STRUCTURE THEORY OF LOCAL FIELDS

PETE L. CLARK

Contents

4. Structure Theory of CDVFs 1
4.1. Serre's Kummer-Dedekind Criterion 3
4.2. Unramified extensions 3
4.3. Totally ramified extensions and Eisenstein's Criterion 4
4.4. Tamely ramified extensions 5
4.5. Wildly ramified extensions 6
4.6. More on the PGM Filtration 6

4. Structure Theory of CDVFs

We now specialize to the following situation: let $(K, |\ |)$ be a complete, non-Archimedean field whose valuation ring R is a DVR and whose residue field k is perfect. Under these hypotheses we can give a much more penetrating analysis of the structure of the absolute Galois group $\mathfrak{g}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and also of the multiplicative group $K^\times$.

Recall that a finite extension L/K is **unramified** if $e(L/K) = 1$; equivalently, $f(L/K) = [L : K]$. (Note that we are using our assumption of the perfection of k here, for otherwise we would need to add the condition that the residual extension l/k is unramified.) An algebraic extension L/K is unramified if all of its finite subextensions are unramified.

A finite extension L/K is **totally ramified** if $e(L/K) = [L : K]$; equivalently, $l = k$. An algebraic extension L/K is totally ramified if each finite subextension if totally ramified; equivalently, $l = k$.

Let p be the characteristic exponent of the residue field k. (In other words, when k has positive characteristic, we take p to be the characteristic; when k has characteristic 0, we take $p = 1$.)

Here is a new definition: a finite extension L/K is **tamely ramified** if $e(L/K)$ is prime to p. An algebraic extension is tamely ramified if every finite subextension is tamely ramified. Note that in particular every unramified extension is tamely ramified, so perhaps more accurate terminology would be "at worst tamely ramified", but the terminology we have given is standard. Note also that if $\mathrm{char}(k) = 0$ then *every algebraic extension* of K is tamely ramified.

An extension L/K is **totally tamely ramified**, or **TTR**, if it is both totally ramified and tamely ramified.

Both unramified and tamely ramified extensions are **distinguished** classes of field extensions in the sense of Lang, as we now explain. A class of field extensions $\mathcal{C} = \{L/K\}$ is said to be distinguished if it satisfies the following two conditions:

(DE1) (Tower condition): if K/F and L/K are both in $\mathcal{C}$, then L/F is in $\mathcal{C}$.
(DE2) (Base change condition): suppose E, F, K are subfields of a common field, and $F \subset K$, $F \subset E$ and $K/F \in \mathcal{C}$. Then $EK/E \in \mathcal{C}$.

Exercise 4.1: Show that from (DE1) and (DE2) we have the following formal consequence:

(DE3) Suppose K, L_1, L_2 are subfields of a common field, with K contained in both L_1 and L_2 and that $L_1/K,\ L_2/K \in \mathcal{C}$. Then $L_1L_2/K \in \mathcal{C}$.

Examples: finite extensions; separable extensions; purely inseparable extensions; finitely generated extensions; purely transcendental extensions.

Important non-examples: normal extensions, Galois extensions: they satisfy (DE2) but not (DE1).

Now we state some of the main results we will prove later in this chapter.

Theorem 1. *Let K be a CDVF with perfect residue field k. Inside the class of all algebraic extensions of K, we have*
a) The class of unramified extensions is a distinguished class.
b) The class of tamely ramified extensions is a distinguished class.

Note that the tower property of unramified and tamely ramified extensions follows directly from the definition, since ramification indices multiply in towers. The base change property is less obvious, and for this we will need more explicit information about the structure of unramified and tamely ramified extensions, coming up soon!

Example: Totally ramified and totally tamely ramified extensions need *not* form a distinguished class. For instance, let $K = \mathbb{Q}((x))$, let $n \geq 3$, and consider the Eisenstein polynomial $f(t) = t^n - x$. The extension $L = K[t]/(f)$ is totally tamely ramified. It is (of course) separable, but it is not normal: rather, the normal closure is $M = K(x^{\frac{1}{n}}, \zeta_n)$, which contains the nontrivial unramified extension $K(\zeta_n)/K$.

