Astérisque
312, 2007, p. 49–55

6. LUBIN-TATE FORMAL GROUPS

by

Volker Meusers

Abstract. — We give an exposition of the theory of formal complex multiplication in local fields after Lubin and Tate. We recall the construction of Lubin-Tate modules, the structure of torsion points of their generic fibre and explicit local class field theory. We follow the original exposition of Lubin and Tate, and the exposition in Neukirch's book.

***Résumé* (Groupes formels de Lubin-Tate).** — Nous donnons une exposition de la théorie de la multiplication complexe formelle dans les corps locaux d'après Lubin et Tate. On rappelle la construction des modules de Lubin-Tate, la structure de leurs modules de torsion de leur fibre générique et la théorie du corps de classes locale explicite. On suit l'article original de Lubin et Tate, et le livre de Neukirch.

1. Construction of Lubin-Tate Modules

Let K be a field complete with respect to some discrete valuation. Let $\mathcal{O}_K$ be its ring of integers, $\mathfrak{p}$ its maximal ideal. Assume the residue field $\mathcal{O}_K/\mathfrak{p}$ to be finite and let q be the number of its elements. Prime elements of $\mathcal{O}_K$ are denoted by π or $\overline{\pi}$. Let k be an algebraic closure of $\mathcal{O}_K/\mathfrak{p}$. Let K^{sep} be a fixed separable closure of K and $K^{\mathrm{nr}} \subseteq K^{\mathrm{sep}}$ the maximal unramified extension of K. Let M and C denote the completions of K^{nr} and K^{sep}. Denote by $\mathcal{O}_M$ (resp. $\mathcal{O}_C$) the ring of integers of M (resp. C). Let $\widehat{\mathcal{C}}$ be the category of complete local noetherian $\mathcal{O}_K$-algebras with residue field k.

Definition 1.1. — Let $i\colon \mathcal{O}_K \to R$ be an $\mathcal{O}_K$-algebra, e.g. $\mathcal{O}_K$, $\mathcal{O}_M$ or k. A formal $\mathcal{O}_K$-module over R is a pair (H, γ_H) consisting of a (one-dimensional commutative) formal group law $H(X,Y) \in R[[X,Y]]$ together with a ring homomorphism

2000 ***Mathematics Subject Classification.*** — 11S31, 14K22, 14L05.
Key words and phrases. — Lubin-Tate formal groups, local class field theory, complex multiplication.

$\gamma_H\colon \mathcal{O}_K \to \mathrm{End}_R(H) \subset R[[T]]$ given by sending an element $a \in \mathcal{O}_K$ to the endomorphism $\gamma_H(a)(T) \in R[[T]]$ of $H(X,Y)$. As a normalization condition we require that the $\mathcal{O}_K$-algebra structure on R induced by the isomorphism

$$\mathcal{O}_K \xrightarrow{\cong} \mathrm{Lie}(H),\ a \longmapsto \left.\frac{\partial \gamma_H(a)(T)}{\partial T}\right|_{T=0}.$$

agrees with the structure given by $i\colon \mathcal{O}_K \to R$, in other words we require $\gamma_H(a)(T)$ to be of the form

$$\gamma_H(a)(T) = i(a)T + \cdots \in R[[T]].$$

We write $[a](T)$ for $\gamma_H(a)(T)$ and $a = i(a) \in R$ if no confusion is possible.

For $R \in \widehat{\mathcal{C}}$ write $H(R)$ for the abelian group $(\mathfrak{m}_R, +_H)$ where we have set $x +_H y = H(x,y)$ for $x, y \in \mathfrak{m}_R$. This converges since R is assumed to be complete. This group is also an (ordinary) $\mathcal{O}_K$-module by setting $ax = a \cdot_H x = [a](x)$. Note that unless (H, γ_H) is the formal additive group, *i.e.*, $(\widehat{\mathbb{G}}_a(X,Y) = X+Y, \gamma_{\widehat{\mathbb{G}}_a}(a)(T) = aT)$, this $\mathcal{O}_K$-module structure is not the standard structure on $\mathfrak{m}_R$ as an ideal of R. For a finite extension $L|K$ with ring of integers $\mathcal{O}_L \in \widehat{\mathcal{C}}$ and maximal ideal $\mathfrak{m}_L \subset \mathcal{O}_L$ we set $H(L) = H(\mathfrak{m}_L)$. Similarly for infinite extensions after completion.

