Galois groups of local and global fields

The goal of the talk today is to try to better understand the fine grain structure of the groups G_K when K is either a local (usually p-adic) field or a global field (usually a number field). A special emphasis will also be paid to how these two types of Galois groups interact, and how this interaction can be used to give a more fruitful study of the groups individually.

We also wish to emphasize, due to its importance later, why the main difficulty of the local factor $G_{\mathbb{Q}_p}$ is in the subgroup $P_{\mathbb{Q}_p}$—the wild ramification group. We will try to give examples of how wild ramification can manifest itself in concrete geometric complications.

Some geometric motivation

One of the main themes/goals of this note is to discuss how every Galois group $\mathrm{Gal}(E/F)$, where F is a number field, comes equipped with a bunch of conjugacy classes of "local data" in the form of Galois groups of local fields. While this is certainly technically nice, it is somewhat difficult to have intuition about what this is really doing and, in particular, what this means "geometrically" if anything at all.

The point of this first section is to give a very explicit, concrete example of a Galois group which can be studied by its local constituents in the same way that $G_{\mathbb{Q}}$ can be studied by its local constituents $G_{\mathbb{Q}_p}$. There will be no argument that in this example these packets of local data are, in a literal geometric sense, not only extremely intuitive/obvious but actually 'local'.

After we set up the formal definitions/results of local and global fields we will then revisit this example attempting to explain how, in a very real sense, the literal geometric local of the below example is the same notion of local when we talk about local and global fields allowing us, consequently, to transfer our geometric intuition from the explicit topological example below to the arithmetic example of, say, $G_{\mathbb{Q}}$.

Setting up the geometry

Here we setup our explicit geometric example that we will use later to intuit the role of $G_{\mathbb{Q}_p}$ in $G_{\mathbb{Q}}$.

The Galois group that we are going to study in this section is the Galois group $G_{\mathbb{C}(T)}$ which, for various reasons, is extremely simple (this is somewhat disingenuous: a better phrase being "non-mysterious", or "given the name of something well-known"). In fact, $G_{\mathbb{C}(T)}$ is the free profinite group on $\#(\mathbb{C})$ many generators. But, this is not important here, what is important is how one can "see" the structure of the "local factors" and how they contribute to the global picture.

The main observation that shades the study of $G_{\mathbb{C}(T)}$ in a geometric hue is the following:

$$G_{\mathbb{C}(T)} = \varprojlim_{S \subseteq \mathbb{P}^1_{\mathbb{C}}} \widehat{\pi_1(U_S)} = \varprojlim_{S \subseteq \mathbb{P}^1_{C}} \pi_1^{\text{ét}}(U_S) \tag{1}$$

where S travels over the finite subsets of $\mathbb{P}^1_{\mathbb{C}}$ and $U_S := \mathbb{P}^1_{\mathbb{C}} - S$. The fundamental group $\pi_1(U_S)$ here is the topological one, and the second equality in (1) is just the well-known fact that $\pi_1^{\text{ét}}(U_S) = \widehat{\pi_1(U_S)}$.

Remark 0.1: We are being a little sassy by not picking base points in (1) but since this is obvious, but also tedious, we ignore it. That said, it IS an important thing to keep track of and we will explain later what the analogy of not picking the base point in the arithmetic world is. ♦

The reason for (1) is actually quite simple depending on how hard one wants to think about it. Specifically, let us give a hand-wavey argument here which, hopefully, will convince the reader, and let those doubters see Remark 0.2 below.

To see why an equation like (1) should hold, begin by recalling that there is an equivalence of categories

$$\left\{\begin{array}{c}\text{Smooth projective}\\ \text{curves over } \mathbb{C}\\ \text{with a map } X \to \mathbb{P}^1_{\mathbb{C}}\end{array}\right\} \xrightarrow{\approx} \left\{\begin{array}{c}\text{Finitely generated}\\ \text{extensions of } \mathbb{C}(T)\end{array}\right\} \tag{2}$$

given by $X \to \mathbb{P}^1_{\mathbb{C}}$ maps to the induced map on function fields $\mathbb{C}(T) \hookrightarrow K(X)$. Now every non-constant map $X \to \mathbb{P}^1_{\mathbb{C}}$ is ramified at only finitely many places of $\mathbb{P}^1_{\mathbb{C}}$, call that set S. Then, by considering $V := X \times_{\mathbb{P}^1_{\mathbb{C}}} U_S$ (the preimage in X of U_S) we get a finite étale cover $V \to U_S$ which, of course, is a finite covering space of U_S. Moreover, $V \to U_S$ is Galois (as a covering space) if and only if the corresponding extension $\mathbb{C}(T) \hookrightarrow K(X)$ is Galois. Thus, with this in mind, one should believe (1) because both sides classify the same thing—$G_{\mathbb{C}(T)}$ classifies the finite Galois extensions of $\mathbb{C}(T)$ and $\varprojlim \widehat{\pi_1(U_S)}$ classifies the finite Galois covers of all the possible puncturings of $\mathbb{P}^1_{\mathbb{C}}$—but what the previous sentence explains is precisely that these two sets of data are the same.

Remark 0.2: So, for those unhappy with the above argument here is a slightly more rigorous justification: see Section 3.4 of Szamuely's text *Galois Groups and Fundamental Groups*. ♦

So, now that we have connected the study of $G_{\mathbb{C}(T)}$ with geometry/topology, let's try and exploit it by tapping into our deeply ingrained notions of "zooming in" or "localizing" and how this might break the study of $G_{\mathbb{C}(T)}$ into simpler local parts.

To this end, let us define for each $p \in \mathbb{P}^1_{\mathbb{C}}$ the subspace D_p to be a "small punctured disk around p". The reason for the scare quotes is our current unwillingness to specify precisely how small "small" means. In fact, we won't make this specification since, in practice, it doesn't matter. Namely, if D and D' are two small punctured disks around p then for any third small punctured disk D'' around p contained in both D and D' we see that the maps

$$\pi_1(D) \leftarrow \pi_1(D'') \to \pi_1(D')$$

are isomorphisms which justifies this snakey phrase "small"—we can make D_p as small as we'd like, and it won't affect the fundamental group.

Note then that for each U_S we get natural maps $\pi_1(D_p) \to \pi_1(U_S)$ (and thus induced maps on their profinite completion) as follows. If $p \notin S$ then this map is the zero map. If $p \in S$ then we can assume that D_p is a small enough punctured disk that it is contained entirely within U_S in which case $\pi_1(D_p) \to \pi_1(U_S)$ is the natural inclusion. Regardless, one can see that these maps $\pi_1(D_p) \to \pi_1(U_S)$ respect the natural system that occurs by varying S and thus, consequently, we get maps from $\pi_1(D_p)$ into their inverse limit—we get maps $\pi_1(D_p) \to G_{\mathbb{C}(T)}$ for all p. Of course, consequently, we get maps $\widehat{\pi_1(D_p)} \to G_{\mathbb{C}(T)}$. Note, moreover, that this map is an injection (it's even an isomorphism when composed with the natural quotient $G_{\mathbb{C}(T)} \to \widehat{\pi_1(U_{\{q,p\}})}$ for any $q \neq p$!).

So, we see that the group $G_{\mathbb{C}(T)}$ comes with a natural system of injections

$$\left\{\widehat{\pi_1(D_p)} \to G_{\mathbb{C}(T)}\right\}_{p \in \mathbb{P}^1_{\mathbb{C}}} \tag{3}$$

which, if we think of $G_{\mathbb{C}(T)}$ as classifying ramified covers of $\mathbb{P}^1_{\mathbb{C}}$, are essentially sussing out the complicatedness of such a cover "near p" or "locally at p". So, for example, if we are looking at a representation $\rho : G_{\mathbb{C}(T)} \to \mathrm{GL}_n(A)$ that factors through $\widehat{\pi_1(U_S)}$ with $p \notin S$ (so the representation only cares about finite covers unrmamified over p) then, necessarily, $\widehat{\pi_1(D_p)}$ is killed by ρ since the topology of covers classified by $\widehat{\pi_1(U_S)}$ is trivial near p.

Remark 0.3: Note that, as we will mention it again later, that the system of embeddings as in (3) is only well defined *up to conjugacy*. Indeed, this is precisely the price we pay by being noncommittal about choosing a base point—different choices of base point will yield conjugate (in each $\pi_1(U_S)$) subgroups. ♦

Thus, one might imagine that these injections are somehow the "local constituents" of the Galois group $G_{\mathbb{C}(T)}$ at every point of $\mathbb{P}^1_{\mathbb{C}}$—they are measuring the complicatedness of the Galois group $G_{\mathbb{C}(T)}$ "at p". This method of thought is extremely powerful since it allows one to try and study the Galois group of $\mathbb{C}(T)$ or, equivalently, the finite ramified covers of $\mathbb{P}^1_{\mathbb{C}}$, by studying how that cover looks "point-to-point" which allows us to eliminate a huge amount of the complicatedness of the cover—instead of having worry about a space like U_S we instead just have to worry about the tiny punctured disk D_p.

This is precisely the sort of nice geometric picture that we'd like to have when thinking about something like the Galois group $G_{\mathbb{Q}}$ and its local constituents $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$. But, before we go into this in more detail, we give an extended reminder on local and global fields and their Galois groups.

1 Local fields and their Galois groups

1.1 Basic definitions

Somewhat contravariant to the historical point of view, we'd like to start discussing local fields before global fields. This is largely due to the relative simplicity of this setting compared to the vast, uncharted wilderness of their global counterparts. In particular, local fields, and their Galois groups, have much simpler to define structures. These structures then, by the nature of the connection between local and global Galois groups, transfer to structures on the global Galois groups. But these structures are somewhat less apparent/intuitive when viewed through a strictly global lens. It is somewhat similar to how global class field theory came historically first but, in terms of relative complicatedness, and the fact that the global case is "built from the local cases", it's somewhat more logical to begin locally and then move globally.

So, let us start, as we must, with the titular definition of this section: A *local field* is a non-discrete, locally compact, Hausdorff field.

It turns out that there are essentially two flavors of such fields. Specifically, let us recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the absolute value $|p^n x|_p := p^{-n}$ (if x contains no power of p) and $\mathbb{F}_p(\!(T)\!)$ is the completion of $\mathbb{F}_p(T)$ with respect to the valuation $|T^n f(T)| = p^{-n}$ (if $f(T)$ contains no power of T). The classification of local fields is then as follows:

Theorem 1.1 (Classification of local fields): *An exhaustive irredundant list of local fields is given by the finite extensions of $\mathbb{Q}_p$, the finite extensions of $\mathbb{F}_p(\!(T)\!)$, and $\mathbb{R}$ and $\mathbb{C}$. Here p is allowed to vary over all primes p.*

One calls the local fields $\mathbb{R}$ and $\mathbb{C}$ the *archimedean* local fields, and the rest are called *non-archimedean local fields* and they are characterized by the fact that their absolute values satisfy the ultrametric inequality: $|x+y| \leqslant \max\{|x|, |y|\}$ which, as we will see, makes their study much more algebraic in nature. We shall focus on the finite extension of $\mathbb{Q}_p$, the so-called *p-adic local fields*, and so when we say "local field" below this should always be taken to mean "p-adic local field". That said, most of what we will say will also apply to the finite extensions of $\mathbb{F}_p(\!(T)\!)$ the so-called *completed function fields*.

Remark 1.2: In the above classification one must be careful to interpret the result correctly. Namely, a local field is both a field K together with a topology. The above list only gives the underlying fields of the local fields. That said, there is a unique valuation extending that on $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(T)\!)$ and can be defined as in (6) as is discussed below. ♦

Let us consider some basic examples:

Example 1.3: The fields $\mathbb{Q}_p(\sqrt[p^n]{p})$ are prime examples of local fields other than $\mathbb{Q}_p$ itself. ▮

Example 1.4: The field $\mathbb{Q}_7(\zeta_{7^2-1})$ is a non-trivial extension of $\mathbb{Q}_7$ but, perhaps surprisingly, is only an extension of degree 2. ▮

Example 1.5: Consider $K := \mathbb{Q}(i)$ and the prime $\mathfrak{p} := (i+2)$ of $\mathcal{O}_K = \mathbb{Z}[i]$. One then obtains a valuation $|\cdot|_{\mathfrak{p}} : \mathbb{Q}(i) \to \mathbb{R}_{>0}$ by sending a non-zero $x \in K$ to 5^{-n} if $(x) = \mathfrak{p}^n \cdot I$ with I a fractional ideal of $\mathcal{O}_K$ coprime containing no power of $\mathfrak{p}$. Then, $K_{\mathfrak{p}}$, the completion of K at this absolute value, is a local field (since it's

non-discrete, complete, and locally compact). That said, it's not clear what it's structure as an extension of some $\mathbb{Q}_p$ is—in fact, it's isomorphic (naturally) to $\mathbb{Q}_5$. ▮

Now, what makes the study of a local field $K/\mathbb{Q}_p$ considerably easier than their global counterparts is that they are complete with respect to a valuation $|\cdot| : K \to \mathbb{R}_{>0}$ which simplifies their algebraic structure considerably—specifically, completeness implies that there is at most one absolute value on L extending that on K for any extension L/K. This is patently false for the case of number fields as we will later see.

Remark 1.6: This statement about unicities of valuation extensions is an amusingly elementary fact. Namely, one might recall that all norms on finite-dimensional $\mathbb{R}$-vector spaces are equivalent. If one analyzes the proof they can see that all that is really needed is that $\mathbb{R}$ is a *complete* valued field. Thus, the same argument works on finite extensions L/K of local fields, since any valuation on L extending that on K is a norm on the finite-dimensional K-vector space L—all such are equivalent. ♦

Note that local fields have a naturally defined subrings

$$\mathcal{O}_K := \{x \in K : |x| \leqslant 1\} \tag{4}$$

which is a DVR. We shall denote the maximal ideal of $\mathcal{O}_K$ by $\mathfrak{m}_K$ and note that it is precisely

$$\mathfrak{m}_K := \{x \in K : |x| < 1\} \tag{5}$$

Note that $\mathfrak{m}_K$ must be principal and we call any such generator a *uniformizer* of K. We shall denote the residue field $\mathcal{O}_K/\mathfrak{m}_K$ by κ_K.

As a matter of notational convention, let us mention the following. Fix an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ and let us consider only local fields as subextensions of this algebraic closure. Note that we can re-normalize the norm on any such local field K so that its restriction to $\mathbb{Q}_p$ is $|\cdot|_p$ (the standard such absolute value). In fact, in this case we can explicitly, and concretely write down the norm (owing, again, to the fact that there is only one such norm up to equivalence). Namely,

$$|x|_K = \left|N_{K/\mathbb{Q}_p}(x)\right|_p^{\frac{1}{n}} \tag{6}$$

if $n = [K : \mathbb{Q}_p]$. Note then that since we have a family of compatible norms on the finite extensions of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}_p}$ that we can, in fact, extend the norm on $\mathbb{Q}_p$ to *any* algebraic subextension $\mathbb{Q}_p \subseteq L \subseteq \overline{\mathbb{Q}_p}$. We then still have a natural valuation ring as in (4) with maximal ideal in (5) and a residue field κ_K. That said, one should be wary that L will not in general be complete (in fact, it will be so if and only if $L/\mathbb{Q}_p$ is finite) and $\mathcal{O}_L$ will not be a PID, and thus have no uniformizer (this is because $|\cdot|_L$ needn't be discrete).

