32 Lubin-Tate formal groups

The local Artin reciprocity theorem (Theorem 29.1) whose proof was completed in the previous lecture implies that for every finite abelian extension of local fields $L/K$ we have a continuous surjective homomorphism

$$\theta_{L/K} : K^\times \rightarrow \text{Gal}(L/K)$$

whose kernel is the norm group $N(L^\times) := N_{L/K}(L^\times)$, which we note is an open subgroup of $K^\times$, since it is the kernel of a continuous homomorphism whose image has the discrete topology. The norm limitation theorem (Theorem 31.8) implies that every norm group is the norm group of a finite abelian extension. To complete the proof of local class field theory we need to prove the existence theorem (Theorem 27.8), which states that every finite index open subgroup of $K^\times$ arises as the norm group of a finite abelian extension $L/K$; if it exists the field $L$ is clearly unique, since it is the fixed field $(K^{ab})^{\theta_K(N(L^\times))}$.

The archimedean case is clear: any open subgroup of $\mathbb{R}_{>0}^\times$ must contain an open interval about 1, say $U = (1 - \epsilon, 1 + \epsilon)$ for some $\epsilon > 0$, but then it also contains $\cup_{n \geq 1} U^n = \mathbb{R}_{>0}^\times$, which has index 2, so the only open subgroups are since $\mathbb{R}_{>0}^\times$ and $\mathbb{R}^\times$, corresponding to the norm groups $N_{C/\mathbb{R}}(C)$ and $N_{\mathbb{R}/\mathbb{R}}(\mathbb{R})$.

We henceforth assume $K$ is a nonarchimedean local field, with valuation ring $\mathcal{O}_K$ and maximal ideal $\mathfrak{p}$. If we fix a uniformizer $\pi$ for $\mathfrak{p} = \langle \pi \rangle$, then we have an isomorphism

$$K^\times \simeq \mathcal{O}_K^\times \times \langle \pi \rangle,$$

and for every integer $n \geq 1$ we have an open subgroup of $K^\times$ defined by

$$U_{\pi,n} := (1 + \mathfrak{p}^n)\langle \pi \rangle.$$

If $U_{\pi,n}$ is a norm group, then there is a finite abelian extension $K_{\pi,n}/K$ with $N(K_{\pi,n}^\times) = U_{\pi,n}$.\(^1\) Local artin reciprocity implies that

$$[K_{\pi,n} : K] = [K^\times : U_{\pi,n}] = [\mathcal{O}_K^\times : 1 + \mathfrak{p}^n] = (q - 1)q^{n-1},$$

where $q := \#\mathcal{O}_K/\mathfrak{p}$ is the cardinality of the residue field; so see the last equality, consider the $\pi$-adic expansions of elements of $\mathcal{O}_K$. Note that $\pi \in N(K_{\pi,n}^\times)$ for all $n \geq 1$, and this implies that $K_{\pi,n}$ is totally ramified: the maximal unramified subextension $E$ of $K_{\pi,n}/K$ must satisfy $N(E^\times) \supseteq \langle \pi, \mathcal{O}_K^\times \rangle = K^\times$, since $\mathcal{O}_K^\times \subseteq N(E^\times)$ for any unramified extension (by Corollary 30.18) and $\pi \in N(K_{\pi,n}^\times) \subseteq N(E^\times)$, and this implies that $\text{Gal}(E/K)$ is trivial and therefore $E = K$, by local Artin reciprocity. It follows that $K_{\pi,1}/K$ is tamely ramified and $K_{\pi,n}/K$ is wildly ramified for all $n > 1$.

To prove the local existence theorem it suffices to construct the fields $K_{\pi,n}$ and show that they satisfy a certain compatibility with the local Artin homomorphism. More precisely, we have the following theorem, in which we assume that all separable extensions of $K$, including $K^{\text{unr}}$ and $K^{ab}$, are contained in a fixed separable closure $K^{\text{sep}}$.

**Theorem 32.1.** Let $K$ be a nonarchimedean local field, $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_K$, and let $q := \#\mathcal{O}_K/\mathfrak{p}$. Let $K_m$ be the unique unramified extension of $K$ of degree $m$ in $K^{\text{sep}}$ and let $\text{Frob}_K \in \text{Gal}(K_m^{\text{unr}}/K)$ denote the Frobenius element. Suppose that the following hold for every uniformizer $\pi$ of $\mathfrak{p}$:

\(^1\)We use $N(L^\times)$ as shorthand for $N_{L/K}(L^\times)$ for any finite extension $L/K$; in this case $L = K_{\pi,n}$.

Andrew V. Sutherland
(i) For every $n \in \mathbb{Z}_{\geq 1}$ there is an abelian extension $K_{\pi,n}/K$ of degree $(q - 1)q^{n-1}$ for which $\pi \in N(K_{\pi,n}^\times)$; define $K_{\pi,n,m} := K_{\pi,n}K_m$ and $U_{\pi,n,m} := (1 + p^n)[\langle \pi^m \rangle]$, and let $K_\pi := \bigcup_{n \geq 1} K_{\pi,n}$ and $K_\pi^{ab} := K_\pi^{unr}$.