Because the unramified extensions form a distinguished class, there is a unique maximal unramified extension – namely, the compositum of all finite degree totally unramified extensions, K^{unr}. The residue field of K^{unr} is $\overline{k}$. The extension $K^{\mathrm{sep}}/K^{\mathrm{unr}}$ is (necessarily) Galois and totally ramified. The extension K^{unr}/K is also Galois. Moreover, we have a short exact sequence of Galois groups

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \xrightarrow{\rho} \mathrm{Gal}(\overline{k}/k) \to 1.$$

The map ρ is defined as follows: since every element $\sigma \in \mathfrak{g}_K$ is continuous, it preserves the valuation ring R and also the maximal ideal $\mathfrak{m}$ and therefore induces an automorphism $\rho(\sigma)$ of $R/\mathfrak{m}$. This short exact sequence follows from passage to the limit of the special case of the inertia group / decomposition group / residual extension short exact sequence that we get from a finite Galois extension S/R of Dedekind domains and primes $\mathcal{P}|\mathfrak{p}$. See e.g. XXXX for details.

Similarly, because the tamely ramified extensions form a distinguished class, there is a unique maximal tamely ramified extension, K^{tame} of K, which is Galois over K. This gives rise to a short exact sequence of Galois groups

$$1 \to \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \to \mathrm{Gal}(K^{\mathrm{tame}}/K) \to \mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathfrak{g}_K \to 1.$$

In fact, the group $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$ is the easiest to understand.

Theorem 2. *We have* $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

This will also follow from the structure theory of tamely ramified extensions.

An extension is called **wildly ramified** if it is not tamely ramified. The remaining piece of the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}})$ describes the "purely wildly ramified" extensions. In general, this is the most complicated and scariest part of the absolute Galois group of a CDVF, but there is one important fact which comes for free:

4.1. **Serre's Kummer-Dedekind Criterion.**

Let R be a DVR with maximal ideal $\mathfrak{m}$ and residue field k. Let $n \in \mathbb{Z}^+$ and $f \in R[t]$ a monic degree n polynomial. Let $S_f = R[t]/(f)$. (We shall try to reserve t for an indeterminate and write $\bar{t}$ for the image of t in S_f.) Then S_f is a one-dimensional semi-local ring, and the determination of its maximal ideals is a variant on the Kummer-Dedekind criterion from classical number theory.

Proposition 3. *(Serre) Let* $\overline{S}_f = S_f/\mathfrak{m}S_f = R[t]/(\mathfrak{m}, f) = k[t]/(\overline{f})$. *Factor* $\overline{f}$ *over* $k[t]$ *as* $\overline{f} = \prod_{i=1}^g \overline{f}_i^{e_i}$. *Lift each* $\overline{f_i}$ *to a monic polynomial* $f_i \in R[t]$. *Put* $\mathfrak{m}_i = \langle \mathfrak{m}, f_i \rangle$. *Then the* $\mathfrak{m}_i$*'s are the distinct maximal ideals of* S_f, *and* $S_f/\mathfrak{m}_i \cong k[t]/(g_i)$.

Proof. Serre, *Local Fields*, p. 18. (To be added to these notes shortly. □

4.2. **Unramified extensions.**

Let us come at things from a slightly different perspective. Suppose L/K is any finite extension. We know it induces a residue extension l/k. Since we are assuming k is perfect, l/k is finite separable, and may therefore be written as $l = k[t]/\overline{f}$ for a monic irreducible $\overline{f}$. Now lift $\overline{f}$ to a monic polynomial $f \in R[t]$. f is certainly irreducible in $R[t]$; by Gauss's Lemma it is also irreducible in $K[t]$. Therefore we may form an extension $L' = K[t]/(f)$. It follows from Hensel's Lemma that L' is a subextension of L/K. What we would like to show is that the residual extension l'/k is simply l/k: it follows that L' is unramified and is the maximal unramified subextension of L/K. The following consequence of Serre's Lemma gives this and a bit more.