Example 1.7: Let $L := \mathbb{Q}_p(\sqrt[p^\infty]{p})$ be the extension of $\mathbb{Q}_p$ obtained by adjoining all p^{th}-power roots of p to $\mathbb{Q}_p$. This is non-complete (it's an infinite degree extension) and it's also true that $\mathcal{O}_L$ is not a PID. Indeed, $|\cdot|_L$ is not discrete since, using equation (6), one sees that $|\sqrt[p^n]{p}|_L = (p^{-1})^{p^n}$. ▮

Example 1.8: Define $\mathbb{Q}_p^{\text{ur}}$ to be $\mathbb{Q}_p(\{\zeta_{p^n-1} : n \geqslant 1\})$—this is called the *maximal unramified extension of* $\mathbb{Q}_p$, the reason for the naming of which will be made clear later. Then $\mathbb{Q}_p^{\text{ur}}$ is a non-complete extension of $\mathbb{Q}_p$ but, in fact, $\mathcal{O}_{\mathbb{Q}_p^{\text{ur}}}$ is a PID with uniformizer p. ▮

We will need very few general facts about local fields for this talk, but is useful to know when discussing some aspects of higher ramification groups:

Theorem 1.9: *Let L/K be an extension of local fields. Then, $\mathcal{O}_L$ is monogenic—in other words, there is some $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.*

This is in stark contrast the case of number fields where, in general, number rings are not monogenic extensions of one another—in fact, there are extensions of number fields L/K with $\mathcal{O}_L$ not even a free $\mathcal{O}_K$-module!

1.2 The beginning of a filtration: inertia

1.2.1 The definition

Now, the study of the Galois group G_K of a local field K (or any subextension of $\overline{\mathbb{Q}_p}$) is largely going to be informed by how well the various automorphisms in G_K respect the structure of the ring $\mathcal{O}_K$. Indeed, note that by the explicit nature of $|\cdot|_K$ given in (6) one can see that for any automorphism of K acts by isometries—we have that $|\sigma(x)|_K = |x|_K$ for all $x \in K$. In particular, σ preserves both $\mathcal{O}_K$ and $\mathfrak{m}_K$.

Remark 1.10: There is, ostensibly, a tiny gap in the logic used above. Namely, it's clear that $\sigma \in \mathrm{Aut}(K)$ will act by isometries on K if σ fixes $\mathbb{Q}_p$. But, this is guaranteed since $\mathbb{Q}_p$ is rigid—it has no non-trivial automorphisms. This is an exercise in cleverly checking that any automorphism of $\mathbb{Q}_p$ is continuous—this implies the result since any automorphism fixes $\mathbb{Q}$ (necessarily) and thus, by continuity, is trivial since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. The proof that such automorphisms are continuous is done in a similar way to the classic proof that $\mathbb{R}$ has no automorphisms. ♦

So, for a Galois extension L/K, where K is a local field, we have a natural map

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa_K) \tag{7}$$

coming from the fact that elements of $\mathrm{Gal}(L/K)$ stabilize $\mathfrak{m}_K$. We call the the kernel of this map the *inertia group of* L/K (or just inertia group when L/K is clear from context) and denote it $I(L/K)$. We then have the following defining exact sequence

$$1 \to I(L/K) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa_K) \to 1 \tag{8}$$

called the *inertia exacts sequence* (the verification that the map in (7) is surjective is not very difficult). We shall abbreviate $I(\overline{K}/K)$ to I_K.

Note that since κ_K is a finite field (being the residue field of a local field which, as one can check, are all finite) and κ_L is an algebraic extension of κ_K, the group $\mathrm{Gal}(\kappa_L/\kappa_K)$ is exceedingly simple—it's procyclic. This realization amply motivates the following rough credo guiding our studies: the hard part of G_K is I_K. In other words, any statement "Property/claim _____ about G_K is hard" is really a statement about I_K. We will later refine this credo.

As an example of this with an eye towards Galois representations note that if we have such a representation $\rho : G_K \to \mathrm{GL}_n(A)$ that we will be in a particularly simple situation if it satisfies $\rho(I(\overline{K}/K)) = \{I_n\}$. Indeed, if this is true then ρ will factor through $G_K/I_K \cong G_{\kappa_K}$. In particular, if ρ is continuous (as will be the case for all our representations) then the induced representation $G_{\kappa_K} \to \mathrm{GL}_n(A)$ will be determined by its value on the topological generator (i.e. on the Frobenius map).

In fact, in reasonable situations one can completely describe the set of Galois representations of G_{κ_K} valued in some field. For example:

Theorem 1.11: *Let k be a finite field. Then, $\rho \mapsto \rho(Frob)$ is a bijection*

$$\mathrm{Hom}_{cont.}(G_k, \mathrm{GL}_n(\mathbb{Q}_\ell)) \xrightarrow{\cong} \{T \in \mathrm{GL}_n(\mathbb{Q}_\ell) : |\lambda| = 1 \text{ for all eigenvalues } \lambda \text{ of } T \text{ in } \overline{\mathbb{Q}_\ell}\}$$

Regardless, we see that, whether focusing directly on the structure of G_K or on the structure of its Galois representations, almost the entire difficulty is bundled in the inertia group I_K.

1.2.2 A recasting

It is extremely helpful to put the inertia subgroup $I(L/K)$ in the context of actual field extensions of K. Namely, we know that $I(L/K) = \mathrm{Gal}(L/F)$ for some subextension $L/F/K$, and the understanding of what this field F is will largely dictate our treatment of $I(L/K)$.

So, let us first get down some basic terminology concerning extensions L/K of local fields or, more generally, discretely valued fields. We then define the *ramification index* of L/K, denoted $e(L/K)$, to be the integer such that $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L^{e(L/K)}$ or, equivalently, the index $[|L^\times| : |K^\times|]$. We define the *residual index*, denoted $f(L/K)$, to be equal to $[\kappa_L : \kappa_K]$. It is easy to verify that the equality $[L : K] = e(L/K)f(L/K)$ holds as long as L/K is finite and K is a local field.

Remark 1.12: The equality $e(L/K)f(L/K) = [L : K]$ holds true more generally any time K is Henselian. In particular, it *does* hold true for K any algebraic extension of K and L/K finite—but we won't need this here. ♦

Let us say that an extension L/K (again of discretely valued fields) is *unramified* if $e(L/K) = 1$ and *totally ramified* if $f(L/K) = 1$. Note that saying that L/K is unramified is equivalent to saying that if π_K is a uniformizer of $\mathcal{O}_K$ then π_K is also a uniformizer of $\mathcal{O}_L$. A trivial observation is that for a tower $L/F/K$ of discretely valued fields one has that $e(L/K) = e(L/F)e(F/K)$ and similarly for the residual index.

The key theorem concerning unramified extensions is their relationship to their extensions of the residue field:

Theorem 1.13: *Let K be a local field*

1. *L/K a finite extension. Then, L/K is unramified if and only if for any (equival. for one) $\overline{\alpha} \in \kappa_L$ with $\kappa_L = \kappa_K(\overline{\alpha})$ one has that $L = K(\alpha)$ for any lift $\alpha \in \mathcal{O}_L$ of $\overline{\alpha}$.*
2. *The functor $L \mapsto \kappa_L$ induces an equivalence of categories:*

$$\left\{\begin{array}{c}\text{Algebraic unramified}\\ \text{extensions of } K\end{array}\right\} \xrightarrow{\approx} \left\{\begin{array}{c}\text{Algebraic extensions}\\ \text{of } \kappa_K\end{array}\right\}$$

Remark 1.14: There are two comments concerning Theorem 1.13 that may be enlightening to some readers. First, the inverse functor in 2. is given by sending k/κ_K to $\mathrm{Frac}(W_K(k))$ where $W_K(k)$ is the ring of K-relative Witt vectors of k.

Also, being an unramified extension L/K means precisely that the map $\mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_K)$ is étale. In this light 2. in Theorem 1.13 is a consequence of the more general equivalence of sites $\mathsf{Ét}_X \cong \mathsf{Ét}_{X_0}$ where $X = \mathrm{Spec}(A)$ with A a Henselian local ring, and X_0 the closed point of X. ♦

From Theorem 1.13 we can easily deduce that if L/K is an unramified extension of local fields, and E/K is any extension of local fields, then LE/E is unramified. Indeed, by the necessary condition of 1. in Theorem 1.13 we see that $L = K(\alpha)$ with $\kappa_L = \kappa_K(\overline{\alpha})$. Then, we see that $LE = E(\overline{\alpha})$. Thus, by the sufficency condition of 1. we see that LE/E is unramified.

In particular, if $L, L'/K$ are two unramified extensions of local fields then LL'/L is unramified so that $e(LL'/L) = 1$. Since $e(L/K) = 1$ we deduce from the multiplicativeness of ramification index in towers that $e(LL'/K) = e(LL'/L)e(L/K) = 1$ and thus LL'/K is unramified.

Note that we have the following important consequence of the fact that unramified extensions are closed under compositum. Namely there is a *maximal unramified extension* of K obtained as the compositum of all finite unramified extensions of K—we denote this extension by K^{ur}. In fact, a corollary of Theorem 1.13 is that we can fairly simplly describe K^{ur}. Namely, if κ_K has size q then $K^{\mathrm{ur}} = K(\{\zeta_{q^n-1} : n \geqslant 1\})$. Indeed, this follows from the fact that the maximal algebraic extension of κ_K, namely $\overline{\kappa_K}$, is just $\kappa_K(\{\zeta_{q^n-1} : n \geqslant 1\})$.

We should now explain how this discussion of unramified extensions helps us to recast the definition of the inertia group $I(L/K)$ of a Galois extension L/K with K a local field. The key observation is that if L/K is finite then $f(L/K) = [\kappa_L : \kappa_K] = |\mathrm{Gal}(\kappa_L/\kappa_K)|$ and thus by the inertia exact sequence $|I(L/K)| = e(L/K)$. Thus, in particular, we see that $I(L/K)$ is trivial if and only if L/K is unramified. More generally, since it's clear that an arbitrary Galois extension L/K, with K a local field, is unramified if and only if every finite subextension is, we can deduce that L/K is unramified if and only if $I(L/K)$ is trivial—no need to restrict to finite extensions.

From this discussion we also derive a very useful alternative way to write $I(L/K)$. Namely, if L/K is an arbitrary Galois extension (with K a local field) then the above shows that $I(L/K)$ is precisely $\mathrm{Gal}(L/L\cap K^{\mathrm{ur}})$ or, equivalently, $L^{I(L/K)} = L \cap K^{\mathrm{ur}}$.

1.3 The next step: wild ramification

In practice one cannot hope to deal solely with unramified extensions of local fields. By the same token one cannot hope that every Galois representation $\rho : G_K \to \mathrm{GL}_n(A)$ is unramified (i.e. that $I_K \subseteq \ker \rho$). That said, we might hope for something slightly weaker to hold in a greater generality. Namely, perhaps there

is a subgroup $P(L/K)$ of $I(L/K)$ which 'small enough' to often be killed in practice, but 'large' enough to have $I(L/K)/P(L/K)$, the subgroup a representation killing $P(L/K)$ must factor through, be reasonable. Thankfully, such a subgroup exists.

So, let us take the reverse role to defining $P(L/K)$ that we took to defining $I(L/K)$. Namely, for $I(L/K)$ we first defined a filtration

$$\{\mathrm{id}\} \subseteq I(L/K) \subseteq \mathrm{Gal}(L/K) \tag{9}$$

which then gave rise to the tower

$$\begin{array}{c} L \\ \Big| \, I(L/K) \\ K^{\mathrm{ur}} \cap L \\ \Big| \, \mathrm{Gal}(\kappa_L/\kappa_K) \\ K \end{array}$$

Let us instead first define the analogue of K^{ur} that will give rise to our subgroup $P(L/K) \subseteq \mathrm{Gal}(L/K)$.

To that end, let us say that an extension L/K, where K is a discretely valued field, is *tamely ramified* if $p \nmid e(L/K)$. We call an extension L/K which is not tamely ramified *wildly ramified*. An abitrary algebraic extension L/K, with K local, is called tamely ramified if every finite subextension is.

Remark 1.15: These definitions may extremely innocuous, perhaps even finicky. But, somewhat surprisingly, will be responsible for the main complicatedness of the group $\mathrm{Gal}(L/K)$ as $\mathrm{Gal}(L/K)$ is very simple if L/K is tamely ramified.

Moreover, it's actually the notion of tame ramification that will make the study of ℓ-adic representations of G_K (where K is p-adic) for $\ell \neq p$ so different from when $\ell = p$ (i.e. the study of p-adic Hodge theory). ♦

So, let us begin by making the same observation that we made for unramified extensions. Namely, let us suppose that $L, L'/K$ are tamely ramified extensions of local fields. Then, we want to say that LL'/K is tamely ramified. Note that an extension F/K is tamely ramified if and only if $FK^{\mathrm{ur}}/K^{\mathrm{ur}}$ is since, evidently, $e(FK^{\mathrm{ur}}/K^{\mathrm{ur}}) = e(F/K)$. Thus, it suffices to assume that $K = K^{\mathrm{ur}}$.

The result then becomes immediate considering the following theorem:

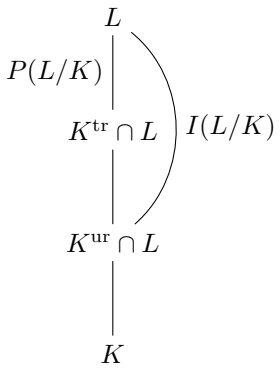
Theorem 1.16: *Let K be a local field and let E/K^{ur} be a finite tamely ramified extension. Then, $E = K^{\mathrm{ur}}(\pi_K^{\frac{1}{n}})$ where $n = [F : K^{\mathrm{ur}}]$.*

Proof: Note that E/K^{ur} must necessarily be totally ramified since $f(E/K^{\mathrm{ur}}) = 1$ (since $\kappa_{K^{\mathrm{ur}}} = \overline{\kappa_K}$). Thus, we know that if π_E is a uniformizer of E then $\pi_K = \pi_E^n u$ for $u \in \mathcal{O}_E^\times$. The claim will then be proven if we can show that u has an n^{th} root in E.

But, note that $\mathcal{O}_E$ is Henselian. Indeed, this is obvious for $\mathcal{O}_M$ for every finite subextension $E/M/K$ (since such a subextension has $\mathcal{O}_M$ complete local) and since the question of lifting roots can be put into the setting of finite extensions Hesenlianess follows.

So, to show that u has an n^{th} root we must merely show that $T^n - \overline{u} \in \kappa_E[T]$ has a simple root. But, this is obvious since κ_E is algebraically closed of characteristic p and $p \nmid E$. ■

So, let us define K^{tr} to be the maximal (algebraic) tamely ramified extension of K. And let us define, for any Galois extension L/K, the *wild ramification group* $P(L/K) \subseteq \mathrm{Gal}(L/K)$ to be $\mathrm{Gal}(L/L \cap K^{\mathrm{tr}})$. In other words, we have the tower



giving rise to the filtration

$$\{\mathrm{id}\} \subseteq P(L/K) \subseteq I(L/K) \subseteq \mathrm{Gal}(L/K) \tag{10}$$

which, by design, has the property that L/K is tamely ramified if and only if $P(L/K)$ is trivial. As per usual, we shorten $P(\overline{K}/K)$ to P_K.

