1 Introduction

In number theory we are interested in studying $\mathbb{Q}$ and its finite extensions (known as **number fields**). This is primarily done using Galois theory and, in particular, the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This is an infinite topological group which is built up from finite Galois extensions $K/\mathbb{Q}$ in a way that can be made precise (more specifically, $G_{\mathbb{Q}}$ is a key example of a profinite group). Since $G_{\mathbb{Q}}$ itself is rather unwieldy, we get at its structure by way of (continuous) representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ for V some finite dimensional (topological) vector space.[1] Several possibilities exist for the space V or, rather, its underlying topological ground field F. Of course, we may take F to be $\mathbb{C}$ (with its Euclidean topology) or a finite field $\mathbb{F}_q$ (equipped with the discrete topology). But there is often also reason to consider $\mathbb{Q}_\ell$ (and its finite extensions) 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 $G_{\mathbb{Q}_p}$. This is in part because the Galois theory of $\mathbb{Q}_p$ is nice and in part because $\mathbb{Q}_p$ captures important "local" information about $\mathbb{Q}$ relative to the prime p. The (topological) field $\mathbb{Q}_p$ provides 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.

2 Basic Theory of Local Fields

We begin by recalling some general notions.

Definition 1. *Let K be a field. An **absolute value** on K is a map $|\cdot| : K \to \mathbb{R}^{\geq 0}$ such that, for every $x, y \in K$,*

(i) $|x| = 0 \iff x = 0$;

(ii) $|xy| = |x||y|$;

(iii) $|x + y| \leq |x| + |y|$.

*We say that $|\cdot|$ is **nonarchimedean** or **ultrametric** if $|x + y| \leq \max\{|x|, |y|\}$ for every $x, y \in K$, and **archimedean** otherwise.[2] A **discrete valuation**[3] on K is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that, for every $x, y \in K$,*

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.[4]

*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 $|\cdot|_2 = |\cdot|_1^c$ for some $c \in \mathbb{R}^{>0}$, which precisely captures when two absolute values on K induce the*

[1] We impose continuity constraints on ρ so that it properly captures the topology on $G_{\mathbb{Q}}$.

[2] For technical reasons we don't consider the trivial absolute value (given by $|x| = 1$ for every nonzero $x \in K$) to be nonarchimedean.

[3] The word 'discrete' here comes from the appearance of $\mathbb{Z}$ in the codomain of v.

[4] The symbol ∞ behaves as one would expect, satisfying $\infty + \infty = \infty$, $a + \infty = \infty = \infty + a$, and $a \leq \infty$ for every $a \in \mathbb{Z}$.

same (metric) topology. Let S_K denote the set of equivalence classes of $\sim$ (known as ***places*** *and sometimes* ***primes****). Note that the notions of archimedean and nonarchimedean extend to places.*

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 a local PID that sits inside of $\mathcal{O}_K$ as a compact open subgroup. Moreover, $\mathcal{O}_K$ has fraction field K, unique maximal ideal $\mathfrak{m}_K := \{x \in K : |x| < 1\}$, and unit group $\mathcal{O}_K^\times = \{x \in K : |x| = 1\}$.[5] 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).[6] 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).[7] 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 $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}$. For the future, we want to keep track of the **residue field** $k_K := \mathcal{O}_K/\mathfrak{m}_K$.

Definition 2. *A* ***local field*** *is a valued field K such that the induced metric topology makes K into a (non-discrete) locally compact topological field.*[8]

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

Proposition 3. *Let K be a nonarchimedean valued field. Then, K is local if and only if K is (Cauchy) complete and k_K is finite.*

It follows that K a nonarchimedean valued field has a unique discrete valuation v_K such that $v_K(\pi_K) = 1$ for any choice of uniformizer π_K.[9] 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.

Theorem 4. *Let K be a valued 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 $|\cdot|_t$. This is no coincidence.

[5]Technically these things depend on $|\cdot|$ and not just K but it is customary to omit $|\cdot|$ from the notation. Hopefully some reassurance comes from the fact that only the associated place of $|\cdot|$ matters.

[6]Geometrically, we think of the 1-dimensional object $\mathcal{O}_K$ as a curve and π_K as a choice of (affine) local coordinate.

