Lubin-Tate

Wenqi Li

April 10, 2024

1 Formal group laws

Definition 1.1. Let A be a ring. A commutative formal group law is an element F in the ring of formal power series $A[\![X,Y]\!]$ satisfying:

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

In [CF10], there are two more axioms:

a) $F(X,Y) = X + Y + $(degree 2 and higher terms)

b) there exists a unique $G \in A[\![X]\!]$ such that $F(X,G(X)) = 0 = F(G(X),X)$.

It is obvious that a) is a consequence of 1. We show that b) is also a consequence.

Lemma 1.2. *Let F be a commutative formal group law. There exists a unique $G \in A[\![X]\!]$ such that $F(X,G(X)) = 0 = F(G(X),X)$.*

Proof. Since $F(X,Y) = X + Y + $(degree 2 and higher terms), $F(X,G(X)) = 0$ means

$$X + G(X) + \text{ higher terms } = 0$$

Therefore the the degree 0 part of $G(X)$ must be 0 and the degree 1 part of $G(X)$ must be $-X$. We will inductively construct $G(X)$. Let G_d denote the degree $\leq d$ part of G. So assume $G_d(X)$ is known and satisfies

$$F(X,G_d(X)) = 0 \mod X^{d+1}.$$

This means

$$F(X,G_d(X)) = c_{d+1}X^{d+1} \mod X^{d+2}$$

for a unique $c_{d+1} \in A$. Let $G_{d+1}(X) = G_d(X) - c_{d+1}X^{d+1}$. Then

$$\begin{aligned} F(X, G_{d+1}(X)) &= F(X, G_d(X) - c_{d+1}X^{d+1}) \\ &= X + G_d(X) - c_{d+1}X^{d+1} + H(X, G_d(X) - c_{d+1}X^{d+1}) \end{aligned}$$

where $H(X,Y)$ has no linear and constant terms. Modulo X^{d+2}, $H(X, G_d(X) - c_{d+1}X^{d+1})$ is just $H(X, G_d(X))$ since other terms has degree at least $d+2$. Thus

$$F(X, G_{d+1}(X)) = F(X, G_d) - c_{d+1}X^{d+1} = 0 \mod X^{d+2}.$$

This completes the inductive step. ■

Definition 1.3. Let F, G be commutative formal group laws. A morphism of formal group laws $h : F \to G$ is a formal power series $h \in A[\![X]\!]$ such that $h \in XA[\![X]\!]$ and $h(F(X,Y)) = G(h(X), h(Y))$. h is an isomorphism if there exist a morphism g such that $g(h(X)) = X = h(g(X))$.

Note that $h \in XA[\![X]\!]$ is necessary since otherwise $G(h(X), h(Y))$ involves a summation of infinitely many elements in A.

Lemma 1.4. *Let $h : F \to G$ be a morphism of formal group laws, so $h(X) = a_1X + \cdots$. It is an isomorphism if and only if a_1 is a unit in A.*

Proof. Suppose $h(X)$ has an inverse $g(X) = b_1X + b_2X^2 + \cdots$. Then

$$h(g(X)) = a_1 g(X) + \cdots = a_1 b_1 X + \cdots$$

All terms in $\cdots$ are of degree 2 or higher. Thus $a_1 b_1 = 1$ so a_1, b_1 are units in A. Conversely, if a_1 is a unit in A, let $b_1 = a_1^{-1}$. Now inductively construct coefficients $b_2, \cdots$: suppose we want to construct b_n. The coefficient before X^n is of the form

$$a_1 b_n + \cdots = 0$$

So we let b_n be the unique solution to the above equation, which exists since a_1 is a unit. ■

Let K be a local field, $\mathcal{O}_K$ its valuation ring, $\mathfrak{m}_K$ the maximal ideal and k the residue field. Let $q = |k|$.

