EXPLICIT LOCAL CLASS FIELD THEORY

ISHAN LEVY

1. Introduction

Local class field theory says there is a bijective correspondence between finite abelian extensions of a local field K and open subgroups of finite index in $K^\times$ given by $L/K \leftrightarrow N_{L/K}(L^\times)$. This leaves the question open of how to get these abelian extensions. In particular we would like to construct K^{ab}, the maximal abelian extension of K. We will first see that the construction problem is easy for unramified extensions, and we can construct K^{ur}, the maximal unramified extension, which will turn out to be abelian. Then we will construct the Lubin-Tate formal group laws, and associated formal modules, which can yield totally ramified abelian extensions by adjoining the torsion points of the formal modules. The compositum of the totally ramified and unramified extensions will be K^{ab}.

This is completely analogous to adjoining torsion points of a CM elliptic curve to yield abelian extensions of an imaginary quadratic field, and hence can be considered "formal complex multiplication".

2. Unramified extensions

For the rest of the time, K will be a non-Archimedean local field, $\mathcal{O}_K$ its valuation ring, $\mathfrak{m}$ the maximal ideal of $\mathcal{O}_K$, and k the residue field of order q. If L is a finite extension, l will be its residue field.

Recall that for a finite extension L/K, one can uniquely extend the valuation on K to L by $v_L(x) = v_K(N_{L/K}(x))$. If the valuation v_L is normalized to have image $\mathbb{Z}$, then the **ramification degree** of the extension L/K is e where $e\mathbb{Z} = v_L(K^\times)$. If $e = 1$ the extension is **unramified**.

To construct unramified extensions we will need to consider the Teichmüller character ω, the unique section of the map $\mathcal{O}_K^\times \to k^\times$, with $\omega(\bar{x}) = \lim_n x^{q^n}$, where x is any lift of $\bar{x}$. It is easy to see that x^{q^n} is a Cauchy sequence, and that ω is unique/well-defined follows from Hensel's lemma on the polynomial $x^{q-1} - 1$. Thus the short exact sequence $0 \to 1 + \mathfrak{m} \to \mathcal{O}_K^\times \to k^\times \to 0$ splits, and $\mathcal{O}_K^\times \cong k^\times \times 1 + \mathfrak{m}$. If μ'_K denote the roots of unity of K of order coprime to q, since it is easy to see that ω is the identity on μ'_K, we must have $\mu'_K = k^\times \subset K$.

Date: 1/15/18.

Proposition 2.1. *There is a unique unramified extension of degree n for each n given by $L = K(\mu_{q^n-1})$, which is cyclic Galois so that $\mathrm{Gal}(K^{ur}/K) \cong \hat{\mathbb{Z}}$. Moreover the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$ is an isomorphism.*

Proof. Let $L = K(\mu_{q^n-1})$. Then l contains $\mathbb{F}_{q^n}$ by our observation above. Let $\bar{g}$ be the minimal polynomial of a, a primitive $q^n - 1^{th}$ root of unity in k, and let g be a lift of $\bar{g}$. By Hensel's lemma, there is a unique root of g in L reducing to each conjugate of a. Letting α be the lift of a, we must have $K(\alpha) = L$, since $\omega(\alpha)$ is a primitive $q^n - 1^{th}$ root of unity. Thus $n = [L : K] \geq [l : k] \geq n$, so equality must hold. Then if π is a uniformizer of K, $[l : k] = [L : K] = [\mathcal{O}_L/\pi\mathcal{O}_L : \mathcal{O}_K/\pi\mathcal{O}_K]$, so π stays prime in L, and the extension is unramified.

Now L contains all the conjugates of α so is Galois. Reduction mod $\mathfrak{m}$ gives a homomorphism from $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(l/k)$, but since α's conjugates reduce to a's conjugates, and $\mathrm{Gal}(L/K), \mathrm{Gal}(l/k)$ act faithfully on the conjugates of α and a respectively, so the homomorphism is injective and hence an isomorphism. Thus L is a cyclic extension.