(ii) There is a homomorphism $\theta_\pi : K^\times \to \text{Gal}(K_\pi^{ab}/K)$ such that $\theta_\pi(\pi)|_{K^{unr}} = \text{Frob}_K$ and $\theta_\pi(a)|_{K_{\pi,n,m}} = 1$ for all $a \in U_{\pi,n,m}$.

Suppose further that $K_\pi^{ab}$ and $\theta_\pi$ do not depend on the choice of $\pi$. Then $K_\pi^{ab} = K^{ab}$ and $\theta_\pi = \theta_K$, and every finite index open subgroup of $K^\times$ is a norm group.

Proof. The field $K_\pi^{ab}$ is abelian (it is a compositum of abelian extensions), thus $K_\pi^{ab} \subseteq K^{ab}$. We have $\theta_K(\pi) = \text{Frob}_K$, by Theorem 31.7, and $\pi \in N(K_{\pi,n})$, by (i), so $\theta_K(\pi) = \text{Frob}_K$ acts trivially on $K_{\pi,n}$, since $\pi \in N(K_{\pi,n}) = \ker(\theta_K|_{K_{\pi,n}})$.

By (ii), $\theta_\pi(\pi)$ also acts trivially on $K_{\pi,n}$, since $K_{\pi,n} = K_{\pi,n,1}$ and $\pi \in U_{\pi,n} = U_{\pi,n,1}$. It follows that $\theta_K(\pi)|_{K_\pi} = \theta_\pi(\pi)|_{K_\pi}$, since $K_\pi = \bigcup_{n \geq 1} K_{\pi,n}$.

We also have $\theta_\pi(\pi)|_{K^{unr}} = \text{Frob}_K = \theta_K(\pi)|_{K^{unr}}$, by (ii), therefore $\theta_\pi(\pi)|_{K_\pi^{ab}} = \theta_\pi(\pi)$. This holds for every uniformizer $\pi$, so for any uniformizer $\pi'$ we have

$$\theta_\pi(\pi') = \theta_\pi(\pi') = \theta_K(\pi')|_{K_\pi^{ab}},$$

under our assumption that $K_\pi^{ab} = K^{ab}$ and $\theta_\pi = \theta_K$. The uniformizers generate $K^\times$, therefore $\theta_\pi(x) = \theta_K(x)|_{K_\pi^{ab}}$ for all $x \in K^\times$.

We know that $\theta_\pi(a)$ acts trivially on $K_{\pi,n}$ for all $a \in U_{\pi,n,m}$, by (ii), hence so does $\theta_K(a)$ (by what we have just proved). Therefore $U_{\pi,n,m} \subseteq N(K_{\pi,n,m}^\times)$, by local Artin reciprocity. We also have

$$[K^\times : U_{\pi,n,m}] = [O_K^\times : 1 + p^n][\langle \pi \rangle : \langle \pi^m \rangle] = (q - 1)q^{n-1}m = [K_{\pi,n} : K][K_m : K] = [K_{\pi,n,m} : K] = [K^\times : N(K_{\pi,n,m})],$$

where we have used $K_{\pi,n} \cap K_m = K$ (since $K_{\pi,n}$ is totally ramified) and local Artin reciprocity. Thus $U_{\pi,n,m} = N(K_{\pi,n,m}^\times)$ is the norm group of $K_{\pi,n,m}$.

For any finite abelian extension $L/K$, the norm group $N(L^\times)$ is an open subgroup of $K^\times$. It thus contains $1 + p^n$ for all sufficiently large $n$ (these form a system of neighborhoods about 1 with radii tending to zero), and it also contains $\pi^{[L:K]}$, since $N_L/K(x) = x^{[L:K]}$ for every $x \in K^\times$. Thus $U_{\pi,n,m} \subseteq N(L^\times)$ for some $m, n \in \mathbb{Z}_{\geq 1}$. By Corollary 27.5 we have

$$L \subseteq K_{\pi,n,m} = K_{\pi,n}K_m \subseteq K_\pi^{unr} = K_\pi^{ab},$$

and therefore $K_\pi^{ab} = K^{ab}$. It follows that $\theta_\pi = \theta_K$, since we have shown that $\theta_\pi(x)$ and $\theta_K(x)$ agree on $K_\pi^{ab}$ for all $x \in K^\times$.