Proposition 4. *With the same hypotheses as in Serre's Lemma, assume* $\overline{f}$ *is irreducible, and put* $L = K[t]/(f)$, *so* L *is a field extension. Then* S_f *is the integral*

closure S of R in L. It has maximal ideal $\mathfrak{m}S$ and residual extension $k[t]/(\overline{f})$. In particular, L/K is unramified.

Proof. By Serre's Lemma, S_f is local with maximal ideal $\mathfrak{m}S_f$ and residue field $k[t]/\overline{f}$. Moreover, let π be a generator for $\mathfrak{m}$. Then the image of π in S_f generates $\mathfrak{m}S_f$ and is not nilpotent. It follows that S_f is a DVR. In particular, S_f is an integrally closed integral extension of R with fraction field L, hence it *is* the integral closure S of R in L. The rest follows from Serre's Lemma. □

Conversely, to every finite extension $l = k[t]/(\overline{f})$ of k, we may lift to a monic $f \in R[t]$ and then the previous proposition shows that $L = K[t]/(f)/K$ is unramified with residual extension l/k. Thus we get a bijective correspondence between unramified extensions of K and algebraic extensions of k.

Note though that we established a little more than this: we get that if L/K is unramified, then S is monogenic as an R-module. In fact we did not use the completeness here, because the existence of a unique prime of S lying over $\mathfrak{m}$ follows from $[l : k] = [L : K]$, so this holds for any unramified extension of a DVF.

Corollary 5. *The unramified extensions of a CDVF form a distinguished class.*

Proof. As mentioned above, it is immediate that if M/L and L/K are unramified, so is M/K. Conversely, suppose K is a CDVF field, L/K is unramified and E/K is any algebraic extension. Then we must show that LE/E is unramified. By the classificaiton of unramified extensions, an algebraic extension is unramified iff it is generated by the lifts to the valuation ring of roots of separable polynomials over k. Certainly this property is preserved by base change, so the proof is complete. □

4.3. **Totally ramified extensions and Eisenstein's Criterion.**

Proposition 6. *Let R be a DVR with maximal ideal $\mathfrak{m}$ and residue field k. $f = t^n + a_{n-1} + \ldots + a_1 t + a_0 \in R[t]$, $a_i \in \mathfrak{m}$, $a_0 \notin \mathfrak{m}^2$. Then S_f is a DVR with maximal ideal generated by the image of t and with residue field k. Thus, if L is the fraction field of S_f, then L/K is totally ramified.*

Proof. Upon reducing modulo $\mathfrak{m}$, we have $\overline{f} = t^n$. By Serre's Lemma, S_f is a local ring with maximal ideal $\langle \mathfrak{m}, t \, rangle$. Moreover, the hypotheses give us that a_0 is a uniformizer of R. Let us write $\bar{t}$ for the image of t in the quotient ring $S_f = R[t]/(f)$. Then we have

$$-a_0 = \bar{t}^n + a_{n-1}\bar{t}^{n-1} + \ldots + a_1\bar{t},$$

so $a_0 \in (\bar{t})$. Therefore $\langle \mathfrak{m}, \bar{t} \rangle = \langle a_0, \bar{t} \rangle = \langle \bar{t} \rangle$. That is, S_f is a local ring with a principal maximal ideal. Since a_0 is not nilpotent, neither is $\bar{t}$, so S_f is a DVR. The rest follows immediately. □

As above in the unramified case, we deduce:

Corollary 7. *An Eisenstein polynomial $f(t)$ is irreducible in $K[t]$, and if $L := K[t]/(f)$, $S_f = S$, the integral closure of R in L.*

Conversely:

Theorem 8. *Let R be a DVR with fraction field K, L/K a degree n field extension, S the integral closure of R in L. Suppose S is a DVR and $n = e(L/K) = [L : K]$. Let π be a uniformizer of S, and let $f(t)$ be the characteristic polynomial of π over K (also the minimal polynomial, since f is necessarily irreducible). Then f is an Eisenstein polynoimal and the homomorphism $R[t] \to S$ mapping $t \mapsto \pi$ induces an isomorphism $S_f \xrightarrow{\sim} S$.*

Proof. Simple integrality considerations show that $f \in R[t]$. Let us write

$$f = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0, \ a_i, a_n = 1 \in R.$$

(The reason for writing out a_n when it is equal to 1 will become clear shortly.) Evaluating at π, we get

$$a_n \pi^n + \ldots + a_0 = 0.$$

Let w be the normalized discrete valuation assocated to S, i.e., such that $w(\pi) = 1$. Then because of total ramification, we have $w(a) \equiv 0 \pmod{n}$ for all $a \in R$.