Definition 1.5. Let π be a uniformizer of $\mathcal{O}_K$. A Frobenius power series is a power series $f \in \mathcal{O}_K[\![X]\!]$ such that

$$f(X) = \pi X \mod X^2$$

and

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

Definition 1.6. Let f be a Frobenius power series. The unique formal group law F_f such that f is an automorphism of F_f is called the Lubin-Tate formal group law (for f).

It is unclear such a formal group law exists. Our next goal is to prove this existence.

2 Lubin-Tate group laws

Proposition 2.1. *Let f, g be Frobenius power series. Let F_1 be a homogenous linear polynomial in variables $X_1, \cdots, X_m$ over $\mathcal{O}_K$. There exists a unique $F \in \mathcal{O}_K[[X_1, \cdots, X_m]]$ such that $F = F_1$ modulo degree 2, and*

$$f(F(X_1, \cdots, X_m)) = F(g(X_1), g(X_2), \cdots, g(X_m)).$$

Proof. We construct F degree by degree. In this proof, when we write mod X^n we mean to mod out by the ideal of homogenous pieces of degrees at least n. We will construct a sequence of polynomial F_n of degree at most n such that $F_{n+1} = F_n \mod X^{n+1}$, $F_n = F_1 \mod X^2$, and

$$f(F_n(X_1, \cdots, X_n)) = F_n(g(X_1), g(X_2), \cdots, g(X_n)) \mod X^{n+1}.$$

For $n = 1$ we take the given F_1. The first two conditions are vacuous, and for the third one we have

$$f(F_1(X_1, \cdots, X_n)) = \pi F_1(X_1, \cdots, X_n) = F_1(\pi X_1, \cdots, \pi X_n) = F_1(g(X_1), \cdots, g(X_n)) \mod X^2.$$

Now assume that we have constructed $F_1, \cdots, F_n$. We know that $f \circ F_n - F_n \circ g$ is zero mod X^{n+1}, so

$$f \circ F_n - F_n \circ g = P_{n+1} \mod X^{n+2}$$

for a unique homogenous P_{n+1} of degree $n+1$.

Suppose $F_{n+1} - F_n = E_{n+1}$ where E_{n+1} is homogenous of degree $n+1$. What should E_{n+1} be? We have

$$f \circ F_{n+1} = f \circ (F_n + E_{n+1})$$

Modulo X^{n+2}, this is equal to $f \circ F_n + \pi E_{n+1}$ since any non-constant term multiplied by E_{n+1} is killed. Also,

$$F_n \circ g + E_{n+1} \circ g = F_n \circ g + \pi^{n+1} E_{n+1} \mod X^{n+2}$$

because in $E_{n+1} \circ g$ only the degree 1 terms of g survive. So we must have

$$f \circ F_n + \pi E_{n+1} = F_n \circ g + \pi^{n+1} E_{n+1} \mod X^{n+2}$$

This means we must take $E_{n+1} = \frac{P_{n+1}}{\pi(1-\pi^n)}$. By the Frobenius property, we have that

$$f \circ F_n - F_n \circ g = F_n(X_1, \cdots, X_n)^q - F_n(X_1^q, \cdots, X_n^q) \mod \pi.$$

In k, $(a+b)^q = a^q + b^q$, so the above difference is 0. This implies π divides P_{n+1}. Therefore E_{n+1} is well-defined since π divides P_{n+1} and $1 - \pi^n$ is a unit.

∎

Proposition 2.2. *Let $f \in \mathcal{O}_K[\![X]\!]$ be a Frobenius power series. There exists a unique formal group law $F_f \in \mathcal{O}_K[\![X,Y]\!]$ such that f is an automorphism of F_f.*

Proof. By Proposition 2.1 applied to $F_1 = X+Y$, we know that there exists a unique $F \in \mathcal{O}_K[\![X,Y]\!]$ such that $F = X+Y \bmod X^2$ and $f(F(X,Y)) = F(f(X), f(Y))$. It remains to check that F is a formal group law, namely it is associative.