Now consider any finite index open subgroup $U \subseteq K^\times$. The intersection $U \cap \langle \pi \rangle$ must be nontrivial because $O_K^\times$ has infinite index in $K^\times \simeq O_K^\times \times \langle \pi \rangle$; thus $U$ contains $\langle \pi^m \rangle$ for some $m$. As noted above, the groups $1 + p^n$ form a fundamental system of neighborhoods about 1, so $U$ contains $1 + p^n$ for all sufficiently large $n$, and therefore $U_{\pi,n,m} \subseteq U$ for some $m, n \geq 1$. If we now let $H := \theta_{K_{\pi,n,m}}|_K(U)$ and consider the fixed field $L := K_H$, we have $N(L^\times) = U$, by local Artin reciprocity, thus $U$ is a norm group as claimed. \qed
To complete the proof of local class field theory, we need to construct fields \( K_{π,n} \) and a homomorphism \( θ_π \) that satisfy the hypotheses of Theorem 32.1; in particular, our construction must produce a totally ramified extension \( K_π := \bigcup_{n \geq 1} K_{π,n} \) such that \( K_{π}^{ab}K_πK^{\text{unr}} \) is independent of \( π \), as is the homomorphism \( θ_π : K^× → \text{Gal}(K_{π}^{ab}/K) \). We will use the theory of Lubin-Tate formal group laws to do this, following the presentation in [1, §1.2].

**Remark 32.2.** We should note that the totally ramified fields \( K_π \) do depend on \( π \); there is no unique maximal totally ramified abelian extension of \( K \). It is only the compositum \( K_π^{ab} := K_πK^{\text{unr}} \) that is independent of \( π \). This is directly analogous to the fact that the decomposition \( K^× \simeq \mathcal{O}_K^× \times \langle π \rangle \) depends on \( π \), in the sense that the isomorphism \( x \mapsto (x/π^ν(x), π^ν(x)) \) depends on \( π \), even though \( K^× \) does not.

### 32.1 Formal groups

Let \( A \) be a commutative ring and \( A[[T]] \) the ring of formal power series \( f(T) = \sum_{n \geq 0} a_n T^n \) with coefficients in \( A \). We should note that writing elements of \( A[[T]] \) as sums of terms \( a_n T_n \) is purely a notational convenience, we could equivalently view elements of \( A[[T]] \) as sequences indexed by \( \mathbb{Z}_{\geq 0} \) that we add component wise and multiply using convolutions: \((fg)_k := \sum_{i+j=k} f_i g_j \). In particular, we should not view elements of \( A[[T]] \) as functions.

In addition to the ring operations, we also have a composition operation \( f \circ g \) defined whenever the constant term of \( g \) is zero (without this restriction the constant term of \( f \circ g \) would be undefined; we cannot formally sum infinitely many elements of \( A \)). This still make sense when one of \( f \) or \( g \) is a power series in several variables. For any \( f \in A[[T]] \) and \( g \in A[[X_1, \ldots, X_r]] \) both with constant term zero we define

\[(f \circ g)(X_1, \ldots, X_r) := f(g(X_1, \ldots, X_r)), \quad (g \circ f)(X_1, \ldots, X_r) := g(f(X_1), \ldots, f(X_r)).\]

We note that the ideal \( TA[[T]] \) generated by \( T \) is precisely the set of univariate power series with constant term 0.

**Lemma 32.3.** Let \( A[[T]] \) be a formal power series ring over a commutative ring \( A \). The following hold:

(i) For all \( f \in A[[T]] \) and \( g, h \in TA[[T]] \) we have \( f \circ (g \circ h) = (f \circ g) \circ h \).

(ii) For each \( f \in TA[[T]] \) there exists \( g \in TA[[T]] \) such that \( f \circ g = T \) if and only if the coefficient of \( T \) in \( f \) is a unit in \( A \).

(iii) The elements of \( TA[[T]] \) for which the coefficient of \( T \) is a unit form a group under composition, with identity \( T \). In particular, \( f \circ g = T \) if and only if \( g \circ f = T \).

**Proof.** For (i) we note that \( f^n \circ g = (f \circ g)^n \) for all \( n \geq 0 \); this is clear for \( n = 0, 1 \) and for \( n > 1 \) we may inductively compute

\[f^n \circ g = (ff^{n-1}) \circ g = (f \circ g)(f^{n-1} \circ g) = (f \circ g)(f \circ g)^{n-1} = (f \circ g)^n\]

If \( f = a_n T^n \) then \( f \circ (g \circ h) = a_n (g \circ h)^n = a_n g^n \circ h = (f \circ g) \circ h \), and this extends to \( f = \sum a_n T^n \), since \( (f_1 + f_2) \circ (g \circ h) = f_1 \circ (g \circ h) + f_2 \circ (g \circ h) \) for all \( f_1, f_2 \in A[[T]] \).

For (ii), let \( f = \sum_{n \geq 1} f_n T^n \) be given; we will attempt to construct \( g = \sum_{n \geq 1} g_n T^n \) such that \( f \circ g = T \). We must have \( f_1 g_1 = 1 \), which is possible if and only if \( f_1 \) is a unit, which we now assume. We next require \( f_1 g_2 + f_2 g_1^2 = 0 \), which has a unique solution \( g_2 \) because
$f_1$ is a unit. Continuing in this fashion, $g_n$ is the unique solution to an equation of the form $f_1g_n + \cdots = 0$, and this determines the coefficients of $g \in A[[T]]$ satisfying $f \circ g = T$.