For uniqueness, if L is unramified, let π be as before, $n = [L : K] = [\mathcal{O}_L/\pi\mathcal{O}_L : \mathcal{O}_K/\pi\mathcal{O}_K] = [l : k]$. Write $l = k(a)$, and since $\omega(a)$ is a $q^n - 1^{th}$ root of unity, $L \supset K(\mu_{q^n-1})$, but they are the same degree, and hence are equal. Then $\mathrm{Gal}(K^{ur}/K) = \lim_n \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}$ □

Thus unramified extensions are easy to understand. Given any Galois extension L/K, we see from Proposition 2.1 that $K(\mu'_L)$ is the maximal unramified subextension with the same residue field, so that if it is the fixed field of I (called the **inertia group**), we have the exact sequence $0 \to I \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k) \to 0$.

3. Formal Group Laws

The theory of Lubin and Tate has to do with constructing totally ramified abelian extensions, which together with K^{ur} will give K^{ab}. To do this we will need the notion of a formal group law. A comment on notation: two power series are congruent "(mod deg n)" if their coefficients on monomials of degree less than n agree.

Definition 3.1. *An **n-dimensional formal group law** over a ring R is a collection of n power series $F = F_1, \ldots, F_n$ in $R[[x_1, \ldots, x_n, y_1, \ldots, y_n]] = R[[\mathbf{x}, \mathbf{y}]]$ such that*

$F(F(\mathbf{x}, \mathbf{y}), \mathbf{z}) = F(\mathbf{x}, F(\mathbf{y}, \mathbf{z}))$, $F(\mathbf{0}, \mathbf{x}) = \mathbf{x} = F(\mathbf{x}, \mathbf{0})$.

These axioms should be considered as associativity and identity.

Definition 3.2. *If F is n-dimensional, and G m-dimensional, A **homomorphism of formal group laws** from F to G is a collection of m power series $f = f_1, \ldots, f_m$ in n variables such that $f(F(\mathbf{x}, \mathbf{y})) = G(f(\mathbf{x}), f(\mathbf{y}))$*

Note that the f_i must have no constant term in order for the composition to make sense. One can easily check associativity so that formal group laws form a category.

A formal group law is like a Lie algebra in that it can be thought of as an "infinitesimal" algebraic group, but whereas Lie algebras are first order approximations (like a derivative), formal groups are arbitrary order approximations (like a Taylor series). The power series can be seen as describing multiplication near the identity of an algebraic group in suitable coordinates. Thus via the analogy to complex multiplication, the Lubin-Tate formal groups we will construct can be seen as local analogs of 1-dimensional abelian varieties, or elliptic curves.

The reason they are called groups instead of monoids (indeed the axioms require no inverse) is the following lemma:

Lemma 3.3. *If $F = F_1, \ldots, F_n$ is a n-dimensional formal group law, then there is a unique inverse $h = h_1, \ldots, h_n \in R[x_1, \ldots, x_n]$ such that $F(\mathbf{x}, h(\mathbf{x})) = \mathbf{0} = F(h(\mathbf{x}), \mathbf{x})$*

Proof. We will just show the existence of a left inverse, as the right inverse exists by considering the "opposite" formal group law $G(\mathbf{x}, \mathbf{y}) = F(\mathbf{y}, \mathbf{x})$, and if both exist, they must be equal and unique by associativity.

By the identity axiom we have $F_i \equiv x_i + y_i \pmod{\deg 2}$. Inductively on k, we will construct h^k, a left inverse mod deg k. $h_i^2 = -x_i$ is an inverse mod deg 2. Given a solution $h^k \bmod \deg k$, we can find a solution $h^{k+1} \bmod \deg k+1$ if we can solve $F(h^k(\mathbf{x}) + g(\mathbf{x}), \mathbf{x}) \equiv \mathbf{0} \pmod{\deg k+1}$ where g is a linear combination of degree k monomials.