Note that by Theorem 1.16 we can explicitly describe K^{tr}. Namely, it's $K^{\mathrm{ur}}(\{\pi_K^{\frac{1}{n}} : (n,p) = 1\})$ or, combining this with our description of K^{ur}, it is $K(\{\pi_k^{\frac{1}{n}}, \zeta_n : (n,p) = 1\})$.

Theorem 1.16 also allows us to give our more refined credo concerning the study of local Galois groups. Since it is one of the main points of this talk I'll put it on a typographical pedestal:

Credo: *Most of the complicated nature of G_K, where K is a p-adic local field, is concentrated in P_K. Thus, statements of the form "Property/claim _____ for G_K is difficult" is really a statement about P_K.*

We attempt to partially justify this claim by showing that, at least in the case of tame ramification, Galois groups are simple. In other words, we want to show that G_K/P_K is a relatively simple group. Namely, we already know that $G_K/I_K \cong G_{\kappa_K} \cong \widehat{\mathbb{Z}}$ and it follows quite readily from Theorem 1.16 that $I_K/P_K \cong \widehat{\mathbb{Z}}^{(p)}$ which, by definition, are those elements of $\widehat{\mathbb{Z}}$ with trivial component in $\mathbb{Z}_p$. In fact, Theorem 1.16 actually shows more. Namely, it shows that P_K is normal in $\mathrm{Gal}(L/K)$ and that

$$G_K/P_K = \mathrm{Gal}(K^{\mathrm{tr}}/K) \cong \widehat{\mathbb{Z}}^{(p)} \rtimes \widehat{\mathbb{Z}} \tag{11}$$

where the morphism defining the semi-direct product

$$\widehat{\mathbb{Z}} \to \mathrm{Aut}(\widehat{\mathbb{Z}}^{(p)}) = (\widehat{\mathbb{Z}}^{\times})^{(p)}$$

is the product of the cyclotomic characters $\chi_{\ell,K}$ as ℓ ranges over primes distinct from p. To be clear, let us recall that if K is a local field then $\chi_{\ell,K} : G_K \to \mathbb{Z}_\ell^\times$ (for any ℓ, even $\ell = p$) is defined as the composition

$$G_K \twoheadrightarrow \mathrm{Gal}(K(\zeta_{\ell^\infty})/K) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}) = \mathbb{Z}_\ell^\times$$

or, less cryptically, $\chi_{K,\ell}$ is defined by the rule that $\chi_{K,\ell}(g) \mod \ell^n$ (an element of $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$) is such that $g(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\chi_{K,\ell}(g) \mod \ell^n}$.

A full justification for why the above credo is actually useful in practice will come later in our talks when we discuss Grothendieck's ℓ-adic monodromy theorem and understand why there is no subject called "ℓ-adic Hodge theory". The rough idea will be that, in practice (for a large class of A's at least), one can expect that for a Galois representation $\rho : G_K \to \mathrm{GL}_n(A)$ one can expect that P_K is "essentially in the kernel of ρ" or, more correctly, $\rho(P_K)$ is finite.

1.4 Ramification filtration: lower indexing

So, having seen the success of the last two subsections, it seems only natural to try and push the sort of filtrations as in (9) and (10) even further. Namely, why not try and create some sort of *separated* filtration

$$\mathrm{Gal}(L/K) \supseteq I(L/K) \supseteq P(L/K) \supseteq G_2 \supseteq G_3 \supseteq \cdots \tag{12}$$

(where separated means that $\bigcap G_i = \{\text{id}\}$) such that, in keeping with the hopes of the previous sections, we have that each subsequent quotient G_i/G_{i+1} is of a relatively simple form. The hope/idea being, as above, that while we can't hope that a general Galois representation is unramified, or even tamely ramified (i.e. contains P_K in its kernel), perhaps it will (in good situations) contain one of the G_i for $i \gg 0$ and thus might be amenable to study by thinking of G_K/G_i as the iterated extensions of the "simple" groups G_i/G_{i+1}.

So, to this end, let us try to make the following definition of G_i which is supposed to mimic the definition of $I(L/K)$. Namely, for each $n \geqslant -1$ define the *n^{th} higher ramification group (in lower numbering)* of an extension L/K of local fields, denoted $I_n(L/K)$, as follows:

$$I_n(L/K) := \ker(\text{Gal}(L/K) \to \text{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{n+1})) \tag{13}$$

So, for example, it's evident that $I_{-1}(L/K) = \text{Gal}(L/K)$ and $I_0(L/K) = I(L/K)$. Slightly less evident, but true (we'll discuss this momentarily), is the fact that $I_1(L/K) = P(L/K)$.

The motivation for this definition is actually fairly simple. Namely, we think of $\mathcal{O}_L/\mathfrak{m}_L^{n+1}$ as being a sort of "n^{th}-order approximation to $\mathcal{O}_L$" in the same way that $\mathbb{C}[T]/(T^{n+1})$ is an n^{th}-order approximation to $\mathbb{C}[\![T]\!]$ (i.e. it only keeps track of a power series up to the degree n term). Thus, in a very rough sense, one might imagine sending $\sigma \in \text{Gal}(L/K)$ to its image in $\text{Aut}(\mathcal{O}_L/\mathfrak{m}_L)$ as being something like a "derivative" and sending it to $\text{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{n+1})$ as being something like an "automorphism of the n^{th}-order jet space" (a fancy notion of higher derivative). It thus makes sense to try and filter $\text{Gal}(L/K)$ by the subgroups of elements which are more, and more difficult to distinguish from their "differential data"—the elements which have jets agreeing with that of the identity map for higher and higher orders.

Now, as claimed above, the *ramification filtration (in lower numbering)*

$$\text{Gal}(L/K) \supseteq I(L/K) \supseteq P(L/K) \supseteq I_2(L/K) \supseteq \tag{14}$$

is separated. Indeed, if $\sigma \in \text{Gal}(L/K)$ is in every $I_n(L/K)$ then it acts trivially on $\mathcal{O}_L/\mathfrak{m}_L^n$ for every $n \geqslant 1$. Letting n tend to infinity shows that it acts trivially on $\varprojlim \mathcal{O}_L/\mathfrak{m}_L^n = \mathcal{O}_L$ and thus acts trivially on L as desired. This makes intuitive sense since what (a ring) A being complete (with respect to a maximal ideal $\mathfrak{m}$) means is precisely that knowledge of A is equivalent to knowledge of all of its n^{th}-order approximations $A/\mathfrak{m}^{n+1}$.

The second property we desired a good filtration to have is that the subsequent quotients G_i/G_{i+1} are of a particularly simple form. The fact that this holds true for the ramification filtration is codified by the following result:

Theorem 1.18: *Let L/K be an extension of local fields. Then:*

$$I(L/K)/I_1(L/K) \hookrightarrow \kappa_L^\times,$$
$$I_n(L/K)/I_{n+1}(L/K) \hookrightarrow \kappa_L, \qquad n \geqslant 1$$

Proof: This is a somewhat annoying, but routine, check. Namely, the maps are

$$I(L/K)/I_1(L/K) \to \kappa_L^\times : \sigma \mapsto \frac{\sigma(\pi)}{\pi} \mod \mathfrak{m}_L$$

and

$$I_n(L/K)/I_{n+1}(L/K) \to \mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} : \sigma \mapsto \frac{\sigma(\pi)}{\pi} - 1 \mod \mathfrak{m}_L^{n+1}$$

respectively where, here, π is any uniformizer of L. One can check that these are, in fact, isomorphisms and that $\mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} \cong \kappa_L$ as κ_L-vector spaces. ■

In particular, we see that the subsequent quotients in the ramification filtration are, in fact, abelian. This proves the following highly non-trivial fact about $\text{Gal}(L/K)$:

Corollary 1.19: *Let L/K be an extension of local fields. Then,* $\text{Gal}(L/K)$ *is solvable*

And, consequently, since every Galois group of an algebraic extension L/K (with K a local field) is a limit of its finite quotients, every Galois group $\text{Gal}(L/K)$ with L/K arbitrary Galois (and K local) is pro-solvable.

Remark 1.20: I don't know if $G_{\mathbb{Q}_p}$ is *actually solvable*. Namely, being pro-solvable does not, in general, imply solvable. I tried to find information on whether $G_{\mathbb{Q}_p}$ was actually solvable, but came up with nothing. If anyone reading knows the answer, please do let me know.

Note, as well, that my usage of 'solvable' in the above is slightly non-standard. Namely, solvable usually means a finite filtration with abelian quotients whereas, here, I really mean a countable separated filtration with abelian quotients. ♦

Another thing that follows from this is that $I_1(L/K)$ is the Sylow p-subgroup of $I(L/K)$ since it's a p-group (since $I_n(L/K)/I_{n+1}(L/K)$ is a p-group for $n \geqslant 1$) and $I(L/K)/I_1(L/K)$ has prime to p-order. Of course, it is *the* Sylow p-subgroup since it's normal. In particular, even better than Corollary 1.19 we see that if L/K is an extension of local fields then $\mathrm{Gal}(L/K)$ is isomorphic to

$$I_1(L/K) \rtimes (\mathrm{Gal}(L/K)/I_1(L/K))$$

and by previous discussion $\mathrm{Gal}(L/K)/I_1(L/K)$ is itself the semidirect product of two cyclic groups.

The last theoretic thing we'd like to prove in this section is the claim that if L/K is finite, then $I_1(L/K) = P(L/K)$:

Theorem 1.21: *Let L/K be a Galois extension of local fields. Then, $I_1(L/K) = P(L/K)$.*

Proof: Since $P(L/K) = \mathrm{Gal}(L/L \cap K^{\mathrm{tr}})$ it suffices to check that the restriction of $I_1(L/K)$ to $L \cap K^{\mathrm{tr}}$ is trivial to show that $I_1(L/K) \subseteq P(L/K)$. So, let's show this first. Of course, it's equivalent to show that if L/K is tamely ramified then $I_1(L/K)$ is trivial. But, since $I_1(L/K) = I_1(LK^{\mathrm{ur}}/K^{\mathrm{ur}})$ we may as well assume that $K = K^{\mathrm{ur}}$. One can then visibly see from Theorem 1.16 that any element of the Galois group acts non-trivially mod $\mathfrak{m}_L^2$. Namely, if $L = K(\pi_K^{\frac{1}{n}})$ then all Galois group elements send $\pi_K^{\frac{1}{n}}$ to $\zeta\pi_K^{\frac{1}{n}}$ for some root of unity ζ, but modulo $\mathfrak{m}_L^2 = (\pi^{\frac{1}{n}})^2$ this is not equivalent to the identity map.

The converse is not difficult, and left to the reader. ■

As a corollary of this we deduce the following:

Corollary 1.22: *Let K be a local field and L/K a Galois extension. Then, $P(L/K)$ is a pro-p-group. In fact, $P(L/K)$ is the pro-p-Sylow subgroup of* $\mathrm{Gal}(L/K)$.

This will actually be the key property to the second part of our justification of our credo—the reason why $\rho(P_K)$ is small for a large class of ρ.

Let us end this subsection with a classic example:

Example 1.23: It is a little tricky, but not overly deep, to compute the higher ramification groups for the extension $\mathbb{Q}_p(\zeta_{p^k})$. Namely, we have that

$$I_n(\mathbb{Q}_p(\zeta_{p^k})/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^k})/\mathbb{Q}_p(\zeta_{p^e})), \quad \text{if } p^{e-1} \leqslant n < p^e$$ ▌

1.5 Ramification filtration: upper indexing

1.5.1 Motivation for necessity

Considering the immense success enjoyed by the ramification filtration considered in the previous subsection, it seems strange to admit that we are not done—that this ramification filtration is not a good candidate for the sort of filtration we need when talking about Galois representations. But, alas, it's not. This is a real shame since the ramification filtration (with lower numbering) in the last subsection is incredibly more apparent/intuitive than the ramification filtration which will be used in practice (the one with upper numbering).

There are many reasons that the upper numbering filtration, the one which will replace the lower numbering filtration, is preferred. Some are fairly fancy, but we will have a very concrete, immediate issue with the lower numbering ramification groups that the upper numbering will fix.

Remark 1.24: The somewhat fancy reason is that it is the upper numbering filtration is relevant in class field theory where, there, the pullback along the Artin map $K^\times \to G_K^{\mathrm{ab}}$ of the upper numbering filtration (on inertia) n is the 'Lie filtration' $1 + \mathfrak{m}_K^i \subseteq K^\times$. This is actually a general phenomenon—when a Galois group is a p-adic analytic Lie group, then the upper numbering filtration corresponds to the very natural Lie filtration (when we think about it as a p-adic analytic Lie group). One can see these notes for example. This provides one reason to think that the upper numbering filtration groups are natural—they provide literal intuition about "filtering by actions on jet spaces" in the case when the Galois group has an analytic structure! ♦

To get to this issue, we begin by considering a thought experiment. Particularly, a simple desire we should have is to have a filtration that works on $I(L/K)$ for *any* Galois extension L/K (with K local). Indeed, it is very rare that a Galois representation $\rho : G_K \to \mathrm{GL}_n(A)$ will factor through $\mathrm{Gal}(L/K)$ for a finite extension L/K. Thus, if we hope to be able to truly carry out our program of studying Galois representations by having ρ be trivial on a sufficiently deep constituent of our filtration, we really do need to have the filtration on an arbitrary Galois extension, in particular, on I_K itself.

So, we then attempt to extend the definition of the previous section to work for L/K Galois. There is, of course, a natural definition. Namely, $\mathcal{O}_L$ is still a valuation ring with maximal ideal $\mathfrak{m}_L$ and the Galois group of L/K still preserves $\mathfrak{m}_L$. Thus the definition

$$I_n(L/K) := \ker\left(\mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{n+1})\right) \tag{15}$$

still makes sense and, hopefully, still works. Unfortunately, the world is not a fair or just place—it does not. In fact, this might be semi-unsurprising since our intuition for why $I_n(L/K)$, when L/K is finite, is useful is that $\mathcal{O}_L/\mathfrak{m}_L^n$ is like an "n^{th}-order approximation" which allowed us to interpret elements of $I_n(L/K)$ as being like functions whose first n-derivatives (or, more formally, its first n jets) are trivial. But, this intuition was predicated upon the idea that $\mathcal{O}_L = \varprojlim \mathcal{O}_L/\mathfrak{m}_L^n$ (just like $\mathbb{C}[\![T]\!] = \varprojlim \mathbb{C}[T]/(T^n)$) and this fails for infinite extensions extensions—they're not complete.

