33 Proof of the local existence theorem

Let K be a nonarchimedean local field. As explained in the previous lecture, to complete our proof the existence theorem of local class field theory (Theorem 27.8), which states that every finite index open subgroup of $K^\times$ is a norm group, we need to construct a system of totally ramified abelian extensions $K_{\pi,n}/K$ and a homomorphism $\theta_\pi\colon K^\times \to \operatorname{Gal}(K_\pi^{\text{ab}}/K)$ satisfying the hypotheses of Theorem 32.1. More precisely, let $\mathfrak{p}$ be the maximal ideal of the valuation ring $A := \mathcal{O}_K$, let π be a uniformizer for $\mathfrak{p}$, and define:

- $q := A/\mathfrak{p}$ is the cardinality of the residue field;
- K_m/K is the unique extension of degree m in K^{unr};
- $K_{\pi,n,m} := K_{\pi,n}K_m$;
- $U_{\pi,n,m} := (1+\mathfrak{p}^n)\langle\pi^m\rangle \subseteq K^\times$;
- $K_\pi := \bigcup_{n\ge 1} K_{\pi,n}$;
- $K_\pi^{\text{ab}} := K_\pi K^{\text{unr}}$;

To satisfy the hypotheses of Theorem 32.1 we need the following to hold:

(i) $[K_{\pi,n} : K] = (q-1)q^{n-1}$ and $\pi \in \mathrm{N}(K_{\pi,n}^\times)$;

(ii) $\theta_\pi(\pi)_{|K^{\text{unr}}} = \operatorname{Frob}_K$ and $\theta_\pi(a)_{|K_{\pi,n,m}} = 1$ for all $a \in U_{\pi,n,m}$;

(iii) K_π^{ab} and θ_π do not depend on the choice of π.

In the previous lecture we associated to any uniformizer π the set of power series

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

We showed that for each $\phi \in \Phi(\pi)$ there is a unique Lubin-Tate formal group law F_ϕ such that $\phi \in \operatorname{End}(F_\phi)$, and we defined an injective ring homomorphism

$$\begin{aligned} A &\hookrightarrow \operatorname{End}(F_\phi)\\ a &\mapsto [a]_\phi \end{aligned}$$

where $[a]_\phi \equiv aT \bmod T^2$ and $\phi \circ [a]_\phi = [a]_\phi \circ \phi$ (these properties uniquely determine $[a]_\phi$), such that $[\pi]_\phi = \phi$.

33.1 Constructing the extensions K_π/K

As above, let K be a nonarchimedean local field with valuation ring A and let π be a uniformizer for A, and let $q = \#A/(\pi)$ be the cardinality of the residue field. The absolute value on K extends uniquely to an absolute value on K^{sep}, via Theorem 10.6. For any $\phi \in \Phi(\pi)$ and all $\alpha, \beta \in K^{\text{sep}}$ with $|\alpha|, |\beta| < 1$ and any $a \in A$ the series $F_\phi(\alpha,\beta)$ and $[a]_\phi(\alpha)$ converge to elements that lie in a finite extension of K (because α and β lie in a finite extension of K which must be complete, by Theorem 10.6, even though K^{sep} is not).

For each $\phi \in \Phi(\pi)$ we define the A-module

$$\Lambda_\phi := \{\alpha \in K^{\text{sep}} : |\alpha| < 1\},$$

with addition given by $\alpha +_{\Lambda_\phi} \beta := F_\phi(\alpha,\beta)$ and A-multiplication by $a \cdot_{\Lambda_\phi} \alpha := [a]_\phi(\alpha)$. For any $\psi \in \Phi(\pi)$ the canonical isomorphism $[1]_{\phi,\psi}\colon F_\psi \to F_\phi$ induces an A-module isomorphism

$\Lambda_\psi \to \Lambda_\phi$, so the A-module structure of Λ_ϕ is really determined by π. In particular, up to a canonical isomorphism that will not change the A-module structure of Λ_ϕ, we can assume without loss of generality that $\phi(T) = \pi T + T^q$ is actually a polynomial, not just a power series (this particular ϕ is clearly an element of $\Phi(\pi)$).

We now define $\Lambda_{\phi,n}$ as the A-submodule of Λ_ϕ killed by π^n, in other words, killed by

$$[\pi \cdots \pi]_\phi = [\pi]_\phi \circ \cdots \circ [\pi]_\phi = \phi \circ \cdots \circ \phi = \phi^{(n)}.$$

This is a finite set (consider the case $\phi(T) = \pi T + T^q$), of cardinality at most q^n (in fact equal to q^n, as we will show below). Thus $\Lambda_{\phi,n}$ is a finite A-module.

Example 33.1. Consider the local field $K = \mathbb{Q}_p$ with valuation ring $A = \mathbb{Z}_p$ and uniformizer $\pi = p$, and let $\phi(T) := (T+1)^p - 1$ (this choice of ϕ is slightly more convenient here than $pT + T^p$). We have $\phi \equiv \pi T \bmod T^2$ and $\phi \equiv T^p \bmod \pi$, so $\phi \in \Phi(\pi)$, and

$$\Lambda_{\phi,n} = \{\alpha \in \overline{\mathbb{Q}}_p : \phi^{(n)}(\alpha) = 1\} = \{\alpha \in \overline{\mathbb{Q}}_p : (\alpha+1)^{p^n} = 1\} \simeq \{\zeta \in \overline{\mathbb{Q}}_p : \zeta^{p^n} = 1\} = \mu_{p^n}(K)$$

is isomorphic to the group of p^nth roots of unity, where addition in $\Lambda_{\phi,n}$ corresponds to multiplication in $\mu_{p^n}(K)$ (but note that $\Lambda_{\phi,n}$ does not itself contain any roots of unity, indeed, its elements cannot be units because they have absolute values less than 1). As an additive group, $\Lambda_{\phi,n} \simeq \mathbb{Z}/p^n\mathbb{Z}$, and the $\mathbb{Z}_p$-action is just multiplication modulo p^n.