For (iii), it follows from (i) that we have a semigroup, it is clear that $T$ is a right identity, and (ii) implies the existence of right inverses; it follows that we have a group, so right inverses are also left inverses (and unique) and $T$ is the unique identity. 

\[\text{\begin{proof}
Lemma 32.5. A homomorphism } \phi: F \to G \text{ of formal group laws over a commutative ring } A \text{ is an isomorphism if and only if the coefficient of } T \text{ in } \phi \text{ is a unit in } A.
\end{proof}}\]

\[\text{\begin{proof}
By Lemma 32.3 part (ii), in order for } \phi \text{ to be an isomorphism the coefficient of } T \text{ in } \phi \text{ must be a unit, which we now assume. Let } \psi \in TA[[T]] \text{ be the inverse of } \phi \text{ under composition. Then } \phi \circ \psi = T = \psi \circ \phi, \text{ we just need to check that } \psi \in \text{Hom}(G,F). \text{ We have } G = G \circ \phi \circ \psi = \phi \circ F \circ \psi, \text{ so } \psi \circ G = \psi \circ \phi \circ F \circ \psi = F \circ \psi \text{ as desired.}
\end{proof}}\]

If $\phi: F \to G$ and $\psi: G \to H$ are homomorphisms of formal group laws, then so is their composition $\psi \circ \phi: F \to H$, and $\phi(T) = T$ is an automorphism of formal group laws that acts as the identity with respect to composition. If $\varphi: A \to B$ is a homomorphism of commutative rings and $F(X,Y) = X + Y + \sum_{i+j>1} a_{ij} X^i Y^j$ is a formal group law over $A$, then the power series $\varphi_*(F) := X + Y + \sum_{i+j \geq 1} \varphi(a_{ij}) X^i Y^j$ is a formal group law over $B$, and if $\phi(T) = \sum_{i+j \geq 1} a_i T_i$ is a homomorphism of formal group laws $\phi: F \to G$, then the power series $\varphi_*(\phi) := \sum_{i \geq 1} \varphi(a_i) T_i$ is a homomorphism of formal group laws $\varphi_*(\phi): \varphi_*(F) \to \varphi_*(G)$.

Proposition 32.6. Let $F \in A[[X,Y]]$ be a formal group law. The following hold:

(i) $F(X,0) = X$ and $F(0,Y) = Y$;

(ii) The is a unique $i_F \in T[A[[T]]$ such that $F(T, i_F(T)) = 0$;

If $A$ contains no nonzero torsion elements that are also nilpotent then also have

(iii) $F(X,Y) = F(Y,X)$.

\[\text{\begin{proof}
See Problem Set 2.
\end{proof}}\]

Formal groups laws that satisfy property (iii) of Proposition 32.6 are commutative; the proposition implies if $A$ is a reduced ring (an integral domain, for example), then all formal group laws over $A$ are commutative. This applies in all the rings of interest to us.
Example 32.7. The additive formal group law \( \mathbb{G}_a \) defined by \( \mathbb{G}_a(X, Y) = X + Y \) and the multiplicative formal group law \( \mathbb{G}_m \) defined by
\[
\mathbb{G}_m(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1
\]
are examples of formal group laws over any commutative ring \( A \).

Example 32.8. Let \( F \) be a commutative formal group law over a commutative ring \( A \). For each integer \( n \) inductively define the power series \( [n]_F \in TA[[T]] \) by putting \( [0]_F := 0 \),
inductively defining \( [n]_F(T) := F([n-1]_F(T), T) \) and \( [-n]_F(T) := i_F([-n]_F(T)) \) for \( n \geq 1 \).
One can show that \( [n]_F(T) \) is an endomorphism of the formal group law \( F \), and that it is an automorphism if and only if \( n \) is a unit in \( A^\times \).

If \( F(X, Y) \) is any formal group law on a commutative ring \( A \), the binary operation
\[
\phi +_F \psi := F(\phi(T), \psi(T))
\]
makes the set \( TA[[T]] \) into a group: closure and associativity follow from the definition of a formal group law, the identity element is 0 (by part (i) of Proposition 32.6), and inverses are given by \( -F \phi := i_F \circ \phi \), by part (ii) of Proposition 32.6.

Proposition 32.9. Let \( A \) be a commutative ring with no nonzero torsion nilpotents and let \( F \) and \( G \) be formal group laws over \( A \). The set of all homomorphisms \( \phi: F \to G \) is an abelian group \( \text{Hom}(F,G) \) under the operation \(+_G\), and the set of all endomorphisms \( \phi: F \to F \) with the addition operation \(+_F\) and multiplication given by composition is a (not necessarily commutative) ring \( \text{End}(F) \) with multiplicative identity \( T \) and unit group \( \text{Aut}(F) \) consisting of all automorphisms of the formal group law \( F \).