Put $r = \inf_{0 \le i \le n} w(a_i \pi^{n-i})$. By the Domination Principle, we must have a tie: i.e., there necessarily exist $i < j$ such that

$$r = w(a_i \pi^{n-i}) = w(a_i) + n - i = w(a_j \pi^{n-j}) = w(a_j) + n - j,$$

so that $j - i \equiv 0 \pmod{n}$. But this forces $i = 0$, $j = n$, $r = n$, $w(a_0) = n$ and $w(a_i) = n - i$ for all $i \ge 1$, so indeed f is Eisenstein. □

4.4. **Tamely ramified extensions.**

Theorem 9. *Let L/K be totally tamely ramified, with $[L : K] = e(L/K) = e$. Then there exists a uniformizer π of K and a uniformizer Π of L such that $\Pi^e = \pi$. In particular, $L = K[t]/(t^e - \pi)$.*

Proof. Lang, *Algebraic Number Theory*, pp. 52-53. To be added to these notes shortly. □

Corollary 10. *The tamely ramified extensions of a CDVF form a distinguished class.*

Proof. Since both unramified extensions and totally tamely ramified extensions have the tower property, so do tamely ramified extensions. It remains to see that the base change of a tamely ramified extension is tamely ramified. Again, by splitting a tamely ramified extension into an unramified extension followed by a totally tamely ramified extension, it suffices to show that the base change of a totally tamely ramified extension is tamely ramified. In view of Theorem 1, we must show that if E/K is any algebraic extension and π is any uniformizer of K, then for any e prime to the residue characteristic p (which we may assume to be positive, otherwise there is nothing to show), the extension $E(\pi^{\frac{1}{e}})/E$ is tamely ramified. Here we need to be a bit careful: by $\pi^{\frac{1}{e}}$ we mean *any root* of the separable polynomial $t^e - \pi$ in $\overline{K}$. In fact it is easier (and sufficient!) to see that the extension $E(\pi^{\frac{1}{e}}, \zeta_e)/E$ is tamely ramified, for this is a Galois extension, namely the splitting field of $t^e - \pi$. As we have seen, adjoining the eth roots of unity gives an unramified extension, and then once we have the eth roots of unity in the ground field, Kummer theory applies to show that $[E(\pi^{\frac{1}{e}}, \zeta_e) : E(\zeta_e)]$ is the order of π in $E^\times / E^{\times e}$, hence divisible by e and therefore prime to p. □

Theorem 11. *Suppose that K is a Henselian DVF with* ***algebraically closed*** *residue field k of characteristic exponent p. Then there exists, for each positive integer e prime to p, a unique degree e tamely ramified extension L_e/K, obtained by taking the eth root of any uniformizing element of K. Moreover, $K^{\mathrm{tame}} = \bigcup_e L_e$ and $\mathrm{Gal}(K^{\mathrm{tame}}/K) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.*

Proof. Our assumption $k = \overline{k}$ implies that K contains all roots of unity of order prime to p and also that all extensions are totally ramified, so any tamely ramified extension is totally tamely ramified. Thus Theorem XX applies to show that every degree e tamely ramified extension L/K is of the form $K[\pi^{\frac{1}{e}}]$ for some uniformizer π of K. Conversely, for any uniformizer π we certainly do get a degree e (hence tamely ramified) extension in this way. So what we wish to show is that for any two uniformizers π and π' we have $K[\pi^{\frac{1}{e}}] = K[\pi'^{\frac{1}{e}}]$. By basic Kummer theory, this occurs iff $\pi \cong \pi' (\mod K^{\times e})$. However, since k is algebraically closed, every element of $k^\times$ is an eth power. The usual Hensel's Lemma argument now shows that every unit in the valuation ring of K is an eth power, in particular π/π' is an eth power. Now let $L_e = K[\pi^{\frac{1}{e}}]$ be the unique degree e extension of K. Again by basic Kummer theory, we have $\mathrm{Gal}(L_e/K) \cong \mathbb{Z}/e\mathbb{Z}$. If $e \mid e'$ then we have natural surjections $\mathrm{Gal}(L_{e'}/K) \to \mathrm{Gal}(L_e/K)$, and one easily checks that the following diagram commutes,