The valuation ring $A = \mathcal{O}_K$ is a DVR, and in particular a PID. The finite A-module $\Lambda_{\phi,n}$ is a finitely generated torsion module over a PID and therefore isomorphic to a direct sum of finite cyclic A-modules

$$A/(\pi^{m_1}) \oplus \cdots \oplus A/(\pi^{m_r}),$$

where the integers $m_1 \le \cdots \le m_r$ are uniquely determined (every non-trivial A-ideal has the form (π^m) for some $m \ge 1$ because A is a DVR). We want to determine the A-module structure of $\Lambda_{\phi,n}$ as a direct sum of finite cyclic A-modules.

Proposition 33.2. *Let A be the valuation ring of a local field K with uniformizer π. For any $\phi \in \Phi(\pi)$ and integer $n \ge 1$ the A-module $\Lambda_{\phi,n}$ is isomorphic to $A/(\pi^n)$.*

Proof. Let $q := \#A/(\pi)$ be the cardinality of the residue field. As noted above, without loss of generality we may assume $\phi(T) = \pi T + T^q$. This is a separable polynomial over A; it thus has q distinct roots α, and $\pi\alpha = -\alpha^q$ implies $\alpha = 0$ or $|\alpha| = |\pi|/(q-1) < 1$, so $\alpha \in \Lambda_\phi$. It follows that $\Lambda_{\phi,1}$ has cardinality q and is therefore isomorphic to $A/(\pi)$ (this is the smallest nonzero cyclic A-module, and it has cardinality q). This prove the lemma for $n = 1$, we now proceed by induction.

The A-module homomorphism $\pi\colon \Lambda_\phi \to \Lambda_\phi$ defined by $\alpha \mapsto [\pi]_\phi(\alpha) = \phi(\alpha)$ is surjective, since for any nonzero $\beta \in \Lambda_\phi$ the polynomial $\phi(T) - \beta = T^q + \pi T - \beta$ is separable and thus has a root α in K^{sep} with $|\alpha||\alpha^{q-1} - \pi| = |\beta| < 1$, which implies $|\alpha| < |\beta| < 1$. It follows that the induced map $\pi\colon \Lambda_{\phi,n} \to \Lambda_{\phi,n-1}$ is surjective, and its kernel is clearly $\Lambda_{\phi,1}$, so we have an exact sequence

$$0 \longrightarrow \Lambda_{\phi,1} \longrightarrow \Lambda_{\phi,n} \xrightarrow{\pi} \Lambda_{\phi,n-1} \longrightarrow 0$$

We have $\Lambda_{\phi,n-1} \simeq A/(\pi^{n-1})$ by the inductive hypothesis, and it follows that $\Lambda_{\phi,n}$ has cardinality q^n and is isomorphic to either $A/(\pi^n)$ or $A/(\pi) \oplus A/(\pi^{n-1})$. The latter cannot occur because the kernel of multiplication by π on the A-module $A/(\pi) \oplus A/(\pi^{n-1})$ has cardinality q^2, not q, and we have already shown that $\Lambda_{\phi,1}$ has cardinality q. $\square$

Definition 33.3. Let K be a nonarchimedean local field, π be a uniformizer π, let $\phi \in \Phi(\pi)$ be the polynomial $\pi T + T^q$, and let $\Lambda_n := \Lambda_{\phi,n}$. We define $K_{\pi,n} := K(\Lambda_n)$ to be the extension of K generated by the elements of Λ_n.

We will prove that $K_{\pi,n}$ is the splitting field of $\phi^{(n)}$ over K, whose roots are precisely the elements of Λ_n. We require the following lemma.

Lemma 33.4. *Let K be a nonarchimedean local field with valuation ring A, and let F be a power series in $R := A[[X_1, \ldots, X_r]]$. Suppose $\alpha_1, \ldots, \alpha_r \in K^{\mathrm{sep}}$ satisfy $|\alpha_1|, \ldots, |\alpha_r| < 1$. Then for every $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ we have*

$$F(\sigma(\alpha_1), \ldots, \sigma(\alpha_r)) = \sigma(F(\alpha_1, \ldots, \alpha_r)).$$

Proof. We first note that σ preserves absolute values, by Lemma 11.9. We can assume that $\alpha_1, \ldots, \alpha_r$ and $\sigma(\alpha_1), \ldots, \sigma(\alpha_r)$ all lie in a finite Galois extension L/K and restrict the action of σ to L. If we now consider the sequence of polynomials $F_n := F \bmod R_{>n}$ obtained by considering only terms of total degree at most n. The equality

$$F_n(\sigma(\alpha_1), \ldots, \sigma(\alpha_r)) = \sigma(F_n(\alpha_1, \ldots, \alpha_r))$$

is immediate, since the field automorphism σ fixes all the coefficients of F. The sequence $(F(\sigma(\alpha_1), \ldots, \sigma(\alpha_r)))_n$ is Cauchy, since $|\sigma(\alpha_i)| < 1$, and L is complete, by Theorem 10.6, so both sides of the equality above converge to the same element of L as $n \to \infty$. $\square$

Theorem 33.5. *Let K be a nonarchimedean local field with valuation ring A and uniformizer π, let $q := A/(\pi)$ be the cardinality of the residue field. The extension $K_{\pi,n}/K$ is separable and we have isomorphisms $(A/(\pi^n))^\times \xrightarrow{\sim} \mathrm{Aut}(\Lambda_n) \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,n}/K)$ induced by the maps $u \mapsto [u]_\phi \mapsto \sigma_u$, where σ_u is the permutation of Λ_n defined by $\alpha \mapsto [u]_\phi(\alpha)$ and*

$$\text{(i)} \quad [K_{\pi,n} : K] = (q-1)q^{n-1} \text{ and } \pi \in \mathrm{N}(K_{\pi,n}^\times).$$

Moreover, the field $K_{\pi,n}$ is a totally ramified abelian extension of K.