Proof. The hypothesis on \( A \) implies \( G(X, Y) = G(Y, X) \), by part (iii) of Proposition 32.6, so \(+_G\) is commutative. To prove the first statement we only need to show that \( \text{Hom}(F,G) \) is closed under \(+_G\), since \( TA[[T]] \) is an abelian group under \(+_G\). For any \( \phi, \psi \in \text{Hom}(F,G) \),
\[
(\phi +_G \psi)(F(X, Y)) = G(\phi(F(X,Y)), \psi(F(X,Y)))
\]
\[
= G(G(\phi(X), \phi(Y)), G(\psi(X), \psi(Y)))
\]
\[
= G(\phi(X), G(\phi(Y), G(\psi(X), \psi(Y))))
\]
\[
= G(\phi(X), G(\psi(X), \psi(Y)), \phi(Y))
\]
\[
= G(\phi(X), G(\psi(X), \psi(Y)), \phi(Y))
\]
\[
= G((\phi +_G \psi)(X), (\phi +_G \psi)(Y))
\]
(definition of \(+_G\))
\[
(\phi +_F \psi) \circ \varphi = F(\phi(T), \psi(T))(\varphi(T)) = F(\phi(\varphi(T)), \psi(\varphi(T))) = (\phi \circ \varphi) +_F (\psi \circ \varphi),
\]
\[
\varphi \circ (\phi +_F \psi) = \varphi(F(\phi(T, \psi(T)))) = F(\varphi(\phi(T)), \varphi(\psi(T))) = (\varphi \circ \phi) +_F (\varphi \circ \psi),
\]
where we used the fact that \( \varphi \in \text{End}(F) \) to get the second equality of the second line. The fact that \( \text{Aut}(F) \) is the unit group of \( \text{End}(F) \) is immediate. 

\( \square \)
### 32.2 Formal group laws over complete DVRs

Let us now specialize to the case where the $A$ is a complete DVR. Let $\mathfrak{m}$ be the maximal ideal of $A$. If $F(X,Y)$ is a formal group law over $A$, for any $x,y \in \mathfrak{m}$ the series $F(x,y)$ converges to an element of $\mathfrak{m}$; indeed, if we define $F_n(X,Y) := F(X,Y)$ mod $(X^n,Y^n)$, the sequence $(F_n(x,y))_n$ is Cauchy, since $v(F_m(x,y) - F_n(x,y)) \geq N$ for all $m,n \geq N$, and therefore converges in our complete ring $A$, and it converges to an element with positive valuation (hence an element of $\mathfrak{m}$), since the constant term of $F(X,Y)$ is zero.

The binary operation

$$x +_F y := F(x,y)$$

makes the set $\mathfrak{m}$ into an abelian group with identity element $0$ and inverse $-F x := i_F(x)$ via parts (i) and (ii) of Proposition 32.6; note that associativity is implied by the definition of a formal group law and commutativity is given by part (iii) of Proposition 32.6, since $A$ is an integral domain. The group $F(\mathfrak{m}) := (\mathfrak{m},+_F)$ is the group associated to $F/A$. Note that if $x,y$ lie in an ideal $\mathfrak{m}^n$, then so does $F(x,y)$, thus we have a filtration of $F(\mathfrak{m})$ by subgroups $F(\mathfrak{m}^n) := (\mathfrak{m}^n,+_F)$. The group $F(\mathfrak{m})$ is also a topological group (in the subspace topology from $A$), since the group operation is defined by the power series $F$, which is continuous as a map $\mathfrak{m} \times \mathfrak{m} \to \mathfrak{m}$, as is the map $\mathfrak{m} \to \mathfrak{m}$ defined by the power series $i_F$.

If $\varphi: A \to B$ is a homomorphism of complete DVRs (as topological rings), then we have an induced homomorphism $F(\varphi): F(\mathfrak{m}^A) \to \varphi_*(F)(\mathfrak{m}^B)$ of topological groups, where $\mathfrak{m}^A$ and $\mathfrak{m}_B$ are the maximal ideals of $A$ and $B$, respectively. This applies in particular when $\varphi$ is an inclusion map, so we can view a formal group law over $A$ as a functor from the category of complete DVRs extending $A$ to the category of topological abelian groups.