$$\begin{array}{ccc} \mathrm{Gal}(L_{e'}/K) & \xrightarrow{\sim} & \mathbb{Z}/e'\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L_e/K) & \xrightarrow{\sim} & \mathbb{Z}/e\mathbb{Z}, \end{array}$$

where the second vertical map is the usual quotient. It follows that $\mathrm{Gal}(K^{\mathrm{tame}}/K) \cong \varprojlim \mathbb{Z}/e\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell$. □

Corollary 12. *Supose that K is a Henselian DVF with perfect residue field k of characteristic exponent p. Then there exists, for each positive integer e prime to p, a unique degree e tamely ramified extension L_e/K^{unr}, obtained by taking the eth root of any uniformizing element of K^{unr}. Moreover,$K^{\mathrm{tame}} = \bigcup_e L_e$ and $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.*

Exercise X.X: Prove Corollary X.X. (This is just a check on your understanding of unramified extensions.)

4.5. **Wildly ramified extensions.**

Theorem 13. *The wild ramification group $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}})$ is a pro-p-group.*

Indeed, every finite quotient is purely wildly ramified, therefore has p-power order.

4.6. **More on the PGM Filtration.**

To summarize, let K be a Henselian, discretely valued field. Then we have split up the Galois extension K^{sep}/K into three pieces by introducing K^{unr}/K, the maximal unramified extension and $K^{\mathrm{tame}}/K^{\mathrm{unr}}$, the maximal totally tamely ramified extension. Corresponding to the tower $K^{\mathrm{sep}}/K^{\mathrm{tame}}/K^{\mathrm{unr}}/K$ we get a **filtration** by normal subgroups

$$1 \subset \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}}) \subset \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{unr}}) \to \subset \mathrm{Gal}(K^{\mathrm{sep}}/K).$$

There are useful things to say about each of the successive quotients of this filtration.

The bottom piece of the filtration is $\mathrm{Gal}(K^{\mathrm{unr}}/K)$. As we showed in §X.X, reduction modulo the maximal ideal gives a canonical isomorphism from this group to the absolute Galois group $\mathfrak{g}_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ of the residue field k. In particular, if k is finite, then via the Frobenius automorphism we have canonically $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \hat{Z}$, a very well understood group.

The middle piece of the filtration is $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$, which is the maximal tamely ramified extension *of* K^{unr}. As we discussed, we have a noncanonical isomorphism $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

The top piece $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}})$ is trivial if $\mathrm{char}(k) = 0$ and is an infinite pro-p-group if $p > 0$: indeed for any uniformizer π of K and all $n \in \mathbb{Z}^+$, the polynomial $t^{p^n} - \pi$ is Eisenstein and hence the corresponding extension has ramification index p^n, so the polynomial remains irreducible over K^{tame}.

We list some immediate consequences of this analysis of the filtration.

Theorem 14. *The absolute Galois group $\mathfrak{g}_K$ is pro-solvable iff the absolute Galois group $\mathfrak{g}_k$ of the residue field is pro-solvable. In particular, this occurs when the residue field k is finite.*

Theorem 15. *Let $K = \mathbb{C}((t))$. Then the algebraic closure of K is the Puiseux series field $\bigcup_{n \in \mathbb{Z}^+} K(t^{\frac{1}{n}})$ and $\mathfrak{g}_K \cong \hat{\mathbb{Z}}$.*

