LUBIN-TATE THEORY

GAL PORAT

ABSTRACT. These are notes for a talk which introduces Lubin-Tate theory, a method which uses formal group laws to generate the maximal abelian extension of a p-adic field. We present the method and describe an application to elliptic curves.

1. Introduction

Let $K/\mathbb{Q}_p$ be a local field, and let K^{ab} be its maximal abelian extension. Local class field theory gives an isomorphism between $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and the profinite completion of $K^\times$, but how can one actually explicitly generate the extension K^{ab}? In this talk we explain how Lubin-Tate theory ([LT65]) answers this question through the use of formal group laws. We also describe an application to the torsion points of an elliptic curve $E/\mathbb{Q}_p$.

2. Local Class Field Theory

Let $K/\mathbb{Q}_p$ be a finite extension. Denote by K^{un} and K^{ab} its maximal unramified and maximal abelian extensions, respectively. Local class field theory describes $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ in terms of the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{un}}) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{un}}/K) & \longrightarrow & 0\ . \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \widehat{K}^\times & \longrightarrow & \widehat{\mathbb{Z}}^\times & \longrightarrow & 0 \end{array}$$

Using Galois theory, this gives rise to the following correspondence:

$$\text{subextensions } K \subset L \subset K^{\mathrm{ab}} \longleftrightarrow \text{closed subgroups } H \leq K^\times,$$

under which

$$\text{maximal totally ramified subextensions } K \subset L \subset K^{\mathrm{ab}} \longleftrightarrow \ \langle \pi \rangle \leq K^\times, \pi \text{ uniformizer.}$$

Write K_π for the field corresponding to $\langle \pi \rangle$. As K_π is a maximal and totally ramified extension, we have $K^{\mathrm{ab}} = K^{\mathrm{un}} K_\pi$. One always has $K^{\mathrm{un}} = \bigcup_{(n,p)=1} K(\mu_n)$, so in order to explicitly generate K^{ab} it suffices to do so for K_π.

Example 2.1. If $K = \mathbb{Q}_p$, it turns out that $K_p = \mathbb{Q}_p(\mu_{p^\infty})$. So in this case K_p is obtained from K by adjoining the p-torsion $\overline{K}$-points of the group scheme $\mathbb{G}_m$, where $\mathbb{G}_m(A) = A^\times$. We will see later how Lubin-Tate theory generalizes this.

3. Formal Group Laws

Let R be any commutative ring.

Definition 3.1. A power series $F(X,Y) \in R[[X,Y]]$ is called a (commutative) formal group law if it satisfies the following three properties:
(i) $F(X,Y) \equiv X+Y \mod \deg \geq 2$,
(ii) $F(F(X,Y),Z) = F(X,F(Y,Z))$,
(iii) $F(X,Y) = F(Y,X)$.

As an exercise, one can check that the conditions imply that $F(X,0) = X$ and there exists an "inverse" power series $i_F(X) \in R[[X]]$ such that $F(X, i_F(X)) = 0$.

If F is a formal group law, we let $\mathrm{End}(F)$ denote the subset of $XR[[X]]$, consisting of elements $f(X)$ such that $F(f(X),f(Y)) = f(F(X,Y))$ ($f \circ F = F \circ f$ for short). It is a ring with respect to addition given by $f\,[+]\,g = F(f,g)$ and multiplication given by composition, the multiplicative identity being X.

Example 3.1. (i) The additive formal group law $\mathbb{G}_a(X,Y) = X+Y$. We have

$$\mathrm{End}(\mathbb{G}_a) = \{f \in XR[[X]] : f(X)+f(Y)\},$$

which is just XR.

(ii) The multiplicative formal group law $\mathbb{G}_m(X,Y) = (1+X)(1+Y)-1$.[1] We have

$$\mathrm{End}(\mathbb{G}_m) = \{f \in XR[[X]] : (1+f(X))(1+f(Y))-1 = f((1+X)(1+Y)-1)\},$$

which contains all the elements $(1+X)^n - 1$ for $n \geq 1$.