If $\phi: F \to G$ is a homomorphism of formal group laws over $A$, then $\phi(x)$ converges to an element of $\mathfrak{m}$ for all $x \in \mathfrak{m}$ (since $\phi$ has constant term zero), and we have an induced group homomorphism

$$\phi: F(\mathfrak{m}) \to G(\mathfrak{m})$$

$$a \mapsto \phi(a).$$

If $\varphi: A \to B$ is any ring homomorphism, we have a commutative diagram

$$\begin{array}{ccc}
F(\mathfrak{m}_A) & \xrightarrow{F(\varphi)} & F(\mathfrak{m}_B) \\
\downarrow{\phi} & & \downarrow{\varphi_*} \\
G(\mathfrak{m}_A) & \xrightarrow{G(\varphi)} & G(\mathfrak{m}_B).
\end{array}$$

We can thus view $\phi$ as a morphism of functors (a natural transformation).

**Example 32.10.** Let $A$ be a complete DVR with maximal ideal $\mathfrak{m}$ and residue field $k := A/\mathfrak{m}$. Then $\mathbb{G}_a(\mathfrak{m}) = \mathfrak{m} \subseteq A$ and we have an exact sequence of topological groups

$$0 \to \mathbb{G}_a(\mathfrak{m}) \to A \to k \to 0.$$ 

We have $\mathbb{G}_m(\mathfrak{m}) \simeq 1 + \mathfrak{m} \subseteq A^\times$ and an exact sequence of topological groups

$$1 \to \mathbb{G}_m(\mathfrak{m}) \xrightarrow{a \mapsto 1+a} A^\times \to k^\times \to 1.$$ 

The endomorphisms $[n]_{\mathbb{G}_a}(T) = nT$ and $[n]_{\mathbb{G}_m}(T) = (1 + T)^n - 1$ corresponds to the multiplication-by-$n$ and $n$-power maps on $\mathfrak{m}$ and $1 + \mathfrak{m}$, respectively.
32.3 Lubin-Tate group laws

We now specialize further and assume that $A$ is a complete DVR with finite residue field; this is equivalent to assuming that $A$ is the valuation ring of a nonarchimedean local field, by Proposition 9.6.

**Definition 32.11.** Let $A$ be a complete DVR with finite residue field of cardinality $q$. For each uniformizer $\pi$ of $A$ we define the set

$$\Phi(\pi) := \{ \phi \in TA[[T]] : \phi(T) \equiv \pi T \mod T^2 \text{ and } \phi(T) \equiv T^n \mod \pi \}. $$

One should think of elements of $\Phi(\pi)$ as “Frobenius endomorphisms”; we will show that for each $\phi \in \Phi(\pi)$ there is a unique formal group law $F_{\phi}(X, Y)$ such that $\phi \in \text{End}(F_{\phi})$. If $\varphi : A \to A/\langle \pi \rangle$ is the natural map from $A$ to its residue field, $\varphi_*(\phi)$ is the $q$-power Frobenius map $x \mapsto x^q$.

For a power series ring $R$ over a commutative ring $A$ (in any number of variables), let $R_n$ denote the $A$-submodule consisting of homogeneous polynomials of degree $n$; we have an obvious $A$-module isomorphism $R \simeq \prod_n R_n$ given by collecting terms of the same degree. We define the $A$-submodules $R_{\leq n} := \prod_{i \leq n} R_i$ and $R_{> n} := \prod_{i > n} R_i$; the latter is simply the $R$-ideal generated by $R_{n+1}$.

**Proposition 32.12.** Let $A$ be a complete DVR with finite residue field of cardinality $q$ and uniformizer $\pi$, let $\phi, \psi \in \Phi(\pi)$, let $r$ be a positive integer, and let $R := A[[X_1, \ldots, X_r]]$. For every $F_1 \in R_1$ there is a unique $F \in R$ such that $F \equiv F_1 \mod R_{> 1}$ and $\phi \circ F \equiv F \circ \psi$.

**Proof.** We will show by induction that there is a unique $F_n \in R_{\leq n}$ for which we have (i) $F_n \equiv F_1 \mod R_{> 1}$, (ii) $\phi \circ F_n \equiv F_n \circ \psi \mod R_{> n}$, and (iii) $F_n \equiv F_{n-1} \mod R_{> n-1}$ if $n > 1$. We may then take $F := \lim_{n \to \infty} F_n$ and the proposition follows.

For $n = 1$ we have $\phi \circ F_1 \equiv \pi F_1 \equiv F_1 \circ \psi \mod R_{> 1}$, so (ii) holds, (i) is given, and (iii) is vacuous; it is clear that $F_1$ is the unique solution for $n = 1$. For $n > 1$ the inductive hypothesis implies that there is a unique homogeneous polynomial $P_{n+1} \in R_{n+1}$ such that

$$\phi \circ F_n - F_n \circ \psi \equiv P_{n+1} \mod R_{> n+1}. $$

Since $\phi, \psi \in \Phi(\pi)$ we have

$$\phi \circ F_n - F_n \circ \psi \equiv F_n(X_1, \ldots, X_r)^q - F_n(X_1^q, \ldots, X_r^q) \equiv 0 \mod \pi$$