[7]The discrete valuation v_K can be more intrinsically defined in terms of $\mathfrak{m}_K$ itself. One first defines v_K on $\mathcal{O}_K$ and then extends to K via $x/y \mapsto v_K(x) - v_K(y)$.

[8]In particular, K is a Hausdorff space such that every point has a compact neighborhood).

[9]In line with an earlier comment, v_K depends on the chosen place associated to K.

Definition 5. *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.*[10]

Corollary 6. *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.

Proposition 7. *Let $(K, |\cdot|)$ be a compete 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.[11]

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.

Corollary 8. *$(K, |\cdot|)$ be a compete 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 $\overline{K}$.[12]

Remark 9. *The extended absolute value $|\cdot| : \overline{K} \to \mathbb{R}^{\geq 0}$ is nonarchimedean and so we can define a (rank 1) 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 $\mathbb{R}$.*[13]

Theorem 10 (Ax-Sen-Tate)**.** *Let K be a complete nonarchimedean valued field. Choose compatible separable and algebraic closures K^{sep} and $\overline{K}$, and let be $\mathbb{C}_K$ the completion of $\overline{K}$. Then, $\mathbb{C}_K$ is*

[10] 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.

[11] Recall that that $N_{L/K}(\alpha)$ is by definition the determinant of the K-linear (left) multiplication map $\mu_\alpha : L \to L$. This can also be expressed in terms of the Galois conjugates of α in the case that L/K is separable.

[12] For the future, we will tacitly assume that $\overline{K}$ is equipped with this extended absolute value.

[13] 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 $\overline{K}$).

algebraically closed, K^{sep} is dense in $\mathbb{C}_K$, and G_K acts continuous on $\mathbb{C}_K$ identifying G_K with $\mathrm{Aut}_{\text{cont}}(\mathbb{C}_K/K)$.[14]

Definition 11. *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 $e(L/K)f(L/K) = [L : K]$.*[15]

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 12.

(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.*

The following result illustrates one way in which unramified extensions are nice.

Theorem 13. *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.*[16] *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.[17] Hence, K has a maximal unramified extension K^{unr} given by

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

  corresponding to the algebraic closure $\overline{k_K}$.

We can also give a nice characterization of totally ramified extensions of K.

Proposition 14. *Let L/K be a finite extension of nonarchimedean local fields.*

[14]Part of this follows from a result called Krasner's lemma. The notation $\mathrm{Aut}_{\text{cont}}(\mathbb{C}_K/K)$ denotes continuous automorphisms of $\mathbb{C}_K$ that fix K.

[15]Note that the extension k_L/k_K of finite residue fields is always separable and so this notion of being unramified agrees with more general notions.

[16]One of the key results used in establishing this correspondence is Hensel's lemma.

[17]In fact, unramified extensions of K form a so-called distinguished class.

(a) *Suppose L/K is totally ramified of degree n. Then, the minimal polynomial over K of any uniformizer π_L is Eisenstein at $\mathfrak{m}_K$.*[18]

(b) *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 15. *Let L/K be a finite extension of nonarchimedean local fields. Then, L/K is **tamely ramified** if $e(L/K)$ is coprime to p and **wildly ramified** otherwise. We say that L/K is **totally tamely ramified** if it is both totally ramified and tamely ramified. Similarly, L/K is **totally wildly ramified** if it is both totally ramified and wildly ramified.*

Note that K admits a maximal totally tamely ramified extension which we will denote K^{tam}. The following gives one reason why totally tamely ramified extensions are nice.

Proposition 16. *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 $L = K(\pi_K^{1/n})$.*

It follows that $K^{\text{tam}} = \bigcup_{n\geq 1} K(\pi_K^{1/n})$, which should be understood as containing all nth roots of all uniformizers for K. In particular, K^{tam} contains all nth roots of unity and so contains K^{unr}. Explicitly, the extension $K^{\text{tam}}/K^{\text{unr}}$ is generated by $\pi_K^{1/n}$ for $\gcd(p,n) = 1$.

3 Galois Theory of Local Fields

Let K be a nonarchimedean local field. Our ultimate goal is to understand the absolute Galois group $G_K := \mathrm{Gal}(K^{\text{sep}}/K)$.[19] Let $q := |k_K|$. As above we have maximal unramified and totally tamely ramified extensions K^{unr} and K^{tam}. Let L/K be a finite Galois extension of nonarchimedean local fields with $G := \mathrm{Gal}(L/K)$. We can understand a lot about L/K by breaking G into more manageable pieces.