In fact, the failure of $I_n(L/K)$'s effectiveness for L/K infinite can be spectacular. For example, if $L = \overline{K}$ then the value group of L is $V = \{|\pi_K|^\alpha : \alpha \in \mathbb{Q}\}$ (where π_K is a uniformizer of K). This then has the property that every element $V \cap [0,1]$ is a square, and thus, in fact $\mathfrak{m}_{\overline{K}}^2 = \mathfrak{m}_{\overline{K}}$ so that, with the definition as in (15), we'd have that $I_n(\overline{K}/K) = I_K$ for all $n \geqslant 1$.

Thus, any definition as in (15) is bound to fail. But, we might have another brilliant idea which, in most other situations, works. Namely, if we've defined $I_n(L/K)$ correctly for L/K finite then for L/K Galois why not just set

$$I_n(L/K) = \varprojlim I_n(L'/K) \tag{16}$$

as L' ranges over finite Galois subextensions $L/L'/K$? But, the reason why this does not work is, while not overly complicated, is subtle and perhaps easily missed on a first read-through of this topic. Specifically, for (16) to make sense, we'd need to know that if L_1 and L_2 are finite subextensions of L/K with $L_2 \supseteq L_1$ that the natural quotient map $\mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$ takes $I_n(L_2/K)$ into $I_n(L_1/K)$—but, it does *not*.

Namely, the lower numbering filtration is great when it comes to looking at subgroups of $\mathrm{Gal}(L/K)$. For example in the situation above one can check that $I_n(L_2/K) \cap \mathrm{Gal}(L_2/L_1) = I_n(L_2/L_1)$ but it is *bad* at respecting quotients which, if we hope to use an equation like (16) to define the filtration on arbitrary Galois extensions, is unforgivable.

So, the way forward is clear: try and adapt the definition of $I_n(L/K)$ so that it works well with quotients instead of subgroups.

Remark 1.25: Note that there is, yet another, way of trying to define $I_n(L/K)$ for L/K arbitrary Galois which, when thought through, exposes the fundamental issue with $I_n(L/K)$ which manifested itself above. One can be inspired to attempt this alternative way by thinking about the inertia and wild inertia groups. Namely, even though we restricted our attention to finite extensions L/K when defining the ramification filtration, the first two non-negative terms, $I_0(L/K) = I(L/K)$ and $I_1(L/K) = P(L/K)$, were actually definable and useful in the coveted situation of arbitrary Galois extensions as subsections 1.2 and 1.3 showed. What gives? Why do those work for any Galois extension and not that of $I_n(L/K)$ for $n > 2$?

To make this more clear, let us set

$$S_n := \{L/K : L/K \text{ is finite, and } I_n(L/K) = 0\}$$

for $n \geqslant 2$. So, for example, S_0 is the set of unramified extensions of K and S_1 the set of tamely ramified extensions of K. Suppose for a second that S_n was closed under composition. We can then define a field K_{S_n} to be the compositum of the elements of S_n. So, again, $K_{S_0} = K^{\text{ur}}$ and $K_{S_1} = K^{\text{tr}}$. A little thinking then shows that a perfectly fine definition of $I_n(L/K)$, for any L/K Galois, would be $\text{Gal}(L/L \cap K_{S_n})$—for example, this is what held true in the case of $I(L/K)$ and $P(L/K)$. So, what goes wrong with this for $n > 2$? Well, it's quite simple: S_n is not closed under compositum. This is, in some sense, the fundamental obstruction which makes our definition of ramification groups (while intuitive) not helpful for dealing with quotients/conducive to being defined for arbitrary Galois extensions

It's a good exercise to find counterexamples showing this for $n > 2$. ♦

1.5.2 Definition and important properties

OK. Now that we have an understanding of what goes wrong with the lower-numbering filtration, we can, as voiced earlier, attempt to fix it to create a filtration which plays well with quotients and, consequently, will be able to be defined for arbitrary Galois extensions (as in (16)).

Unfortunately, I do not have a rich sense of intuition for why the definition we're about to give works beyond, well, *it does*. Even if one is made happy the edifying fact (mentioned in Remark 1.24) that the upper numbering filtration agrees with the Lie filtration when the Galois group is a p-adic Lie group, it doesn't help intuit why the definition is obvious—for this I don't have a great answer. Perhaps a deeper study of the proof of the content of Remark 1.24 would yield the answer, but we don't answer that here.

So, we will obtain the 'correct' filtration, the upper numbering filtration, by a fairly complicated reindexing of the lower numbering filtration. Namely, we'll define $I^v(L/K)$ to be $I_{\psi(v)}(L/K)$ for some function ψ which we'll soon define.

So, let us fix an arbitrary Galois extension L/K of local fields. We will, unless stated otherwise, abbreviate $I_n(L/K)$ to I_n. We also extend the definition of I_n to I_u, for any $u \in [-1, \infty)$, by setting $I_u := I_{\lceil u \rceil}$. This will be important since the function ψ will be much less annoying to define if we don't have to worry about only defining it on integers (or even whether that would suffice!).

So, let us define the function $\eta : [-1, \infty) \to [-1, \infty)$ as follows:

$$\eta(u) := \int_0^u \frac{dt}{[I_0 : I_t]}$$

I wrote the definition this way since it is, after all, the 'classical' way of writing η. But, it's deceivingly complicated. Namely, η is just a piecewise linear function describable as follows:

$$\eta(u) := \begin{cases} -u & \text{if} \quad u \in [-1, 0] \\ \dfrac{1}{|I_0|}\left(|I_1| + \cdots + |I_m| + (u-m)|I_{m+1}|\right) & \text{if} \quad u \in [m, m+1],\ m \in \mathbb{N} \end{cases}$$

written this way it's not hard to check that η is continuously, monotonically increasing, and surjective. Thus, by basic analysis, η must be a homeomorphism. We denote its inverse by ψ.

So, finally we can give the long-awaited definition. For any $v \in [-1, \infty)$ we define the the v^{th}-*higher ramification group (in upper numbering)*, denoted I^v (or $I^v(L/K)$ when we want to emphasize the extension), to be $I^v := I_{\psi(v)}$. One can check, for example, that $\psi(v)$ is an integer if v is an integer. But, beware! It's not true that one can restrict themselves to I^v for $v \in \mathbb{Z}$ for, in general, it's <u>not</u> true that

$$\{I^v : v \in [-1, \infty)\} = \{I^v : v \in (\mathbb{Z} \cap [-1, \infty))\}$$

So, just to point out the obvious, the groups I^v are all just *some* lower ramification group I_n (for some integer n) but it's not at all obvious what n it is (one would have to write down ψ which would require knowledge of $|I_m|$ for all m).

Remark 1.26: It is a fairly deep result that if L/K is abelian (i.e. that $\text{Gal}(L/K)$ is abelian) then, in fact, the above warning is not necessary. Namely, the so-called Hasse-Arf theorem says that for abelian extensions the jumps in the upper numbering filtration (the numbers where a new group appears) are integers. ♦

The two key results that make the above seem worth it are as follows:

Theorem 1.27 (Herbrand): *Let $L_2 \supseteq L_1$ be local fields which are Galois extensions of the local field K. Let $f : \mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$ denote the usual quotient map. Then:*

1. $f(I_u(L_2/K)) = I_{\eta(u)}(L_1/K)$
2. $f(I^v(L_2/K)) = I^v(L_1/K)$

Thus since $\eta(u) \leqslant u$, in general, and $\eta(u) < u$ sometimes, one has that quotient maps don't send $I_u(L_2/K)$ to $I_u(L_1/K)$. But, the same is actually true for upper numbering and thus makes it amenable to be used to define upper numbered ramification groups for an arbitrary Galois extension.

Remark 1.28: One can use Herbrand's theorem to justify the definition of upper numbering filtration. Namely, as soon as one finds a function $\nu : [-1, \infty) \to [-1, \infty)$ such that $f(I_u(L_2/K)) = I_{\nu(u)}(L_1/K)$ then (assuming that ν is invertible) one should, of course, set $I^v(L_2/K) = I_{\nu^{-1}(v)}(L_2/K)$. But, what is non-obvious to me is why one would expect that the function ν one can take is the function η as we described.♦

To this end, if L/K is an arbitrary Galois extension, with K a local field, we then define the *higher ramification groups*, denoted $I^v(L/K)$, for $v \in [-1, \infty)$, by the formula:

$$I^v(L/K) := \varprojlim I^v(L'/K) \tag{17}$$

as L' ranges over the finite Galois subextension of L/K. As per usual, we abbreviate $I^v(\overline{K}/K)$ to I^v_K.

Note that, by design, $\{I^v(L/K)\}_{v\in[0,\infty)}$ gives a descending filtration on $I(L/K)$ called the *ramification filtration (in upper numbering)*. The important properties, for us, of this filtration are as follows:

Theorem 1.29: *Let K be a local field L/K a Galois extension. Then:*

1. $\bigcap_{v\in[0,\infty)} I^v(L/K) = \{\mathrm{id}\}$
2. $I^0(L/K) = I(L/K)$.
3. $P(L/K) = \bigcup_{v>0} I^v(L/K)$
4. $\bigcap_{v'<v} I^{v'}(L/K) = I^v(L/K)$

Example 1.30: Consider the infinite Galois extension $\mathbb{Q}_p(\zeta_{p^\infty})$. Then, note that $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$, and one can show that $I^n(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = 1 + p^n\mathbb{Z}_p$ for all $n \geqslant 1$. Note that since $\mathbb{Q}_\mathfrak{p}(\zeta_{p^\infty})/\mathbb{Q}_p$ is abelian the Hasse-Arf theorem tells us that I really only do have to tell you the values of the filtration at integers.▌

2 Global Galois groups in comparison with local Galois groups

Now that we have a thorough understanding of the basic structure of the Galois groups of local fields, we can explain how these tie into the study of the Galois groups of global fields.

Again, we start as we must. A *global field* is either a finite extension of $\mathbb{Q}$ (a *number field*) or a finite extension of $\mathbb{F}_p(T)$ (a function field). Again, we'll be mainly interested in the case of number fields, but most of what we'll say will apply to global fields at large.

2.1 Connection to local fields

The first obvious question one might have is what is the precise connection between local and global fields? The idea, roughly, is that global fields are "bundled together local fields" and, in a sense, the "local picture" of a global field (where local needs to be interpretted correctly) is that of a local field. We will try and make this geometric intuition more precise in the last section, but for now that little bit will suffice.

So, let us begin in earnest. It is somewhat enlightening, even though slightly counter to what is usually taught in a first course in algebraic number theory, to think of global fields as being valued fields. The real big difference is that, unlike local fields, global fields will have many non-equivalent valuations in general since they are non-complete. In what follows we call an equivalence class of valuations on a global field K a *place* of K.

So, to the end of studying number fields as valued fields, it's helpful to first recall that Big Ostrowski theorem which classifies the places of number fields:

Theorem 2.1 (Big Ostrowski): *Let K be a number field with ring of integers $\mathcal{O}_K$. Then, a complete irredundant list of absolute values on $\mathcal{O}_K$ is given by $|\cdot|_{\mathfrak{p}}$, for each $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, and $|\cdot|_\sigma$ for σ a real embedding $K \hookrightarrow \mathbb{R}$ or a pair of complex embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$.*

Remark 2.2: There is an analogous result to Theorem 2.1 for function fields. Namely, every function field $K/\mathbb{F}_p(T)$ is the function field an integral smooth projective curve $C/\mathbb{F}_p$ (perhaps not geometrically integral!). Then, the absolute values on K correspond precisely the closed points of C. This is, in essence, precisely the statement of the valuative criterion for properness after noting that any valuation is automatically trivial on $\mathbb{F}_p$. ♦

Here, $|x|_{\mathfrak{p}} = q^{-n}$ (where $q = |\mathcal{O}_K/\mathfrak{p}|$) if the fractional ideal (x) is of the form $\mathfrak{p}^n I$ with I containing no power of $\mathfrak{p}$. The absolute values $|x|_\sigma$, for σ an embedding $K \hookrightarrow \mathbb{C}$ are defined by $|x|_\sigma = |\sigma(x)|_\infty$ where $|\cdot|_\infty$ is the standard absolute value on $\mathbb{C}$ (the pairs of complex embeddings just means that $|\cdot|_\sigma$ and $|\cdot|_{\overline{\sigma}}$ give equivalent embeddings). We call the primes $|\cdot|_{\mathfrak{p}}$ *finite primes* and the primes $|\cdot|_\sigma$ *infinite primes*. They are, equivalently, the non-archimedean absolute values and archimedean absolute values respectively. Note that for each finite prime $|x|_{\mathfrak{p}}$ the valuation subring of K is $(\mathcal{O}_K)_{\mathfrak{p}}$ and its valuation ideal is $\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$.

The key result relating local and global fields is the follwoing:

Theorem 2.3: *Let K be a number field and $|\cdot|$ some place of K. Then, the completion $K_{|\cdot|}$ of K with respect to $|\cdot|$ is a local field.*

Proof: If $|\cdot|$ is an infinite place, then evidently the completion is either $\mathbb{R}$ or $\mathbb{C}$ which is local. Thus, we may as well assume that $|\cdot| = |\cdot|_{\mathfrak{p}}$ for some prime $\mathfrak{p}$.

One can check that a complete non-discrete discretely valued field K is locally compact, and thus a local field, precisely when its residue field κ_K is finite—if it's local then $\mathcal{O}_K$ is compact, m_K is open and thus $\mathcal{O}_K/\mathfrak{m}_K$ is both compact and discrete; if κ_K is finite then $\mathcal{O}_K/\mathfrak{m}_K^n$ is finite for all n and since $\mathcal{O}_K = \varprojlim \mathcal{O}_K/\mathfrak{m}_K^n$ this implies that $\mathcal{O}_K$ is compact.

Since the residue field of $K_{|\cdot|}$ is the same as that of $\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$ we see that $K_{|\cdot|}$ has finite residue field and thus is local by the previous paragraph. ■

We shall always abbreviate $K_{|\cdot|_{\mathfrak{p}}}$ to $K_{\mathfrak{p}}$. It's clear, by considering residue fields, that $K_{\mathfrak{p}}$ is a p-adic local field if $(p) = \mathfrak{p} \cap \mathbb{Z}$.

Now, the above says that the completion of global fields at their places are local fields, what is somewhat surprising is that the converse is true:

Theorem 2.4: *If $F/\mathbb{Q}_p$ is a p-adic local field, then there exists a number field $F/\mathbb{Q}$ and a prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F)$ lying over p such that $F_{\mathfrak{p}} \cong K$.*

This follows from Krasner's lemma or, more precisely, from the following corollary thereof:

Lemma 2.5: *Let K be a p-adic local field and $f \in K[x]$. Assume that f is an irreducible monic polynomial of degree n. Then, there exists some $\delta > 0$ such that if $g(x) \in K[x]$ is degree n and such that $|f - g| < \delta$ (where $|h(x)|$ is the supremum of the norm of the coefficients) then $g(x)$ is irreducible and for every root α of $f(x)$ there is a root β of $g(x)$ such that $K(\alpha) = K(\beta)$.*

Remark 2.6: Using Lemma 2.5 we can show that there are only finitely many extensions of a p-adic local field K of a fixed degree n. Indeed, one notes that every extension can be split into a unramified subextension and totally ramified subextension. Since there is only one unramified extension of each degree (by Theorem 1.13) it suffices to deal with the totally ramified case.

one can then show that every totally ramified extension of a local field K is generated by an Eisenstein polynomial: a polynomial $f(x) = x^n + \cdots + a_0 \in \mathcal{O}_K[x]$ with $a_i \in \mathfrak{m}_K$ for $i = 0, \ldots, n-1$ and $a_0 \notin \mathfrak{m}_K^2$. Moreover, such an Eisenstein polynonmial is necessarily irreducible.