The goal of this section is to construct, as for ordinary complex multiplication (see Remark 3.5 below), a formal $\mathcal{O}_K$-module (G, γ_G) over $\mathcal{O}_M$ such that

$$G[\mathfrak{p}] = \bigcap_{a \in \mathfrak{p}} \mathrm{Ker}(a) = G[\pi]$$

is isomorphic to the kernel of the Frobenius $G \otimes k \to (G \otimes k)^{(q)}$ when reduced modulo the maximal ideal of $\mathcal{O}_M$. Lubin and Tate construct G as a base change $G = H_\pi \otimes_{\mathcal{O}_K} \mathcal{O}_M$ of a formal $\mathcal{O}_K$-module H_π over $\mathcal{O}_K$, the so called Lubin-Tate module associated to the prime element $\pi \in \mathcal{O}_K$. As we will see H_π depends on the chosen π while G will be independent of it.
By our normalization condition $\gamma_G(\pi)(T)$ is of the form

$$\gamma_G(\pi)(T) = \pi T + \cdots \in \mathcal{O}_K[[T]].$$

The condition on the Frobenius requires that

$$\gamma_G(\pi)(T) \equiv T^q \bmod \pi.$$

This justifies the following definition:

Definition 1.2. — A power series $f(T) = \pi T + \cdots \in \mathcal{O}_K[[T]]$ such that

$$f(T) \equiv T^q \bmod \pi$$

is called a Lubin-Tate series associated to π. The set of Lubin-Tate series for π is denoted by $\mathcal{F}_\pi$. A formal $\mathcal{O}_K$-module (H, γ_H) over $\mathcal{O}_K$ with $\gamma_H(\pi)(T) \in \mathcal{F}_\pi$ is called Lubin-Tate module.

Examples 1.3

(1) The simplest example of a Lubin-Tate-series is

$$f(T) = \pi T + T^q \in \mathcal{F}_\pi.$$

(2) In the cyclotomic case, *i.e.*, for $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$ and $\pi = p \in \mathbb{Z}_p$ the polynomial

$$f(T) = (T+1)^p - 1 = pT + p(\dots) + T^p \in \mathcal{F}_\pi.$$

is a Lubin-Tate-series associated to $\pi = p$. One easily checks that in this case the formal multiplicative group

$$\widehat{\mathbb{G}}_m(X,Y) = (1+X)(1+Y) - 1$$

is a Lubin-Tate module associated to $f(T)$.

The construction of Lubin-Tate-modules is based on the following lemma.

Lemma 1.4. — *Let $\pi, \overline{\pi}$ be two prime elements of M and $f(T) \in \mathcal{F}_\pi$ resp. $g(T) \in \mathcal{F}_{\overline{\pi}}$. Let $L(X_1,\dots,X_n) = \sum_{i=1}^n a_i X_i$ be a linear form with coefficients in $\mathcal{O}_M$ such that*

$$\pi L(X_1,\dots,X_n) = \overline{\pi} L^\sigma(X_1,\dots,X_n)$$

where σ is the continuous extension of the Frobenius in $\mathrm{Gal}(K^{nr}|K)$ *to M. Then there exists a unique power series $F(X_1,\dots,X_n) \in \mathcal{O}_M[[X_1,\dots,X_n]]$ such that*

$$F(X_1,\dots,X_n) \equiv L(X_1,\dots,X_n) \bmod (X_1,\dots,X_n)^2 \tag{1.1}$$

and

$$f(F(X_1,\dots,X_n)) = F^\sigma(g(X_1),\dots,g(X_n)). \tag{1.2}$$

where $(X_1,\dots,X_n)$ denotes the ideal generated by $X_1,\dots,X_n$. If the coefficients of f, g, L lie in $\mathcal{O}_K$ then F also has coefficients in $\mathcal{O}_K$.