Proof. Let π_1 be a nonzero root of $\phi(T)$ in K^{sep}, and for $1 < m \le n$ choose a root π_m of $\phi(T) - \pi_{m-1}$ so that $\phi(\pi_m) = \pi_{m-1}$. The polynomial $\phi(T)/T = T^{q-1} + \pi$ is Eisenstein and separable, so π_1 generates a totally ramified extension $K(\pi_1)/K$ of degree $q-1$, and π_1 is a uniformizer for the valuation ring of $K(\pi_1)$. For each $m > 1$ the polynomial $\phi(T) - \pi_{m-1} = T^q + \pi T - \pi_{m-1}$ is Eisenstein and separable (by induction, π_{m-1} is a uniformizer), so $K(\pi_m)/K(\pi_{m-1})$ is a totally ramified extension of degree q and π_m is a uniformizer for its valuation ring. We thus have a tower of field extensions

$$K \subseteq K(\pi_1) \subseteq K(\pi_2) \subseteq \cdots \subseteq K(\pi_n) \subseteq K(\Lambda_n) = K_{\pi,n},$$

with $[K(\pi_1) : K] = q = -1$ and $[K(\pi_m) : K(\pi_{m-1}] = q$ for $1 < m \le n-1$. It follows that

$$[K_{\pi,n} : K] \ge (q-1)q^{n-1}.$$

We now observe that $K_{\pi,n} = K(\Lambda_n)$ is the splitting field of $\phi^{(n)}$, since every element of Λ_n is a root of $\phi^{(n)}$, by definition, and Λ_n has cardinality q^n, by Proposition 33.2, which is equal to the degree of $\phi^{(n)}$. Therefore $K_{\pi,n}$ is a Galois extension of K, and the action of $\mathrm{Gal}(K_{\pi,n}/K)$ on Λ_n is compatible with the A-module structure of Λ_n. Indeed, for each $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ and $a \in A$ and any $\alpha \in \Lambda_n$ we have

$$\sigma(a\alpha) \coloneqq \sigma([a]_\phi(\alpha)) = [a]_\phi(\sigma(\alpha)) \eqqcolon a\sigma(\alpha)$$

by Lemma 33.4. We thus have a group homomorphism $\mathrm{Gal}(K_{\pi,n}/K) \to \mathrm{Aut}_A(\Lambda_n)$. This homomorphism is injective, since Λ_n contains all the roots of $\phi^{(n)}$ and each $\sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ corresponds to a distinct permutation of these roots. It must also be surjective, because

$$\mathrm{Aut}(\Lambda_n) \simeq \mathrm{Aut}(A/(\pi^n)) \simeq (A/(\pi^n))^\times,$$

by Proposition 33.2, and $\#(A/(\pi^n))^\times = (q-1)q^{n-1} \le [K_{\pi,n} : K] = \#\mathrm{Gal}(K_{\pi,n}/K)$. Notice that for any cyclic A-module $A/(\pi^n)$ we can identify $\mathrm{End}(A/(\pi^n))$ with the ring $A/(\pi^n)$ and $\mathrm{Aut}(A/(\pi^n))$ with the unit group $(A/(\pi^n))^\times$, because every endomorphism of $A/(\pi^n)$ is determined by its action on $1 + (\pi^n)$.

It follows that $K_{\pi,n} = K(\pi_n)$ and

$$\mathrm{Gal}(K_{\pi,n}/K) \simeq (A/(\pi^n))^\times$$

is abelian, so $K_{\pi,n}/K$ is a totally ramified abelian extension of degree $(q-1)q^{n-1}$. The A-action on Λ_n is (by definition) induced by $a\alpha \coloneqq [a]_\phi(\alpha)$, and this corresponds to the natural A-action on $A/(\pi^n)$ (multiplication-by-a maps) under the A-module isomorphism in Proposition 33.2. Automorphisms of Λ_n and $A/(\pi^n)$ are induced by units $u \in A^\times$, each of which induces a permutation σ_u of Λ_n corresponding to an element of $\mathrm{Gal}(K_{\pi,n}/K)$ under the isomorphism above. We thus have $(A/(\pi^n)^\times \xrightarrow{\sim} \mathrm{Aut}(\Lambda_n) \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,n}/K)$ induced by the maps $u \mapsto [u]_\phi \to \sigma_u$ as claimed.

Now define $f_1(T) = \phi(T)/T$ and for $m > 1$ let $f_m = f_{m-1} \circ \phi$. Then

$$f_n(T) = \pi + \cdots + T^{(q-1)q^{n-1}}$$

is Eisenstein and

$$f_n(\pi_n) = f_{n-1}(\phi(\pi_n)) = f_{n-1}(\pi_{n-1}) = \cdots f_1(\pi_1) = 0.$$

The polynomial $f_n(T)$ is monic of degree $(q-1)q^{(n-1)}$ and $K(\pi_n) = K_{\pi,n}$ is a degree $(q-1)q^{n-1}$ extension of K, so $f_n(T)$ is the minimal polynomial of π_n. The constant term of $f_n(T)$ is π, thus by Proposition 4.51 we have

$$\mathrm{N}_{K_{\pi,n}/K}(\pi_n) = (-1)^{(q-1)q^{n-1}}\pi = \begin{cases} \pi & \text{if } q^n > 2, \\ -\pi & \text{if } q^n = 2. \end{cases}$$

If $q^n = 2$ then $(q-1)q^{n-1} = 1$ and $K_{\pi,1} = K$, in which case $\mathrm{N}_{K_{\pi,n}/K}(\pi) = \pi$, so in every case $\pi \in \mathrm{N}(K_{\pi,n})$ and (i) holds. □

The isomorphisms $(A/(\pi^n))^\times \xrightarrow{\sim} \mathrm{Aut}(\Lambda_n) \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,n}/K)$ given by $u \mapsto [u]_\phi \mapsto \sigma_u$ in Theorem 33.5 are natural in n, since we can reduce units $u \in A^\times$ modulo any ideal π^n to get corresponding isomorphisms for any integer $n \ge 1$. We thus have an isomorphism of inverse systems

$$A^\times \simeq \varprojlim_n A/(\pi^n) \simeq \varprojlim_n \mathrm{Gal}(K_{\pi,n}/K) \simeq \mathrm{Gal}(K_\pi/K),$$

where $K_\pi \coloneqq \bigcup_n K_{\pi,n}$.

