Local Fields and Their Galois Theory

Zachary Gardner

June 25, 2021

Introduction

In a nutshell, we are interested in studying the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This is an infinite profinite topological group that "knows" about all finite Galois extensions of $\mathbb{Q}$. Our primary tools for studying $G_{\mathbb{Q}}$ are Galois representations, continuous homomorphisms $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(F)$ for F some topological field. Natural choices for F include $\mathbb{C}$ (with its Euclidean topology) or a finite field $\mathbb{F}_q$ (equipped with the discrete topology). But there is often also reason to consider $\mathbb{Q}_\ell$ for ℓ prime, giving rise to so-called *ℓ-adic Galois representations*. At the same time, we don't just want to consider representations of $G_{\mathbb{Q}}$ but also of $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. The topological field $\mathbb{Q}_p$ is the simplest example of a so-called *local field*, and it is exactly these kinds of fields that we are interested in studying in these notes.

Absolute Values and Discrete Valuations

Definition

Let K be a field. An **absolute value** on K is a map $|\cdot| : K \to \mathbb{R}^{\geq 0}$ such that, for every $x, y \in K$,

- $|x| = 0 \iff x = 0$;
- $|xy| = |x||y|$;
- $|x + y| \leq |x| + |y|$.

We say that $|\cdot|$ is **nonarchimedean** or **ultrametric** if $|x + y| \leq \max\{|x|, |y|\}$ for every $x, y \in K$, and **archimedean** otherwise. A **discrete valuation** on K is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that, for every $x, y \in K$,

- $v(x) = \infty \iff x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x + y) \geq \min\{v(x), v(y)\}$.

Absolute Values and Discrete Valuations

The data of the pair $(K, |\cdot|)$ is called a **valued field** (we often suppress $|\cdot|$ when it is clear from context). K is then naturally a topological field with respect to the metric topology induced by $|\cdot|$. There is a natural equivalence relation $\sim$ on the set of absolute values on K given by $|\cdot|_1 \sim |\cdot|_2$ if $|\cdot|_2 = |\cdot|_1^r$ for some $r \in \mathbb{R}^{>0}$, which precisely captures when two absolute values on K induce the same (metric) topology. The equivalence classes of $\sim$ are called **places** or sometimes **primes**, and together they form the set S_K.

Given a discrete valuation v on K and $0 < c < 1$, we obtain a nonarchimedean absolute value $|\cdot|_{v,c}$ on K via $|x|_{v,c} := c^{v(x)}$. Note, however, that a (rank 1) nonarchimedean absolute value $|\cdot|$ on K does not necessarily induce a discrete valuation on K. More on this later.

Valuation Rings

Let $(K, |\cdot|)$ be a nonarchimedean valued field. The **ring of integers** or **valuation ring** of K is

$$\mathcal{O}_K := \{x \in K : |x| \leq 1\},$$

which the reader can verify is an open local subring of K. Moreover, $\mathcal{O}_K$ has fraction field K, unique maximal ideal $\mathfrak{m}_K := \{x \in K : |x| < 1\}$, and unit group $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$. We also have a **residue field** $k_K := \mathcal{O}_K/\mathfrak{m}_K$.

In the case that $\mathfrak{m}_K$ is principal, any generator of $\mathfrak{m}_K$ is called a **uniformizer** for K and is typically denoted π_K or ϖ_K (with the subscript K often omitted). Associated to this is the discrete valuation $v_K : K \to \mathbb{Z} \cup \{\infty\}$ recording order of divisibility by π_K (which is independent of the choice of uniformizer). This fits into a short exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

with a choice of uniformizer π_K inducing a splitting – i.e., a (non-canonical) isomorphism $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}$.

Local Fields

Definition

A **local field** is a valued field K such that the induced metric topology makes K into a (non-discrete) locally compact topological field.

We immediately see that $\mathbb{R}$ and $\mathbb{C}$ are examples of (archimedean) local fields.

Proposition

Let K be a nonarchimedean valued field. Then, K is local if and only if K is (Cauchy) complete and k_K is finite.

In this case, $\mathcal{O}_K$ is a compact local PID and K has a unique discrete valuation v_K such that $v_K(\pi_K) = 1$ for any choice of uniformizer π_K. We readily see that $\mathbb{Q}_p$ and $\mathbb{F}_q((t))$ (the field of Laurent series in t over $\mathbb{F}_q$) are examples of nonarchimedean local fields.