The idea of the proof is to construct F inductively modulo powers of the ideal generated by $X_1,\dots,X_n$ and then use the completeness of the power series ring. The induction starts with (1.1). For the induction step one plugs in (1.2) and uses that f and g are Lubin-Tate series to see that the coefficients are in $\mathcal{O}_M$. See [**N**] for a detailed proof.

We use the lemma to construct Lubin-Tate modules as follows:
For $f(T) \in \mathcal{F}_\pi$ let $H_f(X,Y)$ be the unique solution of the equations

$$H_f(X,Y) \equiv X + Y \bmod (X,Y)^2$$

and

$$f(H_f(X,Y)) \equiv H_f(f(X), f(Y))$$

For each $a \in \mathcal{O}_K$ and $f(T), g(T) \in \mathcal{F}_\pi$ let $[a]_{f,g}(T)$ be the unique solution of

$$[a]_{f,g}(T) \equiv aT \bmod T^2$$

and

$$f([a]_{f,g}(T)) \equiv [a]_{f,g}(g(T))$$

To simplify notations we shall write $[a]_f$ instead of $[a]_{f,f}$. The following theorem shows that the series $H_f(X,Y)$ together with $\gamma_{H_f}(a)(T) = [a]_f(T)$ is in fact a Lubin-Tate module associated to $f(T)$.

Theorem 1.5. — *For any $f(T) \in \mathcal{F}_\pi$ the series $H_f(X,Y)$ is a formal group law over $\mathcal{O}_K$, i.e., the following identities hold:*

$$\begin{aligned} H_f(X,Y) &= H_f(Y,X) \\ H_f(H_f(X,Y),Z) &= H_f(X,H_f(Y,Z)) \\ H_f(X,0) &= X \\ H_f(0,Y) &= Y \\ H_f(X,[-1]_f(X)) &= 0. \end{aligned}$$

For $g,h \in \mathcal{F}_\pi$ and $a,b \in \mathcal{O}_K$ we have

$$\begin{aligned} H_f([a]_{f,g}(X),[a]_{f,g}(Y)) &= [a]_{f,g}(H_g(X,Y)) \\ [a]_{f,g}([b]_{g,h}(T)) &= [ab]_{f,h}(T) \\ [a+b]_{f,g}(T) &= H_f([a]_{f,g}(T),[b]_{f,g}(T)) \\ [\pi]_f(T) &= f(T) \\ [1]_f(T) &= T. \end{aligned}$$

In particular $(H_f(X,Y),\gamma_{H_f})$ with $\gamma_{H_f}(a)(T) = [a]_f(T)$ is a Lubin-Tate-module such that $\gamma_{H_f}(\pi)(T) = f(T)$. For two series $f(T), g(T) \in \mathcal{F}_\pi$ we have the canonical isomorphism

$$[1]_{f,g}(T) \colon H_g \xrightarrow{\cong} H_f$$

of formal $\mathcal{O}_K$-modules over $\mathcal{O}_K$.

The equalities in the Theorem are all true modulo squares and follow from the uniqueness assertion of Lemma 1.4. For a detailed proof see [**N**, proof of Theorem V.4.6].

Remark 1.6. — Although H_f does not depend on the particular choice $f \in \mathcal{F}_\pi$ it does depend on the particular choice of the uniformizing element $\pi \in \mathcal{O}_K$. They become isomorphic over $\mathcal{O}_M$ because of the following lemma.