We want to prove an equality of formal power series $F(F(X,Y),Z) = F(X,F(Y,Z))$. Notice that both of them are a formal power series $G(X,Y,Z)$ satisfying $G(X,Y,Z) = X+Y+Z$ mod degree 2, and $f \circ G = G \circ f$. Such a power series is unique by Proposition 2.1, so F is indeed a group law. ∎

Let f,g be Frobenius power series. For any $a \in \mathcal{O}_K$, by Proposition 2.1 there exists a unique formal power series $[a]_{f,g} \in \mathcal{O}[\![X]\!]$ such that $[a]_{f,g} = aX \bmod X^2$, and $f \circ [a]_{f,g} = [a]_{f,g} \circ g$. When $f = g$ we simplify the notation to be $[a]_f$.

Lemma 2.3. *Let f,g be Frobenius power series. $[a]_{f,g}$ is a homomorphism of formal group laws $F_g \to F_f$.*

Proof. We want to show that $[a]_{f,g} \circ F_g = F_f \circ [a]_{f,g}$. Note that both side are equal to $aX + aY$ modulo degree 2. Moreover, we have

$$f([a]_{f,g} \circ F_g) = f([a]_{f,g}(F_g)) = [a]_{f,g}(g(F_g)) = [a]_{f,g}(F_g(g(X), g(Y)))$$

and similarly

$$f(F_f \circ [a]_{f,g}) = F_f(f \circ [a]_{f,g}(X), f \circ [a]_{f,g}(Y)) = (F_f \circ [a]_{f,g})(g(X), g(Y)).$$

However by Proposition 2.1, there is only one formal power series with these properties. Hence $[a]_{f,g} \circ F_g = F_f \circ [a]_{f,g}$. ∎

In particular, $[a]_{f,g}$ is an isomorphism whenever a is a unit in $\mathcal{O}_K$. So for any Forbenius power series f,g, there is a canonical isomorphism $F_f \to F_g$ given by $[1]_{f,g}$.

Let L/K be an algebraic extension. Let $\mathfrak{m}_L, \mathfrak{m}_K$ be the maximal ideals in $\mathcal{O}_L$ and $\mathcal{O}_K$. They consist of elements with absolute value less than 1. Therefore, if F is a formal group law, and $x,y \in \mathfrak{m}_L$, then $F(x,y)$ converges. This turns $\mathfrak{m}_L$ into an abelian group. We denote this abelian group by $F(\mathfrak{m}_L)$.

Now let π be a uniformizer of $\mathcal{O}_K$ and f a Frobenius power series for π. We have the Lubin-Tate formal group law F_f. The abelian group $F_f(\mathfrak{m}_L)$ is an $\mathcal{O}_K$-module: the action is given by $a \cdot x = [a]_f(x)$.

Now we take $L = K^s$ the separable closure of K. Let E_f be the torsion submodule of the $\mathcal{O}_K$-module $F_f(\mathfrak{m}_L)$. Note that any element in $\mathcal{O}_K$ is of the form $u\pi^n$ for some unit u and $n \geq 0$. So if x is an torsion element, then it is killed by some π^n. Hence if we denote by E_n the kernel of $[\pi^n]_f$, we have $E_f = \cup_{n \geq 0} E_n$.

We saw above that any Frobenius power series give the same formal group law. Therefore we might as well choose $f = \pi X + X^q$. Then f commutes with itself, and $f = \pi X \bmod X^2$. Hence $f = [\pi]_f$. It follows also that $f^{(n)} = [\pi^n]_f$. Thus $\alpha \in E_n$ if and only if $f^{(n)}(\alpha) = 0$.

We first focus on E_1. By the above discussion it consists of element $\alpha \in \mathfrak{m}_L$ such that $f(\alpha) = 0$. What are these zeroes?

Lemma 2.4. *For any $z \in \mathfrak{m}_L$, the polynomial $\pi X + X^q - z$ is separable, and its roots have absolute value less than* 1.

