal{G}$ over $\mathcal{O}_C$ the isomorphism classes of formal A-modules over $\mathcal{O}_C$, which are quasi-isogenious to $\mathcal{G}$ are in bijection with $\mathrm{GL}_h(K)/\mathrm{GL}_h(A)$, cf. [Lub67].

References

[Dri74] Vladimir G Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561, 1974.

[Far] Laurent Fargues. An introduction to lubin-tate spaces and p-divisible groups.

[Far10] Laurent Fargues. La filtration de harder-narasimhan des schémas en groupes finis et plats. 2010.

[FF18] Laurent Fargues and Jean-Marc Fontaine. Courbes et fibrés vectoriels en théorie de Hodge p-adique. *Astérisque*, (406):xiii+382, 2018. With a preface by Pierre Colmez.

[Gol81] Robert Gold. Local class field theory via lubin-tate groups. *Indiana University Mathematics Journal*, 30(5):795–798, 1981.

[Gro60] Alexander Grothendieck. Éléments de géométrie algébrique: I. le langage des schémas. *Publications Mathématiques de l'IHÉS*, 4:5–228, 1960.

[Haz78] Michiel Hazewinkel. *Formal groups and applications*, volume 78. Elsevier, 1978.

[HG94] MJ Hopkins and BH Gross. Equivariant vector bundles on the lubin-tate moduli space. *Contemporary Mathematics*, 158:23–23, 1994.

[Hub93] Roland Huber. Continuous valuations. *Mathematische Zeitschrift*, 212(1):455–477, 1993.

[Hub94] R. Huber. A generalization of formal schemes and rigid analytic varieties. *Math. Z.*, 217(4):513–551, 1994.

[Laz55] Michel Lazard. Sur les groupes de lie formels à un paramètre. *Bulletin de la Société Mathématique de France*, 83:251–274, 1955.

[LT65] Jonathan Lubin and John Tate. Formal complex multiplication in local fields. *Annals of Mathematics*, pages 380–387, 1965.

[LT66] Jonathan Lubin and John Tate. Formal moduli for one-parameter formal lie groups. *Bulletin de la Société Mathématique de France*, 94:49–59, 1966.

[Lub67] Jonathan Lubin. Finite subgroups and isogenies of one-parameter formal lie groups. *Annals of Mathematics*, pages 296–302, 1967.

[Lur10] Jacob Lurie. Chromatic homotopy theory. *Lecture notes online*, 2010.

[Mor19] Sophie Morel. Adic spaces. *Lecture Notes. https://web. math. princeton. edu/˜ smorel/adic_notes. pdf*, 2019.

[RZ96] M. Rapoport and Th. Zink. *Period spaces for p-divisible groups*, volume 141 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1996.

[Sen69] Shankar Sen. On automorphisms of local fields. *Annals of Mathematics*, pages 33–46, 1969.

[Ser13] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.

[Sta17] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2017.

[Sut17] Andrew Sutherland. 18.785 number theory i, fall 2017. 2017.

[SW13] Peter Scholze and Jared Weinstein. Moduli of p-divisible groups. *Camb. J. Math.*, 1(2):145–237, 2013.

[SW20] Peter Scholze and Jared Weinstein. Berkeley lectures on p-adic geometry. In *Berkeley Lectures on p-adic Geometry*. Princeton University Press, 2020.

[Tia] Yichao Tian. Lectures on algebraic number theory.

[Vla76] G Vladimir. Drinfeld. coverings of p-adic symmetric domains. *Functional Analysis and its Applications*, 10(2):29–40, 1976.

[Yos08] Teruyoshi Yoshida. Local class field theory via lubin-tate theory. In *Annales de la Faculté des sciences de Toulouse: Mathématiques*, volume 17, pages 411–438, 2008.

Mathematisches Institut, Universität Bonn, Endenicher Allee 60, 53115 Bonn, Deutschland

E-mail address: `ja@math.uni-bonn.de`