since $x \mapsto x^q$ is an automorphism modulo $\pi$, so $\pi$ divides $\phi \circ F_n - F_n \circ \psi$ and therefore $P_{n+1}$. We also note that $\pi^n - 1$ has valuation 0 and is thus invertible in $A$, so we may define

$$F_{n+1} := F_n + \frac{P_{n+1}}{\pi^{n+1} - \pi} \in R_{\leq n+1}. $$

Now $P_{n+1} \equiv 0 \mod R_{> n}$, so $F_{n+1} \equiv F_n \mod R_{> n}$, thus (iii) and (i) hold for $n + 1$. We have

$$\phi \circ P_{n+1} - \psi \circ P_{n+1} \equiv \pi P_{n+1}(X_1, \ldots, X_r) - P_{n+1}(\pi X_1, \ldots, \pi X_r) \mod R_{> n+1}$$

$$\equiv (\pi - \pi^{n+1})P_{n+1} \mod R_{> n+1}, $$

since $P_{n+1}$ is homogeneous of degree $n + 1$, and therefore

$$\phi \circ F_{n+1} - F_{n+1} \circ \psi \equiv \phi \circ F_n + \frac{\phi \circ P_{n+1}}{\pi^{n+1} - \pi} - F_n \circ \psi - \frac{P_{n+1} \circ \psi}{\pi^{n+1} - \pi} \mod R_{> n+1}$$

$$\equiv P_{n+1} + \frac{\phi \circ P_{n+1} - P_{n+1} \circ \psi}{\pi^{n+1} - \pi} \mod R_{> n+1}$$

$$\equiv 0 \mod R_{n+1}, $$

so (ii) holds as well, and the uniqueness of $P_{n+1}$ implies the uniqueness of $F_{n+1}$. \(\square\)
Proposition 32.13. Let $A$ be a complete DVR with finite residue field and uniformizer $\pi$. For every $\phi \in \Phi(\pi)$ there is a unique formal group law $F_{\phi}$ over $A$ such that $\phi \in \text{End}(F_{\phi})$.

Proof. By Proposition 32.12, there is a unique $F_{\phi} \in R := A[[X,Y]]$ satisfying the constraints $F_{\phi} \equiv X + Y \mod R_{>1}$ and $\phi(F_{\phi}(X,Y)) = F_{\phi}(\phi(X),\phi(Y))$ which must hold for any formal group law $F$ over $A$ for which $\phi \in \text{End}(F)$. We only need to check that $F_{\phi}$ is actually a formal group law: we also require $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

The power series $G(X,Y,Z) := F_{\phi}(X,F_{\phi}(Y,Z))$ and $G'(X,Y,Z) := F_{\phi}(F_{\phi}(X,Y),Z)$ satisfy $G \equiv X + Y + Z \equiv G' \mod R_{>1}$ and

\[
\begin{align*}
\phi \circ G &= \phi(F_{\phi}(X,F_{\phi}(Y,Z))) = F_{\phi}(\phi(X),F_{\phi}(\phi(Y),\phi(Z))) = G \circ \phi \\
\phi \circ G' &= \phi(F_{\phi}(F_{\phi}(X,Y),Z)) = F_{\phi}(F_{\phi}(\phi(X),\phi(Y)),\phi(Z)) = G' \circ \phi
\end{align*}
\]

Proposition 32.12 implies that there is a unique $G \in A[[X,Y,Z]]$ congruent to $X + Y + Z$ modulo $R_{>1}$ that satisfies $\phi(G(X,Y,Z)) = G(\phi(X),\phi(Y),\phi(Z))$, so we must have $G' = G$ and therefore $F(X,F(Y,Z)) = F(F(X,Y),Z)$ as desired.

Formal group laws of the form $F_{\phi}$ given by Proposition 32.13, where $\phi \in \Phi(\pi)$ for some uniformizer $\pi$ of a complete DVR $A$ with finite residue field are known as Lubin-Tate formal group laws (for the uniformizer $\pi$).

Definition 32.14. Let $A$ be a complete DVR with finite residue field and uniformizer $\pi$. For $\phi, \psi \in \Phi(\pi)$ and $a \in A$, let $[a]_{\phi,\psi}$ be the unique element of $TA[[T]]$ that satisfies $[a]_{\phi,\psi} \equiv aT \mod T^2$ and $\phi \circ [a]_{\phi,\psi} = [a]_{\phi,\psi} \circ \psi$ given by Proposition 32.12. Let $[a]_{\phi} := [a]_{\phi,\phi}$.

Proposition 32.15. Let $A$ be a complete DVR with finite residue field and uniformizer $\pi$. For all $\phi, \psi \in \Phi(\pi)$ the following hold:

(i) $[a]_{\phi,\psi} \in \text{Hom}(F_{\psi},F_{\phi})$ for all $a \in A$;

(ii) $[1]_{\phi,\psi}$ gives a canonical isomorphism $F_{\psi} \cong F_{\phi}$.