4. Lubin-Tate Formal Group Laws

From now on we take $R = \mathcal{O}_K$. Let q be the cardinality of the residue field of K.

Definition 4.1. Let $\pi \in \mathcal{O}_K$ be a uniformizer. A π-Lubin-Tate power series is an element $f \in \mathcal{O}_K[[X]]$ such that
(i) $f(X) \equiv \pi X \mod \deg \geq 2$, and
(ii) $f(X) \equiv X^q \mod \pi$.

For example, $f(X) = \pi X + X^q$ is a π-Lubin-Tate power series. One has the following key lemma.

Lemma 4.1. *Let f be a π-Lubin-Tate power series, and let $L(X_1,...,X_n)$ be a linear form with coefficients in R.*
Then there exists a unique $F \in \mathcal{O}_K[[X_1,...,X_n]]$ with $F \equiv L \mod \deg \geq 2$ with $f \circ F = F \circ f$.

Corollary 4.1. *(1) There exists a unique formal group law $F \in \mathcal{O}_K[[X,Y]]$ with $f \in \mathrm{End}(F)$.*
(2) Given $a \in \mathcal{O}_K$, there exists a unique power series $[a](X) \in \mathcal{O}_K[[X]]$ with $[a](X) \equiv aX \mod \deg \geq 2$ and $[a] \in \mathrm{End}(F)$. The map $a \mapsto [a]$ is a ring homomorphism.

[1] This $\mathbb{G}_m$ differs from the one appearing in Example 2.1 in the choice of parameters, with X and Y being replaced with $1+X$ and $1+Y$. This is done so that $\mathbb{G}_m$ satisfies condition (i) of Definition 3.1.

Proof. (1) Apply the lemma to $L(X,Y) = X+Y$ to obtain a power series $F \in \mathcal{O}_K[[X,Y]]$ with $f \circ F = F \circ f$. To check F is a formal group law, one uses the uniqueness of F in the lemma. For example, to check condition (ii) in Definition 3.1, note that both of $F(F(X,Y),Z)$ and $F(X,F(Y,Z))$ are congruent to $X+Y+Z \mod \deg \geq 2$ and commute with f.

(2) Apply the lemma to $L(X) = aX$ to obtain a power series $[a](X) \in \mathcal{O}_K[[X]]$ which is congruent to $ax \mod \deg \geq 2$ and which satisfies $[a] \circ f = f \circ [a]$. As both of $F \circ [a]$ and $[a] \circ F$ are congruent to $a(X+Y) \mod \deg \geq 2$ and commute with f, the uniqueness in the lemma implies they are equal. In other words, $[a] \in \mathrm{End}(F)$. The claim that $a \mapsto [a]$ is a ring homomorphism follows similarly. □

Given $x, y \in \mathbb{C}_p$ with $|x|, |y| < 1$, the evaluations $[a](x)$ and $F(x,y)$ converge to some element in $\mathbb{C}_p$. We let

$$W_n = \{x \in \mathbb{C}_p, |x| < 1 : [\pi^n](X) = 0\}.$$

In more fancy terms, these are the $\mathbb{C}_p$-points of the formal group scheme $F[\pi^n]$.

Note that W_n is an abelian group with respect to the operation $x, y \mapsto F(x,y)$. In fact, by Corollary 4.1 (2), it is an $\mathcal{O}_K$-module.

Part (3) of the following theorem establishes the analogy of W_n with the torsion points of an elliptic curve with complex multiplication.

Theorem 4.1. *(1) $W_n \subset \overline{K}$ (in other words, $F[\pi^n](\mathbb{C}_p) = F[\pi^n](\overline{K})$).*
(2) There is a (non-canonical) isomorphism $W_n \cong \mathcal{O}_K/\pi^n$.
(3) The action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathbb{C}_p$ preserves W_n, and the action map

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathcal{O}_K} W_n \cong (\mathcal{O}_K/\pi^n)^\times$$

is surjective.