Since $F(\mathbf{0}, \mathbf{x}) = \mathbf{x} = F(\mathbf{x}, \mathbf{0})$, $F = \mathbf{x} + \mathbf{y} +$ terms involving both the x_i and y_i, so $F(h^k(\mathbf{x}) + g(\mathbf{x}), \mathbf{x}) \equiv F(h^k(\mathbf{x}), \mathbf{x}) + g(\mathbf{x}) \pmod{\deg k+1}$ so the equation can be solved since by hypothesis $F(h^k(\mathbf{x}), \mathbf{x})$ is a linear combination of monomials of degree $k \bmod \deg k+1$. In fact if one is a little careful, this construction also proves uniqueness. □

Now for our purposes we will only need to consider 1-dimensional commutative (i.e. $F(y, x) = F(x, y)$) formal group laws, which will be referred to as formal groups. There are two important examples of these, the additive formal group $x + y$ and the multiplicative formal group $x + y + xy$ which can be written as $(x + 1)(y + 1) - 1$ to explain its name.

Restricting to commutative formal group laws is nice because the category of commutative formal group laws is preadditive, meaning that $\mathrm{Hom}(F, G)$ is an abelian group in a way such that composition of homomorphisms is bilinear.

Lemma 3.4. *The category of commutative formal group laws is preadditive, with addition of two homomorphisms $f, g : F \to G$ given by $(f + g)(\mathbf{x}) = G(f(\mathbf{x}), g(\mathbf{x}))$.*

Proof. Let's first check that $(f+g)$ is indeed a homomorphism.

$$(f+g)(F(\mathbf{x},\mathbf{y})) = G(f(F(\mathbf{x},\mathbf{y})), g(F(\mathbf{x},\mathbf{y}))) = G(G(f(\mathbf{x}), f(\mathbf{y})), G(g(\mathbf{x}), g(\mathbf{y})))$$
$$= G(G(f(\mathbf{x}), g(\mathbf{x})), G(f(\mathbf{y}), g(\mathbf{y}))) = G((f+g)(\mathbf{x}), (f+g)(\mathbf{y}))$$

Now let's check left and right distributivity. Let $h, i : G \to H$ be homomorphisms. Then $(f+g)\circ h = G(f\circ h, g\circ h) = (f\circ h) + (g\circ h)$ and similarly $f\circ(h+i) = f(G(h,i)) = H((f\circ h),(f\circ i)) = (f\circ h)+(f\circ i)$. □

Since this category is preadditive, $\mathrm{End}(F)$ is a ring, and it makes sense to talk about an R-module structure on F, which is a ring homomorphism from R to $\mathrm{End}(F)$. We will call a formal group with an R-module structure a **formal R-module**.

4. Lubin-Tate Formal Groups

Let π be a uniformizer of $\mathcal{O}_K$, and $\mathcal{F}_\pi$ the set of power series $F \in \mathcal{O}_K[[T]]$ such that $F \equiv \pi T \pmod{\deg 2}$ and F reduces to $T^q \pmod{\mathfrak{m}}$, the Frobenius map.

Given $f \in \mathcal{F}_\pi$, we would like to construct a formal group such that f is an endomorphism. To make this construction (and more) we have the fundamental lemma:

Lemma 4.1. *Let $f, g \in \mathcal{F}_\pi$, and $L(x_1,\dots,x_n) = L(\mathbf{x}) = \sum_1^n a_i x_i$ be a linear form with coefficients in $\mathcal{O}_K$. Then there is a unique $F \in \mathcal{O}_K[[x_1,\dots,x_n]] = \mathcal{O}_K[[\mathbf{x}]]$ such that $F \equiv L$ (mod deg 2) and $f(F(\mathbf{x})) = F(g(\mathbf{x}))$.*