Definition 17. *The **(lower)**[20] **ramification series** of L/K is*

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

with $G_i := \{\sigma \in G : v_L(\sigma(x) - x) \geq i+1 \text{ for every } x \in \mathcal{O}_L\}$.[21] *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 valuation v_L is G-invariant and so the action of G preserves $\mathfrak{m}_L$.[22] 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 $i \gg 0$. There is a natural short exact sequence

[18] One way to see this is through the theory of Newton polygons.

[19] Putting K^{sep} instead of $\overline{K}$ makes a difference in the case that K has positive characteristic. Note that Galois extensions are required to be separable by definition.

[20] There is a somewhat more complicated theory of upper ramification series which we will not comment on in these notes.

[21] Using Hensel's lemma one can find $\alpha \in L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Then, $G_i = \{\sigma \in G : v_L(\sigma(\alpha) - \alpha) \geq i+1\}$.

[22] The fact that v_L is G-invariant follows from the fact that the absolute value on L (which is closely linked to v_L) is built from the absolute value on K and $N_{L/K}$ (which is G-invariant).

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

Remark 18. *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 $f(L/K)$). For this reason the notation $K_0 := L_{\mathrm{unr}}$ and $K_1 := L_{\mathrm{tam}}$ is common (more generally we have $K_i := L^{G_i}$).

Corollary 19.

(a) $|I_{L/K}| = e(L/K)$. *In particular, L/K is unramified if and only if $I_{L/K} = 1$.*

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

Pictorially, the extension L/K factors as

$$\begin{tikzcd}[row sep=large]
L \arrow[d, dash, "G_1"', "\text{totally wildly ramified}"] \\
L_{\mathrm{tam}} = K_1 \arrow[d, dash, "G_0/G_1"', "\text{totally tamely ramified}"] \\
L_{\mathrm{unr}} = K_0 \arrow[d, dash, "G/G_0"', "\text{unramified}"] \\
K
\end{tikzcd}$$

Motivated by this diagram, we sometimes call G_0/G_1 the **tame quotient** of L/K. 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.[23] What about $G_K^{\mathrm{tam}} := \mathrm{Gal}(K^{\mathrm{tam}}/K)$? We have a natural short exact sequence

[23] It's not hard to see from this that $\mathcal{O}_{K^{\mathrm{unr}}}$ is a DVR with perfect residue field $\overline{k_K}$. In case it isn't clear, a topological group is topologically cyclic if it has a dense cyclic subgroup.

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

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

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

with topological generator τ_K.[24] Let $\widehat{\mathrm{Fr}}_K \in \mathrm{Gal}(K^{\mathrm{tam}}/K)$ be a lift of $\mathrm{Fr}_K \in \mathrm{Gal}(K^{\mathrm{unr}}/K)$.

Theorem 20 (Iwasawa)**.** $\mathrm{Gal}(K^{\mathrm{tam}}/K)$ *is topologically generated by* $\widehat{\mathrm{Fr}}_K$ *and* τ_K *with sole relation*

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

Analogous to before we have a factorization

$$\begin{tikzcd}[arrows=dash]
K^{\mathrm{sep}} \arrow[d, "P_K"] \arrow[dd, bend right=60, "I_K"'] \\
K^{\mathrm{tam}} \arrow[d] \\
K^{\mathrm{unr}} \arrow[d, "\widehat{\mathbb{Z}}"] \\
K
\end{tikzcd}$$

with I_K the **absolute inertia group** of K and P_K the **absolute wild inertia group** of K. When K has positive characteristic G_K can be described relatively succinctly in terms of P_K and G_K^{tam}. When K has characteristic 0 things are much more difficult, though a result of Jannsen and Wingberg does give a relatively small set of generators and relations in the p-adic case for $p \neq 2$.