Definition 33.6. Let K be a nonarchimedean local field with valuation ring A, let π be a uniformizer for A, let $\operatorname{Frob}_K \in \operatorname{Gal}(K^{\mathrm{unr}}/K)$ be the Frobenius element, let $K_\pi := \bigcup_n K_{\pi,n}$, and define $K_\pi^{\mathrm{ab}} := K_\pi K^{\mathrm{unr}}$. We define the homomorphism $\theta_\pi \colon K^\times \to \operatorname{Gal}(K_\pi^{\mathrm{ab}}/K)$ as follows: for $a = u\pi^m \in K^\times$ with $u \in A^\times$, let $\theta_\pi(a)_{|K^{\mathrm{unr}}} := \operatorname{Frob}_K^m$, and let $\theta_\pi(a)_{|K_\pi} := \sigma_{u^{-1}}$, where $\sigma_{u^{-1}}(\alpha) := [u^{-1}]_\phi(\alpha)$ for all $\alpha \in \Lambda_n$ and $n \geq 1$, with ϕ as in Definition 33.3.

It follows from Theorem 33.5 that the field K_π is totally ramified, so $K_\pi \cap K^{\mathrm{unr}} = K$, which allows us to define the action of $\theta_\pi(a)$ on K_π and K^{unr} independently. In our definition of $\theta_\pi(a)_{|K_\pi}$ we use $\sigma_{u^{-1}}$ rather than σ_u in order to ensure that K_π^{ab} is independent of π (as we will be proved below), but this still defines an isomorphism $A^\times \to \operatorname{Gal}(K_\pi)$.

Theorem 33.7. *Let K be a nonarchimedean local field with uniformizer π and let $\mathfrak{p} := \langle \pi \rangle$. Let $\operatorname{Frob}_K \in \operatorname{Gal}(K^{\mathrm{unr}}/K)$ be the Frobenius element, let K_m/K be the unique extension of degree m in K^{unr}, let $K_{\pi,n,m} := K_m K_{\pi,n}$, and let $U_{\pi,n,m} := (1+\mathfrak{p}^n)\langle \pi^m \rangle \subseteq K^\times$. Then*

(ii) *$\theta_\pi(\pi)_{|K^{\mathrm{unr}}} = \operatorname{Frob}_K$ and $\theta_\pi(a)_{|K_{\pi,n,m}} = 1$ for all $a \in U_{\pi,n,m}$ and all $n, m \geq 1$.*

Proof. It follows immediately from the definition of θ_π that $\theta_\pi(\pi)_{|K^{\mathrm{unr}}} = \operatorname{Frob}_K$, so we only need to prove the second part of (ii).

Let $a \in U_{\pi,n,m}$ and write a as $a = u\pi^e$ with $u \in 1 + \mathfrak{p}^n$ and $e \geq 0$ divisible by m. The image of u in $A/(\pi^n) = A/\mathfrak{p}^n$ is 1, so $\sigma_{u^{-1}}(\alpha) = [u^{-1}]_\phi(\alpha) = [1]_\phi(\alpha) = \alpha$ for all $\alpha \in \Lambda_n$ (here we are using the inverse of the isomorphism $(A/(\pi^n))^\times \simeq \operatorname{Aut}(\Lambda_n) \simeq \operatorname{Gal}(K_{\pi,n}/K)$ defined by $u \mapsto [u]_\phi \mapsto \sigma_u$ given by Theorem 33.5). It follows that $\sigma_{u^{-1}|K_{\pi,n}} = 1$, since $K_{\pi,n} = K(\Lambda_n)$, and therefore

$$\theta_\pi(a)_{|K_{\pi,n}} = \sigma_{u^{-1}|K_{\pi,n}} = 1.$$

For any $\alpha \in K_m \subseteq K^{\mathrm{unr}}$ we have $\theta_\pi(a)(\alpha) = \operatorname{Frob}_K^e(\alpha) = \alpha$, since for the unramified extension K_m/K of degree m, the Galois group $\operatorname{Gal}(K_m/K)$ is cyclic of order m, generated by the restriction of Frob_K to K_m. It follows that

$$\theta_\pi(a)_{|K_m} = (\operatorname{Frob}_k^e)_{|K_m} = 1,$$

and therefore $\theta_\pi(a)_{|K_{\pi,n,m}} = 1$, since $K_{\pi,n,m} = K_{\pi,n}K_m$. $\square$

It remains only to show that the field $K_\pi^{\mathrm{ab}} = K_\pi K^{\mathrm{unr}}$ and the homomorphism θ_π do not depend on the choice of π. To do this we essentially want to show that for any uniformizer $\pi' = u\pi$, the field $K_{\pi'}$ is a subfield of K_π^{unr} conjugate to K_π via $\theta_\pi(u)$

If L/K is a finite unramified extension of local fields and $\mathfrak{q}$ is the maximal ideal of the valuation ring of L lying above the maximal ideal $\mathfrak{p}$ of the valuation ring of K, the valuation $v_\mathfrak{q}$ extends the valuation $v_\mathfrak{p}$ with index index $e_\mathfrak{q} = 1$ (see Theorem 8.20); it follows that the maximal unramified extension K^{unr} is a DVR whose discrete valuation restricts to the discrete valuation on K. However, the valuation ring of K^{unr} is not complete, and we want to work with power series over complete DVRs (so we can guarantee convergence on elements of absolute value less than 1), so we instead work with the completion $\widehat{K}^{\mathrm{unr}}$ of K^{unr}, whose valuation ring is a complete DVR (with infinite residue field isomorphic to the algebraic closure of the residue field of K, the same as K^{unr}).