Proof. The derivative is $\pi + qX^{q-1}$. If y is a root of the derivative that has absolute value less than 1, then

$$|\pi| = |q||y^{q-1}| < |q|.$$

But q is 0 mod π, so $|q| \leq |\pi|$, a contradiction. This means any root y of the derivative satisfies $|y| \geq 1$. If y is also a root of $\pi X + X^q - z$, then reducing mod $\mathfrak{m}_L$ we know that $y^q = 0$, so $y = 0$ in $\mathcal{O}_L/\mathfrak{m}_L$, i.e. y has absolute value less than 1. Therefore $\pi X + X^q - z$ is separable and its roots have absolute value less than 1. ∎

This implies that E_1 is a submodule of $F_f(\mathfrak{m}_L)$ that has q-elements, so it is isomorphic to $k = \mathcal{O}_k/(\pi)$ as $\mathcal{O}_K$-modules. Note that this also means $F_f(\mathfrak{m}_L)$ is a π-divisible $\mathcal{O}_K$-module: for any $z \in \mathcal{O}_K$ that is not a unit, there exists some y such that

$$[\pi]_f(y) = z.$$

Proposition 2.5. *We have $E_f \cong K/\mathcal{O}_K$ as $\mathcal{O}_K$-modules.*

Proof. Each E_n is a finitely generated $\mathcal{O}_K$-module, so by the structure theorem of finitely generated modules over PIDs, and the fact that E_n is torsion, we know that E_n must be a direct sum of modules of the form $\mathcal{O}_K/(\pi^m)$. Multiply the generators by suitable powers of π, we would get linearly independent elements in E_1, so we conclude that each E_n is generated by 1 elements. Thus they are of the form $\mathcal{O}_K/(\pi^m)$.

Multiplication by π gives a surjective map from E_n to E_{n-1}, because for any $z \in E_{n-1}$, there exists y such that $[\pi]_f(y) = z$, and clearly $[\pi^{n-1}]_f(z) = 0$ implies $[\pi^n]_f(y) = 0$. Therefore we have the short exact sequence

$$0 \to E_1 \to E_n \to E_{n-1} \to 0.$$

Counting cardinality shows that $E_n \cong \mathcal{O}_K/(\pi^n)$. Hence

$$E_f = \varinjlim_{n \to \infty} \pi^{-n}\mathcal{O}_K/\mathcal{O}_K \cong K/\mathcal{O}_K.$$

∎

Let $K_\pi^n = K(E_n)$ and let $K_\pi = K(E_f)$. Then the extensions K_π^n/K are all Galois since they are splitting fields of $f^{(n)}$. We have that $\mathrm{Gal}(K_\pi/K) = \varprojlim_n \mathrm{Gal}(K_n/K)$.

Lemma 2.6. *We have* $\mathrm{Aut}(E_f) \cong \mathcal{O}_K^\times$ *and* $\mathrm{Aut}(E_n) \cong (\mathcal{O}_K/(\pi^n))^\times \cong \mathcal{O}_K^\times/(1+\pi^n\mathcal{O}_K)$.

Proof. For notational ease let $A = \mathcal{O}_K$. First note that since $E_f \cong K/A$, the A-linear maps $E_f \to E_f$ are A-linear maps $K/A \to K/A$. For such a map f, we know that 1 must be sent to some element $a \in A$, and then $f(\pi^{-1})$ must be some element in $\pi^{-1}A$ such that $\pi f(\pi^{-1}) = f(1) \bmod A$. Namely, $f(1/\pi^{-1})$ is a uniquely determined element in $\pi^{-1}A/A$. Continuing, $f(\pi^{-n})$ is a uniquely determined element in $\pi^{-n}A/A$. This sequence is then an element in the inverse limit

$$\varprojlim_n \pi^{-n}A/A \cong \varprojlim_n A/\pi^n A = A$$

since A is complete. Such a sequence uniquely determines f, and conversely multiplication by an element in A gives a map $K/A \to K/A$, so we see that $\mathrm{End}_A(K/A) \cong A$. It then follows the automorphisms are $\mathrm{Aut}_A(K/A) \cong A^\times$.