Proof. Indeed, since the residue field is algebraically closed, $K^{\mathrm{unr}} = K$. Moreover, since the residue characteristic is zero, there are no wildly ramified extensions: $K^{\mathrm{sep}} = \overline{K} = K^{\mathrm{tame}}$. Therefore $\mathrm{Gal}(\overline{K}/K) = \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) = \prod_\ell \mathbb{Z}_\ell = \hat{\mathbb{Z}}$. □

Now let us go a little deeper and determine the action of $\mathfrak{g}_k$ on $\prod_{\ell \neq p} \mathbb{Z}_\ell$. First we recall the general procedure for obtaining such an action: let A be a commutative normal subgroup of a group G, with quotient Q:

$$1 \to A \to G \xrightarrow{q} H \to 1.$$

Then we can define a homomorphism $\rho : H \to \mathrm{Aut}(A)$ as follows: take $h \in H$, lift to any $\tilde{h}$ in G, and define $\rho(h)(a) = \tilde{h} a \tilde{h}^{-1}$. First note that the given element maps under the quotient map q to $hq(a)h^{-1} = h \cdot 1 \cdot h^{-1} = 1$, so indeed $\rho(h)(a) \in A$. Second note that it is well-defined indepedent of the choice of lift $\tilde{h}$: indeed, any other lift would differ by an element of A, and since A is abelian, conjugation by an element of A is trivial.

Now we identify the $\mathfrak{g}_k$ action on $\prod_{\ell \neq p} \mathbb{Z}_\ell$. First we recall that for any n prime to p, the reduction map identifies the nth roots of unity in K^{unr} with the nth roots of unity in k^{sep}, of which there will be precisely n (since n is prime to p). In other words, the abelian groups $\mu_n(K^{\mathrm{unr}})$ and $\mu_n(k^{\mathrm{sep}})$ are isomorphic as Galois modules. For any $\ell \neq p$, let $\mathbb{Z}_\ell(1) = \lim_{n \to \infty} \mu_{\ell^n}(K^{\mathrm{unr}})$. As an abelian group, this is isomorphic to $\mathbb{Z}_\ell$, but it has a generally nontrivial $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathfrak{g}_k$-module structure. We may also form the Galois module $\prod_{\ell \neq p} \mathbb{Z}_\ell$ which is the inverse limit over all finite prime to p roots of unity.

We pause for some important terminology. For any field K of characteristic different from p, the Galois action on the inverse limit of ℓ-power roots of unity gives a

homomorphism

$$\mathfrak{g}_K \to \mathrm{Aut}(\mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^\times.$$

This homomorphism is called the (ℓ-adic) **cyclotomic character** and often denoted χ_ℓ. It is the first nontrivial example of a Galois representation. When K has characteristic 0, it is traditional to compile all the ℓ-adic characters together to get one representation

$$\chi : \mathfrak{g}_K \to \mathrm{Aut}(\prod_\ell \mathbb{Z}_\ell) = \mathrm{Aut}(\hat{\mathbb{Z}}) = \hat{\mathbb{Z}}^\times,$$

again called the cyclotomic character. A more down to earth description of this character is as follows: for any $n \in \mathbb{Z}^+$, its image in $(\mathbb{Z}/n\mathbb{Z})^\times$ may be calculated by choosing a primitive nth root of unity ζ_n and writing

$$\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}.$$

Theorem 16. *In the extension*

$$1 \to \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \to \mathrm{Gal}(K^{\mathrm{tame}}/K) \to \mathfrak{g}_k \to 1,$$

the action of $\mathfrak{g}_k$ *on* $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$ *is precisely as the prime to* p *cyclotomic character. We indicate this by writing* $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{sep}}) = \prod_{\ell \neq p} \mathbb{Z}_\ell(1)$. *Moreover, this extension splits (noncanonically) as a semidirect product:*

$$K^{\mathrm{tame}} = \prod_{\ell \neq p} \mathbb{Z}_\ell(1) \rtimes_\chi \mathfrak{g}_k.$$

Exercise: Prove Theorem X.X. (Hint for the splitting:[1] choose a uniformizer π and a compatible system of eth roots of π.)

Here is a not quite standard application of these ideas.