Lemma 1.7. — *Let π and $\overline{\pi}$ be two prime elements of $\mathcal{O}_K$ with $\pi = u\overline{\pi}$ for some unit $u \in \mathcal{O}_K^\times$. Let σ be the Frobenius of M as above. There exists some $\epsilon \in \mathcal{O}_M^\times$ such that $u = \epsilon^{\sigma-1}$. Let $f(T) \in \mathcal{F}_\pi$ and $g(T) \in \mathcal{F}_{\overline{\pi}}$ be Lubin-Tate series. Then there exists a unique power series $\theta(X) \in \mathcal{O}_M[[X]]$ such that $\theta(X) = \epsilon X$ modulo $(X)^2$ and $f \circ \theta = \theta^\sigma \circ g$. Furthermore $\theta(X)$ induces an isomorphism $H_g \xrightarrow{\cong} H_f$ of Lubin-Tate modules (defined over $\mathcal{O}_M$).*

This is proved using Lemma 1.4. For a detailed proof see [**N**, Corollary V.2.3], and also [**LT**, Lemma 2].

2. Torsion points of the Generic Fibre

Now fix some $f \in \mathcal{F}_\pi$. We want to describe the structure of torsion points of the generic fibre of $H_f(C)$ as a Galois module. Recall that for every separable algebraic extension $K \subset L \subset C$ we set $H_f(L) = H_f(\widehat{\mathcal{O}}_L)$. If $L_1 \subset L$ then $H_f(L_1) \subset H_f(L)$. If $L|L_1$ is Galois then $\mathrm{Gal}(L|L_1)$ operates naturally on $H_f(L)$ in a manner compatible with the $\mathcal{O}_K$-module structure. This results from the fact that the Galois group operates continuously on $\widehat{\mathcal{O}}_L$ and that H_f is defined over $\mathcal{O}_K \subseteq \mathcal{O}_{L_1}$. In this way $H_f(L)$ becomes a $\mathrm{Gal}(L|L_1) \times \mathcal{O}_K$-module. For another $g \in \mathcal{F}_\pi$ the canonical map induced by $[1]_{f,g}(T)$ is an isomorphism of $\mathrm{Gal}(L|L_1) \times \mathcal{O}_K$-modules. It commutes with the inclusions $H_f(L_1) \subset H_f(L)$.

Set

$$\Lambda_f = \bigcup_{m \geq 0} H_f(C)[\mathfrak{p}^m] \subset H_f(C)$$

Then Λ_f is a torsion $\mathcal{O}_K$-module, *i. e.*, the union over its sub-modules $\Lambda_{f,m} = \Lambda_f[\mathfrak{p}^m]$. It is clear that the Galois extension $K \subset L_{\pi,m} = K(\Lambda_f[m])$ does not depend on $f \in \mathcal{F}_\pi$. Let us denote its Galois group by $G_{\pi,m} = \mathrm{Gal}(L_{\pi,m}|K)$.

Theorem 2.1. — *Let π be a prime element of $\mathcal{O}_K$ and $f \in \mathcal{F}_\pi$.*
(1) The $\mathcal{O}_K$-module Λ_f is divisible.
(2) For each m, the $\mathcal{O}_K$-module $\Lambda_{f,m}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}^m$.
(3) The $\mathcal{O}_K$-module Λ_f is isomorphic to $K/\mathcal{O}_K$.
(4) For each $\tau \in G_\pi$ there exists a unique $u_\tau \in \mathcal{O}_K^\times$ such that $\tau\lambda = [u_\tau]_f(\lambda)$ for every λ in Λ_f.
(5) The map $\tau \mapsto u_\tau$ is an isomorphism of G_π onto the group $\mathcal{O}_K^\times$, under which the quotients $G_{\pi,m}$ of G_π correspond to the quotients $\mathcal{O}_K^\times/(1+\mathfrak{p}^m)$ of $\mathcal{O}_K^\times$.

See [**LT**] for a proof.

Example 2.2. — In the cyclotomic case we get $1 + \Lambda_{f,m} = \mu_{p^m}$, $1 + \Lambda_f = \mu_{p^\infty}$. We have $\widehat{\mathbb{G}}_m(\mathbb{Q}_p) = p\mathbb{Z}_p$ with addition given by the identification with $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ as a multiplicative subgroup. In this case the multiplicative structure is given by exponentiating, *i.e.*,

$$[a]_f(T) = \sum_{n=1}^{\infty} \binom{a}{n} T^n = (1+T)^a - 1$$

for $a \in \mathbb{Z}_p$.