So,to show that there are only finitely many totally ramified extensions, we merely note that every extension is a root of such an Eisenstein polynomial. But, the coefficients of this polynomial are in $\mathfrak{m}_K \times \cdots \times \mathfrak{m}_k \times (\mathfrak{m}_K - \mathfrak{m}_K^2)$ which is compact. But, by Theorem Lemma 2.5 we know that if the polynomials are sufficiently close (since they are automatically irreducible) they generate the same extension. Since the space $\mathfrak{m}_K \times \cdots \times_K \times (\mathfrak{m}_K - \mathfrak{m}_K^2)$ is compact we need only finitely many such neighborhoods to cover it, and thus there are only finitely many such extensions.

This is in stark contrast to the global case there there are, for example, infinitely many extensions of $\mathbb{Q}$ of every degree.

Note, by the way, that this is one place where the moniker 'p-adic' is important. Namely, Artin-Schrier theory easily shows that $\mathbb{F}_p(T)$ has infinitely many cyclic p-extensions. ♦

From Theorem 2.4 we also deduce the following super important corollary:

Corollary 2.7: *For any choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ the image is dense. Similarly, for any number field F and prime $\mathfrak{p}$ any embedding $\overline{F} \hookrightarrow \overline{F_\mathfrak{p}}$ has dense image.*

Proof: It suffices to show that every p-adic local subextension $K/\mathbb{Q}_p$ has $K \cap \overline{\mathbb{Q}}$ dense in K. That said, this follows immediately from Theorem 2.2 by taking the F such that $K = F_\mathfrak{p}$. Then, F is dense in K and $F \subseteq K \cap \overline{\mathbb{Q}}$. ■

2.2 Comparison of extensions

Let us now think about extension of number fields E/F and how local fields factor into this study. Here, as mentioned above, is where one of the key differences between local and global fields rears its head. Namely, let us fix a finite prime $|\cdot|_\mathfrak{p}$ on F. Unlike the local case where there was a unique extension (up to equivalence) of the absolute value here there is, in general, many.

In particular, note that a finite place $|\cdot|_\mathfrak{q}$ lies over $|\cdot|_\mathfrak{p}$ (in the sense that its restriction to F is equivalent to $|\cdot|_\mathfrak{p}$) if and only if $\mathfrak{q}$ lies over $\mathfrak{p}$ in the sense that $\mathfrak{q} \cap \mathcal{O}_F = \mathfrak{p}$. In particular, since one can have many primes lying over a given prime $\mathfrak{p}$ (in fact, there are always primes $\mathfrak{p}$ with $[E : F]$ distinct primes lying over them) we are unable to canonically identify extensions of number fields with extensions of valued fields. Namely, when thinking about an extension of a local field K we were largely able to conflate the notion of whether the extension was an extension of valued fields (i.e. an extension of fields with the choice of an extension of the absolute value) or just an extension of fields—this is because the unicity of extension made the distinction moot. But, for number fields this is not the case.

But, choosing an extension of (non-archimedean) valued fields E/F, where E and F are number fields, is equivalent to giving an extension of fields E/F and primes $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_E)$ and $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F)$ with $\mathfrak{q} \cap \mathcal{O}_E = \mathfrak{p}$.

If we have such an extension $(F, |\cdot|_\mathfrak{p}) \to (E, |\cdot|_\mathfrak{q})$ (where, one should note, $|\cdot|_\mathfrak{q}$ restircted to F is only equivalent to E in general, not literally equal) one gets an induced continuous map of local fields $F_\mathfrak{p} \to E_\mathfrak{q}$ which can then be studied as we did above. Thus, we see that studying the extension of number fields E/F, with an eye towards their number theoretic properties, is a lot like studying the set of all inclusions $F_\mathfrak{p} \to E_\mathfrak{q}$ and, as we will shortly see, essentially the important number theoretic data of E/F is contained in these various $E_\mathfrak{q}/F_\mathfrak{p}$'s justifying this claim.

But, before we get to this, we can actually give a very clear understanding of how the various absolute values lying over $|\cdot|_\mathfrak{p}$ fit together and justify the phrase "the study of E/F, with an eye towards $|\cdot|_\mathfrak{p}$ on F is a cobbled together study of the various local extensions $F_\mathfrak{p} \to E_\mathfrak{q}$" (a phrase on the lips of every student of number theory during their Sunday morning walks).

Namely:

Theorem 2.8: *Let E/F be an extension of number fields, and $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F)$. Then,*

$$E \otimes_{\mathbb{Q}} F_{\mathfrak{p}} \cong \prod_{\mathfrak{q}|\mathfrak{p}} E_{\mathfrak{q}}$$

as normed $\mathbb{Q}_p$-algebras where, here, $F \otimes_{\mathbb{Q}} M_{\mathfrak{p}}$ is given the unique (up to equivalence) norm obtained by thinking of it as a $[F : M]$-dimensional $M_{\mathfrak{p}}$-space.

2.3 Galois groups of number fields

Suppose now that E/F is an extension of number fields. We would like to understand what precisely is the relationship between $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(E_{\mathfrak{q}}/F_{\mathfrak{p}})$ as in the previous subsection.

The first thing one must realize in this study is that, unlike the case of local fields, the Galois group $\mathrm{Gal}(E/F)$ doesn't act continuously, in general, on E when E is given the $|\cdot|_{\mathfrak{q}}$-topology for some prime $\mathfrak{q}$. Indeed, this should not be shocking since, at least in the case of local fields, the veracity of this statement was essentially due to the unicity of absolute values whereas, here, we have many non-equivalent absolute values on $E_{\mathfrak{q}}$ even non-equivalent absolute values extending $|\cdot|_p$ on F.

We can be even more explicit in the failure for $\mathrm{Gal}(E/F)$ to act continuously on E with the $|\cdot|_{\mathfrak{q}}$-topology. In particular, it's not hard to see that the pullback of the norm $|\cdot|_{\mathfrak{q}}$ along $\sigma : E \to E$ is precisely the norm $|\cdot|_{\sigma^{-1}(\mathfrak{q})}$. Thus, we can qualify the failure of $\mathrm{Gal}(E/F)$ acting continuously on E when given the $|\cdot|_{\mathfrak{q}}$-topology by the following result:

Theorem 2.9: *Let E/F be a Galois extension. Then, $\mathrm{Gal}(E/F)$ acts transitively on $\{\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_E) : q \mid \mathfrak{p}\}$.*

In particular, we see that $\mathrm{Gal}(E/F)$ acts continuously on E with the $|\cdot|_{\mathfrak{q}}$-topology if and only if $\mathfrak{q}$ is the only prime of E lying over $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_F$.

Thus, to fruitfully analogize the inertial theory of local fields, we must restrict to those elements of $\mathrm{Gal}(E/F)$ which are continuous with respect to a given absolute value $|\cdot|_{\mathfrak{q}}$ or, equivalently, which fix the prime $\mathfrak{q}$. So, to this end, let us define for a prime $\mathfrak{q}$ lying over a prime $\mathfrak{p}$ the *decomposition group*, denoted $D(\mathfrak{q} \mid \mathfrak{p})$, to be the set of those $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$ (as a set—not pointwise) or, equivalently, those which are continuous with respect to the $|\cdot|_{\mathfrak{q}}$-topology.

It is then clear that, exactly as in the local case, once we restrict to decomposition groups we have a natural surjective reduction map

$$D(\mathfrak{q} \mid \mathfrak{p}) \to \mathrm{Gal}(\kappa_{\mathfrak{q}}/\kappa_p) \tag{18}$$

where, here, $\kappa_{\mathfrak{q}} := \mathcal{O}_E/\mathfrak{q}$ and similarly for $\kappa_{\mathfrak{p}}$. Thus, naturally, we define the *inertia group* of E/F at $\mathfrak{q}$, denoted $I(\mathfrak{q} \mid \mathfrak{p})$, to be the kernel of this map which then gives rise to the same inertial exact sequence

$$1 \to I(\mathfrak{q} \mid \mathfrak{p}) \to D(\mathfrak{q} \mid \mathfrak{p}) \to \mathrm{Gal}(\kappa_{\mathfrak{q}}/\kappa_{\mathfrak{p}}) \to 1 \tag{19}$$

exactly as in the local case.

Now, just as in the local case, the global case has ramification and residual indices but, just as with the case of inertia groups the difference is that there are now more than one prime to keep track of. Namely, for an extension of number fields E/F and primes $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_E)$ and $\mathfrak{q} \cap \mathcal{O}_F = \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F)$ one defines $e(\mathfrak{q}/\mathfrak{p})$ to the power of $\mathfrak{q}$ which shows up in the factorization of $\mathfrak{p}\mathcal{O}_F$ and $f(\mathfrak{q}/\mathfrak{p})$ to be the degree $[\kappa_q : \kappa_p]$. Equivalently, this is just the normal definition of inertial and residual index when considering the extension of discretely valued fields $(E, |\cdot|_q)/(F, |\cdot|_{\mathfrak{p}})$.

The analogy of $[L : K] = e(L/K)f(L/K)$ in the local case is the following:

Theorem 2.10: *Let E/F be an extension of number fields. Then, for any prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_E)$ one has that*

$$[E : F] = \sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q} \mid \mathfrak{p}) f(\mathfrak{q} \mid \mathfrak{p})$$

If E/F is Galois then Theorem 2.9 guarantees that $e(\mathfrak{q} \mid \mathfrak{p}) = e(\mathfrak{q}' \mid \mathfrak{p})$ for any $\mathfrak{q}, \mathfrak{q}' \mid \mathfrak{p}$ and thus, in that case, we denote the common numbers by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$. If $g_{\mathfrak{p}}$ denotes the number of primes lying over $\mathfrak{p}$ then Theorem 2.10 reduces to $[F : M] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$. Again noting that if E/F is Galois that

$$f_{\mathfrak{p}} = [\kappa_{\mathfrak{q}} : \kappa_p] = |\operatorname{Gal}(\kappa_q/\kappa_{\mathfrak{p}})|$$

(for any $\mathfrak{q} \mid \mathfrak{p}$) allows one to deduce that $|D(\mathfrak{q} \mid \mathfrak{p})| = e_{\mathfrak{p}} f_{\mathfrak{p}}$ and $|I(\mathfrak{q} \mid \mathfrak{p})| = e_{\mathfrak{p}}$. Thus, as in the local case, we see that $\mathfrak{q}$ is ramified if and only if $I(\mathfrak{q} \mid \mathfrak{p})$ is trivial.

2.4 Connection between local and global Galois groups

We would now like to make precise the earlier statement that the interesting number theoretic information contained in a Galois extension E/F of number fields is essentially a bundling of the number theoretic information contained in the various extensions of local fields $F_{\mathfrak{p}} \to E_{\mathfrak{q}}$.

The key observation to making this precise is the following. Suppose that E/F is a Galois extension of number fields and let $\mathfrak{q} \in \operatorname{Spec}(\mathcal{O}_E)$ and $\mathfrak{q} \cap \mathcal{O}_F = \mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_F)$. Then, as we've noted many times above, the natural inclusion $F \to M$ induces a natural inclusion $F_{\mathfrak{p}} \to E_{\mathfrak{q}}$. Note then that by restriction we obtain a map $\operatorname{Gal}(E_q/F_{\mathfrak{p}}) \to \operatorname{Gal}(E/F)$ and a natural question is what this map is really describing. This is completely answered by the following:

Theorem 2.11: *Let E/F and $\mathfrak{q}, \mathfrak{p}$ be as above. Then, the natural map $\operatorname{Gal}(E_q/F_{\mathfrak{p}}) \to \operatorname{Gal}(E/F)$ is injective with image precisely $D(\mathfrak{q} \mid \mathfrak{p})$. The image of $I(E_{\mathfrak{q}}/F_{\mathfrak{p}})$ is precisely $I(\mathfrak{q} \mid \mathfrak{p})$.*

Proof: To see that $\operatorname{Gal}(E_q/F_{\mathfrak{p}}) \to \operatorname{Gal}(E/F)$ is injective we merely note that if σ is in the kernel, then $\sigma : E_{\mathfrak{q}} \to E_{\mathfrak{q}}$ is continuous and fixes E. But, since E is dense in $E_{\mathfrak{q}}$ continuity implies that $\sigma = \mathrm{id}$ as desired.

Now, note that since any element of $\operatorname{Gal}(E_{\mathfrak{q}}/F_{\mathfrak{p}})$ is continuous for the valuation $|\cdot|_{\mathfrak{q}}$ the same holds for its image in $\operatorname{Gal}(E/F)$. Thus, the image of $\operatorname{Gal}(E_{\mathfrak{q}}/F_{\mathfrak{p}})$ lies in $D(\mathfrak{q} \mid \mathfrak{p})$. To see that it's surjective we note that since any element $\sigma \in D(\mathfrak{q} \mid \mathfrak{p})$ is an isometry for $|\cdot|_{\mathfrak{q}}$ it's, of course, uniformly continuous. Thus, it lifts uniquely to a map $E_{\mathfrak{q}} \to E_{\mathfrak{q}}$ (since uniformly continuous maps lift to completions) which is necessarily a ring map since this can be checked (for a continuous map) on the dense subset E. This proves surjectivity, and thus the first part of the theorem statement.

The statement concerning the inertia groups follows immediately from the observation that the natural inclusions $\kappa_{\mathfrak{q}} \to \kappa_{E_{\mathfrak{q}}}$ and $\kappa_{\mathfrak{p}} \to \kappa_{F_{\mathfrak{p}}}$ are isomorphisms. ■

Thus, we see that when we want to study E/F, or its Galois group, from the perspective of a given pair of primes $(\mathfrak{p}, \mathfrak{q})$ as above, when we want to focus on that aspect of the extension, when we want to "localize at these primes", we may as well replace E/F with $E_{\mathfrak{q}}/F_{\mathfrak{p}}$—we may as well replace our global fields with local ones.

We then see, immediately, that we may bring to bear the entire theory of local fields, and their Galois groups, when studying global fields and their Galois groups. In particular, inside of every Galois extension we have the natural subgroups $\operatorname{Gal}(E_{\mathfrak{q}}/F_{\mathfrak{p}})$ and thus, by the theory of ramificaiton filtration, subgroups $I_n(\mathfrak{q} \mid \mathfrak{p})$ and $I^v(\mathfrak{q} \mid \mathfrak{p})$ defined, not shockingly, to be $I_n(E_{\mathfrak{q}}/F_{\mathfrak{p}})$ and $I^v(E_{\mathfrak{q}} \mid F_{\mathfrak{p}})$.