Recall that $E_n \cong A/(\pi^n)$, so $\mathrm{Aut}(E_n) \cong (A/(\pi^n))^\times$. A unit in $A/(\pi^n)$ is an element $a \in A$ such there exists some b with $ab = 1 \bmod \pi^n$. Certainly a unit in A satisfies this condition, and if a, a' are units and $a = (1+b\pi^n)a'$, then $a = a'$ in $A/(\pi^n)$. On the other hand, if a is not a unit in A, then $a = b\pi$ for some $b \in A$, so there is no b such that $ab = 1 + c\pi^n$ because $|1+c\pi^n| = |1| = 1$ but $|ab| < 1$. ■

Proposition 2.7. *We have* $\mathrm{Gal}(K_n/K) \cong \mathcal{O}_K^\times/U_K^n$ *and* $\mathrm{Gal}(K_\pi/K) \cong \mathrm{Aut}(E_f) = \mathcal{O}_K^\times$, *where* $U_K^n = 1+\pi^n\mathcal{O}_K$.

Proof. If $\sigma \in \mathrm{Gal}(K_\pi/K)$, then $\sigma|_{E_f}$ is an automorphism of E_f. This gives an injection $\mathrm{Gal}(K_\pi/K) \to A^\times$. Similarly, if $\sigma \in \mathrm{Gal}(K_n/K)$, then $\sigma|_{E_n}$ is an automorphism of E_n, and if σ is the identity on E_n then it fixes K_n, so $\sigma = 1$ in $\mathrm{Gal}(K_\pi/K)$. Therefore for each n we have injections $\mathrm{Gal}(K_n/K) \to \mathrm{Aut}(E_n)$.

Let $\Phi_0 = X$, and $\Phi_n = f^{(n)}/f^{(n-1)} = (f^{(n-1)}(X))^{q-1} + \pi$. Then $f^{(n)} = \Phi_n \cdots \Phi_0$. Notice that Φ_n has degree $(q-1)q^{n-1}$, and is irreducible since it is Eisenstein. A primitive element for K_n is a root of Φ_n since it is killed by π^n but not by π^{n-1}, so the degree of K_n is $(q-1)q^{n-1}$. On the other hand, $\mathrm{Aut}(E_n) = \mathcal{O}_K^\times/U_K^n$, and we note that $\mathcal{O}_K^\times/U_K^1 \cong (A/\pi)^\times$ has size $q-1$, and $U_K^n/U_K^{n+1} \cong A/\mathfrak{m}$ has size q ($1+u\pi^n$ goes to $1+u$ is surjective with kernel U_K^{n+1}), so $\mathcal{O}_K^\times/U_K^n$ has size $(q-1)q^{n-1}$. Hence we see that the injection $\mathrm{Gal}(K_n/K) \to \mathrm{Aut}(E_n)$ are all isomorphisms. Passing to the inverse limit gives $\mathrm{Gal}(K_\pi/K) \cong \mathrm{Aut}(E_f)$. ■

Corollary 2.8. *The extensions* K_n/K *are totally ramified.*

Proof. We saw in the proof above that $K_n = K(\alpha)$ where α is a root of Φ_n, which is a Eisenstein polynomial. Thus K_n/K is totally ramified (proved in class). ■

3 Local class field theory

We want to study the field $L_\pi = K_{nr}K_\pi$ where K_{nr} is the maximal unramified extension of K. Let $\widehat{K_{nr}}$ be its completion and $\widehat{A_{nr}}$ be its valuation ring. There is a Frobenius element $\sigma \in \mathrm{Gal}(K_{nr}/K)$, lifted from the Frobenius for the residue field extension. Suppose π is a uniformizer of K, and $\omega = \pi u$ is another uniformizer. Let f be a Frobenius power series for π, and g a Frobenius power series for ω. Then