Let K_n be the field corresponding to $\mathrm{Ker}\left(\mathrm{Gal}(\overline{K}/K) \to (\mathcal{O}_K/\pi^n)^\times\right)$ via the homomorphism above. Then part (3) of Theorem 4.1 implies $\mathrm{Gal}(K_n/K) \cong (\mathcal{O}_K/\pi^n)^\times$.

Theorem 4.2. *(1) K_n/K is totally ramified.*
(2) $K_\pi = \bigcup_{n \geq 1} K_n$.

In other words, in order to explicitly generate K_π (and hence also K^{ab}), one can pick any π-Lubin-Tate power series and adjoin its $[\pi^n]$-torsion points. In fact, the uniqueness Lemma 4.1 implies that $[\pi^n]$ is the composition of f with itself n times. For example, one may choose $f = \pi X + X^q$ and adjoin the roots of its composition with itself to generate K_π.

5. The case $K = \mathbb{Q}_p$

We now describe in detail the case $K = \mathbb{Q}_p$, $\pi = p$.

Take $f(X) = (1+X)^p - 1$, it is a p-Lubin-Tate power series. Then one checks that $F(X,Y) = \mathbb{G}_m(X,Y)$ from Example 3.1 (ii) is the unique formal group law commuting with it, and that for $a \in \mathbb{Z}_p$ we have $[a](X) = (1+X)^a - 1 = \sum_{n \geq 0} \binom{a}{x} X^n - 1$. Then $W_n = \mathbb{G}_m[p^n] = \left\{x : (1+x)^{p^n} - 1 = 0\right\} = \mu_{p^n} - 1$. Therefore, $K_n = \mathbb{Q}_p(\mu_{p^n} - 1) = \mathbb{Q}_p(\mu_{p^n})$ and $K_p = \mathbb{Q}_p(\mu_{p^\infty})$, recovering Example 2.1.

6. The Formal Group law of an Elliptic curve

Let $E/\mathbb{Z}_p$ be a an elliptic curve with good reduction at p. Let $\widehat{E}$ be the formal group law associated to E. Then $\widehat{E}$ can be described in terms of the characteristic polynomial of (arithmetic) Frobenius $X^2 - a_p X + p$ and the reduction $\widetilde{E} \mod p$.

Proposition 6.1. *(1) If $\widetilde{E}$ is ordinary, then $X^2 - a_p X + p = (X - \pi)(X - p/\pi)$ for some uniformizer $\pi \in \mathbb{Z}_p$, and $\widehat{E}$ is the Lubin-Tate formal group law corresponding to π.*
(2) If $\widetilde{E}$ is supersingular and $p \geq 5$, then $\widehat{E}$ is a Lubin-Tate formal group law to $-p$ in $\mathbb{Z}_{p^2}$.

Here is a very concrete application of the above proposition, using what we know about Lubin-Tate formal group laws. It is well known that there is an exact sequence

$$0 \to \widehat{E}(p\mathbb{Z}_p) \to E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p) \to 0.$$

For example, suppose $\widetilde{E}$ is ordinary. Then we know that $\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$ acts on W_n faithfully. In particular, $\widehat{E}$ has no nontrivial $[\pi^n]$-torsion defined over $\mathbb{Q}_p$. So $\widehat{E}(p\mathbb{Z}_p)[\pi^n] = 0$, and hence also $\widehat{E}(p\mathbb{Z}_p)[p^n] = 0$. Arguing similarly for the case of a supersingular elliptic curve, we have established the following fact:

Theorem 6.1. *The reduction map $E(\mathbb{Q}_p)[p^n] \to \widetilde{E}(\mathbb{F}_p)[p^n]$ is injective.*

References

[LT65] Jonathan Lubin and John Tate. Formal complex multiplication in local fields. Ann. of Math. (2), 81:380–387, 1965.