Classification of Local Fields

Theorem

Let K be a local field. Then, K is described up to isomorphism as a topological ring by one of the following (where $p > 0$ is prime).

Case	char(K)	char(k_K)	Isomorphism Type
Equichar. 0	0	0	$\mathbb{R}, \mathbb{C}$
Mixed char.	0	p	Finite extension of $\mathbb{Q}_p$
Equichar. p	p	p	Finite extension of $\mathbb{F}_p((t))$

Notice how $\mathbb{R}$ arises from $\mathbb{Q}$ by completing with respect to the usual Euclidean absolute value $|\cdot| = |\cdot|_\infty$. Similarly, $\mathbb{Q}_p$ arises from $\mathbb{Q}$ via $|\cdot|_p$ and $\mathbb{F}_q((t))$ arises from $\mathbb{F}_q(t)$ via $|\cdot|_t$ or $|\cdot|_{t^{-1}}$. This is no coincidence.

Completion

Let K be a field and $v \in S_K$. Given $|\cdot|$ representing v, define the **completion** K_v of K at v to be the (Cauchy) completion of K with respect to the metric topology induced by $|\cdot|$. This is a well-defined object since choosing a different representative for v changes K_v by a unique isomorphism (in fact, K_v has a universal property that gives us this result for free). Note also that we can describe K_v in a more algebraic way using the process of adic completion.

Corollary

Let K be a global field (i.e., a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_p(t)$). Then, the completions of K correspond precisely with the local fields – i.e., every completion of a global field is a local field and every local field arises as a completion of a global field.

This explains one way in which local fields are "local." We could say a lot more about the connections between local and global fields, but let's leave it at that for right now.

Extending Absolute Values

Proposition

Let $(K, |\cdot|)$ be a complete nonarchimedean valued field and L a finite extension field of K. Then, $|\cdot|$ admits a unique extension to L via the formula

$$|\alpha| := |N_{L/K}(\alpha)|^{1/[L:K]},$$

where $N_{L/K}(\alpha)$ is the norm of $\alpha \in L$ with respect to K.

Note that, given $\alpha \in L$ as above, we have a tower of field extensions $K \subseteq K(\alpha) \subseteq L$ and so $N_{L/K} = N_{K(\alpha)/K} \circ N_{L/K(\alpha)}$ and $[L:K] = [L:K(\alpha)][K(\alpha):K]$. Hence, the extension of $|\cdot|$ to L can be defined relative to each element of L. We obtain the following result.

Extending Absolute Values

Corollary

$(K, |\cdot|)$ be a complete nonarchimedean valued field and L an algebraic extension field of K. Then, $|\cdot|$ admits a unique extension to L via the formula

$$|\alpha| := |N_{K(\alpha)/K}(\alpha)|^{1/[K(\alpha):K]}.$$

In particular, we can extend $|\cdot|$ all the way to $\overline{K}$.

The extended absolute value $|\cdot| : \overline{K} \to \mathbb{R}^{\geq 0}$ is nonarchimedean and so we can define a valuation

$$v_c : \overline{K} \to \mathbb{R} \cup \{\infty\}, \qquad \alpha \mapsto \frac{\log |\alpha|}{\log c},$$

where $0 < c < 1$. This is, however, not a *discrete* valuation – i.e., $v(\overline{K}^{\times})$ is not a discrete subgroup of $\mathbb{R}$. An easy way to see this is to note that $p \in K$ and then consider all the rational powers of p (which must be contained in $\overline{K}$).

Ramification

Definition

Let L/K be a finite extension of nonarchimedean local fields with uniformizers π_K and π_L. To this we associate the **ramification index** $e(L/K) := v_L(\pi_K)$ and **inertia degree** $f(L/K) := [k_L : k_K]$. We say that L/K is **unramified** if $e(L/K) = 1$ and **totally ramified** if $e(L/K)$ is as large as possible – i.e., $e(L/K) = [L : K]$ since $e(L/K)f(L/K) = [L : K]$.

The extension L/K is unramified if and only if $\mathfrak{m}_K$ is inert in $\mathcal{O}_L$ – i.e., $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L$. Equivalently, any uniformizer for K is a uniformizer for L.