2.5 Making statements over $\overline{K}$

One must be somewhat careful when extending the results of the previous section to arbitrary Galois extensions of number fields. Namely, if E/F is an arbitrary Galois extension (possibly infinite) with F a number field then, of course, we sill have that $\mathcal{O}_E$ (defined, as usual, to be the integral closure of $\mathbb{Z}$ in E) is integrally closed and dimension 1, but possibly non-Noetherian. We can then still make the claim that the non-archimedean valuations on E correspond to the primes $\mathfrak{q}$ of $\mathcal{O}_E$ or, equivalently (and also what makes this apparent) compatible systems of primes/absolute values on the finite subextensions E'/F.

So, if we have a prime $\mathfrak{q}$ of E and the corresponding prime $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_F$ we get an extension of valued fields $(F, |\cdot|_{\mathfrak{p}}) \to (E, |\cdot|_{\mathfrak{q}})$ and, by completing, a map of complete valued fields $F_p \to E_{\mathfrak{q}}$. But, here is where one must be slightly careful. Namely, it is tempting to say that $E_{\mathfrak{q}}$ should be an algebraic extension of $F_{\mathfrak{p}}$ but, unfortunately, this is not the case.

For example if, as per usual, one denotes $\widehat{\overline{\mathbb{Q}_p}}$ by $\mathbb{C}_p$ then, in fact, $(\overline{\mathbb{Q}})_{\mathfrak{p}} = \mathbb{C}_p$ for any prime of $\mathcal{O}_{\overline{\mathbb{Q}}}$ lying over p. Thus, it's not immediate how to apply the general theory of local fields, and their arbitrary Galois extensions, to the study of arbitrary Galois extensions of number fields.

So, to be extra careful, we spell out what must be modified in Theorem 2.11 to work for arbitrary Galois extensions. Namely, it still makes sense to define $D(\mathfrak{q} \mid \mathfrak{p})$ and $I(\mathfrak{q} \mid \mathfrak{p})$ even if E/F is an infinite Galois extension. The correct analogue of Theorem 2.11 is then the following:

Theorem 2.12: *Let F be a number field and E/F a Galois extension (possibly infinite). Let $\mathfrak{q}$ be a prime of E and $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_F$. Then, the map $\mathrm{Gal}_{cont.}(E_\mathfrak{q}/F_\mathfrak{p}) \to \mathrm{Gal}(E/F)$ is injective with image $D(\mathfrak{q} \mid \mathfrak{p})$. The image of $I_{cont.}(E_\mathfrak{q}/F_\mathfrak{p})$ in $\mathrm{Gal}(E/F)$ is $I(\mathfrak{q} \mid \mathfrak{p})$.*

Here $\mathrm{Gal}_{\mathrm{cont.}}$ denotes, as expected, continuous automorphisms of $E_\mathfrak{q}/F_\mathfrak{p}$—an automorphism is no longer guaranteed to be continuous if E_q is not algebraic over $F_\mathfrak{p}$ which, as mentioned above, happens if E/F is infinite. The definition of $I_{\mathrm{cont.}}(E_\mathfrak{q}/F_\mathfrak{p})$ is defined precisely as one would imagine. Then, the proof of Theorem 2.12 is precisely (literally verbatim) as that of Theorem 2.11.

This is somewhat messy to think about in general, so let us spell out what happens in the case of greatest interest to us: the case of $E = \overline{F}$. Here we can create an edulceration of Theorem 2.12 that will serve our purposes quite nicely.

Namely, instead of directly trying to make Theorem 2.11 (or the correct analogue as in Theorem 2.12) work for $\overline{F}/F$ let us just consider the following. Note that even though we have, for a prime $\mathfrak{p}$ of F, natural embeddings $F \hookrightarrow \overline{F}$ and $F \hookrightarrow F_\mathfrak{p}$ given an algebraic closure $F_\mathfrak{p} \hookrightarrow \overline{F_\mathfrak{p}}$ of $F_\mathfrak{p}$ there is no canonical embedding $\overline{F} \hookrightarrow \overline{F_\mathfrak{p}}$. In fact, thinking for a moment, one can see that the choice of such an embedding is equivalent to the choice of a prime $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_{\overline{F}})$ lying over $\mathfrak{p}$. So, let us choose such an embedding—any two equivalent embeddings are conjugate by an element of G_F.

Then, we get a natural map $G_{F_\mathfrak{p}} \to G_F$ by restriction. It follows by Theorem 2.7 that this map is injective since, every element of $G_{F_\mathfrak{p}}$ acts continuously on $\overline{F_\mathfrak{p}}$. Thus, we needn't fiddle with Theorem 2.12 and, instead, just think that we have $G_{F_\mathfrak{p}}$ sitting naturally (up to conjugation) inside of G_F. A moment's thought shows, moreover, that the image of $G_{F_\mathfrak{p}}$ is precisely $D(\mathfrak{q} \mid \mathfrak{p})$ if $\mathfrak{q}$ is the prime of $\overline{F}$ corresponding to the embedding $\overline{F} \hookrightarrow \overline{F_\mathfrak{p}}$, and similarly the image of $I_{F_\mathfrak{p}}$ is $I(\mathfrak{q} \mid \mathfrak{p})$.

Thus, at least in the case of the absolute Galois group, we do have a completely perfect analogy of Theorem 2.11 and the pursuant implications (e.g. that $G_{F_\mathfrak{p}}$ contains $I^v_{F_\mathfrak{p}}$).

Remark 2.13: If one is willing to think a little harder, one can get this much better version of Theorem 2.12, where we actually have $D(\mathfrak{q} \mid \mathfrak{p})$ as the image of $\mathrm{Gal}(L/K)$ for some Galois extension with K a local field.

Namely, let's for each prime p an algebraic closure $\overline{\mathbb{Q}_p}$. Then, if E/F is a Galois extension with F a number field, then, of course, $E_\mathfrak{q}$ embeds into $(\overline{\mathbb{Q}})_\lambda = \mathbb{C}_p$ (for some prime λ lying over $\mathfrak{q}$). Let $L := E_\mathfrak{q} \cap \overline{\mathbb{Q}_p}$, the intersection taken in $\mathbb{C}_p$. Then, naturally, L is dense in $E_\mathfrak{q}$ and thus one can see that $\mathrm{Gal}_{\mathrm{cont.}}(E_\mathfrak{q}/F_\mathfrak{p}) = \mathrm{Gal}(L/F_\mathfrak{p})$ which gives a more useful version of Theorem 2.12. The reason that we separated this from the discussion of the case $E = \overline{F}$ is that, in that case, we explicitly know that the L is: it's just $\overline{F_\mathfrak{p}}$.

This line of thought quickly leads to some very interesting, somewhat difficult, and incredibly important questions. For example, if we have that (with the notation above) $\mathrm{Gal}_{\mathrm{cont.}}(E_\mathfrak{q}/F_\mathfrak{p}) = \mathrm{Gal}(L/F_\mathfrak{p})$ one might wonder if there is some sort of "continuous Galois theory" for $\mathrm{Gal}_{\mathrm{cont.}}(E_\mathfrak{q}/F_\mathfrak{p})$ related to the standard Galois theory of $\mathrm{Gal}(L/F_\mathfrak{p})$. In fact, there is. Namely, it is a difficult theorem of Ax-Sen-Tate that if $H \subseteq \mathrm{Gal}(E_\mathfrak{q}/F_\mathfrak{p})$ is closed then $E_\mathfrak{q}^H$ is precisely $\overline{L^H}$. So, the answer to how this continuous Galois theory reacts to the normal Galois theory is that it is, in some sense, a *completed* Galois theory. ♦

3 Making geometric connections

3.1 A 'just look at it' connection

Now that we have discussed the necessary technical details in the study of local and global fields, and their Galois groups, I'd like to return to the first section and make a more explicit connection between the system $\{G_{\mathbb{Q}_p} \hookrightarrow G_\mathbb{Q}\}$ and the system $\{\widehat{\pi_1(D_p)} \hookrightarrow G_{\mathbb{C}(T)}\}$.

Remark 3.1: Here is where we can start to see the relevance to the selection of base points in the choice of $\widehat{\pi_1(D_p)}$. Namely, not doing so has given us only a system of *conjugacy class* of inclusions into $G_{\mathbb{C}(T)}$ just

like refusing to specify which prime $\mathfrak{p}$ of $\mathcal{O}_{\overline{\mathbb{Q}}}$ lying over p (i.e. choosing an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$) results in only a conjugacy class of embeddings $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$

The idea, not surprisingly, is that just like $G_{\mathbb{C}(T)}$ classifies topological data and that the restriction to $\widehat{\pi_1(D_p)}$ is the study of how this topological data looks like "locally at p", one should imagine that $G_{\mathbb{Q}}$ is classifying arithmetic data (or, perhaps more fittingly, arithmetico-geometric data) and that $G_{\mathbb{Q}_p}$ is the study of how this data looks like "locally at p".

If one is happy to just accept this fact as being reasonable then they can stop reading here. But, I'd like to take a second to explain why this plausible and then, once we are semi-convinced that it is, what the more fine structural data looks like under this analogy.

So, let us begin, as we did with $G_{\mathbb{C}(T)}$, with an equality:

$$G_{\mathbb{Q}} = \varprojlim_{S \subseteq \overline{\mathrm{Spec}(\mathbb{Z})} \text{ finite}} G_{\mathbb{Q},S} \tag{20}$$

here $\overline{\mathrm{Spec}(\mathbb{Z})} = \mathrm{Spec}(\mathbb{Z}) \cup \{|\cdot|_\infty\}$ or, equivalently, the set of places of $\mathbb{Q}$. The group $G_{\mathbb{Q},S}$ is equal to, by definition, $\mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q})$ where $\mathbb{Q}^S$ is the maximal extension of $\mathbb{Q}$ unramified outside of S (NB: an infinite place ramifies precisely when a real place becomes a complex place). The fact that the equality in (20) holds is trivial: interpreted correctly it just says that every finite extension of $\mathbb{Q}$ ramifies at only finitely many places which is obvious. This is not surprising if one believes the analogy (and is good evidence for the analogy), namely one can boil down the intuitive argument for (1) to the statement "a finite algebraic cover $\mathbb{P}^1_{\mathbb{C}}$ can only ramify at finitely many places".

Remark 3.2: In fact, the arguments are essentially the same. Since the maps $X \to \mathbb{P}^1_k$ or $\mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_K)$ are finite flat, it suffices to show that $\Omega^1_{X/\mathbb{P}^1_k}$ or $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ is supported at finitely points. That said, since both X and $\mathrm{Spec}(\mathcal{O}_L)$ are one-dimensional (and Ω^1 is coherent) this is equivalent to showing that Ω^1 is not zero in both cases. But, this is obvious since the map on generic fibers is a separable extension of fields with has non-vanishing cotangent sheaf. ♦

This equality suggests, perhaps, that in the analogy between $G_{\mathbb{C}(T)}$ and $G_{\mathbb{Q}}$ the following identifications could be made:

Geometric side	Number theory side
$\mathbb{C}(T)$	$\mathbb{Q}$
$\mathbb{P}^1_{\mathbb{C}}$	$\overline{\mathrm{Spec}(\mathbb{Z})} := \mathrm{Spec}(\mathbb{Z}) \cup \{\|\cdot\|_\infty\}$
U_S	$\overline{\mathrm{Spec}(\mathbb{Z})} - S$
$\widehat{\pi_1(U_S)}$	$G_{\mathbb{Q},S}$
D_p	$\mathrm{Spec}(\mathbb{Q}_p^{\mathrm{ur}})$
$\widehat{\pi_1(D_p)}$	$I_{\mathbb{Q}_p}$

although some of these should be justified. Namely, why is D_p equal to $\mathrm{Spec}(\mathbb{Q}_p^{\mathrm{ur}})$ and not $\mathrm{Spec}(\mathbb{Q}_p)$? The idea, roughly, is to think about what a small punctured disk around p should be—what algebraic space is that represented by (at least intuitively)? Well, if we think about what the functions on an arbitrarily small disk around p should be they are we get, not shockingly, the ring of convergent power series $\mathbb{C}\{\{z-p\}\}$. That said, since we're interested in the world of algebraic geometry where the convergence itself doesn't make sense, we take the next natural replacement: the ring of power series $\mathbb{C}[\![T]\!]$.

Remark 3.3: There is a slightly more convincing way to intuit why the disk we're after is $\mathbb{C}[\![T]\!]$ and not $\mathbb{C}\{\{z-p\}\}$ but it requires a serious diversion into a discussion of Henselizations and the points of the étale topos, and so is perhaps not appropriate here. ♦

So, if a small disk around p should have functions like $\mathbb{C}[\![T]\!]$ then the disk itself, or at least an algebraic modeling of it, would be like $\mathrm{Spec}(\mathbb{C}[\![T]\!])$. But, of course, we are not interested in the disk around p but the

punctured disk which means that we need to remove the point p from the disk—we need to remove the closed point from $\mathrm{Spec}(\mathbb{C}[\![T]\!])$. Thus, in fact, the most natural algebraic model for D_p is actually $\mathrm{Spec}(\mathbb{C}(\!(T)\!))$. Note then that the algebraic reason why D_p should be analogized to $\mathrm{Spec}(\mathbb{Q}_p^{\mathrm{ur}})$, or equivalently the reason that $\mathbb{C}(\!(T)\!)$ should be analogized to $\mathbb{Q}_p^{\mathrm{ur}}$, is that $\mathbb{C}(\!(T)\!)$ has no unramified extensions! Indeed, this is because the residue field of $\mathbb{C}(\!(T)\!)$ is already algebraically closed.

More geometrically, if D_p was analogized to $\mathrm{Spec}(\mathbb{Q}_p)$ (opposed to the maximal umramified extension) then we'd have the the un-punctured disk $\mathrm{Spec}(\mathbb{C}[\![T]\!])$ should be analogized to $\mathrm{Spec}(\mathbb{Z}_p)$. But, the issue is that the center point of the disk, the point p, has no interesting topology: $\pi_1(\{p\}) = 0$. So, if this analogy holds one would imagine that the central point of $\mathrm{Spec}(\mathbb{Z}_p)$, the closed subscheme $V((p)) = \mathrm{Spec}(\mathbb{F}_p)$, would have no interesting arithmetico-geometric information contained in it. But, of course, it does—it has non-trivial covers! Thus, we try and fix this analogy by eliminating the arithmetico-geometric data contained in the center point, we think about trying to make this central point algebraically closed without altering the surrounding "disk" too much. Thinking about it shows that this is precisely what passing from $\mathrm{Spec}(\mathbb{Z}_p)$ to $\mathrm{Spec}(\mathbb{Z}_p^{\mathrm{ur}})$ does—it changes the central point to no longer be arithmetico-geometrically interesting (it turns it from $\mathrm{Spec}(\mathbb{F}_p)$ to $\mathrm{Spec}(\overline{\mathbb{F}_p})$) while keeping the surrounding disk essentially intact.

To further convince ourselves that our analogy is correct, wes should note that if $\mathrm{Spec}(\mathbb{C}(\!(T)\!))$ is the right analogy of D_p then $G_{\mathbb{C}(\!(T)\!)}$ should be the same as $\widehat{\pi_1(D_p)}$. Since the latter is obviously $\widehat{\mathbb{Z}}$ this comes down to the question as to why $G_{\mathbb{C}(\!(T)\!)}$ is $\widehat{\mathbb{Z}}$. But, this is essentially done as in Theorem 1.16. Namely, note that any extension of $\mathbb{C}(\!(T)\!)$ is tamely ramified (since its residue field is characteristic 0), and since it's already its own maximal unramified extension, the same proof works to show that all the extensions of $\mathbb{C}(\!(T)\!)$ are of the form $\mathbb{C}(\!(T^{\frac{1}{n}})\!)$ (for any n) and thus the Galois group is $\widehat{\mathbb{Z}}$.