Lemma 3.1. *There exists a power series $\phi \in \widehat{A_{nr}}[\![X]\!]$ such that $\phi = aX$ where a is a unit, and*

1. $\sigma(\phi) = \phi \circ [u]_f$
2. $\phi \circ F_f = F_g \circ \phi$
3. $\phi \circ [a]_f = [a]_g \circ \phi$ *for all $a \in A$. Here A is the valuation ring for K.*

Proof. We will inductively produce ψ_n. Let $\psi_1 = aX$. We have that

$$(\psi_1 \circ [u]_f)(X) = auX \mod X^2$$

so a must satisfy $\sigma(a) = au$. It is a fact that $x \mapsto \sigma(x)/x$ is a surjection onto the group of units in $\widehat{A_{nr}}$, so there exists a that satisfies this equation. Now suppose we have a compatible sequence ψ_n such that $\sigma(\psi_n) = \psi_n \circ [u]_f \bmod X^{n+1}$. We want to construct

$$\psi_{n+1}(X) = \psi_n(X) + c_{n+1}X^{n+1}$$

satisfying the same condition. Namely, modulo X^{n+2}

$$\psi_{n+1}([u]_f(X)) = \psi_n([u]_f(X)) + c_{n+1}([u]_f(X)^{n+1}) = \sigma(\psi_n)(X) + r_{n+1}X^{n+1} + c_{n+1}u^{n+1}X^{n+1}$$

So we require $\sigma(c_{n+1}) = r_{n+1} + c_{n+1}u^{n+1}$. Let $c_{n+1} = c'a^{n+1}$, so it suffices to solve for c' since a is a unit. The equation becomes

$$\sigma(c')\sigma(a)^{n+1} = r_{n+1} + c'(au)^{n+1} = r_{n+1} + c'\sigma(a)^{n+1}$$

i.e.

$$\sigma(c') - c' = \frac{r_{n+1}}{\sigma(a)^{n+1}}$$

But $\sigma - 1$ is surjective on $\widehat{A_n r}$, so such a c' exists. This completes the construction of ψ_n, so we obtain a series ψ satisfying the requirement 1.

What about conditions 2 and 3? Note that since a is a unit, the series ψ is invertible. Let

$$h = \sigma(\psi) \circ f \circ \psi^{-1} = \psi \circ [u]_f \circ f \circ \psi^{-1} = \psi \circ [\omega]_f \circ \psi^{-1}.$$

The series h is in $A[\![X]\!]$ since it is fixed by σ. The trick is to define let $\phi = [1]_{g,h}\psi$. The degree one coefficient is unchanged, and 1 is still satisfied because σ commutes with series (simply by definition). Then

$$\sigma(\phi) \circ f \circ \phi^{-1} = [1]_{g,h} \circ \sigma(\psi) \circ f \circ \psi^{-1} \circ [1]_{g,h}^{-1} = [1]_{g,h} \circ h \circ [1]_{g,h}^{-1} = g$$

Then 2 and 3 are verified via the uniqueness of series satisfying commuting properties with g. ■

The extensions K_{nr} and K_π are linearly disjoint: K_{nr} is Galois over K, so to test linear disjointness we just need to check that $K_{nr} \cap K_\pi = K$. This is true because K_π is totally ramified and K_{nr} is unramified. Thus the extension L_π makes sense.

We would like to use the above lemma to prove that L_π is independent of the choices of π. So let $\omega = \pi u$ be another uniformizer. The lemma implies that ϕ is an isomorphism of the group laws F_f and F_g, considered as group laws over $\widehat{K_{nr}}$. Thus the torsion submodules of F_f and F_g (this really means $F_f(\mathfrak{m}_{K^s})$) are the same, so $\widehat{K_{nr}}K_\pi = \widehat{K_{nr}}K_\omega$. Here are we considering $\widehat{K_{nr}}K_\pi$ as an extension of $\widehat{K_{nr}}$ by adjoining the torsion element. Taking completion, we get $\widehat{K_{nr}K_\pi} = \widehat{K_{nr}K_\omega}$.