Proof. (c.f. Lemma 3.3) We will construct inductively a unique sequence of approximations $F_k \pmod{\deg k+1}$ such that $f(F_k(\mathbf{x})) \equiv F_k(g(\mathbf{x})) \pmod{\deg k+1}$. L itself is clearly the unique solution for F_1. Now supposing we have a unique solution F_k, F_{k+1} must be of the form $F_k + \phi$, where ϕ is a linear combination of degree $k+1$ monomials. Thus we would like a unique ϕ satisfying $f((F_k+\phi)(\mathbf{x})) \equiv (F_k+\phi)(g(\mathbf{x})) \pmod{\deg k+2}$, but we have $\pi\phi(\mathbf{x}) + f(F_k(\mathbf{x})) \equiv f((F_k+\phi)(\mathbf{x})) \equiv (F_k+\phi)(g(\mathbf{x})) \equiv F_k(g(\mathbf{x})) + \pi^{k+1}\phi(\mathbf{x})$, so we see that the unique solution is $\phi = \frac{f(F_k(\mathbf{x})) - F_k(g(\mathbf{x}))}{\pi^{k+1}-\pi}$ which is in $\mathcal{O}_K$ since $f(F_k(\mathbf{x})) - F_k(g(\mathbf{x})) \equiv F_k(\mathbf{x})^q - F_k(\mathbf{x}) \equiv 0 \pmod{\pi}$. □

Now we can construct the Lubin-Tate formal groups.

Proposition 4.2. *For $f \in \mathcal{F}_\pi$, there is a unique formal group F_f such that f is an endomorphism.*

Proof. Apply $L = x+y, f = g$ to Lemma 4.1 to get F_f. To verify associativity, use the uniqueness in the Lemma on $f = g, F = F_f(x, F_f(y,z)), F_f(F_f(x,y),z)$, which both reduce to $L = x+y+z$ mod deg 2. One similarly gets commutativity. To get identity, from associativity we have $F_f(x,0) = F_f(x, F_f(0,0)) = F_f(F_f(x,0),0)$, so $h = F_f(x,0)$ is a power series that is x mod deg 2, and satisfies $h(h(x)) = h(x)$. It is then easy to see that $h(x) = x$, so that F_f is a formal group. An alternate (but

silly) method to verify $F_f(x,0) = x$ is to use uniqueness from the lemma again on $f = g, F = F_f(x,0), x$. □

Again using the lemma with $f, g \in \mathcal{F}_\pi$, and $L = ax, a \in \mathcal{O}_K$, we get a unique power series $[a]_{f,g}$ that is ax mod deg 2 and satisfies $f \circ [a]_{f,g} = [a]_{f,g} \circ g$. We will write $[a]_{f,f} = [a]_f$ for concision. From uniqueness in the lemma we can deduce that $[a]_{f,g}$ is a homomorphism from F_g to F_f, that $[ab]_{f,h} = [a]_{f,g} \circ [b]_{g,h}$, that $[a+b]_f = F_f([a]_f, [b]_f)$, $[\pi]_f = f$, and $[1]_f = x$. The last few statements are summarized in the proposition below:

Proposition 4.3. *The map $a \mapsto [a]_f$ makes F_f a faithful formal $\mathcal{O}_K$-module, and $\pi \mapsto f$. Moreover, $[a]_{g,f} : F_f \to F_g$ is a module homomorphism. The modules F_f, F_g are canonically isomorphic via $[1]_{f,g}$.*

Proof. That $[a]_{g,f}$ is a module homomorphism comes from the fact that $[a]_{g,f} \circ [b]_f = [ab]_{g,f} = [b]_g \circ [a]_{g,f}$. □

Thus we can view the F_f as models of the same formal module which only depends on π.

If L/K is a Galois extension of K, $\mathfrak{m}_L$, the maximal ideal of L, can be made into a $\mathcal{O}_K[\mathrm{Gal}(L/K)]$-module, where the underlying addition is given by $a + b = F_f(a,b)$, which is seen to converge since a, b are not units. Multiplication is given by $xa = [x]_f(a)$ for $x \in \mathcal{O}_K$, and $\tau a = \tau(a)$ for $\tau \in \mathrm{Gal}(L/K)$. The action of $\mathrm{Gal}(L/K)$ commutes with that of $\mathcal{O}_K$ by continuity, and it is easy to see that $[1]_{f,g}$ gives an isomorphism between the different module structures on $\mathfrak{m}_L$ for different $f, g \in \mathcal{F}_\pi$.