Theorem 17. *Let* $K = \mathbb{C}((t_1))((t_2))$. *Then* $\mathfrak{g}_K \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$.

Proof. Since the residue characteristic is 0, we have $K^{\mathrm{sep}} = K^{\mathrm{tame}}$ hence a short exact sequence

$$1 \to \prod_\ell \mathbb{Z}_\ell(1) \to \mathfrak{g}_K \to \hat{\mathbb{Z}} \to 1.$$

By Corollary X.X, the sequence splits and $\mathfrak{g}_K = \hat{\mathbb{Z}} \ltimes \hat{\mathbb{Z}}$. But moreover the semidirect product is given by a homomorphism $\rho : \hat{Z} \to \mathrm{Aut}(\hat{\mathbb{Z}})$ which is nothing else than the cyclotomic character on the Galois group of the residue field $\mathbb{C}((t_1))$. But the residue field contains $\mathbb{C}$ and hence all roots of unity, and therefore the cyclotomic character is trivial, ρ is trivial, and the product is direct. □

Remark: An easy induction argument gives that the absolute Galois group of an iterated Laurent series field in n variables over $\mathbb{C}$ (or any algebraically closed field of characteristic 0) is isomorphic to $\hat{\mathbb{Z}}^n$.

Corollary 18. *When* $K = \mathbb{Q}_p$, *the Galois group* $\mathrm{Gal}(K^{\mathrm{tame}}/K$ *is isomorphic to the profinite completion of the discrete group*

$$\mathcal{T} = \langle \sigma, \tau \mid \varphi, \tau \mid \varphi\tau\varphi^{-1} = \tau^p \rangle.$$

Exercise: Prove Corollary X.X. (Suggestion: c.f. my notes on Local Fields.)

[1] Thanks to Brian Conrad.

Corollary 19. *Suppose that $\mathfrak{g}_K \cong \hat{\mathbb{Z}}$. Then the extension*

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \to \mathfrak{g}_k \to 1$$

splits (noncanonically) as a semidirect product. Equivalently, there exists a (nonunique!) extension L/K such that (i) L/K is totally ramified and (ii) K^{sep}/L is unramified.

Proof. This is the profinite analogue of the fact that a short exact sequence $1 \to A \to G \to \mathbb{Z} \to 1$ splits, because to get a splitting we need a section $\iota : \mathbb{Z} \to G$, and since $\mathbb{Z}$ is a free group, there are no relations to satisfy: a section ι is determined simply by choosing any lift of $1 \in \mathbb{Z}$ to G. In the profinite case, we lift any topological generator of $\hat{\mathbb{Z}}$ to get a map $\iota : \mathbb{Z} \to \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and then ι extends uniquely to a continuous homomorphism on $\hat{\mathbb{Z}}$. We leave to the reader the task of checking this carefully and also verifying that the splitting of the sequence is equivalent to the existence of a totally ramified extension L/K such that K^{sep}/L is unramified. □

Remark: More generally, a profinite group H for which any short exact sequence

$$1 \to N \to G \to H \to 1$$

of profinite groups splits as a semidirect product is called **projective**. A profinite group is projective iff each of its Sylow p-subgroups are free pro-p-groups. In particular, most profinite groups are *not* projective. So far as I know, in general the short exact sequence

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \to \mathfrak{g}_k \to 1$$

need not split. It would be nice to know a specific example!

Exercise X.X (Requires more background): Suppose that K is a Henselian discrete valuation field with residue field k, and **assume** that the short exact sequence

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \to \mathfrak{g}_k \to 1$$

splits, i.e., that there exists a totally ramified field extension L/K such that K^{sep}/L is unramified.
a) (Serre-Tate) Let $A_{/K}$ be an abelian variety with potentially good reduction. Show that there exists a totally ramified extension L/K such that $A_{/L}$ has good reduction.
b) (Clark-Xarles) Deduce that there exists an injection $A(K)[\mathrm{tors}'] \hookrightarrow A(k)[\mathrm{tors}']$, where for an abelian group G, $G[\mathrm{tors}']$ means the subgroup of elements of order prime to the residue characteristic.