Lemma 3.2. *Let E be any algebraic extension of a local field. If $\alpha \in \hat{E}$ is algebraic and separable, then $\alpha \in E$.*

Proof. Let E' be the closure of E is a separable closure. Then $\alpha \in E'$. But any Galois automorphism fixing E also fixes E' by continuity, so $E = E'$. ■

This means $K_{nr}K_\pi = K_{nr}K_\omega$, so $L_\pi = L$ is independent of the choice of π.

Now we define a homomorphism $r_\pi : K^\times \to \mathrm{Gal}(L_\pi/K)$ as follows: any element of $K^\times$ is a product $u\pi^n$ where $u \in A^\times$ and $n \in \mathbf{Z}$. So it suffices to prescribe what $r_\pi(u)$ is for $u \in A^\times$ and what $r_\pi(\pi)$ is. We set

1. $r_\pi(\pi) = 1$ on K_π and σ on K_{nr}
2. $r_\pi(u) = [u^{-1}]_f$ on K_π and 1 on K_{nr}.

We want to show that this is also independent of the choice of π. So again let $\omega = \pi u$ be another uniformizer. We want to show that $r_\pi(\omega) = r_\omega(\omega)$. Namely, we need to compute $r_\pi(\omega)$ on K_ω.

Recall that $K_\omega = K(E_g)$ where E_g is the torsion elements of $F_g(\mathfrak{m}_{K^s})$. Let $\phi \in \widehat{A_{nr}}[\![X]\!]$ as in Lemma, which gives an isomorphism between E_f and E_g. For any $\lambda \in E_g$, there is $\mu \in E_f$ such that $\lambda = \phi(\mu)$. What we want to show is that $r_\pi(\omega)$ acts as 1 on E_g, i.e. $r_\pi(\omega)(\lambda) = \lambda$. We have

$$r_\pi(\omega)(\phi) = r_\pi(\pi)r_\pi(u)(\phi) = \sigma(\phi) = \phi \circ [u]_f$$

because $r_\pi(u)$ is 1 on K_{nr} and $r_\pi(\pi)$ is σ on K_{nr}. Thus

$$r_\pi(\omega)(\lambda) = r_\pi(\omega)(\phi(\mu)) = r_\pi(\omega)(\phi)(r_\pi(\omega)(\mu)) = \phi \circ [u]_f[u^{-1}]_f(\mu) = \phi(\mu) = \lambda$$

So $r_\pi(\omega) = r_\pi(\pi)$.

We also want to show that $r_\pi(u) = r_\omega(u)$ on E_g. We have

$$r_\pi(u)(\lambda) = r_\pi(u)(\phi(\mu)) = \phi([u^{-1}]_f(\mu)) = [u^{-1}]_g(\lambda)$$

by condition 3 of the lemma. Thus the homomorphism $r_\pi = r$ is independent from the choice of π. However such a homomorphism is uniquely determined, and the norm residue symbol θ is such a homomorphism, so $r = \theta$.

Notice that $r|_{A^\times}$ maps into $\mathrm{Gal}(L/K_{nr}) = \mathrm{Gal}(K_\pi/K)$, by $u \mapsto [u^{-1}]_f$. We proved earlier that $\mathrm{Gal}(K_\pi/K) \cong \mathrm{Aut}(E_f) \cong A^\times$, so this is an isomorphism. This implies that the composition

$$A^\times \to \mathrm{Gal}(K^{ab}/K_{nr}) \to \mathrm{Gal}(L/K_{nr})$$

is an isomorphism. The first step is the absolute θ, which is surjective, and the second step is the natural surjection. Hence both θ and the second step are isomorphisms. This proves the theorem on norm subgroups, and that $L = K^{ab}$.

References

[CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union*. London Mathematical Society, 2010. ISBN: 9780950273426.