Example

1. Let $L := \mathbb{Q}_p[x]/(x^e - p) \cong \mathbb{Q}_p(p^{1/e})$. Then, $L/\mathbb{Q}_p$ is totally ramified of degree e.
2. Let $L := \mathbb{Q}_p(\zeta_{p^n})$. Then, $L/\mathbb{Q}_p$ is totally ramified of degree $\phi(p^n) = p^{n-1}(p-1)$. A uniformizer π_L is given by $1 - \zeta_{p^n}$.
3. Let $L := \mathbb{Q}_p(\zeta_{p^n-1})$. Then, $L/\mathbb{Q}_p$ is unramified of degree n.

Unramified Extensions

Theorem

Let K be a nonarchimedean local field. The correspondence $L \mapsto k_L$ induces an equivalence of categories between the category of finite unramified extensions of K and the category of finite extensions of k_K. This correspondence preserves, among other things, composita, Galois groups, and splitting fields of polynomials admitting lifts to $\mathbb{Z}[x]$.

This has several important consequences which we record here.

- K has a unique (up to isomorphism) unramified extension K_n of degree n. This corresponds to the degree n extension of k_K, which is obtained as the splitting field of $x^{p^n} - x$ over k_K. Hence, $K_n = K(\zeta_{p^n-1})$ for $\zeta_{p^n-1} \in K^{\text{sep}}$.
- The compositum of unramified extensions of K is unramified. Hence, K has a maximal unramified extension K^{unr} given by

$$K^{\text{unr}} = \bigcup_{n \geq 1} K_n = \bigcup_{\gcd(a,p)=1} K(\zeta_a).$$

More Ramification

Proposition

Let L/K be a finite extension of nonarchimedean local fields.

1. *Suppose L/K is totally ramified of degree n. Then, the minimal polynomial over K of any uniformizer π_L is Eisenstein at $\mathfrak{m}_K$.*
2. *Conversely, suppose that $\alpha \in \overline{K}$ is a root of an Eisenstein polynomial over K of degree n. Then, $K(\alpha)/K$ is totally ramified of degree n and α is a uniformizer for $K(\alpha)$.*

Definition

Let L/K be a finite extension of nonarchimedean local fields. L/K is

- **tamely ramified** if $e(L/K)$ is coprime to p;
- **wildly ramified** if p divides $e(L/K)$;
- **totally tamely ramified** if it is both totally ramified and tamely ramified; and
- **totally wildly ramified** if it is both totally ramified and wildly ramified

More Ramification

Proposition

Let L/K be totally tamely ramified of degree n. Then, there exists a uniformizer $\pi_K \in K$ and an nth root $\pi_K^{1/n} \in L$ such that $L = K(\pi_K^{1/n})$.

This allows us to realize the maximal totally tamely ramified extension K^{tam} of K as $\bigcup_{\gcd(p,n)=1} K(\pi_K^{1/n})$. This should be understood as containing all relevant nth roots of all uniformizers for K. In particular, K^{tam} contains all nth roots of unity with $\gcd(p, n) = 1$ and so contains K^{unr}. Explicitly, the extension $K^{\mathrm{tam}}/K^{\mathrm{unr}}$ is generated by $\pi_K^{1/n}$ for $\gcd(p, n) = 1$.

Our ultimate goal is to understand the absolute Galois group $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, where K^{sep} is a chosen separable closure of K. We do this by studying finite Galois extensions L/K. For convenience let $q := |k_K|$ and $G := \mathrm{Gal}(L/K)$.

Ramification Groups

Definition

The **(lower) ramification series** of L/K is

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots$$

with $G_i := \{\sigma \in G : v_L(\sigma(x) - x) \geq i + 1 \text{ for every } x \in \mathcal{O}_L\}$. Of these ramification groups, $I_{L/K} := G_0$ is called the **inertia subgroup** and $P_{L/K} := G_1$ is called the **wild inertia subgroup** (we will see where these names come from in a moment).