The Frobenius element Frob_K is a topological generator for $\operatorname{Gal}(K^{\mathrm{unr}}/K)$ (it generates a subgroup isomorphic to $\mathbb{Z}$ which is dense in $\operatorname{Gal}(K^{\mathrm{unr}}/K) \simeq \widehat{\mathbb{Z}}$), and the same applies to its lift to $\operatorname{Gal}(\widehat{K}^{\mathrm{unr}}/K)$, which we also denote Frob_K (the action of Frob_K on $\widehat{K}^{\mathrm{unr}}$ is completely determined by its action on K^{unr}, since elements of $\widehat{K}^{\mathrm{unr}}$ are Cauchy sequences and Frob_K acts on the sequence by acting on each term).

Lemma 33.8. *Let K be a nonarchimedean local field with valuation ring A, let B be the valuation ring of $\widehat{K}^{\mathrm{unr}}$, and let $\sigma := \mathrm{Frob}_K \in \mathrm{Gal}(\widehat{K}^{\mathrm{unr}}/K)$ be the Frobenius element. We have exact sequences*

$$0 \longrightarrow A \longrightarrow B \xrightarrow{x\mapsto\sigma(x)-x} B \longrightarrow 0$$

$$1 \longrightarrow A^\times \longrightarrow B^\times \xrightarrow{x\mapsto\sigma(x)/x} B \longrightarrow 1$$

Proof. Let $\mathfrak{p}$ be the maximal ideal of A, and let R be the valuation ring of K^{unr} with maximal ideal $\mathfrak{m}$. For $n \geq 1$ let $A_n := A/\mathfrak{p}^n$ and $R_n := R/\mathfrak{m}^n$. Let τ be the map $x \mapsto \sigma(x) - x$ and let τ_n denote the induced map $R_n \to R_n$. We will show by induction that the sequence $0 \longrightarrow A_n \longrightarrow R_n \xrightarrow{\tau_n} R_n \longrightarrow 0$ is exact; the exactness of the first sequence in the lemma then follows, since $A = \varprojlim A_n$ and $B = \varprojlim R_n$.

The case $n = 1$ follows from the exactness of $0 \longrightarrow k \longrightarrow \bar{k} \xrightarrow{\tau_1} \bar{k} \longrightarrow 0$, where $k = A_1 = A/\mathfrak{p}$ is the finite residue field, and τ_1 is the map $x \mapsto x^{\#k} - x$. Assuming we have proved exactness for $n-1$, consider the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & R_1 \arrow[r] \arrow[d, "\tau_1"] & R_n \arrow[r] \arrow[d, "\tau_n"] & R_{n-1} \arrow[r] \arrow[d, "\tau_{n-1}"] & 0 \\
0 \arrow[r] & R_1 \arrow[r] & R_n \arrow[r] & R_{n-1} \arrow[r] & 0
\end{tikzcd}$$

The map $R_1 \to R_n$ is the isomorphism from R_1 to the kernel of the reduction map from R_n to R_{n-1}. The snake lemma and the inductive hypothesis yield the kernel-cokernel sequence

$$0 \to A_1 \to \ker\tau_n \to A_{n-1} \to 0 \to \operatorname{coker}\tau_n \to 0,$$

thus $\operatorname{coker}\tau_n = 0$, and $\ker\tau_n$ contains A_n and must be equal to it, since $\#A_n = \#A_1\#A_{n-1}$. Replacing A_n with $A_n^\times$ and R_n with $R_n^\times$ and taking τ to be the map $x \mapsto \sigma(x)/x$ yields the second exact sequence in the lemma. $\square$

For any power series F with coefficients in a field L and any $\sigma \in \mathrm{Aut}(K)$ we use $\sigma(F)$ to denote the power series obtained by applying σ to all the coefficients of F.

Proposition 33.9. *Let K be a nonarchimedean local field with valuation ring A and uniformizer π, let B be the valuation ring of the completion $\widehat{K}^{\mathrm{unr}}$, let $\iota\colon A \to B$ be the inclusion map, let $\sigma := \mathrm{Frob}_K \in \mathrm{Gal}(\widehat{K}^{\mathrm{unr}}/K)$ be the Frobenius element, and let $\phi \in \Phi(\pi)$ and $\psi \in \Phi(u\pi)$. There is an isomorphism of formal group laws $\varphi\colon \iota_*F_\phi \to \iota_*F_\psi$ such that $\sigma(\varphi) = \varphi \circ [u]_\phi$ and $\varphi \circ [a]_\phi = [a]_\psi \circ \varphi$ for all $a \in A$. The inverse isomorphism $\varphi^{-1}\colon \iota_*F_\psi \to \iota_*F_\phi$ satisfies $\sigma(\varphi^{-1}) = \varphi \circ [u^{-1}]_\psi$ and $\varphi^{-1} \circ [a]_\psi = [a]_\phi \circ \varphi^{-1}$ for all $a \in A$.*

Proof. Via Lemma 33.8, choose $v \in B^\times$ so that $\sigma(v) = uv$ and let $\varphi_1 := vT$; we then have $\sigma(\varphi_1) = uvT$. We will inductively construct polynomials $\varphi_n \in B[T]$ that satisfy

$$\varphi_n \equiv \varphi_{n-1} \bmod T^n \qquad \text{and} \qquad \sigma(\varphi_n) \equiv \varphi_n \circ [u]_\phi \bmod T^{n+1}.$$