Remark 21. *It's worth saying a little more about extensions and valuations. Let L/K be a degree n extension of nonarchimedean local fields. Choose valuations v_L, v_K and uniformizers π_L, π_K with $v_L(\pi_L) = 1 = v_K(\pi_K)$. Fix $0 < c < 1$. We obtain*

$$|\cdot|_{K,c} : K \to \mathbb{R}^{\geq 0}, \qquad x \mapsto c^{v_K(x)}$$

and similarly get $|\cdot|_{L,c}$. Then, $|\pi_K|_{K,c} = c = |\pi_L|_{L,c}$. Now, consider the unique extension $|\cdot|_c$ of $|\cdot|_{K,c}$ to L and write $\pi_L = u\pi_K^e$ for $u \in \mathcal{O}_L^\times$. Then,

$$|\pi_L|_c = |N_{L/K}(\pi_L)|_{K,c}^{1/n} = |N_{L/K}(u\pi_K^e)|_{K,c}^{1/n} = |N_{L/K}(\pi_K)|_{K,c}^{e/n} = c^e$$

and so $|\cdot|_c$ and $|\cdot|_{L,c}$ don't agree. What this does show is that $|\cdot|_{L,c}^e = |\cdot|_c$.

4 Differents

Let L/K be a finite extension of nonarchimedean local fields. Then, L/K is separable if and only if the trace pairing

$$t_{L/K} : L \times L \to K, \qquad (x, y) \mapsto \mathrm{tr}_{L/K}(xy)$$

[24] Note that $\widehat{\mathbb{Z}} \cong \prod_\ell \mathbb{Z}_\ell$.

is nondegenerate. Assume L/K is separable. Then,

$$\mathcal{O}_L' := \{x \in L : t_{L/K}(x,y) \in \mathcal{O}_K \text{ for every } y \in \mathcal{O}_L\}$$

is a fractional ideal of $\mathcal{O}_L$ (i.e., $\mathcal{O}_L' \in \mathcal{I}_L$). Its inverse

$$\mathcal{D}_{L/K} := (\mathcal{O}_L')^{-1} = \{x \in L : x\mathcal{O}_L' \subseteq \mathcal{O}_L\}$$

is called the **different** of L/K and is an ideal of $\mathcal{O}_L$. The different is well behaved with respect to extensions – given a tower $K \subseteq L \subseteq M$, we have

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}.$$

For convenience let $v_L(\mathcal{D}_{L/K}) := \inf\{v_L(x) : x \in \mathcal{D}_{L/K}\}$. The utility of the different comes from its ability to capture ramification.

Proposition 22. *Let L/K be a finite separable extension of nonarchimedean local fields with ramification index e.*

(i) $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ *for some* $\alpha \in L$ *and* $\mathcal{D}_{L/K} = m_\alpha'(\alpha)$ *for* $m_\alpha(x)$ *the minimal polynomial of* α *over* K*.*

(ii) $\mathcal{D}_{L/K} = \mathcal{O}_L$ *if and only if* L/K *is unramified.*

(iii) $v_L(\mathcal{D}_{L/K}) \leq e - 1$*.*

(iv) $v_L(\mathcal{D}_{L/K}) = e - 1$ *if and only if* L/K *is tamely ramified.*

In terms of ramification groups, we have

$$v_L(\mathcal{D}_{L/K}) = \sum_{i \geq 0}(|G_i| - 1).$$

5 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.[25] 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

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

in the sense that we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & I_\mathfrak{q} \arrow[r] \arrow[d, "\cong"] & D_\mathfrak{q} \arrow[r] \arrow[d, "\cong"] & \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{p}) \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & I_{L_\mathfrak{q}/K_\mathfrak{p}} \arrow[r] & D_{L_\mathfrak{q}/K_\mathfrak{p}} \arrow[r] & \mathrm{Gal}(k_{L_\mathfrak{q}}/k_{K_\mathfrak{p}}) \arrow[r] & 1
\end{tikzcd}$$

[25] Recall that the former is defined to be the stabilizer of $\mathfrak{q}$ under the action of $\mathrm{Gal}(L/K)$.

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

$$
\begin{tikzcd}
& K \arrow[rr, equal] \arrow[dl, hook'] \arrow[dd, hook] & & K \arrow[dl, hook'] \arrow[dd, hook] \\
L \arrow[rr, "\sigma"] \arrow[dd, hook] & & L \arrow[dd, hook] & \\
& K_{\mathfrak{p}} \arrow[rr, equal] \arrow[dl, hook'] & & K_{\mathfrak{p}} \arrow[dl, hook'] \\
L_{\mathfrak{q}} \arrow[rr, dotted, "\exists!"'] & & L_{\mathfrak{q}} &
\end{tikzcd}
$$