The discrete valuation v_L is G-invariant and so the action of G preserves $\mathfrak{m}_L$. It follows that G_i consists of $\sigma \in G$ acting trivially on $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$. We conclude that $G_i \trianglelefteq G$ and $G_i = 1$ for $i \gg 0$. We also have a natural short exact sequence

$$1 \longrightarrow G_0 \longrightarrow G \longrightarrow \mathrm{Gal}(k_L/k_K) \longrightarrow 1$$

giving $G/G_0 \cong \mathrm{Gal}(k_L/k_K)$.

Ramification Groups

At the same time, we have

$$G_0 \to k_L^\times, \qquad \sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$$

inducing an injection $G_0/G_1 \hookrightarrow k_L^\times$ (hence $G_1 \trianglelefteq G_0$) and

$$G_i \to k_L, \qquad \sigma \mapsto \frac{\sigma(\pi_L) - \pi_L}{\pi_L^{i+1}}$$

inducing an injection $G_i/G_{i+1} \hookrightarrow k_L$ (hence $G_{i+1} \trianglelefteq G_i$, where $i \geq 1$).

Let L_{unr} and L_{tam} respectively denote the maximal unramified and tamely ramified subextensions of L/K. L_{unr}/K is Galois with $\mathrm{Gal}(L_{\mathrm{unr}}/K) \cong \mathrm{Gal}(k_L/k_K)$. Since $G/G_0 \cong \mathrm{Gal}(k_L/k_K)$ it follows that $L_{\mathrm{unr}} = L^{G_0}$. A similar argument shows that $L_{\mathrm{tam}} = G_1$ with $\mathrm{Gal}(L_{\mathrm{tam}}/K) \cong G/G_1$ (which has order $f(L/K)$).

Ramification Groups

Corollary

1. $|I_{L/K}| = e(L/K)$. *In particular, L/K is unramified if and only if $I_{L/K} = 1$.*
2. *Write $e(L/K) = q^r m$ with $\gcd(q, r) = 1$. Then, $|P_{L/K}|$ divides $|k_L|$ with order q^r. In particular, L/K is tamely ramified if and only if $P_{L/K} = 1$.*

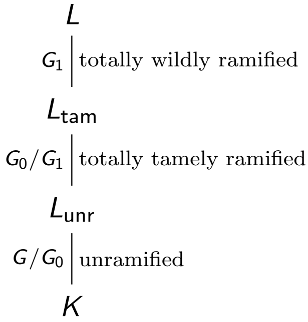


Figure: Factoring the extension L/K

The Unramified Case

Suppose now that L/K is unramified. Then, there is a natural isomorphism $G \cong \mathrm{Gal}(k_L/k_K)$ and so G is cyclic generated by the **Frobenius element** $\mathrm{Fr}_{L/K}$ corresponding to the canonical generator of $\mathrm{Gal}(k_L/k_K)$ and characterized by $\mathrm{Fr}_{L/K}(x) \equiv x^q \pmod{\pi_K}$ for every $x \in \mathcal{O}_L$ (where we have identified π_K as a uniformizer of L).

Continuing in this manner lets us describe the Galois group $G_K^{\mathrm{unr}} := \mathrm{Gal}(K^{\mathrm{unr}}/K)$. Namely, $G_K^{\mathrm{unr}} \cong G_{k_K} \cong \widehat{\mathbb{Z}}$ is topologically cyclic with 1 corresponding to Fr_K characterized by $\mathrm{Fr}_K(x) \equiv x^q \pmod{\pi_K}$ for every $x \in \mathcal{O}_{K^{\mathrm{unr}}}$ or, equivalently, $\mathrm{Fr}_K|_L = \mathrm{Fr}_{L/K}$ for every finite unramified extension L/K. As above, we call Fr_K the **Frobenius element** of K. Note that K^{unr} is **almost** a local field in the sense that $\mathcal{O}_{K^{\mathrm{unr}}}$ is a DVR with perfect residue field $\overline{k_K}$.