Given $\varphi_{n-1}(T)$, let b be the coefficient of T^n in $\sigma(\varphi_{n-1}) - \varphi_{n-1} \circ [u]_\phi$. Via Lemma 33.8, choose $a \in B$ so that $\sigma(a) - a = b/(uv)^n$ (note that $uv \in B^\times$, so $b/(uv)^n \in B$). Now define $\varphi_n := \varphi_{n-1} - av^nT^n$. Then

$$\sigma(\varphi_n) - \varphi_n \circ [u]_\phi \equiv (b - \sigma(av^n) + av^nu^n)T^n \equiv (b - \sigma(a)u^nv^n + av^nu^n)T^n \equiv 0 \bmod T_{n+1}.$$

If we now put $\varphi := \lim_n \varphi_n$, then $\sigma(\varphi) = \varphi \circ [u]_\phi$ as desired.

We have $\varphi(T) \equiv vT \bmod T^2$ with $v \in B^\times$, so there is a unique $\varphi^{-1} \in TB[[T]$ such that $\varphi \circ \varphi^{-1} = T$, by Lemma 32.3, and we note that $\varphi^{-1}(T) \equiv v^{-1}T \bmod T^2$. Now define

$$\psi' := \sigma(\varphi) \circ \phi \circ \varphi^{-1} = \varphi \circ [u]_\phi \circ \phi \circ \varphi^{-1} = \varphi \circ \phi \circ [u]_\phi \circ \varphi^{-1}.$$

The Frobenius element σ fixes the coefficients of ϕ and $[u]_\phi$ (since they lie in A), and we note that $T = \varphi \circ \varphi^{-1} = \sigma(\varphi) \circ \sigma(\varphi^{-1}) = \varphi \circ [u]_\phi \circ \sigma(\varphi^{-1})$, so $\varphi^{-1} = [u]_\phi \circ \sigma(\varphi^{-1})$, and therefore

$$\sigma(\psi') = \sigma(\varphi) \circ \phi \circ [u]_\phi \circ \sigma(\varphi^{-1}) = \sigma(\varphi) \circ \phi \circ \varphi^{-1} = \psi',$$

which implies that $\psi' \in A[[T]]$, and we have

$$\psi'(T) \equiv \sigma(v)\pi v^{-1}T \equiv u\pi T \equiv \bmod T^2$$

and if $q := A/\langle \pi \rangle$ is the cardinality of the residue field, then $\phi \circ \varphi^{-1} \equiv (\varphi^{-1})^q \bmod \pi$ and

$$\psi'(T) \equiv (\sigma(\varphi) \circ (\varphi^{-1})^q)(T) \equiv \sigma(\varphi) \circ \sigma(\varphi^{-1})(T^q) \equiv T^q \bmod \pi,$$

which implies $\psi'(T) \equiv T^q \bmod u\pi$, so $\psi' \in \Phi(u\pi)$. If $\psi' \neq \psi$ then we can replace φ with $\varphi' := [1]_{\psi,\psi'} \circ \varphi$, which will still satisfy $\sigma(\varphi') = \varphi' \circ [u]_\phi$, since σ acts trivially on $[1]_{\psi,\phi}$, and this changes ψ' to $\psi' \circ [1]_{\psi,\psi'} = \psi$. We thus assume $\psi' = \psi$, and have $\psi = \sigma(\varphi) \circ \phi \circ \varphi^{-1}$.

We now show that $\varphi \circ F_\phi \circ \varphi^{-1} = F_\psi$. We first note that

$$\sigma(\varphi \circ F_\phi \circ \varphi^{-1}) = \sigma(\varphi) \circ F_\phi \circ \sigma(\varphi^{-1}) = \varphi \circ [u]_\phi \circ F_\phi \circ [u^{-1}]_\phi \circ \varphi^{-1} = \varphi \circ F_\phi \circ \varphi^{-1},$$

since $[u]_\phi$ and $[u^{-1}]_\phi$ are inverse automorphisms of F_ϕ, by Proposition 32.16. It follows that $\varphi \circ F_\phi \circ \varphi^{-1} \in A[[X,Y]]$. Let $R := A[[X,Y]]$. It follows from Propositions 32.12 and 32.13 that $F_\psi \in A[[X,Y]]$ is uniquely determined by $F_\psi(X,Y) \equiv X + Y \bmod R_{>1}$ and $\psi \circ F_\psi = F_\psi \circ \psi$. We now observe that

$$(\varphi \circ F_\phi \circ \varphi^{-1}(X,Y) \equiv v(v^{-1}X + v^{-1}Y) \equiv X + Y \bmod R_{>1}$$

and

$$\begin{aligned}\psi \circ (\varphi \circ F_\phi \circ \varphi^{-1}) &= \sigma(\varphi) \circ \phi \circ F_\phi \circ \varphi^{-1}\\ &= \sigma(\varphi) \circ F_\phi \circ \phi \circ \varphi^{-1}\\ &= \sigma(\varphi) \circ F_\phi \circ \sigma(\varphi^{-1}) \circ \psi\\ &= (\varphi \circ F_\phi \circ \varphi^{-1}) \circ \psi,\end{aligned}$$

so $\varphi \circ F_\phi \circ \varphi^{-1} = F_\psi$, by uniqueness, and therefore $\varphi \circ F_\phi = F_\psi \circ \varphi$. Thus φ is an isomorphism of formal group laws $\iota_* F_\phi \to \iota_* F_\psi$ as claimed, and φ^{-1} is the inverse isomorphism.