Of course, this connection also shows that, perhaps, the correct analogy for $\widehat{\pi_1(D_p)}$ is actually I_K/P_K since, as we noticed above, the space D_p has no wildly ramified covers (since it's residue field is characteristic 0) but I think this is not that I_K is not the right analogy to $\widehat{\pi_1(D_p)}$ but that the analogy is not perfect due to the nice properties of $\mathbb{C}(T)$ not enjoyed by $\mathbb{Q}$.

Hopefully the above was semi-convincing that the analogy between $G_{\mathbb{C}(T)}$ and $G_{\mathbb{Q}}$, with a focus on how $G_{\mathbb{Q}_p}$ is like $\widehat{\pi_1(D_p)}$ (and thus giving geometric backing to the claim that $G_{\mathbb{Q}_p}$ is the study of the objects $G_{\mathbb{Q}}$ classifies "locally at p"). That said, as the title of the subsection suggests, this justification was mostly just "the same things are showing up on both sides and thus they are analogous". In the next section we give slightly higher-tech justification.

3.2 Connection using $\pi_1^{\text{ét}}$

We would now like to make a slightly more precise justification as to why these two situations are analogous by using the formalism of Grothendieck's étale fundamental group. We will not recall the definition of it here but, suffice it to say, that nothing I can say will match the exposition in Szamuely's text *Galois groups and fundamental groups*.

Specifically, let's start again by looking at (20). Namely, let's rewrite it as

$$G_{\mathbb{Q}} \cong \varprojlim G_{\mathbb{Q},S} \tag{21}$$

where now S ranges over finite subets of $\overline{\mathrm{Spec}(\mathbb{Z})}$ which contain the infinite place $|\cdot|_\infty$. This equality still holds true since the statement justifying (20) "an extension ramifies at only finitely many places" now becomes the even simpler statement "an extension ramifies at only finitely many primes" (which justfies (21)). The reason to work with this version of the inverse limit is that it avoids having to work with archimedean places (objects of analysis) focusing, instead, on the finite places (objects of algebra). This also valuable in the analogy since $\mathbb{P}^1_{\mathbb{C}}$ is in bijection with the *finite places* (the non-archimedean ones) of $\mathbb{C}(T)$.

The key observation then to make is that $G_{\mathbb{Q},S} = \pi_1^{\text{ét}}(V_S)$ where, here $V_S = \overline{\mathrm{Spec}(\mathbb{Z})} - S$. Indeed, since V_S is normal it's well known that $\pi_1^{\text{ét}}(V_S)$ is $\mathrm{Gal}(K(V_S)^{\mathrm{ur},S}/K(V_S))$ where $K(V_S)$ is the function field of V_S and $K(V_S)^{\mathrm{ur},S}$ is the maximal extension of $K(V_S)$ unramified outside the primes of S. This is *precisely* the definition of $G_{\mathbb{Q},S}$. Indeed, $K(V_S) = \mathbb{Q}$ and then $K(V_S)^{\mathrm{ur},S} = \mathbb{Q}^S$.

Thus, we can rewrite (21) as

$$G_{\mathbb{Q}} \cong \varprojlim \pi_1^{\text{ét}}(V_S) \tag{22}$$

which then provides a semi-convincing argument for why one might analogize $\pi_1^{\acute{e}t}(V_S)$ and $\pi_1^{\acute{e}t}(U_S)$. This, in turns, then explains why one might then analogize V_S and U_S. From where then one can make the jump to analogizing $\mathbb{P}^1_{\mathbb{C}}$ to $\overline{\mathrm{Spec}(\mathbb{Z})}$ fairly easily.

One might then imagine that for a fixed place v of $\mathbb{Q}$ that the analogy of $\mathbb{Q}_p$ for $\mathbb{C}(T)$ should be the completion of $\mathbb{C}(T)$ under that place. Specifically, the (finite) places of $\mathbb{C}(T)$ are the valuations v_p corresponding to the points $p \in \mathbb{P}^1_{\mathbb{C}}$ and the completion of $\mathbb{C}(T)$ at this place is $\mathbb{C}(\!(T)\!)$ (or $\mathbb{C}(\!(T-p)\!)$ if we're trying to emphasize p). But, we discussed in the last section why D_p was like $\mathrm{Spec}(\mathbb{C}(\!(T)\!))$ and thus we see that this gives a fairly convincing argument as to why $\mathrm{Spec}(\mathbb{Q}_p)$ is like D_p. Thus, they should have the same étale fundamental groups, which shows that $\widehat{\pi_1(D_p)} = \pi_1^{\acute{e}t}(D_p)$ is like $\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}_p)) = G_{\mathbb{Q}_p}$. Of course, in the last section explained why it was, perhaps, more enlightening to think about the analogy that D_p is like $\mathrm{Spec}(\mathbb{Q}_p^{\mathrm{ur}})$ and then, by taking fundamental groups, we obtain the analogy between $\widehat{\pi_1(D_p)}$ and $\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}_p^{\mathrm{ur}})) = I_{\mathbb{Q}_p}$ as in our table.

Hopefully the reader will take this slightly enhanced version of the last section as even further justification for why the analogy we've been making is an apt one.

3.3 A more 'advanced' justification

A lot of the above intuitive justification seems fair, but has one (as far as I can see) major hole in its logic. Namely, when thinking about obtaining the 'local difficulty of' $\widehat{\pi_1(U_S)}$ 'at p' we really were computing something like

$$\varinjlim_{V} \widehat{\pi_1(V)} \tag{23}$$

as V traveled the neighborhoods of p in the complex topology. Indeed, the point we made earlier is that this is just, essentially, computing the fundamental group of a punctured disk since these punctured disks form a cofinal system of these V's and that the maps between the fundamental groups of these disks are isomorphisms—this is a rigorous phrasing of why 'how small we made the disk' didn't matter.

Now, the usual/natural replacement for the complex topology on schemes is the étale topology. Thus an extremely natural way of trying to analogize the study of the 'local geometry of $\mathbb{P}^1_{\mathbb{C}}$ at p' to the case of studying $G_{\mathbb{Q}}$ is to try and compute something like

$$\varinjlim_{(U,\overline{u})} \pi_1^{\acute{e}t}(U^*, \overline{v}) \tag{24}$$

where $(U, \overline{u})$ travel over pointed étale neighborhoods of $(V_S, \mathrm{Spec}(\overline{\mathbb{F}_p}))$ $\overline{v}$ is some geometric point of U^* (where V_S is in the last section, and $p \notin S$ is a prime (we're trying to be more careful with base points since we're going to make an actual formal statement) and U^* is U minus the image of $\overline{u}$ (we'll make an actual rigorous statement later that will undo any of the annoying details of this—just take it as intuition)

Now, if X is a scheme and $\overline{x}$ a geometric point of X then there is a name for the colimit $\varinjlim_{(U,\overline{u})} \mathcal{O}_U(U)$ as $(U, \overline{u})$ travels of the pointed étale neighborhoods of $(X, \overline{x})$. Namely, we call it the *strictly local ring of X at $\overline{x}$* and denote it $\mathcal{O}_{X,\overline{x}}$. Now then $\mathrm{Spec}(\mathcal{O}_{X,\overline{x}})$ should be like an 'arbitrarily étale zoomed in neighborhood around x' and $\mathrm{Spec}(\mathcal{O}_{X,\overline{x}})^*$ should be the result of 'removing x' from this—this should be the analogy of a small disk around p and a small punctured disk around p (since, again, at least on $\mathbb{P}^1_{\mathbb{C}}$ cofinal systems of neighborhoods/punctured neighborhoods where disks/puncutred disks). Thus, perhaps, the real, honest, correct analogue of studying $\widehat{\pi_1(D_p)}$ is studying $\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathcal{O}_{X,\overline{x}})^*, \overline{v})$ since, after all, this is the direct analogue of (23)—and this is 'more convincing' since the étale topology is well-known to be the 'correct topology' when thinking 'topologically' about schemes.

Let us make this somewhat more rigorous. Namely, if $(R, \mathfrak{m}, \kappa)$ is a local ring let us define a *Henselization* to be a Henselian local ring $(R^h, \mathfrak{m}^h, \kappa^h)$ together with a map of local rings $(R, \mathfrak{m}, \kappa) \to (R^h, \mathfrak{m}^h, \kappa^h)$ which is universal (i.e. its initial amongst maps of local rings from $(R, \mathfrak{m}, \kappa)$ to $(S, \mathfrak{n}, \eta)$ with S Henselian). Choose a separable closure $\kappa \hookrightarrow \kappa^{\mathrm{sep}}$ we call a local ring $(R^{sh}, \mathfrak{m}^{sh}, \kappa^{sh})$ a *strict Henselization* of $(R, \mathfrak{m}, \kappa)$ and $\kappa \hookrightarrow \kappa^{\mathrm{sep}}$ if given any other Henselian local ring $(S, \mathfrak{n}, \eta)$, a local map $(R, \mathfrak{m}, \kappa) \to (S, \mathfrak{n}, \eta)$, and an embedding $k^{\mathrm{sep}} \hookrightarrow \eta$ there is a unique factorization $(R^{sh}, \mathfrak{m}^{sh}, \kappa^{sh}) \to (S, \mathfrak{n}, \eta)$.

Now, one can show that $\mathcal{O}_{X,\overline{x}}$ is a local ring, and, moreover, that the natural map $\mathcal{O}_{X,x} \to \mathcal{O}_{X,\overline{x}}$ is local. If then one has chosen $\overline{x}$ to just be an embedding $\kappa(x) \hookrightarrow \kappa(x)^{\text{sep}}$ then one can show that the map $\mathcal{O}_{X,x} \to \mathcal{O}_{X,\overline{x}}$ realizes $\mathcal{O}_{X,\overline{x}}$ as a strict Henselization of $\mathcal{O}_{X,x}$.

Now, here's a non-trivial fact that one can show. Namely, if $X = \text{Spec}(R)$ with X a DVR then R^h is a DVR as well and $R^{sh} = \mathcal{O}_{(\text{Frac}R^h)^{\text{ur}}}$. In particular, choosing $X = V_S$ (as a above—a punctured Spec($\mathbb{Z}$)) and $p \in S$ an 'arbitrarily small étale small disk around' should be Spec($\mathbb{Z}^{sh}_{(p)}$) and an 'arbitrarily small étale *punctured* disk at p' should be Spec(Frac($\mathbb{Z}^{sh}_{(p)}$)) since Spec($\mathbb{Z}^{h}_{(p)}$) minus its closed point (corresponding to the center of the disk: p) is this spectrum. Thus, honestly, truly (given that the étale topology is the topology mimicking our usual notions of 'closeness') really the replacement for $\widehat{\pi_1^{\acute{e}t}(D_p)}$ should be $\pi_1^{\acute{e}t}(\text{Spec}(\text{Frac}(\mathbb{Z}^{h}_{(p)})) = G_{\text{Frac}(\mathbb{Z}^{sh}_{(p)})}$.

But, this might make us sad—this entire time we've been working under the assumption that the correct analogue of studying $\widehat{\pi_1(D_p)}$ for $G_{\mathbb{Q}}$ was studying $G_{\mathbb{Q}_p}$ but this (fairly solid) intuition strongly suggests that we should really be considering $G_{\text{Frac}(\mathbb{Z}^{sh}_{(p)})}$. So, have we erred? Have we made some grave misstep of intuition? Well, thankfully, no, not really (otherwise I wouldn't be writing this...).

To make these two notions commensurate we use the following beautiful fact:

Theorem 3.4: *Let R be a DVR with perfect residue field. Then, there is a natural isomorphism $G_{\text{Frac}(R^h)} \cong G_{\text{Frac}(\widehat{R})}$.*

This is not so difficult, but uses (and is largely immersed in) the study of Artin-Popescu approximation which, roughly, relates zeros of polynomials over R^h and over $\widehat{R}$.

In particular, Theorem 3.4 says, taking $R = \mathbb{Z}_{(p)}$, that $G_{\text{Frac}(\mathbb{Z}^{h}_{(p)})} \cong G_{\mathbb{Q}_p}$. Thus, using all of the above intuition we see that the correct analogue of $\widehat{\pi_1(D_p)}$, the group $G_{\text{Frac}(\mathbb{Z}^{sh}_{(p)})}$ is actually $G_{\mathbb{Q}_p^{\text{ur}}} = I_{\mathbb{Q}_p}$. It is not totally shocking that we're getting $I_{\mathbb{Q}_p}$ and not $G_{\mathbb{Q}_p}$ directly—in the case of $\mathbb{P}^1_{\mathbb{C}}$ the point we're zooming in on had no topology of its own whereas in the case of V_S the point Spec($\mathbb{F}_p$) does have topology, and precisely the difference between $\mathbb{Z}^{h}_{(p)}$ (whose fundamental group is just $G_{\mathbb{Q}_p}$) and $\mathbb{Z}^{sh}_{(p)}$ is that the latter ignores any interesting 'geometry' coming from the point Spec($\mathbb{F}_p$). Moreover, in practice, the difference between $G_{\mathbb{Q}_p}$ and $I_{\mathbb{Q}_p}$ is minimal since, as our credos mentioned, it's really $I_{\mathbb{Q}_p}$ that is the interesting/hard part of $G_{\mathbb{Q}_p}$.

3.4 An example of the intuition going another way

In all of the above we've tried to make analogies on the number theory side from facts we already knew on the topological side. To show a semi-robustness of the total analogy, let us, instead, try and go the other way—show a result on the topological side which is (perhaps) less known and is motivated by what is natural on the number theory side.

Namely, we made claims above that one should think about $\pi_1(D_p)$ as being the study of $G_{\mathbb{C}(T)}$ 'at p' and that it should be simpler since we've focused on just this one point. Let us try to make this somewhat precise. How we do so is influenced largely by what happens in the number theoretic case. This result will also make clear precisely what the geometric analogy of looking at $E_{\mathfrak{q}}/F_{\mathfrak{p}}$ is.

So, let us give the setup. Suppose that X is a compact (connected) Riemann surface—it is not strictly necessary to think only in the case of Riemann surfaces, but it certainly allows one to ignore some technical difficulties. Suppose further that that $\pi : Y \to X$ is a finite (connected) ramified cover of X. Recall that this means that there is some finite subset $S \subseteq X$ of *ramified points* such that if we consider $Y_S \to X_S$ where here (as usual) $X_S = X - S$ and $Y_S = \pi^{-1}(X_S)$ (where $\pi^{-1}(S)$ are the *branch points* of π) then we obtain an actual covering space. It is well-known Y has a unique structure of a compact (connected) Riemann surface such that π is holomorphic but, again, this is not strictly necessary knowledge for what we're doing. We'll assume further that $Y' \to X'$ is a Galois covering or, what amounts to the same thing, the field extension $K(Y)/K(X)$ is Galois.