The Tame Case

What about $G_K^{\text{tam}} := \text{Gal}(K^{\text{tam}}/K)$? We have a natural short exact sequence

$$1 \longrightarrow \text{Gal}(K^{\text{tam}}/K^{\text{unr}}) \longrightarrow \text{Gal}(K^{\text{tam}}/K) \longrightarrow \text{Gal}(K^{\text{unr}}/K) \longrightarrow 1$$

Recalling that $K^{\text{tam}} = \bigcup_{\gcd(p,n)=1} K^{\text{unr}}(\pi_K^{1/n})$, we have

$$\text{Gal}(K^{\text{tam}}/K^{\text{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$$

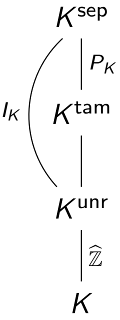
with topological generator τ_K arising from the generators of $\mathbb{Z}/n\mathbb{Z}$ for $\gcd(n,p) = 1$. Let $\widehat{\text{Fr}}_K \in \text{Gal}(K^{\text{tam}}/K)$ be a lift of $\text{Fr}_K \in \text{Gal}(K^{\text{unr}}/K)$.

Theorem (Iwasawa)

$\text{Gal}(K^{\text{tam}}/K)$ *is topologically generated by* $\widehat{\text{Fr}}_K$ *and* τ_K *with sole relation*

$$\widehat{\text{Fr}}_K \tau_K \widehat{\text{Fr}}_K = \tau_K^q.$$

Analogous to before we have a factorization



We call I_K the **absolute inertia group** of K and P_K the **absolute wild inertia group** of K. These are given respectively by inverse limits over $I_{L/K}$ and $P_{L/K}$ for L/K finite Galois. Equivalently, since inverse limits preserve kernels, we have

$$I_K = \ker(G_K \twoheadrightarrow G_{k_K})$$

and

$$P_K = \ker(I_K \to \overline{k_K}^{\times}).$$

Some Success

When K has positive characteristic G_K can be described relatively succinctly as a certain semidirect product of P_K and G_K^{tam}. The key ingredient comes from looking at the maximal pro-p extension $K(p)$ of K with Galois group $G_K(p) := \text{Gal}(K(p)/K)$. In a nutshell, one looks at the Artin-Schreier exact sequence

$$0 \longrightarrow \mathbb{F}_p \longrightarrow K(p) \xrightarrow{x \mapsto x^p - x} K(p) \longrightarrow 0$$

of $G_K(p)$-modules and studies the associated long exact sequence.

When K has characteristic 0 things are much more difficult, though a result of Jannsen and Wingberg does give an explicit set of generators and relations in the p-adic case for $p \neq 2$.

Local-to-Global

Fix a number field K. Let L be a finite Galois extension field of K and $\mathfrak{q}$ a prime of L lying above a prime $\mathfrak{p}$ of K (i.e., $\mathfrak{p} = \mathfrak{q} \cap K$). Denote the associated residue fields by $k_{\mathfrak{q}} := \mathcal{O}_L/\mathfrak{q}$ and $k_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$. Let $D_{\mathfrak{q}}$ and $I_{\mathfrak{q}}$ denote the associated decomposition and inertia group. We have a natural short exact sequence

$$1 \longrightarrow I_{\mathfrak{q}} \longrightarrow D_{\mathfrak{q}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \longrightarrow 1$$

which is in fact isomorphic to the short exact sequence

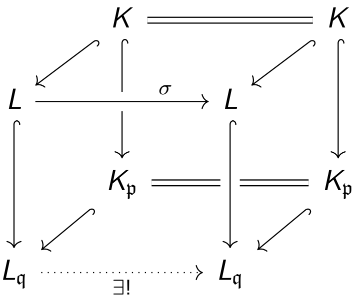
$$1 \longrightarrow I_{L_{\mathfrak{q}}/K_{\mathfrak{p}}} \longrightarrow \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(k_{L_{\mathfrak{q}}}/k_{K_{\mathfrak{p}}}) \longrightarrow 1$$

in the sense that we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_{\mathfrak{q}} & \longrightarrow & D_{\mathfrak{q}} & \longrightarrow & \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) & \longrightarrow & 1 \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\ 1 & \longrightarrow & I_{L_{\mathfrak{q}}/K_{\mathfrak{p}}} & \longrightarrow & \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) & \longrightarrow & \mathrm{Gal}(k_{L_{\mathfrak{q}}}/k_{K_{\mathfrak{p}}}) & \longrightarrow & 1 \end{array}$$

Local-to-Global

This follows from the fact that $\sigma \in D_{\mathfrak{q}}$ induces a commutative diagram



This provides us with one way to define absolute inertia and decomposition subgroups $I_{\mathfrak{p}}$ and $D_{\mathfrak{p}}$ of G_K.