Finally, for any $a \in A$ we have

$$\sigma(\varphi \circ [a]_\phi \circ \varphi^{-1}) = \sigma(\varphi) \circ [a]_\phi \circ \sigma(\varphi^{-1}) = \varphi \circ [u]_\phi \circ [a]_\phi \circ [u^{-1}] \circ \varphi^{-1} = \varphi \circ [a]_\phi \circ \varphi^{-1},$$

so $\varphi \circ [a]_\phi \circ \varphi^{-1} \in A[[T]]$. Now $[a]_\psi \in A[[T]]$ is uniquely determined by $[a]_\psi \equiv aT \bmod T^2$ and $[a]_\psi \circ F_\psi = F_\psi \circ [a]_\psi$. We have $\varphi \circ [a]_\phi \circ \varphi^{-1}(T) \equiv vav^{-1}T \equiv aT \bmod T^2$ and

$$(\varphi \circ [a]_\phi \circ \varphi^{-1}) \circ F_\psi = \varphi \circ [a]_\phi \circ F_\phi \circ \varphi^{-1} = \varphi \circ F_\phi \circ [a]_\phi \circ \varphi^{-1} = F_\psi \circ (\varphi \circ [a]_\phi \circ \varphi^{-1}),$$

so $\varphi \circ [a]_\phi \circ \varphi^{-1} = [a]_\psi$, by uniqueness. Therefore $\varphi \circ [a]_\phi = [a]_\psi \circ \varphi$ for all $a \in A$.

We now observe that $\sigma(\varphi) = \varphi \circ [u]_\phi = [u]_\psi \circ \varphi$ and therefore

$$\sigma(\varphi^{-1}) = \sigma(\varphi)^{-1} = ([u]_\psi \circ \varphi)^{-1} = \varphi^{-1} \circ [u]_\psi^{-1} = \varphi^{-1} \circ [u^{-1}]_\psi,$$

and $\varphi \circ [a]_\phi = [a]_\psi \circ \varphi \implies [a]_\phi = \varphi^{-1} \circ [a]_\psi \circ \varphi \implies [a]_\phi \circ \varphi^{-1} = \varphi^{-1} \circ [a]_\psi$ for all $a \in A$, which shows that the inverse isomorphism $\varphi^{-1} \colon \iota_* F_\psi \to \iota_* F_\phi$ has the desired properties. $\square$

Theorem 33.10. *Let K be a nonarchimedean local field with valuation ring A and uniformizer π. Then*

(iii) $K_\pi^{\text{ab}} := K_\pi K^{\text{unr}}$ and $\theta_\pi\colon K^\times \to \operatorname{Gal}(K_\pi^{\text{ab}}/K)$ are independent of π.

Proof. Consider any uniformizer $\pi' = u\pi$ with $u \in A^\times$. Let $\phi \in \Phi(\pi)$ by $\pi T + T^q$ and let $\psi \in \Phi(\pi')$ be $\pi' T + T^q$, where $q = \#(A/\langle\pi\rangle)$. Let B be the valuation ring of $\widehat{K}^{\text{unr}}$, and let $\sigma := \operatorname{Frob}_K \in \operatorname{Gal}(\widehat{K}^{\text{unr}}/K)$. Now let $\varphi \in B[[T]]$ be the isomorphism given by Proposition 33.9, so that $\sigma(\varphi) = \varphi \circ [u]_\phi$ and $\varphi \circ [a]_\phi = [a]_\psi \circ \varphi$ for all $a \in A$. Then

$$\sigma(\varphi) \circ [\pi]_\phi = \varphi \circ [u]_\phi \circ [\pi]_\phi = \varphi \circ [u\pi]_\phi = \varphi \circ [\pi']_\phi = [\pi']_\psi \circ \varphi.$$

Recalling that $[\pi]_\phi = \phi$ and $[\pi']_\psi = \psi$, by Proposition 32.16, we have $\sigma(\varphi) \circ \phi = \psi \circ \varphi$. Proposition 33.9 also implies $\sigma(\varphi^{-1}) = \varphi^{-1} \circ [u^{-1}]_\psi$ and $\varphi^{-1} \circ [a]_\psi =]a]_\phi \circ \varphi^{-1}$ for all $a \in A$, so we similarly obtain

$$\sigma(\varphi^{-1}) \circ [\pi']_\psi = \varphi^{-1} \circ [u^{-1}]_\psi \circ [\pi']_\psi = \varphi^{-1} \circ [u^{-1}\pi']_\psi = \varphi^{-1} \circ [\pi]_\psi = [\pi]_\phi \circ \varphi^{-1}$$

and therefore $\sigma(\varphi^{-1}) \circ \psi = \phi \circ \varphi^{-1}$.

Now consider any $\alpha \in \Lambda_{\phi,1}$. If $\phi(\alpha) = 0$ then $\psi(\varphi(\alpha)) = \sigma(\varphi)(\phi(\alpha)) = \sigma(\varphi)(0) = 0$. Conversely, if $\psi(\alpha) = 0$ then $\phi(\varphi^{-1}(\alpha)) = \sigma(\varphi^{-1})(\psi(\varphi)) = \sigma(\varphi^{-1})(0) = 0$. It follows that φ induces a bijection from $\Lambda_{\phi,1}$ to $\Lambda_{\psi,1}$, and we therefore have

$$\widehat{K}^{\text{unr}}(\Lambda_{\psi,1}) = \widehat{K}^{\text{unr}}(\varphi(\Lambda_{\phi,1})) \subseteq \widehat{K}^{\text{unr}}(\Lambda_{\phi,1}) = \widehat{K}^{\text{unr}}(\varphi^{-1}(\Lambda_{\psi,1})) \subseteq \widehat{K}^{\text{unr}}(\Lambda_{\psi,1}).$$

Here we are using the fact that a finite separable extension of a complete DVR is complete, by Theorem 10.6 (the elements of $\Lambda_\phi, 1$ and $\Lambda_{\psi,1}$ are separable, by Theorem 33.5), which is needed to guarantee the two inclusions above (evaluating a convergent power series over a complete field yields an element of the field; consider the Cauchy sequence of partial sums). We thus have $\widehat{K}^{\text{unr}}(\Lambda_{\phi,1}) = \widehat{K}^{\text{unr}}(\Lambda_{\psi,1})$. Taking intersections with K^{sep} on both sides of this equality yields $K^{\text{unr}}(\Lambda_{\phi,1}) = K^{\text{unr}}(\Lambda_{\psi,1})$ and therefore $K^{\text{unr}} K_{\pi,1} = K^{\text{unr}} K_{\pi',1}$.