Of course, the idea that we have in our head is that $Y \to X$ is like the map $\pi : \text{Spec}(\mathcal{O}_E) \to \text{Spec}(\mathcal{O}_F)$, for an extension of number fields E/F. The set $S \subseteq \text{Spec}(\mathcal{O}_F)$ is the set of ramified primes of L/K. Moreover, we know that $\pi : (\text{Spec}(\mathcal{O}_E) - \pi^{-1}(S)) \to (\text{Spec}(\mathcal{O}_F) - S)$ is a finite étale cover. Now, one of the natural things we considered in this setup was the decomposition group $D(\mathfrak{q} \mid \mathfrak{p})$ or, equivalently, (assuming the cover

was Galois), the image $\mathrm{Gal}(E_\mathfrak{q}/F_\mathfrak{p})$ under the image of the map $\mathrm{Gal}(E_\mathfrak{q}/F_\mathfrak{p}) \to \mathrm{Gal}(E/F)$. So, a natural question is what this corresponds to on the 'topological side'.

Now, since $\pi : Y' \to X'$ is a connected cover, we know that for any point $p \in X'$ the group $\mathrm{Aut}(Y'/X')$ acts simply transitively on $\pi^{-1}(p)$. In particular, if $\sigma \in \mathrm{Aut}(Y'/X')$ is such that $\sigma(q) = q$ for some $q \in \pi^{-1}(p)$ then $\sigma = \mathrm{id}$. That said, since $Y \to X$ is <u>not</u> a covering map, it is conceivable (and actually necessary as we'll soon see!) that $\sigma(q) = q$ for some branch point $q \in \pi^{-1}(S)$ and some $\sigma \in \mathrm{Aut}(Y/X)$. Thus, we might imagine that for a branch point $q \in \pi^{-1}(S)$ we could define a 'decomposition group' $D(q \mid p)$ to be those elements of $\mathrm{Aut}(Y/X)$ fixing q. So, what can we say about the structure of this group?

Well, let's recall that most natural way to study the group $D(\mathfrak{q} \mid \mathfrak{p})$ in the number theory side is to realize it was $\mathrm{Gal}(E_\mathfrak{q}/F_\mathfrak{p})$. What is the analogy here? Well, we already said that intuitively considering $F_\mathfrak{p}$ is like 'zooming in on' $\mathfrak{p}$ and thus, perhaps, we should start by zooming in on $p \in X$. In particular, let us choose a small enough disk D around p where, here, small enough is so that it contains no other ramified points of $\pi : Y \to X$ and, moreover, that $\pi^{-1}(D_p) \to D_p$ is a trivial cover where, here, $D_p := D - \{p\}$.

Now, if we imagine that D_p is like $F_\mathfrak{p}$ then what do we expect $\pi^{-1}(D_p)$ to look like? Well, note that since tensor product is pullback in algebraic geometry, the analogy of $\pi^{-1}(D_p)$ in the number theoretic world would be $F_\mathfrak{p} \otimes_F E$ which, as Theorem 2.8 tells us is precisely $\prod_{\mathfrak{q}\mid\mathfrak{p}} E_\mathfrak{q}$. Thus, we might imagine that $\pi^{-1}(D_p)$ should break up into pieces. Namely, we can think of each $E_\mathfrak{q}$ as being being the connected components of $F_\mathfrak{p} \otimes_F E$ (it's the connected components of the spectrum of this $F_\mathfrak{p}$-algebra), and so we might imagine that $\pi^{-1}(D_p)$ breaks up into natural pieces.

To make this slightly more clear, let us adapt our construction of the D and D_p slightly. Namely, let us take disjoint neighborhoods V_i of each branch point q_i lying over p so that $\pi\,|_{V_i}$ is (up to biholomorphic change of coordinates) $z \mapsto z^e$. Let us then let $D \subseteq X$ be a disk around p containing all the $\pi(V_i)$ and, finally, let $D_p := D - \{p\}$. Thus, while we have not made a substantive change to the above, the added precision of the construction now makes it clear that $\pi^{-1}(D_p)$ has connected components U_i corresponding to each point $q_i \in \pi^{-1}(p)$.

Now, since $\pi^{-1}(D)$'s connected components are like the connected components of $K\mathfrak{p} \otimes_F E$ we see that while D_p is like $F_\mathfrak{p}$ the extension $E_\mathfrak{q}/F_\mathfrak{p}$ is like the map $\pi : U_i \to D_p$ which, of course, is a connected cover. Thus, to create the analogy between $D(\mathfrak{q} \mid \mathfrak{p}) = \mathrm{Gal}(E_\mathfrak{q}/F_\mathfrak{p})$ we would like to make a claim such as $D(q_i \mid p)$ 'equals' $\mathrm{Aut}(U_i/D_p)$. But, this certainly needs justified.

For example, it's not immediately obvious why there should even be a map $\mathrm{Aut}(U_i/D_p) \to \mathrm{Aut}(Y/X) = \mathrm{Aut}(Y'/X')$. The key is that since Y'/X' is a Galois cover, given two points $y, y' \in \pi^{-1}(x)$ in the fiber of $x \in X'$ there is a *unique* element $\sigma \in \mathrm{Aut}(Y'/X')$ such that $\sigma(y) = \sigma(y;)$. So, if $\tau \in \mathrm{Aut}(U_i/D_p)$ we can then map it to $\sigma \in \mathrm{Aut}(Y'/X') = \mathrm{Aut}(Y/X)$ according to the rule that $\sigma(y) = \tau(y)$ for any point $y \in U_i$ (which, of course, is a point of $\pi^{-1}(x)$ with $x = \pi(y)$). By the above rule there is a unique such σ and, as one can check, this map is evidently an injective group map $\mathrm{Aut}(U_i/D_p) \hookrightarrow \mathrm{Aut}(Y'/X') = \mathrm{Aut}(Y/X)$.

We claim that the image of this map is precisely $D(q \mid p)$ which, of course, is what we'd expect from the case of number fields. To see this we note that since U_i/D_p is a connected cover we can *almost* reverse the process above. Namely, given $\sigma \in \mathrm{Aut}(Y'/X')$ it's tempting to say that it can be mapped to $\tau \in \mathrm{Aut}(U_i/D_p)$ by the rule $\tau(y) = \sigma(y)$ for any $y \in U_i$. Unfortunately, this process presupposes that $\sigma(y) \in U_i$ or, equivalently, that σ stabilizes U_i. That said, it's clear σ stabilizes U_i *precisely* when $\sigma \in D(q \mid p)$.

Thus, we can summarize the above as follows:

Theorem 3.5: *Let $\pi : Y \to X$ be a ramified cover of connected compact Riemann surfaces. For any ramified point $p \in X$ choose a D containing p subject to the condition that $\pi^{-1}(D)$ decomposes into neighborhoods U_i of each $q_i \in \pi^{-1}$ which, up to biholomorphisms, look like $z \mapsto z^e$ (as an endomorphism of the unit disk). Then, the connected components of $\pi^{-1}(D_p)$, where $D_p := D - \{p\}$ are precisely the U_i and the map $\mathrm{Aut}(U_i/D_p) \to \mathrm{Aut}(Y/X) = \mathrm{Aut}(Y'/X')$ as described above is injective with image precisely $D(q \mid p)$.*

Now, this theorem certainly hearkens to Theorem 2.11, strengthening our geometric intuition for what $E_\mathfrak{q}/F_\mathfrak{p}$ is like (it's like $U_i \to D_p$) and thus what studying the local 'geometry' at $\mathfrak{q}$ over $\mathfrak{p}$ in terms of $\mathrm{Gal}(E_\mathfrak{q}/F_\mathfrak{p})$ really means. But, it also allows us to give a nice conceptual proof of the following fact:

Corollary 3.6: *Let $\pi : Y \to X$ be as above. Then, for any points $q \in Y$ and $p = \pi(q) \in X$ the group $D(q \mid p)$ is cyclic of order $e(q \mid p)$.*

Proof: As Theorem 3.5 shows us, we're trying to show that $\mathrm{Aut}(U_i/D_p)$ is cyclic. That said, since $U_i \to D_p$ is a Galois cover of D_p, we know that $\mathrm{Aut}(U_i/D_p)$ is a quotient of $\pi_1(D_p, x)$ (for any point $x \in D_p$), but, of course, $\pi_1(D_p, x)$ is $\mathbb{Z}$, thus proving that $D(q \mid p)$ is cyclic. Since it acts simply transitively on a size of set $e(q \mid p)$ we see that it must be of order $e(q \mid p)$. ■

I find this to be a very nice, very conceptual proof of this result emphasizing the key idea: the simplicity of the local geometry of X' is reflected in the simplicity of the 'local groups $D(q \mid p) = \mathrm{Aut}(U_i/D_p)$'. Moreover, and perhaps this is my failing as an amateur topologist, I actually didn't know an obvious/conceptual way of thinking about Corollary 3.6 without attacking through Theorem 3.5 which I only happened upon by the number field/topology analogy.

3.5 The geometric reason P_K is hard

In this last section I'd just like to give an example of how wild ramification makes geometry hard. Namely, after the last few sections it seems plausible to have geometric intuition for some of the difficulty in studying $G_{\mathbb{Q}_p}$ and, as our credo says, this would really be geometric intuition about why P_K is difficult—about why wild ramification is difficult.

So, how can we see explicitly how wild ramification can mess with our geometry—how wild ramification can make the geometry more difficult? Well, unfortunately, we can't see this directly through the analogy between $G_{\mathbb{C}(T)}$ and $G_{\mathbb{Q}}$ since, unfortunately, the former has no wild ramification. We need to go a closer comparision to $G_{\mathbb{Q}}$, somehow an interpolation between $G_{\mathbb{C}(T)}$ and $G_{\mathbb{Q}}$—we need to talk about $G_{\mathbb{F}_p(T)}$. This simulatenously has a natural connection to geometry since $\mathbb{F}_p(T)$ is the function field of $\mathbb{P}^1_{\mathbb{F}_p}$ (although not nearly as nice as $\mathbb{C}(T)$ where we could interpret things in a literal, topological notion when we said "geometric"), but also has many of the arithmetic subtleties present in $\mathbb{Q}$.

So, let's go forward as we have been doing. Namely, let's try and write down the analogy of (1) and (21) for $G_{\mathbb{F}_p(T)}$. Specifically we get the following:

$$G_{\mathbb{F}_p(T)} = \varprojlim_{S \subseteq \mathbb{P}^1_{\mathbb{F}_p}} \pi_1^{\acute{e}t}(W_S) \tag{25}$$

where, here, for $S \subseteq \mathbb{P}^1_{\mathbb{F}_p}$ finite we set $W_S = \mathbb{P}^1_{\mathbb{F}_p} - S$. One might then imagine that since W_S is very geometric, that computing $\pi_1^{\acute{e}t}(W_S)$ might be easy. I mean ,$U_S \subseteq \mathbb{P}^1_{\mathbb{C}}$ was very geometric and it was precisely this geometric interpretation that led to the incredibly simple description $\pi_1^{\acute{e}t}(U_S) = \widehat{F_n}$ if $n = \#S - 2$. Unfortunately, this is not the case.

But, and this is the important thing I want to emphasize in this section, is that what stops the computation of $\pi_1^{\acute{e}t}(W_S)$ from being simple, what impedes the geometry of curves of W_S, is *precisely* wild ramification. In fact, as we'll momentarily see the exact same sort of geometric thinking that computes $\pi_1^{\acute{e}t}(U_S)$ goes through (essentially untouched) to computing the covers of W_S for which wild ramification doesn't meddle (in a way we'll soon make precisely).

In particular, I'd like to focus on what might be, perhaps, the simplest case of this. Namely, let's consider $S = \{\infty\}$ so that $W_S = \mathbb{A}^1_{\mathbb{F}_p}$. Then, we'll see that simple geometric considerations will imply that a finite étale cover $X \to \mathbb{A}^1_{\mathbb{F}_p}$ is geomtrically trivial if, at one point in our discussion, we can assume that a map is tamely ramified. In particular, we will see that it's precisely wild ramification that is going to gum up our geometric machinations.

So, what we really interesting in studying is connected finite étale covers $X \to \mathbb{A}^1_{\mathbb{F}_p}$ So,to this end, let $\overline{X}$ denote the natural smooth projective integral compactification of X (note that X is a smooth integral affine curve so we can do this) and consider the induced map $\overline{X} \to \mathbb{P}^1_{\overline{\mathbb{F}_p}}$. If we can show that this is finite étale then we're done since $\pi^1_{\acute{e}t}(\mathbb{P}^1_{\overline{\mathbb{F}_p}}) = 0$ (which follows trivially from Riemann-Hurwitz).

Now, let's think about what Riemann-Hurwitz says about the map $\overline{X} \to \mathbb{P}^1_{\overline{\mathbb{F}_p}}$ (which is separable, since it's generically étale, so that Riemann-Hurwitz applies). Namely, it says that

$$2(g(\overline{X}) - 1) = -2n + \deg(\Omega_{X/Y}) \tag{26}$$

Now, note ∞ is the only point of $\mathbb{P}^1_{\overline{\mathbb{F}_p}}$ that can ramify (since it's étale over $\mathbb{A}^1_{\overline{\mathbb{F}_p}}$) and so

$$\deg(\Omega_{X/Y}) = \sum_{x \mapsto \infty} (e_x - 1) \tag{27}$$

where e_x is literally the ramification of x. But, note that

$$\sum_{x \mapsto \infty} (e_x - 1) = \sum_{x \mapsto \infty} e_x - \#\{x \mapsto \infty\} = n - \#x \mapsto \infty$$

and thus putting this into (26) gives

$$2(g(\overline{X}) - 1) = -n - \#\{x \mapsto \infty\}$$

but since $\#\{x \mapsto \infty\} \leqslant n$ the only way this equality could happen is if $g(\overline{X}) = 0$, $n = 1$, and $\#\{x \mapsto \infty\} = 1$. But, this implies precisely that $X \to \mathbb{A}^1_{\overline{\mathbb{F}_p}}$ is an isomorphism as desired.

But, what I've just told you is a lie. For example, $t \mapsto t^p - t - 1$ is a non-trivial finite étale cover $\mathbb{A}^1_{\overline{\mathbb{F}_p}} \to \mathbb{A}^1_{\overline{\mathbb{F}_p}}$. So, where did we go wrong above? We just did nice old geometry, so pure, so simple that we couldn't have made a mistake, right? Well, this is the nastiness of wild ramification.

Namely, we have the following result showing precisely where we screwed up above, and why the culprit was wild ramification:

Theorem 3.7: *Let $f : X \to Y$ be as separable map of smooth, projective, integral curves over k (an algebraically closed field). Then,*

$$\deg(\Omega_{X/Y}) \geqslant \sum_{x \in X} (e_x - 1)$$

with equality if and only if f is tamely ramified.

We thus see that the fatal lie in the above was that $\deg(\Omega_{X/Y})$ is $\sum_{x \mapsto \infty} (e_x - 1)$.

Thus, we see that tame ramification messes with our geometry—it screws up our usually neat geometric formulas and turns them into something which is much harder to use. This is a good geometric intuition about why our credo is correct.