Let $\Lambda_{f,m}$ be the torsion submodule of $\mathfrak{m}_L$ killed by $[\pi^m]_f$, and Λ_f be $\cup_1^\infty \Lambda_{f,i}$. $x \in \Lambda_{f,m}$ iff $[1]_{g,f}(x) \in \Lambda_{g,m}$, so the extension $K[\Lambda_{f,m}]$ doesn't depend on f, so we will call it $L_{\pi,m}$ and its Galois group $G_{\pi,m}$, with $L_\pi = \cup_1^\infty L_{\pi,i}$ with Galois group G_π. We will see below that the extensions $L_{\pi,i}/K$ are totally ramified abelian.

Theorem 4.4. *Let L be a separable closure of K. Then:*

The module $\mathfrak{m}_L$ is divisible.

$\Lambda_{\pi,m} \cong \mathcal{O}_K/\pi^m\mathcal{O}_K, \Lambda_{\pi,m} \cong K/\mathcal{O}_K$ as $\mathcal{O}_K$-modules.

For each $\tau \in G_\pi$, there is a unique unit u such that τ acts as u on Λ_π.

The map $\tau \mapsto u$ is an isomorphism of G_π onto $\mathcal{O}_K^\times$, and $G_{\pi,m}$ correspond to the quotients $\mathcal{O}_K^\times/(1+\mathfrak{m}^m)$

π is a norm of each extension $L_{\pi,m}/K$.

Proof. Since our choice of f doesn't matter, we can choose $f = T^q + \pi T$. To show $\mathfrak{m}_L$ is divisible, it suffices to show that $\pi x + x^q = [\pi]_f(x) = y$ has a solution for each y. Indeed, the roots of $f - y$ lie in in $\mathfrak{m}_L$ since the derivative $qT^{q-1} + \pi$ has no roots in $\mathfrak{m}_K^{ab}$, where K^{ab} is the algebraic closure.

The module $\Lambda_{\pi,1}$ consists of the q roots of f, so is a one dimensional $\mathcal{O}_K/\mathfrak{m}$ vector space. Each $\Lambda_{\pi,m}$ is a finitely generated module since it consists of roots of $f^{(m)} = f(f(\dots(f)\dots))$ so $\Lambda_{\pi,m} \cong \mathcal{O}_K/\pi^m\mathcal{O}_K, \Lambda_{\pi,m} \cong K/\mathcal{O}_K$ follows from classification of f.g. modules over a PID and since m_L is divisible.

Each $\tau \in G_\pi$ acts as an automorphism on $\Lambda_\pi \cong K/\mathcal{O}_K$, but the only automorphism are given by multiplication by a unit u. Moreover, it is clear that the map $\tau \mapsto u$ reduces to a map $G_{\pi,m} \to \mathcal{O}_K/(1+\mathfrak{m})^m$ by looking at the automorphisms of $\Lambda_{\pi,m}$. These maps are injective since $\Lambda_{\pi,m}$ generates $L_{\pi,m}$, and are surjective by counting. $|G_{\pi,m}| = [L_{\pi,m} : K]$, and to find this degree, since that we are adjoining the roots of $f^{(m)}$, and hence those of $\frac{f^{(m)}}{f^{(m-1)}} = f^{(m-1)} + \pi$ which is degree $q^m - q^{m-1}$ and irreducible by Eisenstein's criterion, which is also the same size as $\mathcal{O}_K/(1+\mathfrak{m})^m$.

Finally, since the constant term of $\frac{f^{(m)}}{f^{(m-1)}}$ is π, π is a norm. □

Thus L_π is a totally ramified abelian extension, and we see that it can be constructed by adjoining the roots of $f^{(m)}$. It is instructive to consider the case $K = \mathbb{Q}_p$. Here we can choose $f = (1+x)^p - 1$, so that totally ramified abelian extensions are produced by adjoining roots of $f^{(m)} = (1+x)^{p^m} - 1$, which are of the form $\zeta_{p^m} - 1$ where $\zeta_{p^m}^{p^m} = 1$.