We now prove by induction on $n \geq 1$ that $\sigma^n(\varphi) \circ \phi^{(n)} = \psi^{(n)} \circ \varphi$. The base case was proved above. For $n > 1$ we have

$$\sigma^n(\varphi) \circ \phi^{(n)} = \sigma^{n-1}(\sigma(\varphi) \circ \phi \circ \phi^{(n-1)}) = \sigma^{(n-1)}(\psi \circ \varphi \circ \phi^{(n-1)}) = \psi \circ \sigma^{(n-1)}(\varphi) \circ \phi^{(n-1)}$$

and $\psi \circ \sigma^{(n-1)}(\varphi) \circ \phi^{(n-1)} = \psi \circ \psi^{(n-1)} \circ \varphi = \psi^{(n)} \circ \varphi$ by the inductive hypothesis. We similarly have $\sigma^{(n)}(\varphi^{-1}) \circ \psi^{(n)} = \phi^{(n)} \circ \varphi^{-1}$.

For any $\alpha \in \Lambda_\phi$, if $\phi^{(n)}(\alpha) = 0$ then $\psi^{(n)}(\varphi(\alpha)) = \sigma^n(\varphi)(\phi^{(n)}(\alpha)) = \sigma^n(\varphi)(0) = 0$, and conversely, if $\psi^{(n)}(\alpha) = 0$ then $\phi^{(n)}(\varphi^{-1}(\alpha)) = \sigma(\varphi^{-1})^n(\psi^{(n)}(\alpha)) = \sigma^n(\varphi^{-1})(0) = 0$. Thus φ induces a bijection $\Lambda_{phi,n} \to \Lambda_{\psi,n}$ for all $n \geq 1$ and therefore $\widehat{K}^{\text{unr}}(\Lambda_{\phi,n}) = \widehat{K}^{\text{unr}}(\Lambda_{\psi,n})$ and $K^{\text{unr}} K_{\pi,n} = K^{\text{unr}} K_{\pi',n}$ for all $n \geq 1$. We therefore have

$$K_\pi^{\text{ab}} = K_\pi K^{\text{unr}} = \bigcup_{n\geq 1} K_{\pi,n} K^{\text{unr}} = \bigcup_{n \geq 1} K_{\pi',n} K^{\text{unr}} = K_{\pi'}^{\text{ab}},$$

which implies that the field K_π^{ab} is independent of π.

Let us now consider the homomorphisms $\theta_\pi\colon K^\times \to \operatorname{Gal}(K_\pi^{\text{ab}}/K)$ (see Definition 33.6). We have $\theta_\pi(\pi') = \theta_\pi(u\pi) = \theta_\pi(u)\theta_\pi(\pi)$. By definition, $\theta_\pi(u)$ acts trivially on K^{unr} and acts as $\sigma_{u^{-1}}$ on K_π, meaning that it sends $\alpha \in \Lambda_{\phi,n}$ to $[u^{-1}]_\phi(\alpha)$, while $\theta_\pi(\pi)$ acts trivially on

K_π and as Frob_K on K^{unr} (which implies that $\theta_\pi(\pi)(\varphi(\alpha)) = \sigma(\varphi)(\alpha)$ for any $\alpha \in K_\pi$). For any $\alpha \in \Lambda_{\phi,n}$ we have

$$\begin{aligned}\theta_\pi(\pi')(\varphi(\alpha)) &= \theta_\pi(u)(\theta_\pi(\pi)(\varphi(\alpha))) = \theta_\pi(u)(\sigma(\varphi)(\alpha)) = \sigma(\varphi)(\theta_\pi(u)(\alpha)) = \sigma(\varphi)(\sigma_{u^{-1}}(\alpha))\\ &= \sigma(\varphi)([u^{-1}]_\phi(\alpha)) = (\varphi\circ[u]_\phi\circ[u^{-1}]_\phi)\varphi(\alpha) = \varphi(\alpha).\end{aligned}$$

It follows that $\theta_\pi(\pi')$ acts trivially on $\Lambda_{\psi,n}$, hence on $K_{\pi',n}$ for all $n \ge 1$; therefore $\theta_\pi(\pi')$ acts trivially on $K_{\pi'} = \bigcup_{n\ge1} K_{\pi',n}$. Thus $\theta_\pi(\pi')_{|_{K'_\pi}} = 1$ and $\theta_\pi(\pi')_{|K^{\mathrm{unr}}} = \mathrm{Frob}_K$, and therefore $\theta_\pi(\pi') = \theta_{\pi'}(\pi')$, since this is precisely the definition of $\theta_{\pi'}(\pi')$. Our choice of $\pi' = u\pi$ was arbitrary, so $\theta_\pi(\pi'') = \theta_{\pi''}(\pi'')$ for every uniformizer π'' of K. The uniformizer π was also arbitrary, so the same argument applies to π', that is, $\theta_{\pi'}(\pi'') = \theta_{\pi''}(\pi'')$ for every uniformizer π'' of K. Thus $\theta_\pi(\pi'') = \theta_{\pi''}(\pi'') = \theta_{\pi'}(\pi'')$ for every uniformizer π'' of K. The uniformizers generate $K^\times$, so $\theta_\pi = \theta_{\pi'}$ and this shows that θ_π is independent of π. $\square$

References

[1] J.S. Milne, *Class field theory*, version 4.02, 2013.