Here $F_{\phi}$ and $F_{\psi}$ are the Lubin-Tate formal group laws for the uniformizer $\pi$ corresponding to $\phi$ and $\psi$, respectively.

Proof. (i) Let $\varphi := [a]_{\phi,\psi}$ and $R := A[[X,Y]]$. We have $\varphi \equiv aT \mod T^2$, so $\varphi \in TA[[T]]$, and

$$
\varphi \circ F_{\psi} \equiv aX + aY \equiv F_{\phi} \circ \varphi \mod R_{>1}.
$$

We have $\phi \circ \varphi = \varphi \circ \psi$ with $\phi \in \text{End}(F_{\phi})$ and $\psi \in \text{End}(F_{\psi})$, so

$$
\begin{align*}
\phi \circ (\varphi \circ F_{\psi}) &= (\varphi \circ F_{\phi}) \circ F_{\psi} = (\varphi \circ (\psi \circ F_{\psi})) = \varphi \circ (F_{\psi} \circ \psi) = (\varphi \circ F_{\psi}) \circ \psi \\
\phi \circ (F_{\phi} \circ \varphi) &= (\varphi \circ F_{\phi}) \circ \varphi = (F_{\phi} \circ \phi) \circ \varphi = F_{\phi} \circ (\phi \circ \varphi) = F_{\phi} \circ (\varphi \circ \psi) = (F_{\psi} \circ \varphi) \circ \psi.
\end{align*}
$$

Proposition 32.12 now implies $\varphi \circ F_{\psi} = F_{\phi} \circ \varphi$, so $[a]_{\phi,\psi} = \varphi \in \text{Hom}(F_{\psi},F_{\phi})$.

(ii) By (i) and Lemma 32.5, $[1]_{\phi,\psi}$ is an isomorphism $F_{\psi} \to F_{\phi}$, and it is clearly canonical (since 1 is).

Proposition 32.16. Let $A$ be a complete DVR with finite residue field and uniformizer $\pi$. For each $\phi \in \Phi(\pi)$ the map $a \mapsto [a]_{\phi}$ is an injective ring homomorphism $A \to \text{End}(F_{\phi})$ that sends $\pi$ to $\phi$ and $A$ into the centralizer of $\phi$. 

18.786 Spring 2018, Lecture #32, Page 8
Proof. It follows from Proposition 32.15 that \([a]_\phi \in \text{End}(F_\phi)\) for all \(a \in A\); the map \(a \mapsto [a]_\phi\) is clearly injective, since \([a]_\phi \equiv aT \mod T^2\). It follows from Proposition 32.12 that every \(\varphi \in \text{End}(F_\phi)\) for which \(\phi \circ \varphi = \varphi \circ \phi\) is uniquely determined by its reduction modulo \(T^2\). This applies in particular to every \(\varphi\) of the form \([a]_\phi\), since the condition \(\phi \circ [a]_\phi = [a]_\phi \circ \phi\) was used to define \([a]_\phi\). For all \(a, b \in A\) we have
\[
[a]_\phi + F_\phi \cdot [b]_\phi \equiv aT + bT \equiv [a + b]_\phi \mod T^2
\]
and therefore \([a]_\phi + F_\phi \cdot [b]_\phi = [a + b]_\phi\) and \([a]_\phi \circ [b]_\phi = [ab]_\phi\). We also have \([1]_\phi \equiv T \mod T^2\), and \(\phi \circ T = \phi \circ T\), so we must have \([1]_\phi = T\). It follows that the map \(a \mapsto [a]_\phi\) is a ring homomorphism. Finally, \([\pi]_\phi \equiv \pi T \equiv \phi \mod T^2\), and \(\phi \circ \phi = \phi \circ \phi\), so \([\pi]_\phi = \phi\), and \([a]_\phi\) commutes with \(\phi\) (both by construction and because \(A\) is commutative) for all \(a \in A\).

It follows from Proposition 32.16 that if \(A\) is complete DVR with finite residue field and maximal ideal \(m\), then for any choice of uniformizer \(\pi\) and any \(\phi \in \Phi(\pi)\), the group \(F_\phi(m) = (m, +F_\phi)\) has an \(A\)-module structure defined by \(am := [a]_\phi(m)\), for any \(a \in A\) and \(m \in m\), in which \(\pi\) corresponds to the endomorphism \(\phi\) whose reduction modulo \(\pi\) is the Frobenius map \(x \mapsto x^q\), where \(q := \#(A/m)\). Proposition 32.15 implies that up to a canonical isomorphism, the \(A\)-module \(F_\phi(m)\) depends only on \(\pi\), not on the choice of \(\phi\).

If \(B/A\) is a finite extension of complete DVRs with finite residue fields, and \(m_B\) is the maximal ideal of \(B\), then \(F_\phi(m_B)\) is also an \(A\)-module, via the embedding \(A \hookrightarrow \text{End}(F_\phi)\).

References